MALWARE KEYMARBLE RAT

17 de Agosto del 2018
CONFIDENCIAL

MALWARE KEYMARBLE RAT

NIVEL DE ALERTA

Crítica
Sin CVE asociado a la fecha

PRODUCTOS AFECTADOS

A continuación, se relacionan los sistemas operativos que son vulnerables:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10

DESCRIPCIÓN DEL MALWARE

El 9 de Agosto del 2018, el Departamento de Seguridad Nacional (DHS) y el FBI de los Estados Unidos identificaron un nuevo malware **troyano** llamado *KEYMARBLE* utilizado por el gobierno de Corea del Norte en su proyecto *HIDDEN COBRA*.

El malware es un archivo ejecutable de Windows de 32 bits que funciona como un RAT (Remote Access Trojan) y es capaz de acceder a los datos de configuración del dispositivo, descargar archivos adicionales, ejecutar comandos, modificar el registro, realizar capturas de pantalla y extraer datos; cuando se ejecuta, desactiva las interfaces de programación de aplicaciones (API) y utiliza el puerto 443 para intentar conectarse a las siguientes direcciones IP:

100.43.153.60
104.194.160.59
212.143.21.43

El análisis revela que el malware usa un algoritmo criptográfico XOR personalizado para asegurar sus transferencias de datos y sesiones de comando y control. Está diseñado para aceptar instrucciones del servidor remoto y realizar las siguientes funciones:

- Descargar y subir archivos
- Ejecutar cargas secundarias
- Ejecutar comandos de shell
- Terminar procesos en ejecución

- Borrar archivos
- Buscar archivos
- Establecer atributos de archivo
- Crear entradas de registro para almacenar datos: *(HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ WABE \ DataPath)*
- Recopilar información de los dispositivos de almacenamiento instalados (espacio libre en el disco y su tipo)
- Lista de información de procesos en ejecución
- Realizar capturas de pantalla
- Recopilar y enviar información sobre el sistema de la víctima (sistema operativo, CPU, dirección MAC, nombre de la computadora, configuración de idioma, lista de dispositivos de disco y su tipo, tiempo transcurrido desde que se inició el sistema e identificador único del sistema de la víctima)

Actualmente, las casas de antivirus que ya tienen mapeada la firma del malware son las siguientes:

Antivirus	
Ahnlab	Trojan/Win32.Agent
Antiy	Trojan/Win32.AGeneric
Avira	TR/Agent.rhagj
BitDefender	Trojan.GenericKD.4837544
ESET	a variant of Win32/NukeSped.H trojan
Emsisoft	Trojan.GenericKD.4837544 (B)
Ikarus	Trojan.Agent
K7	Trojan (0050e4401)
McAfee	GenericRXBP-FF!704D491C155A
NANOAV	Trojan.Win32.Agent.eqcfki
NetGate	Trojan.Win32.Malware
Quick Heal	Trojan.IGENERIC
Symantec	Process timed out
TACHYON	Trojan/W32.Agent.126976.CTO
Zillya!	Trojan.NukeSped.Win32.5

INDICADORES DE COMPROMISO (IoC)

A continuación, se relacionan los indicadores de compromiso que a la fecha se han identificado:

Archivo (SHA256)	e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09
Dominios	KRYPT.COM SERVPAC.COM
URL	Sin URL´s conocidas a la fecha
Direcciones IP	100.43.153.60 104.194.160.59 212.143.21.43
Puertos	TCP 443

RECOMENDACIONES

Desde el Centro de Seguridad y Vigilancia Digital, se realizan las siguientes recomendaciones:

1. Bloquear los dominios y direcciones IP mencionados en los IoC desde el Firewall; esto como mecanismo de contención para bloquear la comunicación entre el atacante y su objetivo (en caso de que la estación de trabajo se encuentre infectada y la organización aún no tenga conocimiento de esto).

2. Mantener firmas y motores de antivirus actualizados.

3. Mantener los parches del sistema operativo actualizados.

4. Tener cuidado al abrir archivos adjuntos de correo electrónico, incluso si el archivo adjunto se espera y el remitente parece ser conocido.

