NOVETTA

BIRD'S EYE VIEW

ISSUE 001
MARCH 2015

SUMMARY

This summary makes use of published reports and open-source research to draw inferences. Novetta has not added any additional evidence or information to the threat groups or malware discussed below, unless otherwise indicated.

MIDDLE EASTERN CYBER ESPIONAGE ACTIVITY REVEALED

Two recent reports have linked cyber espionage activity to a group of Middle Eastern attackers. This group is said to have targeted victims using spear phishing emails, fake websites, and phony social networking accounts to deliver custom-made Windows and Android malware. Nearly 3,000 victims have reportedly been affected in three different attack campaigns since 2013, comprising mostly government, media, and financial organizations largely concentrated in the Middle East[1]. One campaign tied to this group specifically focused on Israeli victims in government, transportation, infrastructure, military, and academic organizations, while other campaigns have targeted a wider geographic range of victims.

The tactics, techniques, and procedures (TTPs) attributed to this group show that attack techniques that are not especially technically advanced can still be effective. This is in part strengthened by the relatively poor security practices of computer users in the Middle East. While other APT campaigns may use custom zero-day exploits and other advanced tools, this group was able to infect a wide range of targeted individuals using custom spear phishing emails. Social engineering can easily bypass even stringent perimeter security practices. In particular, fake social media profiles, such as those used by this group to target activists, have previously been used to infiltrate organizations. IT[2] and HR personnel are frequently targeted in these kinds of social engineering attacks, as they often have access to data of interest or credentials that could allow an attacker to penetrate further into a target network or compromise sensitive information.

These operations do not appear to be tied to a specific nation state: researchers have posited that up to 30 members are behind these attacks, all of whom are native Arabic speakers but are located across the geographic region, including some in Palestine, Egypt, and Turkey. Since the publication of the reports on this group, however, at least one identified Gaza Strip individual linked to the group's activity has denied any involvement[3], illustrating the potentially risky nature of attribution with cyber attacks.

Middle Eastern Cyber Espionage Activity Revealed

1 http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-arid-viper-bypassing-the-iron-dome
http://securelist.com/blog/research/68817/the-desert-falcons-targeted-attacks/

2 http://www.pcworld.com/article/2059940/fake-social-media-id-duped-securityaware-it-guys.html

3 http://www.forbes.com/sites/thomasbrewster/2015/02/24/trend-micro-worrying-attribution-of-gaza-strip-businessman/

EQUATION GROUP BEHIND ADVANCED CYBER ESPIONAGE CAMPAIGNS SINCE 2001

The Equation Group is a sophisticated cyber espionage group that has been linked by Kaspersky Sky researchers to the US National Security Agency. The group is said to have operated since at least 2001 and to have developed custom zero-day exploits, some of which were later used in the Stuxnet and Flame attacks. Tactics used by the group include zero-day exploits, an extensive malware library including OS X and iOS malware, wateringhole attacks, and advanced obfuscation methods[4]. The group is also reportedly capable of infecting hard drive firmware. Previous research into this area of attacks has covered the impact of mobile/baseband attacks[5], BIOS implants[6], router firmware backdoors[7], and other attacks impacting a wide variety of firmware. Use of firmware backdoors are notable because of their persistence and the fact that it is difficult for many users to detect potential problems. Furthermore, tampering of firmware can potentially be done along the supply chain well before reaching consumers, with little to no outward indications of compromise.

The Equation Group is likely interested in some of the same specific targets sought by other advanced nation-state groups: researchers first came across malware used by the Equation Group when investigating a computer in the Middle East also infected by malware from Regin, Turla, Careto/Mask, ItaDuke, and Animal Farm threat groups. Additionally, the Equation Group has reportedly gone to great lengths to reach high-value targets that may otherwise be unreachable via web-based attacks. For instance, on at least two occasions, the group physically tampered with CDs, affecting Oracle database installation CDs as well as CDs delivered to attendees of a science conference. The group has also potentially leveraged USB malware to reach air gapped networks.

Yet while the Equation Group apparently went to great lengths to reach certain machines, there are also indications that the group deliberately ignored vulnerable ones that did not meet the group's specific criteria for its targeting. These highly specific operations may speak to the environment that the Equation Group might operate in: not only stringent OPSEC but also possible legal or procedural frameworks limiting some activity. This is particularly apparent when comparing the Equation Group's activity to other known state-sponsored groups, whose operations are often uncovered due to the prevalence of infected machines or other indicators. For example, most recently a Chinese state espionage group was implicated in the watering hole attack on Forbes[8], which may have impacted a large number of the site's visitors rather than only those of interest to that group. This difference in operational procedures speaks to potential restrictions in place on these parties as well as to their perspective into the realms of intelligence gathering and cyber operations.

MILLIONS STOLEN BY ADVANCED CYBER CRIMINAL GROUP

The Carbanak cyber criminal gang is reportedly responsible for a string of attacks that have stolen over $17 million to date from over 100 financial institutions. The Carbanak group operates out of Eastern Europe and has targeted organizations worldwide in a series of ongoing attacks[9].

