2023

Global Threat Intelligence Report

Line between cyberthreats and physical impact continues to blur

NTT | Security Holdings

Global Scalable Security Solutions
security.ntt

Today’s global cyberthreats pose an increased threat to our daily lives on a local level.

Understanding the threats is the first step in protecting your digital assets and infrastructure.

Foreward

As technology advances and the world becomes increasingly interconnected, cybersecurity will continue to grow more important than ever before. Robust cybersecurity defenses must keep pace to protect our digital assets and infrastructure from malicious actors.

For our 2023 Global Threat Intelligence Report, NTT Security Holdings analyzed the threats we observed, the wider threat landscape and its increasing impact on daily life. 2022 saw an acceleration in politically motivated responses, major incidents resulting in critical infrastructure and supply chain disruption, as well as significant focus on government response to cyberthreats through new agencies or legislation.

This complex and dynamic threat landscape requires constant vigilance and proactive response.

To ensure you can do just that, NTT Security Holdings provides the essential tools, resources, and services you need to protect your cloud, network, endpoint, and data effortlessly and effectively. We encourage business and technical leaders to leverage this report’s insights to plan and execute security strategies internally. By doing this, you’ll not only be prepared to detect and respond to attacks across all levels of your digital landscape, but you’ll also be a part of creating a connected future that’s better for all people and society as a whole.

Gregory Garten

CTO, NTT Security Holdings

Greg has been with NTT for over 10 years where he has focused on engineering and product development of their cybersecurity platforms, products, and services. Additionally, Greg has held various engineering and executive roles at companies such as Intuit, Cisco, Silver Lake Sumeru, Exodus Communication, Cybera, and several overseas technology startups and multinational technology companies.

NTT Global Threat Intelligence Platform

1500
enterprise customers

800 billion+
logs processed per month

20+ years
experience in 24/7 Managed Security Services

Global Tier 1 Internet backbone telemetry and honeypot sensors

This year’s report contains analysis based on attack and incident reports, vulnerability trends and threat intelligence from January 1, 2022, to December 31, 2022.

Ransomware and data breaches are only the beginning.

Attacks on power grids could lead to blackouts, while supply chain breaches could disrupt the delivery of essential goods.

Key findings

In 2022, a growing concern for businesses, organizations, and governments around the world was the cyber risk to critical infrastructure and supply chains – and with good reason. Cyberattacks have real-world consequences. A cyberattack on a power grid, for example, could cause widespread blackouts, while a breach of a supply chain could lead to disruption in the delivery of essential goods and services.

As unsettling as that is, developments in technology also advanced the severity of threats and the number of malicious actors. Cyberthreats to critical infrastructure and supply chains came from a variety of sources, including nation-state actors, organized crime groups, and individual hackers. The devastating and far-reaching consequences of these cyberattacks range from ransomware attacks and data breaches to disrupting operations and even physical damage.

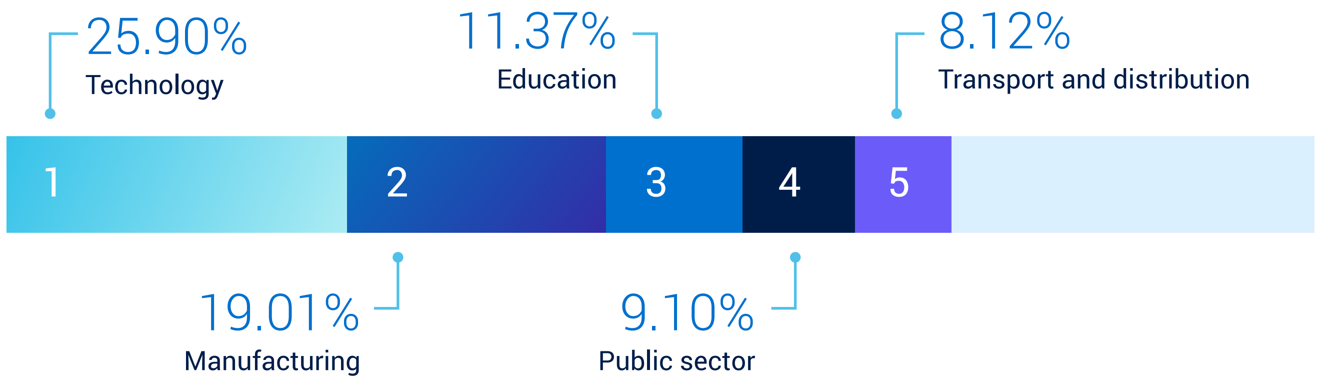
Our key findings focus on:

