NTT | Security Holdings

2022 Global Threat Intelligence Report

A year of more sophisticated and substantial threats.

Together, we secure the connected future

security.ntt

Society is rapidly changing as organizations look to safely navigate an increasingly uncertain geopolitical environment.

A dynamically evolving threat landscape comprised of determined cyber adversaries, innovative tools and refined techniques are challenging the status quo. With COVID-19 pandemic and mounting supply-chain disruptions impacting business continuity, companies – now more than ever – are looking for cybersecurity partners to navigate this landscape.

Introduction

In the 2022 NTT Security Holdings Global Threat Intelligence Report, we address challenges organizations face globally and provide recommendations you may consider in managing cybersecurity risk.

We continue to observe changes in both the scope and scale of infrastructure, network and application targeting, especially related to supply chain operations. From headline news of attacks targeting critical infrastructure to the unfolding cyber events related to geopolitical conflict, the importance of securing the supply-chain and digital society has never been more critical to business and national economies.

Against this backdrop, we analysed that the threats that shaped 2021 from NTT's perspective. Details in this report enable organizations to understand potential threats to their own environment using insights sourced from NTT's unique global network telemetry, managed security services client base, global honeypot network and our dedicated human intelligence.

Through collaboration and innovation, we deliver world-class cybersecurity solutions that protect our clients, society and the global community. I encourage cybersecurity leaders and defenders to utilize the insights shared here to make informed decisions in how to enhance your security posture.

Kazu Yozawa *CEO, Security Service division, NTT*

Kazu has over 40 years of experience in the ICT industry, with 12 years in managed security services. He was appointed Chief Executive Officer of NTT Security in April 2021. Before he was appointed CEO, Kazu held the position of CTO for NTT's broader cybersecurity team in Global R&D for Managed Security Services and CEO of NTT Security Japan.

This year's report contains global attack data collected and analyzed from January 1, 2021, to December 31, 2021.

Analysis is based on log, even, attack, incident and vulnerability data from:

1500 enterprise customers

7 R&D centers around the world

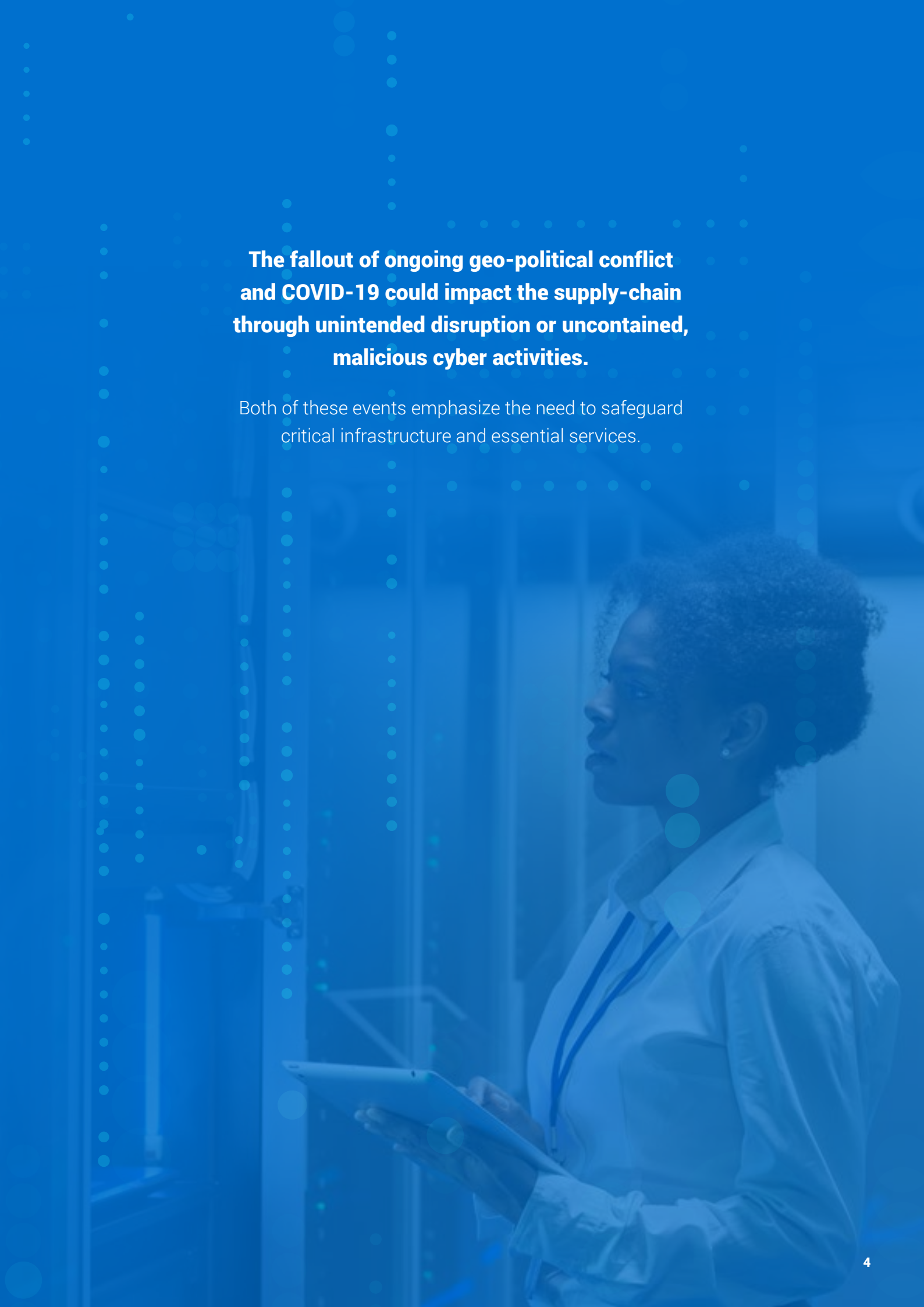
20 years experience in 24/7 Managed Security Services

800 billion + logs processed per month

Global Internet backbone telemetry and honeypot sensors

The fallout of ongoing geo-political conflict and COVID-19 could impact the supply-chain through unintended disruption or uncontained, malicious cyber activities.

