dimension data

accelerate your ambition

NTT Security 2018 Global Threat Intelligence Report

Executive Guide

Cybersecurity insights for protecting your digital business

Insights
Driven by data

Contents

1. Foreword

In 2017, the World Economic Forum rated cybersecurity as one of the top risks facing the world today. Independently, business leaders reprioritised cybersecurity as a strategic initiative demanding further focus and investment. It remained top of mind and garnered significant media attention, as cybercriminals showed how easy it is to disrupt digital business while continuing to adapt their tradecraft to target specific business, industry, and geographic profiles.

Once again, finance was the most attacked sector. Business and professional services is a new entrant to the top five most attacked industry sectors globally.

Attractive and lucrative in its ability to generate profits with minimal risk of attribution or interdiction, cybercrime is a pervasive threat. Diversification of illicit subscription services, automated software toolkits, and vast online criminal support forums are reducing barriers to entry. Cybercriminal ingenuity continues to mature, making the most of attack opportunities arising from new technology adoption.

The relentless evolution of the threat landscape places the onus on businesses to innovate more rapidly than their adversaries. Cyber-awareness from the top down is imperative if the business, clients, and employees are to be protected.

Also, protecting a network from compromise upfront is far less costly than dealing with post-event financial repercussions, reputational damage, legal ramifications, regulatory penalties, and breach recovery costs.

In this Executive's Guide to the NTT Security 2018 Global Threat Intelligence Report we highlight findings that will help you make investment decisions aligned with your industry sector, geographic profile, and risk appetite.

As part of NTT Group, we have extensive visibility into global traffic and threats faced by thousands of clients across many industries. Our security experts analyse millions of attacks each year using data gathered by our global security operations centres and research facilities.

In addition, the findings in this Executive's Guide are based on the analysis of data from 18 industry sectors, conducted by NTT Security's Global Threat Intelligence Center. They include the most frequently targeted sectors spanning Europe, Middle East & Africa (EMEA), the Americas, Asia Pacific (APAC), and Australia.

This Guide also looks into the future, covering emerging trends such as ransomware, threat intelligence, industry targeting, and compliance regulations.

For Dimension Data, cybersecurity is at the centre of what we do, how we think, and how we accelerate our clients' ambitions. We urge you to consider security's enabling role in meeting mission-critical objectives and driving sustainable business value, providing the certainty needed in an otherwise disruptive world.

NTT Security

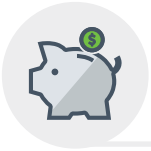
Mark Thomas

Group CTO Cybersecurity, Dimension Data

For the past 16 years, Mark has worked in the cybersecurity field, establishing pragmatic, business-aligned risk minimisation strategies and developing intelligence-led computer network defences. His broad knowledge and in-depth expertise result from extensive engagements in Consulting, Technical, and Managed Services with large enterprises across numerous industry sectors including finance, government, utilities, retail, and education.

2. Eight key insights into the global cybersecurity landscape

The cyberworld continues to expand, converging information and operational technology (IT and OT), industrial controls (ICS), and the Internet of Things (IoT) into an ever-evolving technology ecosystem across hybrid infrastructures: on-premise, cloud, and mobile.



1. Finance tops 'most targeted sector' list

Fast-paced adoption of disruptive technologies and expanding digital footprints motivate adversaries to routinely conduct automated reconnaissance to uncover potential infrastructure and application vulnerabilities. **Rising technology adoption places this sector at elevated risk**.

Adequate response demands focus **on patch and vulnerability management, advanced endpoint protection, and identity-driven controls.**

2. Supply chain risks catch digital businesses off-guard

Cybercriminals prioritise the supply chain. As business ecosystems grow, and data and applications migrate to hybrid environments, they expand adversaries' options for compromising business through indirect means.

For this reason, the business and professional services sector is one of the top five attacked sectors globally, ranking third overall. **It's a prime target for trade secrets and intellectual property theft, potentially exposing customer and business partner data or credentials**.

This emphasises the need for **third-party supply chain risk management, adoption of best practice standards, risk frameworks, and assurance practices.**

3. Ransomware: the cybercriminals' weapon of choice

Globally increasing by 350% in 2017, ransomware represents 7% of total malware – up from 1% last year. Many organisations fell victim to financially motivated crime via ongoing outbreaks, attracting significant media attention. **Leaked classified government hacking tools have made ransomware even more dangerous**, enabling greater attack and tooling sophistication. The persistence and relentlessness of cyber-adversary campaigns indicate that ransomware popularity and prevalence will continue.

Rethink your approach **to backup and recovery to avoid the risks of ransomware.**

4. Ransomware morphs to become destructive

As ransomware evolves, cybercriminals use social engineering as a core technique to search for exploitable vulnerabilities, with destructive malware masquerading as ransomware. Adversary campaigns have expanded into the supply chain. **Widespread infection by the NotPetya virus was the first observed destructive malware masquerading as ransomware**.

Encourage employees to be suspicious **of received emails, particularly those asking them to open attached documents or click on weblinks.**

5. Technology sector targeted for IP

The technology sector's significant intellectual property is a prime target for competitive advantage, making the sector the second most attacked, globally. It's in the top five across all regions, signalling a shift in adversary intentions.

The sector tends to accept more risk in pursuit of greater innovation, open collaboration, and business opportunities created by being first-to-market. This inherently exposes infrastructure to vulnerability. Failure to embed cybersecurity in organisational culture and business processes will impact productivity and business profitability.

Prioritise investment in network security policies and technology controls **to support risk reductions.**

6. Manufacturing and operational technology in line of fire

Manufacturing ranks fourth for attacked sectors globally. **The line between traditional and digital forms of manufacturing has begun to blur, creating a unique landscape where high-value manufacturing and advanced technologies are key for global competitiveness**.

Once isolated systems are now converging via OT, IOT, cloud computing, and data sharing expanding into supply chains and other business ecosystems. The attack surface has widened. Smart factor cyber-physical systems are exposed to greater risk. The sector is at high risk of intellectual property and trade secrets theft, sabotage of processes and output, extortion and disruption of computing resources.

