Deloitte.

Cyber Trends and Intelligence Report

November 2021

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Introduction

Cyber risks are growing rapidly, and the past year has seen a significant increase in the number of several large-scale incidents using double extortion ransomware, where data is exfiltrated as well as encrypted. These incidents have included an American oil pipeline operator having their operations temporarily halted, and companies within Japan having to delay the release of their financial statements.

Based on analysis by Deloitte Japan's Cyber Intelligence Centre, this report (a translation of an excerpt from Deloitte's *Cyber Trends & Intelligence Report 2021* in Japanese) examines the trends in cyberattacks and ransomware, the increase in leak sites, and what kind of damage double extortion ransomware has inflicted by region and industry.

To protect against the damage from ransomware attacks, it is important for organisations to remain vigilant and to continue implementing basic countermeasures. Drawing on our experience in helping organisations deal with cyber incidents and improve their cyber defences, the second section of the report outlines suggested preparations to help prevent damage from double extortion ransomware attacks.

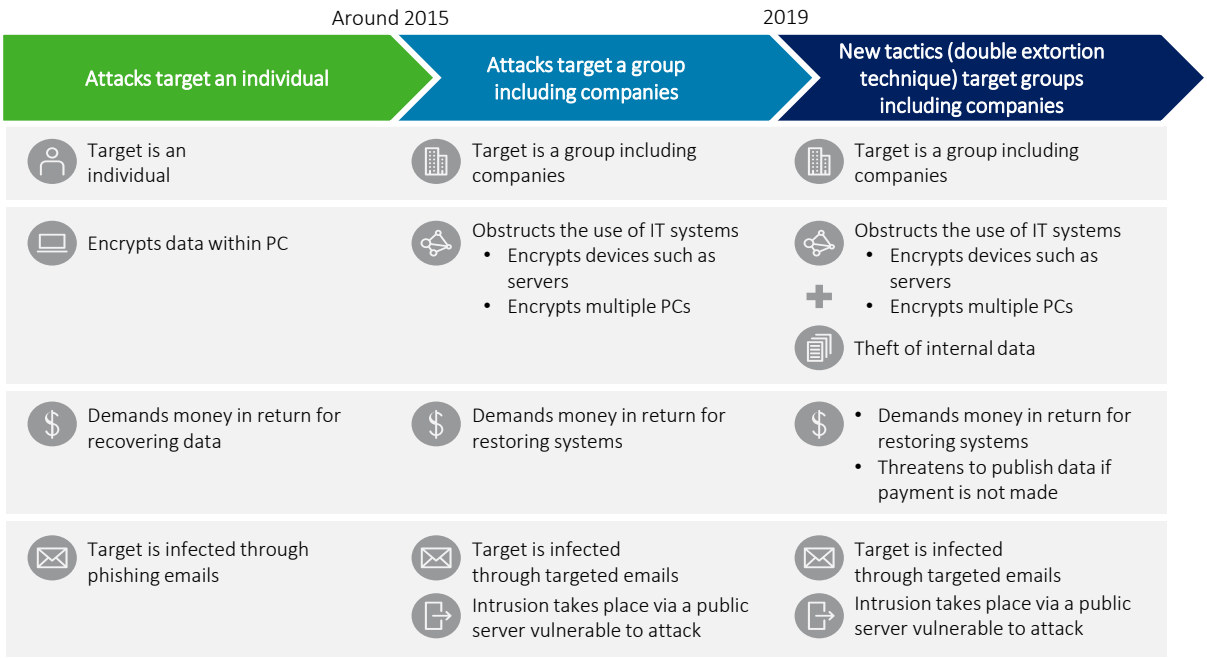
We hope that this report provides useful insights on what cyber threats are facing organisations across many industries, and that it will serve as one of the sources of information for your company's cyber security response.

A growing trend in double extortion ransomware attacks

Ransomware is a type of malware that encrypts data stored on a device, such as a PC, with a demand then following for money in exchange for a key that releases this data. Although ransomware was used to mainly target individual PCs, starting from around 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.