Both of these events emphasize the need to safeguard critical infrastructure and essential services.



Key findings

As the threat environment shifted in 2021 and continue to play out in 2022, organizations must continue to adapt in order to effectively manage their security posture.

Global key findings

2021 gave rise to five significant trends across the global threat landscape.

1. Attacks shift to critical infrastructure and supply chains.

COVID-19 and digital transformation caused a shift across the threat landscape. More recently, geo-political tensions and ongoing supply chain disruption have affected industry targeting. **Attacks more than doubled in the technology, telecommunications, and transport and distribution sectors.** Technology and telecommunications attacks increased because of greater reliance on digital environments and shift to remote working. Noticeably, these attacks also increasingly affected critical infrastructure, targeting technology, transport, and manufacturing.

2x

Industry targeting attacks **more than doubled** in the technology sector. Attacks also doubled in both telecommunications and transport and distribution.

Technology was the most targeted industry with **21%** of all attacks.

Manufacturing was the 3rd most targeted industry at **14%**.

Transport and distribution moved into the **top 5** most targeted industries for the first time.

Finance (17%) and **education** (11%) sectors continued to experience significant attacks throughout 2021 as the 2nd and 4th most targeted industries.

2. Cloud migration is shaping global attacks.

Migration to cloud environments helped mitigate attacks targeting platforms and network services. Over the past few years, these attacks dropped as cloud providers strengthened their infrastructure and security platform-enabled services. Supported applications, however, continue to be under control of the client organization. **Our analysis indicates the percent of web-application (42%) and application-specific (30%) attacks continues to rise.** These two attack types accounted for 72% of all attacks (32% in 2018, 55% in 2019, and 67% in 2020).

Web application (42%) and **application-specific** (30%) attacks combine to account for 72% of all attacks. The percentage of these attacks increased in four of the top five industries.

2018	2019	2020	2021
32%	55%	67%	↑ **72%**

35% **Apache products** were the most commonly attacked technology globally, targeted in 35% of all attacks.

8% **ThinkPHP** a popular content management system, was the second most targeted application (down from 30%).

Increasing **software application attacks** as organizations rapidly migrate data and applications into cloudbased environments.

Digital acceleration, **time to market** and **agile service development** result in more frequent application development cycles – often without security in mind.

3. Diversifying target scope and attack intensity.

NTT observed about a 30% increase in hostile activity targeting clients, led by attacks against applications and network infrastructure, along with denial of service and brute-force attacks. **Attack volumes increased for 7 of the top 10 most targeted industries** with web-application attacks and application-specific attacks up in most industries and nearly every geographic region. The relative rate of attacks targeting all top three industries dropped, indicating more industries experienced sustained elevated levels of hostile activity.

30%

NTT observed a 30%+ increase in hostile activity targeting clients led by **application** and **network infrastructure**, along with **denial of service** and **brute force attacks**.

Hostile activity predominantly comprised of **web-application** and **application-specific attacks** (72%).

21,957

Vulnerability disclosures in 2021 was the highest ever.

24 minutes

On average, a **new vulnerability** was registered **every 24 minutes** in 2021.

Although the recent **Log4j vulnerabilities** were not disclosed until late December 2020, Log4j became the **8th most targeted technology** for the entire year, and the **most targeted that month**.

	2018	2019	2020	2021
Top 3 Industries	46%	51%	62%	↓ **51%**
Top 5 Industries	65%	69%	78%	↓ **72%**

Total attacks targeting the top 3 industries decreased, meaning **threat actors are diversifying scope of targets** by refocusing **hostile attacks** directed at other industries and organizations.

4. Trojan deployments soar as botnets re-emerge.

Trojans accounted for 65% of malware in 2021, up from 35% in 2020. Trojans were five of the top 10 most common malware globally, five of the top 10 in every region, and five of the top 10 in almost every industry. **Overall, we observed a 50% increase in detected malware led by Trojans and botnets during 2021.** Increased use of banking Trojans indicates a rise in cybercriminal activity, while increased use of other Trojans suggests a rise in espionage and theft of trade secrets. This indicates attackers' desire to increase control over an environment by maintaining long-term persistence.

50%

NTT observed a **50% increase in malware** year on year led by **trojans** and **botnets** during 2021.

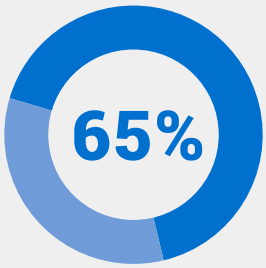
Trojans made up 5 of the top 10:

most common malware globally

malware in **every region**

in almost **every industry** analyzed

Trojans accounted for **65% of malware** in 2021, up from **35%** a year earlier, followed by **botnets** (**11%**).



Trojans also accounted for at least **60%** of all **malware detections** in **every industry** analyzed excluding education (49%)

Ursnif was the most detected malware globally (**20%**), followed by **Ramnit** (**13%**), and the resurgence of **Emotet** (**9%**) and **Trickbot** (**6%**) banking trojans.

