GTIC Monthly Threat Report

September 2019

Contents

ECHOBOT Evolution from Mirai Clone to Extended "Spray and Pray" Exploitation

Lead Analyst: GTIC Research Team

ECHBOT first came into the limelight in June 2019 when our Cyber Threat Alliance[1] (CTA) partners at Palo Alto's Unit 42 wrote about a new variant of Mirai which added eight new exploits targeting additional Internet of Things devices. Over time we found added exploitation capabilities as ECHOBOT continued to evolve. A slight lull in late June through mid-July appears to have been due to the threat actor(s) building more capabilities into the bot, as it now boasts over 60 exploits. NTT subsequently observed an increase in traffic related to ECHOBOT between July and August.

To gain a better understanding of ECHOBOT's innate functionality, researchers analyzed 17 samples. The objective was to identify how and when new features were added or changed as the bot evolved. Based on identifiable properties, observations, and other attributes of the samples, six operational categories were identified.

- **Scan** – Methods for scanning various products and or services. In this dataset, not including standard ECHOBOT activities, 57 were identified.
- **Attack** – Methods for attack generation using various TCP/IP protocols; 11 were identified in the samples.
- **Traffic Generation** – Methods for generating traffic and or commands; four in total were identified.
- **ECHO** – Methods specifically related to ECHOBOT; this was consistent with all analyzed binaries.
- **Uncategorized** – Two methods were found that did not fit the same convention as the others. They specifically targeted two product lines; however, they are implemented differently than the others that fall into the Scan category.
- **Flood** – Three functions were identified for providing denial of service (DOS) or distributed denial of service (DDOS) attack functionality.

The earliest ECHOBOT sample was originally submitted to VirusTotal on 20 February 2019. This sample included Flood, Traffic Generation, Scanning, Attack, and ECHO properties. This is the only

[1] https://www.cyberthreatalliance.org/

binary containing overtly defined traffic generation functionality. It also uses only XMAS scanning for reconnaissance. This activity evolved as the bot matured. This initial version also includes a reference to downloading a cryptocurrency miner, which deviates from newer samples of Echobot.

Since the submission of the original sample, ECHOBOT has undergone a series of evolutionary steps. Examples of these changes include new samples of ECHOBOT in June targeting over 25 unique vulnerabilities, and a spike in exploitation attempts in August dropping the latest downloader titled ‘richard’. This highlighted another infrastructure change and a deviation from the previous downloader naming structure.

Although ECHOBOT infrastructure was offline as of late September, NTT observed exploitation attempts of these vulnerabilities – along with attempts to deploy ‘richard’ – throughout most of the month. We anticipate this will shift again soon to a new IP/ISP as ECHOBOT continues to evolve.

For further details, read more at the NTT blog[2] on ECHOBOT.

[2] https://technical.nttsecurity.com/post/102frhw/echobot-evolution-from-mirai-clone-to-extended-spray-and-pray-exploitation

