Stop Ransomware with Carbon Black

Block, Detect, and Respond to CryptoLocker, Locky, TeslaCrypt and more

Key Takeaways

- CryptoLocker and other ransomware variants can be downloaded through conventional techniques like phishing and spam emails to encrypt and hold valuable files for ransom.
- Ransomware can also be delivered through readily available exploit kits (EKs) like Angler and Nuclear, new variants are seen regularly.
- CryptoLocker takes ransomware up a notch by holding asymmetric encryption keys hostage with a countdown to their destruction.
- Antivirus can't detect the types of behaviors that signal a ransomware attack, and new variants are released so often, antivirus research teams cannot keep up.
- Choosing the right prevention is the best way to deny CryptoLocker variants access to your precious data and critical infrastructure.
- Detecting patterns commonly used by most ransomware variants is a critical step to mitigating risk of ransomware attacks and stopping them in their tracks.
- The Carbon Black Security Platform's continuous monitoring and recording gives you visibility, detection, response, prevention and integration with network security solutions—in a single solution.

Ransomware-as-a-Service — a threat so prevalent, it's an established vertical

Every year, CryptoLocker and its variants, collectively known as ransomware, target new verticals and find fresh victims. Ransomware makes itself known by presenting users with a message indicating that their critical files have been encrypted and offering to decrypt the files for a fee, usually in bitcoin, US Dollars, or Euros. The attackers threaten to delete the private key needed to decrypt the files unless their ransom is met. Banks, hospitals, and many SMBs are targeted by ransomware every day.

Users fall victim to ransomware through conventional means like phishing and spam emails, but in the last few years, attackers have started leveraging exploit kits (EKs) such as Angler and Nuclear. As a result, users no longer need to intentionally run malware on their machines. Simply visiting the wrong web page can drop a damaging CryptoLocker variant, like TeslaCrypt.

Stop ransomware before it starts

Even the most educated end users, that never click on email attachments, and practice good security procedures can become victims of sophisticated exploits, through drive-bys and other exploit kits. The best way to stop malware like Locky, TorrentLocker, and other ransomware variants is to implement a security system that continuously, centrally records all endpoint activity and stops untrusted code from executing on endpoints.

Traditional signature-based antivirus can only protect your endpoints from existing, known-bad malware, and there are new variants of CryptoLocker every day. Relying on traditional security tools and policies practically ensures you will see malware successfully run in your environment. This logically leads to blindly re-imaging machines and never improving your security posture through root cause analysis.

Carbon Black Enterprise Protection is the only next-generation endpoint threat prevention solution to deliver a portfolio of prevention options, real-time visibility across environments, and comprehensive compliance rule sets in a single platform. Cb Enterprise Protection introduces a more modern approach to application and file control and helps address the question, how do you address software that isn't known good or bad already? With Cb Enterprise Protection, you can leverage automation and trust-based approval mechanisms to keep ransomware from even running in the first place.

Only Cb Enterprise Protection runs across Windows, Mac and Linux machines to keep all endpoints and servers secure, whether on or off network, dramatically reducing an organization's attack surface. Cb Enterprise Protection goes beyond basic security with advanced file integrity monitoring and control capabilities, enabling organizations to exceed PCI-DSS, HIPAA/HITECH, SOX, NERC CIP, NIST 800-53, and other regulatory frameworks. Cb Enterprise Protection also

CARBON BLACK
ARM YOUR ENDPOINTS

Discovered by Carbon Black, PowerWare

The Carbon Black Threat Research Team has recently discovered a new family of ransomware, which they dubbed "PowerWare," that targets organizations via Microsoft Word and PowerShell. PowerShell is the scripting language inherent to Microsoft operating systems.

"PowerWare" is a new instance of ransomware utilizing native tools, such as PowerShell on operating systems. "Traditional" ransomware variants typically install new malicious files on the system, which, in some instances, can be easier to detect. "PowerWare" asks PowerShell, a core utility of current Windows systems, to do the dirty work. By leveraging PowerShell, this ransomware attempts to avoid writing new files to disk and tries to blend in with more legitimate computer activity.

Deceptively simple in code, "PowerWare" is a novel approach to ransomware, reflecting a growing trend of malware authors thinking outside the box in delivering ransomware.

provides flexibility allowing you to choose the right prevention, your end user endpoints and critical infrastructure servers have very different requirements and prevention needs. Regardless of the level of enforcement you choose, Cb Enterprise Protection is always recording endpoint activity and base image drift, providing unprecedented visibility into your endpoints.

Rapidly detect and respond to ransomware

What happens if someone in your organization does fall victim to a ransomware attack? How quickly will you catch the attack? How do you respond?

Most defenders don't know about the attack until their end users escalate the issue, and by then it's too late. The response is often reimaging the machine and using backups, if they exist. However, this response is lacking improvement and leaves you blind to the root cause of the incident. Nothing will stop another member in your organization falling victim to the same malware delivered through the same exploit, whether ransomware or other advanced malware.

Cb Enterprise Response leverages pattern-based threat detection to provide reliable detection of ransomware variants by looking for behaviors and actions that are indicative of a ransomware attack. The security team can be alerted of a potential ransomware attack that's taking hold of their enterprise, isolate the host and stop the attack before it spreads.

Carbon Black Enterprise Response also provides the visibility you need by continuously and centrally recording all endpoint activity, including network connections, process trees, file and registry modifications, file executions, and copies of executed binaries. This visibility provides you with full root cause analysis so they can make intelligent decisions on how to improve your security posture to prevent future attacks, instead of blindly re-imaging machines or deleting malware and hoping for the best.

It's clear traditional endpoint security isn't cutting it

Ransomware is on the rise. Threat researchers are raising the red flag and the number of cases of enterprises being forced to pay criminals to decrypt their files, is growing every day. It's particularly worrisome because it can be exceedingly difficult to stop and it hits businesses where it hurts — time and money. Not only does it result in stolen dollars but it dramatically disrupts business operations.

Attackers can easily go around anti-virus, next-gen AV and other signature-based detection engines. Re-imaging will never be the right solution to this problem. Whether you're being attacked with Cryptolocker, Locky, TeslaCrypt, or today's hot ransomware, you can be sure the Carbon Black Security Platform will provide you with the tools you need to prevent, detect, and remediate the threats to your endpoints and your end users.

About Carbon Black

Carbon Black leads a new era of endpoint security by enabling organizations to disrupt advanced attacks, deploy the best prevention strategies for their business, and leverage the expertise of 10,000 professionals from IR firms, MSSPs and enterprises to shift the balance of power back to security teams. Only Carbon Black continuously records and centrally retains all endpoint activity, making it easy to track an attacker's every action, instantly scope every incident, unravel entire attacks and determine root causes. Carbon Black also offers a range of prevention options so organizations can match their endpoint defense to their business needs. Carbon Black has been named #1 in endpoint protection, incident response, and market share. Forward-thinking companies choose Carbon Black to arm their endpoints, enabling security teams to: Disrupt. Defend. Unite.

CARBON BLACK
ARM YOUR ENDPOINTS

1100 Winter Street
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.carbonblack.com