Cryptocurrency miners dropped significantly to 6% down from 41% a year ago.

Ursnif is a common banking Trojan also known as **Gozi**. It steals sensitive information, including computer and network details, user credentials and other internal information. Attackers also use Ursnif to install additional malware components.

Emotet was taken offline by a collaborative and coordinated effort involving multiple countries, law enforcement and judicial authorities coordinated by **Europol** and **Eurojust** in Jan 2021.

The botnet resurfaced in November continuing to provide malware-as-a-service to cybercriminal groups who rent access to infected systems for further malware propagation including **Trickbot**, **Qakbot**, and **Ryuk** malware deployments.

5. Ransomware prevalence impacting business continuity.

24% of all incident response engagements with NTT's Digital Forensics and Incident Response team in 2021 were related to ransomware – a 240% growth from 7% in 2019. Such activity indicates organizations are increasingly challenged defending and responding to ransomware incidents. **The most common method attackers use to infect organizations is via email containing malicious links or attachments.** Average ransom demands are up, payouts are up, and the total cost of ransomware for 2021 is expected to near USD 20 billion.

240%

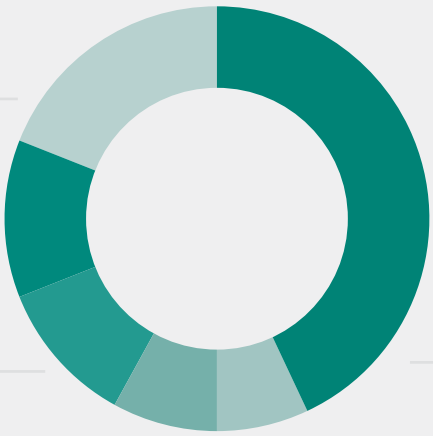
NTT observed a **240% engagements by industry growth** in ransomware incident response engagements over the past 24 months.

24%

Incident response engagements were related to **ransomware**.

Most common method of **ransomware** infection via **emails** with embedded **malicious links** or **attachments**.

Engagements by industry



19% Retail

12% Manufacturing

11% Insurance

8% Technology

43% All others

7% Healthcare

Spotlight on: Russia-Ukraine conflict

Similar to the impact COVID-19 had on the cybersecurity domain over the past two years, the **Russian invasion of Ukraine** may also have a lasting impact on **cyber and information security domains**.

In light of recent events, the NTT GTIC analyzed relevant issues in the conflict between Ukraine and Russia. We looked at some of the potential effects of cyber operations and the potential for spillover into NATO countries globally.

NTT Security Holdings has been tracking infrastructure associated with the Gamaredon APT actors, which have been actively targeting Ukrainian government organizations and officials. Utilizing NTT's unique network visibility, GTIC identified actor-controlled nodes used to manage Gamaredon infrastructure. Multiple compromises were identified inside Ukraine during the early weeks of the conflict as well as communications to regions within EMEA. This visibility allows us to automatically detect changes to the threat infrastructure as it is updated and push new indicators to NTT's SamurAI XDR platform.

The Russian-Ukraine conflict brought economic sanctions, physical operations, and cyber operations targeting critical infrastructure, financial institutions and oil and gas organizations. Businesses and industries and, therefore, the entire supply chain is being affected due to tight relationships in global economies and could easily be crippled.

The physical invasion of Ukraine began on 24 February 2022; cyber operations began much earlier.

Observed threats

- Ransomware
- Malware
- Data wipers
- DDoS
- Vulnerabilities
- Credential compromise
- Compromised systems
- Phishing
- Smishing
- Defacement
- Deep fakes
- Disclosures
- Disinformation and influence operations
- Doxing

The invasion was preceded by a series of operations using Whispergate, a data-wiping malware that targeted multiple industries in Ukraine, including government, non-profit, and information technology organizations.

In January 2022, attackers likely aiding Russian strategic objectives defaced nearly 70 Ukrainian government websites. These defacements warned Ukrainians to 'expect the worst.' In mid-February, DDoS attacks targeted Ukraine's armed forces, defense ministry, public radio and the two largest national banks, crippling services for several hours.

