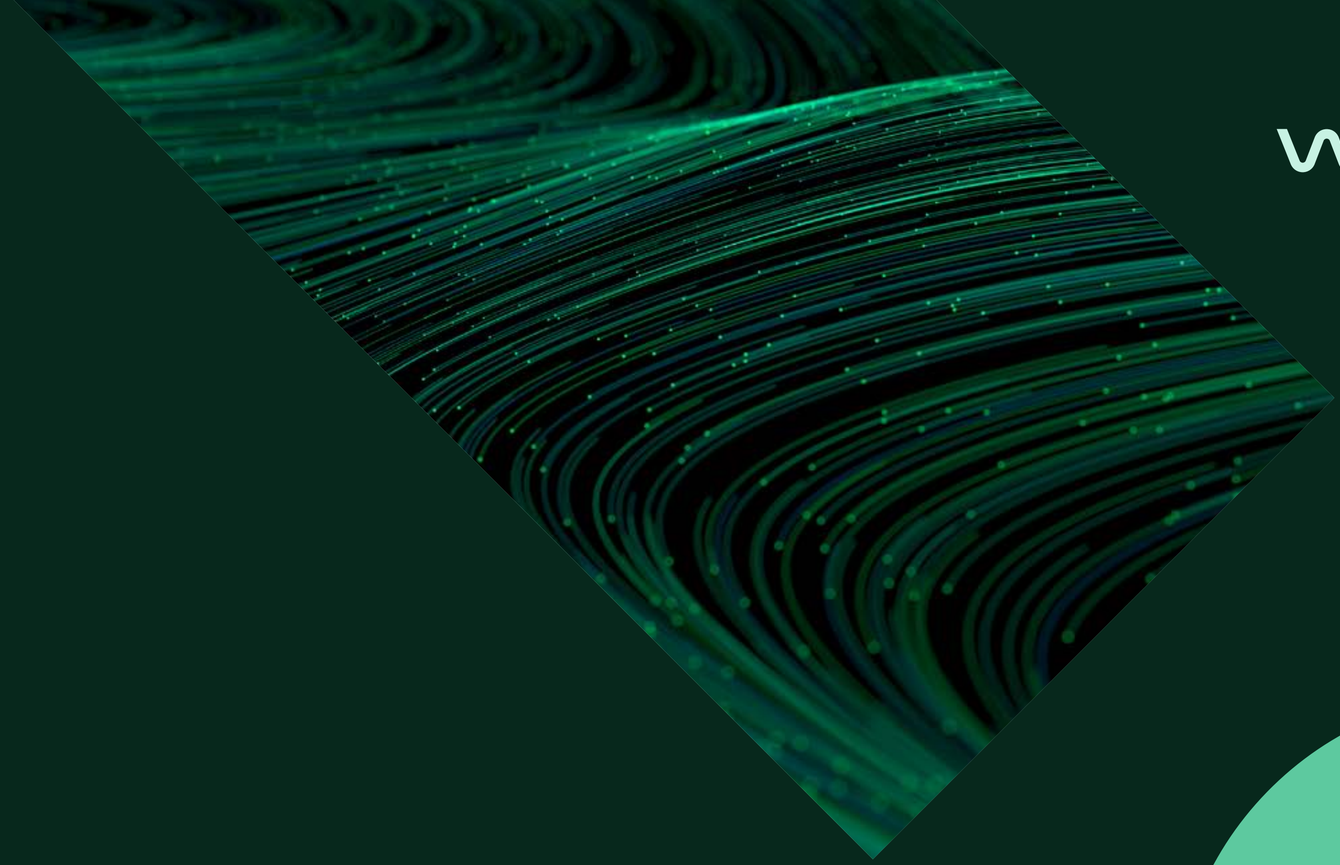
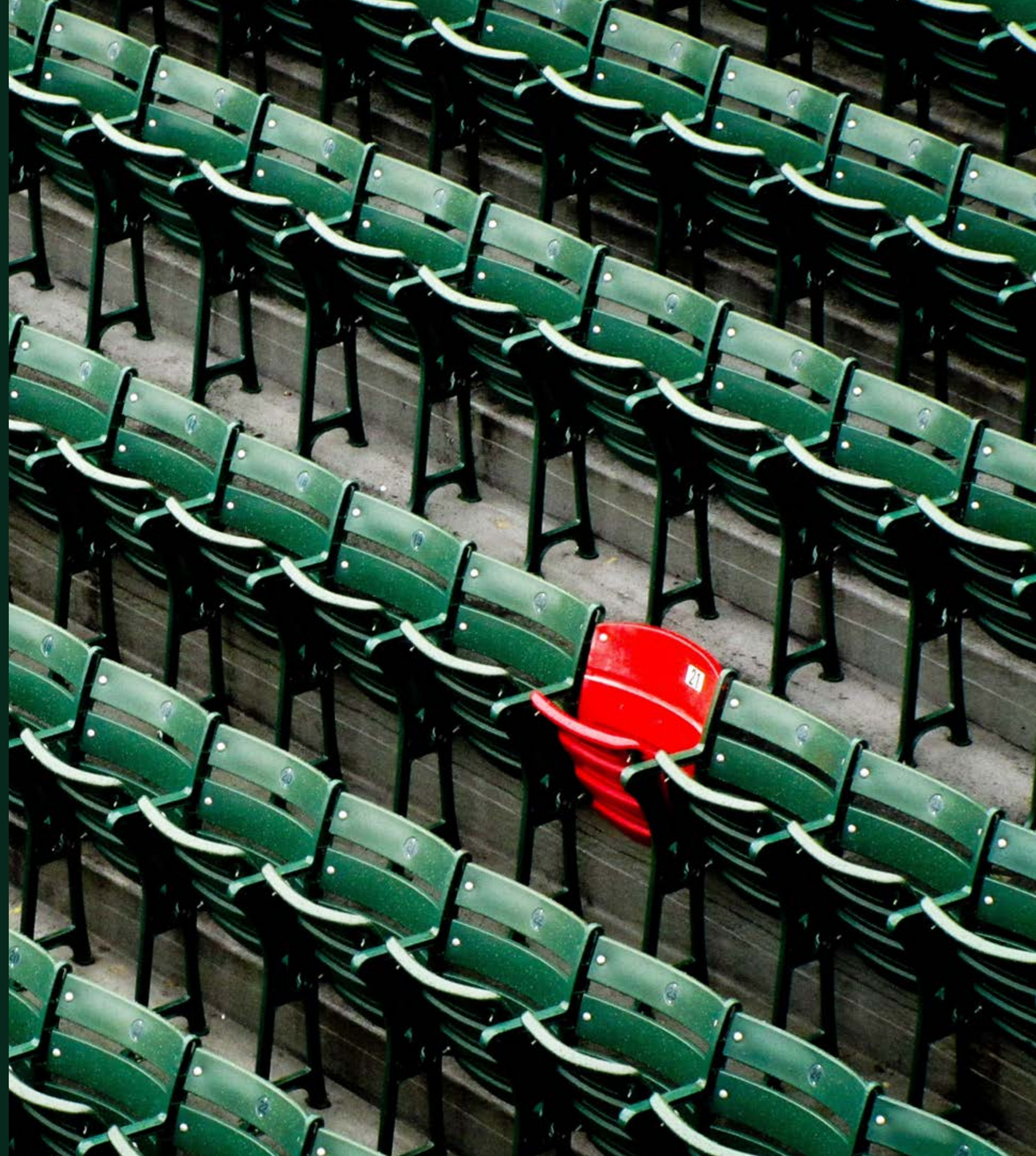