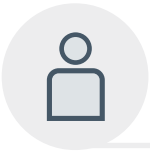
Identify threats and risks **across multifaceted, distributed architectures, including on-premise, cloud, and hybrid environments. Ensure that your detection and incident response capabilities are robust.**

7. The balance between compliance and cybersecurity remains challenging

With standards groups, industries, and governments constantly implementing new and revised policies, many organisations struggle to achieve an optimal balance between operational security and compliance.

Compliance pressure grew with the introduction in 2017 of the General Data Protection Regulation (GDPR) in EMEA and the Notifiable Data Breach (NDB) scheme In Australia in 2018. **Companies must notify individuals whose personal information is involved in a data breach that's likely to result in serious harm**.

Embrace compliance **without detriment to other security initiatives. Falling behind on patch management or regular backups can undermine compliance.**



8. Improved user awareness drives incident response maturity

Ransomware-related incident response outsourced engagements dropped sharply from 22% in 2016 to 5% in 2017, despite accelerated ransomware infection rates globally.

Organisations have improved their in-house ability to prevent and respond to attacks through continued investments in endpoint controls, incident response playbooks, and backup and recovery plans.

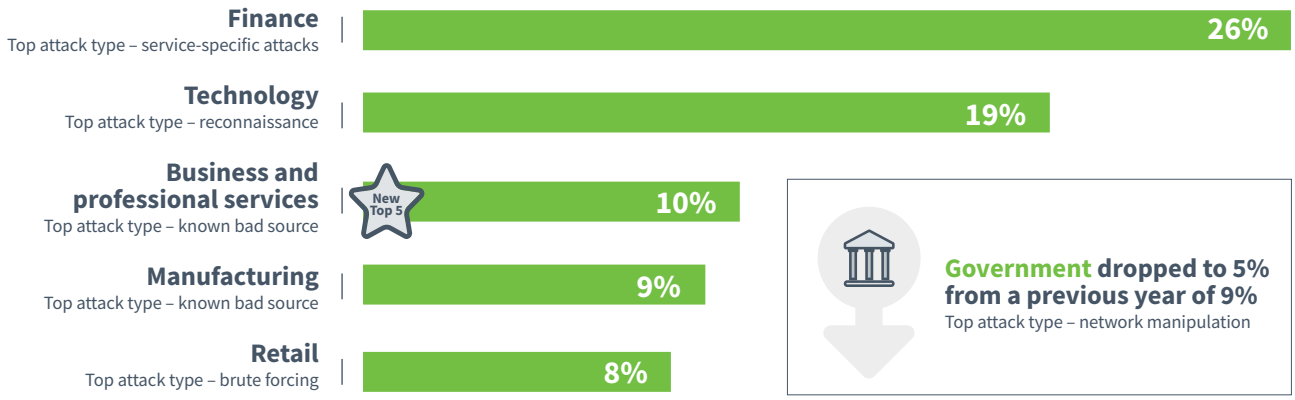
Establish a predictive environment with a disaster recovery plan **that allows you to identify and isolate uncompromised critical data and ensure complete recovery.**

3. Sectors most at risk

Significant changes in the topmost attacked industries

- **Finance regained its position as the most targeted sector**, with 26% of all attacks. This was driven by a decline in attacks targeting other sectors, such as government.
- **The technology sector** experienced a significant 19% attack volume, an increase of 25% over the previous year. Threat actors are lured by the opportunities to target proprietary information, trade secrets, and personal financial data. Often, stolen data is illegally traded in dark markets and used to bribe or blackmail victims. The sector was also characterised by more reconnaissance activity (18%) and known bad sources (16%). Reconnaissance activity isn't necessarily hostile, though it's often a precursor to more hostile attacks. Activity from known bad sources is also not necessarily hostile, but is identified as activity from sites which are previously known to be associated with hostile activity.
- **Business and professional services** moved from the sixth to the third most targeted sector globally (10%). In our modern, independent services economy, outsourcing of business and professional services is common. This practice broadens the attack surface and opportunities available to attackers.
- **Manufacturing among the top five attacked industry sectors in four regions**, signalling a strategic shift in adversary interest motivated by cybercrime and corporate espionage. Attacks in this sector are providing the impetus to increase investment in anomaly detection capabilities and enhanced endpoint as well as identity-driven controls to support improved authentication and access.
- **Finance and healthcare** were the most likely sectors to seek outsourced assistance for incident response services.