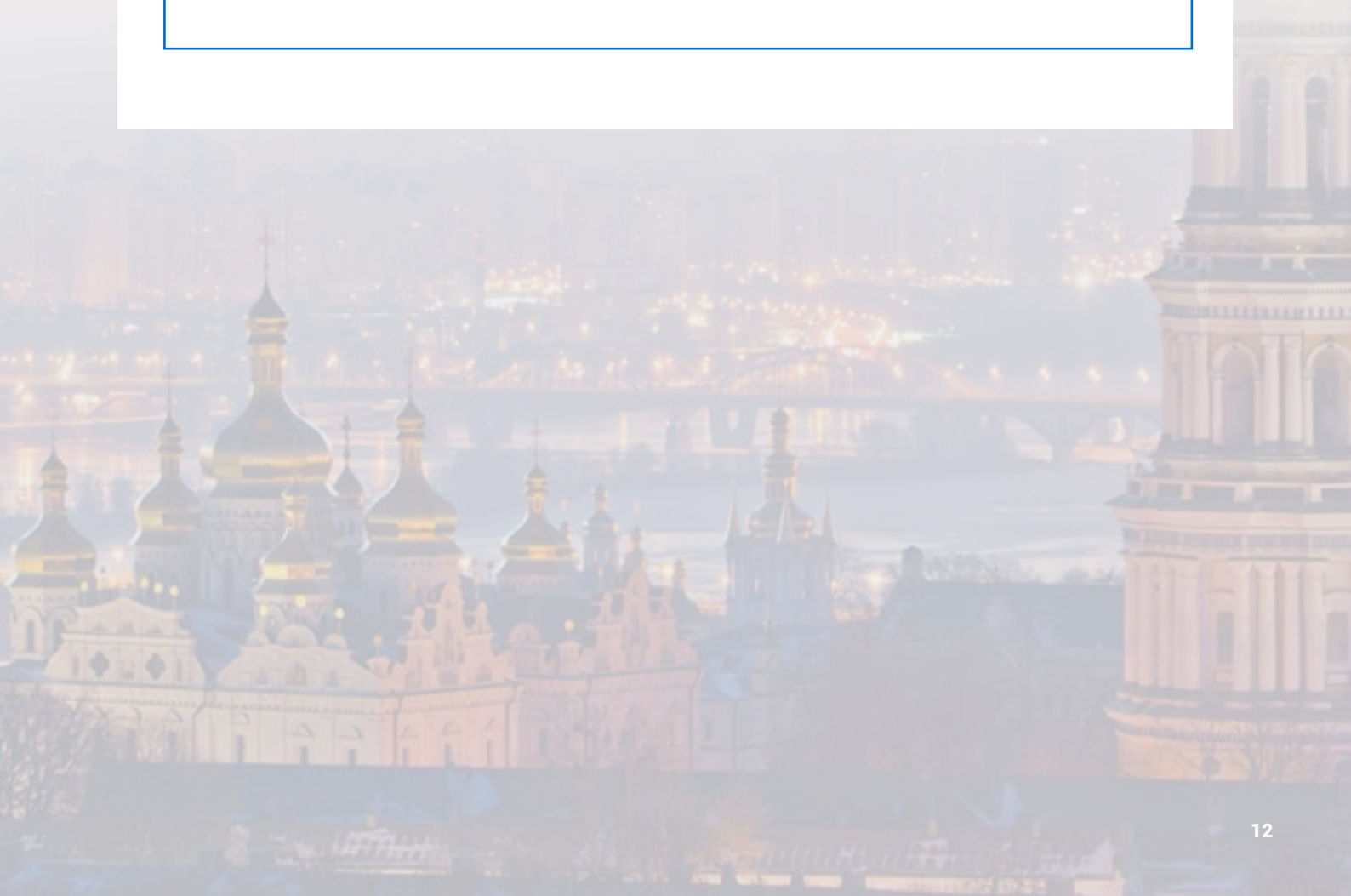
Agencies in the US and UK issued warnings regarding data-wiping malware. They cautioned 'further disruptive cyberattacks against organizations in Ukraine are likely to occur and may unintentionally spill over to organizations in other countries,' meaning any organization in any country could be affected by cyberattacks.

The groundwork may already be laid for additional cyberattacks on targeted networks.

What to expect in the future in 2022 and beyond

This war could set a precedent for how cyber operations will not only be leveraged for offense but will support traditional physical, economic and diplomatic actions, sanctions and outcomes.

We have observed a full range of cyberattacks employed to support conflict during the Russian invasion. Organizations, particularly custodians of critical infrastructure, will need to continue operating under higher levels of vigilance. Ongoing disruptive cyber activity is to be expected and will likely target high-value assets and those of assets of strategic importance – nationally and economically. The key will be in learning from such attacks in order to improve cyber readiness and resilience.



Similar to the impact COVID-19 had on the cybersecurity domain over the past two years, the Russian invasion of Ukraine may also have a lasting impact on cyber and information security domains.

In fact, evidence suggests hybrid warfare leveraging both integrated cyber and other traditional domains.

Global analysis

Regardless of industries, regions and targeted technologies, the volume of web-application and application-specific attacks has continued to increase annually.

Global analysis

In 2021, we saw the greatest number of newly discovered vulnerabilities compared to any previous year. This increase emphasizes how much attention researchers and attackers dedicate to discovering new targets and methods. This shift included two dominant evolutions in malware:

1. Ransomware continued evolving and is one of the greatest cyberthreats an organization may face.
2. A surge in Trojans and botnet activity demonstrates attackers are seeking longer-term strategic objectives.

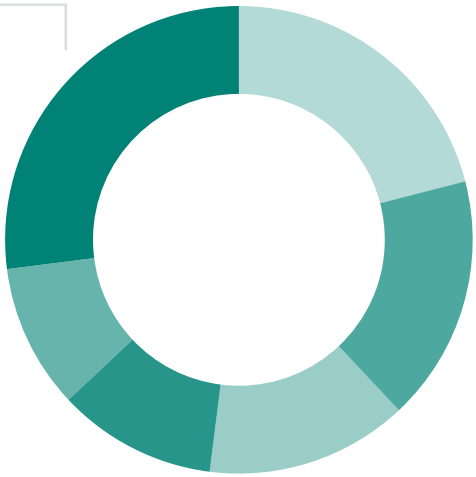
Top global attack targets and types

21% Technology

Percent of attack types
40% Web-application
25% Application-specific
15% Network manipulation

17% Finance

Percent of attack types
38% Application-specific
24% Web-application
22% Reconnaissance



10% Transport & Distribution

Percent of attack types
38% Web-application
20% Application-specific
20% Reconnaissance

14% Manufacturing

Percent of attack types
51% Web-application
31% Application-specific
9% Reconnaissance

11% Education

Percent of attack types
50% Web-application
30% Application-specific
14% Reconnaissance

