Assignment 1

Case Study: Angler Exploit Kit

Angler, one of the most popular exploits used in cyber-attacks, was first identified in 2013. It was the successor to the Blackhole Exploit Kit which disappeared after its author Paunch was arrested. According to the Global Trustwave Security Report in 2015[1], Angler accounted for 17% of the infections. It gained popularity because of the special characteristics it has. Angler became even more active in March 2015 and dominated the exploit kit landscape. Cisco’s Midyear Security Report of 2015[1] reported that Angler was responsible for 40% of user penetration in cyber-attacks.

The reason for the rise in popularity of Angler was mainly that it could easily be used by attackers who lacked deep technical knowledge. Script kiddies used Angler as they didn’t have to know the kit themselves but could still use it for attacks. Additionally, it was also equipped with a user interface which made it easy for literally anyone to operate. Furthermore, Angler was sold in the cybercriminal world for a good price. According to Sophos[2], it could have also been sold in a pay-per-install model in which Angler developers charge the users only for successful malware infections.

Angler was mostly used in drive-by attacks and it had the capability to execute malware without needing to write any files to the disk which is why antivirus could not detect an infection. Angler uses an encrypted payload making it even more difficult for the antivirus since it has to decrypt and then take action. This is the reason why usually antivirus take a considerable amount of time to generate an alert. The time an antivirus takes to detect Angler’s malware, the system has already been compromised and confidential information has already been stolen. These technological advances tackled security countermeasure which added to its popularity. Angler’s developers constantly adapted their tactics to avoid detection by countermeasures like antivirus by switching hostnames and IP addresses at regular intervals to avoid reputation filtering. Angler also used encryption techniques to prevent content detection. Angler could perform a vast number of actions like collect confidential data, install malware or use the infected system as a botnet. Angler also takes advantage of vulnerabilities found in outdated software. Additionally, Angler’s developers regularly added new vulnerabilities. A lot of zero-day attacks were identified in software like Adobe Flash Player and Internet Explorer of which Angler’s developers took complete advantage.

Angler was one of the most popular exploit kits in 2015 and attacks using angler were more than 19.5 million[2]. The reason for widespread use of Angler was the variety of distribution methods. Attackers compromised web servers and created high numbers of subdomains, loading it with Angler. Then they used distribution techniques like spam campaigns and malvertising to compromise users. This tactic was effective as there would be no pattern and the lifespan of these subdomains was small making it difficult for authorities to analyze it.

In 2016, activity of Angler reduced and disappeared completely in June. The [SANS ISC Infosec Forum](https://isc.sans.edu/forums/diary/Neutrino+EK+and+CryptXXX/21141/) noted that CryptXXX ransomware (Ransom.CryptXXX), which was spread using Angler, started to show as a Neutrino associated malware[3]. It is speculated that a Russian hacking gang who were arrested in connection with the trojan lurk were connected to Angler as the disappearance of Angler coincided with the arrest.

I find Angler an important case study for a few reasons. The first reason being the extent it was used in. Angler’s popularity grew mainly because of two reasons: ease of usage and the fact that it wasn’t easily detected by antivirus. The lack of discovery encouraged more users to use Angler for malicious activities. The user-friendly interface also proved to be a great boost for amateur users. The second reason I find Angler is important is because of the distribution options it offered. Users could use a variety of ways to bait victims. Angler was responsible for more than 40% of the attacks in 2015. Thirdly, the way Angler was provided as a service to the user was very interesting. This instilled confidence in users as support to the code was provided and new vulnerabilities were added regularly. To conclude, Angler was an important exploit kit for study as it reflects on multiple aspects of the malware market.

**References:**

1. The Ultimate Guide to Angler Exploit Kit for Non-Technical People

<https://heimdalsecurity.com/blog/ultimate-guide-angler-exploit-kit-non-technical-people/#standout>

1. A closer look at the Angler exploit kit

https://news.sophos.com/en-us/2015/07/21/a-closer-look-at-the-angler-exploit-kit/

1. Say Goodbye to the Angler Exploit Kit

https://securityintelligence.com/news/say-goodbye-to-the-angler-exploit-kit/