GTIC Monthly Threat Report

December 2019

Contents

NTT Ltd. Monthly Observations

Lead Analyst: Terrance DeJesus, Threat Research Analyst, Global Threat Intelligence Center

As this decade comes to an end, GTIC researchers focused the December monthly GMSSP data observations on malware detections. Throughout 2019, banking Trojans and keyloggers were particularly observed being distributed via high volume malicious spam (malspam) campaigns. These campaigns were equipped with popular families like Trickbot, Emotet, Ursnif, and Agent Tesla. GTIC researchers also continue to observe unique remote access Trojan (RAT) malware types, as well as worms, botnets, and webshells. As shown in **Figure 1**, 74% of malware detections in December were RATs, followed by worm activity at 9%, and botnets at 5%.

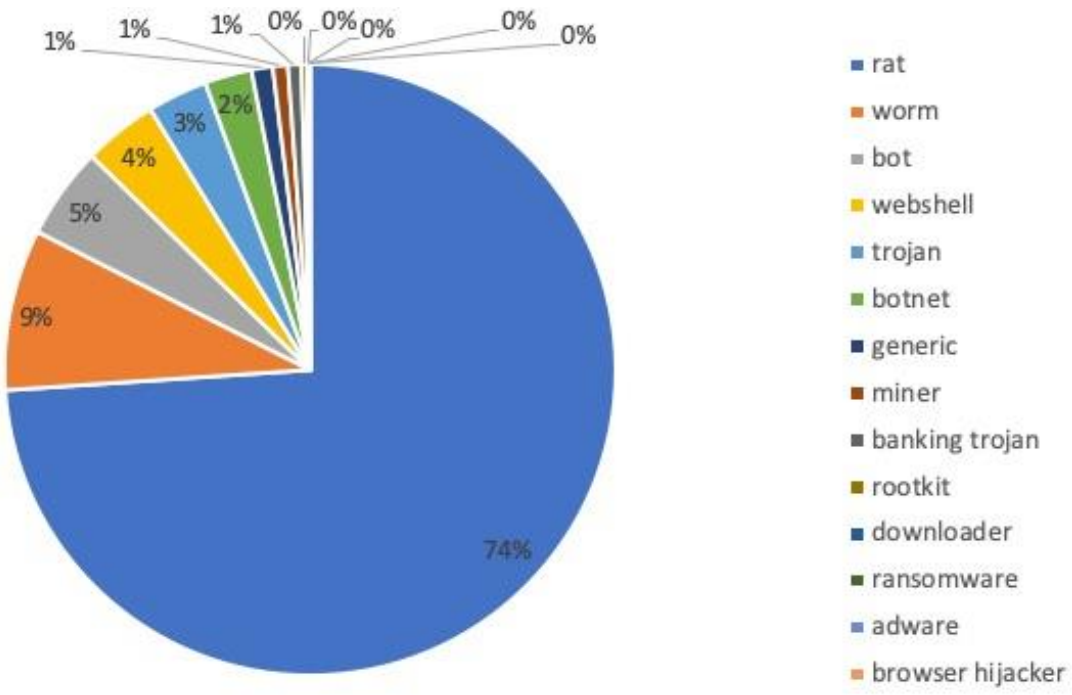

Figure 1: Malware types for December 2019

A majority of RAT detections derived from the Zegost malware family. Zegost has been around since 2011 and has received multiple updates from adversaries. These updates allow Zegost to exploit multiple vulnerabilities, run as fileless, and act as a backdoor. Typically, Zegost is delivered via malspam campaigns and is compiled as a portable executable (PE) for Windows-based environments.

In addition to Zegost RAT detections, NetWiredRC was another popular RAT detected during December. This specific family of RAT was observed intermittently throughout 2019, though never in consistent volume, which is typical of popular malspam

campaigns. NetWiredRC has the capability to modify files, use a SOCKS proxy, record audio, start remote shells, more. This makes it very versatile.

Other popular RATs detected were Gh0st, Gracewire, and njRat.

In addition to RAT activity, GTIC researchers also observed several banking Trojan campaigns. Tiny Banker (aka Tinba or Zusy) was the most detected banking Trojan. Tinba has been around since 2012 and contains code from the popular Zeus family. Tinba attempts to gather sensitive data from users including passwords, Social Security Numbers, banking information, and more. Tinba is only about 20kb in size, making anti-virus (AV) detection difficult. Unlike most banking Trojans, Tinba is delivered via infected websites, with some campaigns leveraging email. Most victims remain unaware of an infection due to Tinba's propensity for AV evasion, along with modification of user browser settings which disable warning messages indicating the malware is being downloaded.

