https://securitybrief.com.au/story/ransomware-getting-worse-heres-how-stop-it/
Ransomware is getting worse. Here's how to stop it
13/01/17

January 13, 2017 8AM Shannon Williams

Ransomware is today's most visible and most-talked-about cybersecurity threat. Afflicting consumers and enterprises alike, ransomware has attacked laptops, desktops and servers by encrypting data and destroying backups. These attacks have cost millions of dollars is ransom – that is, untraceable payments to hackers in the hope that they will send a decryption key and allow data to be recovered. Sometimes victims pay the ransom and don't receive the decryption key, or find that the key doesn't work, or even find another demand for even more money.

How is ransomware delivered to the victim? Often by using spearphishing, that is, carefully crafted emails that trick the recipient into opening a malicious document or visiting a corrupted website. From there, malware is installed on the user's computer, and can quickly encrypt data on the user's device and even on network servers. It's bad, and getting worse. Fortunately, a number of leading-edge cybersecurity providers, including Cylance, Javelin Networks, Menlo Security, TrapX Security and Wedge Networks, offer tools that can stop ransomware dead in its tracks.

That's the view from a number of technology experts, said Andrew Braunberg, Managing Director of Research at NSS Labs, a network security consultancy based in Austin, Texas, who pointed out the irony that the United States Federal Bureau of Investigation (FBI) official advises victims

not to pay ransom – but then asks them to report how much they paid. “The FBI says victims should just kind of grin and bear it, but by the way, please send us a little note and tell us how much you pay and all the details about your attack. If you actually did pay to get your data back, they would be curious how much you paid them,ut they would prefer you don't pay at this point.”

Staying Safe Requires Cybersecurity Tools

If you don’t want to be infected, you have two choices: One, ensure that you, your family and your employees are eternally vigilant and never, ever react to spearphishing emails. Good luck with achieving 100% safety. The other is to use cybersecurity tools to protect against spearphishing – blocking those messages before the end user ever sees them.

Once such tool is offered by Cylance, explained Bryan Gale, the company’s Vice President of Product Marketing. “We focus on ransomware specifically. The point in the chain at which we block that is at the endpoint. We're not at the network layer or any other perimeter device whatsoever. One of the things we see with ransomware is the rise of ransomware-as-a-service where anyone can effectively go out and within 10 minutes get a custom crafted binary and payload from a malicious attack at an organization that they choose. That attack is guaranteed to evade defenses from traditional signature-based anti-malware,” Gale explained, because it will only be detected if the vendor’s signature file knows about that specific custom-crafted binary – which might only have been created a minute earlier.

The answer, said Gale, lies in analyzing what actually makes ransomware dangerous, and scanning for that. “By analyzing or extracting the common features within those ransomware variants and being able to predict that something is malicious or not has proven to be very, very successful for us and our customers.”

A Matter of Masked Topology

A different approach is offered by Javelin Networks, which masks the topology of enterprise networks so that attackers can’t get a foothold on servers or other devices.

“Ransomware has become very mature and sophisticated,” said Greg Fitzgerald, Chief Operating Officer of Javelin Networks. “Ransomware isn’t merely encrypting data, locking up an end device and demanding Bitcoins to unlock it. It’s also often siphoning data off that machine and sending it back to the attackers, while trying to gather further information to penetrate other computers on the network. The attacker doesn’t want to just get one machine — he's trying to get to dozens, hundreds, maybe thousands of computers.”

“Javelin automatically and autonomously picks up that movement, or those activities on the host of what it is looking for,” he continued, “such as new credentials, and the details about other machines that it wants to get to. When Javelin sees that activity, it silently alerts IT managers while also locking down that particular machine from the attacker so that that data can't leave, and the attacker can't penetrate further into the organization.”

Menlo Security’s approach to combating ransomware and other malware, including malicious websites, is to ensure that executables are never run on the end-user’s computer. Instead, websites and emails, including attachments, are opened in a cloud-based isolation platform, where threats can be detected and neutralized.

“The Menlo Security isolation platform doesn’t require any endpoint software, and it’s not an appliance,” said Greg Maudsley, the company’s Senior Director of Product Marketing. “We don't make any sort of good versus bad determination, because our assumption is that all websites are bad and all emails are bad. We believe the only way to effectively prevent any end-user from getting infected is to isolate them 100% from any possible threat.”

How is that accomplished? Maudsley explained, “We spawn virtual browsers in our isolation platform in which we fetch and execute all active content and then safely rewrite and transcode only the safe visual elements down to the endpoint. This effectively, by not passing any active content down to the endpoint, insulates the users from ever contracting malware, including ransomware.”

A Vulnerable End-User Computer? It’s a Trap!

