Ransomware: The Cyberthreat that Just Won't Die

Thirty years on from the world's first cyber ransomware attack, cybercriminals continue holding organizations hostage, maliciously encrypting their files and demanding hefty ransoms for the safe return of the data. Indeed, while headlines come and go, ransomware remains stronger than ever, with six- and seven-figure ransom demands now commonplace.

This paper explores the reasons behind ransomware's longevity, including the factors that have enabled it to get faster, smarter, and deadlier over the years, and what we must learn from this history if we are to minimize our risk of attack in the future.

It also dives into three new areas where the dirty tentacles of ransomware are starting to take hold, enabled by recent changes in technology and society. Finally, it looks the technologies and behaviors organizations should adopt to ensure they have the best possible defense against ransomware and showcases how Sophos can help.

A Sophos white paper December 2019

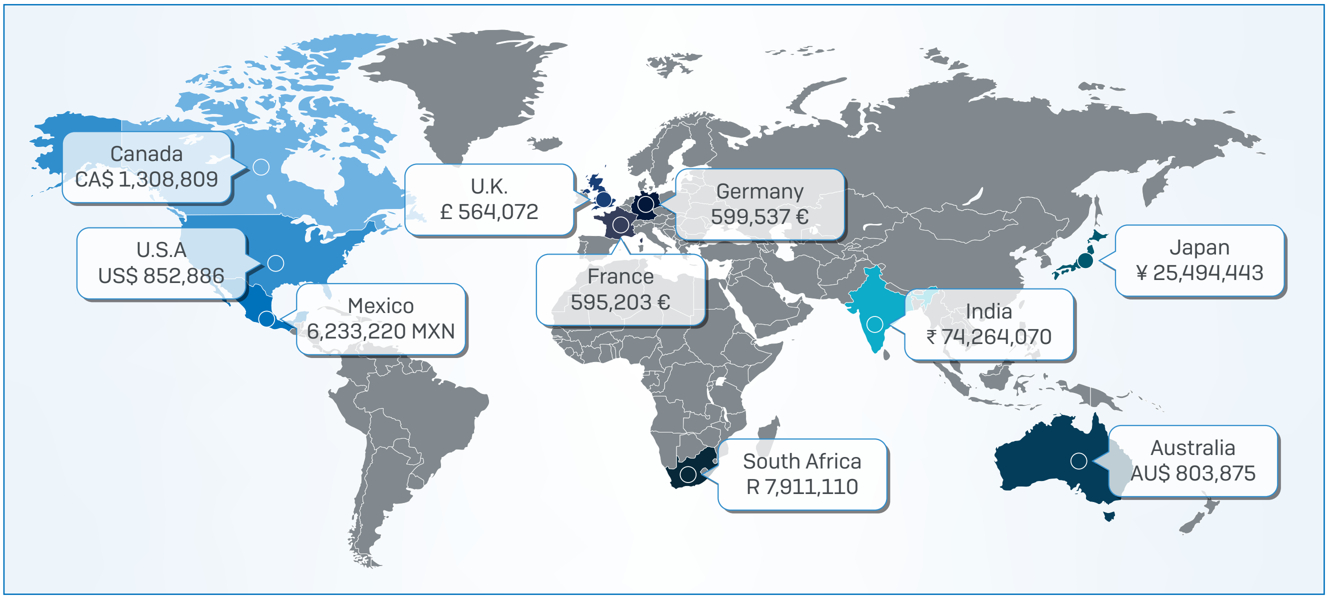
Contents

The Impact of Ransomware

Ransomware is a very real threat for organizations across the world. A recent independent survey of 3,100 IT managers in 12 countries commissioned by Sophos revealed that 21% of organizations were hit by ransomware in 2018. What's more, three in 10 (30%) organizations that fell victim to a cyberattack experienced ransomware.

The financial impact of ransomware is huge. When you add together the full costs of remediation, including downtime, people time, device cost, network cost, lost opportunities, and ransom paid, the final sums per victim are eye-watering.

Cost to rectify a ransomware attack



Source: The State of Endpoint Security Today, Sophos, 2018

Given the extent of ransomware's reach and the high cost of an attack, the natural question is: why is it so persistent? Why, despite all our advances in technology, can't we kill it off? Why is it able to have such a devastating impact?

To answer these questions, we need to understand how we have arrived at today's situation. This requires us to go back in time and see how – and crucially, why – ransomware has evolved over the years.

