Q&A Session for Malware Sessions: Ransomware-Locky (APAC/JP)

Q: does this way block access to word.exe to access online templates or document on sharepoint website?

Priority: N/A-

Answer: Yes, this would interrupt some external functions of word.exe making outbound TCP Port 80 request. For HIPS, you could configure Firewall rules to allow WINWORD.EXE to connect to Trusted Network (specific online templates or SharePoint server) and block the rest of access.

Q: Would you please share the rules details of VSE, ENS and HIPS to prevent the Locky? So our clients can do these rules in their real environment.

Priority: N/A-

Answer: Please refer to PD25203

Q: Update on Cryptxxx ransomware?

Priority: N/A-

Answer: Yes, we are seeing CryptXXX events as the latest ransomware. after Locky campaign. Definitely under consideration for creating content for it for future PD25203 release.

Q: Is mcafee including all the rules for ransomware in products by default configure rule every time is tedious taks so just one can enable the required rules.?

Priority: N/A-

Answer: Currently this is not the case. I would suggest submitting a PER (Product Enhancement Request) via product support channels.

Q: Would you see a possibility of a more evolved ransomware? A more advanced and sophisticated ransomware? If yes, please share your views on it and how it may be advanced.

Priority: N/A-

Answer: Yes, for further information please visit IsEcG Labs blog for further Ransomware information, along with how it's expected to evolve.

http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

"Although a few families—including CryptoWall 3, CTB-Locker, and CryptoLocker—dominate the current ransomware landscape, we predict that new variants of these families and new families will surface with new stealth functionalities. For example, new variants may start to silently encrypt data.

These encrypted files will be backed up and eventually the attacker will pull the key, resulting in encrypted files both on the system and in the backup. Other new variants might use kernel components to hook the file system and encrypt files on the fly, as the user accesses them."

Q: Hi Sean....As per my understanding, we can safeguard our computers from this kind of attach. But, can't we disinfect the compromised files or system.

Priority: N/A-

Answer: Please visit IsEcG Labs blog for “Advice for Unfastening CryptoLocker Ransomware"

https://blogs.mcafee.com/business/advice-unfastening-cryptolocker-ransomware/

"The most frequently asked question about ransomware is “Can we recover the encrypted data?” The answer is generally “No”—unless you pay the ransom and the thieves provide the private key. Ransomware private keys are stored on the criminals’ servers and unless you have access to that server or a copy of it, there is no other way to obtain the private key.

Occasionally, a law enforcement agency executing a takedown is able to seize the ransomware campaign’s control server. If officials can gain access to the database containing the private decryption keys, an encrypted file recovery tool can be built. Recently, the Dutch National High Tech Crime Centre seized the control server commanding the CoinVault ransomware family. Working together with Kaspersky, the Crime Centre created a recovery tool.

In some instances, files can be recovered. If the Windows System Restore option has been turned on (the default for most systems), then files can be recovered from the shadow volume copies. The shadow volume copy service, also known as VSS, is a technology that performs manual or automatic file backups, even when files are in use. From Windows XP through Windows 7 and Windows Server 2008, it is implemented in the Volume Shadow Copy service.

For Windows 8, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, the built-in command “Vssadmin list shadows” will list the available copies for the given volume. There are various ways of mounting a VSS copy through the command line and browsing for the files. There are also a variety of open-source tools that can be used to browse volume shadow copies. It may be possible to restore ransomware-encrypted files using one of those tools."

Q: Is mcafee including all the rules for ransomware in products by default configure rule every time is tedious taks so just one can enable the required rules.?

Priority: N/A-

NOTE Duplicate Question – Answer: Currently this is not the case. I would suggest submitting a PER (Product Enhancement Request) via product support channels.

Q&A Session for Malware Sessions: Ransomware-Locky (NA/LTAM/EMEA)

Q: Is there a reason these rules aren't suggested for HIPS? HIPS has more flexibility to exclude false positives.

Priority: N/A-

Answer: Any VSE/ENS rules can be applied to HIPS which would achieve the same goal. HIPs does offers more granular & flexibility when it comes to custom rules. For more information, Please refer to PD25203

Q: if the administrator user has been renamed to any other name, will it search for the local admin or fail?

