

# Ransomware: A modern threat to data in the finance sector



The financial services industry is an attractive target for ransomware attacks.

Personal and commercial financial, banking, trading and superannuation information is arguably some of the most valuable data held by an organization today. The stakes are incredibly high for the financial services industry to adequately protect and secure their systems.

Aside from the obvious financial implications of failing to protect data, it can also cause irreparable and immeasurable damage to a company's corporate reputation: shattering trust, eroding customer bases and hindering future sales.

The threat against ransomware has only increased under the pressure of the global pandemic. This increase is caused by a combination of weaker controls on home IT networks and a higher likelihood of users clicking on COVID-19-themed ransomware lure emails, owing to heightened levels of anxiety throughout our communities.

When fundamental operations are disrupted, financial institutions find their hands tied and their capabilities lost to customers. According to a recent report from Cyber Security Ventures, an organization fell victim to ransomware every 14 seconds in 2019, and it's expected to be every 11 seconds in 2021<sup>i</sup>. The ransom amount has increased too. In mid-2018, the average ransomware payment was \$41,198. By late-2019, that price more than doubled to \$84,166<sup>ii</sup>.

If you haven't been taking ransomware seriously, you should.

## What is ransomware?

Ransomware is a maliciously-created malware that finds and encrypts files and storage. Financial institutions are particularly at risk of this as they house sensitive data. Through entry points like phishing emails, users can unintentionally allow this attack into their organization.

Typically, cybercriminals use this malware to extort money from an organization. Once data has been compromised, organizations are given the option to pay a high ransom to unencrypt the data or rely on backup to restore. However, many ransomware attacks also seek out all production and backup files and documents. By encrypting those too, the attack leaves the organization no choice but to meet the cybercriminals' demands.

While there are many variations of ransomware today, the three main ones that financial institutions will see are:

- **Ryuk**

First discovered in August 2018, Ryuk immediately turned heads after disrupting operations of a major US-based newspaper publisher. While it was eventually quarantined, Ryuk reinfected and spread onto connected systems in the network because the security patches failed to hold when tech teams brought the servers back. Detections of Ryuk increased by more than 500% in Q1 2019 over the previous quarter; by Q4 2019, detections were up another 43%<sup>iii</sup>.

- **Phobos**

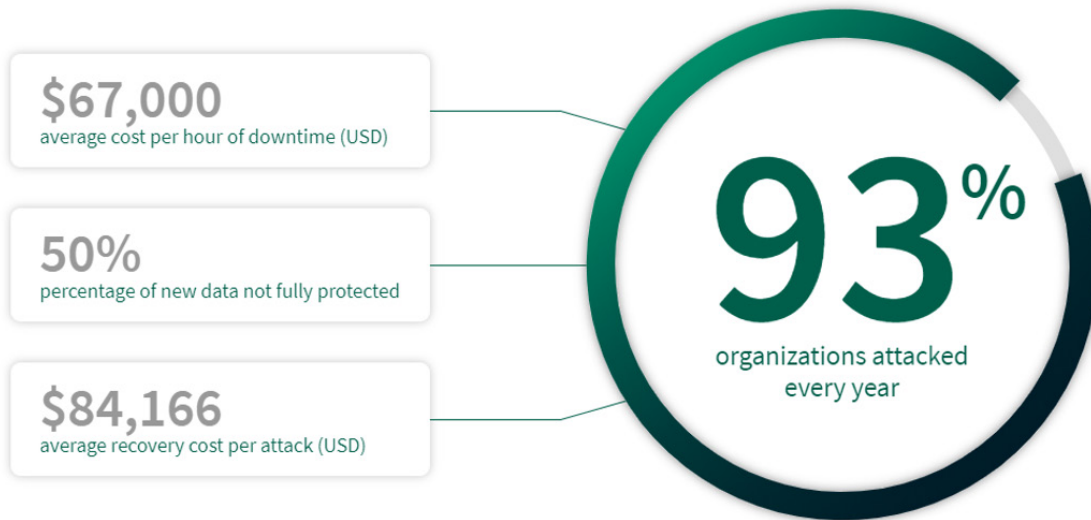
Phobos ransomware appeared in the beginning of 2019. It has been noted that this new strain of ransomware is strongly based on the previously-known Dharma (aka CrySIS) family and was probably distributed by the same group as Dharma. Phobos is one of the ransomware types distributed via hacked Remote Desktop (RDP) connections. Hacked RDP servers are a cheap commodity on the underground market, and can make for an attractive and cost-efficient dissemination vector for threat groups<sup>iv</sup>.