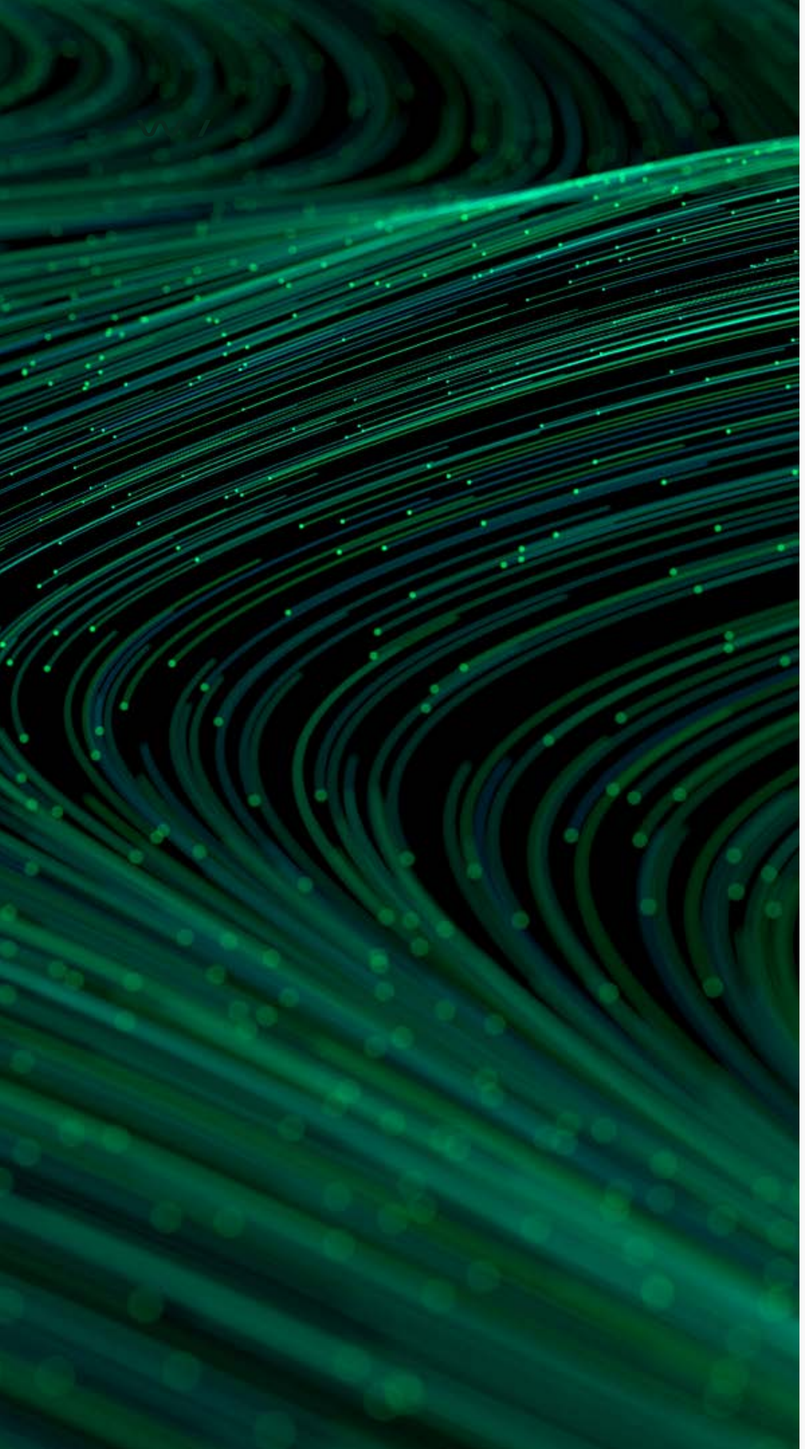


