Nro. Alerta:	AL-2023-058	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	06-dic-2023	**Malware Konni RAT se propaga a través de archivos de Word maliciosos**	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Código Malicioso
Tipo de incidente: Malware
Nivel de riesgo: Medio

II. ALERTA

Investigadores detectaron nuevas campañas activas del malware Konni RAT; los actores de amenazas, envían archivos de Word con macros maliciosas a los usuarios de Windows objetivo, lo que infecta los sistemas.

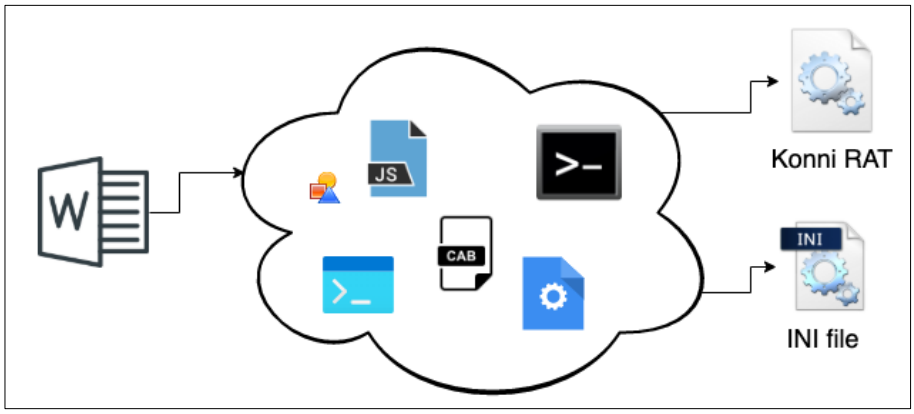


Figura 1.- *Ataque* AtomicStealer – *figura referencial*
Fuente: https://www.malwarebytes.com/blog/threat-intelligence/2022/01/konni-evolves-into-stealthier-rat

III. INTRODUCCIÓN

Investigadores del fabricante Fortinet, detectaron campañas activas del malware Konni RAT. Los atacantes envían archivos de Word con macros maliciosas a los usuarios de Windows objetivo lo que infecta los sistemas. En cuanto al malware, Konni RAT es una amenaza conocida que anteriormente apareció en las noticias por atacar a Rusia y Corea del Norte. Es un potente troyano de acceso remoto que exhibe varias capacidades maliciosas, como robar credenciales, ejecutar comandos con privilegios elevados y

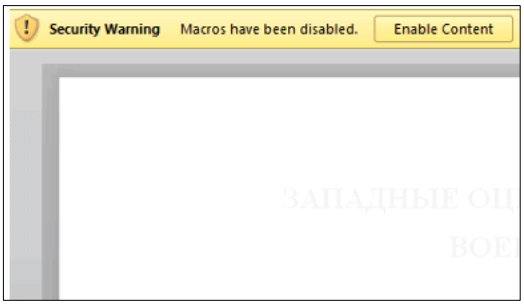
cargar/descargar archivos en los dispositivos de destino. En una campaña reciente, los investigadores descubrieron que el ataque se inició cuando una víctima recibió un documento de Word creado con fines malintencionados. Este documento engaña a los usuarios para que lo abran haciéndose pasar por archivos adjuntos legítimos, como facturas o contratos. Cuando se hace clic, el documento de Word le pide al usuario que habilite el contenido, lo que ejecuta un script VBA que descarga aún más scripts por lotes maliciosos.

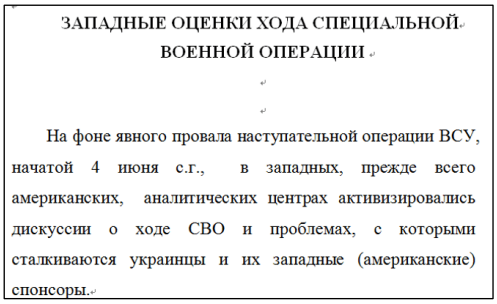
Este script valida la información del sistema, particularmente para Windows y luego realiza las acciones relevantes para permanecer oculto, incluida la omisión de UAC y la obtención de acceso a privilegios elevados. Una vez establecido en los sistemas de destino, el malware gana persistencia y extrae datos, transmitiéndolos al servidor C&C. Además, recibe comandos del C&C y ejecuta cargas útiles según las instrucciones.

Si bien el malware parece peligroso, los usuarios pueden proteger sus sistemas de este ataque protegiendo sus dispositivos con soluciones antimalware sólidas. Dado que la amenaza existe desde hace años, la mayoría del software antimalware puede potencialmente detectar y bloquear esta amenaza antes de su ejecución.

IV. VECTOR DE ATAQUE:

Al abrir el documento muestra la opción de "HABILITAR CONTENIDO"; al seleccionar el botón, se inicia un script VBA que muestra un artículo en ruso que se traduce *como "Evaluaciones occidentales del progreso de la operación militar especial*".




