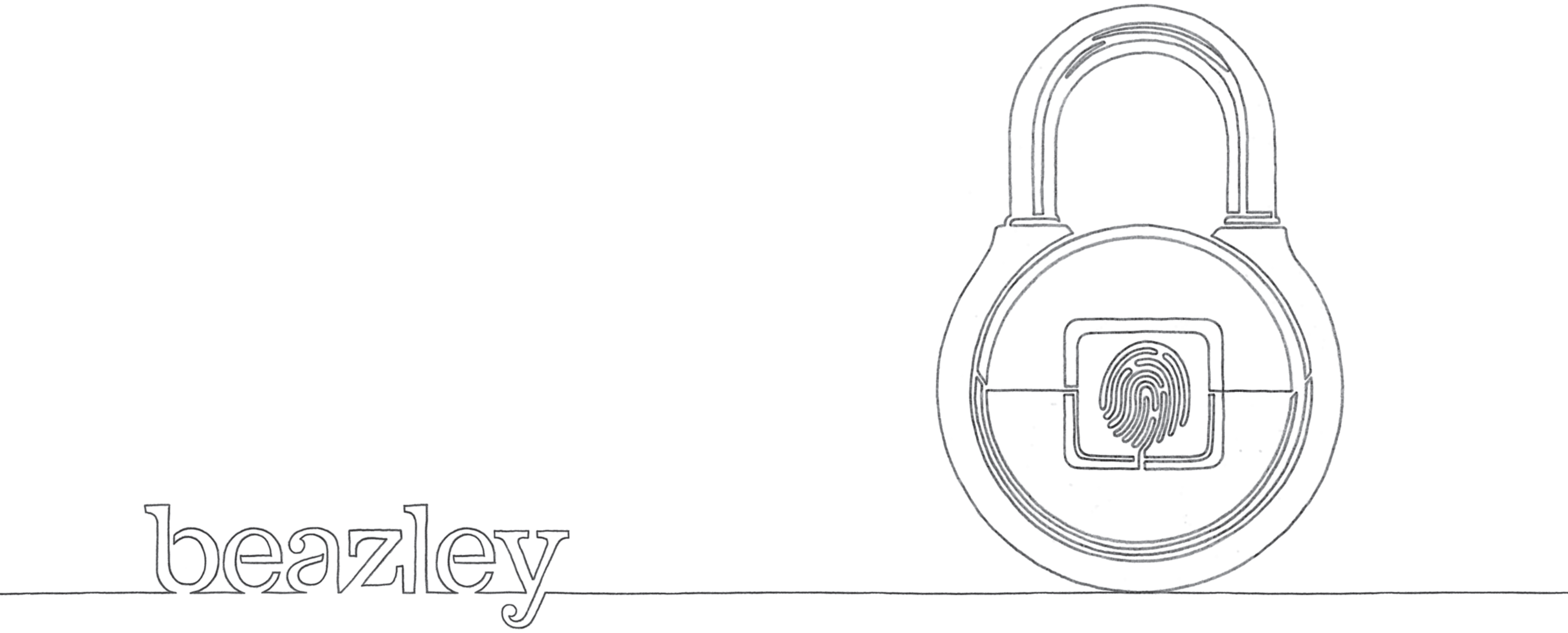
Beazley

2020 Breach Briefing



beazley

Contents

Introduction

Beazley Breach Response (BBR) Services handled hundreds of instances of ransomware on behalf of Beazley policyholders in 2019. Based on our experience and insight into this growing issue, our 2020 Breach Briefing focuses on ransomware.*

The ransomware landscape has been rapidly evolving; until four years ago reports from our policyholders of ransomware attacks were infrequent. Back then, instances of ransomware typically involved the target's data being encrypted, but not accessed or exfiltrated. Today, however, not only has the frequency of ransomware attacks increased substantially, but the added threat of a data breach makes them potentially much more damaging.

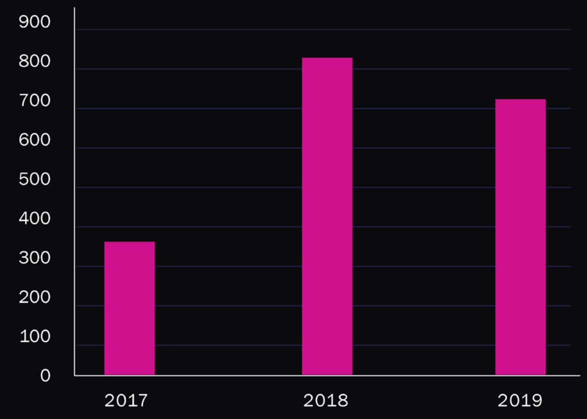
In 2019, ransomware variants, such as Ryuk and Sodinokibi, were increasingly launched in tandem with banking trojans such as Trickbot and Emotet. In these cases not only must the affected company deal with the debilitating impact of its critical systems and data being encrypted by the attackers, but the presence of these trojan artifacts often requires an additional assessment of whether data was also accessed or stolen.

