Remember Fancy Bear?

secjuice.com/fancy-bear-review/

Jmetinfosec August 26, 2018

26 August 2018 / CYBERSEC

Fancy Bear, not to be confused with Cozy Bear, is a cyber-espionage group that has recently become a household name due to the highly publicized Democratic National Committee (DNC) hack in 2016. The group, however, has been *meddling* in the affairs of other groups, business, and nations for more than a decade.

What's in a Name?

The hacker group has several aliases including APT28, Tsar Team, Pawn Storm, Sofacy Group, Sednit, IRON TWILIGHT, and STRONTIUM. The actual name *Fancy Bear* was given to the group by the private cybersecurity firm CrowdStrike and its co-founder Dmitri Alperovitch based on a coding system that he created to name hackers. The coding appoints an animal according to the hacker's country of origin. Russian hackers are bears, Chinese hackers are pandas, and Iranians are kittens *[1]*. CrowdStrike investigated the 2016 DNC Breach at the DNC's request and concluded that the hacks were perpetrated by hackers working on behalf of the Russian Intelligence Service GRUs hence the designation "Bear" *[2]*. The analyst who discovers the new hacker gives the first part of the nickname. That analyst, Iggy Azalea, who discovered the hacker group chose "Fancy" because it sounded like the word "Sofacy" which is prominent in the hacker group's first-state malware (SOURFACE implant) *[1]*. The names Pawn Storm and Sednit were derivatives from the group's 2014 Operation Pawn Storm that used a SEDNIT/Sofacy malware that targeted Microsoft Office products *[3]*. FireEye called the group APT28 or Advanced Persistent Threat 28 and Microsoft uses the code-name STRONTIUM.

Tools of the Trade

Fancy Bear uses different methods that are consistent with the resources and abilities of a nation-state actor, including spear phishing, malware drop websites and zero-day vulnerabilities. From 2011 to 2012, Fancy Bear used its namesake first stage malware called "Sofacy" or SOURFACE before expanding to other backdoors and tools, including CORESHELL, SPLM (aka Xagent, AKA CHOPSTICK) JHUHGIT, AZZY (ADVSTORESHELL, NETUI, EVILTOSS), and OLDBAIT. Also other implants such as X-Agent, X-Tunnel, WinIDS, Foozer, and DownRange droppers. They have even dabbled in malware for Linux, and mobile devices *[4]*.

Sofacy

Sofacy or SOURFACE is a Trojan horse in the form of a .dll file. It is usually attached to a document and once executed, attempts to find 4 remote locations:

- [http://]scanmalware.info/ch[REMOVED]
- [http://]malwarecheck.info/ch[REMOVED]
- [http://]adawareblock.com/ch[REMOVED]
- [http://]checkmalware.org/ch[REMOVED]

It also gathers information about the computer like its name, OS, and running processes. Depending on vulnerabilities in any of those processes combined with the operating system, it will also download exploits to continue the process of gathering more information or escalate privileges. Sofacy was used from around 2011 to 2012.

CORESHELL

CORESHELL is an updated version of SOURFACE, since most endpoint protection services include Sofacy in their definitions. CORESHELL also uses the same attack method, it is a .dll file that is attached to documents. It includes code that is not used in what analysts suspect as an attempt to bypass endpoint security because it mimics legitimate machine instructions. It operates in much the same fashion, as Sofacy did, collecting machine information to send back to a C2 server and run it through an exploit database. It is capable of obfuscating its strings using a stream cipher custom made with 6 or 8-byte keys and can use HTTP, SMTP, or POP3 to reach the C2 server. It also contains code to stay persistent by making autostart extensibility point entries in the run key. This updated version of Sofacy was first seen in 2013

JHUHGIT

JHUHGIT a variant of the updated CORESHELL malware which was modified to be delivered through a zero-day exploit with Adobe Flash. It followed a series of exploit kits that were crafted after a response to Microsoft and Oracle fixing vulnerabilities in Internet Explorer and Java, respectively in 2014-2015.

EVILTOSS

This is one of the exploit kits downloaded by the Sofacy trojan after it establishes a connection. It is used to gain access to the system for reconnaissance. It logs keystrokes, and monitors machines for the purpose of escalating privileges and executing code. It utilizes a public RSA key for encryption and communicates information via SMTP.

CHOPSTICK

This is another tool used by Sofacy that is complex and provides multiple uses. It is another variant used by Fancy Bear that is more modular and flexible, it can be used for keylogging and collecting information like Microsoft files. It is designed to send messages back to its handling server in HTTP format and is capable of using email servers to relay information as well.

OLDBAIT

It is a credential harvester. Installs itself in %ALLUSERPROFILE%\\ApplicationData\Microsoft\MediaPlayer\updatewindws.exe and is used to steal credentials saved in browser software like Mozilla firefox and internet explorer. It can use HTTP or email to send messages back to its handling server with these stolen usernames and passwords.