Priority: N/A-

Answer: Crypto\Ransomwares can inject into system processes such as svchsot.exe and explore.exe obtaining elevated rights. Other will use logged on user accounts.

Q: On the slide showing the notepad window the bullet point read "Files created _HELP_instructions.txt" however the notepad window itself read "_Locky_recover_instructions.txt". Which is the valid filename created by the malware?

Priority: N/A-

Answer: This was done to provide a cleaner help\recovery instructions for Locky. The one executed in the "Symptoms and Characteristics" video had a poorly displayed\coded version. They both are written to achieve the same results with decryption instructions and payment methodology

---

Q: Does the block creation of new files, also block the "rename" operation i.e a new file is not being created, but a current file is being renamed ?

Priority: N/A-

Answer: Yes, If you block creates, then you'll prevent renames as well

---

Q: can HIPS DNS Blocking policy be used to block all traffic to .onion and .tor? would that work?

Priority: N/A-

Answer: No. Tor client do not directly do DNS requests. It is the exit node perform the DNS resolve and open a TCP connection to the target.

____

Q: Does the endpoint need to be on a network server to prevent the encryption of mapped drives? I imagine it does, but would the endpoint on the client PC be sufficient?

Priority: N/A-

Answer: The preventative measure is based on client PC endpoint.

____

Q: How about volume shadow? Is it still deleted or Access Protection kill the chain

Priority: N/A-

Answer: In the case of the Ransomware-Locky video, the shadow volume copies were deleted, as Access Protection prevented the encryption routine and not the Locky installer specific IOC's, i.e. shadow volume copies deletion, Locky cleanup routine, help instructions, etc. However, by blocking prevalent installer location(s) from creating, executing, writing, etc, this would prevent shadow copies from being deleted, as the installer executed payload it interrupted. These locations can be found in PD25203

____

Q: is there anyway we can block Volume shadow delete with AccessProtection rule?

Priority: N/A-

Answer: In short yes, but something that would need to be thoroughly configured, by not allowing access to vssadmine.exe and creating exclusions based on testing in report-only mode, till all "false triggers" were found\excluded.

____

Q: As i know new ransome ware use radmon extension. What prevent this?

Priority: N/A-

Answer: There are many ransomware that utilize randomly generated extension. Please refer to PD25203 for preventative measure.

____

Q: In endpoint security what is the diff between "Create" and "Write" *.locky files

Priority: N/A-

Answer: Create prevents any new files from arriving (being created) on disk to that location. Where writes are preventing an application to writing to a file in that location.

____

Q: Why aren't the Host IPS rules to mitigate this added to Host IPS content updates? Even if disabled allowing us to configure better after the fact.

Priority: N/A-

Answer: I would suggest submitting a PER (Product Enhancement Request) via product support channels, as this would need to come from product development.

Q: Can you provide AV Access Protection Rules, Firewall Rules and HIPS Signatures discussed to customers, rather than each customer having to create them.

Priority: N/A-

Answer: I would suggest submitting a PER (Product Enhancement Request) via product support channels, as this would need to come from product development. However, please refer to PD25203 for other preventative measures for Cryptos\Ransomwares

---

Q: Is the rule set in ePO for HIPS generic enough to minimise the impact of *all* zero day ransomware?

Priority: N/A-

Answer: Yes. The HIPS rule is generic enough to minimize the impact of file based zero day ransomware. The Cryptolocker rule would prevent untrusted application from modifying the protected file extension. Sig set 6010 & 6011 would prevent untrusted application from injecting itself into trusted application process.

Q: Have you seen any ransomeware encrypt files other than local and network drives? For example sharepoint, watchdox etc.

Priority: N/A-

Answer: Yes. Ransomwares can also infect unmapped network drives, USB stick, Dropbox and OneDrive connected folders.

Q: Can Access Protection rules be distributed via DAT file updates?

Priority: N/A-

Answer: Yes, AP rules can be updated via DAT. The vscan.bof file is VSE's content file, and can be carried by the DAT themselves or as their own content package to check into the repository. Normally though, we just include the vscan.bof with each of our patch releases. Keep in mind that the default built-in AP rules can be updated via DAT, but not the custom User-Defined AP rules create by the user.

