Cynet
Advanced Threat Detection & Response

WHAT YOU NEED TO KNOW ABOUT STOPPING RANSOMWARE

Ransomware is not a new threat, but it is a threat that organizations continue to deal with. Cybersecurity analysts predict that the file-locking malware will evolve into new types of attacks in 2017, with more sophisticated capabilities for identifying lucrative targets and for evading detection.

While ransomware initially targeted home users, locking up documents, files and pictures, enterprises are now the #1 Target.

The reason is clear: enterprises can typically pay more money than individuals to release files that are under lock-down. Newer strains of ransomware are capable of infecting hundreds of machines at the same time, encrypting entire networks, and encrypting business-critical documents in minutes. When the files at stake include competitive intelligence and intellectual property, organizations that have not instituted proper security practices will frequently pay up.

HOW RANSOMWARE IMPACTS THE ENTERPRISE

Ransomware's palpable effect on the enterprise is evidenced by what it costs, both financially and in terms of productivity.

In light of the fact that ransomware continues to target enterprises, it is critical to understand how it gains entry into a network and how an enterprise can best protect itself. When it comes to the enterprise network, the extortion malware is commonly circulated as an email attachment or URL link within an email message clicked by unsuspecting employees.

Ransomware can also gain entry into systems when employees are redirected to malicious websites, for example by clicking on malicious ads. With employees being one of the biggest risks to enterprise cybersecurity, it is crucial that enterprises arm themselves with adequate attack detection and remediation methods to limit the damage of a potential ransomware attack.

BEST PRACTICES FOR PROTECTING THE ENTERPRISE AGAINST RANSOMWARE

To avoid the long-lasting, damaging results of ransomware attacks, organizations must take a proactive approach to reducing risk. The best protection an enterprise can achieve against ransomware involves a broad threat detection solution that offers full visibility into the enterprise environment, in order to accurately detect and stop ransomware attacks before damage occurs.

Solutions that identify ransomware through heuristic analysis offer the most powerful protection. Through heuristic analysis, if the system identifies suspicious file or program behavior that in any way resembles the behavior of ransomware, it registers this as a threat and manages it accordingly. Examples of malicious behavior include:

- Removal of files and creation of new, encrypted files
- Encryption of files that are then given new filename extensions
- Emergence of files containing instructions for unencrypting (e.g. "send payment to...")

50

THAT'S THE NUMBER OF NEW STRAINS OF RANSOMWARE

that surfaced in the first five months of 2016 alone, averaging 10 new variants of the malware each month. This illustrates the extent to which ransomware continues to be a growing threat to the enterprise.

$200 million

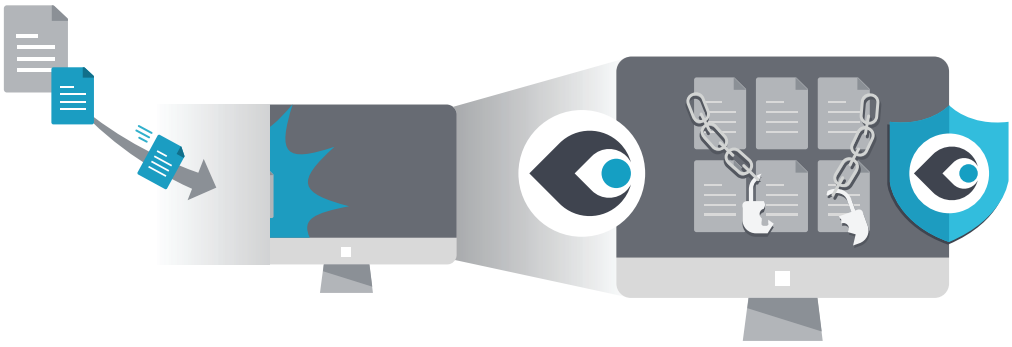
THAT'S THE FBI'S ESTIMATE

of the amount ransomware cost victims – in only the first 3 months of 2016. Considering the countless victims who didn't report paying a ransom, this number is likely much greater.

$9,000

THAT'S THE AVERAGE HOURLY COST

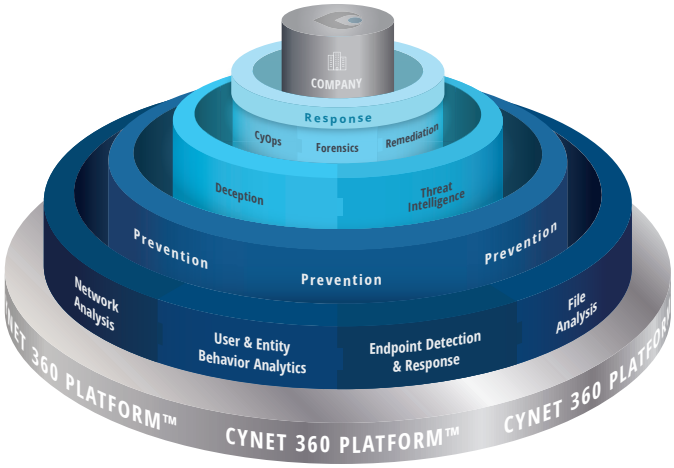
of organizational inactivity for a small business due to ransomware locking down their network, illustrating the extent to which lost productivity costs an organization far more than the actual ransom they might pay.



A comprehensive platform like Cynet that identifies threats using behavioral analysis can keep an enterprise secure, despite the fact that new strains of ransomware are continually emerging.

In addition to heuristic analysis, the platform should also be capable of:

- Blocking malware from the **user, endpoint and network levels** – with an equal focus on the risk inherent in each of these fronts.
- Placing **decoys that attract ransomware** throughout a machine. Placing decoys in the folders that ransomware is known to attack should enable the system to identify and stop ransomware the moment it accesses, scans or encrypts decoy files.



The Cynet 360 Platform

- Detecting and blocking **suspicious file execution and encryption activities, and the removal of backup files.** The system should be able to detect file execution and encryption activities that deviate from normal behaviors and block these activities in real-time. Removal of backup files, a known indicator of ransomware, should immediately raise a red flag.
- Identifying **suspicious scanning activities**. Ransomware is known to take an undiscerning approach to scanning, touching all files and folders at an alarming rate. The ideal security solution should be able to differentiate this behavior from normal scanning behaviors performed by programs such as antiviruses.

To address the risk posed by employees and further reduce their risk of attack, enterprises should:

- **Observe good security** practices including regular backups and updates, timely installment of patches, and implementing Internet and email security policies.
- **Secure every endpoint**, putting into place protection for platforms including Linux, Mac, tablets and mobiles.
- **Provide employee security awareness training** so employee behavior can be informed and secure.

Ransomware is an evolving and continuous threat, but enterprises do not need to be vulnerable. Best practices for protection against ransomware require a broad threat detection and remediation platform like Cynet, with an integrated approach to monitoring and providing full visibility into the enterprise environment. Through this integrated approach, enterprises can accurately detect real ransomware threats and remediate them before their systems and operations are compromised.

SIMPLIFY
YOUR
SECURITY

About Cynet

Cynet is a pioneer and leader in advanced threat detection and response. Cynet simplifies security by providing a scalable, easily deployable protection platform that delivers prevention, precise findings and automated response to advanced threats with near-zero false positives, shortening the time from detection to resolution and limiting damage to an organization.

To learn more visit: www.cynet.com

Cynet
Advanced Threat Detection & Response

www.cynet.com.