NTT Ltd. Global Threat Intelligence Center

Monthly Threat Report

October 2020

Contents

The OZIE Team:

A Nigerian business email compromise threat actor group

Lead Analyst: Jacob Faires, Senior Analyst, Security Threat Intelligence, Global Threat Intelligence Center, US

In August 2019, the NTT Global Threat Intelligence Center (GTIC) began tracking a threat actor group based in Nigeria who specialized in business email compromise (BEC). GTIC has named this group the 'OZIE Team'. At the time this article was written, the OZIE Team had targeted 852,541 domains since becoming active in 2017.

The OZIE Team is non-discriminatory in their targeting. Targets rotate weekly by country, industry and a combination of the two, with generally no more than two malspam campaigns run from the same virtual private servers (VPS). Targets tend to be chosen first by country, then by industry.

The OZIE Team performs massive reconnaissance spam campaigns against a variety of industries looking for victims. After the reconnaissance campaigns, the OZIE Team will analyze the results and focus on an industry based on the results of their reconnaissance campaigns.

The OZIE Team has specifically targeted organizations in almost every industrialized nation in the world but have a penchant for countries with large manufacturing bases like Singapore, China, the United Kingdom and the United States. The OZIE Team has seen success in milling companies, raw materials suppliers and healthcare product manufacturing, and they have directly targeted the following industries:

- Manufacturing
- Healthcare
- Automotive
- Food distribution

Tactics, techniques and procedures

The OZIE Team is a Nigerian group which relies on commodity malware sold through sites like HackForums.net and private discord groups. In order to purchase the commodity malware, the OZIE Team uses Bitcoin and Bitcoin Cash, or internet payment systems like Perfect Money.

Malware

The OZIE Team constantly changes their tactics to evade detection and increase the success rate of their attacks. The primary goal of the OZIE Team during the initial phase of a campaign is to steal victim's credentials in order to gain access the victim's web mail account. The OZIE Team frequently changed which exact malware they used to support these attacks.

In 2019, the OZIE Team ran many malware spam (malspam) campaigns. The group primarily uses the Agent Tesla keylogger but would alternate with the Hawkeye keylogger. The OZIE Team typically sends phishing emails with financial lures to trick the victim into interacting with the malspam. This includes subject lines like 'Quotation Request' and 'Proforma invoice'. To make the malware fully undetectable by antivirus software, the OZIE Team used the Cassandra Crypter for their campaigns. The OZIE Team switched to an Atilla Crypter subscription in the second half of 2019. As the group transitioned into 2020 it has used many different pieces of malware such as the Origin Keylogger, Masslogger, Formbook and FireElement, a private Java remote access trojan (RAT) described in the September GTIC Monthly Threat Report.

> OZIE comes from the Nigerian Igbo language in which **ozi-e means email.**

C2/Exfiltration

Email

Exfiltration of the victim's keylogger data is typically done in multiple stages. The first stage of exfiltration includes sending an email with the keylogger data to us2.smtp.mailhostbox[.]com. The emails are then forwarded to a second stage email inbox at Yandex or a Mail.ru. Vifeki3@yandex[.]com was a prolific email and is used by potentially different groups in many different campaigns. The OZIE Team has recently changed their second stage email inbox to Gmail accounts. The second stage email inbox is intended to filter the keylogger data to reduce the amount of emails that the group must review. After discerning high-value targets in the second stage inbox, the keylogger data is then forwarded to a third email address. The emails in this stage are targets which will likely be targeted by the group.

