2024 Global Threat Intelligence Report

Growing attack surface and threat complexity mixed with reduced staffing and budgets is creating a perfect storm for security professionals

NTT | Security Holdings

Global Scalable Security Solutions

security.ntt

Forward from Gregory Garten

CTO, NTT SECURITY HOLDINGS

While the threat landscape continues to evolve at an unprecedented rate, security budgets and staffing remain stagnant or have begun to shrink. This leaves organizations exposed and struggling to defend against even routine exploitation, malware, and ransom or extortion threats.

The problem becomes significantly more severe when considering the increased reliance on cloud security, third-party integration and supply chains, and the added exposure they bring with them. Nearly 50% of organizations in 2023 had numerous severe incidents and 55% have said the severity of incidents is increasing over the past 2 years.

With this imbalance between threats and the funding to combat them, security teams are being asked to do more with less. Teams need to find ways to strike the right balance between spending on tools and people, and analysts need a holistic view of their organization's security posture to enable more informed and quicker decision-making. Embracing consolidation is not just an option, but a necessity to navigate the increasingly complex threat landscape with limited resources. We need to democratize cybersecurity, empowering small and medium sized businesses to achieve the same level of detection and response that has historically been limited to large organizations with bigger budgets.

In our 2024 Global Threat Intelligence Report, NTT Security Holdings provides insights into the security trends our customers are seeing as well as the threat landscape overall. NTT Security Holdings provides unified visibility and control across network, endpoint, cloud, identity, email and more. We encourage organizations to empower your teams with the insights from this report to identify risks and ensure a robust response plan is in place. Investing in the right tools can enable organizations to weather the storm and emerge stronger.

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 international technology startups and multinational technology companies.

This year's report contains analysis based on attack and incident reports, vulnerability trends and threat intelligence from January 1, 2023, to December 31, 2023.

NTT Global Threat Intelligence Platform

Insights from our Samurai MDR & Samurai XDR customer base

800B+

logs processed per month

20+

years experience in 24/7 Managed Security Services

Global Tier 1 Internet backbone telemetry and honeypot sensors

Key findings

In our 2023 Global Threat Intelligence Report, we highlighted the increase in cyber bleed over – with cyberthreats having greater and greater impact on day-to-day life, economic conditions, and privacy. This continues to be the reality in 2024 with actors resorting to even more aggressive and unscrupulous tactics to achieve their objectives. Cybersecurity professionals are lagging at the same time, often stressed to keep pace with more responsibilities and job complexity. We've long discussed the skills gap in cybersecurity, and that gap grows every year as we see rising fatigue and burnout from professionals become increasingly more reliant on an expanding toolset that has become borderline unmanageable. This leads to analysts and administrators missing key details or failing to follow-up efficiently, opening the door to more severe incidents.

Our key findings this year focus on:

1. Top Attacked Sectors
2. Ransomware Telemetry
3. Malware Telemetry
4. Vulnerability Intelligence
5. Exploitation Insights

We all want to strive to be on the bleeding edge of cybersecurity, yet many teams and organizations are still struggling to keep the basics fresh. Cybersecurity professionals need to find ways to consolidate tools, streamline and automate processes, and establish key performance indicators that help reflect the true value information security programs provide an organization. We'll provide some recommendations at the end of the report which we believe will help, especially for smaller teams that are struggling to stay above water.

1 Top Attacked Sectors

While a lot changed across the threat landscape in 2023, the Global Threat Intelligence Center (GTIC) saw less shuffle in the most attacked sectors across our Samurai platform. Manufacturing, technology, and transportation & distribution sectors maintained their positions in the top 5, as we see a continued focus from adversaries on targeting critical infrastructure and supply chains, posing substantial risks. Manufacturing moved into the top slot as we observed a surge in attacks against entities manufacturing components for the energy and mining industries, as well as construction. Technology dipped to #2 but still made up over 20% of the attacks observed, in particular targeting technology and service providers. Finance, a prime target for financially motivated threat actors, regained its spot in the top 5 after a small dip last year. Financial service companies had been in our top 3 for the prior 5 years before a small decrease in attacks saw them drop to #6 last year.

