5 Ways to Protect Your Organization from Ransomware and Sleep Well at Night

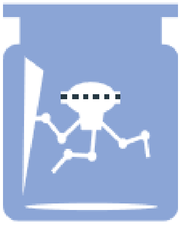
BUFFERZONE

Part 1: The Story of Ransomware

Why Ransomware is King: Where it Came From, Where It's Going

While it's been making headlines over the past year, ransomware has actually been around for over a decade. Seen first in Russia in 2005, the early ransomware variants used scare tactics to extort payment, with varying degrees of success. Then crypto-ransomware was invented.

Encrypting files proved a very effective means of extorting payment from a wide segment of the population. Cryptolocker, the most widely used form of cryptoransomware, first appeared in 2013[i], and quickly picked up speed. In fact, Crypto-ransomware rose to 83%[ii] percent of overall ransomware use in 2015. In 2015 Crypto-ransomware surpassed botnets[iii] as the most popular attack method of choice for cyber-criminals. Cryptowall was the most frequently used variant, arriving on users' computers via email or malicious downloads.



Another reason why ransomware has taken off is because it's so easy for hackers to use. It is part of the Angler exploit kit, which enables any criminal, even those without any technical skill, to start a ransomware campaign. Thanks to its "hacker friendly" approach, Angler became the most frequently used exploit in 2015[iv].

And last but certainly not least, ransomware pays. Only a small percentage of victims need to pay up for hackers to earn a tidy profit. Consider this data from Cisco: In 2015, they monitored Angler campaigns that hit 90,000 targets per server per day. 10% were served exploits. Of those served exploits, 40% were compromised and 62% of those were served ransomware. Though only a small fraction paid the ransom (2.9%) and each instance was a few hundred dollars, that still added up to $34 million per ransomware campaign over the course of a year[v].

How Ransomware Works

While there are now many ransomware variants, they have many common traits. Generally they penetrate an organization using a browser exploit like a drive-by download or through an infected file delivered by email or removable media. Now that targeted ransomware attacks are on the rise, hackers are combining those methods with more sophisticated forms of social engineering to ensure their success.

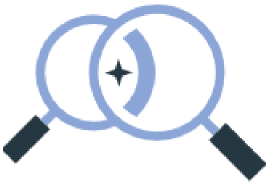
Once inside the organization, they take evasive action. Some use obfuscation and covert launch mechanisms to try to avoid detection by antivirus, while others go so far as to kill the antivirus running on the endpoint. In order to stay hidden, they use obscure filenames, modify file attributes, or run as a part of legitimate programs and services. They use privilege escalation techniques to gain administrator access to the endpoint and often make themselves persistent by installing themselves in the Startup directory.

Before encrypting files, ransomware contacts a command and control server (C&C) to obtain a public key and bitcoin address. To make their network traffic harder to analyze, they encrypt the request as well. The malware then encrypts the files and displays a message to the user with the bitcoin address and payment instructions. In many cases, when the ransom is paid, the user receives the private key and can unlock the files. But there have been many cases where the key was never sent – the hackers have moved on, or are simply malicious.

The Many Flavors of Ransomware

Ransomware is evolving rapidly with new variants emerging every few weeks. A quick look at some of the campaigns that have made headlines this past year highlight a few of the destructive trends that are unfolding.

- **Cryptorbit**[vi] only encrypts the first part of the file and appends it to the end making restoration from a backup ineffective.
- **TeslaCrypt Ransomware.42** was linked to a series of advertisement attacks[vii] striking prominent sites such as The Independent newspaper.
- **Cryptowall 3.0**, a recent incarnation of the famous malware, utilizes C&C servers, spammed messages, spyware, and compromised websites as modes of infection.
- **TeslaCrypt 3** allows criminals to generate a different "key[viii]" for each victim. If one victim pays the ransom and gets the file decryption key, it is only valid for their machine.
- **Locky** was blamed[ix] for the recent £2.4 million ransom attack on a Hollywood hospital and has been sited repeatedly by malware researchers since.
- **Not only Windows, Mac too - KeRanger**[x] secretly encrypts all your data after three days of lying dormant.



Part 2: How to Protect Your Organization Today

1. Prevent Infection from Email Attachments

Infected email attachments are one of the most prevalent attack vectors for ransomware. Users are tricked into opening a file that appears innocuous, but actually downloads or executes malware. Microsoft Word macro malware in particular has made a strong comeback this past year, but it's easy for hackers to hide malicious code in any file.

Educate

As more targeted attacks deploy ransomware, infected attachments will be harder to avoid. Social engineering has proven highly effective at deceiving even relatively cautious employees, by using tactics such as address spoofing to mislead recipients about the sender. Nonetheless, employee education is very important and can prevent a large percentage of opportunistic attacks. It is recommended to organize a lecture or provide an online resource that tells employees what to look out for.

