VECTRA
Security that thinks®

2019 Spotlight Report

The biggest threat from ransomware: Malicious encryption of shared network files

I am artificial intelligence.
The driving force behind the hunt for cyberattackers.
I am Cognito.

VECTRA
Security that thinks®

TABLE OF CONTENTS

Introduction

The most effective weapon in carrying out a ransomware attack is the network itself, which is instrumental in enabling the malicious encryption of shared files on network servers. Ransomware scans the network for shared files on servers and computers to which it has access privileges, and then spreads from one computer to many others.

When ransomware encrypts shared network files, known as *file shares*, attacks become very costly due to resulting operational downtime and data loss. Organizations hit by a ransomware outbreak find themselves in an all-hands-on deck emergency that requires complete attention to restore systems immediately while business functions are held hostage.

Downtime becomes worse when the target is a cloud service provider and the systems encrypted are those of its customers. In 2019, cloud hosting firms DataResolution.net and iNSYNQ were hit by ransomware attacks that prevented over 30,000 customers from using their provided services.

Targeted ransomware attacks are not new. The peak volume of ransomware attacks in a single instance occurred in 2017, when the WannaCry outbreak hit multiple companies simultaneously. WannaCry spread quickly across the globe using opportunistic methods that targeted organizations exposed to the Eternal Blue exploit.

In 2019, ransomware evolved from opportunistic into targeted attacks that victimize organizations likely to pay a larger ransom to regain access to their files. Operational stagnation typically means a greater cost and reputational damage. For cloud service providers, the damage can be devastating.

This is clearly evident with the Ryuk ransomware strain, which sets the ransom according to the victim's perceived ability to pay. Ryuk is one of the more successful ransomware strains observed in the past year.

First seen in August 2018, Ryuk has targeted more than 100 U.S. and international businesses, including cloud service providers like DataResolution.net. CrowdStrike characterizes the approach used by Ryuk as "big-game hunting" because attackers have made off with millions of dollars from a wide range of victim organizations with perceived high annual-revenues.