Cyber criminals are getting more creative and purposeful by the day. Over the past year we managed an increasing number of ransomware incidents reported by policyholders that resulted from attacks on IT managed service providers (MSPs) and other service companies providing organizations with infrastructure and support services. In some cases, these attacks halted the operations of hundreds of customers downstream from the attacked vendor.

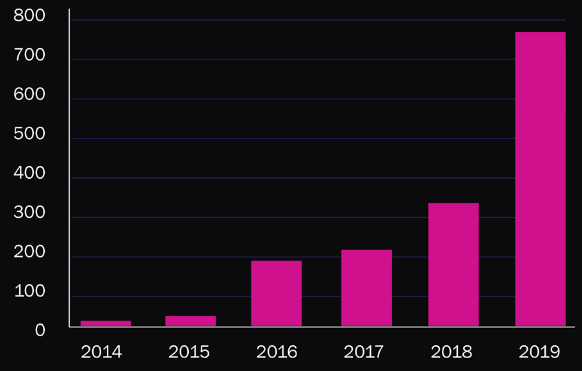
The targets of these attacks were not coincidental; criminals calculate the odds of receiving a ransom payment from an attacked MSP whose entire customer base and business could dissipate due to an attack. Ransomware attacks against the healthcare industry are similarly calculated to evoke ransom payments due to the sensitive nature of patient data and critical impact on patient care.

*Data presented in this briefing is derived from incidents reported to Beazley in 2019.

Business email compromise is down as attackers refocus on ransomware.



The rise of ransomware



BBR Services saw ransomware myth-busting over the last year, including the myth that ransom payment deadlines demanded by attackers must always be met. When ransomware hits with a Bitcoin payment demand and deadline, expert ransomware service providers such as Coveware, which possess data on various attack groups, can often determine the extent to which the attacker is willing to negotiate the amount of the payment beyond the deadline and can assist the attacked company with those negotiations.

Another myth – paying the ransom is always faster than restoring from backups. According to Bill Siegel, CEO of Coveware, which has helped many policyholders negotiate with ransomware attack groups, organizations often falsely assume that once they pay the ransom, data and business operations are immediately restored. According to Coveware, when companies do not have viable back-ups, paying the ransom only facilitates the recovery of the data. It does not cleanse and remediate a compromised network or compromised machines. The process of remediating and ensuring the network is safe to use often takes much longer than the actual decryption of data. In Coveware's experience, restoring from backups is always faster than ransom payment as a means to recover even though it may seem like a time-consuming process.

A final observation is that the profile of ransomware criminals has changed. At one end of the criminal spectrum are businesses (operating in countries where extradition by US authorities is not possible) whose success is based on ensuring their attack victim "customers" who pay the ransom know they will receive their data back quickly and fully. Increasing in numbers at the other end of the spectrum are criminals who purchase ransomware kits on the dark web, launch attacks in the hope of getting some level of payment and care little about the data restoration experience of their victims.

While the explosion of ransomware is unlikely to abate in the near term, organizations do not have to be victims; every organization should be taking active steps to stay out of the ransomware line of fire. See *"Preventing ransomware. 7 steps to take now."* on page 12.

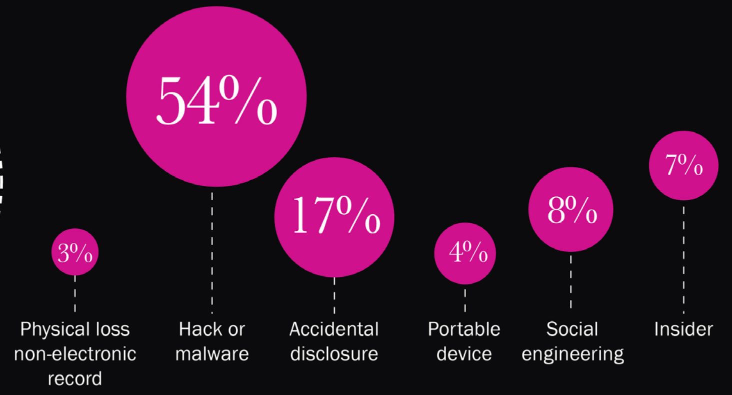
775

number of ransomware incidents reported in 2019

most targeted industries in 2019

Healthcare	Financial institutions	Education	Professional services	Retail
35%	16%	12%	9%	7%