The latter half of 2019 saw the emergence of a new technique that is rapidly spreading and inflicting damage to companies, known as double extortion, where sensitive data is exfiltrated in addition to being encrypted. In May 2021, a large US oil pipeline operator saw its operations halted after being targeted by a cyberattack using a ransomware known as Darkside. This attack also had a large impact on the lives of ordinary citizens, and has shown that ransomware is no longer just a threat to individual companies, but also to society as a whole.

Figure 1: Changes in cyberattack trends



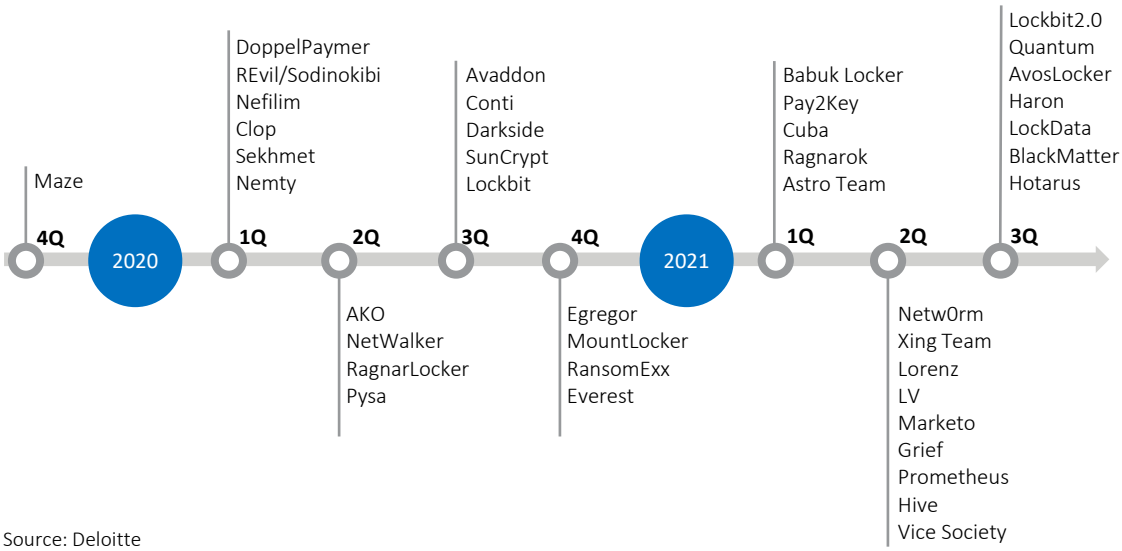
Source: Deloitte

What is double extortion ransomware?

Attackers that use double extortion ransomware do not just encrypt data, they also steal this data in advance and threaten to publish it if their demands for payment are not met. This type of attack is called 'double extortion' as its victims are extorted in two ways: extortion in return for restoring their data (a traditional method), and extortion with threats of having their data published if the attacker's demands are not met.

Organisations targeted by double extortion ransomware attacks that do not respond to these demands have their data slowly published on so-called 'leak sites' set up by attackers on the dark web. Hacking groups have been active in setting up these sites; Deloitte, which provides security monitoring services, has verified approximately 40 such sites (see Figure 2).

