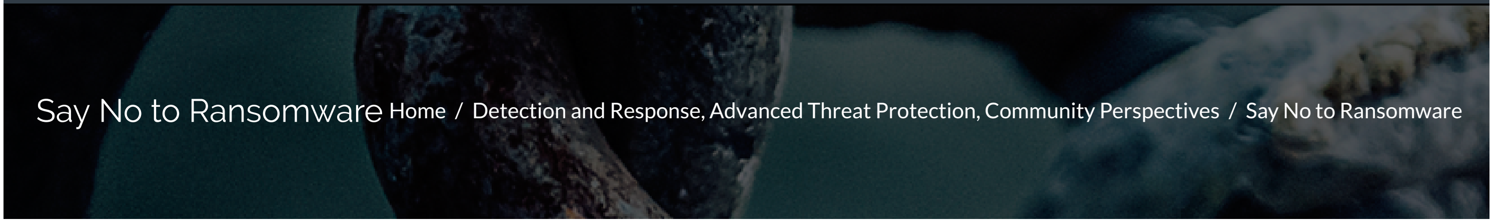
Careers ☎ 855-525-2489 Contact Us REQUEST A DEMO

CARBON
BLACK
ARM YOUR ENDPOINTS

WHY CARBON BLACK PRODUCTS SOLUTIONS PARTNERS RESOURCES COMPANY

BLOG



Say No to Ransomware

Home / Detection and Response, Advanced Threat Protection, Community Perspectives / Say No to Ransomware

Say No to Ransomware

November 7, 2013 / Ryan Nolette / Advanced Threat Protection, Community Perspectives, Detection and Response

Boo! CryptoLocker is here to knock on your door and take your candy. Now that Halloween has passed, it's a good time to unmask this newfangled malware monster and give it the Scooby Doo treatment. This post will describe CryptoLocker at a high level, what a CryptoLocker infection looks like, how you can stop CryptoLocker, and what happens when CryptoLocker is blocked.

First and foremost, know thy enemy. What is CryptoLocker? CryptoLocker is malware that surfaced in late 2013. It is a form of "ransomware" currently targeted at Microsoft Windows-based computers. It encrypts files stored on local hard drives and any mounted network drives it can access. When it has finished encrypting all the files it can find, it presents a branded prompt stating your files will be decrypted if a fee is paid (usually $300). It also threatens that if it is not paid by a specified deadline, CryptoLocker will delete the private key for your data and that decryption will no longer be possible. I have not tested this last point, so it will be out of scope for the rest of the post.

How does CryptoLocker differ from other ransomware? Most ransomware **DOES NOT** encrypt your files. To defend against it, you can usually kill the malicious process, remove the pieces, and carry on with your day. Ransomware is a broad category of malware that restricts access to the computer system that it infects in a variety of ways. After a piece of ransomware infects your machine it demands a ransom paid for the restriction to be removed.

How do I get CryptoLocker? This malware is brought down to the endpoint over the network via a variety of methods, none of which are new. The four most common delivery methods seem to be phishing and spam emails, malicious PDF's, exploit kits, and fake downloads.

Good news! If you are in high-enforcement mode while using the Bit9 Security Platform, no unknown/unapproved/untrusted interesting files can execute. This is by far the best method of defense against the unknown. For defense-in-depth and for customers who do not run their environment in high-enforcement mode, we have created an example blocking rule for registry values and files on the host that are effective against potential infections of CryptoLocker.

How do you know if you're infected? This malware makes very little effort to hide what it is doing; the big red screen you'll see is also a huge hint that you are infected….

So what is CryptoLocker doing when it runs? Before you see the big red ransom screen, CryptoLocker is running in the background encrypting every file it can. It finds them by searching for files with a long list of extensions. These extensions include office documents and pictures, as well as a few dozen other extensions that cover most common files on a computer. For each file that is encrypted, a resulting registry value will be created under the key HKCU\Software\CryptoLocker\Files. When the malware has finished running on the host, it will present the red ransom screen and start the countdown.

How do you stop CryptoLocker? Lock down that host! As stated before, disallowing the execution of unknown/unapproved/untrusted files is the safest course of action. Since locking down everything is not always an option, there is another common method of deterrence available. You can use GPO to block the execution of executable files in the %AppData% directory (%AppData%*.exe). This method is similar to how Bit9 does not allow execution of interesting files. The biggest difference is that the GPO is limited to hardcoded file paths with ".exe" in the file name, whereas Bit9 can tell what is executable and what isn't regardless of the file name or path. When CryptoLocker v2.0 comes out and changes paths, your GPO protection will no longer work.

What else is Bit9 doing to help you? We've provided material to customers that will allow them to stop CryptoLocker attacks even if they are not running Bit9 in high enforcement mode. This demonstrates the flexibility and power of the Bit9 solution.