top causes of loss in 2019



3% Physical loss non-electronic record

54% Hack or malware

17% Accidental disclosure

4% Portable device

8% Social engineering

7% Insider

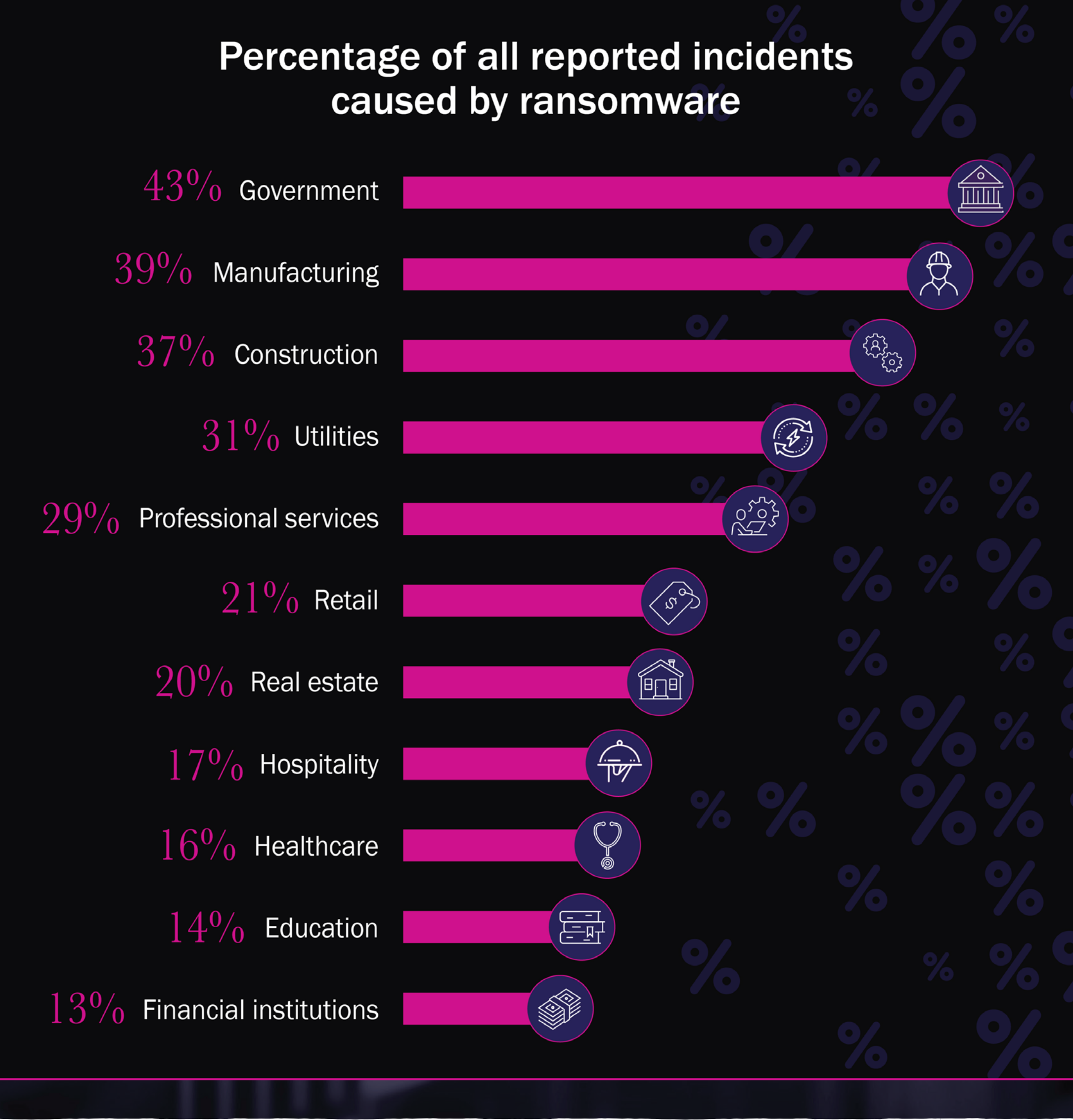
Top causes of loss in healthcare

Portable device	Social engineering	Physical loss non-electronic record	Insider	Accidental disclosure	Hack or malware
4%	4%	5%	11%	27%	39%

Hack or malware

is the top cause of loss across industries

39% Healthcare	56% Financial institutions	58% Education
68% Professional Services	67% Retail	60% Hospitality
78% Manufacturing	55% Real estate	73% Government


Percentage of all reported incidents caused by ransomware

What is the attack?

The two most common forms of attack used to deploy ransomware are phishing emails and poorly secured remote desktop protocol (RDP). In this section, we explain both attack vectors and ways to mitigate the risks associated with each.

Phishing

Today, direct email of malware and links to credential-stealing sites lead to a large number of incidents. There are a lot of protections available, in the forms of email filters and added layers of authentication, however, few of these solutions are broadly implemented. People have access to the information and technology that the attackers want, and attackers will continue to find new ways to reach people and exploit them. It would be incorrect to view phishing as the vulnerability; phishing just happens to be the most effective way of getting to the real vulnerability – people.

Mitigating phishing risk

- Enable multi-factor authentication (MFA)
- Force regularly scheduled password resets, preventing recycled passwords
- Train employees to recognize and report suspicious email traffic.

