APT29 & APT Groups

My Journey in Cyber Security

APT29 & APT Groups

Marcos Felix Random July 30, 2018 | 0

This report aims to give an understanding about Advanced Persistent Threat (APT). In doing so, I will be using a famous APT group "APT29". The structure is as follow:

- Description of APT
- Description of APT29
- Mapping APT29 on the Cyber Kill Chain
- Providing SIEM solutions
- Conclusion

Description of APT as a Threat:

I will use the US National Institute of Standards and Technology (NIST) definition of APT:

An expert and resourceful adversary with the means to create opportunities to help achieve their goals. The goals of an APT group are establishing and expand their foothold within a compromise system. Most APT groups stay stealthy within a system for long periods of time, either stealing information or waiting for the right time to accomplish their goals. APT groups tend to adapt their mechanism according to the defender's effort to stop it *(NIST, 2011).*

Why is it a threat?

McAfee says that what makes APT groups unique are their motives and persistency to their goals *(Dmitri, 2011).* The persistency refers to the continuous act of launching attacks against their target *(Frankie, 2011).*

The goal of APT is to gain data on intellectual property over an extended period of time due to its stealthy nature, rather than being focused on immediate financial gain like most attacks. Often times, these APT attacks make use of either trusted connections or insider threat to target systems *(ISACA, 2013).*

All of this, plus the fact that the APT group behind the attack are comprised of expert hackers, all that there is left is the motivation. The motivation comes from the APT group being either cyber mercenaries *(Kaspersky, 2013)* or work for a governmental cyber unit *(Mandiant, 2013).*

Description of APT29

As mentioned, this report will look into a famous APT group called APT29. This group goes by many names (Cozy Bear, APT29, the Dukes etc.), and it's usually given by the cybersecurity firm that's investigating the group *(Anon, 2016).*

Overview of APT29:

This APT group is very well adaptive and disciplined. They hide within their targets network and communicates irregularly and in a way that looks like a legitimate network traffic. APT29 is considered to be one of the most advanced and capable APT threat groups. They are also very flexible, constantly patching their own bugs and add new features by deploying new a backdoor. They also have a fast development cycle for their malware and quickly alters their tools in order to remain undetected *(Anon, 2016).* APT29 also likes to monitor the network defender's activity to constantly be in control of the system.

Motivations and Affiliation:

APT29 is believed to have close affiliations with the Russian Intelligence services and to be engaged with political and economic espionage. Their attacks are typically against West Governments which benefits the Russian Government *(Dmitri, 2016).*

APT29 Activity in the recent years:

In recent times, the group APT29 has been known for the 2016 Democratic National Committee hack:

The attack happened in 2016, where APT29 coordinated cyber-attacks towards the **Democratic National Committee (DNC)** *(Dmitri, 2016).* It is believed that the goal of that was to assist Donald Trump in winning the presidency *(Adam et al, 2016).*

The impact of APT29:

The elaborated hacks from APT29 has brought a massive attention to cyber espionage from Russian Government. This in turn, forces Governments to be more careful with their cyber security and personnel.

Search ...

RECENT POSTS

[HTB] Writeup Walkthrough November 6, 2019

[HTB] Bastion Walkthrough September 16, 2019

Linux Enumeration May 9, 2019

Powershell: Extract O365 Users and License Type January 16, 2019

Using Powershell to Export Group Members from Active Directory December 18, 2018

CATEGORIES

Hack the Box Walkthroughs

Infrastructure Pentesting

Kali Linux

Linux

Log Management/Analysis

Management Side

Random

System Administration

Talks

Web Application Security

Windows Security

ARCHIVES

November 2019

September 2019

May 2019

January 2019

December 2018

November 2018

October 2018

September 2018

August 2018

July 2018

HITS

22886

ADs

- This had a massive social impact as it is believed that the goal of that was to assist Donald Trump in winning the presidency *(Adam et al, 2016)*. With the DNC hack, the USA launched an ongoing investigation of Donald Trump presidential campaign and any Russian interference in the This investigation touches on any possible links between Donald Trump and the Russian Government *(Rod, 2017)*.

APT29 and the Cyber Kill Chain:

In this section, I will be using the cyber kill chain to do the mapping of tactics and techniques of the APT29 group. Cyber Kill Chain are phases or stages of a targeted attack. Each stage presents an opportunity to detect and react to an attack *(Lockheed Martin, Unknown)*. These stages form a link which if broken, it can stop the attack. Each stage will link back to the DNC Hack that occurred in 2016, that way we are able to see each stage of the attack and possibly prevent future ones.