1. **The top 5 most-attacked sectors**
2. **Cloud and SaaS attacks**
3. **Web application attacks**
4. **Banking trojans and cryptominers**
5. **High-impact and top targeted vulnerabilities**

While it's important to have awareness of the threats, it's essential to know how to safeguard your business or organization from them. At the end of the report, you'll find **five recommendations** you can start implementing immediately. In many cases, the recommendations simply require enabling functionality that is readily available in products that you have already purchased.

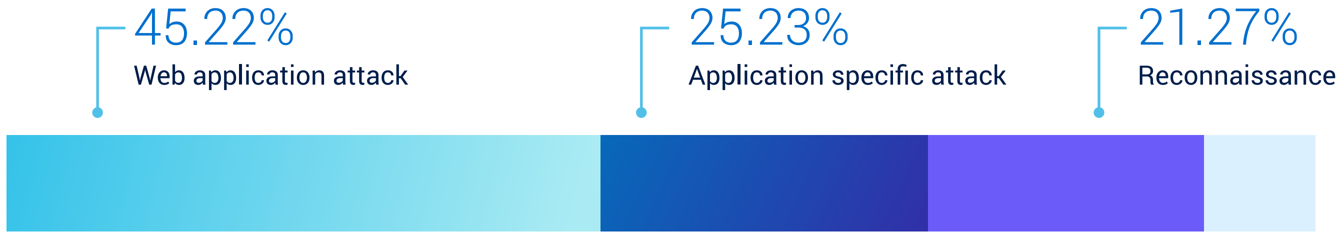
1. Top 5 most-attacked sectors

Critical infrastructure and supply chain remained high-value targets. Since Technology, Manufacturing, and Transport/Distribution are heavily integrated into these integral infrastructure and supply aspects of day-to-day life, those industries remained in our top 5 most-attacked sectors. The Public sector made the biggest jump in the past year, moving from #6 in 2021 to #4 in 2022. The heating geopolitical climate accounted for this movement. Like last year, Education remained in the top 5, largely due to Microsoft Office attacks and cryptomining stemming from student devices and more open networks on many campuses.



2. Cloud and SaaS attacks

As anticipated, attacks on cloud and SaaS continued to increase based on the Global Threat Intelligence Center's (GTIC) telemetry. Web-based application and desktop application threats made up 70% of attacks. Content Management System (CMS) software such as WordPress, Apache products and utilities like Log4J and Atlassian products such as Confluence combined to form a total of around 80% of web-hosted targets. This trend was further highlighted by critical vulnerabilities in products such as JIRA, Confluence and Bitbucket which were patched throughout the year but could lead to account takeover.



3. Web application attacks

Globally we saw a relatively even distribution of attacks against CMS software, plugins, and PHP web applications, comprising a notable portion of the attacks above. WordPress was the most attacked (CMS software) in the Americas, APAC (Asia Pacific) and EMEA (Europe, the Middle East and Africa) despite the fact that nearly half of publicly accessible hosts running WordPress reside in the United States, compared to a smaller usage in other regions.