25.66%
MANUFACTURING

7.94%
PUBLIC

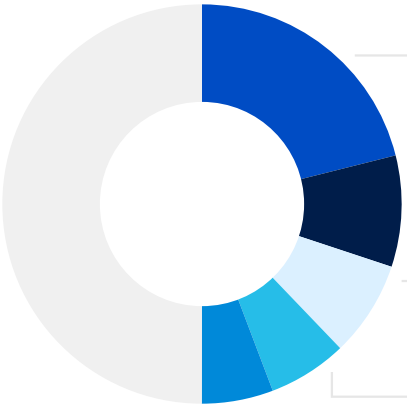
10.20%
TRANSPORT & DISTRIBUTION

21.42%
TECHNOLOGY

10.84%
FINANCE

2 Ransomware Telemetry

As anticipated after a down year in 2022, ransomware and extortion incidents surged quickly. In 2023, there was a rise in both victims and payments, with more than 5,000 victims being posted across multiple channels, up from approximately 3,000 in 2022. It is worth noting these are only those discovered by NTT Security Holdings and reported or disclosed on operator sites. These numbers do not capture incidents where a ransom was paid before it was made public, so the actual number of incidents should be assumed to be notably higher.



21.09% LOCKBIT

9.01% ALPHV (BLACKCAT)

7.75% CL0P

6.40% PLAY

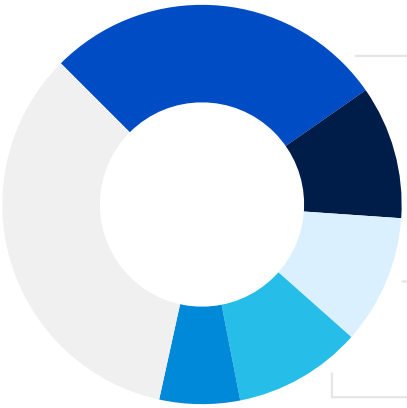
5.79% 8BASE

United States and Manufacturing companies top the charts. Both had the most victims posted, with each leading the way in their respective area every year since we began tracking in 2020.

Top targeted sectors can largely be categorized as organizations that need near perfect uptime, increasing the probability of negotiating a ransom.

Lockbit claimed the most victims for the second year in a row after ramping up into the top 3 in 2021.

GTIC continues to see small and medium-sized businesses (SMBs) face significant risk, with over 50% of victims we tracked having less than 200 employees and two thirds having less than 500 employees.



