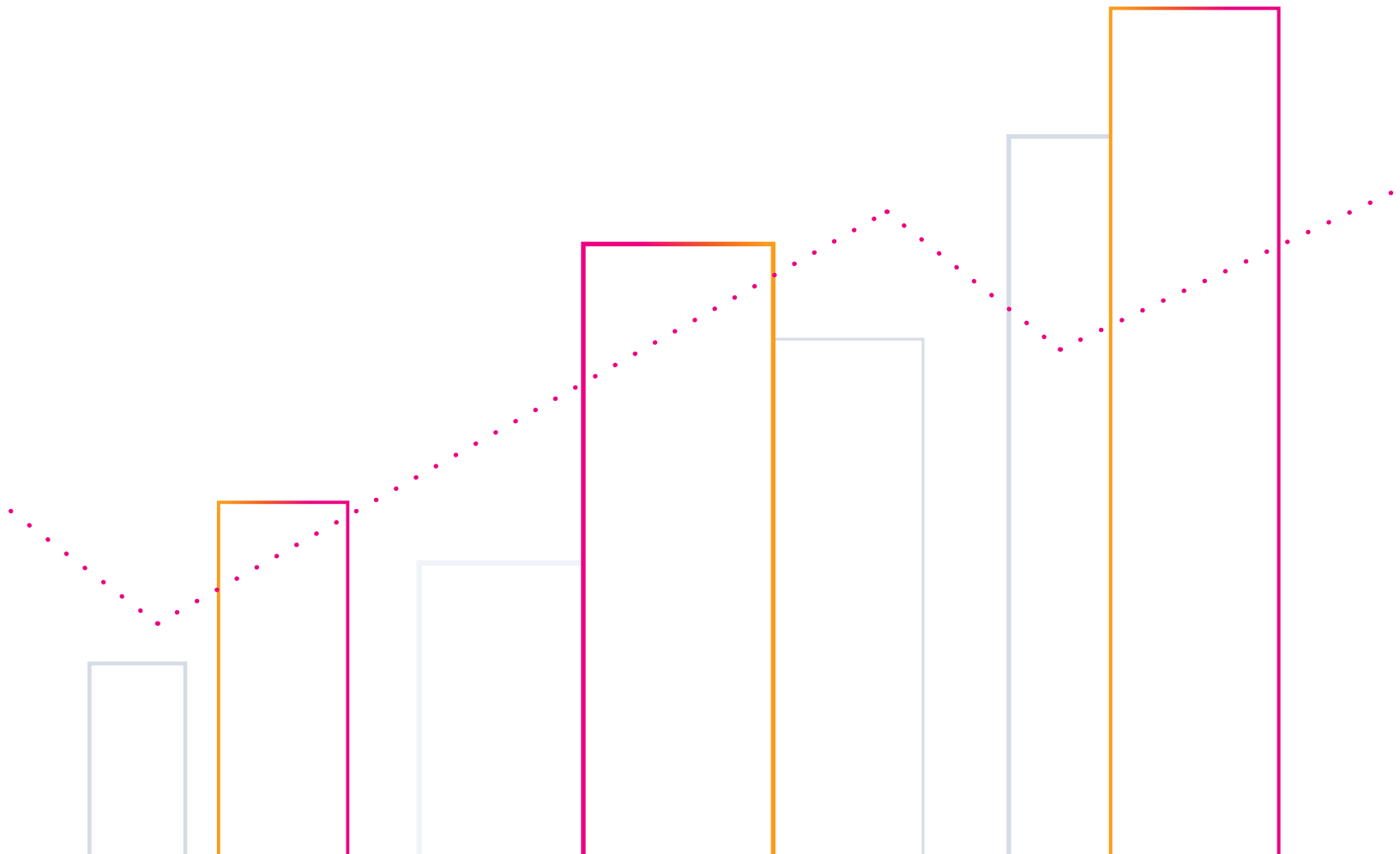
splunk> turn data into doing™

WHITE PAPER

Ransomware 101

Key ways to combat ransomware



Ransomware is a growing problem for organizations of every size with the numbers of attacks and the money spent to clean up the damage on the rise. Ransomware now regularly steals the headlines and gone are the days when it is just a minor corporate issue.

So, what exactly is ransomware? It is a type of malware that holds network data "hostage." Ransomware attacks typically target vulnerabilities on endpoints, preying on organizations that may not be fully up to date in their "security hygiene." This translates into basic security practices, such as patches, antivirus and logging critical data, which are especially important in today's world of cybersecurity where it can be difficult to stay ahead of adversaries. Although security hygiene can be time-consuming and difficult to maintain, it's these fundamentals that are the most important focus areas for enterprise organizations.