Spotlight on Manufacturing

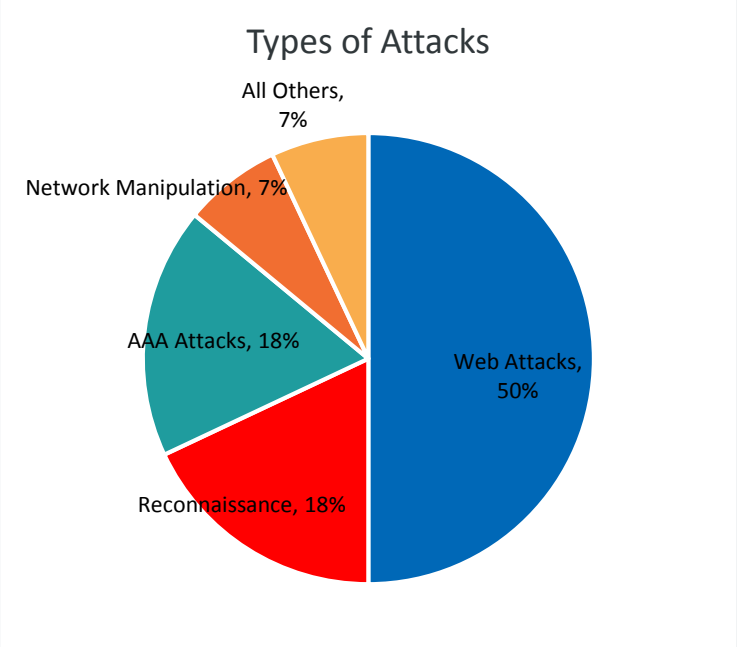
Lead Analyst: Jon Heimerl

According to data gathered for the annual NTT Global Threat Intelligence Report (GTIR), Manufacturing has historically been one of the most highly attacked industries year after year. Web, denial of service (DoS), brute force, and a plague of IoT/OT attacks challenge not only manufacturing organizations, but their vendors, suppliers, and transportation providers. At a time when it is even more important that manufacturing organizations manage margin, economies in supply management, and resilient operations, those same organizations are challenged with attacks which can have dramatic impacts on their capability to deliver.

Based on reviewing data from NTT's GTIR, in the past five years, manufacturing has only been out of the top five most highly targeted industries one year, and by less than 2% of total attacks. Current hostile activity is mostly consistent with historical activity.

Technical Attacks

From mid-August to mid-September, hostile activity within manufacturing was dominated by DoS and brute force attacks. These attacks tend to show as spikes of transient activity and irregular volume, and can often impact operations.



Globally, 32% of all attacks tend to be some form of web attack (application specific or web application attacks). From mid-August to mid-September, 50% of attacks against manufacturing were web attacks. Throughout 2018, web attacks accounted for 50% of all attacks against these same manufacturing organizations, so the most common types of attacks have not changed significantly. These attacks tend to be highly automated and more common in industries with a strong web presence.

Authentication, authorization, and accounting (AAA) attacks are attempts to bypass proper authentication and authorization to gain access to organizational resources. Researchers observed similar attacks throughout 2018, though AAA attacks and network manipulation attacks

against manufacturing have all increased in the past year. Some of these attacks indicate more focused activity from attackers with a high degree of skill or better tools.

Profiling Technical Attacks

For most industries, the actual vulnerabilities exploited and technologies attacked is narrow. This is just as true for attacks against manufacturing. Nearly 89% of all exploit attempts in the previous month focused on the top five most targeted CVEs. It is also worth noting that three of the top five CVEs are over two years old and all five CVEs have patches or mitigating controls available.

Vulnerability CVE	Technology	CVSS
CVE-2016-3303	Microsoft Live Meeting	9.3
CVE-2014-6278	gnu bash	10.0
CVE-2017-7973	Schneider Electric uMotion Builder	7.5
CVE-2019-9184	J2store for Joomla!	7.5
CVE-2019-0708	Microsoft Windows 7	10

CVE-2014-6278 is related to Shellshock and, historically, most of these attacks have been reconnaissance activity to determine if the vulnerability is present.

CVE-2019-9184 is a more recent vulnerability, as it was defined in February 2019. This vulnerability saw a surge in activity starting in August 2019. This is an SQL vulnerability in the popular Joomla! shopping cart extension. Analysis suggests a majority of these detections are blind SQL injection attempts, which are most likely reconnaissance against servers running Joomla!.

CVE-2019-0708 is also known as BlueKeep, a vulnerability in the Remote Desktop Protocol (RDP) available on select Microsoft operating systems. BlueKeep gathered attention when first announced not only because of the potential numbers and variety of affected systems, but because the vulnerability is wormable – making successive infections easier and recovery more challenging. BlueKeep saw a resurgence in attention around 6 September when researchers announced they had created proof of concept code and had implemented exploit code within Metasploit.

81% of all detected attacks against manufacturing clients during the timeframe focused on the top three vulnerabilities, all of which are more than two years old.

As with most industries, manufacturing also faced a wide variety of malware. Observations revealed that, while over 20 malware variants were detected, nearly 74% of all malware detections within manufacturing clients were related to China Chopper. China Chopper is a web shell designed to remotely control web servers.