TrapX Security uses deception to fight cybercrime, including ransomware, according to its Chief Executive Office, Greg Enriquez. “We shift the cost to the attacker. We put fake networks and fake assets out there, so as soon as the attackers hit the end-user they get directed to a fake shared hard drive or a fake server. When the attacker begins encrypting the fake system, we immediately alert the system that the encryption has begun. You may lose the endpoint, but you won't lose the corporate data or the government database that you're most interested in. We’ve been successful in shifting the cost to the attacker and evolving our approach to stopping ransomware so that criminals can't get what they're after,”

“At Wedge Networks we scan the data and remove threats before they’re delivered to the end-user,” said Frank Wiener, the company’s Vice President of Marketing. “We have two different sets of solutions. One operates at the cloud layer to inspect all data flowing to and from all users at all locations. We're about to introduce our second set of products, which is focused on the enterprise with the same types of capabilities. Both will detect spam, malware and viruses - the types of things that are introducing ransomware.”

Wiener added that the company recently announced a new initiative to bring artificial intelligence into the network layer. “We can use this technology to protect not only the endpoints running AI locally, but also the Internet of Things and other devices that are introduced into the enterprise that might not yet have AI running on the device. By taking the traditional multi-layered approach into the artificial intelligence realm, we expect to raise new barriers to make it more and more difficult for ransomware and other threats to enter end-user devices.”

Who Would Attack a Hospital?

Hospitals and other healthcare organizations have become well-known victims of ransomware, in part because they have many diverse technologies within the facility, and in part because hospitals have been more open with disclosing attacks. One well-publicized example: Kansas Heart Hospital was hit with ransomware and after it paid the ransom, the attackers demanded more money, reported Healthcare IT News on May 23, 2016.

NSS Labs’ Andrew Braunberg asked the question any reasonable human would ask: “When you think about it, who would lock up healthcare records in a hospital? It's just crazy. But it gets to the point of motivation.” He pointed out that not only are ransomware attacks easier to create, but the sophistication of those attacks is increasing. What can be done?

TrapX’s Greg Enriquez admitted that it’s a thorny challenge. “What we've seen with hospitals is that attackers will get in. They will get in through an administrator or through a spearphishing approach. Once they do get in, they will find the most unmanaged and the simplest devices and those could be the medical devices, the blood gas analyzers, the imaging systems, the radiology equipment that's running old versions of Windows that aren’t equipped with current-generation advanced cybersecurity defenses because they're protected by the manufacturers and the FDA. So those are places for the attackers to hide out or dwell with ransomware and other areas” – and therefore look like easy marks, easy way for criminals to make money.

“Ransomware is basically easy money, but it's not just easy money for the cybercriminal that is extorting the money from you,” added Wedge Networks’ Frank Wiener. “Criminals are beginning to commercialize the technology and make it available in the form of ransomware as a service on the dark web. That is lowering the bar for the skillset for cybercriminals to be able to go in and

execute very advanced technologies in terms of breaking in and delivering ransomware. So there is a whole commercialization and, if you will, industrialization that's beginning to happen that's just going to increase the amount of activity on this front. So the value and the effort being lower, that's an interesting set of drivers for the increase in cyberattacks."

Menlo Security's Greg Maudsley agreed that ransomware attackers are taking advantage of the inherent and increasing vulnerability of today's Internet. "You and I as users of the Web demand a rich experience. We want scrolling videos. We want all kinds of interactive content. In order to do that, today's most popular websites have to pull from dozens of different other domains all over the world. They have no control over the OS that those other domains are running and in many cases they're running very, very old operating systems with known vulnerabilities. It's not enough to simply compromise or install a drive-by attack on a site. You can go to a background domain which is much easier to compromise and that's what they're taking advantage of in a large number of ransomware attacks today."

Who Ate My Cheese?

Cybersecurity is a cat-and-mouse game, believes Javelin Networks' Greg Fitzgerald, and the mouse — the attacker — has been winning for a long time. Maybe it's time for that to change? "With all the technologies you've got we're finally trying to give power back to the cat. The idea is to let the mouse get the cheese, but don't let him get the entire block. Let the mouse get a little crumb because trying to prevent the entire cheese block from getting eaten is much easier than it is to allow them to have nothing."

Why? "The mouse is going to get into the network in some way, shape or form," insists Fitzgerald, "whether it's through malware, or whether it's through credential stealing, or even a rogue employee. They'll get in – so let's control the situation, and control the damage."

The value of the stolen cheese can be pretty high, explained Cylance's Brian Gale. "A recent report highlighted one single ransomware platform, syndicate, whatever you want to call it, that brought in nearly $121 million of revenue in the first half of 2016 alone. That's about a quarter of a billion dollar run rate as a ransomware platform." The report, the McAfee Labs Threat Report, was published September 2016.

Gale added that for their customers, "the hackers built an admin console, they provide support, and they guarantee the binaries will evade detection. This is entirely financially motivated and way too easy for anyone to go create a custom package and attack an organization today." Ignore Big Ransomware at your peril, he warned.

Thankfully, with companies like Cylance, Javelin Networks, Menlo Security, TrapX Security and Wedge Networks, enterprises can tackle the ransomware danger head-on.