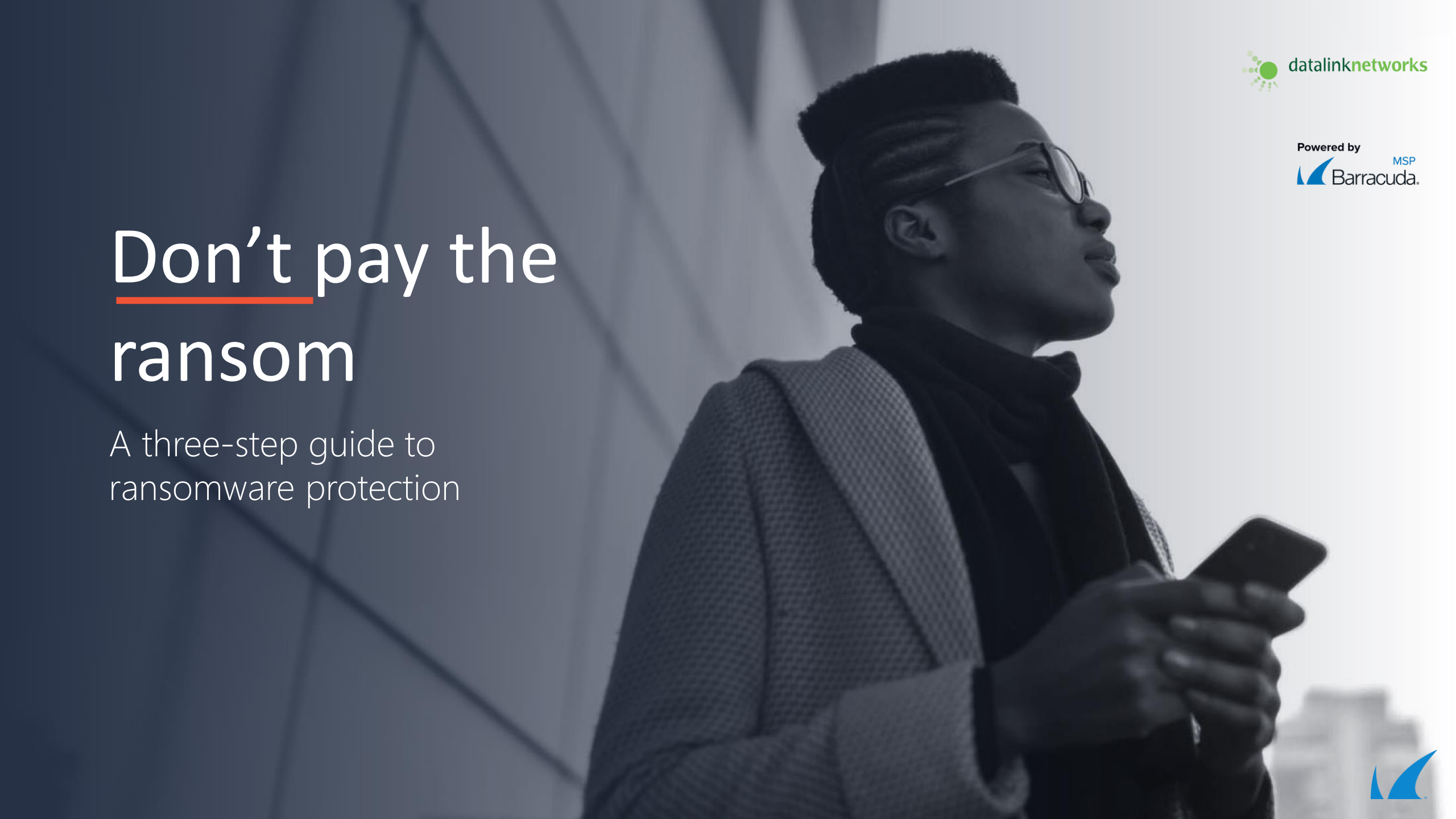


datalinknetworks

Powered by MSP Barracuda

Don’t pay the ransom

A three-step guide to ransomware protection

Table of contents

Ransomware and how it’s evolving

In simple terms, ransomware is malicious software that either encrypts your data or otherwise stops you from accessing your own systems. The criminals then demand a ransom in exchange for the decryption key, although, of course, there is no guarantee that the key will work, and you will get your data back. Many victims have paid up but not gotten their data back.

Compared to the straightforward WannaCry-style “compromise and encrypt” attacks of a few years ago, attackers are now taking a more sophisticated multi-vector approach. Attacks still often start with a spear-phishing email, but today’s ransomware attacks aren’t triggered immediately when the target clicks the malicious link.

