proofpoint.

Threat Briefing: **Ransomware**

Fast Facts

Description:

Ransomware encrypts critical data or locks users out of their devices until they pay a ransom to the attacker, typically a crime syndicate.

Tools of the trade:

Cryptolocker, WannaCry, Bad Rabbit, Cerber, Crysis, CryptoWall, GoldenEye, Jigsaw, Locky, Petya, Conti, Sodinokibi and Ryuk

Origin:

1989, AIDS Trojan created by Joseph Popp. Popp sent 20,000 infected diskettes labeled "AIDS Information—Introductory Diskettes" to attendees of the World Health Organization's international AIDS conference and created what is now believed to be the world's first ransomware attack.

Types:

- **Crypto ransomware**
  Cyber criminals encrypt files on a computer, making it impossible for the user to access it.
- **Locker ransomware**
  Malware that locks a victim out of the computer, preventing them from accessing the device until a ransom is paid.
- **"Scareware"**
  Malware designed to trick victims into thinking they have been infected with ransomware and sending payment to the attacker. Though not technically ransomware, scareware can have the same effect on victims.

Risk factors:

- Vulnerable software and systems
- No easily accessible backups
- Ineffective or nonexistent cybersecurity
- Untrained and vulnerable users

Possible damages:

- Monetary loss
- Loss of sensitive or proprietary data
- Potential reputational harm
- Operational disruption and productivity loss

Ransomware—which gets its name from the payment it demands after locking away victims' files—is a major issue for all modern businesses. It's one of today's most disruptive types of cyber attacks, putting victims out of business, forcing hospitals to turn away patients, and bringing entire city governments to a standstill. The best way to manage ransomware is preventing it from entering your environment. Here's a primer on this growing threat.

Notable Ransomware Attacks

Universal Health Services loses $67 million in Ryuk ransomware attack

A ransomware attack on Universal Health Services (UHS) cost the company an estimated $67 million in downtime and related expenses. The Fortune 500 healthcare organisation has tens of thousands of employees in the US and UK and annual revenues exceeding $10 billion.[1]

UCSF pays $1.14 million ransom to regain research data

Attackers struck the university locking up the UCSF School of Medicine's IT systems. Administrators quickly attempted to isolate the infection and ringfence a number of systems that prevented the ransomware from traveling to the core UCSF network and causing further damage.[2]

Cognizant earnings hit with $50M–$70M ransomware costs

IT services provider Cognizant was hit with a ransomware attack in April 2020 that hit its Q2 earnings. The incident incurred legal, consulting and other costs to investigate the incident, restore service and remediate systems.[3]

1 Phil Muncaster (*Infosecurity*). "Universal Health Services Estimates $67 Million in Ransomware Losses." March 2021.
2 Charlie Osborne (*ZDNet*). "University of California SF pays ransomware hackers $1.14 million to salvage research." June 2020.
3 Catalin Cimpanu (*ZDNet*). "Cognizant expects to lose between $50m and $70m following ransomware attack." May 2020.

Ransomware attack disrupts U.S. fuel supply

One of the nation's largest pipelines shut down in May 2021 in the wake a ransomware attack, halting operations throughout a 5,500-mile system that supplies nearly half of the total fuel supply to the East Coast.[4] The pipeline's operator paid attackers $4.4 million to unlock the data, but "it ultimately wasn't enough to immediately restore the pipeline's systems."[5]

World's largest meat processor suspends beef production after ransomware attack

The Brazilian company shut down meatpacking plants in Colorado, Iowa, Minnesota, Pennsylvania, Nebraska and Texas, due to an attack that U.S. officials say originated in Russia.[6] In a news release, the company said it detected the attack on its computer networks in North America and Australia. Fortunately, its backup servers were not affected.[7]

