IMPORTANTE

Nueva variante de Ransomware

BADRABBIT

(Documento versión 1.2 – 25/oct/2017)

El 24 de octubre de 2017, la mayoría de firmas de seguridad detecto una nueva variante de Ransomware, la cual se ha estado distribuyendo en grandes cantidades en todo el mundo. Esta nueva variante tiene el nombre de Bad Rabbit, y comparte muchas similitudes al Ransomware llamado Petya.

¿Qué hace Bad Rabbit?

Bad Rabbit es un ransowmare de cifrado de discos duros y archivos individuales. Solicita se realice un pago con BitCoin para que sea entregada la llave para descifrar la información.

¿Vectores de infección?

- Por medio de un correo de Phishing, se solicita la descarga de un instalador de Flash, desde un sitio fraudulento
- Una vez infectado el equipo, utiliza mecanismos de comunicaciones de redes de Windows para infectar los equipos vecinos de la red
    - SVCCTL: the remote service management
    - SMB2
    - SMB
    - NTLMSSP authentication brute force

Recomendaciones Generales:

- Asegurese que sus soluciones de seguridad se encuentren actualizadas.
- NO descarguen o ejecuten programas sugeridos por un correo electrónico.
- Verifique las bitácoras de las soluciones de seguridad, si una computadora presenta signos de comunicación errática por los servicios antes mencionados de Microsoft, o intenta comunicación a los sitios indicadores de compromiso, desconéctela de la red y proceda a sanitizarla.

Indicadores de compromiso:

- Comunicación a los siguientes sitios:
  - 1dnscontrol[.]com
  - Argumentiru[.]com
  - Fontanka[.]ru
  - Adblibri[.]ro
  - Spbvoditel[.]ru
  - Grupovo[.]bg
  - www.sinematurk[.]com
- Abuso de utilización de los siguientes mecanismos:
  - SVCCTL: the remote service management
  - SMB2
  - SMB
  - NTLMSSP authentication brute force
- Nuevas tareas programadas en los equipos de usuario, con los siguientes nombres:
  - viserion_
  - rhaegal
  - drogon

Recomendaciones específicas para las soluciones de seguridad:

Cisco FirePOWER

Actualice la librería VDB a la última versión, por lo menos versión 290; verifique que los siguientes filtros esten activos en modalidad de notificación para segmentos de redes internas y en modalidad de bloqueo para segmentos de redes públicas:

Microsoft Security Bulletin MS17-010 Security Update for Windows SMB Server	Microsoft Windows Server Message Block Service Arbitrary Code Execution Vulnerability	–	9.8	CVE-2017-0143
Microsoft Security Bulletin MS17-010 Security Update for Windows SMB Server	Microsoft Windows Server Message Block Service Arbitrary Code Execution Vulnerability	–	9.8	CVE-2017-0144
Microsoft Security Bulletin MS17-010 Security Update for Windows SMB Server	Microsoft Windows Server Message Block Service Arbitrary Code Execution Vulnerability	–	9.8	CVE-2017-0145
Microsoft Security Bulletin MS17-010 Security Update for Windows SMB Server	Microsoft Windows Server Message Block Service Arbitrary Code Execution Vulnerability	–	9.8	CVE-2017-0146
Microsoft Security Bulletin MS17-010 Security Update for Windows SMB Server	Microsoft Windows Server Message Block Service Information Disclosure Vulnerability	–	7.5	CVE-2017-0147
Microsoft Security Bulletin MS17-010 Security Update for Windows SMB Server	Microsoft Windows Server Message Block Service Arbitrary Code Execution Vulnerability	–	9.8	CVE-2017-0148
Microsoft Security Bulletin MS17-012 Security Update for Microsoft Windows	Microsoft Windows SMB Tree Connect Response Denial of Service Vulnerability	Microsoft Windows SMB Stack Overflow	7.5	CVE-2017-0016
Microsoft Security Bulletin MS17-012 Security Update for Microsoft Windows	Microsoft Windows DNS Query Information Disclosure Vulnerability	–	4.3	CVE-2017-0057
Microsoft Security Bulletin MS17-019 Security Update for Active Directory Federation Services	Microsoft Windows Active Directory Federation Services Information Disclosure Vulnerability	–	4.3	CVE-2017-0043

La actualización de reglas del 25 de octubre ya incluye protección especifica contra Bad Rabbit, por medio de las siguientes reglas, que por defecto se activan en el equipo:

