NTT

INSIGHTS
DRIVEN BY DATA

2021 Global Threat Intelligence Report Executive Guide

Accelerating cybersecurity: intelligence-driven and secure by design

The 2021 Global Threat Intelligence Report reminds us that in a world of evolving cyberthreats, we need to stay ahead of the curve to secure the next horizon of cyber-resilience. Success lies in rethinking what you need to accommodate new ways of working; engaging with your ecosystem of partners and customers to entrench trust across the supply chain; and securing all elements of your infrastructure to drive business value and transformation.

We're here to keep you secure by design with our intelligence-driven cybersecurity.

Foreword

We design and implement innovative cybersecurity solutions to address challenges impacting clients across many industries. In our **2021 Global Threat Intelligence Report**, we identify the threats organizations faced globally over the last year, and **provide the operational, tactical and strategic recommendations** they should consider implementing to manage risk.

In this year's Report, we continue reinforcing the theme of 'cyber-resilience' and 'secure by design solutions', but also include discussions related to trust. Organizations can no longer simply assign blind trust to new alliances, partners or vendors. It's also not wise to permit unvetted access to your organization's data. As in previous years, we continue our analysis of attacks against several industries. This includes deep dives into finance, healthcare, education, manufacturing and technology. We share our findings for each industry and look closely at where we observed changes in nefarious cyberattack activity.This Executive Guide shares key insights to help cybersecurity leaders and defenders decide where to focus their investments in, and improvements to, their security capabilities. It will also enable them to evaluate threats which may impact their environments and help them identify where risks can be reduced and where detection and response capabilities may be improved. Should you wish to access deeper analysis of the findings of this Guide, **read our Technical Report here.**

Kazu Yozawa
CEO, Security Service division, NTT Ltd.

Kazu has more than 40 years' experience in the ICT sector, with 12 years in managed security services. He was appointed Chief Executive Officer of NTT Security in April 2021. Prior to his appointment as 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.

FOLLOW KAZU ON LINKEDIN

Mark Thomas
Global Head of Threat Intelligence, NTT Ltd.

For the past 20 years, Mark has worked in the cybersecurity field establishing pragmatic, business-aligned risk minimization strategies and developing intelligence-led computer network defenses. His broad knowledge and in-depth expertise are a result of working extensively in consulting, technical and managed security services with large enterprises across numerous industry sectors including finance, government, utilities, retail and education. Mark leads the Global Threat Intelligence Center (GTIC) responsible for building and integrating threat intelligence to empower NTT's security services, global threat research, publications and sharing alliances.

FOLLOW MARK ON LINKEDIN

Four sources of insight

Our insights and analysis are garnered from four proprietary NTT resources.

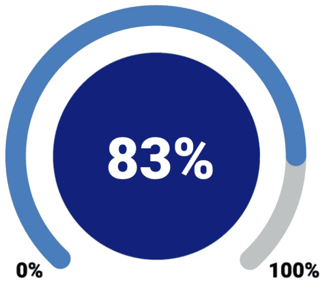
- **NTT Global Threat Intelligence Center (GTIC)**
- **Cybersecurity Advisory data**
- **NTT's WhiteHat Security**
- **NTT Ltd. global research, December 2020**

Spotlight: impact of COVID-19

Spotlight: impact of COVID-19

Throughout 2020, the COVID-19 pandemic wreaked havoc and concerns forced operational changes in many industries. Recurring global lockdowns to mitigate the spread of the disease continue to impact businesses dramatically.

Nearly five in six organizations **(83%)** completely re-thought their IT security to accommodate new ways of working brought about by the pandemic, according to recent research.



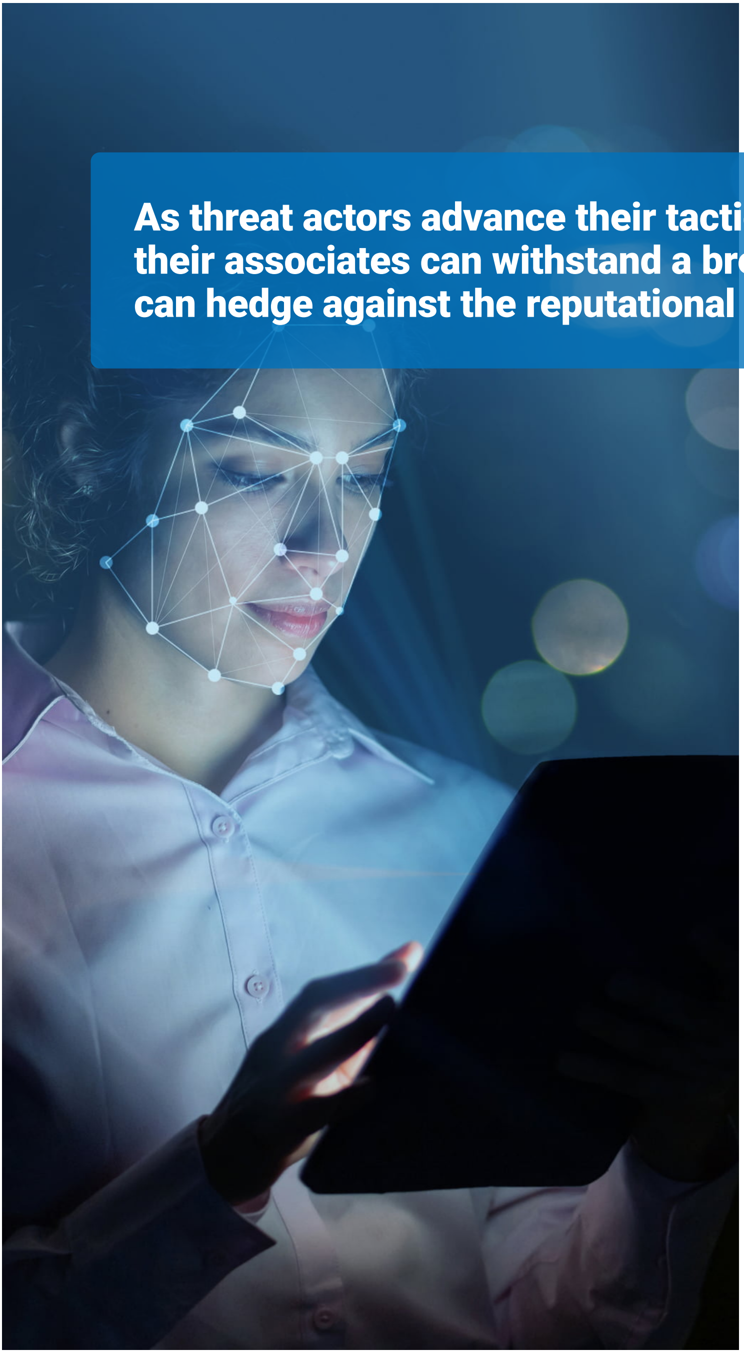
of organizations have **completely re-thought their IT security** to accommodate new ways of working brought about by the pandemic

Figure 1: NTT 2020 Intelligent Workplace Report (Aug '20)

Remote working has become a mainstay of the business environment

Some employees may never permanently return to an in-office working environment. This was illustrated in the **NTT 2020 Intelligent Workplace Report**, which showed that more than half of organizations **(54%)** would never return to their pre-pandemic operating model or would pursue a hybrid operating model with expanded flexible working. **With this new approach, organizations must place a higher priority on:**

- managing risk
- addressing cybersecurity issues related to supporting their online presence
- optimizing and securing work-from-home arrangements
- preparing to defend against supply chain attacks



As threat actors advance their tactics, techniques and procedures, organizations need to ensure that they and their associates can withstand a breach and recover from an attack in a timely manner. No amount of insurance can hedge against the reputational damage suffered after a breach becomes public.

A distributed workforce, or remote working, is a business model with which some organizations have had limited experience. It creates demand for employee equipment, additional networking, and VPN support and support for a culture that provides for limited hands-on management of employees. Irrespective of their work location, employees must be able to accomplish their tasks and effectively communicate with colleagues while adhering to organizational policies and procedures designed to keep all data safe. Organizations must adapt and maintain a secure network to allow uninterrupted business continuity. This has become increasingly difficult as security professionals have often been redirected to serve the additional demand for more general ICT support, effectively deprioritizing security initiatives.