Instead, cybercriminals use this step to steal the credentials of the victim. The credentials are then used to access the organization’s network and lurk there, evaluating assets, servers, databases, and the email platform. This surveillance can last for weeks or even months before they unleash their attack. This is exactly what happened in the ransomware attack against the Irish health service body, the HSE. The attackers claim they spent weeks inside the HSE’s network before launching the attack that encrypted and stole 700GB of patient data.

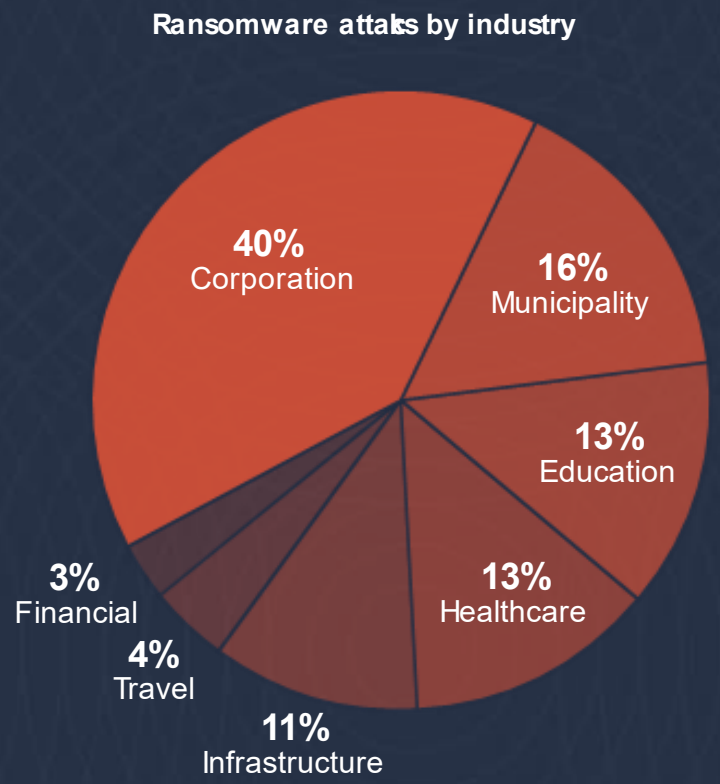
One reason why you are hearing more about ransomware now is that the barriers to entry have disappeared. The technology of crime is getting easier to use. Now you can buy a ransomware kit and choose your target. The gangs offer technical support in exchange for a percentage of the ransom. If that’s too daunting, the would-be criminal can hire cybercriminals to do the attack for them in a cybercrime-as-a-service arrangement. The increased value of cryptocurrency and the popularity of cyber insurance have also made ransomware attacks more profitable for cybercriminals, attracting highly organized gangs, and state-sponsored ransomware attacks have taken cyberwarfare to a new level.

Cybercriminals are raising the stakes

Ransomware attacks have escalated to the point that governments are now treating them as acts of terrorism. This is not an overreaction. These attacks have caused massive operational disruption to local governments, law enforcement, educational institutions, healthcare networks, critical infrastructure, and more. No industry, organization, or government entity is immune to these attacks.

According to recent research by Barracuda, attacks on corporations, such as infrastructure, travel, financial services, and other businesses, made up 57% of all ransomware attacks between August 2020 and July 2021, up from just 18% in our 2020 study. Infrastructure-related businesses account for 11% of all the attacks we studied.

Ransom amounts are also increasing dramatically, and now the average ransom ask per incident is over $10 million. Only 18% of the incidents analyzed by Barracuda between August 2020 and July 2021 had less than $10 million ransom asks, and 30% of the incidents had greater than $30 million ransom asks.