APAC

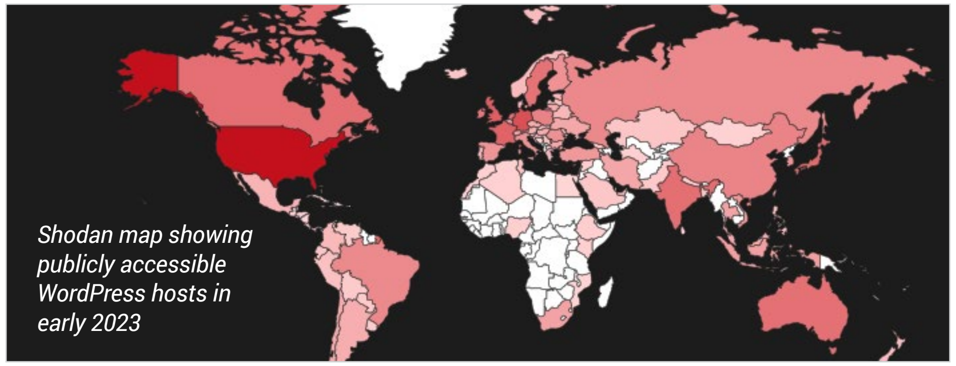
Framework	Percentage
WordPress	31.10%
PHPUnit	30.91%
ThinkPHP	21.67%

Americas

Framework	Percentage
WordPress	36.10%
PHPUnit	20.33%
Drupal	13.20%

EMEA

Framework	Percentage
WordPress	38.82%
Drupal	24.03%
vBulletin	14.14%

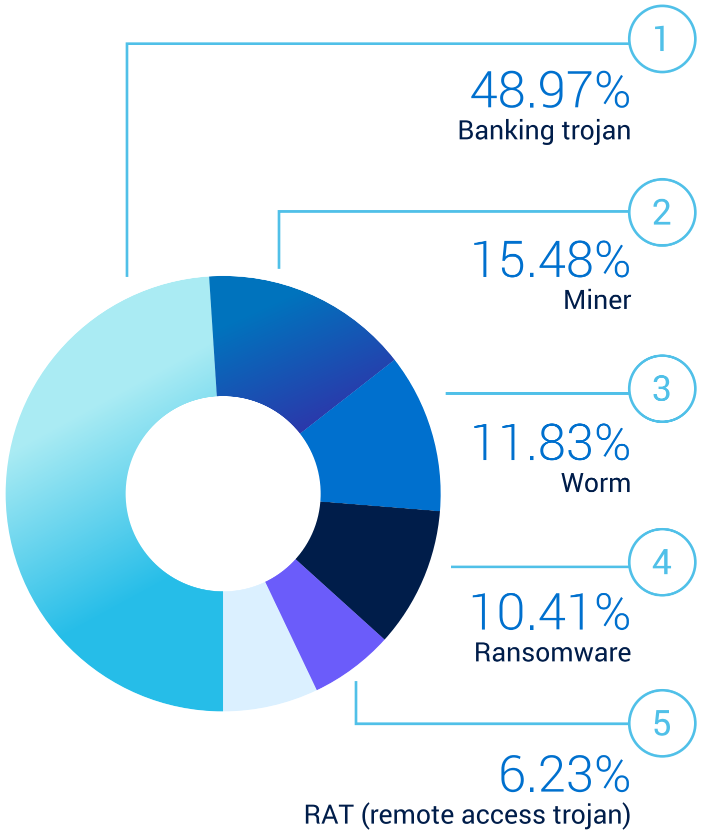


Shodan map showing publicly accessible WordPress hosts in early 2023

As opposed to targeted campaigns, such as a threat actor trying to beat down the front door via a noisy WordPress exploit, attacks on many applications tended to be based more heavily on exploits integrated into malware and botnets. For example, a Go language Linux trojan began targeting WordPress in 2022. This targeting was reflected in the volume increase GTIC observed as opposed to being more focused in a single country or region. GTIC saw a similar increase in attacks against Realtek, a continuation of the exploitation which began with the announcement of vulnerabilities in the Realtek SDK in Q3 of 2021. These vulnerabilities were integrated further into botnets such as Mirai, Mozi and later in 2022, RedGoBot. Realtek chipsets are found in large numbers of devices in the IoT space and were the number one most targeted in the Americas at 57%, primarily in the Technology sector.

