NTT Security

NTT DATA

Global Threat Intelligence Report

NTT Security

NTT DATA

Note from our leader

Mike Barch

VP, Security Services, NTT DATA

The digital age is increasingly getting delicate. It has been the fundamental pillar of today's world, a catalyst for internet of things and innovations that continue to evolve and drive growth.But today's world is full of challenges. Cybercriminals threaten the security of this digital world, which becomes more fragile with each attack. The Internet, which was once a tool for information sharing and communication, has grown increasingly complex, and new, digital innovations are outpacing the ability to keep it secure. Security is not optional when people are engaging in data sharing which creates business value.

As global cybersecurity company, we provide you with the tools to understand your current security posture, to support your cyber-security decision making, and to build trust in the data you receive. Our global visibility means we take a smart, multilateral approach to security by leveraging our global reach, knowledge, expertise and our strategic investment.

At NTT DATA we have identified the top threats, analyzed their activities based on our analysis of trillions of security logs over the past year and determined how they should be handled by organizations. These recommendations will assist you in understanding just how ubiquitous certain types of attacks are so you see how they affect all organizations. We hope you find the NTT Group 2019 Global Threat Intelligence Report insightful and worthwhile.

Table of Contents

Executive Summary

As organizations continue to move toward digital transformation, the challenges they face are evolving. True transformation requires exploring new ways of doing business while reducing cost, increasing efficiency and realizing a greater return on investment. Cautiously navigating these new frontiers, we must remain aware we may also be increasing our risk as networking, data requirements and delivery become more abstract. Our infrastructures are becoming more complex, often relying on external dependencies. As we proceed, some legacy problems will disappear from view, some will remain, and some new challenges will come clearly into view.

As NTT Security leverages our global reach and continues to optimize our collaboration both internally and externally, we are happy to share our observations in this, our seventh annual NTT Security Global Threat Intelligence Report (GTIR). Our increasing client base, data from our R&D teams, and deeper analysis within our Global Threat Intelligence Platform, all provided more data for analysis and resulted in many interesting findings. In this year's report, we continue our analysis of attacks against 18 industry sectors (defined in the appendix) and share our observations of the challenges faced by organizations globally.

As in previous years, we provide detailed analysis and key findings at both the global and regional levels. We also provide insight into specific sectors, using threat intelligence from our global security operations centers (SOCs) and research centers, with thousands of security analysts analyzing millions of attacks.

Some of the most prevalent activity during the past year was related to *credential theft, coin mining* and *web-application attack activities*. Due to increased activities in these areas, we have included a high-level overview of these threats, motives, and malicious actors behind them or attributed to them, as well as a discussion of business impact and recommendations.

We continue to observe the long-term trend of attacks against the Finance sector which accounted for 17 percent of all attacks and has been the most attacked sector over the last six years. A significant increase in attacks against Health Care organizations in the Americas was also clearly visible. Web-application and application-specific attacks also doubled over the last year.

In the 2019 GTIR, we also include details on some of the innovative research NTT is conducting to help identify and mitigate different types of threats. In this report you will find three separate overviews exploring how NTT is making business safer across the internet.

We also include updates related to governance, risk and compliance affecting multiple regions globally, as well as discussion of some of the security trends we expect to evolve over the next year.

Although we provide multiple recommendations throughout the report, we believe the following principles can be valuable to consider as you move toward your information security and data protection goals.

Innovative products and solutions require innovative security.

Legacy methods and tools are still quite effective at providing a solid foundation for consistent mitigation, as most attacks can be prevented with basic security controls. But tactics change, and new attack methods are constantly being developed by malicious actors. Security leadership should ensure basic controls remain effective but also embrace innovative solutions if they provide a good fit and true value.

Threats to data security and privacy are here to stay.

Data security and privacy have been a hot topic for the last few years. Today there is no shortage of tools for information sharing and collaboration. As maturity in these areas continues to evolve, it is vital to keep up with regulatory requirements. NTT Security has seen success where organizations have invested in people, processes and tools to provide a solid foundation of security and privacy expertise. Proper documentation of compliance initiatives is vital to securing your organization's data.

Use all your resources to protect your organization, but keep it simple where you can.

In this "there's an app for that" generation, many organizations are caught up in simply buying solutions to problems. Our consulting teams at NTT Security often observe solutions being implemented to address a problem that does not really exist, or a solution that costs more than the potential loss being prevented. When we see this type of activity, it is often based on the premise of "this worked great for company X" or "a vendor told me this will solve all our problems." Leverage relationships that are effective and keep an eye on product maturity in the cybersecurity space. It is essential to know where the real risks lie and develop your solutions accordingly. Businesses need to ensure they are performing due diligence but also need to maximize the return on investment for their security spending.

This report provides a view of the types of threats we see impacting organizations. Every organization has different ideologies on what security looks like and what challenges are most important. This report can help support your tactical and strategic security goals.

Key Findings

NTT Security analyzed data observed during delivery of our managed security services and incident response engagements, as well as vulnerability data and threat intelligence sources. This analysis revealed information about attacks, and techniques to help shape the ways organizations approach securing their data. Refer to the Glossary in the appendix for definitions of *italicized* words in this report.

Global Analysis

Throughout 2018 illicit *coin mining* represented a significant amount of activity – at times accounting for more detections than all other malware combined (discussed in **Security Challenge: Coin Mining** in this report). But other threats challenged organizations globally as web attacks escalated, partially due to the number of vulnerabilities found in common applications. Attackers also appeared to increase focus on attacks against Government and Technology organizations.

NTT Security regularly identifies attack sources as an IP address from which a specific attack was launched. More often than not, that happens to be an offensive base or launch pad used by the attacker, who is often located somewhere else entirely. Compromised systems, purchased hosting, outsourced *exploit kits* or *botnets* are making it easier than ever for attackers to utilize remote resources, and obfuscate their trail.

Figure 1
Vulnerability Counts

Cybersecurity attacks are constantly evolving. Attack volumes don't always increase, but complexity changes as new threats are introduced. The growth of coin mining activity in 2017 had an effect similar to the impact of *ransomware* in 2016, as organizations learned how to manage such threats. The current explosion in the number of vulnerabilities has only served to increase complexity as organizations strive to keep up with patches and mitigating controls on a weekly and daily basis. As shown in **Figure 1**, 2018 set a record for the number of new vulnerabilities identified and reported in a single year.[1] Some of these vulnerabilities were in processor chips and thus have the potential to shake up the entire computing world. Many of these vulnerabilities were discovered in older software and have been present for years. For instance, consider the GNU Bash vulnerability discovered in 2014, also known as *"Shellshock,"* which affects most Unix, Linux and Mac OS X platforms, and continues to be one of the most commonly targeted vulnerabilities today.

Other vulnerabilities were new this year, and some were introduced through patches originally intended to fix other vulnerabilities. The increase in vulnerabilities over the past two years presents a challenge to organizations, as many of these vulnerabilities exist in common systems, utilities and applications, and in application code libraries used to support daily operations.

1 https://www.cvedetails.com/browse-by-date.php

Global Key Findings

- Finance remained the most attacked sector in 2018, as it has been in six of the previous seven years. It was joined by Technology as a top targeted sector this year.
- 35 percent of all attacks originated from IP addresses within the United States and China.
- Application-specific and web-application attacks accounted for over 32 percent of all hostile traffic, making them the top category of hostile activity.
- 73 percent of all hostile activity falls into four categories: *web attacks, reconnaissance, service-specific attacks,* and *brute-force* attacks.

Global Highlights

On a global scale, the variety of attacks is not as broad as would seem likely. The attack types shown in **Figure 2** tended to be most prevalent, just as activity from the United States and China were the most common attack sources. In most cases, the third most common attack type and third most common attack source contribute much less to the overall attack picture.

Global	Top Attack Types	Top Attack Sources
Finance 17%	Web Attacks – **46%** Service-Specific Attacks – **28%** DoS/DDoS – **8%**	United States – **42%** China – **8%** United Kingdom – **6%**
Technology 17%	Reconnaissance – **20%** Brute-Force Attacks – **17%** Known Bad Source – **14%**	China – **37%** United States – **21%** Russia – **5%**
Business and Professional Services 12%	Web Attacks – **42%** DoS/DDoS – **20%** Known Bad Source – **15%**	United States – **26%** China – **15%** France – **10%**
Education 11%	Brute-Force Attacks – **47%** Web Attacks – **18%** Reconnaissance – **16%**	United States – **25%** Netherlands – **16%** Vietnam – **15%**
Government 9%	Service-Specific Attacks – **27%** Reconnaissance – **21%** DoS/DDoS – **16%**	United States – **37%** Germany – **14%** France – **13%**

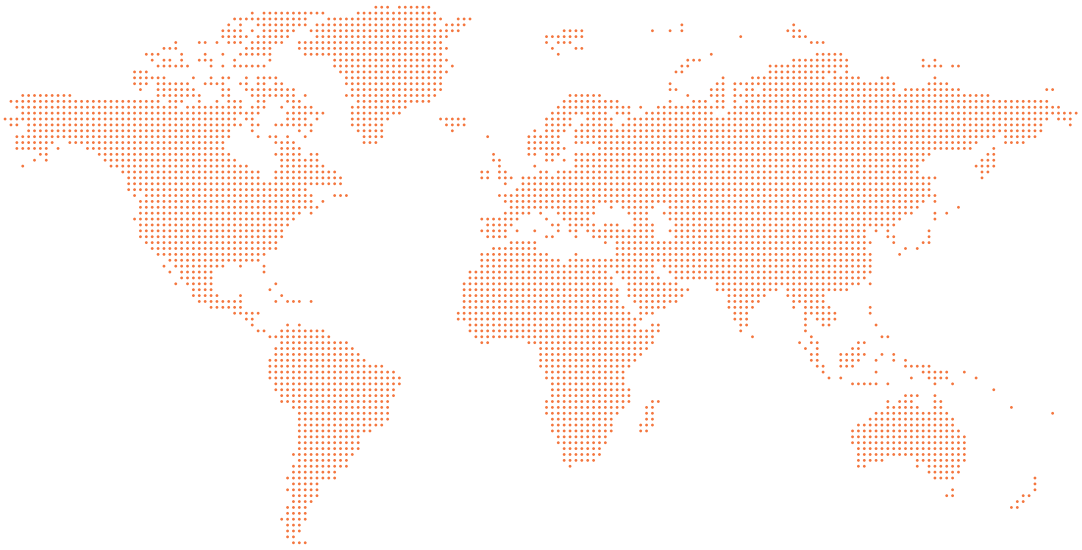


Figure 3

Most Common Attack Sources

Global		EMEA		Americas		APAC	
United States	22%	United States	16%	United States	32%	United States	20%
China	13%	China	13%	China	11%	China	14%
Japan	6%	France	9%	Russian Federation	5%	Japan	8%
France	5%	United Kingdom	9%	Japan	4%	Thailand	5%
Netherlands	5%	Germany	5%	Hong Kong	4%	Netherlands	5%

Figure 3 shows the United States and China as the most common sources of attack in every region. The remaining attack sources varied across regions, with EMEA and APAC each showing a significant number of attacks from within their own region. Combined, a total of ten different countries comprised all of the top five attack sources in the regions.

Globally, sectors experienced some shifts in attacks. As shown in **Figure 4**, Finance tied with Technology this year as one of the most attacked sectors in 2018.

The Business and Professional Services sector remained a popular target, as attackers leveraged vendor trust relationships to access shared data. Education and Government were both new to the global top five due to continued long-term activity against those sectors. Education has always attracted a large amount of attention from cybercriminals. Coin mining campaigns in educational environments contributed to these increased attacks.

Coin mining traffic significantly impacted the Technology sector and accounted in part for the relative gain of hostile activity against Technology when compared to Finance.

The top five attacked sectors accounted for 66 percent of all attacks, supporting trends which imply attackers continue to focus on specific sectors.

While most countries in the list of the most common attack sources remain consistent year to year, 2018 did experience some small changes. Globally, 35 percent of all attacks originated from IP addresses within the United States and China, as shown in **Figure 5**. Attacks from Japanese sources rose slightly and moved them into the top five. Even though attacks from German sources increased, Germany dropped out of the top five due to slightly larger increases in activity observed in Japan and the Netherlands. Attacks from sources in the Russian Federation increased slightly, but they remained the seventh most common attack source.

Figure 4

Globally Most Attacked Sectors

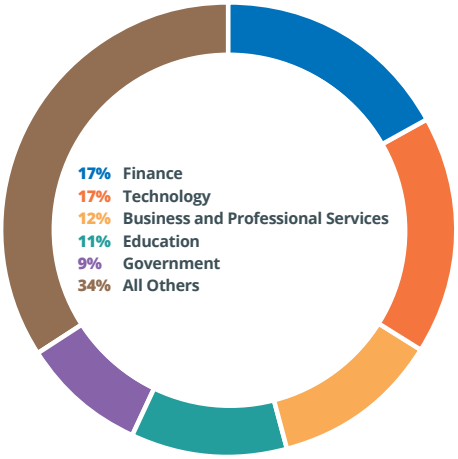
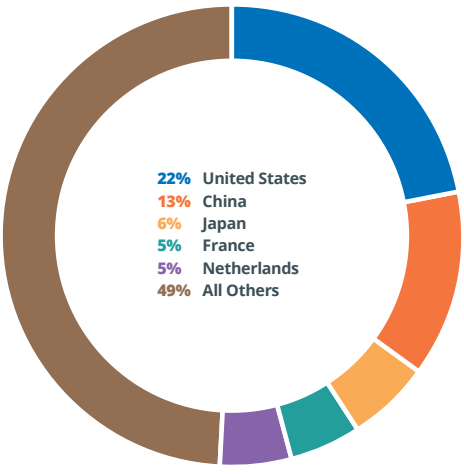


Figure 5

Global Attack Sources



Application-specific and web-application attacks accounted for over 32 percent of all hostile traffic, making them the single most common form of hostile activity. These attacks targeted some of the most commonly used technologies, such as *bash, Apache Struts* and *Samba,* as discussed in the **Security Challenge: Web-Based Attacks** section of this report.

Web attacks were not the only hostile activity which affected organizations. 73 percent of all hostile activity can be grouped into the four attack types as displayed in **Figure 6**: web attacks, reconnaissance, service-specific attacks, and brute-force attacks.

Brute-force attacks accounted for nearly 12 percent of hostile traffic globally, but 21 percent of the hostile activity in APAC. This was primarily directed against Education and Retail targets. Brute-force attacks accounted for 47 percent of all the hostile activity targeting educational institutions.

Service-specific attacks accounted for 13 percent of all attacks globally and ranked as the third most common type of hostile activity. In the Finance sector, service-specific attacks accounted for 28 percent of hostile activity, ranking service-specific attacks immediately behind web attacks in that sector.

Figure 7 illustrates the distribution of protocols or services targeted through service-specific attacks.

Figure 6
Global Hostile Activity

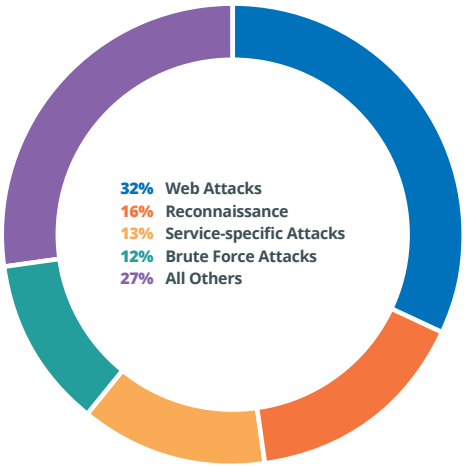
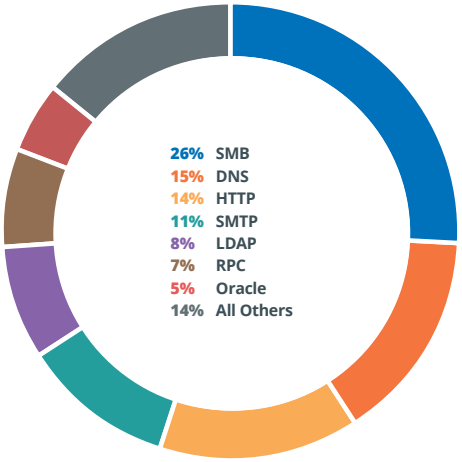
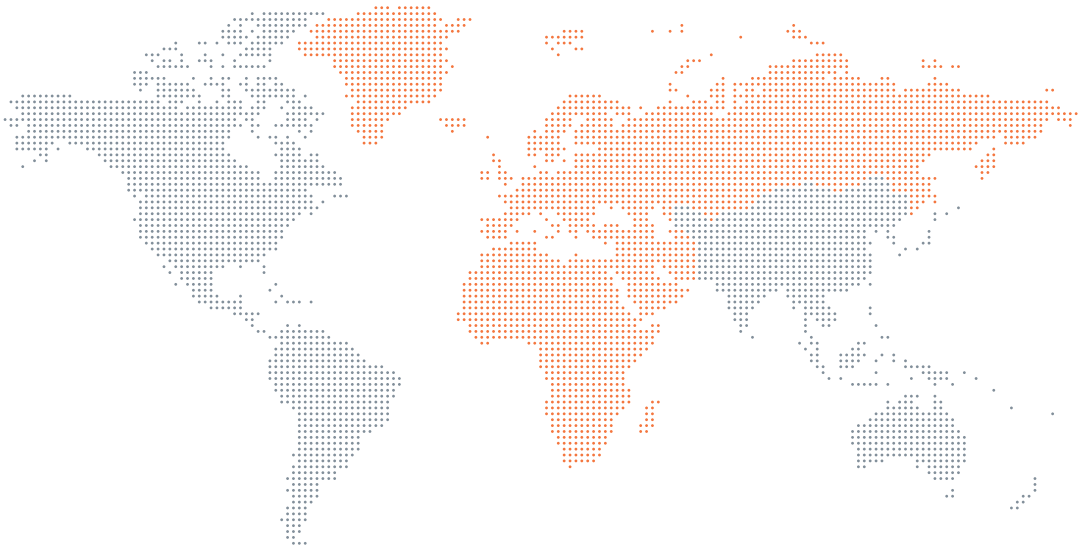


Figure 7
Targeted Services





Europe, Middle East and Africa Analysis

Attacks in Europe, Middle East and Africa (EMEA) were marked by smaller evolutions in attack profiles. Small changes in sources and types meant changes in attack details, but the changes were primarily a reorganization of the most highly targeted sectors, as seen in **Figure 8**. Increased web and service-specific attacks resulted in Finance becoming the most attacked sector in EMEA accounting for 30 percent of all attacks, outpacing Business and Professional Services, which increased to 24 percent of attacks. Technology experienced a slight increase in attacks, while attacks against Manufacturing fell due to fewer malicious campaigns.