A Sleuth of Hacks

Fancy Bear has a long resume of notable hacks including the Windows zero-day (2016), French television hack (2015), and the now infamous DNC hacks. They have targeted Aerospace, Defense, Energy, Government, and Media sectors, and it favors a variety of targets from security-related organizations and its members like NATO *[4]*, corporations like Boeing, Lockheed Martin and Raytheon, journalist/bloggers, politicians/political activists, to even private citizens, like five United States military wives in 2015 *[5]*. The cybersecurity firm Secureworks found targets of the group from 116 different countries, however from March 2015 and May 2016, they identified most of the targets were from the United States, Ukraine, Russia, Georgia, and Syria. The most common thread among the varied targets leads back to strategic Russian interests.

The Masked Unmasked?

In 2016, after CrowdStrike had announced that the DNC hack had been committed by the Russian Intelligence Agencies, an online persona called Guccifer 2.0 took credit for the breach. Shortly, after Guccifer 2.0 developed an online social media presence (WordPress and Twitter accounts) and started to leak the stolen emails and documents. Many experts, including CrowdStrike had their doubts about Guccifer and its claimed identity because of forensic analysis of the leaked documents (including tampering and editing of information contained in the documents) and communications made by Guccifer to members of the media.

From October 2016 to January 2017, Guccifer's social media posts started to show a better command of English, and according to sources from the Daily Beast, it was because the responsibility of the accounts was given to a more senior GRU officer that had better proficiency with the English language. The hacktivist was further discredited when a Russia intelligence official maintaining the Guccifer 2.0 social media accounts made the fatal error of failing to use a virtual private network to access the US-based social media platform. The IP address left in the service logs was located at GRU HQ in Moscow *[10]*.

This past year, Deputy Attorney General Rod Rosenstein announced twelve Russian Intelligence officers were indicted by Special Counsel Robert Mueller for “conspiracy to commit an offense against the United States”, “aggravated Identity theft”, and “conspiracy to launder money” in order to influence and meddle in the 2016 Presidential campaign. The alleged hackers reportedly worked for Russia’s Intelligence GRU Units 26165 and Unit 74455, the same Russian intelligence units theorized by the different cybersecurity firms. The indictment outlines how the GRU Units hacked the DNC and DCCC’s email accounts and computer networks and used spear phishing and malware to gather damaging information. The information was then disseminated through fabricated online personas, including DCLeaks and Guccifer 2.0. Robert Mueller having access to classified intelligence reports must have concluded that Guccifer 2.0 was at the very least an agent working for Russian intelligence as it was made part of the formal accusation.

Conclusion

Fancy bear is a cyber group that is highly sophisticated, organized and thorough. They use tools that are complex and custom made and have been used successfully to attack countries. They should be respected and not taken lightly because they are a danger to their opposition. When faced with adversity they have proven the ability to adapt and overcome it. With the success they have had one should assume they are out there right now, working to undermine their enemies. Just because we know who they are doesn't mean they will stop.

Works Cited

[1] V. Ward, "The Russian Expat Leading the Fight to Protect America," Esquire, 24 10 2016. [Online]. Available: https://www.esquire.com/news-politics/a49902/the-russian-emigre-leading-the-fight-to-protect-america/. [Accessed 18 08 2018].
[2] *The American Journal of International Law,* vol. 111, no. 2, pp. 483-504, 2017.
[3] J. Gogolinkski, "Operation Pawn Storm: The Red in SEDNIT," *Trend Micro,* vol. 22, p. October, 2014.
[4] D. Alperovitch, "CrowdStrike," 15 06 2016. [Online]. Available: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. [Accessed 24 08 2018].
[5] GReAT, "SecureList," 04 12 2015. [Online]. Available: https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/. [Accessed 24 08 2018].
[6] J. Brown, "Report: Russian Hackers Posed as ISIS to Attack U.S. Military Wives," 08 05 2018. [Online]. Available: https://gizmodo.com/report-russian-hackers-posed-as-isis-to-attack-u-s-mi-1825855349. [Accessed 24 08 2018].
[7] Secureworks Counter Threat Unit Threat Intelligence, "Secureworks," 30 03 2017. [Online]. Available: https://www.secureworks.com/research/iron-twilight-supports-active-measures. [Accessed 24 08 2018].
[8] S. Gallagher, "ARS Technica," 23 03 2018. [Online]. Available: https://arstechnica.com/tech-policy/2018/03/dnc-lone-hacker-guccifer-2-0-pegged-as-

