Malwarebytes

Malwarebytes Endpoint Security vs. Ransomware

Defeating the pervasive threat of ransomware

Ransomware is notoriously difficult to stop. Once it infects devices, its victims face the hard decision of either paying the attackers for a key to unlock the data or forever losing their files.

A Malwarebytes-sponsored global survey of security professionals demonstrates the scale of the business threat. Twenty-six percent of the surveyed organizations were impacted by a ransomware attack during the previous 12 months.[1] Across the industries, ransomware attacks are most common in the healthcare and financial services-related industries, including banking and insurance.

26% of the organizations surveyed
had been impacted by a ransomware attack during the previous 12 months.

The financial costs incurred from ransomware are significant, from either the loss of digital assets or the expense from paying a hefty sum. The FBI says ransomware is now a billion-dollar business, and Cybersecurity Ventures predicts ransomware costs will exceed $11.5 billion in 2019. Globally, nearly 40 percent of ransomware victims pay the ransom.[2]

However, paying the ransom doesn't guarantee you'll recover your data.[3] Globally, nearly 20 percent of organizations that paid the ransom still lost their data. So it doesn't come as a surprise that security professionals are worried, boosting ransomware from fifth to the second-highest concern of all the types of cyberthreats targeting the organization.[4]

Ransomware's economic impact

On top of the financial costs, ransomware poses a safety and economic risk from interruptions to operations. We've seen ransomware cripple businesses: 20 percent of businesses stop operations immediately after discovering a ransomware attack. Hospital emergency rooms forced to turn people away; global shipping and ports experience massive disruption; and even a summer blockbuster movie held up for ransom. The list of victims goes on and on.

Attacking healthcare organizations is easy money for ransomware criminals. According to the Ponemon Institute, healthcare records fetch a high price on the dark web, with individual records commanding around $380. This is because health records often contain credit card data, email addresses, social security numbers, medical history records, and employment information. Ransomware attacks usually deny access to the healthcare organization's systems until a ransom is paid. And in the event it isn't paid, some attackers may threaten to sell PHI on the black market.

One event can have catastrophic impact. Hancock Health knows this risk firsthand. They were hit with the SamSam ransomware in 2018 and had to pay the $47,000 ransom to avoid an interruption in operations.[5]

Why cybercriminals love it

Nothing succeeds like success, and a perfect storm of success factors buoys the rise of ransomware. As Adam Kujawa, Head of Malware Intelligence at Malwarebytes, points out, "The amount of attention that ransomware has been getting from the media is the most accurate danger vs. exposure that we have ever experienced."

In other words, the high incidence of ransomware and the real threat it poses are not media hype. Based on Malwarebytes' own statistical analysis of ransomware drops through malvertising attacks, Kujawa says, "the bad guys are giving up other malware types and adopting ransomware."

Put simply, ransomware is the cybercriminal's weapon of choice because:

▸ **It's profitable, demanding a quick payment that rewards criminals with instant gratification.** Typically, attackers demand payment in cryptocurrencies, such as Bitcoins. Such currencies are mostly anonymous and virtually untraceable, allowing the cybercriminals to launder their ill-gotten gains into their local currency. And just like lawful big businesses, ransomware organizations sometimes offer "customer service," whose helpful representatives walk victims through the process for purchasing a suitable cryptocurrency.

▸ **It's easy to use and getting easier.** Ransomware developed by experienced criminals is finding its way into an online marketplace, offering ransomware as a service (RaaS) for less technically adept scammers. In effect, the ransomware developers are outsourcing their malware to a distribution network of scriptkiddies, so the applications can be deployed in a turnkey fashion in return for a percentage of the take for the original ransomware developer.[6]

▸ **Defending against ransomware is very difficult.** According to a Malwarebytes-sponsored survey of executives in IT-related roles,[7] U.S. respondents were most concerned about malware infiltration through email and browsing. For example, opening an email attachment containing an exploit lets malware take advantage of any weaknesses it finds in common software on the system and delivers ransomware. Malvertising booby-traps ads on reputable websites with malicious code, which can download ransomware even if visitors do not click on the infected ads. Consider that in 2018, Google reported they remove 100 bad ads per second, totaling more than 3.2 billion ads throughout the previous year.[8] In fact, according to Malwarebytes threat researchers, an estimated 70 percent of malvertising campaigns deliver ransomware as the payload.

