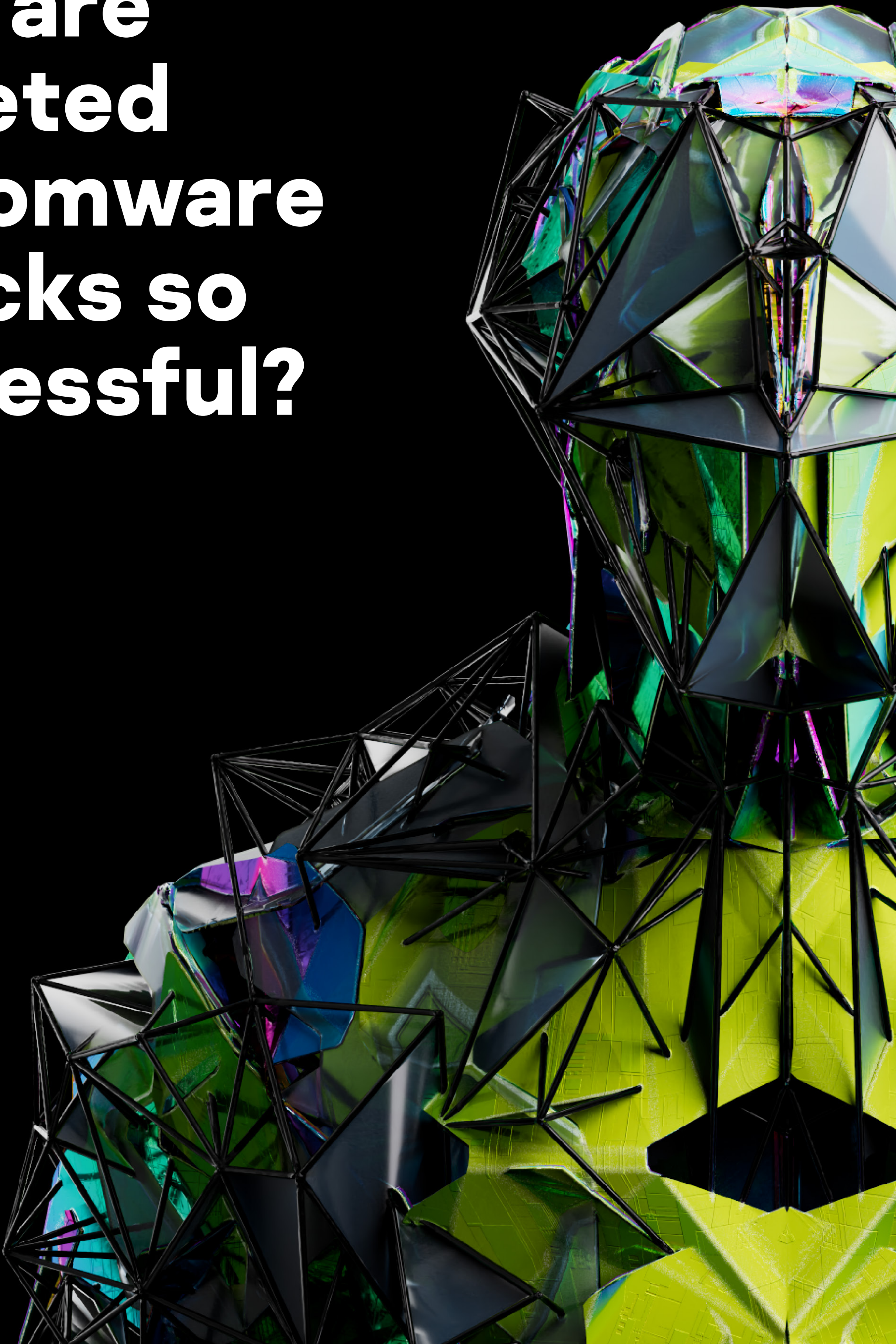