Additional banking Trojan families observed in December were Dridex, Ursnif, Hancitor, and Redaman.

GTIC researchers believe banking Trojans, RATs, information stealers, and keyloggers will be the primary detections throughout 2020. Many of these well-documented malware families are distributed daily through high volume malspam campaigns. In addition, malware-as-a-service (MaaS) offerings make it easy for small adversary groups or script kiddies to leverage these types of malware. Mitigation often starts with employee security awareness training and a defense-in-depth approach to security measures. Many of the crippling news stories about ransomware attacks often start with a simple downloader distributed via email or infected websites. It is not as common to see this infection process during a more targeted attack.

The takeaway from this activity is that any business or organization may be infected at any time; it is not dependent on being the target of an advanced adversary.

Lean In Advice We Give to Our Customers

Lead Analyst: Derrell Cole, Ph.D., PMP, Manager, Client Services, Global Services

As anyone who has been a victim of a robbery can tell you, even when all the stolen items are returned in their original state, the psychological effect of having had your privacy violated leaves a bitter taste which takes a long time to wash away. This is one more reason organizations should prepare for – rather than simply avoid – cyber threats.

We are inundated almost daily by news about criminals hacking and stealing data from movie studios, major retailers, and even our most secure (or perceived as secure) government agencies. While these incidents may lead us to believe big companies are the targets of hackers, the harsh reality is that small businesses are at as much risk as large corporations.

McAfee, a leading provider of security software, recently reported 90% of small and medium-sized U.S. businesses do not sufficiently protect their electronic company and customer information. This is a sobering statistic, especially when you consider one established professional-services firm estimated breaches can cost small firms up to $100,000 USD to remedy and, for larger firms, well into the millions of USD.

There's more: beyond data, *how secure is your business's banking and credit card information?* Having your credit or bank account compromised can be a significant inconvenience and disruption to your business when the bank suspends your accounts as it conducts an investigation over the course of several days. For an organization, breaches can also compromise trust relationships with buyers and suppliers, continuing to impact the organization for far into the future.

Here are several recommendations to ensure privacy, as well as the confidentiality and security of your data:

1. Invest in alerting and pay close attention to those alerts

All banks and credit cards have alerts which you can set to receive a text when a transaction has exceeded a stated amount; or when your bank or credit card balance hits a certain level. For some card companies, these notifications can be configured to be a voice call.

It can be easy to set up notifications for sports scores, news, and social media. If we are truly interested in our privacy and protecting our data, it should be 'business as usual' to set up important business financial notifications.

2. Make sure your employee and vendors are aligned with your security stance

Research historically demonstrates that approximately 80% of security-related incidents are a result of employee behavior. For this reason, your employees need to be well trained about, and aware of, the threats to your company's cyber

security. Policies and processes should be clearly stated within and throughout the organization.

Additionally, your vendors and other business partners, especially those with which you conduct financial transactions or share sensitive information, should be vetted and required to uphold stringent internet security protocols. Of course, not every vendor will be able to comply, but demonstrating your willingness to make cyber protections a priority will help lead and drive home its importance.

3. Place proper focus on compliance

Security compliance is a legal concern for organizations in many industries today. Regulatory standards like PCI DSS, HIPAA, GDPR, and ISO 27001 provide recommendations for protecting data and improving information security management in the enterprise. In demonstrating security compliance, enterprises are better able to define and achieve specific IT security goals as well as mitigate the threat of network attacks through processes like vulnerability management. At worst, the act of gaining compliance can drag security controls towards a more mature state. In some cases, such as with HIPAA, failure to achieve and maintain security compliance can result in financial and legal penalties.

Major security standard involve an evolving set of specific requirements. Achieving, and then maintaining, security compliance can be complicated and costly. And in order to gain protection from the liabilities that accompany security breaches, companies are spending large amounts of time and money on regulatory compliance efforts.

4. Support your risk management plan with appropriate insurance

If your business transacts a significant amount of business through the internet, stores sensitive information online, or communicates electronically, it is probably worth discussing with your insurance provider the potential loss which could result from a major data breach in your company. Protection for unforeseen cyber security threats is becoming as standard as liability insurance for company vehicles.

The point is organizations need to be proactive. If scaring someone into action helps, that might be an effective approach. But, while businesses probably can't avoid breaches, they can certainly take great strides in preparing for the worst.