Figure 8
EMEA Attack Types and Sources

EMEA	Top Attack Types	Top Attack Sources
Finance 30%	Web Attacks – **43%** Service-Specific Attacks – **33%** Reconnaissance – **15%**	United States – **14%** China – **10%** United Kingdom – **10%**
Business and Professional Services 24%	Web Attacks – **73%** DoS/DDoS – **25%** Reconnaissance – **1%**	France – **22%** United States – **17%** Netherlands – **10%**
Technology 17%	Reconnaissance – **67%** Network Manipulation – **16%** Brute-Force Attacks – **7%**	United States – **23%** Russia – **13%** China – **9%**
Manufacturing 9%	Web Attacks – **42%** Reconnaissance – **27%** Known Bad Source – **22%**	China – **27%** United States – **16%** Russia – **6%**
Transport and Distribution 4%	Web Attacks – **55%** Reconnaissance – **27%** Service-Specific Attacks – **11%**	United States – **19%** Ireland – **16%** China – **8%**

Europe, Middle East and Africa Key Findings

- Web attacks accounted for over 43 percent of hostile activity against the most attacked sectors in EMEA. Comparatively, the global average was 32 percent.
- Attacks from sources in China against all targets in EMEA dropped nearly 40 percent.
- 75 percent of attacks against the top five targeted EMEA sectors originated from IP addresses within EMEA.

Europe, Middle East and Africa Highlights

Transport and Distribution entered the top five attacked sectors in EMEA based on the intensity of increased web attacks. Web attacks were the most common attack type in four of the top five sectors in EMEA, averaging over 43 percent of all attacks against those sectors, well above the global average of 32 percent for web attacks. Transport and Distribution was the only sector new to the top five. The percentage of web attacks increased as shown in **Figure 9**, nearly doubling for Finance, while significantly increasing for Manufacturing as well as Transport and Distribution.

The Technology sector in EMEA experienced a sizable increase in *network manipulation* attacks, which tend to be more technical and focused than many other attack types. The remaining attack types and most attack sources remained relatively consistent.

While the Manufacturing sector experienced a surge in web attacks, the overall attack volume across EMEA decreased. Sources within China dropped from 67 to 27 percent of all attacks targeting EMEA Manufacturing, but still accounted for more hostile activity than any other attack source.

Attacks from sources within China against all targets in EMEA dropped nearly 40 percent. This does not imply the actual attackers have changed, rather the source of the attacks has changed.

Figure 10 shows that the top five attacked sectors in EMEA experienced attacks from a similar number of sources compared to other regions. In EMEA, 12 countries attacked the top five sectors within EMEA, 9 countries targeted the top 5 sectors in the Americas, and 10 countries in APAC attacked their top 5 sectors.

Figure 11 shows that more of the attacks originated from within EMEA (EMEA sources attacking EMEA targets) than from any other region (75 percent). This supports the common notion that attackers tend to leverage attack sources near their targets, an observation which was demonstrated more strongly in EMEA than in other regions.

Figure 9
Increases in Web Attacks in EMEA

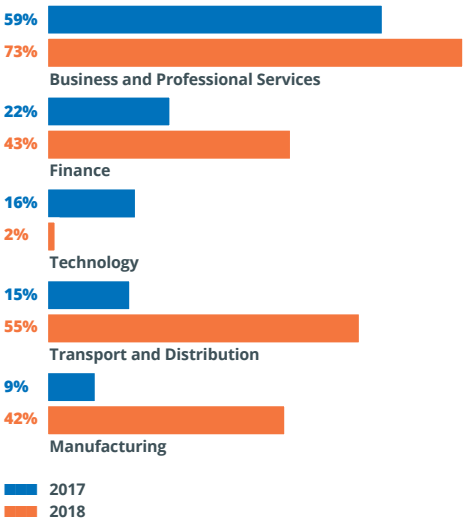
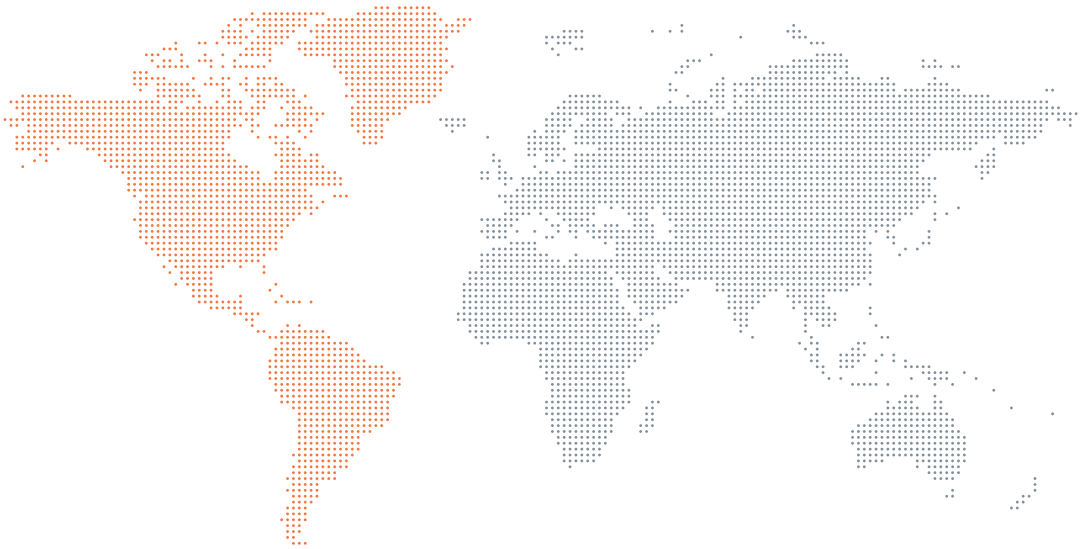


Figure 10
Countries Attacking Top Five Sectors Per Region

Figure 11
Percentage of Attacks From Within Same Region



Americas Analysis

Cyber attacks against targets in the Americas changed dramatically in 2018. While the top two targeted sectors in both 2017 and 2018 were Finance and Technology, their share of attacks dropped, as shown in **Figure 12**. Attacks in Business and Professional Services, Health Care and Education all increased, and the Health Care and Education sectors are both new to the top five in the Americas.

Figure 12
Americas Attack Types and Sources

Americas	Top Attack Types	Top Attack Sources
Technology 17%	Known Bad Source – **37%** Reconnaissance – **28%** Web Attacks – **20%**	United States – **34%** China – **15%** Hong Kong – **7%**
Finance 16%	Web Attacks – **46%** Service-Specific Attacks – **16%** DoS/DDoS – **14%**	United States – **63%** Hong Kong – **4%** Norway – **4%**
Business and Professional Services 16%	Known Bad Source – **47%** Reconnaissance – **21%** DoS/DDoS – **12%**	China – **29%** United States – **26%** Russia – **5%**
Health Care 12%	Reconnaissance – **44%** Known Bad Source – **32%** Network Manipulation – 1**4%**	United States – **24%** Nigeria – **12%** China – **9%**
Education 7%	Web Attacks – **34%** Known Bad Source – **25%** Service-Specific Attacks – **17%**	Japan – **49%** United States – **10%** China – **9%**

Americas Key Findings

- Attacks targeting Health Care in the Americas increased nearly 200 percent.
- Coin mining activity moved Education into the top five attacked sectors in the Americas.
- Russia ranked higher (number 3) against targets in the Americas than against any other region.

Americas Highlights

The United States was the single largest source of attacks against Health Care organizations in the Americas. Similar to last year's report, Chinese and Nigerian sources accounted for a significant portion of the activity, resulting in approximately 21 percent of attacks. Sources from Nigeria accounted for a substantial amount of *phishing* activity related to *credential theft* which explicitly targeted Health Care organizations. Other sources in Africa and Eastern Europe (Kenya, Armenia and Russia) also contributed to heightened levels of activity.

Health Care organizations in the Americas averaged 57 percent of attacks from the top five most common attack sources, indicating the attacks were much more distributed. This is common for sectors experiencing increasing levels of attacks, such as Health Care in the Americas and Finance in EMEA (48 percent of attacks).

The Education sector was new to the top five in the Americas. Nearly 34 percent of this activity was related to a combination of web-application and application-specific attacks. This is an increase from less than five percent last year, suggesting a change in attacker tactics when targeting educational institutions. These attacks also included sources from APAC, most notably Japan, Australia and China. It is likely much of this change in tactics is related to web attacks installing coin miners in educational institutions. Coin mining is discussed in more detail in the **Security Challenge: Coin Mining section**.

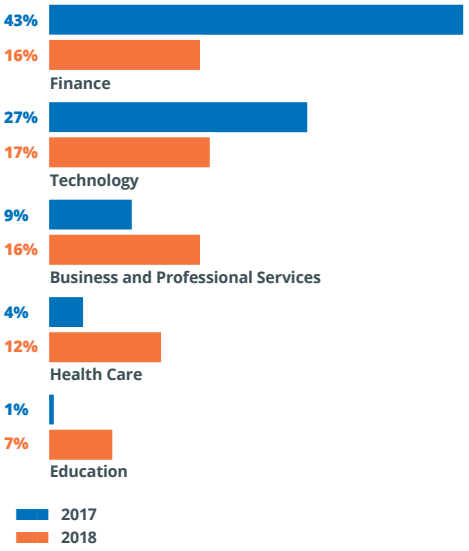
As shown in **Figure 13**, the Americas experienced changes in attack targets. While attacks against Finance and Technology dropped, they still ranked as the most attacked sectors in the Americas, accounting for 33 percent of attacks. Within the Finance sector, specifically the general banking and investment banking sub-sectors, we observed significantly less activity; however, other sub-sectors maintained pace against previous baselines.

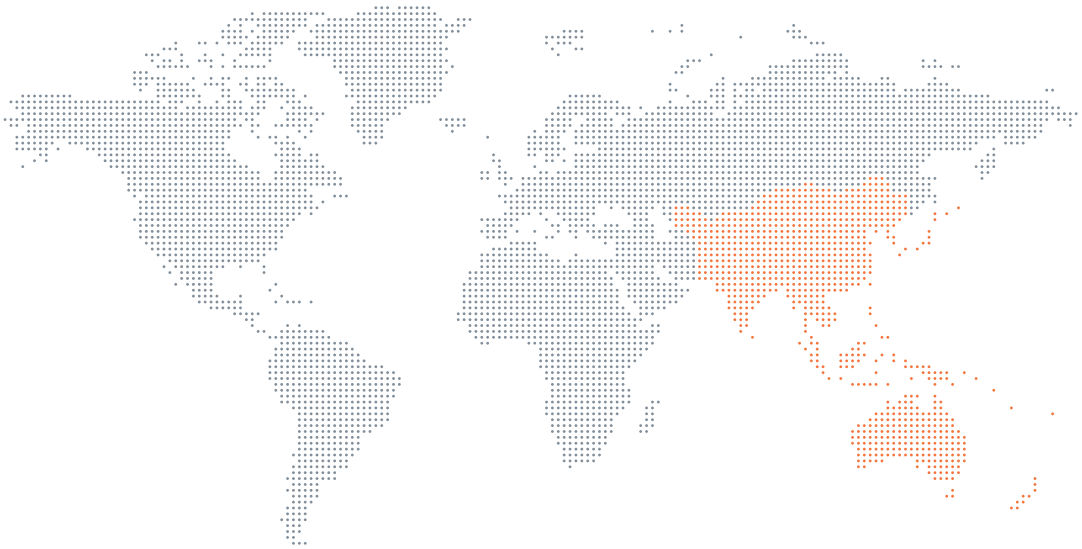
Of all attacks directed at the Finance sector in the Americas, 46 percent were web attacks, about the same levels as the previous year (48 percent in 2017). Web attacks targeting all sectors within the Americas followed global trends, accounting for 25 percent of all attacks, nearly doubling their percentage from last year. The Americas had the lowest percentage of web attacks of any region.

Technology companies experienced the same types of hostile activity as the previous year – known bad source, reconnaissance and web attacks. Business and Professional Services demonstrated similar known bad source and reconnaissance activity as the previous year and was the only sector to experience high levels of *Denial of Service (DoS)* and *Distributed Denial of Service (DDoS)* attacks (over 12 percent) in every region.

While attack types remained similar to previous years, attack sources in APAC, most notably Hong Kong and Japan, surpassed some of the active sources within EMEA (like the Netherlands, France and Germany). Russia was the third most active source against targets in the Americas, but ranked sixth against EMEA, ninth against APAC, and seventh globally.

Figure 13
Changes in Targeted Sectors: Americas





Asia-Pacific Analysis

The Asia-Pacific region (APAC) saw small adjustments in attack targets compared to previous years. **Figure 14** shows that attack sources and attack types evolved, quite substantially in some cases, as attackers found new venues from which to attack, and leveraged new attack vectors. The APAC region realized more dynamic shifts than the other two regions.

Prior to this year's report, APAC and Japan were reported as separate regions. For the 2019 GTIR, all Japan data sources are now part of the APAC dataset, so some of the observed changes are the result of the combination of data.

Figure 14
APAC Attack Types and Sources

APAC	Top Attack Types	Top Attack Sources
Technology 19%	Web Attacks – **34%** Brute-Force Attacks – **27%** Network Manipulation – **11%**	China – **55%** United States – **15%** Egypt – **7%**
Education 17%	Brute-Force Attacks – **56%** Reconnaissance – **16%** Web Attacks – **15%**	United States – **27%** Netherlands – **19%** Vietnam – **17%**
Finance 15%	Web Attacks – **48%** Service-Specific Attacks – **31%** Network Manipulation – **7%**	United States – **75%** China – **9%** Russia – **3%**
Government 13%	Service-Specific Attacks – **34%** DoS/DDoS – **20%** Web Attacks – **18%**	United States – **27%** Germany – **18%** France – **16%**
Manufacturing 8%	Reconnaissance – **47%** Web Attacks – **21%** Brute-Force Attacks – **13%**	Japan – **44%** United States – **16%** China – **7%**

Asia-Pacific Key Findings

- Technology was the most attacked sector in APAC due to a doubling of the percentage of web attacks from the previous year (34 percent).
- 21 percent of all activity in APAC was related to brute-force attacks, compared to 12 percent globally.
- The most common attack types in APAC were web attacks accounting for 36 percent overall. This was the highest percentage of web attacks in any region.

Asia-Pacific Highlights

Chinese sources contributed to the surge in brute-force attacks (from two percent last year to 27 percent this year). A 100 percent increase in web attacks accounted for the Technology sector becoming the most attacked sector in APAC. A decrease in brute-force attacks accounted for the Finance sector dropping from the most attacked last year.

Attacks against the Technology sector from sources in China increased from eight percent to 50 percent of all attacks; however, attacks from sources in the United States and Australia decreased.

Scanning against Internet of Things (IoT) devices by Egypt was internet-wide but had the most visible impact against targets in the Technology sector in APAC. This helped increase the Technology sector's share of attacks.

Figure 15 shows the regional differences between the levels of brute-force and DoS/DDoS attacks. APAC activity was characterized by increased levels of brute-force attacks. These attacks accounted for less than 12 percent of all hostile activity globally but resulted in 21 percent of observed activity in APAC. Education and Retail sectors were the primary targets of this activity. **Figure 15** also shows that, unlike the APAC region, EMEA experienced higher rates of DoS/DDoS attacks.

While attacks against the Technology sector in APAC from sources in China were increasing, the same attacks against the Education sector decreased, as attacks from China dropped from 18 percent to under 4 percent. Web attacks from Vietnam and brute-force attacks from the Netherlands accounted for over a third of hostile activity affecting educational institutions in APAC. Attack activity from Japan accounted for 49 percent of attacks against the Education sector in the Americas region.

Attacks against the Government sector in APAC remained at 13 percent of attacks, but the makeup of those attacks changed dramatically. Government targets in APAC experienced significant decreases in activity from other countries in the region which, as shown in **Figure 16**, was replaced by activity from the United States and multiple EMEA countries who combined for over 78 percent of activity against this sector.

Activity targeting Manufacturing in APAC remained consistent in volume and ranking with previous years. Attacks from Japan and the United States along with China, France, the Netherlands, Thailand, Russia, and the United Kingdom combined to contribute the majority of the hostile activity against the Manufacturing sector in APAC. Activity from Japan sources accounted for 27 percent of attacks against Manufacturing globally and was the top source targeting Manufacturing in APAC with 44 percent of attacks.