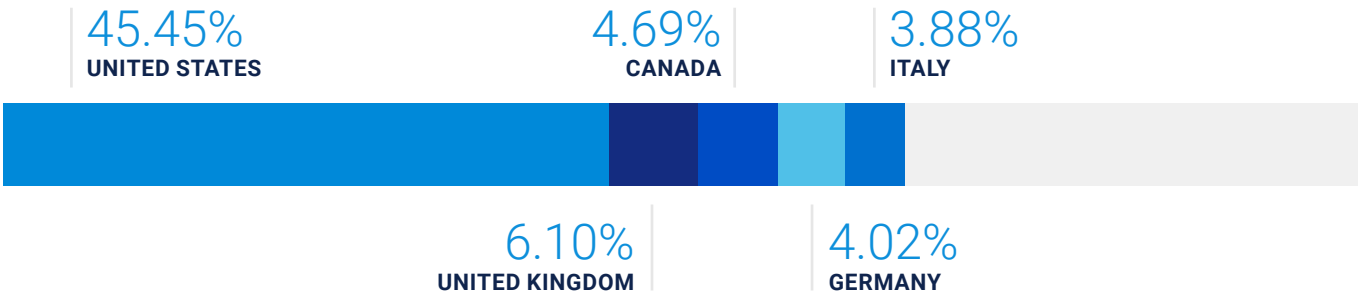
27.75% MANUFACTURING

10.78% TECHNOLOGY

10.44% FINANCE

10.36% RETAIL

6.50% HEALTHCARE



45.45% UNITED STATES

4.69% CANADA

3.88% ITALY

6.10% UNITED KINGDOM

4.02% GERMANY

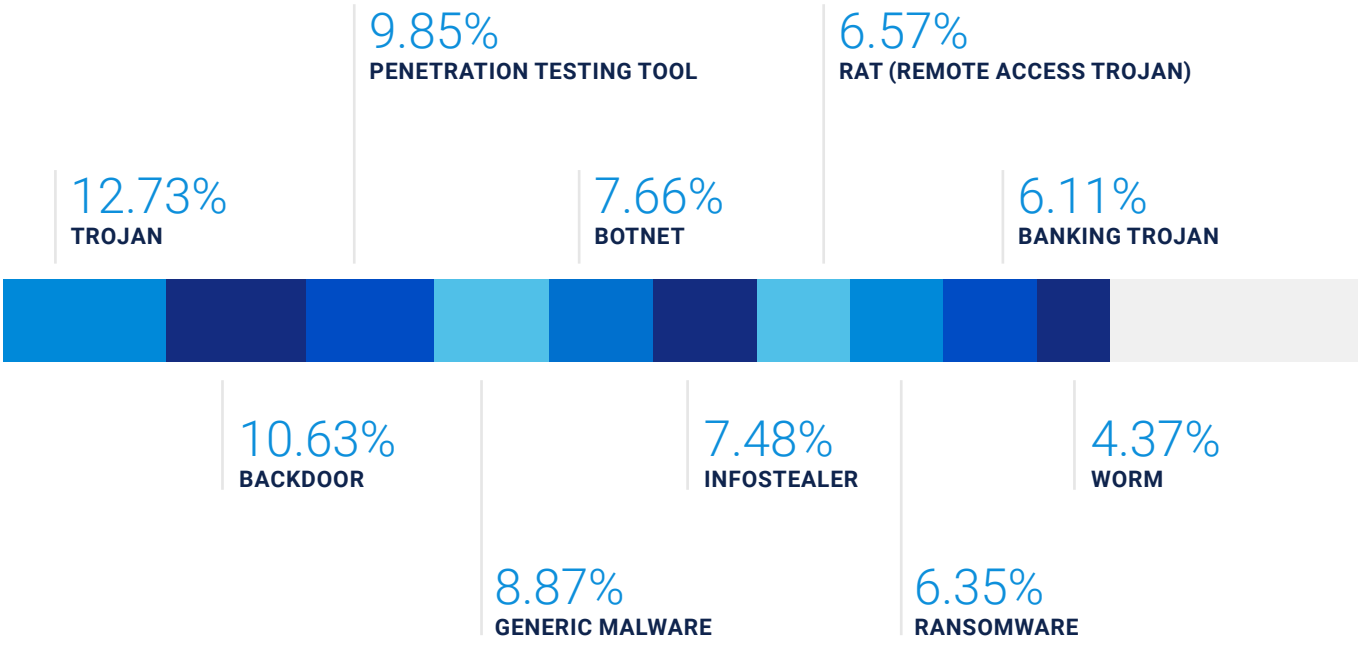
These statistics are based on GTIC research and MDR/XDR detections, as well as a collection of listings on extortion sites, social media (e.g., Telegram) channels and public reporting and disclosures.

3 Malware Telemetry

Malware continues to evolve to gain initial access, evade detection, and maintain persistence. To account for the modularization, we have updated our taxonomy to account for the distribution of these capabilities and delivery stages. This provides a more detailed breakdown of malicious files our Samurai customers are seeing than we have previously reported.

We see a steep drop from banking trojans this year with the new breakout due to better classifying certain malware behaviors more accurately. Trojans continue to be a major factor, with Agent Tesla and Remcos being detected most frequently. The breakdown also resulted in an increase in infostealers identification, such as RedLine and Lumma, to account for when it isn't limited to banking sites and financial data. We introduced a new class for malicious detections of penetration testing tools, for example Cobalt Strike and Metasploit. Generic malware accounts for artificial intelligence and heuristic detections where a more specific classification isn't available. Rounding out the top 5 is botnet activity, primarily lead by Androxgh0st and Mirai. In 2023, ransomware detections decreased, with numerous operators shifting away from the traditional encryption and ransom strategy, focusing instead on faster data exfiltration for extortion purposes.

The modularization of malware, and the increase in adversaries living off the land, highlights the need for organizations to have more comprehensive protections in place. Teams must be prepared to defend against and hunt for the behaviors and tactics, techniques, and procedures (TTPs) of malware as opposed to just known malicious hashes and artifacts.



4 Vulnerability Intelligence

Patch management is a simple concept at its core, however there can be quite a bit of nuance that is often overlooked. A small gap in the process can leave your attack surface and organization exposed. As the saying goes – we must be right every time, whereas attackers must only be right once.