Figure 2: Periods in which double extortion ransomware leak sites were set up



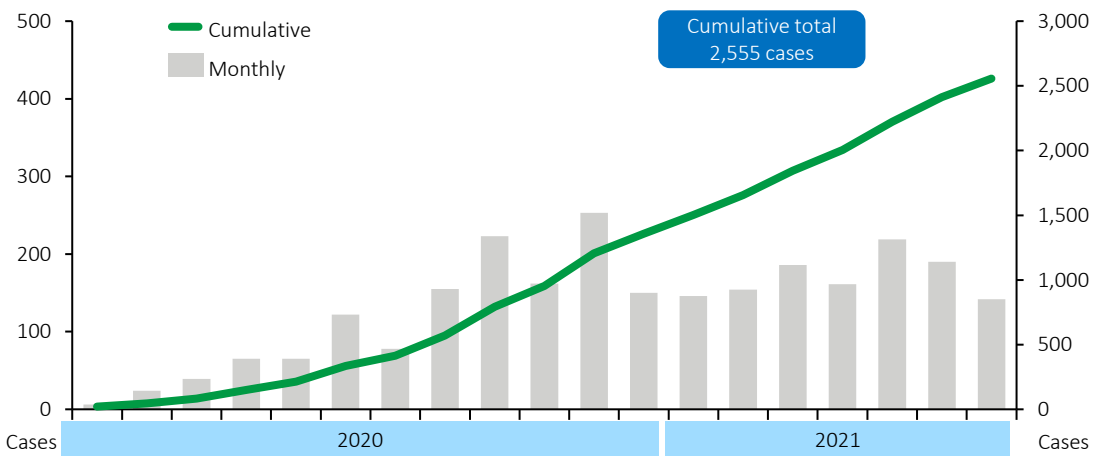
Source: Deloitte

How much damage double extortion ransomware attacks have caused by publicising data

Figure 3 shows the changes in the number of cases globally in which companies have had their data published on ransomware leak sites, based on Deloitte estimates.

At the end of July 2021, the cumulative total of these cases exceeded 2,500 cases. After August 2020, most months saw a minimum of 150 cases. This has shown that attacks have intensified over the past year.

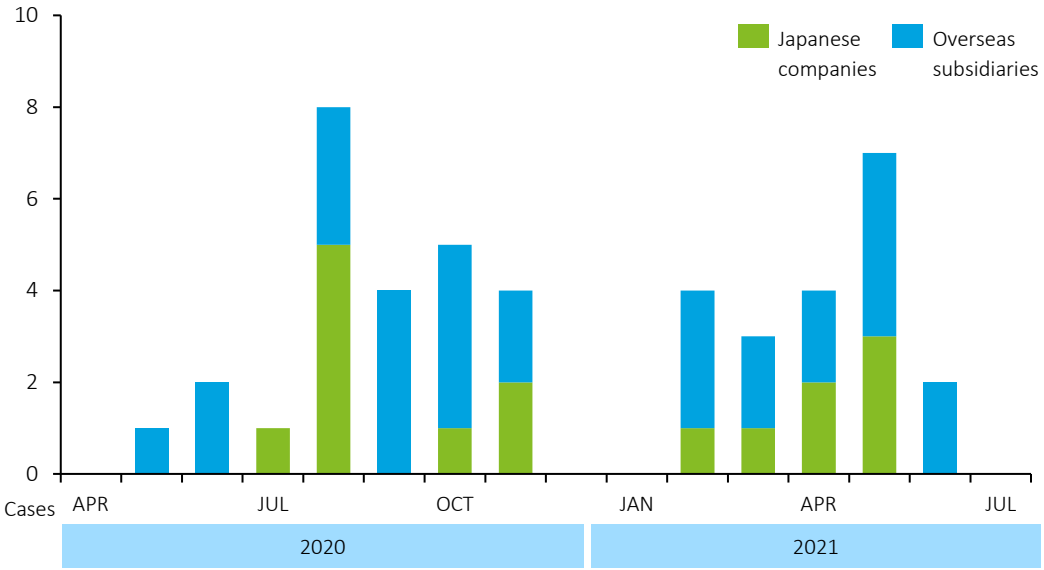
Figure 3: Changes in the number of companies globally that have had their information published on ransomware leak sites



Source: Deloitte

Based on analysis by the Deloitte Japan Cyber Intelligence Centre, Figure 4 shows just how much damage Japanese companies and their overseas subsidiaries have incurred as a result of their data being published. Although the number of cases is small, these attacks have impacted companies on a near monthly basis since May 2020. This analysis shows that Japanese companies cannot afford to view ransomware attacks as an issue that will not affect them.

