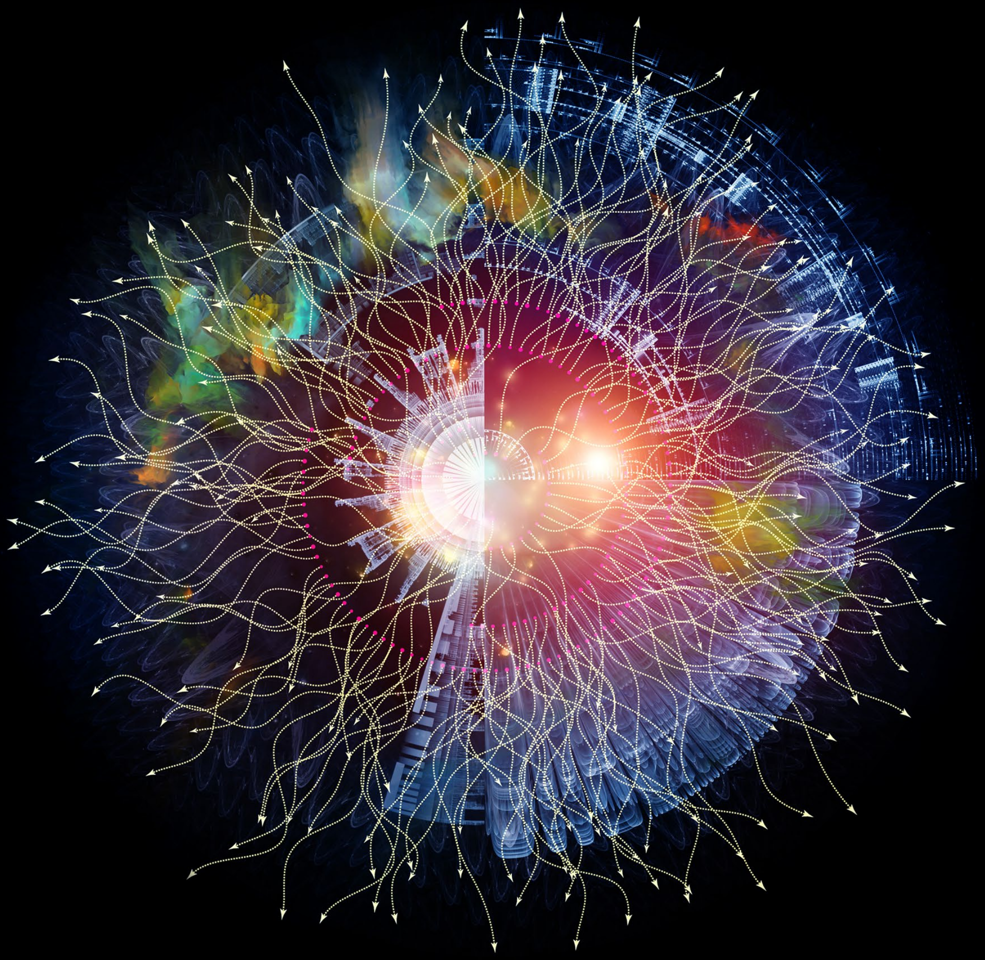
Deloitte.



Cyber Trends and Intelligence Report

November 2022
Deloitte Japan Cyber Intelligence Centre

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Introduction

The start of 2022 was an omen for heightened cyber risks soon to come. In the new year, rising tensions between countries increased geopolitical risks, and auto parts manufacturers fell victim to ransomware that ultimately forced affiliated original equipment manufacturers (OEMs) to shut down their production lines.

International conflicts and cyberattacks have also shifted. A new form of cyber warfare between countries is emerging in the unprecedented structure of "cyber armies" composed of hacktivists and civilians recruited by states to participate in attacks on other countries and their critical infrastructure.

The ransomware epidemic has also continued to wreak havoc with several large-scale incidents. For example, a food delivery co-op in Nara Japan fell victim to a ransomware attack in October 2022. About half of the residents of Nara Prefecture are members of the co-op, and recent media reports indicate that food deliveries will likely remain suspended for an extended period.

Double extortion ransomware, a newer and increasingly prevalent subcategory of ransomware, randomly targets vulnerable or improperly configured internet-connected devices, regardless of industry or target demographic. It has also proven capable of significantly impacting our everyday lives.

Incidents like these have sparked renewed discussions over supply chain risks and how a company's own production could be impacted by ransomware attacks suffered by their business partners.

