

SE IDENTIFICÓ ATAQUES DEL GRUPO CIBERCRIMINAL LAZARUS DIRIGIDOS A ORGANIZACIONES EN RUSIA

securitysummitperu.com/articulos/se-identifico-ataques-del-grupo-cibercriminal-lazarus-dirigidos-a-organizaciones-en-rusia

20 de febrero de 2019



Investigadores de seguridad han concluido que el grupo cibercriminal patrocinado por el estado de Corea del Norte, Lazarus, estaría realizando actividades sospechosas dirigidas a compañías con sede en Rusia. Esto con base a las conexiones descubiertas entre las tácticas, técnicas y herramientas detectadas y el modo de operación del grupo también conocido como Hidden Cobra.

Servicios Afectados

- Sistemas Operativos Microsoft Windows

Detalles Técnicos

La campaña de Lazarus dirigida a Rusia utiliza documentos de Office maliciosos entregados como archivos ZIP, junto a un documento PDF llamado NDA_USA.pdf que contiene un acuerdo de StarForce Technologies, que es una compañía rusa de software que proporciona software de protección contra copia.

La comunidad de seguridad cree que Lazarus está dividido en al menos dos subdivisiones: la primera llamada Andariel, que se centra en atacar al gobierno y organizaciones de Corea del Sur, y la segunda, Bluenoroff, cuyo foco principal es la monetización y las campañas de espionaje global.

Este incidente, sin embargo, representa una elección inusual de víctima por parte del actor de amenazas de Corea del Norte. Por lo general, estos ataques reflejan las tensiones geopolíticas entre la República Popular Democrática de Corea (RPDC) y naciones como Estados Unidos, Japón y Corea del Sur.

Cadena de infección

El flujo de infección principal consta de los siguientes tres pasos principales:

1. Un archivo ZIP que contiene dos documentos: un documento PDF de señuelo benigno y un documento de Word malicioso con macros.
2. La macro maliciosa descarga una secuencia de comandos VBS desde una URL de Dropbox, seguida de la ejecución de la secuencia de comandos VBS.
3. El script VBS descarga un archivo CAB desde el servidor de la zona de descarga, extrae el archivo EXE incrustado (KEYMARBLE) con la utilidad “expand.exe” de Windows y, finalmente, lo ejecuta.

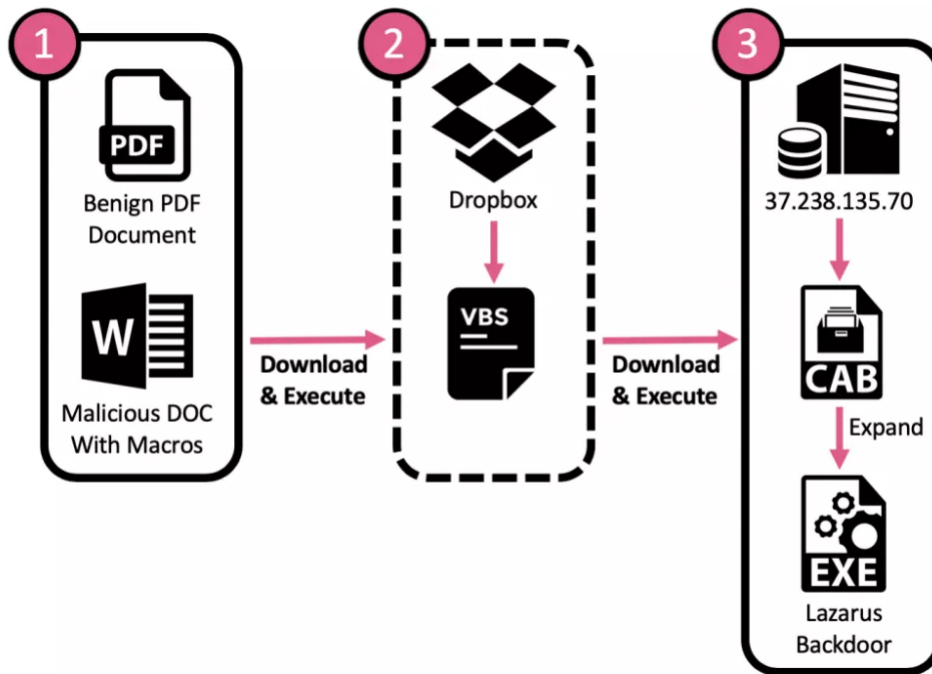


Figura 1: Secuencia de infección del malware KEYMARBLE de Lazarus.