Equation Group Behind Advanced Cyber Espionage Campaigns Since 2001

4 https://securelist.com/blog/research/68877/equation-group-from-houston-with-love/

5 http://www.pcworld.com/article/216842/coming_soon_a_new_way_to_hack_into_your_smartphone.html, https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf

6 http://www.computerworld.com/article/2505096/cyberwarfare/researcher-creates-proof-of-concept-malware-that-infects-bios--network-cards.html

7 http://conference.hackinthebox.org/hitbsecconf2011ams/materials/D2T3%20-%20Guillaume%20Delugre%20-%20Reverse%20Engineering%20Broadcom%20NetExtreme%20Firmware.pdf

8 http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/10/forbes-web-site-was-compromised-by-chinese-cyberespionage-group-researchers-say/

Millions Stolen by Advanced Cyber Criminal Group

9 http://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

While most cyber crime targets individuals' banking accounts using fraud, the Carbanak group targets the banks themselves directly. Typically, the group gains an initial foothold into a target network with a spear phishing email with malicious attachments exploiting disclosed and patched vulnerabilities. Once the initial backdoor is executed and installed, the group is able to install additional malware tools to move laterally within the network, following typical methods often attributed to APT attacks. Following a period of reconnaissance into bank operations, money is stolen while the gang manipulates bank databases to hide the loss of money.

Carbanak's bank attacks show that this campaign, unlike many other banking attacks, is seeking highly specific targets: operations include a period of observation from within a bank's networks, allowing the group to learn how the bank operates. The group is said to spend 2 to 4 months on each bank in order to steal the maximum amount of money without alerting any bank security to their activity on a victim network.

The group's activity is strongly reminiscent of APT-style targeted attacks often attributed to nation-state cyber espionage groups; cyber criminal gangs have increasingly begun using advanced techniques, as observed with the string of POS breaches affecting retailers across the United States since late 2013. Much like actors behind well-financed cyber espionage campaigns, some cyber criminal gangs have the capabilities to develop or modify their own custom malware, while widely available commodity malware and exploit kits further contribute to a diverse attack toolkit. In particular, organized gangs in Eastern Europe or Russia continue to be among the most technically savvy cyber criminals, possibly receiving official or unofficial government support either through sharing of tools in the underground, personal contacts, or lack of prosecution for foreign victims of cyber crime[10]. It has also been suggested that many government and IT workers in the Former Soviet Union region have side jobs as hackers due to low wages.

Even with advanced techniques demonstrated by Carbanak and other cyber criminal gangs, it is worth noting that penetration of the targeted networks is often accomplished by basic tactics: spear phishing and exploiting known vulnerabilities. From there, attackers are generally able to gain an initial foothold into a network in order to elevate privileges and move laterally within the network. Skilled attackers can also potentially deploy additional tools in order to remain undetected for long periods of time while either monitoring activity or exfiltrating data. The ability of adept attackers to penetrate a network from a phishing email emphasizes the importance of OPSEC in every organization, even for users without privileged accounts or access to important data.

CYBER ESPIONAGE MALWARE LINKED TO FRENCH INTELLIGENCE OPERATION

Malware mentioned in leaked Communications Security Establishment Canada (CSEC) documents has reportedly been identified and analyzed by security researchers[11]. Dubbed Babar, the malware is believed to be one of the malware components used in Operation Snowglobe[12], along with a previously identified Remote Access Trojan (RAT), EvilBunny, and a possible unidentified third malware variant. According to CSEC, the malware is likely the work of a French-speaking nation-state group.

Given the difficulty researchers have had finding and identifying these malware families, they were likely intended to be used as espionage tools for

Millions Stolen by Advanced Cyber Criminal Group

[10] http://www.reuters.com/article/2013/08/22/russia-cybercrime-idUSL6N0G61KM20130822

Cyber Espionage Malware Linked to French Intelligence Operation

[11] https://blog.gdatasoftware.com/blog/article/babar-espionage-software-finally-found-and-put-under-the-microscope html, https://drive.google.com/a/cyphort.com/file/d/0B9Mrr-en8FX4dzJqLWhDblhseTA/

[12] http://www.lemonde.fr/international/article/2014/03/21/quand-les-canadiens-partent-en-chasse-de-babar_4387233_3210.html http://www.securityweek.com/researchers-analyze-spyware-linked-french-intelligence

a select number of victims. How exactly the Babar malware is spread has not been determined. EvilBunny, however, was observed spreading by exploiting an Adobe Reader vulnerability; it is unclear if the exploit was quickly incorporated into the operation's activity following disclosure of the vulnerability or was in fact a 0-day at the time[13].

According to leaked CSEC information, Operation Snowglobe targeted organizations in Iran, France, Norway, Spain, Greece, Algeria, and the Ivory Coast[14]. The configuration data of the identified malware provides similar insight into the targeting: command-and-control domains used for EvilBunny seemingly mimic domain names of a French newspaper, an Algerian university, and an Iranian news organization; the C2 domains of Babar, meanwhile, appear to be compromised legitimate domains in Algeria and Turkey. Overall, these geographic areas of interest seem to suggest that France is behind the operation.

The leaked CSEC document and discovery of these malware families suggest that other Western countries are possibly developing cyber capabilities for data collection and/or monitoring. Furthermore, the samples found by researchers appear to be a newer version of the malware to the version described by CSEC, suggesting continued development of espionage tools.

Cyber Espionage Malware Linked to French Intelligence Operation

[13] http://0x1338.blogspot.co.at/2014/11/hunting-bunnies.html

[14] http://www.securityweek.com/researchers-analyze-spyware-linked-french-intelligence