Sources in Thailand were responsible for a greater share of attacks than in past years. Hostile activity from Thailand was reported globally, targeting all 18 sectors and over 60 destination countries. Along with Manufacturing, these attacks were active in the Health Care sector within APAC.

A reduction in activity targeting the Retail sector in APAC dropped it out of the top five targeted sectors. A modest increase in web and service-specific attacks from Japan against Retail did not offset a nearly 50 percent drop in brute-force attacks from sources within the United States. Japan was the top attack source against Retail in APAC, accounting for 56 percent of all attacks.

Figure 15
Brute Force vs. DoS/DDoS

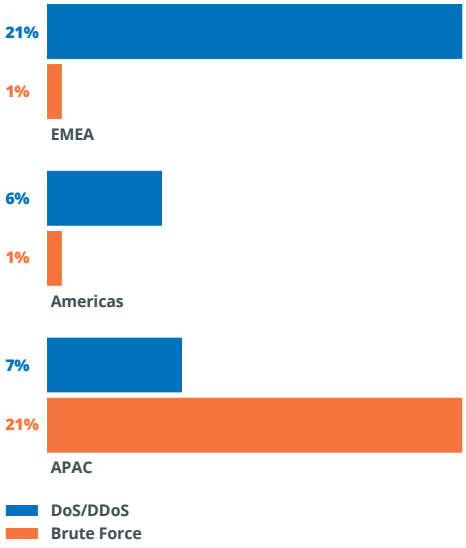


Figure 16
Percentage of Attacks Targeting APAC Government

Source Country	2017	2018
United States	5%	27%
Germany	<1%	18%
France	2%	16%
China	<1%	12%
United Kingdom	<1%	10%

Governance, Risk Management, and Compliance

The biggest story in 2018 was data protection and privacy. With GDPR coming into force in May, inboxes were flooded with re-consent emails (many unnecessary). Those of us working in the sector were preparing new registers of processing, a GDPR requirement explaining what user information is processed and for what reason. We were simultaneously working out where we would have to do our first Data Protection Impact Assessments.

By the end of the year, the first fines had arrived, albeit much smaller than the headlines had predicted. More interesting were the enforcement cases brought for activity under the old rules. With two major corporations facing large fines in the UK under the 1995 Data Protection Directive, this perhaps provided an indicator of the regulators' moods. We also saw various national exceptions come into force in EU member states, underlining that despite the initial intent, GDPR does not wholly harmonize privacy regulations, even within the borders of the EU.

In the United States, the California Consumer Privacy Act was born, drafted, passed and ratified in only a few days. The Act will have profound implications. Due to the number of tech giants which will be caught up in it, and the GDPR-esque territorial scope, the Act challenges the U.S. federal government to catch up. As we approach its implementation on January 1, 2020, this year will be in part spent on assessing impact, gaps and requirements as companies prepare to meet this additional regulatory shift. We can expect to see other states within the U.S. follow suit as many states already have privacy protection statutes, with the State of Washington recently adding its own version.

Elsewhere, Australia brought in its new Notifiable Data Breaches scheme in February 2018, with Israel doing likewise in May. China and Singapore have continued to strengthen regulation both in terms of personal data and wider cybersecurity protections, while the Philippines has strengthened its guidance across the board. India published its draft Personal Data Protection Bill in July with public consultation ongoing.

It's safe to say data protection is not just here to stay, but will increasingly need to be on board-level agendas – not just in the EU or for companies trading in the EU, but for all businesses, whether operating globally or in any jurisdiction having its own privacy laws.

What can we expect to see in 2019?

More of the same. Draft regulations will be ratified, and others strengthened. Governments from Latin America to APAC are identifying the need to protect their citizens' privacy rights, and realizing that personal data is a useful economic, social and political commodity that companies are hungry to use. Data protectionism has been a feature of some regulations since at least 2015, with Russia leading the way, and plenty of other governments following on.

We will also see enforcement start to ramp up. A large fine issued by the CNIL[2] (the French regulator) to a social media operator in January is a further indicator of EU regulators' intent – though, given the size of the company, even €50m may not serve to get their attention. With ongoing investigations into several well-known companies, plus various large-scale breaches which occurred after May 2018, we can expect to see further enforcement action, this time under the new rules.

2 https://www.theguardian.com/technology/2019/jan/21/google-fined-record-44m-by-french-data-protection-watchdog

We have started to see a shift away from enforcement based on data breach or loss, to enforcement based on breaches of individuals' rights. The two cases brought under the old Directive were related not just to the loss of data, but to misuse. The companies had failed to put internal safeguards in place, to enforce rules, or to inform individuals of what was being done with their data.

These cases clearly show that not losing an individual's data is no longer enough. Respect for privacy as a fundamental right was codified in the new regulation, and regulators will be looking at this when assessing how companies have reacted to the new regulation. They will be looking for changes in services, design and delivery, building in protection for individuals' rights across all the data protection principles.

This makes data protection by design central to developing a compliance program. Understanding how your company interacts with personal data, in terms of security, accuracy, and ability to meet requests from individuals, will need to shape both the services you consume and those you deliver.

No intent to disregard security, of course. There is no quicker way to draw both public and regulatory scrutiny than to have a major security breach, with containment and recovery costs, informing individuals, and the inevitable hits on revenue and reputation.

A breach of personal data can continue to be an inconvenience even years after the event. Safeguarding personal data is a matter of compliance, trust, and fundamentally, ethics. Companies taking data protection seriously are those which consumers and partners will want to do business with.

This brings us back to the increasing importance of data protection impact assessments. These are now the law for high-risk processing in the EU, and any kind of security monitoring focused on employees is deemed to be high-risk. This means that companies operating under the GDPR will need to be vigilant in striking a balance between a proportionate, threat-related security program and protecting the privacy rights of their employees.

Brexit is one of the political features of 2019 that will impact a range of data protection issues. Uncertainty surrounding the future trading relationship between the EU and the UK will play into various data protection topics. The UK has been clear on its position: it is aligning to GDPR for the foreseeable future, adopting elements like the EU Model Clauses, recognizing pre-existing Binding Corporate Rules and Privacy Shield as a way of maintaining the current regime. This means suppliers from the EU and other jurisdictions can continue to work with UK companies based on current compliance frameworks.

For UK companies doing business into the EU, there is less certainty. The transition deal provided for a period of stability, but in the event of a no-deal Brexit, the UK immediately becomes a third country, without an Adequacy arrangement in place. The UK government will seek to address this, but in the short term, companies will need to look to their existing arrangements between third-country affiliates and the EU as examples of the arrangements that could be put in place, including Model Clauses.

This brings us to another point of interest for 2019. In 2015, the Schrems case overturned the Safe Harbor arrangements between the EU and the USA. A similar case, brought by the same plaintiff (known inventively in the field as Schrems 2), is now in the Courts of Justice of the EU (CJEU), this time questioning the validity of the EU Model Clauses. Following the demise of Safe Harbor, many companies opted for standard contractual clauses (SCCs) as a "go-to" model, rather than invest in Binding Corporate Rules. Should this case succeed, it has profound implications for the ability to transfer data outside of the territorial boundary of the EU/European Economic Area.

Compliance Improves but Effective Response Still Lags

- Organizations are improving at keeping up with changing compliance and regulatory requirements; however, their incident response capabilities remain behind the curve or are satisfying requirements by only a thin margin.
- There is a clear gap in knowledge, processes, tools and qualified personnel required to support most organizations in the event they are faced with a significant impact.
- Organizations which treat compliance as the end-game will likely suffer significant losses due to a "check it and forget it" approach.

What we recommend:

- Proactive response and mitigation are all about identifying threats to your organization – develop the capability to identify gaps, mitigate potential loss, and respond when necessary.
- Prevention is about taking the appropriate steps prior to an incident and is preferable to poor response. Constantly update your plans to be resilient and maintain business continuity.

Don't let complacency, and thinking your organization is not a target, lead you to settle for the capabilities you have today.

Many APAC jurisdictions also regulate cross-border transfers, and in a less harmonized way. The Asia-Pacific Economic Cooperation countries – including the US, Japan and Australia – have taken the lead in addressing this, with the Cross-Border Privacy Rules. Similar in some respects to Binding Corporate Rules, they allow a significant degree of variation between the different jurisdictions, while in effect recognising the "adequacy" of each, to the extent data can be allowed to transit. Japan, the recent recipient of its own Adequacy agreement with the EU, is well-placed to operate under both frameworks.

Moving forward into 2019:

- **Data protection by design is key, wherever you are in the world.** As AI and machine learning become more widespread, considering data protection at an early stage in business transformation, system development and product delivery will be a differentiator for customers, whether business to business or business to consumer, and will build your reputation as a good custodian. Make sure your new product or service has considered data protection at the design stage – not as a bolt-on.
- **Put data protection on your Board agenda alongside cybersecurity.** Reinforce it's not just about stopping data from being hacked or lost.
- **Make sure you have access to good data protection advice, and that it's correctly positioned for your business.** Typically, this will include a blend of legal, information security, risk management, and the ability to talk to stakeholders.
- **Train employees in your compliance regulations.** Key stakeholders – decision makers, as well as policy and architecture leaders – need the best training, but training developers, designers, and all employees in appropriate levels of compliance regulations can dramatically improve compliance communication.
- **Prioritize compliance efforts with all other operational initiatives.** Not only designing compliance as component parts of larger projects, but prioritizing compliance initiatives with other work helps ensure the most important elements get managed first, and helps set organizational expectations about those priorities.

Regulatory compliance is a well-known challenge faced by many sectors. NTT Security analysis of risks facing organizations reveals a variety of other business challenges, including managing the threat of illicit coin mining which we discuss in the next section.

Security Challenge: Coin Mining

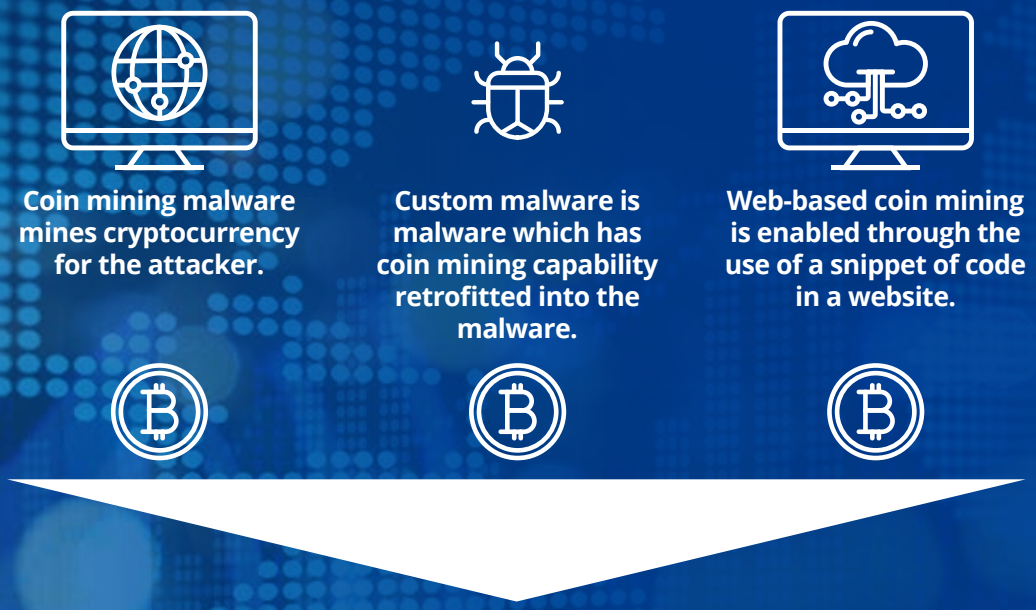
Threat Overview

NTT Security researchers constantly monitor cryptomining malware activities, analyzing new variants and their capabilities as this class of malware continues to evolve. According to the Cyber Threat Alliance (CTA), an NTT Security strategic partner, in a joint paper[3] with NTT Security and other members, the threat of illicit cryptocurrency mining represents an increasingly common cybersecurity risk for enterprises and individuals, with mining detections increasing 459 percent between 2017 to 2018.

Coin mining is known by several other names, including cryptomining, cryptocurrency mining and cryptojacking. All these names essentially refer to the same thing – code which generates or "mines" cryptocurrency.

Coin mining can occur on a system with or without a user's knowledge. There are three primary types of coin mining, as shown in **Figure 17**.

Figure 17



Coin mining malware (CMM), custom malware with coin mining capabilities, and web-based coin mining, are all relatively new threats. Coin mining activity in your environment often indicates a bigger problem. In the case of CMM or custom malware, it likely indicates unpatched vulnerabilities, or someone in your environment has fallen victim to a phishing attack, allowing an attacker unauthorized access to your network. This is a risk that cannot be overstated – illicit coin miners in an environment were installed via illicit means, which indicates some level of compromise.

3 https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf

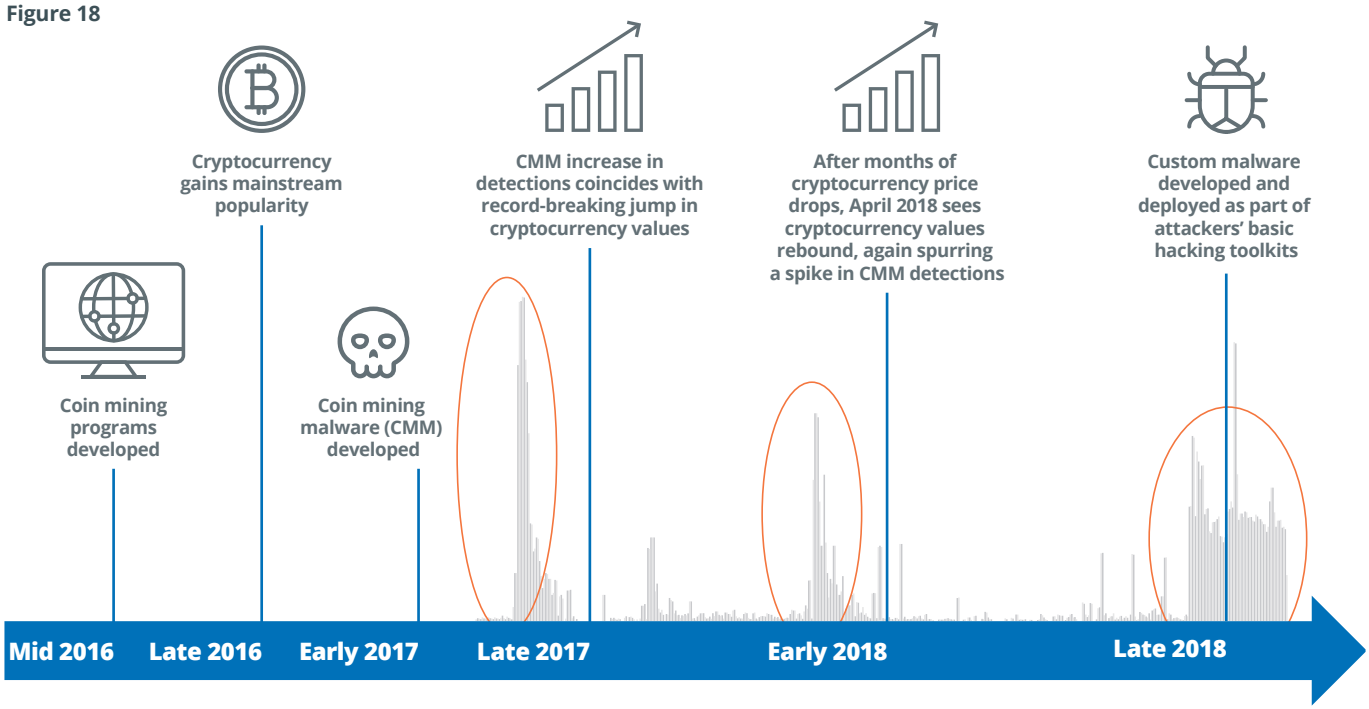
NTT Security Observations

Illicit cryptocurrency mining is still in its infancy, and the practice has only recently been catching on with attackers around the globe. The dramatic uptick in detections is due in part to the detection capabilities NTT Security has implemented within our managed security service platform, as well as the rise in cryptocurrency mining as an integral part of attackers' toolkits.

NTT Security observed several attack peaks throughout the past year or so, as depicted in **Figure 18**. We identified a spike in late 2017, coinciding with a record-breaking jump in cryptocurrency values. The value of Bitcoin alone jumped 225 percent in December 2017. Cryptocurrency values (and generally, CMM detections) experienced dramatic drops during 2018, though April saw a rebound in both cryptocurrency values and CMM detections.

CMM detections decreased a bit in the following months, but by October 2018, attackers began building cryptocurrency mining capabilities into their toolkits, unsurprisingly resulting in an associated spike in detections. The average number of detections remained rather steady through the end of the year.

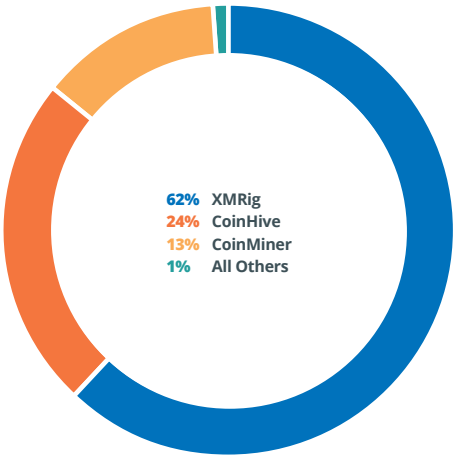
Figure 18



The most common coin miners detected throughout the year are identified in **Figure 19**:

- XMRig – A coin mining application that can be installed on computers and used to mine Monero cryptocurrency.
- CoinHive – Uses a snippet of JavaScript code embedded in a website, which then uses site visitors' computing power to mine Monero cryptocurrency. Some variants request authorization from site visitors before coin mining activities begin.
- CoinMiner – Another variant of a cryptocurrency mining application, similar to XMRig, that can be installed and generate cryptocurrency without the system owner's knowledge.