The Evolution of Ransomware

The sheer volume in the variety of types of ransomware attacks has increased since 2014 with improved encryption capabilities and the growing adoption of cryptocurrency driving cybercriminals. But the origins of ransomware attacks trace back to the 1980s when malicious actors used floppy disks to install malware on unsuspecting victims.

Since that time, ransomware attacks have only grown in sophistication and ease of delivery thanks in part to the internet. Europol, the European Union-backed organization that fights major crimes and terrorism, recently declared ransomware the second most dangerous online threat to consumers and organizations. The crime-fighting organization also said ransomware attacks show no signs of slowing down.

Europol's warning was highlighted in May 2017 when one of the worst ransomware attacks seen to date struck globally. The WannaCry attack disabled corporate computing systems worldwide, becoming what was likely the largest and possibly most damaging Windows-based ransomware attack seen.

Also, threats just don't go away when a particular attack is out of the news cycle. Legacy ransomware attacks such as Locky and Spora have re-emerged as high-profile threats even after long periods of relatively few mentions.

The Landscape – Who Are the Players?

Multiple variants of ransomware continue to appear on the threat landscape. Here is a look at the ransomware landscape from 2017 to 2019.

2017	2018	2019
NotPetya (lock and toss key)	SamSam	GandCrab
WannaCry	Ryuk (Hermes)	HiddenTear
CrySis	LockyCrypt	Buran
Nemucod	CryptoJoker	MegaCortex
Spora	Locky	RobbinHood
Crytomix	Petya	LockerGaga
BadRabbit	GandCrab	Sodinokibi/ REvil/Sodin
Scarab	Zenis	PureLocker
	Blackheart	MedusaLocker
	Satan	

Notable Ransomware

SamSam

SamSam either used vulnerabilities in remote desktop protocols (RDP), Java-based web servers, or file transfer protocol (FTP) servers, or employed brute force efforts against weak passwords to obtain an initial foothold and gain access to the victims' network. Turning an understanding of corporate pricing behaviors to their advantage, the SamSam hackers seemingly perfected their pay model to achieve results, setting ransoms at amounts that many organizations could quickly decide to pay.

GandCrab

Distributed as ransomware-as-a-service (RaaS) by a Russian crime group through a profit-sharing affiliate partner program, GandCrab is considered the most popular multi-million dollar ransomware of 2018. One of the few widely deployed ransomware variants, it dominated the market. Multiple infiltration vectors included exploit kits, stolen credentials, phishing emails and compromised websites. GandCrab also relied heavily on MS Office macros, VB Script and Powershell to avoid detection.

Ryuk

Ryuk debuted August 2018 and is specifically and exclusively used in targeted, tailored attacks on big enterprises that can pay a lot to recover their files. Covering its tracks, it deletes all files the dropper used to deploy the malware, making it difficult to determine the exact cause of infection. It's also able to identify and encrypt network drives and resources while deleting Shadow copies on the endpoint. Additionally, it disables the Windows System Restore option, making it impossible to restore encrypted files without a backup.

Filling Out the Ranks

- WannaCry occasionally still infects targets, but remains one of the biggest, if not the biggest, coordinated ransomware attack.
- LockerGaga arrives via compromised credentials. It modifies the passwords of infected systems' user accounts and prevents the infected systems from being rebooted.
- RobbinHood arrives via insecure remote desktops or Trojans and encrypts each file with a unique key.
- MegaCortex is purpose-built to target corporate networks. Once attackers penetrate the network, they roll out the ransomware to all servers and workstations using the organization's own Windows domain controllers.
- MedusaLocker makes sure mapped network drives are accessible, erases Shadow Volume copies, removes backups and disables Windows Automatic Startup repair. Following encryption, it sleeps before scanning for more files to encrypt. Further, it creates scheduled tasks that relaunch the program every half hour.

Infection Vectors

Although ransomware has been around for some time, creators are getting more sophisticated in how they infect systems, avoid detection and foil decryption efforts.

Email. Email is a popular cyber weapon because it can exploit social engineering by creating a sense of urgency and legitimacy to perform various actions. It's not surprising that it continues to be the most common vector for attack, with attachments disguised as innocuous files or links to a software download. Once clicked it leads to the ransomware infection.

Drive-by download. The ransomware infection is caused by visiting a compromised website, usually with an old browser, software plug-in or unpatched third-party application. The infected website runs an exploit kit that looks for unpatched vulnerabilities.