- **Sodinokibi**

Sodinokibi is a Ransomware as a Service (RaaS) threat model that first appeared in May 2019. Sodinokibi has shown to be nearly as much of a threat as Ryuk, with high spikes of detections that outweigh what we've seen with other business-focused ransomware families in 2019, such as Phobos. Since its introduction, Sodinokibi detections have increased by 820%, a foreboding number as we look ahead<sup>v</sup>.

## The real cost of ransomware

Ransomware is no longer a question of **if**, but **when**.



These numbers are a concern, especially to institutions within the finance sector that hold crucial patient data. Data growth is exploding, and by 2023, 60% of the new data created will require some level of protection, but only half will have it. This feels like we're on a path to destruction, however, with the right ransomware investments, the finance sector can feel confident that, even if attacked, they can respond with little or no cost (or availability issues) to the institution.



## Ready for the fight

If financial institutions want to win a ransomware battle, here are three resilient strategies: Education, implementation and remediation

- **Education:** The education aspect must be taken seriously. Whether it is assessing the phish risk, removing the most frequent attack vectors or keeping systems and software up to date, taking these steps are essential. If these steps are not taken, ransomware risk is increased. There are two major audiences that should be targeted from an education perspective: IT staff and users. It's important to target both groups since threats can be introduced from both personas. Knowing that RDP, phish and software updates are the three main mechanisms for entry is a huge help in focusing the scope of where to invest the most effort to be resilient against ransomware from an attack vector perspective.
- **Implementation:** Regarding ransomware resiliency, implementing a backup solution is a lot like going through a compliance audit. A product is not necessarily compliant or non-compliant to a standard. Rather, compliance is completely dictated on how the product is implemented and audited. When it comes to a ransomware incident, resiliency is completely based on how the backup solution is implemented, the behavior of threat and the course of remediation.

As an important part of ransomware resiliency, implementing your Veeam® backup infrastructure is a critical step. Implementation recommendations for ransomware resiliency include:

- Protection of the backup server and components
- Implementing capabilities for ransomware detection
- Ultra-resilient backup storage and the 3-2-1 Rule
- Multiple recovery techniques configuration
- Endpoint protection
- NAS protection
- Encryption of backup data
- Orchestrated recoveries of backups and replicas
- **Remediation:** Despite all the education and implementation techniques that are employed to be resilient against ransomware, finance institutions should be prepared to remediate a threat if introduced. At Veeam we have agreed upon the approach to remediating ransomware as:
  - Do not pay the ransom
  - The only option is to restore data

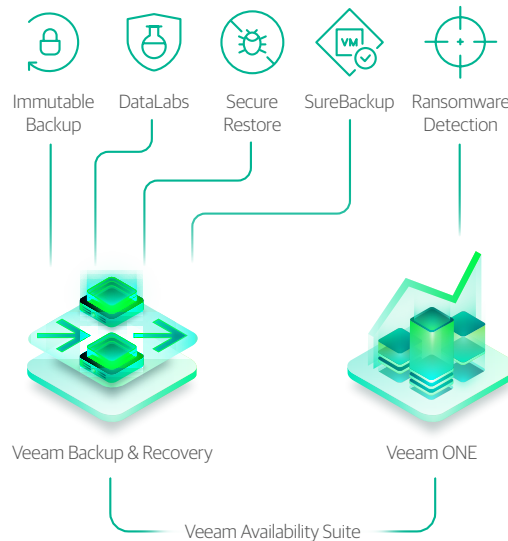
With the recommendations previously outlined in this document, the financial sector should be prepared to have layers of resiliency to defend against a ransomware incident. What institutions may not have thought about is specifically what to do when a threat is discovered. When a ransomware attack occurs, look for a strong remediation plan, including:

- **Support:** Tap into your backup vendor support organization. For example, Veeam has specific operations to guide customers through data restores in ransomware incidents.
- **Communications first:** In disasters of any type, communication becomes one of the first challenges to achieve. Have a plan for how to communicate to the right individuals out-of-band.
- **Experts:** Have a list of security, incident response, identity management, (etc.) experts that are ready to be contacted if needed. They can be within the institution or external experts.
- **Chain of decision:** One of the hardest parts of recovering from a disaster is decision authority. Who makes the call to restore, to fail over, etc.? Have business discussions about this beforehand.
- **Ready to restore:** When the conditions are right to restore, implement additional safety checks before putting systems on the network again.
- **Restore options:** Depending on the situation, maybe a whole VM recovery is best. Possibly a file-level recovery makes sense.
- **Restore safely:** Trigger an antivirus scan of the backup image or file before the restore completes. Use the latest antivirus and malware definitions and perhaps an additional tool to ensure a threat is not reintroduced.
- **Force password resets:** Users don't like this, but implement a sweeping forced change of passwords.

