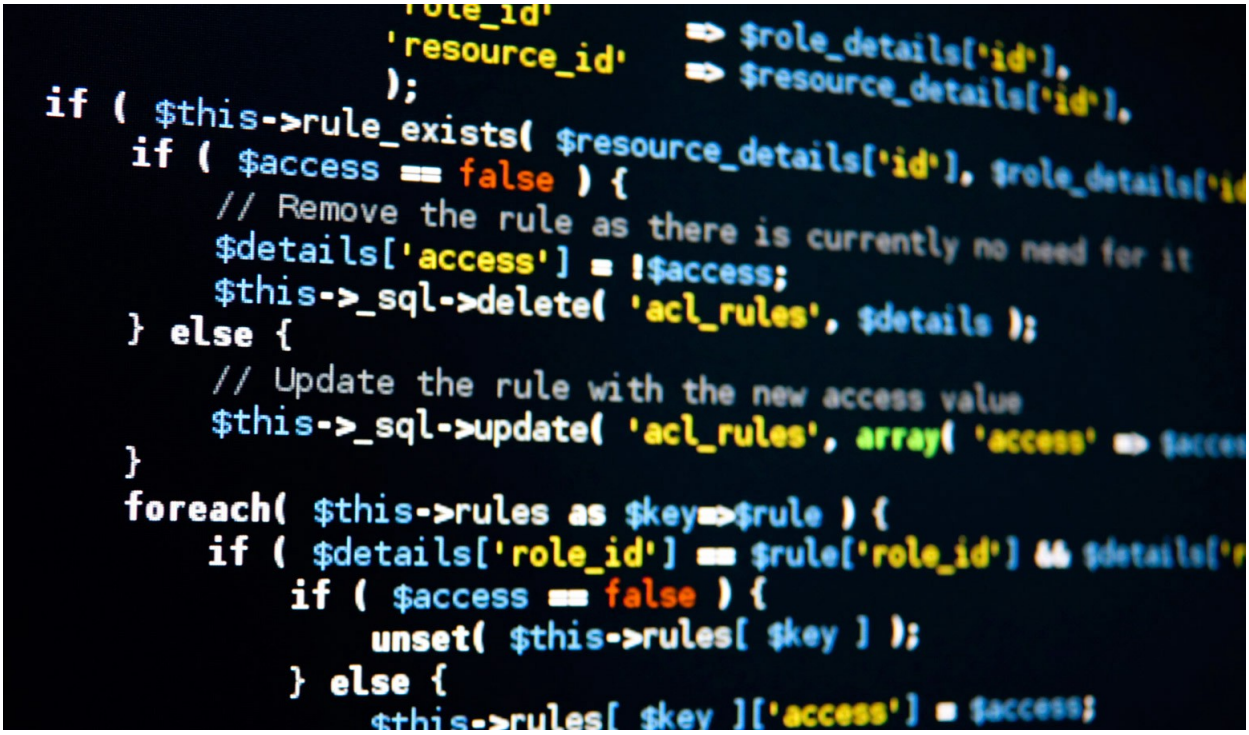
The APT Chronicles_December 2018 edition

medium.com/@z3roTrust/the-apt-chronicles-december-2018-edition-e3e5125ffcd2

z3rotrust January 6, 2019

z3rotrust
Jan 7 ★



Credit: The MITRE Corporation

Join me for a short foray into the publicly reported Advanced Persistent Threat (APT) group activity over the last month. The following is information that I've compiled using freely available Open-Source Intelligence (OSINT) information collection methods.

1. Chinese-attributed APT 10 (a.k.a., *"Red Apollo," "CVNX," "Stone Panda," "MenuPass," "HOGFISH," "POTASSIUM"*) has been focusing on compromising Managed Service Providers (MSP), you know the companies you pay to manage your IT services that have likely have some level of privileged access into your networks. Of course, it is not difficult to understand why they are targeting MSPs. If you can compromise an MSP, well just imagine all of the privileged accesses to different organization's networks you will have.