Figure 4: How much damage Japanese companies and their overseas subsidiaries have incurred due to their data being published



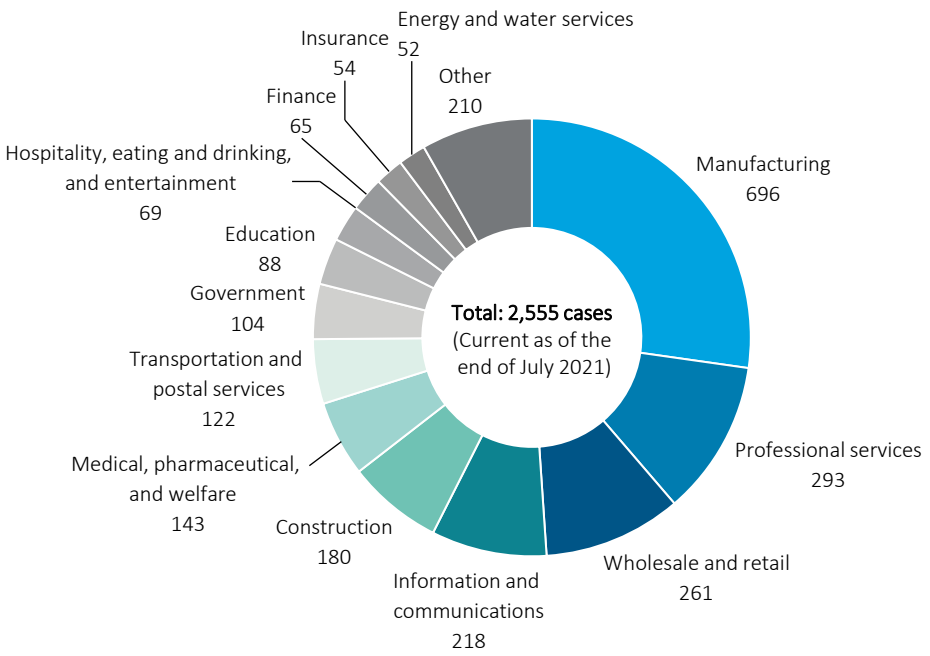
Source: Deloitte

Trends in damage by industry of companies which have had their data posted on leak sites

Figure 5 shows how many companies globally by industry have had their data posted on leak sites, based on Deloitte analysis. When separated by industry, the manufacturing industry accounts for the majority of affected companies. However, we do not believe that the manufacturing industry is being singled out for attack. Instead, we believe that this trend stems from the fact that the manufacturing industry has a large number of companies compared to other industries, and that medium to small sized companies tend to possess lower levels of security.

In recent ransomware attacks, the primary method of intrusion has been through remote access systems, such as virtual private network (VPN) devices. It is believed that attackers seek out remote access systems on the internet and attack systems that are vulnerable. This is why it is more important than ever to continue to maintain levels of security that do not provide an opening for external intrusions.

Figure 5: Number of companies globally (by industry) that have had their information posted on leak sites