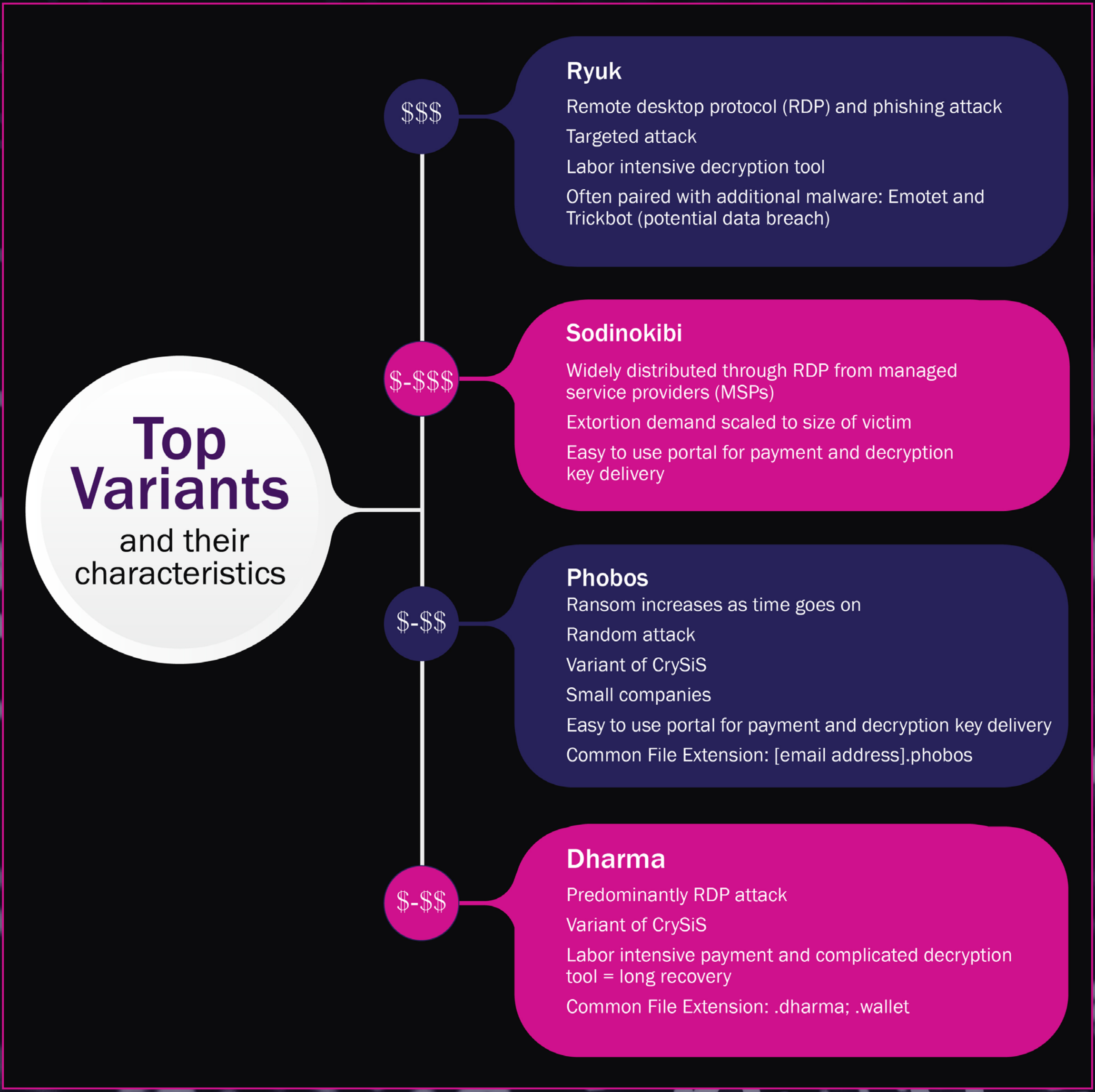
Remote desktop protocol (RDP)

RDP is a very powerful tool that provides a lot of convenience to its users. It is also extremely easy to enable. If the computer you want to access is on the public internet, you gain immediate access to your work computer from home or your company's primary file server while you are on vacation with the press of a button. However, problems arise from these basic facts:

- RDP runs on a standard port (tcp/3389) and is easily identified while scanning
- Companies have very poor password policies, giving a brute force attack a high probability of success
- More than 20 vulnerabilities have been identified within RDP, many of which allow unauthenticated access to the target computer
- Companies tend to have very poor patching policies. So, not only is it easy to turn on, it is also very easy to discover and break into.

Mitigating RDP risk

- Require access via a virtual private network (VPN) with MFA
- Whitelist IP addresses that are allowed to connect via RDP
- Require unique credentials for remote access, especially for vendors.