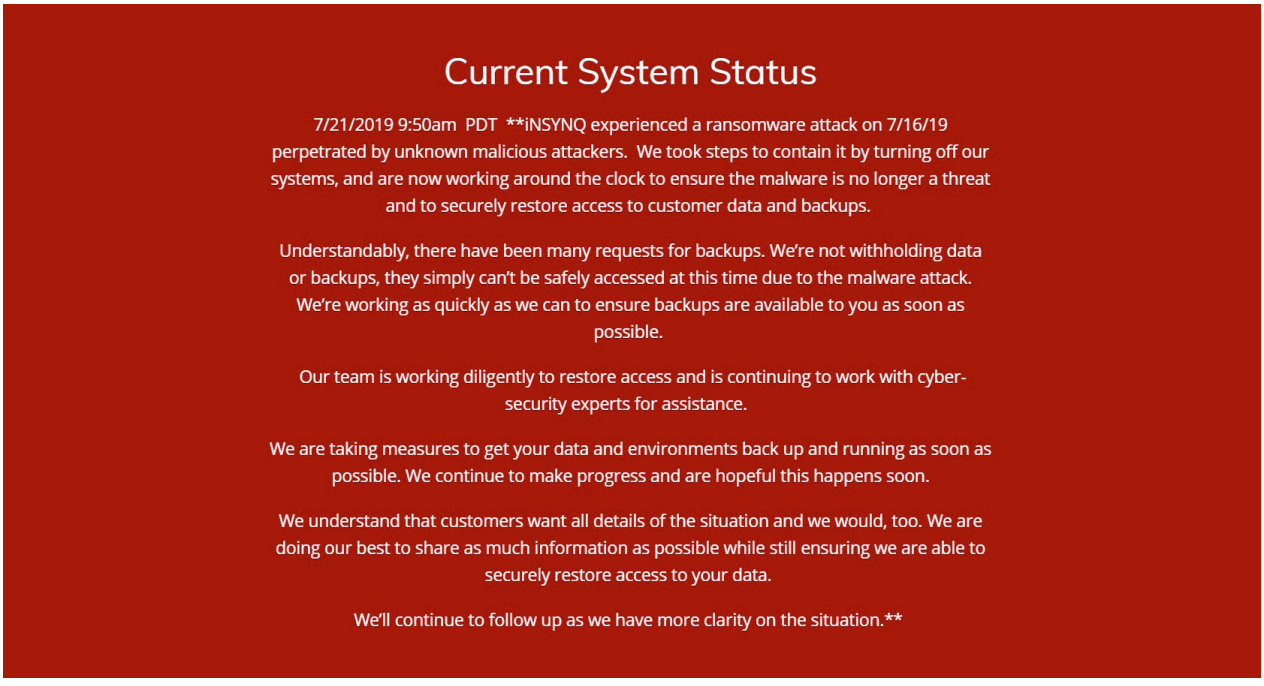


Figure 1: iNSYNQ ransomware notice to customers

With Ryuk, ransomware attacks are modular. Different pieces of malware and attacker techniques are combined as needed. For example, malware packages that contain banking trojans have been quite effective in attacks against the financial services sector.

Ryuk does not self-propagate inside the network. Instead, a malware trojan like TrickBot is used to launch Ryuk to enumerate network file shares and encrypt everything in the attack radius. To make matters worse, ransomware's use of anti-forensic recovery techniques – such as manipulating the virtual shadow copy – makes recovering from backups difficult.

What is network file encryption in ransomware?

Because the goal in a ransomware attack is to propagate as wide and as quickly as possible, it is desirable for file encryption to occur beyond the local files. When the infected computer has access to documents in network share volumes – with their high capacity data storage – that single host can lock access to documents across several departments in a targeted organization.

It is standard practice to employ volume-sharing protocols, such as the Server Message Block (SMB), with networked shares in order to make documents easily accessible to the users. This occurs in both cloud and private data centers.

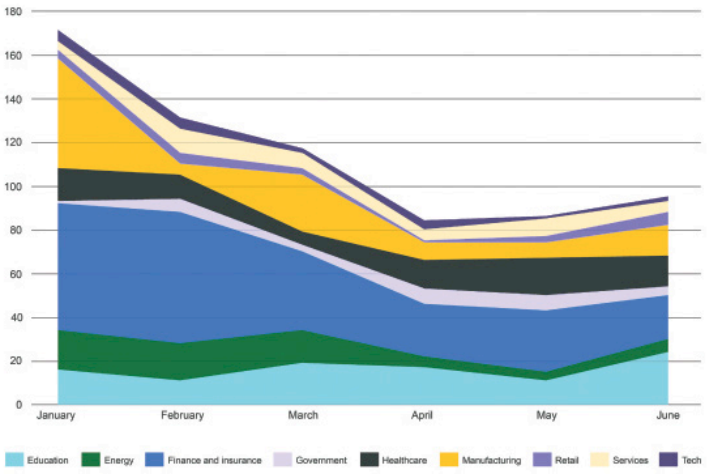
Documents are stored in shared volumes to ensure proper backup procedures and for productivity in sharing content for teamwork, especially for a mobile workforce. However, this also makes files more vulnerable to exposure because the shared volumes are reachable from any system in the organization, which might include an infected system.

In a volume-sharing system, a single infected host could encrypt an entire networked volume, resulting in a global impact on the target organization's business and systems. The files must be recovered from the most recent cold backup if the ransom is not paid. Backup systems attached to a network are also at risk, which is why cold offline backups are critical for recovery.

Nightly backups are a common policy and the main recovery mechanism from a ransomware attack. They are easier to implement in scenarios with centralized volumes shared through a network.

The target of network file encryption in ransomware attacks

By analyzing data from the 2019 Black Hat Edition of the Attacker Behavior Industry Report, we can identify where ransomware encrypts network files.



The stacked area graph represents the total volume of incidents with network file encryption from January-June 2019. A ransomware file activity detection indicates an internal host is connected to multiple files via the SMB protocol and is rapidly encrypting files. Given the level of damage that can occur from a single host encrypting multiple file shares, the the level of threat of a single detection is high.

