Detección y Prevensión de Ransomware con Firewall Inteligente de Hillstone Next-Generation

Resumen

El Viernes Negro de 2016, un poderoso ataque de ransomware cerró sistema de tren ligero Muni de San Francisco [1], amenazando con destruir más de 30 GB críticos de la base de datos, correo electrónico, capacitación del personal, nómina, venta de entradas y otros datos del sistema, a menos que Muni pagara a la autores 100 Bitcoin (valor aproximado de US $ 70,000). Muni se negó, desconectando su sistema de boletas durante dos días, y forzando a la agencia de absorber miles de pasajes libres.

A mediados de 2016 el Informe de Ciberseguridad de Cisco [2], declara ransomware "el tipo de malware más rentable de la historia", haciendo eco de otros estudios que han rastreado un rápido ascenso del ransomware como una de las amenazas a la seguridad empresarial más frecuentes y virulentas en todos los sectores.

De acuerdo con una encuesta de Osterman Research en junio de 2016 [3], casi una de cada tres organizaciones encuestadas han sufrido algún ataque de ransomware en los últimos 12 meses.

Ransomware bloquea los sistemas empresariales mediante la encriptación de sus datos críticos, descifrándolos sólo después de que la víctima pague a los atacantes un rescate monetario.

Una de las razones que esta amenaza se ha vuelto tan amplia y efectiva es la facilidad con la que los hackers pueden adquirir herramientas de apalancamiento para ransomware. Hay código fuente utilizable como ransomware fácilmente disponible a través de varios sitios en Internet.

Una vez infectados, los propietarios pueden optar por contratar a profesionales de seguridad para la desinfección de sus sistemas. Desafortunadamente, todo el proceso puede durar horas, días o semanas, a un costo probablemente mucho más alto que el rescate exigido por los atacantes. Es por eso que muchas empresas simplemente pagan el rescate para poder volver al trabajo tan pronto como sea posible, y esa es la razón de que ransomware sea un negocio tan rentable y en rápido crecimiento.

Con el rápido aumento de los ataques ransomware, las empresas y organizaciones se ven en apuros para encontrar e implementar soluciones de seguridad viables que puedan detectar y mitigar estos ataques, rápida y efectivamente antes de que puedan causar daño.

Hillstone Intelligent Next-Generation Firewall (iNGFW) es precisamente esa solución. Esta emplea una defensa de múltiples capas de arquitectura especial para detectar y mitigar el ransomware antes de que pueda causar algún daño a la empresa. La defensa por capas de iNGFW (ver Figura 1) aprovecha varios motores de seguridad de alto nivel de protección contra amenazas ransomware: Antivirus (AV), Sistema de prevención de intrusiones (IPS), Amenaza Detección Avanzada (ATD), Detección de Comportamiento Anormal (ABD) y Detección de Reputación (RPD) y así sucesivamente. Con su defensa en capas, el Hillstone Intelligent Next-Generation Firewall de próxima generación es capaz de detectar y mitigar incluso las variantes de ransomware más sofisticadas y de rápida evolución en cualquier etapas del ataque, incluidos aquellos después de la intrusión.

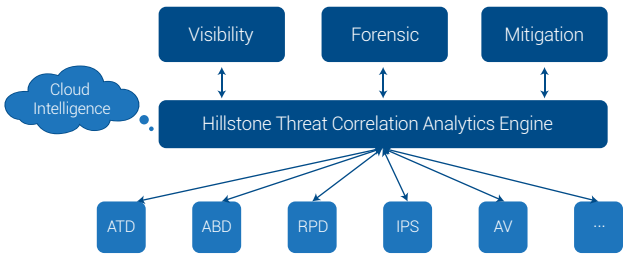


Figura 1. Arquitectura del Sistema Hillstone iNGFW

Para ilustrar el poder defensor de iNGFW, hemos enumerado los pasos de un ransomware típico, seguido de una descripción detallada de la forma inteligente que el Hillstone intelligent Next-Generation Firewall (iNGFW) puede detectar y mitigar la amenaza en cualquier etapa.

Ejemplo: Ataque del Ransomware Locky

El ransomware Locky es una de las amenazas de ransomware más prevalentes en Internet. Un ataque típico Locky ransomware, que se ilustra en la Figura 2, toma las siguientes medidas para paralizar los sistemas y extraer la extorsión:

- El atacante envía spam de correo electrónico con archivos maliciosos adjuntos a decenas de miembros del personal de la organización.
- Gracias a las sofisticadas tácticas de ingeniería social del atacante, engaña a una o más víctimas para que hagan clic y ejecuten el archivo adjunto.
- La carga maliciosa del adjunto se ejecuta, se conecta a un servidor de alojamiento ransomware a través de Internet y descarga una copia de ransomware Locky en la red corporativa.
- Tras la ejecución, el ransomware Locky en secreto se instala en la red y un servidor de contactos (CNC) a través de Internet de mando y control para recuperar una clave de cifrado, que utiliza para cifrar archivos locales críticos y carpetas compartidas en la red.
- Una vez que se haya completado el cifrado, el ransomware Locky despliega una ventana en el sistema del usuario, exigiendo un rescate a cambio de recuperar los archivos cifrados.