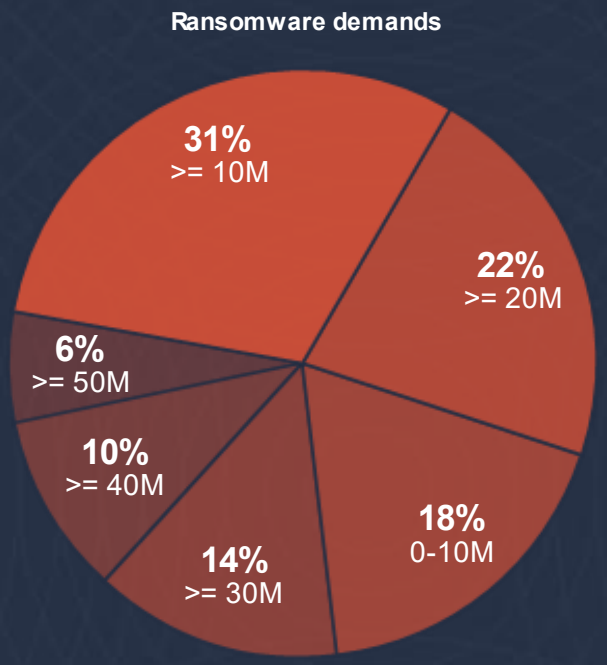


Ransomware is not a new threat, but it has evolved into a more destructive creature. Criminals have expanded their skillsets and refined their tactics to create a double extortion scheme. They base their ransom demands on research they perform ahead of the attack. They steal sensitive data from their victims and demand payment in exchange for a promise to not publish or sell the data to other criminals. Since criminals cannot be trusted, victims who pay are often contacted several months later and asked for another payment to keep the stolen data secret. Some ransomware criminals will accept payment but sell the data anyway.

There has never been any guarantee that paying a ransom would result in the recovery of all encrypted data. Victims should now understand that any data stolen in a ransomware attack is compromised forever. There is simply no reason to pay criminals for their crimes.

You should assume that there will be ransomware attacks against your company. If the attack is successful, you should have a plan to not pay the ransom.

Protecting your company from ransomware attacks is all about protecting your data. You can break this down into three focus areas: protecting your credentials, securing your web applications, and backing up your data. Let's take a closer look at each of these steps.



Step 1: Protect your credentials

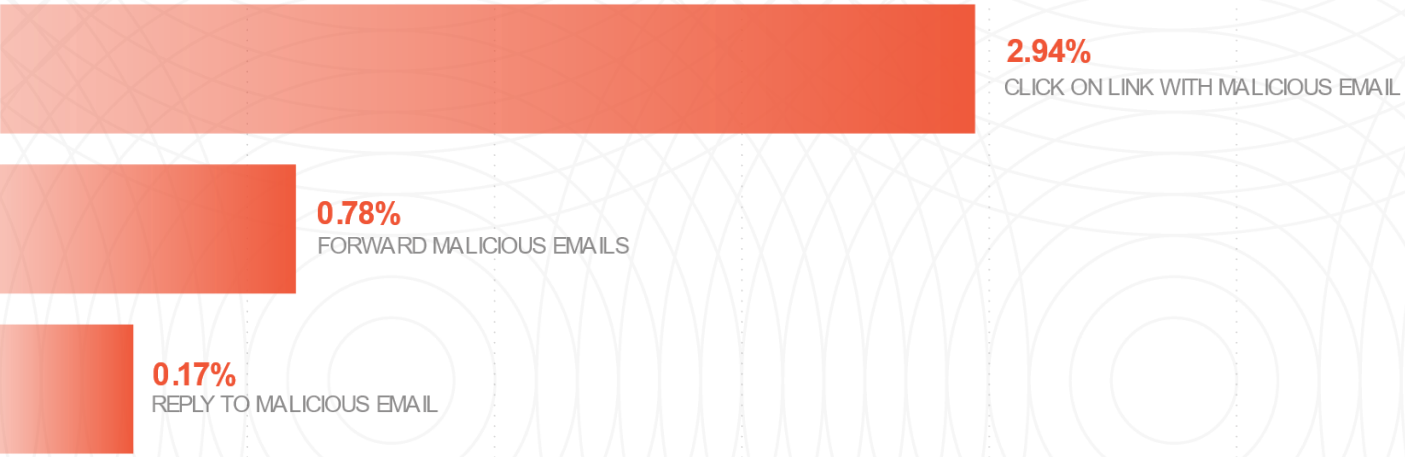
First of all, ransomware relies on either breaching email or otherwise securing credentials. With tens of thousands of usernames and passwords readily available online, this first step can be frighteningly easy. Attackers then use these stolen credentials to access your systems.

Because phishing is the primary attack vector for ransomware, you must maintain a culture of awareness around credential security. Develop a process to train users on email security and deploy anti-phishing technology that can identify and flag unusual activity. If the attacker cannot access credentials, it is much more difficult to escalate the attack from phishing to ransomware.

Phishing attacks work because people like to click on things. Hackers carefully tailor attacks to their victims by collecting publicly available personal information about them and playing to their sense of urgency to get a response. The attackers only need one person within your organization to click on the link or open an attachment. Recent Barracuda research showed that on average 3% of people who receive a phishing email will click on the link. Usually, the goal of the attack is to capture account credentials, allowing the hacker to move laterally across the company and ransom the entire organization.

Protecting credentials and access requires a two-pronged approach: first invest in detection and response tools and then focus on training your users.

