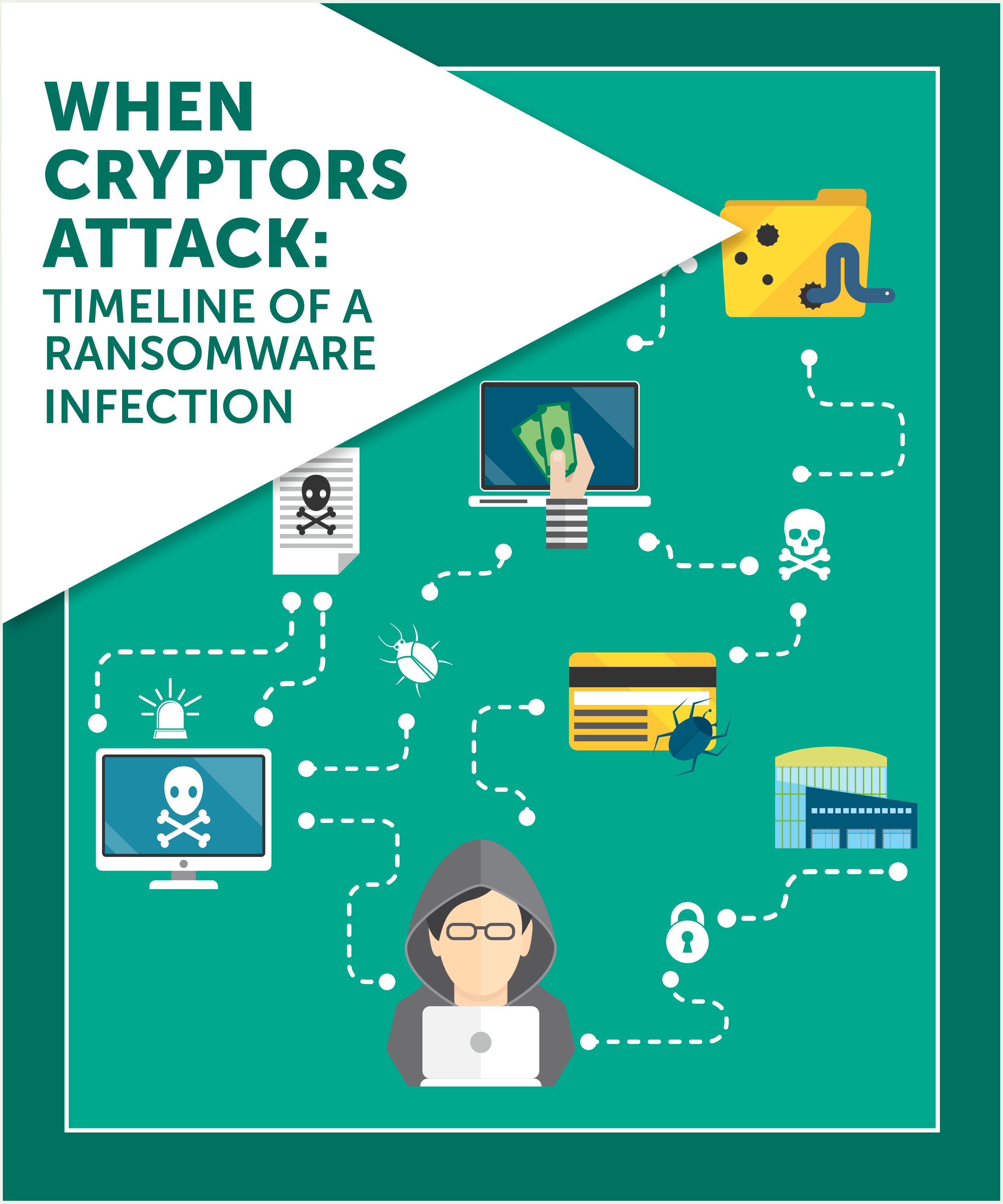
SECURITY SNAPSHOT

WHEN CRYPTORS ATTACK:

TIMELINE OF A RANSOMWARE INFECTION



KASPERSKY lab

HOW BIG A THREAT IS CRYPTOMALWARE TO SMBS?