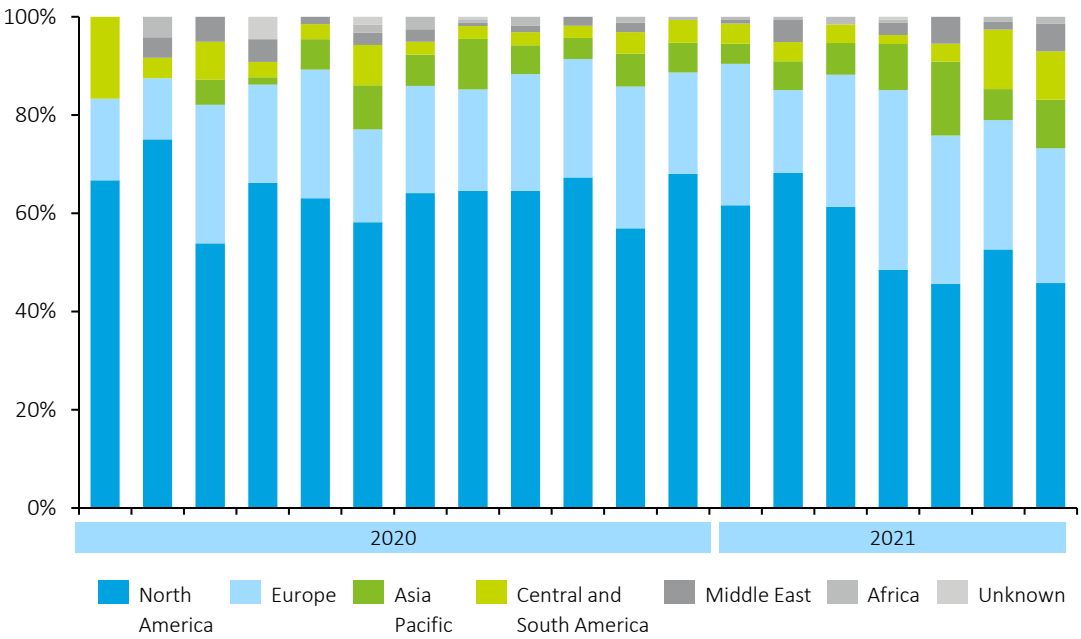


Source: Deloitte

Based on analysis by the Deloitte Japan Cyber Intelligence Centre, Figure 6 breaks down how many damaging incidents there have been each month by region around the world. Although North America continues to account for the majority of these incidents, the number of incidents in North America along with North America's overall share of such incidents have fallen since 2021. It is unclear whether this fall in damage in North American companies stems from the fact that ransomware attackers have begun to avoid attacking American companies for political reasons, or if the number of organisations that can be easily infiltrated and expected to pay a ransom has fallen.

Ransomware attacks are simple in that they take hostage of a company's ability to continue its operations. As these attacks do not differentiate between country or industry, it is believed attackers will shift their target if a more appealing market makes itself available.

Figure 4: Breakdown of which regions have seen data stolen from companies and posted on leak sites



Source: Deloitte

Can the threat from ransomware be stopped?

With attacks such as the one directed towards a large US oil pipeline operator in May 2021, the damage that cyberattacks can inflict on society has grown more serious. The ransomware that has accompanied these attacks has also developed into a political problem. The G7 Summit held on June 2021 released a formal statement urging all nations to disrupt ransomware criminal networks within their own borders.[1]

A portion of underground networks have had their activities curtailed as a result of these political trends. A well-known Russian-language forum that had been used to find partners for ransomware attacks has now banned ransomware related topics, and a number of leak sites linked to ransomware have been closed.

However, it must be remembered that this is still only a portion of the networks and does not mean that similar trends have spread to all ransomware groups. Even after the statement from the G7 Summit was released, new leak sites have continued to be opened, with there being no immediate signs indicating an end to ransomware attacks.

1. G7 Cornwall UK2021, "Our Shared Agenda for Global Action to Build Back Better," *Carbis Bay G7 Summit Communiqué*, June 2021.

Remaining vigilant

Ransomware attacks do not discriminate in who they target. This is because what they take hostage is a company's ability to continue their business. This means that attackers can target anyone who would be left at a disadvantage if their IT systems were to be rendered inoperable. Just because a company does not possess cutting edge technology, deal with large volumes of personnel data, or undertake work from the government does not mean they will not be targeted.

With the acceleration of digital transformation and the wide-spread adoption of remote work, society's reliance on IT systems as a whole has only continued to grow. However, this also means that attackers will increasingly find the infrastructure and core systems that organisations use to provide their services as attractive targets.

A ransomware attack could suddenly place an organisation in any of the following situations:

- The organisation's PCs stop working
- The organisation's customer servers are shut down
- The organisation's data is posted on a leak site.

To protect against the damage from ransomware attacks, it is important for organisations to remain vigilant and to continue implementing basic countermeasures such as:

- countermeasures for vulnerabilities in public external devices
- monitoring internal networks
- safeguards for so-called end points or critical data
- preparing backups of data.

Preparing to respond to an incident

The damage from double extortion ransomware attacks has continued to increase not just overseas, but also in Japan. There was the aforementioned ransomware attack at a US pipeline operator that saw its operations halted, as well as examples involving Japanese companies–which included a major construction company and games developer–having their classified information leaked to the dark web. Furthermore, recently there have been instances of companies experiencing 'triple extortion', in which attackers force a company's sites and services offline by sending large amounts of data to their servers or networks. Some companies have even experienced a 'quadruple threat', in which attackers apply pressure to the targeted company by going so far as to contact their clients and customers directly. The threat from these types of extortion is only continuing to rise.