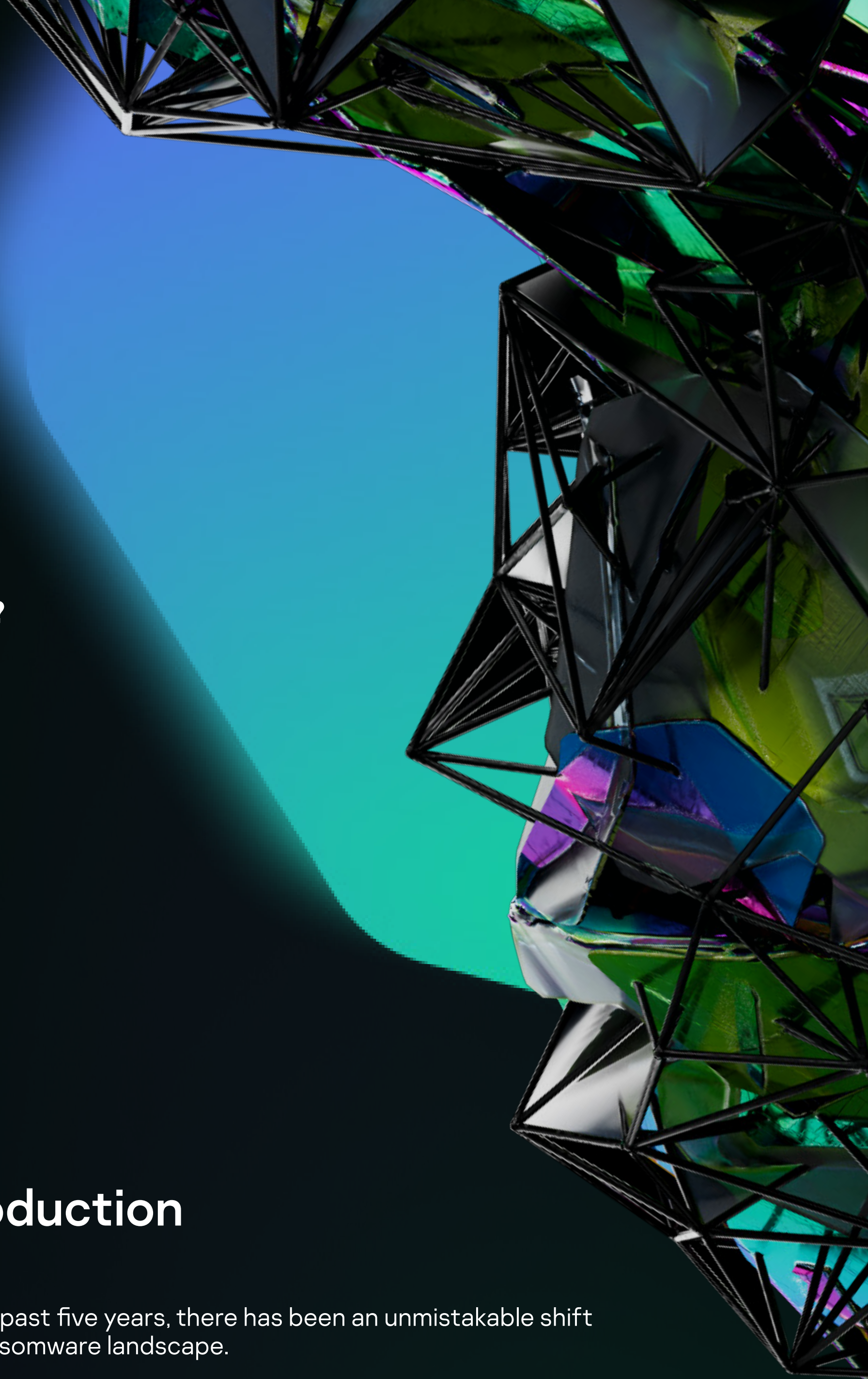
kaspersky