Anatomy of a Ransomware Attack

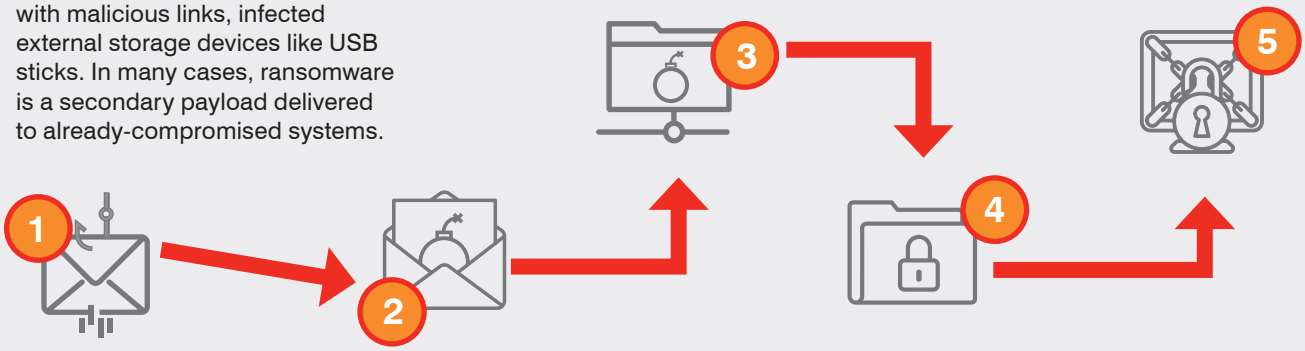
For over three decades, ransomware has evolved into one of the most menacing cyber threats. Digital currency like Bitcoin have made it easy for cyber criminals to collect ransoms. Besides, attackers are getting savvier at targeting old, outdated systems.

Here is how most ransomware attacks play out:

1. Distribution | Attackers trick users into accessing malicious software using phishing emails, social engineering, fake websites with malicious links, infected external storage devices like USB sticks. In many cases, ransomware is a secondary payload delivered to already-compromised systems.

3. Staging | The ransomware payload dropped by the file conceals and embeds itself within the system.

5. Ransom note | A note is then displayed to the victim demanding payment for the release of files.

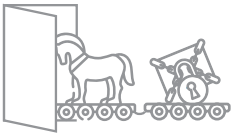


2. Infection | The user then unknowingly downloads an executable file called a loader (or downloader) that installs the ransomware.

4. Scanning and Encryption | The malware then scans the system and the network and encrypts files.

Cyber criminals are also learning that most victims of ransomware have data backup and refuse to entertain their ransom demands. So threat actors have evolved. They start with stealing and encrypting files and move on to threatening to release the stolen data. The information could be highly sensitive, personal and can have devastating consequences if it becomes public knowledge. Sophisticated ransomware strains even seek out and encrypt backups, too.

4 David E. Sanger, Clifford Krauss and Nicole Perlroth (*The New York Times*). "Cyberattack Forces a Shutdown of a Top U.S. Pipeline." May 2021.
5 Collin Eaton and Dustin Volz (*The Wall Street Journal*). "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom." May 2021.
6 Jacob Bunge (*The Wall Street Journal*). "Meat Buyers Scramble After Cyberattack Hobbles JBS." June 2021.
7 Hamza Shaban, Ellen Nakashima and Rachel Lerman (*The Washington Post*). "JBS, world's largest meat processor, shut down U.S. beef plants amid cyberattack." June 2021.



HOW RANSOMWARE ATTACKS HAVE EVOLVED

Ransomware was once a primary payload in malicious email campaigns, but it's now seen more often as a secondary infection.

Cyber criminals distributing trojans and other kinds of malware allow ransomware groups to use backdoors into infected systems in return for a share of the profits.

This means that for most businesses, the first line of defence against ransomware is making sure they are protected from initial infection. In other words, block the loader and you block the ransomware.