Reconnaissance:

The first stage is when APT29 collects information on the target. The report by the DHS and FBI shows that there are two main reconnaissance techniques used on the DNC hack, one was network scanning and the other was credential harvesting.

The network scanning was done in an attempt to find websites that are vulnerable to cross-site scripting (XSS) and Structured Query Language (SQL) injections. These vulnerabilities were exploited to allow APT29 into the DNC network.

The other method is credential harvesting pages. A spear-phishing email was used in this method to get users to click a link where they had to enter their details. This was effective to APT29 and gave them access to their network through legitimate credentials *(DHS & FBI, 2016)*.

Weaponization:

APT29 is well-known for their skills in embedding malicious macros into files (PDF, Word) as part of the Weaponization stage *(Eyal, 2018)*. The same report by Eyal, shows that APT29 made use of Microsoft Office Documents to create a macro that would launch a backdoor PowerShell code called POSHSPY/PowerDuke.

This file with the malicious code was sent in a spear-phishing email to the DNC. PowerDuke was embedded as a backdoor while POSHSPY was embedded as a second backdoor.

Delivery:

This stage is how APT29 delivers the weaponized files to their target. It is widely known that APT29 traditionally use spear-phishing emails to infect their targets with malicious attachments or URL's with malicious payload *(DHS & FBI, 2016)*. This method of delivery was used on the DNC hack in 2016 by APT29 *(Steven, 2016)*.

Example of spear-phishing email by APT29:

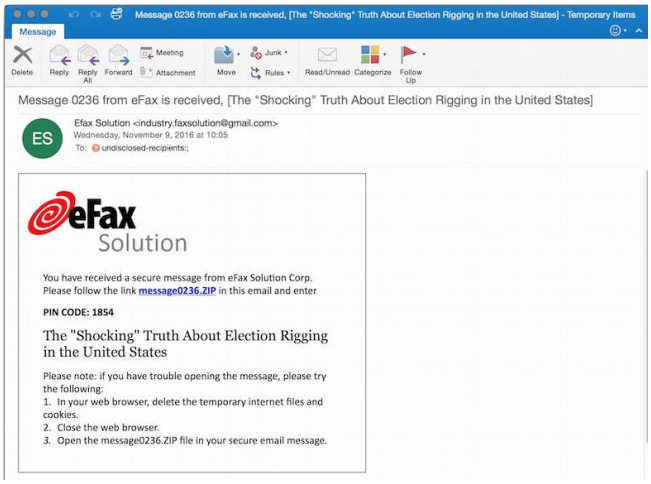

Figure 3: Spear-phishing email from APT29 (Steven, 2016)

Exploitation:

The exploit stage refers to APT29 taking advantage of a vulnerability to for their gain. In the DNC hack it is safe to say that APT29 made use of Human Engineering (spear-phishing) skill to exploit the weakest link in any organisation – humans.

APT29 also developed a number of malware to exploit common vulnerabilities and exposures (CVEs) within a system. APT29 also commonly targets Microsoft Office exploits because of its popularity amongst users/organisations *(SecurityWeek News, 2016)*.

Some of the Microsoft Office exploits used by APT29 in the past are:

- **CVE-2015-1641:** Microsoft Office Memory Corruption Vulnerability *(NIST, 2015-2017)*
- **CVE-2009-3129:** Microsoft Office Compatibility Pack for Remote Attacks *(NIST, 2009-2017)*
- **CVE-2014-1761:** Microsoft Office Denial of Service (Memory Corruption) *(NIST, 2014)*

Installation:

This stage defines the installation of the malicious code in the victim's system which allows APT29 to permanently remain there until kicked out *(Lockheed Martin, Unknown)*. In the DNC hack, users were sent a spear-phishing email, within this email there was a zip file:

Figure 4: DNC Zip contaminated File (Steven, 2016)

Inside this zip file there was a decoy document with a dropper. This dropper would drop APT29 backdoor in the user's system ("%APPDATA%\Roaming\"). Then after the main backdoor which was PowerDuke was installed, APT29 would download POSHSPY straight from their Command and Control Server *(Eyal, 2018)*.

Command & Control:

This stage refers to the communication between the hosts (APT29) and the infected system (DNC). During the DNC hack, CrowdStrike found out that APT29 was using a malware called SeaDaddy. This malware allowed APT29 to program a specific schedule to launch a malicious code. Therefore, communicating to and from the server.