Threat Update

Ransomware

Contents





Intro

Ransomware is a type of malware that's plagued people and organizations for the last decade. From its origins as a floppy disc release demanding rather insubstantial sums of money via snail mail, the ransomware threat has grown in sophistication and scale. Increasingly large ransoms have turned ransomware into a problem with the potential to paralyze multinational corporations or critical national infrastructure relied on by millions of people.

This report contains a brief overview of relevant observations from 2021 with the aim of providing defenders with an update on trends and developments regarding the ransomware threat. Relevant trends highlighted in the report include the steady development of new ransomware families and variants, the evolution of ransomware's capabilities and characteristics, ransomware's prevalence in the global threat landscape, notable families/variants, and observations from WithSecure's first-hand experience in helping victims and would-be victims detect and respond to attacks.

Based on these and other observations, it is clear that ransomware is a significant but manageable threat to organizations.

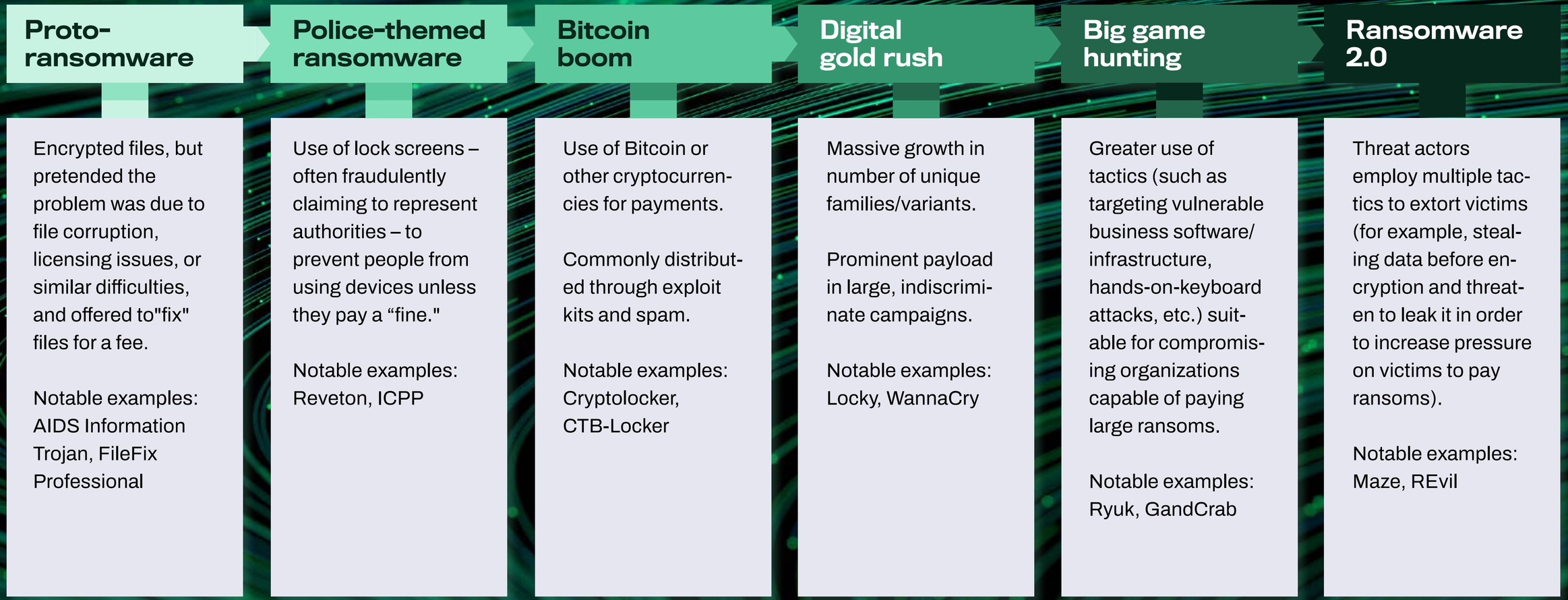
Ransomware’s multi-year evolution

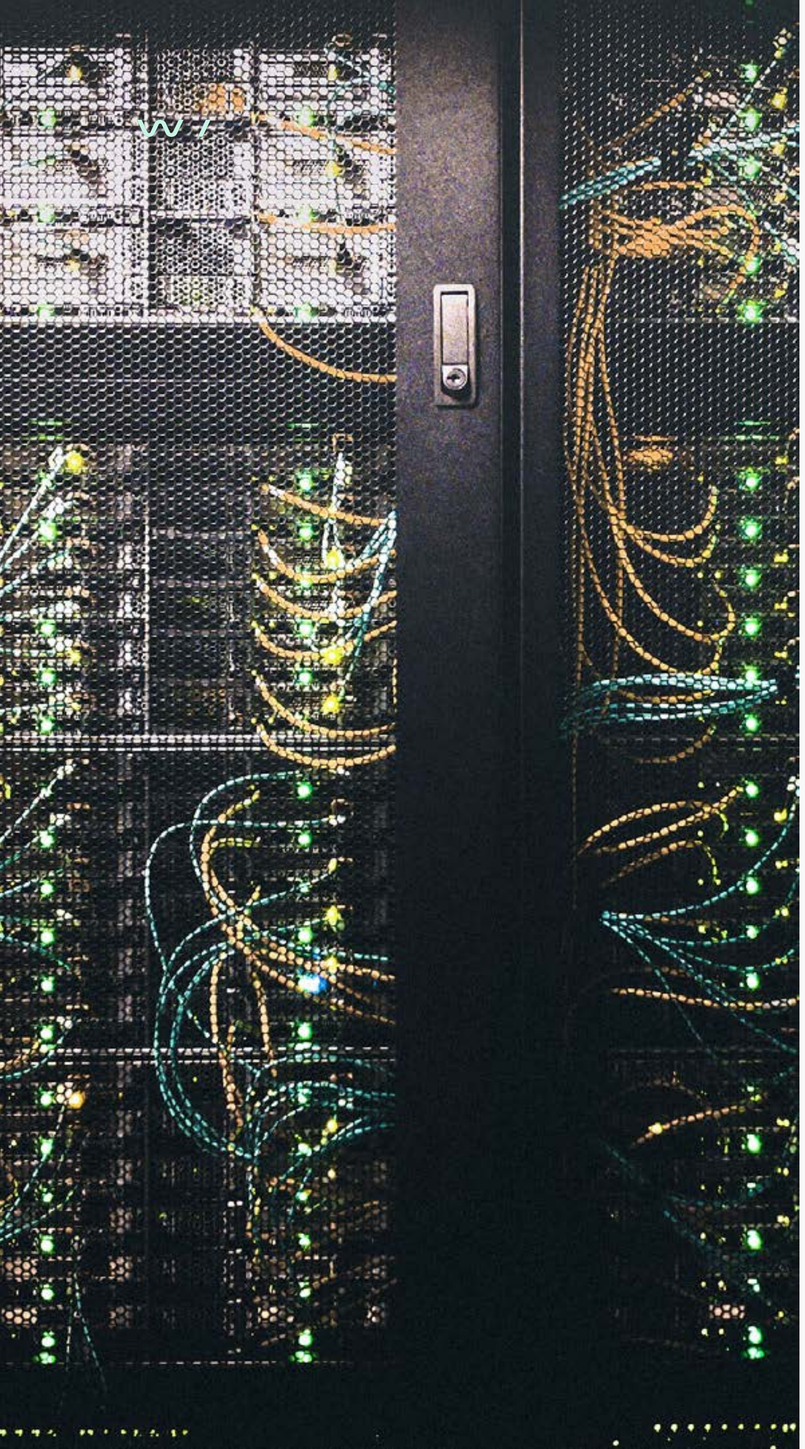
Ransomware is a type of malicious software (malware) that steals control of the user’s machine or data. Most often this is done through encrypting data stored on one or more devices. Once the legitimate users’ access is blocked, the attacker offers to restore access for a ransom. Over the past decade, this approach has become an increasingly effective method of online extortion for cyber criminals and other threat actors, which is generally the primary motivation for these attacks.

Encryption is the most well-known method cyber criminals use to pressure victims. Recently however, attackers have adopted secondary extortion methods, such as stealing and leaking the victims' data before encrypting it.