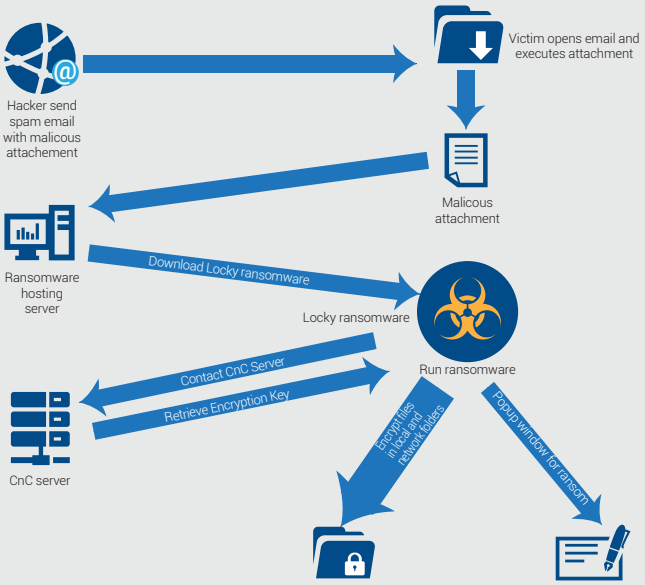


Figura 2. Ataque típico de Locky ransomware

Estas son tan sólo algunas de las tácticas y pasos que fueron utilizados para atacar el sistema del tren ligero de San Francisco, engañando a un empleado para que ejecutara un archivo malicioso adjunto al correo.

Detección y Prevención Inteligente Multicapa de Ransomware vía el Firewall de Próxima Generación de Hillstone

El siguiente caso demuestra cómo el uso de defensa por capas de iNGFW detecta y mitiga un ataque entrante del ransomware Locky.

- El motor antivirus de iNGFW (AV) explora todo el correo entrante en busca de malware, y detecta y pone en cuarentena los archivos adjuntos infectados. Como se ilustra en la Figura 3, el motor antivirus de Hillstone iNGFW detecta y reconoce la carga útil del ransomware como Trojan/Generic.ASMalwRG.70 y lo pone en cuarentena.

- En el caso improbable de que los datos adjuntos maliciosos logren burlar el motor de detección antivirus indemnes, fueran ejecutados por un usuario involuntariamente e intentara conectarse por Internet al servidor de control

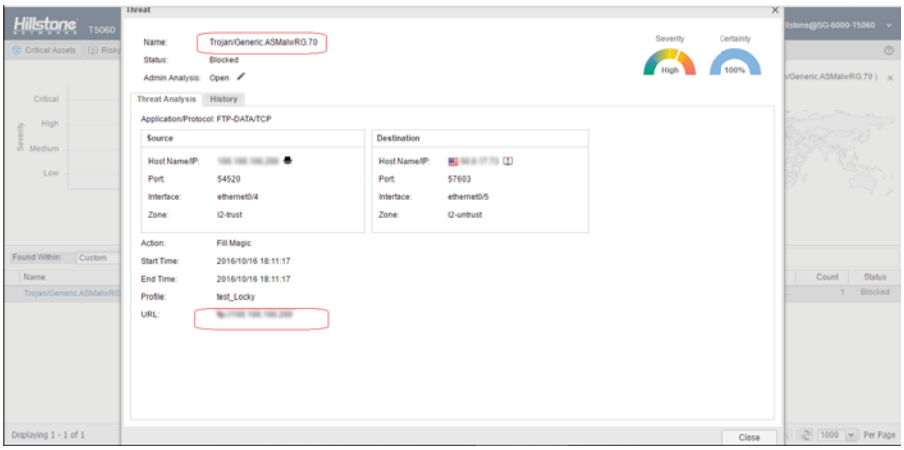


Figure 3. iNGFW Device Detect Locky Ransomware Attachment

numérico, el motor de detección de reputación iNGFW aprovecha un servicio de inteligencia en la nube (véase la Figura 4), para reconocer el nombre de dominio del servidor ict-net.com CNC desde el servicio en la lista negra de dominios conocidos y actualizada continuamente. Paso siguiente, bloquearía la conexión, evitando que el ransomware Locky se descargue de la red. El motor de detección de reputación de iNGFW se sincroniza con el servicio de inteligencia continuamente para obtener las últimas actualizaciones de la lista negra de dominios.

