Boletín de Ciberseguridad

Precauciones con Ocasión del Conflicto Rusia - Ucrania

08-Mar-2022

El conflicto Rusia – Ucrania ha exacerbado una serie de ciberataques que ya habían estado ocurriendo desde hace varios años (hay referencias de ciberataques de Rusia a Ucrania desde 2016). Estas últimas semanas, hemos visto una respuesta mucho más decidida de parte de Ucrania y sus aliados, así como de los aliados de Rusia, y hasta organizaciones como Anonymous y otros.

Entre las formas más conocidas de ciberataque, el favorito en estos casos es el ataque de Denegación de Servicio Distribuído (DDoS), por su facilidad y rapidez de despliegue. Lo preocupante de los ataques DDoS, y en particular de la variante DrDoS que se ha vuelto muy popular, es que utilizan a terceros para generar el tráfico masivo contra el objetivo, a través de una red de computadoras controladas por los atacantes (Botnet o red zombie).

En el caso de una ciberguerra, la infraestructura de un país no involucrado directamente, como el nuestro, es ideal para cosechar estos recursos. En el caso de la variante DrDoS, ni siquiera requiere controlar nuestra infraestructura, ya que la red zombie involucra a computadoras no infectadas, haciéndolas lanzar solicitudes hacia el objetivo.

Por otro lado, **la Cybersecurity and Infrastructure Security Agency (CISA)** y el **Federal Bureau of Investigation (FBI)**, han lanzado advertencias conjuntas sobre malware circulando en la red. En el mundo físico, recibir uno de estos malware sería el equivalente a ser víctima de una “bala perdida”. Si bien es imposible que una bala llegue al otro lado del mundo, un ciberataque sí puede llegar desde cualquier parte del mundo.

En este contexto, **las recomendaciones básicas de ciberseguridad a considerar son las siguientes**:

- De no tener relaciones comerciales con los países involucrados o sus aliados, realice un bloqueo de tráfico por geolocalización en sus herramientas de seguridad de red.
- Habilite la autenticación multifactor para sus aplicaciones.
- Configure los programas antivirus y antimalware para que realicen análisis programados frecuentes.
- Habilite filtros y políticas de spam rigurosas, para evitar que los correos electrónicos de phishing lleguen a los usuarios finales.
- Actualice su software, especialmente el Sistema Operativo (OS) y las aplicaciones críticas; y evalúe eliminar aquellas que no sean necesarias para el negocio.
- Monitoree permanentemente el tráfico de su red, ya sea a través de un servicio de CyberSOC o de herramientas especializadas de seguridad.

A continuación, compartimos con ustedes algunas de las alertas más relevantes a considerar:

Nombre de la alerta	OutSteel, SaintBot enviados por ataques Spear Phishing con Ucrania como objetivo
Tipo de ataque	Explotación de vulnerabilidades conocidas mediante spear phishing
Medios de propagación	Correo, internet, entre otros

Descripción

1. **Productos afectados inicialmente por el spear phishing:**
   Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016.

2. **Resumen:**
   El 1 de febrero de 2022, la Unidad 42 (unidad especializada de ciberseguridad de PaloAlto) observó un ataque contra una organización de energía en Ucrania. El Equipo de Respuesta ante Incidentes de Ciberseguridad de Ucrania (CERT-UA) atribuyó públicamente el ataque a un grupo-agente de amenaza al que rastrean como UAC-0056. El ataque dirigido involucró un correo electrónico de phishing dirigido a un empleado de la organización, que utilizó una mensaje de ingeniería social que sugería que el empleado había cometido un delito. El correo electrónico tenía un documento de Word adjunto que contenía un archivo JavaScript malicioso que descargaría e instalaría una carga útil conocida como SaintBot (un descargador) y OutSteel (un ladrón de documentos). La Unidad 42 descubrió que este ataque era sólo una parte de una campaña más grande que se remonta al menos a marzo de 2021. La Unidad 42 determinó que el grupo-agente de esta amenaza estaba dirigido a una entidad gubernamental occidental en Ucrania, así como a varias organizaciones gubernamentales ucranianas.

