Ransomware: Everything You Need to Know

You're busy. You're tired. You just want to play Pokémon Go or access your company's intranet. Whatever the reason, whenever you click "Remind me later" on a software update, you make your device vulnerable to ransomware.

That is just one of the many ways ransomware can enter your system. Malvertising, phishing emails, and even sophisticated thumb-drive schemes are common tactics that adversaries use to compromise your system. Let's take a closer look at one common scenario.

You Click "Remind Me Later"

No software is perfect. Developers regularly identify bugs in their programs and release patches to fix them. When you delay updating your plug-ins or applications, adversaries can easily exploit those known vulnerabilities. When it came to one popular exploit kit, Flash accounted for 80 percent of successful attempts. Be it Flash, Silverlight, or even Google Chrome, regularly update and patch.

You're Infected

On your device, ransomware now takes control of targeted systems. It then uses an asymmetric key exchange to encrypt your files. Basically, it's able to scramble your data without your consent—and only the developer of the ransomware has the key to solve it. Some forms of ransomware also spread across the network. Security experts predict that this self-propagation will become more prevalent.

A Ransom Note Appears

Once the infection is complete, a message will appear on your screen, demanding that you pay a ransom in bitcoins for your data. A typical ransom can be anywhere from $200 to $10,000, but some institutions have paid a far higher price. One hospital in California coughed up $17,000 in exchange for its data. This was after they had lost $100,000 every day that it couldn't operate normally.

Security experts advise that you don't pay the ransom. Some types of ransomware either can't unlock your files or automatically destroy them. Talos threat researchers have found that these malicious, destroy-all types of ransomware are becoming more prevalent. According to our 2016 Midyear Security Report, threat researchers warn that data integrity is a new concern in ransomware. Adversaries can't be trusted to keep the integrity of the data they encrypt, and the potential fallout from tampered medical records or engineering designs, for example, can be massive.

Plus, by paying the ransom, you're supporting a criminal enterprise. As long as they can make money from these schemes, attackers will continue to create even more potent strains of ransomware.

How to Stop Ransomware

The best way to prepare for ransomware is to deploy a layered security approach.

Before an Attack

You can strengthen your defensive position in several simple ways. You should strongly consider using a disaster recovery partner as a backup plan to keep your business running smoothly if the worst occurs. But you can take even simpler measures. Regularly back up your files to protect your important data. Install ad blockers and always update your software when prompted.

But ad blockers alone can't detect and block all malvertising or identify bad hyperlinks. Consider using Cisco® Umbrella, which can be installed in under 5 minutes. It detects malicious sites and blocks requests at the host level.

During an Attack

With Umbrella the vast majority of ransomware files will be stopped at the DNS layer, before they even reach an end user's device. Despite the best prevention efforts, no method will give you complete protection from ransomware.

You need to see what's happening in your network and be able to identify attacks as they happen. Cisco Stealthwatch™ threat detection monitors your network traffic and sees when something anomalous occurs—like a ransomware infection. It issues an alert that the system has been compromised.

As the file tries to run, Cisco has powerful tools to stop it:

- Umbrella protects your system by blocking the file's request to the encryption key infrastructure. This means that the ransomware can't communicate back and get the information needed to encrypt your data.
- As Umbrella blocks the request, Cisco's next-generation firewall will block the connection, giving you extra protection.
- If a file makes it past both the DNS layer and the firewall, Cisco Advanced Malware Protection (AMP) for Endpoints can block the file from running and then goes a step further. It continually analyzes all of the file activity across the system, giving you the ability to find and remove all malicious files.

After the Attack

If you've already been compromised by ransomware, you need to scope the damage and stop it from spreading. AMP can stop known malware files from running and remove the file on the endpoint.

To stop the spread of ransomware across a network, dynamic segmentation with Cisco TrustSec® technology can identify what parts of the network the ransomware has reached and help stop its spread.

Want to learn more? Check out cisco.com/go/ransomware.

C11-737870-00 09/16