Bot

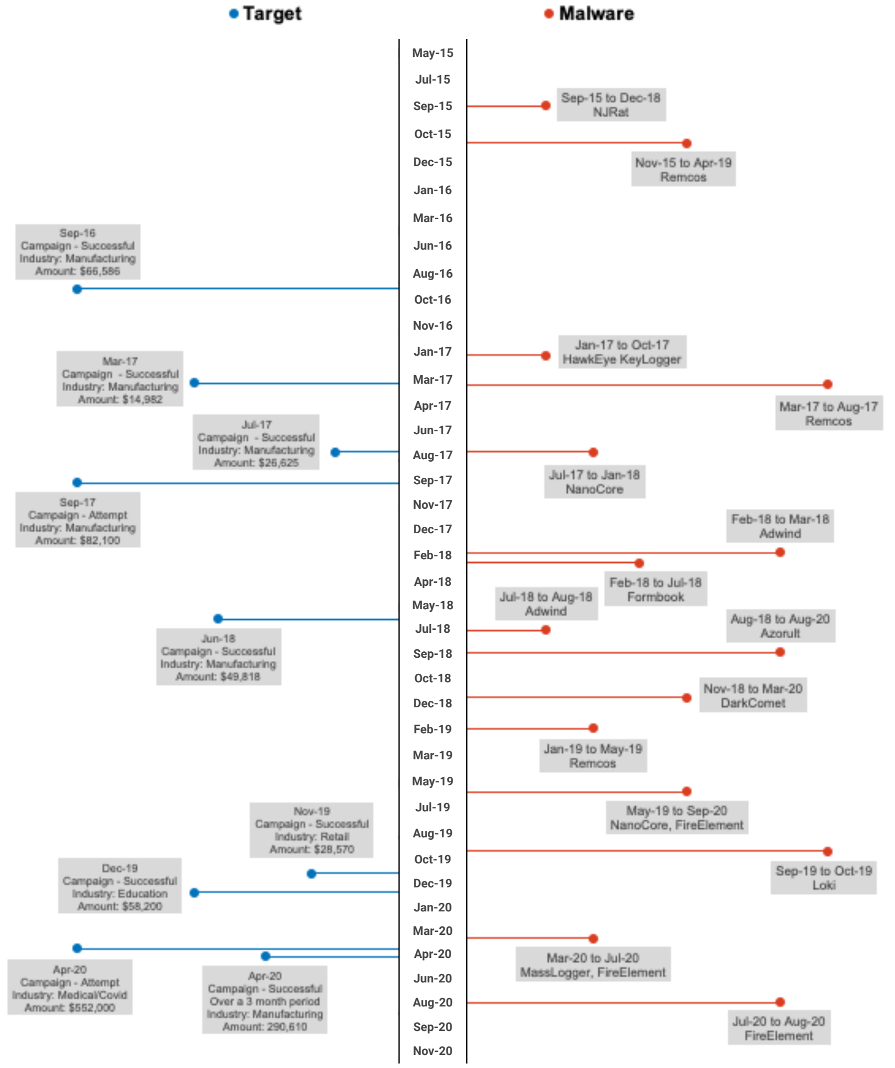
The OZIE Team configures bots from Java RATs and Formbook to report back on non-standard ports to a static IP address assigned to an nVPN account. A VPS is configured with the OpenVPN profile generated by nVPN and used to run the bot server for data exfiltration.

Distribution

VPS have historically been provisioned weekly to bi-weekly depending on efficacy of the targets' spam filtering and blacklisting. The OZIE Team used separate email addresses to collect the victim keylogger data and to manage the procurement of the VPS infrastructure. Due to the large number of ongoing campaigns, the OZIE Team did suffer lapses in OpSec (operational security) and the GTIC identified cases where several email addresses related to the victim data collection overlapped with the acquisition of the VPS infrastructure.

Gammadyne Mailer is the group's mailer of choice. An email template is created and distributed to members specifically for each campaign, both for the target industry/region and to vary the wording in hopes of avoiding blocked emails. The malware of choice is uploaded to the VPS and used as an attachment on the distributed emails.

Timeline



Business email compromise (BEC)

To compromise an organization's email, an actor goes through a fairly standard process flow:

1. Gather target email addresses from public and private sources.
2. Send malspam to a targeted group. Generally, a country/region or industry.
3. Use keylogger data of successfully compromised victims to access email accounts.
4. Identify lucrative transactions.
5. Gain access to the conversation in a way that enables the actor to change bank account information.
6. Commit wire fraud.

Analyzing an actual BEC incident can give a more detailed insight into the process. Names and indicators are omitted or changed for the protection of the original organizations.

The OZIE Team has targeted organizations in many industrialized nations, especially those with large manufacturing bases like **Singapore, China, the United Kingdom and the United States.**

Case study: PVC Polymer purchase between Texas and Mexico

This case study details BEC executed against a Mexican company during an attempt to purchase PVC polymer from a Texas company. During a seven-month operation the Mexican company lost over USD 290,000 and the Texas company received no payments.