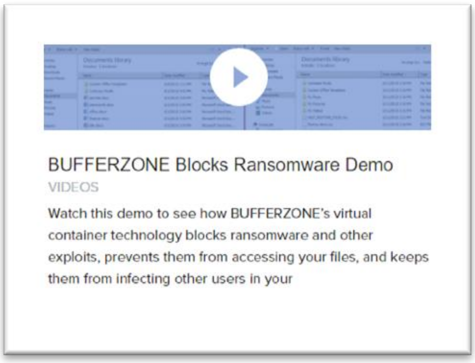
Update Security Software

As we saw earlier, once a form of ransomware goes up for sale, many hackers start using it. You can avoid infection by known variants of ransomware simply by keeping your antivirus and email protection software up to date. This will not protect you against the next new threat, but it does eliminate a large number of simpler, opportunistic threats.

Block Known and Unknown Ranswomare with a Virtual Container

BUFFERZONE opens and runs email attachments such as Microsoft Office and PDF files in a virtual container. The container is a 'safe zone' on the computer that is isolated from the user's actual file system, memory, registry and network. So if the file contains ransomware, it's trapped inside the container, where it cannot do any real harm.

When any application running inside the virtual container wants to read a file, BUFFERZONE copies it into the container. In the case of ransomware, as it tries to access files to grant itself write permission and encrypt, BUFFERZONE copies them into the container, where the ransomware encrypts the copies. The original files are untouched. When the user receives the ransomware notice, it's a simple matter to wipe the container clean – deleting both the encrypted files, and the malware itself.



BUFFERZONE Blocks Ransomware Demo

VIDEOS

Watch this demo to see how BUFFERZONE's virtual container technology blocks ransomware and other exploits, prevents them from accessing your files, and keeps them from infecting other users in your

2. Prevent Infection via Web Browsers

After email attachments, web browsers are the most common attack vector for ransomware. Many exploit kits leverage zero-day flaws in popular browsers and plug-ins such as Java and Flash to deliver malware to the unaware user. Drive-by downloads and malvertising attacks download malware when the user simply visits a web site. Since malvertising in particular has affected even the most respectable sites, education is not very effective in preventing this sort of attack.

Update Browsers and Extensions

Zero-day exploits take advantage of bugs in browsers and plug-ins that have yet to be discovered and patched by the vendor. Many experts advise against installing plug-ins like Java if they are not strictly necessary. Flash, in particular, has been heavily exploited and is growing obsolete, so it is probably wise to remove it.

But even if you reduce the risk from plug-ins, zero-days flaws will always be present in browsers and essential applications like Acrobat. Vendors release patches as soon as they discover weaknesses, so it is essential to keep your browser and desktop applications up to date.

Block Web-Based Ranswomare with a Virtual Container

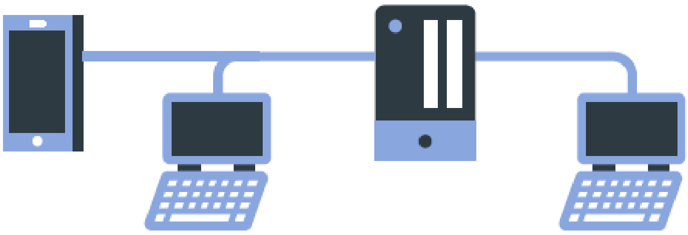
BUFFERZONE isolates web browsers in a virtual container. If a user accidentally downloads ransomware via a drive-by download or zero-day exploit, it will not be able to encrypt the users' files or spread laterally to another computer on the network.

BUFFERZONE's virtual container prevents malware from accessing the file system, memory, registry and network. When the user receives the encryption notice, it's a simple matter to wipe the container clean and delete the malware. All of the original files are safe.

3. Prevent Infection via Phones and Thumb Drives

Last, but not least, pay attention to smartphones, thumb drives, and other removable storage devices. If your organization does not block the use of external devices, ransomware can easily penetrate the organization via on an innocuous-looking smartphone.

With BUFFERZONE, you can enable employees to safely view and open files on removable media without putting the organization at risk. BUFFERZONE's virtual container isolates the removable device and any applications used to open and view files from the rest of the endpoint, so if any malware is downloaded, it is unable to access the actual resources of the endpoint or the network.



4. Reduce the Sting: Keep it from Spreading

Until recently, ransomware generally infected a single endpoint. So in the very worst case, both the damage and the downtime were limited in scope. However ransomware attacks are growing more sophisticated and according to a recent warning from the FBI, they are starting to spread laterally throughout the network.