A ransomware incident can result in severe financial losses for an organization, even without paying the ransom. An attack can lead to a shutdown in operations leading to a loss in revenue, and even if the systems are not revenue-generating, having them offline costs the organization vital productivity time. Over and above the direct financial losses, there are also indirect costs. Organizations may not detect an attack in time to stop it, and tight budgets may leave them struggling to find the resources needed to restore operations. Therefore, either directly or otherwise, any financial loss may force the reallocation of funds from one department to another, leading to service disruptions.

Figure 1. Evolution of the ransomware threat.





As a threat, ransomware dates back to 1989, although at the time it was not recognized as such. The AIDS trojan is commonly described as the first ever ransomware attack and was distributed via floppy disks that used basic encryption to prevent access to the files unless users paid a $189 “fee.”[1]

However, since that time, attackers have continued to develop this business model in many different ways. The idea of paying a “fee” rather than a ransom proved appealing to attackers as it allowed them to represent their restoration service as a legitimate solution to a real problem. Some attackers went as far as developing “police-themed ransomware” that claimed to be spread on behalf of authorities in response to some sort of illegal activity conducted by users. Often, this type of ransomware simply prevented access to devices/data with a message that blocked the screen and could not be closed rather than using encryption. Because the message claimed the user was doing something illegal, the user felt pressured into paying the fee before someone else saw the message accusing them of some sort of crime. In reality, it was simply a method of extorting innocent people and companies.

