yubico

WHITE PAPER

Mitigate ransomware risks

The critical role of strong authentication and modern MFA

Contents

Mitigate ransomware risks

The critical role of strong authentication and modern MFA

Ransomware grew by over 485% in 2020[1]

The new ransomware-as-a-service (RaaS) model of profit-sharing in exchange for ransomware tools has proven to be effective.

Introduction

What do a PC manufacturer, a meat supplier and a mental health clinic have in common? They have all been victims of ransomware attacks. They're not alone. Ransomware attacks grew by over 485% in 2020, leveraging the new ransomware-as-a-service (RaaS) model of profit-sharing in exchange for ransomware tools.

Intense media coverage followed the recent Colonial Pipeline ransomware attack that disrupted daily life for millions of people across the eastern United States. More recently, the White House announced a range of initiatives and global conferences to disrupt attackers and assist victims. When it comes to ransomware it's not a question of *if* your organization will be targeted, but *when.* What is your organization doing to prepare for that day? That's a question every business leader needs to consider.

Ransomware and its connection to strong authentication is not well understood today. After all, ransomware is a type of malware designed to attack a system and its data, then hold it hostage with encryption until a ransom has been paid. What does that have to do with authentication? Strong authentication involves establishing a trusted identity of a user or machine before authorizing access to data. The connection between strong authentication and ransomware lies in thinking about the ways actors using ransomware can infiltrate your organization. While a common way it occurs is by users clicking on spurious links and unwittingly downloading malware on to their system, a secondary and more insidious way is for an attacker to take over an account through stolen credentials and then enter the network guised as a legitimate user and installing malware on to a system themselves and watching the harmful process play out. This is a very deliberate chain of events which, if organizations could thwart with stronger forms of authentication beyond passwords and legacy multi-factor authentication (MFA), can significantly foil the plans of attackers.

This whitepaper demystifies what ransomware is, who are typically involved, the way strong authentication and modern MFA can play a critical role in mitigating ransomware risks, and recommendations for good security and process hygiene to stay protected against this fast-growing and disturbing phenomenon.

Defining ransomware

Most cyberattacks rely on malicious software (malware) designed to harm or exploit a target system. As mentioned earlier, ransomware is a type of malware that attacks a system and its data, then holds it hostage till a ransom comes through. It's difficult to trace digital currencies such as Bitcoin, which is often the currency of choice for ransomware attackers. Typically, valuable data is copied to an attacker-controlled system, and a threat of public data exposure is made as part of the ransom demand.

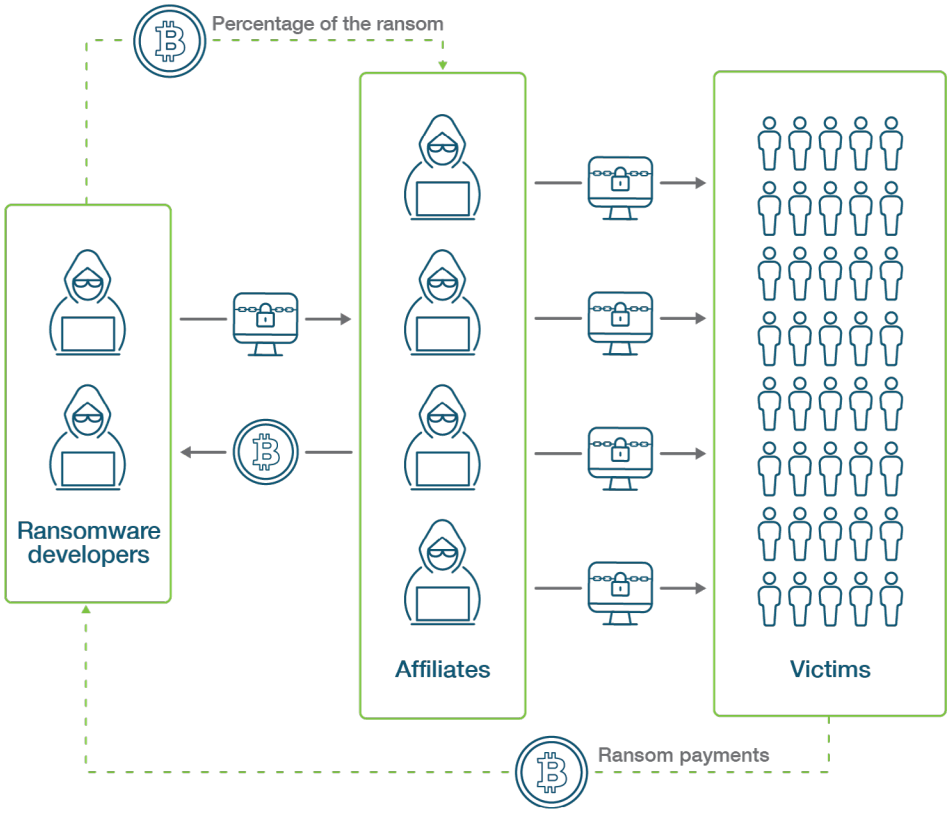
The average ransomware recovery cost in 2021 per attack is $1.85 million, including the ransom, business downtime, lost sales, operational costs and legal fees. Ransomware attacks with more sensitive or critical data or systems involved bring costs closer to $4.44 million, higher than an average data breach cost ($3.86 million). Over 57% of victims end up making a payment to recover their data or prevent its exposure – yet only 8% of victims actually get all their data back after paying the ransom.

