GTIC Monthly Threat Report

February 2018

Contents

GTIC Observations

In February during an incident response case, responders provided GTIC researchers with a malware sample for analysis and reverse engineering. The sample turned out to be Agent Tesla and contained three stages, two droppers and a payload. After analysis, it was clear to GTIC researchers that keyloggers have indeed come a long way and are now fairly advanced, yet inexpensive.

How does Agent Tesla work?

Stage one concatenates a series of strings and decrypts them to become objects, finally decrypting the resource's bytes into the second stage. During analysis, GTIC researchers successfully stepped into the final object call, allowing for the next stage to load for further analysis.

Stage two is named *rp.dll* and facilitates dropping the Agent Tesla payload. Function and variable names are obfuscated by using Unicode characters. In this case, all the function names were in Japanese. Additionally, all strings were obfuscated as byte arrays which were then deobfuscated via XOR. Google translates the function name as "*To give up*".

Similar to stage one, many of the grouped strings ended up loading as objects for decrypting in the final stage. The last object called the decryption function for the final payload which was then dumped directly into a file for further analysis.

GTIC researchers determined stage three was the actual Agent Tesla malware. The malware puts the current date in *%APPDATA%\des_date.txt* or, if that location is not available, depicts the current date in *%TEMP%\des_date.txt* if *%APPDATA%*. The function and variable names were heavily obfuscated and essentially unreadable, requiring additional analysis.

By running the analyzed functions in Dot Net String Decoder (dnsd), GTIC researchers determined the decryption function. Analysis indicated that the decryptor generates a password using the PBKDF1 algorithm by passing the details shown in Figure 1:

Password: amp4Z0wpKzJ5Cg0GDT5sJD0sMw0IDAsaGQ1Afik6NwXr6rrSEQE=
key salt: aGQ1Afik6NampDT5sJEQE4Z0wpsMw0IDAD06rrSswXrKzJ5Cg0G=
hash name: SHA1
number of iterations: 2

Figure 1. Credentials determined via Dot Net String Decoder (dnsd)

After this double pass of SHA1 with the key and salt, the first 32 bytes were used as the key for AES-256 CBC, which allowed for decryption of the encrypted string. Rewriting the decryption routine for a dnsd plugin yielded quick results by GTIC.

The key, salt, hash type, and initialization vector are the first four strings in the decrypted file. The location of the dropped malware is also listed as *\nxp\nxp.exe*, all of which is in clear text. GTIC identified registry changes for starting the malware at boot and PowerShell (PS) commands within the Agent Tesla malware itself during static analysis. Additionally, GTIC found an email address and upload information for Imgur.

Using dnsd to replace all the strings in the original binary allowed for deeper analysis with less obfuscation. Searching for the email address found in the strings yields the exfiltration mechanism. Other exfiltration mechanisms were available for use but not configured in this particular instance. Agent Tesla's website states it supports exfiltration via webpanel (HTTP), FTP upload, or SMTP. All samples received were analyzed by GTIC and configured for exfiltration to the same Gmail account. Even though NTT Security researchers knew the username and password, the email account was set up so only approved devices could log into the account. Without knowing the backup account email address, logging in was not possible. The backup email address was listed asata••••••@pro•••••••.com, with the user needing to fill in the • values. As of 16 Feb 2018, the password to the original account has been changed from *qwerty124*.

Agent Tesla shows that modern keyloggers are becoming increasingly complex and more likely to be able to evade anti-virus (AV) software. Simple keyloggers will be immediately found by AV and protection software. This malware contained several anti-analysis capabilities, including exiting if it determines it's running in a virtual machine and searching running processes for unwanted applications.

Agent Tesla is also fairly inexpensive, costing $12 USD a month and up to $69 USD for an annual subscription. Obtaining access to illegal software is growing simpler, especially now that cryptocurrencies are becoming more accessible to the general public.