Based on analysis by Deloitte Japan's Cyber Intelligence Centre, this report (a translation of an excerpt from Deloitte's *Cyber Trends & Intelligence Report 2022* in Japanese) examines threat trends of double extortion ransomware and considers potential countermeasures such as attack surface management (ASM), an approach that has recently gained considerable interest in addressing supply chain risks, among other areas.

We hope that this report provides useful insights on cyber threats facing organisations across many industries, and that it will serve as one of the sources of threat information for your company's cyber security response.

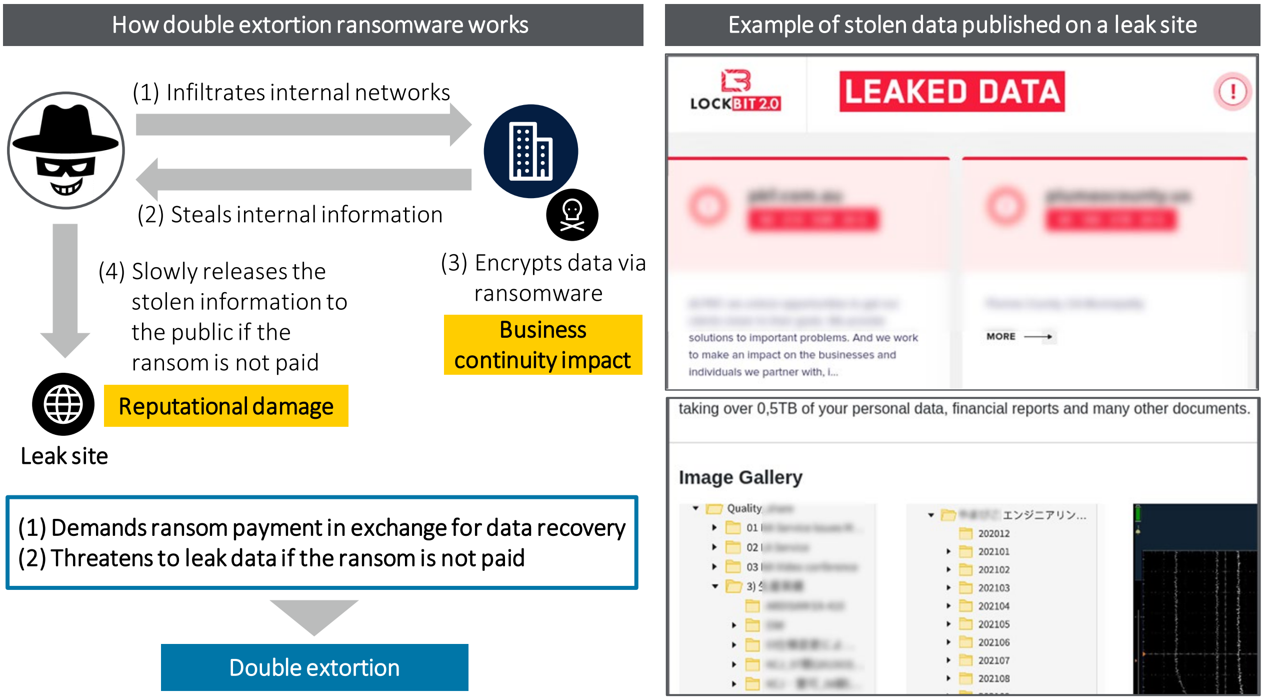
Trends in ransomware threats

Ransomware is a type of malware that encrypts data stored on a device, such as a PC, making the data unavailable to its users. The attackers then demand payment in return for providing a decryption key. Ransomware was initially used to mainly target individual PCs. However, as far back as 2015 there have been cases in which organisations have been targeted and their IT systems paralysed, with threats being made to the continuity of their operations.

Double extortion ransomware attacks then emerged in the latter half of 2019 and have wreaked increasing havoc by exfiltrating data before encrypting it, then threatening to leak the data if the victim does not pay. This method of attack not only threatens business continuity by disabling IT systems, but also damages an organisation's reputation if their data is leaked.

When the ransomware victims do not pay, cyber criminals will often publish the data to a leak site hosted on the dark web, where anyone–so long as they have access to the site–can download the data. Many ransomware gangs now operate such leak sites. The Deloitte Japan Cyber Intelligence Centre, which provides security monitoring services, has identified more than 70 leak sites so far.