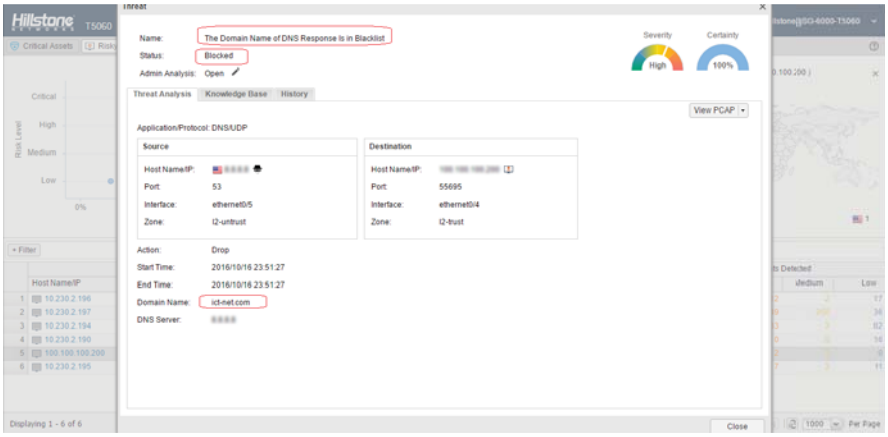
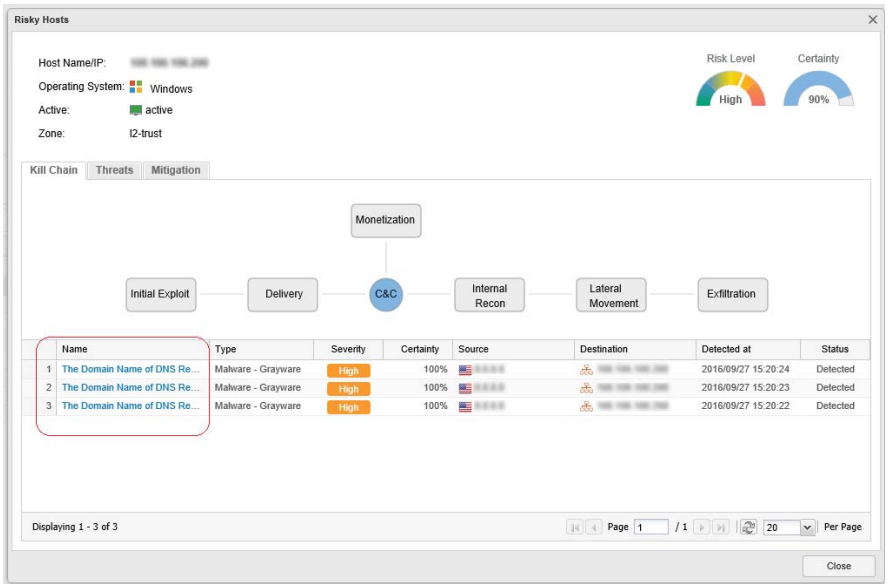


Figura 4. El motor de detección de reputación bloquea la descarga del ransomware Locky

- Si el ransomware Locky lograra traspasar más allá tanto del iNGFW Antivirus como de los motores de detección de reputación e incluso consigue penetrar en los sistemas internos, la Detección Avanzada de Amenazas de iNGFW (ATD) y los motores de detección de comportamiento anormal (ABD) aún pueden detectar y mitigar la amenaza. En lugar de depender de las firmas de ataques - como hacen la mayoría de motores de detección de malware - el motor ATD de iNGFW aprovecha el aprendizaje de máquina para reconocer el comportamiento anormal de la red y el comportamiento potencialmente perjudicial, tales como los callback del malware CnC. Al instalar, el motor ABD monitoriza la red a lo largo del tiempo para construir perfiles de comportamiento normal de la red, posteriormente monitorea cualquier presencia de anomalías en el comportamiento. El motor ABD incluye un módulo que reconoce los nombres de dominio generados por algoritmos de generación de dominio (DGA), utilizados por Locky y muchos otros ataques ransomware. En este caso, detecta el ataque de ransomware de Locky (Ver Figura 5) mediante la consulta de dominio DGA en dypvxigdwyf.org y alerta al administrador para que tome acciones de mitigación, tales como el bloqueo de este dominio DGA. Hillstone CloudHive es una solución de seguridad avanzada, diseñada desde cero para las exigencias del centro de datos virtual, multiusuario y multi-nube habilitado.