Why are targeted ransomware attacks so successful?



kaspersky BRING ON THE FUTURE



Contents

Introduction

Over the past five years, there has been an unmistakable shift in the ransomware landscape.

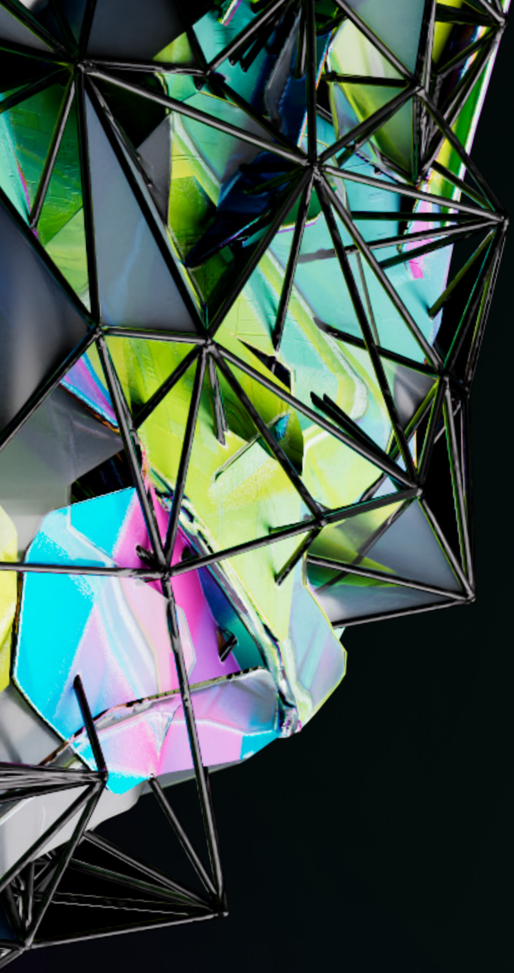
No longer are scattered gangs of disorganized actors carrying out mass ransomware campaigns, simply trying to infect as many computers as possible and extorting relatively small amounts of money from users to get their encrypted data back.

We've entered the era of so-called "Big-Game Hunting": high-profile, fully-fledged ransomware businesses targeting large organizations with sophisticated, planned attacks aimed at extorting huge sums, sometimes with highly destructive, real-world consequences. These criminals often deploy new ransomware written in "cross-platform" programming languages, able to flexibly adapt at scale to the different combinations of architectures and operating systems of complex organizations. And they're employing a new tactic known as "double extortion": threatening to publicly release stolen, sensitive data if the victims don't pay up.

How do these "big-game hunters" choose their "prey"? How are they organized, and why are their attacks so extraordinarily successful? How come even relatively mature, large organizations fall prey to their maneuvers? What makes an organization particularly vulnerable, and what steps can be taken to shore up the defenses? These are the questions we'll be tackling in this whitepaper.

According to data from the US Treasury's Financial Crimes Enforcement Network (FinCEN), organizations in the U.S. alone may have paid nearly 600 million dollars to ransomware groups in the first half of 2021. And, according to the same report, if you look at the most prolific actors from the past year, they have potentially received $5.2 billion in transfers over the last three years.
From 2019 to 2020, the number of unique users affected by targeted ransomware — ransomware that is designed to affect specific users — increased from 985 to 8,538, a 767% jump.[1]

[1] https://securelist.com/ransomware-by-the-numbers-reassessing-the-threats-global-impact/101965/



Criminal Ecosystems

It's worth spending a little time at this point looking at how these criminal gangs operate. This will help us understand what kind of victims they look for, and how they achieve their goals.

With the rise of big-game hunting, we've seen the emergence of high-profile groups in the ransomware world: names such as Maze, Conti and REvil may be familiar. These criminals realized that cultivating a strong "brand presence" (through press releases, for example) would increase their credibility, making victims more likely to pay up.

However, such branding makes it seem like single entities are behind these attacks, pulling all the strings. But in fact it's typically a complex ecosystem of independent actors, supplying services to each other through dark web marketplaces. These actors don't need to know each other personally, since they interact through internet handles and pay for services with cryptocurrency.

(By the way, this is one reason why paying ransoms is strongly advised against: a criminal ecosystem must be dealt with systematically, for example by preventing the money from circulating inside of it. Simply arresting a single entity will not make a big impact, since other supplies will immediately rise up to fill the void.)

So who are these actors, and what roles do they play?

How does a ransomware attack work?

The Long Game

In 62.5% of attacks, attackers spend more than a month inside the network before encrypting data.[2] For example, in the REvil attack against foreign exchange company Travelex, the cybercriminals had infiltrated the company's network six months before they actually encrypted the data and demanded the ransom. A properly organized process of attack detection and response reduces the time it takes to detect attackers in the network and prevent final damage.

Initial Access:

The first group are *Botmasters* and *Account Resellers*. The goal of both of these actors is the same: to gain access to as many potential victims as possible by installing malware and exploiting network vulnerabilities. They then sell this access as a monetizable resource to anyone who's interested — in our case, ransomware criminals.

