HOW TO DETECT AND CLEAN CRYPTOLOCKER

CryptoLocker is by now a well known piece of malware that can be especially damaging for any data-driven organization. Once the code has been executed, it encrypts files on desktops and network shares and "hold for ransom", prompting any user that tries to open the file to pay a fee to decrypt them. For this reason, CryptoLocker and its variants have come to be known as "ransomware."

Malware like CryptoLocker can enter a protected network through many vectors, including email, file sharing sites, and downloads. New variants have successfully eluded anti-virus and firewall technologies, and it's reasonable to expect that more will continue to emerge that are able to bypass preventative measures. In addition to limiting the scope of what an infected host can corrupt through buttressing access controls, detective and corrective controls are recommended as a next line of defense.

CRYPTOLOCKER BEHAVIOR

On execution, CryptoLocker begins to scan mapped network drives that the host is connected to for folders and documents (see affected file-types[i]), and renames and encrypts those that it has permission to modify, as determined by the credentials of the user who executes the code. CryptoLocker uses an RSA 2048-bit key to encrypt the files, and renames the files by appending an extension, such as, ".encrypted," or ".cryptolocker," or – ".[7 random characters]," depending on the variant. Finally, the malware creates a file in each affected directory linking to a web page with decryption instructions that require the user to make a payment (e.g. via bitcoin). Instruction file names are typically "DECRYPT_INSTRUCTION.txt," or "DECRYPT_INSTRUCTIONS.html".

As new variants are uncovered, information will be added to the Varonis Connect discussion on CryptoLocker. For example, a variant known as "CTB-Locker" creates a single file in the directory where it first begins to encrypt files, named, "!Decrypt-All-Files-[RANDOM 7 chars].TXT" or "!Decrypt-All-Files-[RANDOM 7 chars].BMP".

MITIGATION TIPS

Prevent What's Preventable

The more files a user account has access to, the more damage malware can inflict. Restricting access is therefore a prudent course of action, as it will limit the scope of what can be encrypted. In addition to offering a line of defense for malware, it will mitigate potential exposure to other attacks from both internal and external actors.

While getting to a least privilege model is not a quick fix, it's possible to reduce exposure quickly by removing unnecessary global access groups from access control lists. Groups like "everyone," "authenticated users," and "domain users," when used on data containers (like folders and SharePoint sites) can expose entire hierarchies to all users in a company. In addition to being easy targets for theft or misuse, these exposed data sets are very likely to be damaged in a malware attack. On file servers, these folders are known as "open shares," if both file system and sharing permissions are accessible via a global access group.

Although it's easiest to use technologies designed to find and eliminate global access groups, it is possible to spot open shares by creating a user with no group memberships, and using that account's credentials to "scan" the file sharing environment. For example, even basic net commands from a windows cmd shell can be used to enumerate and test shares for accessibility:

- net view (enumerates nearby hosts)
- net view \\host (enumerates shares)
- net use X: \\host\share (maps a drive to the share)
- dir /s (enumerates all the files readable by the user under the share)

These commands can be easily combined in a batch script to identify widely accessible folders and files. Remediating these without automation, unfortunately, can be a time-consuming and risky endeavor, as it's easy to affect normal business activity if you're not careful. If you uncover a large amount of accessible folders, consider an automated solution. Automated solutions can also help you go farther than eliminating global access, making it possible to achieve a true least-privilege model and eliminate manual, ineffective access-control management at the same time.

HOW TO DETECT AND CLEAN CRYPTOLOCKER

Detect What You Can Detect

If file access activity is being monitored on affected files servers, these behaviors generate very large numbers of open, modify, and create events at a very rapid pace, and are fairly easy to spot with automation, providing a valuable detective control. For example, if a single user account modifies 100 files within a minute, it's a good bet something automated is going on. Configure your monitoring solution to trigger an alert when this behavior is observed. Instructions for configuring an automated alert with Varonis are available here (login required).

If you don't have an automated solution to monitor file access activity, you may be forced to enable native auditing. Native auditing, unfortunately, taxes monitored systems and the output is difficult to decipher. Instead of attempting to enable and collect native audit logs on each system, prioritize particularly sensitive areas and consider setting up a file share honeypot.

A file share honeypot is an accessible file share that contains files that look normal or valuable, but in reality are fake. As no legitimate user activity should be associated with a honeypot file share, any activity observed should be scrutinized carefully. If you're stuck with manual methods, you'll need to enable native auditing to record access activity, and create a script to alert you when events are written to the security event log (e.g. using dumpel.exe).

Correct What You Detect Faster With Automation

If your detective control mechanism can trigger an automated response, such as disabling the user account, the attack is effectively stopped before inflicting further damage. For example, a response to a user that generates more than 100 modify events within a minute might include:

- Notifying IT and security administrators (include the affected username and machine)
- Checking the machine's registry for known keys/values that CryptoLocker creates:
    - Get-Item HKCU:\Software\CryptoLocker\Files).GetValueNames()
- if value exists, disable user automatically:

See the Varonis PowerShell Resource Kit for examples and instructions, including disabling the user and removing a user's access to a share.

HOW TO DETECT AND CLEAN CRYPTOLOCKER

Recover With Confidence

If recorded access activity is preserved and adequately searchable, it becomes invaluable in recovery efforts, as it provides a complete record of all affected files, user accounts, and (potentially) hosts. Varonis customers can use the output from report 1a (as described here) to restore files from a backup or shadow copy.

Depending on the variant of CryptoLocker, encryption may be reversible with a real-time disassembler.

NEED HELP?

Contact us if you have questions, or if you'd like to set up a free consultation.

Want more helpful tips like this including in-depth articles and scripts that we don't post publicly? Visit the Security Corner in our Varonis Connect community.

WORLDWIDE HEADQUARTERS
1250 Broadway, 31st Floor, New York, NY 10001 **T** 877-292-8767 **E** sales@varonis.com **W** www.varonis.com

UNITED KINGDOM AND IRELAND
Varonis UK Ltd., Warnford Court, 29 Throgmorton Street, London, UK EC2N 2AT **T** +44 0207 947 4160 **E** sales-uk@varonis.com **W** www.varonis.com

WESTERN EUROPE
Varonis France, 13-15 rue Jean Jaures (1er Etage) 92800 Puteaux **T** +33 184 88 56 00 **E** sales-france@varonis.com **W** sites.varonis.com/fr

GERMANY, AUSTRIA AND SWITZERLAND
Varonis Deutschland GmbH, Welserstrasse 88, 90489 Nürnberg **T** +49(0) 911 8937 1111 **E** sales-germany@varonis.com **W** sites.varonis.com/de