
NTT
INSIGHTS
DRIVEN BY DATA
Executive Guide to the 2020 Global Threat Intelligence Report
The nature of security:
Be resilient to thrive
Together we do great things
hello.global.ntt

The Executive Guide to the NTT Ltd. 2020 Global Threat Intelligence Report reminds us that the threat landscape is **continuously changing, especially during these tumultuous times.** In such a **dynamic environment,** and with absolute security as an impossible goal, businesses **must be ready for anything.**

To this end, our Guide recommends that businesses strive to be both **secure by design** and **cyber-resilient.** It's through finding the right **application and balance** of these two concepts that they can **truly minimize business risk.**

# Contents





 

# Foreword

**As the world unites and draws on all available resources to contain the global Coronavirus (COVID-19) pandemic, unfortunately, there will be those who'll try to take advantage of the crisis for nefarious purposes.**

As organizations continue to drive business practices through digital transformation, the challenges they face evolve as well. Cybercriminals are among this group. With large numbers of employees and students working from home, businesses are facing increasing risk of becoming victims of cybercrime. **Every organization should go the extra mile to protect their customers, partners and employees during these unprecedented and uncertain times.**

**NTT Ltd. provides solutions for challenges impacting clients across many industries globally.**

In our Executive Guide to the NTT Ltd. 2020 Global Threat Intelligence Report, we identify the unique challenges regions and industries face, and the operational, tactical and strategic considerations organizations should leverage to manage risk.

**Our Guide identifies modern and emerging trends observed across many industries and regions**. Armed with this knowledge, cybersecurity leaders will gain greater situational awareness allowing them to guide investments and support decisions to aid in improving their security posture.

Additionally, cybersecurity defenders should leverage this information to assess identified threats against their own risk profile and technology footprint to bolster targeted threat detection and response efforts.

Should you wish to find out more information or access deeper analysis of the findings of this Guide, read our full Report here.

**Mark Thomas**

**Global Head of Threat Intelligence, NTT Ltd.**

For the past 19 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 NTT Ltd Global Threat Intelligence Centre (GTIC) responsible for global threat research, communications and sharing alliances, and building intelligence-driven security services.

**Follow Mark on LinkedIn**

# Spotlight

## Coronavirus (COVID-19) is changing the way we do business

### COVID-19 is impacting the globe like no event has since World War 2. In this environment, organizations need to learn how to continue to operate while managing the wellbeing of their people, along with the changing demands of the market.

The **pandemic has brought its own cyberthreats** along with the actual virus. **Phishing attacks leveraging COVID-19 started in mid-January 2020**. Cyberattack types and volumes **escalate daily**, with attacks including:

- **websites posing as 'official' information sources**, but host exploit kits and/or malware – created at an incredible rate, sometimes **exceeding 2,000 new sites per day**
- **campaigns** which distribute Emotet, Trickbot, Lokibot, Kpot, CoronaVirus (a ransomware variant), Zeus Sphinx and **other malware variants**
- **attacks which spoof DNS, or hijack router DNS settings** via weak or default admin passwords
- the use of an open redirect which pushes Raccoon **information-stealing malware to the affected system, and prompts the user to download a 'COVID-19 Inform App' allegedly from the World Health Organization**
- **exploit attempts** against **a previously known remote code execution vulnerability** in Citrix Application Delivery Controller and Citrix Gateway devices
- **cyberattacks on healthcare and support organizations** responsible for helping people through this **health emergency**
- **organizations are relying more on their web presence at this time** (e.g. customer portals and supported web applications); this is increasing reliance on the very systems which **attackers have already been targeting**

**Phishing attacks leveraging COVID-19** started in mid-January 2020.



 

# 6 key insights

**We've identified six areas where the threat landscape has evolved significantly over the last 12 months**

Chameleons lack necessary internal defenses. They don't possess a poisonous bite and the majority move at an incredibly slow pace.

However, they've evolved some exceptional camouflage capabilities that protect them from predators. They can also change colour to send social signals or dynamically respond to their changing environment.

# 6 key insights

## 1 Threat actors are innovating

Attack volumes **increased across all industries** between 2018 and 2019. Due to the overwhelming success of the use of tools such as web shells, exploit kits and targeted ransomware, **adversaries are still developing effective multifunction attack tools and capabilities**.

