NTT Security

GTIC Monthly Threat Report

August 2019

A Global Threat Intelligence Center
publication from NTT Security

Contents

Automated Clustering of Bots

Lead Analyst: Kenji Takahashi

Gartner estimates there will be more than 64 billion IoT devices by 2025, up from about 10 billion in 2018. At this rate, roughly 15 thousand new devices will be connected to the internet by the time you finish reading this article. At the same time, we are experiencing this growth in devices, the threat of botnets is increasing dramatically.

During the past year, the connected world experienced a considerable jump in botnet activities. For example, the number of detected command and control (C&C) servers increased from 9,503 to 10,263. We need to face the reality that not all IoT devices are being properly secured, and are becoming part of these botnets. To address the challenge of the growing threats of botnets, NTT Security has been analyzing client data to better understand the inner workings of botnets by applying machine learning to the analysis of the Internet backbone data; in particular, netflow data.

In this article, NTT discusses a new method of automated detection and clustering of bots propagating the internet. Clustering is a machine learning technique to group objects into “clusters” based on the calculated similarity. In the proposed method, objects are bots, and similarities between them are calculated based on netflow data generated by those bots. Bots are “perpetrators” which directly attack victims, such as via distributed denial of service (DDoS) under the control of C&C servers. For example, researchers have observed a strain of Mirai IoT malware taking more than 100,000 home routers under its control. Also, botnets evolve rapidly, resulting in many variants. Keeping up with the sheer number of bots and their variants requires automated support for researchers. To accommodate this, NTT has developed a method to detect and cluster bots for analysts to use as basis for further analysis and validation of the entire botnet structure.

Currently-leveraged methods consist of two steps:

1. feature subspace and
2. frequent pattern mining based clustering.

Figure 1 provides further descriptions of how these methods work, which is also described further in a 2019 IEEE Conference.

The first method separates more than 300 features to several feature subspaces (e.g., flow-size based subspace or TCP flag based subspace) and clusters all hosts in each subspace. As a result, each host may have a set of multiple sub-labels from different subspaces. Second, the proposed method applies frequent pattern mining for all hosts to discover frequent combinations of multiple sub-labels. Finally, analysts identify several hosts with different frequent combinations. Because each label in a subspace represents a partial characteristic (e.g., low-size flows or high TCP-SYN rate), it is easier to explain the holistic behaviors of hosts with the same set of partial characteristics. Furthermore, by interpreting these results in combination, we can identify the characteristics of bots – something which would be difficult for humans to do, given the 300-plus features being evaluated. This automated interpretation enables security analysts to prioritize additional analysis in an effective and efficient manner, according to the bot cluster characteristics of greatest interest or relevance.

By combining subspace clustering and frequent pattern mining, the proposed method extracts features considered to be bots from the internet in a scalable manner. Furthermore, it can tell which features represent the role of each cluster.