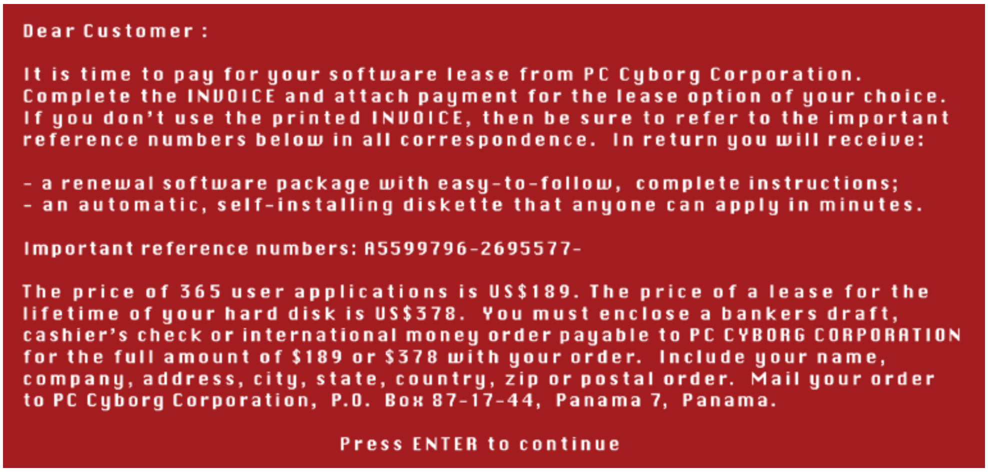
The Evolution of Ransomware

The Birth of Ransomware

Ransomware is not new. In fact, the first cyber ransomware attack was released in December of 1989. Dr. Joseph V. Popp mailed out 20,000 floppy disks infected with the AIDS Information Trojan. The program purported to be an expert system to advise you about your risk of contracting HIV and AIDS, but after you'd run it 90 times, it scrambled your hard disk.

Those of us around at the time will remember that back in 1989 everyone switched off their computer at the end of the day, so the 90th reboot generally took place four to five months after first running the program. The user was then presented with a ransom note demanding US$189 – for one year's use of the program – or $378 for lifetime use. Payment was via a Bankers Draft to a company in Panama.