Figure 1: Global industry attack rankings

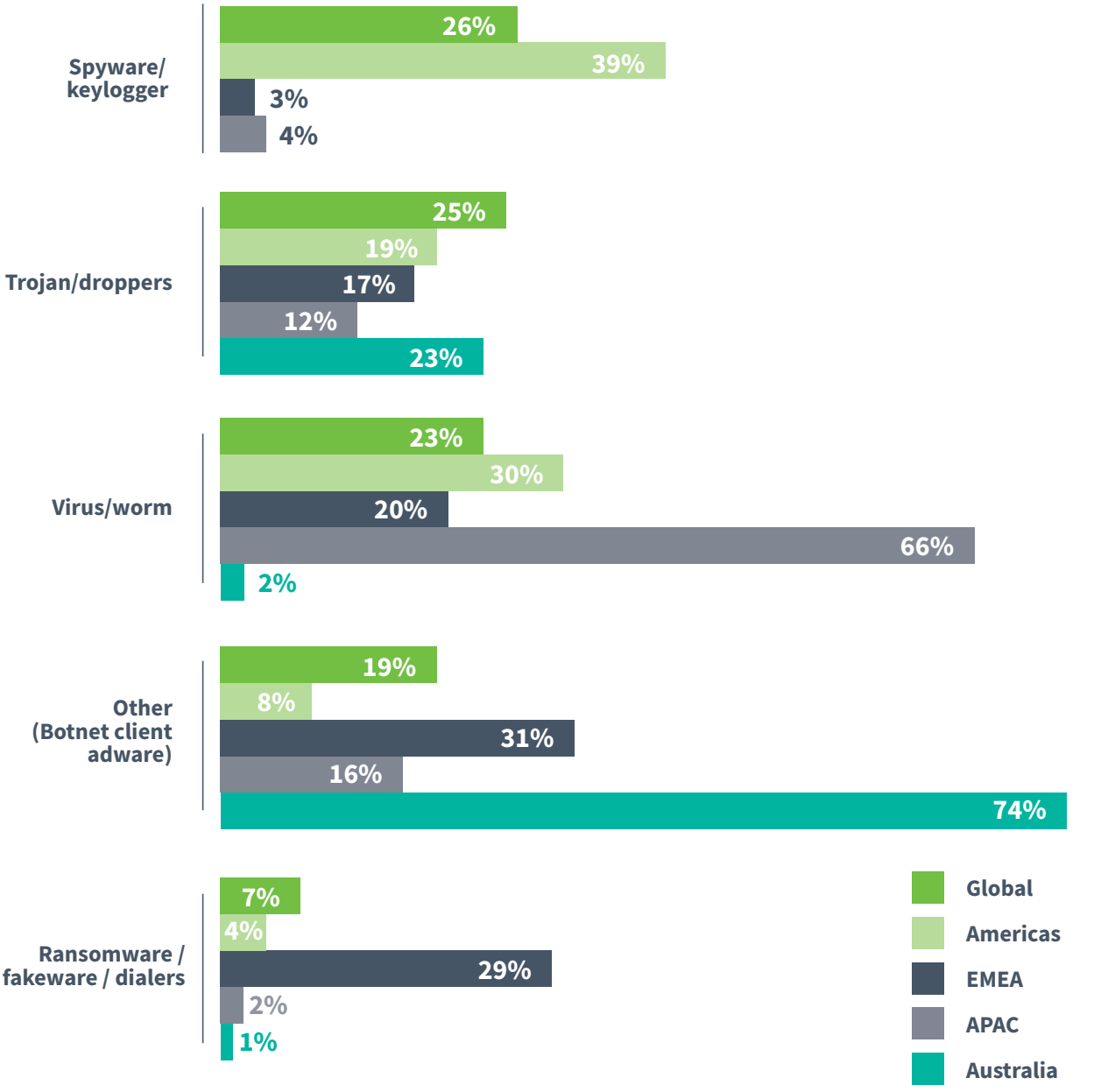


4. Common attack types

Spyware/key loggers and Trojans/droppers were the most common malware types:

- **Spyware/key loggers** ranked first in volume of malware, at 26%.
- **Trojans/droppers** ranked second globally at 25%.
- **Virus/worms** were the third most common form of malware, at 23%.

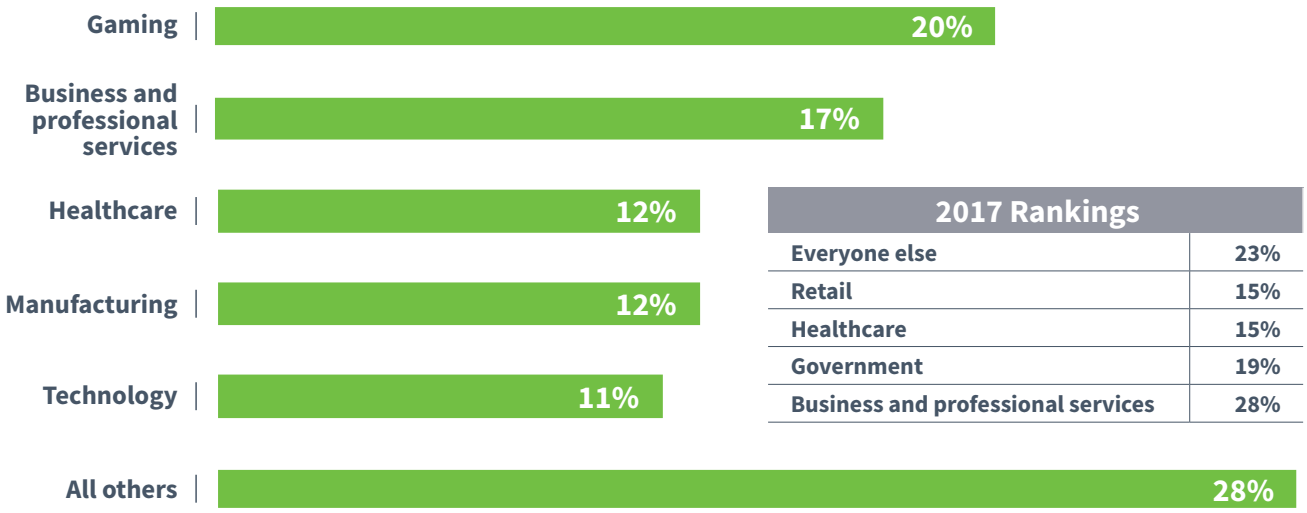
Figure 2: Top malware by region



Ransomware up by a staggering 350%:

- Ransomware volumes increased by 350% in 2017, rising from less than 1% of global malware in 2016, to nearly 7%.
- Ransomware targeted mainly the gaming, business and professional services, and healthcare industry sectors.
- Globally, 75% of ransomware detected was **Locky** (45%) or **WannaCry** (30%).
- Ransomware-related incident response engagements dropped, however, from 22% in 2016 to 5% in 2017. This indicates improved adoption of advanced endpoint controls enabled by machine-learning and maturing incident response capabilities such as playbooks and simulated table-top exercises.