Technical Indicators

1.1.1 Email Addresses

ariel[.]lee2000@gmail.com
ata••••••@pro•••••••.com

1.1.2 SHA-256

0ebe6e46e01e2e368378c1966a6da262509fb469bf7e95be900e2827bd215202 (2018HC_Info.exe.txt)
61e8699ae6cab354502a1d0a557b7cf11eeb43c8101d6fc8dedb06160568b565 (jri.exe)
66f979635aa9ac1ec8d0cf0c1add9b1e0572b91b1a979d13b189cc1d770064ed (Activity Survey.exe)
4981013848b272d53c3fc61a317f8896ba3f56c534db1e2363509423d6e044a3 (zmp.exe)
2279e2202d455baa0d1a8c2f43e36ba44d260d1c521d7b8af38389f051fbe61a (Club Sponsor Survey.exe)
9245e2d83f6fb069ec3ea41d3c8bc5b0db09e2c175b480996a7b86948874a3bc (nxp.exe)
0b04b277485d364544aeb03d664eb68b48c97d381c7612aa05e7c3489be86401 (rp.dll)

Cisco ASA Remote Code Execution Vulnerability

Threat Status: Critical

CVE-2018-0101

Severity: Critical (CVSS: 10)

Date: 16 Feb 2018

Remediation Details: Cisco has released free software updates that address the vulnerability

Affected Versions:

- 3000 Series Industrial Security Appliance (ISA)
- ASA 5500 Series Adaptive Security Appliances
- ASA 5500-X Series Next-Generation Firewalls
- ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- ASA 1000V Cloud Firewall
- Adaptive Security Virtual Appliance (ASAv)
- Firepower 2100 Series Security Appliance
- Firepower 4110 Security Appliance
- Firepower 4120 Security Appliance
- Firepower 4140 Security Appliance
- Firepower 4150 Security Appliance
- Firepower 9300 ASA Security Module
- Firepower Threat Defense Software (FTD)
- FTD Virtual (FTDv)

Analyst Note: A vulnerability in the XML parser of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code. It is also possible that the ASA could stop processing incoming Virtual Private Network (VPN) authentication requests due to a low memory condition.

The vulnerability is due to an issue with allocating and freeing memory when processing a malicious XML payload. An attacker could exploit this vulnerability by sending a crafted XML packet to a vulnerable interface on an affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system, cause a reload of the affected device or stop processing of incoming VPN authentication requests.

To be vulnerable the ASA must have Secure Socket Layer (SSL) services or IKEv2 Remote Access VPN services enabled on an interface. The risk of the vulnerability being exploited also depends on the accessibility of the interface to the attacker. For a comprehensive list of vulnerable ASA features please refer to the table in the Vulnerable Products section.

Cisco has released software updates that address this vulnerability. There are no workarounds that address all the features that are affected by this vulnerability.

Operation PZChao: Espionage Campaign with Cryptocurrency Mining Capability

Researchers recently reported on the possible return of an advanced persistent threat (APT) called Iron Tiger (Emissary Panda/APT27/Threat Group 3390). The group is suspected to be linked to the People's Republic of China (PRC). The newest campaign, which began in July 2017, is nicknamed Operation PZChao, and researchers have observed this campaign targeting technology, education, manufacturing, government, and telecommunications organizations across APAC, Japan and the United States.

This APT has been active since at least 2010, originally focusing on dissident groups, particularly those in Hong Kong. Iron Tiger also targeted other organizations in the APAC region, as well as government organizations in the United States. In 2013, the APT seemed to have shifted its focus, targeting primarily U.S. based technology and defense organizations.

The newest campaign, which shows some overlap in tools and command and control (C2) infrastructure used in previous operations, shows yet another shift in targeting – and, as mentioned above, focuses primarily on technology, education, manufacturing, government, and telecommunications organizations across APAC, Japan, and the U.S.