The most common techniques observed globally were **remote code execution (15%)** and **injection (14%)** attacks. In most cases, these attacks continue to be effective due to organizations' **poor practices** related to network, operating system, and application configuration, testing, security controls and **overall security hygiene**.

**21%**

Adversaries are also leveraging **artificial intelligence and machine learning** and investing in the **automation** of attacks. Some **21%** of malware detected was in the form of a vulnerability scanner which also supports the premise that **automation is a key focus** point of attackers. In addition, adversaries are **taking advantage of the current COVID-19 pandemic by re-purposing their toolsets**, deploying new infrastructure and developing innovative campaigns to proactively target **vulnerable organizations**.

**Key highlights:**

- Threat actors are **innovating and evolving** their tradecraft.
- Globally, **21% of malware** detected was a form of vulnerability scanner.
- The **most common techniques** attempted worldwide are now remote code execution attacks.
- **Emotet banking trojan** has also undergone a series of stealth modifications.

**Emotet banking trojan** has undergone a series of stealth modifications.

## 2 Internet of Things (IoT) weaponization

Botnets such as Mirai and Echobot have **advanced in automation,** improving their propagation capabilities. Mirai and variants **targeted network backbone devices from several different vendors.** Mirai and IoTroop are well-known for **spreading through IoT attacks**, then propagating through scanning and subsequent infection from identified hosts.

Based on NTT Ltd.'s observations, **Mirai and IoTroop lead in malware detections** with more vulnerability scanning activity from these variants than any other family of malware. Many of these attacks are **directly related to activity from botnets like Mirai and IoTroop,** including the high levels of vulnerability scanning activity detected globally.

**Key highlights:**

- We've seen the re-emergence of IoT weaponization: IoT devices continue to be compromised.
- The re-surge of Mirai and derivatives has helped spread IoT attacks.
- IoTroop remains a persistent threat, making up 87% of all botnet detections in Japan.
- We've seen a spike in IoT attacks specifically in the Americas – a market that craves IoT but hasn't evolved to secure it effectively.
- There are many regulations governing the manufacturing subsectors, particularly manufacturing medical devices. In addition to medical device manufacturing, we expect to see a growing number of laws and regulations related to industrial IoT, which also influences this industry.

The **re-emergence of Mirai** and **derivatives** has helped **spread IoT attacks**.



 

## 3 Old vulnerabilities persistently remain an active target

As with previous years' Reports, **attackers are still focusing on leveraging vulnerabilities that are several years** old, have patches available, but are **still not being addressed** by organizations patch and configuration management programs.

When a device is introduced into an environment, a specific version of the software is installed and configured. Often, however, **businesses never patch the device or revisit the operating system version** for the duration of its lifetime. Very few businesses have **clear patch management policies.** Even those that do often **fail to implement policies** on their networking infrastructure consistently. As a result, we've observed **notable increases in the vulnerability of networks.**

**15%**

A total **of 258 new vulnerabilities** were identified in Apache frameworks and software over the last two years. Additionally, Apache software was the **third-most targeted** in 2019, accounting for over **15%** of all attacks observed.

**Key highlights:**

- Organizations **aren't following patch-management best practices.**
- This trend becomes particularly problematic in industrial environments, such as manufacturing plants and critical infrastructure production and distribution facilities.
- We've seen an **increase in threats and attacks** by cybercriminals in these industries as a result.

**Apache frameworks** experienced **258** new vulnerabilities defined in the past two years.

## 4 Content management systems (CMSs) are at risk

Malicious actors leverage **compromised web servers** to steal valuable data and use these powerful resources to conduct **additional cyberattacks**. Some of the most dominant activity during the past year was related to attacks against **popular CMS**, malware activity and web-application attacks. **Popular CMS platforms such as WordPress, Joomla!, Drupal, and noneCMS** account for about 70% of CMS market share.

**20%**

They are also the target of approximately **20% of all attacks globally**. Additionally, nearly **55%** of all attacks were application-specific **(33%) and web-application (22%) attacks.**

**Key highlights:**

- **Content management systems** (**CMSs) were heavily targeted** over the last year.
- **Almost 20%** of all attacks **targeted CMS platforms.**
- **Every region** included **two to four CMSs** in their top 15 targeted technologies.
- Interestingly, **Hong Kong didn't show any CMS** suites in their most-commonly attacked technologies.