Defending against supply chain attacks has taken on a new level of urgency

Depending on the threat actor's goal, a supply chain attack on COVID-19 vaccine manufacturing and cold storage facilities could stop vaccine production and distribution. This would impact treatment and possibly cause patient deaths. Exfiltrating vaccine formulas and manufacturing processes would benefit nation-state threat actors whose countries have yet to produce a highly effective treatment for the virus. Sowing discord via vaccine delays could also provide attackers with additional attack vectors for follow-on attacks.

Threat actors and phishing campaigns escalate efforts

COVID-19 phishing campaigns have spanned the globe and targeted organizations studying the effects of the virus, those researching a vaccine and possibly the Vaccine Alliance's Cold Chain Equipment Optimization Platform program. Any disruption to the temperature-controlled storage facilities or transportation vehicles endangers the integrity of vaccines with cold-storage requirements, possibly endangering lives by contributing to increasing infection rates if people can't get vaccinated.

We have been actively tracking many cybercriminal and advanced persistent threat (APT) group campaigns that have been exploiting the pandemic to further their activities. While cybercriminal groups have exploited the pandemic to spread malware for financial gain, APT groups have leveraged pandemic-related concerns to define targets and establish footholds in victims' systems. Attackers have:

- distributed malicious PDF, RTF and Word documents
- disseminated spyware, keyloggers and other malware
- used specific COVID-19 related phishing lures
- targeted education or healthcare institutions involved in COVID-19 patient care and vaccine research, development and distribution

As with all disasters, threat actors exploit opportunities to launch attacks. Industrious cybercriminals have had prolonged opportunities to launch various COVID-19 related attacks, particularly pandemic-themed phishing attacks and vaccine phishing campaigns.

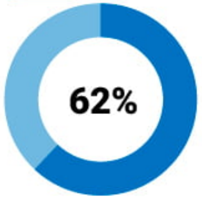
COVID-19 continues to evolve, affecting industries, businesses and human interactions around the globe. We must continue to seek ways to manage risk in all forms related to the pandemic and adjust our strategies, focusing on changing operations and providing continued support for clients and employees, as well as COVID-19 related research and vaccine distribution. These are highly complex issues that only serve to complicate the operations and security profiles of affected organizations. As a result, all organizations must continue to innovate and create resilient solutions for a more secure human and cyber environment.

6 key insights into the cybersecurity landscape

6 key insights into the cybersecurity landscape

1

Finance, manufacturing and healthcare industries in line of fire



of all attacks are against these top three industries

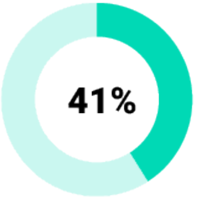
2

Malware sees a metamorphosis

Miners and Trojans replace spyware as most common malware family globally

3

Cryptocurrency miners proliferate



of all malware detected are coin miners

4

COVID-19 cybercriminal opportunism intensifies

Cybercriminal groups and nation-state actors took advantage with attacks related to COVID-19 vaccine and associated supply chains

5

Remote work attracts more web and application attacks

More than 67% of all attacks were remote access: either web-application (32%) or application specific (35%)

6

Privacy and protection define our 'new normal'

Increasing obligations, restrictions or limitations on the ability to transfer personal data to other countries

Global analysis

Global analysis

Some trends were visible on a global basis, like increasing numbers of application-specific and web-application attacks. But certain details about hostile activity differed by the geographic areas in which they occurred:

- Cryptominers dominated activity in Europe, the Middle East and Africa (EMEA) and the Americas but were relatively rare in Asia Pacific (APAC).
- OpenSSL was the most targeted technology in the Americas but was not even on the top 10 list in APAC.

Analysing the differences in techniques and tools can provide insight into how hostile threat actors are targeting organizations in different geographic regions and countries.

Industry preparedness

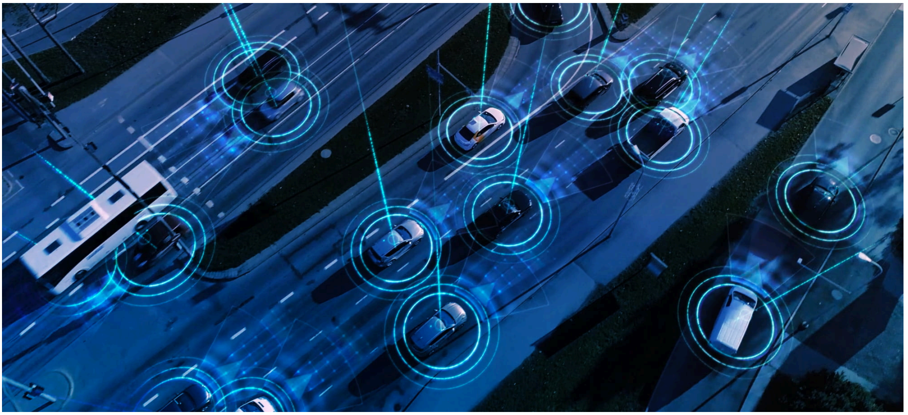
Finance, while top in cybersecurity maturity or preparedness overall, is still among the most attacked industries.

Most concerning is that healthcare and manufacturing have relatively low maturity scores. Their ability to close the gap in required maturity has seen a drop, at a time when attacks against these industries have intensified.

Figure 2 shows comparisons between 2018, 2019 and 2020's benchmark scoring using NTT's Cybersecurity Advisory (CA) consulting service. The CA score is based on a 0-6 scale which defines the maturity of the organization's security program in several areas (with a higher number indicating a more mature program).

Industry	2018 baseline	2019 baseline	2020 baseline
Technology	1.66	1.64 ↓	1.64 —
Finance	1.71	1.86 ↑	1.84 ↓
Business and professional services	1.31	1.54 ↑	1.79 ↑
Education	1.21	1.02 ↓	1.04 ↑
Manufacturing	1.45	1.32 ↓	1.21 ↓
Healthcare	1.03	1.12 ↑	1.02 ↓

Figure 2: Comparisons between 2018, 2019 and 2020's benchmark Cybersecurity Advisory scores



Baseline scores (measured against the organization's current maturity) have largely remained within the same range as the previous year.

Finance continues to show the highest benchmark score for the third consecutive year.

Small decreases in baseline scores likely result from challenges in prioritization, which potentially affected allocation of resources and didn't allow the organization's program to mature. This isn't unexpected in healthcare. The industry faced challenges in keeping up with infrastructure issues during the pandemic.

Manufacturing organizations experienced a three-year decline in scores, most likely due to changes in the operating environment, evolution of attacks and a greater inclination to benchmark their overall cybersecurity posture.

Maturity levels defined in the Cybersecurity Advisory

Maturity Scale	Non-existent 0.00–0.99	Initial 1.00–1.99	Repeatable 2.00–2.99	Defined 3.00–3.99	Managed 4.00–4.99	Optimized 5.00–5.99
Process	No process costs	Ad-hoc and informal	Some basic templates or checklists exist	Formally documented processes are consistent	Formal integrated workflows	Mature and automated workflows
Metrics	No metrics exist	Ad-hoc reporting	Basic metrics, informal reporting	Formally documented metrics, manual reporting	Advanced metrics and semi-automated reporting	Fully automated reporting
Tools	No technology control exists	Planning underway	Basic functionality implemented with only elemental capabilities	Functionality implemented and aligned to policies	Integrated logging, manual correlation	Integrated platform, automated correlation

Figure 3: Maturity levels as defined in the Cybersecurity Advisory

The maturity of security programs in the business and professional services industry increased for a third year in a row. Improvements during 2020 are likely reflective of the industry's ability to continue managing priorities and make good investments in both strategy and implementations in response to COVID-19.

Maturity level gap

Figure 4 illustrates the gap between the current and desired state of several industries. Industries seeking to close the gap must maintain a constant focus on tools, executive support and the maturity of underlying processes. However, various factors such as cost, compliance and the availability of resources can result in industries not achieving their desired goals. Our research found a gap between organizations' perception of their cybersecurity posture and their actual score.