The network file-encryption component represents the most damaging of ransomware attacks. Vectra® found that that while ransomware is dangerous, the total volume of detections has been decreasing for some time. The trend over the last six months confirms previous trends across 2018.

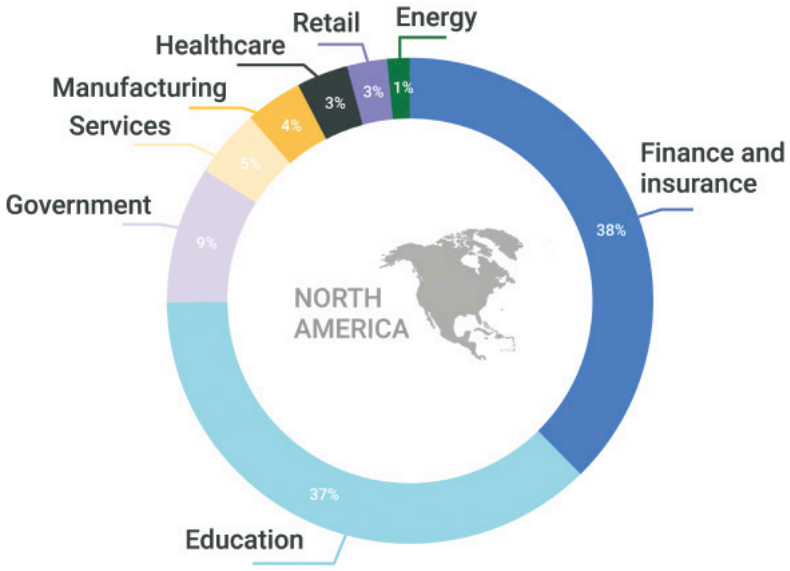
This downward trend in the total volume of detections does not mean organizations should be any less vigilant. The damage from successful ransomware attacks, especially when encrypting network file shares, is very costly.

By combining industry data over time, the 2019 data also shows industries that were most impacted based on region. In this report, Vectra focused on North America, Europe and the Middle East. While no group is safe from a ransomware attack, some experience a higher volume of network file encryption across the organization.

Case study: North America, Europe and the Middle East

North America by industry

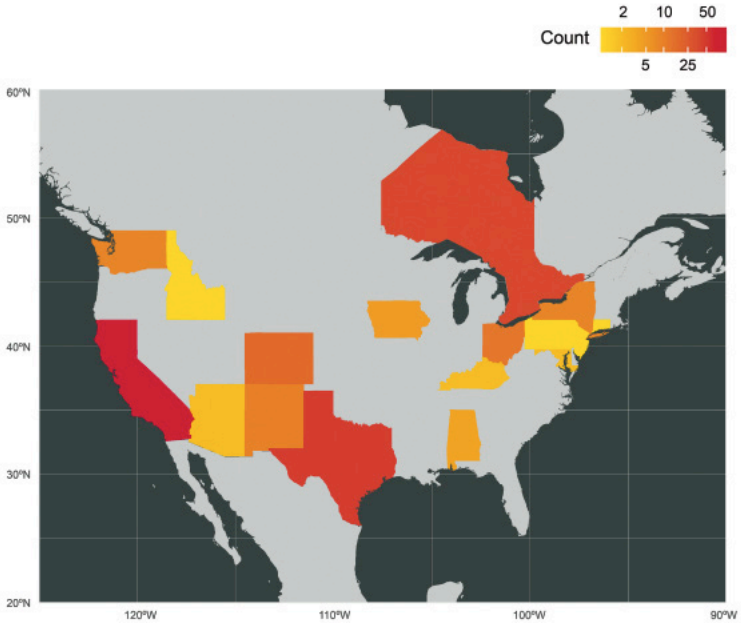
The chart represents the percentage of the total number of incidents exhibiting ransomware network file encryption per industry in North America, from January-June 2019.



