What is Ransomware?

During a ransomware attack, devices are essentially held hostage by a malicious actor in exchange for a “ransom”. Often, there is a time limit within which the funds must be paid to restore access—if the victim doesn’t meet these demands, they may lose their information forever. Ransomware isn’t new—in fact, it’s over 30 years old. Attacks date back as far as 1989 and have been the most pervasive cyber threat since 2005, with a dramatic spike in recent years. The resulting costs to targeted businesses are soaring.

In fact, according to the 2018 Verizon Data Breach Investigations Report, ransomware has moved from the 22nd most common variety of malware in 2014 to the most common variety in 2018. It is estimated that, by the end of this year, ransomware will attack a business once every 14 seconds.
How Does It Work?

Ransomware is similar to other malware in that it installs itself on a computer and runs in the background without the user’s knowledge. But unlike malware that hides and steals valuable information, ransomware doesn’t hide. As soon as ransomware has locked a user’s machine and/or encrypted files, it notifies the user of its presence to make the ransom demand.

To amplify the victim’s distress, ransomware often includes a countdown clock with a deadline for paying the ransom—or else the decrypt key will be destroyed, eliminating any chance of recovery. Paying the ransom often means the attacker will unlock the victim’s machine or provide the key to decrypt files. However, it rarely means the originating malicious binary, “ransomware.exe” in the case below, has been removed. That will require IT and SecOps support.

And the attack doesn’t necessarily end there. Attackers often load additional malware onto a user’s machine, allowing them to harvest personal information, intellectual property, and credentials to sell for additional revenue.
**PHASE 1**
- Attacker Sends Spam Email
- Bypasses Victim's Spam Filter
- Hits User's inbox
- User clicks on malicious link

**PHASE 2**
- Malware XYZ.exe is delivered, launches legitimate child processes cmd.exe, PowerShell, VSSadmin
- Encryption

**PHASE 3**
- Encryption
- Ransom Note Delivered
- Ransomware copied to %AppData%, Startup, C://
- Encryption connects with attacker's C&C server to deliver info / get instructions
- Attacker attempts to move laterally across the enterprise
How VMware Carbon Black Combats Ransomware

VMware Carbon Black uses several approaches to combat ransomware, the most important of which centers around visibility. More advanced adversaries have frequently embedded their ransomware into non-traditional formats—such as PDFs, Word documents, Excel sheets, etc. With this in mind, VMware Carbon Black prioritizes comprehensive endpoint visibility. We know that a motivated attacker could likely weaponize anything—so we need to watch everything.

From here, our behavioral analytics engine constantly analyzes all endpoint behavior in the cloud, looking for malicious intent through any application or executable. Our signature based ransomware prevention uses local indicators and canary files on the endpoint to immediately block any “ransomware-like” behavior, including encryption of files, editing of
the master boot record (MBR), and unauthorized access to system backups.

While existing families of ransomware are easily recognized as known malware, zero-day ransomware attacks pose a larger threat. By focusing on ransomware’s unique characteristics, VMware Carbon Black possesses the unique ability to stop new and emerging attacks—allowing our customers to feel confident knowing that they are protected in the modern attack landscape.

TO LEARN MORE AND SEE HOW YOU CAN COMBAT THREATS IN YOUR ENVIRONMENT, VISIT CARBONBLACK.COM/EPP-DEMO