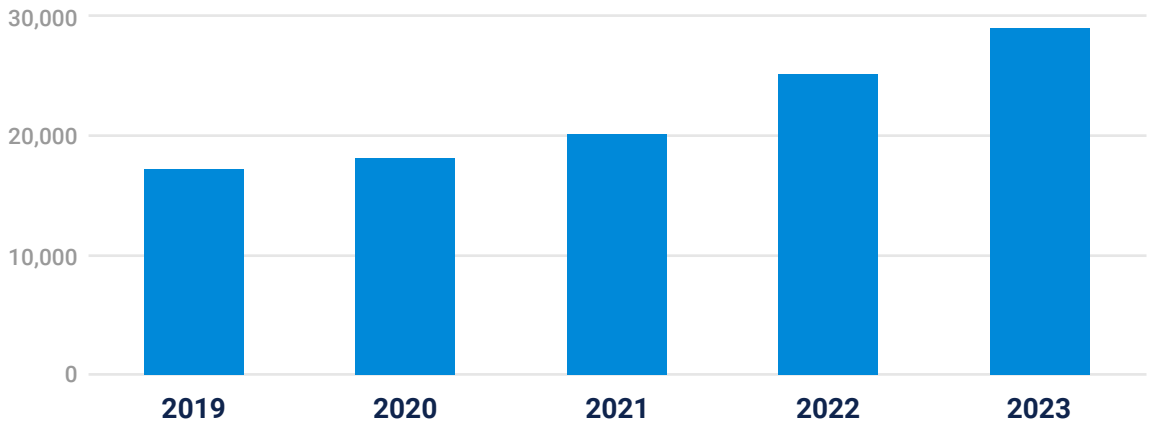
Common pitfalls we see include:

- Improper asset discovery and management, both internally and externally
- Maintaining up-to-date inventory
- Establishing and enforcing software and version restrictions
- Patch prioritization and testing
- Incomplete assessment of supply chain

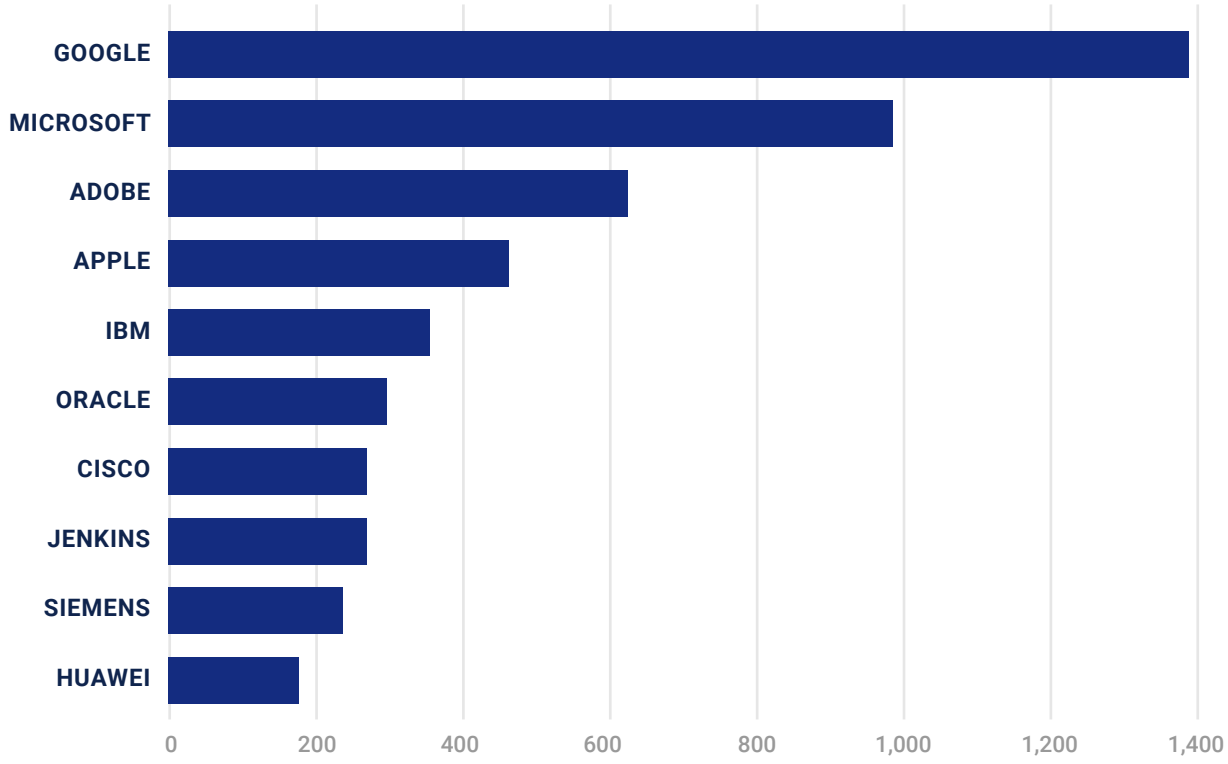
Vulnerability intelligence is an important aspect of threat intelligence that can provide key data points to help protect your business. It can help guide policy and enforcement decisions on authorized software or hardware, help establish data driven risk metrics, and assist with prioritization in patch management. While Common Vulnerabilities and Exposures (CVEs) aren't a definitive listing of every known weakness, it provides valuable contribution to vulnerability management programs, particularly when contextualized further for your environment and based on known exploited vulnerabilities. With over 8,500 unique products being assigned a CVE last year, it is safe to say this is an area businesses must keep close tabs on to protect themselves.

