Ransomware: Block Attackers with a Layered Defense

What You Will Learn

The Los Angeles Times has suggested that 2016 is shaping up to be the year of ransomware. And ransomware is proving to be highly profitable. Campaigns have shown to generate up to $60 million annually.

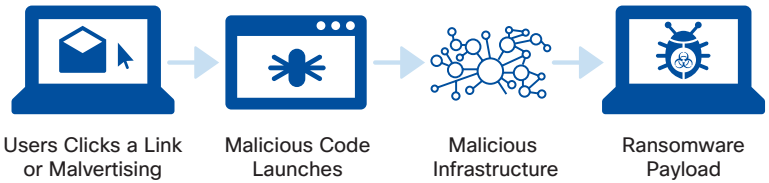
As reported in news accounts, Cisco has been active in the fight against ransomware. We see it affecting companies across all industries at an alarming rate. Invariably, customers will ask us whether they are secure.

This paper describes what ransomware is, what it does, and how customers can defend their organizations against it. We focus on ransomware here, but the process we describe applies to other threats as well.

What Ransomware Is and What It Does

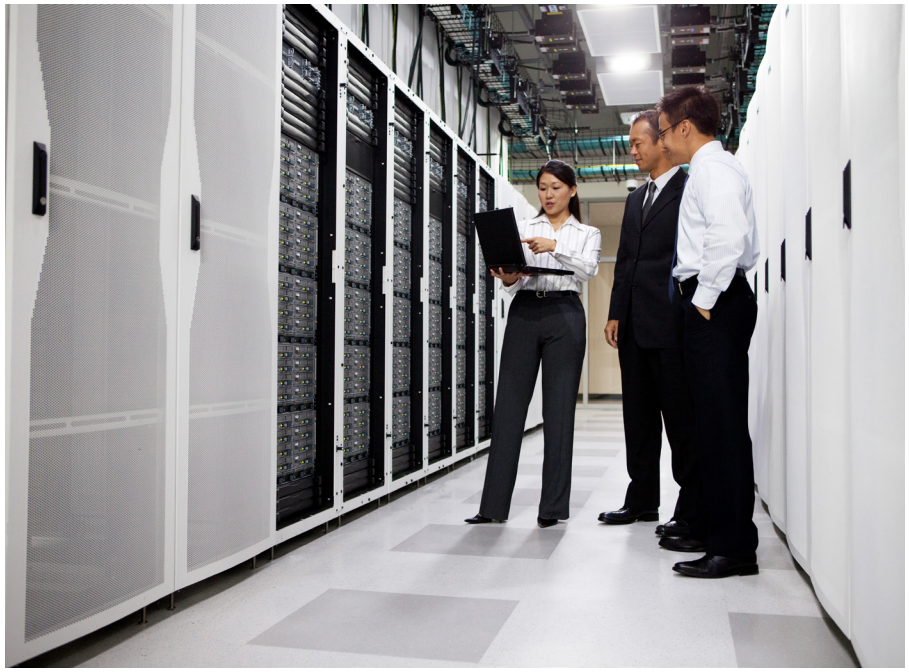
Ransomware is malicious software designed to hold a user's files (such as photos, documents, and music) for ransom. Hackers encrypt the files and demand that the user pay a fee, usually in Bitcoin, to decrypt them. One recent example: a Los Angeles hospital infected with ransomware lost access to important data. Being reduced to record keeping with pen and paper, it paid a ransom of 40 bitcoins (some $17,000) to regain access to its files.

Figure 1. How Ransomware Infiltrates a Network



Ransomware is commonly delivered through exploit kits, malvertising (infected ads on a website), phishing (fraudulent emails masquerading as trustworthy), or spam campaigns. The actual infection can begin when people click on a link or an attachment in a phishing email, an infected ad, or a compromised webpage that infect anyone going to that site.

