APT28: Cybercrime or State-sponsored Hacking?

POSTED IN GENERAL SECURITY, HACKING ON JUNE 4, 2015

SHARE

Once upon the APT28

In October of 2014, the security firm FireEye published a report that revealed the existence of a group of Russian hackers, dubbed APT28, which managed a long-running cyber espionage campaign on US defense contractors, European security organizations and Eastern European government entities.

The hackers also targeted the attendees of European defense exhibitions, including the EuroNaval 2014, EUROSATORY 2014, and the Counter Terror Expo and the Farnborough Airshow 2014.

The majority of the files analyzed by FireEye were set to Russian language settings; this circumstance suggests, "that a significant portion of APT28 malware was compiled in a Russian-language build environment consistently over the course of six years."

As usually happens in these cases, in order to profile the attacker the researchers analyzed compile times and discovered that they were aligned with working hours in Moscow and St. Petersburg, another element that suggests the involvement of a Russia-based team. Nearly 96 percent of the malware was compiled between a Monday and Friday during an 8 AM to 6 PM workday in the Moscow time zone.

The researchers at FireEye analyzed the malicious code used by the APT28 group and their "modus operandi," the investigation lead the experts to link the APT group with the Russian Government. The APT group "does not appear to conduct widespread intellectual property theft for economic gain, but instead is focused on collecting intelligence that would be most useful to a government."

"APT28 appeared to target individuals affiliated with European security organizations and global multilateral institutions. The Russian government has long cited European security organizations like NATO and the OSCE as existential threats, particularly during periods of increased tension in Europe," FireEye reported."

Further investigation allowed FireEye to discover that the APT28 is active since 2007 and it has always targeted the same kind of organizations, including government entities, militaries, and security organizations.

The hypothesis of state-sponsored hackers

The researchers at FireEye explained that the APT28 focused its hacking campaigns on targets that would be of interest to Russia, such as the Caucasus region with a focus on Georgia.

"Despite rumors of the Russian government's alleged involvement in high-profile government and military cyber-attacks, there has been little hard evidence of any link to cyberespionage," said Dan McWhorter, FireEye vice president of threat intelligence. "FireEye's latest advance persistent threat report sheds light on cyberespionage operations that we assess to be most likely sponsored by the Russian government, long believed to be a leader among major nations in performing sophisticated network attacks."

The APT28 ran spear phishing campaign. It used malicious emails to trick victims into to open the infected file or to serve a malicious link.

Figure 1 – APT 28 Targets (FireEye Report)

The malicious code used by the APT 28 appears very sophisticated, the group made a large use of backdoor that was undetected across the years. Like good detectives, let's try to summarize which elements of the analysis published by FireEye can help us to profile the threat actors.

Evidence	Hypothesis
Choice of targets indicates a political motivation of the attacks APT28 has been active since 2007 Sophisticated malicious code that requested a significant effort for the	**Threat Actor is a state sponsored hacker**

FREE TRAINING TOOLS
Phishing Simulator
Security Awareness

EDITORS CHOICE
How big is the skills gap, really?
Top Cybersecurity Predictions for 2020
Getting started with ethical hacking
Phishing technique: Message from the boss
Cyber Work podcast: Email attack trend predictions for 2020
Virtualization-based sandbox malware
MITRE ATT&CK: System shutdown/reboot
Cyber Work: How to become an APT hunter with Carbon Black
Domain vs Workgroup accounts in Windows 10
Phishing techniques: Clone phishing
Bluetooth security in Windows 10
Network traffic analysis for IR: Basic protocols in networking
The top 5 states for cybersecurity jobs
Jackpotting malware
Cyber Work: How data science and machine learning are affecting cybersecurity

RELATED BOOT CAMPS
Information Security
Security Awareness
DoD 8140
Ethical Hacking
Hacker Training Online
Security+
Computer Forensics
CISA
CCNA
PMP
Incident Response

MORE POSTS BY AUTHOR
Top Cybersecurity Predictions for 2020
Holiday Season Cybersecurity Scams and How to Avoid Them
Cybercrime and the Underground Market [Updated 2019]

development Exploitation of Zero-Days	
Hacking campaigns managed by APT28 hit targets that would be of interest to Russia Malware Source codes were set to Russian language settings The compile times and discovered that they were aligned with working hours in Moscow and St. Petersburg	**Threat Actor is Russian**

Security experts involved in the investigation believe that APT28 was responsible for the data breach at U.S. State Department computers in November 2014 aimed to gather information to conduct further attacks. The experts speculate that the team used the stolen information to compromise an unclassified network at the White House accessing sensitive information, including the President Obama agenda.

FireEye doesn't confirm that APT28 is behind the two incidents.

A look to the APT28 Arsenal

The APT28 group used for his hacking campaigns numerous common tools, including a downloader called Sourface (aka Sofacy), the backdoor Eviltoss and a modular implant dubbed Chopstick.