Figure 19
Coin Miners



Threat Targets

As shown in **Figure 20**, the Technology and Education sectors account for over 86 percent of all coin mining detections, with the Health Care, Business and Professional Services, and Finance sectors rounding out the top five sectors impacted. All remaining sectors accounted for just over two percent of total detections of coin mining activities.

Some cryptocurrency mining is legitimate: a user may install a coin mining program on their personal system to generate cryptocurrency for themselves. We often see this in the Education sector, where distinctions may not be made between the faculty network and student network. Students regularly use their own computing resources to conduct legitimate coin mining, but it is not always easy to identify what coin mining is legitimate and what is fraudulent when both activities are taking place in the same environment.

As shown in **Figure 21**, coin mining generally takes place on a system which the malicious application was using as a host, as opposed to JavaScript (web-based) coin mining. The Education sector experienced the greatest number of host-based coin mining detections. "Dorm room mining operations" are a common way for university students to generate cryptocurrency which they can later exchange for cash. In many cases, the educational institution does not control these end-user devices.

Technology was the second most observed sector for host-based coin mining, at 46 percent, with all other sectors making up the remaining two percent, as shown in **Figure 22**. NTT Security clients in the Technology sector include internet service providers and data center providers. While the Technology sector is heavily impacted because they are hosting data services for a variety of other sectors, the reality is that virtually every sector is impacted by coin mining.

Figure 20

Sectors Most Affected by Coin Mining

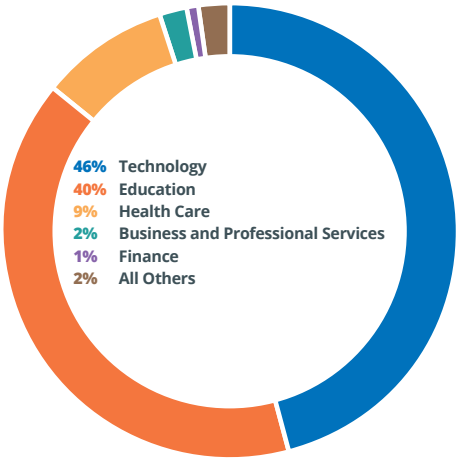
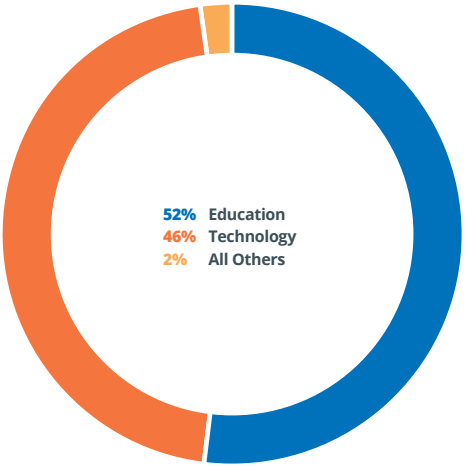


Figure 21

Mining Type	Percentage
Host-based	75%
Web-based	25%

Figure 22

Host-Based Coin Mining



Active Actors and Groups

During 2018, much of the activity related to coin mining was associated with three distinct groups, detailed in **Figure 23**. These groups (Rocke, 8220 Mining Group, Tor2Mine) used variants of XMRig and targeted a wide variety of server software including Apache Struts 2, Jenkins, and JBoss. Each group had their own focus and twist on techniques, as summarized in the following table:

Figure 23
Top Coin Mining Groups Detected

Group	Description
Rocke	Rocke was first observed in the spring of 2018. Various indications suggest Rocke is part of a crimeware group based in China. Rocke made extensive use of vulnerabilities in Struts, WebLogic, and Java, and *social engineering* attacks including fake Google Chrome and Adobe Flash updates. Rocke also delivered destructive ransomware as cryptocurrency prices dropped, but activity faded in late 2018.
8220 Mining Group	8220 Mining Group was first observed in May of 2017, using malicious Docker images. Indications are that members of the group are from China and developed whatMiner. The group has targeted Drupal, Apache Struts2 and Hadoop YARN, among other technologies.
Tor2Mine	Tor2Mine uses tor2web, which allows Tor Hidden Services to be accessed from a browser without connecting to the Tor network. Tor2Mine uses this for command and control services in coin mining campaigns. Tor2Mine uses malicious shell scripts camouflaged as JPEG files which execute code when downloaded and deploy malware. It has used Oracle WebLogic and Apache Struts2 to help deliver mining malware, and also uses PowerShell.

Attacker Motive

The motive behind coin mining is simple – profit. Coin mining is incredibly lucrative for potential attackers and has a much lower barrier to entry than other vectors. Coin mining itself is not malicious, so some anti-virus engines will not flag coin mining activity as suspicious.

Additionally, coin mining is a highly passive method of generating funds. Once an attacker has placed the coin miner in the environment, there is nothing left for the attacker to do except wait while cryptocurrency is generated and delivered to the attacker's wallet.

Attack Pattern and Intrusion Set

Attackers have adapted their attack patterns and intrusion sets to include coin mining in their toolkits. Coin miners usually include other, more malicious functionality. When attackers combine coin mining-capable malware with credential theft campaigns, they obtain a wide range of attack capabilities, not only to execute the initial attack, but also to pivot across the network and solidify their persistence within the environment.

In some cases, NTT Security observed malware which previously had a single capability, but had coin mining capability added to it, making it a more functional malware. Coin mining malware can often be very difficult to detect, with very few indicators of compromise. It is common for malware with coin mining functionality to be detected for other, non-coin mining activities such as malicious script execution, credential theft, and unauthorized network communication.

Linux appears to be the preferred platform for coin mining. This would, however, only be a viable target for certain enterprise servers and IoT devices. Windows systems are the enterprise user platform of choice, so most malware with coin mining capabilities has been designed to target Windows servers.

Coin mining attacks often target systems with high-end Graphics Processing Units (GPUs). These are most often found in end-user graphics cards, which are very efficient at processing the mathematical computations required for coin mining. While enterprise servers may not have the same GPU power available, CPU power and RAM help to close the gap, increasing server viability as coin mining targets.

Historically, one way to detect coin mining was to monitor CPU usage, so an organization can observe when coin miners are consuming available CPU cycles. NTT Security has learned CMM is increasingly being built with "throttles" in place, having a built-in meter to gauge the level of CPU usage. Once that meter reaches a certain level (e.g., 80 percent), the CMM will temporarily stop mining until the CPU usage is below a defined threshold. This is a relatively simple way to obfuscate CMM activity, so while monitoring CPU usage is part of detecting illicit activity on devices, it is not a complete solution.

Of note, coin mining malware tends to be detected due to direct download attempts from IoT botnets or web-based exploit attempts. There are also JavaScript mining options for "drive-by" mining which uses the browser to mine as long as the page is open. The most popular supplier of this code is CoinHive.

Attackers who are dropping only coin mining malware in the environment typically don't want to break the targeted system. These attackers want the malware to run undetected over the long term, enabling them to maintain a revenue stream.

Even though coin mining has become a larger threat over the past year, many organizations simply aren't looking for coin mining malware in their environment. Even after patching the vulnerability which allowed coin mining malware to infiltrate the environment, the attacker continues generating cryptocurrency as long as the infected systems remain online.

Business Risk and Impact

Historically, coin miners have not been overtly hostile to the environments in which they have been found. This is changing somewhat as coin miners evolve and become more efficient. In current scenarios, discovering coin mining malware in the network is an indicator of a bigger problem – namely, how the malware got there in the first place.

Coin mining malware typically enters an environment in the same way as other malware would – by exploiting vulnerabilities. Very often, these are technical vulnerabilities, but phishing is also an often-used tactic.

Coin mining malware can cause hardware resources to run hotter, increasing energy consumption and shortening the lifespan of the systems. While the impact of this is challenging to objectively measure, in a production environment where system resources are critically important, organizations may see a degradation in system capabilities.

Of note, the ability of the coin mining malware to remain relatively difficult to detect may also increase the risk of an inadvertent insider attack from a member of your organization with administrative access.

NTT Security has observed several coin mining attacks, which had varying degrees of impact. In one case, the attacker exploited an Oracle WebLogic vulnerability and gained access to a single internal server. From there, the attacker executed a Monero cryptominer which ran for about three days until the initial server compromise was discovered. The organization removed the malware with limited cost and no ongoing impact.

In another case, an attacker was able to gain remote access, eventually installing coin mining malware in the organization's server farm. After several months, an administrator detected the breach. Recovery activities eventually led to the reimaging of most corporate servers and cost the organization hundreds of thousands of dollars in internal and outsourced security expertise. The attack resulted in the loss of many clients, and the resignation of the company's Chief Information Security Officer.

Whether you bring in an incident response team to help eradicate the coin miner in your environment or manage the removal internally, there will be costs associated with removing the malware. If your customers learn there is coin mining occurring in your environment, it may impact your organization's reputation and may prompt them to go to your competitor.

Coin mining is a big topic today but not the only risk in the world of cryptocurrencies. Attackers are also focused on stealing cryptocurrency from exchanges and personal wallets. As an example, Coincheck and Zaif, Japan based cryptocurrency exchanges, were attacked resulting in the theft of 58 billion JPY (approximately $52.8 million USD) of cryptocurrency in January and 7 billion JPY (approximately $6.3 million USD) in September, respectively.

Personal wallets are also targeted by attackers. For example, Xian News in China reported 600 million RMB (approximately $89 million USD) of cryptocurrency was stolen from a personal wallet. Three attackers were arrested by Chinese police after several months of investigation.

Defense Considerations

NTT Security provides the following five recommendations for mitigating the threat of unauthorized coin mining in your network.

- **Apply least privilege controls for user, developer and application accounts.** Limit or restrict access to resources which a user or application account requires to perform normal functions. This can make it more difficult for coin mining malware to obtain the permissions required for installation.
- **Implement egress and ingress restrictions on the firewall.** This helps to ensure only authorized traffic is allowed. Review firewall rules to ensure only approved traffic can reach production servers.
- **Limit browser-based cryptomining.** There are browser plugins designed to help limit functionality of browser-based cryptomining. The evaluation and installation of effective plugins may help limit the practice. Since many browser-based miners rely on JavaScript, restricting the ability of users to run JavaScript can help cripple this software – though for many users and organizations, this may not be viable, as many websites use JavaScript functionality.
- **Deny Stratum[4] protocol usage.** As of this writing, cryptocurrency mining malware connects to mining pools via the Stratum protocol. Disabling this protocol stops miners before they have to a chance to start mining.
- **Segregate network environment.** This is not a panacea, but it will help narrow down where cryptocurrency mining is taking place and can help guide your next steps to address the threat.

Clearly, coin mining is not likely to subside in the near future – particularly in the Technology and Education sectors – as this is quite a lucrative business. The next section takes a look into another lucrative business, targeting web-based applications.

4 https://slushpool.com/help/manual/stratum-protocol

Security Challenge: Web-Based Attacks

Threat Overview

Web-based attacks, those targeting web-application and application-specific vulnerabilities, are heavily used by threat actors. Successful exploitation can often lead to enormous amounts of back-end data as attackers gain access to supporting databases and systems. These types of attacks target an organization's internet-facing applications and are often associated with large, widely publicized data breaches.

Successful exploitation and subsequent access or manipulation of data could prove catastrophic to an organization's finances or reputation, even if based solely on the sheer amount of data which could potentially be accessed.

These attacks include cross-site scripting (XSS), injection attacks, buffer overflows, mishandled parameters, and many more[5]. While attackers often exploit older vulnerabilities, the threat of unpatched newer vulnerabilities (especially in highly used technologies), or technologies which are often misconfigured (like content management systems), cannot be ignored. Such attacks are regularly integrated into automated tools, so it is not uncommon for the sheer volume of these attacks to be quite high.

Percentage of Web-based Attacks Observed by NTT Security

Historically, as shown in **Figure 24**, web-based attacks account for approximately 25-35 percent of all attacks NTT Security observes across our client base, making these the most commonly used category of attacks globally. For 2018, the number crept up slightly to 32 percent of all attacks, from 29 percent in 2017.

Figure 24

2016	2017	2018
33%	29%	32%

Attacks Against Operational Technology (OT)

The last few years have illustrated how cyberattacks can have a profound impact on critical infrastructure, Health Care, Finance, and Transportation, but we have yet to see the full capabilities of an organized attack.

NTT Security believes:

- Attacks will focus less on specific applications and more on the elements that can impact critical national infrastructure.
- Smart cities and smart homes are on the rise, which may introduce a wider footprint for attacker activities.

What we recommend:

- Consider extending good cybersecurity practices into your operational technology.
- Change default passwords and configurations.
- To the extent possible, segregate operational technology into protected networks which include firewalls and other enhanced security controls.
- Prevent public and wireless access to the OT environments.
- Follow standard security hygiene practices.

5 https://cwe.mitre.org/data/definitions/699.html

Threat Targets

While every sector is targeted by such attacks, NTT Security researchers have historically observed higher volumes of application-specific and web-application attacks in certain sectors. In 2018, the five most targeted sectors were Finance, Business and Professional Services, Health Care, Retail, and Manufacturing, as shown in **Figure 25**. The most targeted sectors often have similarities – one of which is that they tend to have a strong internet presence. Typically, a stronger internet presence means more applications are exposed to the public web, creating a larger attackable surface. For this reason, sectors like Retail and Finance tend to be highly targeted. These sectors are more reliant on external connectivity, have customer portals, and maintain a strong web presence which generates visits and traffic. They also often maintain financial information with tangible value.

Business and Professional Services, and Manufacturing are widely considered high priority targets due to the high-value data and intellectual property they hold and the sensitive trust relationships they maintain with third parties. Health Care has historically also been a high priority target due to the large amount of sensitive patient information they hold. In every case, the five sectors in **Figure 25** showed a higher than average share of web attacks.

These attacks target organizations with high volumes of sensitive data, which could be used for purposes of financial gain, industry superiority, or corporate espionage. They often give attackers remote access to back-end systems and are known to result in significant data loss. NTT Security researchers have observed nation-state actors leveraging these types of attacks to infiltrate organizations across all vertical markets, to obtain sustained access, and to gather sensitive data for enhancing their own technical capabilities (their technology or manufacturing capabilities). Stolen financial details can prove valuable regardless of whether the attacker uses the credentials them self or sells them on the *dark web*.

Threat Geographic Activity

Globally, organizations experienced an average of 32 percent of all attacks as web attacks. Regionally, there were small differences between the percentages and relative volumes of these attacks, as shown in **Figure 26**. Clients in both EMEA and APAC experienced slightly higher ratios of web attacks, and clients in the Americas experienced slightly under the global average.

While 32 percent of all global activity was related to web attacks, there were some significant geographic differences; the most notable are shown in **Figure 27**. EMEA Retail targets experienced an average of 85 percent of their hostile activity being a combination of web-application and application-specific attacks. Globally, for some clients, web attacks represented more than 90 percent of all their hostile activity. Web attacks focused on Japan accounted for 53 percent of all attack activity against the country.

Active Actors and Groups

A large variety of threat actors take advantage of web-application and application-specific attacks. Advanced attackers and nation-state actors develop and *weaponize* exploits for new vulnerabilities, including vulnerabilities discovered by those same actors. Mature, high quality and reliable exploits are implemented into exploit toolkits. These kits are sold to any hostile actor with the funds and inclination to buy the tools. Once included in a toolkit, these attacks can be performed with little or no skill. As a result of this automation, attacks which may have in the past focused on a single target, sector, or geographic area can now rapidly spread around the globe and throughout the targeted sector.

Figure 25
Highly Impacted Sectors

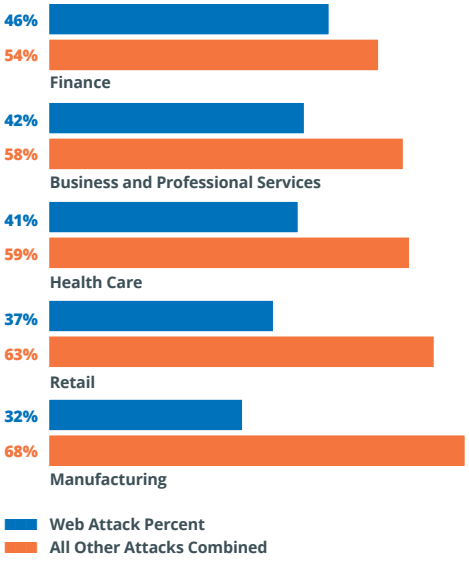
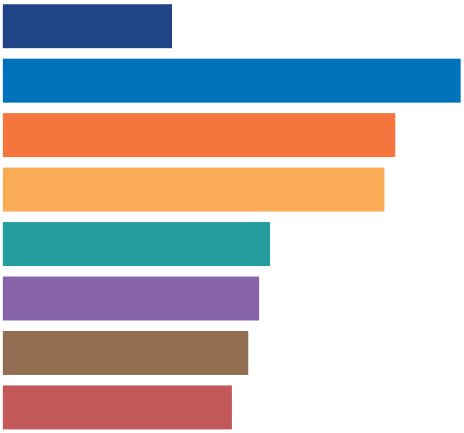


Figure 26
Percentage of Web Attacks by Region

32% Global Average
33% EMEA Average
25% Americas Average
36% APAC Average

Figure 27
Percentage of Web Attacks by Specific Sectors



32% Average
85% EMEA Retail
73% EMEA Business and Professional Services
71% APAC Health Care
50% Americas Manufacturing
48% APAC Finance
46% Americas Finance
43% EMEA Finance

Below are several of the threat actors, from state-sponsored to cybercriminal, which NTT Security observed during 2018 leveraging various application vulnerabilities against multiple sectors. Various security companies often have different naming conventions for applying attribution to malicious actors and campaigns.