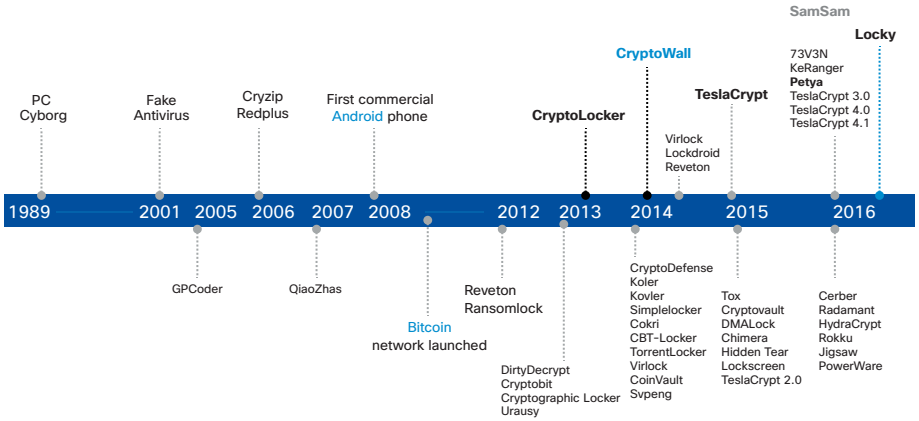
Figure 2. A Typical Ransomware Notice



The Evolution of Ransomware

The confluence of easy and effective encryption, the popularity of exploit kits and phishing, and the willingness of victims to pay have caused an explosion of ransomware variants (Figure 3).

Figure 3. The Evolution of Ransomware Variants



Protection Against Ransomware

A combination of people, processes, and tools must be applied to solve the problem of ransomware. The business owner needs to have proper visibility, the ability to see and manage business and network operations. A map of policy and behavior can then detail how the business and the network normally operate.

Regulatory and business rules, also known as policy, will describe how far from the norm a transaction can deviate before it is determined to be anomalous. The ability to see deviations from the norm and to mitigate threats, perceived or real, is referred to as "applying controls through the lifecycle of the kill chain." A kill chain consists of the phases in a cyber attack, from locating a target's vulnerability to delivering malware and, in the case of ransomware, encrypting the target's files.

Ransomware defense is interesting. Forensic data sets list the known bad talkers and who they talk to, so attacks can often be stopped before they happen. In ransomware, malware uses the Domain Name System (DNS) to resolve the IP address as part of the command and control, known as C2. When it does, Cisco is able to stop the threat before it becomes an issue and you can avoid having to pay ransom.

However, protection against ransomware isn't just about visibility and mitigation (the application of technology to fix the problem). An effective business process is also essential. In particular, you should consider two questions:

Do you have a tested disaster recovery procedure?

In some cases, a tested procedure means having an active/active configuration for disaster recovery. Cisco has a number of partners who provide this service. How you go about disaster recovery is a key consideration. It is a best practice to not have your disaster recovery site mounted as a drive on your workstations.

Many corporate configurations will mount a drive letter (like drive F) to a specific network share. You don't want to do that for your disaster recovery site. Why not? The nature of ransomware is that any mounted drive and the files on it will be encrypted by the ransomware process. Therefore, proper segmentation and isolation of the disaster recovery site is a must. Application of Cisco TrustSec® policy control methods is an integral part of this strategy. Segmentation in the network and policy control that the disaster recovery provider delivers is also very important.

How do you handle a critical disruption?

The answer to this question is equal parts business process and technology (your backup strategy, the frequency of backups, the validation of backups, and so on). The business part is usually not fully developed. But at the time of an attack, it's too late to pull a process together. If part of the business has to be shut down to mitigate an attack, do you have the functions in your business ranked in importance? And have your business leaders already agreed to the ranking as corporate policy?