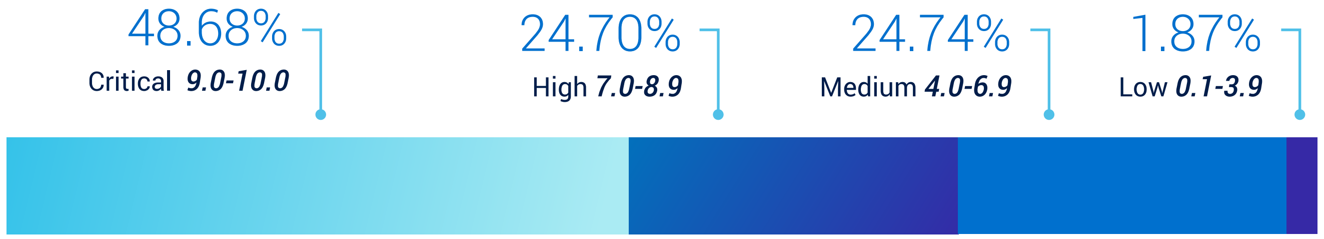
4. Banking trojans and cryptominers

Banking trojans tapered off a bit from last year, but still lead the pack. Cryptominers rose back up after a 2021 lull, despite many currencies losing value. These fluctuations are relatively common as industry partners, hosting providers and law enforcement attempt to disrupt and dismantle actors and malware infrastructure – as well as resurgences observed in previously disrupted malware, such as Emotet. Malware is evolving more quickly with some changing more than their TTPs; Ursnif dropping the financial theft capability in 2022 with a new variant for example.



5. High-impact & top targeted vulnerabilities

GTIC continues to observe attackers targeting high-impact vulnerabilities, with nearly 75% having critical- or high-severity CVSSv3 scores. While there is continuous scanning of vulnerabilities to exploit 24x7, more effort is being put into weaponizing code toward CVEs that have low attack complexity and higher impact scores.



The top targeted vulnerabilities are often widely known and publicized, yet still successful. Three of the top five CVEs we saw targeted in 2022 are all in the US Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerability Catalog. This finding highlights that gaps still exist in vulnerability management and response, as well as visibility gaps within organizations on their own attack surfaces.

Product	CVE	Percentage	CVSS
Apache Log4J	CVE-2021-44228	26.25%	10
Realtek SDK	CVE-2021-35394	5.02%	9.8
Spring Cloud	CVE-2022-22963	2.93%	9.8

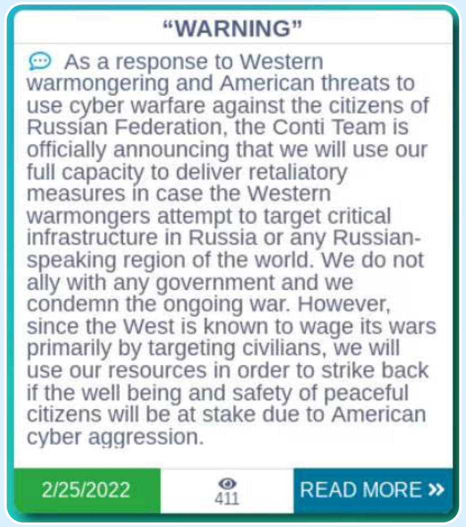
Spotlight on: Ransomware insights

While ransomware has been a high-profile threat for years, Lapsus$ quickly reminded everyone it wasn't slowing down in the beginning of 2022 with a series of high-profile attacks and data leaks.

In April and May, several Costa Rican government institutions were impacted with both Conti and Hive claiming responsibility for different stages of the attacks.

Medibank, Australia's largest private health insurer, saw millions of customer records accessed late in the year.

Ransomware also crept into the geopolitical space, with Conti threatening American and Western nations in relation to Russia's invasion of Ukraine.



"WARNING"

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

Ransomware continues to evolve rapidly, both in terms of the number of active groups at a given time and the tactics, techniques and procedures leveraged by them to compromise organizations. 2022 saw several successful groups persist and some resurfacing through rebranding. New high-profile groups continue to emerge frequently to replace others that fade away or get disrupted by law enforcement.