While the results of the research indicated organizations believed their cybersecurity posture averaged **3.16** (**17%** of organizations believed their posture is optimized, and CEOs believed their cybersecurity posture was higher, at **3.44)** the average of all initial Cybersecurity Advisory scores was **1.35**, indicating organizations may not have a true understanding of the strength of their security programs.

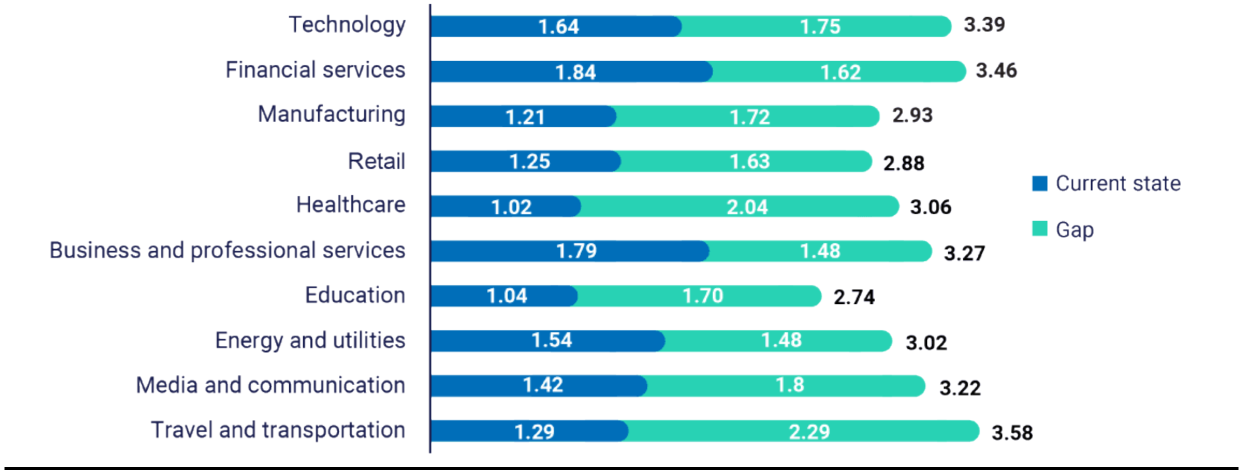


Figure 4: Current and target maturity levels and the gap between them, by sector

Target vs goal state

The target state doesn't necessarily indicate where an industry needs to be, it indicates a goal state as defined by the organizations in each industry. Typically, active compliance with more stringent regulations, and the motivation to protect more sensitive public or client information can help encourage organizations to strive for a higher maturity goal. A commitment to a higher goal with executive stakeholder support can lead directly to improved prioritization of security initiatives and better outcomes.

Top five cybersecurity focus areas for next 18 months

Our research shows a focus on protecting cloud services as top cybersecurity focus over the next **18 months**, followed closely by protecting the network **(49%)** and securing data and applications **(49%)**. Ensuring that an estate is secure by design **(47%)** and takes data privacy and GRC into account **(47%)** are close contenders across respondents we interviewed.

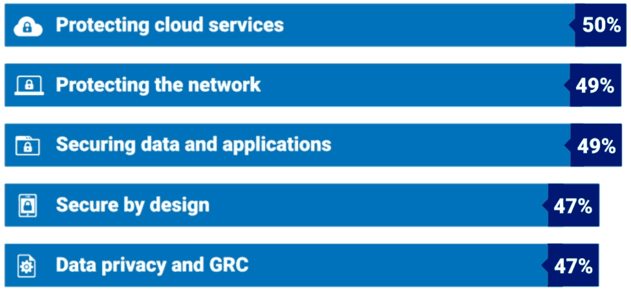
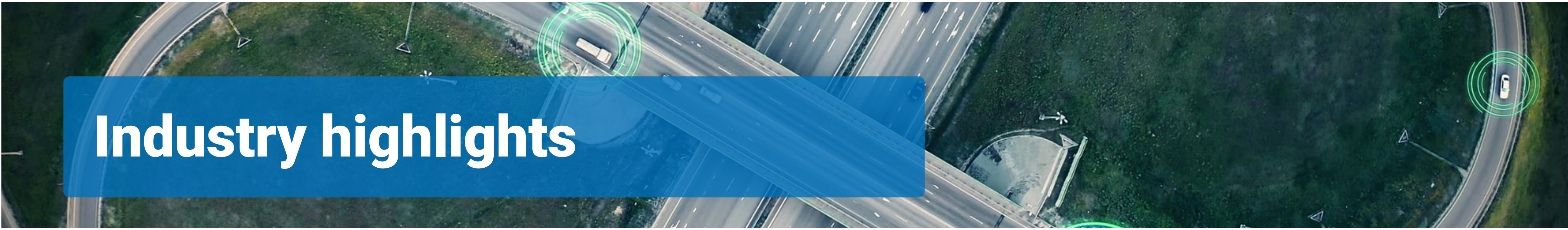


Figure 5: Top cybersecurity focus for next 18 months

Note: 'Secure by design' was described in the questionnaire in fuller terms: 'Ensuring security is designed into our processes and technology.'

Attack types defined:

- **Botnets:** comprise multiple infected internet-connected devices used to carry out coordinated actions, such as sending spam or conducting distributed denial-of-service (DDoS) attacks; Mirai, Echobot and IoTroop are examples of botnets.
- **Application-specific attacks:** target vulnerabilities in applications, including broken authentication and session management, non-secure direct object references, lack of encryption for data at rest and in transit, escalation of privileges, and Trojanized or unpatched third-party components.
- **Web attacks and web-application attacks:** attacks against services and applications that support a web presence, such as command injection, SQL injection and cross-site scripting.
- **Reconnaissance:** activity related to an attacker identifying systems and services that may be valuable targets.
- **Brute-force attacks:** the systematic use of username and password combinations to guess and identify credentials, to access a system or resource.



Industry highlights

In 2020, we observed less correlation between attack types and targeted industries. But in every region and country, we observed greater correlation between the malware used, the technologies being targeted and the industry of interest.

Industries have a set of technologies of concern, on which they focus their cybersecurity initiatives. Meanwhile, attackers have their own priorities, and the technologies they focus on are almost predictable, with the top few technologies regularly accounting for **50%** or more of attacks.

Highest areas of risk

Considering the landscape of the threats that organizations are least prepared for, our research revealed the breadth and depth of the threat landscape, from organized cybercrime to insider threats. The top threat that organizations admit they're least prepared for, and which could be construed as the highest risk, is from nation-state, state sponsored and organized cybercriminal groups **(76%)**. This is compounded by the second-ranking risk of failing to meet compliance obligations **(76%)** and insider threats **(73%)**.