Source: Threat Spotlight: Post-delivery email threats



Detection and response tools

Your email protection technology should focus not only on the detection of malicious payloads delivered through links or attachments, but also recognize when attacks use social engineering tactics designed to bypass filtering technology and trick users into action. It should look for malicious intent within an email, even when it does not include a malicious payload. Email security that uses machine learning algorithms can detect social engineering attacks with a higher degree of accuracy, looking for the smallest deviations from usual communication patterns.

Protecting your users' credentials can't be done without proper protection against account takeover. Multifactor authentication (MFA) remains a best practice and is something that should be adopted by every organization today. However, it's not a silver bullet, and it's not always enough. Attackers try to find ways to get around MFA either by tricking users into installing malware on their verification devices or giving fake apps access to their accounts. Organizations need to have account takeover protection in place that will quickly identify and alert about malicious activity such as suspicious log-ins or attacks launched from compromised accounts.

Protecting credentials and access requires a two-pronged approach: first invest in detection and response tools and then focus on training your users.

Training your users

As the last line of defense, it's crucial to train your employees to recognize and report attacks. Make security awareness training and phishing simulation part of your email security strategy. Historically, phishing attacks were associated with email only, but today cybercriminals will use other channels such as SMS and voice. Use phishing simulation for emails, voicemail, and SMS to train users to identify cyberattacks, test the effectiveness of your training, and evaluate the users most vulnerable to attacks.

Make sure cybersecurity training is not just part of induction day for new hires. It must be ongoing to keep staff up to date with evolving threats. For example, today's gangs use sophisticated social engineering that's hard to spot. Spear-phishing attacks target one individual, or part of one department, such as finance, with very tailored messages.

Crucially, your training needs to win staff trust and make them willing to raise an alarm, even if it's a mistake they caused by accident. Remedial training may be needed, but don't punish staff who come forward with an alert. Many attacks go unreported because staff fear they'll be blamed for clicking on a link or opening an attachment. Early warnings are extremely valuable and should be praised.

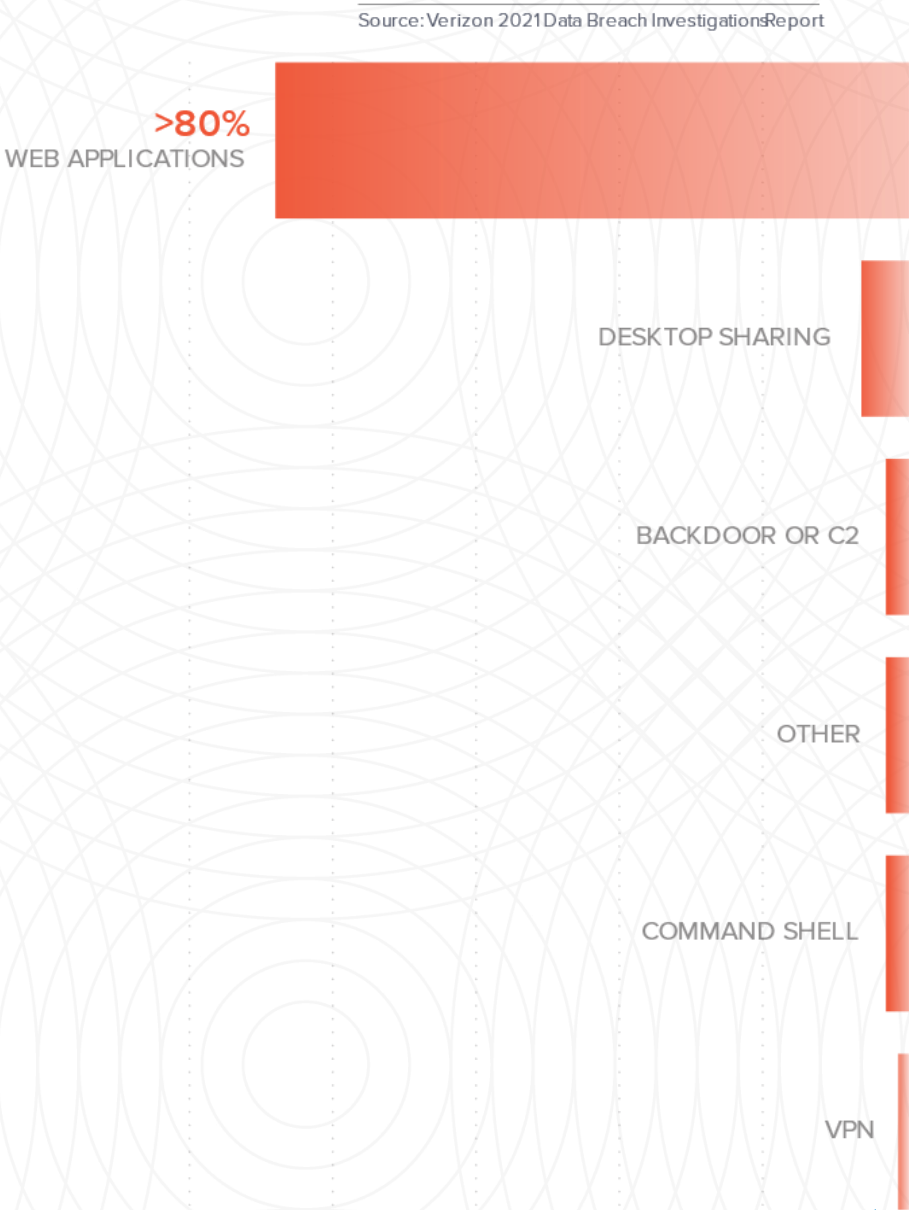
Step 2: Secure your web applications and access

