Ransomware–Detection and Prevention via Hillstone's Intelligent Next-Generation Firewall

Overview

On Black Friday 2016, a powerful ransomware attack slammed San Francisco's Muni light rail system [1], threatening to destroy more than 30GB of critical database, email, staff training, payroll, ticketing and other system data, unless Muni paid perpetrators 100 Bitcoin (worth roughly $70,000). Muni refused, throwing its ticketing system offline for two days, and forcing the agency to absorb thousands of free passenger rides.

Cisco's 2016 Midyear Cybersecurity Report [2], declares ransomware "the most profitable malware type in history," echoing other studies that have tracked ransomware's rapid ascendance to one of the most prevalent and virulent enterprise security threats across all business sectors. According to a June 2016 Osterman Research survey [3], almost one out of every three surveyed organizations suffered a ransomware attack in the previous 12 months.

Ransomware locks businesses out of their systems by encrypting critical data, decrypting it only after the victim pays the attackers a monetary ransom. One reason this threat has become so widespread and effective is the ease with which hackers can acquire and leverage ransomware tools. Usable ransomware source code is easily available across several sites on the Internet.

Once infected, owners can choose to hire security professionals to disinfect their systems. Unfortunately, the entire process can take hours, days or weeks, at a cost likely much higher than the ransom demanded by attackers. That's why so many business owners simply pay the ransom so they can get back to work as soon as possible, and why ransomware is such a profitable, rapidly growing exploit.

With the rapid rise in ransomware attacks, enterprises and organizations are hard pressed to find and deploy viable security solutions that can detect and mitigate these attacks early, quickly and effectively before they can wreak their damage.

Hillstone Intelligent Next-Generation Firewall (iNGFW) is just such a solution, employing a uniquely architected multilayered defense to detect and mitigate ransomware before it can do any business damage. iNGFW's layered defense (see Figure 1) leverages several high-level security engines to protect against Ransomware threats: Antivirus (AV), Intrusion Prevention System (IPS), Advanced Threat Detection (ATD), Abnormal Behavior Detection (ABD) and Reputation Detection (RPD) and so on. With its layered defense, Hillstone Intelligent Next-Generation Firewall can detect and mitigate even the most sophisticated and rapidly evolving ransomware variants at any or all attack stages, including post breach.

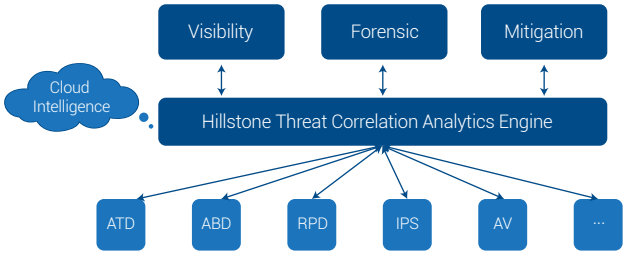


Figure 1. Hillstone iNGFW System Architecture

To illustrate the full power of iNGFW's ransomware defense, we've laid out the steps of a typical ransomware exploit followed by a detailed description of how Hillstone intelligent Next-Generation Firewall (iNGFW) can detect and mitigate the threat at any stage.

Example: Locky Ransomware Attack

Locky ransomware is one of the most prevalent ransomware exploits on the Internet. A typical Locky ransomware attack, illustrated in Figure 2, takes the following steps to cripple systems and extract ransom:

- Attacker sends spam email with malicious attachments to scores of your organization's staff members.
- Thanks to the attacker's sophisticated social engineering tactics, one or more victims is tricked into clicking and executing the attachment.
- The attachment's malicious payload executes, connects to a ransomware hosting server over the Internet and downloads a copy of Locky ransomware into the corporate network.
- Upon execution, Locky ransomware secretly installs itself on the network and contacts a command-and-control (CnC) server over the Internet to retrieve an encryption key, which it uses to encrypt critical local files and network shared folders.
- Once encryption is complete, the Locky ransomware pops up a window on the user system, demanding ransom in return for recovering the encrypted files.

