

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/348268266>

# Case Report of Email Spying

Article · June 2020

DOI: 10.24966/FLIS-733X/100046

---

CITATIONS

0

---

READS

328

1 author:



Rodrigo Ruiz

London Metropolitan University

62 PUBLICATIONS 87 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Security Assessment [View project](#)



LITERATURE REVIEW TOOL AND METHOD [View project](#)

(<https://www.heraldopenaccess.us/>)

☎ Contact (<https://www.heraldopenaccess.us/contact-us>)

f (<https://www.facebook.com/herald.open.92>)    t (<https://twitter.com/heraldopenaces>)

in (<https://www.heraldopenaccess.us/>)



📖 *Journal of Forensic Legal & Investigative Sciences*

📁 *Category: Forensic science*

📄 *Type: Case*

*Report*

## Case Report Of Email Spying

**Ruiz R<sup>1\*</sup>, Winter R<sup>2</sup>**

<sup>1</sup> CTI Renato Archer, Campinas, Department Of Crime, Research Institute In Campinas, Brazil

<sup>2</sup> Brazilian Army/UNICAMP, Department Of Crime, Brazil

### \*Corresponding Author:

Ruiz R

CTI Renato Archer, Campinas, Department Of Crime, Research Institute In Campinas, Brazil

**Tel:**+55 19 3746-6000,

**Email:**rodrigoruiz@outlook.com

**Received Date:** Mar 03, 2020

**Accepted Date:** Jun 03, 2020

**Published Date:** Jun 10, 2020

**DOI:**10.24966/FLIS-733X/100046 (<http://dx.doi.org/10.24966/FLIS-733X/100046>)

Abstract 

^

This case report is about Brazilian researchers that did have their e-mail invaded by Uk Ministry of Defence with cooperation from Microsoft Corp. The work show details of the invasion and steps that permitted this discovery.

## Keywords

*Cold War; Data Leakage; Email; MoD UK; Outlook; Privacy; Spy; Terrorism*

## INTRODUCTION

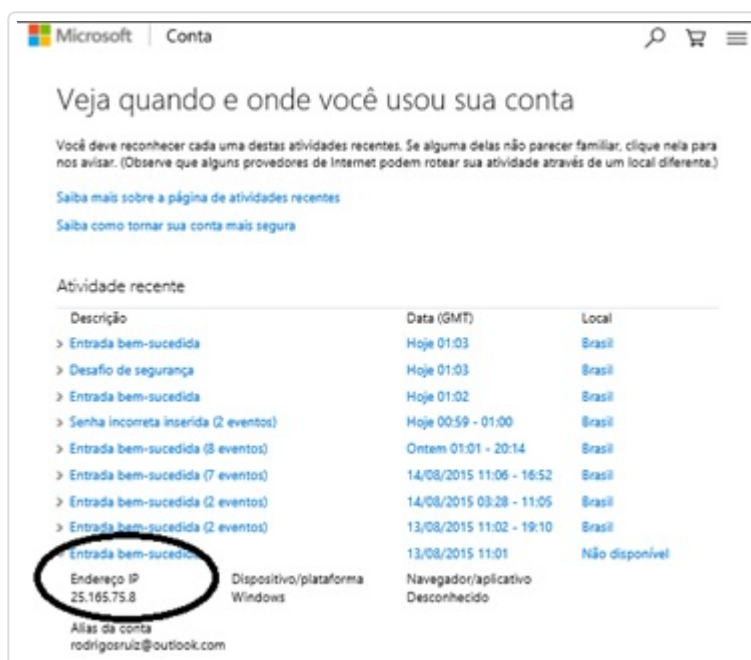
In times where the opponent was a state, as, during the Second World War, all efforts were made to ensure secure communication. During the war itself, the Allies deciphered the German encryption machine, beginning a real obsession with how to decode cyphers of the opponents and, at the same time, create powerful cyphers for their own use. The pigeons have been replaced by emails. Today, instant messages are the most common form of communication between companies, individuals and governments. In that fraction of a second between sending and receiving messages via email, who else will have access to them? In response, service operators include guarantees within their contracts about user privacy, along with the use of SSL [1] to protect communications.