5G: Inviting New Attacks?

Lead Analyst: Danika Blessman, Senior Threat Intelligence Analyst, Threat Intelligence Communications Team

As with previous generations of telecommunications technologies, the introduction of 5G brings with it not only inherited risks from its predecessors, but new risks and vulnerabilities – many of which remain unknown – as it begins to play a role in connecting everything from mobile and Internet of Things (IoT) devices to smart cars and smart cities.

Many vulnerabilities[1] have already been identified within 5G, and this number is likely to significantly increase as 5G is implemented.

While 5G promises incredibly low latency, blazingly fast speeds, and an increase in signal reliability, new features in 5G may have yet to undergo rigorous security evaluations. Worse, **many organizations have yet to secure their 4G and older smart devices**. With ongoing past and present risks, 5G implementation will add to the ways networks and connected devices can be attacked.

Introducing 5G technology, its components, and associated devices into a network environment will increase your organization's threat profile, providing a much broader attack surface for avenues into your network. Attackers **always** try to exploit anything new and vulnerable – so it shouldn't be any surprise that 5G is high on that priority list. So, who would target 5G – and why?

The list of potential attackers is substantial, as are potential impacts.

Based on already identified vulnerabilities, there are fears of snooping[2], disconnecting or altering communications, and attackers possibly being able to acquire a user's location – increasing not only the digital threat but adding potential physical threats as well.

5G technologies are likely of particular interest to nation-state threat actors from multiple standpoints, including from espionage and military perspectives. Control of networks and devices could easily give a government insight into an adversary's communications – or even influence these communications – especially if the government controls the manufacturing of 5G components.

The expanded 5G attack surface could also increase the risk of an organization facing insider threats – either from a novice user causing unintentional damage or from a malicious insider leveraging access to vital network functions to cause widespread damage.

---

[1] https://www.wired.com/story/5g-vulnerabilities-downgrade-attacks/

[2] https://www.forbes.com/sites/kateoflahertyuk/2019/11/13/new-5g-security-threats-spark-snooping-fears/#3b1d96225025

Cyber criminals, particularly those in organized groups with sophisticated capabilities, could leverage 5G for data theft or financial fraud. Hacktivists may also attempt to target the technology itself – or the entities responsible for rolling out the infrastructure – due to reported[3] health concerns surrounding the radio frequencies emitted by 5G.

But, even with the threats inherent to 5G – and what feels like an overwhelming task to manage this vast ecosystem of devices, services, and applications – researchers continue to work to mitigate[4] these threats. This is good news, since security is too often an after-thought with the latest and greatest technologies.

NTT Security recommends that, as with any new technology, organizations approach 5G implementation and security with caution, ensuring potential security risks are considered and mitigated from the start of the transition. Secure deployment may not be achievable immediately in your network environment, despite its convenience or appeal. Plan any implementations strategically, considering security impacts, controls, and configurations to help minimize negative outcomes. In addition, ensure users and your organization purchase and use equipment only from vetted vendors which employ strict supply chain security. It is also critical to enforce your organizations' security policies across the incoming 5G supply chain.

[3] https://www.howtogeek.com/423720/how-worried-should-you-be-about-the-health-risks-of-5g/

[4] https://www.fiercewireless.com/5g/5g-security-enhancements-take-aim-at-emerging-threats

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

- Threat research
- Vulnerability research
- Detective technologies development
- Threat intelligence management
- Communication to NTT Ltd. 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 Ltd. 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 Ltd.'s global internet infrastructure, clouds, and datacenters along with third-party intelligence feeds. NTT Ltd. works to understand, analyse, curate, and enrich threat data using advanced analysis techniques and proprietary tools, then curates and publishes these for the benefit of NTT Ltd. clients using the Global Threat Intelligence Platform (GTIP).

About Security and NTT Ltd.

Security is a division of NTT Ltd., a global technology services company bringing together the expertise of leaders in the field, including NTT Communications, Dimension Data, and NTT Security. The Security division helps clients create a digital business that is secure by design. With unsurpassed threat intelligence, we help you to predict, detect, and respond to cyberthreats, while supporting business innovation and managing risk. Security has 10 SOCs, seven R&D centers, over 2,000 security experts and handles hundreds of thousands of security incidents annually across six continents. Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology.

NTT Ltd. partners 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 ICT provider, we employ more than 40,000 people in a diverse and dynamic workplace, and deliver services in over 200 countries and regions. Together we enable the connected future. Visit us at our new website hello.global.ntt