The shift to remote work has pushed even more applications out of the data center and onto the internet. Sometimes the rush to keep business services functioning meant that security was overlooked, and cybercriminals are ready to exploit these vulnerabilities.

The Verizon 2021 Data Breach Investigations Report shows that for hacking, web applications are the biggest attack vector in use, accounting for more than 80 percent of all data breaches.

Online applications like file-sharing services, web forms, and e-commerce sites can be compromised by attackers. Web applications are attacked through the user interface or an API interface. Often these attacks involve credential stuffing, brute force attacks, or OWASP vulnerabilities. Once the application has been compromised, the attacker can introduce ransomware and other malware into the system. This can go on to move laterally to further infect your network as well as users of your application.

It's important to understand that protecting applications and access is as critical as email security in defending against ransomware and other malware. The Open Web Application Security Project (OWASP) works to raise public awareness around the most common application vulnerabilities that can be exploited in a ransomware attack.



One recent example is the REvil ransomware supply chain hack that came to light in July 2021. Vulnerabilities in a public-facing internet MSP application were exploited to spread ransomware to their customers. In this case, because the application had deep permissions, the ransomware was able to spread quite easily and have a significant impact before it was stopped. This type of hack could happen through any of your internet-facing applications — attackers hack into the application and then move laterally to wreak havoc. A similar scenario can occur if you leave your RDP systems open to the internet — even if you change the default port. Attackers use harvested credentials against such RDP systems to try to infect the entire network with ransomware through this unprotected attack vector.

Four attack vectors for web applications

Applications are now a leading target for ransomware, so there are four attack vectors you need to protect: application access, web application vulnerabilities, infrastructure access, and lateral movement.

1. Application Access

To identify if application access is a problem that could be compromised for your organization, there are a few key questions you need to answer.

- **Do your remote or contract workers use unmanaged devices or Bring Your Own Device (BYOD)?** Mobile devices are the most common example. An unmanaged or BYOD device can be compromised and then used to extract credentials or further attack your application.
- **Do you have visibility into all the users and devices on the network?** For example, you need to know who is connecting to your guest network and if it is properly segmented.
- **Do you have an audit trail for who is accessing what when?** You should be able to look back and see who is accessing your applications, how they are accessing them, and if they have the right permissions.

If a device that is not supposed to be allowed on the network is connected to your network and someone has set up some hacking tools on it, that is a serious problem. And if you don't have visibility into all of this, it becomes a challenge to identify who is accessing what and what the vulnerability is, so you won't be able to close the vulnerable surface or block the attacker's access.

2. Web application vulnerabilities

Web application vulnerabilities are the next attack vector you need to assess to determine how secure your applications really are.

Consider the following questions:

- How secure is your website? When was it last updated?
- Do you have forms on your site? How do you prevent attacks through forms?
- Do you accept file uploads on your website? How do you secure against malware?

Turning on HTTPS is not enough to secure your site. It simply means an attacker cannot eavesdrop on someone logging into your site to steal their credentials. Cybercriminals can still perform a brute force attack within that HTTPs frame to try to figure out correct logins for your site.

Having CAPTCHA or reCAPTCHA in front of login forms on your site is also insufficient because it is easy for people to automate and bypass these services.

Rate-limiting logins or IPs is another security measure that hackers are easily able to get around using low-and-slow attacks and various automations systems.

If you accept file uploads, that's another problem you need to address. It's fairly common for attackers to attempt to breach a website by uploading either a virus or ransomware malware.

3. Infrastructure access

Since the beginning of the COVID-19 pandemic, many organizations have used VPN for providing access to internally hosted applications. It happens when there are no SaaS replacements for some self-hosted applications. Providing VPN access from home is the only way to keep the business running. Without proper identity and access practice, though, this approach is a “ticking time bomb waiting to explode.” Many already stolen credentials may share usernames and passwords used for accessing the infrastructure, therefore creating a real risk that could expose your network, applications, and data.