Ransomware’s popularity continued to grow throughout the 2010s, greatly aided by the advent and growing popularity of cryptocurrencies. Cryptocurrencies provided a new way for the attackers to collect ransom payments without relying on more traditional, better-regulated methods. An example that speaks to the enabling effect of bitcoin is the use of CryptoLocker ransomware by one gang that extorted approximately 3 million USD from 500,000 victims between 2013 and 2014.[2]

The popularity of ransomware surged during this time, attracting significant attention from a wide variety of cyber criminals with varying degrees of professionalism. This surge seemed to hit a peak in 2017. During this time, ransomware became increasingly prevalent in large, indiscriminate spam campaigns, attempting to infect as many victims as possible. This was also the year of the notorious WannaCry ransomware attack. WannaCry was notable as it automatically spread itself to vulnerable devices. While patches for the vulnerability targeted by WannaCry (CVE-2017-0144)[3] had been made available two months prior to the attack, many organizations had yet to update their devices. Consequentially, WannaCry quickly spread among organizations across the globe.[4]

1. https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#3

2. https://www.bbc.com/news/technology-28661463

3. https://www.cve.org/CVERecord?id=CVE-2017-0144

4. https://www.bbc.com/news/world-europe-39907965

After 2017, many ransomware attacks became more sophisticated, evolving into a more pressing threat tailored for extorting organizations. It seemed many ransomware gangs hoped that they could extort larger sums of money from fewer targets by focusing efforts on quality of targets rather than quantity. Rather than relying only on indiscriminate spam campaigns or drive by downloads, these attackers began targeting vulnerabilities in software used by organizations.

More recently, ransomware gangs began to devise ways of increasing pressure to pay up. Perhaps the most common way to do this was by stealing the data prior to encryption, and then threatening to publish the stolen data if the ransom wasn't paid. This development proved to be a considerable challenge for defenders. Even organizations that prepared for ransomware attacks with reliable backups and well-prepared incident response plans, would face considerable business challenges in the event their data (sometimes highly sensitive, confidential data) was exposed to the public.

Adversaries continue to develop this model by finding additional ways to threaten their victims (such as SunCrypt and Ragnar Locker's use of denial-of-service attacks[5]).

Estimates suggest that the "ransomware industry" is now inflicting billions of dollars in damage on companies[6]. There have been some recent high-profile examples when huge ransoms were paid by companies to recover their data after an attack. In 2021, meat processing company JBS confirmed that it had paid $11 million to the REvil ransomware gang after their systems were compromised.[7] Later that year, the U.S. Colonial Pipeline was reported to have paid a $4.4 million ransom after suffering a sophisticated attack from DarkSide that compromised computer systems across the pipeline, leading to fuel shortages and panic in the U.S.[8] These figures confirm that ransomware's business model is a profitable method of online extortion, and helps explain its notoriety.

Organizations, regardless of size, or industry, can be brought to a standstill by a successful ransomware attack. Ransomware infections can often jeopardize a company's business interests, making it easier for criminals to pressure them into paying the ransom. Many organizations depend on IT systems and databases to operate and in some cases, they'll have legal obligations to manage and protect customer data. It's for these reasons that organizations often feel pressure to resolve ransomware infections quickly (and quietly) by paying the ransom.

5. https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/

6. https://www.europarl.europa.eu/resources/library/images/20220126PHT21867/20220126PHT21867_original.jpg

7. https://www.bloomberg.com/news/articles/2021-06-09/jbs-paid-11-million-in-ransom-to-resolve-cyberattack-dj?s-ref=CIpmV6x8

8. https://edition.cnn.com/2021/06/07/politics/colonial-pipe-line-ransomware-recovered/index.html

Ransomware trends

Figure 2. New ransomware families/unique variants discovered in 2021.