To prepare for a malspam campaign, attackers use a VPS to scrape email addresses and send malspam. The OZIE Team used Web Data Extractor Pro to scrape desired public web pages for email addresses. In this case, they specifically targeted the steel industry. The actors run a Google search for anything and everything to do with the steel industry and feed the related domains into Web Data Extractor Pro. The extractor then scours all supplied domains for email addresses. These become the targets for their malspam campaign targeting the steel industry.

Once a set of target email addresses are identified, generally in the tens to hundreds of thousands, they are fed into Gammadyne Mailer for delivery. An attacker crafts a simple email asking for the victim to open an attached file to view an invoice. A remote access trojan (RAT) or keylogger is attached to the email. In the case of this campaign, a keylogger called MassLogger was attached.

The keylogger was set up in the OZIE Team's standard configuration, with SMTP log exfiltration to an email address which was then redirected to a secondary address hosted in Gmail. The first address is setup through Domains4Bitcoins.com to ensure an exfiltration domain for each campaign. From the secondary email address logs are analyzed for victims, a majority of the keylogger data returned is from sandboxes. When they can identify a valid and prospective target email account, the OZIE Team sets up a filter to send copies of all emails to another Gmail account, specifically used for receiving emails from compromised accounts. It is from this account that tangible actions are decided on. If a transaction between two companies begins to transpire then the actors will inject themselves in the middle of the conversation.

The Mexico-based company was compromised by the OZIE Team on 11 October 2019. A typosquatting domain was created for the Mexico company on 25 December 2019 and the Texas company on 14 January 2020. The OZIE Team began to act on transactions between the Texas and Mexico companies from 20 January 2020. A PVC polymer order required just over USD 290,000 to be made to the Texas company in five separate payments over three months.

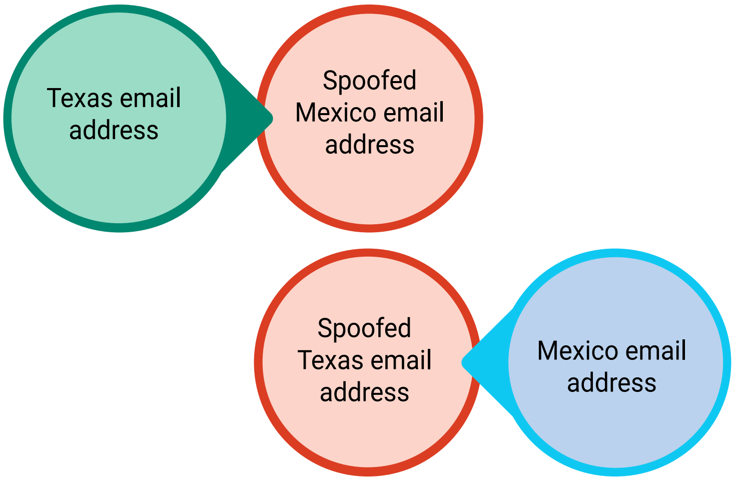
The OZIE Team injected themselves in this conversation first by registering a domain similar to the companies involved, (for instance, 'texascompanys.net' instead of the official 'texas-company.com' and 'mexicocompany-mx.com' instead of the official 'mexicocompany.com.mx'). They created email accounts mimicking four of the sales personnel in Texas and three accounts of personnel involved in the Mexico company (if the email address began with 'smith', they created a 'smith' on their own domain. They initiated conversation with the Texas company from the typosquat Mexico email to initiate a man-in-the-middle (MitM) attack in the conversation. Emails were then passed between the spoofed accounts to MitM the communication between two companies. They basically ran entire conversations with each targeted organization and managed the flow of communications to each entity.

By controlling the flow of the conversation, the OZIE Team was able to maintain visibility into the transaction. When banking information was exchanged for payment, they replaced it with their own fraudulent account. During the three-month period the Mexico company was supposed to be making payments, the OZIE Team informed the Texas company that the Mexico company would have to delay payments. All the while, the Mexico company was conversing with, and making payments to the OZIE Team, thinking they were making payments to the Texas company.