Ransomware demand note in AIDS Information Trojan



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence.  In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order.  Include your name,
company, address, city, state, country, zip or postal order.  Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                         Press ENTER to continue
```

Unfortunately for Dr. Popp, the cypher used was trivial to crack and free decryption tools quickly became available. Plus, the idea of sending payment via a Bankers Draft to Panama was a non-starter. As a result, the enterprise failed to generate any revenue, and instead landed him with a court appearance.

There are three main hurdles that cybercriminals need to overcome to effect a successful ransomware attack: getting the ransomware onto the victim's devices; encrypting and decrypting the files; and receiving the payment.

While Dr. Popp had identified an effective, although not really scalable, approach to get his threat onto the victims' devices (he had to write those 20,000 floppy discs manually), he fell down with the encryption and payment parts of the process.

☑ Installing the ransomare

☒ Encrypting and decrypting the files

☒ Receiving payment

Exploiting opportunities

The AIDS Information Trojan attack did have one hallmark of success: it took advantage of a wider environmental opportunity, namely the widespread concern around HIV/AIDS at that time. Since then, cybercriminals have continued to take advantage of developments in both technology and wider society to evolve and finesse their ransomware attacks, including:

- **The rise of free email services like AOL and Yahoo**. These services enabled hackers to create unlimited, untraceable email addresses for the first time, leading to the start of large scale spam campaigns used to spread ransomware.
- **The move from dial-up to ADSL connections**, which enabled more people to use the internet, and for longer periods of time, gave the crooks a larger target area for their attacks.
- **Geo-targeting abilities** allowed cybercriminals to focus their attacks on a particular country/ region. Geo-targeting increased success rates by enabling attackers to exploit local hot topics in email attacks while also customizing the language for their audience.
- **Prepaid credit cards** gave the crooks an accessible, anonymous way for people to pay ransom demands.
- **The availability of cryptocurrencies**, particularly Bitcoin, gave criminals another reliable and accessible way to get payments.

As a result of exploiting these (and other) opportunities, by 2010 cybercriminals had solved the three main challenges facing ransomware, enabling it to become a viable commercial business.

☑ Installing the ransomare

☒ Encrypting and decrypting the files

☒ Receiving payment

Playing cat and mouse

Once ransomware became mainstream, the cybercriminals focused their efforts on refining and enhancing their attacks in order to increase revenue. This included:

- **Branding**. Savvy cybercriminals realized that people would only pay up if there was a high chance their data would be restored. As a result, a reliable decryption tool was essential for ransomware to be an ongoing revenue generator. At the same time, not all decryption tools were equal. Ransomware actors with an effective tool didn't want to be tainted by association with less effective ones. This led them to use a marketing technique that's been common practice in the commercial world for decades: branding. A quick internet search on a ransomware name informs the victim of the likelihood of getting their data back if they pay up.
- **Ransomware-as-a-service**, where ransomware experts took advantage of the business opportunity to provide ransomware 'packages' to fellow crooks who lacked encryption knowledge and payment systems, but who were good at distributing threats. The service included the malware and backend payment through a central site, in return for 30% of revenue received.