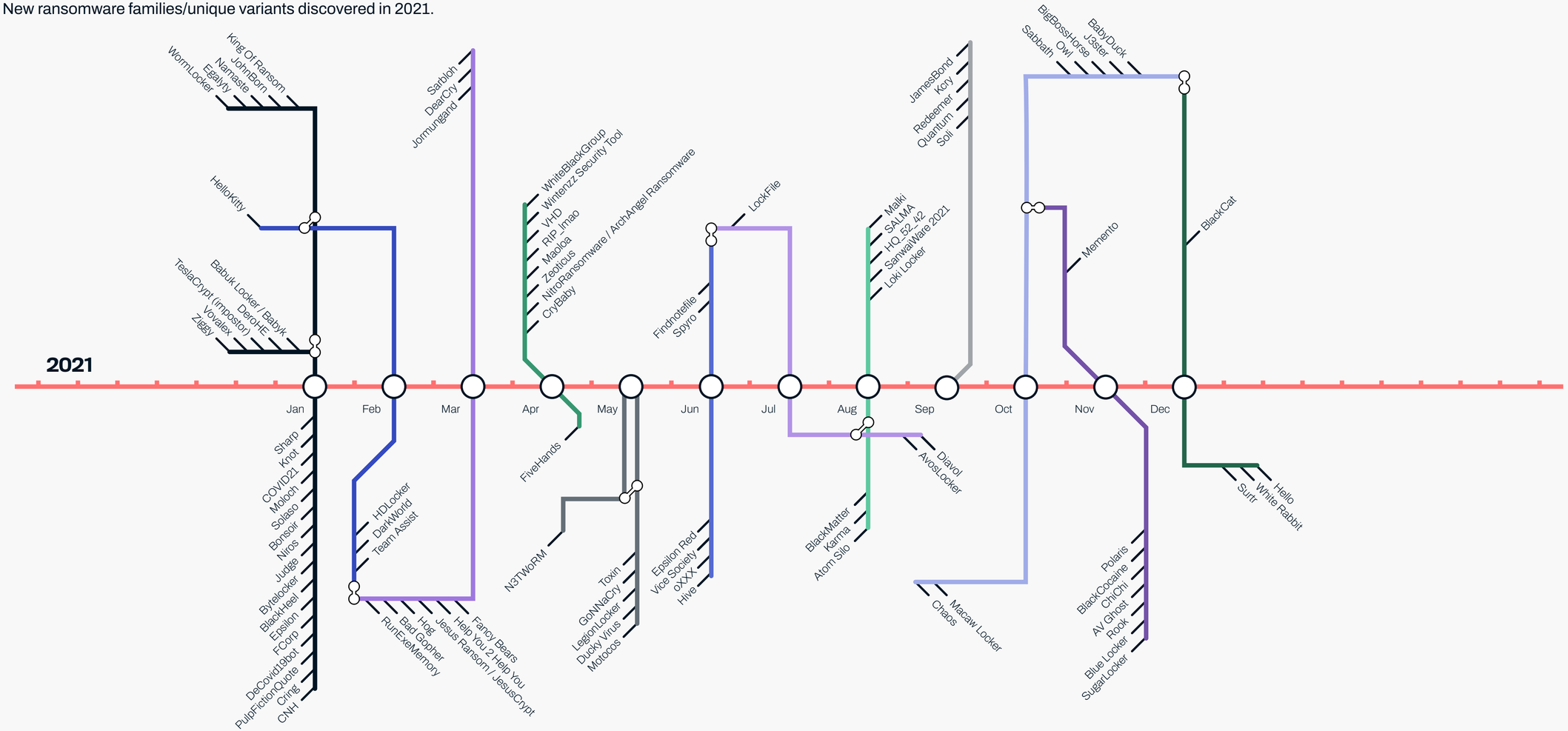


Figure 3. # of new ransomware families/unique variants per year

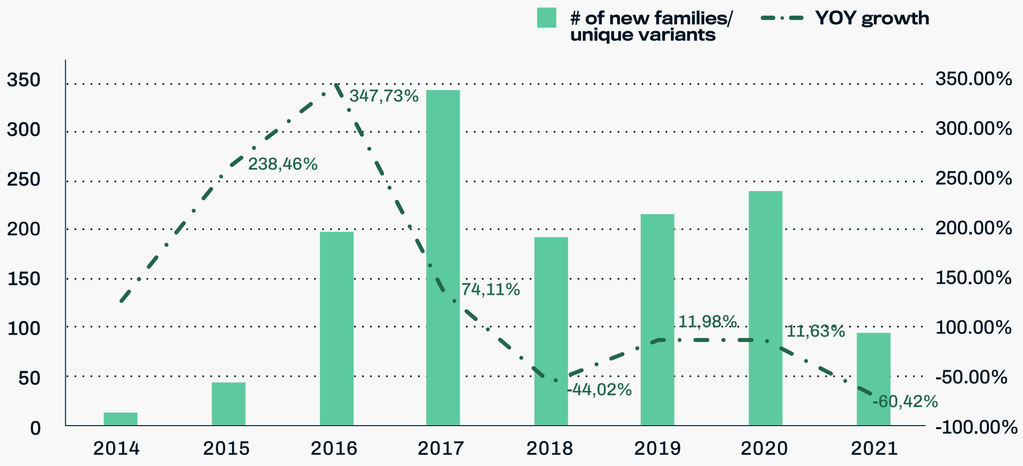
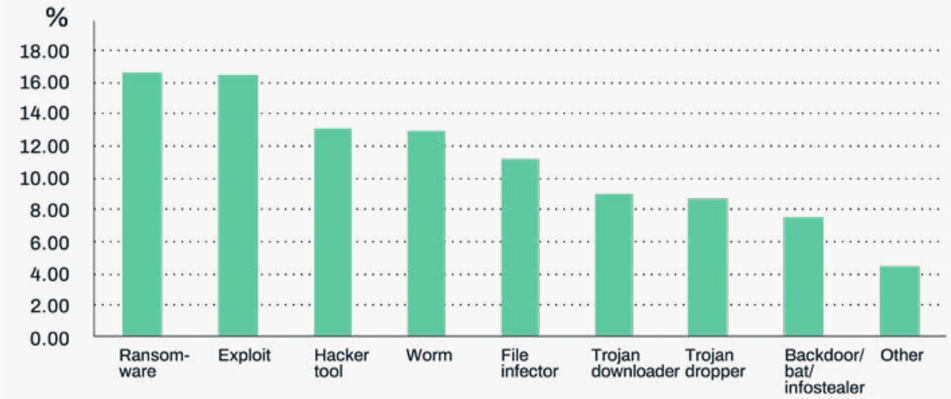


Figure 4. Prevalence of threats by identified type in 2021



Ransomware has remained a prevalent threat for the better part of the last decade. Creating new ransomware is relatively easy. Thanks to the success it's experienced in extorting victims, it's attractive to threat actors. This has resulted in hundreds of new families and unique variants appearing each year. This activity peaked around 2017, but remained relatively stable for most of the latter half of the last decade. 2021 saw a significant drop in the amount of new ransomware discovered by security researchers. It is difficult to say for certain what's behind the apparent drop. One possibility is consolidation around existing ransomware-as-a-service (RaaS) offerings, such as REvil. These services lower the bar for cyber criminals to conduct ransomware campaigns by eliminating the need to develop their own ransomware and other infrastructure.

