

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

CISA ADVIERTE SOBRE ZERO-DAY EN WINDOWS Y OFFICE

18/ Julio/2023

CONTENIDO

INTRODUCCIÓN	3
CVE-2023-36884	4
CONTEXTO	5
STORM-0978	5
TTPs	5
RANSOMWARE	6
CVE-2023-36884	8
CISA ADVIERTE.....	9
RECOMENDACIONES	10
INDICADORES DE COMPROMISO	10
CONTACTOS DE SOPORTE	11

INTRODUCCIÓN

Se Recientemente el grupo de actores maliciosos denominado Storm-0978 ha sido visto llevando a cabo campañas de phishing hacia entidades de gobiernos europeos y Norteamérica, mediante la explotación de una vulnerabilidad Zero-day en productos Windows y Office, dicha vulnerabilidad ha sido rastreada como CVE-2023-36884.

La vulnerabilidad en cuestión ha sido descrita como una vulnerabilidad de ejecución remota de código HTML que afecta directamente a productos de Windows y Office, mediante la implementación de un documento de Microsoft Office especialmente diseñado, el cual simula ser un documento que hace referencia al congreso mundial de Ucrania.

Las campañas se han asociado al actor malicioso denominado como Storm-0978, también conocido como RomCom, nombre que hace alusión al backdoor utilizados por estos. Storm-0978 también ha sido visto llevando a cabo ataques de ransomware mediante el binario denominado Industrial Spy ransomware, así como variantes de este.

CVE-2023-36884

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_07_18_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	CLEAR
Fecha de publicación:	18/07/2023
Es día cero (0 day):	Sí

CONTEXTO

Recientemente la Agencia de ciberseguridad y seguridad de las infraestructuras CISA ha advertido a múltiples agencias gubernamentales mitigar la vulnerabilidad Zero-day la cual afectaría a productos de Windows y Office. La vulnerabilidad en cuestión es una vulnerabilidad de Código de ejecución remoto.

Microsoft ha identificado una campaña activa de phishing, conducida por los actores maliciosos rastreados como Storm-0978, los cuales dirigen estos ataques a entidades de gobierno, principalmente en Europa y Norteamérica. Esta campaña aprovecha una vulnerabilidad Zero-day, ahora rastreada como CVE-2023-36884. Dicha vulnerabilidad hace referencia la ejecución remota de código. Esta vulnerabilidad habría sido explotada previo a su divulgación a Microsoft, mediante documentos de Word los cuales simulaban ser documentos relacionados a Congreso mundial de Ucrania.

STORM-0978

La campaña ha sido atribuida a los actores maliciosos rastreados como Storm-0978, también conocidos como RomCom, quienes tienen su origen en Rusia. El grupo es mayormente conocido por conducir operaciones de ransomware y doble extorsión, así como sus campañas de recolección de credenciales, con fines de inteligencia.

Los actores maliciosos también son conocidos por liberar versiones troyanizadas de softwares populares, con la finalidad de instalar "RomCom". Como resultado de estos ataques, múltiples dependencias militares y gubernamentales, siendo el primer objetivo Ucrania y posteriormente esparciéndose a organizaciones europeas y Norteamérica que se hayan visto involucradas en los acontecimientos actuales de Ucrania-Rusia.

Mediante campañas de phishing, los actores maliciosos Storm-0978 buscan la distribución de backdoors a organizaciones y robar toda la información que resulte de utilidad como credenciales, para ser utilizadas en posteriores operaciones.

TTPs

Storm-0978 es principalmente conocido por la implementación de versiones troyanizadas de software legítimo con la finalidad de instalar "RomCom", el cual ha sido desarrollado por los mismos actores maliciosos. Entre los softwares más comunes suplantados por Storm-0978 son Adobe, Advanced IP Scanner, Solarwinds Orion, KeePass, entre otros. Estas versiones troyanizadas son alojadas por los actores maliciosos, en dominios que buscan simular al del software legítimo utilizado para cada caso específico.

Más recientemente, Storm-0978 ha sido observando, utilizando exploits que tienen como objetivo la vulnerabilidad Zero-day, ahora rastreada como CVE-2023-36884. Storm-0978 también se ha observado utilizando el "industrial Spy ransomware" en ataques con motivaciones meramente financieras. Este es una cepa de ransomware observada por primera vez en mayo de 2022.