Organizations should leverage these insights to assess vendors and limit what is allowed within their environments – especially with increasing adoption of hybrid and remote working situations. Many of the most popular vendors by market share and reputation are also among the highest in announced CVEs each year, as well as vulnerabilities added to the CISA's Known Exploited Vulnerabilities Catalog. Popular vendors, software-as-a-Service (SaaS) and remote management tools are key targets for adversaries looking to maximize victim count with exploitation.

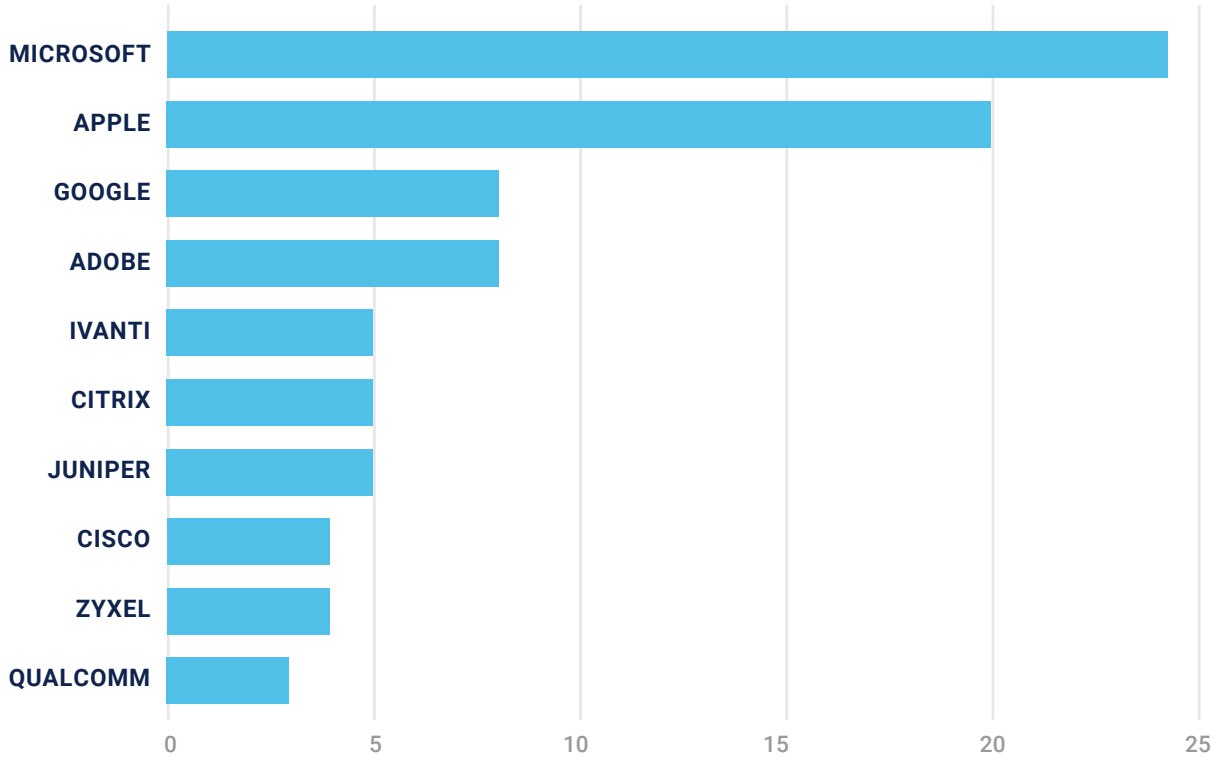
CVEs by Year



2023 CVEs by Vendor



2023 Known Exploited Vulnerabilities by Vendor



5 Exploitation Insights

We highlighted last year that malware and botnets continue to integrate exploit code for high and critical severity vulnerabilities quickly, increasingly so when aided by generative AI. GTIC also observed several threat actors utilize critical severity 0days for massive gains in 2023. This trends with the vulnerability releases above with the majority of targeted platforms aligning to vendors with the highest volume of CVEs acknowledged or vendors with the highest market share. Of these 10 CVEs, 9 appear in the Known Exploited Vulnerabilities Catalog which reiterates the importance of leveraging insights such as this to inform patch management programs. This is true for vital software and systems such as email or firewalls, but also needs to account for IT service management and SaaS integrations.