Fighting back with Malwarebytes Endpoint Security

Most of today's security software offers limited efficacy against ransomware. Ransomware does not act like traditional malware: some forms are automatically updated every day and even use polymorphic (shapeshifting) code to evade detection. This makes it exceedingly hard to detect, especially because traditional and legacy endpoint protection platform solutions use static technologies that rely on signatures that simply cannot spot the evolving behaviors of ransomware activity. In addition, the ransomware seen today is so sophisticated that the advanced encryption it uses makes it impossible to recover files without paying the ransom.

Unfortunately, online and locally connected backup systems can fail as an effective countermeasure, because ransomware actively looks for different types of backup systems and encrypts the saved files. In the case of online backups, automatic file uploads may corrupt files that the user assumes will remain secure.

In contrast, Malwarebytes Endpoint Security is designed to fight—and defeat—advanced ransomware that other security solutions miss. It deploys across business networks and protects endpoints against malware and other advanced threats thanks to a powerful multi-layered combination of proactive signature-less, heuristic, and behavioral technologies.

Also, Malwarebytes Endpoint Security offers another layer of protection against ransomware-based attacks with a new dedicated technology built from the ground up to detect and block all ransomware, known and unknown, from encrypting users' files. This differs from other endpoint security solutions' anti-ransomware efforts, if they exist at all, which typically consist of pieced-together old technology that has already been proven ineffective.

Malwarebytes Endpoint Security breaks the attack chain of ransomware with a four-layered approach:

1. Malwarebytes Endpoint Security's anti-ransomware layer constantly monitors endpoint systems and automatically kills processes associated with ransomware activity. It features a dedicated real-time detection engine that does not use signatures, nor requires updates. Plus, it has a small system footprint and is compatible with third-party security solutions.

2. The anti-exploit layer proactively blocks exploits before they can deliver their malware payload. It wraps vulnerable applications and browsers in defensive layers designed to stop zero-day attacks at inception. Employing signature-less technology that identifies behaviors characteristic of an exploit, anti-exploit can even protect against unidentified malware and ransomware that other technologies cannot perceive because they haven't previously been exposed to them.

3. Malwarebytes Endpoint Security's anti-malware layer employs heuristic and behavioral rules to detect and remove general malware in real-time, so that it cannot execute its code.

4. The malicious website blocking layer stops access toknown and suspected command-and-control servers, so that ransomware cannot obtain encryption keys oraccess and download the ransomware.exe file.

Breaking the ransomware attack chain with Malwarebytes

Here's how Malwarebytes Endpoint Security's technologies block a ransomware attack delivered by malvertising exploit. The best way to explain this is by looking at the various stages of the ransomware attack chain:

1. Profiling → 2. Delivery → 3. Exploitation → 4. Payload Execution → 5. Malicious Behavior
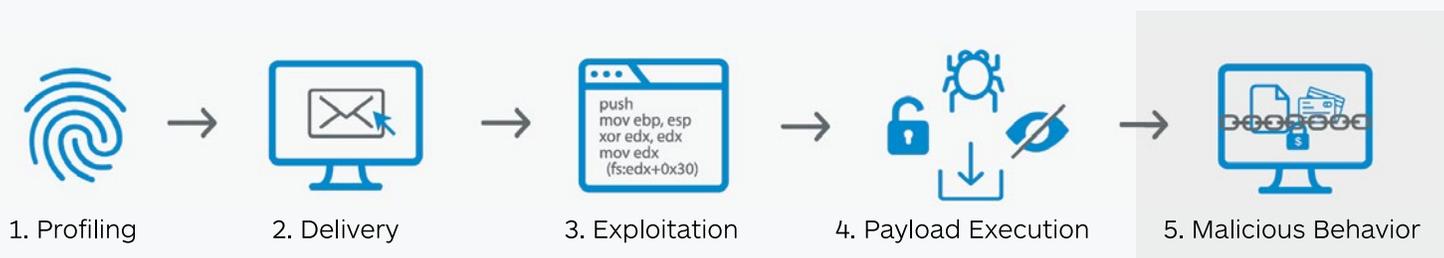
Profiling
The attacker performs reconnaissance on your endpoint via an infected banner ad, trying to identify your OS, browser type, IP address and endpoint security program.