Comparison of most attacked industries

Industry	2019	2020	2021
↑ **Technology**	#1 – 25%	#6 – 6%	#1 – 21%
↓ **Finance**	#2 – 15%	#1 – 23%	#2 – 17%
↓ **Manufacturing**	#5 – 7%	#2 – 22%	#3 – 14%
↑ **Education**	#4 – 10%	#5 – 6%	#4 – 11%
↑ **Transport & Distribution**	#11 – 1%	#11 – 2%	#5 – 10%

Percent of attacks on the top three industries

2019	2020	2021
51%	62%	51%

Global attack types

- **42%** Web Application
- **4%** DoS / DDoS
- **30%** Application Specific
- **3%** Brute Forcing
- **13%** Reconnaissance
- **6%** Network Manipulation

Global targeted technology

Target application or technology	Percent of attacks 2021
Apache products	35%
ThinkPHP	8%
Microsoft products	7%
Realtek	5%
PHPUnit	5%

Specific malware

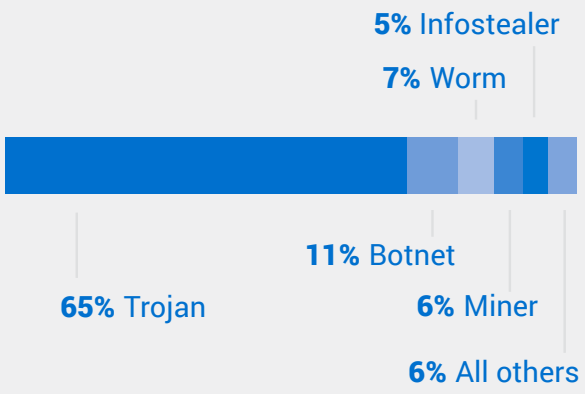
Malware	Malware family	Percent of malware
Ursnif	Banking Trojan	20%
Ramnit	Trojan	13%
Emotet	Banking Trojan	9%
Trickbot	Banking Trojan	6%
Conficker	Worm	5%

Top 10 specific malware

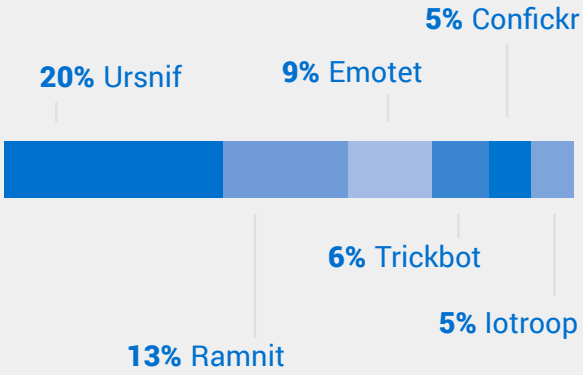
	Global	Americas	EMEA	APAC	Japan
1	Ursnif	Ramnit	Cryptominer	Ursnif	Ursnif
2	Ramnit	Xmrig	Emotet	Conficker	Conficker
3	Emotet	Emotet	Trickbot	Mariposa	Mariposa
4	Trickbot	Icedid	Bottle	Njrat	Njrat
5	Conficker	Trickbot	Remcos	Trickbot	Iotroop
6	Iotroop	Wannacry	Staser	Iotroop	Emotet
7	Njrat	Razy	Coinmine	Emotet	Trickbot
8	Mariposa	Andromeda	Fallout	Andromeda	Andromeda
9	Cryptominer	Njrat	Njrat	Zeus	Crosswalk
10	Formbook	Conficker	Xmrig	Crosswalk	Vobfus

Trojan | Miner | Botnet | Worm | Ransomware | ExploitKit | Infostealer

Global malware families



Global malware variants



Increased usage of **trojan deployment** indicates a change in adversarial preference with the intention for greater target victim control and objective for long-term persistence.

Regional highlights

Many attacks followed global trends, regardless of their region or industry. However, there were also some notable differences between regional experiences.

Americas

- Technology was the most attacked industry.
- Organizations in the Americas experienced DoS/DDoS and network manipulation attacks at a rate **twice the global average**.
- Even though technology in the Americas experienced increased web-application and application-specific attacks, **the region experienced the lowest rate of such attacks of any region**.
- ThinkPHP was the only technology in America's top five most targeted technologies in both 2020 and 2021.
- The most targeted technology in the Americas was Realtek products and there were enough attacks that it helped push the technology into the top five most attacked technology globally.

EMEA

- Finance was the most attacked industry and had the highest rate of attacks of any region.
- The only region to observe coin miners in their top 10 malware, and the **only region that did not have Trojans as the most commonly detected malware**. EMEA showed three coin miners in their top 10 most common malware.
- The only region to observe detections of exploit kits in their top 10 malware. EMEA showed two exploit kits (Bottle 7% and Fallout 2%) in their top 10 most common malware.
- Experienced the **highest amount of web-application and application-specific attacks** of any region.
- Experienced more targeting of Microsoft products than any other region.

APAC

- Experienced the largest increase in web-application and application-specific attacks.
- For the third consecutive year, **APAC experienced more botnet detections than any other region**.
- Detected more activity from worms than any other region.
- The volume of attacks targeting the transport and distribution industry in APAC helped push the industry into the top five industries for the first time.
- APAC was the **only region to observe attacks targeting Oracle products** at the top of their targeted technology.
- APAC was the only region to observe enough attacks targeting Log4j that the technology was in their top 10 most targeted technologies.