3. Lateral movements

After compromising your application or infrastructure with stolen credentials, attackers will try to go deeper into the network and perform further attacks that way, so that is the fourth attack vector you need to address. Ask the following questions:

- How secure is your website? When was it last updated?
- Do you have forms on your site? How do you prevent attacks through forms?
- Do you accept file uploads on your website? How do you secure against malware?

Setting proper segmentation for your network takes a lot of time and effort, and it’s easy to find reasons to open up two segments and allow access from one segment to another. Ultimately, that leads to access being open in ways you did not want.

Multifactor authentication adds another important layer of protection to help stop attackers from gaining access to the network.

How a ransomware attack exploits application vulnerabilities

Here is another scenario: An imaginary yet realistic series of steps that an attacker might execute to exploit poor application security to create a successful ransomware attack. The attack is going to attempt a common coupon scam by riding on the reemerging wave of browser coupon plugins.

Step 1

The attacker creates a website that mimics a legitimate coupon website. The attacker impersonates a popular coupon site, which is relatively straightforward using domain impersonation and automated web scraping. Let's call this fake site Website X.

Step 2

The attacker probes for one or more of the OWASP top 10 vulnerabilities to steal credentials from a legitimate but poorly protected company website, which we'll call Website Y. Vulnerabilities like broken authentication and sensitive data exposure allow the hacker to harvest user credentials and other sensitive information from the Website Y.

Step 3

The attacker uses the stolen credentials to begin a credential stuffing attack against a legitimate e-commerce website, which we'll designate Website Z. This is an automated attack that can be run slowly over multiple weeks. This attack attempts to match stolen credentials to real accounts at these sites.

Step 4

If the attack finds a match and the hacker can log in to a victim's account, the next step is to use that account to post reviews of popular products on Website Z. A common example in this step is "This product is great! Save 50% off this price with this coupon by clicking here." The link to the coupon takes the visitor to the Website X, the fake website from step one.

Step 5

The potential victims log onto Website Z and proceed to click through the product review, following the link to Website X, unaware that they have been taken to a scam site unless they look extremely carefully at the domain name, URL, site certificate, and other details. Victims who trust the site then provide their contact information in exchange for the coupon. The attacker now has the address of someone expecting an email from that website. The attacker is gaining the victim's trust, and the victim has lowered their guard.

Step 6

The victim receives a personalized email about the product and the coupon, with an attachment that the victim is told to install for the coupon to work. This attachment may be an executable or a browser extension that uses JavaScript to carry out the attack. Because this email is thoroughly customized and is expected by the recipient, it is likely to be allowed through traditional email defenses. The victim's operating system prompts them not to install untrusted executables, but at this point the victim likely has complete trust in the attacker and clicks through.

Step 7

The victim installs the attachment, and the ransomware attack is launched. Several types of attacks can be launched once an executable is installed, for example infecting the master boot record, encrypting the file system table, and even preventing the operating system from booting. Shortly after that, the demand for payment will be delivered to the victim. The attacker will usually try to expand this attack and harvest more credentials and any other data that can be found on the network. When this is completed, the ransomware will encrypt the network data.

In this example, the ransomware only succeeds because application security vulnerabilities on multiple websites allowed the convincing scenario to be constructed — the web scraping of a legitimate site in step one, the credentials stolen in step two, the credential stuffing in step three, the comment spam and malicious URL in steps four and five, and the installation of the executable in step seven. Proper application security at any of these steps could have stopped this attack.

How to secure your applications and access

Secure your network

Prevent ransomware from spreading within your network with network segmentation and intrusion prevention. Look for a next-generation firewall solution that:

- How secure is your website? When was it last updated?
- Do you have forms on your site? How do you prevent attacks through forms?
- Do you accept file uploads on your website? How do you secure against malware?