3. **Detalles:**
   La vulnerabilidad de severidad ALTA identificada como **CVE-2017-11882** (según la base de datos de Vulnerabilidades y Amenazas Comunes), permite que un atacante ejecute código arbitrario en el contexto del usuario actual al no manejar correctamente los objetos en la memoria, también conocida como "vulnerabilidad de corrupción de memoria de Microsoft Office"

4. **Solución:**
   Para esta vulnerabilidad específica, el parche fue publicado en noviembre de 2017. Sin embargo, se recomienda tomar medidas contra el correo no deseado y malicioso, así como concientizar a los usuarios a reconocer las técnicas de ingeniería social.

Fuentes de información	• https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

Nombre de la alerta	Malware Destructivo Dirigido a Organizaciones en Ucrania
Tipo de ataque	Explotación de Vulnerabilidades
Medios de propagación	Correo electrónico, redes sociales, entre otros

Descripción

1. **Resumen:**
   El 12 de noviembre de 2021, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento que los operadores del troyano TrickBot están colaborando con el grupo de atacantes Shathak para distribuir sus productos, lo que finalmente lleva al despliegue del ransomware Conti en las máquinas infectadas.

2. **Detalle:**
   Antes del ataque no provocado de Rusia contra Ucrania, los atacantes desplegaron malware destructivo contra organizaciones en Ucrania, para destruir los sistemas informáticos y dejarlos inoperativos.

   - El 15 de enero de 2022, el Microsoft Threat Intelligence Center (MSTIC) reveló que el malware conocido como WhisperGate se estaba utilizando para atacar organizaciones en Ucrania. Según Microsoft, WhisperGate está destinado a ser destructivo y está diseñado para dejar inoperativos los dispositivos infectados.
   - El 23 de febrero de 2022, varios investigadores de ciberseguridad revelaron que el malware conocido como HermeticWiper se estaba utilizando contra organizaciones en Ucrania. Según SentinelLabs, el malware se dirige a los dispositivos de Windows, manipulando el registro de arranque maestro, lo que resulta en una falla de arranque posterior.

   El malware destructivo representa una amenaza directa para las operaciones diarias de una organización, afectando la disponibilidad de activos y datos críticos. Es probable que se produzcan más ataques cibernéticos disruptivos contra organizaciones en Ucrania, y que a partir de ahí se extiendan involuntariamente a otros países. Las organizaciones deben aumentar la vigilancia y evaluar sus capacidades, de manera que estas consideren las etapas de planificación, preparación, detección y respuesta al incidente de ciberseguridad.

Tabla 1: IOCs asociados con WhisperGate

Name	File Category	File Hash	Source
WhisperGate	stage1.exe	a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	Microsoft MSTIC
WhisperGate	stage2.exe	dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	Microsoft MSTIC

Tabla 2: IOCs asociadas con HermeticWiper

Name	File Category	File Hash	Source
Win32/KillDisk.NCV	Trojan	912342F1C840A42F6B74132F8A7C4FFE7D40FB7761B25D11392172E587D8DA3045812A66C3385451	ESET research
HermeticWiper	Win32 EXE	912342f1c840a42f6b74132f8a7c4ffe7d40fb77	SentinelLabs
HermeticWiper	Win32 EXE	61b25d11392172e587d8da3045812a66c3385451	SentinelLabs
RCDATA_DRV_X64	ms-compressed	a952e288a1ead66490b3275a807f52e5	SentinelLabs
RCDATA_DRV_X86	ms-compressed	231b3385ac17e41c5bb1b1fcb59599c4	SentinelLabs
RCDATA_DRV_XP_X64	ms-compressed	095a1678021b034903c85dd5acb447ad	SentinelLabs
RCDATA_DRV_XP_X86	ms-compressed	eb845b7a16ed82bd248e395d9852f467	SentinelLabs
Trojan.Killdisk	Trojan.Killdisk	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591	Symantec Threat Hunter Team
Trojan.Killdisk	Trojan.Killdisk	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da	Symantec Threat Hunter Team
Trojan.Killdisk	Trojan.Killdisk	a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e	Symantec Threat Hunter Team
Ransomware	Trojan.Killdisk	4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382	Symantec Threat Hunter Team

3. **Propagación:**
   Los métodos usuales de propagación de malware son el correo electrónico, los dispositivos USBs, los sitios web infectados, entre otros.

4. **Se recomienda:**
   Implementar las recomendaciones mencionadas anteriormente en este boletín.

Fuentes de información	• https://thehackernews.com/2021/11/trickbot-operators-partner-with-shatak.html