Drawing on our experience assisting organisations to deal with cyber incidents and improve their cyber defences, the following section outlines what kind of preparations are necessary to help prevent and minimise the damage from double extortion ransomware attacks. We narrow down six points that many targeted companies fail to prepare for in advance.

1. Applying a whitelist to internet exits

Attackers prepare backdoors so that they can further intrude upon systems even if the entrances they initially exploited are blocked. If a company responds to an incident without blocking these backdoors, they may be subjected to a secondary attack during their response, which may lead to even more of their information being leaked or their systems being halted due to their data being encrypted. All of this will very negatively impact the company's reputation amongst its customers and clients. Further issues may also rise, such as setbacks and reworks during recovery operations.

One approach for deterring secondary attacks is countermeasures against backdoors. However, it is difficult to discover where backdoors have been set up, and many backdoors access the internet through infected devices. This is difficult as it would be necessary to completely block internal access to the internet to halt such activities.

It is common for businesses these days to use cloud services and exchange data with their clients through the internet. A company can expect a large impact to its operations if it completely blocks all its internal exits to the internet. For this reason, we would advise companies to prepare contingencies, verify how blocking access to the internet will impact their operations, and prepare a whitelist that can be applied immediately. The whitelist should contain a minimum number of required internet destinations. In addition, web isolation can be used as a technical countermeasure against backdoors. Although this is a powerful countermeasure, it can also negatively impact convenience. Therefore, companies need to consider what impact such a countermeasure will have on their operational efficiencies.

Furthermore, as most unauthorised intrusions are made using an overseas IP address, one conceivable method to prevent such intrusions would be to completely block access from overseas IP addresses. However, caution is required when considering such an action, as companies cannot uniformly block such access if they are using a cloud service or if they have clients overseas.

2. Gathering and storing logs that will be necessary for investigations

An additional countermeasure to deter secondary attacks is to identify–and update for–methods of attacks/intrusion routes that were exploited. To identify these intrusion routes and methods of attack, the logs from a number of sources will be necessary. When broadly classified, these will come from networks, computers, and security products. It would be wise to gather these logs and to keep them stored for a certain period of time.

Network logs will be necessary to investigate when the targeted computer was attacked, what type of computer was used in the attack, and how much data was transmitted. In particular, this will be necessary to identify the computer connected to the internet that the attackers used and to identify how much information was leaked externally. The logs that will be required will primarily come from firewalls, proxy servers, Domain Name System (DNS) servers, VPN devices, and electronic mail servers.

The kind of computer logs that can be obtained will differ depending on the operating system (OS) type. However, event logs will serve as an important clue for Microsoft Windows, which may be an easy target for double extortion ransomware attacks. With these logs, clues can be obtained including when the unauthorised login took place and what type of unauthorised program was run.

Furthermore, these event logs will also be necessary to investigate which computers the attackers travelled between, with the goal being to identify the extent of damage. Information from cyber security centres such as JPCERT/CC[2] or the Center for Internet Security (CIS)[3] should be referenced to change how the event logs are configured, as the logs that will be necessary for the aforementioned investigations cannot be obtained with the default settings.

For security product logs, logs from Endpoint Detect and Response (EDR) products, anti-virus products, and products that obtain records on computer operations will be useful for investigations. As there is a great variety of security products, it would be wise to understand what makes each security product unique, and to examine beforehand how these products can be used to investigate intrusion routes, methods of attack, and extent of damage.

The Deloitte Japan Cyber Intelligence Centre also sees many cases in which logs that fall within the period of investigation no longer exist as they have exceeded their storage period. JPCERT/CC recommends that logs are stored for a minimum of one year for investigations into advanced cyberattacks.[4] What's more, it is not uncommon for attackers to delete logs on purpose during an attack. For this reason, we would advise finding a way to safely store these logs, such as by creating an offline backup, or by transferring logs that will be necessary for an investigation to a separate location, which could include a log collection server.

