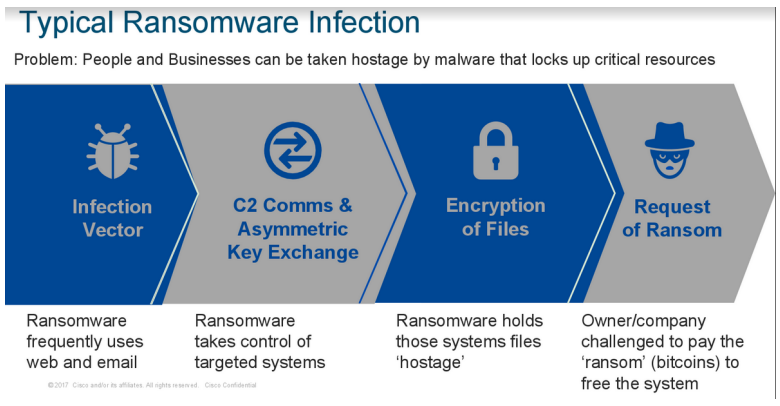
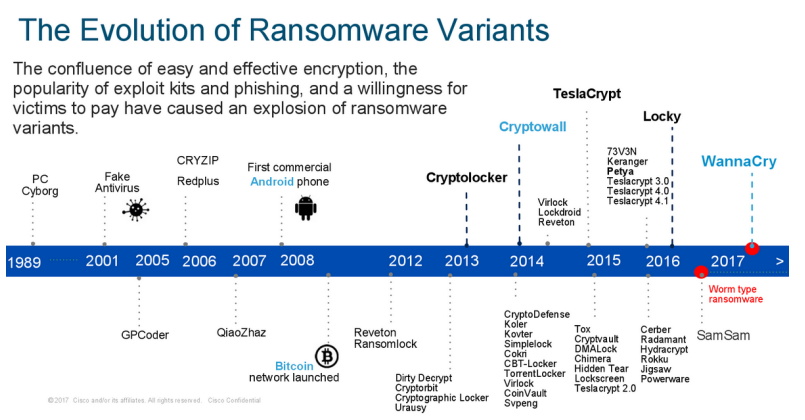

# *Combating Ransomware challenge with Cisco Ransomware Defense solution*

Ransomware criminals are indiscriminately attacking small, medium and large business, taking them hostage and locking up critical resources thus causing drastic loss of business, disrupting hospital patient treatment, loss of sensitive or proprietary information, impacting public safety to name a few. Law enforcement agencies are limited in its ability to help in most cases, requiring organizations to rise up to the challenge. Due to the persistence and sophistication of attackers and methods, this extortion type criminal business has become the most profitable type of malware in history. Ransomware can infiltrate an organization in multiple ways and can use a range of vectors such as web, email, malvertising, exploit kit on systems( eg: WannaCry). An architecture based security approach is required to defend and contain the attacks.