Ransomware highlights

Despite being disrupted by DDoS attacks in Q3, Lockbit continues to see success year after year, with nearly 30% of the reported victims of ransomware gangs tracked by NTT in 2022 being infected by Lockbit 2.0 or 3.0.

Several groups began adopting newer techniques as well, leveraging intermittent encryption or partial encryption of victim files to improve the speed of the encryption process and to evade detection systems.

Manufacturing was the most impacted sector, compromising over 20% of reported leaks.

North American and European organizations made up roughly two thirds of reported leaks – with companies in the US and Canada making up nearly 50% of the victims.

Newcomers

Became active in 2022.

BlackBasta
Royal
BianLian

Play
Stormous

Survive & profit

Multi-year operations, successful in 2022.

Lockbit
AlphaV
Hive

Karakurt
Vice Society

Inactive

No longer active in 2022.

Cerber
Darkside
Egregor

Locky
Prometheus

Staying power

Active for 3+ years, less successful in 2022.

Cl0p
Cuba
Suncrypt

RagnarLocker
Snatch

These statistics are based on GTIC research and collection of listings on dark web data leak "shame" sites, social media (e.g., Telegram) channels and public reporting and disclosures.

Spotlight on: Cyber bleed over

Cybercriminals and state-sponsored hackers are continually developing new tactics, techniques, and procedures to circumvent security measures and exploit vulnerabilities. These attacks can have far-reaching consequences, both short- and long-term, such as economic losses, social upheaval, and political instability. For example:

- The Costa Rican ransomware incident in 2022 impacted the country for several months.
- Managed service provider (MSP) Advanced was hit by a ransomware attack, which disrupted emergency services to the NHS.
- A cyberattack disrupted Germany's fuel distribution and payment systems at some filling stations.

Responding to Cyberthreats

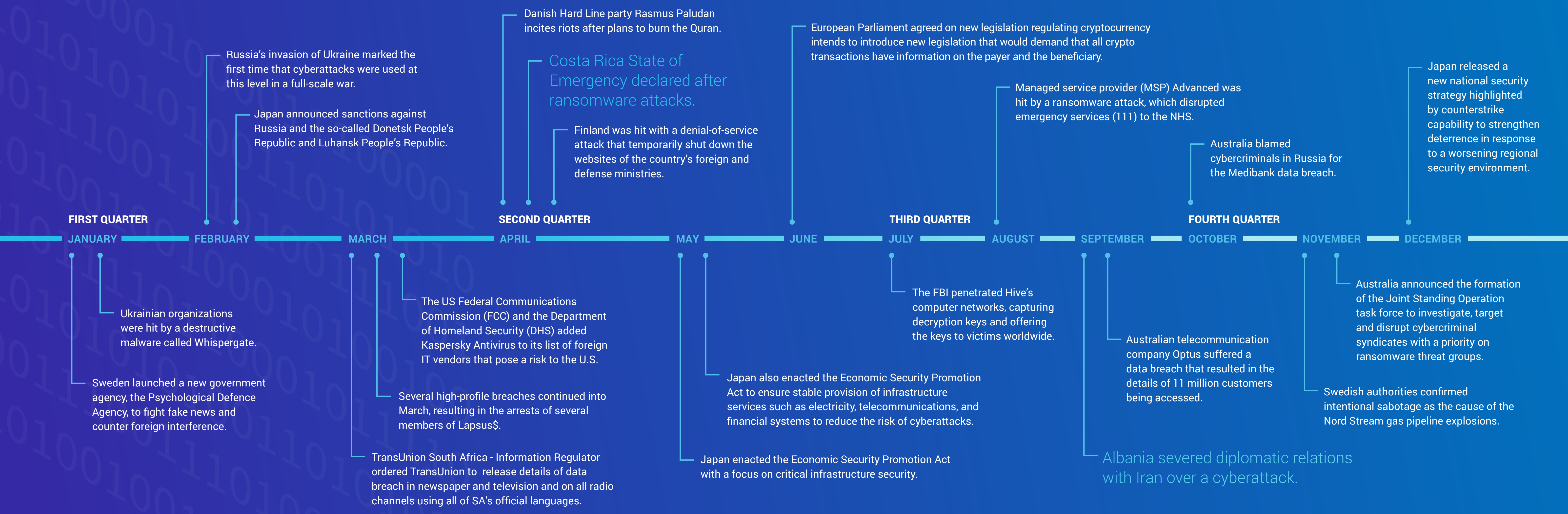
While cyberthreats are becoming increasingly sophisticated and constantly evolving, individuals, organizations, and governments are responding to the challenges of keeping pace with the rapidly changing threat landscape. Many governments and organizations have already revisited their privacy and breach disclosure policies to enact change at various levels.