- **High impact ransomware**, enabling ransomware actors to improve their return on investment (ROI) by targeting a small number of victims with crippling attacks. Targeted attacks required less effort, and had less exposure, while by increasing the impact of their attack they also increased the victim's propensity to pay.

At the same time, the cybersecurity industry was busy evolving its defensive technologies, identifying how to spot and block ransomware attacks to stay ahead of the cybercriminals.

Ransomware evolved: Ryuk

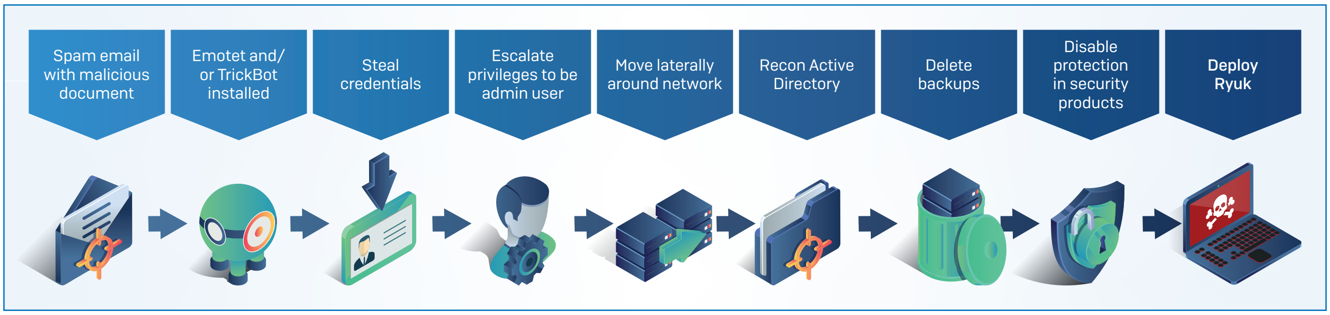
Ryuk is arguably the most evolved form of ransomware around today, named after a character in the manga series Death Note. The actors behind Ryuk typically target organizations that cannot withstand any downtime, such as newspapers, municipalities, and utilities, to increase the likelihood of payment, and demand six- and seven-figure ransom payments.

To get around anti-ransomware technologies, these active adversaries combine advanced attack techniques with interactive, hands-on hacking. Ryuk attacks often start with a spam email containing a malicious attachment. The attachment triggers an Emotet or TrickBot attack, which enables the cybercriminals to get on the victim's network.

Once inside the network, the hackers steal credentials and escalate their privileges until they create a new admin user. With their escalated admin privileges in place, the hackers move laterally around the network using multiple techniques including Remote Desktop Protocol (RDP), survey the Active Directory, and delete any backups.

With the victim's safety net out of the way, they attempt to disable cybersecurity products before finally releasing the Ryuk ransomware, encrypting files and demanding huge ransom payments.

Typical Ryuk ransomware attack chain


Spam email with malicious document
Emotet and/ or TrickBot installed
Steal credentials
Escalate privileges to be admin user
Move laterally around network
Recon Active Directory
Delete backups
Disable protection in security products
Deploy Ryuk

What's next for ransomware?

The big lesson we can take from looking at the history of ransomware is **that cybercriminals will continue to exploit changes in technology and society to inflict their ransomware attacks**. In essence, ransomware is going to keep evolving. With that in mind, let's explore three new areas where the dirty tentacles of ransomware are starting to reach, driven by the opportunities presented by technology advances.

Public cloud ransomware

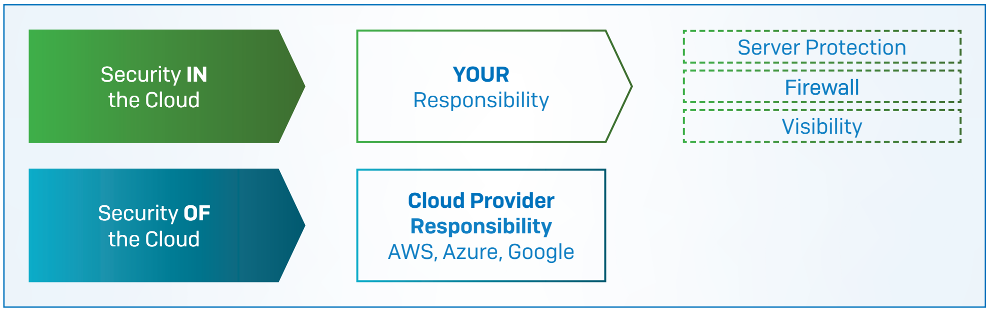
First on the list is public cloud ransomware, by which we mean ransomware that targets and encrypts data stored in public cloud services like Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP). Public cloud adoption is growing, with organizations using it in multiple ways.

For many, it is simply a **replacement for the physical on-premises servers** they used to store data. Whereas previously employees would save files to the server at the back of the office, now they save them to servers in the cloud. Another popular use case is for **running web applications**, such as running a website or providing web-based services. The third main use case for the public cloud is **software development**. Software engineers are increasingly writing code on public cloud servers as spinning up a server in the cloud is quicker and easier than building physical environments.

The public cloud offers lots of advantages. When it comes to security, however, there is a lot of uncertainty and confusion around responsibilities. Many people are unaware of which parts of security ownership sit with the public cloud providers, and which parts sit with the customer. This uncertainty leads to gaps in protection, presenting ransomware actors with a treasure trove of valuable data that's ripe for encryption.

The allure of the public cloud doesn't stop there. The rapid increase in volume and value of data stored in the cloud gives cybercriminals a greater target to go after. Plus, weak configuration and open public access to cloud resources (be that storage buckets, databases, user accounts, etc.) make it easier for criminals to breach open databases.