Malwarebytes technology: Application hardening reduces the vulnerability surface, making the computer more resilient, and proactively detects fingerprinting attempts by advanced attacks. (signature-less)

Delivery
How the attacker places their exploit and payload onto your endpoint.

Malwarebytes technology: Web protection protects users by preventing access to malicious websites, ad networks, scammer networks, and "bad neighborhoods."

Exploitation
The attacker exploits vulnerable code in your web browser, Adobe Flash, Microsoft Word, etc., to deliver and remotely execute the ransomware payload.

Malwarebytes technology: Exploit mitigations proactively detect and block attempts to abuse vulnerabilities and remotely execute code on the machine, which is one of the main infection vectors nowadays. (signature-less)

Application behavior ensures that installed applications behave correctly and prevents them from being abused to infect the machine. (signature-less)

Payload execution
The attacker delivers and executes the ransomware payload on your system.

Malwarebytes technology: Payload analysis is composed of heuristic and behavioral rules to identify entire families of known and relevant malware.

Malicious behavior
The ransomware activates on your system. It contacts a command-and-control server to download the encryption keys and then encrypts your files.

Malwarebytes technology: Ransomware mitigation is a behavior monitoring technology that detects and blocks ransomware from encrypting users' files (signature-less). Callback protection prevents access to command-and-control (C&C) servers and other malicious websites.

Summary

As more devices are connected to the vast target landscape referred to as the Internet of Things (IoT), ransomware will pose an ever-greater threat to victims. Especially since experts predict we will continue to observe multiple, new ransomware variants throughout.

Malwarebytes Endpoint Security is an endpoint protection platform that proactively protects your computers against unknown and known threats. Malwarebytes Endpoint Security has added an additional layer of protection against ransomware-based attacks with a unique anti-ransomware technology that automatically monitors, detects, and blocks ransomware before it even touches user files. Besides handling known threats such as Cryptolocker, CryptoWall, or CTBLocker, it defeats new ransomware the moment it is released, proactively protecting users from ransomware that's never even been seen before.

Business customers benefit from Malwarebytes Endpoint Security because it:

▸ Reduces vulnerability to ransomware attack. Automatically detects and blocks unknown and known ransomware, versus just alerting user by means of an automated email that there is an attack, as some security products do.

▸ Blocks encryption in real-time. Stops ransomware before it can get started, eliminating the need for complicated, and often ineffective, decryption tools.

▸ Works against zero-day (previously unidentified) ransomware by employing specialized behavior-monitoring technology that protects from new ransomware that other technologies can't detect because they haven't previously been exposed to them.

▸ Employs a unique design engineered from scratch to defeat ransomware faster and more effectively. Malwarebytes built this technology from the ground up to defend against ransomware. Other anti-ransomware solutions or capabilities rely on obsolete technologies or a collection of repurposed technologies originally built to do something else.

▸ Uses signature-less technology in the anti-ransomware and anti-exploit layers, so protection is even effective against new ransomware that doesn't have a signature yet.

▸ Preserves a business's reputation, allowing it to avoid the public relations nightmare that usually accompanies an attack or breach.

▸ Protects business revenue that would be needed to ransom encrypted data.

WEBSITE RESOURCES

For more information on Malwarebytes Endpoint Security and the new ransomware technology, go to:
malwarebytes.com/business/endpointsecurity/

Latest news:
blog.malwarebytes.com/

References

[1]*Survey published August 2018 by Osterman Research, Inc*
[2]*CyberEdge Group. 2018 Cyberthreat Defense Report. 2018.*
[3]*CyberEdge Group. 2018 Cyberthreat Defense Report. 2018.*
[4]*CyberEdge Group. 2018 Cyberthreat Defense Report. 2018.*
[5]*HealthcareITNews. Hancock Health pays $47,000 ransom to unlock patient data. 2018.*
[6]http://www.techrepublic.com/article/ransomware-as-a-service-is-exploding-be-ready-to-pay/
[7]*Survey conducted June 2016 and published August 2016 by Osterman Research, Inc.*
[8]*Google. An advertising ecosystem that works for everyone. 2018.*

M | 🖥 malwarebytes.com/business ✉ corporate-sales@malwarebytes.com 📞 1.800.520.2796

Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware and exploits that escape detection by traditional antivirus solutions. Malwarebytes completely replaces antivirus with artificial intelligence-powered technology that stops cyberattacks before they can compromise home computers and business endpoints. Learn more at www.malwarebytes.com.