MANDIANT®

Perfil del grupo FIN11: Campañas de correo electrónico generalizadas como precursoras de ransomware y robo de datos

Índice

Perfil del grupo FIN11: Campañas de correo electrónico generalizadas como precursoras de ransomware y robo de datos

- FIN11 es un grupo de intrusiones con motivaciones financieras, activo desde al menos 2016, que ha entregado malware como FlawedAmmyy y FRIENDSPEAK en campañas de phishing generalizadas que han afectado a organizaciones en una amplia gama de sectores y regiones geográficas.
- Para monetizar sus operaciones, FIN11 implementa ransomware CLOP y extorsiona a las víctimas para no divulgar los datos robados compartidos a través de su sitio público de "filtración". En al menos un caso, Mandiant Threat Intelligence ha observado que FIN11 usa malware de punto de venta (POS).
- FIN11, previamente rastreado por Mandiant Threat Intelligence como TEMP. Warlock, es un subconjunto de actividad que los investigadores de seguridad denominan TA505, que data del año 2014.
- Aunque no exhibe un alto nivel de sofisticación técnica, FIN11 es notable dada su constante evolución de las tácticas y técnicas de entrega de malware. El grupo también ha confiado en una serie de servicios de apoyo para cumplir su misión.
- Creemos que los perpetradores detrás de las operaciones de FIN11 están ubicados en la Comunidad de Estados Independientes (CEI) según los metadatos de archivos en idioma ruso, lapsos de actividad durante las vacaciones ortodoxas rusas y la falta de despliegue de CLOP en los países de la CEI.

Descripción general

FIN11 es un grupo de amenazas con motivaciones financieras que ha llevado a cabo algunas de las campañas de distribución de malware más grandes y de mayor duración observadas entre nuestros grupos FIN hasta la fecha. Mandiant ha observado que FIN11 procura monetizar sus operaciones al menos una vez utilizando malware de punto de venta (POS) con nombre y con más frecuencia utilizando ransomware CLOP combinado con extorsión tradicional. El grupo ha estado activo desde al menos 2016, pero identificó superposiciones con la actividad rastreada por los investigadores de seguridad, ya que TA505 sugiere que pueden haber estado realizando operaciones desde 2014. Además de sus campañas no deseadas de alto volumen, FIN11 también se destaca por su constante evolución de las tácticas y técnicas de entrega de malware.

- Nuestra definición de FIN11 se caracteriza principalmente por campañas desde 2016 que utilizan familias de códigos que se cree que son exclusivas del grupo (FlawedAmmyy, FRIENDSPEAK, MIXLABEL), así como otras tácticas y técnicas superpuestas.

- Hay superposiciones notables entre FIN11 y un conjunto de actividades que los investigadores de seguridad denominan TA505. Este término ha sido ampliamente utilizado en la comunidad de seguridad para discutir campañas no deseadas a gran escala, que datan del año 2014 y han distribuido varias familias, incluido Dridex y varios tipos de ransomware. Las superposiciones entre la actividad de FIN11 y TA505 incluyen tácticas, técnicas y procedimientos (TTP), ataques y uso de malware similares. Sin embargo, no hemos atribuido las primeras operaciones de TA505 y la precaución contra la fusión de los dos grupos.
- Las campañas no deseadas de alto volumen de FIN11 han afectado a una amplia variedad de sectores y regiones geográficas. Desde septiembre de 2019, estas campañas no deseadas han entregado archivos de Office maliciosos que contienen el cargador FRIENDSPEAK y, finalmente, han llevado a la implementación del ransomware CLOP.
- Si bien FIN11 ha realizado cambios frecuentes en sus TTP a lo largo del tiempo, los cambios se han relacionado principalmente con la entrega y distribución iniciales, mientras que sus cargas útiles de malware y TTP posteriores a la explotación se han mantenido relativamente consistentes. Estos cambios a lo largo del tiempo indican cierta adaptabilidad en sus intentos de evadir los mecanismos iniciales de detección basados en el correo electrónico, pero no son necesariamente indicativos de un alto nivel de sofisticación técnica.