Figure 1: General overview of a double extortion ransomware attack


How double extortion ransomware works
(1) Infiltrates internal networks
(2) Steals internal information
(3) Encrypts data via ransomware
Business continuity impact
(4) Slowly releases the stolen information to the public if the ransom is not paid
Reputational damage
Leak site
(1) Demands ransom payment in exchange for data recovery
(2) Threatens to leak data if the ransom is not paid
Double extortion
Example of stolen data published on a leak site
LOCKBIT 2.0
LEAKED DATA
MORE
Image Gallery
Quality
01
02
03
3)
エンジニアリン...
202012
202101
202102
202103
202104
202105
202106
202107
202108

solutions to important problems. And we work to make an impact on the businesses and individuals we partner with, i...

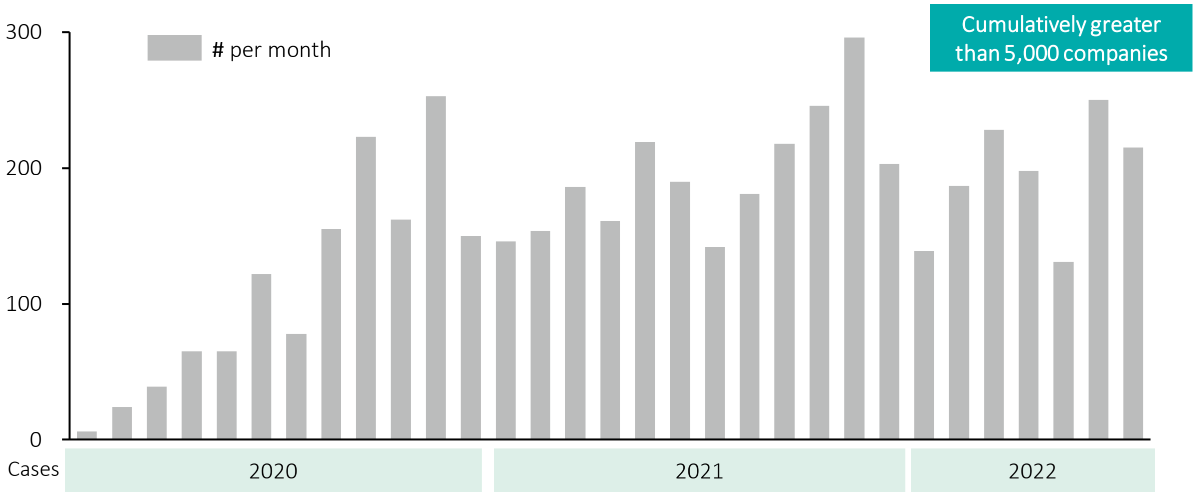
taking over 0,5TB of your personal data, financial reports and many other documents.

Damage caused by data leaked via double extortion ransomware attacks

Figure 2 illustrates trends in the number of cases globally in which companies have had their data published on ransomware leak sites, based on Deloitte estimates. Since around March 2020, there has been an uptick in the number of cybercrime gangs opening leak sites, and the number of victims has increased accordingly. As of the end of July 2022, more than 5,000 companies have fallen victim to such data leaks around the world.

Although new leak sites launch just as frequently as they shut down, at least 20-30 are always in operation, and this has been the situation since 2021. Nowadays, the data of approximately 200 companies is leaked each month.

Figure 2: Trends in the number of companies globally that have had their information published on ransomware leak sites

