NTT Ltd. Global Threat Intelligence Center

Monthly Threat Report

September 2020

Contents

Feature article: Is the US election infrastructure in trouble? 03

Spotlight article: Technical analysis of QUA R&D's Java Rat 05

Spotlight article: 5G Faces widely-varied threats 08

About NTT Ltd.’s Global Threat Intelligence Center 09

Is the US election infrastructure in trouble?

Lead Analyst: Jeannette Dickens-Hale — Sr. All Source Threat Intelligence Analyst, Global Threat Intelligence Center, US

The state of the US election infrastructure

With the US 2020 elections in November of this year, ensuring and maintaining election security has become a high stakes endeavor, and a key national security focus as part of the US critical infrastructure. Threats to the US voting processes are numerous, diverse, continue to evolve with technology changes and threat actors' skills and toolsets. Foreign interference, disinformation campaigns, potential changes in the United States Postal Service operating procedures, ransomware attacks, aging technology (including hardware and end-of-life software), voter role purge, voter apathy – and particularly for this year – the fear of coronavirus contagion at voting precincts are just a few of the threats facing the elections process.

Each part of the ecosystem – pre-election activities, election day activities, and postelection activities – has its own unique set of challenges. A cyber or physical attack on the election infrastructure, whether election systems or processes are interconnected or not, could potentially lead to overall election system dysfunction, errors in vote count, delays in voting results and erroneous election reporting.

Two types of technology-related threats exist within the US election infrastructure: Threats related to election hardware (e.g., voting machines); and election software. End-of-life hardware running aging software is a combination that continues to plague the US elections ecosystem. This potentially leaves several attack vectors open to bad actors, both foreign and domestic. It would be prudent to prioritize and address the risk of end-of-life, aging hardware and software, as these are the nuclei of the entire election ecosystem. The most important elements of security are those which attackers will most likely target first. The first line of defense against cyber-intrusion, and other threats, must be a secure and resilient US election infrastructure.

What is election infrastructure?

The US election infrastructure is an ecosystem comprised of various subsets of voting systems, networks, and processes. In each jurisdiction, the election infrastructure has its own unique ecosystem, which might or might not be electronically connected to other voting jurisdictions. These voting districts must function seamlessly to conduct the election process from registering voters, to election day activities and voting, to postelection activities and certifying votes.

The technology infrastructure and systems used in managing elections, voting machine systems, voting software; voter registration databases; counting, auditing, displaying election results, and postelection reporting to certify and validate election results are all part of the election infrastructure ecosystem.

We can break down and address the threats relative to the three sections of the election ecosystem:

Threats to pre-election activities: In-person, mail-in and online voter registration

Attacks of voter registration information could involve tampering with or deleting voter registration details so that the potential voter is unregistered and thus unable to vote. Malware planted on a voter registration system could compromise the integrity of that data just like any other breach. The voters' data could be mined for personal identifying information and held for ransom, or it could be sold for criminal profit on the dark web.

Threats to election day activities: Ballot casting, vote tallies and election result reporting

Preparing ballots, voting machines and other voting equipment is similar in threat risk to pre-election activities. Physically tampering with paper ballots at polling locations could invalidate ballots once they have been cast. Votes physically counted by human hand are potentially subject to count error.

Voting on a Direct Record Electronic (DRE) voting machine – a machine that directly records votes and vote totals into computer memory – does not use a paper ballot. Votes counted and tallied by DRE machines would seem to be susceptible to physical damage by a bad actor or to cyberattack at points in time between the voting machine being stored, in transit and set up at polling locations. However, some DRE machines have a Voter-Verified Paper Audit (VVPAT) which is a permanent record of votes used for counts, audits and recounts.

Election results submitted electronically, or via email on election night, face cyberthreats, intentional or unintentional physical threats by poll workers entering flawed data. Election results submitted by fax, or phone could fall prey to human error in reporting accurate vote totals.

Optical scan voting ballots are vulnerable to invalidation if the ballot ovals are not completely coloured in, which may render the vote null. As with the DRE machines, if an attacker is able to obtain either physical or electronic access, malware could potentially be planted on the optical scan machine at any point from warehouse, to delivery, to set up at polling locations.

Threats to postelection activities: Election results tallied and released to the public

Before releasing election results to the public, votes must be certified and states must conduct postelection canvassing. Postelection canvassing is a 'Compilation of election returns and validation of the outcome that forms the basis of the official results by political subdivision (VVSG Volume 1, Version 1.0, A-6).'

Vote certification and canvassing also includes postelection audits. 'A postelection audit checks that the equipment and procedures used to count votes during an election worked properly, and that the election yielded the correct outcome.' These guidelines are available at https://www.eac.gov/.

To secure the US election infrastructure and defend against the numerous threats that plague it, the US Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) published the Cyber Incident Detection and Notification Planning Guide for Election Security. CISA has also prepared materials to help state and local election officials strengthen their election security. Information on CISA can be found here https://www.cisa.gov/.

Known cyberthreats

Ransomware poses a significant threat to the US election infrastructure as aging software and voting machines potentially support vulnerabilities which may be easily targeted by criminal elements, or by foreign-based cyberattacks. Ransomware could be deployed and lying in wait to be activated on election day, or once the voting machines are activated, could pose a significant threat to voting processes and procedures, potentially bringing voting operations to a halt.

Election threats from ransomware, or from other types of cyberattacks, do not come solely from foreign governments. Cyberattacks against the US election infrastructure can be launched by any criminal threat actor seeking financial gain.

What can we do? Threat mitigations and recommendations

NTT Ltd.'s analysts recommend following the latest cybersecurity practices and maintaining good cyber-hygiene as a first line of defense against cyber-intrusions. Proper patching and updates, proper custodianship of hardware and security awareness are basic controls which require appropriate enforcement. In addition to maintaining best practices, NTT Ltd.'s analysts recommend following steps in the CISA publication *Cyber Incident Detection and Notification Planning Guide for Election Security*.

Summary

There are threats throughout the entire election process, from disinformation, to using influencers, as well as a plethora of technical threats to each part of the election ecosystem. While it would take compromising many individual voting machines to have a significant impact on the outcome of an election, any attempt to compromise even a single voting machine violates the basic tenets of the US democracy.

> We recommend **following the latest cybersecurity practices** and maintaining good cyber-hygiene as a first line of defense against cyber-intrusions; along with the steps in CISA publications.

References
https://www.cisa.gov/sites/default/files/publications/cyber-incident-detection-and-notification-planning-guide-for-election-security-508_0.pdf

#Spotlight 1

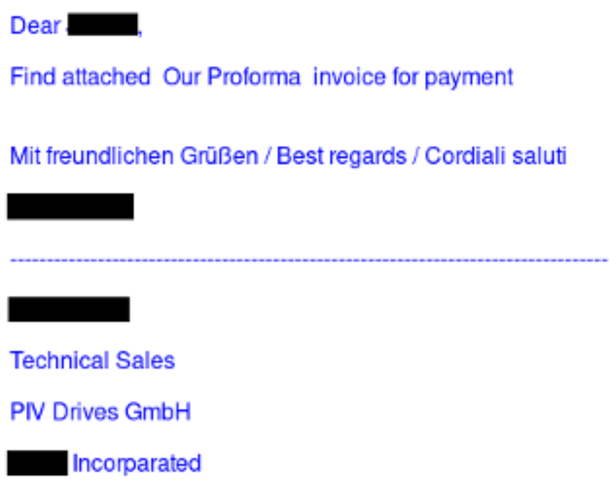
Technical analysis of **QUA R&D's Java Rat**

Lead Analyst: Jacob Faires — Sr. Threat Research Analyst,
Global Threat Intelligence Center, US

Organizations face a wide variety of threats as they try to meet their operational goals. Modern malware is only one of those threats, especially in a case where the malware is readily spread through effective campaigns, as in the case of FireElement. NTT Ltd. researchers analyzed FireElement to better understand this threat.

FireElement is a Java-based remote-access Trojan (RAT) generated with a polymorphic bot generator. It can provide an attacker with remote administrative-level control, allowing the attacker full access over the targeted system. It was introduced to the world in November 2019, available only in private sales and requires an invitation by a reliable customer. The malware has developed a good reputation among spammers and continues to grow its userbase. A crypter is included in the bot builder for the convenience of the customer and the detriment of antivirus solutions. Newer versions of FireElement are still not detected by antivirus.

FireElement is distributed via malspam campaigns. These campaigns are opportunistic in nature, lacking a specific target or industry. Campaigns have targeted organizations in the United States, Bulgaria, India, Columbia and Turkey. The phishing lures used in the campaigns all follow a similar, simple structure:



Dear [redacted],

Find attached Our Proforma invoice for payment

Mit freundlichen Grüßen / Best regards / Cordiali saluti

[redacted]

[redacted]

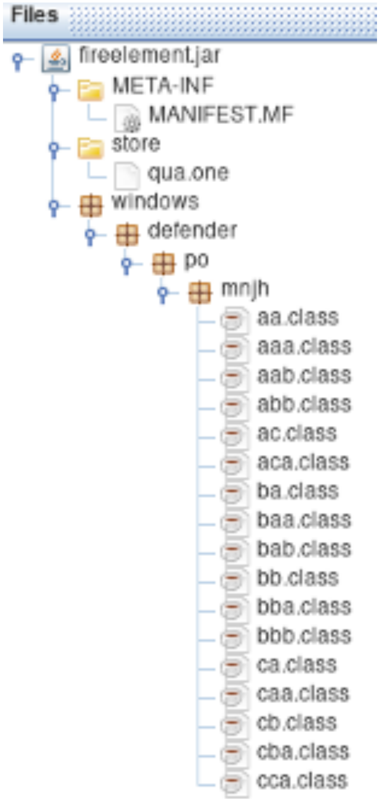
Technical Sales

PIV Drives GmbH

[redacted] Incorparated

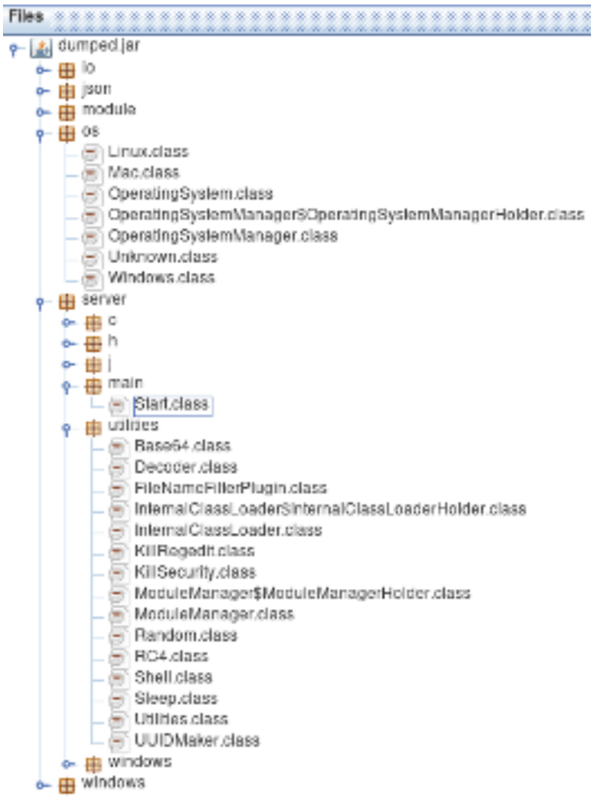
Analysis

FireElement is delivered as a JAR file. The basic structure is an obfuscated unpacker with the malware stored as a resource, RC4 encrypted.



```
Files
fireelement.jar
    META-INF
        MANIFEST.MF
    store
        qua.one
    windows
        defender
            po
                mnjh
                    aa.class
                    aaa.class
                    aab.class
                    abb.class
                    ac.class
                    aca.class
                    ba.class
                    baa.class
                    bab.class
                    bb.class
                    bba.class
                    bbb.class
                    ca.class
                    caa.class
                    cb.class
                    cba.class
                    cca.class
```

The string encryption/obfuscation method used in the unpacker is also used in the malware source, resulting in an increase in the time required to analyse the malware. Instead of rewriting the decryption routine, analysts dumped newly loaded class files from memory and built a JAR file to show the malware source. The files reveal that the malware has numerous generic operating system capabilities as well as some Windows-specific functionality.



```
Files
dumped.jar
  io
  json
  module
  os
    Linux.class
    Mac.class
    OperatingSystem.class
    OperatingSystemManager$OperatingSystemManagerHolder.class
    OperatingSystemManager.class
    Unknown.class
    Windows.class
  server
    c
    h
    i
    main
      Start.class
    utilities
      Base64.class
      Decoder.class
      FileNameFilterPlugin.class
      InternalClassLoader$InternalClassLoaderHolder.class
      InternalClassLoader.class
      KillRegedit.class
      KillSecurity.class
      ModuleManager$ModuleManagerHolder.class
      ModuleManager.class
      Random.class
      RC4.class
      Shell.class
      Sleep.class
      Utilities.class
      UUIDMaker.class
    windows
  windows
```

Strings in the decrypted payload are obfuscated with the same custom encryption functions used by the unpacking stub, which makes for a good detection signature. A YARA rule for finding this method's Java bytecode can be found below. This will trigger on the .class file, not the JAR file itself, so an analyst will need to unzip the JAR file before scanning. VirusTotal extracts all class files from JAR packages, so this rule will work within VirusTotal's Retrohunt tool.

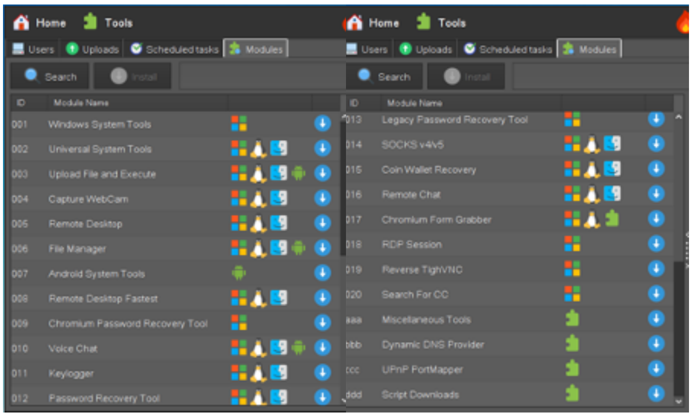
```
rule fireelement_string_encryption
{
 meta:
  description = "FireElement JRat string encryption method"
  author = "Jacob Faires"

 strings:
  $1 = { 04 59 58 3D 2B BE 04 59 59 58 64 59 3E 36 04 2B 3A 05 1C 36 06 15 04 9B 00 }
  $2 = { 19 05 2A 1D B6 00 03 15 06 82 92 36 07 1D 15 06 82 92 10 3F 04 59 58 7E 92 36 08 1D 15 07 84 03 FF 55 1D 9C 00 07 A7 00 }

 condition:
  all of them
}
```

At this point it's easier to look at the control panel/bot builder to see what functionality the bot has.

Taking a look at the builder shows support for Windows, Linux, Android and OSX. The user is able to specify a C2 DNS/IP and port they wish to use, along with a server ID. C2 communication is sent over TLS using a Let's Encrypt signed certificate or supports the option of including your own certificate in the settings. There are also anti-analysis options with the ability to check for VMware, VirtualBox, disable 32 different antiviruses, as well as disabling 12 different security and analysis tools. There is far more support for Windows than the other versions, with several plugins, including password recovery and remote access tools.

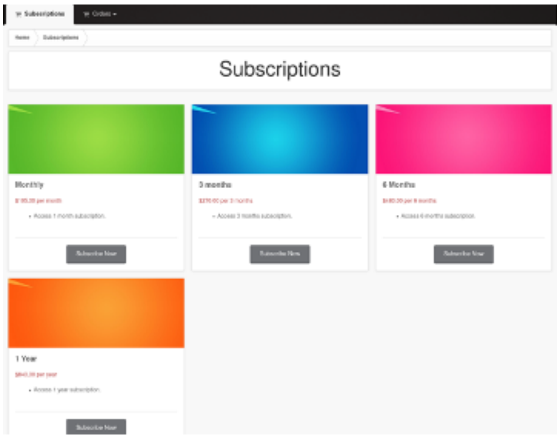


ID	Module Name		
001	Windows System Tools	⊞	⬇
002	Universal System Tools	⊞ 🐧 🍎	⬇
003	Upload File and Execute	⊞ 🐧 🍎 🤖	⬇
004	Capture WebCam	⊞ 🐧 🍎	⬇
005	Remote Desktop	⊞ 🐧 🍎	⬇
006	File Manager	⊞ 🐧 🍎 🤖	⬇
007	Android System Tools	🤖	⬇
008	Remote Desktop Fastest	⊞ 🐧 🍎	⬇
009	Chromium Password Recovery Tool	⊞	⬇
010	Voice Chat	⊞ 🐧 🍎 🤖	⬇
011	Keylogger	⊞ 🐧 🍎	⬇
012	Password Recovery Tool	⊞ 🐧 🍎	⬇
013	Legacy Password Recovery Tool	⊞	⬇
014	SOCKS v4/v5	⊞ 🐧 🍎	⬇
015	Coin Wallet Recovery	⊞ 🐧 🍎	⬇
016	Remote Chat	⊞ 🐧 🍎	⬇
017	Chromium Form Grabber	⊞ 🐧 🧩	⬇
018	RDP Session	⊞	⬇
019	Reverse TighVNC	⊞	⬇
020	Search For CC	⊞	⬇
aaa	Miscellaneous Tools	🧩	⬇
bbb	Dynamic DNS Provider	🧩	⬇
ccc	UPnP PortMapper	🧩	⬇
ddd	Script Downloads	🧩	⬇

FireElement is only available for purchase by invitation. Along with several java crypters, it can be found on japp.store, located at 185.61.153.96. It is hosted at the same IP address that the bot control panel calls back to for authentication and verifying a subscription. The only contact information available is a TOX chat client ID:

1A455ACB7517D09EA0312C8CD8EFACB602475FE66CB497595BD296E0482DAF656F03F3280DFE

Similar to other Java RATs, FireElement has a monthly subscription to maintain access to the control panel and the downloads section of the web site. The monthly rate of USD 105 shows the developers think highly of their product. As a comparison, the popular keylogger MassLogger sells for USD 45, or USD 94 with their LimeCrypter crypter.



Clues to the identity of the developers

Executing the packed sample will print the following to the command prompt, ‘Powered by QUA IT Solutions - https://store.qua.one Mod for Ardemis Team’. Store.qua.one offers standard web hosting and what they call Qhub, a web dashboard for RDP services.

Subdomains for qua.one implies heavy use of the domain for sales, development and storage.

store.qua.one	68.183.209.77		DIGITALOCEAN-ASN, US
www.qua.one	68.183.209.77	207.154.232.69	DIGITALOCEAN-ASN, US
qhub.qua.one	165.22.25.162	157.230.98.37	DIGITALOCEAN-ASN, US
livezilla.qua.one	165.227.147.227		DIGITALOCEAN-ASN, US
gitlab.qua.one	165.227.171.175		DIGITALOCEAN-ASN, US
cdn.qua.one	205.185.216.10	205.185.216.42	HIGHWINDS3, US
ocentral.qua.one	159.65.222.255	167.172.164.197	DIGITALOCEAN-ASN, US
license.qua.one	138.197.180.57		DIGITALOCEAN-ASN, US
verdaccio.qua.one	134.122.94.40		DIGITALOCEAN-ASN, US
qhs.qua.one	207.154.242.18		DIGITALOCEAN-ASN, US
gitlab2.qua.one	167.99.243.233		DIGITALOCEAN-ASN, US
docker.qua.one	167.99.129.240		DIGITALOCEAN-ASN, US

In 2016, Qrypter was released as a major rival to the Adwind Java RAT and was claimed by ‘QUA R&D’. The Registrant Organization for qua.one is also 'QUA R&D'. Based on available information, it appears FireElement is either a variant of Qrypter, or a new RAT written by individuals with access to the Qrypter source code.

FireElement is growing in popularity among commodity malware users due to its active development and built-in antidetection features. It is an effective RAT because of the malspam distribution method, the obfuscation techniques which hide it from antivirus and analysts, as well as the efficiency of the RAT itself. It is an excellent example of the evolving threat with which organizations must contend every day. NTT Ltd. has implemented the YARA rule and updated detection technologies and will continue to monitor for future developments.

> Introduced in November 2019, the FireElement RAT **provides cyber-attackers with remote administrative-level control over the targeted system** and is distributed via malspam campaigns.

#Spotlight 2

5G Faces widely-varied threats

Lead Analyst: Jeremy Bender — Security Intelligence Writer,
Global Threat Intelligence Center, US

The rollout of 5G promises to enable a digital society.

Successful implementation will improve support for the integration of systems as varied as Internet of Things (IoT) devices, self-driving cars and smart cities. 5G relies on software and virtualization, notably via software-defined networking (SDN), network function virtualization (NFV), mobile cloud infrastructure and multi-access edge computing (MEC). Taken together, these components decrease centralization and allow for low latency and increased flexibility.

MEC allows for lower latency by shifting demands from central data servers to a distributed computing constellation. To stitch these distributed systems together, providers rely on tools such as interoperable SDNs and NFVs, web-application delivery frameworks and APIs. This increases complexity and leads to security challenges.

For example, the expansion of MEC and the increasing number of devices joining the network means an increase in the overall attack surface. This leads to a greater number of entry points for attackers. Additionally, an increase in unsecured devices can lead to a heightened risk of denial-of-service attacks.

The increase in complexity can also lead to an increase in unauthorized access. Poor software development practices can lead to vulnerabilities, thereby increasing the entry points for attackers into the network. If systems are not consistently monitored for vulnerabilities and routinely patched, malicious actors could achieve long-lasting intrusions.

Similarly, the reliance on third-party software exposes mobile providers to increased supply-chain risks. Third-party suppliers could be pressured by a foreign country to include backdoors to facilitate cyber-attacks or espionage. This could be achieved by either deliberately injecting vulnerabilities into the software or by allowing a third country to exploit unintentionally embedded, and unpatched, vulnerabilities.

Lastly, as more systems migrate to 5G, the risk of over-reliance increases. Potential degradation of 5G networks could lead to the disruption of dependent systems, such as healthcare, power and water utilities, and self-driving cars. The potential fallout from a 5G network being brought down can become catastrophic if systems which have come to need the 5G support become unreachable.

All these risks are compounded as mobile providers will no longer be fully in control of data in the network or the systems underpinning the architecture. Instead, operators will work with different actors, such as Communication Service Providers and network infrastructure providers, which may have differing privacy and security priorities. This also poses the danger of adding complexity, risks from that complexity and risks inherited from the various providers.

In response to these changes, mobile providers must require security to be built into the deployment process. A single, coherent security framework addressing the full range of security risks, accepted and universally applied, is required to ensure 5G systems can safely and reliably deliver on their promise. This framework must address issues as varied as security policies for the centralized data centers and the edge, volumetric DDoS attacks, advanced persistent threats and intrusions, and web-application layer vulnerabilities.

References:

https://www.researchgate.net/profile/Ijaz_Ahmad8/publication/322753634_Overview_of_5G_Security_Challenges_and_Solutions/links/5a75aec1aca2722e4dedf166/Overview-of-5G-Security-Challenges-and-Solutions.pdf

https://www.raconteur.net/technology/5g-2020/5g-security

https://www.csoonline.com/article/3567450/security-challenges-facing-the-shift-to-5g.html

https://techcrunch.com/2019/10/09/european-risk-report-flags-5g-security-challenges/

NTT Ltd.'s Global Threat Intelligence Center

The NTT Ltd. Global Threat Intelligence Center (GTIC) protects, informs and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT Ltd. to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT Ltd.'s threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT Ltd.'s security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

> Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2020 Global Threat Intelligence Report

The 2020 NTT Ltd. Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month.

NTT