**Almost 20%** of all attacks targeted **CMS platforms** (Joomla!, Drupal, 5nine, WordPress).

## 5 The evolution of governance, risk and compliance (GRC)

Authorities have gained a **greater understanding** of their role in holding businesses accountable for their use of personal data (i.e. information about people) and have demonstrated their commitment to **enforcing legislation** that protects individual rights.

In the last year, authorities in the European Union (EU) and the US, in particular, have issued **a number of fines** against businesses that have failed to act transparently, fairly, and responsibly in their **use of personal data.**

Global health emergencies like the **Coronavirus outbreak** do, and should, affect the way organizations manage security-related initiatives. **Health and safety** concerns over employees and the public **override many compliance initiatives** and should be taken into account when designing and implementing security controls, business continuity and disaster recovery plans.

**Complacency can lead to serious consequences** and put your business, employees, and customers at risk. Moving forward steadfastly and **continuing to make the appropriate investments** is critical.

**Key highlights:**

- 2019 was a year of enforcement … but GRC is becoming more **complex and challenging** to navigate.
- Encouragingly, we're seeing **more data privacy professionals** driving the business agenda.
- Compliance and **complacency** don't mix.
- New regulations are being implemented or are coming soon; to name a few:
  - California Consumer Privacy Act
  - Brazilian General Data Protection Law
  - India's Personal Data Protection Bill
  - Singapore Personal Data Protection Act
  - South Africa's Protection of Personal Information Act

The regulatory landscape is **constantly changing**.

## 6 Shift in sector targeting

**The technology and government sectors** have now moved into the unenviable position of being the **most targeted industries globally**.

Technology was the most attacked industry in 2019 accounting for 25% of all attacks, compared to 17% last year.

Attacks on the **government sector have been driven by geo-political activity,** and now represent 6% of all attacks, **compared to 9% last year**.

The **technology sector experienced the highest rate of ransomware of any industry: 9%** of all threat detections were ransomware; **no other industry showed detections for this malware category above 4%**.

The **WannaCry ransomware** was the most-commonly detected variant, **accounting for 88% of all ransomware detections**

The **OpenSSL vulnerability CVE-2017-3731 and the Joomla! CMS vulnerability** CVE-2015-8562 accounted **for 99% of targeting**. Some **23% of detected malware** belonged to the Remote Access Trojan **(RAT) malware family**.

When it comes to applications, the technology sector has the **lowest performance of all** industries with an average of **over 12 serious vulnerabilities per site**.

The technology sector also has the most **diverse set of applications** from a **diverse set of organizations**.

**Key highlights:**

- The technology and government sectors now **most targeted globally.**
- **Technology was the most attacked industry in 2019 accounting for 25%** of all attacks, compared to **17% last year**.
- Attacks on the **government sector have been driven by geo-political activity**, and now represent 6% of all attacks, **compared to 9% last year.**

**Technology and government** now the most targeted.



 

# Global and regional insights

A species thought to be over 310-320 million years old, reptiles possess a hardy exterior. Found on every continent, they have a talent for adapting to even the harshest environments.

From the first amphibian emerging from the water, to the giant Tyrannosaurus Rex stalking the earth in the Mesozoic era, and the household pet lizard, reptiles could singularly define evolutionary success.

# Global analysis

## Industry preparedness

The data used within this report includes sanitized current and target state maturity levels analysed globally covering multiple industries. The data is used to **benchmark clients against their industry peers on a regional and global level.** The focus areas for the evaluation include security vision and strategy, information security framework, risk management, operations, applications, devices and infrastructure.

We evaluate current versus future maturity levels based on an organization's **processes, metrics, and tools.** These maturity levels are identified as **Non-existent, Initial, Repeatable, Defined, Managed and Optimized.**

| Level of Maturity | Non-existent | Initial | Repeatable | Defined | Managed | Optimized |
|---|---|---|---|---|---|---|
| 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 |

### Benchmark score by industry

| Industry | 2019 Baseline | 2018 Baseline |
|---|---|---|
| Technology ↓ | 1.64 | 1.66 |
| Finance ↑ | 1.86 | 1.71 |
| Business and Professional Services ↑ | 1.54 | 1.31 |
| Education ↓ | 1.02 | 1.21 |
| Manufacturing ↓ | 1.32 | 1.45 |
| Healthcare ↑ | 1.12 | 1.03 |

*Figure 1: Benchmark score by industry*

Figure 1 shows comparisons between 2018 and 2019's benchmark scoring using the Cybersecurity Advisory Service. Overall **baseline scores have not progressed appreciably** in the past year, but individual industries do show some **small variations.**

Small decreases in baseline scores are likely a result of **poor prioritization** which may indicate misallocated resources and potentially interferes with **security's ability to deliver** for the business.