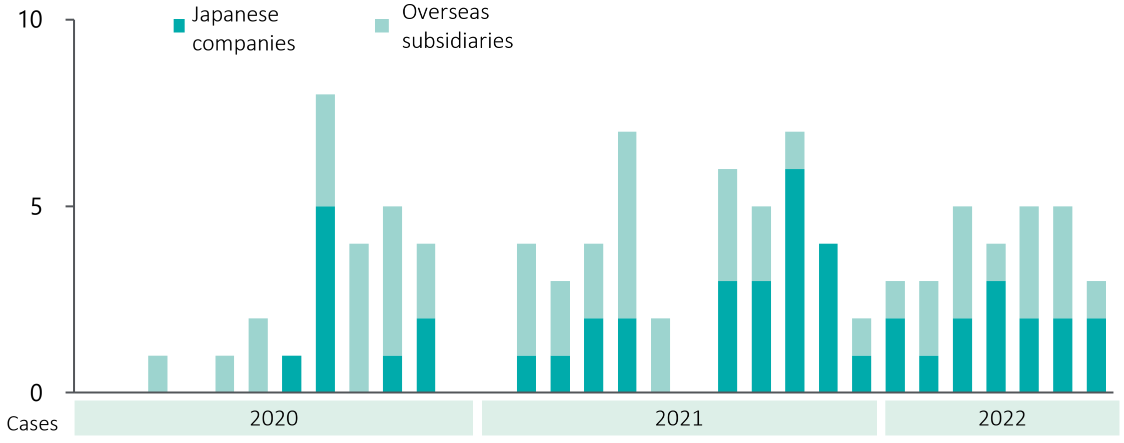


Source: Deloitte

Based on analysis by the Deloitte Japan Cyber Intelligence Centre, Figure 3 shows how many Japanese companies and their overseas subsidiaries have had their data published on leak sites.

Leak sites have been exposing the data of about five Japanese companies per month since mid-2021 when incidents from both Japanese and overseas locations are combined.

Figure 3: Trends in the number of Japanese companies and their overseas subsidiaries that have had their data published on leak sites



Source: Deloitte

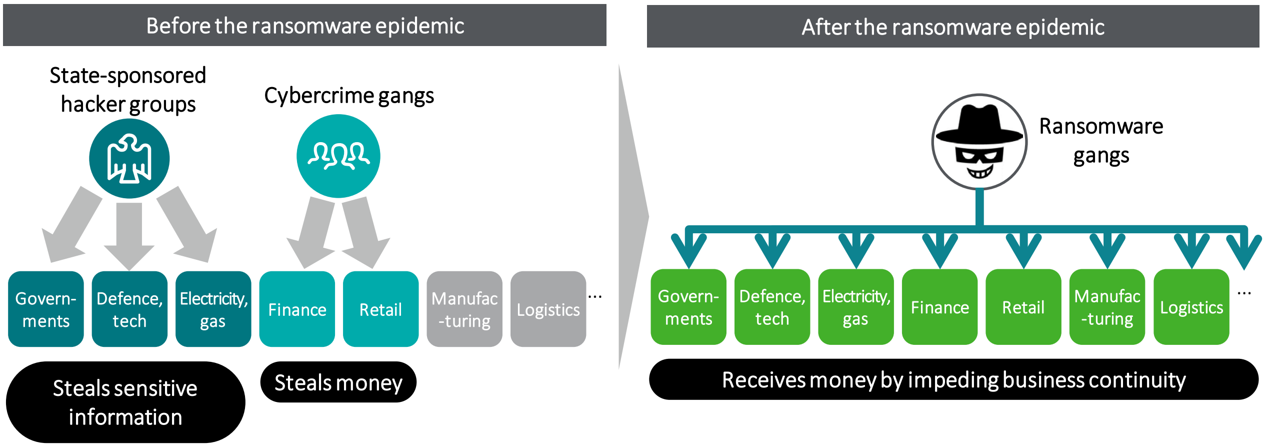
Ransomware victims and the types of industries subject to attacks

The tactics used by ransomware gangs are nothing new, yet the growing number of victims indicates that many organisations are ill equipped to deal with ransomware when it infiltrates their networks. This issue can be attributed in large part to dramatic shifts in the threat environment after ransomware emerged.

Previously, the majority of cyber attackers infiltrated networks to steal sensitive information. State-sponsored hacker groups tended to target government agencies, the defence industry, advanced technologies, and critical infrastructure while cybercrime gangs tended to target financial institutions and retail stores. As such, the attack patterns per industry were typically easier to define.

The outbreak of the ransomware epidemic has upended this well-worn attack pattern. Ransomware targets every industry it can infiltrate because the goal is to hold business continuity to ransom (Figure 4). Organisations that might rarely have been the target of cyberattacks can now suffer immense damage if they have inadequate countermeasures.