Malicious actors behind ransomware

The growth in ransomware has been driven by organized criminal groups, mostly based in Russia, other former Soviet states, and China, with names like DoppelPaymer, REvil, Ryuk, Darkside, and Maze.

These ransomware groups are players in sophisticated criminal networks in which software developers create ransomware, then hand it off to operators called "affiliates" who find vulnerable points in companies to deploy the ransomware. They share ransom payments received from victims. We will see shortly how these actors infiltrate weak points in organizations using a variety of techniques and install ransomware on-behalf-of the user. Fortunately there are methods available today to prevent account takeovers so that malicious actors cannot penetrate systems by logging in on your users' behalf and installing malware.

Crimeware ecosystem



Ransomware attacks have a long reach

Ransomware groups attack all industries and geographies, but large businesses and government entities are their favorite targets. In March 2021, REvil claimed responsibility for a $50 million ransom attack against Acer – revealing some stolen documents as proof of the breach. That ransom was the largest individual demand so far. JBS S.A., a Brazil-based meat conglomerate whose U.S. subsidiary accounts for more than one-fifth of the nation's meat supply, also paid a $11 million ransom to REvil this June after an attack took their IT systems offline, halting operations.

One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators

Colonial Pipeline Chief Executive Joseph Blount told a U.S. Senate committee that the attack occurred using a legacy Virtual Private Network (VPN) system that did not have multi-factor authentication (MFA) in place.

While the size of these ransom demands is shocking, the impact on operations is frequently the most devastating. For Ireland's Health Service Executive (HSE), the spread of a Conti ransomware variant triggered a full IT system shut down, impacting patient appointments and access to Electronic Health Records, with several systems still offline weeks later. While HSE did not pay a ransom to the responsible group (Wizard Spider), the total impact was still more than $118 million (€100m). In Finland, mental health provider Vastaamo was attacked by ransomware; the attacker blackmailed both Vastaamo as well as individual patients under threat of exposing therapy session notes. Vastaamo had to file for bankruptcy as a result of the attack. In April 2021, a compromised password was used by the DarkSide group to introduce malware that shut down the Colonial Pipeline until a $4.4 million ransom was paid. Very simply, the Darkside ransomware group infiltrated Colonial Pipeline through an inactive account that didn't use multifactor authentication. The only thing standing in the way was a weak and vulnerable password that was compromised for a virtual private network (VPN) account to get into the network. While the FBI's seizure of a Bitcoin wallet recovered a portion of this ransom, estimates suggest that DarkSide has netted over $90 million in Bitcoin from their combined efforts during the last two years.

Cyber-criminals often squeeze through holes in the supply chain. In July 2021, CISA and FBI responded to a series of ransomware attacks that leveraged an exploit in the Kaseya VSA (virtual system administration) software. The attack hit as many as 1,500 businesses in a month, beginning with around 60 direct customers, then trickling down to other customers. That trickle-down effect included a weeklong shutdown of 800 grocery stores in Sweden after their point-of-sale systems were breached. Criminals and opportunists are further pursuing victim companies and interested parties by sending out phishing emails that appear to be updates related to the ransomware attack.

Who is vulnerable to ransomware attacks?

Attackers will always look for the low-hanging fruit when they plan where to strike next. Like any criminal enterprise, ransomware outfits want the best return for the least effort and risk. The most vulnerable targets will be those industries that have large revenues (i.e. are able to make large ransom payments), but also may have complex environments that are difficult to fully secure. Oil and gas companies, other energy firms and financial services companies can all fall into that category.