Other examples of real-world actions include:

- In response to misinformation and foreign interference, Sweden established the Psychological Defense Agency in 2022.
- The U.S. Federal Communications Commission added Kaspersky Lab to a growing list of companies deemed to pose a threat to national security or the security of the United States due to allegations of Russian government connections.
- Albania severed diplomatic relations with Iran following a 2022 cyberattack.

Cybersecurity is Everyone's Job

To mitigate the risks and minimize the potential impact of attacks, it is crucial for organizations and governments to invest in cybersecurity measures and raise awareness of cyberthreats. Doing this, however, cannot be a siloed effort. Powerful security requires a collaborative effort between governments, businesses, and individuals to create a safer and more secure digital environment.



FIRST QUARTER

JANUARY

Ukrainian organizations were hit by a destructive malware called Whispergate.

Sweden launched a new government agency, the Psychological Defence Agency, to fight fake news and counter foreign interference.

FEBRUARY

Russia's invasion of Ukraine marked the first time that cyberattacks were used at this level in a full-scale war.

Japan announced sanctions against Russia and the so-called Donetsk People's Republic and Luhansk People's Republic.

MARCH

The US Federal Communications Commission (FCC) and the Department of Homeland Security (DHS) added Kaspersky Antivirus to its list of foreign IT vendors that pose a risk to the U.S.

Several high-profile breaches continued into March, resulting in the arrests of several members of Lapsus$.

TransUnion South Africa - Information Regulator ordered TransUnion to release details of data breach in newspaper and television and on all radio channels using all of SA's official languages.

SECOND QUARTER

APRIL

Danish Hard Line party Rasmus Paludan incites riots after plans to burn the Quran.

Costa Rica State of Emergency declared after ransomware attacks.

Finland was hit with a denial-of-service attack that temporarily shut down the websites of the country's foreign and defense ministries.

MAY

Japan also enacted the Economic Security Promotion Act to ensure stable provision of infrastructure services such as electricity, telecommunications, and financial systems to reduce the risk of cyberattacks.

Japan enacted the Economic Security Promotion Act with a focus on critical infrastructure security.

JUNE

European Parliament agreed on new legislation regulating cryptocurrency intends to introduce new legislation that would demand that all crypto transactions have information on the payer and the beneficiary.

THIRD QUARTER

JULY

The FBI penetrated Hive's computer networks, capturing decryption keys and offering the keys to victims worldwide.

AUGUST

Managed service provider (MSP) Advanced was hit by a ransomware attack, which disrupted emergency services (111) to the NHS.

SEPTEMBER

Australian telecommunication company Optus suffered a data breach that resulted in the details of 11 million customers being accessed.

Albania severed diplomatic relations with Iran over a cyberattack.

FOURTH QUARTER

OCTOBER

Australia blamed cybercriminals in Russia for the Medibank data breach.

NOVEMBER

Australia announced the formation of the Joint Standing Operation task force to investigate, target and disrupt cybercriminal syndicates with a priority on ransomware threat groups.

Swedish authorities confirmed intentional sabotage as the cause of the Nord Stream gas pipeline explosions.

DECEMBER

Japan released a new national security strategy highlighted by counterstrike capability to strengthen deterrence in response to a worsening regional security environment.

Recommendations

Today's active digital landscape means that businesses and organizations can no longer ignore threats. Attacks are likely to happen, regardless of a company's size or industry. Preparation and vigilance are key, starting with these five recommendations.