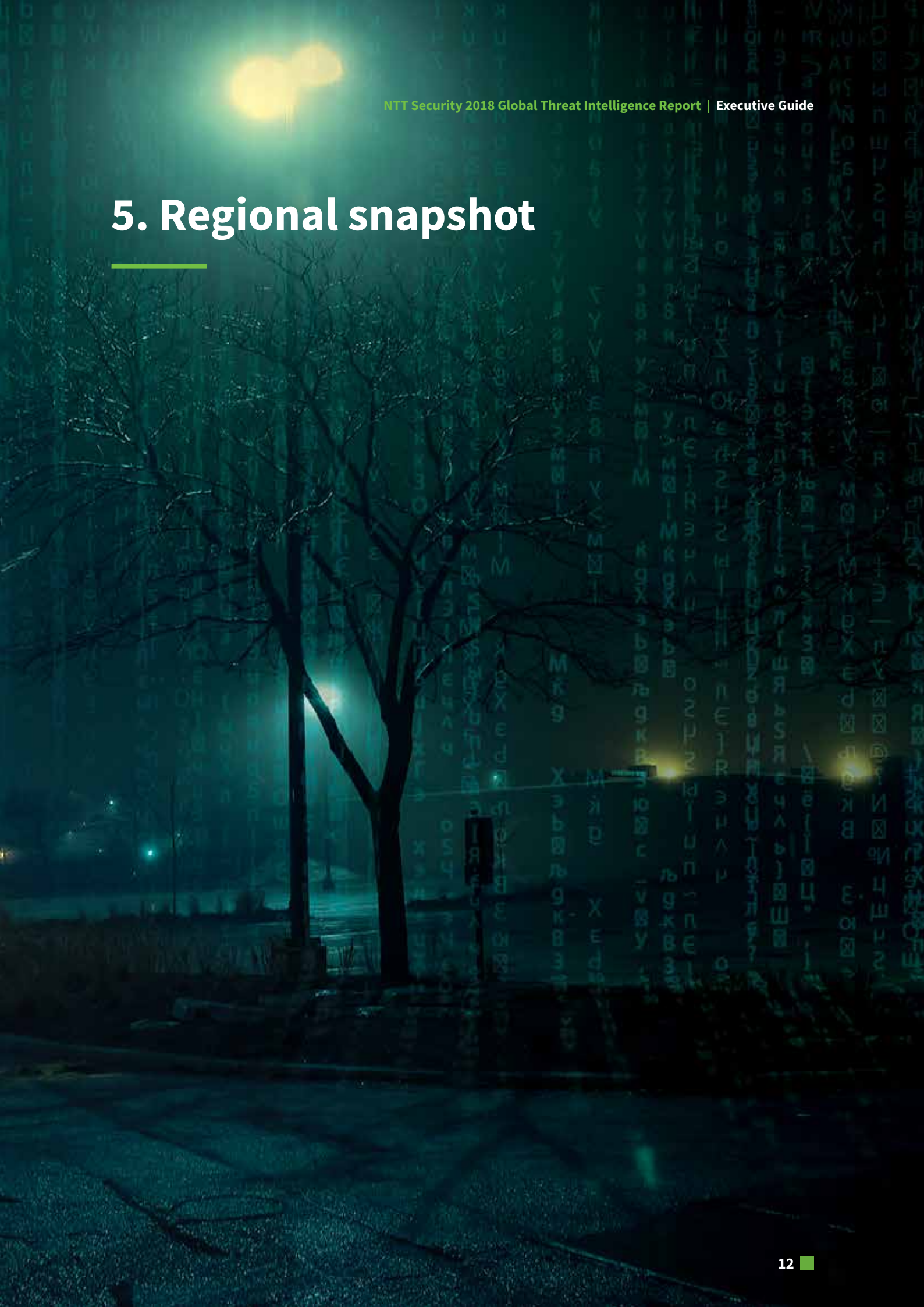
Figure 3: Global ransomware targets



2017 Rankings	
Everyone else	23%
Retail	15%
Healthcare	15%
Government	19%
Business and professional services	28%

Globally, 75% of ransomware detected was *Locky (45%)* or *WannaCry (30%)*.

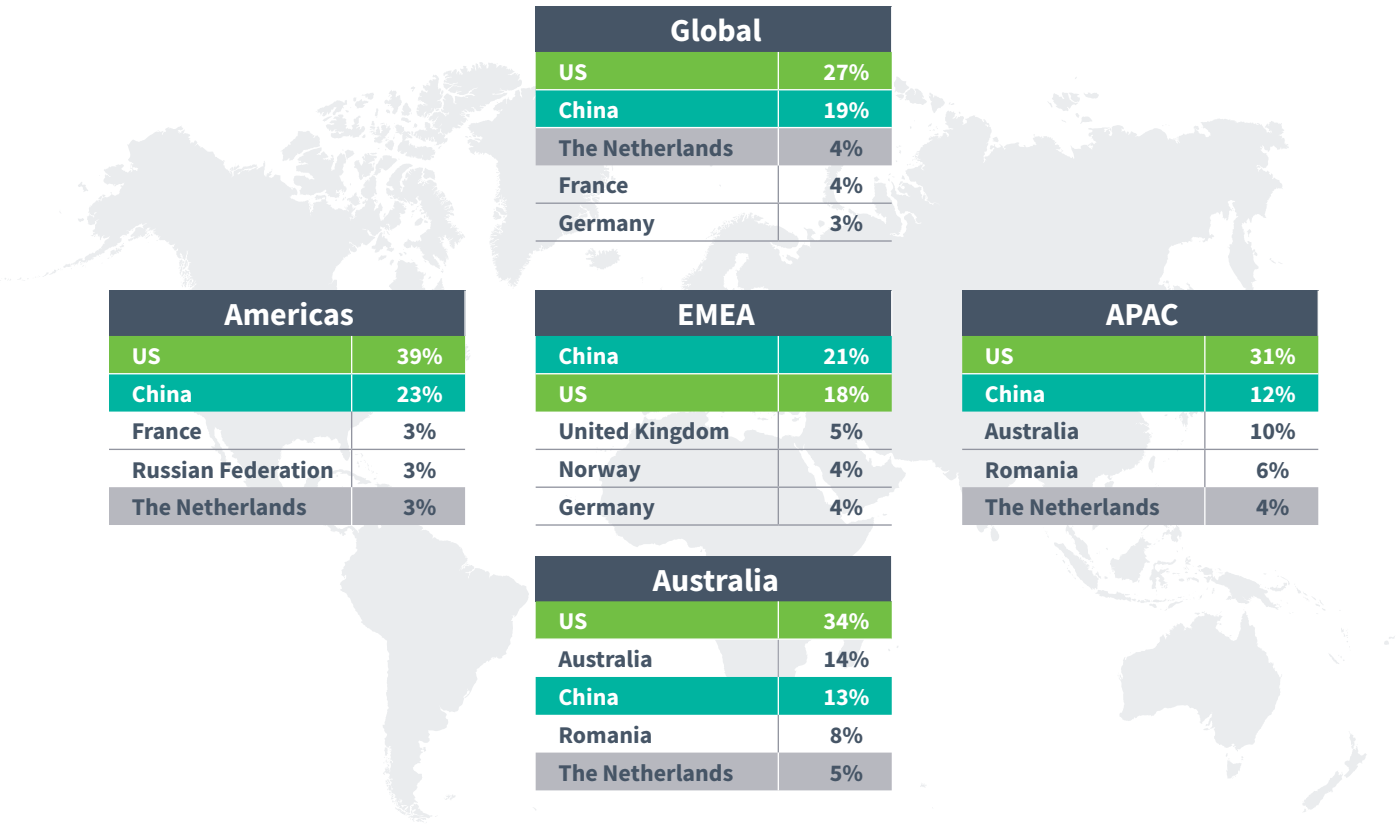
5. Regional snapshot



Regional attack sources:

- The **US** is the first or second most common attack source in all regions.
- **China** ranked first as an attack source country only for EMEA, and second or third for the remaining regions.
- The **Netherlands** ranked among the top five attack source countries in four regions, missing the EMEA region by less than a quarter percent.
- **Top attack sources were often located in the same region as their victims**, except Russian Federation (ranked fourth in the Americas), Romania (fourth in APAC), and Ukraine (fourth in Japan).