Remote Desktop Protocol (RDP). Internet-exposed RDP sessions are common means of infecting computers. Ideally, such sessions are used to remotely log in to Windows' computers and allow the user to securely control the computer. Unfortunately, hackers have become skilled at brute force attacking these exposed computers. In compromising RDP vulnerabilities, hackers use both brute force methods and credentials purchased on Dark Web marketplaces.

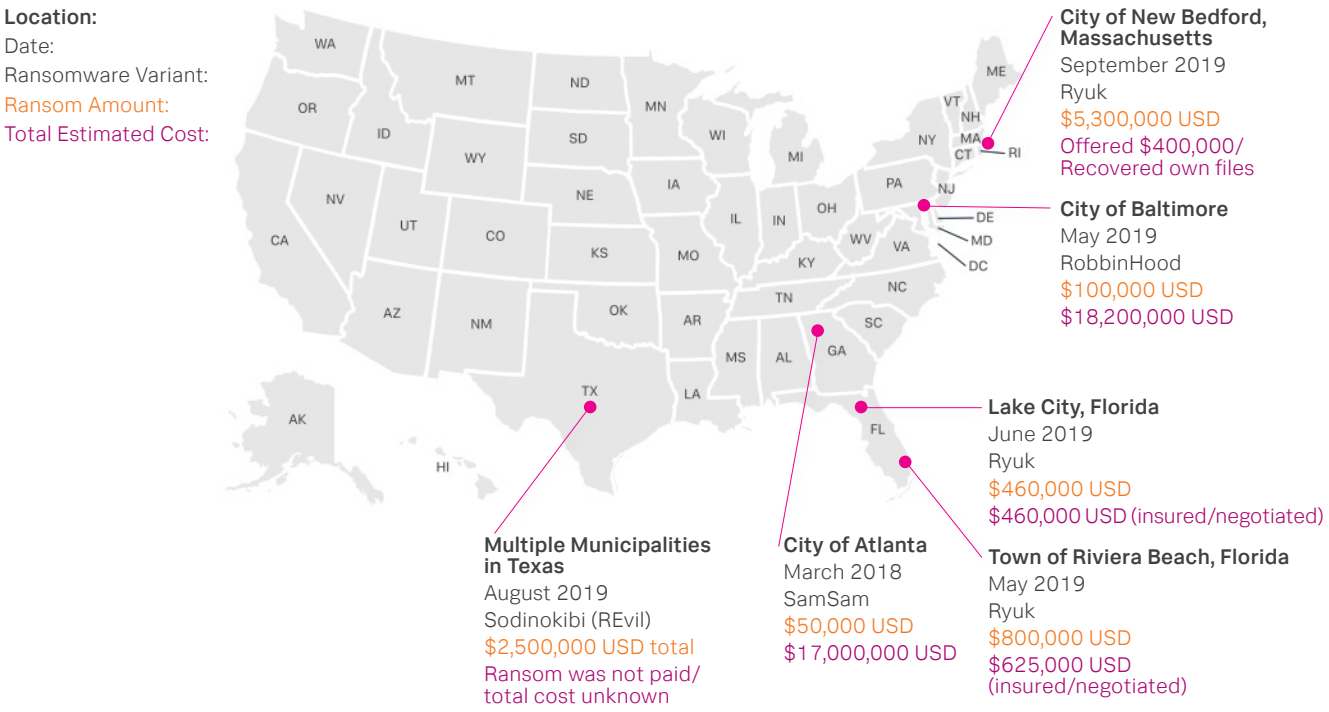
Free software. Despite the promises, free software comes with a hefty price. The deliverable comes in many forms and preys on human desire for something free to get past firewall filters. Downloads of files from infected websites and torrent sites include cracked versions of games, music, free software, game mods, adult content and screensavers.

Common Targets

In 2018, enterprises accounted for 81% of ransomware as the shift from consumer to business targets accelerated. The chief infiltration vector was email campaigns (Symantec ISTR19). There was also a pivot to targeted attacks and big game hunting, where attackers break in, survey a network, move laterally, and delete backups before encryption.

In 2019, cybercriminals increasingly targeted government agencies, municipalities, schools, hospitals and healthcare providers, either directly or through managed service providers (MSPs). Ransomware operators furthered their strong-arm schemes by compromising mission-critical systems, intimidating organizations and demanding hefty payments. Not paying ransom often means replacing equipment and starting over, leaving leadership faced with difficult business decisions. Targeted organizations often believe that paying the ransom is the most cost-effective way to get their data back. This may be the reality, but it directly funds the development of the next generation of ransomware.