Figure 4: Comparing threats by industry before and after the ransomware epidemic

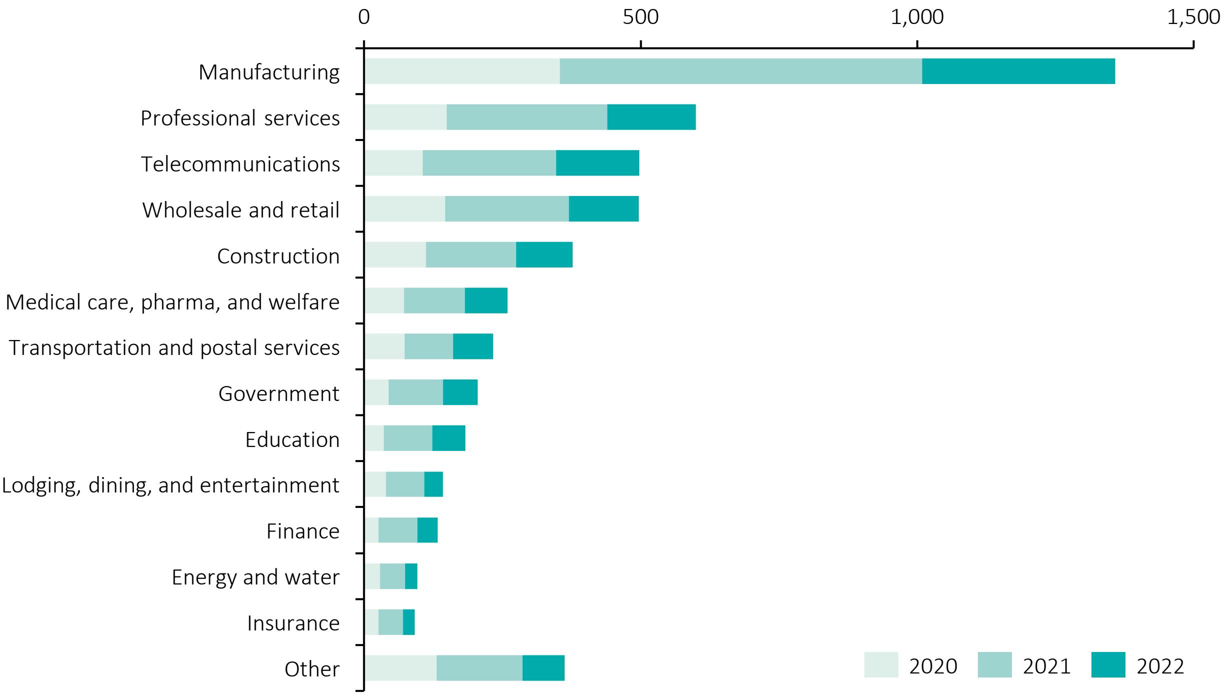


Based on Deloitte Japan Cyber Intelligence Centre analysis, global data on victims of double extortion ransomware data leaks, when separated by industry, shows that a wide variety of industries are affected by these attacks, though the manufacturing industry has been hit especially hard (see Figure 5). This could be due to the large number of companies in manufacturing compared with other industries. Many of these companies are also small- to medium-sized businesses with lower cyber security maturities.

What's more, if a ransomware attack disrupts the operations of a supplier responsible for the production of a critical component, the damage can easily spread to companies that purchase the component and many other stakeholders.

Cyber attackers are launching ransomware attacks on the manufacturing industry that are impacting business continuity at an alarming rate. This represents a growing supply chain risk for corporate production activities.

Figure 5: Number of companies globally (by industry) that have fallen victim to double extortion ransomware data leaks