Infiltration:

Next, another group (known as *Partners, Affiliates* or *The Red Team*) uses this initial access to quietly infiltrate the system. This stage can take months, as the criminals obtain administrative privileges, deploy backdoors, and identify and exfiltrate any valuable data to extort the victims with later. They may also employ the services of *independent analysts* to help them estimate the financial health of the target, the value of any exfiltrated data, and the highest ransom price they can set.

Deployment:

The red team is ready to deploy the ransomware, encrypt the data, and start negotiations. But they don't deploy their own in-house ransomware, no — they purchase a ready-made, user-friendly ransomware kit from *Ransomware Developers* on the Dark Web, who sell their products for a percentage of the ransom. This business model, known as "Ransomware-as-a-Service" (RaaS), lowers the technical expertise required to carry out an attack.

Negotiations:

Finally, yet another team with a different skillset may be employed to handle the ransom negotiations and launder the subsequent cryptocurrency reward.

[2] Kaspersky Incident Response Analyst Report 2022

Low-Hanging Fruit

The key point to bear in mind about all the above is that these are not criminal masterminds, sitting down together to carefully study the Forbes 400 and decide who they're going to target next. They are more like opportunistic highwaymen, spotting an underprotected caravan full of lucrative bounty and jumping on it. In that sense, a "targeted" ransomware attack is a bit of a misnomer.

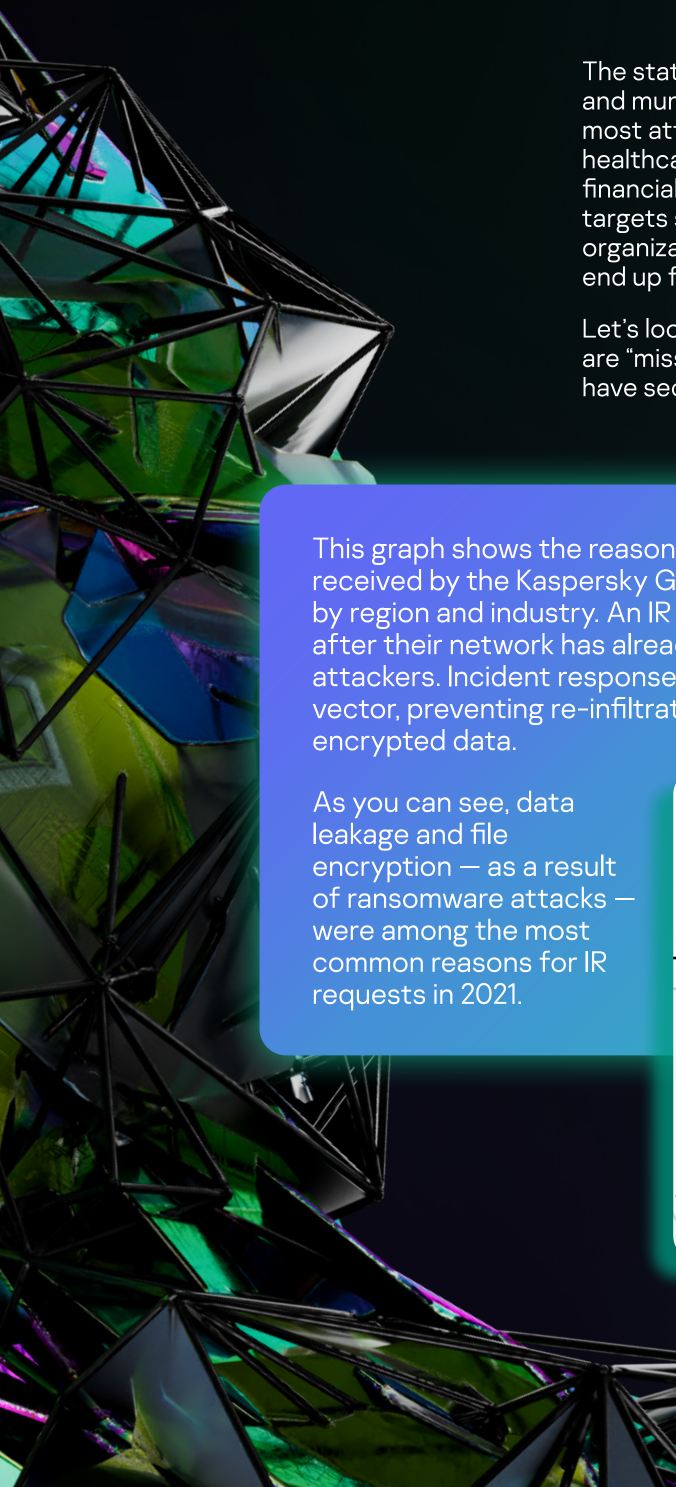
This has important implications for how organizations can protect themselves against ransomware: essentially, **fix those basic system vulnerabilities, and criminals won't get the initial foothold they need to launch their attacks.**

Later on, we'll take a closer look at what makes large organizational systems open to exploitation; but first: which kinds of companies are criminals typically attacking, and why?

Vulnerable Sectors

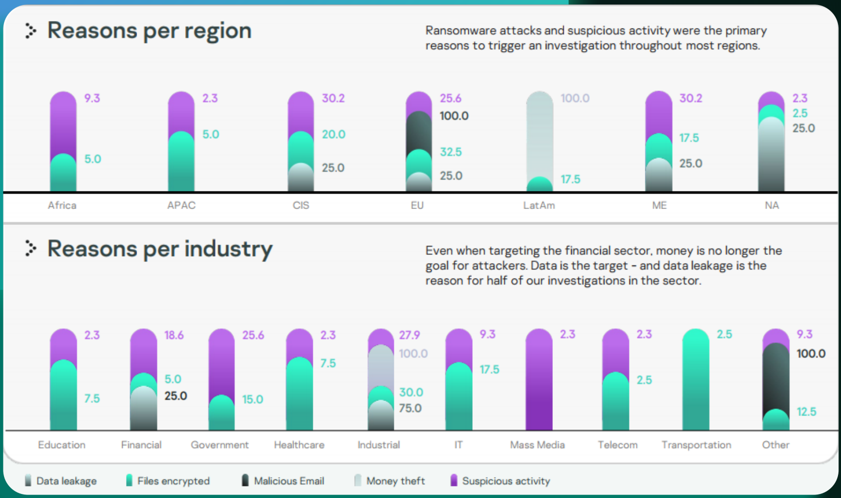
The statistics are clear that public institutions (such as governmental agencies and municipalities) and businesses (particularly in the industrial sector) are the most attractive prey for big-game hunters. Organizations in the education, healthcare, IT and finance sectors are also likely targets. Besides the obvious financial rewards of targeting large, wealthy organizations, what makes these targets so attractive to ransomware attackers? And how is it that such large organizations, which should presumably have well-financed security programs, end up falling prey to the hunters?

Let's look at three factors that organizations in these sectors often share: they are "mission critical", they possess vast amounts of sensitive data, and they have security system weaknesses.



This graph shows the reasons for incident response (IR) requests received by the Kaspersky Global Emergency Response Team in 2021, by region and industry. An IR request is made by a company usually after their network has already been completely compromised by attackers. Incident response involves establishing the initial attack vector, preventing re-infiltration, and attempting to restore the encrypted data.

As you can see, data leakage and file encryption — as a result of ransomware attacks — were among the most common reasons for IR requests in 2021.