The total amount of damage caused by cryptomalware can be divided into two parts: the ransom and the related losses. Drawing from our survey of over 4,000 small- and medium-sized companies conducted by Kaspersky Lab and B2B International, we take a closer look at the numbers behind the damage.

49%	SMB representatives who say that they consider cryptomalware to be one of the most serious threats that their organization could face.
$99,000	Average amount of damage to SMBs caused by one cryptomalware attack
1 out of 5	Companies who failed to get back data after paying the ransom
67%	SMBs that report complete or partial loss of corporate data due to a cryptomalware attack

WHAT IS CRYPTOMALWARE?

Cryptomalware is a type of ransomware—the malware that attempts to extract a ransom payment in exchange for unblocking access to your computer, your server or your files. In the case of cryptomalware, the kidnapped assets are the files and data that are stored on the infected device. The malware encrypts the data into an unreadable form, and the data can only be decrypted by using the necessary decryption key—a key that is only released after the victim has paid the ransom demand.

Cryptomalware is a pernicious threat that makes the recovery of your corporate data virtually impossible. Furthermore, there is the added pressure of a time limit, since the ransom must be paid within a matter of days or else all data will be lost.

TIMELINE OF A CRYPTOR ATTACK

How exactly does a cryptomalware attack unfold? We'll walk you through each step of an attack and the action items you can take to prevent it along the way.

1 Perimeter is breached.

Cybercriminals are looking for easy access to your systems, and they can get that access by sending an email with an infected attachment that employees will open. Or they can infect a web site with malware that will use exploit kits to identify software vulnerabilities in the user's PC. This exploit kit then communicates with the PC and loads malicious code onto their computer. Often, this happens without the user ever knowing that they uploaded malicious software.

ACTION ITEM:

Install a robust, multi-layered security solution that continually checks for malware from many different angles in order to protect your system from a breach.

2 Discovery and Panic.

At this point, the IT department discovers that a breach has occurred, and everything comes to a grinding halt. Many questions must be answered. How many computers are infected? Is the server infected? Has data been stolen? Do we have backups that can restore everything to normal and get everything back up and running smoothly?

ACTION ITEM:

For the IT department, this is a bad day at work. No one wants to face the scenario of having computers infected or—even worse—an entire server taken offline. Have a plan in place for steps to take if your company is attacked by a cryptor and has to face this unwelcome scenario.

3 Do we pay the ransom?

Most cybercriminals will demand a payment in bitcoin--a currency that is untraceable by authorities. But keep in mind that one out of every five companies did not get their files back even after paying the ransom.

ACTION ITEM:

We do not recommend paying the ransom for several reasons. In addition to the fact that there is no guarantee that you'll get the decryption key from the cybercriminals, there is also the issue that the ransomware is not your only problem. If paying the ransom is your only option, then it's a pretty good indication that you don't have a disaster recovery plan in place. If this is the case, then you certainly won't be able to remediate from the attack and fully clean your infrastructure from the infection. Finally, all of us have to break the cycle and not feed the cybercriminal machine. If there is no profit to be made, cybercriminals will not continue to develop more ransomware.

4 Downtime and Business Interruption.

Most cryptomalware gives you a time limit to pay the ransom, usually three days. According to our survey, 48% of companies take several days to recover their data. And in that time, 41% report losing a significant number of files entirely if it takes up to a day or more to detect an attack. While all this is happening, normal operations at your company are interrupted. How much of a disruption occurs depends largely on the preventive measures your IT staff took before an infection even occurred. Do you have up-to-date backups? Have you updated and patched your software? Does the rest of your staff know the steps to take to stop the spread of an infection? All of this affects your downtime and your losses in the face of an attack.