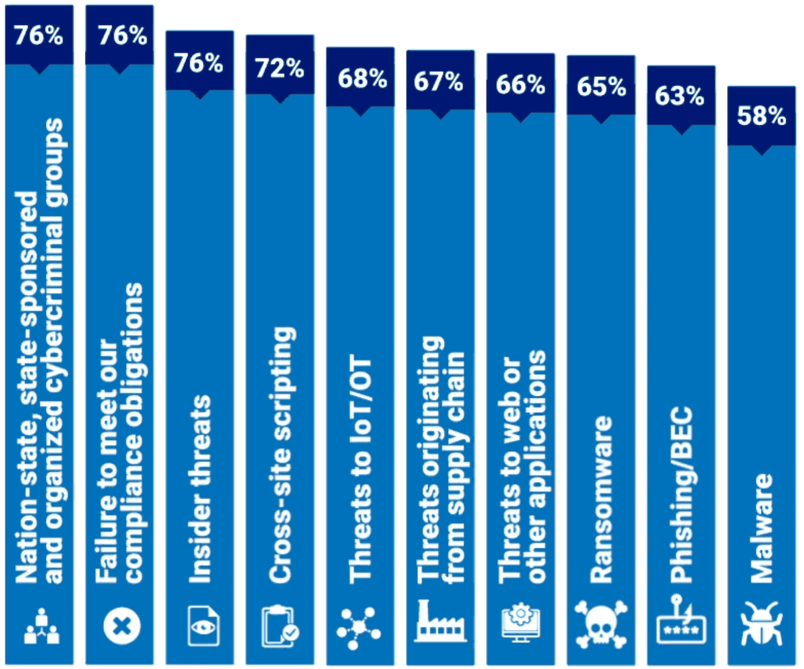
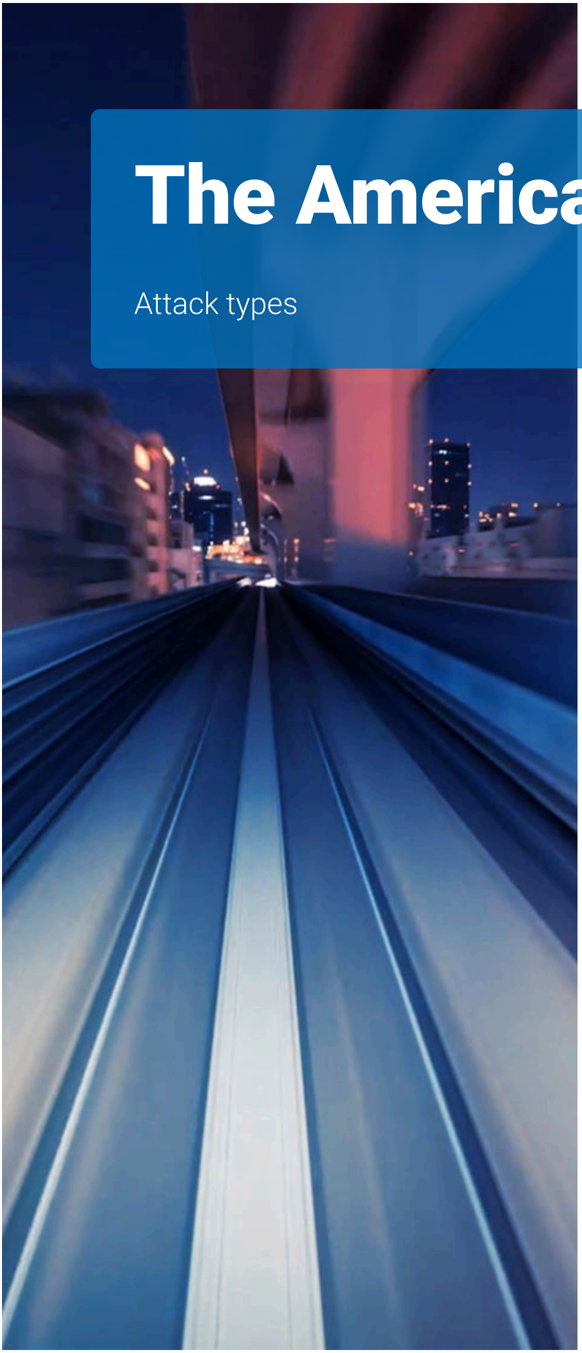


Figure 6: Threats that organizations aren't prepared for

Regional hotspots



The Americas

Attack types

Like every other region, as well as globally, the top two attack types in the Americas were application-specific and web-application attacks.

- But the Americas showed the lowest total for those combined attack types, at **56%**.
- This was below the global average of **67%**.
- This gap was filled by DoS/DDoS and brute-force attacks, both of which were higher in the Americas than any other region.

Within the Americas, the US accounted for two of the highest rates of reconnaissance activity of any country analysed:

- Some **64%** of all hostile activity targeting the technology industry was some form of reconnaissance.
- In the education industry, **58%** of all hostile activity was reconnaissance.
- Despite the high levels of reconnaissance in these two industries, overall reconnaissance in the Americas accounted for **23%** of all hostile activity. This was only slightly above the global average of **20%**.

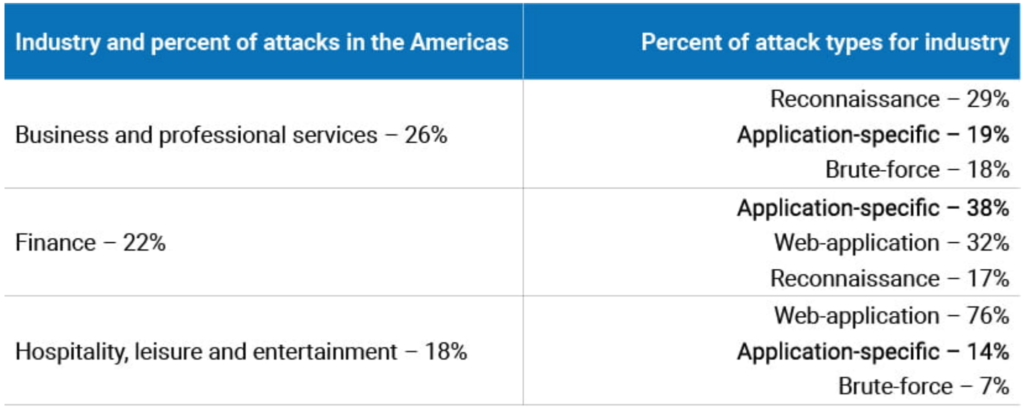
Globally, denial-of-service (DoS), distributed-denial-of-service (DDoS) and brute-force attacks tended to appear relatively low on the list of common attack types.

- The Americas observed **8%** of all attacks as DoS/DDoS attacks, while these attacks accounted for under **4%** in APAC and **1%** in EMEA.
- Attacks in specific industries were higher; for example, DoS/DDoS attacks accounted for **28%** of all attacks against manufacturing organizations in the US.

Most attacked industries

Business and professional services was the most attacked industry in the Americas.

- The only other country in which the industry was highly attacked was Sweden **(#3 at 11%).**



Industry and percent of attacks in the Americas	Percent of attack types for industry
Business and professional services – 26%	Reconnaissance – 29% **Application-specific – 19%** Brute-force – 18%
Finance – 22%	**Application-specific – 38%** Web-application – 32% Reconnaissance – 17%
Hospitality, leisure and entertainment – 18%	Web-application – 76% **Application-specific – 14%** Brute-force – 7%

Figure 7: Percent of attacks and percent of attack types per industry in the Americas

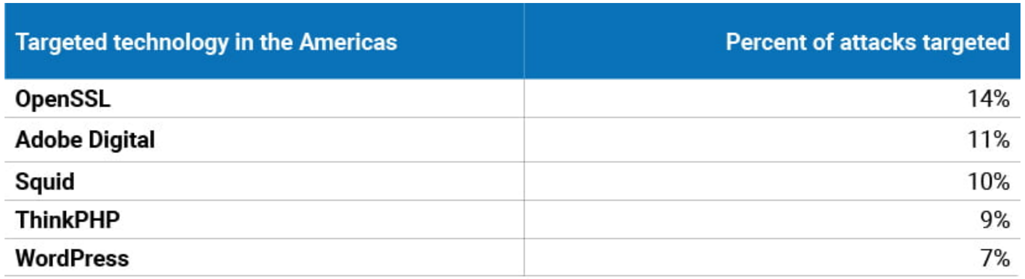
It was also uncommon to see more than **1–2%** of brute-force attacks against a specific industry.

- However, attackers targeting business and professional services **(18%)** and hospitality, leisure and entertainment **(7%)** made use of brute-force attacks during targeting.

Most attacked technologies

The most common technologies attacked in the Americas also differed from global observations.

- In the Americas, OpenSSL was the most targeted technology.
- ThinkPHP, which was the most attacked application globally, emerged at fourth place as the target of **9%** of all attacks.
- This was well below the global average of **30%**.



Targeted technology in the Americas	Percent of attacks targeted
OpenSSL	14%
Adobe Digital	11%
Squid	10%
ThinkPHP	9%
WordPress	7%

Figure 8: Top targeted technology in the Americas

Malware observations

With **34%** of all malware detections, XMRig was the most detected malware in the Americas and in the US, but comparably, EMEA observed significantly more XMRig.

- NetSupport Manager was the second most detected malware globally **(6%)** and in the US **(13%)**.
    - The US observed a higher rate of NetSupport Manager than any other country. While it was observed in other countries, it did not appear in any other list of top five malware.