Most critical CVEs leveraged by ransomware operators in 2023

CVE ID	CVSS	Vulnerability Name	Actor(s)
CVE-2023-27350	9.8	PaperCut MF/NG Improper Access Control Vulnerability	CIOp, Bl00Dy
CVE-2023-34362	9.8	Progress MOVEit Transfer SQL Injection Vulnerability	CIOp
CVE-2023-47246	9.8	SysAid Server Path Traversal Vulnerability	CIOp
CVE-2023-20269	9.1	Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability	LockBit, Akira
CVE-2023-28252	7.8	Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability	Nokoyawa

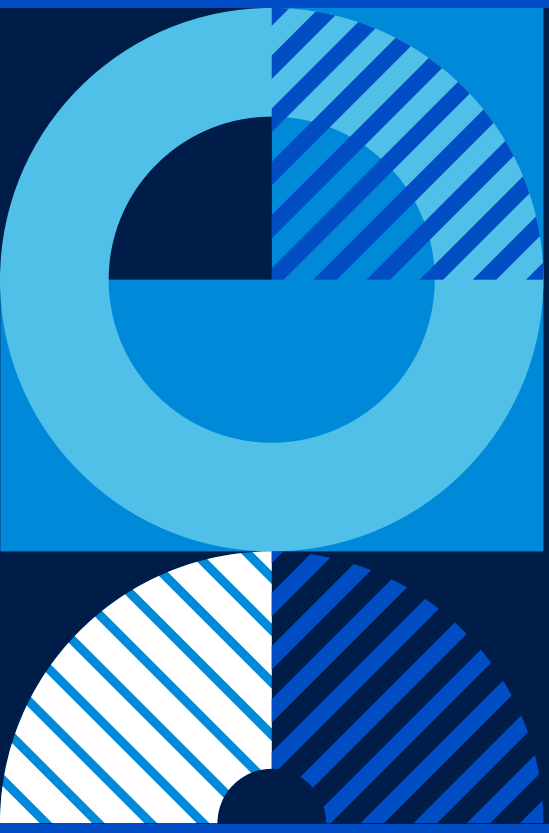
Most critical CVEs leveraged by malware & botnets targeting our Samurai customers in 2023, by percentage of attacks

CVE ID	CVSS	Vulnerability Name	Percentage
CVE-2022-41040	8.8	Microsoft Exchange Server Server-Side Request Forgery Vulnerability	16.25%
CVE-2014-6271	9.8	GNU Bourne-Again Shell (Bash) Arbitrary Code Execution Vulnerability	13.72%
CVE-2021-44228	10	Apache Log4j2 Remote Code Execution Vulnerability	10.95%
CVE-2023-25725	9.1	HAProxy Empty Header Name Access Control Bypass	3.60%
CVE-2021-34473	9.1	Microsoft Exchange Server Remote Code Execution Vulnerability	2.87%

Spotlight On: Billion Dollar Industry

According to a report from Chainalysis, ransomware payments in 2023 reached an all-time high of over $1 billion after a decline in 2022. Despite increasing competition from new operators and affiliates as well as law enforcement disruption efforts, ransomware payments are climbing, highlighting the profitability of this criminal activity.

This escalation can be attributed to a few evolutions; an increase in ransomware operators, successful ransomware-as-a-service (RaaS) programs and a shift to more aggressive tactics for extorting organizations and victims of organization data leaks. Some notable highlights from 2023:



- Cl0p leverages 0days and exploitation in larger scale operations, with over 50% of victims having over 1,000 employees.
- AlphV (BlackCat) and Ransomed weaponized federal agencies and regulations to increase likelihood of payment.
- Operators are targeting industries that used to be considered 'off limits' such as aviation, healthcare, non-profits, and energy (oil, gas, water). Healthcare and non-profits saw more than 2 times as many victims in 2023 than 2022, and aviation and energy saw more than a 50% increase.
- Many groups have begun to cross moral lines in addition to criminal ones. Groups such as Hunters International have begun to extort individual patients and customers of breached organizations. Groups such as AlphV (BlackCat) and Medusa have threatened to release sensitive medical photos or records of patients and students if ransoms are not paid.

The jump in victims across more sensitive industries such as hospitals, critical infrastructure providers, and large corporations is concerning. Many RaaS and affiliate programs historically prohibited targeting some of these industries and banned partners who attacked or leaked their data. The shift in belief that these institutions are more likely to pay large ransoms to restore access to their vital systems and data due to the potential consequences of service disruptions increases concerns around future targets and both the immediate and lasting impacts of industries whose uptime can hold lives in the balance.