Ataques

Las campañas de FIN11 han impactado una amplia variedad de sectores y regiones geográficas. Las campañas no deseadas del grupo desde el 2017 al 2018 se dirigieron principalmente a organizaciones de los sectores financiero, minorista y de restaurantes. En 2019 y 2020, FIN11 amplió su ataque a un conjunto más grande de industrias y países, más indiscriminado y diverso, a menudo utilizando engaños financieros genéricos. Sin embargo, una parte de las campañas de FIN11 entre 2019 y 2020 se dirigió a organizaciones en industrias o regiones específicas, a menudo utilizando el idioma nativo del objetivo junto con información manipulada del remitente del correo electrónico, como nombres de correo electrónico falsificados para mostrar y direcciones de remitente de correo electrónico, para parecer más legítimas. El cambio en los ataques observado durante los últimos dos años puede ser el resultado de la transición de FIN11 de implementar malware de punto de venta (POS) al ransomware como su principal método de monetización.

Engaños genéricos
A finales de 2019 y principios de 2020, observamos campañas de lanzamiento de FIN11 utilizando engaños en inglés con términos financieros relativamente genéricos, tales como: "sales order" (pedido de venta), "bank statement" (extracto bancario) y "invoice" (factura), entre otros. El grupo también utilizó varios nombres de visualización diferentes, algunos como departamentos organizativos genéricos, como "recepción" y "asistente". Por ejemplo, en septiembre de 2019, observamos que el grupo inició campañas de phishing de alto volumen contra varias industrias. En algunas de estas campañas, el grupo envió miles de correos electrónicos a organizaciones de todo el mundo.

- El 9 y el 10 de septiembre, FIN11 envió miles de correos electrónicos principalmente a entidades bancarias de África, Asia Occidental, Asia Oriental, Oceanía, Europa y América del Norte. Los asuntos de los correos electrónicos no fueron adaptados para ninguno de los destinatarios. En su lugar, se utilizaron asuntos como "factura y documentos", "debe solicitarse" y "documento para firma".
- Entre el 27 y el 28 de septiembre, se enviaron más de miles de correos electrónicos de manera indiscriminada en todas las industrias, que incluyen: viajes aéreos, tecnología, servicios financieros, fabricación y otros. Al igual que en otras campañas, este ataque global utilizó engaños relativamente genéricos. Estos engaños incluían "cheques pendientes", "documentos" y, un poco fuera de lugar, "minutas de la asoc. de padres y maestros".
- De manera similar, a principios de octubre, FIN11 atacó a múltiples sectores en varios países con engaños mediante asuntos como: "enviando correo electrónico: doc", "enviando correo electrónico: inv" y más.

Engaños geográficos y específicos del sector
FIN11 también ha adaptado algunos de sus engaños y nombres de correo electrónico para mostrar al país o el sector que está siendo objeto de ataques.

- Durante varias operaciones de phishing en 2019, el grupo atacó únicamente a organizaciones surcoreanas, a menudo utilizando engaños en coreano. Estos engaños eran igualmente genéricos y podían traducirse fácilmente utilizando servicios en línea, como Google Translate. Uno de esos engaños fue **송금 증** $<amount>, que se traduce en "envío" seguido de una cantidad en dólares. El nombre del correo electrónico para mostrar **최성은** - "Choi Sung-eun" (una actriz de Corea del Sur) se utilizó para esta campaña para hacerse pasar por un remitente coreano. Otros engaños estaban relacionados con los impuestos, como: **과세 요청** - "solicitud de impuestos" y **국세청 송장** – "Factura del servicio nacional de impuestos". Ambas campañas utilizaron un nombre de remitente para mostrar en coreano con la intención de sugerir que fueron enviadas por el Servicio Nacional de Impuestos de Corea del Sur ("**국세청**").
- FIN11 también utilizó con frecuencia engaños en alemán en enero y febrero de 2020, generalmente con temas relacionados con facturación. Por ejemplo, una campaña utilizó el nombre del remitente del correo electrónico "buchhaltung", que se traduce en contabilidad, y el asunto "Rechnung Nr. <number>": número de factura.
- FIN11 lanzó con frecuencia operaciones de phishing personalizadas contra empresas farmacéuticas en los primeros meses de 2020. Por ejemplo, en enero de 2020, FIN11 inició una serie de operaciones de phishing con asuntos de correo electrónico que incluían: "informe de investigación N-<five-digit number>", "asistente de investigación: informe" y "accidente de laboratorio". Otra operación en marzo de 2020 aprovechó el engaño "<pharmaceutical company name> hoja de cálculo de facturación del año 2020 hasta la fecha".