The first step to protecting yourself from public cloud ransomware is understanding the public cloud shared responsibility model. In short, this means that you are responsible for securing everything you put in the cloud, including all your data, as well as access to the public cloud. The public cloud providers are responsible for the security of the cloud. This includes the security of the physical facility where the data centers are located.



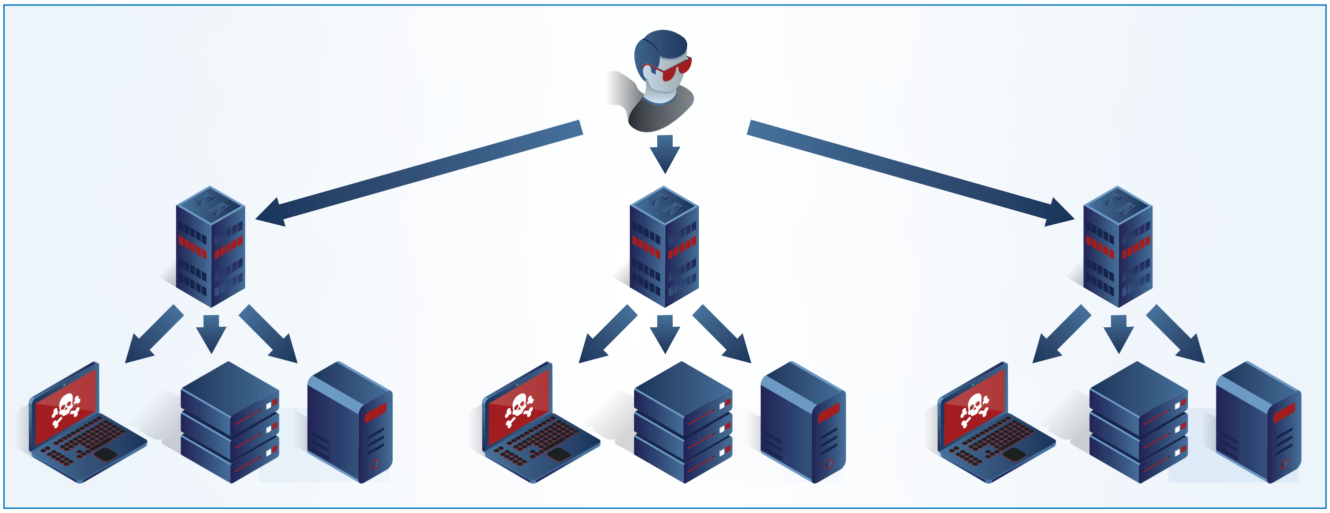
You should apply the same basic principles to your cloud-based data as your on-premises data. So just as you use server protection and a firewall on premises, so you should use server protection and a firewall to secure data in the public cloud. Plus, you need to know what you've got in the public cloud, so you can make sure it's secure.

Service provider attacks

The second area where we expect to see growth in ransomware is service provider attacks. As technology and threats become ever more complex, companies are increasingly outsourcing their IT to specialist managed service providers (MSPs). These MSPs manage all aspects of IT for their customers, from printers to security. To do this, they need to have direct access to their customers' networks.

Traditionally, ransomware actors target a single organization at a time. One victim, one ransom. However, ever on the alert for opportunities to increase their ROI, cybercriminals have realized that targeting MSPs enables them to hold multiple organizations hostage with a single attack. One attack, many ransoms.

Service provider attack model



The answer here is not to keep your security in-house. MSPs who specialize in security offer a very high level of expertise that is hard to replicate for many businesses. Instead, make **security one of your selection criteria** when choosing your MSP. Ask them about the security products and practices they use within their own organization. A good MSP will be happy to share.

And **ask yourself about your priorities**. Is protection #1? Cost is of course a consideration for pretty much every organization, but don't compromise long term protection for short term cost savings. As we saw at the start, the cost of dealing with a ransomware attack outweighs many other expenses.

Encryption-free attacks

Ransomware has now come full circle. The ability to encrypt files was one of the core capabilities needed to make ransomware a viable cybercrime. However, cybercriminals no longer need to encrypt your files to hold you hostage. Why? Because they'll think you'll pay up just to stop your data going public.

There are two types of data that are particular targets for this type of attack. The first is personal data, information on an individual, sometimes called personally identifiable information (PII). Over recent years legislation to protect personal data has strengthened significantly, with pan-national (such as GDPR), national, regional, and industry-specific laws in place to protect data.

This legislation comes with very stiff financial penalties for anyone who suffers a relevant data breach – the maximum fine under the GDPR is up to 4% of annual global turnover or €20 million, whichever is greater – for organizations that infringe its requirements. Cybercriminals are able to hold organizations hostage with the threat of releasing personal information, thereby opening up the victim to the consequences of a data breach.

In October 2019 the City of Johannesburg in South Africa suffered an encryption-free ransomware attack. They were attacked by a group calling itself the Shadow Kill Hackers. According to a note shared on Twitter, they didn't encrypt data. Instead they stole it and threatened to upload it to the internet if the City didn't pay up. The note read:

> *All your servers and data have been hacked. We have dozens of back doors inside your city. We have control of everything in your city. We also compromised all passwords and sensitive data such as finance and personal population information.*

The group reportedly demanded a payment of four Bitcoins (£30,347), although at the time of writing the ransom does not appear to have been paid.