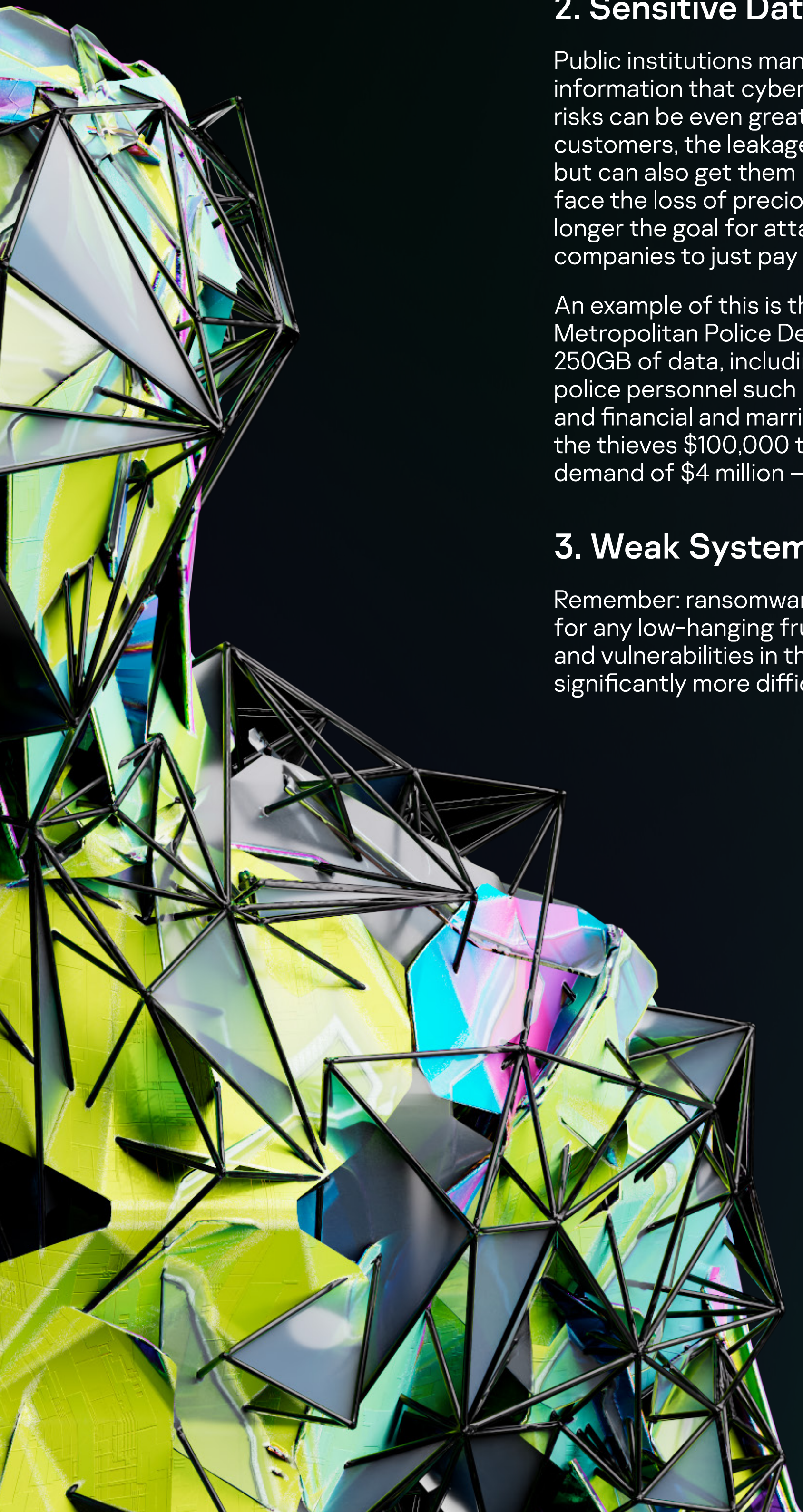


Reasons per region

Ransomware attacks and suspicious activity were the primary reasons to trigger an investigation throughout most regions.

Reasons per industry

Even when targeting the financial sector, money is no longer the goal for attackers. Data is the target - and data leakage is the reason for half of our investigations in the sector.



1. “Mission Critical Companies”

Many of the organizations in these sectors cannot afford to stay offline for very long. For example, the damage caused by production stoppage in an industrial company can run into millions of dollars per day, and conducting an investigation into the attack can take weeks, without clear hope of a resolution. The danger for healthcare providers of their vital systems not functioning is obvious. And if municipal services are blocked, the welfare of citizens is directly affected both financially and in other significant and sensitive ways. Dramatic, real-world consequences like these make such organizations much more likely to just pay the ransom to get things up and running again.

The 2021 Colonial Pipeline attack is a classic example of this type of vulnerability. Colonial Pipeline CEO Joseph Blount explained that he decided to pay the ransom ($4.4 million) because, at the time the demand was made, it wasn’t clear how widespread the intrusion was or how long it would take the company to restore the compromised systems. Paying the ransom seemed like the fastest way to get back to business.

2. Sensitive Data

Public institutions manage huge databases of personal, confidential information that cybercriminals can use to extort them. For businesses, the risks can be even greater: they also may have large amounts of data on their customers, the leakage of which would cause not only great reputational harm, but can also get them in trouble with regulatory authorities. They could also face the loss of precious trade secrets. Even in the financial sector, money is no longer the goal for attackers; data is the target.[3] It makes more sense for these companies to just pay the ransom and keep everything behind closed doors.