Figure 4: Attack source countries by region



Global	
US	27%
China	19%
The Netherlands	4%
France	4%
Germany	3%

Americas	
US	39%
China	23%
France	3%
Russian Federation	3%
The Netherlands	3%

EMEA	
China	21%
US	18%
United Kingdom	5%
Norway	4%
Germany	4%

APAC	
US	31%
China	12%
Australia	10%
Romania	6%
The Netherlands	4%

Australia	
US	34%
Australia	14%
China	13%
Romania	8%
The Netherlands	5%

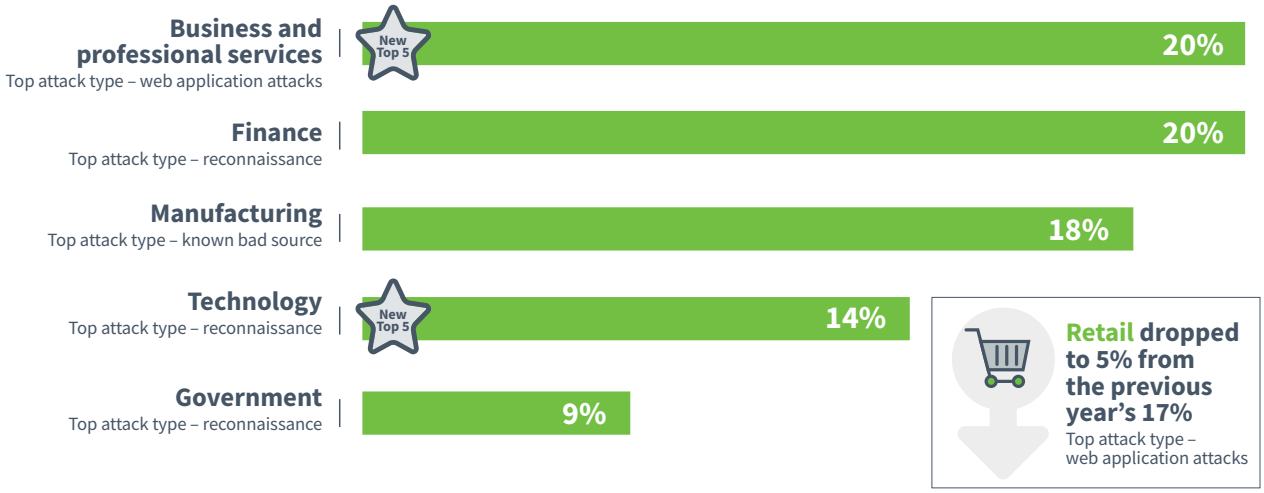
Attack sources continue to be problematic

Attack sources continue to highlight the difficulty of assigning attribution for a specific attack. We regularly identify attack sources as an IP address from which a specific attack was launched. More often than not, that source is an offensive base or launch point used by the attacker, who is located elsewhere.

Europe, Middle East & Africa (EMEA) – *Key findings*

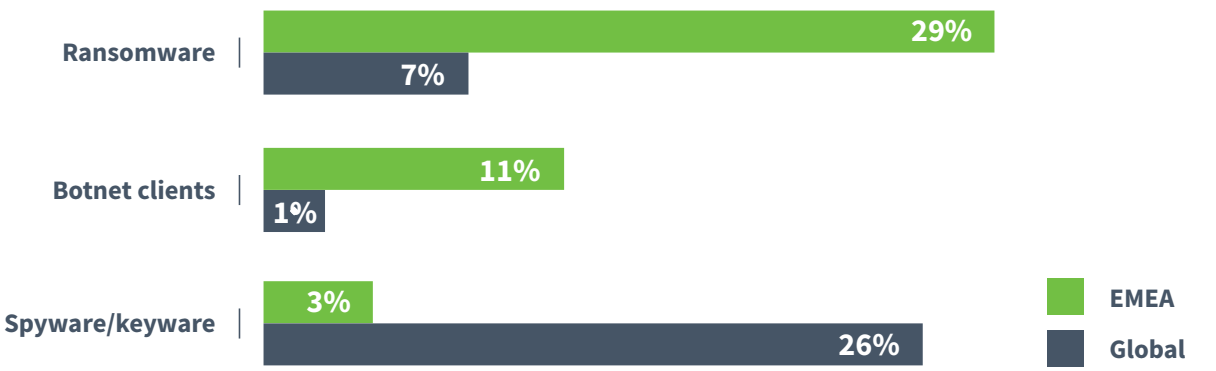
- Business and professional services became the most attacked sector in EMEA, with just over 20% of attacks.
- A 25% increase in the volume of attacks against the technology sector resulted in a 12-point jump to 14% of attacks in 2017, pushing technology into the top five most targeted sectors in EMEA.
- Retail dropped to sixth place, with 5% of attacks compared to 17% observed in the previous year.

Figure 5: EMEA industry attack ratings



- Ransomware ranked first on the list of top malware in EMEA, at 29%, in sharp contrast to only 7% of global malware. Additionally, EMEA was the only region in which ransomware was the number one type of malware.
- Spyware/key loggers made up only 3% of malware in EMEA, in contrast to 26% globally.
- EMEA observed notably high volume of botnet client activity compared to global results.
- Reconnaissance was the top hostile activity for finance, technology, and government within EMEA and ranked second for almost every other industry sector for EMEA.