Conclusions

The manufacturing industry has consistently been among the industries most targeted by malicious actors and trends suggest continued high levels of activity. Though much of the hostile activity now being detected appears to be more focused on reconnaissance, organizations should keep in mind that

prolonged periods of reconnaissance are often followed by sustained attacks and other hostile activity. While technical attacks against manufacturing organizations in the August/September timeframe have affected a wide variety of systems, nearly 89% of all detected exploit attempts focus on five vulnerabilities.

Truly mitigating ongoing attacks requires a multi-level security program with a wide variety of overlapping technical and non-technical controls, however, focusing on these recommendations is a start:

1. Prioritize patching – especially on critical and exposed systems, and especially for systems affected by the top five vulnerabilities.
2. Protect against web attacks. Manufacturing organizations should take actions to protect against the sheer volume of web attacks they are experiencing. Improve internal development processes, vet applications developed by external sources, implement web application firewalls, and perform web app testing to help identify vulnerabilities.
3. Review webserver policies and controls. 74% of all detected malware was in relationship to China Chopper, which enables remote management of web servers. It appears likely that attackers are targeting this as an effective attack vector at this time. It is worth verifying that your organization is not affected by China Chopper and is implementing controls which will increase the likelihood of future detection.

Reviewing the vBulletin Threat

Lead Analyst: Terrance DeJesus

On 23 September 2019, an anonymous researcher using Guerilla Mail uploaded Python code for a vBulletin remote code execution (RCE) vulnerability. CVE-2019-16759[3] affected any 5.x version of vBulletin. The code itself includes 27 lines, is straight-forward and easy enough to start mass-scanning and exploitation. In this section, we review what vBulletin is, telemetry data from our MSS, as well as open-source data to identify whether or not this is a considerable threat.

vBulletin is a proprietary saw forum software package written in PHP which uses a MySQL database server. This software is similar to WordPress, Joomla!, Drupal, and other Content Management Systems (CMS). As vBulletin was passed from company to company via acquisitions, technical support confirmed that vBulletin 3 was considered “End of Life” software, with no further development planned. However, vBulletin 5 is actively managed and versions 5.x of the software received a patch on 25 September 2019 to mitigate this vulnerability.

During our initial research, we found there are roughly 83,000 sites still running some form of vBulletin. In addition, NTT researchers identified HTML code representing ‘vbulletin’ in approximately 3,500 sites; however, these results contained IP addresses, hostnames, and organizations. Therefore, mass-scanning and exploitation is very simple to accomplish. Previously, NTT only observed a handful of vBulletin exploit attempts against CVE-2015-7808, but upon the release of CVE-2019-16759 and deployment of updated signatures NTT immediately observed an increase in scanning and exploit attempts.

Although threat actors may not be highly focused on vBulletin targeting, this exploit brings an opportunity to target the MySQL databases behind this application. The Global Threat Intelligence Center (GTIC) at NTT has implemented detection signatures at the time of this writing to protect our client base. Additionally, GTIC suggests affected clients evaluate and apply the patch to mitigate exposure.

[3] https://nvd.nist.gov/vuln/detail/CVE-2019-16759

WannaCry – Still Causing Tears?

Lead Analyst: Danika Blessman

Since it first emerged on the cyber threat scene in 2017, WannaCry has been the bane of security professionals' lives; and it hasn't let up.

In May 2019, it was reported that over a million computers *remained* at risk of infection. As recently as August 2019, WannaCry remained the most leveraged ransomware, with over 7,000 new variants emerging in that month alone.

Fascinatingly, researchers note that the original WannaCry file was detected only 40 times in attempted attacks, a number so low that it could be attributed to simply testing the malware as opposed to a real attack. Alternatively, the 40 detections could have indicated a very targeted campaign, selectively seeking out a few specially targeted hosts. This scenario is possibly more realistic as WannaCry has been attributed to North Korean threat actors. (On a side note, were recently levied against the actors thought to be responsible for WannaCry.)