- **APT39** is an Iranian group of threat actors who routinely identify and exploit vulnerable web servers to install web shells such as ANTAK and ASPXSPY. They have been observed using stolen credentials to compromise externally facing Outlook Web Access (OWA) resources.
- **APT34** (OilRig) is another Iranian group whose activities are similar to APT39 in terms of targeting and infrastructure.
- **APT27** (Emissary Panda, TG-3390) is a suspected Chinese threat group which has extensively used strategic web compromises to target its victims.
- **APT35** (Newscaster, Magic Hound), is a suspected Iranian threat group known for using Havij, an automated SQL Injection tool distributed by the Iranian ITSecTeam security company.

As we observe each year, new vulnerabilities are quickly exploited by sophisticated actors, once again highlighting the fact that critical vulnerabilities should be patched as quickly as possible in client environments.

Attacker Motives

The goal of web-application and application-specific attacks is determined by the motivation of each actor, as detailed in **Figure 28**.

- **Access** pertains to attackers wishing to further infiltrate the targeted organization or to conduct additional attacks against other victims.
- **Influence** refers to attackers using system access to interfere with the target's operations, typically for hacktivism or extortion.
- **Profit** is typically the primary motive behind web-application and application-specific attacks. Most often, actors attempt to steal sensitive information, such as trade secrets, personal data or financial data.

Attacker Pattern and Intrusion Set

Application-specific and web-application attacks most often rely on leveraging an unpatched vulnerability or misconfigured system in the targeted environment. The true effectiveness of these attacks stems from two facts:

- New exploits can be very effective if they are developed before patches or signatures are released. While patches for many new vulnerabilities are released reasonably quickly, some are not, and weaponized exploits for vulnerabilities can be very effective.
- These attacks are regularly automated and conducted using a wide variety of tools, which enables more attackers to use them. Tools can be used to scan for vulnerable applications, verify the existence of the vulnerability, and attempt to exploit the vulnerability, all with minimal interaction by the attacker.

Figure 28

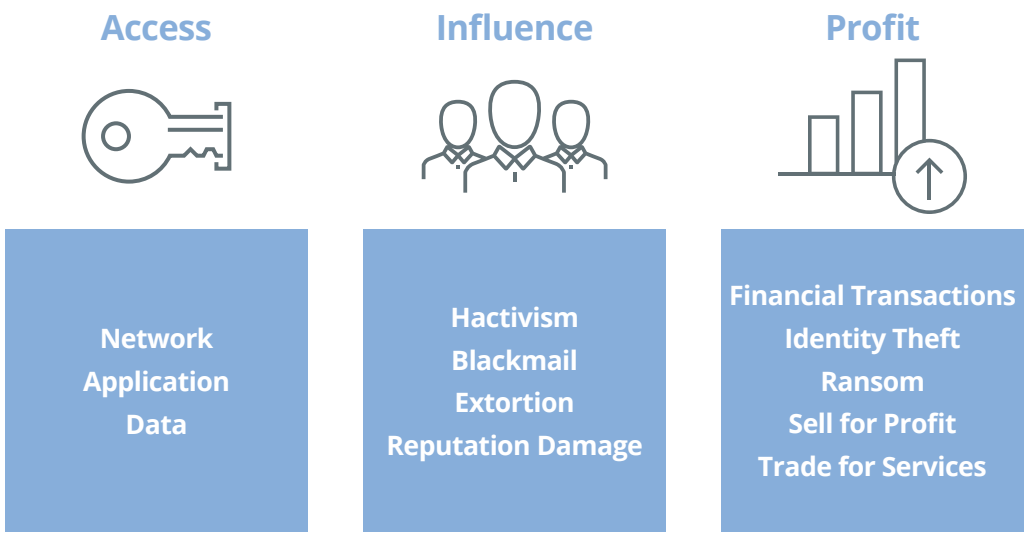
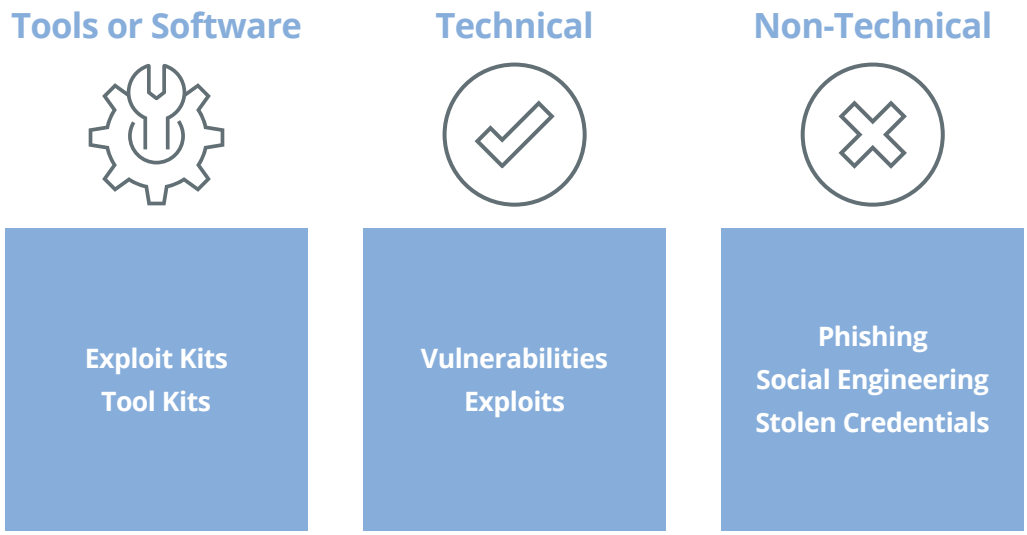


Figure 29



Further detailed in **Figure 29**, these attacks are often one component of a multi-vector attack which can include social engineering, phishing, stolen credentials, and other techniques which work with web-based attacks in a complementary manner. While these non-technical attacks are not part of the web-application or application-specific attacks, their use can increase the effectiveness of the more technical attacks.

Business Risk and Impact

Web-application and application-specific attacks target vulnerabilities in the technologies most widely used in organizations. Any organization with a web presence is exposed to these attacks, and the larger the web presence, the larger the attack surface. Successful exploitation of these vulnerabilities can lead to system compromise, providing the attacker remote access to the application, data, and the underlying system.

Successful attacks have resulted in significant data breaches. Depending on the breach, these attacks can be easily detected or quite stealthy depending on the goals of the attacker. Some of these breaches may last for an extended period, for example, if the attacker is attempting to maintain long term persistence for data theft. Others may embrace being easily detected in cases of ransomware and political website defacement campaigns.

In one example, a large financial company was breached via an unpatched instance of Apache Struts, which had been subject to many critical vulnerabilities. Threat actors gained access to the company's internal environment and exfiltrated database tables containing financial details, including social security numbers, for millions of users. The breach exposed the account numbers and credit card details of many users, and this data became readily available on the dark web. The company spent hundreds of millions of dollars in actual recovery costs, and their stock value dropped about four percent over the next year (while their main competitor's stock increased 55 percent).

Defense Considerations

- **Prioritize patching.** Ensure operating system and application patching processes are comprehensive and reliable. Prioritize patching efforts based on your exposure, most critical systems, and highest risk vulnerabilities.
- **Segment your network environment.** Segmentation can restrict unauthorized movement across your environment. If attackers can breach back-end servers, they may be able to move laterally to access other portions of your network, doing further damage, and possibly gaining a foothold across multiple systems.
- **Enforce secure coding.** Ensure secure coding techniques are taught and enforced for all internally developed applications. For third-party applications and tools, use reputable vendors, and prioritize organizations which have a verifiable secure coding practice.
- **Implement application gateway firewalls.** Use web and application gateway firewalls to help protect key internal and external applications.
- **Perform regular vulnerability scanning.** Evaluate your own environment regularly, track all discovered vulnerabilities, and prioritize and patch them in an aggressive manner. Evaluate scan results for trends in the types of vulnerabilities observed. Adapt internal processes and controls to help reduce future exposure.

Web-based and application-specific attacks can result in devastating access to an organization's network. These types of attacks can provide access for threat actors far beyond just the initial compromise. In our next segment on credential theft, we look at the value stolen credentials can provide to attackers.

Security Challenge: Credential Theft

Threat Overview

NTT Security's Global Incident Response Team recently supported a client who was impacted by a series of credential leaks. This caused significant privacy and data security concerns for their existing clients, a circumstance which we observe all too often in today's digital society.

Every day we use credentials for access to websites, computers, smart devices and other resources to complete business and personal transactions. We engage in these activities so frequently that the use of credentials is often taken for granted. According to a 2017 study by LastPass[6], the average business user has 191 passwords, and 61 percent of users share the same passwords across multiple accounts.

Regardless of the attack pattern, some facts remain constant: obtaining and using compromised credentials is valuable, and an attacker's process behind credential theft receives the attention to detail you might expect to find in any legitimate organization's workflow, as shown in **Figure 30**.

Figure 30

During collection, credentials are harvested from sources using a wide variety of creative techniques discussed later in this section. The information associated with the credential collection is then processed to remove data which does not fit the attacker's goals. The attacker may perform additional validation to identify the value of the stolen credentials, verifying the credentials are valid and exploring what type of access they provide. Finally, the attacker may use the credentials to further their own objectives or perhaps sell or trade them to other cybercriminals who can find value in their use.

NTT Security Observations

NTT Security researchers continue to analyze widespread activity related to credential theft. Some of the most common activities include phishing (targeting details are shown in **Figure 31**), malware activity, social engineering and other technical and non-technical means. We discuss these activities in more detail in the Attack Pattern and Intrusion Set section below.

6 https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose.html/

Figure 32 shows some of the common technical attacks used to help commit credential theft. "Malware" means the attack was based on detection of malware which had credential theft as at least one capability. "Phishing"-related activity indicates an attempt, for instance, to direct a user to a hostile site designed by an attacker to look like a legitimate website but with the goal of stealing the user's credentials. As an example, a fake banking site may attempt to gather user credentials or other sensitive information like account numbers. From NTT Security observations, both techniques were highly utilized during 2018.

Phishing attack targets included a variety of end user credentials, including productivity software suites, online document signing software, and financial organization logins, as shown in **Figure 31**. The most targeted Microsoft credentials were O365 credentials, with a significant amount of the phishing traffic originating from systems in Nigeria. The Google accounts being targeted included user accounts for Google Drive, Google Sheets and Gmail. In every case, attackers were targeting username/password pairs.

Not only were Microsoft applications targeted in phishing attacks, but *malspam* campaigns were used as well. Over 95 percent of all malspam related to credential theft targeted the vulnerabilities in either a Microsoft Office application or a Microsoft operating system, with nearly 35 percent of this activity taking advantage of CVE-2017-11882, a Microsoft Office memory corruption vulnerability.

Malware-related attacks were associated with the delivery of malware using credential-theft capabilities. Keyloggers have advanced to the point that it is hard to call a keylogger "just a keylogger" any longer, as information stealing and credential theft modules continue to migrate into a wider variety of malware. **Figure 33** includes the malware most commonly observed by NTT Security containing keylogger capabilities. Relatively few phishing websites for banking credentials were observed in 2018. However, NTT Security observed more credential theft malware, specifically banking *Trojans,* associated with credential theft attacks. Much of the spam distributed throughout 2018 delivered banking malware, such as:

- **Trickbot** – a banking Trojan and credential stealer, capable of harvesting emails. For much of 2018 it saw significant activity because of its association with the Necurs botnet, which spread Trickbot through extended malspam campaigns.
- **Hancitor** – a banking Trojan and downloader. It most commonly spreads via phishing emails, especially downloadable faxes or a variety of shipping notifications.
- **Fareit** – a Trojan, credential stealer and downloader often associated with Pony. Fareit is commonly distributed by phishing emails, especially invoices, delivery notices and tax notices.
- **Emotet** – a banking Trojan which functions mostly as a *dropper* or downloader of other banking trojans. Emotet is most commonly spread via phishing emails, especially receipts, shipping notifications and invoices.
- **LokiBot** – a Trojan and information stealer, including credential stealing, which can also target Android devices. LokiBot is commonly distributed via malspam, especially invoices, shipping notifications or order confirmations.

While NTT Security detected dozens of different malware families, the most effective credential stealers were equipped with additional capabilities to help ensure they spread easily, were difficult to detect, and were hard to remove. Most were spread via phishing emails with a wide variety of subjects, though some of the more common subjects were listed for each variant above.

Figure 31
Phishing Targets

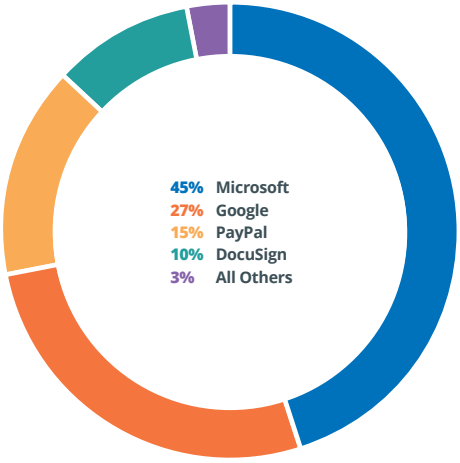


Figure 32
Technical Attacks for Credential Theft

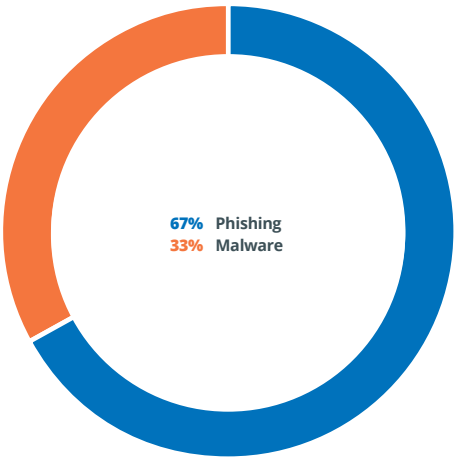
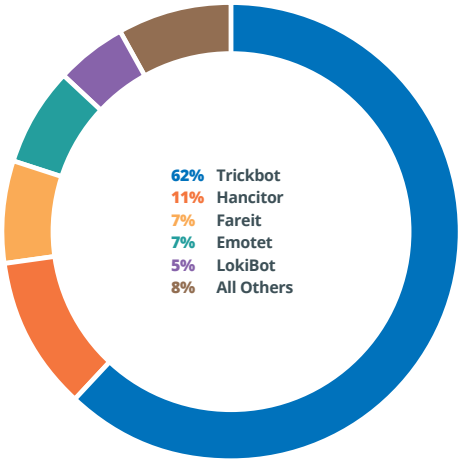


Figure 33
Keylogger Malware



Although no sector is immune to credential theft, it is important to realize activity in specific sectors may help prioritize mitigation efforts. We identify the sectors targeted the most in 2018 in **Figures 34** and **35**. This is a diverse list of sectors, which are targeted for a combination of data and access, some for the following reasons:

- **Retail and Finance** are targeted for access to customer data, including credit card and other financial details.
- **Telecommunications** is targeted for access to infrastructure and environments supported by ISPs and datacenters.
- **Health Care** is targeted for access to sensitive systems as well as both private and financial data.
- **Technology, Manufacturing, and Business and Professional Services** are targeted for long-term system access designed to locate and exfiltrate proprietary information.
- **Media** is targeted for theft of content and access to servers for long-term system access and theft of computing services.

Phishing attacks and malware were both highly used. In most cases, the techniques supported each other directly. For instance, phishing-related attacks delivered more malware to end-user systems than other techniques; in contrast, phishing attacks also focused on luring users to phishing sites. Variances in the focus of these attacks account for the differences in the targeted sectors.

- Malware attacks tended to target the users in the given environment, providing more than the user credentials associated with that organization. For instance, credential theft malware targeting a retail organization not only gathered credentials for that organization, but also gathered credentials for other email accounts, social media, and financial services sites.
- Phishing attacks which focused on credential theft gathered a wide variety of credentials as well, but tended to focus on credentials for the targeted sector. A phishing attack against a technology company, for instance, would include a fake technology site to gather credentials for specifically that target.

Threat Geographic Activity

The Americas and EMEA each accounted for about 40 percent of malspam, with sources in APAC accounting for the rest. NTT Security detected malspam related to credential theft from 94 countries across all regions. The top 10 sources accounted for nearly 82 percent of all the malspam activity with the top five listed in **Figure 36**.