- While every country experienced a variety of malware, the US and Japan were the only countries analysed to see more than one form of worm in their top 10 most commonly detected malware (Morto **(13%)** and Conficker **(2%)** for the US).
    - The US also experienced a higher rate of Morto detections than any other country analysed.

Malware detections in the US	Percent of all malware	Malware family
XMRig	34%	Miner
NetSupport Manager	13%	RATs
Morto	13%	Worm
Cryptominer	10%	Miner
Torpig	4%	Botnet

Figure 9: Top malware detections by malware family in the US

Europe, Middle East & Africa

Attack analysis

Attack types

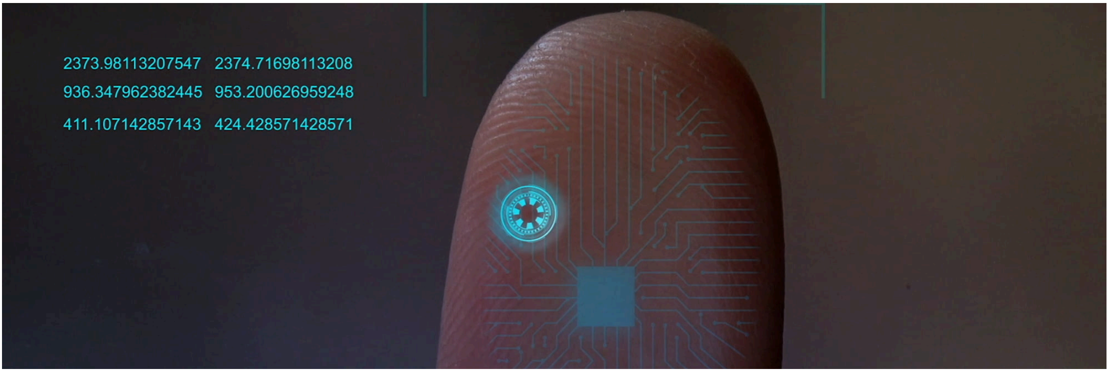
Attacks in Europe, Middle East & Africa (EMEA) followed many of the same global trends, while showing some significant differences in technologies and malware observations.

- As a region, EMEA experienced **79%** of all attacks as combined application-specific **(42%)** and web-application **(37%)** attacks. At **91%** of all such attacks, the UK had the highest rate of combined web attacks of any country analysed.

Most attacked industries

- Targeted industries were quite narrow across the region, considering the differences in countries and their respective policies and initiatives.
- While the numbers varied somewhat in each country, healthcare, manufacturing and finance were the most attacked industries in EMEA, but some of the activity in those industries showed marked differences from other regions.
- Healthcare was the most attacked industry in EMEA.
- The levels of attacks in all the healthcare, manufacturing and finance industries were a result of the sheer amount of additional attack volume placed on these industries during the global pandemic.
- The combined attacks from web-application **(62%)** and application-specific **(36%)** attacks targeting healthcare in EMEA accounted for **98%** of all hostile activity.

- This is well above the global average of **67%**. It emphasizes just how much attention attackers focused on the web presence of these organizations, and how strongly they targeted their web-enabled applications.



Industry and percent of attacks in EMEA	Percent of attack types for industry
Healthcare – 37%	Web-application – 62% Application-specific – 36% Network manipulation – 1%
Manufacturing – 31%	Application-specific – 50% Web-application – 27% Reconnaissance – 19%
Finance – 14%	Application-specific – 68% Web-application – 16% DoS/DDoS – 8%

Figure 10: Percent of attacks and percent of attack types per industry in EMEA

- While technology has been among the top one or two most attacked industries in five of the past seven years, it did not appear in the top five industry list for any country analysed in EMEA.

Targeted technology in EMEA	Percent of attacks targeted
ThinkPHP	32%
Zeroshell Net Services	10%
PHPUnit	6%
Microsoft SQL Server	6%
Palo Alto Networks devices	5%

Figure 11: Percent of attacks and percent of attack types per industry in EMEA

Most attacked technologies

- In EMEA, targeting of ThinkPHP slightly exceeded the global average of **30%**, and like other regions, targeted technologies dropped off sharply.
- Targeted technologies varied greatly by country in EMEA. Palo Alto Networks devices were the most targeted in the United Kingdom and Ireland (UK&I); Zyxel devices in Germany; OpenSSL in France; and ThinkPHP in Sweden, Benelux and the Netherlands.
- But the technologies targeted were highly dependent on the industries being attacked.
- ThinkPHP and PHPUnit were highly targeted in finance and manufacturing organizations, which were the two most attacked industries in EMEA.
- Healthcare was highly targeted via Zeroshell Net Services.

Malware observations

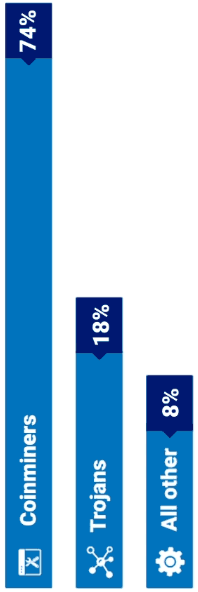


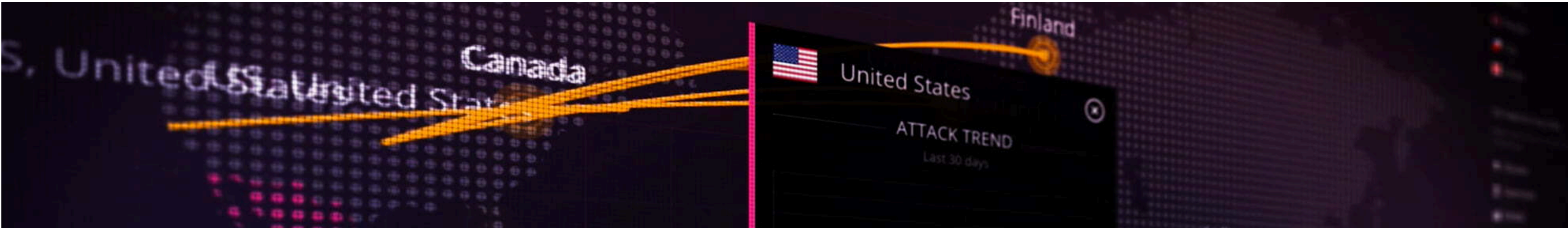
Figure 12: Breakdown of malware family detections in EMEA

Despite the differences between the countries, malware in EMEA was more consistent than in other regions.

- Overall, EMEA was dominated by miners, which accounted for **74%** of all malware activity in the region.
- Miners were the most detected form of malware in the UK&I, Germany and Benelux.

Malware	UK&I	Germany	Sweden	Norway	Benelux
XMRig	86%	65%	2%	<1%	89%
Other coin miners	1%	2%	44%	37%	<1%
Trojans	Tofsee – 8%	Emotet – 15% Tofsee – 12% Trickbot – 2%	NetWiredRC – 17% GraceWire – 16%	GraceWire – 23% NetWiredRC – 17%	Trickbot – 2%

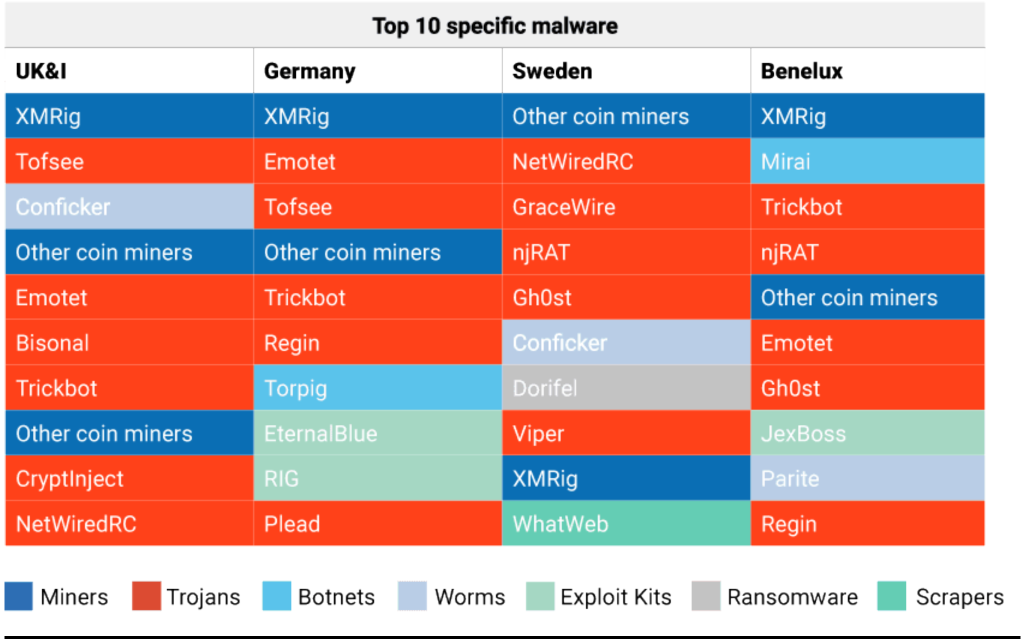
Figure 13: Percent of malware detections by country in EMEA