Notable Attacks of U.S. Cities



Ransomware as a Business

Ransomware is marketed openly on the Dark Web. More than 230,000 new sites and over 350,000 new malicious malware programs and potentially unwanted applications are produced every day — and this is predicted to only keep growing.

For example, GandCrab was offered as ransomware-as-a-service. Marketed as an affiliate model, the developers provided technology to enterprising criminals (a.k.a, affiliates) and ransoms were split between the affiliate and the GandCrab crew at a 60/40 split or 70/30 split for top affiliates.

Additionally, GandCrab was responsive to security researchers. In their ads on the Dark Web the developers often included references to reports about the ransomware and how they adapted the malware in response.

Escalations like these in RaaS and open-source malware kits in the first half of 2019, made it easy for criminals with very basic coding skills to grab their preferred variant, customize it and launch attacks.

Advertising is also involved. RaaS developers run ads on the Dark Web and sell their technology as a kit — eliminating many of the risks and hard work of distribution while still allowing them to collect a cut of the proceeds.

Enablers and the Rise of Ransomware Attacks

Cyber insurance

Risk management specialists are concerned cyber insurance companies are increasing the rate ransomware attacks in both the private and public sectors. While law enforcement warns that organizations should never pay ransom demands, there is **increasing evidence** that the system of cyber insurance is exacerbating the problem, enabling criminal activity and emboldening ransomware crime groups.

Insurance companies are incentivized to pay the ransom, and are nudging organizations to meet the ransom demands because it is less expensive, faster and easier to pay the ransom than cover the cost of rebooting an organization from the ground up.

Because hackers are aware of this mindset, they target firms that have cyber insurance and conduct reconnaissance to determine the size of the policy and how likely it is that the organization will pay — setting the ransom slightly below the cost. While insurance firms provide negotiation services and support recovery from a ransomware attack, the bottom line is that firms with cyber insurance are more prone than others to pay the ransom.

Cryptocurrency

Payment methods were limited in the early days of ransomware. The odd hacker could deliver a message to send money via Western Union or to a bank account, but the transfer was traceable once the authorities became involved. Then came Bitcoin.

Bitcoin offers a secure and untraceable method of making and receiving payments. It is more flexible than traditional payment methods, which require specific financial or login details to use. By operating as a decentralized currency, in which people anywhere in the world pay each other without a middleman, oversight or regulation, it provides an acceptable level of anonymity.

While Bitcoin is the best-known cryptocurrency, industry analysts are taking note of Monero, which is being heavily used on Dark Web marketplaces and is becoming a new payment method of choice for ransomware demands because of its privacy features. The potential for cryptocurrency to enable ever bigger cybercrime is hard to assess, but extortion attempts taking place are now skyrocketing.

Ransomware Trends

Ransomware creators are getting more sophisticated in how they infect systems, avoid detection and foil decryption efforts. Ransomware trends include:

Blended campaigns. Nation-state threat actors are blending cryptocurrency mining and ransomware campaigns to generate revenue and/or distract from other threat campaigns.

Big game hunting. Spray and pray methods are being replaced by big game hunting, where one big target, such as a hospital or large corporation, gets hit for a big payout. Ransomware is being custom-built for a target to cause the most damage and demand higher ransoms.

Intelligence gathering. Ransomware crime groups gather intelligence on intended victims. In addition to penetrating the network and performing reconnaissance, threat actors study SEC filings for an organization's financial position and use the information to scale ransom demands.

Increased stealthiness. Strategies to get below the level of detection include:

- Slowing down the encryption process by spreading it out over a longer period of time
- Randomizing the process instead of encrypting in a linear fashion
- Delaying the attack by laying Easter eggs that lay dormant for a period of time before activating
- Using polymorphic code that changes
- Deploying multi-threaded attacks that launch child processes

Increased impact. Strategies to both increase the impact and thwart recovery include:

- Encrypting the hard drive and master boot record
- Attacking shared network drives
- Attacking files stored in Infrastructure-as-a-Service
- Deleting Windows Shadow copies and any files with backup extensions
- Targeting high-value assets like web servers, applications servers and collaboration tools

Attacks on managed service providers (MSPs). Managed service providers are a growing target for ransomware attackers. An attack on an MSP has the potential to devastate virtually any business. By exploiting vulnerable security systems typically seen in resource-constrained service providers that manage multiple businesses and municipalities, attackers can get economies of scale and exert pressure for payment.

Attacks on cloud services providers. Ransomware writers are now targeting cloud service providers with network file encryption attacks as a way to hold hostage the maximum number of customers possible. The fallout from ransomware attacks against cloud service providers is devastating because the business systems of every cloud-hosted customer are encrypted.

