Malwarebytes

Malwarebytes Endpoint Security vs. Ransomware

Defeating the growing 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 recent Malwarebytes-sponsored global survey of IT executives[1] demonstrates the scale of the business threat. Thirty-nine percent of the organizations surveyed had been impacted by a ransomware attack during the previous 12 months. Across the various industries surveyed, ransomware attacks were most common in the healthcare and financial services-related industries, including banking and insurance.

Thirty-nine percent of the organizations surveyed had been impacted by a ransomware attack during the previous 12 months.

The costs incurred from ransomware are significant, either through loss of digital assets or being forced to fork over a hefty sum. Almost 20 percent of all ransomware victims in the survey reported demands that exceeded $10,000. Globally, nearly 40 percent of ransomware victims paid the ransom. In Canada, 82 percent of organizations that opted not to pay ransom lost files as a result.

A December 2015 Senate inquiry to the US Attorney General and Department of Homeland Security Secretary about ransomware attacks revealed that an estimated 234,000 computers were infected with a specific type of ransomware named Cryptolocker.[2] Barely more than 1 percent of the victims paid the ransom, yet the extortion extracted about $27 million from infected users in two months. Another copycat variant of Cryptolocker netted more than $18 million from about 1,000 victims between April 2014 and June 2015.[3]

What's more, the rate of ransomware attacks in the US is escalating. The FBI received complaints for nearly 2,500 ransomware attacks in 2015, which cost victims $24 million. In contrast, in just the first quarter of 2016, ransomware extortions added another $209 million to that toll.[4] Even worse, when victims pay the ransom, the criminals don't always decrypt the files. Plus, according to industry think tank Institute for Critical Infrastructure Technology, there's no guarantee that the system won't get hacked again after a payment[5].

Cyber extortion's human toll

In addition to creating a fundamental economic problem, ransomware can also disrupt important human services. In May 2016, the FBI warned about a significant uptick in ransomware activity that included a series of high-profile incidents against hospitals.[6] According to a report published in eWeek.com, Hollywood Presbyterian Medical Center admitted in February 2016 that it paid a $17,000 ransom to decrypt data infected with ransomware.

Attacking healthcare organizations is easy money for ransomware criminals. The stakes are high for protecting patient care, and hospitals may not have an option besides paying to get their data back. Although much of the ransomware activity goes unreported, a statement from the Health Information Trust Alliance (HITRUST) indicates that some 18 percent of midsize hospitals have been infected with crypto-ransomware.[7]

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 script kiddies, so the applications can be deployed in a turnkey fashion in return for a percentage of the take for the original ransomware developer.[8]
- Defending against ransomware is very difficult. According to a Malwarebytes-sponsored survey of executives in IT-related roles,[9] 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 2015, Google disabled more than 780 million infected malvertising ads. In fact, according to Malwarebytes, 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:

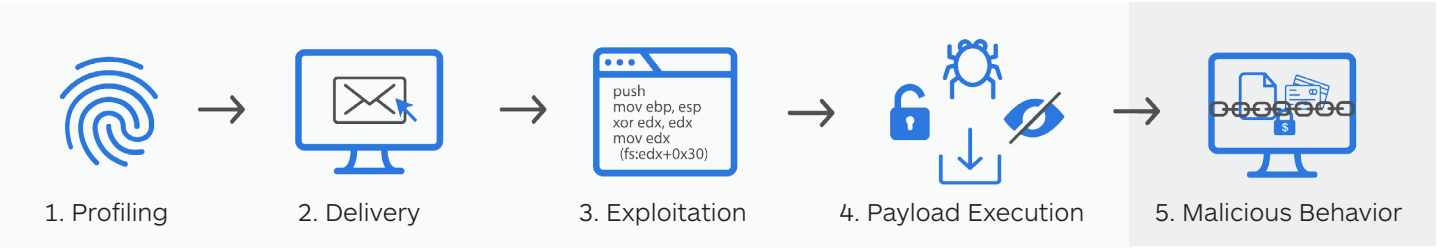
1. Malwarebytes Endpoint Security's anti-ransomware layer constantly monitors endpoint systems and automatically kills processes associated with ransomware activity. It features a dedicated real-time detection engine that does not use signatures, nor

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 to known and suspected command-and-control servers, so that ransomware cannot obtain encryption keys or access 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: The attacker performs reconnaissance on your endpoint via an infected banner ad, trying to identify your OS, browser type, IP address, and your 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)

2. 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."

3. 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)

4. 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.

5. 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/
Request a trial: malwarebytes.com/business/licensing

References

[1]Survey conducted June 2016 and published August 2016 by Osterman Research, Inc
[2]https://www.hsgac.senate.gov/media/minority-media/senators-carper-johnson-seek-information-on-threat-of-ransomware-to-our-nations-cyber-defenses-and-to-the-american-public
[3]Ibid.
[4]http://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746
[5]http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report.pdf
[6]https://blog.malwarebytes.com/101/2016/06/malvertising-and-ransomware-the-bonnie-and-clyde-of-advanced-threats/
[7]http://www.eweek.com/security/ransomware-poses-a-rising-threat-to-hospital-operations.html
[8]http://www.techrepublic.com/article/ransomware-as-a-service-is-exploding-be-ready-to-pay/
[9]Survey conducted June 2016 and published August 2016 by Osterman Research, Inc.

About

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

Santa Clara, CA
malwarebytes.com
corporate-sales@malwarebytes.com
1.800.520.2796