Source: Deloitte

Ransomware countermeasures and attack surface management

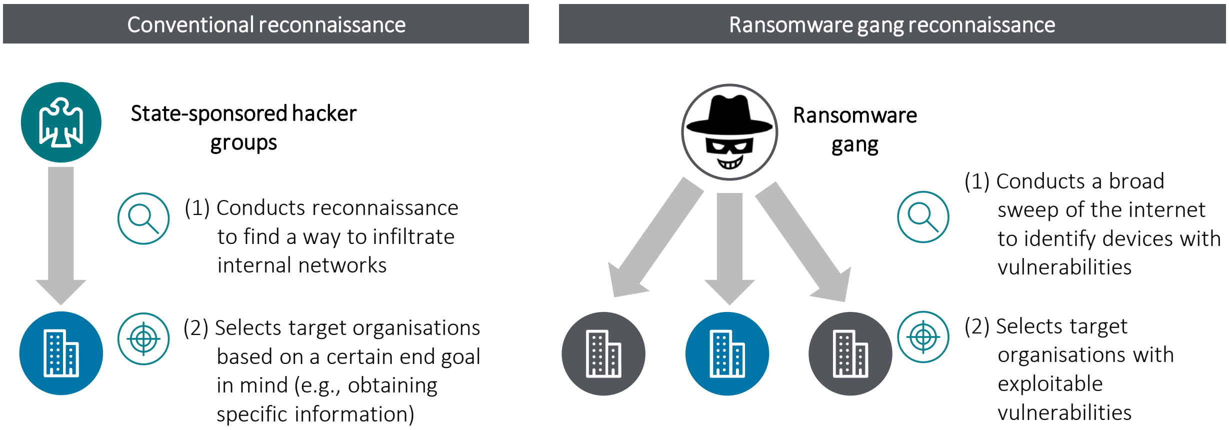
Cyber attacker reconnaissance

As noted in the previous section, ransomware targets every industry it can infiltrate–it generates profit by holding business continuity to ransom. While typical cyber attackers conduct reconnaissance to investigate a target's weaknesses before launching an attack, ransomware gangs take a different approach.

As illustrated in Figure 6, in a conventional cyber attack attackers select a target organisation based on a specific end goal in mind, then conduct reconnaissance to find a way to infiltrate the organisation's internal network.

With ransomware attacks, cyber attackers conduct a broad sweep of the internet to identify devices with vulnerabilities they can exploit to infiltrate networks from the outside, then they target the organisations that own or are connected to those devices.

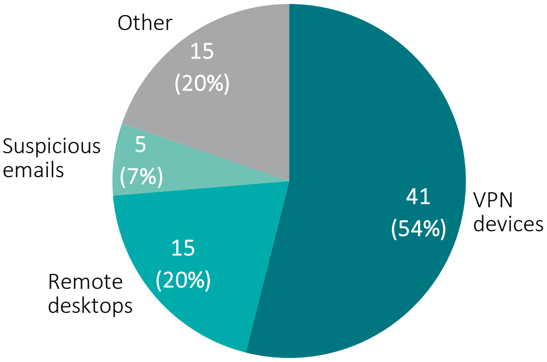
Figure 6: Conventional and ransomware gang reconnaissance


Conventional reconnaissance
State-sponsored hacker groups
(1) Conducts reconnaissance to find a way to infiltrate internal networks
(2) Selects target organisations based on a certain end goal in mind (e.g., obtaining specific information)
Ransomware gang reconnaissance
Ransomware gang
(1) Conducts a broad sweep of the internet to identify devices with vulnerabilities
(2) Selects target organisations with exploitable vulnerabilities

For Japan, the data shows that virtual private network (VPN) devices and remote desktops, which can be externally accessed, account for over 70% of the entry points from which ransomware attacks are launched (see Figure 7). While the security of devices connected to the internet may seem like a basic concept, its importance cannot be understated.

Source: Deloitte analysis; Tokyo Metropolitan Police Department, "Threats to Cyberspace in 2021", April 7, 2022.

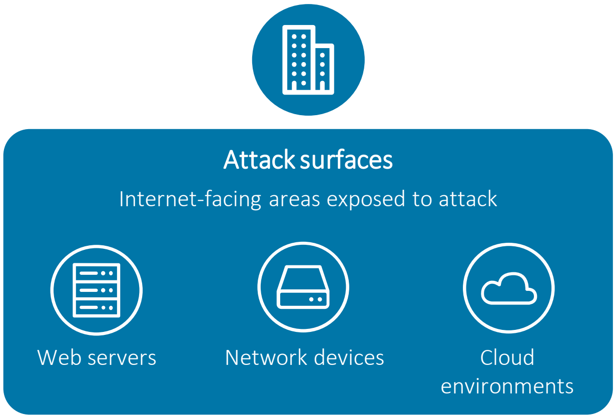
Figure 7: Entry paths for ransomware attacks in Japan



What is attack surface management (ASM)?

Areas exposed to external attacks, such as VPN devices and web servers, are referred to as attack surfaces. With the rise in ransomware attacks, it has become more and more important to effectively protect devices (that is, attack surfaces) targeted by cyber attackers in recent years.

Figure 8: What is an attack surface?