Top Variants and their characteristics

$$$

Ryuk

Remote desktop protocol (RDP) and phishing attack

Targeted attack

Labor intensive decryption tool

Often paired with additional malware: Emotet and Trickbot (potential data breach)

$-$$$

Sodinokibi

Widely distributed through RDP from managed service providers (MSPs)

Extortion demand scaled to size of victim

Easy to use portal for payment and decryption key delivery

$-$$

Phobos

Ransom increases as time goes on

Random attack

Variant of CrySiS

Small companies

Easy to use portal for payment and decryption key delivery

Common File Extension: [email address].phobos

$-$$

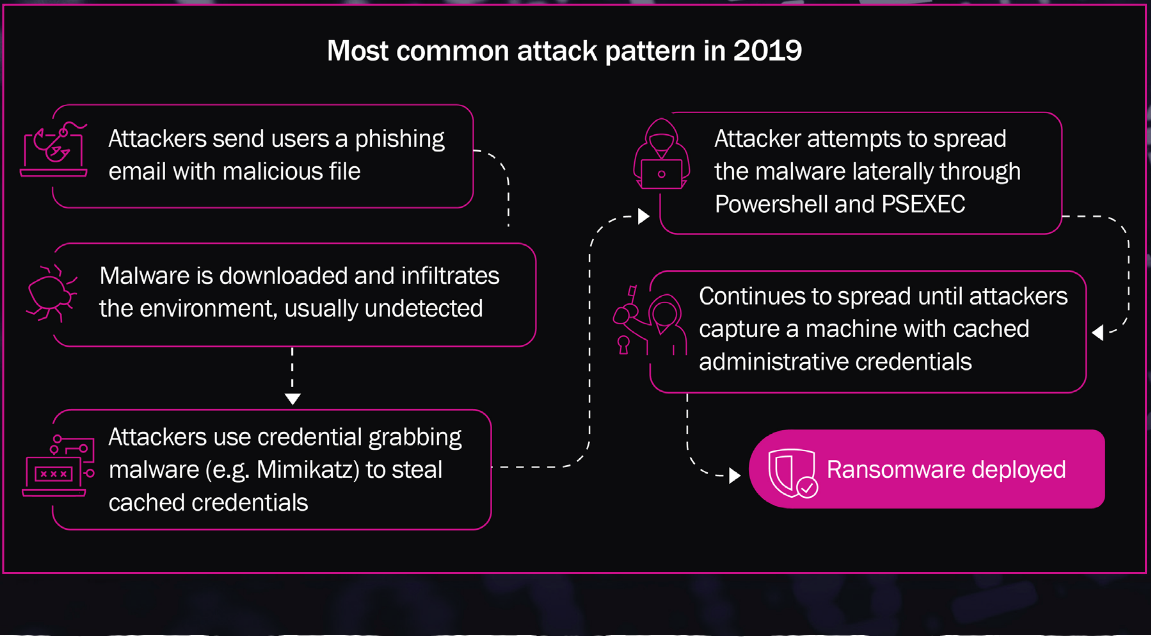
Dharma

Predominantly RDP attack

Variant of CrySiS

Labor intensive payment and complicated decryption tool = long recovery

Common File Extension: .dharma; .wallet



Most common attack pattern in 2019

Attackers send users a phishing email with malicious file

Malware is downloaded and infiltrates the environment, usually undetected

Attackers use credential grabbing malware (e.g. Mimikatz) to steal cached credentials

Attacker attempts to spread the malware laterally through Powershell and PSEXEC

Continues to spread until attackers capture a machine with cached administrative credentials

Ransomware deployed

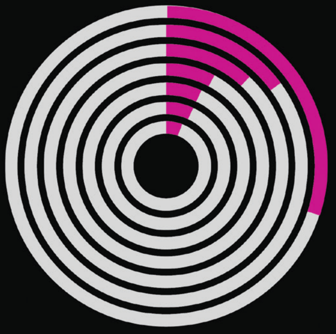
Who is the target?

Ransomware can be devastating to an individual or an organization. Traditionally, these attacks were designed to deny access and interrupt business operations. However, the recent shift towards ransomware paired with banking trojans, and towards threats to expose data, changes the landscape. Anyone with important data stored on their computer or network is a target – from municipalities or hospitals through to law firms. Important data at risk was traditionally thought to be personally identifiable information (PII) and protected health information (PHI), but it could also include intellectual property, litigation strategies, unpublished financials, and project bids. It is a myth that attackers are not interested in small companies. As our data shows, small and medium-sized business are often easier to exploit, and therefore, very attractive targets.

Seven-figure ransom demand

A university learned on a Monday morning that their system was encrypted with ransomware. They notified Beazley, and by that afternoon, BBR Services had arranged a call with computer forensic services, privacy counsel, and a company to negotiate the ransom. As the university investigated further, it learned that it had viable back-ups for most of the system, but a critical server did not have a back-up. This server contained student financial data, as well as personally identifiable data on its employees. Because the university needed this data to continue operations, it had the vendor reach out to the threat actors to negotiate a ransom. In the meantime, approximately 1,500 end points were being restored into service from back-up systems, and computer forensics was deployed to confirm no access to personally identifiable information. The initial demand from the threat actors was just over $1 million. The university wanted to negotiate for a lower payment, and ultimately decided to pay approximately $500,000 by Thursday morning in order for payroll and other financial services to continue. They received the decryption key as well as assistance to decrypt the critical server and its data.