But, like any other threat, users who don't mitigate are still susceptible[4]. Even the Melissa virus, now 20 years old – and Conficker, over a decade old – are still threats to those hosts which have not yet been patched.

What is different about WannaCry?

WannaCry was a self-spreading worm, meaning that, if it was not immediately defended against, it spread much more quickly. New research shows that the continued survival of WannaCry in the wild was primarily due to the ability of its newest variants to bypass the "kill switch" by which the initial outbreak was thwarted in 2017.

It was recently reported[5] that there are close to 13,000 variants in existence today, many of which are able to evade this "kill switch." Newer variants spread more effectively and remain undetected longer than the initial WannaCry. Interestingly, the analyzed variants have proven incapable of encrypting files on infected machines due to their malicious payloads being corrupted.

[4] https://nakedsecurity.sophos.com/2019/09/18/wannacry-the-worm-that-just-wont-die/

[5] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf

Ironically, these new variants have become an “accidental vaccine” against the initial WannaCry, offering yet unpatched hosts a type of “immunity” from later attack via the same malware. (Of note, it is NOT advised to become infected with a newer variant of WannaCry to prevent infection of the initial variant!)

Could there be additional factors at play behind this apparent resurgence in WannaCry? Since WannaCry was attributed to North Korean actors, is it *possible*, given the current geopolitical climate[6], that WannaCry was re-deployed by its initial developers? Granted, there are MANY users who have not yet patched their systems to mitigate this threat. Given this lack of patching and the geopolitical climate, was the WannaCry resurgence planned? Was it opportunistic? Or were these variants simply born of other actors trying to make a buck by capitalizing on an infamous ransomware brand?

Regardless of the reasoning, NTT recommends immediate patching for WannaCry variants. As always, standard best practices remain the most effective preventative measure against WannaCry. It is also recommended that users keep an up-to-date inventory of all endpoints on a network and maintain current patching.

[6] https://securityboulevard.com/2019/09/us-treasury-levies-sanctions-against-north-korean-group-behind-2017-wannacry-ransomware/

NTT Annual Reports

Risk:Value 2019

In 2019, 33 percent of organizations around the world would consider paying a ransom to a hacker rather than investing more in cybersecurity because paying the ransom is cheaper. Read more about this and other trends in the 2019 Risk:Value report.

Download your copy today!

2019 Global Threat Intelligence Report

This year's report focuses on several security challenges we have observed in organizations over the past year. Our analysis shows an escalation in coin mining, web-based attacks, and credential theft, along with changes in the sectors most targeted.

Download your copy today!

Global Threat Intelligence Center (GTIC)

The NTT Global Threat Intelligence Center protects, informs, and educates NTT clients through the following activities:

- Threat research
- Vulnerability research
- Detective technologies development
- Threat intelligence management
- Communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking its threat and vulnerability research and combining it with its detective technologies development to produce applied threat intelligence. Its mission is to protect and provide NTT clients with services and tools to prevent and provide early warning notifications of risks and threats 24/7.

Threat intelligence management is where it all comes together. The GTIC continuously monitors the global threat landscape for new and emerging threats using NTT's global internet infrastructure, clouds, and datacenters along with third-party intelligence feeds. NTT works to understand, analyze, curate, and enrich threat data using advanced analysis techniques and proprietary tools, then curates and publishes these for the benefit of NTT clients using the Global Threat Intelligence Platform (GTIP).

About us

NTT is a leading, global technology services company. We believe that together we do great things. We've combined the capabilities of 28 remarkable companies to create one, leading technology services provider. We partner with organizations around the world to shape and achieve outcomes through intelligent technology solutions. For us, intelligent means data driven, connected, digital, and secure. As a global technology services provider, we employ 40,000 people to be where our clients are based, across 57 countries. Working together, we deliver sustainable outcomes to your business and the world. Innovation is part of our DNA. So, we strive to move forward, challenge the status quo, and drive excellence through the technologies we integrate and the services we deliver around the world. Together we enable the connected future.