Global attack highlights

The top industries targeted in 2021 were:

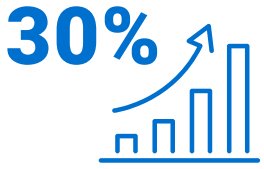
21% Technology

17% Finance

14% Manufacturing

11% Education

10% Transport & Distribution



Total attack volume targeting clients increased by about **30%** over levels from 2020.

21,957

Researchers published a record **21,957** new vulnerabilities in 2021 – an average of a new vulnerability **every 24 minutes** in the year.

Attack volumes increased in **seven of the top 10 industries**, increased in the most attacked technologies for every region and nearly every industry analyzed.

Log4j was discovered with only 23 days left in 2021, yet in that time, it became the **single most attacked technology** in December – and the eighth-most attacked technology for the entire year.

Attacks targeting the **technology industry** more than doubled from 2020 to 2021, leading technology to become the **most attacked industry**, accounting for **21%** of all attacks.

The single largest change in the top five most targeted industries was the addition of **transport and distribution**, which climbed from out of the top 10 to be the **fifth most attacked** industry of 2021.

DoS/DDoS and **network manipulation** attacks targeting the technology industry were both well above the global average.

Web-application and **application-specific attacks** combined to account for **72%** of all attacks in 2021.

	2018	2019	2020	2021
Web-application and application-specific attacks	32%	55%	67%	↑ **72%**

The shift to **cloud computing** has fundamentally changed the way organizations and their web infrastructure are supported. In most cases, moving to the cloud means an organization's **biggest potential target** for attackers are the external-facing applications the organization manages.

Malware highlights

50%

Overall **malware activity** in 2021 increased by **nearly 50%** over levels from 2020.

65%

Some form of **Trojan** accounted for **65% of all malware** in 2021, up from 35% in 2020.

While **ransomware disruption** became one of the most significant cyber threats to business continuity an organization may face, **Trojans** and **botnets** dominated observed **malware volume**.

Spotlight on: Threats in software supply chain

Researchers and analysts reported several major software supply-chain attacks in 2020 and 2021. We categorize past attack cases into two types based on how the threats were directed against the software supply chain:

- **Incorporated Threats:** attacks that exploit originally built-in vulnerabilities
- **Insertion Threats:** attacks created by intentionally implementing malicious artifacts into software

In July 2021, the European Union Agency for Cybersecurity (ENISA) released a report on confirmed supply-chain attacks in the European Union (EU) . In the report, ENISA defined a supply-chain attack as a combination of at least two attacks targeting both supplier and customer. It distinguishes between common attacks exploiting certain software vulnerabilities and compromising only a client (i.e., end-user). According to this classification, an attack compromising just an end-user client is not a software supply-chain attack.[1]

Incorporated Threats

This type of threat stems from security flaws in software code or misconfigured settings allowing unintended manipulation by the adversary. These threats can be a starting point from which attackers can exploit both suppliers and clients.

Vulnerability

Kaseya is a supplier of software services and tools for remote IT monitoring and management. The organization's main clients are Managed Service Providers (MSPs) who use on-premise software or cloud services. The MSPs, in turn, supply IT management services to their clients. In July 2021, attackers compromised Kaseya's Virtual System/Server Administrator (VSA) servers by exploiting a zero-day vulnerability (CVE-2021-30116) to bypass authentication and run arbitrary commands.[2] After compromising Kaseya, the attackers undermined the MSPs by executing commands to deploy malware through remote software updates on their VSA instances. The malware then deployed ransomware to clients being managed by the MSPs. In total, Kaseya disclosed under 60 clients employing on-premise servers, but the attacks compromised an additional 1,500 MSP clients.

Misconfiguration

Codecov is an organization that provides a tool that analyses and visualizes test coverage rates for code development. In this case, the attackers exploited a configuration vulnerability in Codecov's Docker image and obtained valid access credentials.[3] After compromising the Docker image, the attackers took over modification rights for the 'Bash Uploader script' used by Codecov clients. By making the clients download and execute the script, the attackers could steal client credentials. These credentials allowed the attackers to access client services, databases and application code.

Insertion Threats

Insertion threats are caused by attackers deliberately inserting malicious code into software for future attacks. The Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) described the three common techniques to deliberately insert malicious code as 'Hijacking updates' and 'Undermining code signing or 'Compromising open-source code.'[4]

Hijacking Updates and Undermining Code Signing

In December 2020, the security organization FireEye reported it had been compromised through a supply-chain attack.[5] A follow-on report from software provider SolarWinds acknowledged hackers broke into the organization and distributed malware-contaminated updates via its Orion IT monitoring and management software to distribute a backdoor dubbed 'SUNBURST.'[6] FireEye reportedly used the software and was compromised in the attack. SolarWinds reported up to 18,000 clients were affected.

Compromising Open-source Code

Although not established as an attack, Bleeping Computer reported in April 2020 that an assistant professor and students from the University of Minnesota (UMN) secretly introduced vulnerabilities into the Linux Kernel project as part of their research activities.[7] In response, the Linux Kernel community banned UMN from the project and reverted all code commits ever submitted from UMN. If this were a real attack, everyone using the source code would have been affected.

What to expect in the future in 2022 and beyond

Supply-chain attacks can cause wide-ranging damages by impacting both suppliers and their clients. Depending upon the popularity of a supplier's compromised product, a successful supply-chain attack can potentially impact tens of thousands of downstream organizations. Both suppliers and their clients must work to increase their overall security posture. Suppliers should be transparent with their clients about the security measures they take. In contrast, clients should employ a zero-trust model, which seeks to minimize the potential for any damages from a potential supply-chain compromise.