ЗАПАДНЫЕ ОЦЕНКИ ХОДА СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

На фоне явного провала наступательной операции ВСУ, начатой 4 июня с.г., в западных, прежде всего американских, аналитических центрах активизировались дискуссии о ходе СВО и проблемах, с которыми сталкиваются украинцы и их западные (американские) спонсоры.

Una vez ejecutado el Script VBA, el código malicioso ejecuta las siguientes acciones:

- El script VBA recupera información de *"OLEFormat.IconLabel"* y la almacena en una carpeta temporal con el nombre de archivo *"temp.zip".*
- Después de extraer el contenido del archivo, ejecuta el script *"check.bat"* usando el parámetro "vbHide", asegurando que el script por lotes se ejecute sin presentar una ventana de símbolo del sistema al usuario. Este método es valioso cuando un actor de amenazas busca ejecutar discretamente un script en segundo plano, evitando la interacción del usuario o las ventanas visibles.
- Preparación del archivo check.bat. El archivo de script inicial, denominado “check.bat”, realiza varias comprobaciones. Inicialmente verifica la presencia de una sesión de conexión remota. Si se detecta, inicia directamente el script "netpp.bat".
- Luego, el script evalúa si el sistema actual está ejecutando Windows 10, asignando un valor de 1 a la variable "%Num%" independientemente del resultado. Esta variable luego juega un papel en la selección del método de derivación de UAC.
- El script además, examina si el sistema funciona con una arquitectura de 64 bits. Si es así, cambia el nombre de los archivos DLL correspondientes a “netpp.dll” y “wpns.dll” y elimina los archivos DLL redundantes.
- Finalmente, ejecuta "wpns.dll" con tres parámetros: "QQQQQQQ" como nombre del punto de entrada de destino, "%Num%" que indica el método de omisión de UAC elegido y "netpp.bat" para acciones adicionales.

Figura 6: Módulo de derivación UAC

V. IMPACTO:

La carga útil (script malicioso) incorpora una derivación de UAC y comunicación cifrada con un servidor C2, lo que permite al actor de amenazas ejecutar comandos privilegiados.

VI. INDICADORES DE COMPROMISO

FortiGuard Antivirus detecta y bloquea el malware identificado como:

- VBA/Agente.CXE!tr
- BASH/Agente.KON!tr

- W64/Agente.ATC!tr
- W32/Agente.AEQN!tr

Lista C2:

kmdqj1[.]c1[.]nosotros
ouvxu2[.]c1[.]nosotros
9b31n8[.]c1[.]nosotros
3pl0y5[.]c1[.]nosotros
dpgbep[.]c1[.]nosotros
7qnbae[.]c1 [.]biz
glws5m[.]c1[.]biz
ewqqa4[.]c1[.]biz
3897lb[.]c1[.]biz
558ga9[.]c1[.]biz
b91stf[.]c1[.]biz
bg5pl1 [.]c1[.]nosotros
caoy9n[.]c1[.]nosotros
rziju6[.]c1[.]nosotros
pm90p1[.]c1[.]nosotros
pxyunf[.]c1[.]nosotros
m2jymd[.]c1[.]nosotros
aocsff[.]c1[.]nosotros
6e2nbc[.]c1[.]nosotros
vqt9i1[.]c1[.]nosotros

Archivos:

- ac9b814b98a962bc77b2ab862d9c3b1ba5f7e86b80797259b4fcb40bfb389081
- f07e55ce20e944706232013241d23282e652de2c9514904dede14d4a711a5d1d
- 085cdb09aba0024c0cadbefe428817829bbe4ab0f68598572ebccc2f6f25e78f
- 793b8e72fded73ae6839e678b03bd5c99959f47a1ad632095ba60fb89f66fa91
- 83e66d912ca592bc2accfd9c275647f287b6dc72a859054a348e616537999b64
- 656dd6e67a51aebc6c69dc35eaba2e1502f225ae6fd9d0a5ff70879982427844
- cfbc7e6a89e4a23a72c7bcd9019197721f18506d9ab842011e0ab9d9eb24c2cc

VII. RECOMENDACIONES:

El EcuCERT pone a consideración de su comunidad objetivo las siguientes recomendaciones:

- Utilizar, actualizar y monitorear periódicamente herramientas antivirus y antimalware.
- Actualizar periódicamente el sistema operativo.
- Bloquear las fuentes de descargas y archivos de los indicadores de compromiso expuestos en el presente documento.
- Mantenerse informado sobre las últimas amenazas para conocer cómo actúan los atacantes y cuáles son sus motivaciones.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

Hashim, A. (27 de 11 de 2023). *latesthackingnews.com*. Obtenido de https://latesthackingnews.com/2023/11/27/konni-rat-malware-campaign-spreads-via-malicious-word-files/

Lin, C. (20 de 11 de 2023). *Fortinet*. Obtenido de https://www.fortinet.com/blog/threat-research/konni-campaign-distributed-via-malicious-document