* 1:44650 <-> ENABLED <-> MALWARE-OTHER Win.Ransomware.BadRabbit propagation via SMB transfer attempt (malware-other.rules)
* 1:44649 <-> ENABLED <-> MALWARE-OTHER Win.Ransomware.BadRabbit propagation via SMB2 transfer attempt (malware-other.rules)
* 1:44648 <-> ENABLED <-> MALWARE-OTHER Win.Ransomware.BadRabbit propagation via SMB transfer attempt (malware-other.rules)
* 1:44647 <-> ENABLED <-> MALWARE-OTHER Win.Ransomware.BadRabbit propagation via SMB2 transfer attempt (malware-other.rules)
* 1:44646 <-> ENABLED <-> MALWARE-OTHER Win.Ransomware.BadRabbit propagation via SVCCTL remote service attempt (malware-other.rules)

KASPERSKY

Kaspersky Lab's detecto el ataque con el siguiente veredicto:

Trojan-Ransom.Win32.Gen.ftl
DangerousObject.Multi.Generic
PDM:Trojan.Win32.Generic

Para evitar ser víctima de "Bad Rabbit":

- Actualizar las bases de datos de antivirus de forma inmediata.
- asegúrese de que todos los mecanismos de protección estén activados como se recomienda; y que los componentes KSN y System Watcher (que están habilitados por defecto) no están deshabilitados.
- Asegurar que el componente de System Watcher y Kaspersky Security Network este corriendo.
- Bloquee la ejecución de los archivos c:\windows\infpub.dat and c:\Windows\cscc.dat.
- Deshabilite el servicio WMI (si es posible en su entorno) para evitar que el malware se propague a través de su red.
- Configurar y habilitar el modo Denegar predeterminado en el componente Control de inicio de aplicaciones de Kaspersky Endpoint Security para garantizar y hacer cumplir la defensa proactiva contra este y otros ataques.
- Haga una copia de seguridad de sus datos.
- No pague por el rescate.

Ref:
https://www.kaspersky.com/blog/bad-rabbit-ransomware/19887/

Palo Alto

Para poder mitigar los ataques de Bad Rabbit con Palo Alto se debe contar con las suscripciones de WildFire, Threat Prevention, URL Filtering como mínimo al día 24 de octubre del 2017.
A continuación se detalla de qué forma mitiga los ataques de Bad Rabbit cada una de las 3 suscripciones de Palo Alto:

1. WildFire:

Clasifica todas las muestras conocidas como malware, bloqueando automáticamente la entrega de contenido malicioso a los usuarios.

2. Threat Prevention:

Bloquea cargas útiles maliciosas y actividad DNS C2. Los clientes pueden consultar los ID de amenaza 3088946, así como las firmas de Virus / WIn32.WGeneric.nkrca y Virus / Win32.WGeneric.nkquc

3. URL Filtering:

Bloquea todas las URLs de inyección conocidas.
Para información más detallada favor consulta el siguiente link.
https://researchcenter.paloaltonetworks.com/2017/10/threat-brief-information-bad-rabbit-ransomware-attacks

SOPHOS

Los clientes de Sophos Intercept X y Exploit Prevention estaban protegidos contra este ataque de manera proactiva, sin necesidad de actualizaciones.

Para obtener más información sobre la protección en otros productos de Sophos, consulte la tabla a continuación:

Sophos product	Protection Available from	Action needed
Endpoint and Server products		
Endpoint Protection	October 24, 2017 18:48 UTC	Ensure Sophos is up to date
Intercept X	Already protected	None required
Endpoint Exploit Prevention (EXP)	Already protected	None required
Server Protection	October 24, 2017 18:48 UTC	Ensure Sophos is up to date
Sophos Home	October 24, 2017 18:48 UTC	Ensure Sophos is up to date

Ref:
https://community.sophos.com/kb/en-us/127730

TrendMicro TippingPoint

Actualizar la librería de Digital Vaccine (DV) a la versión 1429. verifique que los siguientes filtros esten activos en modalidad de notificación para segmentos de redes internas y en modalidad de bloqueo para segmentos de redes públicas:

1) 27931: SMB: Microsoft Windows SMBv1 Information Disclosure Vulnerability (EternalRomance)
2) 27928: SMB: Microsoft Windows SMB Remote Code Execution Vulnerability (EternalBlue)
3) 28471: SMB: SMBv1 Successful Protocol Negotiation

Ante cualquier inquietud por favor contáctenos al +502 24104329 o +502 23294329.

SISAP