Threat intelligence week 3

Jurjen de Jonge
500731921
Hogeschool van Amsterdam

September 30, 2018

Contents

1. *Threat intelligence*

1.1 Linkedin persona's

The intrusions detected are those of of spearphishing or the use of malicious websites. Most of the targets were from the middle east and a quarter from the targets were working in telecommunication.

From the given article the group TG-2889 infiltrated Teledyne by submitting malware that looked like a sadly the report that describes additional information by this APT is not available any more on the referenced url.

Eight leading persona's were created and and 18 support persona's which adds up to a total of 26 persona's in total. These persona's are connected to each other and vouch for each other to create a realistic looking person that is good in "his" field of work.

After gaining access to a system they will use psexec to move lateral through the computer network using password and tickets dumped using mimikatz and net crawler. [1]

1.2 Social engineering

The attack was simply and elegantly executed using osint and social engineering. Each of the targets where selected for a reason and a lot of thought and experience was showed in the attack. The example of this is requesting information from the sales team to copy some information.

This kind of attack would be more easy to perform against a large scale company. Where smaller companies would be more difficult to target. When the company is smaller it would be easier for such an attack to be detected. The CEO might just sit next to all his employees while working. But even then it could be possible to do such an attack using a different approach.

All the right defense mechanics should be in place to defend a company against these attacks. More importantly the employees should be trained

[1] https://attack.mitre.org/wiki/Group/G0003

to recognize these situations and report them along with all the technical solutions.

1.3 Well-Known Cyber attacks

1.3.1 Home Depot Security Breach

The home depot breach was the breach of the credit card system. This allowed hackers to steal 56 million credit cards. The breach occured in the Point of sales (POS) system that was infected with malware. The stolen credit cards were soled on the darkweb to other criminals. The criminals would use these cards to buy things they would later sell on secondhand websites for cash.

1.3.2 Target Credit Card Breach

Similar to the Home Depot breach, the POS was infected with malware which allowed hackers to steal customers their credit card information. 40 million cards have been stolen during this attack. Using the citadel malware on a third party supplier they managed to steal credentials that allowed them to use the Target vendor portal. From this server they managed in a undisclosed way to gain access to the POS server on which they installed malware that used memory scanning techniques to extract credit cards.

1.3.3 The stuxnet virus

Stuxnet is a virus that is very complex. It's a cyber weapon that was responsible for damaging Iran's nuclear program. It targeted programmable logic controllers (PLC's) that are used to automate the nuclear centrifuges. The malware would make the centrifuges to tear themselves apart.

1.4 Sony Pictures Entertainment Hack

Sony has been breached in 2014 by state hackers that are related to North Korea. The hackers stole 100TB of data and leaked a big portion on the internet. This data contained Social security numbers, movies, salaries and personally identifiable information. The hackers promised not to dump further information if the movie "The interview" would be canceled. Sony pulled the films from all the cinema's because of threats. Obama told them that they made a mistake and that the should not give in to these threats and set

an example. On december on Christmas day Sony allowed 300 independent cinema's to show the movie. Later Sony released the movie on streaming websites.

1.5 Vulnerable Shiraz!

Using Shodan to scan for Shiraz ip addresses will turn up different Mikrotik routers. In the past it would be more but since this became known they have removed and or patched these routers. A possible attack on these vulnerable routes that are in use by a big DSL company could disrupt the internet access for Shiraz. A company could be Shatel DSL Network. Executing a mass exploit against all the vulnerable would possible disrupt the internet access and could cause chaos. When looking at Manchester is seems like there are less routers exposed this way. You'll mostly find webservers with Mikrotik routers mixed within.

To fix this problem they should have done as they already have. Upgrade their networking infrastructure to non vulnerable routers or remove those that cannot be updated.