Summary

The OZIE Team has been conducting successful cyberattacks since 2017. They have relied heavily on commodity malware and have improved the efficiency of their operations by changing malware to ensure their attacks remain current and successful. They focus on stealing organizational email credentials, then using those credentials to conduct business email compromise (BEC) attacks. These attacks have had varying degrees of success but continue to generate significant income for the group.

BEC attacks continue to be a threat, and the OZIE Team is a good example of a threat actor group who maximizes their ability by making efficient use of modern malware and a proven approach. We have every expectation that this group will continue to operate and continue to be successful as long as they are able to operate.



#Spotlight 1

The evolution of **business email compromise**

Lead Analyst: Jon Heimerl, CISSP, Sr. Manager, Global Threat Intelligence Center, US

Business email compromise (BEC) is not a new type of attack, but has greatly evolved over the past seven or eight years. The United States' FBI started tracking BEC attacks in 2013, through reporting via the www.ic3.gov site.

What is a BEC attack?

BEC attacks are a combination of social engineering and phishing. These attacks rely on the actor being able to trick selected people within the targeted organizations to provide some amount of funds based on directions provided via email.

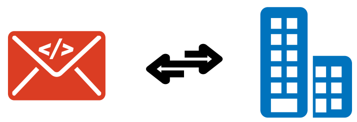


Figure 1: Transactional BEC between attacker and victim

In the early days, BEC attacks were labour-heavy, manual attacks. Through social media and available corporate information, the attacker would identify a few important email addresses in the target organization (like someone in finance, human resources and an executive). The attack would potentially include only a limited number of emails establishing a direct communication with the targeted user(s). The attacker masquerades as a person of importance in the organization, initiates a conversation and asks for funds. A sample email from an early attack is included in Figure 2.

In this example, CEOKevin is the CEO of the company, BantaBall. The attacker has registered his own domain, substituting 'ones' for the two 'L' in the name. This is a technique called 'typosquatting' and is a fundamental part of most BEC attacks. The attacker would send an email to (for instance) someone in finance, pretending to be the CEO, asking them to transfer money. The fake email can be difficult to identify.

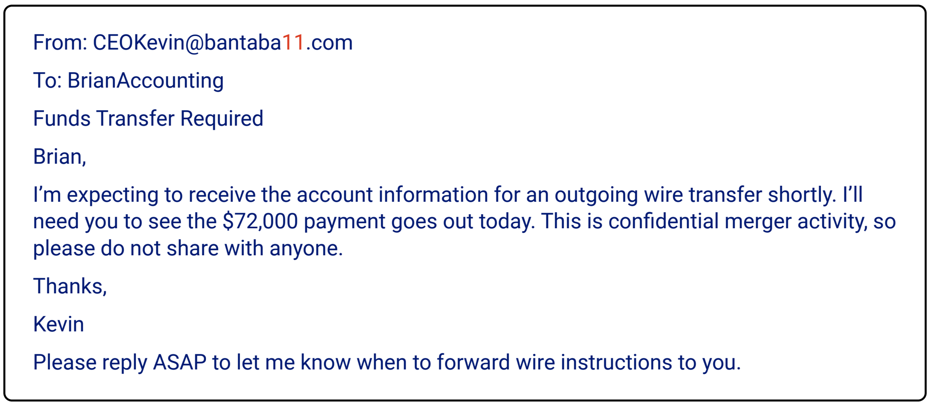
This technique has been surprisingly effective. Over a 21-month period spanning 2013 through 2015, the United States FBI tracked 8,179 successful BEC attacks around the globe. These attacks yielded nearly USD 800 million, accounting for BEC-related losses of about USD 38,000 per month.

This email would be shortly followed by another email with an account number owned by the attacker. The method relies on the targeted person being eager to satisfy the needs of the person who originated the request.

Have BEC attacks matured?

Over the past several years, BEC attacks have matured greatly. The article on the OZIE Team in this month's report describes an example of this modern attack more fully. The attack process is a more complex process, which can be highly automated with effective use of proper toolsets. A relatively unskilled attacker can conduct these attacks and be highly successful.