ACTION ITEM:
Prepare. Make regular back-ups. Stay on top of software updates and patches. Educate your employees on email best practices.

5 Post-mortem and Forensics.

One of the only good things to come out of an attack is knowledge and understanding. Chances are, you just got a crash course in ransomware and can use that knowledge to prevent another infection.

ACTION ITEM:
You and your IT staff should ask yourself the following questions. What went wrong? How can we protect ourselves in the future? Do we need employee education? What is our weakest point? How can we shore that up? Do the analysis and make the necessary changes.

HOW DO YOU PREVENT A CRYPTOMALWARE ATTACK?

It’s clear that prevention is the superpower that defeats cryptomalware. Here are the 10 steps we recommend to ensure that you can prevent an attack from sidelining your company.

1. **BACK UP YOUR FILES REGULARLY.** The only way to ensure that you can immediately handle ransomware attack is to implement a regular backup schedule so that you don’t have to rely on the cybercriminals to get your systems back up and running.

2. **CHECK YOUR BACKUPS.** There are times when something can damage your files. Be sure to check regularly that your backups are in good shape.

3. **PROTECT AGAINST PHISHING ATTACKS.** Teach employees that they must never open attachments from an unknown sender or even suspicious attachments from a friend in case they have been hacked.

4. **TRUST NO ONE.** Or rather, trust but verify. Malicious links can even be sent by your friends or your colleagues whose accounts have been hacked. If employees receive something out of the ordinary from a friend, they should call that person directly to verify the message.

5. **ENABLE ‘SHOW FILE EXTENSIONS’ OPTION IN THE WINDOWS SETTINGS.** Because Trojans are programs, employees should be warned to stay away from file extensions like “exe”, “vbs” and “scr.” Scammers could use several extensions to masquerade a malicious file as a video, photo, or a document.

6. **REGULARLY UPDATE YOUR OPERATING SYSTEM.** Cybercriminals exploit vulnerabilities in software to compromise systems. With Kaspersky Lab’s automated Vulnerability Assessment and Patch Management tools, your system will be scanned and patches will be distributed regularly in order to keep your system updated.

7. **USE A ROBUST ANTIVIRUS PROGRAM TO PROTECT YOUR SYSTEM FROM RANSOMWARE.** Our Kaspersky Lab products employ a multi-layered system of defense that checks malware from many different angles to ensure that it does not corrupt your system.

But if ransomware hits…

8. **CUT OFF YOUR INTERNET CONNECTION IMMEDIATELY.** If you discover ransomware, shut off your internet connection right away. If the ransomware did not erase the encryption key from the computers in question, then there is still a chance you can restore your files.

9. **DON’T PAY THE RANSOM.** If your files become encrypted, we do not recommend paying the ransom unless instant access to some of your files is critical. Each payment made helps the criminals to prosper and thrive to go on to build new strains of ransomware.

10. **TRY TO IDENTIFY THE MALWARE.** If you are hit by ransomware, try to find out the name of the malware. Older versions of ransomware used to be less advanced, so if it is an earlier version, you may be able to restore the files. Moreover, cybersecurity experts, including Kaspersky Lab experts, collaborate with law enforcement to provide file restoration tools online and, hopefully, detain the adversaries. Some victims are able to decrypt the files without having to pay the ransom. To check whether that’s possible, visit NoMoreRansom.org

TRY KASPERSKY LAB

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

Get Your Free Trial Today >

JOIN THE CONVERSATION

- Like us on Facebook
- Follow us on Twitter
- Join us on LinkedIn
- Watch us on YouTube
- Review Our Blog

ABOUT KASPERSKY LAB

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at usa.kaspersky.com.

Contact Kaspersky Lab today to learn more about Kaspersky Endpoint Security for Business and our other IT security solutions and services:

usa.kaspersky.com/business-security

(866) 563-3099

corporatesales@kaspersky.com

KASPERSKY lab

THE POWER
OF PROTECTION