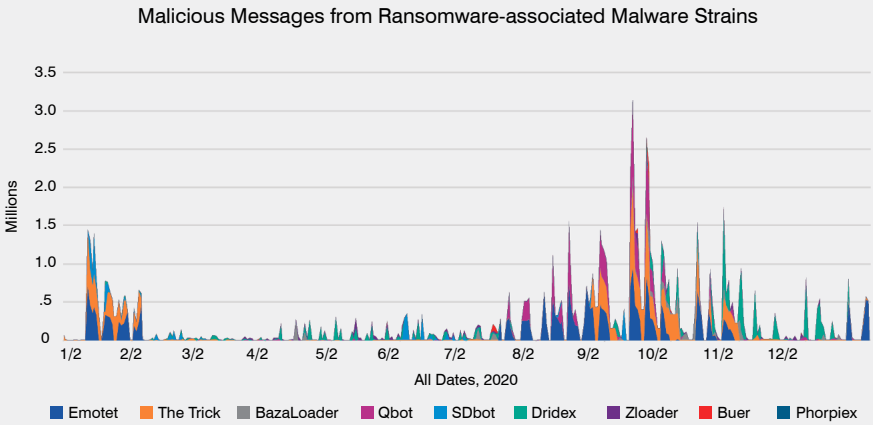
Research Insights

Ransomware is commonly delivered as a secondary infection after a system is first compromised through a malicious email. Many of the most prolific malware strains are closely associated with subsequent ransomware infection in our own observations and those by other researchers.

Here is a list of common malware strains and ransomware mostly closely associated with them.

MALWARE/DOWNLOADER	ASSOCIATED RANSOMWARE
Emotet	Ryuk
The Trick	Conti
Dridex	BitPaymer/DoppelPaymer
Qbot	Egregor
SDBbot	Clop
ZLoader	Egregor and Ryuk
Buer (Buer Loader)	Ryuk
Phorphiex/Trik	Avaddon

Emotet, The Trick, Dridex and Qbot were among the most prolific malware we saw in 2020, with steady volumes across the year and significant spikes in the fall.



More organisations are paying up—with mixed results

According to Proofpoint's 2021 State of Phish Report, 68% of U.S. organisations surveyed said they paid a ransom in 2020. That's twice the global average. While 41% of Spanish organisations refused to pay the ransom after being infected. On a global scale, they were considered least likely to negotiate with attackers.

Upon paying a one-time ransom, 78% of French organisations were able to regain access to their data. The U.S. was the second highest at 76%.

Infosec professionals revealed that in 2020, 34% of organisations were infected and opted to pay the ransom. 32% were infected but didn't pay the ransom and 34% said they did not experience ransomware.

How to Protect Your Organisation

The best way to deal with ransomware is to avoid it in the first place.

Before the attack

Start with the assumption that you will become a victim of ransomware. Your next plan should be prevention, detection and response. For example:

- Back up critical data, test data-restore procedures and keep backups segmented from primary file systems
- Update and patch systems
- Train and educate users
- Invest in people-centric security solutions
- Use network segmentation to limit spread
- Decide before the attack whether, how much and under what circumstances your organisation is willing to pay a ransom if attacked.

During the attack

If you are under attack, your next steps should be to prevent further damage and have a response plan. For example:

- Call law enforcement
- Disconnect from the network
- Determine the scope of problem based on threat intelligence
- Orchestrate a response
- Use network segmentation to limit spread
- Look for other vulnerabilities, malware and system compromises that likely came with the ransomware
- Don't count on free ransomware decryption tools
- Restore critical data—be sure to look for any malware that may have been backed up with other data

After the attack

In the aftermath of a ransomware attack take steps to restore and resolve the issues caused by the incident. For example:

- Cleanup and remediation
- Post-mortem security review
- Assess user awareness
- Risk-based, people-centric controls
- Reconsider security posture and align investment with the greatest areas of risk

Should you pay the ransom?

Paying a ransom funds criminal activity. But the consequences of an attack can be severe for both the business and its customers. The right answer isn't always clear.

Organisations must consider a few factors before deciding the course of action:

- Safety of the customers and employees
- Time and resources needed to recover
- Responsibilities to the shareholders to keep the business running
- Kind of criminal activity the payment would potentially fund

Whatever the decision, it should take place before an attack, when executives aren't under the pressure of a looming deadline and severely disrupted business. Beyond whether the organisation will pay a ransom, leaders should decide how much they're willing to shell out and under what conditions. Keep in mind that some payments—such as those made to attackers on U.S. sanctions lists—may be illegal.

LEARN MORE

The best way to stop ransomware is proactive prevention. A robust ransomware prevention plan involves people-centric security. It comes with making your employees aware through training based on real-world attack techniques. It detects and blocks ransomware and malware downloaders that target your people. It helps you quickly respond and take the necessary action before something goes wrong.

To learn more about how to effectively stop ransomware, download our Ransomware Survival Guide

For more information, visit **proofpoint.com**.