An example of this is the 2021 ransomware attack on Washington D.C. Metropolitan Police Department, in which the Babuk group reportedly stole 250GB of data, including a gang database and masses of personal data about police personnel such as Social Security numbers, psychological assessments, and financial and marriage history. In this case, the police department offered the thieves $100,000 to stop the leaks, but this didn’t satisfy the crew’s initial demand of $4 million — so they kept leaking.

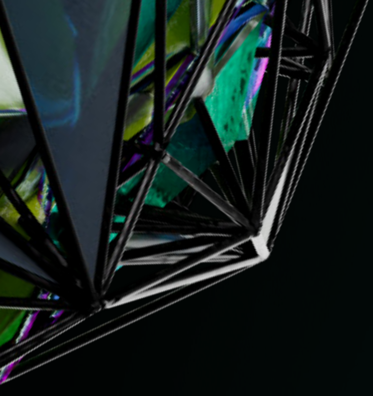
3. Weak Systems

Remember: ransomware attackers are opportunistic highwaymen, looking for any low-hanging fruit in the form of misconfigurations, weaknesses and vulnerabilities in the network. Without these cracks in the system, it’s significantly more difficult for attackers to slip in and do further damage.

Easy Access

According to investigations by Kaspersky’s Global Emergency Response Team, in **more than half** of all incidents in 2021, the initial attack vectors that intruders exploited were vulnerabilities in public-facing applications, such as VPNs, Citrix, VNC, RDP. These vulnerabilities are generally widely-known and easy to remedy — the hackers do not need to be rocket scientists to exploit them. Another 17.9% of the attack vectors were compromised accounts (stolen credentials), and 14.3% malicious email (phishing). Again, these vectors should in principle be relatively straightforward to block. So why are ransomware attacks so successful? In fact, there are a number of compounding factors which can make it particularly difficult for large organizations to secure their IT perimeters.

[3] Data leakage was the reason for half of Kaspersky’s investigations in the financial sector in 2021. Kaspersky Incident Response Analyst Report 2022



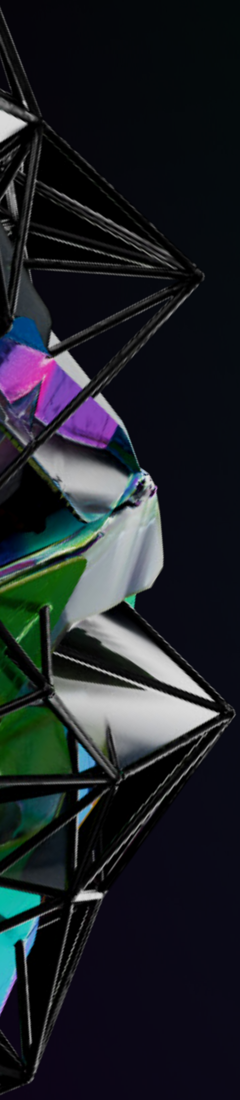
5 Compounding Factors

1. Outdated software and equipment -

As mentioned, old versions of applications and operating systems are full of known vulnerabilities which bad actors can exploit to gain entry. There are lists available on the Internet for anyone to find. The problem here is a lack of awareness and diligence about keeping all software absolutely up-to-date and all known vulnerabilities patched. This problem most often applies to public institutions, which do not always place a high priority on having fresh, modern IT systems (as we all know). Implementing an appropriate patch management policy alone will reduce the likelihood of becoming a victim by 50% .[4]

When a hacker finds and exploits a previously-undiscovered vulnerability, this is known as a "zero-day attack". They're harder to protect against, but not impossible — if well-trained, keen-eyed security teams are provided with relevant threat intelligence. On the other side, some companies make use of "bug bounty programs: hiring professional hackers to search for such vulnerabilities so they can be protected against.

2. An expanded attack surface -



Modern organizations often have complex, interconnected systems stretching onto cloud, mobile devices and remote access — all multiplying the number of gaps that attackers can slip in through. Particularly in the post-COVID 19 pandemic world, huge numbers of organizations have hurriedly switched to remote working, without setting up thorough security standards and procedures for their remote workers to follow. This is a headache for security teams, and a goldmine for ransomware looters: higher volumes of corporate traffic, the use of third-party data exchange services, employees using home computers (and potentially insecure Wi-Fi networks), and widespread use of remote-access tools are all expanding the attack surface.