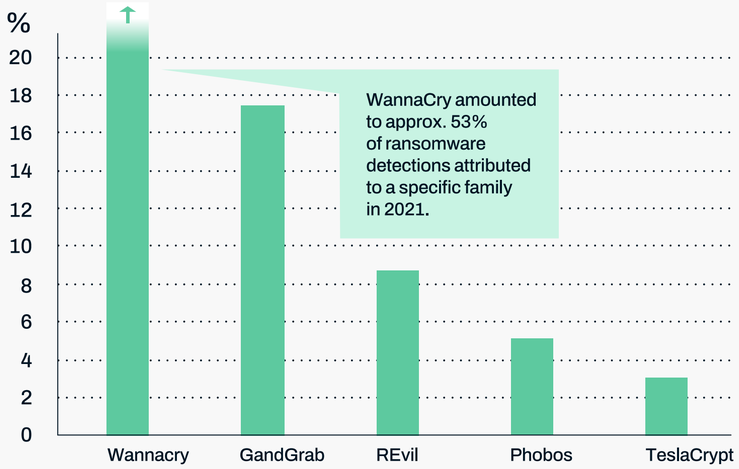
Regardless of this drop, ransomware's continued prevalence is a clear indicator that it remains a significant threat to organizations Ransomware accounted for nearly one-fifth of identified threats encountered by users in 2021, making it the year's most prevalent threat type.

WannaCry was the most prevalent family identified in our telemetry by a considerable margin. It accounted for over half of non-generic ransomware detections, which was more than the next 4 prevalent families combined. Its dominance is largely driven by its automated spread. It can make multiple attempts to infect a small number of hosts, which inflates its dominance in prevalence statistics.

The next three most prevalent families, GandCrab, REvil, and Phobos, are all RaaS offerings. GandCrab, a ransomware family first identified in 2018, announced in 2019 that they would cease operations. However, despite their apparent shutdown, many suspect that REvil (first seen in 2019 shortly before GandCrab announced their retirement) is actually operated by the same gang, and that the responsible individuals simply rebranded their operation.[9]

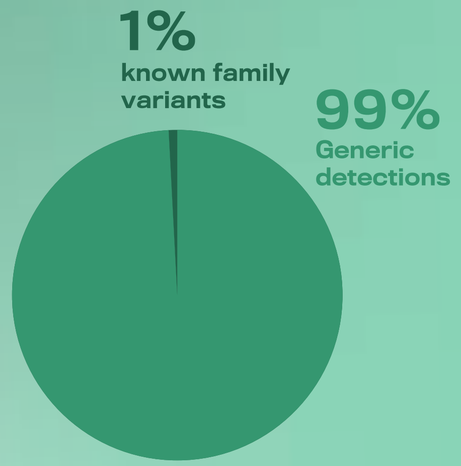
TeslaCrypt, an older ransomware variant, rounded out the top 5. Its prevalence was driven by a modest spike in the first quarter of the year. One possible explanation for this is that there was an unsuccessful effort to resurrect this older ransomware family by using a slightly modified version of the original.

Figure 5. 2021's most prevalent ransomware families



9. https://www.darkreading.com/attacks-breaches/gandcrab-developers-behind-destructive-revil-ransomware

Figure 6. Generic ransomware detected vs. ransomware associated with a known family/variant



While prevalent ransomware families are noteworthy, it is also important to realize that they do not paint a complete picture of the threat. Only about 1% of ransomware in our telemetry is attributed to a particular family. The other 99% are identified as ransomware based on its behavior (such as file encryption) rather than associating it with specific families/variants. Using this approach allows endpoint protection products to block new or obscure ransomware variants before researchers spend time attempting to map the threat to existing variants, giving organizations a fast, effective method of protecting themselves from a significant amount of potential ransomware infections.

Ransomware in the trenches

Figure 7. 2021 IR/DRT ransomware engagements by industry

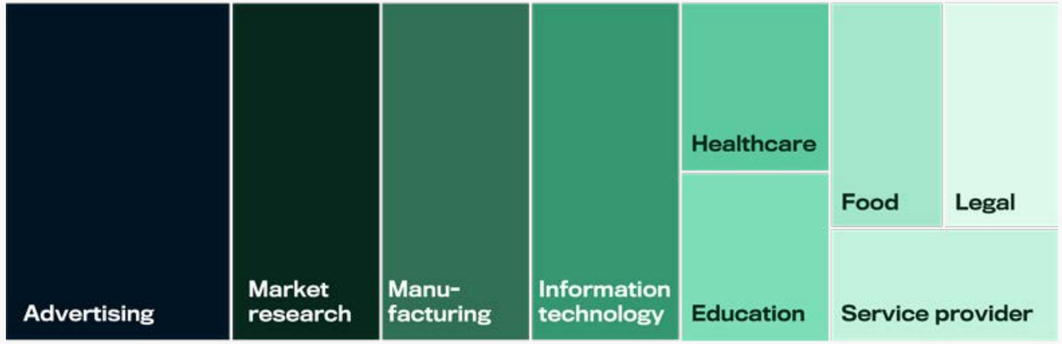
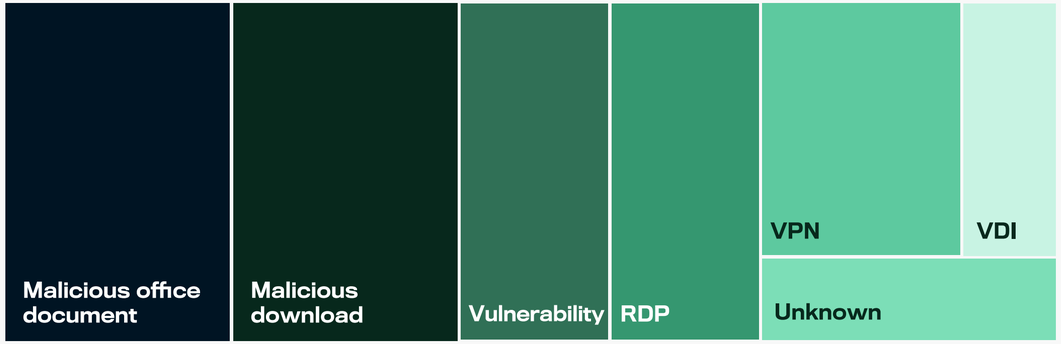