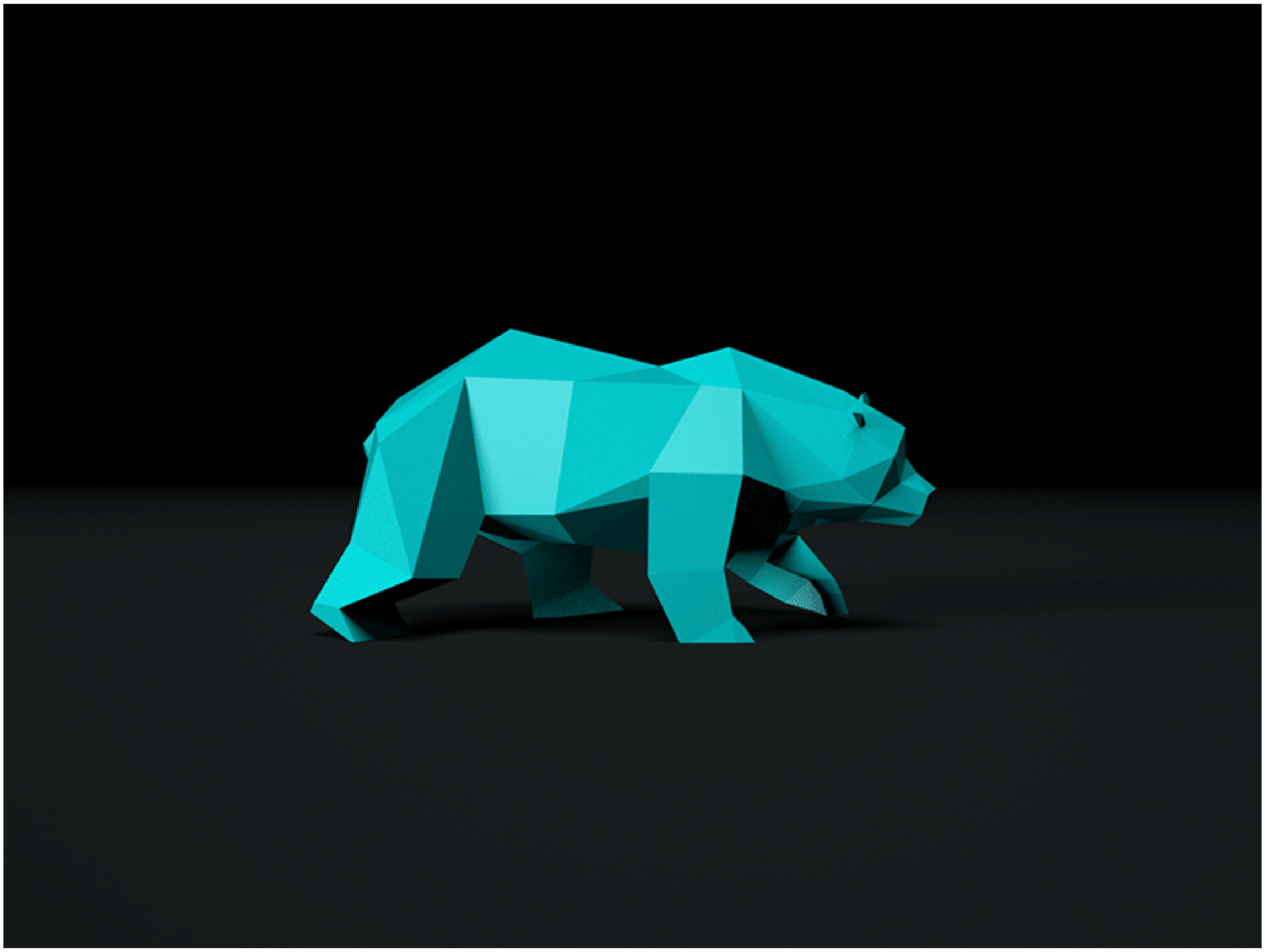
russian-spy-after-opsec-fail/. [Accessed 24 08 2018].

[9] P. Muncaster, "InfoSecurity Magazine," 21 04 2015. [Online]. Available: https://www.infosecurity-magazine.com/news/apt28-back-russiandoll-attack/. [Accessed 24 08 2018].

[10] M. Ostrowski and T. Pietrzyk, "Security Case Study," 05 2015. [Online]. Available: https://www.securitycasestudy.pl/wp-content/uploads/2015/05/SCS14–MOstrowski.TPietrzyk.pdf. [Accessed 24 08 2018].

[11] J. Vrijenhoek, "Komplex Malware: The Return of Sofacy's XAgent," 16 02 2017. [Online]. Available: https://www.intego.com/mac-security-blog/komplex-malware-the-return-of-sofacys-xagent/. [Accessed 24 08 2018].

[12] UNITED STATESDISTRICT COURT FOR THE DISTRICT OF COLUMBIA, "Case 1:18-cr-00215-ABJ," U.S. Justice Department, https://www.justice.gov/file/1080281/download, 2018.



The artwork used to head this article is called 'Low Poly Bear' and it was created by Jeremiah Shaw.