

Devin Nunes, Chairman
Permanent Select Committee on Intelligence
U.S. House of Representatives
U.S. Capitol Building
WASHINGTON, DC 20515-6415

Richard Burr, Chairman
Permanent Select Committee on Intelligence
U.S. Senate
211 Hart Senate Office Building
WASHINGTON, DC 20515

Satya Nadella, Chief Executive Officer
Microsoft Corporation
1 Microsoft Way
REDMOND, WA 98052

Vice Adm. Nancy A. Norton, Director
Defense Information Systems Agency
DISA.MEADE.BD.MBX.BDM1-AGENCY-FEDERAL@MAIL.MIL
FORT MEADE, MD

Christopher A. Wray, Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
WASHINGTON, DC 20535-0001

Lewis M. Eisenberg, Ambassador
U.S. Embassy Rome
Via Vittorio Veneto 121
00187 ROME, ITALY

GOVERNMENT-SPONSORED CYBER THREAT

Monday, February 19, 2018

Dear Sirs,

my name is Giulio Occhionero and I am an Italian nuclear engineer and a financial professional. I am writing today to expose criminal activity on the part of Italian governmental authorities: **Polizia Postale** and its special cyber division **CNAIPIC** against US and Italian citizens as well as a US company with interests in the US and Italy, **Westlands Securities**.

Over the last year, I have been involved in a complex criminal case along with my sister Francesca Occhionero, who is a US citizen. I am referring to Italian cyber criminal case of **Procura della Repubblica di Roma, n. 21245/2016** in which we think we have been involved also because of our connections to the US.

Material evidence arising in this case suggests that a **continued activity of hacking** into US information servers has been conducted by the above authorities over a period of several years. It also emphasizes an attack technique aimed to hack into US computer systems which impersonates the digital identity of **Microsoft**. Additional evidence finally points into the direction of **industrial espionage** purposes and a potential will to **interfere with public affairs** in the United States.

THE ATTACK

During the investigation phase, Procura di Roma, under the direction of public prosecutor **Eugenio Albamonte** and chief prosecutor **Giuseppe Pignatone**, has employed, with the cooperation of ISP Telecom Italia Mobile (TIM), a technique, aimed at delivering a Trojan to my computer. This technique relies on the impersonation of **Microsoft's** digital identity, and it is acted by the use of a bogus Microsoft website and certificate.

The attack in question is based on inducing a user to download a false update for Microsoft SQL Server; which I in fact downloaded, getting infected by the Trojan.

In this regard, it is important to mention that I was, and I currently am, a Domain Administrator in the **Westlands Securities'** Active Directory Domain, a US Limited Liability Company whose Domain Controllers were based respectively on the East and West coasts of the United States. These servers also ran several virtual servers that maintained services of multiple kinds such as email, file shares and websites; including hosting mail services for Westlands' clients in the US and Italy.

While the attack was conducted against my desktop computer, it was designed to take control of the global Active Directory Domain. This was later attempted on **October 5, 2016** by CNAIPIC officers in my presence, shortly before launching a planned major national criminal case, now named **EyePyramid**, whose relevant press you can retrieve here:

<https://news.google.com/news/search/section/q/eyepyramid/eyepyramid?hl=en&gl=US&ned=us>

Materially, on the evening of **September 29, 2016** I was working at my desktop in Rome when, on launching **SQL Server Management Studio**, I was notified by a tray pop-up about the availability of an update for SQL Server 2014. On clicking on the pop-up balloon, I was in fact redirected to the mentioned bogus Microsoft website from which I downloaded the infected update, bundled with the Trojan. This part surely involved the cooperation of the ISP; as only techniques like IP translation and DNS manipulation could have led to a similar redirection.

One of the most alarming issues of this case is the fact that, as mentioned in the paperwork of the file, I even checked the validity of the https certificate, after doing the download. Suspects loomed on me for the fact that the downloaded executable was unsigned. However, being the website certificate valid, I proceeded to install the supposed update, assuming a wrong scenario of a legitimate though unsigned file.

