WEI INSIGHTS TECH BRIEF

USING NETWORK SEGMENTATION TO MANAGE MALWARE AND RANSOMWARE RISKS

Focused on efficient management of networks and privileges, many enterprise IT teams are not designing networks in a way that will effectively contain the damage of a ransomware attack or other breach. An increasing number of enterprises and individuals have been facing the unsavory decision of whether to pay a ransom in order to regain access to their own files.

The number of ransomware attacks more than doubled between 2013 and 2014, according to Symantec's 2015 Internet Threat Report and other reports, and that trend is expected to continue through 2016. In addition, ransomware innovations are emerging such as "ransomware-as-a-service" (RaaS); the ransomware vendor typically charges the attacker a percentage of the ransom, for instance 25%, with no upfront charge. In January 2016, researchers identified a new RaaS called **Ransomware32** with a user-friendly dashboard to track income statistics and manage individual attacks. By removing the upfront cost and technical barriers, the RaaS trend is making ransomware accessible to the less technical hacker (known as a "script kiddie").

While other types of malware attempt to steal data, ransomware blocks access to systems or files, typically through encryption, until a payment is made. Hackers have been attacking personal computers with ransomware for years, for a typical ransom of $300. Now they are focusing on enterprises, for much larger payouts. While the value of ransoms for enterprises is not publicized, stories about victimized police departments and other public-sector organizations began emerging in 2015. For instance, an attacker demanded $125,000 in equivalent Bitcoin from a school district in New Jersey. FBI agents responsible for investigating reported ransomware incidents note that paying the ransom is the most reliable way of recovering the data held hostage.

HOW RANSOMWARE WORKS

Ransomware typically enters a device through some sort of phishing scam. An attacker tricks a user into a bad electronic move by behaving like a trusted party.

Ransomware blocks access to systems or files, typically through encryption until a payment is made.

The most common phishing scams are the phishing email and the phishing website. Once the user unknowingly downloads a piece of malware software, the attacker expands from there to explore resources and, in enterprises, may attempt to move laterally to explore the network and encrypt shared and network drives. Both Crypto and CryptoLocker have this capability, according to the United States Computer Emergency Readiness Team. In 2015, a researcher known on Twitter as @kafeine discovered CryptoFortress, a ransomware variant that even encrypts unmapped shared network drives; prior ransomware only encrypted network shares that were mapped to a drive

WEI

letter. Because the threats are evolving, enterprises must evolve in responding to threats.

Any technique an enterprise uses to avoid phishing scams will help avoid getting ransomware. However, there is no way to guarantee that an enterprise can avoid infection. Therefore, in addition to prevention, every enterprise needs to consider how to contain a ransomware breach with network segmentation, clean backups, and other strategies once the attacker penetrates first-line defenses.

CONTAIN THE BREACH WITH NETWORK SEGMENTATION

The objective with security-minded network segmentation is to ensure that attackers have access to as few digital resources as possible. This technique also will help contain the damage of other types of attacks. Network segmentation, in part, limits the volume of resources that an attacker can access. Segmentation is the process of logically grouping network assets, resources, and applications together into compartmentalized areas called segments and allowing only approved types of communication in and out of the segment. Segments that are physically separated from other segments and have no established trust to allow interaction are known as segregated. For example, devices involved with financial transactions should be fully segregated both logically and physically from devices that can surf the web.

Since departments and teams have different access needs, an enterprise divides a network into segments and then controls each segment's communication to the outside world. In addition, the enterprise should control communication between segments of the same network. With limited access between segments, an attacker's movement to another segment is either stopped or slowed enough to allow monitoring tools to alert enterprise staff to the intrusion before massive harm is done.

To secure a segment, an enterprise would simply prevent all communication and physical access, which in part includes emails, websites, file sharing, cloud services, and any external devices such as storage or mobile devices that have both external access and access to the network. Of course, such restrictions aren't generally feasible.

On the other hand, an enterprise inadvertently makes life easier for hackers with what FishNet Security describes as an "**egg network,**" a network that, like an egg, has a "strong perimeter surrounded by their soft, gooey, defenseless (data) yolks." Such organizations have false confidence in outward facing firewalls and other tools that protect the network's external perimeter while liberally allowing internal communication between network segments. An attacker who stumbles into such liberal access would be able to block and ransom large volumes of enterprise electronic resources.

Often, an enterprise ends up with an egg network when business needs override security concerns on an ongoing basis. For instance:

- A network that has less complicated segmentation requires less skill and less effort to manage, which results in lower costs. For instance, to ease management, an enterprise may have a secondary management network or backup network that spans network segments rather than implementing a more secure strategy, forcing this traffic through security software that inspects traffic.
- Enterprise tools are often selected on the basis of business needs with security as an afterthought. After a tool is selected, businesses ask, "How can we best secure this?"
- Vendor implementation teams known for quality business implementations may not have security expertise to advise enterprise teams on best practices.

ADDITIONAL CONSIDERATIONS FOR CONTAINING RANSOMWARE

Sometimes an enterprise doesn't recognize its IT staff's lack of security knowledge. They don't know what they don't know. "I think fundamentally, a lot of people don't fully understand what it means to segment," said Jerry Bell on the August 2, 2015 **Defensive Security Podcast.**

"I can't tell you the number of times I've seen shock and horror when people have realized that an attacker has crossed from one network to another where they thought segmentation existed," said Andrew Kalat on the same podcast episode.

Enterprise IT teams should additionally consider their network backup strategy. "The best line of defense against any ransomware is to have backed up your machines yesterday," said **Kaspersky Labs.** "Some ransomware variants are smart enough to also encrypt every backup they are able to locate, including those residing on network shares. That is why it is important to make 'cold' backups (read and write only, no delete/full control access) that cannot be deleted by the ransomware."

In summary, enterprises should ensure that their approach to network management reaches beyond efficiency and considers how best to use segmentation to thwart attackers. Enterprises should confirm that staff members who are responsible for segmentation truly understand the security implications of the segmentation architecture. Business areas that are responsible for selecting software should draw security and IT resources into the conversation before a solution is selected and should ensure that the vendor's implementation team has a strong background in the security of the software being purchased.

TALK TO WEI TODAY

Our security experts want to answer your toughest questions. We can assess your current networking environment to identify any gaps in security and can help your company develop a proactive, comprehensive plan for the prevention and containment of ransomware.

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 25 years.

WEI Dedication meets innovation.

info@wei.com
www.wei.com
43 Northwestern Drive | Salem, NH 03079
800.296.7837