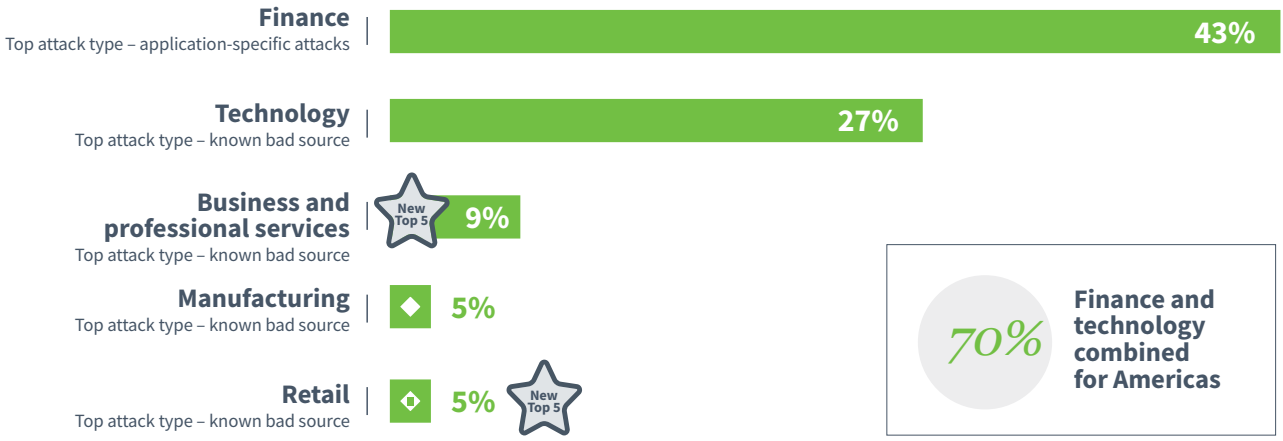
Figure 6: Top types of attack in EMEA



Americas – *Key findings*

- The technology and finance sectors together account for 70% of all attack targets within the Americas.
- Finance sector attacks increased to 43% of attacks in the Americas, up from 15% in 2016. These were predominantly driven by application-specific attacks.
- Attacks against the technology sector increased to 27% in the Americas, up from the 11% observed in 2016.
- Attacks against the manufacturing sector dropped from 23% to 5% of attacks.

Figure 7: Americas industry attack ratings

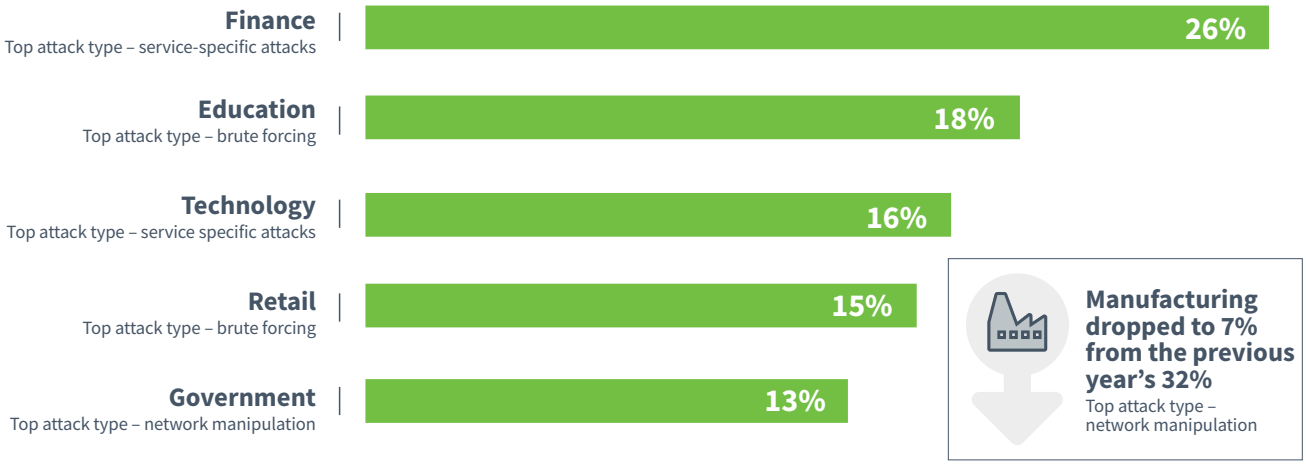


- Attackers continued to exploit known vulnerabilities in conjunction with social engineering. Finance felt the most impact with 59% of phishing attacks, followed by the education sector at 28%.
- For the retail sector, 71% of incident response engagements resulted from malware.
- Malware (35%) was the primary driver for engaging advanced incident response services.
- Trojan/dropper malware ranked first at 57% for both the technology and business and professional services sectors.
- Virus/worms lead the manufacturing sector with 49% of detected malware.
- Spyware/key loggers accounted for 39% of malware targeting the Americas, significantly higher than 26% globally.

Asia Pacific (APAC) – *Key findings*

- Attacks against the finance sector decreased from 46% in 2016 to 26% in 2017, but it remained the most attacked sector in APAC. This was caused by service-specific attacks.
- Increased attacks against education resulted in the sector, jumping from 9% of attacks in 2016 to 18% of attacks in 2017.
- The manufacturing sector dropped out of the top five most targeted sectors this year, moving to sixth position (7%) in APAC, despite ranking second in last year's report at 32%.