Figure 34
Sectors Targeted by Credential Theft Phishing

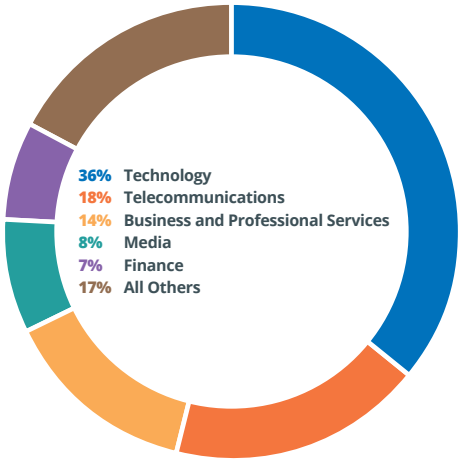
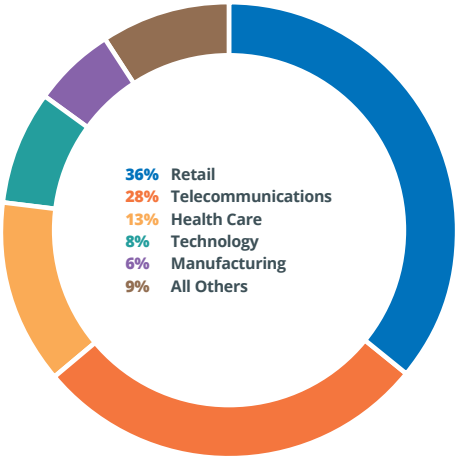


Figure 35
Sectors Targeted by Credential Theft Malware



Retail Will Remain a Focus for Attackers

Retailers spend millions of dollars on advertising to ensure their brand makes it into your home. One of the best opportunities an attacker has to achieve their goals and gain notoriety is to attack those well-known brands.

- Retailers will continue to be a target for attackers – whether the attacker is just trying to make a statement, or if they are cybercriminals intent on stealing financial data.
- Large brick-and-mortar establishments will continue to be invaluable targets for attackers due to the size, complexity, and inherent security challenges of maintaining geographically diverse infrastructures.

What we recommend:

- Leverage a defense-in-depth security strategy.
- Implement an operational patch management program (one which mitigates risk while ensuring operational continuity)

A defense-in-depth strategy and an operational patch management program are critical to reducing risk associated with the continued targeting of organizations in the Retail sector.

Active Actors and Groups

NTT Security continually monitors malicious actors and groups who focus on a variety of threats, including credential theft. It is important to understand which individuals or groups are behind the attacks, what their motives are, and what attack patterns they use. Many of these actors use techniques which are similar in nature and motivations, yet each actor tends to employ their own methods. The table in **Figure 37** summarizes some of the known characteristics of selected actors. Though a box may not be marked, an actor may still employ that technique or tool; however, it is not something they are particularly known for.

- **APT10** (menuPass) has used a modified version of the penetration tools wmiexec.vbs and secretsdump.py to dump credentials. RedLeaves, which has been attributed to APT10, can harvest usernames and passwords typed into or stored in a web browser.
- **Seedworm** (MuddyWater) uses a tool which steals passwords saved in users' web browsers and email, as well as open-source tools such as LaZagne and Crackmapexec to obtain Windows authorization credentials.
- The Lazarus Group also leveraged **Mimikatz** to extract Windows credentials of currently logged-in users and steal passwords stored in web browsers.
- The **Oilrig** threat actor group has used their TwoFace webshell to issue commands to gather credentials using the Mimikatz and LaZagne tools. In cyber espionage campaigns, credential harvesting is often used to move laterally through targeted networks.
- **APT28**, like many other APT groups, regularly uses both publicly available and custom password harvesting tools.
- **Other criminal groups**, such as the one behind **Emotet**, primarily collect usernames and passwords for monetary gain.

Figure 36

Most Common sources of Phishing Malspam

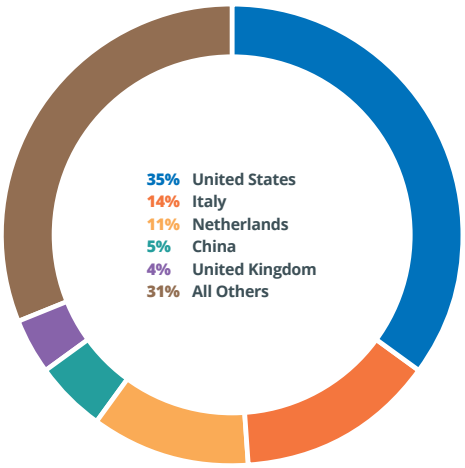


Figure 37

Known Characteristics of Selected Actors

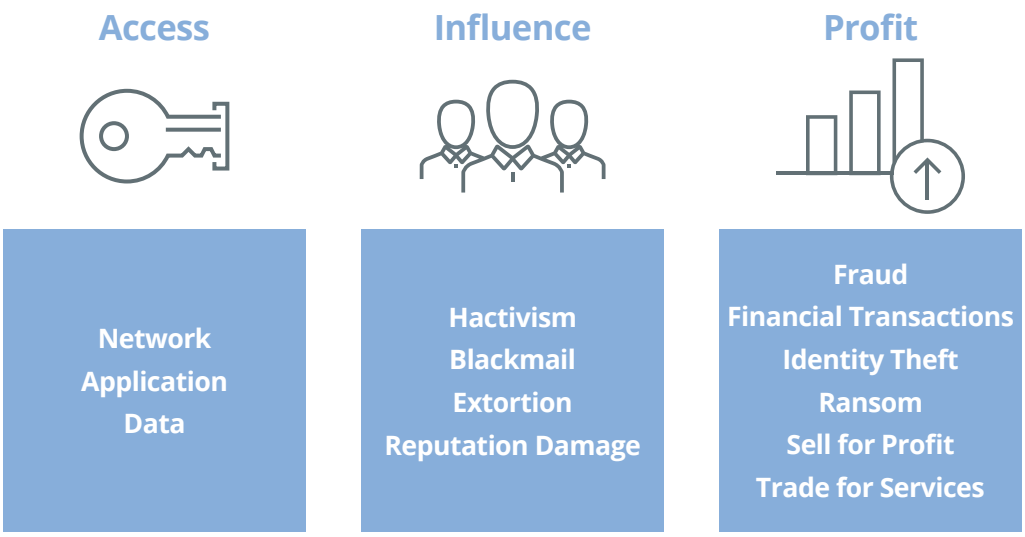
	APT10 (menuPass)	Seedworm (MuddyWater)	Lazarus Group	OilRig	APT28	Other Criminal Groups
Collects usernames and passwords for monetary gain	✗	✗	✗	✗	✗	✗
Deploys publicly available and custom password tools	✗	✗	✗	✗	✗	✗
Uses TwoFace webshell to issue credential gathering demands				✗		
Uses harvested credentials to move laterally throughout the network				✗		✗
Uses modified version of wmiexec.vbs to dump credentials	✗					
Uses modified version of secretsgump.py to dump credentials	✗					
Steals passwords stored in email		✗				
Steals passwords stored in browsers	✗	✗	✗			
Uses crackmapexec tool		✗				
Uses Mimkatz tool		✗	✗	✗		
Uses LaZagne tool		✗	✗	✗		
Uses RedLeaves	✗					

Attacker Motives

Credentials are the keys which protect an organization's networks and data from unauthorized access. This makes stolen credentials a valuable target for cyber-criminals, hacktivists and nation-state actors. In fact, the use of stolen credentials has been involved in some of the largest data breaches of recent years. Although we often associate the use of credentials with direct access to resources, there are many other ways attackers can benefit from their use.

NTT Security organizes attacker motives into three categories: access, influence and profit as depicted in **Figure 38**. Attackers may have even more specific motives depending on their goals.

Figure 38



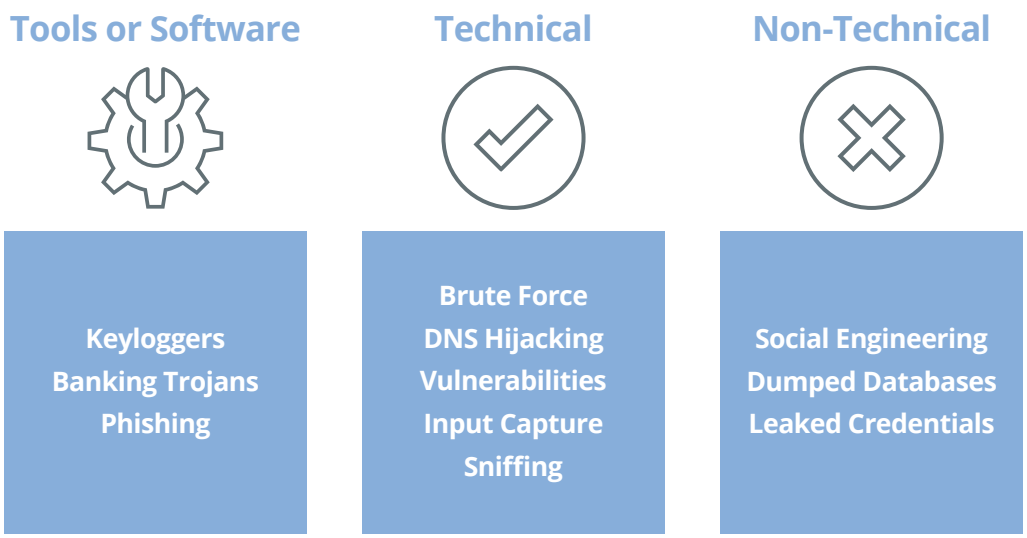
- **Access** relates to the use of stolen credentials to gain access to resources and the underlying data and may involve both short-term and persistent access.
- **Influence** can involve manipulating a person, or our impression of a person, brand or product. It may include activities related to reputation damage, blackmail and extortion.
- **Profit** relates to using stolen credentials for fraudulent activities including financial transactions, bartering with other cybercriminals and identity theft for financial gain.

Attack Pattern and Intrusion Set

Attackers continue to refine their attack patterns and intrusion sets and develop new tools. Attackers also often rely on timeless and effective methods such as social engineering, keyloggers, and phishing attacks. **Figure 39** provides an overview of some of the different tactics and tools malicious actors may employ during credential theft activities.

Using stolen credentials to gain an initial foothold into a targeted network negates the need for an attacker to leverage *zero-day* vulnerabilities or customized malware. In order to maintain a low profile, some threat actors use stolen credentials in a limited manner, to aid in avoiding detection and ensure long-term access. Other attackers prefer to strike quickly by logging in using stolen credentials and quickly stealing any data that may be of value.

Figure 39



Credential theft and reuse enables prolonged access within the target environment. Since access is accomplished with valid credentials, it is less likely the access will trigger an alert. This potentially allows an attacker to evade detection, and bypass security controls which would normally be effective against other attack methods such as application-based attacks, brute-force activity or *spyware*.

Keyloggers are typically distributed through email or drive-by download attacks. Specific keyloggers, such as Pony, Agent Tesla, and Hawkeye have been extremely popular keyloggers used during credential harvesting campaigns. Agent Tesla is often distributed manually while Pony is found frequently in large malspam campaigns and HawkEye is often associated with spear-phishing attacks. Keylogger software has been distributed as PE32 and PE64 executable binaries, and is primarily used in environments with Windows operating system architectures.

Zero Trust Is Moving Toward Digital Trust

During 2018, an increasing sophistication of attacks, along with the rise of insider threats, led IT teams across the globe to adopt a "trust no one" philosophy, resulting in identity verification solutions implemented at a level well before anyone inside or outside the organization could access company data. This implementation often resulted in lost productivity or reduced effectiveness in customer engagement.

Digital trust is the way of the future

While "trust no one" has paved the way for IT teams to build "digital fingerprints" for employees, only time will tell if this results in increased productivity and a better experience for the end user.

An evolving workforce increases digital trust challenges

Whether or not you have implemented a "trust no one" type of policy in your organization, a digital trust model is challenging to maintain, especially as the workforce continues to evolve. Activity once considered abnormal (e.g., logging in and working at 23:00) is the new normal, making it more difficult to establish a digital fingerprint for employees.

Ensure there is adequate flexibility to ensure productivity

If you do choose to implement a digital trust model, ensure there is enough flexibility in your organization to shoulder a potential loss in productivity and an increased workload on your IT teams.

Data collection techniques depend on the type of campaign being carried out, and the attacker's preference and familiarity with the tools available. Web requests are typically sent to a Command and Control server once data has been collected and is ready for exfiltration. Some keyloggers use SMTP, which sends the data directly to the attacker's email box. FTP servers are also commonly used and prove valuable to attackers since they can transport large amounts of data very quickly. SQL servers can also be used to push entire database contents to attacker-controlled database servers using standard SQL statements.

Victims are also subject to follow-on attacks, as attackers regularly sell stolen credentials on the dark web. Prices vary greatly depending on the type of credentials, but valid credentials often sell for US $10-$50 or more. Cybercriminals who are active in the credential market can generate millions of dollars in income, making these activities very lucrative.

Business Risk and Impact

Stolen credentials can have a severe impact on organizations. This often includes loss of confidentiality, integrity, or availability of sensitive data related to theft of proprietary information, disruption of regular operations, financial losses, and potential harm to an organization's reputation.

Longer term impact may also include loss of revenue, a C-level executive being forced to resign, devaluation of stock, impact on potential mergers and acquisitions, loss of intellectual property, and compliance penalties. The organization may also be exposed to blackmail, extortion and corporate espionage, all having similar consequences to those previously mentioned.

In one case, a student sent phishing emails to several teachers. At least one of the teachers clicked the link in the phishing email and ended up installing the Agent Tesla keylogger on their system. The student used captured credentials to change their grades and to post falsified transcripts. The breach was discovered by the teacher, and recovery included reimaging of compromised systems. This was followed by disciplinary action taken by the school and criminal prosecution of the student. While the long-term effect of this breach was minimal, it had a very real short-term impact for the student and the educational institution.

Another example occurred in 2013, as a large retailer suffered a damaging data breach, where skilled attackers gained access through compromised credentials. The exfiltrated data involved millions of customer records, including account details and credit card numbers. The organization's 2016 annual report indicated the cost of the breach was hundreds of millions of dollars and its earnings fell nearly 50 percent during the months following the breach. Additionally, the retailer's stock price dropped more than 10 percent, leading to the resignation of key C-level executives. Organizations around the world are continuously faced with similar circumstances, highlighting that even the smallest details in a security program are important.

Defense Considerations

Although every organization has different data, controls, and requirements, the following defensive considerations will aid in mitigating the threat of credential theft:

- **Implement multi-factor authentication.** Organizations must leverage multi-factor authentication on key systems, particularly where the account has administrative level access. This defensive control makes it considerably harder for attackers to gain access to sensitive information and networks by exploiting legacy username and password controls.
- **Segment your network environment.** Increase access control throughout internal and external networks so even employees with legitimate credentials can only access areas of the network supporting their job function.
- **Enforce "least privilege" and segregation of duties.** Control access to data, tools, applications and users with the lowest privilege level possible, the concept of "need to know." This will result in less privileged access available for an attacker and ensure processes cannot be completed entirely from start to finish by a single person, role or application. This will reduce the potential impact of fraudulent activity.
- **Implement network activity and data leak monitoring.** Ensure your organization implements and enforces a data leak protection policy. As part of the policy, your organization should monitor for data exfiltration, public disclosure of sensitive information and abuse of privileges. Leveraging threat intelligence capabilities can greatly assist in the identification of leaked data.
- **Train employees to be vigilant against phishing attacks.** Such attacks are often designed to compromise user credentials and harvest other sensitive data. Increased employee vigilance will not stop these attacks from occurring, but can decrease the likelihood of exposure while enhancing the organization's ability to manage and respond to the threat.

Compliance, coin mining, web-based attacks, and credential theft, have been big challenges for organizations to face in 2018, and likely will continue into 2019. Threats will continue to evolve, and NTT Security researchers are vigilant in identifying what threats lie ahead. NTT Security, along with our extended NTT capabilities, are looking beyond 2019 to innovative solutions to address current and future challenges. Read more about some of the interesting research and solutions being developed in our next section, NTT Innovation Highlights.

NTT Innovation Highlights

Botnet Monitoring and Global Backbone Visibility

Applying Machine Learning to Internet Traffic Analysis and Botnet Infrastructure Detection

NTT is in a unique position as a Tier 1 backbone internet carrier, which allows the company the access needed to analyze much of the traffic flowing across the internet. As cloud adoption and the Internet of Things (IoT) are driving digital transformation at an accelerated pace, cybersecurity perimeters are being rapidly extended. Conventional perimeter defense is not as effective as once perceived. Attackers continue to increase the sophistication of their capabilities by building and operating botnets, *their* cloud infrastructures, and exploiting IoT devices.

In collaboration with NTT Communications and NTT Secure Platform Laboratories (SC Labs), NTT Security strives to protect its customers from botnet attacks. Using our visibility beyond perimeters while collecting and analyzing data from our global backbone networks, and using the latest machine learning technologies, NTT Security is gaining a detailed understanding of botnet structures. Currently, we are focusing on the detection of *Command and Control (C&C)* servers, a core component behind botnets, by applying machine learning to analyze massive amounts of network data in real time.

Many existing detection techniques involve advanced machine learning for classifying internal malware infections and distinguishing C&C call-back from normal traffic patterns. However, today's threat actors migrate botnet infrastructure (e.g., C&C servers) daily, and traditional perimeter defense is subject to limitations on coverage and agility. In the near future, with the constant increase in sophisticated attack tactics and the growth of IoT, threat actors may extend their resources globally, thereby reducing an enterprise's capability to protect themselves due to their lack of global visibility of a botnet's infrastructure.