With roughly 100 ransomware operators active in 2023, organizations need to ensure they're prepared for the variety of approaches leveraged by these groups and their affiliates. Organizations should assess their incident response plans to ensure it covers best business practices and common standards for ransomware incidents, conduct gap assessments and tabletop exercises and develop playbooks to prevent, respond to and hunt for signs of ransomware or data leaks which could lead to extortion.

Spotlight On: Human Vulnerabilities

Humans are often considered the weakest link in the cybersecurity chain for a multitude of reasons. Most non-technical and even some technical users can be dismissive towards threat awareness and often prioritize ease of use over security. This includes using weak passwords or reusing passwords across multiple sites, including outside of work such as social media sites. Users tend to be too trusting or "click happy" – easily falling for social engineering and phishing emails or websites.

While some organizations have begun returning to offices, many continue to have a fully remote or split work force. This, combined with hybrid cloud environments, bring your own device (BYOD) and third-party integrations, has expanded the attack surface for most organizations. This distribution of workforce and infrastructure has highlighted gaps in proper asset management for organizations, leaving blind spots in security controls and data collection.

The expansion of work responsibilities across cybersecurity roles and the proliferation in tools required to complete these responsibilities continues to increase staff fatigue and burnout. With most businesses seeing budgets tighten, keeping on top of this all has become increasingly challenging.

In fall 2023, the National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) released the most common misconfigurations found during their red and blue team engagements.

1. Default configurations of software and applications
2. Improper separation of user/administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication (MFA) methods
8. Insufficient access control lists (ACLs) on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

This list perfectly encapsulates these human vulnerabilities in practice. Teams are struggling to keep users up-to-date and educated, get a complete picture of their hybrid workforce and infrastructure, and maintain an effective balance with staff to stay on top of it all. Many of the largest breaches in 2023 were the result of human error or oversight.

- Salesforce administrator misconfigurations expose private information to guest users
- DarkBeam and KidSecurity expose over 4 billion records due to unprotected Elasticsearch and Kibana interfaces
- 1.5 billion records exposed due to unprotected databases for Real Estate Wealth Network and TuneFab
- Multiple service desk and support teams socially engineered, resulting in compromised Okta super administrator accounts
- Unprotected Amazon Web Services endpoint exposed Pizza Hut Australia customer data

These weak links can expose organizations to a significant amount of risk if not properly mitigated. Organizations should regularly educate employees on the latest threats and cybersecurity best practices with customized training for their business. Phishing resistant forms of MFA are key to protect against threats that can bypass more simple MFA implementations, and employees should be made aware of how to spot the threats that still exist with your implementation. Change happened quickly the past few years so teams may also need to revisit any asset discovery and inventory processes to ensure new hybrid infrastructure and workforce models are covered. This should incorporate any cloud or SaaS services, third-party or API integrations, and remote workforce access methods and VPNs. By addressing these human vulnerabilities, putting technical controls in place on top, and fostering a culture of cybersecurity awareness within organizations, we can significantly improve our overall cybersecurity posture.

Predictions

EDGE DEVICE ABUSE

We expect to see a continued uptick in abuse of edge network devices. These devices – such as routers, firewall managers, and IOT devices – typically aren't monitored as well as user machines and typically don't support security software such as application whitelisting, AV or EDR like a desktop or server would. Adversaries are using these as proxies into the network for access/persistence or data storage/staging for exfiltration.

LEGITIMATE SOFTWARE ABUSE

This is not a new technique, however we've observed a noteworthy uptick in living off the land (LOTL) and legitimate software abuse by adversaries. This approach helps actors reduce effort by utilizing existing software that doesn't require any custom development or weaponization and isn't flagged by detection software. This includes initial access, lateral movement and exfiltration of data leveraging primarily or entirely legitimate software that already exists within a corporate environment.

TAKING ADVANTAGE OF TRUST

Similar to above, there has been more use of legitimate accounts via stolen or leaked credentials or account takeover to take advantage of existing trust within environments. We've also seen this with more trust being placed in cloud, third-party integrations, and SaaS providers to gain access to corporate environments.

DISCOVERY OF SIGNIFICANT DWELL TIMES

While ransomware/extortion actors are focused on getting in and getting data out as quickly as possible, nation state or more advanced adversaries are looking to remain within an environment as long as possible. We have seen and will continue to see several high-profile breaches lately where an actor may have been in the network for months or even years. We expect these types of breaches will continue to be discovered and announced, particularly via supply chain channels.