Small increases in the baseline tend to be related to **improvements in visibility and strategy.**



 

Figure 2 below illustrates the **gap between the current versus the desired state** of several industries. The difference between current and target state is one **driven by aspiration**, not necessarily where they need to be. Many business drivers, including cost, compliance and resources all factors which may result in **achieving less** than the desired goals. In order to close the gap, each of these industries must ensure a **constant focus is placed on:**

- maturity of processes
- tools
- executive support

### Maturity level gap

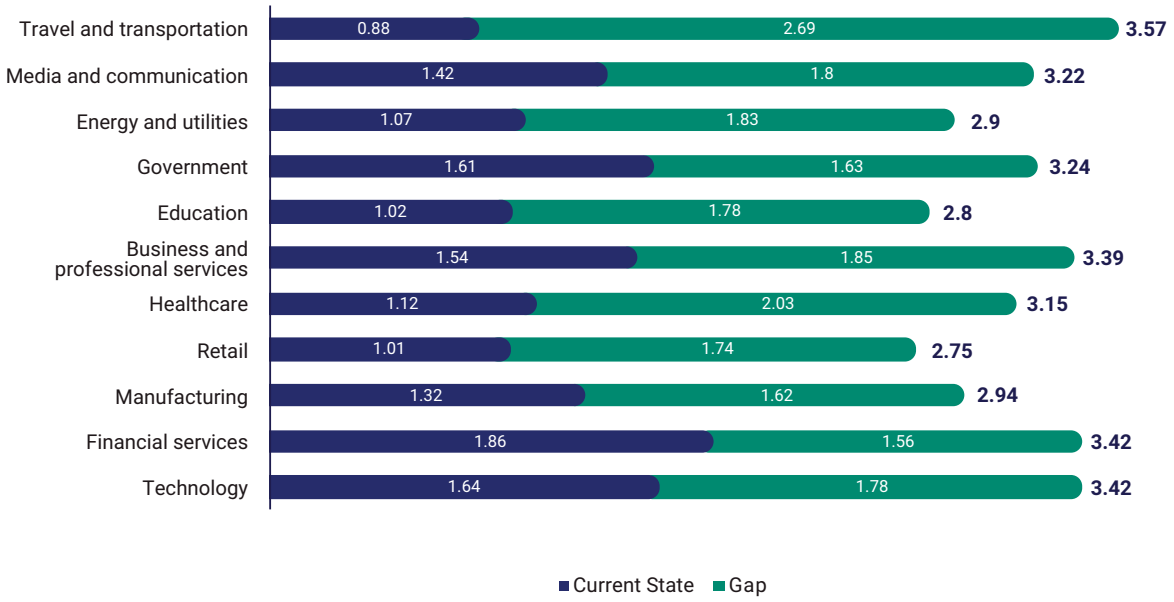


*Figure 2: Maturity level gap*

## What are the most high-risk vulnerabilities?

Botnets such as Mirai and Echobot have **advanced in automation,** improving their propagation capabilities. They target network backbone devices from **several different vendors.** Mirai and IoTroop are known for spreading through the Internet of Things (IoT) attacks, then propagating throughout an organization's infrastructure.

Globally, organizations continue to experience high levels of **malicious scanning** focused on identifying Shellshock (CVE-2014-6271) vulnerabilities.

Nearly **55% of all attacks were application-specific attacks (33%)** and **web-application attacks (22%).**

Botnets are comprised of multiple infected internet-connected devices used to carry out coordinated actions, such as sending spam or conducting distributed denial-of-service attacks. **Mirai, Echobot, and IoTroop are examples of botnets.**

## Which are the most targeted technologies?

Continued attacks against certain vulnerabilities help make **OpenSSL the second-most targeted software technology** with 19% of hostile activity globally.

As shown in Figure 3, **OpenSSL was often the first- or second-most targeted technology.** OpenSSL was also the most targeted technology in both the **manufacturing and technology** industries.