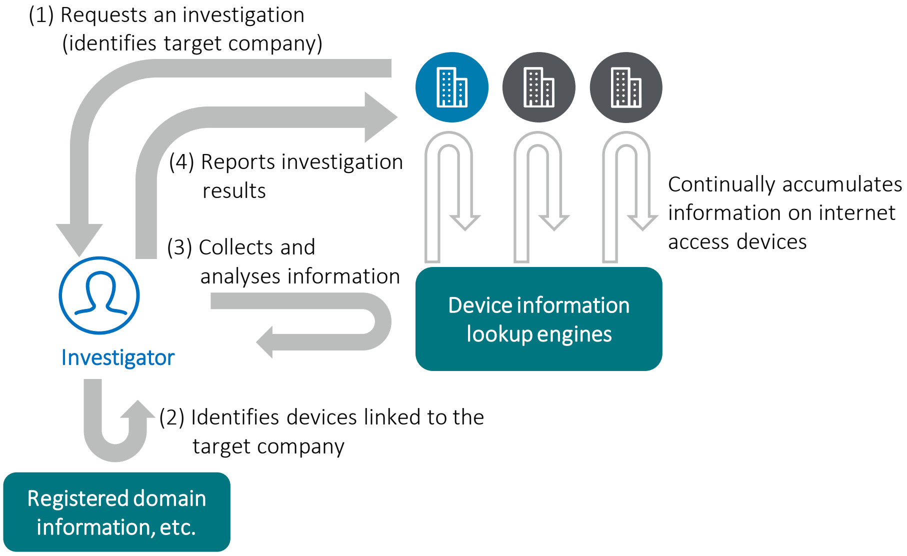
The importance of effective internet access device management is no secret, but its implementation is no easy task either. Internet access enabled devices are often left in a vulnerable state as a result of:

- IT departments not knowing about and not managing devices that are independently operated by other business units, leaving vulnerability management patchy or non-existent.
- IT environments in overseas locations being entrusted to local staff without supervision.
- Temporary modifications made to device configurations for maintenance purposes not being rolled back.

When managing such devices, it is not enough for administrators to self-assess these internet accessible devices, because they may not know of the gaps in the attack surface. Consequently, ASM has garnered interest as an approach that could solve these and other similar problems.

ASM investigates and monitors an organisation's internet accessible devices from the outside. These investigations avoid using internal IT asset ledgers and other internal information, instead only referencing externally available information sources that anyone can access, such as device lookup services. This way, organisations can see from the perspective of would-be cyber attackers as these investigations use the same type of information sources that attackers use for their reconnaissance.

Figure 9: Attack surface management flow


(1) Requests an investigation (identifies target company)
(4) Reports investigation results
(3) Collects and analyses information
Investigator
Continually accumulates information on internet access devices
Device information lookup engines
(2) Identifies devices linked to the target company
Registered domain information, etc.

How ASM and platform diagnostics differ

Platform diagnostics is the traditional method of monitoring internet access devices. While the purpose of monitoring device conditions is the same between either method, ASM and platform diagnostics take very different approaches.

Under the platform diagnostics approach, requestors have to know the devices they are managing, which requires them to know that the device exists. This approach also requires prior coordination with the device managers, lest their investigation attempts are incorrectly deemed as a hostile attack.

In contrast, ASM can investigate any device even if it has been overlooked by the organisation's management as investigators identify their own targets. ASM also sets itself apart in its convenience, as investigations can be safely conducted on devices currently in use without prior coordination because investigators seldom need to access target devices.

Figure 10: Difference in approach between ASM and platform diagnostics

	ASM	Platform diagnostics*
Target devices	Identified by investigator	Specified by requestor
Investigation methods	• Uses external information sources • Seldom needs to access target devices	Sends fake attack code to target devices

* Platform diagnostics generally involve directly communicating with (e.g., sending fake attack code, conducting port scanning) target devices for the purpose of investigation. However, platform diagnostic methods differ from company to company, and some organisations may not take this approach.

ASM and supply chain risks

The fact that ASM investigations don't need to directly access devices means that companies can review devices outside of their control without advance coordination with the organisations that own the target devices.

As covered in the previous section, many suppliers have fallen victim to ransomware attacks in the past few years, and their business partners have consequently experienced increased risks to their own production activities. However, companies can enhance cybersecurity not just within their group, but up and down the whole supply chain, by monitoring core suppliers through ASM. Certain Japanese companies have already begun to adopt this approach.

Authors and key contacts

Kohei Sato
Partner
Japan
kohei.sato@tohmatsu.co.jp

Kenichi Inoue
Managing Director
Japan
kenichi.inoue@tohmatsu.co.jp

This report is a translation of an excerpt from Deloitte's *Cyber Trends & Intelligence Report 2022* (in Japanese).

Deloitte.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Member of
Deloitte Touche Tohmatsu Limited