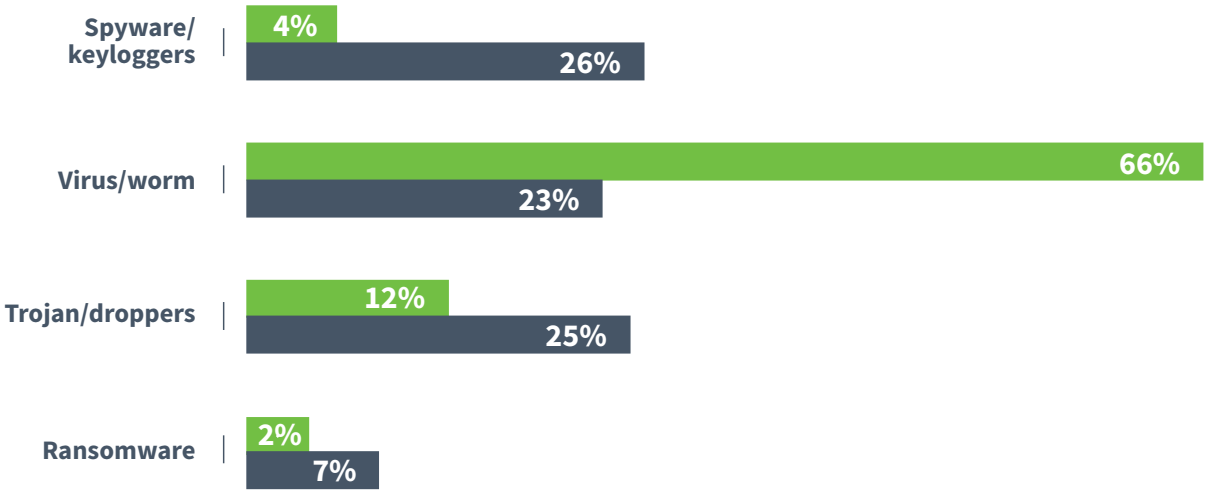
Figure 8: APAC industry attack ratings



Malware and brute force attacks continue to dominate:

- The top attack type within the APAC region for all industry sectors was brute forcing at 26%.
- Virus/worms accounted for 66% of malware in APAC compared to 23% of global malware, indicating lack of investment in endpoint controls.
- Spyware/key loggers were low at 4% compared to 26% globally.
- Ransomware measured at only 2% versus 7% globally.
- 60% of traffic related to the Mirai IoT botnet showed source IP addresses in APAC. OT and IoT attacks continued in 2017, both originating from and focused on resources within APAC.

Figure 9: Malware comparison: APAC versus Global



Australia – *Key findings*

- The education sector topped the list of attacked industries in Australia (26%), followed by technology (17%), finance and government (both 13%), and manufacturing (12%).
- Australia was the source country for 66% of attacks against the finance sector.
- For the government sector, 84% of attacks originated from Australia-based IP addresses.
- For retail targets within APAC, the US and Australia were the source of 92% of attacks and, at 64%, brute force attacks was the most common hostile activity.
- Australia was the leading attack source country for technology sector targets in Australia.

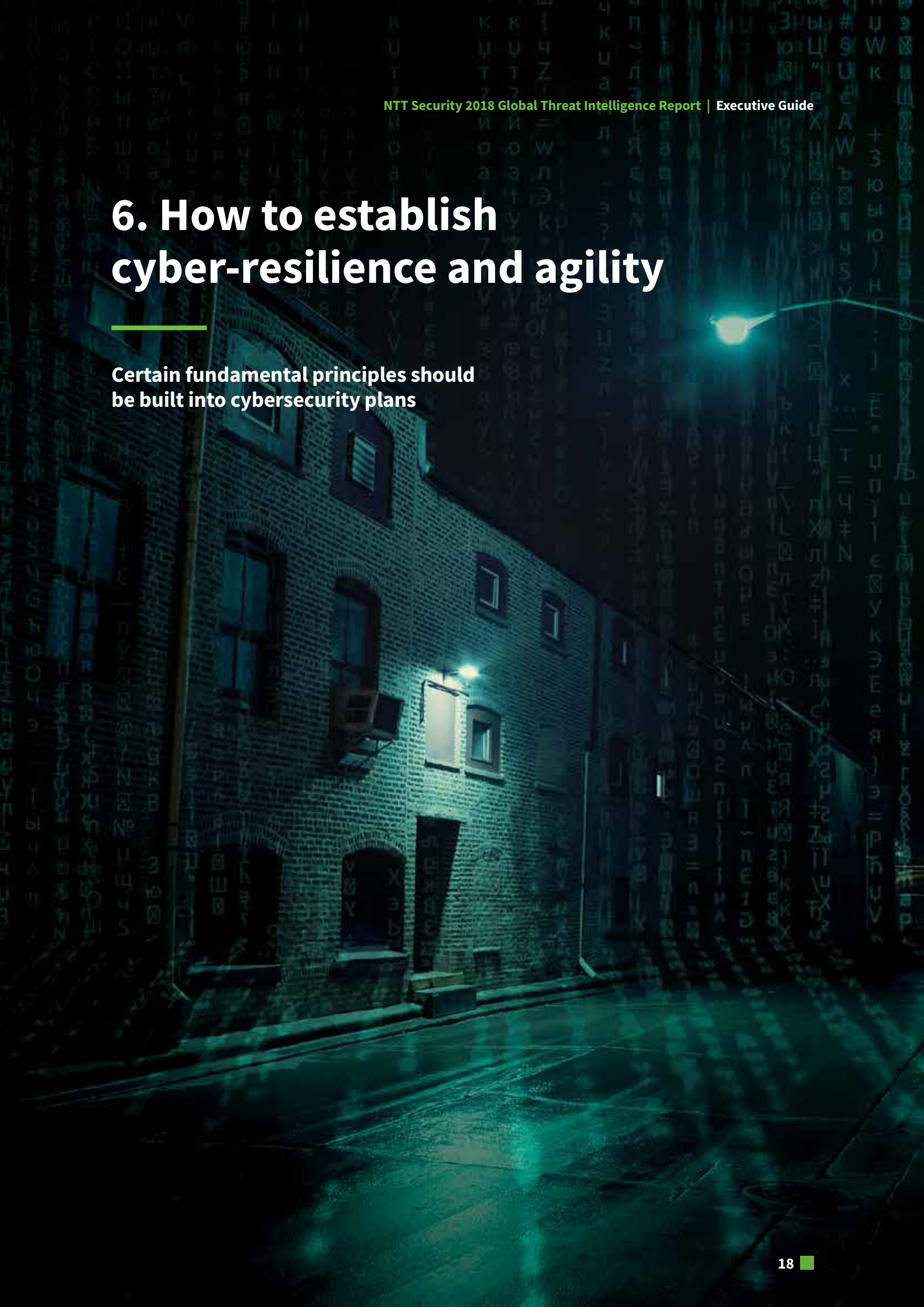
The table below illustrates the types of attacks most commonly perpetrated in this region:

Figure 11: Types of attacks most commonly perpetrated in Australia

Australia	Percentage
Service-specific attack	28%
Brute forcing	25%
Application-specific attack	14%
Network manipulation	8%
Reconnaissance	5%
DoS / DDoS	4%
OS specific exploit	2%
Known bad source	0%
Evasion attempts	0%
Baiting / social engineering	0%

6. How to establish cyber-resilience and agility

Certain fundamental principles should be built into cybersecurity plans



Embed cybersecurity into the core business strategy

Cybersecurity must be core to and aligned with business strategy. It needs to be enabled by default and embedded across technology stacks by design. It must begin from a project's inception and be continuously validated across its lifecycle, thereby reducing risk potential and maximising delivery assurance. Organisations inherently gain greater understanding of the risks they face, embrace the innovation needed to counter identified risks, and have the resilience to restore operations in the event of a breach.