The other type of data particularly at risk from these attacks is intellectual property, or IP. This is often the source of a business' success – whether it be a secret recipe, a proprietary technology, or unique data. If that IP got into the public arena it could mean the death knell for the business.

The most public example of this type of ransomware attack was the one experienced by the band Radiohead in mid-2019. Frontman Thom Yorke's archive was hacked, and the crooks stole 18 hours of unheard music from around the time of the release of the 1997 album OK Computer. The extortionist threatened to make the music public unless the band paid a ransom of US$150,000 – a request that Radiohead eschewed, preferring instead to make the music public themselves in return for an £18 (around $23) donation to aid the climate advocacy group Extinction Rebellion.

Stopping encryption-free attacks means stopping the hackers getting hold of your data. It requires many of the same technologies and behaviors that you need for encrypting ransomware, which is a nice segue into our next section.

How to defend against ransomware

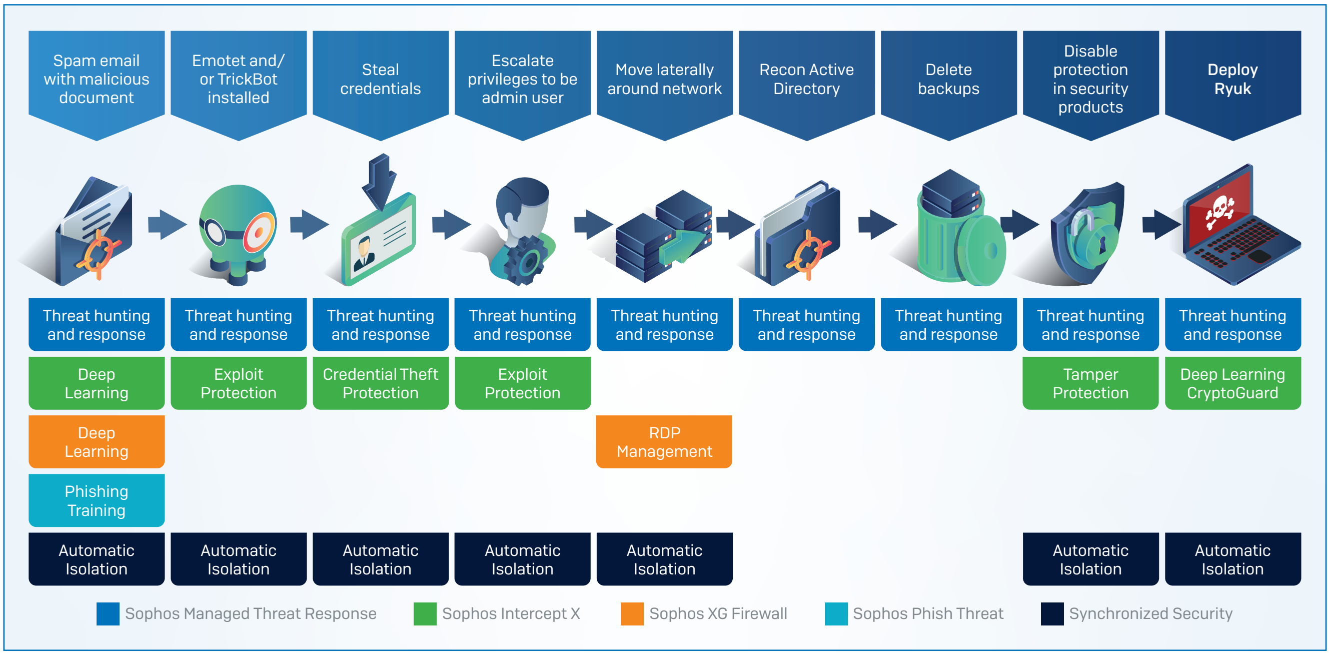
Ransomware has evolved into a highly advanced, highly complex threat – and it's only going to evolve further. With that in mind, how can you minimize your risk of being affected by ransomware? The answer is that you need to make it as hard as possible for ransomware actors to deploy their complex attacks, and to take advantages of opportunities presented by changes in technology and society. To do this we recommend:

- Using the best cybersecurity technology, with a focus on disrupting the whole attack chain not just a single piece of malware.
- Applying best security practices at all times.
- Educating your staff on the risks and required behaviors through regular security awareness training.

Threat protection that disrupts the whole attack chain

The best protection requires the best defenses, both for data held on premises and data stored in the public cloud.

Looking at the Ryuk example, we can see how different technologies work at different stages of the attack chain.



Spam email with malicious document	Emotet and/ or TrickBot installed	Steal credentials	Escalate privileges to be admin user	Move laterally around network	Recon Active Directory	Delete backups	Disable protection in security products	**Deploy Ryuk**
Threat hunting and response	Threat hunting and response	Threat hunting and response	Threat hunting and response	Threat hunting and response	Threat hunting and response	Threat hunting and response	Threat hunting and response	Threat hunting and response
Deep Learning	Exploit Protection	Credential Theft Protection	Exploit Protection				Tamper Protection	Deep Learning CryptoGuard
Deep Learning				RDP Management				
Phishing Training								
Automatic Isolation	Automatic Isolation	Automatic Isolation	Automatic Isolation	Automatic Isolation			Automatic Isolation	Automatic Isolation

🟦 Sophos Managed Threat Response 🟩 Sophos Intercept X 🟧 Sophos XG Firewall 🟦 Sophos Phish Threat ■ Synchronized Security

Sophos Intercept X

Sophos Intercept X includes advanced protection technologies that stop ransomware on your endpoints and servers at multiple stages of the attack chain.

- AI-powered threat protection detects threats in malicious emails
- Exploit protection detects and blocks more than two dozen exploit techniques, including those used to distribute and install ransomware and escalate privileges
- Credential theft stops hackers getting your valuable credentials, blocking unauthorized system access, and admin privilege escalation
- Tamper protection stops the ransomware from disabling your endpoint protection
- Deep learning looks at the "DNA" of the file to determine if it's ransomware and, if so, stops the ransomware from executing
- CryptoGuard's behavioral detection blocks the unauthorised encryption of files, rolling them back to their safe state in seconds

Sophos XG Firewall

Sophos XG Firewall is packed with advanced protection to detect and block ransomware attacks, and stop hackers moving laterally around your network to escalate privileges.