Network Segmentation Limits the Spread of Ransomware

It is more important than ever to ensure that malware cannot move freely throughout the network. Most security standards recommend network segmentation to prevent any non-essential access to the most sensitive resources. Unfortunately, since using firewalls to segment the network is fairly complex to manage, many organizations choose not to go this route. Furthermore, ransomware can still wreak a great deal of havoc on a single network segment, as it encrypts and eventually destroys files on every file system it can access.

Network Separation Prevents the Spread of Ransomware

BUFFERZONE provides network separation to ensure that ransomware cannot spread throughout the network, regardless of whether it entered via email, web browser, or external media. As we explained in the previous section, BUFFERZONE isolates at-risk applications in a virtual container. Applications inside the container can access the internet, but they cannot access the internal network. So if malware enters the container, it cannot move laterally throughout the organization.

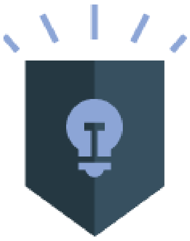
5. Limit the Risk: Backup Wisely

Ransomware is simply another reminder of why any well-run organization should back up data daily and have a disaster recovery procedure in place. In some cases, if ransomware does get in the door, recovering files from a backup will make sense. In other cases, a simple ROI analysis will show that the cost of the work that was lost between backup intervals is higher than the cost of the ransom. But keep in mind that even if you pay, sometimes you will not receive the decryption key.

It's important to do a forensic analysis and understand the source and time of the infection before backup to ensure that you do you restore the ransomware as well as your files. It is also important to get to the root cause so you can verify that the infection is not present anywhere else on your network.

Conclusion: An Ounce of Prevention is Worth a Pound of Cure

With the number of breaches growing each year, some have come to the conclusion that preventing threats is impossible. Much of the focus in cyber security has turned to trying to detect threats after they occur, rather than trying to stop them at the door.



The rise of ransomware has demonstrated the high cost of giving up on threat prevention. Detecting ransomware once it's started encrypting files is simply too late. As ransomware grows more sophisticated - targeting shared drives and moving laterally – so does the cost of cleaning up the mess.

Fortunately there is a way to block ransomware. BUFFERZONE's virtual container isolates the most common attack vectors – email, web browsers, removable storage – along with any malware that enters the organization. Regardless of whether the threat is old or new, known or unknown, opportunistic or targeted, it will be trapped in the virtual container, where is cannot ransom your files or spread throughout the network.

See for yourself. Contact us to being a trial of BUFFERZONE today.

[i] http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-101-what-it-is-and-how-it-works

[ii] http://www.scmagazineuk.com/out-with-botnets-crypto-ransomware-king-of-cyber-crime-attack-modes/article/481964/?DCMP=EMC-SCUK_Newswire&spMailingID=13943208&spUserID=MjMzNTk2MjAxMwS2&spJobID=740796478&spReportId=NzQwNzk2NDc4S0

[iii] http://www.scmagazineuk.com/out-with-botnets-crypto-ransomware-king-of-cyber-crime-attack-modes/article/481964/?DCMP=EMC-SCUK_Newswire&spMailingID=13943208&spUserID=MjMzNTk2MjAxMwS2&spJobID=740796478&spReportId=NzQwNzk2NDc4S0

[iv] http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-101-what-it-is-and-how-it-works

[v] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwi8h8-E7obMAhVItRoKHe8gAfwQFgg0MAQ&url=http%3A%2F%2Fwww.techrepublic.com%2Farticle%2Fciscos-2016-security-report-attacks-getting-stronger-defender-confidence-dropping%2F&usg=AFQjCNEd83WKwDqAAdmuGPSRHrArNGFJCA&bvm=bv.119028448,d.bGs

[vi] http://themerkle.com/bitcoin-ransomware-education-cryptorbit/

[vii] http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-101-what-it-is-and-how-it-works

[viii] http://www.fierceitsecurity.com/story/ransomware-has-become-black-plague-internet-warns-cisco-talos-team/2016-03-17?utm_medium=nl&utm_source=internal&mrkid=%257B%257Blead.Id%257D%257D&mkt_tok=3RkMMJWWfF9wsRokuK%252FIde%252FhmjTEU5z17%252BklXKOzhokz2EFye%252BLIHETpodcMSsZqMrHYDBceEJhqyQJxPr3HJdQN18R7RhHnDg%253D%253D

[ix] http://www.scmagazineuk.com/locky-ransomware-on-the-rampage-globally/article/481656/?DCMP=EMC-SCUK_Newswire&spMailingID=13921767&spUserID=MjMzNTk2MjAxMwS2&spJobID=740632852&spReportId=NzQwNjMyODUyS0

[x] http://www.cultofmac.com/416299/stealthy-malware-will-hold-your-mac-ransom/