Effective Security Against Ransomware

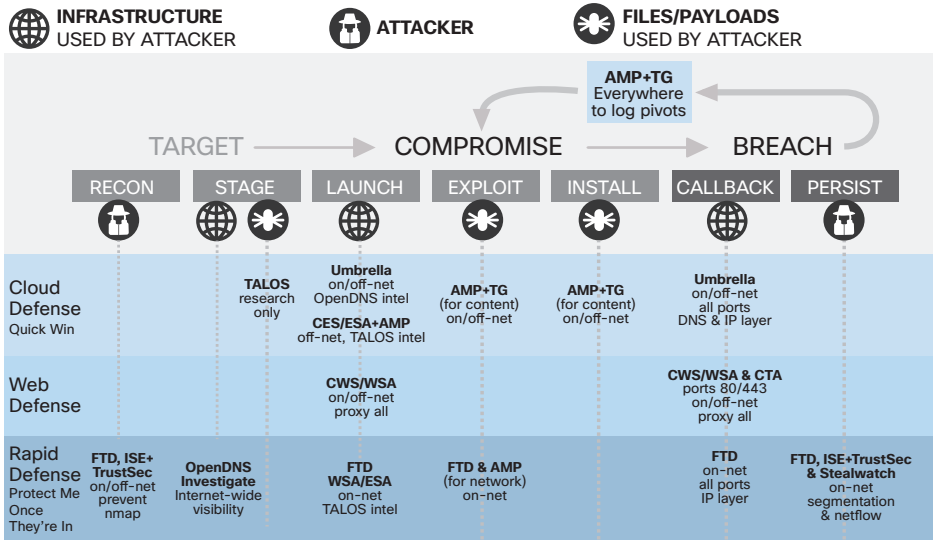
Cisco protects against ransomware with a layered security approach backed by industry-leading threat research from the Talos Security Intelligence and Research Group. We have done more threat research on ransomware than any other vendor. We provide layered protection to fight it and to block it if it slips through the cracks to get into an organization–as it is bound to do at some point.

As is always the case, criminals figure out ways to get around single-point solutions. A "defense in depth" approach is necessary to fight them.

Our layered approach protects you from the DNS layer to the endpoint to the network, email, and web. We deliver integrated defenses that combine ultimate visibility with ultimate responsiveness against ransomware. This layered approach is articulated to partners and customers in the form of offers. These offers allow you to deploy sets of people, processes, and tools that mitigate ransomware.

Figure 4 shows how Cisco® products work together against ransomware. They include Advanced Malware Protection (AMP), Threat Grid (TG), Cloud Email Security (CES), the Email Security Appliance (ESA), Cloud Web Security (CWS), the Web Security Appliance (WSA), Cognitive Threat Analytics (CTA), Cisco Firepower Threat Defense (FTD), and the Identity Services Engine (ISE).

Figure 4. How Cisco Defends Against the "Kill Chain"



Quick Win: In this layer, solutions from the cloud give you exceptional protection with little invasive impact on the network.

Web Defense: Content protection, web proxy, and other antimalware features add an element of web protection to the assets applied in the Quick Win.

Rapid Defense and Protect Me Once Threats Are In: When added to the Quick Win and Web Defense layers, this set of solutions makes up a next-generation firewall. You gain application visibility and control, intrusion protection services, malware protection, and content protection. Segmentation control plus the ability to see and analyze network behavior leads to the automatic update and distribution of policy. You get protection against behavioral aspects of things that "look" like ransomware, so policy can be applied quickly.

Sometimes, if there's a new variant of ransomware, suspect behavior can be identified before we know what it really means. Intelligence from the Talos group gives Cisco the agility to react quickly to new variants across the kill chain. It delivers the most up-to-date, most agile solutions to the ransomware problem.

In the worst-case scenario of an infection, dynamic segmentation provided by Cisco TrustSec technology can block ransomware from moving broadly once it's inside the network. It cannot run rampant and affect the majority of systems. Cisco malware protection services (AMP and Threat Grid) provide the ability to retrospectively remove the malware from endpoints where it has been seen. In a worst-case scenario, one or two endpoints might be affected while learning takes place. Then the defense-in-depth approach removes the offending malware from endpoints where it might sit dormant.

But where should we start in terms of immediate protection? Let's begin with the simplest and most effective.

Immediate Protection

For those who would like to bolster their defenses immediately, Cisco Advanced Malware Protection and OpenDNS Umbrella are two great starting points.