These shifts appear to follow both the overall geopolitical interests of China and generally align with each new Chinese five-year plan.

What does the group do?

Using custom malware, actors associated with Operation PZChao are capable of scraping passwords, providinge hackers with complete remote access and control of infected systems.

PZChao attackers delivered highly targeted spear-phishing emails containing a malicious VBS file, which retrieves second-stage payloads.

Compromised targets are controlled with a network of malicious subdomains, each containing the string *PZChao*. Of note, each of these subdomains is used for a specific task, such as malware delivery, upload or download, remote access control, etc.

This campaign also leverages a Bitcoin miner, disguised as a *java.exe* file. To avoid detection, the miner only runs every three weeks early in the morning, with the Bitcoin generated likely used to fund the campaign.

The primary goal of Operation PZChao appears to be cyber espionage, as suggested by the use of the Gh0sT remote access Trojan (RAT), which can log keystrokes, listen remotely, scrape credentials, as well as modify and exfiltrate files, and maintain persistent access.

References

Espionage malware snoops for passwords, mines bitcoin on the side

Ransomware Refuses to Take a Backseat to Cryptocurrency Malware

Nearly every day throughout February, the GTIC saw one or more stories trending across the globe concerning the meteoric rise of cryptocurrency-mining malware.

Threat actors are propagating various types of this malware via a variety of channels – phishing, unpatched exploits, plugin hijacking, and website code tainting, to name a few.

But in all the hype surrounding this worrying trend, the very real threat of ransomware persists.

In February, researchers identified a new CryptoMix variant which uses the *.SYSTEM* extension and uses generally the same functionality as other CryptoMix varients.

Saturn ransomware burst onto the scene as well, and as of this writing, there is no known method (apart from paying the ransom) to decrypt the files. Researchers continue the hunt for how Saturn ransomware is being delivered.

Additionally, there is a new strain of Gojdue ransomware dubbed ShurL0ckr which is incredibly difficult to detect, even for tools like VirusTotal, where only seven percent of anti-virus engines detected the new malware.

References

CryptoMix Ransomware
Saturn Ransomware
Gojdue Ransomware (ShurL0ckr)

Turla APT Updates Malware after Public Advisories

In November 2017, the United Kingdom's National Cyber Security Centre (NCSC) released an advisory highlighting suspected Russian Advanced Persistent Threat (APT) Turla Group's use of the tools Neuron and Nautilus. The NCSC recently identified a new version of the Neuron malware, modified to evade previous detection methods.

During its most recently identified campaign, which is designed to embed Turla into compromised networks and stealthily conduct espionage, Turla appears to have primarily set its sights on targets in the UK, particularly Windows mail servers and web servers.

It appears that the Neuron malware was updated five days after the NCSC published a public advisory on Turla activity. This suggests a fast-moving threat actor who understands the slow reaction time for enterprise environments to patch or update defenses.

The Neuron malware dropper mechanism was modified to avoid previous detection signatures published by the NCSC. Analysts suspect that Turla is responding to public reporting on its indicators of compromise (IoCs) and known tactics, techniques and procedures (TTPs). Alternatively, Turla may have had limited success following the advisory, following the implantation of additional defensive measures.

The sophisticated abilities of the group suggest that Turla is continually updating its attacks and developing its TTPs. It may take some time to discover many of the Turla group's newest IoCs.

IoCs and TTPs will continue to shift as mitigation efforts attempt to keep up. Until that time, although the NCSC believes that it is likely that standard anti-virus software will detect an updated Turla payload, it is imperative for organizations to know what 'normal' network behavior looks like in their network environment, while continuing to monitor network logs and administrator-level accounts.

References

NCSC Advisory: Turla group malware
Turla hacking group updated Neuron malware to attack UK organizations

About GTIC

The NTT Security GTIC protects and informs NTT Security clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including vulnerability disclosures, threat reports and white papers, visit the resource page on www.nttsecurity.com or our blog.