Drive security from the top-down and encourage bottom-up reporting

Security is everyone's responsibility. The Board and Executives must demonstrate accountability and support for security across the organisation. Recognise and empower employee vigilance and engagement as an extension of the cybersecurity programme with the power to drive cultural change. Create cybersecurity consciousness. It's far more cost-effective to investigate suspicious or fraudulent activity observed by an employee early on in the attack cycle than to respond after it has occurred.

Mitigate the impact of ransomware

Remain risk-focused. Minimise exposure of data by enforcing 'need to know' policies and implementing data and network segmentation. Prioritise and enforce endpoint hygiene, including acceptable usage policies and end-user training to reduce the likelihood of users running malicious files. Boost monitoring to identify ransomware infections early. Enforce backup strategies and store backups offline. Maintain focus on foundational practices such as patch and vulnerability management, data encryption, and identity and access controls.

Leverage multi sourced intelligence

Use threat intelligence to prioritise resources effectively and mitigate threats before they impact your business. Incorporate it into attack and breach simulations to improve cyberdefences and incident management processes.

Outpace adversary sophistication through cybersecurity agility

Cybersecurity must move at the speed of digital business. The attack surface is fed by continuous releases by DevOps of features and application components that expose new vulnerabilities daily, rather than over the much longer release cycles of pre-digital development. Be agile and responsive. Shift resources based on the changing risk landscape and short development cycles.

7. Final word: scaling at pace

The threat landscape is dominated by email phishing threats, exploitable vulnerabilities, and insider actions. Attackers are using macros, scripts, and social engineering methods, finding unpatched vulnerabilities, and compromising access credentials.

They're also using newer methods, such as compromising trusted supply chains, shared infrastructure, source code, and applications, thereby increasing the need for software component validation. Although their methods continue to evolve, attackers still favour the path of least resistance.

Risks are less predictable than before, and attackers are developing more sophisticated ways of breaching defences. This calls for a mature and comprehensive approach to cybersecurity, understanding the risks while gaining buy-in from organisational leaders.

Over the last decade, one observation has remained constant: our adversaries operate on a global level, and we must counter this by investing in the right capabilities across people, process, and technologies to scale at the pace at which cybercriminals operate. With this approach in mind, and considering increasing demands by customers, industry, regulators, and governments, organisations must establish cybersecurity agility to seek competitive advantage.

Global data analysis methodology

Research referenced in the Executive Guide is sourced from The NTT Security 2018 Global Threat Intelligence Report. It contains global attack and incident response data gathered from NTT Security and supported NTT operating companies from 1 October 2016 to 30 September 2017.

The analysis is based on log, event, attack, incident, and vulnerability data from clients. It also includes details from NTT Security research sources, including global honeypots and sandboxes located in over 100 different countries in environments independent from institutional infrastructures.

With visibility into 40 percent of the world's internet traffic, NTT Security summarises data from over 6.1 trillion logs and 150 million attacks for the 2018 GTIR. NTT Security gathers security log, alert, event and attack information, enriches it to provide context, and analyses the contextualised data.

Global Threat Intelligence Center

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

- threat research
- vulnerability research
- detective technologies development
- threat intelligence management
- communication to NTT Group clients

The GTIC combines its threat and vulnerability research with its detective technologies development to produce applied threat intelligence. Its mission is to protect and provide NTT Security clients with the services and tools to prevent and provide early warning notifications of risks and threats 24/7.

Threat intelligence management is where these efforts all come together. The GTIC continuously monitors the global threat landscape for new and emerging threats using NTT's global Internet infrastructure, clouds, and data centres along with third-party intelligence feeds. NTT Security works to understand, analyse, curate, and enrich threat data using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP), for the benefit of NTT Security clients.

About Dimension Data security

Dimension Data's security business supports organisations in creating an adaptable and predictive security posture across their network, data assets, cloud, applications, and end-user environments. With our wide range of security capabilities, including consulting, and a suite of technical, support, and managed security services, we assist clients through the full security lifecycle.

Founded in 1983, Dimension Data is a USD 8 billion global leader in designing, optimising, and managing today's evolving technology environments. This enables its clients to leverage data in a digital age, turn it into information, and extract insights.

Headquartered in Johannesburg, Dimension Data employs 28,000 people across 47 countries. The company brings together the world's best technology provided by market leaders and niche innovators with the service support that clients need for their businesses – from consulting, technical, and support services to a fully managed service.

Dimension Data is a proud member of the NTT Group.

NTT Group Resources

NTT Security
www.nttsecurity.com

Dimension Data
www.dimensiondata.com

NTT Data
www.nttdataservices.com

NTT Communications
www.ntt.com

NTT-CERT
www.ntt-cert.org.

NTT Innovation Institute
www.ntti3.com

Meeting the challenges of an evolving cybersecurity landscape

With Dimension Data's cybersecurity expertise, you're better prepared to detect and respond to cyberthreats while supporting business innovation and managing risk. We help you to avoid downtime and build an agile and predictive security ecosystem across your users, applications and infrastructure.

Research shows that:

Incident response is 69% faster and repair time 32% faster on networks monitored by Dimension Data. (2016 Network Barometer Report)

Cybersecurity skills are scarce. With NTT Security, we have more than 2,000 cybersecurity specialists supporting clients around the world. Our Managed Security Services leverage our 10 Security Operation Centres and our threat intelligence and analytics to monitor, optimise, operate, and manage your security.

Our solutions span:

- securing your digital workplace
- protecting against ransomware
- securing your hybrid infrastructure
- securing your enterprise applications

Don't know where to start? With our Cybersecurity Advisory, we assess your security posture, identify gaps, and deliver recommendations for improvement.

To learn more about how we can help to protect your digital business, visit our **cybersecurity expertise page**