Industries with highest percentage of ransomware incidents



29% Healthcare
14% Professional services
11% Financial institutions
8% Manufacturing
8% Education
8% Retail
6% Government

Ransomware by market segment

62% Small and medium-sized businesses

38% Middle market

Ransomware incidents increased

131%

since last year.

20% 2019

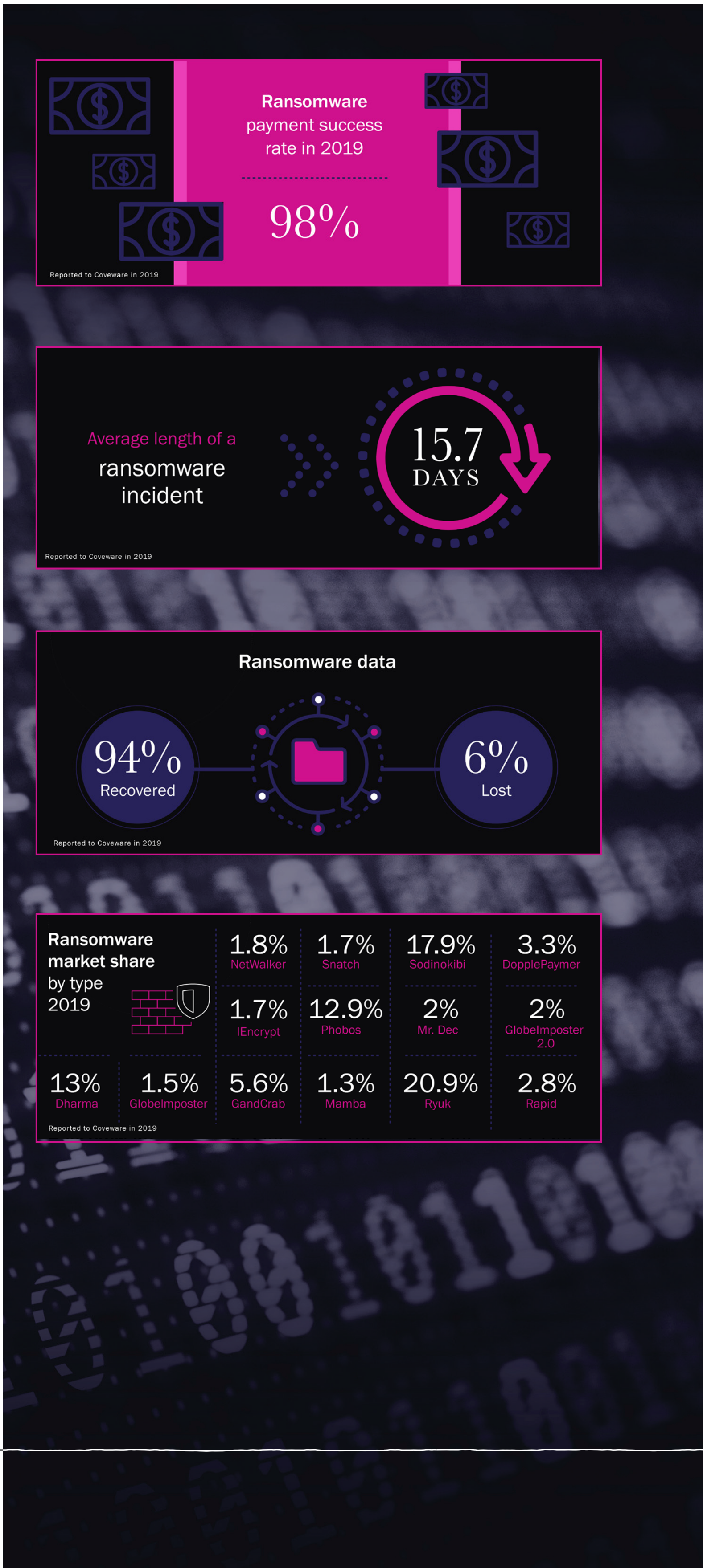
VS

9% 2018

What are the costs?

Ransomware attacks skyrocketed in 2019, with BBR Services reporting a 131% increase in the number of ransomware attack notifications against clients compared to 2018. While the frequency of these attacks is on the rise, so is the severity and disruption caused by these events. With the rise in the number of attacks, the sums being demanded by cybercriminals have also expanded exponentially, with seven or even eight figure demands not being unusual.

According to Bill Siegel of Coveware, any time the average ransom demand goes up, it attracts more attack groups interested in making money. Paired with the easy availability of exploit kits (such as banking trojans) and ransomware-as-a-service (RaaS), there is a lower barrier to entry for would-be hackers. While RaaS attacks remain commonplace and tend to hit unsuspecting small businesses, sophisticated attack groups associated with the Ryuk and Sodinokibi ransomware variants targeted larger organizations through phishing emails and exploiting vulnerable RDPs.