In the case of ransomware, Umbrella denies the DNS request, blocking the connection at the DNS layer before any ransomware compromise occurs. What is more, Umbrella can be up and running in less than an hour.

Advanced Malware Protection (AMP) for Endpoints blocks ransomware files from running. It also continuously analyzes all file activity on the system, so you can find and remove ransomware with confidence.

The combination of AMP and Umbrella can block an overwhelming majority of threats at the DNS layer, before they can reach an organization. Endpoints are protected during and even after attacks. You can get rid of all ransomware in two clicks.

Added Layers of Defense

Many customers may well already have Cisco security products in place that they can call on to fight ransomware, in addition to AMP or Umbrella.

As mentioned, ransomware often looks to infiltrate by means of spam, phishing messages, infected webpages, or online ads. Email protection and web security are vital.

What to expect from email security: Email security products, such as the Cisco Email Security Appliance, should block spam and phishing emails that are used to deliver ransomware. They should block the malicious attachments that also deliver ransomware (Figure 5).

What to expect from web security: Web security products should prevent access to malicious websites associated with malvertising that delivers ransomware. They should also detect the malware used in these attacks. The Cisco Web Security Appliance and Cloud Web Security fill the bill here (Figure 6).

Network Security's Role

Organizations should expect their next-generation firewalls (NGFWs) to block known malicious network activity, including ransomware attempts to "phone home" to C2 servers. Cisco NGFWs are very well suited to this.

Figure 5. Email Security

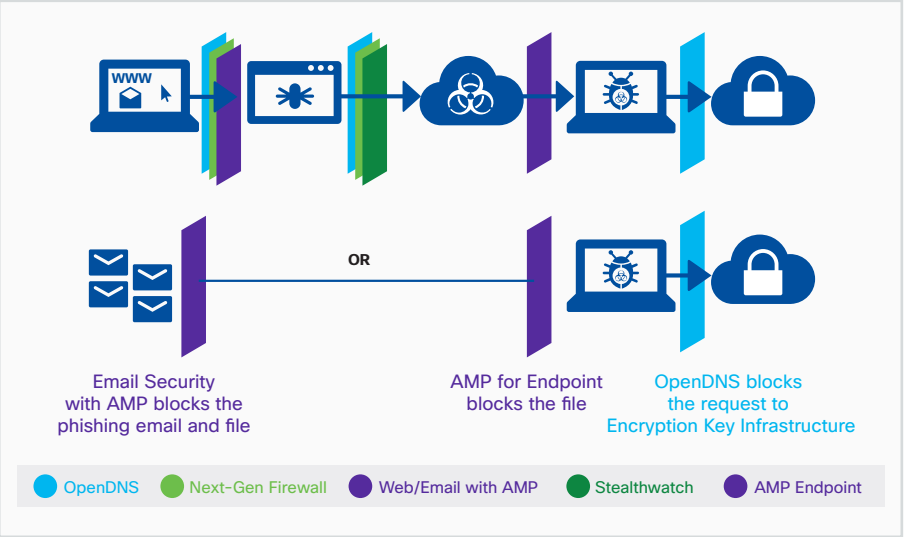
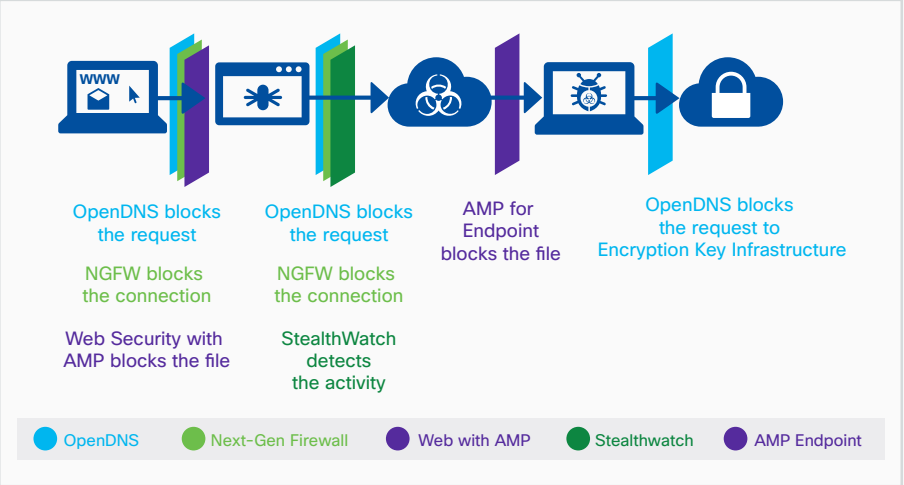