### Attacks targeting SSL by region

| Attacks targeting SSL by region | | |
|---|---|---|
| **Grouping** | **Targeted technology rank** | **2019 baseline** |
| Global | #2 | 19% |
| Americas | #2 | 10% |
| United Kingdom | #2 | 20% |
| Hong Kong | #1 | 67% |
| Australia | #2 | 21% |

*Figure 3: Attacks targeting SSL by region*

Apache products like **Struts, Tomcat and others experienced 258 new vulnerabilities** defined in the past two years. Apache software implementations were the third-most targeted during 2019, accounting for over 15% of all attacks observed.

Additionally, attacks against Apache solutions were in **the top seven vulnerabilities** targeted in each industry, and **the top five** in each country analysed.

Attacks **targeting CMS platforms** were also significant in this year's analysis **(20% of all attacks globally).** Additionally, **every region** included two to four CMSs in their **top-15 targeted technologies,** and most countries included either Joomla! or WordPress in their **top five.**

**Application-specific attacks** target vulnerabilitie 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.

## 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 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:** 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.
- **Service-specific attacks:** attacks directed at services which often don't require authentication; they're most frequently observed in exploit attempts against common services, but often target databases and remote access services.

## Industry highlights

The **top-five targeted** industries have been heavily **targeted in previous years.** Attacks against the web presence of organizations in these industries are common, as attackers attempt to either **compromise public-facing applications,** or compromise the **underlying systems** supporting web services.

**Technology** remained at the top of the list of most-attacked industries **(25%), compared to 17%** in 2018.

Attacks on the **finance sector** dipped slightly **(15% in 209 compared to 17% in 2019)**

**Government jumped into second place**, up from **9% in 2018 to 16% in 2018**.

Organizations view **vendor, supplier or customer portals** and external access as required services, and attackers are taking advantage of this, regardless of the industry.

**Application-specific attacks or web-application attacks were the most common** attack type in **all five of the top attacked industries**.

### Industry comparisons

| Industry | 2019 Rank | 2019 % | 2018 Rank | 2018 % |
|---|---|---|---|---|
| Technology | 1 | 25% | 2 | 17% |
| Government | 2 | 16% | 5 | 9% |
| Finance | 3 | 15% | 1 | 17% |
| Business and Professional Services | 4 | 12% | 3 | 12% |
| Education | 5 | 9% | 4 | 11% |

*Figure 4: Industry comparisons*



 

# Americas (AM)

**The re-emergence of Mirai and derivatives has helped spread the Internet of Things (IoT) attacks in a market that craves IoT but has not evolved to secure it effectively. News organizations report breach after breach, making breaches resemble the new norm.**

- Attackers have directed attacks towards **small and medium-sized businesses,** and effectively spread ransomware into state and local governments.
- The Americas was dominated by **reconnaissance** activity likely for the same reason it affected global attacks; the automation of scanning in common malware like Mirai, Echobot, IoTroop, and derivatives.
- Reconnaissance activity was followed by **application-specific and web-application attacks**.
- Joomla! was targeted more than any other application, **accounting for 45% of all attacks.**
- The **most common type of malware in the Americas was the webshell family.** China Chopper accounted for **54%** of all webshell activity and was **the second-most** detected malware.
- The **single most detected malware in the Americas was WannaCry ransomware**.

### Americas – industry details

| Top targeted industries | Top attack types |
|---|---|
| Business and Professional Services – 41% | Application Specific – 36%<br>Reconnaissance – 32%<br>Web Application – 16% |
| Manufacturing – 20% | Application Specific – 25%<br>Reconnaissance – 20%<br>Web Application – 13% |
| Technology – 17% | Network Manipulation – 48%<br>Brute Forcing – 17%<br>Reconnaissance – 16% |
| Finance – 15% | Reconnaissance – 29%<br>Network Manipulation – 19%<br>Web Application – 19% |
| Telecommunications – 6% | Reconnaissance – 92%<br>Application Specific – 2%<br>Web Application – 2% |

*Figure 5: Americas – industry details*

The most-attacked industry in the countries analysed was **business and professional services (41%)** followed by manufacturing **(20%)**, technology **(17%)**, and finance (15%).

The most detected malware was the **WannaCry ransomware; China Chopper was second.** Germany **(18% of malware as ransomware)** and the UK **(12%),** were the only countries that showed a higher percentage of ransomware than the US **(10%)**.