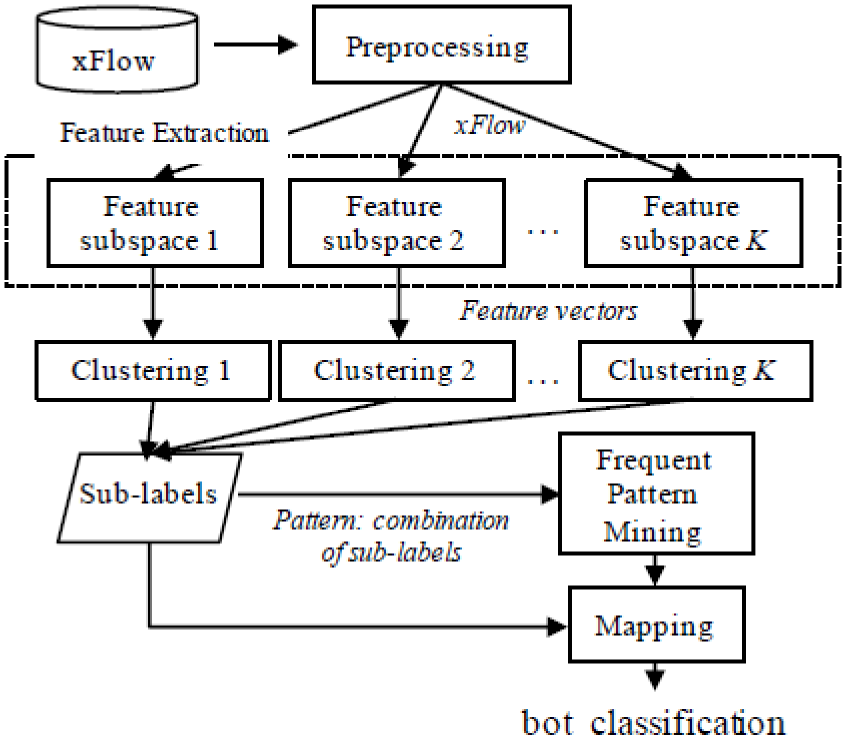
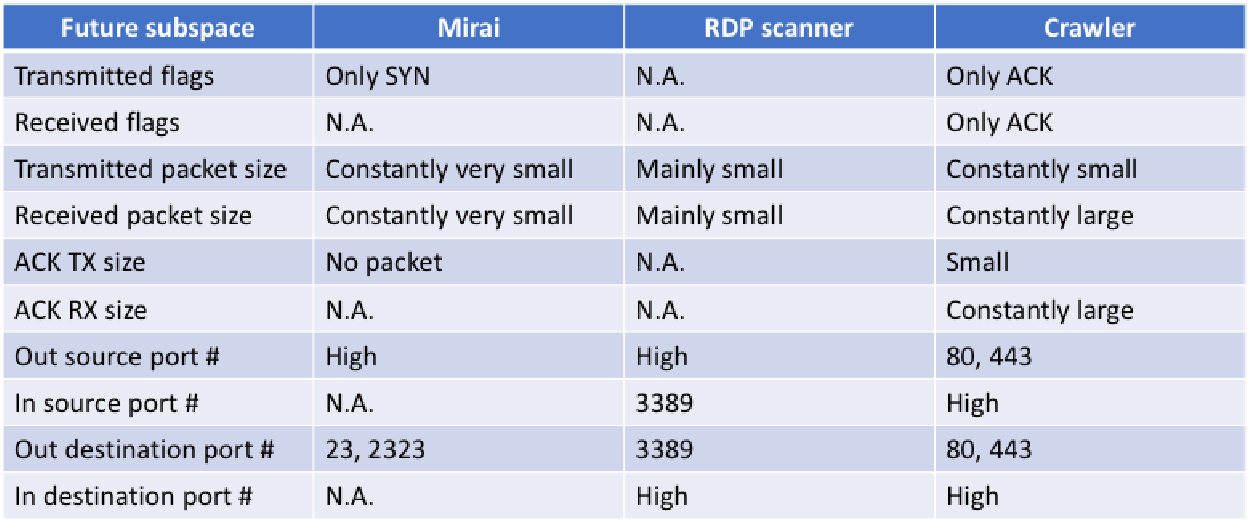


Figure 1 Overview of automated bot clustering process

By using this method, NTT detected 295 bot clusters from 408,118 IP addresses. Furthermore, we identified the functionalities of the bot clusters. Figure 2 shows the details of three clusters: Mirai, RDP scanner, and crawler.



Future subspace	Mirai	RDP scanner	Crawler
Transmitted flags	Only SYN	N.A.	Only ACK
Received flags	N.A.	N.A.	Only ACK
Transmitted packet size	Constantly very small	Mainly small	Constantly small
Received packet size	Constantly very small	Mainly small	Constantly large
ACK TX size	No packet	N.A.	Small
ACK RX size	N.A.	N.A.	Constantly large
Out source port #	High	High	80, 443
In source port #	N.A.	3389	High
Out destination port #	23, 2323	3389	80, 443
In destination port #	N.A.	High	High

Figure 2 Examples of identified bot clusters

In an automated manner, NTT identified traits associated with sets of botnets and was able to successfully classify their related activity to define botnet clusters. NTT will continue improving the methods used to protect our networks and customers in the era of IoT. Improving the speed and efficiency of this identification and clustering process has the potential to improve defensive and protective measures associated with mitigating the threats of botnets, especially as they continue to evolve.