The data shows a high percentage of financial organizations as the most impacted, closely followed by education and then government organizations. Although no instances of network file encryption in ransomware were detected within education organizations in Europe and the Middle East, in North America it was the second largest component of overall network file encryption in ransomware detections.

North America by region

The map represents the overall density of where incidents exhibiting ransomware network file encryption occurred by state and territory in North America from January-June 2019.



California experienced the largest percentage of the total volume of file encryption in ransomware attacks, followed by Texas and Ontario. The distribution of network file encryption in ransomware is logarithmic – regions with high detection rates have orders of magnitude more detections than states with only a few detections.

For example, California and Texas combined represent 56% of the observed incidents with ransomware network file encryption. This demonstrates that network file encryption in ransomware tends to cluster and the top victims experience a vastly greater share of overall attacks than mid-level victims.

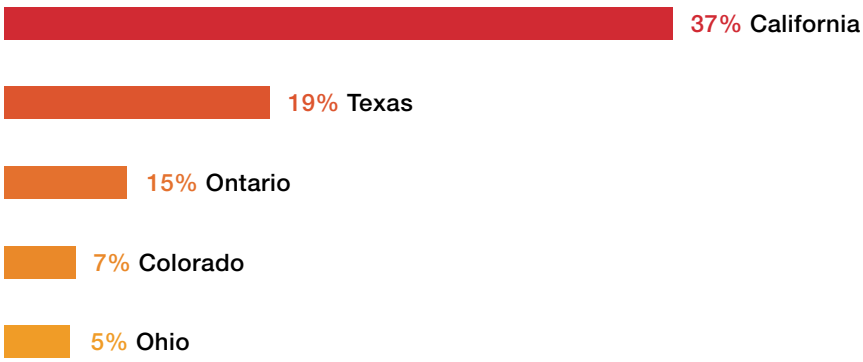
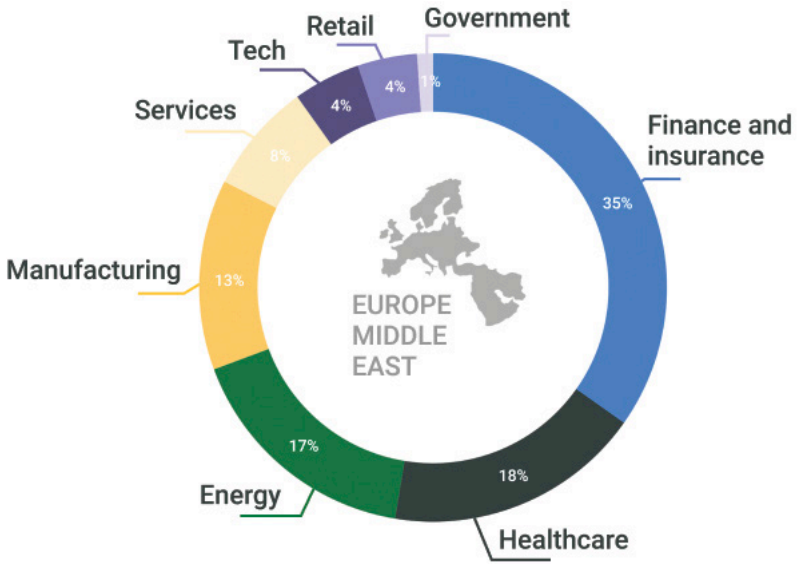


Figure 2: Top 5 North America regions

Europe and the Middle East by industry

This chart shows the percentage of the total number of incidents exhibiting ransomware network file encryption per industry in Europe and the Middle East, from January-June 2019.