The Sofacy downloader was also identified by experts at TrendMicro that assigned to the APT28 the responsibility for the "Operation Pawn Storm." Chopstick is considered a distinctive element of the hacking group because according to the researchers it "demonstrates formal coding practices indicative of methodical, diligent programmers."

The Chopstick agent has a modular structure that gives it flexibility, an essential ability for long-term use. The researchers at FireEye analyzed two different strains of the CHOPSTICK malware that presented "vastly different functionality", depending on modules the authors added to the core of the malware.

In the arsenal of the APT28, there is also a Backdoor dubbed Eviltoss that uses asymmetric encryption to encrypt syphoned data from victims, and some sample detected by the experts also use SMTP to transfer stolen data outside the organization.

"APT28 is most likely supported by a group of developers creating tools intended for long-term use and versatility, who make an effort to obfuscate their activity," it wrote. "This suggests that APT28 receives direct ongoing financial and other resources from a well-established organization, most likely a nation state government."

The experts at Trend Micro referred the ATP28 with the name Operation Pawn Storm. According to the investigation conducted by Trend Micro, the hacking crew compromised government websites in Poland in June 2014 and in September of the same year; they infected the website for Power Exchange in Poland. The attackers exploited several attack techniques, including spear-phishing to watering hole attacks, to serve the *SEDNIT malware.*

"The cyber criminals behind Operation Pawn Storm are using several different attack scenarios: spear-phishing emails with malicious Microsoft Office documents lead to SEDNIT/Sofacy malware, very selective exploits injected into legitimate websites that will also lead to SEDNIT/Sofacy malware, and phishing emails that redirect victims to fake Outlook Web Access login pages," states Trend Micro in a blog post.

The hackers run high-targeted attacks, among the weapons used by the hacking team there is also a collection of malicious iframes pointing to very selective exploits that were also used to compromise the Polish government websites.

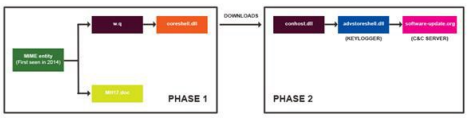


Figure 2 – SEDNIT/Sofacy malware (Trend Micro)

The post explains that in an attack on a billion-dollar multinational firm the group behind the Operation Pawn Storm reached via email just three employees.

"The e-mail addresses of the recipients are not advertised anywhere online," he noted. "The company in question was involved in an important legal dispute, so this shows a clear economic espionage motive of the attackers."

The malware researchers believe that the bad actors behind the Operation Pawn Storm have great cyber capabilities, they consider very interesting the use of SEDNIT that was designed to compromise targets and remain persistent in their network to syphon sensitive data.

"Their choices of targets and the use of SEDNIT malware indicate the attackers are very experienced; SEDNIT has been designed to penetrate their targets' defenses and remain persistent in order to capture as much information as they can." said Jim Gogolinski, Senior Threats Researcher at Trend Micro.

The hackers also adopted a very effective technique for their phishing campaigns, to

avoid raising suspicions in fact; they used well-known events and conferences such as the Asia-Pacific Economic Cooperation (APEC) Indonesia 2013 and the Middle East Homeland Security Summit 2014 as bait.

Trend Micro has disclosed the details of its investigation in research in a paper titled "Operation Pawn Storm."

Zero-day

On April 2015, researchers at FireEye discovered a new cyber espionage campaign, dubbed "Operation RussianDoll," managed by APT28 group. Differently from previous attacks, the hackers run highly targeted attack by exploiting two zero-day vulnerabilities to target an "international government entity".

The hackers exploited security flaws affecting Adobe Flash software (CVE-2015-3043) and the Windows operating system (CVE-2015-1701).

"While there is not yet a patch available for the Windows vulnerability, updating Adobe Flash to the latest version will render this in-the-wild exploit innocuous," states the report published by FireEye. "We have only seen CVE-2015-1701 in use in conjunction with the Adobe Flash exploit for CVE-2015-3043. We are working with the Microsoft Security Team on CVE-2015-1701."

"Because CVE-2015-3043 is already patched, this remote exploit will not succeed on a fully patched system," FireEye said. "If an attacker wanted to exploit CVE-2015-1701, they would first have to be executing code on the victim's machine. Baring authorized access to the victim's machine, the attacker would have to find some other means, such as crafting a new Flash exploit, to deliver a CVE-2015-1701 payload."

The iOS Spyware

The arsenal of the APT28/ Operation Pawn Storm is rich of surprises demonstrating that the hacking crew is very prolific. Early this year, experts at TrendLabs discovered that the group was using also a mobile spyware. The researchers have found a poisoned pawn spyware specifically designed to spy on Apple iOS devices.

"In our continued research on Operation Pawn Storm, we found one interesting poisoned pawn—spyware specifically designed for espionage on iOS devices. While spyware targeting Apple users is highly notable by itself, this particular spyware is also involved in a targeted attack," *states a blog post published by TrendLabs.*

The researchers discovered two distinct malicious iOS spyware used by hackers behind the Operation Pawn Storm, a first one dubbed *XAgent* and *MadCap*, this second name is also the name of a legitimate iOS game.