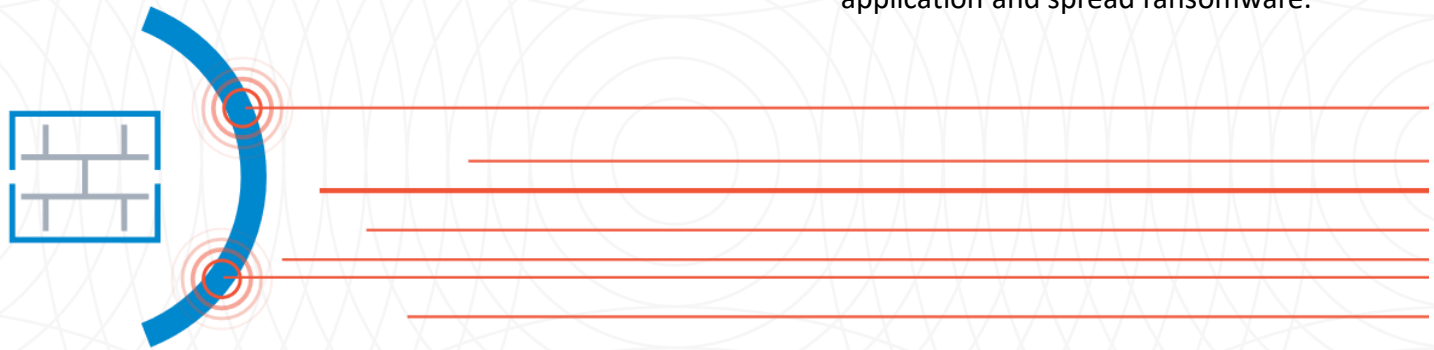
Secure your application access

You should secure your application access with a Zero Trust Network Access (ZTNA) solution that provides secure access to applications and workloads from any device and any location.

Look for a solution that:

- Continuously verifies that only the right person with the right device can access company resources
- Enforces role-based and attribute-based access control to provide least privilege access

By blocking unauthorized access, ZTNA stops attackers trying to breach your application and spread ransomware.



Secure your web applications

One of the best ways to deploy application security is with a web application firewall (WAF) to protect your software, your users, and their data wherever they may be. That will stop bot attacks, denial of service attacks, and give you far greater insight into what is going on. Look for a solution that has the following features:

Easy to deploy and customize to your environment

A WAF cannot fully protect you if you are not able to configure it for your environment.

Scalable

Business growth, digital transformation, and other factors can increase the demand on your applications and websites. Your WAF should be able to grow with your business as needed.

Comprehensive protection against advanced threats

OWASP Top Ten protection and application-layer DDoS protection are the table stakes one should expect from a good WAF. For complete protection, look for a solution that defends against zero-day attacks, credential stuffing, data leakage, malicious bots, and more.

Easy to deploy and customize to your environment

A WAF cannot fully protect you if you are not able to configure it for your environment.

Continuous threat intelligence

Business growth, digital transformation, and other factors can increase the demand on your applications and websites. Your WAF should be able to grow with your business as needed.

By blocking common web application vulnerabilities and zero-day threats, a good web application firewall stops ransomware from getting a foothold in your systems.

Step 3: Back up your data

ny serious ransomware protection strategy should start with thinking about backup and disaster recovery. The trouble is criminals know this, too.

Backup solutions are a focus for attackers during the ‘lurking’ period when they are exploring the network. The backup admin console is particularly important to them because it gives them access to backup schedules, configuration, retention policies, and the ability to start deleting things.

Attackers also target backup storage itself, hoping to delete your primary backup server and any secondary disaster recovery backup copies you maintain. Once they capture Active Directory passwords so that no one can log in to their accounts, that's when they can pull the trigger. They're in control.

There is also still an all-too-common misconception that because your data is in the cloud it can't be affected by ransomware. That simply isn't true.

For example, a child browsing the web on their school tablet or laptop at home can easily be tricked into clicking on a malicious link by accident. If that device is connected and synced to OneDrive as part of the school's Office 365 account, a ransomware file can be automatically uploaded to OneDrive and encrypt the school's files and data held in the Microsoft cloud.

We've also seen examples where SharePoint, Exchange, and other data sources have been hit. And if network drives are mapped to document libraries in Office 365 using the 'open with Explorer' feature, the ransomware can also scan for and infect files on connected drives.

Consider disaster recovery as a crucial, strategic part of your infrastructure.

Test it regularly and realistically — that means doing an actual restore, not just checking it's running.

Even cloud and SaaS data can be encrypted with ransomware. Microsoft guarantees the availability of the service, but they recommend that you back up your data using a third-party backup solution. Your data may be saved in Microsoft Office 365, but Office 365 is not designed to recover entire instances as may be required after a ransomware attack.

So, you need to properly defend and isolate backup data. Think about how often systems need to be mirrored and how fast you can rebuild systems from those images.

You need to make sure that restoring systems from backup versions is actually possible in a reasonable timeframe and with sufficiently up-to-date information. That means you have to take control and actually do it. You can't just check logs to see if data is being replicated often enough and accurately enough.

You need to run real drills to prove that systems work. You might choose one department, or even just one application, rather than bringing everything to a stop. But it is vital that you are fully confident in bringing back systems in a timely way.

This is your backstop defense. Even if everything else fails, if you have genuinely up-to-date and secure backup then the criminals can't stop you.