ACTORS USING LLMs

Cyber professionals are increasing their use of AI technology to help protect and prevent attacks by tapping large language models (LLM) to defend their networks and assets but it is also one of the number one cybersecurity concerns as well. Threat actors have begun adopting this technology more heavily as well, utilizing it for reconnaissance, delivery, and assistance with production of malicious code and deception approaches. The continuation of deep fakes, targeted phishing toolkits and misinformation with this technology has become simple to create as well.

Recommendations

ENABLE

As cybersecurity leadership, we need to listen to and enable our teams. The boots on the ground generally feel unheard, underprepared, and overwhelmed. Most are working within environments that require multiple tools to handle a single task or respond to even simple issues. Teams need to be empowered to voice suggestions, recommend improvements in tools and find time for training and innovation.

COLLABORATE

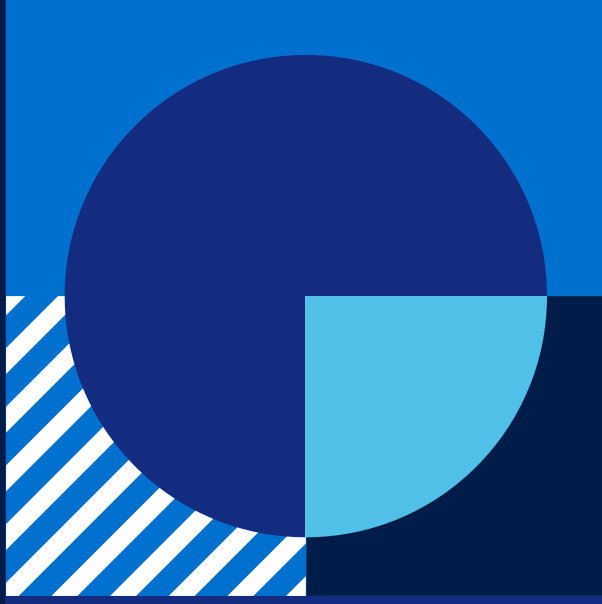
As budgets and staffing tightens, we encourage teams to evaluate joining Information Sharing and Analysis Centers, intelligence sharing communities, or collaboration efforts. These can often provide organizations with high quality insights and actionable intelligence at a lower price than one or many commercial threat intelligence feeds. The added benefit is that most allow real time analyst collaboration to gain additional viewpoints and intuition from others across the intelligence community.

TEST

Ensure you are frequently testing your various programs and procedures – attacks surface management, vulnerability management, digital forensics and incident response planning, threat hunting program. These should be living processes that are kept up-to-date and informed by the latest actionable threat intelligence.

BLOCK

Organizations should revisit their device and application management policies to ensure strict enforcement. This should cover employee devices which access corporate resources and include locking down default integrations. Application enforcement or whitelisting should be leveraged to reduce not only your vulnerable attack surface but tooling that would be available in the event of a breach allowing an adversary to live off the land.



GLOBAL DATA ANALYSIS METHODOLOGY

1

NTT Security Holdings gathers security alert and incident information from our Samurai MDR & XDR services 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 and our Security and Trust Office.

4

Collaboration and expert insights from our intelligence alliances with the Cyber Threat Alliance, Microsoft, US CERT and Recorded Future.

About NTT Security Holdings

NTT Security Holdings brings together over 20 years' experience of proactive cyber defense and services from across the NTT Group, combining the strengths of human capital, threat intelligence and technology developed by NTT to detect and defend against threats. Together with its partners across the world NTT Security Holdings works to create a safe and secure digital world.

Cybersecurity is a constant challenge. That's why more than 1,500 businesses around the world depend on NTT. By monitoring our customers' IT/OT environments 24/7 with our proprietary intelligence, we can discover and respond to threats instantly and effectively with near-zero false positives – no matter how sophisticated and malicious the threats may be.

Samurai XDR

Managed Detection and Response (MDR), powered by Samurai XDR

NTT Global Threat Intelligence Center Security Holdings

About GTIC

NTT Security Holdings' Global Threat Intelligence Center goes beyond traditional research, taking threat research and combining it with NTT proprietary detection technologies to produce applied cyber threat intelligence. The GTIC's mission is to protect stakeholders and clients by providing advanced threat research and cybersecurity intelligence enabling NTT Security Holdings to prevent, detect and respond to cyberthreats. The combination of proprietary intelligence capabilities and the truly unique vantage point enabled by NTT's Tier 1 Internet backbone equip GTIC with exceptional insights into threat actors, vulnerabilities and malware enriched with the tactics, techniques, and procedures (TTPs) they leverage.


NTT
Security Holdings
Together we do great things.
security.ntt