RANSOMWARE

Como se hizo mención brevemente, más arriba, Storm-0978 es conocido por la implementación de Industrial Spy ransomware. Según se ha podido observar en intrusiones del grupo malicioso, estos han accedido a credenciales mediante el descarte de hashes de contraseñas del administrador de cuentas de seguridad (SAM) mediante el registro de Windows.

Para que el grupo malicioso pueda acceder al administrador de cuentas de seguridad o SAM, por sus siglas en Inglés, estos deben, primeramente, hacerse con privilegios a nivel de SYSTEM. Para el movimiento lateral, se ha observado a Storm-0978 haciendo uso de las funcionalidades SMBExec y WMICExec del macro Impacket.

Para el cifrado y descifrado, Industrial Spy ransomware, hace uso del mismo binario, y su actividad se puede resumir de la siguiente manera:

- Analizar los argumentos de la línea de comandos.
- Borra las copias de instantáneas.
- Inicia un hilo de cifrado para cifrar todos los drivers o bien rutas proporcionadas.
- Auto borrado.

```
*(_DWORD *)Operation = 0x70006F;           // open
v2 = 0x6E0065;
v3 = 0;
*(_DWORD *)File = 0x730076;                // vssadmin.exe
v5 = 0x610073;
v6 = 0x6D0064;
v7 = 0x6E0069;
v8 = 0x65002E;
v9 = 0x650078;
v10 = 0;
*(_DWORD *)Parameters = 0x650064;          // delete shadows /all /quiet
v12 = 0x65006C;
v13 = 0x650074;
v14 = 0x730020;
v15 = 0x610068;
v16 = 0x6F0064;
v17 = 0x730077;
v18 = 0x2F0020;
v19 = 0x6C0061;
v20 = 0x20006C;
v21 = 0x71002F;
v22 = 0x690075;
v23 = 0x740065;
v24 = 0;
ShellExecuteW(0164, Operation, File, Parameters, 0164, 0);
return 0164;
```

Imagen 1. Seudocódigo para la eliminación de instantáneas.

De ser provisto algún argumento en la línea de comandos, Industrial Spy ransomware iniciara un hilo para cifrar cada ruta especificada en el argumento, de lo contrario, Industrial Spy enumerará todos los drivers

e iniciara un hilo de cifrado por volumen, cada uno de estos enumerará y cifrará archivos, evitando las rutas:

- \microsoft\
- \google\chrome
- \mozilla\firefox
- \opera\

Así como las extensiones:

.	.mst	.inf1	.shs	.dll	.scr	.cmd	.ps1	.jse
.bat	.paf	.ins	.u3p	.exe	.sct	.com	.reg	.vbscript
.bin	.pif	.inx	.vb	.gadget	.shb	.cpl	.rgs	.msi
.job	.vbs	.isu	.vbe	.lnk	.ws	.msc	.wsf	.wsh

Tabla 1. Extensiones excluidas del proceso de cifrado.

El ransomware cifra cada archivo mediante la utilización del algoritmo 3DES, luego del proceso del cifrado, el archivo original es renombrado con datos adicionales como el contenido del archivo cifrado, el blob de RSA cifrado, el marcador 0xFEEDBEEF y el tamaño original del archivo.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	B4	36	5A	B9	5E	15	3B	20	08	A6	55	D9	AC	63	8E	FA	'6Z^.;.¡UÛ-cŽú
00000010	27	AD	E4	5A	3A	70	EE	6D	65	0C	E0	8F	FA	6A	8E	B9	'..äZ:pime.ä.újŽ^
00000020	9C	A2	F5	F1	8A	03	45	4E	8B	72	6C	64	6F	BD	A0	63	æöäŠ.FN<rldots c
00000030	4F	28	63	15	F1	71	06	BC	A1	E0	39	F4	8A	55	07	C6	O(c.ñq.4;à9ôŠU.Æ
00000040	08	18	E6	4E	68	34	79	50	E7	87	79	47	7E	8D	4A	E7	..æNh4yPç+yG~.Jç
00000050	47	C9	3F	44	8E	F7	24	0A	FD	C7	00	0A	CD	E4	CD	DB	GÊ?DŽ+\$..ýÇ..íäİÜ
00000060	42	D1	E7	80	AC	11	14	BD	53	83	D0	4E	2F	2C	C4	CA	BÑç€~..½SfĐN/,ÄÊ
00000070	35	75	B3	2F	73	3D	BB	28	EE	37	89	78	2D	6A	05	06	Su³/s=»(i7%x-j..
00000080	F8	7C	44	84	31	06	8B	D6	EF	CE	55	32	E6	0D	1D	3F	ø D„l.<ÖiİU2æ..?
00000090	1C	70	84	C0	8F	17	BA	53	73	CD	A0	EF	9B	02	41	5A	.p„À..°SsÍ i>.AZ
000000A0	98	01	69	BF	F9	F6	DE	FB	E3	83	07	3D	63	C4	90	47	~.i;ùöBûäf.=cÄ.G
000000B0	25	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	%.....i%ip
	Original file size								0xFEEDBEEF Marker								