1

Enable multi-factor authentication.

This is our strongest recommendation, and in many cases, you may not have to spend large amounts of money to get started. Multi-factor authentication is often included in many products, and many allow it to be set and enforced policy-wide rather than per user. We recommend enabling multi-factor authentication especially for any third-party tools and vendors, as well as any management consoles and control panels.

2

Monitor all malware.

Many organizations tend to only monitor the primary threat actors and malware targeting their sectors. However, it's essential to monitor overall commodity malware TTPs as well. Most organizations will observe these exploit and delivery attempts much more frequently than targeted campaigns.

3

Review and test continuously.

Cybersecurity is not a "set it and forget it" protocol. Instead, revisit attack surface and vulnerability management approaches, and test often to validate maturity. While some announced vulnerabilities are overhyped or more complex to exploit, a mature approach should alleviate pain points associated with overreacting to the media cycle. GTIC still observes many legacy vulnerabilities exposed, which leaves entry points into networks via perimeter devices or third-party integrations.

4

Disable unused plugins.

Another simple and affordable recommendation is to disable unused plugins and features. You'll also want to ensure that you have security capabilities enabled on top of publicly exposed software — especially open-source tools. These are easy to profile and even easier to take advantage of.

5

Assess third-party vendor security.

To safeguard against supply chain attacks, assess third-party vendor security and ensure that the necessary security features are enabled to protect your assets. Insufficient review and validation in this area increases exposure to the ever-increasing volume of supply chain exploits. Like our first recommendation, this step is affordable and may simply require enabling functionality that is available in products already in your environment.

Final thoughts

As threats continue to evolve,
we will continue to also see the threat
landscape accelerate and evolve.

Third party vendors and APIs

Large-scale and significant breaches will keep moving forward, especially across companies and industries related to one another. Shared vendors, hosting providers and applications are increasingly being targeted in the hope that they can be used as conduits to target their customers. These make for incredibly valuable targets in order to facilitate supply chain attacks.

Public AI evolution

The evolution of tools such as ChatGPT has rapidly increased the capability of users, allowing anyone to write (malicious) code by simply asking questions or listing a statement of requirements. While these tools have guardrails in place that are intended to prevent this kind of exploitation, enterprising users can still find ways to leverage AI to write malicious code.

As these same tools are leveraged by users in new and innovative ways, it is important to ensure policy, procedure, guidelines, and DLP safeguards prevent well-intentioned actions from exposing intellectual property or PII.

Further impact on international relations

The geopolitical climate will see further state-backed cyberattacks and increasing tensions in various regions. We've already seen the cascading implications of this after a 2022 breach of X_TRADER by North Korean actors, which then targeted critical infrastructure and continued with a secondary supply chain breach of 3CX.

Global data analysis methodology

1 NTT Security Holdings gathers security log, alert, event, and attack information from which it enriches, and analyzes contextualized data.

2 NTT's unique visibility into global Internet telemetry and data collected from NTT's globally deployed honeypot sensors.

3 Expert contributions provided by SOC embedded intel analysts, NTT CERT, Security and Trust Office.

4 Collaboration and expert insight from our intelligence alliance with the Cyber Threat Alliance, Microsoft, CISA and National Cyber Forensics and Training Alliance (NCFTA).

About GTIC

NTT Security Holdings Global Threat Intelligence Center goes above and beyond the traditional pure research organization, by taking threat research and combining it with NTT proprietary detective technology to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence enabling NTT Security Holdings to prevent, detect and respond to cyberthreats.

To provide a truly unique vantage point within our products and services, GTIC leverages proprietary intelligence capabilities and NTTs unique ISP backbone visibility to gain understanding of and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures used by attackers.

We’re here for you

Cybersecurity can feel like an overwhelming challenge, but you’re not alone in this battle. NTT can help you assess your current risk-profile and then work with you to map out a security strategy that works best for your organization and budget. We encourage you to contact us today for more information about our security products and services.

Contact us at
security.ntt/contact

NTT Security Holdings

Together we do great things.

security.ntt