KEYMARBLE

Este malware es una herramienta de administración remota (RAT) que proporciona a sus operadores una funcionalidad básica para recuperar información de la computadora de la víctima. Una vez ejecutado, realiza varias inicializaciones, se pone en contacto con un servidor de Comando y Control (C&C) y espera indefinidamente a recibir nuevos comandos. Cada comando recibido es procesado por el backdoor y se maneja dentro de una función apropiada, que a su vez recopila una información o realiza una acción en la computadora objetivo.

Indicadores de Compromiso (IoC)

IP

194[.]45[.]8[.]41
37[.]238[.]135[.]70

Hashes

MD5: dc3fff0873c3e8e853f6c5e01aa94cf

SHA256: 1c4745c82fdb9d05e210eff346d7bee2f087357b17bfcf7c2038c854f0dee61

MD5: 704d491c155aad996f16377a35732cb4

SHA256: e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09

MD5: 2b68360b0d4e26d2b5f7698fe324b87d

SHA256:

49a23160ba2af4fba0186512783482918b07a32b0e809de0336ba723636ae3b6

MD5: a7be38e8f84c5ad9cce30d009dc31d32

SHA256: f4bdf0f967330f9704b01cc962137a70596822b8319d3b35404eafc9c6d2efe7

MD5: 7646d1fa1de852bb99c621f5e9927221

SHA256: 9894f6993cae186981ecb034899353a04f1a9b009bdf265ceccda9595b725ee20

MD5: 22d53ada23b2625265cdbddc8a599ee0

SHA256: 8e099261929b1b09e9d637e8d054d5909b945b4157f29337977eb7f5fb835e5d

Recomendación

Se recomienda a nuestros clientes, seguir las siguientes acciones preventivas para reducir riesgos:

Para el personal de seguridad de información:

- Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.
- Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.
- Restringir la capacidad (permisos) de los usuarios para instalar y ejecutar aplicaciones de software no deseadas. No agregue usuarios al grupo de administradores locales a menos que sea necesario.
- Bloquear los indicadores de compromisos (IOC) mostrados, en los dispositivos de seguridad de su infraestructura.


** Antes de realizar el bloqueo de IOCs es importante que previamente en ambiente de desarrollo se valide y confirme a nivel de servicios internos y externos, con el propósito de aplicar los cambios de manera controlada.

Para usuarios finales:

- Verificar la información de la cuenta que le envía un correo electrónico, el nombre y la dirección del destinatario para identificar si son sospechosas.
- No abrir correos electrónicos de dudosa procedencia (remitente desconocido), ni dar clic en enlaces, ni descargar archivos adjuntos desconocidos.
- De detectar un correo spam o phishing reportarlo inmediatamente a los encargados de seguridad de la información de su institución.
- Escanear todo el software descargado de Internet antes de la ejecución.
- Visitar páginas web seguras (https), y verificar el certificado digital con un clic en el candado de la barra de estado.

Fuentes

- Fuente 1: [North Korea Turns Against New Targets?!](#)
- Fuente 2: [North Korean APT Lazarus Targets Russian Entities with KEYMARBLE Backdoor](#)

A dark blue banner with a red top border and a background of circuitry. The word "Contáctenos" is written in white, bold, sans-serif font.

Si usted tiene alguna pregunta no dude en contactarse con nosotros: informes@securesoftcorp.com

**Cyber Security Operation Center
SECURE SOFT CORPORATION**

Síguenos en :



Somos miembros de :