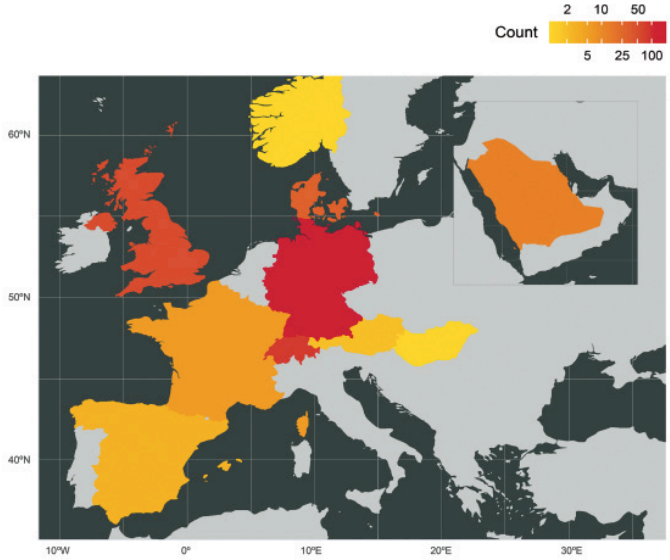


The data shows a high percentage of financial organizations impacted, followed by healthcare and energy in that time period. In both Europe, the Middle East and North America, financial organizations had the highest proportion of overall network file encryption in ransomware detections.

However, that is one of the only industry-level similarities between the two regions. In Europe and the Middle East, energy companies fell victim to the third-highest number of network file encryption in ransomware attacks, but the energy industry in North America comprised only 1% of all ransomware detections.

Europe and the Middle East by region

This map represents the overall density of where incidents exhibiting ransomware network file encryption occurred by state and territory in Europe and the Middle East, from January-June 2019.



The frequency distribution of network file encryption in ransomware is again logarithmic. Germany experienced almost as many instances of network encryption in ransomware as every other country in Europe and the Middle East combined.

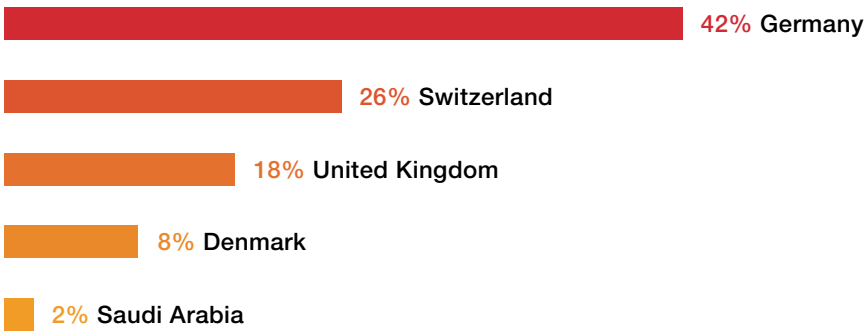


Figure 3: Top 5 Europe and Middle East regions

How to detect and respond to ransomware

Look for early indicators of a ransomware attack. Because modern ransomware attacks are targeted and modular, attacker dwell-times can be quite lengthy before shared network files are encrypted.

From the time of the initial infection to the deployment of the ransomware, attackers perform reconnaissance inside a compromised network to discover which systems are critical before encrypting files. There are many steps in the attack lifecycle that organizations can proactively monitor for early signs of ransomware behaviors inside the network.

It is important to have detailed plans on how to manage a ransomware incident, including customer communication. Having a documented and rehearsed incident response process is as important as the ability to proactively detect attacks.

This should include knowing how to hunt for ransomware and precursor behaviors, investigate incidents, and understanding the appropriate response methods. For example, incident response teams should know that unplugging a malware-encrypted system can destroy the system BIOS, rendering that system unrecoverable. Alternatives like network segmentation and host isolation should be considered.

It is also vital to observe privileged access to know which accounts have access to critical systems. Ransomware can only run with the privileges of the user or the application that launches it.

Comprehensive knowledge about the systems and users that access specific services will enable security operations teams to monitor misuse of privileged access and respond when that access is compromised – well before network file encryption occurs.

To learn more about cyberattacker behaviors seen in other real-world cloud, data center and enterprise environments, read the 2019 Black Hat Edition of the Attacker Behavior Industry Report from Vectra.

VECTRA
Security that thinks.®

Email info@vectra.ai **Phone** +1 408-326-2020 www.vectra.ai