By properly following these steps, companies within the finance sector can learn where threats lurk, how to build a resilient IT environment and how to secure safe restores of patient data. Trying to play catch up with your protection during a ransomware attack will be a disaster. These preventive measures are the best way to fight ransomware and avoid data loss, financial loss, business reputation damage and more.

## Veeam solutions

Veeam prides itself on being in the front lines, fighting the good fight against ransomware and protecting important data kept by the finance sector. Veeam offers transparent and actionable strategies on how to educate employees, rotate backup copies across several locations, and leverage cloud options for making your backups practically immutable.



### Protecting backup data from attack

Air-gapped or "immutable" backups offer a powerful technique for being resilient against ransomware and other threats. Enabling a replica of your backup, stored out of reach from cyberattacks, utilizing controls that ensure deletions or changes cannot happen without strict multi-level approvals. [Veeam's Scale-out Backup Repository™ \(SOBR\)](#), partnered with [Capacity Tier \(also known as Cloud Tier\)](#), enables an easy-to-use capability that writes backup data into object storage either on Microsoft Azure, Amazon Web Services (AWS), IBM Cloud or any platform that supports object store. Using AWS S3 or select S3-compatible storage, you also get access to Object Lock, enabling backup data to be stored as an immutable backup.

### Detecting ransomware

Detecting a ransomware attack in its initial stages can be difficult. [Veeam ONE™](#) provides the ability to monitor your environment closely and be aware of any suspicious or abnormal activity. By analyzing CPU usage, datastore write rate and network transmit rate, [Veeam ONE](#) can help identify if there are higher than normal amounts of activity on a particular machine. When the alarm is triggered, this immediately notifies you to inspect the machine, look at the resource counters and determine for yourself whether the activity is normal. If it's not, this is a good indicator that more steps should be taken to determine if ransomware is the culprit.

### Ensuring ransomware-free backups

Viruses can be undetected and dormant in your current systems, ready to pounce. Use the power of your backup to root out ransomware threats before they attack. At all stages of backup and recovery, you want to be protected. Keep ransomware out for good with an automated step to scan the backup for malware, delivering confidence for future restorations. [Veeam SureBackup®](#) provides immediate notice that a system may not be recoverable due to an undetected ransomware or malware threat.

### Restoring guaranteed virus-free workloads

What happens if your backups have an undetected virus? Viruses can be undetected and lay dormant in older backups. Make sure you can protect yourself. [Secure Restore](#) enables a complete anti-virus scan of your backups when restoring. Having access to the latest virus definitions helps safeguard against previously unknown viruses, providing greater confidence that dormant threats won't be reintroduced back into the environment.

### Testing your workloads securely

Unsure of a current workload? Suspect that it may be infected? Restore them into a fully secured and isolated environment to test. Tap into the power of [Veeam DataLabs™](#) to restore data, workloads and applications into a fully isolated virtual sandbox environment. Test for cyberthreats and other issues while performing potential remediation activities – without impacting any production systems.

Ransomware is a real threat to the finance sector. If you're ready to prepare yourself, then Veeam can help. Start today with an easy 12-question gap assessment to identify areas of ransomware threat, and then download the Ransomware Preparation Kit to get started today.

**ACCESS YOUR  
RANSOMWARE THREAT**

**DOWNLOAD THE RANSOMWARE  
PREPARATION KIT**

## About Veeam Software

Veeam® is the leader in Backup solutions that deliver Cloud Data Management™. Veeam provides a single platform for modernizing backup, accelerating hybrid cloud, and securing data. With 375,000+ customers worldwide, including 82% of the Fortune 500 and 67% of the Global 2,000, Veeam customer-satisfaction scores are the highest in the industry at 3.5x the average. Veeam's 100-percent channel ecosystem includes global partners, as well as HPE, NetApp, Cisco and Lenovo as exclusive resellers. Veeam has offices in more than 30 countries. To learn more, visit <https://www.veeam.com> or follow Veeam on Twitter [@veeam](#).

---

i [Steve Morgan, Global Ransomware Damage Costs Predicted To Reach \\$20 Billion \(USD\) By 2021, Cybercrime Magazine, October 2019.](#)

ii [Coveware, Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate, Report on Q4 2019.](#)

iii Malware Labs. [2020 State of Malware Report.](#) February 2020.

iv Malwarebytes Labs. [A deep dive into Phobos ransomware.](#) July 2019.

v Malware Labs. [2020 State of Malware Report.](#) February 2020.



# Cloud Data

Backup  
for what's next

Learn more: [veeam.com](https://www.veeam.com)