- AI-powered threat protection, including sandboxing, detects ransomware at the gateway
- RDP management tools give you a simple, elegant way to manage your RDP, stopping hackers from using it to move laterally around your network
- IPS can detect any attempts to exploit network vulnerabilities such as those in RDP or any other part of the network stack

Synchronized Security

Intercept X and XG Firewall are great on their own, but even better together, with Synchronized Security. If anything triggers a detection in either product, XG Firewall and Intercept X work together to automatically isolate the affected devices – preventing the threat from spreading further.

Managed Threat Response (MTR)

Sophos Managed Threat Response (MTR) – many organizations don't have the expertise, resources, or desire to monitor their network 24/7. The Sophos MTR service is a dedicated, round-the-clock team of threat hunters and response experts who constantly scan for and act on suspicious activity.

Strong security practices

In addition to having strong technologies to disrupt the attacks, there are also a number of best practices you should apply to increase your defensive shield:

- Use multi-factor authentication (2FA)
- Use complex passwords, managed through a password manager
- Limit access rights; give user accounts and administrators only the access rights they need and nothing more
- Make regular backups, and keep them offsite and offline where attackers can't find them – they could be your last line of defense against a six-figure ransom demand
- Patch early, patch often; ransomware like WannaCry and NotPetya relied on unpatched vulnerabilities to spread around the globe
- Lock down your RDP; turn off RDP if you don't need it, and use rate limiting, 2FA, or a VPN if you do
- Ensure tamper protection is enabled – Ryuk and other ransomware strains attempt to disable your endpoint protection and tamper protection is designed to prevent this from happening

Ongoing staff education

People are invariably the weakest link in cybersecurity, and cybercriminals are experts at exploiting normal human behaviors for nefarious gain. Most Ryuk attacks arrive via an email with a malicious attachment. If you can stop people clicking on the attachment in the first place, you stop the threat getting into your network. We therefore recommend you invest – and keep investing – in staff training. To help, the Sophos free anti-phishing toolkit gives you a set of handy resources to educate your team on phishing, including:

- Educational poster for your office
- Examples of phishing emails
- Top tips to spot a phish
- PowerPoint deck for internal training sessions
- Phishy flowchart to help people identify phishing emails

Download for free at www.sophos.com/phishing.

Conclusion

Ransomware is the cyberthreat that just won't die. Why? Because criminals keep taking advantage of new developments in technology and society to refine and enhance their ransomware attacks. If we take one lesson away from our 30-year history of fighting ransomware, it's that ransomware is going to keep evolving.

The best defense against ransomware is a combination of layered protection at the endpoint and gateway to disrupt the attack chain, diligent application of security best practices at all times, and ongoing user education.

☑ Threat protection that disrupts the whole attack chain

☑ Strong security practices

☑ Ongoing staff education

Further reading

For a detailed breakdown of the behavioral patterns of the ten most common, damaging, and persistent ransomware families read How Ransomware Attacks by Mark Loman, Sophos Director of Engineering.

To learn more about the Sophos solutions that help you fight back against ransomware, visit:

- Sophos Intercept X
- Sophos XG Firewall
- Sophos MTR service
- Free anti-phishing toolkit

To stay up to date with the latest ransomware news follow **Naked Security**, Sophos' security news service.

- Daily email newsletter. Sign up at nakedsecurity.sophos.com
- Weekly podcast. Find us wherever you get your podcasts
- Regular social posts. Follow us on Twitter, Facebook, Instagram and YouTube

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS