A3SEC S.A.S. Colombia, Carrera 49 No. 94 - 76 Oficina 304 Bogotá D.C. COLOMBIA T. +57 (1) 309 95 33 M. +57 300 352 81 21 M. +57 318 715 93 50

ALERTA DE SEGURIDAD

Contenido

NIVEL DE ALERTA

Muy Alta

DESCRIPCIÓN DE LA AMENAZA

El **Centro de Seguridad y Vigilancia Digital** de A3SEC ha sido alertado de un ataque masivo del Ransonware **NYETYA** denominado asi por (**Cisco Talos - Comprehensive Threat Intelligence).** Este malware es una variante más de **WannaCRy y Petya**. **NYETYA** es un ransonware que se identificó el **28/06/2017** haciendo su primera aparición en **UCRANIA** en organizaciones gubernamentales, su ejecución es llevada a cabo atreves de una **actualización de un software de gestión de impuestos llamado MeDoc**, ya se ha identificado que este malware se ha esparcido a diferentes países como lo son España, Francia, Dinamarca, Reino Unido, Rusia y EE.UU. Igualmente, como las anteriores versiones de esta famila de Ransoware su comportamiento es similar al momento de sobre escribir **master boot record (MBR)** y cifrarlo.

Lo curioso de esta variante de **PETYA** es que **NYETYA** no tiene fin financiero, puesto que el sitio donde se solicita hacer el pago para la **key de decifrado** esta caída, además su comportamiento sobre el footprinting del sistema infectado es mucho más profunda.

El ransoware una vez haya sido exitoso o no al momento de hacer la escala de privilegios atreves de **Adjust TokenPrivilege,** pasa a sobre escribir el **master boot record** ,después el malware inicia un mapeo de red atreves del puerto 139-TCP **NetBIOS,** así de esta manera encontrar posibles maquinas vulnerables a **CVE-2017-0199 especialmente a EternalBlue y EternalRomance,** una vez el malware este dentro de la maquina este creara un archivo en los temporales basado en una herramienta llamada ***Mimikatz*** el cual recolectara credenciales de usuarios desde la memoria .

SISTEMAS AFECTADOS

- Windows XP
- Windows 2003
- Windows 2008
- Microsoft Windows Vista SP2
- Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows 8.1 for 32-bit Systems
- Windows 8.1 for x64-based Systems
- Windows RT 8.1
- Windows Server 2012 and R2
- Windows 10
- Windows Server 2016
- Microsoft Office 2010 Service Pack 2 (32-bit editions)
- Microsoft Office 2010 Service Pack 2 (64-bit editions)

ACCIONES RECOMENDADAS

- Identificar si hay equipos vulnerables con InsightVM (aka Nexpose) utilizando la firma **CVE-2017-0143,** Puede descargar una versión de prueba de InsightVM desde https://www.rapid7.com/products/insightvm/download/virtual-appliance/, en formato OVA, y luego montarla en cualquier sistema de virtualización, incluido Virtualbox. Recibirá en su correo un serial para el periodo de prueba.

- Borrar todo los archivos en %TEMP%, lo más frecuentemente posible , puede acceder a ella con la combinación de teclas (**win + r)** y escriba %TEMP% y borre todo lo que se encuentre dentro de esa carpeta.

- Seguir instrucciones acerca como fortalecer el puerto **139 TCP/UDP** (ver link)

- Crear un archivo en la ruta **C:\Windows\perfc.dat y** establecerle permisos de solo lectura.

- Instalar en los equipos vulnerables el boletín MS17-010 (Kb 4013389).

- Si ya fue víctima del ataque manténgase actualizado a través de las redes sociales sobre los avances que hay para solucionar el problema #Nyetya.

REFERENCIAS

NOTICIA: New Ransomware Variant "Nyetya" Compromises Systems Worldwide

http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html?m=1

MICROSOFT: Microsoft Security Bulletin MS17-010 - Critical

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

CVE: Escala de privilegios Adjust TokenPrivilege

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-4113

MICROSOFT: Microsoft Security Bulletin MS14-058 - Critical

https://technet.microsoft.com/en-us/library/security/ms14-058.aspx

PORT 139 DETAILS:

https://www.speedguide.net/port.php?port=139