Wiperware. Ransomware is being used as a foil to cover up serious incidents such as data breaches. Although the attack looks like regular ransomware, typically delivered through phishing emails, the goal is to distract the organization from other security events happening on the network and delete breadcrumbs of the ancillary attack. The hope of the attacker is that the organization is so relieved to have recovered from ransomware that it doesn't investigate further.

Oldies but goodies. Ransomware continues to exploit older vulnerabilities and those with lower security scores. Research has found that vulnerabilities as far back as 2010 are still trending. Organizations that use CVSS scores as an exclusive way to prioritize patching vulnerabilities for patching will likely miss vulnerabilities being used by ransomware. (**RiskSense Enterprise Ransomware Spotlight Report**, September 2019)

Leaked data. Ransomware attacks have taken an unwelcome turn as ransomware attackers have started to leak the victim's files as a way to exert additional pressure to pay the ransom. With such an escalated attack, victims now need to be concerned both about recovering their encrypted files and what would happen if their stolen unencrypted files were leaked to the public.

Impact on Business

Ransomware drains billions from the global economy and shows no signs of slowing down. Beyond the ransom itself, the greatest cost is the financial damage that consists of downtime, lost data, tarnished reputations, system rebuild and recovery costs, and regulatory fines. Sadly, the effects to businesses continues to mount:

Ransoms in excess of $50,000 to $400,000 are no longer uncommon. Depending on the target, ransom demands have reached into the millions. Global ransomware damage is predicted to reach $11.5 billion by year-end 2019 and $20 billion USD by 2021. (Cybersecurity Ventures Ransomware Damage Report)

Data (and Splunk) Is the Answer to the Problem

Fortunately, while organizations should be wary of ransomware threats, they don't have to be scared of them. This type of malware can often be prevented. For instance, keeping track of suspicious network traffic with endpoint detection-and-response systems that block a hash and prevent new processes from spawning from nefarious executables, or detecting any domains associated with known ransomware are two options. Automating security responses according to well-known ransomware variants and behaviors is another route.

Additionally, there are methods that can be developed for specific ransomware variants, especially with Splunk Security Suite. In the case of SamSam, searches that detect and investigate unusual activities that might relate to the SamSam ransomware — including looking for file writes associated with SamSam, RDP brute force attacks, the presence of files with SamSam ransomware extensions, suspicious psexec use, and more — can be leveraged.

More specifically, Splunk can look for file modifications across your hosts, as well as for evidence of batch files being written to paths that include "system32." This activity would be consistent with some SamSam attacks and is, in general, suspicious.

This can all be done by ingesting data that records the file-system activity from your hosts to populate the Endpoint file-system data-model node. If using Sysmon, a Splunk Universal Forwarder on each endpoint can be used to collect data.

But what if you do if you're too late in catching the ransomware attack?

Management and executive boards must consider in what circumstances they would or would not pay a ransom, and then set processes for decision-making and launching an investigation. A policy and communications strategy guided by legal and business factors will reduce stress and allow for an informed response.

Here are additional tips from experts on how to prepare for and defend against ransomware attacks:

- Understand what techniques are being used. Emotet and Trickbot infections can signal the coming of Ryuk, typically starting about one to two weeks before the delivery of the ransomware. Perform a full compromise assessment at any sign of intrusion.
- Recognizing that threat actors are attacking the cloud, ensure you have full visibility over cloud services.
- Keep all software up to date, including operating systems and applications, as well as clear inventories of all digital assets and their locations.
- Identify valuable data and segment the network. Avoid putting all data on one file share accessible by everyone in the organization.
- Perform daily backups, including data on employee devices. Consider online, local and secure offsite locations.
- Perform penetration testing to find and patch vulnerabilities, ensure Remote Desktop Protocol ports can't be accessed by default credentials, and maintain good security hygiene.
- Train staff on security practices, emphasizing the importance of not opening attachments or links from unknown sources.
- Endpoint security software will block many attempts at infection through email, but securing the endpoint is no longer sufficient. Employ a multi-layered threat defense solution.
- Create an isolation plan to remove infected systems from the network.
- In mitigating an attack, perform research to see if similar malware has been investigated by other IT teams and if it is possible to decrypt the data on your own.

To learn more about how you can prevent or deal with ransomware attacks read the Splunk **blog**.

Try the **Splunk Online Demo Experience—Endpoint** where you can use sample data to safely practice security investigation techniques. Also try the **Online Demo for Splunk Security Essentials** to get started addressing different malware use cases and understand how to build a strong security portfolio.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

2020-Splunk-SEC-Ransomware 101-105-WP