Organizations in the following types of industries are often considered as “highly vulnerable”, given the intersection of high revenue potential combined with relatively lower security maturity and modernization, compared to industries such as Technology:

- Energy
- Healthcare
- Legal (law firms)
- Construction
- Trade organizations
- Education (school districts)
- Municipal governments (or smaller government agencies)

Ransomware attacks are likely to go after legacy environments with a low security maturity. “Low maturity” refers to firms without a continual and consistent investment in information security. These organizations may not have a dedicated security team and poor password and patch management practices. It is no surprise then that the most attractive targets for ransomware, across some of these industries, have also faced an increase in cyber insurance. In fact, some cyber insurance policies may require MFA to be implemented, or else their policy premiums could increase or even be denied.

Role of strong authentication

Strong authentication and modern MFA, such as using FIDO hardware security keys can play a very important role in mitigating ransomware risks. FIDO hardware security keys are much more secure, and provide much stronger phishing defense than legacy MFA such as SMS and mobile authentication.

Mitigating ransomware risks

There is no one size fits all guidance that can be given, and each organization needs to look at their existing infrastructure and future plans for development and growth and make a determination of steps that can be taken to enhance their security posture and mitigate ransomware threats. One thing is clear based on prior attacks, passwords or even legacy MFA approaches leave a lot of room for error as all of these authentication mechanisms are weak and highly vulnerable to phishing, man-in-the-middle attacks, and a host of other techniques meant to infiltrate systems.

Strong authentication and modern MFA, such as using FIDO hardware security keys, can play a very important role in mitigating ransomware risks. Malicious attackers look for vulnerabilities in the system and use a variety of methods to introduce malware into systems. One common technique is to use a compromised password to gain access to the network and then install the ransom malware, otherwise referred to as ransomware, on the systems.

As in the case of the Colonial Pipeline event, the malicious actors used a batch of leaked passwords on the dark web to log into a virtual private network (VPN) that didn’t use multifactor authentication in order to gain access to Colonial’s network. Once on the network, the attackers then installed the malware. Besides buying stolen passwords on the dark web, passwords can also be obtained through other means like credential phishing. Therefore putting phishing resistant modern multi-factor authentication in place can be a very effective way of stopping account takeovers in their tracks, which in turn prevents the attacker from installing the ransomware on-behalf-of the user. FIDO hardware security keys, as a form of modern MFA, is far more secure than legacy MFA such as SMS and mobile authentication, users can instantly get strong phishing defense that prevents these ransomware malware scams from taking hold.

Another common technique used to infect a system is through click-bait spam – attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access.

An important consideration, where possible, is to move data to the cloud combined with modern phishing resistant MFA for user authentication to significantly reduce the impact of ransomware threats. But the cloud isn't a panacea – poorly configured cloud systems are also susceptible to ransomware. When considering what cloud setup to configure, it should be noted that SaaS (software-as-a-service) solutions do not require patching, but PaaS (platform-as-a-service) systems will need regular patching, so patch policies and guidelines should be in place before full migration.

A secure organization working in the cloud typically has:

- Single-sign-on (SSO) system protecting all relying parties.
- Phishing-resistant MFA on all systems
- Management controls and separation of duties to ensure users do not have conflicting responsibilities.

It may not be possible to move all data to the cloud for a variety of reasons. An organization with on-premises infrastructures with local servers running the latest database versions with all of the appropriate authentication and access controls can also ensure the right level of security to mitigate against ransomware risks. However, on-premises environments can be complex to manage and keep up-to-date over time.

Planning ahead for a possible ransomware attack

The key is to be as proactive as possible, and learn from unfortunate events that have already occurred. Some key elements to effective strategies involve incorporating ransomware into your business continuity and IT disaster recovery plans. Assess your overall security strategy and general security hygiene and ensure users are employing strong authentication and a variety of best practices to protect sensitive data and systems.

Top mistakes organizations make when it comes to ransomware, and how to avoid them

The recommended overall approach is to be proactive and ensure that your organization has a sound and modern security strategy and posture. That will go a long way towards mitigating the threat of ransomware in the first place. However, if a ransomware attack does take place, the day a breach is discovered, there's a tendency to move immediately into "hair-on-fire" mode. Resist the temptation to panic! Here are a few reasonable steps to take to mitigate and then to manage a ransomware event, and avoid some common mistakes.