Modern processes use automated tools to help identify large volumes of email addresses across many potential victims. The attackers still make use of typosquatting techniques to help disguise their fake domains. But, where earlier



From: CEOKevin@bantaba11.com

To: BrianAccounting

Funds Transfer Required

Brian,

I'm expecting to receive the account information for an outgoing wire transfer shortly. I'll need you to see the $72,000 payment goes out today. This is confidential merger activity, so please do not share with anyone.

Thanks,

Kevin

Please reply ASAP to let me know when to forward wire instructions to you.

Figure 2: Sample early BEC email

BEC attacks were very transactional in nature – usually relying on a single score – the most effective BEC attacks progress as described in the OZIE Team article. The attacker uses a man-in-the-middle (MitM) attack to effectively insert themselves into an existing relationship and communication, in order to intercept a series of payments over a more sustained time period.

Figure 3: Man-in-the-middle attack intercepting communications

The attacker identifies an ongoing business relationship, then uses fake domains and emails to actively manage communications between the two parties. 'Business as usual' communications are essentially passed through the attacker who acts like a transparent proxy. As funds transfers (valid payments being made by one company for products or services) are arranged, the attacker substitutes their own account information for payments. While normal communications are passed through, any communications about payments, delays in goods, or delivery details, are deleted, edited out or created by the attacker to maximize the amount of funds which can be gathered while they manage the relationship and try to avoid making the victim suspicious for as long as possible.

Are BEC attacks really that big?

These attacks have proven highly successful. There are multiple accounts of multiple victims losing in the order of USD 47 million each. In the 37 months from the summer of 2016 to the summer of 2019, the US FBI, through their Internet Crime Complaint Center, reported 166,349 successful BEC attacks yielding over USD 26 billion in losses. This equates to losses of about USD 708 million per month and an increase in monthly losses of nearly 1,800%.

The FBI's most recent analysis indicated that they track about USD 3.5 billion in annual losses due to cybercrime, and that BEC attacks account for about USD 1.77 billion of that – meaning BEC attacks likely account for over 50% of all losses due to cybercrime.

And attacks are getting bigger (see Table 1), which suggests that these numbers are likely to rise. According to the Anti-Phishing Working Group, during the first quarter of 2020, the average BEC attempt was USD 54,000. As of 1 September 2020, that number had risen to about USD 80,000 per attempt. And, some groups are looking for even higher numbers. The Russia-based BEC group called Cosmic Lynx averages USD 1.27 million per attempted BEC attack.

Summary

BEC attacks continue to increase in complexity and size. The amounts targeted are growing, and advanced toolsets are making the attacks easier than ever, not only allowing existing actors to be more efficient, but allowing less mature threat actors enter the market. BEC attacks have proven profitable, effective, and are likely to continue. Organizations need to be aware of such threats and must strive to ensure good conformance to standard practices, and to avoid reliance on email for verification of financial transactions.

	2013-2015	2016-2019
Global incidents:	8,179	166,349
Total losses:	USD 799 million	USD 26 billion
Losses per month:	USD 38 million	USD 708 million

Table 1: Increase in BEC attacks

Election security: What *not* to do

Lead Analyst: Michael Daniel, President & CEO, Cyber Threat Alliance

Over the last few months, many articles and blogs have discussed threats to the United States' elections and how to combat them.

Those pieces usefully distinguish between the threats to the different elements of our elections, including the electoral infrastructure (the systems and processes used to conduct elections), campaigns (breaking in and stealing information either for espionage or to release publicly), or the general information environment (including disinformation in the form of deliberately creating or disseminating false information). Logically, those articles also focus on what actions cybersecurity companies, organizations and individuals should take to better protect our elections, political campaigns and information space. However, relatively little attention has been paid to the inverse question: Are there actions that are counterproductive and should be avoided?

Over the past year, the Cyber Threat Alliance (CTA) has actively engaged on election security, primarily through a voluntary working group of interested members. Many of the working group members have significant expertise in election security. While we focused primarily on election security within the United States, most of these concerns also apply to many other areas around the globe. As part of its work, the group has identified some common actions that are counterproductive at best and actively harmful at worst. This article will lay out some actions that organizations or individuals should not take in tackling these threats.

