cybereason

Defeat Ransomware with Cybereason

The Challenge

Ransomware attacks are one of the top concerns for organizations today. These attacks have become significantly more prevalent in the past year, and attackers are demanding huge ransoms estimated to cost a total of $1 billion in 2016[1]. In addition to the financial losses that victims face, ransomware attacks can also significantly impact productivity by encrypting data on multiple endpoints and sometimes entire network drives and file servers.

One of the main reasons these attacks are so successful is that traditional AV can't detect ransomware. Attackers create new strains and repackage existing strains of ransomware every day. The number of ransomware families has grown an estimated 600% since December of 2015[2]. Signature-based defenses simply can't keep up with the rapid creation of new strains. In addition, many types of ransomware are polymorphic which means it can generate a new hash every time it propagates to avoid detection.

The Solution

A unique approach to detecting and blocking ransomware. Cybereason has conducted extensive research on tens of thousands of strains incorporating dozens of different families of ransomware.

Cybereason Labs has identified the typical pattern of behavior, we know how, when, and where ransomware will start encrypting files–so we also know where to stand on-guard to stop it.

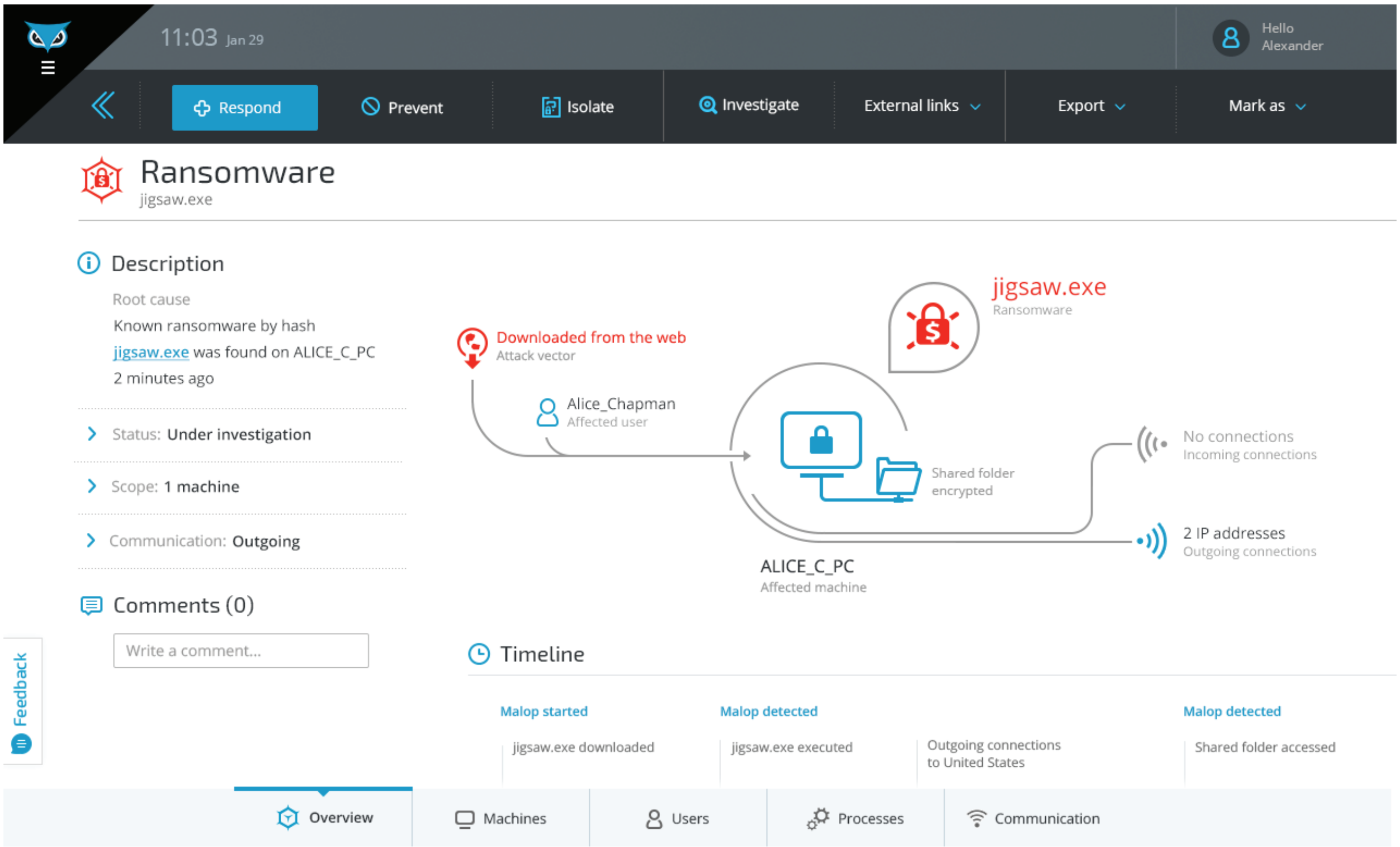
Even though many ransomware strains were written by different criminal teams, the Cybereason Labs team identified that all of the tested ransomware strains exhibit common behaviors. Following similar behavioral patterns, ransomware attempts to encrypt as many files as possible, as quickly as possible.