Imagen 2. Estructura de archivo cifrado

CVE-2023-36884

A mediados de junio de 2023, Storm-0978 inicio una campaña de phishing, haciendo uso de cargadores falsos de OneDrive, con la finalidad de desplegar un backdoor en los sistemas objetivo, cabe resaltar que dicho backdoor comparte algunas similitudes con RomCom. La campaña tiene como objetivo principal, entidades de gobierno en Europa y Norteamérica, y simulan ser documentos relacionados al congreso mundial de Ucrania.



Imagen 3. Correo phishing del congreso mundial de Ucrania.

La vulnerabilidad en cuestión hace referencia a una vulnerabilidad Zero-Day, ahora rastreada como CVE-2023-36884. Esta es una vulnerabilidad de ejecución remota de código HTML en Office y Windows. Mediante un documento especialmente diseñado de Microsoft Office, un atacante tendría la capacidad de llevar a cabo ejecución remota de código, en el contexto de la víctima, sin embargo, para una explotación exitosa, el atacante, primeramente, debe convencer a la víctima a abrir dicho archivo. CVE-2023-36884 ha sido puntuada como CVSSv3 8.8/10, lo cual la vuelve una vulnerabilidad alta y debe ser abordada lo antes posible.



Severity		CVSS Version 3.x	CVSS Version 2.0
CVSS 3.x Severity and Metrics:			
	NIST: NVD	Base Score: 8.8 HIGH	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
	CNA: Microsoft Corporation	Base Score: 0.0 NONE	Vector: CVSS:3.1/AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:N

Imagen 4. Severidad de CVE-2023-36884.

CISA ADVIERTE

Posterior a la revelación de la vulnerabilidad CVE-2023-36884, CISA ha ordenado a todas las agencias federales, así como a usuarios en general, realizar las acciones necesarias para la mitigación de dicha vulnerabilidad que fuera explotada por los actores maliciosos Storm-0978 para dirigir ataques contra los países aliados de la OTAN.

Según la directiva operativa vinculante (DBO 22-01) emitida en noviembre de 2021, EE. UU. Las agencias de la rama ejecutiva civil federal (FCEB) ahora deben proteger los dispositivos Windows en sus redes contra ataques que explotan CVE-2023-36884. Las agencias tendrán un máximo de tres semanas para implementar dichas medidas con la finalidad de asegurar los sistemas.

Si bien, Microsoft no ha provisto de algún parche que aborde CVE-2023-36884, sin embargo, la empresa ha expresado su compromiso para el desarrollo de dichos parches con gran diligencia, esperando liberar los parches en las siguientes semanas para que coincida con su lanzamiento de actualizaciones mensuales.

Hasta que haya parches disponibles, los clientes que utilizan Defender para Office 365, Microsoft 365 Apps (Versiones 2302 y posteriores), y aquellos que ya han aplicado la regla de reducción de superficie de ataque "bloquee todas las aplicaciones de Office para crear procesos secundarios" están protegidos contra los ataques de phishing CVE-2023-36884.

Por otro lado, aquellos sin esta protección, pueden agregar los siguientes nombres de procesos a la clave de registro "FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION" como un valor de tipo REG-DWORD con data 1 para remover el vector de ataque, como se muestra a continuación.