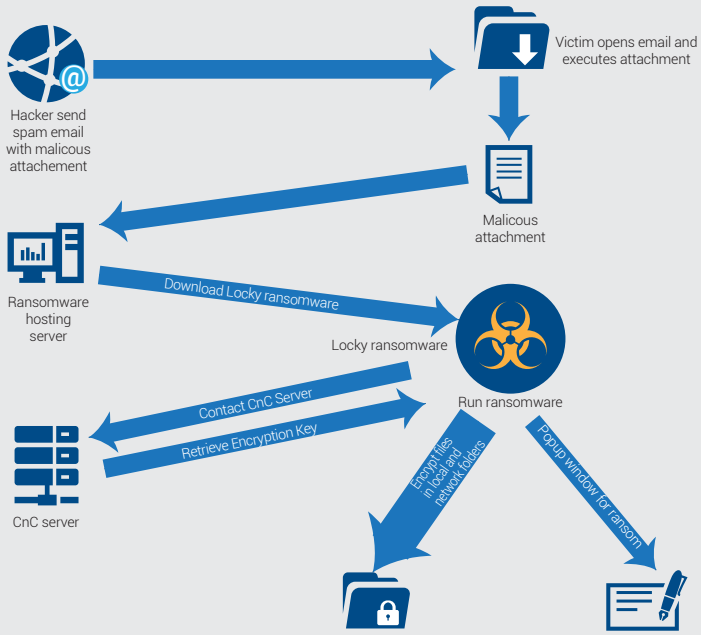


Figure 2. Typical Locky Ransomware Attack

These are just the tactics and steps used to attack San Francisco's Light Rail System, tricking a Light Rail System employee into executing a malicious email attachment.

Multilayered Ransomware Detection and Prevention via Hillstone Intelligence Next-Generation Firewall

The following use case demonstrates how iNGFW's layered defense detects and mitigates an incoming Locky ransomware attack.

- iNGFW's Antivirus Engine (AV) scans all incoming email for malware, and detects and quarantines any infected attachments. As illustrated in Figure 3, Hillstone iNGFW's antivirus engine detects and recognizes the ransomware payload as Trojan/Generic.ASMalwRG.70 and quarantines it.

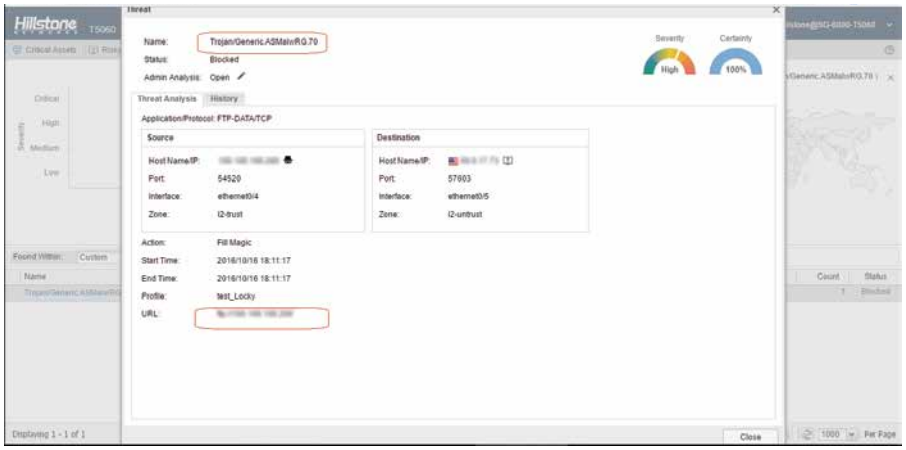


Figure 3. iNGFW Device Detect Locky Ransomware Attachment

- In the unlikely event the malicious attachment makes it through the Antivirus detection engine unscathed, is executed by an unwitting user and attempts to connect over the Internet to the CnC server, the iNGFW Reputation Detection Engine leverages a cloud intelligence service (see Figure 4), to recognize the CnC server's ict-net.com domain name from the service's continually updated list of known black domains. It then blocks the connection, preventing the Locky ransomware from downloading into the network. iNGFW's Reputation Detection engine synchronizes with the intelligence service continually to get the very latest domain blacklist updates.