James Bond 007, is also associated with real-life versions of the National Security Agency (NSA) of United States of America [2], the CIA [3] and the extinct KGB (FSB) [4]. Meanwhile, the Edward Snowden case [5] has resulted in geopolitical consequences for, as well as caused discomfort and financial damages among, former allies as evidence of espionage on a large scale are no longer limited to the declared enemy. After 9/11, the game of espionage changed again. Fear changed the way of life around the world. Privacy and confidentiality are characteristics, which, when lost, result in financial losses and demand a considerable effort to regain them, although recovery is virtually impossible. This issue is well characterized by Scheneier [6]. Society has opened up its privacy in exchange for the promise of more security. Who decides which particular individual should be the focus of monitoring focus, and in what form? In January 2015, the magazine Science published a special issue titled "The End of Privacy" [7]. Large companies are often blamed for providing data on people and institutions indiscriminately to governments without appropriate legal actions. As there are no effective means of control, businesses and individuals essentially depend on the trust that people have in these large companies that hold records on us. On 11<sup>th</sup> July 2013, the British newspaper The Guardian [8] published the contents of top-secret documents, showing that Microsoft works in conjunction with the NSA and the FBI, helping these agencies to circumvent new encryption procedures in its products, including Outlook. Microsoft was given the right to reply by the newspaper: "We have clear principles which guide the response across our

entire company to government demands for customer information for both law enforcement and national security issues. First, we take our commitments to our customers and to compliance with applicable law very seriously, so we provide customer data only in response to legal processes.”

## THE GAME'S AFOOT

Despite our indignation towards this breach in our email security, rather than scare the hacker, we decided to exploit the situation and expand our knowledge of email privacy. During the first months of 2015, email communications were made using controlled messages in order to protect the integrity of our research, while our curiosity about the hacker continued to increase. By monitoring the situation, we obtained Outlook access reports (see Figure 1). As can be seen in Table 1, IP address properties were established through consultations with ARIN [9] and RIPE.net Figure 1 [10].



Microsoft Conta

Veja quando e onde você usou sua conta

Você deve reconhecer cada uma destas atividades recentes. Se alguma delas não parecer familiar, clique nela para nos avisar. (Observe que alguns provedores de Internet podem rotear sua atividade através de um local diferente.)

Saiba mais sobre a página de atividades recentes

Saiba como tornar sua conta mais segura

Atividade recente

Descrição	Data (GMT)	Local
> Entrada bem-sucedida	Hoje 01:03	Brasil
> Desafio de segurança	Hoje 01:03	Brasil
> Entrada bem-sucedida	Hoje 01:02	Brasil
> Senha incorreta inserida (2 eventos)	Hoje 00:59 - 01:00	Brasil
> Entrada bem-sucedida (8 eventos)	Ontem 01:01 - 20:14	Brasil
> Entrada bem-sucedida (7 eventos)	14/08/2015 11:06 - 16:52	Brasil
> Entrada bem-sucedida (2 eventos)	14/08/2015 03:28 - 11:05	Brasil
> Entrada bem-sucedida (2 eventos)	13/08/2015 11:02 - 19:10	Brasil
> Entrada bem-sucedida	13/08/2015 11:01	Não disponível
Endereço IP 25.165.75.8	Dispositivo/plataforma Windows	Navegador/aplicativo Desconhecido

Alias da conta  
rodrigossruiz@outlook.com

**Figure 1:** Microsoft Outlook® access report and IP 25.165.75.8, which is the property of the UK’s Ministry of Defence.

The password used to protect the account assigned at the time of the incidents was regarded as “strong,” that is, it contained a great number of numbers, upper and lower case letters, and special characters, which is a format typically used in IT (e.g., “f5Gr\$ekslanhjo”). It would be unthinkable that a corporation, which is one of the symbols of America, would be institutionally involved with an unfriendly foreign government. During recent years, the entire world’s media has regularly referred to the NSA in the context of any espionage action, control and invasion of privacy against people, businesses and governments around the world.

These reports have also shown that there is at least another player in the game, the UK, as seen in Figures 2 and 3, Table 1. The evidence, which is indisputable, point to actions of the UK in the USA, specifically in Microsoft. In the search for an answer, we contacted the UK's Ministry of Defence [11], who was evasive in response, as can be seen in Figure 3. When the UK Government answers by saying, "We do not confirm and we do not deny," it alerts everyone to the privacy and security of the UK's business, industrial and scientific secrets.

<b>Date/time</b>	<b>IP</b>	<b>Owner</b>	<b>Local</b>
15-01-2015 13:22	157.56.238.188	Microsoft Corporation	Redmond
29-01-2015 14:39	132.245.80.92	Microsoft Corporation	Redmond
02-02-2015 04:10	132.245.32.12	Microsoft Corporation	Redmond
02-02-2015 04:10	132.245.32.11	Microsoft Corporation	Redmond
03-02-2015 04:49	132.245.11.4	Microsoft Corporation	Redmond
03-02-2015 14:15	132.245.32.4	Microsoft Corporation	Redmond
09-02-2015 12:15	198.11.246.181	Softlayer/F-Secure	Chantilly/ Washington
20-03-2015 10:41	25.163.90.11	Ministry of Defence, UK	London
20-03-2015 16:46	25.160.164.153	Ministry of Defence, UK	London
31-07-2015 20:04	25.165.74.23	Ministry of Defence, UK	London
13-08-2015 11:01	25.165.75.8	Ministry of Defence, UK	London
30-10-2015 09:24	25.165.118.133	Ministry of Defence, UK	London
27-11-2015 11:28	25.165.74.25	Ministry of Defence, UK	London

**Table 1:** List of IP addresses through which the email account was accessed improperly accessed. ^

apps.db.ripe.net/search/query.html?searchtext=25.165.74.24#resultsAnchor

### Search results

This is the RIPE Database search service. The objects are in RPSL format. The RIPE Database is subject to Terms and Conditions.

Abuse contact info: [hostmaster@mod.uk](mailto:hostmaster@mod.uk)

```
inetnum:      25.0.0.0 - 25.255.255.255
netname:      UK-MOD-19850128
descr:        UK Ministry of Defence
country:      GB
org:          ORG-DMO01-RIPE
admin-c:      PN1891-RIPE
tech-c:       PN1891-RIPE
status:       LEGACY
notify:       hostmaster@mod.uk
mnt-by:       UK-MOD-MNT
mnt-domains:  UK-MOD-MNT
mnt-routes:   UK-MOD-MNT
mnt-by:       RIPE-NCC-LEGACY-MNT
changed:      hostmaster@ripe.net 20050823
changed:      hostmaster@ripe.net 20060426
```

**Figure 2:** The RIPE Network Coordination Centre, the organization responsible for coordinating IP registries in Europe, assigns the range 25.0.0.0 to 25,255,255,255 to the UK's Ministry of Defence.

Ministry of Defence  
Main Building (02/M)  
Whitehall  
London SW1A 2HB  
United Kingdom

Telephone: +44 (0)20 7218 9000

E-mail: [ISSHQ-MB-GroupMailbox@mod.uk](mailto:ISSHQ-MB-GroupMailbox@mod.uk)

Ref. TO\_2015\_06

Mr Rodrigo Ruiz  
[rodrigosruiz@outlook.com](mailto:rodrigosruiz@outlook.com) 29 June 2015

Mr Ruiz,

Thank you for your email dated 6 June 2015 to the Ministry of Defence. As the Information Systems and Services (responsible for the delivery of Defence Information and Communications Technology) point of contact within the Department, it falls to me to respond.

Having considered the information provided in your email, we would recommend that any concerns over the possible hacking of your Outlook account should be raised directly with Microsoft.

Yours sincerely,

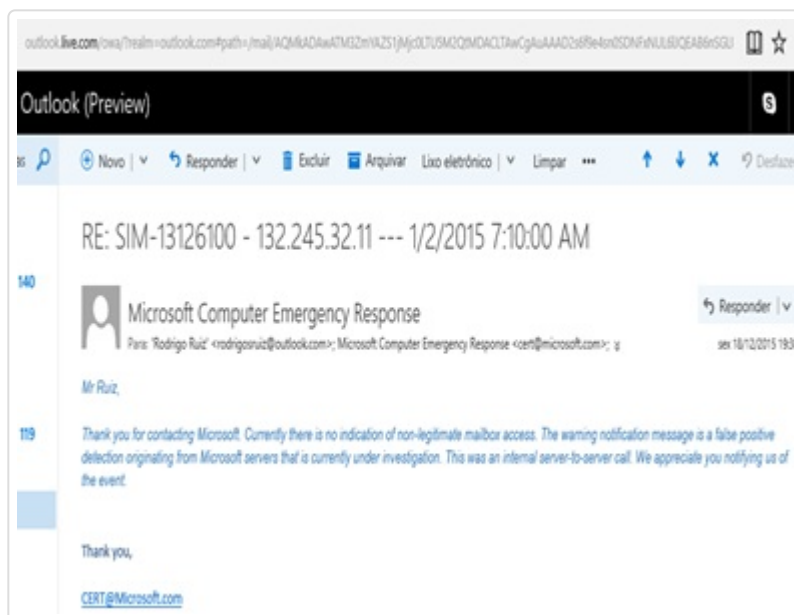
ISS HQ-MB Secretariat

**Figure 3:** Response from the UK's Ministry of Defence when asked if it authorized the intrusion into the researcher's email account or whether its own computers had been hacked by third parties, thereby allowing access.

When questioned about these incidents, Microsoft [12] provided the following protocols: 1076B89D; 9023A4AE; 4FB0DD02; B860A2E9; 102FD43B. On 18 December 2015, Microsoft Computer Emergency Response provided the response as shown in Figure 4. When Microsoft declared that the access simply involves a Microsoft server-to-server call, we might ask the following:

1. Are Microsoft Outlook servers embedded in the UK's Ministry of Defence infrastructure? If so, why?

2. In Figure 6, we present an example of human interaction in Washington DC in which a user typed in a wrong password a few days before London received access to the email account. Why would Microsoft imagine that an automated server system would type in wrong passwords?

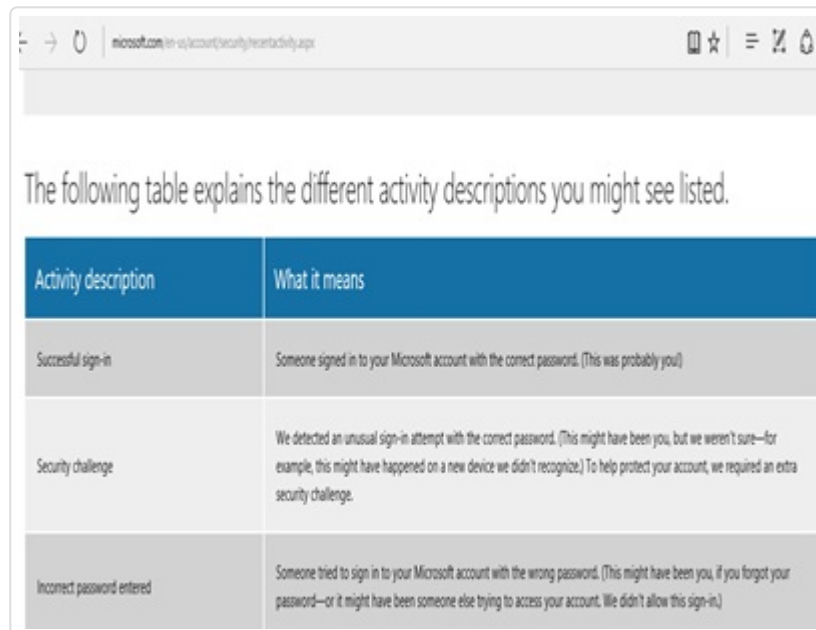


**Figure 4:** Microsoft’s response that the incident in question is just a false positive with regard to its own server-to-server communications: “Thank you for contacting Microsoft. Currently, there is no indication of non-legitimate mailbox access. The warning notification message is a false positive detection originating from Microsoft servers that are currently under investigation. This was an internal server-to-server call. We appreciate you notifying us of the event.”

This answer does not correspond to the information that Microsoft published on its site [12] about the security and privacy of Outlook Figures 5,6 and 7. On the same page Microsoft, says:

“When you tell us that you don’t recognize an activity, it’s possible that a hacker or a malicious user has gotten access to your account. To help protect your account, we’ll walk you through several steps, including changing your password and reviewing and updating your security info.”

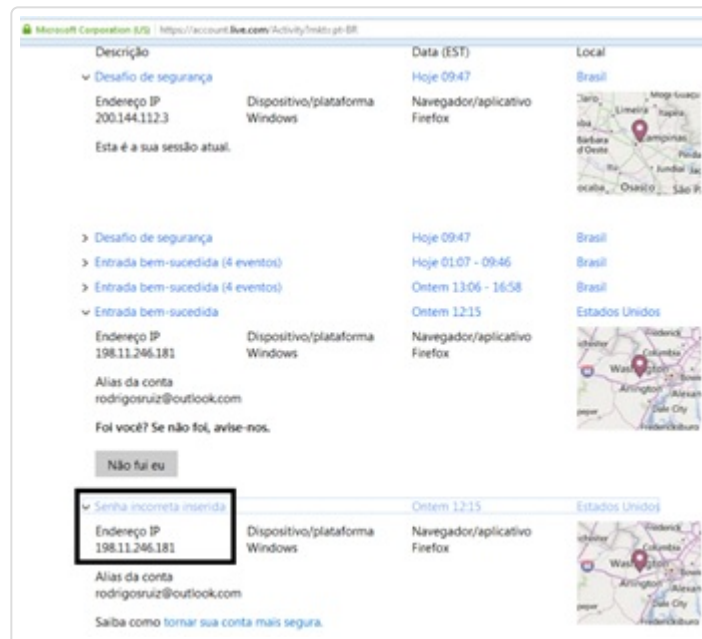




The following table explains the different activity descriptions you might see listed.

Activity description	What it means
Successful sign-in	Someone signed in to your Microsoft account with the correct password. (This was probably you)
Security challenge	We detected an unusual sign-in attempt with the correct password. (This might have been you, but we weren't sure—for example, this might have happened on a new device we didn't recognize.) To help protect your account, we required an extra security challenge.
Incorrect password entered	Someone tried to sign in to your Microsoft account with the wrong password. (This might have been you, if you forgot your password—or it might have been someone else trying to access your account. We didn't allow this sign-in.)

**Figure 5:** Microsoft describes on the user's page [12] the different activities relating to an Outlook access report.

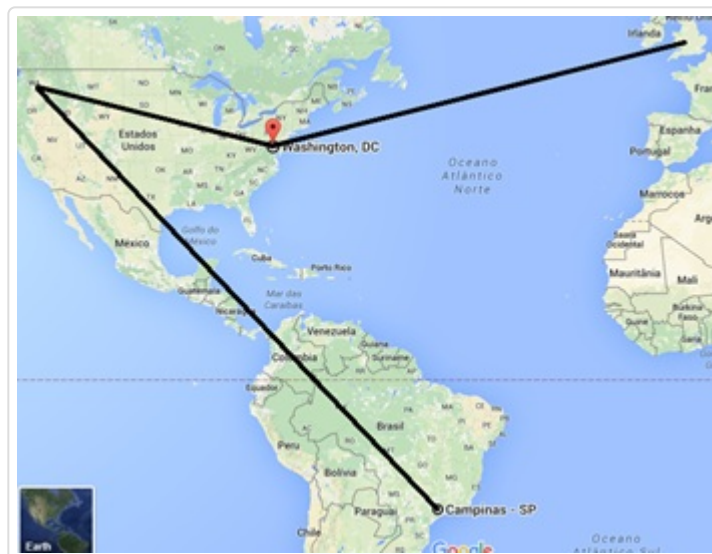


Descrição	Data (EST)	Local
<ul style="list-style-type: none"> <li>Desafio de segurança</li> <li>Endereço IP: 200.144.112.3</li> <li>Dispositivo/plataforma: Windows</li> <li>Navegador/aplicativo: Firefox</li> <li>Esta é a sua sessão atual.</li> </ul>	Hoje 09:47	Brasil
<ul style="list-style-type: none"> <li>Desafio de segurança</li> <li>Entrada bem-sucedida (4 eventos)</li> <li>Entrada bem-sucedida (4 eventos)</li> <li>Entrada bem-sucedida</li> <li>Endereço IP: 198.11.246.181</li> <li>Dispositivo/plataforma: Windows</li> <li>Navegador/aplicativo: Firefox</li> <li>Alias da conta: rodrigosruiz@outlook.com</li> <li>Foi você? Se não foi, avise-nos.</li> <li><input type="button" value="Não fui eu"/></li> <li>Senha incorreta inserida</li> <li>Endereço IP: 198.11.246.181</li> <li>Dispositivo/plataforma: Windows</li> <li>Navegador/aplicativo: Firefox</li> <li>Alias da conta: rodrigosruiz@outlook.com</li> <li>Saiba como tornar sua conta mais segura.</li> </ul>	Hoje 09:47 Hoje 01:07 - 09:46 Ontem 13:06 - 16:58 Ontem 12:15	Brasil Brasil Brasil Estados Unidos

**Figure 6:** A wrong password was typed in by a human in Washington DC a few days before London got access to the email account. “Senha incorreta inserida” is Portuguese for “Wrong password typed”.







**Figure 7:** The way of shame, starting in Brazil, where the real user accessed their webmail and where the hacking took place in Microsoft, connecting in Washington DC and finally arriving in London. Image from Google Maps.

## MORE QUESTIONS THAN ANSWERS

What are the conditions that might have led to the UK becoming involved in this incident? Or was the UK Government also a victim, ashamed to admit that it had been hacked? And did Microsoft fall prey to one of its employees? What is the impact of this type of espionage in the world on researchers and the general public? Are thousands of researchers vulnerable to the shady methods and almost unlimited resources of organized hackers? How many patents are at risk? Is the crime no longer about stealing, but simply getting caught? The Los Angeles Times reported in 2001 that the relationship between scientific research and intelligence agencies did not cool off after the Cold War as previously thought. But, while these researchers continue to fully cooperate with their intelligence masters [13], they should not forget that the same person who pays the wages of these scientists may also be reading their emails on a daily basis.

## REFERENCES

1. What is SSL? (2019) SSL and Digital certificates, SSL/TLS. (<http://info.ssl.com/article.aspx?id=10241>)
2. National Security Agency central security service, USA. (<https://www.nsa.gov/>)
3. Central Intelligence Agency, Washington, D.C, USA. (<https://www.cia.gov/index.html>)
4. The russian government, Federal Security Service, Russia. (<http://government.ru/en/department/113/>)
5. NSA FILES DECODED, What the revelations means for you. (<http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations->

decoded)

6. Schneier B (2012) Securing Medical Research: A Cybersecurity Point of View. Science 336: 1527-1529. (<https://science.sciencemag.org/content/336/6088/1527>)
  7. The end of privacy (2015). Science AAAS. (<http://www.sciencemag.org/site/special/privacy/index.xhtml>)
  8. Microsoft handled the NSA access to encrypted messages. (<https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data>)
  9. American registry for internet numbers. (<https://www.arin.net/>)
  10. Ripe Network Co-Ordination Center. (<https://www.ripe.net/support/contact>)
  11. Ministry of Defence UK. (<https://www.gov.uk/government/organisations/ministry-of-defence>)
  12. What is the recent activity page? Microsoft (2015). (<https://support.microsoft.com/en-us/help/13782/microsoft-account-what-is-the-recent-activity-page>)
  13. Academics and Spies: The Silence that roars, USA. (<http://articles.latimes.com/2001/jan/28/opinion/op-18012>)
- 

**Citation:** Ruiz R, Winter R (2020) Case Report of Email Spying. Forensic Leg Investig Sci 6: 046.

**Copyright:** © 2020 Ruiz R, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

## ABOUT HERALD

Herald Scholarly Open Access is a leading, international publishing house in the fields of Sciences. Our mission is to provide an access to knowledge globally.

## SOCIAL LINKS


[f](#) [t](#) [in](#)


## NEWSLETTER





Email Address 

## CONTACT US

 2561 Cornelia Rd, #205, Herndon, VA 20171, UNITED STATES

 Phone: +1 202-499-9679

 Fax: +1 202-217-4195

 Email: [contact@heraldsopenaccess.us](mailto:contact@heraldsopenaccess.us)