Subsequent to its install, the Trojan begun collecting credentials from my computer and transmitting them to the servers of **Polizia Postale Italiana**, along with screenshots of my sessions, keylogs and other information. Some evidence of this activity appeared immediately clear to me, as on our network we employ tools designed to detect attacks and notify them. On booting my laptop on the same home LAN of the infected desktop, the former immediately notified being attacked by some actor on the LAN. This further evidences the intention to propagate the attack deeper into the Active Directory Domain.

A few days later, on **October 5 2016**, the agents of **CNAIPIC**, equipped with the stolen credentials, raided my house for a search and, in that occasion, they tried, in my presence, from their mobile computers, to log into our Domain Controllers to take ownership of them.

My reminding them as to what the legal consequences for the US Justice Department would be, for such a conduct, were ignored while they proceeded to several hacking attempts via Remote Desktop. In these attempts, they tried the many stolen credentials they had gathered, but they all failed because of the domain-wide Group Policies that restricted access to smartcards, sided by other security requirements.

This type of attack has *specifically* been designed to gain illegal access by a peripheral member of an Active Directory Domain, and then potentially using his **credentials or Kerberos ticket** to move to inner servers and to their resources. Therefore, penetration onto the US, or another foreign ground, begins by an attack done on the *Italian* ground.

Following my release from jail, I have begun inspecting the files of the case and I am writing a software tool named Valiriya which is mining data and producing additional forensic evidence. Results show that the prosecutors in Rome were in possession of data and files illegally gained by hacking into free email and file share services, in both the US and Germany, for years.

These services include **GMX, Storegate, Strato, Box and 4Shared** (at least), while the practice of hacking into them, with no authorization, begins (at least) in April 2015 and goes on to (at least) February 2016.

A new hypothesis of illegal hacks into **Irish servers** is now surfacing; and we will notify the prosecutors if it materializes.

ROLE OF THE ITALIAN GOVERNMENT

The above technique must be deemed **highly critical** because it entails the cooperation of an ISP, in order to succeed. This requires the intervention of a government agency, whose authority is needed to obligate the ISP to cooperate; at least during the phase of infection.

Because of the very facts above, and those that followed in this bold case, I decided to inform **COPASIR**; the **Italian Parliamentary Commission on Intelligence Services** whose responsibility is, among others, to ensure that no member of any Italian armed or police force can ever engage in acts that can be deemed *hostile* against a foreign country; without an appropriate governmental mandate to do so.

After the arrest of my sister Francesca and me on **January 9, 2017**, I also decided to inform the Italian **Minister of Interior Marco Minniti** and the **Ministry of Defense Roberta Pinotti**. Certified emails were sent to them by our lawyers, and they will be eventually available to you.

I also notified the **US Embassy in Rome** writing several emails to **Mr. Domenico Taliani**, in which I detailed the **facts**, some **technicalities** of the attacks and the potential **risks** it all emphasized. This also included risks for US citizens merely travelling to Italy and potentially being attacked because of their being a gate to US corporate resources.

My final act to prosecute the above was that of **filing a criminal case with Procura di Perugia** which is the one allowed to investigate crimes committed by prosecutors at Procura di Roma, by their police investigators and by their consultants. At the time of this writing, I have been interrogated twice by Procura di Perugia; the first time in **June 2017** and the last in **January 2018**, for more than five hours.

Prosecutor **Eugenio Albamonte** and two members of **CNAIPIC** are now under investigation for several crimes and we are awaiting developments. I also think that while **CNAPIC** has sought and obtained cooperation from the **US Department of Justice** on this case, in order to seize our servers in May 2017 and have them handed over, CNAIPIC has never disclosed its practice of hacking into US information servers to the FBI.