References:

1. https://www.businessinsider.com/internet-of-things-report
2. https://www.spamhaustech.com/botnet-threat-report-2019/
3. https://arstechnica.com/information-technology/2017/12/100000-strong-botnet-built-on-router-0-day-could-strike-at-any-time/
4. Araki, Shohei, et al. "Subspace Clustering for Interpretable Botnet Traffic Analysis."*ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019

Cyber Threat Alliance – A Lesson in Collaboration

Lead Analyst: Jeremy Nichols

In the spring of 2018, NTT Security announced a partnership with the Cyber Threat Alliance (CTA). The CTA is a not-for-profit organization working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field.

While we were certainly excited about the partnership to begin with, it has proven more fruitful than initially expected. The CTA facilitates sharing of tactical and strategic intelligence between members as part of their ‘give to get’ model. There are several key areas of the partnership which helped NTT improve research and hunting, timeliness of protections and communication processes, as well as participate with other members in joint research and analysis.

Technical Sharing

As an affiliate member, NTT must meet scoring requirements related to the threat intelligence we share. Each tactical indicator and surrounding context are scored based on factors such as whether they have been observed or submitted before by other members. This model has served as a good gauge of not only the value and timeliness of the intelligence we’re producing, but our processes, procedures, and automation as well. This model ensures members aren’t merely regurgitating OSINT or honeypot sightings which nearly all of us observe regularly.

As we’ve progressed in the partnership, this sharing has helped the NTT Global Threat Intelligence Center (GTIC) improve our research and hunting efforts against our data sources. We retrieve the intelligence shared by other CTA members and aggregate this data into our Global Threat Intelligence Platform (GTIP) to support research initiatives, telemetry, and analysis. This helps us cast a significantly wider net as we investigate, compare, and profile the threats our customers face.

Situational Awareness

NTT also has participated in several CTA committees, discussing ongoing and breaking research with other member organizations. Additionally, we have had the opportunity to participate in several joint analysis subcommittees – highlighting research in the areas of illicit cryptomining and threats against edge devices with other members.

An additional aspect of this awareness is the CTAs ‘early sharing’ process, in which members share upcoming research and blogs in advance of their publication. While the information is generally under embargo until the member goes public, this often allows NTT to prepare protections or notifications for our customers, notify our global SOCs and hunt for the IOCs within our data before the information being publicly available. This has provided significant value to NTT and our customers behind the scenes.

Moving Forward, Together

As we move forward, we are working with the Cyber Threat Alliance to adopt the upcoming version of their platform, enabling even more contextualization of intelligence, automation around the ‘early sharing’ and improved scoring. We’re very excited to continue this partnership and help to protect not only ourselves and our customers, but the digital ecosystem as a whole.

References:

1. https://www.cyberthreatalliance.org/press-releases/cyber-threat-alliance-marks-first-anniversary-new-members-continued-momentum-global-threat-data-sharing/
2. https://technical.nttsecurity.com/post/102f28k/the-cryptojacking-threat-landscape-a-report-from-the-cyber-threat-alliance
3. https://technical.nttsecurity.com/post/102fjfb/the-forgotten-threat-cta-joint-analysis-report-on-perimeter-and-edge-devices

Monthly Observations

Lead Analyst: Terrance DeJesus

Targeted Software

As shown in Figure 3, J2Store was amongst the most popular software targeted by exploit attempts. This can be attributed to CVE-2019-9184, which is an SQL vulnerability in the popular Joomla shopping cart extension. Analysis suggests a majority of these detections are blind-SQL attempts, most notably, reconnaissance against servers running Joomla. There is no indication that this vulnerability is being actively used in targeted attacks at this time.

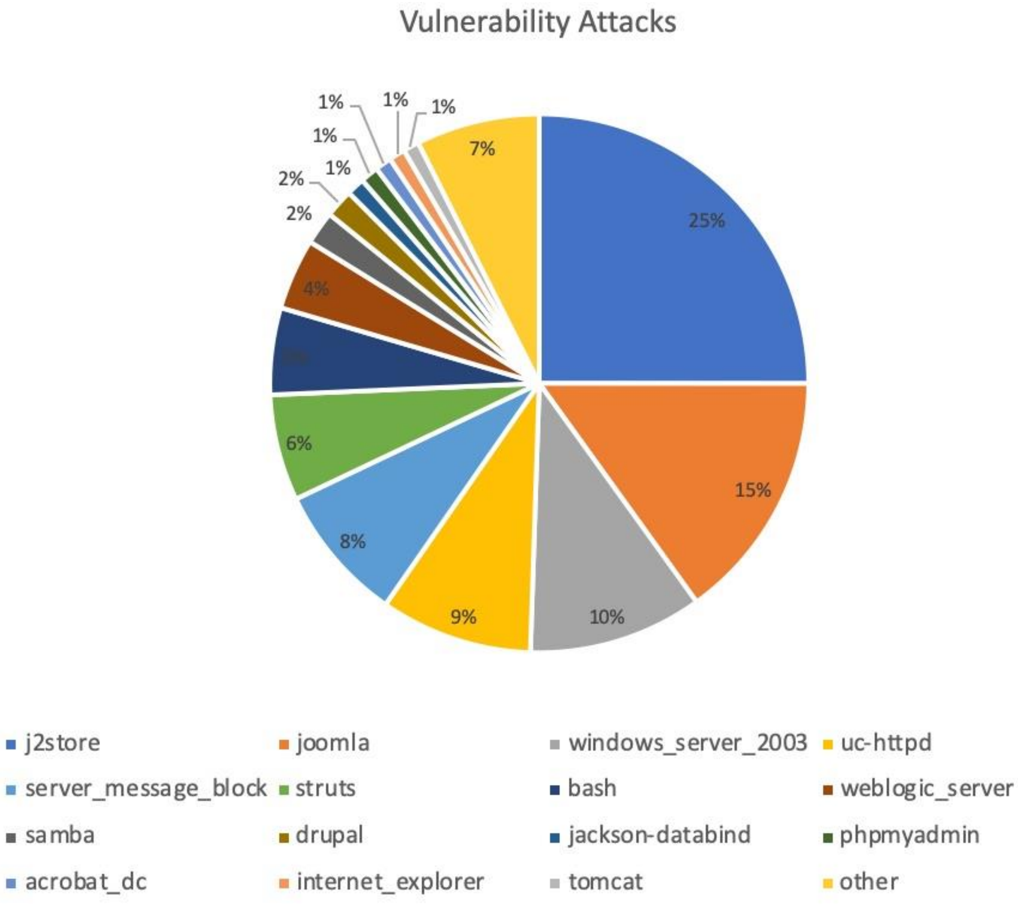


Figure 3 Vulnerability Attacks by Software Target

CVE-2019-9184 is applicable for an extension to Joomla, so exploit attempts against Joomla accounted for 40 percent of all vulnerability-driven attacks in August. CVE-2015-8562 was the only other Joomla vulnerability being actively targeted in this timeframe. CVE-2015-8562 is easy to exploit by manipulating the User-Agent in custom HTTP requests. Cyberattacks focusing on this vulnerability first appeared in

2015, soon after it was disclosed. At that time, researchers reported the installation of backdoors and botnets after successful exploitation. Attacks using exploits for CVS-2015-8562 continue to this day but generally tend to be opportunistic as threat actors are hoping patches have not been applied in the four years they have been available.

Another popular content management system (CMS) software, Drupal, has risen in targeting popularity since the beginning of August, thanks to vulnerabilities CVE-2019-6340 and CVE-2018-7600. Specifically, researchers have noted a 46 percent increase in Drupal attacks since the beginning of August. These vulnerabilities are the result of development issues pertaining to the sanitization of user input and configuration modules with poor error handling. It is worth noting that Joomla and Drupal are in the top three market share of all CMSs.

Oracle WebLogic Vulnerabilities

Oracle WebLogic is a Java EE application server which is part of Oracle's Fusion Middleware portfolio, supporting a variety of popular databases. As a result, deserialization vulnerabilities are commonly found in certain functionalities and can be extremely dangerous. These vulnerabilities often allow remote code execution on the vulnerable system. Insecure deserialization occurs when untrusted or unknown data is pulled from a file, stream, or network socket, and transformed into an object. The vulnerability is based on common code libraries found in web development, like those from the apache commons library in which user input is often not checked.

In August, vulnerabilities CVE-2017-10271 and CVE-2019-2729 were popular targets to attempt exploit of Oracle WebLogic. GTIC researchers analyzing these attacks commonly found cryptominers such as XMRig or XMR-STAK. GTIC researchers also observed Sodinokibi ransomware being distributed via CVE-2019-2729. Discovered in April of 2019, Sodinokibi ransomware is a ransomware-as-a-service (RaaS), just as the notorious GandCrab had been. This ransomware family is also delivered via RIG exploit kit and malicious spam (malspam) campaigns. Ransom for infection of a single system typically costs between .10 and .20 bitcoin (BTC), and increases if the allotted time given expires. For more information on Sodinokibi, GTIC researchers recommend reading Malwarebytes Labs analysis.

It worth noting that, during August, 76 percent of vulnerabilities being attacked allow remote code execution (RCE) if successfully exploited. This is true regardless of if the activity was targeted, or more closely related to internet-scanning. This suggests that threat actors prefer to focus on recent vulnerabilities which allow RCE. Patch management and vulnerability awareness is key to mitigating these attacks as new vulnerabilities are released because proof-of-concepts (PoCs) will eventually be released allowing for easier and faster weaponization of payloads which exploit the vulnerability targeted.

References:

1. https://www.opensourcecms.com/cms-market-share
2. https://blog.malwarebytes.com/threat-spotlight/2019/07/threat-spotlight-sodinokibi-ransomware-attempts-to-fill-gandcrab-void/

APT 41: A Little “on the Side”

Lead Analyst: Danika Blessman

Researchers recently released a detailed report regarding a suspected Chinese state-sponsored cyberespionage group called APT41.

Not your typical Advanced Persistent Threat (APT) group, APT41 has been identified as “agile and persistent,” appearing to have taken to financial crimes in addition to the “normal” espionage-type operations seen from suspected APT actors.

This type of behavior is uncharacteristic of Chinese threat actors – especially those that are state-sponsored — as they likely operate under stringent rules and controls, suggesting that these money-raising endeavors may also be state-sanctioned.

Active since at least 2012, APT41 began by conducting operations against targets in the gaming industry, where malicious code was inserted into legitimate video game files to distribute malware. APT41 has used similar tactics to target companies in many organizations’ supply chain.

For about seven years, APT41 successfully conducted cyber-espionage operations against organizations in varying industries including telecommunications, virtual currencies, retail, education, health care, media — in 14 different countries including the U.S., the U.K., Japan, France, the Netherlands, Switzerland, Turkey, India, Singapore, South Korea, South Africa, and Italy.

All these targets and campaigns apparently are meant to further the goals of the Chinese government. In fact, this group’s campaigns seem to align with the newest Five-Year Plan. Compromises by APT41 have historically been timed to acquire intelligence related to major endeavors related to a targeted organization, like acquisitions, mergers, or political events.

Interestingly, the group doesn’t appear to have stolen intellectual property since late 2015. Perhaps the focus now is on financial gain, or the group remains dormant — and undetected — on targeted systems. The shift from “theft of information” to “financial gain,” appears well-defined, but it doesn’t mean APT41 has abandoned its ways of the past.

Over the years, APT41 operations and tactics, techniques, and procedures (TTPs) seem to overlap with those of two other suspected Chinese APTs, Winnti and Barium, but what makes this group unique?

APT41 is blurring the lines between state-sponsored actions (i.e., espionage) and for-profit cybercrime, leveraging non-public malware to manipulate virtual currency and deploy ransomware. They have a knack for maintaining persistence and regaining a foothold even after having been discovered and kicked out of a network. In fact, the group was observed having deployed over 150 unique samples of malware in a year-long campaign against a single target.

Moreover, the group’s capabilities and targeting efforts have grown over time, potentially putting more organizations at risk.

As always, NTT Security recommends clients use best practices and keep software and firmware patches up to date. Stay current on the latest geopolitical events, especially those which pertain to a given industry. Always be vigilant to the fact that your sensitive data is valuable to many threat actors — from state-sponsored APTs to industry competitors.

References:

1. https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html
2. APT41: A Dual Espionage and Cyber Crime Operation

NTT Security Annual Reports

NTTSecurity
Risk:Value 2019
Destination standstill.
Are you asleep at the wheel?
Why many organizations are failing to make progress with cybersecurity.
International research report

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 Security Global Threat Intelligence Center protects, informs, and educates NTT Security 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 Security 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 Security 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 Security clients using the Global Threat Intelligence Platform (GTIP).

NTT Security

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more about NTT Security or visit www.ntt.co.jp/index_e.html to learn more about NTT Group.