CAPINTECH

Understanding Ransomware: Malware in Its Cruelest Form

By Lisa Traina, Partner

Ransomware is a type of malware, but with an extra sting. If infected with this malware, access to your operating system or files will be prevented or limited. The hacker will demand payment (ransom), but often will not unlock the systems or files even if ransom is paid.

Ransomware is nothing new, dating back to the AIDS Trojan in the late 1980s. Because it was the 80s, instead of paying electronically with bitcoin the victim had to mail money to a post office box.

Payment requirements aren't the only change, of course. Ransomware attacks have become increasingly sophisticated and increasingly common. And with the rise of Ransomware-as-a-Service (RaaS), anyone can purchase ransomware and use it to extort money from victims of their choosing.

Let's look at how ransomware works.

Step 1: Infection

How does a device or system get infected with ransomware? All of the usual malware methods are applicable to ransomware infection:

- Emails with malicious links or attachments
- Visiting websites that install malware on your computer
- Clicking malicious links on a website
- Malvertising (malicious advertising) links
- System vulnerabilities
- Access via stolen credentials
- Self-propagating ransomware (cryptoworms)

Step 2: Execution

Once the ransomware is on your system, the real damage begins. Earlier ransomware was known for blocking system access immediately upon boot up or when your operating system loaded. Recent variants encrypt files on your hard drive, mapped network drives, or unmapped drives, leaving your files inaccessible. Some variants also lock your bitcoin wallet. This is the digital equivalent of physically stealing someone's wallet. The more vicious versions of ransomware slowly delete files as a ransom clock ticks. Advanced ransomware goes as far as detecting backup files and deleting or encrypting them. The latest variants not only take your files hostage but threaten a data dump if you do not pay.

The major takeaway: ransomware is evolving, and cybercriminals are going to do whatever it takes to make the victim pay.

WARNING: Nothing is safe. If it's connected, it's at risk!

This includes:

- Workstations
- Servers
- Laptops
- Smartphones/tablets
- External hard drives
- USB removable media
- SAN/NAS
- Synced cloud storage

What to Do if Your Organization is Attacked

Take these actions if your organization is affected by ransomware:

- Disconnect infected devices from the network to prevent the ransomware from spreading to other devices.
- Turn off any cloud syncing. If your system is hit with ransomware, files that sync with the cloud will be

Ransomware is evolving, and cybercriminals are going to do whatever it takes to make the victim pay.

encrypted and those encrypted files will sync with the cloud.

- Implement your Incident Response Plan if you have one. (If you don't, this article explains what an Incident Response Plan should include.)
- Restore from backups on either a disconnected drive or a connected drive that has not been compromised. Be aware that malware could still exist on your systems even after you contain the attack and restore your data.
- If you do not have backups, you could research whether the algorithms or decryption key tables have been released. While this is not always the case, sometimes you can obtain the decryption key without paying the ransom.
- Contact your legal counsel. They will be able to advise you on steps such as contacting law enforcement and notifying affected parties, if necessary.
- Contact your insurance company. There may be a provision in your policy that could be impacted or mitigated if protocol is followed.

Tips for Fighting Ransomware

There are several useful resources to help you evaluate comprehensive cybersecurity protections for your organization, including:

- The Center of Internet Security's top controls
- The Cybersecurity Framework from the National Institute of Standards and Technology (NIST)
- This comprehensive Ransomware Guide from the Cybersecurity & Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC)

The following protections are critical for providing baseline controls for mitigating the risks of malware, including ransomware. Keep in mind that cybersecurity controls should be layered and there may be additional protections not listed here that would be appropriate for your organization.

- **Endpoint and data management** – Endpoint management is critical to protecting your assets. To manage the risks comprehensively, you must first know what you have, where it is located, and how it connects to your greater network. Similarly, you need to know what data you have and where it is, and ensure you're only keeping the data you truly need. With the availability and relatively low cost of data storage these days, it is easy to keep everything in multiple places; however, that increases the attack surface, exposure, and potential impact.
- **Backup processes** – Establishing robust backup processes is one of the most critical controls for being able to recover your data from a ransomware attack without paying the ransom. But to do that, your backups must be recent, successful, and comprehensive. In addition, they should be properly segmented, or "air-gapped," from your network and be unchangeable so that ransomware cannot impact both the source data and backups simultaneously.
- **Anti-malware, patch, and vulnerability management** – Once you identify your endpoints, you should establish processes to ensure security updates are applied promptly, and that any device that supports it has robust anti-malware protections. Patching is critical to securing devices, and applying security updates in a timely manner decreases the opportunity for a ransomware attack. Similarly, a robust anti-malware solution may be able to prevent or contain various ransomware strains that gain access to your network. In addition, performing comprehensive vulnerability scanning with automated tools can help you identify vulnerabilities in your environment so you can close them to decrease the ways that bad actors and ransomware can infiltrate your network and systems.
- **Filtering capabilities** – While many organizations use filtering, it's important to review this control to see if you can make it more robust. Increasing your web filtering can prevent your employees from accessing sites that are known to be malicious or have a higher risk of being associated with malicious links (such as social networking sites). Email platforms can allow you to configure controls such as spam filtering or deactivating links in emails so users cannot click them. It's also important to ensure that you are filtering through your firewall so that during an incident, you prevent your internal systems from talking to command-and-control-servers used by the ransomware and bad actors, which may help reduce the impact of the incident.
- **Configure strong application controls** – Strong application security is a baseline control for practicing good cyber hygiene. However, ransomware also finds its way into many networks when bad actors compromise login credentials to remote access tools that allow them to access the internal network. Deploying controls such as lockout

These protections are critical for providing baseline controls for mitigating the risks of malware, including ransomware.

settings and multi-factor authentication can reduce the likelihood of an account being exploited and used to spread malware.

- **Employee training** – Your end users are one of your largest assets — but they also are often your riskiest. Employee cybersecurity training is crucial to helping your staff understand cybersecurity risks and their role in protecting your organization. You can put significant technical controls in place, but if you have end users who can't identify a phishing email or who circumvent controls, it can jeopardize the success of the measures you've implemented.
- **Other controls** – Disabling macros in Microsoft Office, limiting access rights and administrative privileges, implementing application whitelisting, and discontinuing the use of Remote Desktop Protocol (RDP) when exposed directly to the public Internet are additional ways to reduce your risk.

Now that you understand how ransomware works, take a look at the current threats and far-reaching impacts of ransomware with our article on The Current State of Ransomware. Then learn how to evolve your controls to tighten your defenses with our How to Take Your Ransomware Controls to the Next Level article.

If you have questions about this or other cybersecurity issues, please contact us at cybersecurity@capincrouse.com.

Additional Resource:

The State of Ransomware and Enhanced Controls Recorded Webcast

This article has been updated.

About the Author

Lisa Traina, Partner
CapinTech
ltraina@capincrouse.com
o 505.50.CAPIN ext. 2000

Lisa uses her more than 35 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa also holds an AICPA Not-for-Profit Certificate.

Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017 and is now CapinTech.

About CapinTech

Capin Technology, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintechnology.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.