- **While most countries in EMEA experienced multiple miners, XMRig accounted for nearly 99% of all miner activity in EMEA and for over 87% of all malware detections.**
  - XMRig or other coin miners were the most common malware detected in every country analysed in EMEA.

Trojans were the second most common form of malware within EMEA.

- In the UK&I, six of the 10 most observed malware were some form of Trojan. In Sweden, four of the top five malware were Trojans.
- Three of the top five malware in Germany were some form of Trojan. The most common Trojans observed in EMEA were Tofsee and Emotet.
- While miners dominated overall volume, each country experienced a greater variety of Trojans.
- Activity in each country was led by different Trojans, but Trickbot was in the top 10 most detected malware in over **80%** of the countries analysed in EMEA.
- While the global average for botnets was **10%**, barely **2%** of malware activity in EMEA was associated with botnets.



Top 10 specific malware

UK&I	Germany	Sweden	Benelux
XMRig	XMRig	Other coin miners	XMRig
Tofsee	Emotet	NetWiredRC	Mirai
Conficker	Tofsee	GraceWire	Trickbot
Other coin miners	Other coin miners	njRAT	njRAT
Emotet	Trickbot	Gh0st	Other coin miners
Bisonal	Regin	Conficker	Emotet
Trickbot	Torpig	Dorifel	Gh0st
Other coin miners	EternalBlue	Viper	JexBoss
CryptInject	RIG	XMRig	Parite
NetWiredRC	Plead	WhatWeb	Regin

■ Miners ■ Trojans ■ Botnets ■ Worms ■ Exploit Kits ■ Ransomware ■ Scrapers

Figure 14: Top 10 detected malware in the UK&I, Germany, Sweden and Benelux

- Despite the global average of ransomware rising to **6%** of malware, organizations in EMEA experienced less than **1%** of their malware as ransomware.

Asia Pacific

Attack analysis

Attack types

While many observations on activity within the Asia Pacific (APAC) region were consistent with details from global and other regional data, APAC experienced significant differences from some of the other geographic areas.

- Attacks were consistent with the types of attacks observed globally, with web-application **(51%)** and application-specific **(22%)** attacks combining to account for **74%** of all hostile activity.
- This was slightly higher than the global average of **67%**. Service-specific **(18%)** attacks were the third most common in APAC.
- These attacks tend to be more advanced and less commoditized than many of the application-oriented attacks.

Most attacked industries

- Attacks against education dominated in several countries, and the industry joined finance and manufacturing as the most common targets in APAC.

Industry and percent of attacks in APAC	Percent of attack types for industry
Finance – 24%	Web-application – 51% Application-specific – 22% Service-specific – 18%
Manufacturing – 22%	Application-specific – 59% Reconnaissance – 30% Web-application – 5%
Education – 18%	Web-application – 30% Application-specific – 26% Brute-force – 25%

Figure 15: Percent of attacks and percent of attack types per industry in APAC

- This was the highest rate of reconnaissance in any industry in the region.
- While reconnaissance was the third most common form of hostile activity **(20%)** globally, most industries in APAC, other than manufacturing, experienced less than **6%** of attacks as reconnaissance.

- While most attacks targeting education followed global expectations, brute-force attacks targeting education in APAC accounted for **25%** of all hostile activity.
- This was the highest rate of brute-force attacks against any industry in any region or country analysed.

Most attacked technologies

With **35%** of all attacks, ThinkPHP was the most targeted application in APAC, exceeding the global average of **30%**.

- Targeting of ThinkPHP was higher in Japan than many other APAC countries.
- ThinkPHP was widely used by attackers of finance, manufacturing, technology and education. These were also the top four industries attacked in the region.
- Targeting of other technologies was distributed widely throughout APAC, with only targeting of D-Link devices also appearing in the global list.
- All five of the most targeted technologies appeared heavily in the most targeted industries in the region.

Targeted technology in APAC	Percent of attacks targeted
ThinkPHP	35%
Apache Struts	6%
D-Link devices	5%
vBulletin	5%
Linux	4%

Figure 16: Top targeted technologies in APAC

Malware observations

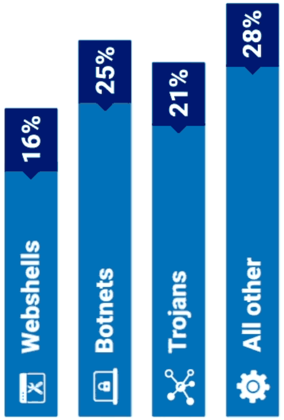


Figure 17: Breakdown of malware family detections in APAC

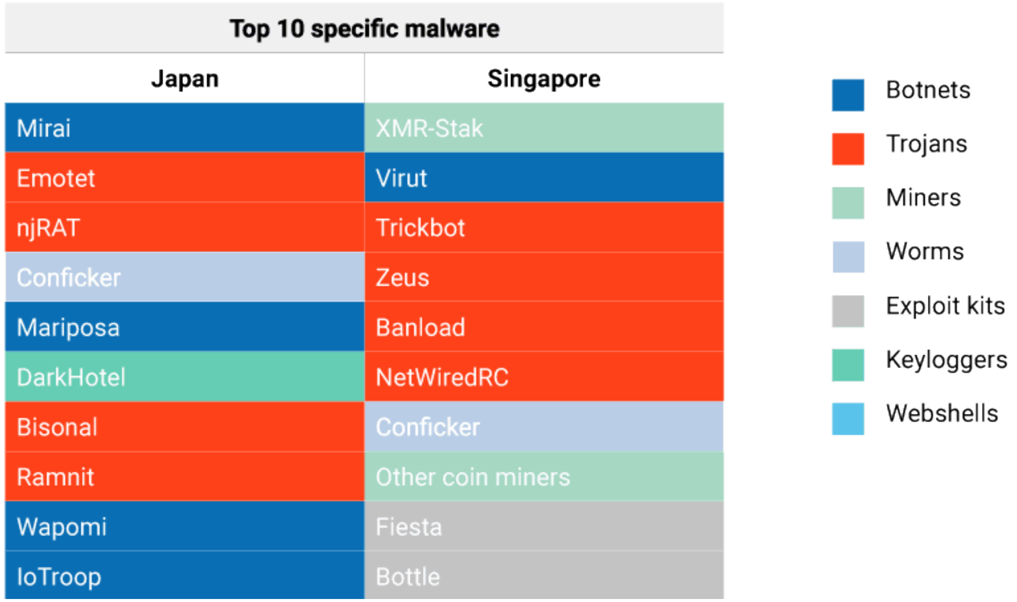
Malware varied greatly throughout APAC, but webshells, botnets and all forms of Trojans combined to account for **72%** of all malware. The type of malware detected depended greatly on the country and industry being targeted.

- While Mirai was observed in nearly every country in APAC, it was the single most detected malware in Japan, especially targeting manufacturing and technology.

Malware detection	Malware family
Mirai – 19%	Botnet
Emotet – 17%	Trojan
njRAT – 7%	Trojan
Conficker – 6%	Worm
Mariposa – 5%	Botnet

Figure 18: Top malware detections in Japan

- Throughout APAC, botnets showed the highest volume of any malware family.
- Like EMEA, most countries in APAC tended to show activity from at least four different Trojans in their list of top 10 most observed specific malware.
- Throughout the region, Emotet and NetWiredRC were the most commonly detected Trojans.