Ransomware payment success rate in 2019

98%

Reported to Coveware in 2019

Average length of a ransomware incident

15.7 DAYS

Reported to Coveware in 2019

Ransomware data

94% Recovered

6% Lost

Reported to Coveware in 2019

Ransomware market share by type 2019

Ransomware	Market share
NetWalker	1.8%
Snatch	1.7%
Sodinokibi	17.9%
DopplePaymer	3.3%
IEncrypt	1.7%
Phobos	12.9%
Mr. Dec	2%
GlobeImposter 2.0	2%
Dharma	13%
GlobeImposter	1.5%
GandCrab	5.6%
Mamba	1.3%
Ryuk	20.9%
Rapid	2.8%

Reported to Coveware in 2019

Is there a data breach?

Failing to preserve evidence leads to data breach notification

A small healthcare practice was hit with ransomware that initially gained access through a telecommunications server. That server did not contain any PII or PHI, however, the practice cleaned and restored the whole environment from viable backups before confirming if a separate server containing legacy electronic medical records (EMR) was encrypted. Unfortunately, the evidence needed by a forensics firm to determine whether any data was viewed or accessed was not preserved during the restoration. Since the executable file that kicked off the encryption was not available for analysis, the forensics firm was unable to determine the type and capabilities of the malware involved in this incident. Under the Office for Civil Rights (OCR) guidance on ransomware, a healthcare entity must assume that a ransom attack is a reportable breach, unless evidence shows there is no access to or exfiltration of PHI.

Since there was not enough evidence to say the server with the legacy EMR had not been compromised, the practice had to notify roughly 9,600 patients whose information was on the server containing PHI. It is likely notification could have been avoided had evidence of the attack been preserved.

Failing to contain trojan infection leads to ransomware and data breach notification

A hospital caught an attempted automated clearing house diversion of approximately $600,000. As the IT team investigated how the fraudulent request originated from a legitimate account of an employee, they discovered Trickbot on their system. The IT team concluded that Trickbot had succeeded in stealing log-in credentials and they believed the issue was contained once passwords were changed and a malware scan was run. About 60 days later, systems were crippled by ransomware and an initial demand of $1m. Forensics ultimately showed the initial Trickbot infection was paired with a delayed distribution of the Ryuk ransomware. Unfortunately, the pervasive Trickbot infection prevented forensics from being able to confirm whether or not there was data access to the infected systems. Because of this uncertainty, the insured had to notify about 100,000 patients, which has led to ongoing regulatory scrutiny.

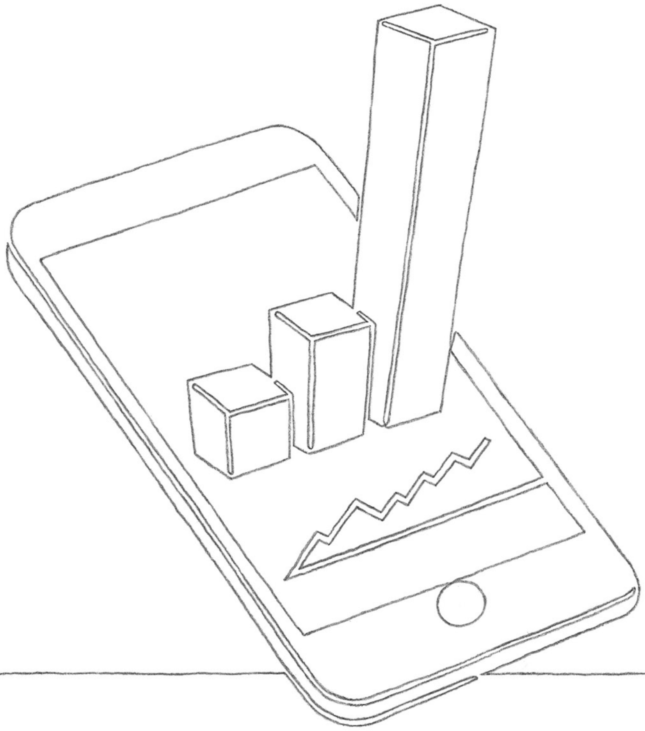
Vendor ransomware

What is the trend?

Many organizations rely on vendors to perform multiple services, which can help reduce overall costs and administrative burdens. But when you no longer control all of your data or when you provide third parties direct access to your systems, it inevitably increases your exposure to data privacy and security risks. Third-party vendors were aggressively targeted by cybercriminals deploying ransomware in 2019, and at least 17% of all ransomware incidents reported to Beazley originated from attacks on vendors. These attacks caused business interruption to many downstream customers, ranging from the inability to access data housed in a software application, to a full blown attack on the customer systems as well.

Why are vendors targeted?

Cybercriminals realized that interrupting the dependent and deeply interconnected relationship between vendor and customer would create the most pressure. Hitting a single vendor can cause catastrophic interruptions for hundreds of companies, making it more likely for the vendor to pay.



