NTT Security

GTIC Monthly Threat Report

April 2018

Contents

©2018 NTT Security

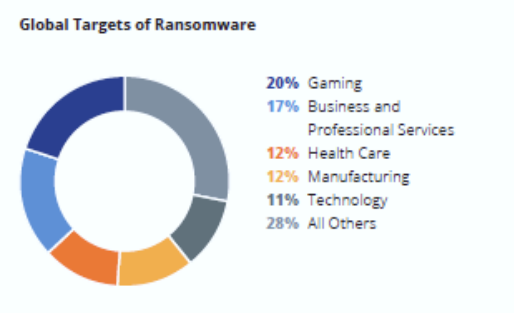
Ransomware and Cryptojacking Battle for Top Spot

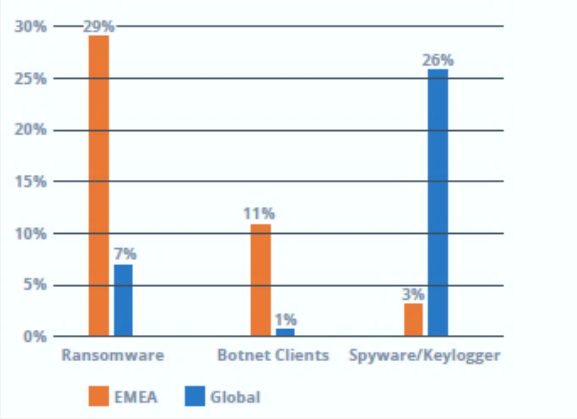
Lead Analyst: Terrance DeJesus

In the 2017 Global Threat Intelligence Report (GTIR), ransomware detections accounted for less than one percent of all malware detections, as this type of attack was fairly uncommon in 2016. Ransomware detections skyrocketed in 2017 – up 350 percent – accounting for nearly seven percent of all global malware attacks. Although ransomware detections increased significantly, incident response related engagements fell from over 22 percent of incidents in 2016 to just five percent in 2017 thanks to increased threat awareness and preparation by NTT Security clients.

GTIC researchers analyzed Q1 '18 data regarding ransomware detections and compared them to data from 2017. Researchers found that both February and March of 2018 had over 90 percent more detections for ransomware specifically in comparison to February and March of 2017, indicating ransomware attacks are continuing to rise in volume as compared to previous years. Of these detections, ransomware families GlobeImposter, GandCrab, LockCrypt, Jaff and others.

The gaming (gambling and associated entertainment) sector was the most targeted by ransomware during 2017. This follows a common target pattern by threat actors in which several of the most targeted sectors are characterized by high uptime requirements, where an impact in system availability could directly lead to loss of revenue. NTT Security detected ransomware attacks in every industry sector; however, the top five sectors targeted – finance, technology, business and professional services, manufacturing and retail – accounted for 72 percent of all ransomware detections.





In Europe, the Middle East and Africa (EMEA), ransomware accounted for 29 percent of malware detections, making it the only region in which ransomware was the top type of malware. As the breakout of the infamous "WannaCry" ransomware made media headlines, health services in the United Kingdom were impacted, resulting in the impacted health care facilities finding it necessary to cancel appointments and divert incoming patients to alternate medical facilities. WannaCry and Petya, both originating in EMEA, also affected the gaming sector, which experienced 36 percent of ransomware attacks. In comparison, the Americas accounted for 26 percent of ransomware detections, where business and professional services were the most targeted.

©2018 NTT Security

According to Malwarebytes' Cybercrime tactics and techniques report, business detections for ransomware have increased by 28 percent from their observations of Q4 '17. In addition, ransomware variant GandCrab is the most popular ransomware at the time of this report, whereas Locky and Cerber, once extremely popular, are no longer being distributed by ransomware actors. GTIC researchers have not observed any Locky or Cerber since November 2017.

As cryptomining malware detections continue to increase significantly, GTIC researchers assess that this new attack vector will soon dethrone ransomware in regard to popularity for money-motivated threat actors. Even so, a recent ransomware attack against the city of Atlanta resulted in a $2.6 million loss, as the attack crippled the city's municipal operations last month. To carry out the attack, threat actors used the SamSam ransomware family which, coincidentally, was the subject of GTIC research in 2017. This indicates that, although ransomware may have been dethroned by cryptomining malware, it is still effectively being used, and costlier than ever.

Find out more on ransomware in the 2018 Global Threat Intelligence Report (GTIR).

Russia Nation-State Actors Target Network Infrastructure

Lead Analyst: Aaron Perkins

The ongoing threat of "Russia state-sponsored attacks" is as common in the cybersecurity field as grass is to a football pitch.

In other words, it comes as no surprise, and is in fact, expected.

Defending against these attacks does not make the challenge any easier to address though, even when we're expecting it.

In April, US-CERT posted a joint technical alert (TA) concerning Russia state-sponsored attacks targeting network infrastructure such as routers, switches, firewalls, network-based intrusion detection devices (NIDS), etc. This TA was the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the United Kingdom's National Cyber Security Centre (NCSC)

How does this impact you?

This campaign is targeting multiple network infrastructure devices, including routers, switches, firewalls, Network-based Intrusion Detection Systems, etc.)

If you believe your network device(s) may be vulnerable to this attack campaign, consult the Technical Alert (link in References section of this article) and follow the procedures appropriate for your device's vendor.

What can you do?

©2018 NTT Security

Attacks being used as part of these Russia-based initiatives are varied and cover a wide variety of network infrastructure devices. If successful, these attacks can relinquish control of the device to the hostile cyber actor.

NTT Security recommends organizations review the specific technologies referenced in the joint TA, along with the respective use of those technologies in the organization's own environment.

Additional information is available in the TA, linked in the References section of this article.

Additional information includes:

- Cisco related command and configuration settings
- Other vendor command and configuration settings
- SNMP queries
- SMI queries
- Additional references

References

US-CERT Joint Technical Alert

Cisco Advisory

Supply Chain Attacks

Lead Analyst: Danika Blessman

Supply chain attacks are quite popular these days. Cybercriminals – and likely nation state actors – are targeting vendors to maximize their chances of obtaining sensitive information across a wide target area, or gaining access to a specific target. We describe these attacks against the business and professional services industry in the NTT Security 2018 Global Threat Intelligence Report (GTIR).

These attacks continue – because they're effective.

Many organizations – across *all* industries – often overlook their supply chains, despite this potentially being their most vulnerable surface, especially in hardware and software supply chains.

One recent study detailed the threat to the health care industry, in which researchers reported that supply chain attacks actually pose a greater threat than exposed medical devices.

Another example of a recent supply chain attack affected at least four U.S. natural gas pipeline communication channels, possibly impacting hundreds more. One of the companies affected by this apparent attack reported an issue with its Electronic Data Interchange (EDI) system, a platform used by organizations of all types to encrypt, track, and exchange documents with clients.

There is very little publicly available information on this specific attack to date, but it should be noted that supply chain attacks could be meant for one particular target in a given supply chain. Granted,

©2018 NTT Security

supply chain attacks could be used as a broad sword, intending to glean as much information or access to as many networks as possible, but, depending on the intent of the attacker, casting a wide net could easily hide the fact that a threat actor may have a specific target in mind.

These are not isolated cases, and there seems to be no end to breaches due to weaknesses in the supply chain. According to a study conducted by the Ponemon Institute, ***56 percent of breaches were due to a weak spot in a third-party vendor.*** This type of attack could be a huge blow to any organization, as clients' data, regardless of the vector, is still at stake – and the organization itself could take the fall.

In addition, watchdog groups are increasingly looking at third-party risks. In 2017, financial regulators in New York began requiring financial firms to confirm their supply chain met required network protections. Next month, the General Data Protection Regulation (GDPR), also highlighted in the NTT Security 2018 GTIR, looks to do the same.

No industry or organization is truly safe. It is recommended that organizations fully vet anyone in their supply chain. Third-party vendors could be your weakest link, and are an easy vector for threat actors to impact your organization.

Again, in this case, it is not only the oil and gas industry susceptible to attacks via the EDI, as this platform is used across the board. This time, it was oil and gas, and next time, it could any other industry which leverages EDI.

Ensure your networks and security practices – along with all those in your supply line vendors – are compliant with local and global regulations, not only to protect your networks, but your clients' data as well.

References

Supply Chain Attacks Could Pose Biggest Threat to Healthcare

Insecure SCADA Systems Blamed in Rash of Pipeline Data Network Attacks

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.

©2018 NTT Security