Based on this research, Cybereason has developed a unique behavioral approach to stop ransomware in its tracks. Since we've identified the typical pattern of behavior, we know how, when, and where ransomware will start encrypting files – so we also know where to stand on-guard to stop it.

Defeating ransomware with a combination of techniques:

Behavioral analytics. The solution hunts for common low level file related behaviors that ransomware exhibits as it executes, such as file enumeration and multiple write-access events.

Deception techniques. The Cybereason Sensor deploys "bait files" on endpoints in strategic locations on hard drives and network drives where ransomware often begins its encryption process.



Ransomware
jigsaw.exe

Description

Root cause
Known ransomware by hash
jigsaw.exe was found on ALICE_C_PC
2 minutes ago

Status: Under investigation

Scope: 1 machine

Communication: Outgoing

Comments (0)

Timeline

Malop started – jigsaw.exe downloaded

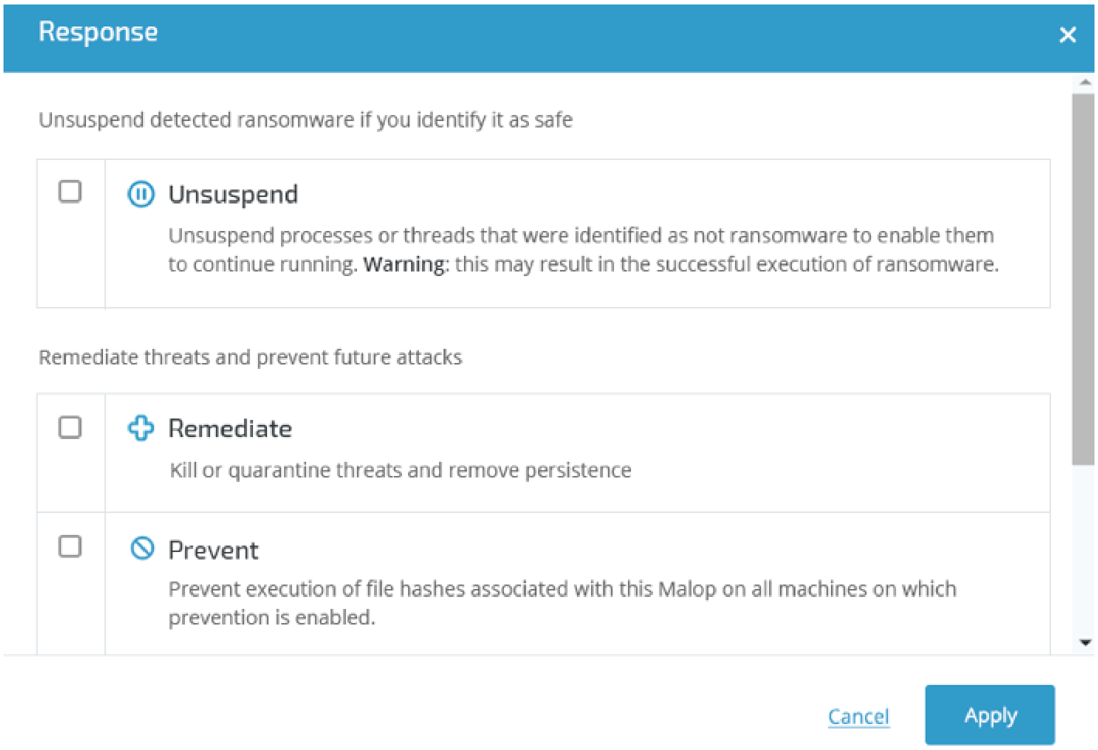
Malop detected – jigsaw.exe executed

Outgoing connections to United States

Malop detected – Shared folder accessed

Detecting over 95% of all tested ransomware strains

Some ransomware regenerates itself as it attempts to evade detection by a tool that has successfully blocked the initial strain. Cybereason's unique approach enables you to detect and stop even polymorphic ransomware by looking for behavioral characteristics as opposed to relying on hash or signature like other security tools, such as anti-virus software.