1 https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

2 https://www.kaseya.com/potential-attack-on-kaseya-vsa/

3 https://about.codecov.io/security-update/

4 https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

5 https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html

6 https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm

7 https://www.bleepingcomputer.com/news/security/linux-bans-university-of-minnesota-for-committing-malicious-code/

Attacks more than doubled against technology and telecommunications industries because of greater reliance on digital environments and remote working.

Additionally, attacks also increasingly affected critical infrastructure by targeting technology, transport, and manufacturing.

Industry analysis

Attackers used a wide variety of malware and attacked different technologies. Regardless of industry, all organizations must prepare for supply-chain targeting.

Industry analysis

NTT observed an increase in attack volume targeting nearly every industry. While web-application and application-specific attacks dominated all industries, most other characteristics were industry-specific. Additionally, as the COVID-19 pandemic persisted in 2021, technology enabled organizations across industries to allow for work-from-home arrangements. This increased dependency upon technology and a continuing migration to the cloud led to a larger and more complex attack surface, with employees emerging as the new network edge.

Top 10 specific malware

	Technology	Finance	Manufacturing	Education	Transport and distribution
1	Ursnif	TrickBot	Ursnif	Cryptominer	Ursnif
2	Emotet	Rimecud	Emotet	TrickBot	Vobfus
3	TrickBot	Emotet	Tiggre	Bladabindi	Dridex
4	Crosswalk	Ursnif	njRAT	XMRig	Emotet
5	IoTroop	Andromeda	Zeus	Ursnif	Vidar
6	Kovter	AdLoad	Conficker	Tiggre	China Chopper
7	Vobfus	Qbot	IcedID	PlugX	IoTroop
8	Mimikatz	Valyria	Bottle	Fiesta	TrickBot
9	Floxif	Vobfus	Mimikatz	Locky	Dloader
10	DorkBot	Virut	TrickBot	Emotet	Conficker

Trojan Miner Botnet Worm Ransomware ExploitKit Infostealer Webshell Adware

Top industries targeted annually

	1	2	3	4	5
2012	Finance	Technology	Business & Professional Services	Energy & Utilities	Manufacturing
2013	Finance	Technology	Retail	Business & Professional Services	Healthcare
2014	Finance	Business & Professional Services	Retail	Manufacturing	Healthcare
2015	Retail	Hospitality	Insurance	Government	Manufacturing
2016	Government	Finance	Manufacturing	Retail	Education
2017	Finance	Technology	Business & Professional Services	Manufacturing	Retail
2018	Finance	Technology	Business & Professional Services	Education	Government
2019	Technology	Finance	Government	Education	Manufacturing
2020	Finance	Manufacturing	Healthcare	Business & Professional Services	Education
2021	**Technology**	**Finance**	**Manufacturing**	**Education**	**Transport & Distribution**

Spotlight on: Privacy, governance, risk, and compliance

Each year we look across the landscape reviewing updated regulations or legislation that may affect privacy, governance, risk and compliance.

Throughout 2021, we saw a struggle in the balance between security and freedom, between privacy versus safety. The world wants to protect the private healthcare information of individuals yet wants available information regarding vaccinations and infections. At the same time, the world placed greater stress on financial and retail systems, which have been required to support online transactions with more security and regulatory compliance yet demand greater levels of privacy and protection.

Organizations will need to evaluate their data requirements, determine the impact in their own environments and client base, and assess operational requirements to implement the required measures for compliance.

Regulation	Affected Geography	Effective Date	Affected Industries	Summary
Personal Data Protection Bill	India	Pending	All	India's proposed data protection law, not yet enacted, will include the protection of personal and non-personal data. Along with many other protections, it aims to hold social media organizations liable for content published on their platforms.
Act on Protection of Personal Information	Japan	April 2022	All	This amended act is slated to take effect in April 2022. It will address several data protection requirements, including related to transferring personal data outside Japan, transferring person-related information, and the notification of data security breaches.
Personal Data (Privacy) (Amendment) Ordinance 2021	Hong Kong	October 2021	All	Amends the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) to criminalize doxing and expand enforcement powers.
Personal Information Protection Law	China	August 2021	All	China passed the PIPL to 'protect the rights and interests of personal information, regulate personal information processing activities, and promote the rational use of personal information' and includes strict enforcement of cross-border data transfers. Failure to comply could result in fines of up to 5% of an organization's annual revenue or up to USD 7.7 million, whichever is greater.
Protection of Personal Information Act (POPIA)	Republic of South Africa	July 2021	All	The POPIA grants South Africans new data privacy rights such as the right to access, correct, and erase personal data. Similar to other data privacy laws, it aims to both establish these rights and define data privacy as a protectable asset belonging to the people.

Regulation	Affected Geography	Effective Date	Affected Industries	Summary
GDPR Update	EU and countries doing business with the EU	June 2021	All	European Commission issued new standard contractual clauses for personal data transfers to countries outside the EU.
The Brazilian Data Protection Law (LGPD)	Brazil	September 2020	All	Initially enacted in 2018, fines for non-compliance came into effect in 2021. The Brazilian National Data Protection Authority (ANPD) put together a two-year plan to address various guidelines and regulations, focusing on major leaks and mass distribution of personal data.

During efforts to support the increased digitalization of services, some organizations did not prioritize compliance at the level it deserved. Overall, GDPR fines imposed for non-compliance ranged up to USD 887 million.

GDPR fines surpassed EUR one billion in 2021.
74% of GDPR fines issued since January 2019 have not been collected.