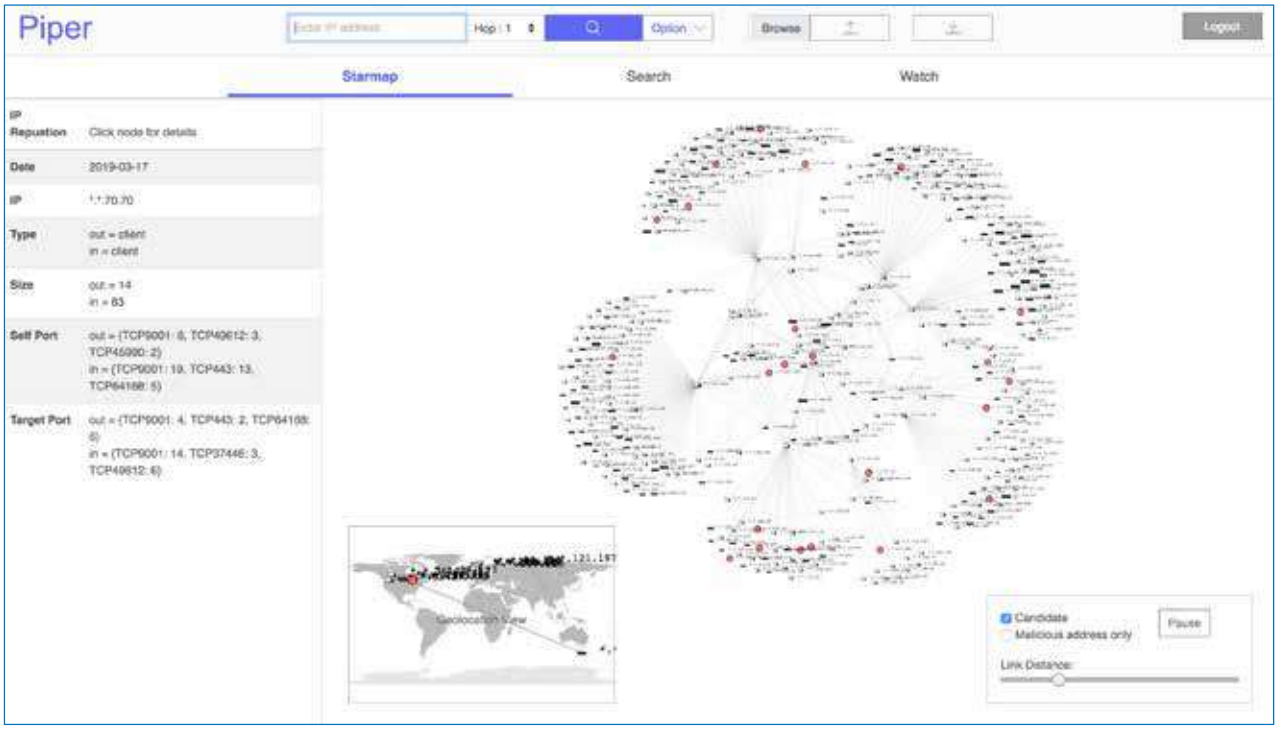
To capture a holistic view of botnet infrastructure, NTT Secure Platform Laboratories and NTT Security focus on internet traffic data collected from our global network infrastructure. With large-scale traffic data analysis, we dig into hierarchical botnets consisting of various functional components such as bots, C&C servers and botmasters while tracking real-time changes to their ecosystems.

We use two distinct but complementary techniques to analyze network traffic for botnet detection: machine learning and graph mining. Machine learning can detect C&C servers in a broader scope, is capable of detecting unique variations between botnets, and requires a lower degree of human intervention to implement and operate. In contrast, graph mining produces highly-accurate prediction in a narrower scope and can detect botnets in nearly real time. Also, the predictions from graph mining are interpretable because it is based on well-known rules created by human experts. These techniques are complementary because we can apply machine learning to results from graph mining and vice versa. In this way, we are continuously expanding our knowledge on botnets and as a result, our predictions constantly precede major vendors, in some cases by weeks.

We have implemented a platform named Piper, a highly-scalable machine learning pipeline. Based on our patent pending algorithms, it enables us to handle billions of flows hourly, generating 300+ unique statistical features (for example, global geolocation distribution) for each internet host and track their locations.

Figure 40

Piper Machine Learning Pipeline Maps Relationships Between Detected Hosts



Piper can concurrently pipeline multiple modules for detecting threat actors by leveraging supervised, unsupervised and semi-supervised machine learning techniques in a highly flexible manner. For mapping the relationships among detected hosts, our visualization tools implemented as Piper modules search hundreds of millions of interconnected hosts, as shown in **Figure 40**.

Graph mining implements our patent pending algorithms and analyzes traffic data as graph stream to detect botnets rapidly. Graph mining assumes neighbors of malicious hosts with specific traffic patterns are also malicious. For example, a host that is a direct neighbor of a victim and has many connections (or high centrality) is detected as malicious (**Figure 41**). We have defined several sets of graph patterns, each of which is for a specific malware family, and we detect new malicious sites by applying these patterns to traffic data of known malicious hosts. We have implemented a distributed graph mining pipeline that can analyze more than 300,000 flows per second.

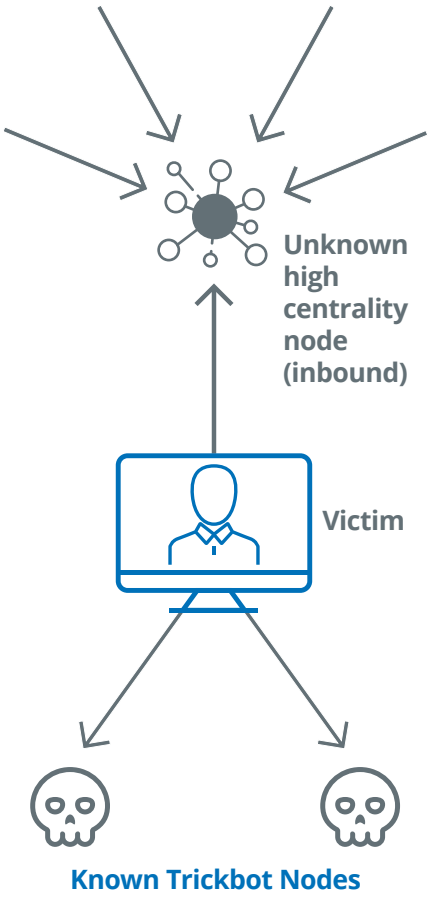
With managed security services powered by the broad internet visibility of botnet infrastructure, we have the capability to deliver comprehensive threat intelligence beyond the perimeter. The intelligence is not only actionable but can also be valuable in the early detection of moving targets.

NTT continues to further leverage our global visibility and R&D capabilities which includes the detection of botnet structures beyond C&C servers, correlation with passive DNS data analysis, integration with active scanning, automated network and security orchestration, and broader collaboration across service providers.

In 2018, NTT Security officially announced adding these botnet detection activities to its Managed Security Services. The visibility NTT has into an extensive portion of all internet traffic offers numerous ways to analyze, detect, and most importantly, defend against threats. The next section looks further into automation of threat sensing from a holistic perspective.

Figure 41

Malicious Host



Cyber Threat Sensor: Location Agnostic, Holistic, Software Defined Threat Detection

Digital transformation projects strive to improve the organization's services and to differentiate their market offerings from their competitors. This may be through improved customer experience, new innovative services, process improvement, or a completely new business model.

This focus on transformation is driving the consumption of new service delivery architecture models, moving away from conventional practices such as static data centers with a clearly defined perimeter. Typically, these new architectures consume cloud-based services, often with large scale connectivity to thousands of devices, fueled by IoT projects.

With transformation, we should also consider the increased adoption of automation and orchestration in order to "flex" architectures based on the demand being placed upon them, service availability and the cost of computing and storage. This poses a significant challenge to organizations' cybersecurity practices attempting to deliver a holistic view of potential cyber threats, regardless of where their assets may be.

In order to deliver a location agnostic, holistic view of these threats to future service architectures, NTT Security's threat detection needs additional components that are fluid and agile. NTT Security is currently developing Cyber Threat Sensor to handle this demand.

Cyber Threat Sensor is a software defined threat detection system that can be deployed rapidly within cloud environments, on edge devices, within virtual/container environments, as part of SDN/SD-WAN orchestration, and in many other use cases, in a consistent, automated, timely manner.

The intention is for Cyber Threat Sensor to be deployed in any location, on almost any platform, alongside a customer's assets. Once deployed, Cyber Threat sensor ingests all network traffic, translating this traffic to event logs which are then analyzed by our proprietary rule engine and AI powered analytics. Should a threat be detected, Cyber Threat Sensor will automatically capture the network packets triggering this event and raise this as an incident in our portal, or escalate to a SOC analyst for further investigation, analysis and remedial action. Depending on the deployment, Cyber Threat Sensor is also capable of full packet capture which can aid incident response should detailed analysis be required.

Figure 42

Deploying multiple instances of Cyber Threat Sensor across multiple locations also provides the ability to cross correlate attacks, in real time, to keep track of adversaries climbing the Lockheed Martin Cyber Kill Chain®[7] across multiple locations.

With the complementing features of Cyber Threat Sensor and NTT's MSSP services, customers can regain holistic cybersecurity visibility that is often lost when consuming diverse delivery architectures.

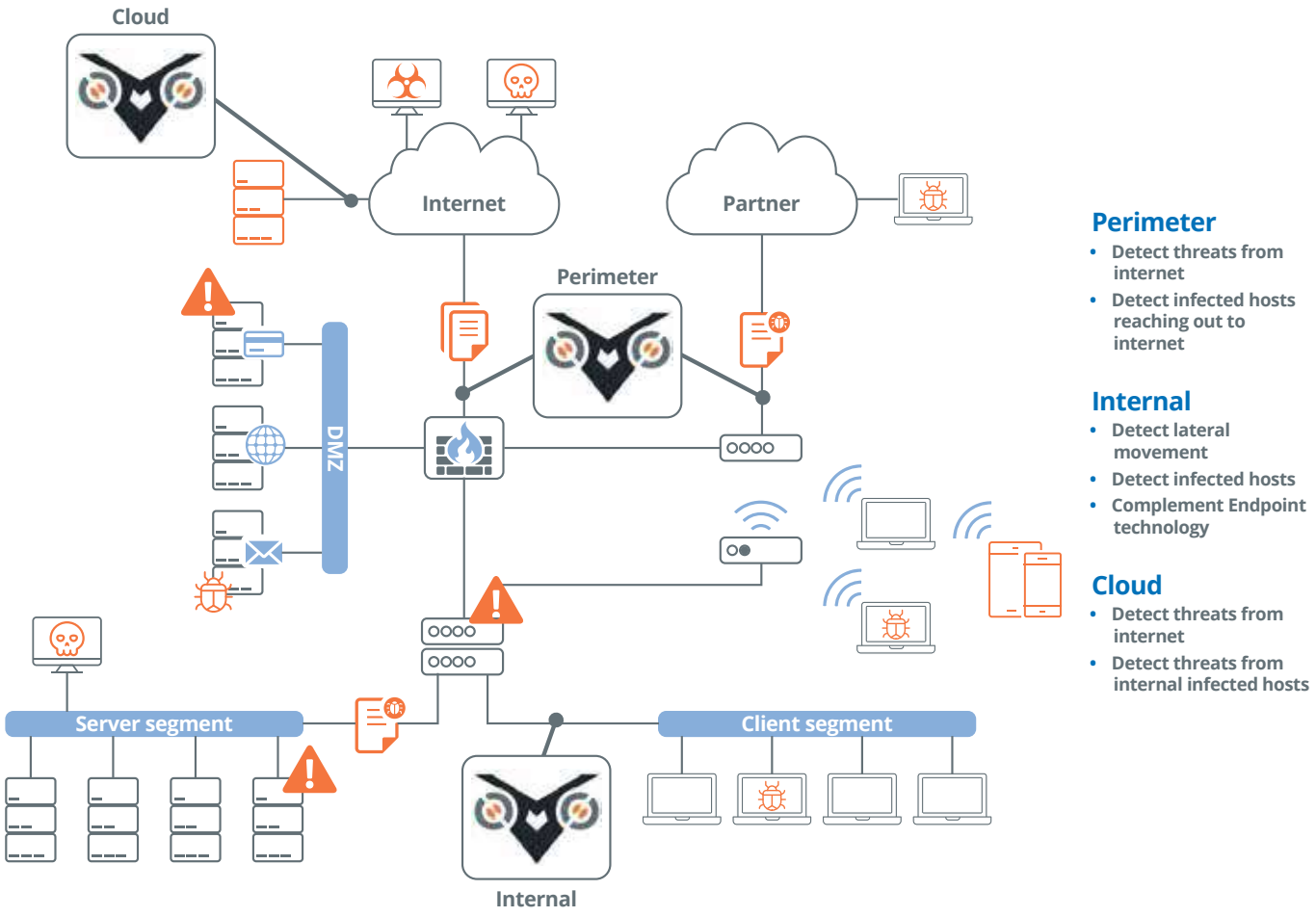
Cyber Threat Sensor complements our broad internet traffic analysis and botnet infrastructure detection which provides threat detection and intelligence outside of your perimeter. It provides full visibility inside your perimeter, however you may choose to define that perimeter, without the need to use separate security services from individual providers.

Cyber Threat Sensor is currently on our product development roadmap and is planned to be available by Q1 FY 2019/2020 as a proof of value (POV). This will allow present and future customers to understand and test the capabilities of NTT Security's threat detection service offering.

Our next section looks a bit deeper into defensive considerations, specifically, how organizations can ensure access to organizational data when they need it, and securely share with peers.

Figure 43

Cyber Threat Sensor



7 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

San-Shi – Secure Multi-Party Computation across Confidential Information

A good cybersecurity defense strategy will include an understanding of what to defend, and how to defend it. The "what" is relatively straightforward to comprehend, as this will be the assets most important to an organization. The "how" is often more challenging.

In order to approach an understanding of "how," organizations need to adopt a risk-based approach to managing their cybersecurity defenses. In order to define this, an organization will need to perform analytics across several different sources of information, then prioritize the steps to create a defense strategy catering to their risk appetite, at a manageable cost. A major source of information when taking this approach is cyber threat intelligence.

The value of cyber threat intelligence depends on the sources used to create it. The cybersecurity industry has argued for years that organizations should share threat intelligence with their peers, competitors, vertical market and any other parties who may benefit from it. However, some organizations deem this information confidential as it could be used against them.

It is clear that sharing this information would benefit all organizations adopting a risk-based approach to cybersecurity practices. The challenge we must overcome is related to how can we remove trust barriers and do a better job of serving each other in order to fight for a common goal.

We need a platform allowing the sharing and accumulation of cross-sector, confidential cyber threat intelligence in a safe and secure manner. The application of this data would be expected to foster innovation and promote development of improved cyber defense strategies for all organizations. An effective platform must prevent or mitigate the risk of incidents, while supporting the need for data security measures to protect corporate strategy.

To enable safe and secure big data analytics across confidential data, NTT has become a world leader in the research and development of secure computation technology, enabling data processing while keeping the data encrypted and confidential.

NTT has developed a secure computation system named San-Shi. This technology enables aggregation and statistical processing, at high performance levels, of proprietary data while keeping the data encrypted and confidential.

As detailed in **Figure 44**, organizations can submit data to the secure computation system. This data is encrypted, and the only organization having the ability to decrypt the raw information is the data owner (organization submitting data). Within the system, allowed third parties can run analytics across this data in order to identify statistics, trends and other analytical functions. The analytics are run across the data in its encrypted form maintaining confidentiality at all times. Once the analysis is complete, only the results are shared with the third party.

Collaboration and Sharing are the New Normal

After decades of remaining in their respective corners, organizations across the cybersecurity community are finally sharing experiences, capabilities, and lessons learned, to a much higher degree – all in the name of fighting for a more secure internet. This sharing has been made a reality through working groups, government-sponsored programs, international relationships across a variety of sectors, and perhaps most importantly, a commitment to helping the online world become a more secure place.

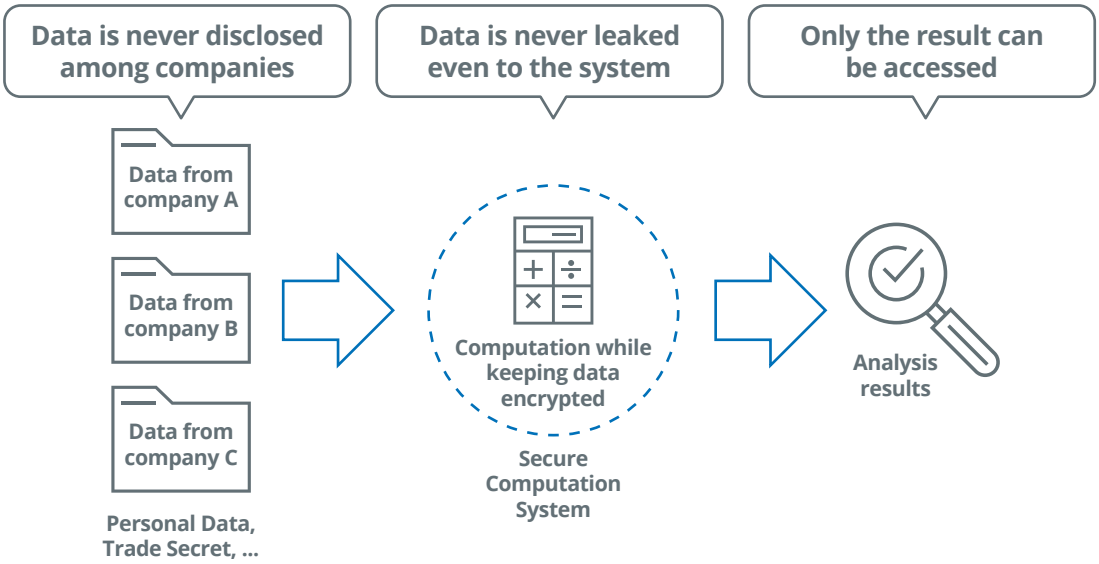
What we recommend:

- Explore opportunities for sharing and collaboration across your industry.
- Actively engage in collaboration, which serves to strengthen the resilience of industries around the globe.
- Share experiences, which may help to prevent a future attack on your own organization.