### Americas most common malware

| Most common malware in the americas | Malware type |
|---|---|
| WannaCry | Ransomware |
| China Chopper | Webshell |
| jsp | Remote Access Trojan |
| Ramnit | Trojan |
| Virut | Botnet |
| zmeu | Vulnerability Scanner |
| muieblackcat | Vulnerability Scanner |

*Figure 6: Americas most common malware*

# Asia Pacific (APAC)

**The APAC region showed significant activity related to the technology and manufacturing industries – the design, development, and manufacturing of technical components and products. Tension in the region can impact operations and have an impact on the priority and attention provided for cybersecurity.**

- **Attacks in APAC were very different to those in other regions**. While the **second most attacked technology in Japan was Joomla!,** Hong Kong didn't show any content management systems (CMS) suites in their most-commonly attacked technologies.
- **DoS/DDoS attacks** were more common than in other regions, regularly appearing in the top five common attack types (Singapore #4, and Japan #5).
- Web-application and application-specific attacks **dominated the region.** They were the two most common attack types and application-specific attacks were the most-common attack types in Singapore and Hong Kong.
- Attacks in Japan **included three CMS platforms in the eight most targeted technologies. Joomla!** was the most highly targeted CMS in every country analysed.
- **IoTroop** made up **87%** of all botnet detections in Japan. Botnet activity, accounting for **32%**, was the most common form of malware activity detected in Japan.

### APAC industry details

| Country | Top targeted industries | Top attack types |
|---|---|---|
| Japan | Technology – 29%<br>Manufacturing – 25%<br>Transport and Distribution – 13% | Web Application – 36%<br>Application Specific – 23%<br>Brute Forcing – 22% |
| Singapore | Government – 38%<br>Education – 29%<br>Finance – 15% | Application Specific – 32%<br>Brute Forcing – 21%<br>Reconnaissance – 19% |
| Hong Kong | Manufacturing – 46%<br>Technology – 25%<br>Business and Professional Services – 23% | Application Specific – 46%<br>Service Specific – 18%<br>Reconnaissance – 17% |

*Figure 7: APAC industry details*

As depicted in Figure 7, **technology** was regularly among the most-attacked industry in many countries. Attacks against **government, finance and education** also appeared with some regularity.

**Conficker and IoTroop** were the most commonly detected malware in APAC.

### Most common malware APAC

| Most common malware in APAC | Malware Type | Japan | Singapore | Hong Kong |
|---|---|---|---|---|
| Conficker | Worm | X | X | X |
| IoTroop | Botnet | X | | X |
| zmeu | Vulnerability Scanner | X | | |
| muieblackcat | Vulnerability Scanner | X | | |
| gh0st | Remote Access Trojan | X | X | |
| jsp | Remote Access Trojan | X | X | |
| China Chopper | Webshell | X | | |
| pmabot | Trojan | | X | |

*Figure 8: Most common malware APAC*



 

# Australia

**Australia showed significant activity related to the technology and government industries – those that are responsible for the design, development and manufacturing of technical components and products, as well as bodies responsible for providing government services to the public. A generally mature cybersecurity profile did not stop Australia from being affected by hostile cyberactivity.**

- **The most highly attacked industries in Australia were technology (35%) and government (26%). These two industries accounted for nearly 61% of all attacks in Australia**.
- The most-commonly attacked technology included **targeting of Netis/Netcore and related routers.** A significant amount of these attacks likely came from **automation** of attacks and inclusion in Mirai, IoTroop and derivatives; exploit kits; and other tools.
- **Conficker was the single most-common malware,** accounting for **14%** of all malware detections.
- **Application-specific (40%) and web-application (20%)** attacks **dominated Australia**, accounting for nearly 60% of all attacks combined. This was **above the global average of 55%.**

## Australia industry details

| Country | Top targeted industries | Top attack types |
|---|---|---|
| Australia | Technology – 35%<br>Government – 26%<br>Finance – 13%<br>Education – 11%<br>Business and Professional Services – 8%<br>Retail – 6% | Application Specific – 40%<br>Web Application – 20%<br>DoS/DDoS – 19% |

*Figure 9: Australia industry details*

As depicted in Figure 9, organizations in **technology and government** were regularly targeted. Like many countries in the Australia region, attacks against **finance and education** also appeared with some regularity.

The Conficker worm, zmeu scanner and China Chopper webshell were the most commonly detected malware in Australia.