INDUSTRIAL ESPIONAGE

While the real aims of Procura di Roma and CNAIPIC must be further investigated, we suspect that one of their intentions was that of **gaining possession of Westlands Securities's corporate documental and data baseline**. In previous years CNAIPIC had in fact already been involved in other corporate espionage cases left with no satisfactory explanation, nor with any significant counter-measure ever taken by the Italian Government. However, being CNAIPIC a mere police force, and not an intelligence agency, any such kind of activity clearly falls far outside of its mandate.

The global hackers group **Anonymous** had already shown in **2011** that CNAPIC was in possession of files and data illegally gained by the **Russian** oil company **Gazprom** and the **Indian Embassy in Rome**.

In our case, we suspect that the core industrial interest in getting Westlands' corporate documents was the Taranto Harbor project. This project, notoriously followed by **Westlands Securities** and its US partner company **Automated Terminal Systems**, aimed at realizing the largest container terminal in the Mediterranean. Westlands filed a criminal complaint years ago for supposed wrongdoings at the Port Authority which led to arrests. While the project was seen with favor by the **US Department of Commerce** and by the **US Ambassador to Italy Mel Sembler**, Italian local

governmental authorities wanted it to be withdrawn in favor of other carriers in the Port. This all could well have happened in retaliation for that complaint.

INTERFERENCE IN THE PUBLIC AFFAIRS OF THE UNITED STATES

Another item needing deeper attention is the kind of cooperation provided to **Polizia Postale Italiana** and **Procura di Roma** by the **FBI** and the **US Department of Justice**. In fact, while the FBI is supposed to have helped on a *bona-fide* basis, it is appalling that it has failed to detect the daily hacking practices of CNAIPIC and its consultants into US information servers.

In a similar fashion, the US Department of Justice has handed over our servers to CNAIPIC without ever realizing that they had never done a single illegal access to any other server on the web; as it is clearly surfacing in trial. Moreover, upon being called to testify in court, the FBI attaché to the US Embassy in Rome, **Kieran Ramsey**, has communicated his intention not to show up, by sending a lawyer invoking such right. This is apparently contemplated under US-Italian justice cooperation agreements.

In this regard, it is furthermore impossible not to notice that the press covering this case outside of Italy happens to be the same journalists at **The Guardian** who kept rolling out the **Russiagate** story, which reveals a potential attempt to interfere with US affairs by another pre-fabricated dossier, possibly authorized at the highest levels of Italian government. The only difference in this case is that the source to The Guardian was the head of Polizia Postale **Roberto Di Legami**, with or without an FBI middleman.

BOTTOM LINES

The matter above, as an Italian citizen, raised a severe alert on me, pushing me into the direction I took; as it is more than clear that such a behavior by a national police force does lead to corporate damages also for those Italian companies who side with CNAIPIC.

In my opinion, while the facts and circumstances above do underline a major threat to the security of US and other foreign cyber spaces, they also deserve further attention for a number of related issues. These issues involve the friendly relationships of Italy with other European Community partners and, most of all, with its **NATO** allies.

I therefore wanted to bring it to the attention of those who are concerned with security.

OUR LAWYERS:

Roberto Bottacchiari

Via Oslavia 28

00195 Rome, ITALY

robertobottacchiari@ordineavvocatiroma.org

Office +39 (06) 37351107

Mobile +39 (335) 676-2334

Stefano Parretta

Piazzale Clodio 12

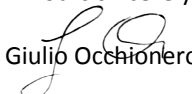
00195 Rome, ITALY

stefanoparretta@ordineavvocatiroma.org

Office +39 (06) 3751-3292

Mobile +39 (335) 657-2460

Yours sincerely,


Giulio Occhionero

Giulio Occhionero

Via di Vigna Stelluti 176

00191 Rome, ITALY

giulio.occhionero@gmail.com

Home +39 (06) 329-7771

Mobile +39 (347) 238-4800