Most successful organizations are highly active in cybersecurity working groups and extended intelligence sharing relationships.

Figure 44

San-Shi Secure Computation System

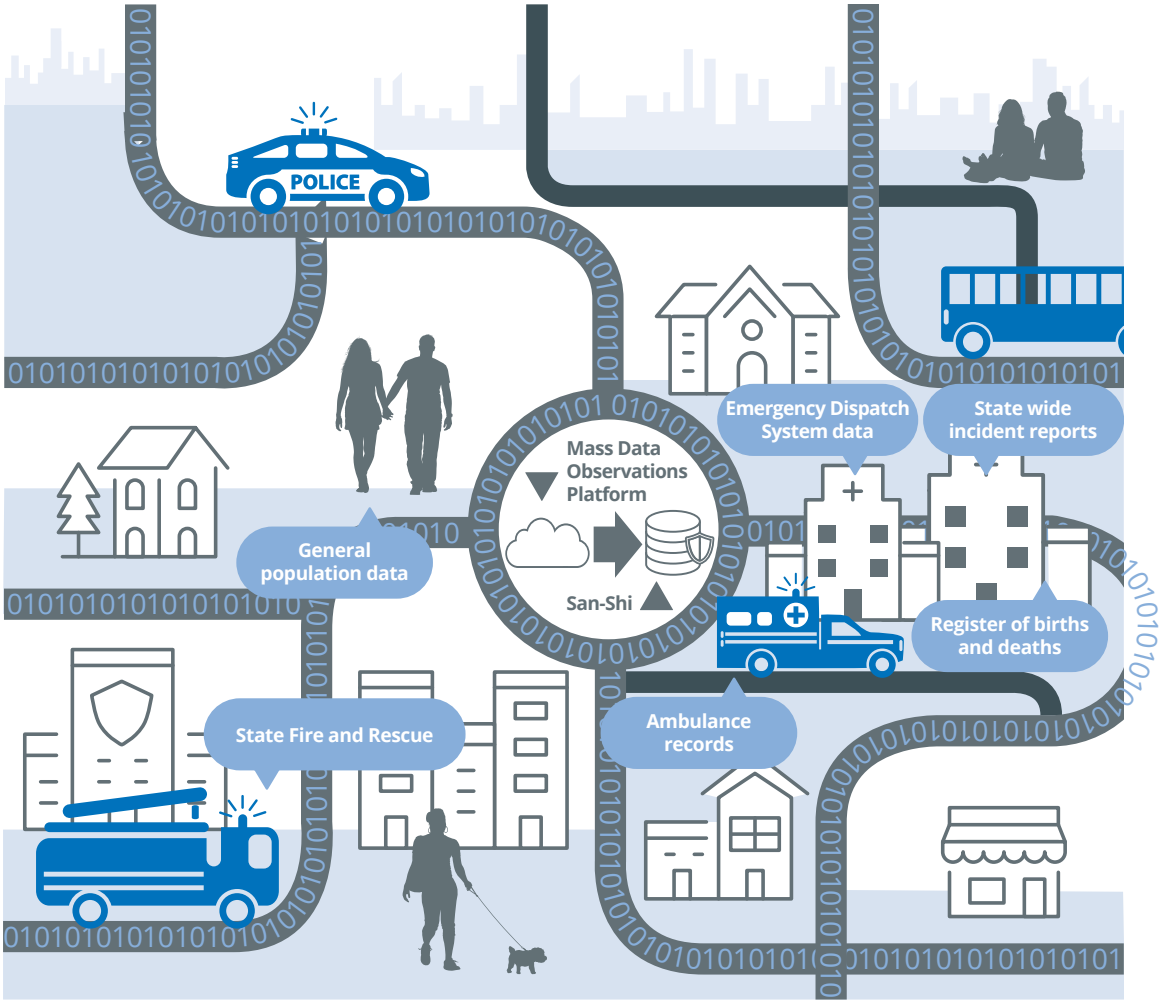


During the development of the secure computation system San-Shi, NTT has been demonstrating its effectiveness in various fields through applied examples such as multi-facility clinical research data analysis and genome data analysis. NTT has also been making continuous improvements to San-Shi in order to address concerns typical with big data analytics such as expanding operations, functions and increasing operational speed.

One field experiment, depicted in **Figure 45**, has been driven in collaboration between NTT R&D, NTT group company Dimension Data Australia, and Western Sydney University. This experiment was delivered out of the NTT Group Client Innovation Centre in Australia. It uses the Mass Data Observation Platform and San-Shi to enable a study of the health and economic costs of residential fires in New South Wales (NSW) Australia.

Figure 45

Collaboration Leveraging the Mass Data Observation Platform and San-Shi



The study, performed by Western Sydney University researchers, tracks the injuries from residential fires in NSW Australia. The NSW Australia fire service, ambulance service, hospitals, doctors and coroners all maintain separate records which are deemed confidential to each individual organization. Using San-Shi, the technology ensured confidentiality for all parties while returning results identical to the version of the study which did not use San-Shi technology. San-Shi can unlock the value of data by overcoming some of the challenges regarding ethics and regulations.

While San-Shi is yet to be applied to cyber threat intelligence, NTT continues to develop this platform and capabilities. NTT is currently running trials with our customers in order to demonstrate the value of the system and understand potential new usage scenarios across multiple sectors.

NTT will leverage the trial service of secure computation system San-Shi to further promote the safe and secure use of corporate secrets and personal data while endeavoring to develop and popularize data usage techniques including secure computation technology on a global basis.

Additional resources and information about San-Shi are available at these locations:

http://www.ntt.co.jp/sc/project_e/data-security/secure_computation.html

http://www.ntt.co.jp/news2018/1808e/180808a.html#a1

https://www.youtube.com/watch?v=ttojUxlPWmQ

Should you be interested in running a proof of concept please contact:

seg-product-p-ml@hco.ntt.co.jp

Conclusions

Digital transformation is driving changes in the way organizations operate. Challenges associated with these changes are not always easy to identify, but keeping a keen eye on historical challenges can assist in predicting and avoiding negative circumstances.

The evolution of attack techniques, and understanding the threats they can pose in the future, are also important. Credential theft and web-application attacks are not new, but our data clearly shows these attacks are still very much part of the challenges we need to address. The rise of coin mining activity, although new at this point, is certainly a challenge we will be addressing for the next 10+ years.

Our data analysis revealed many interesting trends. Some of the key findings in this year's report included:

- Finance and Technology were the most attacked sectors, each with 17 percent of all attacks. Finance has been a top attacked sector for six of the seven years NTT Security has been publishing the GTIR. Finance is one of only two sectors (with the Technology sector) to appear in the top five in every region.
- Application-specific and web-application attacks doubled over the past year. Attacks targeting bash, Apache Struts and Samba continue to be a focus of hostile activity.
- The percentage of attacks targeting Health Care organizations in the Americas increased 200 percent.
- 73 percent of all hostile activity falls into four categories: web attacks, reconnaissance, service-specific attacks, and brute-force attacks.
- 75 percent of attacks against the top five targeted EMEA sectors originated from IP addresses within EMEA.
- Web attacks accounted for over 43 percent of hostile activity against the most attacked sectors in EMEA. The global average was 32 percent.

Defending your organization is no small task, but focusing on key areas can assist in developing an effective security strategy.

Architecture is the key to success and not only applies to the technology side of managing risk, but also to the processes and procedures related to daily operations.

- Define solutions based on your short-term and long-term business objectives.
- Ensure that the architecture supporting network and data processing has security as an integrated part of the solution.
- Implement and enforce appropriate policies and procedures to drive successful deployment, improvements and maintenance.

Embrace proactive assessment and intelligence capabilities.

- Define a plan for regular assessments, both technical and non-technical.
- Governance, risk and compliance should be part of your organization's regular discussions, not something delayed until an audit is looming.
- Technical assessments help identify and reduce the number of possible attack vectors. Include not only traditional penetration testing activities, but also application testing and social engineering.
- Leverage threat intelligence capabilities to help identify and rapidly make decisions about mitigation of threats.

Use employee education as a force multiplier as well as a protection capability.

- Train your employees to be aware of the most common threats that may target them, and how to handle those threats.
- Teach your employees that it is fine to report anything that "just doesn't seem right."
- Help your employees to be ambassadors for the security program. Make it part of the culture and not a task.
- All employees have a key role to play in the protection of the organization's assets and clients. Make it easy for employees to have engagement in the process.

NTT Security Global Data Analysis Methodology

The NTT Security 2019 Global Threat Intelligence Report contains global attack data gathered from NTT Security and supported operating companies from October 1, 2017, to September 31, 2018. 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.

From our unique and comprehensive global view of internet traffic, NTT Security gathers security log, alert, event and attack information from which it enriches and analyzes contextualized data. This process enables real-time global threat intelligence and alerting. The size and diversity of our client base, with over 10,000 security clients on six continents, provides NTT Security 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 Security provides a highly accurate representation of the ever-evolving global threat landscape.

NTT Resource Information

Global Threat Intelligence Center (GTIC)

The NTT Security Global Threat Intelligence Center 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 goes above and beyond the traditional pure research organization, by taking its threat and vulnerability research and combining it with detective technologies development to produce applied threat intelligence. Its mission is to provide NTT Security clients with services and tools to deliver early warning notifications of risks and threats 24/7.

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

NTT Group Resources

NTT Security
NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of managed security services, security consulting services and security technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **http://www.ntt.co.jp/index_e.html** to learn more about NTT Group.

NTT-CERT
NTT-CERT, a division of NTT Secure Platform Laboratories, serves as a trusted point of contact for Computer Security Incident Response Team (CSIRT) specialists, and provides full-range CSIRT services within NTT. NTT-CERT generates original intelligence regarding cybersecurity threats, helping to enhance NTT companies' capabilities in the security services and secure network services fields. To learn more about NTT-CERT, please visit **www.ntt-cert.org**.

Partnering for Global Security

NTT DATA
NTT DATA partners with clients to navigate and simplify the modern complexities of business. As a top 10 global IT services and consulting provider, we wrap deep industry expertise around a comprehensive portfolio of infrastructure, applications and business process services. Visit **nttdataservices.com** to learn more.

NTT Communications
NTT Communications provides consultancy, architecture, security and cloud services to optimize the information and communications technology (ICT) environments of enterprises. These offerings are backed by the company's worldwide infrastructure, including the leading global Tier 1 IP network, the Arcstar Universal One™ VPN network reaching over 190 countries/regions, and over 140 secure data centers worldwide. NTT Communications solutions leverage the global resources of NTT Group companies including Dimension Data, NTT DOCOMO and NTT DATA. Visit **www.ntt.com** to learn more..

Dimension Data
Dimension Data is a global systems integrator and managed services provider for Hybrid IT. Headquartered in Johannesburg, Dimension Data employs over 28,000 people across 47 countries. We bring together the world's best technology provided by market leaders and niche innovators, providing clients with the service support that they need for their business, from consulting, technical, and support services to a fully managed service. Dimension Data's cybersecurity practice helps clients to envision and build digital businesses that are secure by design. Together with NTT Security, we have more than 2,000 experts across 47 countries to support clients on a secure digital transformation journey.

As a proud member of the NTT family, our continued investment in innovation enables us to find new ways to deliver services to clients today, while also keeping an eye on the future.

Visit us at **https://www.dimensiondata.com/** to learn more.

Appendix A: Glossary

The following terminology is used within the GTIR.

0-day (Zero-Day) Attack: an attack that exploits a previously unknown vulnerability in software, meaning that the attack occurs on "day zero" of awareness of the vulnerability.

Apache Struts: is an open-source solution for creating Java web applications and uses a Model-View-Controller (MVC) approach. The Apache Struts project is maintained by a community of volunteers who continuously focus on improving the framework.

Application-Specific Attacks: target vulnerabilities in applications, including broken authentication and session management, insecure direct object references, lack of encryption for data at rest and in transit, escalation of privileges, and Trojanized or unpatched third-party components.

Bash: is a text-based command processor utility included in virtually every variation of Unix. It provides functionality as a log-in interface as well as the capability to perform system and file functions on an operating system.

Botnet: similar to a backdoor except that multiple computers associated with the botnet receive instructions or commands at the same time from the same controller.

Brute-Force: the systematic use of username and password combinations in order to guess proper credentials to access a system or resource.

C&C (Command and Control): communications channels used by bots in a botnet to receive instructions.

Coin Mining: the process of generating cryptocurrency by leveraging CPU and GPU power from host computing systems.

Credential Theft: the process of stealing valid credentials for use in follow-on attacks, sale on the dark web, unauthorized access and a variety of other malicious purposes.

Dark Net or Dark Web: private networks not accessible by the general public. These networks are often used for nefarious or illegal purposes.

DoS (Denial of Service) and DDoS (Distributed Denial of Service): attacks which make a machine or network resource unavailable to intended users. A DDoS attack originates from many devices at once.

Dropper: a helper program that is used to download other components of malware, such as Trojans and rootkits.

Exploit Kit: a malicious toolkit used to exploit vulnerabilities in software applications.

Malspam: the delivery of malware via email.

Network Manipulation: Attacks target network protocols. These types of attacks typically include spoofing IP addresses and hijacking and are often used to bypass network-based security controls like intrusion detection systems and firewalls.

Phishing: attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication (email). Spear-phishing is highly targeted phishing, using knowledge about a specific person or organization.

Ransomware: malware which encrypts a victim's data and demands a ransom payment in exchange for a decryption key.

Samba: a suite of tools that provides cross platform compatibility for file and print services between Unix and Microsoft Windows-based operating system platforms.

Reconnaissance: identifying systems and services that may be valuable to attack. May include activities such as identifying a network or application's features and the technologies implemented. Reconnaissance is often a key indicator of a pending attack.

Service-Specific Attacks: are directed at services which often do not require authentication and run on a server, desktop or mobile devices. These are most frequently seen in exploit attempts against common services such as SMTP, DNS, SMB, FTP and Telnet, but often target databases and remote access services. Such attacks often provide the attacker access to the underlying operating system allowing opportunities for further exploitation.

Shellshock: a set of vulnerabilities associated with the Unix **bash** shell which could give the attacker control over the targeted system. It is notable because the bug had been present in application code for many years before it was discovered, and bash is part of every version of Unix.

Social Engineering: obtaining passwords or other access materials through methods such as personal visits, telephone calls or social media websites.

Spyware: a type of malware installed on computers that collects information about users without their knowledge.

Trojan: a type of malware that masquerades as a legitimate file or helpful program but has been designed for nefarious acts.

Vulnerability: a weakness in software which hackers can use to their advantage.

Weaponization: to develop or adapt software with a malicious intent.

Web-Application Attacks: are attacks against services and applications that support a web presence. Some examples of these attacks are SQL injection, cross-site scripting, command injection, and directory traversal.

Appendix B: Sector Definitions

Business and Professional Services Sector: consists of organizations which specialize in performing professional, scientific, and technical activities designed to help other organizations produce products and solutions.

Education Sector: consists of public or private schools, colleges, universities and educational institutions. The sector is classified into three categories: K-12, higher education and vocational education.

Finance Sector: consists of organizations which provide financial services to commercial and retail customers. This sector includes banks, mortgage companies, investment funds, brokerage firms, private equity, credit card and real estate companies.

Gaming Sector: consists of organizations which generate revenue from online and physical casinos or other gambling focused services.

Government Sector: consists of local, state, province, central or federal government.

Health Care Sector: consists of organizations which specialize in providing medical services, design, manufacture and sale of medical equipment, biomedical technology research and development, or facilitating the provision, delivery or management of dental, health care or mental health services to patients.

Hospitality, Leisure and Entertainment Sector: consists of organizations which produce and promote live performances and sporting events, or exhibits. It also includes hotel, motel and vacation clubs, cruise lines, and related services.

Insurance Sector: consists of providers in the insurance market, and includes all forms of insurance, including mortgage, health, dental, home, auto, and any other insurance related products or services.

Legal Sector: consists of practitioners primarily engaged in the practice of law and supporting services. Organizations in this sector provide expertise in legal support, such as criminal, corporate, family and estate, patent, real estate, or tax law.

Manufacturing Sector: consists of organizations focused on the transformation of materials and components into products or finished components for additional assembly. It includes organizations which build distributable or finished products from raw materials or sub-assemblies.

Media Sector: consists of organizations associated with a variety of communication or news media, including animation, computer games, film, writing, interactive media, photo imaging, radio, print, online content, social media and TV.

Non-Profit Sector: consists of organizations with federal tax-exempt status which generally provide support for charitable causes or the welfare of the public.

Pharmaceuticals Sector: consists of organizations which focus on discovery, development, production, testing and marketing pharmaceutical drugs.

Public Sector: consists of organizations that provide goods or services to the public. Examples include infrastructure and public transit services.

Retail Sector: consists of organizations which sell goods through brick and mortar stores, online, or through direct sales to consumers.

Technology Sector: consists of organizations which research, develop and distribute technological goods and services, such as computers, smartphones, and similar products.

Telecommunications Sector: consists of organizations which are telecommunications and telephone service providers (both cellular and land line) and internet service providers.

Transport and Distribution Sector: consists of organizations which provide services or infrastructure to aid in moving people and goods. The sector includes freight, transportation of people and supporting logistics associated with airlines, marine, road and rail.

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.

www.nttsecurity.com