Consider disaster recovery as a crucial, strategic part of your infrastructure. Test it regularly and realistically — that means doing an actual restore, not just checking its running.

What you need in your backup solution

To mitigate risks associated with ransomware, you need a comprehensive backup solution that provides the following:

Immutable storage

Even if the attacker gains access to your backups, he can't modify or delete that data.

Air-gapped cloud

Maintain a copy of your backup in a secure cloud that resides on an isolated network.

Multifactor authentication (MFA)

Secure the accounts and credentials used to access the backup.

Redundancy

Replicate your on-premises and cloud backups to another location.

Role-based access control

Follow the principle of least privilege for all users who have access to the backup system.

Conclusion

Your company might have cyber insurance or other resources to pay a ransom, but it's extremely dangerous to assume that paying a ransom will get your data restored. There is no guarantee hackers will unencrypt data when a ransom payment is made, and even if they do, the latest research shows that 80% of organizations that paid a ransom were attacked again.

Even if you've done everything outlined above, you're still going to be attacked. Even with the best protection in place, it is common sense to prepare for the worst. Criminals have millions to invest in breaking into your systems. The only sensible way to prepare is to assume that one day they will get in.

You need to think about what happens on that day. You need a plan not to pay the ransom.

- Who is in your ransomware response team?
- Who gets called if something happens over a weekend or holiday?
- Who's in charge?
- When do you tell customers and suppliers?
- Who is providing legal advice?
- Do you need to tell a regulator or the police?
- Do you need a PR person involved from the very start?

It's just like a fire drill — the time to practice is not when the office is on fire. But current and most likely attacks change over time, so your strategy and defense tactics will need regular updating. Download our ransomware checklist to help get your plan started.

Be prepared to respond to an attack

You need to think about what happens the moment an attack is identified and what happens if that attack becomes a breach. Can it be contained or restricted to one part of your infrastructure by stopping network traffic? Do you need to take systems offline temporarily? If so, who is taking responsibility for this?

Speed is absolutely essential here. Focused speed. You don't want to be waiting for your CTO to return a call. Everyone needs to know what to do right now.

If this happens fast enough, you may even be able to stop the encryption from happening. You also need a plan to rapidly check across your systems to get a definitive view of what is going on.

Modern attackers tend to use more than one attack type simultaneously. You might be busy dealing with a denial-of-service attack while a ransomware attack is aimed elsewhere. Once you understand what has happened, and where, you can start thinking about what you need to do to eradicate the malware and get systems back online.

Once you've restored systems and data, whether from backup or by isolating the attack in time, and checked for corrupt or missing data, it is time to start the forensics.

Evaluate how your response worked against a real attack. Analyze what worked well, what worked only because you got lucky, and what came up wanting. Consider how to improve and accelerate your response next time.

With the right systems in place, you will have a wealth of forensic data to consider. You may even have enough for police to start investigating. Whatever data you have, you should take the time to debrief the response team and think about the lessons learned.

Once again, this is not just about technology; it's also about people and processes. Do you need to look again at staff training? Was your response team working well, or does it need to be bolstered?

Stay informed

Today's defense strategies need to be active, not just reactive. You need the greatest possible transparency into your security systems. You need to watch what is happening, when and how often. You need to pay attention to your peers — ransomware attackers often target a specific vertical market or geography. You should also stay up to date on the latest threats, trends, and industry news through resources such as the Barracuda blog.

Data is crucial to a successful security strategy — your organization's stance or profile is likely to change over time. You need to be ready and informed to make that change when necessary. Security-as-a-service can help remove some of the drudge work of keeping up with developments especially when today's cybersecurity landscape is changing faster than ever.

For some companies with a very active stance, or a high-risk profile, this might mean having full-time staff doing intelligence work to get an early warning of possible attacks.

But for most organizations this is more than what's required. Choose the right partner and get the basics in place. Real attackers — unlike what we see in movies and TV — are not evil geniuses who love picking apart the most elaborate security systems. For the most part, they are looking for an easy payday from someone who's been lax and not paying attention or not investing in the right security.

Taking those three steps — protecting your credentials, securing your web applications and access, and backing up your data — will not guarantee that you won't be attacked by ransomware. But it will guarantee that you never have to pay a ransom to get your data back.

About Datalink Networks

Datalink Networks is a managed service and IT solutions provider that serves clients of all industries and sizes nationwide. Our team provides IT services and solutions in the following main categories: Managed Services, Cybersecurity, Microsoft Services, Communication & Collaboration, Data Center, and Networking Services. Contact us today to schedule your free IT consultation with our team. Visit www.datalinknetworks.net for additional information.

About Barracuda MSP

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP management platforms. Barracuda MSP's partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business. Visit barracudamsp.com for additional information.