5. Generar fullscan periódico a las estaciones de trabajo de la Organización; escanee y elimine archivos adjuntos de correo electrónico sospechosos; asegúrese de que el archivo adjunto escaneado sea su "tipo de archivo verdadero" (es decir, la extensión coincide con el encabezado del archivo).

6. Deshabilitar los servicios de uso compartido de archivos e impresoras. Si estos servicios son necesarios, usar contraseñas seguras o autenticación de Active Directory.

7. Restrinjir los permisos de los usuarios para instalar y ejecutar aplicaciones de software no deseadas. No agregar usuarios al grupo de administradores locales a menos que sea necesario.

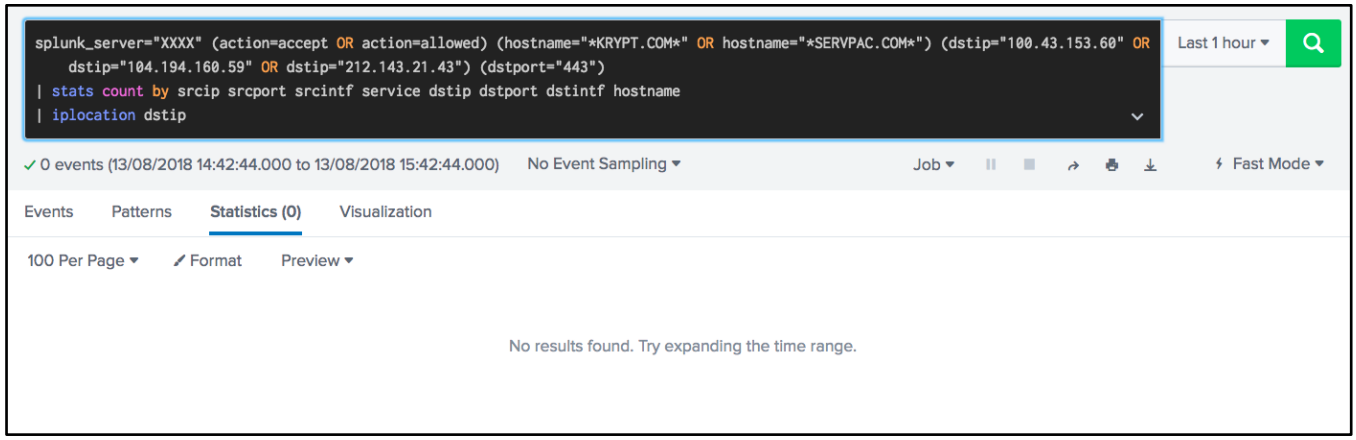
8. Hacer cumplir una política de contraseña segura e implementar cambios regulares de contraseña.

9. Monitorear los hábitos de navegación web de los usuarios; restringir el acceso a sitios con contenido malicioso.

10. Tener cuidado al usar medios extraíbles (por ejemplo, unidades de almacenamiento USB, unidades externas, CD, etc.).

11. Escanear todo el software descargado de Internet antes de la ejecución.

Adicional, desde el CSVD (Centro de Seguridad y Vigilancia Digital), se configuró la respectiva alerta de manera que se active cuando se identifique tráfico permitido a los dominios utilizados para la comunicación entre el atacante y la estación de trabajo.



REFERENCIAS

https://www.us-cert.gov/ncas/analysis-reports/AR18-221A

https://otx.alienvault.com/pulse/5b6d552dacee62457f95910e?utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_subscribed

https://blog.joshlemon.com.au/keymarble/

https://csrc.nist.gov/publications/detail/sp/800-83/archive/2005-11-23

A3SEC. ESPAÑA C/ Aravaca, 6 2º Piso 28040 Madrid, España T.+34 915330978	**A3SEC S.A.S** Carrera 49A # 94-76 Oficina 304 Edificio Empresarial Castellana Bogotá, COLOMBIA **T.**+57 1 3099533	**A3SEC USA** 1401 Brickell Ave #320 Miami, FL 33131, USA T. +1 786 556 90 32	**A3SEC. México** Shakespeare 30 Piso 2 Anzures 11590, Miguel Hidalgo Tel.+52 55 7822 8093 CDMX