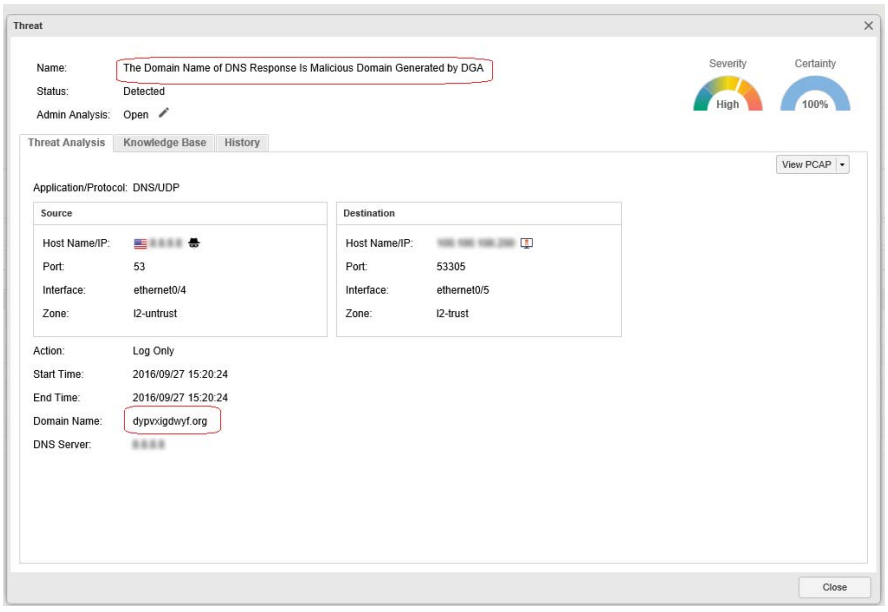


Figura 5. El motor ABD detecta el dominio DGA de Locky

Para asegurar que cualquier anomalía detectada no sea un falso positivo o represente un ataque ilegítimo, iNGFW aprovecha un motor de correlación para analizar y correlacionar eventos de amenazas probables reportadas por varios motores de detección para generar un nivel de confianza y nivel de gravedad. Por ejemplo, el motor de correlación probablemente correlacionaría un host interno descargando un ejecutable desde un servidor HTTP con el inicio de una conexión a un servidor CnC externo y conocido, lo que aumentaría la puntuación confianza/gravedad de una probable amenaza. Luego identificaría el host interno correspondiente con probabilidad de ser infectado y alertaría al administrador del sistema para que investigara más a fondo. Una vez que se ha confirmado la infección, los administradores de sistemas pueden aprovechar la interfaz de usuario de iNGFW para tomar acciones de mitigación.

El iNGFW aprovecha todo un ecosistema de inteligencia en la nube, que va desde el malware, pasando por los dominios, hasta los feeds de reputación IP. Como se muestra en la página web del tracker de ransomware, https://ransomwaretracker.abuse.ch/tracker de dominios relacionados ransomware alimentados por el público. Sistema de Inteligencia en la Nube de Hillstone sincroniza los feeds de dominios ransomware en lista negra y empuja el contenido a todos los dispositivos iNGFW para proporcionar protección actualizada contra las amenazas ransomware.

Conclusión

Con su defensa sofisticada en capas, varios motores robustos para la detección de amenazas y su capacidad para la correlación de amenazas específicas, el firewall inteligente de próxima generación de Hillstone es la solución de seguridad más robusta y completa del mercado contra el ransomware, capaz de detectar y mitigar ransomware en cada etapa de su trayectoria.

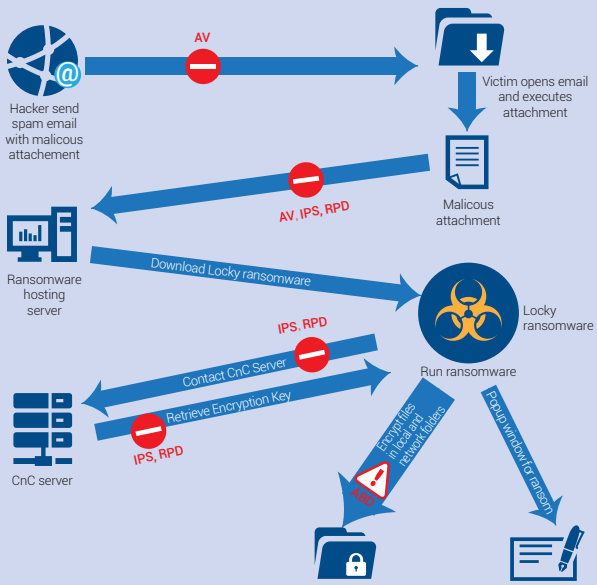


Figure 6. Hillstone iNGFW stop Ransomware Attack

Referencias:

[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

Como contactarse con Hillstone Networks

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

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

Email: inquiry@Hillstonenet.com