Q: will this also prevent service accounts using things like SCCM from running legitimate installs using the systems %temp% folder?

Priority: N/A-

Answer: Yes, this is very possible. This is why we suggest to always first run in report-only mode and add exclusions based on findings. You can push a first run out to trusted set of individuals and create exclusions based upon "false triggers". Then hit a large group and so on, until exclusions have been added.

Q: Will the slides be made available from this presentation? Does Mcafee over prebuilt HIPS rule organizations can use as a baseline? Set to Report Only initially

Priority: N/A-

Answer: Presentation will be posted in conjunction with the QA section, but slides won't be made available. The HIPS 6010 & 6011 Sig is available, the Cryptolocker rule set will need to be created manually. The Cryptolocker rule set is available for download here: https://community.mcafee.com/docs/DOC-6553

Q: it would be good to have such rules proactively available in a next version of ENS - downloadable

Priority: N/A-

Answer: Currently this is not the case. I would suggest submitting a PER (Product Enhancement Request) via product support channels.

Q: What are some good resources to learn more about HIPS rule configuration?

Priority: N/A-

Answer: Please refer to PD25203 for Crypto\Ransomware related HIPs rules. However, "Appendix A – Writing Customer Signatures and Exceptions" from HIPS 8.0 Product Guide is a good starting point.

Q: can you cover exceptions to the AP rules?

Priority: N/A-

Answer: Please refer to PD25203

Q: also Hips rule exceptions?

Priority: N/A-

Answer: Please refer to PD25203

Q: Is there any instructions documentation from what we went over on this Webinar?

Priority: N/A-

Answer: The information provided in this presentation can be found in PD25203 which includes other Crypto\Ransomware preventative measures, as well

---

Q: What recommendations do you have for creating and automating containment groups?

Priority: N/A-

Answer: Can you please reword your question in the "Comments" section, as I am not sure what sort of containment group and product usage, you are looking for. Thanks!

Q: Can you execute both methods then for blocking locky? HIPS & VSE without issue? ALso, HIPS can provide addiitonal protection against other crypto threats because it protects the files extensions themselves, correct?

Priority: N/A-

Answer: Yes, VSE and HIPs can run simultaneously and achieve similar results, depending on the rule(s) configured. It's always suggest to thoroughly test all rules prior to enabling\set to block.

Q: What's the best way to set up a test box for malware execution testing like you did and ensure it is isolated from our corporate network?

Priority: N/A-

Answer: While we may not be able to give advice on this, there are many online resources available for setting up isolated environment for malware analysis.

Q: Can Locky delete shadow copies on network shares?

Priority: N/A-

Answer: Not at the moment, with current Locky variants in the wild. Subject to change any new variant release

---

Q: I missed the first 5 minutes of the presentation. Is the .locky the most prevelant ransomware attack at the moment? Are there other common Ransomware vectors?

Priority: N/A-

Answer: Ransomwares come in various waves. While Locky is a prevalent variant, new variants come daily, changing the landscape often. Please refer to PD25203 for preventative measures for Crypto\Ransomwares

---

Q: Have you more informations according to McAfee ENS?

Priority: N/A-

Answer: Please refer to PD25203 for ENS preventative measures for Crypto\Ransomwares

---

Q: We have Seen Many Crpto locker variants do you recommend any rule in HIPS?

Priority: N/A-

Answer: Please refer to PD25203 for HIPs preventative measures for Crypto\Ransomwares

---

Q: with access protection rule with block *.locky files I can prevent that my files are encrypted?

Priority: N/A-

Answer: Yes, as the encryption routine is being prevented. This is for specific Locky builds, as other Crypto\Ransom can use different methods during encryption. Please refer to PD25203 for other preventative measures for Cryptos\Ransomwares

---

Q: In Today's world Behavior blocking is only way to mitigate new threats, as mentioned for Win37 downloader, do we recommend any other rules.

Priority: N/A-

Answer: Please refer to PD25203 for other preventative measures for Crypto\Ransomwares