> The most highly attacked industries in Australia were **technology (35%)** and **government (26%)**. These two industries accounted for nearly 61% of all attacks in Australia.

## Most common malware in Australia

| Most common malware | Percentage(%) |
|---|---|
| conficker | 14% |
| zmeu | 14% |
| chinachopper | 11% |
| jsp | 11% |
| cknife | 9% |
| muieblackcat | 6% |
| gh0st | 5% |
| jexboss | 5% |
| pmabot | 5% |

*Figure 10: Most common malware in Australia*

# Europe, Middle East & Africa (EMEA)

**Events in Europe, Middle East & Africa (EMEA) were affected by the requirements to meet Global Data Protection Regulation (GDPR) compliance. As is the case with any significant compliance activity, GDPR initiatives helped reinforce maturing security programs, but in some cases, distracted organizations from advancing their efforts.**

- Hostile activity in EMEA **resembled those of other regions** with notably high levels of web-application attacks, application-specific attacks, and a variety of reconnaissance activity.
- Denial of Service (DoS) and brute-force attacks **spiked in some industries** and countries, but overall resembled those observed globally.
- **Reconnaissance activity** was the most common form of activity in EMEA, often accounting for more than **40%** of observations. Reconnaissance was pronounced in **Sweden (67%), the UK (50%), Benelux (50%), and Germany (47%).**
- **Content management systems (CMSs) were common attack vectors in EMEA,** with several countries including multiple CMSs in their list of technologies most commonly attacked.
- While targeted industries varied by country, the most commonly attacked industries in EMEA were **finance, business and professional services, technology, manufacturing and retail.**

## EMEA industry details

| Country | Top targeted industries | Top attack types |
|---|---|---|
| United Kingdom and Ireland | Manufacturing – 29%<br>Technology – 19%<br>Business and Professional Services – 17% | Reconnaissance – 50%<br>Web Application – 22%<br>Brute Forcing – 12% |
| Sweden | Pharmaceuticals – 62%<br>Finance – 22%<br>Telecommunications – 12% | Reconnaissance – 67%<br>Application Specific – 12%<br>Brute Forcing – 11% |
| Germany | Technology – 51%<br>Manufacturing – 21%<br>Finance – 11% | Reconnaissance – 47%<br>Service Specific – 13%<br>Application Specific – 13% |
| Norway | Business and Professional Services – 45%<br>Retail – 19%<br>Transport and Distribution – 15% | Application Specific – 36%<br>Web Application – 29%<br>DoS/DDoS – 16% |
| Benelux | Technology – 33%<br>Transport and Distribution – 31%<br>Manufacturing – 22% | Reconnaissance – 50%<br>Application Specific – 18%<br>Web Application – 15% |
| South Africa | Insurance – 50%<br>Finance – 44%<br>Retail – 3% | Web Application – 66%<br>Application Specific – 27%<br>DoS/DDoS – 4% |

*Figure 11: EMEA industry etails*

**40%** Reconnaissance activity was the most common form of activity in EMEA, often accounting for more than 40% of observations.

Similar to the global analysis, vulnerability scanners, testing tools and malware appeared in the top-five most common malware and attacker tools in EMEA.

## Most common malware in EMEA

| Most common malware in EMEA | Malware type |
|---|---|
| Pmabot | Trojan Horse |
| IoTroop | Botnet |
| Sqlmap | Vulnerability Scanner |
| Nmap | Vulnerability Scanner |
| muieblackcat | Vulnerability Scanner |

*Figure 12: Most common malware in EMEA*



 

# Recommendations

Hummingbirds are amongst the fastest and most agile species in nature.

They are the only genus of bird that can sustain long-term hovering – and even fly upside down when required. They've developed a long bill in order to extract nectar with precision. And when resources are scarce, they can enter near-hibernation – known as torpor – to protect their reserves.