As mentioned, hijacking remote access tools such as VPNs and Remote Desktop Protocol (RDP) is one of the most common attack vectors that bad actors utilize to gain access to systems — as in the case of Colonial Pipeline.

3. Unmanageable complexity -

Large organizations may have blindly invested in a wide range of security tools, hoping that the more tools they add to their inventory, the more secure they will make themselves; unfortunately, the opposite is often the case. If the tools are not seamlessly integrated to build up a coherent, comprehensive picture of the organization's infrastructure, security teams end up drowning in a flood of disparate data streams. They are unable to detect the presence of an incident — particularly if the intruders are employing sophisticated stealth techniques — and they are unable to respond rapidly and efficiently.

4. The cybersecurity skills gap -

Dealing with the kind of complex attacks that large organizations are facing is not child's play — it requires seriously trained and skilled professionals. According to the US National Initiative for Cybersecurity Education (NICE), in January 2021 there were 521,617 job openings for cybersecurity professionals in the US, versus a total employed cybersecurity workforce of 941,904 — in other words, a simply huge demand for trained security professionals in the cybersphere. These statistics reflect a global trend. And, given the huge demand, those well-trained cybersecurity professionals aren't likely to stick with an average wage in the public sector when they could land a juicy job in a private corporation, leaving such public institutions particularly at risk.

5. The human factor -

This is a problem at all times and in all places: attackers relying on gullible employees to infiltrate the system. Although, again, this may afflict public institutions more, where staff awareness around the dangers of modern cyberspace may not be so strong. Social engineering attacks such as phishing, vishing (voice phishing via telephone), and smishing (SMS phishing) have all been used to get users to install malware onto their devices or steal

[4] Kaspersky Incident Response Analyst Report 2022

their credentials. These tactics can be used in tandem with the previously mentioned vulnerabilities: for example, hackers discover an exposed remote access service, and then profile the organization for relevant information to launch a targeted spear phishing attack with.

Anti-Ransomware Recommendations

Prevention is the best protection, particularly with regard to ransomware: as we've seen, if you don't provide attackers with any easy access to the system, and you pay close attention to any suspicious activity, in all likelihood they'll move on to easier prey. Here are 9 guidelines to follow:

1. **Update software on all used devices** to prevent the exploitation of any known vulnerabilities. Make sure VPNs are installed with the latest available patches.
2. **Set up offline backups that intruders can't tamper with.** Make sure you can access it quickly in an emergency, to minimize idle time and potential damage.
3. **Enable ransomware protection for all endpoints.** Implement a tool which shields computers and servers from ransomware and other types of malware, prevents exploits and is compatible with previously-installed security solutions.
4. **Install anti-APT and EDR solutions,** enabling capabilities for advanced threat discovery and detection, investigation, and timely remediation of incidents.
5. **Focus your defense strategy** on detecting lateral movements and data exfiltration to the Internet. Remote desktop services (such as RDP) shouldn't be exposed to public networks unless absolutely necessary.
6. **Pay special attention to the outgoing traffic** to detect cybercriminals' connections. All network connections, especially those using VPNs or remote access devices, should be kept to a minimum and with privilege restrictions. And of course, ultra-strong passwords everywhere.
7. **Provide your SOC team with access to the latest threat intelligence (TI),** so they can keep an eye out for incoming threats and know how best to counter them.
8. **Provide your SOC team with access to professional training.** Employees should be up-to-speed with the best cybersecurity practices, with special attention to raising awareness on typical ransomware attack vectors.
9. **And remember: never pay the cybercriminals!**

If you would like to learn more about protecting your organization against ransomware, Kaspersky can help. Kaspersky Expert Security — XDR based on a cloud-native EDR solution — provides your organization with enhanced visibility and functionality for AI-based detection and auto-response logic across all endpoints and the network, facilitating a wide range of automated incident response scenarios. The platform's built-in advanced technology for detection and analysis is complemented by world-leading threat intelligence. Kaspersky XDR's unified architecture provides centralized management from a single web console.

To learn more please visit go.kaspersky.com/expert