NTT Security

GTIC Monthly Threat Report

March 2018

Contents

GTIC Observations

Analysis

Threat Background

In March 2018, Global Threat Intelligence Center (GTIC) researchers investigated a client incident involving suspected command and control (C2) traffic to several IPv4 addresses with a malicious reputation. A closer inspection revealed these addresses were part of a botnet called 'Dark Cloud' aka Fluxxy and the malware beaconing out was GozNym, a modular banking trojan.

GozNym is a hybrid of Gozi ISFB and Nymaim malware. Gozi ISFB is an infamous banking Trojan malware whose source code has been publicly available since 2007, whereas Nymaim is a downloader for ransomware. This malware has been found in more than 24 U.S. and Canadian banks, stealing millions of dollars (USD). The inclusion of Nymaim components allows for stealth and persistence, whereas Gozi components allow banking Trojan capabilities to facilitate fraud. The suspected original author of GozNym had been arrested in 2016 in connection to GozNym distribution via a criminal network titled, Avalanche.

The Dark Cloud botnet is mainly hosted in Eastern Europe infrastructure by bulletproof hosting providers. The botnet infrastructure is known to host various malicious activities from carding forums to distribution of malicious emails and malware C2. *Fast-flux* is a technique leveraged to make tracking the infrastructure difficult by moving registered domains across multiple IP addresses over a given period of time by setting the time-to-live (TTL) extremely small.

Observations Briefing

In total, researchers identified 19 IPv4 addresses receiving HTTP traffic from the infected devices. This traffic consisted of POST requests to an 'index.php' file located in a random eight-character directory on each host. These requests sent back stolen data from the infected machines.

A public sandbox check for any malware reaching out to these same IPv4 addresses returned several different samples recently submitted in March. GTIC researchers are currently analyzing this malware, and several are portable executables (PE) were identified as Nymaim.

While analyzing the IPv4 addresses, researchers identified several different carding forum registered domains, such as paysell[.]bz. This carding forum sells everything from spamming tools and equipment to stolen PayPal accounts. Of the domains identified, researchers noticed each reversed to one of 10 different IPv4 addresses, mainly owned by providers in Romania, although others were hosted in Hungary and Bulgaria. GTIC observations show that RCS & RDS S.A. were the most popular providers for hosting Dark Cloud botnet infrastructure at this time.

Additionally, researchers used DNS requests for start of authority (SOA) records on each domain identified during the investigation, and noticed each TTL was set to approximately 150 seconds or 2.5 minutes, matching what is known about the fast-flux techniques used by Dark Cloud. This means that DarkCloud reregisters new domains every 2.5 minutes.

GTIC continues investigating Gozi ISFB, GozNym and Nymaim malware, as well as the Dark Cloud botnet, however, all are either actively being used and distributed or helping distribute malware and host carding forums.

Cisco IOS XE Software Static Credential Vulnerability

Threat Status: Critical

CVE-2018-0150

Severity: Critical (CVSS: 9.8)

Date: May 28, 2018

Remediation Details: Cisco has released software updates that address this vulnerability.

Affected Versions:

- Cisco IOS XE release 16.x

Analyst Note:

A vulnerability in Cisco IOS XE Software could allow an unauthenticated, remote attacker to log in to a device running an affected release of Cisco IOS XE Software with the default username and password used at initial boot. The vulnerability is due to an undocumented user account with privilege level 15 (the level of access permitted by the enable password) which has a default username and password. An attacker could exploit this vulnerability by using this account to remotely connect to an affected device. A successful exploit could allow the attacker to log in to the device with privilege level 15 access. A workaround to address this vulnerability, administrators may remove the default account by using the **no username cisco** command in the device configuration. Administrators may also address this vulnerability by logging in to the device and changing the password for this account.

Chinese APT Backdoor Found in CCleaner Supply Chain Attack

In September 2017, researchers discovered that several versions of CCleaner, a popular computer cleaning/optimizing software, had been infected by hackers, possibly compromising nearly two million users.

This compromise is believed to be attributed to APT17 (also known as Axiom Group and DeputyDog), an advanced persistent threat (APT) group suspected of having ties to China. Discovered about a decade

ago, APT17 has targeted major tech firms in the past, including the Operation Aurora hack in 2009, and NTT Security believes this APT will continue focusing on targets in the information technology industry.

In addition to the initial malware, research showed evidence of a second malware payload delivered only to certain targets, and researchers believe the second-stage malware was intended to maintain persistence in the targeted hosts.

Initial reporting suggested 40 targets downloaded this secondary payload, but additional research from Avast suggested hundreds of major tech firms could have been affected. It is quite telling that the targets were predefined in the C2 server configuration. This suggests the attack was designed to find hosts inside the networks of these specific targets, then deliver the secondary payload.

The fact that the targets receiving the second stage malware were all tech companies is also of significance. Perhaps not coincidentally, the newest Chinese Five Year Plan (FYP), released in 2016, suggested a focus on advancing its technological expertise. Historically, industries of focus in the FYP have been targeted by suspected Chinese actors, typically for intellectual property theft.

Researchers recently discovered yet another piece to this puzzle: a backdoor in ShadowPad, a remote cyber-attack platform and known "calling card" of APT17. This backdoor existed on several hosts, indicating attackers planned to further leverage these systems in the future.

This attack campaign appears to be an example of a supply chain attack, meant for very specific targets. Hackers often cast a wide net in the hopes of catching a handful of victims, while more advanced actors may attempt to infect many users in an effort to hide their hyper-specific targeting methodology.

Users are encouraged to be aware of all vendors in their supply chain, and implement an active vendor management program, as this attack vector is becoming more commonplace.

References

Avast: CCleaner hackers planned to infect victims with third-stage Chinese hacking tool

Growing Capabilities of APT37 (North Korean APT)

Security researchers recently published a report detailing the activity of suspected North Korea nation-state actors, APT-37 (a.k.a., Reaper). Researchers observed APT-37 targeting companies in the manufacturing, automotive, aerospace, health care and chemical industries, primarily in South Korea, though additional targets were also observed in Japan, Vietnam and the Middle East.

The capabilities and operations of APT-37 suggest a more sophisticated actor, as the group is reportedly targeting flaws in the Hangul Word Processor, a commonly used word processing application in South Korea. Security researchers also observed the group leveraging zero-day vulnerabilities and flaws in Adobe Flash Player, specifically CVE-2018-0802 and CVE-2018-4878.

Another suspected North Korean state actor, Group 123, has also previously exploited CVE-2018-4878, suggesting possible operational ties.

During this APT-37 campaign, the primary initial entrance vector into targeted networks appears to be strategic waterhole attacks on South Korean websites in the targeted industries. While APT-37 motivations remain unclear, the actors have successfully evaded law enforcement, exfiltrated stolen data and installed wiper malware. Unsurprisingly, the targeting also aligns with North Korean state interests.

Organizations within the targeted industries should immediately patch and update any instances of Hangul and Adobe Flash Player in their network environments.

References

North Korea steps up cyber powers with shadowy 'Reaper' hacker group

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.