NTT Security

GTIC Monthly Threat Report

November 2017

Contents

GTIC Observations: IoT Attacks

In November, GTIC observed a spike in targeted attacks against client-owned routers in several different industries. Analysis indicated some of the tactics, techniques and procedures (TTPs) observed matched recent high priority threats, along with relatively new vulnerabilities. Actions on objective included bitcoin mining, DDoS bot usage, administrative control and remote access. The following analysis considers the more targeted attacks against routers, as observed by NTT Security.

Routers Targeted

GTIC observed reconnaissance and other activity against several different routers. Linksys and D-Link routers were primary targets where attacks spiked to nearly six thousand some days. For Linksys, the majority of these attacks were authentication bypass attempts within the administrative consoles or dictionary brute-force login attempts where attackers were likely attempting to achieve remote access, posing as an authorized user. This helps explain the spikes in attacks.

Monero Miner

When analyzing attacks against D-Link routers, GTIC found attempts to exploit CVE-2017-3193 and CVE-2016-6277. A deeper investigation shows odd HTTP POST requests to several different public-facing client servers with Linux commands in the HTTP body.

NTT Security researchers traced the commands back to a malware sample in VirusTotal and Hybrid-Analysis, which, according to several anti-virus engines, is a Monero miner. A quick look at the network traffic from the sandbox suggests attackers mine Monero using mining pools from different remote servers.

GTIC has included the IOCs for this Monero miner in the technical indicators section of this report.

IOT_Reaper

While triaging the attack sources, GTIC found two addresses which targeted two or more different types of routers. This information can be found below.

177.80.161[.]59 - Linksys and D-Link

Continent: South America
Country: Brazil
City: Sao Bernardo Do Campo
Attack Activity: Attacks attempted to exploit an Authentication Bypass vulnerability in Linksys Routers. The vulnerability is caused by a lack of input validation when handling a crafted HTTP request. Additionally, researchers observed attacks on D-Link DIR800 Series routers. These attacks attempted to exploit a vulnerability which may allow information disclosure.

125.133.107[.]187 – D-Link and Netgear

Continent: Asia
Country: South Korea
State: Gyeonggi-do
City: Seongnam
Activity: This host appears to be compromised with IOT_Reaper. When analyzing the HTTP requests, the following string was included, *'echo+nuuo+123456'*.

According to Radware, this string is hardcoded into IOT_Reaper to check for remote code execution (RCE) capability prior to propagation attempts. In searching for follow-up requests, GTIC discovered logs detailing more HTTP requests to the same client routers, except the requests were for '*setup.cgi'* where attackers attempted to leverage the 'syscmd' function inside of the script to execute *wget* and pull down malicious configuration files from kagbe[.]nl.

News spread of IOT_Reaper in October 2017; however, the bot still seems to be very active in attempting to establish a larger foothold, although DDoS attacks are yet to be observed.

Technical Indicators

Domains:
Kagbe[.]nl

IPv4 Addresses				
201.82.147[.]228	186.220.1[.]166	179.105.19[.]55	177.32.254[.]75	201.21.160[.]185
191.180.125[.]142	189.32.221[.]226	177.81.25[.]180	177.83.124[.]114	191.180.127[.]170
179.158.250[.]105	187.23.160[.]187	179.209.45[.]209	191.188.20[.]73	177.142.117[.]57
187.36.155[.]250	187.21.240[.]129	177.141.248[.]71	201.82.153[.]11	179.219.112[.]7
179.157.61[.]181	177.33.226[.]61	187.180.190[.]85	186.206.80[.]55	189.54.76[.]174

Figure 1. Monero miner IoCs

HIDDEN COBRA Continues Operations Against Multiple Industries

HIDDEN COBRA (a.k.a., Lazarus Group) threat actors, thought to be associated with the government of North Korea, have been conducting operations since at least 2009. Their activity has become increasingly sophisticated and includes a wide range of targets, to include aerospace, telecommunications and finance industries.

HIDDEN COBRA actors generally target systems running older, unsupported versions of Microsoft Windows operating systems, as those systems may remain unpatched or have out-of-date software, providing environments ripe for exploitation. In addition, HIDDEN COBRA actors have repeatedly leveraged Adobe Flash player vulnerabilities as the initial access vector.

US-CERT recently released two alerts highlighting HIDDEN COBRA activity, detailing operations leveraging a remote administration tool (RAT), FALLCHILL, and a Trojan, Volgmer.

FALLCHILL, in use since 2016, is the primary component of a command and control (C2) infrastructure which uses multiple proxies to obfuscate network traffic between HIDDEN COBRA actors and a victim's system. The communication flows from the victim's system to HIDDEN COBRA actors using a series of proxies.

In use since at least 2013 to target government, financial, automotive and media industries, Volgmer is a backdoor Trojan capable of internal reconnaissance, registry key modification, system command execution and more.

These US-CERT alerts include IOCs related to HIDDEN COBRA, IP addresses linked to systems infected with Volgmer malware, malware descriptions, along with associated signatures. This report details the findings and IOCs associated with HIDDEN COBRA's Volgmer backdoor.

Previous US-CERT alerts pertaining to HIDDEN COBRA activity include an alert in June 2017 (updated with additional details in August) detailing suspected HIDDEN COBRA DDoS botnet infrastructure. US-CERT also published details on suspected HIDDEN COBRA malware, Delta Charlie, in August 2017.

HIDDEN COBRA has been an active threat, and NTT Security expects these trends to continue for the foreseeable future. NTT Security issued security bulletins to clients concerning these alerts and continues to trend these IoCs.

References:

HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL

HIDDEN COBRA – North Korean Trojan: Volgmer

Fancy Bear Exploiting Popular Microsoft Office Feature

Fancy Bear, also known as APT28, Sofacy Group and Pawn Storm, is an advanced persistent threat (APT) group, widely suspected to be associated with Russian intelligence services.

Researchers have discovered a phishing campaign in which this APT emailed a malicious Word document concerning the recent terror attack in New York City.

Using current geopolitical and news topics to create spear-phishing campaigns is not a new tactic by any means. This technique continues to be used because it is highly effective.

The new tactic in this campaign, which employs a sophisticated multi-stage infection process, leverages Microsoft Office's Dynamic Data Exchange (DDE) feature. DDE sends messages between applications which share data, and uses shared memory to exchange data between applications. Attackers have mis-used DDE to execute hostile scripts, bypassing traditional script protections. Since DDE is a legitimate method, its use by threat actors will likely appear as normal system behavior, allowing attackers to execute these attacks while remaining hidden.

So far, targets appear to be mostly limited to users in Germany and France, and at this time, there is little intelligence available concerning additional targets or the true intent of this campaign. Typical targets of this APT group (APT28) have historically been government, military and security organizations, and the campaigns have focused on U.S.-based topics. One of the topics APT28 included in the Word document was a U.S. Army exercise, SabreGuardian, suggesting that those associated with that particular exercise may be specifically affected.

GTIC analysts expect that threat actors will continue to continue to exploit DDE, especially if remediation efforts are not implemented. The GTIC recommends that users make sure Windows Protected Mode is enabled. This DDE attack method requires user interaction, and NTT Security reminds users to not click through prompts when opening an email attachment – especially those asking to run *cmd.exe* or *PowerShell*.

References:

Fancy Bear hackers are now exploiting the New York terror attack to spread their malware

Microsoft Security Advisory 4053440: Securely opening Microsoft Office documents that contain Dynamic Data Exchange (DDE) fields