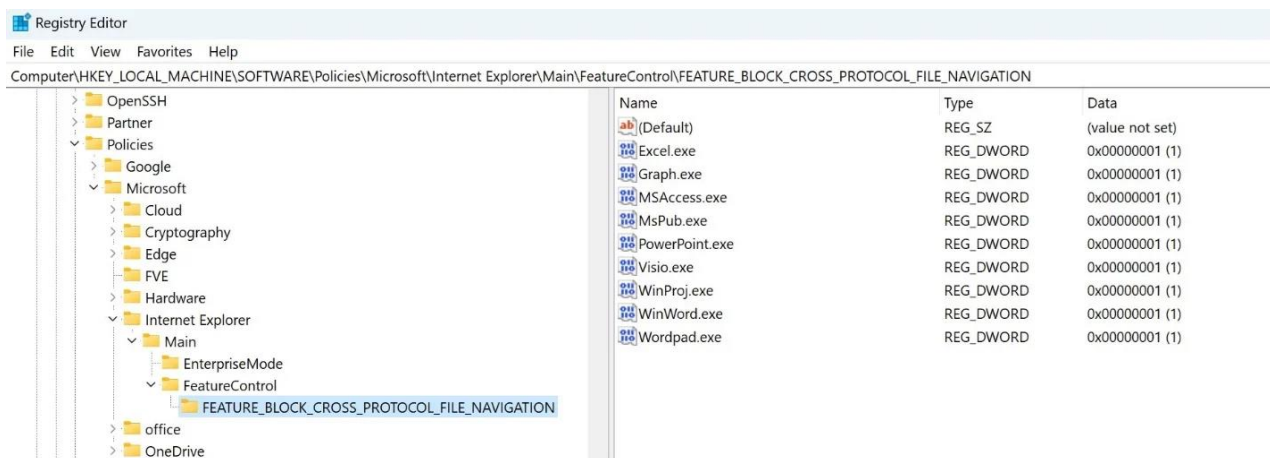


Imagen 5. FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION.

RECOMENDACIONES

Microsoft recomienda llevar a cabo las siguientes acciones, con la finalidad de reducir el impacto de la campaña de ataques llevada a cabo por Stor-0978.

- Habilitar la protección en la nube para poder cubrir de manera rápida las herramientas y tácticas utilizadas por atacantes.
- Ejecutar el modo de bloque en el EDR, de manera que si el software de antivirus instalado en la maquina comprometida no detecta la amenaza, el EDR en modo de bloqueo trabaja tras escena, para remediar artefactos maliciosos que se encuentran, post ataque.
- Habilitar investigación y remediación para tomar acción inmediata sobre las alertas y así resolver las infracciones, reduciendo, a su vez, el volumen de las alertas.
- Verificar siempre la autenticidad de los remitentes de correos electrónicos antes de hacer clic en enlaces o proporcionar información sensible.
- Utilizar filtros de spam y sistemas de detección de phishing confiables para bloquear correos electrónicos maliciosos.
- Mantener el software y las aplicaciones actualizadas con los últimos parches de seguridad para evitar vulnerabilidades explotables por los atacantes.
- Habilitar filtros comunes de archivos adjuntos para restringir archivos que regularmente contienen malware.
- Evitar descargar software o archivos de fuentes no confiables o sospechosas.
- Configurar las opciones de seguridad de los navegadores web para bloquear descargas automáticas y sitios web maliciosos.
- No hacer clic en enlaces o anuncios sospechosos y evitar visitar sitios web no seguros.
- Utilizar firewalls y filtrado de contenido para bloquear el acceso a sitios web y servicios maliciosos conocidos.
- Realizar análisis de malware periódicos en los sistemas para detectar y eliminar posibles amenazas.
- Los agentes Cortex XDR y XSIAM ayudan a proteger contra las actividades posteriores a la explotación asociadas a la explotación de CVE-2023-36884, así como a utilizar detecciones de análisis local para binarios RomCom en entornos Windows.
- Advanced WildFire puede ayudar a detectar y prevenir ataques con malware altamente evasivo.
- Next-Generation Firewall con suscripciones de seguridad Advanced Threat Prevention puede ayudar a bloquear cargas útiles y ataques asociados.
- Cloud-Delivered Security Services puede clasificar como maliciosos los dominios C2 asociados a esta actividad.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/07edcd18ea69ec41598bdb2efac97caffec1c52e1/20230718_01_CVE-2023-36884--RomCom

CONTACTOS DE SOPORTE



Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: <https://www.devel.group/reporta-un-incidente>