# Recommendations

**Constant pressures in the market, the spread of Coronavirus (COVID-19) and the need to deliver consistent, reliable services require much more than having the ability to recover from disruptions.**

Cyberattacks can take weeks, if not years, **to recover from**, which is a key reason why organizations must have the ability to **anticipate and prevent disruptions.** Successful organizations account for **all aspects** of business operations, technology, people and controls to actively manage disruptive events – **before the event impacts regular operations.**

Based on our observations related to current and emerging threats, we believe businesses should focus their efforts on the following areas:

## Ensure your cybersecurity is resilient as the threat landscape changes

- **Organizations need to ensure they're addressing the challenges as the threat landscape evolves with COVID-19 being a good example of how things can change fast.** The pandemic has brought about fundamental changes to businesses. Organizations must support their employees in this **potentially chaotic environment.** They must also continue to meet appropriate **regulatory** obligations, maintaining customer/patient security from both a physical and data perspective. To do this effectively organizations must:
  - clearly, effectively and regularly **communicate** changing business and security requirements, policies and procedures
  - ensure employees **flag roadblocks** to effective collaboration and workflow

## Implement infrastructure, applications and operations that are secure by design

- This means including security as a key and conscious deciding factor in the approach to designing end-to-end business solutions.
- This will result in a cyber-resilient solution and enable businesses to better cope with unprecedented and unexcepted events such as the COVID-19 outbreak.

## Leverage intelligent cybersecurity

- This will enhance support business agility and help maintain an acceptable risk level for the organization.
- Leverage proactive threat intelligence capabilities to identify and rapidly make decisions to manage risk.

## Ensure your organization has proper visibility across the information and communication technology environment

- A vital part of being able to manage risk and mitigate threats is having proper real-time visibility into activities happening within the ICT environment so rapid decisions can be made on how to best address the threat.

## Conduct regular penetration testing activities

- These should include application testing and social engineering. Leverage intelligence services to help add a realistic approach from an attacker's perspective.

## Governance, risk and compliance must be part of your organization's regular agenda

- Conduct regular technical and non-technical assessments to identify potential weak areas of your program.

Above all, remember that the **true purpose** of cybersecurity controls within an organization is to **enable that organization to meet its operational goals in a safe, secure and resilient manner**.

Cyberattacks can take weeks, if not years, **to recover from**, which is a key reason why organizations must have the ability **to anticipate and prevent disruptions**. Successful organizations account for **all aspects** of business operations, technology, people and controls to actively manage disruptive events – **before the event impacts regular operations**.



 

## NTT Ltd. global data analysis methodology and resource information

This Guide contains global attack data gathered from NTT Ltd. and supported operating companies **from October 1, 2018 to September 31, 2019.** The analysis is based on log, event, attack, incident and vulnerability data from clients. 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.

NTT Ltd. **gathers security log, alert, event, and attack information** from which it enriches and analyses contextualized data. This process enables **real-time global threat intelligence** and alerting. The size and diversity of our client base, with **over 4,000 security clients** on six continents, provides NTT Ltd. 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 the **10 SOCs and seven research and development centers** of NTT Ltd. provides a highly accurate representation of the ever-evolving global threat landscape.

The **Cybersecurity Advisory data** used within this report includes sanitized current and target state maturity levels analysed globally **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 over 150 assessments** used to measure clients in terms of the maturity of processes, metrics, and tools. The **focus areas** for the evaluation include:

- security vision and strategy
- information security framework
- risk management
- operations
- applications
- devices
- infrastructure

The application security data and analysis are provided by **WhiteHat Security.** This data is collected from our **Dynamic Application Security Testing Service.**

## Global Threat Intelligence Center

The NTT Ltd. Global Threat Intelligence Center (GTIC) **protects, informs and educates** NTT Ltd clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to clients

The GTIC goes above and beyond the **traditional pure research organization**, by taking their threat and vulnerability research and combining it with their detective technologies development to produce **applied threat intelligence.** The GTIC's mission is to **protect clients** by providing advanced threat research and security intelligence to enable NTT Ltd. to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining an understanding of, and insight into the **various threat actors,** exploit tools and malware – and the **techniques, tactics and procedures** used by attackers.

Vulnerability research pre-emptively **uncovers zero-day vulnerabilities** which are likely to The GTIC continually monitors the global threat landscape for **new and emerging threats** using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to **understand, analyse and enrich** those threats using advanced analysis techniques and proprietary tools; and curates and publishes them using the **Global Threat Intelligence Platform**.

## NTT-CERT

NTT-CERT, a division of NTT Secure Platform Laboratories, serves as a **trusted point of contact for Computer Security Incident Response Team specialists** and provides full range CSIRT services within NTT. NTT-CERT **generates original intelligence** regarding cybersecurity threats, helping to enhance our capabilities in the security services and secure network services fields.

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

**How can we help you?**

**Get in touch** with us today for a **Cybersecurity Advisory 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.


**Together we do great things**