What to expect in the future in 2022 and beyond

These trends will likely continue through 2022, as governments continue to take a more proactive role in security, and GRC and privacy issues are increasingly becoming drivers of growth.

- 2022 will bring substantial changes to AI regulation.
- SEC proposed cybersecurity risk management rules and amendments for registered investment advisers and funds (Feb 2022).
- SEC proposed new cybersecurity mandates for publicly traded companies (Mar 2022).
- US Congress' recently enacted Cyber Incident Reporting for Critical Infrastructure Act (Mar 2022).

While the regulatory landscape is becoming trickier for global organizations to navigate, organizations that take a principled approach to transparency, data ethics, and protection may fare better than those merely checking the compliance checkbox.

Recommendations

As the threat environment shifted in 2021, organizations must continue to adapt in order to manage risk. Organizations who invest in resiliency for all aspects of business operations and proactively understand and prepare for the dynamic cyber threat environment will be more likely to consistently and reliably deliver services securely.

Cyber-resilience, Secure by Design, and Zero-trust

Organizations must prepare for today's threats by securing their supply chains, implementing third-party software and hardware in a zero-trust environment, prioritizing security throughout the design and implementation of a product lifecycle, and creating operational contingency plans for supply-chain disruptions.

Implement and Prioritize Patch Management

Organizations must be ready for increases in attack activity and an ever-shrinking time-to-exploit timeframe. NTT observed almost a 30% increase in all hostile activity targeting clients. Attacks consistently focused on technology with wide customer bases, using a wide variety of significant vulnerabilities.

Perform Continuous Monitoring, Threat Detection and Response

Organizations must improve visibility into attacks targeting cloud, network, and endpoints. Specifically, threat detection and incident response capabilities will minimize the scope and impact of a breach by enabling faster, and more effective response.

Protect your digital landscape with SamurAI XDR – a vendor-agnostic, cloud-native, advanced threat detection and response platform. SamurAI XDR combines, world-class cutting-edge analytics, machine learning, threat intelligence, automation with experienced security analysts to detect and respond to known and unknown threats.

Secure Data at Rest, in Use, and in Transit

Organizations must take steps to secure their data while at rest, in use, and in transit. Ransomware incidents have increased drastically, and numerous ransomware groups also steal data to sell later or demand additional ransoms. Organizations should enhance policies, procedures, and practices by adopting recommendations from frameworks such as NIST CSF, ISO27001, and MITRE ATT&CK.

Frequently Review Business Continuity and Disaster Recover Plans

Organizations must prioritize creating, updating, and consistently re-evaluating their business continuity plans. An evolving and dynamic threat environment necessitates organizations revisit plans if they have them or create ones if they do not.

Security controls

1. Enforce multifactor authentication
2. Privileged account management
3. Password policies
4. Update software
5. Vulnerability scanning
6. Network segmentation
7. Network intrusion prevention
8. Filter network traffic
9. Limit access to resources over the network
10. Disable or remove features or programs
11. Operating system configuration
12. Execution prevention
13. Exploit protection
14. Anti-malware protection
15. Behaviour prevention on endpoint
16. Encrypt sensitive information
17. Protect public-facing applications
18. Data backup
19. Audit
20. User training

Final thoughts

As threats continue to evolve, we are likely to observe the following activity throughout 2022:

- **Ransomware** will continue to evolve and mature as attackers reap substantial financial profits from successful attacks, creating incentives in the market. Additionally, due to increased geopolitical tensions, some ransomware operatives may find safe havens from which to operate, making coordinated law enforcement actions more difficult, if not impossible.
- **Privacy laws** will continue to expand and cover a greater share of the world population, challenging organizations to keep up to date with growing compliance mandates.
- The success of high-profile **supply-chain attacks** in 2021 will inspire copycat threat actors. While most such attacks will not be successful, organizations will need to increase their attention to security throughout the entire supply chain and foster an environment of zero trust.
- As **cryptocurrency** continues to become more mainstream, cryptocurrency exchanges will become a focal point for attacks, both among financially motivated cybercriminals and state- sponsored actors looking to garner funds and bypass sanctions.

With these threats in mind, organizations must remember to remain vigilant and constantly update threat detection and response capabilities. Cyber-resilience must be a key focus area that organizations prioritize in order to achieve their security ambitions to safeguard critical business assets in a digital world.

Global Data Analysis Methodology

1. **NTT Security Holdings** gathers security log, alert, event, and attack information from which it enriches, and analyses 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 **NTT CERT**, a division of **NTT Social Information Laboratories**.
4. Collaboration and expert insight from our intelligence alliance with the **Cyber Threat Alliance** and **National Cyber Forensics and Training Alliance**.

Need cybersecurity support?

Get in touch with NTT today for a security consulting engagement. We'll help you to understand your current risk-profile in order to chart your future security strategy. Or, if you're ready to work with a partner to manage, monitor and optimize your current security platform, reach out to us and one of our Managed Security Services experts will be in touch.

Global Threat Intelligence Centre

NTT Security Holdings, Global Threat Intelligence Centre (GTIC) protects, informs and educates NTT Security clients.

The GTIC 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 to prevent, detect, and respond to cyber threats.

NTT-CERT

NTT-CERT, a division of NTT Social Information Laboratories, serves as a trusted point of contact for Computer Security Incident Response Team (CSIRT) specialists and provides full range CSIRT services within NTT. NTT-CERT contributes to the improvement of information-systems security for the NTT Group as well as for the information network community in general.

To learn more about NTT-CERT, please visit **www.ntt-cert.org**.

Together, we secure the connected future

security.ntt