In addition, companies should consider how important it is to preserve the data on an impacted computer prior to its reformatting. We do see cases in which companies reformat their computers without attempting to preserve their data to speed up restoration operations. All logs on a computer will be lost if a computer is reformatted, which will complicate investigations on intrusion routes, methods of attack, and the extent of damage. As a result, this may make deterring secondary attacks more difficult, or might make it impossible to properly report information to impacted parties and stakeholders.

2. JPCERT Coordination Center, "Detecting and mitigating attacks against Active Directory using logs" (in Japanese), July 28, 2017.
3. Center for Internet Security, "Center for Internet Security homepage", accessed September 9, 2021.
4. JPCERT Coordination Center, "How logs are used to respond to advanced cyberattacks and how such attacks are analyzed" (in Japanese), October 19, 2016.

3. Offline backups

Digitalisation in companies is advancing at a rapid pace, with the amount of data that is retained by information systems continuing to increase. As a result, it has become popular to create online backups using hard disks, as this shortens the time needed to create such backups. However, data backed up online is also at risk of being encrypted, as ransomware will encrypt any data regions it can access from the computers it intrudes on.

Based on a report published by the company CrowdStrike, ransomware attacks in Japan have resulted in 32% of targeted companies paying some sort of ransom.[5] Although these companies have not disclosed why they paid these ransoms, it may be that many of these companies were forced to pay as they would struggle to recover their data from their backups. Based on cases we have seen in the Deloitte Japan Cyber Intelligence Centre, it is likely that a number of companies had their online backups encrypted as well.

If a company is unable to recover its data from its backups due to critical systems being encrypted, this will make it very difficult for the company to continue its operations. The impact on a company's operations could be significant if the company could no longer recover core systems such as ordering or accounting systems, which includes past data. We would advise preparing for the worst and discussing what mitigations could be taken in the event a company's backed up data is encrypted due to ransomware. Vendors are now providing data backup solutions that have measures in place to counter ransomware. Taking advantage of such solutions is one way to reduce the risk posed by ransomware.

4. Information management

In the event that a computer is compromised and evidence is found that a certain amount of data was transmitted to an external location, it is very likely that some sort of data within the impacted computer was leaked externally. If this computer contained personal information or important information relating to a client, it will be necessary to identify what kind of data was stored on the computer to prevent any secondary damage. In trying to identify this data, if the company did not manage where data was stored or what kind of data was being stored on this computer, they will need to investigate all the data within the computer. This will require a large amount of time and money for the investigation. For this reason, we would advise first understanding what kind of information your company possesses, and to create a management ledger for important information such as personnel information or information relating to clients.

Current laws in Japan only require companies to make an effort to file a report or notify impacted parties when personnel information is leaked. However, legal reforms that have taken effect from April 2022 make reporting such incidents an obligation.[6] According to the regulatory offices, companies will be obligated in certain situations to file a report when it appears that a data leak may have taken place. Furthermore, there will situations in which companies will be obligated per their contracts to file a report when important information regarding a client is leaked. If there is a high probability that a data breach has occurred, companies are advised at a minimum to take the following actions for information that must be reported: obtain access logs, give access rights to the bare minimum number of users, and limit where data can be stored so that your company can precisely identify where the information was leaked from.

5. CrowdStrike, "Announcing the results of CrowdStrike's 2020 Global Security Attitude Survey" (in Japanese), November 2020.
6. Personal Information Protection Commission Homepage, "2020 amendments to the Act on the Protection of Personal Information" (in Japanese), accessed September 9, 2021.

5. Restricting access to internal networks

Most ransomware is also equipped with the ability to self-replicate. After infecting its first computer, the malware will seek out a computer that can connect to a company's network, broadening the extent of the damage it can cause. The damage a ransomware can inflict will instantly spread if a company has no restrictions in place for accessing its internal networks. To avoid such a situation, companies are advised to limit access to their internal networks to the bare minimum number of individuals. In particular, companies are advised to consider strengthening restrictions for accessing networks that link critical systems and office environments, as well as for networks that link company headquarters with branch/subsidiary locations. Likewise, companies will also need to think carefully when using Server Message Block (SMB) and Remote Desktop Protocol (RDP) communications for their operations, as these are often used by attackers. Companies are advised to anticipate the risk of attackers exploiting these communications, and to consider additional mitigations, such as strengthening monitoring or limiting which devices can utilise these communication protocols.