Response

Unsuspend detected ransomware if you identify it as safe

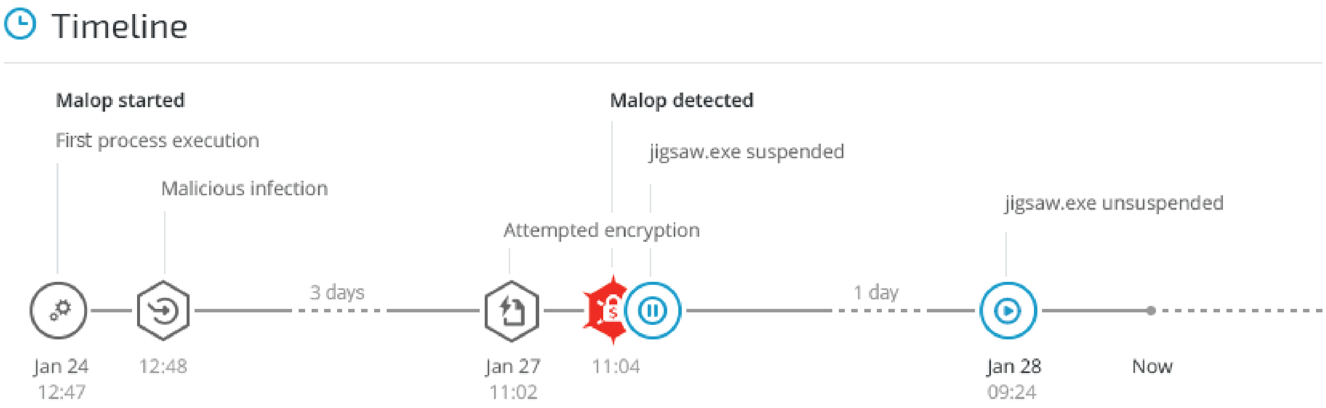
□ Unsuspend
Unsuspend processes or threads that were identified as not ransomware to enable them to continue running. **Warning**: this may result in the successful execution of ransomware.

Remediate threats and prevent future attacks

□ Remediate
Kill or quarantine threats and remove persistence

□ Prevent
Prevent execution of file hashes associated with this Malop on all machines on which prevention is enabled.

Upon detection, Cybereason automatically suspends the ransomware and generates a Malop for forensics, investigation, and response. The team member can choose to investigate the attack, download the ransomware for forensics, isolate the infected machines, and terminate and quarantine the process or thread and prevent it from running again throughout the organization.



The Cybereason Detection and Response Platform

Automatically detect and classify ransomware

With a combination of deception techniques, behavioral analytics, machine learning, and threat intelligence, the solution automatically detects and stops ransomware in your environment without the need to write and maintain rules.

Detect known and never-before-seen ransomware with deception

Unlike any other security vendor, Cybereason uses deception techniques to detect ransomware, which enables you to quickly detect both known and unknown ransomware strains. This approach is not based on hash or signature, so never-before-seen ransomware strains including file-less ransomware, are identified and blocked just as quickly as known ransomware.

Block ransomware based on behavioral detection

By luring ransomware with Cybereason's deception methods, the solution is able to identify and stop its progression before it is able to encrypt all files on an endpoint. In addition to blocking the ransomware from spreading, you can also download it for forensics, easily identify and isolate other machines that have already been infected, and prevent it from running again on any endpoint throughout the organization.

Protect data from ransomware without impacting users

The solution is designed to have little to no impact on users. Deception mechanisms are strategically placed on endpoints with little to no impact on users. They are virtually unnoticeable to end users, yet will lure ransomware and immediately alert you of malicious activity.

Leverage Cybereason Labs

As ransomware strains evolve, Cybereason Labs constantly evaluates new ransomware strains and other types of attacks to continuously analyze the latest threats and develop detection and response techniques to combat them.

[1] http://www.prnewswire.com/news-releases/ransomware-damages-predicted-to-reach-1-billion-annually-by-close-of-2016-592573371.html

[2] https://www.proofpoint.com/sites/default/files/quarterly_threat_summary_apr-jun_2016.pdf