Pre-planning/mitigation:

- Incorporate ransomware into your business continuity and IT disaster recovery planning to ensure it is properly evaluated across the organization
- Ensure a sound security posture and enhance general security hygiene
- Make sure patch management is patching all systems properly – address any gaps starting with entry points
- Develop modern phishing resistant MFA capabilities and modernize your IAM systems if you have them so attackers don't login on your behalf and install malware
- Move data to the cloud if possible, and adopt migration plans that add new functionality to support the business
- Ensure you have backups that are protected and stored elsewhere. Protect the backups with strong authentication

Ransomware payments are staggering

In March 2021, REvil claimed responsibility for a $50 million ransom attack against Acer – revealing some stolen documents as proof of the breach. That ransom was the largest individual demand so far.

JBS S.A., a Brazil-based meat conglomerate whose U.S. subsidiary accounts for more than one-fifth of the nation's meat supply, also paid a $11 million ransom to REvil in June 2021 after an attack took their IT systems offline, halting operations.

- Consult with your insurance companies, which may have immediate action plans in place to guide you
- Educate employees about ransomware to lower risks

Attack day one:

- Engage your incident response team to stop the leakage and attack ensuring that the attack will not continue or spread. Additionally ensure any forensic data is secured for the investigation
- As part of the incident response plan, consult outside counsel, that have already been contracted with, who have helped other organizations with this scenario and can provide guidance on processes and entities to consider in responding to the attack
- Consult information from key compliance entities (ideally this research has already been done, reviewed and is in an easily accessible place. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), for example, has issued guidelines on what to be aware of when dealing with ransomware attackers

Some pitfalls to avoid:

- **Don't let payment be your first option.** First do adequate due diligence, and review CISA recommendations about ransomware. In some cases paying an attacker who is listed as a "sanctioned actor" by the government could put your company in jeopardy.
- **Don't get caught without a ransomware incident response plan.** This plan should be in place well before any attack and updated and tested regularly. The plan needs to be detailed enough so that during an attack, key decisions do not need to be made on the fly. Senior leadership needs to be engaged and responsible for the plan while experienced security and operational employees need to be given the authority to build a viable and actionable plan. The plan needs to be aligned and integrated with business continuity and disaster recovery plans and teams.
- **Using third-party vendors to manage an attack?** Ensure support level agreements are adequate to support day one activities and they are sanctioned by compliance entities.

Combating attacks – best practices to defend against ransomware

There is no silver bullet for ransomware, but a multi-pronged approach can help organizations respond to and recover from ransomware attacks.

- **Use phishing resistant authentication for any accounts.** Again and again, weak passwords, reused passwords, and SMS, One-Time Passwords (OTP), or push app-based multi-factor solutions enable ransomware and other attacks. Mutual TLS and WebAuthn/FIDO both protect against these weaknesses. YubiKeys are designed to work with these modern phishing resistant protocols as well as with legacy authentication like OTP.
- **Patch management.** It takes a lot of effort to actively patch everything in a timely manner across the enterprise. Access points should be patched as quickly as possible with automatic patch management being the goal. All systems should have a patch schedule with limited to no exceptions. And, any exceptions should be approved by the CISO and the highest business leaders who will accept the risk.

Ransomware can have a devastating impact on operations

For example, for Ireland's Health Service Executive (HSE), the spread of a Conti ransomware variant triggered a full IT system shut down, impacting patient appointments and access to Electronic Health Records, with several systems still offline weeks later.

In Finland, mental health provider Vastaamo was attacked by ransomware; the attacker blackmailed both Vastaamo as well as individual patients under threat of exposing therapy session notes. Vastaamo had to file for bankruptcy as a result of the attack.