6. Procedures for responding to the outbreak of a serious incident

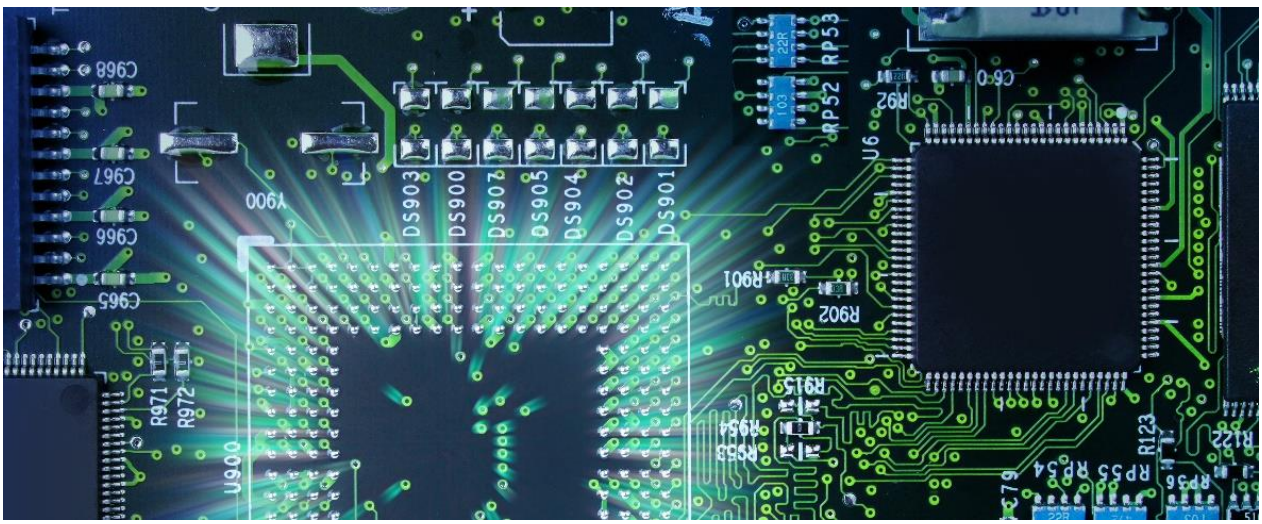
If a company is impacted by a double extortion ransomware attack, it will need to respond concurrently to both the cyberattack and information leak, and also find a way to maintain business operations. However, it is often the case that separate departments are responsible for leading these responses, which makes it easy to confuse which department should be leading the overall response. There are many cases in which companies were delayed in their response due to oversights and duplicate efforts. It is important for companies to work out in advance how their organisation is structured and to allocate responsibilities so that they can respond swiftly to an emergency. It is also important for companies to determine, as a part of these preparations, what kind of external experts they would hire to assist in areas they would struggle to cover by themselves. This could include carrying out technical investigations (forensic investigations) or formulating a response to stakeholders (crisis management).

Companies are advised to consider in advance taking the following actions in responding to a serious incident:

- establishing a crisis control committee based on a resolution from the company's board of directors
- creating a system in which top management leads any response to an incident.

These actions will be important for strengthening the company's effective control and in enhancing its external accountability.

An even more important point is to determine which operations are critical, and to identify the IT systems and infrastructure that support these operations. While this may seem like a simple task, it may require more time than originally anticipated. There may be instances in which a company is looking to restore a certain system that is used in its operations, but must first restore another system that operates in the background. Or if the company is very large, they will need to hold hearings with each of their IT officers, as no single officer will have a complete understanding of the entire IT system. For this reason, companies are advised to identify these operations and their supporting IT systems/infrastructure in advance.



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 2021* (in Japanese).

Deloitte.