Top 10 specific malware	
Japan	**Singapore**
Mirai	XMR-Stak
Emotet	Virut
njRAT	Trickbot
Conficker	Zeus
Mariposa	Banload
DarkHotel	NetWiredRC
Bisonal	Conficker
Ramnit	Other coin miners
Wapomi	Fiesta
IoTroop	Bottle

Botnets
Trojans
Miners
Worms
Exploit kits
Keyloggers
Webshells

Figure 19: Top ten detected malware in Japan and Singapore

- While XMRig was the most commonly detected malware globally, no country in APAC showed XMRig in their top 10 most common malware.
- In fact, Singapore was the only country analysed in APAC that experienced a significant amount of activity from any form of cryptominer (**75%** of activity in Singapore, while less than **1%** in the rest of APAC).

Australia and New Zealand

Attack analysis

Attack types

Several industries in Australia and New Zealand (ANZ) showed elevated levels of reconnaissance **(32%)**.

- This was followed by web-application attacks **(28%)**.

Attacks (categories)	Percentage of attacks
Reconnaissance	32%
Web-application attack	28%
Application-specific attack	19%
Service-specific attack	8%
Brute forcing	8%
DoS/DDoS	3%

Figure 20: Top attack types in ANZ

Most attacked industries

- Finance was the most attacked industry in ANZ **(42%)**.
- While finance was the most attacked industry globally, the only analysed country in which finance was the most attacked industry was Australia, where it was the target of **46%** of all attacks.
- The industry is generally perceived as a target-rich environment containing both personal and financial data.

Industry	Percentage of attacks
Finance	42%
Education	24%
Technology	14%
Manufacturing	11%
Public sector	8%

Figure 21: Top attacked industries in ANZ

Most attacked technologies

Attacks on D-Link technologies were the most common in the region during 2020 **(11%)**.

Targeted applications/products in attack categories	Percentage of attacks
D-Link	11%
vBulletin	9%
Cisco Ative Security Appliance (asa)	7%
Linux	7%
ThinkPHP	5%
Oracle	5%
HP Universal CMDB	5%
Apache (unclassified) product	4%
Apache Struts	4%
Shenzhen TVT DVR	3%

Figure 22: Top technologies targeted in ANZ

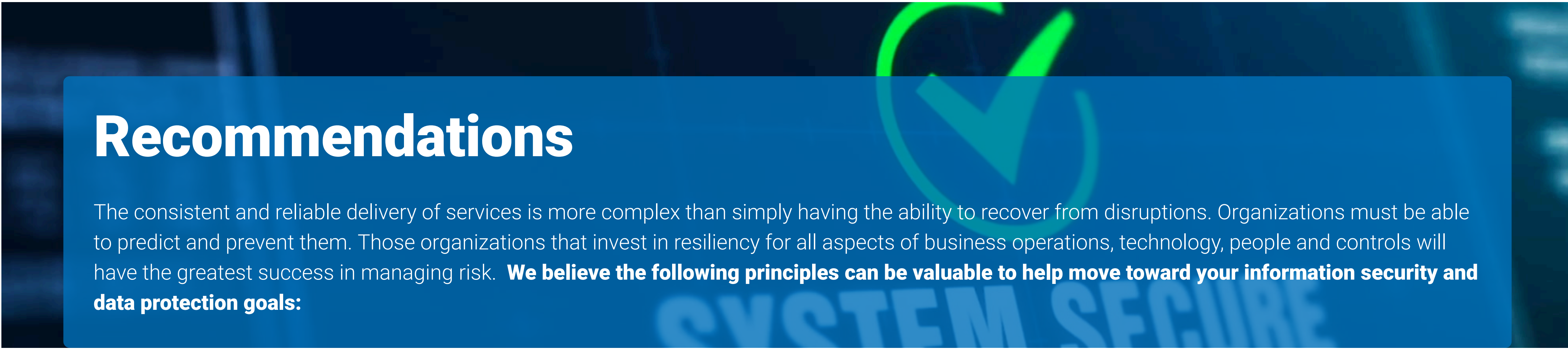
Malware observations

Mariposa and China Chopper were the two most common malware in Australia and New Zealand, especially in education.

Malware family	Percentage of attacks
Mariposa	34%
China Chopper	26%
Winnti	12%
Mirai	5%
NetWiredRC	5%
Emotet	4%
Morto	4%
Gh0st	2%
Ganiw	2%
Bladabindi	2%

Figure 23: Top malware detected in ANZ

Recommendations



Recommendations

The consistent and reliable delivery of services is more complex than simply having the ability to recover from disruptions. Organizations must be able to predict and prevent them. Those organizations that invest in resiliency for all aspects of business operations, technology, people and controls will have the greatest success in managing risk. **We believe the following principles can be valuable to help move toward your information security and data protection goals:**

1

Position cybersecurity as a key strategic component of the business

Organizations are trying to modernize. A key part of this is enabling effective digital transformation that better supports the current demands of the business. Given the scale of threats organizations are currently facing, they must include cybersecurity as a Board-level agenda item and treat it as a fundamental business requirement to support operations.

2

Prioritize people and process

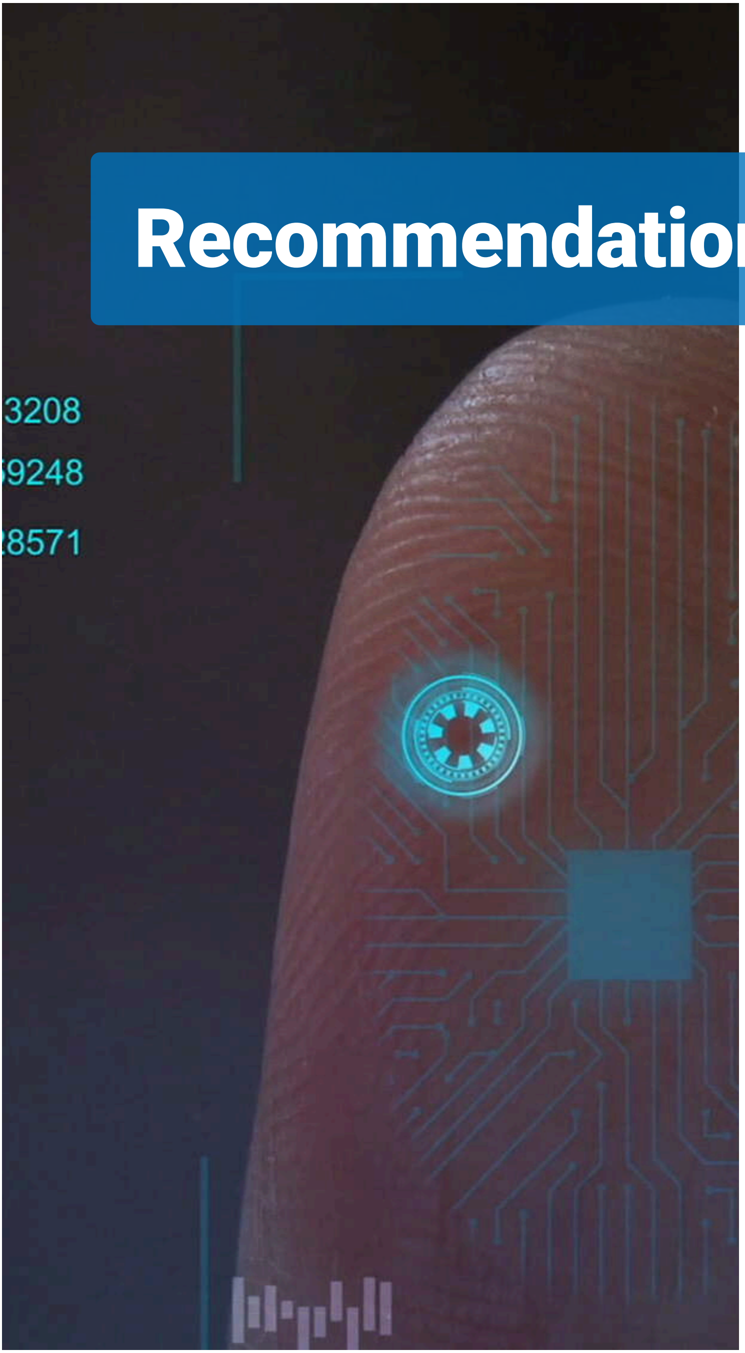
Organizations should embrace people as their most critical resources. Appropriate user education will help employees understand the role they play in the organization's security posture. Train employees to work in a 'security aware' manner – not to be the weakest link, nor the strongest link, but a key component. Those with technical component responsibility of the security profile must ensure their organizations provide employees with technology and security training.