Indicators of Compromise:

IOC	Adversary	IOC Type	Additional Info
6c1bce76f4d2358656132b6b1d471571820688ccdbaca0d86d0ca082b9390536	COZY BEAR	SHA256	pagemgr.exe (SeaDaddy implant)
b101cd29e18a515753409ae86ce68a4cedbe0d640d385eb24b9bbb69cf8186ae	COZY BEAR	SHA256	pagemgr.exe (SeaDaddy implant)
185[]100[]84[]134:443	COZY BEAR	C2	SeaDaddy implant C2
58[]49[]58[]58:443	COZY BEAR	C2	SeaDaddy implant C2

Figure 5: SeaDaddy Implant Indicators of Compromise (IOC) (Dmitri, 2016)

Actions on Objectives:

The last stage is the Actions on the Objective. So, what was APT29 end goal and did they achieve it? Yes. Although, the goal is not necessarily clear, we have an ongoing federal investigation on the President of the United States Donald Trump and the Hack made by APT29 *(Rod, 2017)*. Perhaps, the goal was to elect Trump into presidency. This means that the original goal of APT29 was to steal intellectual property, such as Email accounts and passwords *(Dmitri, 2016)*. This stolen information was then leaked via WikiLeaks, which in turn harmed the DNC reputation thereby favouring Trump on winning the presidency *(Adam et al, 2016)*.

Providing SIEM Solutions

In the fourth section of this report, I will be providing SIEM solutions to different phases of the kill chain mentioned in the third section. As well, as solutions I will be also identifying relevant Indicators of Compromise.

Solution for Reconnaissance stage:

In the reconnaissance stage a solution to networking scanning is to have a security analyst identifying the types of scans that are carried out against their systems that way the security analysist is able to identify and patch vulnerabilities within their system. A famous tool to help with this task is Splunk.

Indicators of Compromise and further solution:

Common IOC's are IP Addresses. A solution would be to feed normal traffic to the system and flag anything that stands out from the traffic it was fed. Geoff Webb, a director of solution strategy for NetIQ said that compromised system will send traffic back to its attackers during Command and Control phase and a security analyst could identify a threat before any real damage is done *(Geoff W, 2014)*.

Geoff also mentions credential harvesting. A method used by APT29 on the DNC hack. A mitigation is to monitor the changes in the behaviour of users with escalated privileges as a hacker might be trying to establish a foothold in the network. A security analyst would look for: time of activity, systems accessed, and the type of information accessed *(Geoff W, 2014)*.

This can also be used by a Security Operation Centre Analyst to detect **Actions on Objective** before any data is stolen just by looking for any signs of files and user credentials being moved within their own network.

Solution for Delivery stage:

Perform analysis of their system to identify any malicious email that is similar to APT29 common spear-phishing email themes. For instance, the defender would gather emails sent by APT29 and analyse their subject heading, text and their themes.

Figure 6: DNC Spear-Phishing Email Header (Steven, 2016)

An example is given above, we see a topic from current events which is the election rigging in the U.S. Since that is a hot topic, it is likely to be opened due to curiosity. This is a form of psychology used by APT groups but especially APT29. Another example of email sent by APT29 during the DNC hack is:

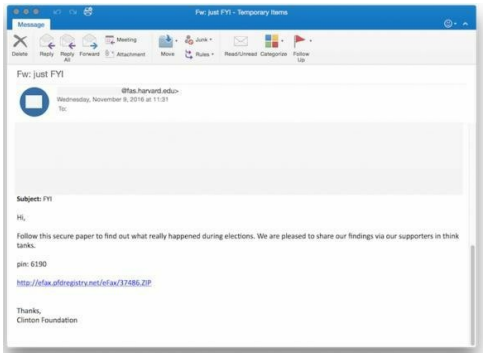

Figure 7: Phishing email by APT29 (KrebsonSecurity, 2016)

We can see common similarities to the previous email shown, they all have a link to a password protected zip file and they all focus on recent events *(U.S.A 2016 Election)*. The security analyst can use this in his favour and blacklist certain emails or set up an alert that would go off whenever an email similar to the ones mentioned is received.

Solution for Installation stage:

Security analysists could review their systems for any unauthorized web shells which is another indicator of compromise. Web shell is a script that can be used on a web server to allow remote administration of that machine *(US-Cert, 2015)*. This can also be used to leverage other exploitation techniques, so it is important for the security analyst to review their system often to try preventing this from escalating.

Conclusion

To conclude, the threat of APT is ever growing and often companies don't know how to deal with it due to its complexity and its stealthy nature. I believe that in order to detect attacks from any APT group, the security analyst must use tools to help them analyse traffic. Since reconnaissance is the most important stage of an attack, it is important to use software such as Splunk to analyse logs to prevent any damage being done.

References

« Previous: Dashboard on Kibana

Next: Graylog Installation Tutorial »