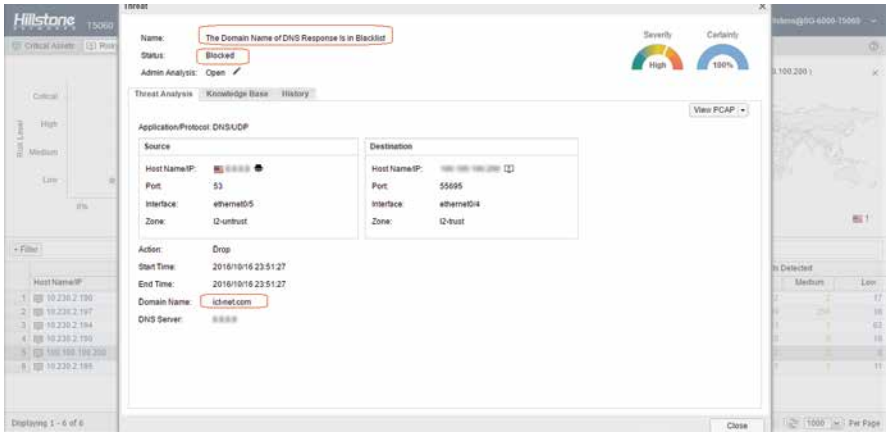
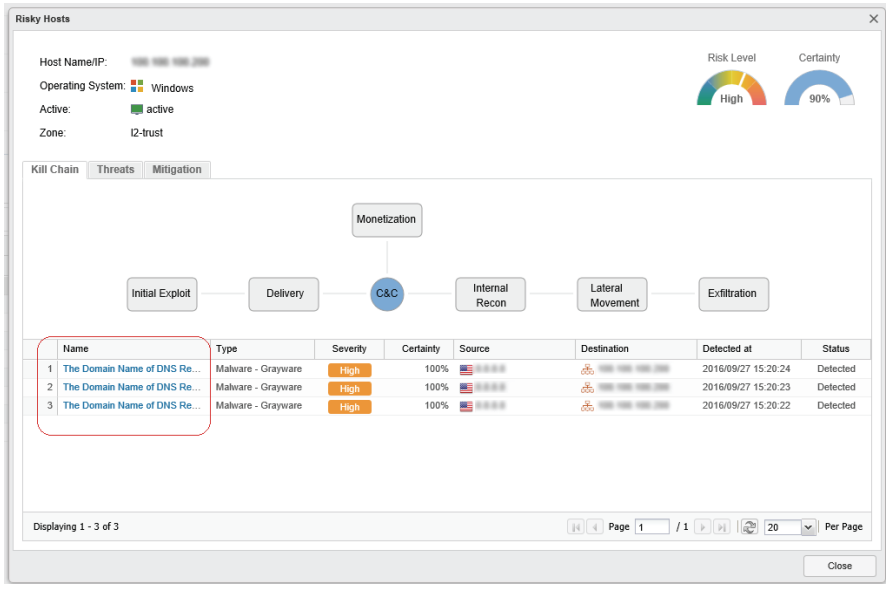


Figure 4. Reputation Detection Engine Blocks the Download of Locky Ransomware

- If Locky ransomware gets past both iNGFW's Antivirus and Reputation Detection Engines and even succeeds in penetrating internal systems, iNGFW's Advanced Threat Detection (ATD) and Abnormal Behavior Detection (ABD) Engines can still detect and mitigate the threat. Rather than depending on attack signatures--as most malware detection engines do--iNGFW's ATD engine leverages machine learning to recognize abnormal and potentially damaging network behavior, such as malware CnC callbacks. On installation, the ABD engine monitors the network over time to build normal network behavior profiles, then subsequently monitors for any behavior abnormalities. The ABD engine includes a module that recognizes domain names generated by Domain Generation Algorithms (DGA), which are used by Locky and many other ransomware attacks. In this case it detects the Locky ransomware attack (See Figure 5) by querying a dypvxigdwyf.org DGA domain and alerts the administrator to take mitigation actions, such as blocking this DGA domain.