3

Embrace security by design

Organizations simply can't plug-in or add on the security required for them to operate in an effective manner. They must build security best practices into policies, procedures, infrastructures and applications. In what's functionally a systems design process, the organization should include consideration of security tactics in the foundations of any project, product development or functional implementation.

Recommendations



4

Adopt existing cybersecurity frameworks and standards

Organizations should continue to emphasize leveraging standards, knowledgebases and frameworks defined by leaders in the cybersecurity community. MITRE ATT&CK and the NIST Cybersecurity Framework are examples of resources that contain valuable information from seasoned cybersecurity professionals and working groups. Leveraging these resources can provide your organization with a wealth of knowledge that can rapidly bolster your organization's security posture.

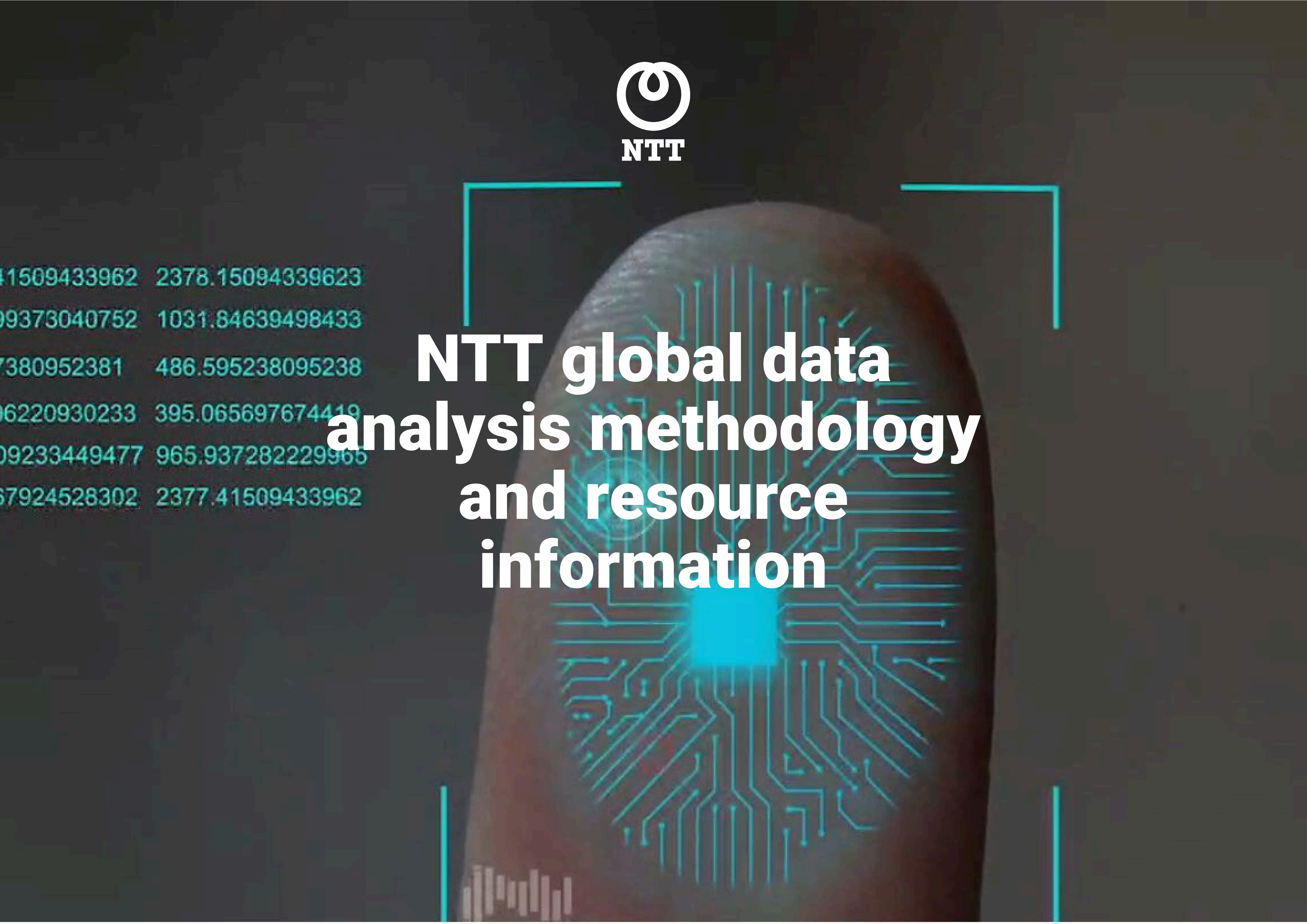
5

Prioritize continuous monitoring

Organizations need to be able to identify and react to attacks and breaches faster. Many breaches include compromises that have gone undetected for months, or even years. If we operate with a 'breach posture', we're functioning with less trust in the component parts of our organizations. Prioritize security in the context of enabling the organization to identify and manage breaches when they occur. The goal of security programs should be to focus detection and response activities on the breaches that have the greatest potential to affect the organization.

Lastly, organizations must remember that the keys to an effective cybersecurity program are planning, execution, monitoring and accountability. Remaining vigilant and constantly updating your threat intelligence, detection, response and business continuity plans are vital to success.

NTT



NTT global data analysis methodology and resource information

Our 2021 Global Threat Intelligence Report contains data gathered from four proprietary NTT resources:

NTT Global Threat Intelligence Center (GTIC)

The 2021 Global Threat Intelligence Report contains global attack data gathered from NTT and supported operating organizations from 1 January, 2020 to 31 December, 2020. The analysis is based on log, event, attack, incident and vulnerability data from clients as well as from our global honeypot network. Leveraging the indicator, campaign and adversary analysis from our Global Threat Intelligence Platform has played a significant role in tying activities to actors and campaigns.

We gather security log, alert, event and attack information which we enrich. We then analyse the contextualized data. This process enables real-time global threat intelligence and alerting. The size and diversity of our client base, which includes 15,000 security engagements with clients spanning 57 countries in multiple industries, provides us with security information which is representative of the threats encountered by most organizations.

The data is derived from worldwide log events identifying attacks based on types or quantities of events. The use of validated attack events, as opposed to the raw volume of log data or network traffic, more accurately represents actual attack counts. Without proper categorization of attack events, the disproportionately large volume of network reconnaissance traffic, false positives, authorized security scanning and large floods of DDoS monitored by Security Operations Centers (SOCs), would obscure the actual incidence of attacks. The inclusion of data from our SOCs and research and development centers provides a highly accurate representation of the ever-evolving global threat landscape.

Cybersecurity Advisory data

The Cybersecurity Advisory data used includes sanitized current and target state maturity levels analysed globally and covering multiple industries. The data is used to benchmark clients against their industry peers on a regional and global level. In our benchmarking data we consolidate all global assessments used to measure clients' maturity of processes, metrics and tools. The focus areas for the evaluation include Security Vision and Strategy; Information Security Framework; Risk Management; Operations; and Applications, Devices and Infrastructure.

NTT's WhiteHat Security

The application security data and analysis are provided by NTT's WhiteHat Security. This data is collected from our Dynamic Application Security Testing service and is sourced from testing running applications in production and pre-production environments.

NTT's global research

We commissioned Jigsaw Research to undertake 1,350 online interviews of technology and business decision-makers in large organizations in 15 sectors and 21 countries, including 1,046 IT and cybersecurity professionals.

How can we help you?

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