Figure 6. Web Security



The NGFW can used with AMP for Endpoints. Then, if it is aware of malicious C2 servers on the Internet, it can block phone-home attempts. The NGFW prevents ransomware from running while AMP finds and removes the malicious files.

Stealthwatch brings the network as a sensor and the network as an enforcer to work in concert along with ISE. Together they can identify ransomware traffic on the network and automatically quarantine suspect devices.

Security for Branch Locations

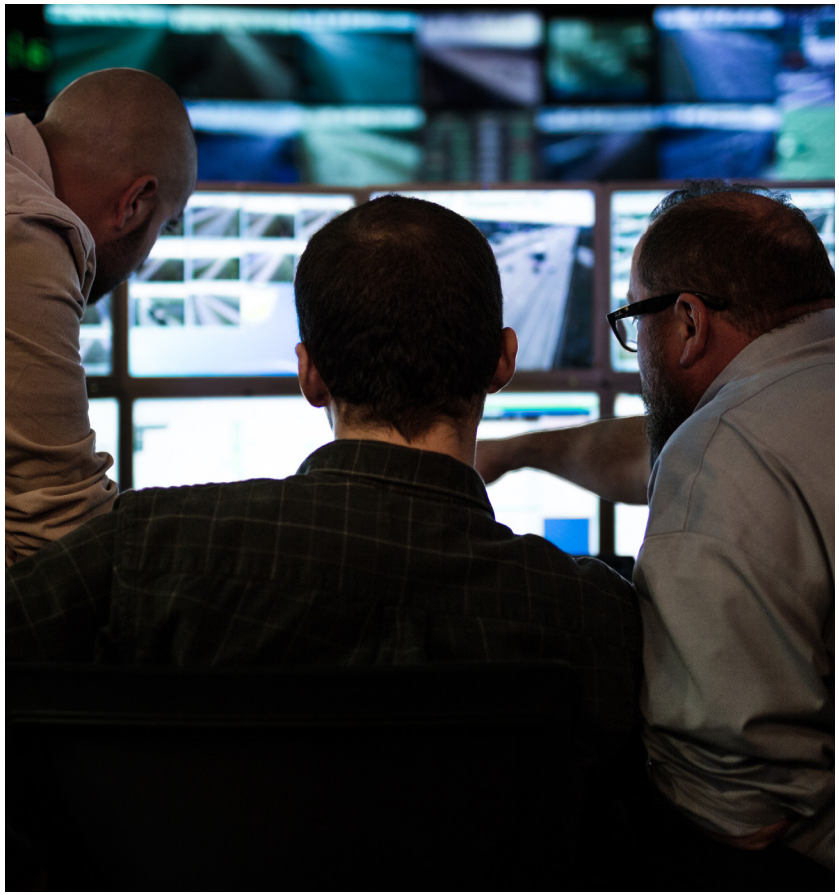
Branch locations that want direct Internet access but also protection against ransomware can set up OpenDNS Umbrella for an initial layer of protection. Cisco Firepower™ Threat Defense for Cisco Integrated Services Routers, including AMP, can also be activated to boost security at the branch. Both these deployments reduce WAN costs with no need to backhaul traffic.

For More Information

To learn more about fighting ransomware, check out our webinars: https://security-mktg.cisco.com/CiscoSecurityWebinarSeries.

Read the Talos blog post: Ransomware: Past, Present and Future.

Visit: www.cisco.com/go/ransomware.



C11-737871-00 09/16