According to the researchers, the malicious XAgent app was written for iOS 7, but it is not optimized to hide its presence on iOS 8 devices, the second app MadCap doesn't work on jailbroken devices.

Both mobile apps are strains of the SEDNIT spyware that allowed the group to steal personal data, acquiring audio from the microphone and making screenshots. The C&C server contacted by the iOS malware is still live according to the malware researchers.

The malicious app infected Apple iOS devices without having to jailbreak them.

"We have seen one instance wherein a lure involving XAgent" states the report."We have seen one instance wherein a lure involving XAgent simply says "Tap Here to Install the Application."

The attackers used the "lure" website to serve the malware via Apple's ad-hoc provisioning feature for developers, the malicious application is provided with a .plist file hosted on the remote server.

Experts discovered also other methods of infection, including the connection of the iOS devices to a compromised or infected Windows laptop via a USB cable.

APT28 is planning to hit financial organizations

So far, we have taken the view that the group APT28 is politically motivated and therefore far from the criminal ecosystem, but new revelations complicate the scenario.

A new report published by the intelligence firm root9B seems to call into question the assertion that the APT28 is a state-sponsored hacking team. The researchers at root9b affirm to have uncovered plans by the APT28 group to target international financial institutions.

The information reveals that the group targeted Bank of America, the Commercial Bank International (CBI) in the United Arab Emirates, TD Canada Trust, Regions Bank, the United Nations Children's Fund, United Bank for Africa, and possibly Germany-based Commerzbank.

"While none of the targeted organizations are clients of root9B, we felt it imperative to disclose the findings to them, and as broadly as possible to the security community," said Eric Hipkins, CEO of root9B.

In April, the researchers uncovered the plans during a routine investigation; they spotted a spear phishing campaign that was targeting a financial organization in the United Arab Emirates.

The link with the group APT28 is a server used to run the phishing campaign that was previously used by the Russian hackers. The researchers also detected several components of a new strain of malware with signatures specific to APT28.

By analyzing the fake information used by the hackers to register the phishing domains, the experts discovered other domains set up to target other financial institutions.

"While the continued vector of the attack remains unclear, root9B assesses that it will most likely be a spear-phishing campaign. This attack vector will likely use a well-crafted email containing either a malicious file or web hyperlink to what recipients believe is the actual website; but is instead a fake landing page," states a report *from the company.*

Conclusions

The recent report published by *root9B* on the APT28 regarding the plans for cyber-attacks against financial organizations does not contradict my opinion the initial considerations on the state-sponsored origin of the APT28 group.

The hypothesis of state-sponsored hacking remains the most plausible due to the element highlighted at the beginning of the post. The fact that the hackers are being targeting financial institutions could be analyzed under different perspectives:

- Financial institutions are anyway among critical infrastructure of a country, attacking them is one of primary targets for state-sponsored hackers.
- The overlap between cybercrime and state-sponsored hacking make difficult to discriminate their actions, but the elements collected by various teams involved in the investigation suggest the involvement of high-skilled hackers backed by a government.

Security experts will continue to monitor the group despite the disclosure of its activities that will make it very difficult to track them in the future, because the APT surely will change its TTPs.

References

https://www.fireeye.com/resources/pdfs/apt28.pdf

http://securityaffairs.co/wordpress/29683/intelligence/apt28-fireeye-russian-espionage.html

http://securityaffairs.co/wordpress/36105/cyber-crime/apt28-russian-hackers.html

https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html

http://securityaffairs.co/wordpress/29517/cyber-crime/operation-pawn-storm.html

http://securityaffairs.co/wordpress/36808/cyber-crime/apt28-financial-institutions.html

https://www.alienvault.com/open-threat-exchange/blog/from-russia-with-love-sofacy-sednit-apt28-is-in-town#When:04:30:00Z

http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-the-red-in-sednit/

http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/pawn-storm-espionage-attacks-use-decoys-deliver-sednit

http://securityaffairs.co/wordpress/36139/cyber-crime/op-pawn-storm-continues.html

http://securityaffairs.co/wordpress/33118/cyber-crime/operation-pawn-storm-ios-spyware.html

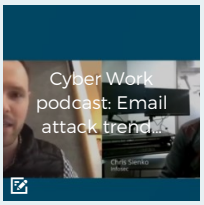
http://securityaffairs.co/wordpress/36139/cyber-crime/op-pawn-storm-continues.html

http://www.mediafire.com/view/bdr77piwp0ij0qz/FSOFACY.pdf

http://thegoldenmessenger.blogspot.de/2012/12/3-disclosure-of-another-0day-malware.html

AUTHOR
Pierluigi Paganini

Pierluigi Paganini is CTO at Cybaze Enterprise SpA Pierluigi is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, member of Cyber G7 Workgroup of the Italian Ministry of Foreign Affairs and International Cooperation, Professor and Director of the Master in Cyber Security at the Link Campus University. He is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines.



Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

+ = 9

Post Comment