- **Know what critical data you have, and why it's critical.** Follow data-centric security management strategies and validate the data classification list regularly with key business owners. Evaluate what systems hold, operate on, or transmit critical data. Evaluate your industry's data classification best practices to evaluate the data, and then properly align the data to the appropriate controls.
- **Don't forget to include other trusted systems, even if they don't handle critical data directly.** Supply chain attacks can be devastating when IT teams overlook or do not have visibility into systems that control access to or administer other systems. These centralized points of control, whether on-premise, in the cloud, or operated by third parties, require a very high security bar.
- **Make sure you have reliable backups by testing them.** Focus on critical data and restoring mission-critical business systems. That means not just making backups, but also testing restores, and understanding the permissions model of your backup system to ensure backups can't be deleted easily.
- **Make isolating critical systems a priority.** Most depth-focused infiltrations will compromise as much data and as many systems as possible before demanding a ransom. Zero Trust principles say everything should be isolated. But it's worth focusing on your most critical systems first after you gain confidence in your design and deployment. Include vulnerability management and patching strategies. Make sure to focus not just on access to a system, but access from a system. The easier it is to extract data from a system without being detected, the greater likelihood of pressure and impact from ransomware gangs.
- **Only keep the data you need.** Data retention policies and procedures need to be established and regularly reviewed. Consider keeping data not being actively used offline, or consider destroying it entirely. What isn't there can't be stolen and used against you, or those who trust you with their information.
- **Use experts to routinely test your systems.** Don't scope only "prove to me you can break this" style penetration tests. Use collaborative tabletop exercises where you assume that a "zero day" vulnerability exists in one or more of your systems, and determine if you could detect a breach, isolate it and recover quickly.
- **Avoid paying ransoms.** Paying is unlikely to return full data or access and only fuels further ransomware attacks. In some cases, it could be illegal because the entity receiving the payment may be sanctioned. Investing in the time and effort to properly prepare for an attack will put you in the best situation to limit its impact.

Top action items to form your ransomware risk mitigation plan

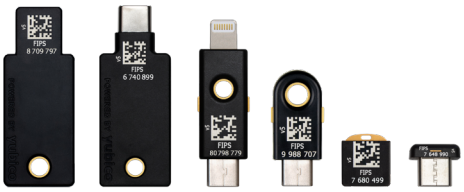
- Ensure a sound security posture and enhance general security hygiene
- Make sure patch management has no holes
- Develop modern phishing resistant MFA capabilities and modernize your IAM systems if you have them
- Move data to the cloud if possible, and adopt migration plans that add new functionality to support the business
- Ensure you have backups that are protected and stored elsewhere. Protect the backups with strong authentication.
- Educate employees about ransomware to lower risks.

YubiKeys and the YubiHSM

Modern authentication as critical components of your ransomware mitigation strategy

The YubiKey 5 Series

From left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano



The YubiKey 5 FIPS Series

From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS

YubiKey Bio Series - FIDO Edition

From left to right: YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition

The YubiHSM 2 Series

From left to right: YubiHSM 2 and YubiHSM 2 FIPS

Yubico's phishing-resistant hardware security solution – YubiKeys – supports a zero-trust approach: "Trust nothing, verify everything." YubiKeys are a strong user identity and device authentication solution, purpose-built for security and designed to stop phishing and other forms of account takeover in their tracks, delivering strong authentication at great scale.

Leveraging the FIDO2/WebAuthn and smart card authentication standards, YubiKeys work seamlessly across on-premises or cloud environments, do not rely on shared secrets between registered services, and require no cellular connectivity. In other words, YubiKeys can work offline, anytime, anywhere providing always-on security for the user and their identity. And with a FIPS 140-2 validated lineup that meets the most stringent Authenticator Assurance Level 3 (AAL3) requirements, it delivers strong security with an intuitive user experience for those organizations that need to meet the FIPS requirement.

YubiKeys can be delivered to users easily, whether at corporate or residential addresses, ensuring the remote or hybrid workforce is secured efficiently. And with security keys that offer easy user self-registration, and integrate with your existing security infrastructure, identity and access management platforms, and hundreds of other services right out-of-the-box, user identities can be protected in just minutes. With YubiKeys, an organization can experience strong security, a fast and easy user experience, and lower TCO.

In the trust "no one" and "no thing" world of zero trust, organizations need protection for credentials used by internal systems so that they cannot be used by attackers to gain privileged access. The YubiHSM 2 offers a powerful solution in this regard, as a FIPS 140-2 validated, Level 3 solution, or as a non-FIPS solution, both with the same capabilities. Both solutions ensure uncompromised cryptographic hardware security for applications, servers and computing devices at a fraction of the cost and size of traditional HSMs.

The future of ransomware

There's no endpoint on the timeline for ransomware – it's likely to be with us for the foreseeable future. Given its success so far, ransomware will continue to proliferate across industries and organizations of all sizes. Ransomware has multiple points of entry – it exploits vulnerabilities through a variety of techniques (for example, phishing). To respond to that, organizations have to tighten their security posture by shining light on any weak links among people, processes and technologies, as your overall security posture is only as strong as it's weakest link. Tightly coordinated patch management and data back processes need to be put in place. Additionally, strong authentication, moving data to the cloud and installing modern MFA are essential steps to thwarting the next ransomware attack. Having a solid incident response plan that is approved by the highest levels of the company and regularly exercised will prepare you to handle an attack that will come.

yubico

About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.