"Godkiller" and "Atreexp;" the 2 APT 10 Chinese nationals indicted by the U.S. DoJ

> "The indictment alleges, among other things, that by hacking into a single New York-based MSP, APT10 was able to compromise data from companies in a dozen countries [and 45 tech companies], from Brazil to the United Arab Emirates. With a single initial intrusion, Chinese spies could leapfrog to industries as varied as banking and finance, biotech, consumer electronics, health care, manufacturing, oil and gas, telecommunications, and more." ~Brian Barrett, Wired 12.20.18

China has been involved with over 90% of computer network espionage (CNE) cases in the U.S. over the last decade or so. APT 10's entry point into the MSP has been linked to a simple phishing email titled "C17 Antenna problems" that contained a malicious MS Word document called "12–204 Side Load Testing." APT 10 is alleged to have stolen "hundreds of gigabytes" of sensitive data including tech and space and satellite technologies. APT 10 has over 1,300 unique domains registered to this CNE campaign and is known to use the *QuasarRAT, PlugX,* and *RedLeaves* malware among many others. For more information on APT 10, check out their MITRE ATT&CK page.

Considering the fact that China just landed their "Yutu 2" rover on the far side of the moon as of 2 Jan 2019, it serves to demonstrate how China's massive CNE campaigns over the last two decades have leapfrogged the country into becoming a formidable threat to other nuclear superpowers like the U.S. and Russia economically and militarily.

2. New information released in the massive Marriott hotel Starwood reservation system data breach of over 500 million guests (later amended to 383 million after duplicates were discovered) now includes 5 million passports that were left unencrypted that were accessed over a 4-year hacking campaign attributed to Chinese hackers dating back to 2014. Which Chinese APT is involved is not evident or publicly known at this point, but the attackers are suspected of working on behalf of China's Ministry of State Security. This particular interested is further complicated that Marriott

acquired Starwood Hotels in 2016 and inherited the APT CNE activity in their acquisition that wasn't discovered for another 2 years when Marriott noticed that someone was attempted to remove data from their systems.

Credit: Picture Joliet

3. China's Strategic Support Force (SSF) of the People's Liberation Army (PLA) is attributed to a massive diplomatic cyber espionage campaign against the European Union (EU) and more than 100 organizations that was conducted over the last 3 years and which resulted in the interception of thousands of diplomatic cables (i.e., messages) containing sensitive and protected information.

> "Initial access to the network was gained using a phishing attack against network admins and senior staff to steal their login credentials."

Though we all like to think that we're smart enough not to fall for a phishing attack, they continue to be an unremarkable but highly effective method of compromise for many cybercriminals. So much so, in fact, that email has become incredibly risky for businesses, governments, and organizations of all shapes and sizes. SSF teams of hackers exfiltrated the data by chunking it into small segments of data and then silently siphoning the data out of the network to public Cloud storage services. Of the EU data that was stolen and compromised, the list included the following types of data:

- Criminal Appeal Court
- Foreign Affairs Ministers
- United Nations
- Consular Affairs
- Non-proliferation
- Security
- European Council
- Human Rights

4. FireEye has reported that Russian hackers attributed to the "*TEMP.Isotope*" APT (a.k.a., *"Energetic Bear,"* or *"Dragonfly 2.0"*) group continue to probe U.S. critical infrastructure in an effort to map it out and locate potential cyber vulnerabilities. *"Isotope"* prefers to use a hacking strategy known as "living off the land" whereby they try to use only native tools on the hacked operating system (OS) as much as possible to avoid raising intrusion suspicion. However, they still use custom-built backdoors to maintain persistence. "Isotope" is likely part of the same Russian APT groups that have targeted Ukrainian power grids over the last few years.

Industrial Control Systems (ICS) have been adhering to the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) best practice standards for network defense ever since 2003 in the aftermath of the Northeastern blackout which caused a cascade failure that left 50 million Americans and a Canadian province without electrical power for nearly 2 days. Many have attributed this power outage to a Chinese-based cyber attack, but the analysis was inconclusive and was instead attributed to a number of different factors.