How could this impact you?

The impact and response challenges will vary depending on the services provided by the vendor.

- **External IT/MSP**
  For small businesses that completely rely on outsourced IT, a massive ransomware attack across clients draws on the MSP's resources and inevitably leaves many businesses in the dark. Small business owners without a technical background struggle to understand and assist external legal and forensics vendors hired to help them respond to the attack. The response is further complicated when the MSP itself is also infected with ransomware. Where an attack group knows they have hit an MSP, and also infected downstream clients, they may refuse to negotiate with the end clients and instead only respond to the MSP in order to increase their ransom demands. This tactic can also leave clients with little to no control over their data software recovery.

- **Software**
  Even if the ransomware does not spread throughout systems, it could still prevent access to critical data and cause a dependent business interruption. Downstream customers cannot control the pace of the recovery and have to wait to see what forensics conclusions are shared by the vendor. Customers also have limited ability to verify vendor findings, and often have to trust the investigation follows best practices and engages expert advice. Ultimately organizations are responsible for the data they provide to their vendors, and must be able to rely on the conclusions provided by vendors to determine if data has been accessed.

Preventing ransomware

Preventing ransomware. 7 steps to take now.

Here are seven steps for IT teams to protect their organization against a ransomware attack.

1. **Lock down RDP.** The RDP attack vector is regularly targeted by ransomware attacks. Disable RDP where not required. Apply secure configurations where RDP is enabled, including use of strong passwords (at least 16 characters in length) and MFA.
2. **Require MFA.** Turn on MFA for internal administrative accounts and for external access to all applications, particularly sensitive ones such as email, RDP and VPNs.
3. **Disable PowerShell.** Update PowerShell to the latest framework on all computers. Improved logging and security controls are available with the latest version. Disable PowerShell on workstations where possible. Where PowerShell cannot be disabled, logging and continuous monitoring of PowerShell activity is critical.
4. **Patch systems.** Allow automatic patching of the operating system and internet browsers. Stay on top of anti-virus software updates to detect new emerging threats that can go unnoticed in a system if the anti-virus program is out of date.
5. **Apply web filtering.** Ransomware infections can occur through malicious websites or malicious ads hosted on legitimate business websites that will redirect a user to a bad site. Apply filtering at the network and endpoint level that blocks connections to known-malicious sites.
6. **Limit administrative rights.** Admin rights should be limited to IT roles requiring these privileges and be protected with MFA. IT staff should have non-privileged accounts for day-to-day activities such as email and browsing.
7. **Conduct security awareness training.** Train employees on how to recognize common threats and scams and how to report any suspicious security incident. Conduct phishing exercises periodically to enhance security awareness and prepare employees for responding to cyber attacks.

Prepare now to recover later

Unfortunately, it is not always possible to prevent a ransomware infection, but IT departments can position their organization for a faster, smoother recovery.

- **Back up your data**
  A well thought out backup and restoration plan is one of the most important countermeasures against ransomware. Back up data regularly and maintain copies offline and/or in cloud storage. Use unique credentials to secure your backups, and store the credentials separately from other user credentials. Encrypt backups, especially when stored offsite at a third-party location or in a cloud environment.

- **Test backups**
  Test backups periodically to validate that recover is in line with the organization's recovery point and recovery time objectives. Implement automated monitoring that notifies when backups are not functioning correctly.

- **Develop a business continuity plan (BCP)**
  Effective business continuity planning helps identify how to carry out essential operations in the event of a business interruption caused by ransomware.

Conclusion

While it is difficult to predict the next type of attack, we can speculate as to targets. Products and services with a large market share will likely remain on the target list as well as communication devices, smart TVs, and cloud-based security and monitoring tools, as they have a very larger attack surface. Microsoft Windows may no longer be the most common operating system in the world, but it remains most prevalent in business use, and businesses will continue to be seen as high targets. If we overlay high value targets on top of widespread deployment, we can start to guess at what may come next.

We do believe, though, that ransomware is not going away any time soon. Ransomware attacks in their current form are far too successful and profitable for cyber criminals to shift course. Ransomware perpetrators will continue to evolve their tactics as companies implement new defenses. We have already started to see attackers pairing ransomware encryption with data theft. Instead of encrypting data and asking for an immediate ransom, cyber criminals such as the Maze attack group are now starting to name and shame organizations.

In order to combat these devastating attacks and anticipate new threats, organizations need to focus on effective protection and prevention. We are committed to continuing to help our cyber policyholders avoid and respond to these situations through education and access to our BBR Services and Lodestone Security teams. At Beazley, we provide policyholders with information, services and resources to improve their cyber infrastructure, protect policyholders from nefarious activities and, in the event of a ransomware attack, help them get their businesses back online.

beazley.com/bbr

The descriptions contained in this communication are for preliminary informational purposes only. The product is available on an admitted basis in some but not all US jurisdictions through Beazley Insurance Company, Inc., and is available on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd's. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: 0G55497).