Ruiz R and Winter R, J Forensic Leg Investig Sci 2020, 6: 046
DOI: 10.24966/FLIS-733X/100046

HSOA Journal of Forensic, Legal & Investigative Sciences

Case Report

Case Report of Email Spying

Ruiz R[1]* and Winter R[2]

[1]CTI Renato Archer, Campinas, Department of Crime, Brazil

[2]Brazilian Army/UNICAMP, Department of Crime, Brazil

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 The pigeons have been replaced by emails.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 11th 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].

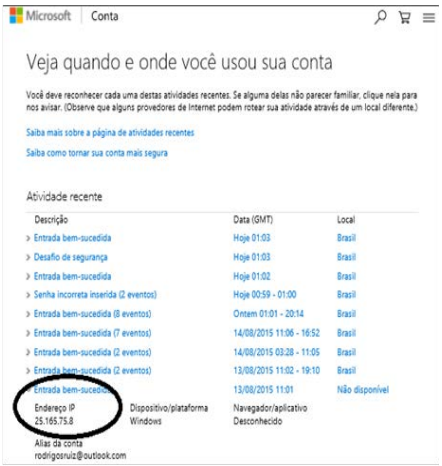

Figure 1: Microsoft Outlook® access report and IP 25.165.75.8, which is the property of the UK's Ministry of Defence.

***Corresponding author:** Ruiz R, Department of Crime, Research Instuite in Campinas, Brazil, Tel: +55 19 3746-6000; E-mail: rodrigosruiz@outlook.com

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

Received: March 03, 2020; **Accepted:** June 03, 2020; **Published:** June 10, 2020

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.

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.

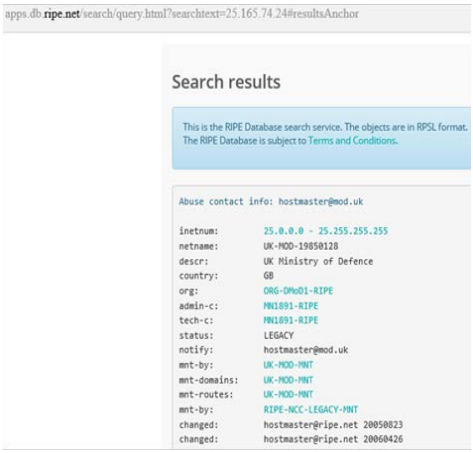

Figure 2: The RIPE Network Coordination Centre, the organization responsible for coordinating IP registries in Europe, assigns the range 25.0.0.0 to 25,255,255,255 to the UK's Ministry of Defence.

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 5, 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?

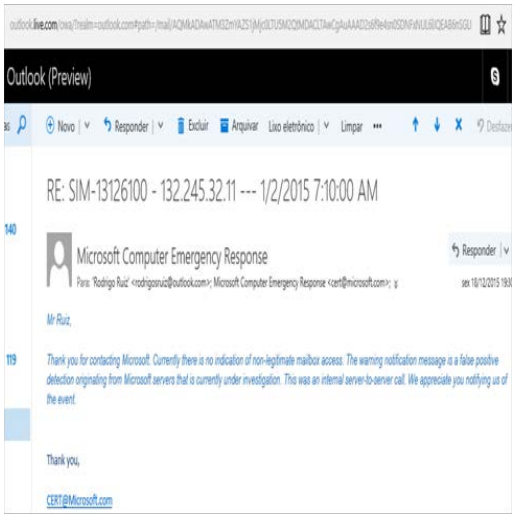

Figure 4: Microsoft's response that the incident in question is just a false positive with regard to its own server-to-server communications: "Thank you for contacting Microsoft. Currently, there is no indication of non-legitimate mailbox access. The warning notification message is a false positive detection 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."

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

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."

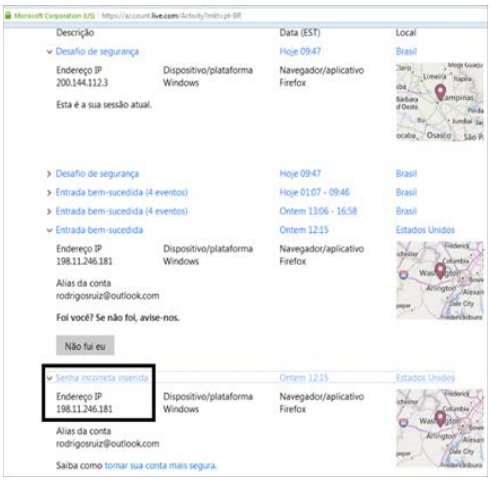

Figure 6: A wrong password was typed in by a human in Washington DC a few days before London got access to the email account. "Senha incorreta inserida" is Portuguese for "Wrong password typed".

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.

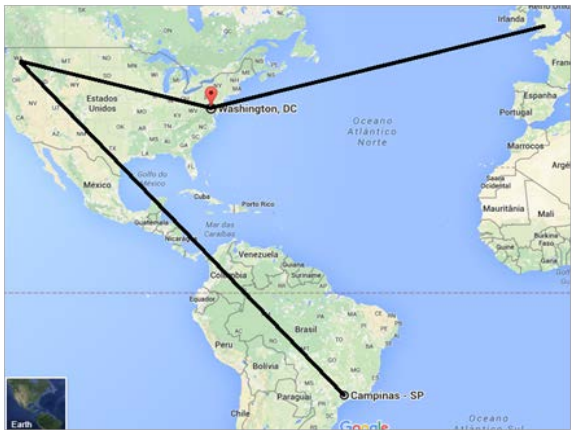

Figure 7: The way of shame, starting in Brazil, where the real user accessed their webmail and where the hacking took place in Microsoft, connecting in Washington DC and finally arriving in London. Im-age from Google Maps.

References

1. What is SSL? (2019) SSL and Digital certificates, SSL/TLS.
2. National Security Agency central security service, USA.
3. Central Intelligence Agency, Washington, D.C, USA.
4. The russian governoment, Federal Security Service, Russia.
5. NSA FILES: DECODED, What the revelations means for you.
6. Schneier B (2012) Securing Medical Research: A Cybersecurity Point of View. Science 336: 1527-1529.
7. The end of privacy (2015). Science AAAS.
8. Microsoft handled the NSA access to encrypted messages.
9. American registery for internet numbers.
10. Ripe Network Co-Ordination Center.
11. Ministry of Defence UK.
12. What is the recent activity page? Microsoft (2015).
13. Academics and Spies: The Silence that roars, USA.

HERALD

Advances In Industrial Biotechnology | ISSN: 2639-5665

Advances In Microbiology Research | ISSN: 2689-694X

Archives Of Surgery And Surgical Education | ISSN: 2689-3126

Archives Of Urology

Archives Of Zoological Studies | ISSN: 2640-7779

Current Trends Medical And Biological Engineering

International Journal Of Case Reports And Therapeutic Studies | ISSN: 2689-310X

Journal Of Addiction & Addictive Disorders | ISSN: 2578-7276

Journal Of Agronomy & Agricultural Science | ISSN: 2689-8292

Journal Of AIDS Clinical Research & STDs | ISSN: 2572-7370

Journal Of Alcoholism Drug Abuse & Substance Dependence | ISSN: 2572-9594

Journal Of Allergy Disorders & Therapy | ISSN: 2470-749X

Journal Of Alternative Complementary & Integrative Medicine | ISSN: 2470-7562

Journal Of Alzheimers & Neurodegenerative Diseases | ISSN: 2572-9608

Journal Of Anesthesia & Clinical Care | ISSN: 2378-8879

Journal Of Angiology & Vascular Surgery | ISSN: 2572-7397

Journal Of Animal Research & Veterinary Science | ISSN: 2639-3751

Journal Of Aquaculture & Fisheries | ISSN: 2576-5523

Journal Of Atmospheric & Earth Sciences | ISSN: 2689-8780

Journal Of Biotech Research & Biochemistry

Journal Of Brain & Neuroscience Research

Journal Of Cancer Biology & Treatment | ISSN: 2470-7546

Journal Of Cardiology Study & Research | ISSN: 2640-768X

Journal Of Cell Biology & Cell Metabolism | ISSN: 2381-1943

Journal Of Clinical Dermatology & Therapy | ISSN: 2378-8771

Journal Of Clinical Immunology & Immunotherapy | ISSN: 2378-8844

Journal Of Clinical Studies & Medical Case Reports | ISSN: 2378-8801

Journal Of Community Medicine & Public Health Care | ISSN: 2381-1978

Journal Of Cytology & Tissue Biology | ISSN: 2378-9107

Journal Of Dairy Research & Technology | ISSN: 2688-9315

Journal Of Dentistry Oral Health & Cosmesis | ISSN: 2473-6783

Journal Of Diabetes & Metabolic Disorders | ISSN: 2381-201X

Journal Of Emergency Medicine Trauma & Surgical Care | ISSN: 2378-8798

Journal Of Environmental Science Current Research | ISSN: 2643-5020

Journal Of Food Science & Nutrition | ISSN: 2470-1076

Journal Of Forensic Legal & Investigative Sciences | ISSN: 2473-733X

Journal Of Gastroenterology & Hepatology Research | ISSN: 2574-2566

Journal Of Genetics & Genomic Sciences | ISSN: 2574-2485

Journal Of Gerontology & Geriatric Medicine | ISSN: 2381-8662

Journal Of Hematology Blood Transfusion & Disorders | ISSN: 2572-2999

Journal Of Hospice & Palliative Medical Care

Journal Of Human Endocrinology | ISSN: 2572-9640

Journal Of Infectious & Non Infectious Diseases | ISSN: 2381-8654

Journal Of Internal Medicine & Primary Healthcare | ISSN: 2574-2493

Journal Of Light & Laser Current Trends

Journal Of Medicine Study & Research | ISSN: 2639-5657

Journal Of Modern Chemical Sciences

Journal Of Nanotechnology Nanomedicine & Nanobiotechnology | ISSN: 2381-2044

Journal Of Neonatology & Clinical Pediatrics | ISSN: 2378-878X

Journal Of Nephrology & Renal Therapy | ISSN: 2473-7313

Journal Of Non Invasive Vascular Investigation | ISSN: 2572-7400

Journal Of Nuclear Medicine Radiology & Radiation Therapy | ISSN: 2572-7419

Journal Of Obesity & Weight Loss | ISSN: 2473-7372

Journal Of Ophthalmology & Clinical Research | ISSN: 2378-8887

Journal Of Orthopedic Research & Physiotherapy | ISSN: 2381-2052

Journal Of Otolaryngology Head & Neck Surgery | ISSN: 2573-010X

Journal Of Pathology Clinical & Medical Research

Journal Of Pharmacology Pharmaceutics & Pharmacovigilance | ISSN: 2639-5649

Journal Of Physical Medicine Rehabilitation & Disabilities | ISSN: 2381-8670

Journal Of Plant Science Current Research | ISSN: 2639-3743

Journal Of Practical & Professional Nursing | ISSN: 2639-5681

Journal Of Protein Research & Bioinformatics

Journal Of Psychiatry Depression & Anxiety | ISSN: 2573-0150

Journal Of Pulmonary Medicine & Respiratory Research | ISSN: 2573-0177

Journal Of Reproductive Medicine Gynaecology & Obstetrics | ISSN: 2574-2574

Journal Of Stem Cells Research Development & Therapy | ISSN: 2381-2060

Journal Of Surgery Current Trends & Innovations | ISSN: 2578-7284

Journal Of Toxicology Current Research | ISSN: 2639-3735

Journal Of Translational Science And Research

Journal Of Vaccines Research & Vaccination | ISSN: 2573-0193

Journal Of Virology & Antivirals

Sports Medicine And Injury Care Journal | ISSN: 2689-8829

Trends In Anatomy & Physiology | ISSN: 2640-7752