> Not leaping to conclusions or blowing events out of proportion **will help maintain the integrity of the process.**

Don't panic

While we should take the threat seriously, our election infrastructure is resilient. Elections in the US are managed at the state and local level, with over 8,000 jurisdictions conducting them. The distributed nature of elections makes it hard to defend, but also hard to attack at scale. This lack of scalability means that altering election results in the aggregate is exceptionally difficult. Further, most jurisdictions have upgraded their cybersecurity since 2016 and 2018, even if many could still make improvements. Finally, the US government, election officials and cybersecurity providers are very focused on protecting the electoral infrastructure. The system's resiliency and distributed nature means that small hiccups and disruptions do not undermine the validity of the overall results. The defensive improvements and increased attention mean that network defenders are more likely to detect attempts to disrupt the electoral infrastructure. As a result, any discussion about threats to our elections should strike a balance between taking it seriously and slipping into hyperbole.

Don't lose perspective

Every election has irregularities and small disruptions, usually due to human error. Prior to 2016, these irregularities rarely seemed newsworthy because the scale of our elections meant small discrepancies did not materially affect the outcome. Today, the digitization of the elections process creates greater concern that small irregularities could indicate more significant problems, so we are more aware of the irregularities. However, while we should pay attention to the irregularities to make sure they are not indicators of malicious activity, the normal rules of cybersecurity still apply: Don't exclusively assume malice until error has been eliminated. Not leaping to conclusions or blowing events out of proportion will help maintain the integrity of the process.

Don't advise actions that officials can't take

To comply with legal requirements, most election jurisdictions 'lock down' their systems several months before an election. After that point, officials cannot make technical changes to electoral

systems, whether those are voter registration databases, voting machines, pollbooks or tallying systems, until after the election. Haranguing officials about technical cybersecurity improvements in the few months before an election is counterproductive because they cannot make them for very legitimate reasons. All such advice does is strain relationships with election officials. This point leads directly to the next one.

Don't fall into the Valley of Death

Many people forget about election security the day after the election. One researcher referred to this as the Valley of Death – the time election officials could make cybersecurity improvements is when most people are least interested in helping them. Instead, the best time to engage with election officials is after the election is complete and before the ramp up for the next election. That period is the time for suggesting technical improvements and process changes.

Don't focus on the opportunistic buck

After the 2016 election, the Federal government provided significant one-time grants to local jurisdictions to upgrade election system cybersecurity. From the perspective of many election officials, they were suddenly bombarded by hard sales pitches that seemed very opportunistic. Not surprisingly, these officials reacted poorly to this approach and it tarnished the image of the entire cybersecurity industry. Thus, cybersecurity providers are often starting with a negative reputation in this sector. In order to overcome that perception, cybersecurity companies need to spend time learning the sector's nuances and the individual state or local jurisdictions. Of course, election officials understand that private sector cybersecurity providers need to make money. They just don't want to feel taken advantage of in the process.

Rushing trust
isn't possible.

Don't rush it

As cybersecurity has evolved beyond protecting wired desktops operating a few business applications on an internal network, providers have had to learn about new operational areas (e.g., medical exam rooms), new technology types (industrial control systems), and new political environments (public utilities). These aspects all apply to the elections sector. It is complex and politically charged, not motivated by profit, and operates in a unique environment. Due to the relatively slower adoption of digital technologies, though, the elections sector is a relative late comer to cybersecurity. Just as cybersecurity providers had to build trust with their clients in other sectors, the same process will need to happen in the elections sector. Rushing trust isn't possible.

Don't try for perfection

As with so many other areas, digitization and connectivity have profoundly and permanently changed the threat profile for our elections. US and other democratic elections will continue to be targets for the foreseeable future. Since malicious activity aimed at this sector can pose an existential threat, cybersecurity providers need to invest in it for the long-term. We'll never eliminate these threats, so we can only seek to manage, mitigate and respond to them. The same risk management mindset used in other sectors and for other threats within this sector, such as voter fraud, needs to be adopted for dealing with cyberthreats to the electoral infrastructure.

Election security is here to stay

Elections form the cornerstone of our democracy. Now that they face significant cyberthreats, the cybersecurity industry needs to learn how to work in the electoral sector, which includes understanding both what to do and what not to do. If the industry can internalize these lessons, we can significantly reduce the risk to our elections. The alternative isn't a path any of us want to go down.

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