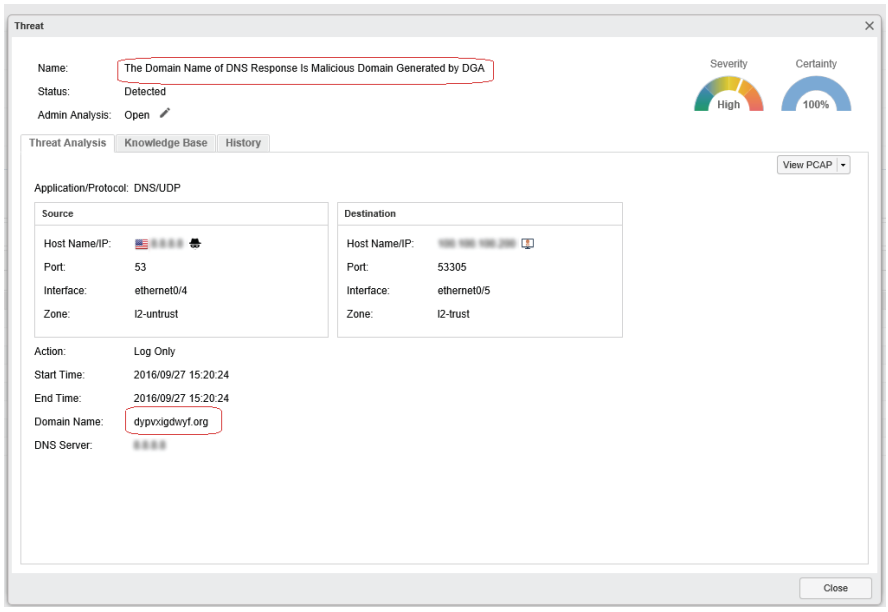


Figure 5. ABD Engine Detects a DGA domain of Locky Ransomware

To ensure any detected abnormalities are not false positives and represent legitimate attacks, iNGFW leverages a correlation engine to analyze and correlate likely threat events reported by multiple detection engines to generate a threat confidence and severity level. For example, the correlation engine would likely correlate an internal host downloading an executable from a HTTP server with initiating a connection to a known external CnC server, thereby increasing the likely threat confidence/severity score. It would then identify the corresponding internal host likely to be infected and alert the system administrator to conduct further investigation. Once the infection is confirmed, system administrators can leverage iNGFW's user interface to take mitigation actions.

iNGFW leverages an entire cloud intelligence ecosystem, ranging from malware to domain to IP reputation feeds. As shown in the ransomware tracker website, https://ransomwaretracker.abuse.ch/tracker crowd sources ransomware related domains. Hillstone's Cloud Intelligence System synchronizes with this ransomware black domain feed and pushes the content to all iNGFW devices to provide up-to-date protections against ransomware threats.

Conclusion

With its sophisticated layered defense, multiple robust threat detection engines, and targeted threat correlation capabilities, Hillstone Intelligent Next-Generation Firewall is the most robust and comprehensive ransomware security solution on the market, able to detect and mitigate ransomware at every stage of its threat trajectory. With Hillstone Intelligent Next-Generation Firewall, organizations can protect themselves from ransomware, even as it evolves with more and more sophisticated threat tactics.

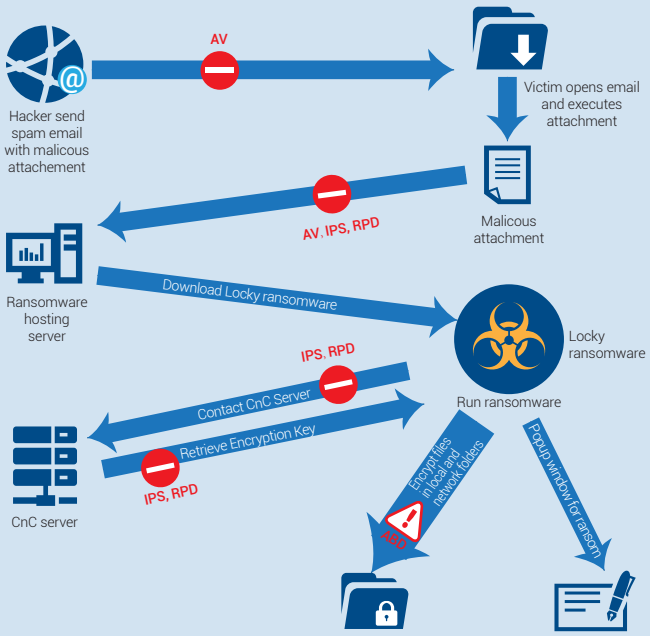


Figure 6. Hillstone iNGFW stop Ransomware Attack

References:

[1] Ransomware Crooks Demand $70,000 After Hacking San Francisco Transport System, http://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/#6a3ec18554dd

[2] Cisco 2016 Midyear Cybersecurity Report, http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html

[3] Osterman Research, Best Practices for Dealing with Phishing and Ransomware, August, 2016, https://dm-mail-inglist.com/subscribe?f=6b1c24a7

How to contact Hillstone Networks

Americas: +1-408-508-6750 | SEA: +65-6678-7660

Europe: +420-721-125-070 | MEA: +971-4557-1493

Email: inquiry@Hillstonenet.com