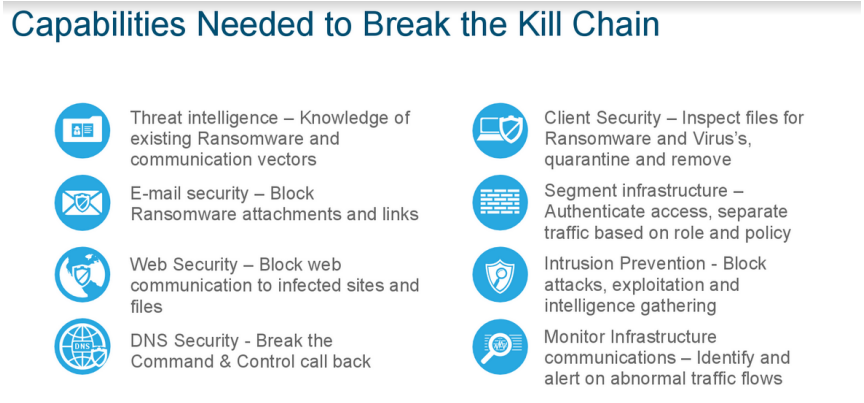


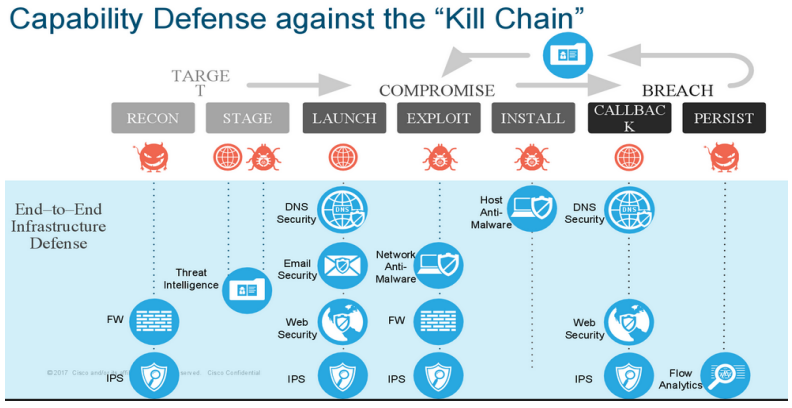




## *Cisco Ransomware Defense solution*

Cisco's integrated Ransomware defense solution is not a silver bullet but helps reduce the risk of Ransomware getting into the network, detect if a breach were to happen and contain rapidly, reducing the impact. Cisco takes a layered approach in combating Ransomware, from DNS layer to endpoint to network, email, and the web. It also brings necessary pieces of Cisco security architecture to address the ransomware challenge. In order to better defend against Ransomware, Cisco identifies primary capabilities needed to break the kill chain and aligns products that are required as part of architecture solution.

RECON, STAGE, LAUNCH, EXPLOIT, INSTALL ,CALLBACK, PERSIST are the common seven stages of a Ransomware kill chain. Cisco Ransomware Defense is a defense- in-depth architecture approach that works together to defend against the stages of Ransomware kill chain. It's also critical to deploy other best practices such as disaster recovery plans, backup, standardization and patching of systems etc to reduce impact of malicious incidents.




Cisco Ransomware Defense comprises of the following components and the solution is offered in bundle packages for easy consumption.

- Cisco Umbrella: Blocks DNS requests and provides IP-layer protection in the cloud before a device can even connect to malicious sites hosting ransomware. It also protects devices on and off your corporate network.

- Cisco Advanced Malware Protection (AMP) for Endpoints: Blocks ransomware from gaining access and encrypting files on endpoint devices.

- Cisco Email Security with AMP: Denies spam and phishing emails as well as malicious email attachments and URLs. (Note: The AMP technology is the same that's applied on endpoints, but it's deployed at the email gateway for this solution.)

- Cisco Threat Grid: Uses static and dynamic file analysis to determine ransomware/malware. It sends actions to all AMP-enabled devices (networks and endpoints), Cisco Firepower™ Next-Generation Firewall (NGFW), and Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS) to block malware trying to infiltrate your IT environment.

- Cisco Firepower NGFW with AMP: Offers fully integrated threat-focused NGFW to mitigate advanced threats quicker (for example, blocks known threats and command-and-control callbacks) and streamlines operations.

- Cisco Identity Services Engine (ISE): Develops policies that the network enforces through Cisco TrustSec® technology. Our solutions work together to contain ransomware attacks through these policies. You can dynamically segment your network, which maintains highly secure access to services and applications. This also prevents the lateral movement of ransomware.

- Cisco TrustSec Technology: Performs dynamic segmentation and containment of ransomware using the network infrastructure and ISE policy enforcement.

- Cisco Stealthwatch: Offers advanced network and data center visibility, analytics, and protection. It detects anomalous behavior, such as ransomware, and alerts ISE to push containment policies to the Cisco TrustSec infrastructure.

- Cisco Security Services: Provides advisory, implementation, and managed services to help you before, during, and after a ransomware attack. For example, you can take advantage of immediate triage in the case of incident response. You can also get expert help streamlining deployments of AMP, NGFW, and other solutions.

**www.cisco.com/go/ransomware**

For more information on Cisco Security solutions and products, please contact your **Cisco Account Manager**

Suggestions/comments on this newsletter contact Joby James at joby@cisco.com