Figure 8. Initial attack vectors observed during 2021 IR/DRT ransomware engagements

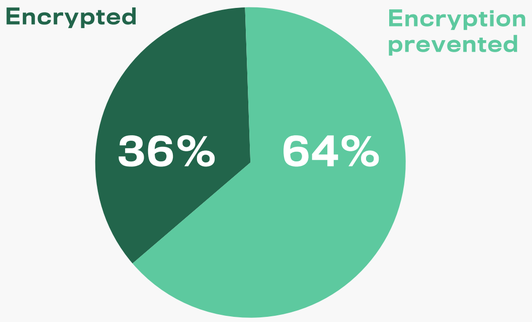


In 2021, WithSecure's Incident Response (IR) and Detection and Response (DRT) teams handled a number of ransomware attacks. Based on these engagements, ransomware is clearly a problem that affects a wide variety of verticals. Essentially, no industry is off-limits to these attackers.

Furthermore, ransomware attackers were observed using a wide variety of techniques to compromise organizations. Malicious office documents and downloads were the most commonly observed in 2021. These techniques can often be employed to opportunistically attack multiple organizations in a single campaign. Exploiting vulnerabilities and accessing networks via exposed remote desktop protocol ports were the next most common initial access vectors seen by WithSecure's IR/DRT teams – both of which require more targeted efforts on the part of attackers. These observations highlight the value of basic security measures in preventing ransomware attacks and other breaches. For example, many of these vectors prey on unpatched vulnerabilities (particularly in internet-facing infrastructure), poor password hygiene, lack of multi-factor authentication to secure online accounts, and other weaknesses that organizations can address.

Fortunately, out of all the ransomware attacks investigated by WithSecure's IR/DRT teams, the vast majority were stopped before the attacker could inflict significant harm the organization. Approximately two-thirds were halted before the attacker could encrypt any data, thereby sparing organizations from significant losses due to downtime, extortion, etc.

Figure 9 . IR/DRT ransomware engagements resulting in data encryption



Minimizing ransomware's impact

Ransomware has proven itself to be a significant threat to organizations working in different industries across the globe. However, it is not an unmanageable threat. While the million-dollar ransoms and other problems highlighted above seem daunting, it is possible for organizations to minimize the potential damages incurred by ransomware attacks.

The specifics can depend on many different things. Ransomware may affect organizations across industries and regions, but the resources defenders have is a different story. Large banks, for example, dedicate significant resources to protecting themselves from ransomware and all manner of threats. A small chain of grocery stores, on the other hand, may not have the same awareness of the threat, or allocate the same amount of resources to protect themselves..

As with many other cyber security challenges, it is important to have a multi-layered defense strategy in place. For this reason, it is appropriate to think of a defense strategy as a program to follow rather than a set of tools.

Prevention

An ounce of prevention is worth a pound of cure, or so the saying goes. This is as true for cyber attacks as it is for fires. As demonstrated by the data contained in this report, there's a considerable amount of ransomware activity that organizations must contend with. While endpoint protection has its limits, it remains an effective tool in preventing ransomware infections.

Detection

Even with reliable prevention measures in place, its important for organizations to prepare themselves for cases where these prevention strategies reach their limits. This can happen for more reasons than people may think. Even when everything works 100% of the time, many of today's biggest ransomware attackers are dedicated, well-resourced cyber criminals. They can often breach networks ahead of time and systematically disable defenses while learning where to strike to inflict the most damage on their victims.

For this reason, organizations need to prepare themselves to detect malicious activity within their own networks. Some organizations, such as large multinational corporations or those working in security-critical industries, invest enough to develop these capabilities in-house. However, there are a multitude of potential partners that organizations can partner with to provide detection capabilities for their networks.

Response

Finally, detection without response is like having a smoke detector without a plan or resources to actually put out a fire. Detecting an imminent ransomware incident or a breach in progress will not actually stop the attack. It is important for organization to prepare to respond to attacks, including ransomware.

Today, responding to a cyber attack can be something simple (such as locking a compromised account), or a company-wide event that requires action across a number of different departments. While it is easy and somewhat tempting for business leaders to view a cyber attack as primarily an IT problem, the potential impact can affect an entire organization and possibly even its customers. For this reason, incident response plans need to go beyond technical considerations and include steps to ensure business continuity.

At the same time, it is important not to cause panic throughout an organization in response to a minor security incident. For this reason, finding a cyber security partner to help organizations prepare for ransomware and other incidents can alleviate the risks posed by an unchecked cyber attack.

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH® secure