2003 Northeastern [U.S.] Blackout; Credit: Huffington Post

Some of the NERC CIP network defense standards include two-factor authentication (2FA), segmenting networks with firewalls, using encryption on stored data, and strict access controls for network owners and third-party network connections. The problem

is, however, that some U.S. critical is publicly owned by the Government whereas other some are privately-owned. Government-managed critical infrastructure is required to adhere to strict NERC CIP and National Institute of Standards and Technology (NIST) standards, but privately-owned critical infrastructure organizations are not required to adhere to the same standards. Why this is even still an option in 2019 is a pretty big question? For a country such as the U.S. that is based on democracy and freedom, national security has long been used by the federal government to trample individual citizen Constitutional rights. However, it seems there is still disparity amongst what the federal government can get away with against corporations with big law firms protecting them and Joe Schmoe, the average U.S. citizen.

"Isotope's" activity thus far appears to be more CNE intelligence gathering-related, but there are signs that, like China, the intelligence information being collected about U.S. power grids is being used to further Russia's development of their own power grid system possibly to advance it and to learn new methods of hardening their own infrastructure against potential cyber attacks. At the same time, of course, this same information can be used to target U.S. power grid cyber vulnerabilities whenever they choose to do so. This type of ICS probing against U.S. Critical Infrastructure and Key Resources (CIKR) is nothing new and has seen other nation-state threat actors like North Korea, China, and Iran involved in similar activities. It is safe to assume that the U.S. has been involved in similar CNE activity against all of its adversaries.

5. A North Korea threat actor or APT group is thought to be the culprit behind a South Korean data breach involving 1,000 North Korean (NK) defectors. The malware (i.e., the specific type of malware is unknown) was found on a North Gyeongsang state-run center computer leaked the information of the 1,000 NK defectors. Now, of course, the families of those defectors still living in NK could possibly be in danger if the NK regime is able to successfully link the defector and their family members. Attribution of malware origin and specific individuals is incredibly difficult, and NK have capitalized on this as a form of international harassment, persuasion, and even as a form of economic revenue.

6. The Shamoon disk wiper malware was used in an attack that disrupted Italian energy (oil and gas) contractor Saipem S.p.A. The attack affected roughly 400 servers which impacted the company's operations globally in countries such as U.A.E., Saudi Arabia, Kuwait, India, and Scotland. Thanks to a robust data backup system, the company didn't lose any data but just imagine if it didn't have a data backup in place. Things could've been a lot worse for the firm. However, operations are still affected costing the company a lot of money while it has to reimage and restore data to hundreds of servers globally assuming the servers can be salvaged at all. Although not for certain, *Shamoon* (a.k.a., Disttrack) is thought to be the work of the Iranian-based OilRig and Rocket Kitten APT groups as well as the Greenbug APT group.

7. Operation 'Sharpshooter' is a global phishing campaign thought to be linked to the North Korean-based Lazarus APT group. This phishing campaign uses fake job recruitment documents targeting defense contractors, government, and critical infrastructure organizations that contains a malicious "fully-functional modular

backdoor" implant called "Rising Sun" that borrowed source code from the Lazarus-attributed "Duuzer" malware. Similarities in the code, library (.dll) names, and dynamic Application Programming Interface (API) exist between both "Rising Sun," and "Duuzer" making attribution to the Lazarus APT likely. Forensic analysis has determined that the English-written fake job recruiting documents were produced in a Korean-language environment. However, there is speculation that the obvious connection to the Lazarus APT may be a false positive. Other skilled APTs can emulate each other's code and may have motivations to make attacks appear to originate from another region than their own. The fake job recruiting phishing documents are, of course, more MS Word documents (with malicious macros) that were stored in a Dropbox container. The macro contained the malware dropper which then corrupted the MS Word application memory and led to the second-stage exploit code.

As with the November 2018 APT Chronicles, that's quite a bit of APT activity for one month. Realize also that there is CNE and CNA activity occurring that we may never learn of due to the covert nature of cyber warfare. Be safe online and use basic information security best practices to avoid becoming a victim of data breaches. Remember though, there is very little you can do when you give your personal data to a company and trust them to safely store it. Most organizations have no chance of defending against an APT.