Campañas de alto volumen y alto ritmo

El uso constante de FIN11 de campañas de phishing de alto volumen distingue al grupo de amenazas de nuestros otros grupos FIN rastreados. Mandiant ha detectado miles de correos electrónicos maliciosos en campañas de phishing atribuidas a FIN11; sin embargo, es casi seguro que el número total de correos electrónicos sea mucho mayor.

- Cuando estuvieron activos, los perpetradores mantuvieron un alto ritmo operativo a lo largo de 2019 y principios de 2020, generalmente realizando de dos a cinco campañas de phishing por semana.
- Hemos observado campañas de phishing FIN11 de distinta magnitud. Esto es consistente con los informes TA505 de 2019 de Proofpoint, que indicaron que habían observado campañas con cientos de miles de mensajes y, a veces, incluso millones de correos electrónicos enviados durante una sola campaña.
- El volumen de correos electrónicos de phishing de FIN11 aparentemente disminuyó a partir de octubre de 2019. Sin embargo, continuamos observando algunas campañas con miles de destinatarios. Dado que los perpetradores cambiaron simultáneamente los TTP de entrega y los ataques, es plausible que su volumen se mantuviera constante y la aparente disminución puede haber sido una limitación en nuestra visibilidad en la cadena de entrega completa.

Períodos de inactividad

A pesar de su alto ritmo operativo, hemos observado algunos períodos de duración variable en los que FIN11 aparentemente ha tomado descansos en la realización de sus campañas de phishing.

- Los perpetradores parecen realizar campañas de phishing durante la semana, no los fines de semana, posiblemente para alinearse con las semanas laborales de los objetivos corporativos.
- FIN11 ha estado inactivo durante las vacaciones de invierno, en algunos casos desde finales de diciembre hasta la Navidad ortodoxa rusa a principios de enero.
- FIN11 parece haber cesado su actividad por completo desde mediados de marzo de 2020 hasta finales de mayo de 2020. Si bien la duración de este período de inactividad fue atípica para FIN11, existen varias explicaciones posibles, incluyendo el hecho de tomar precauciones después del arresto de más de 30 personas por parte de FSB en marzo de 2020, una pausa planificada (por ejemplo, debido a vacaciones, exámenes, COVID-19), o un cambio para centrarse en la actividad posterior al ataque o la reestructuración.

Evolución de las TTP en las campañas

Un sello distintivo de la actividad de FIN11 desde al menos enero de 2019 ha sido su rápida evolución de las TTP de las campañas de phishing. A lo largo de sus campañas de phishing de 2019 y 2020, el grupo ha realizado pequeños cambios en sus mecanismos de entrega iniciales, probablemente en un intento por eludir los regímenes de detección de víctimas. Estos cambios incluyeron los métodos de entrega de cargas útiles, las alteraciones de los cargadores en los documentos habilitados para macros, las funciones de la API de Windows que utilizó el cargador FRIENDSPEAK, los idiomas del engaño y las cargas útiles en sí. Evaluamos que estas modificaciones relativamente menores y menos novedosas no reflejan la sofisticación del grupo.

Campañas de enero a agosto del 2019

De enero a agosto de 2019, las campañas de phishing de FIN11 utilizaron principalmente archivos de Office maliciosos para entregar los cargadores de FlawedAmmyy y ServHelper; sin embargo, las cargas útiles de la primera etapa del grupo también incluyeron Amadey, AndroMut y la herramienta de acceso remoto (Remote Access Tool, RAT) RMS [Remote Manipulator System (Sistema de manipulación remota)].
A lo largo del año, observamos que el grupo modificaba sus TTP para entregar estas cargas útiles, probablemente para evitar la detección. FIN11 alternaría entre adjuntar archivos de Office habilitados para macros o adjuntar archivos HTML que redirigieran a las URL de descarga que entregan los archivos de Office maliciosos. Estos cambios en las TTP se produjeron rápidamente: la Figura 1 ilustra algunas de las TTP de entrega observadas durante el segundo trimestre de 2019. En agosto, FIN11 comenzó a pasar de la puerta trasera FlawedAmmyy al cargador FRIENDSPEAK.

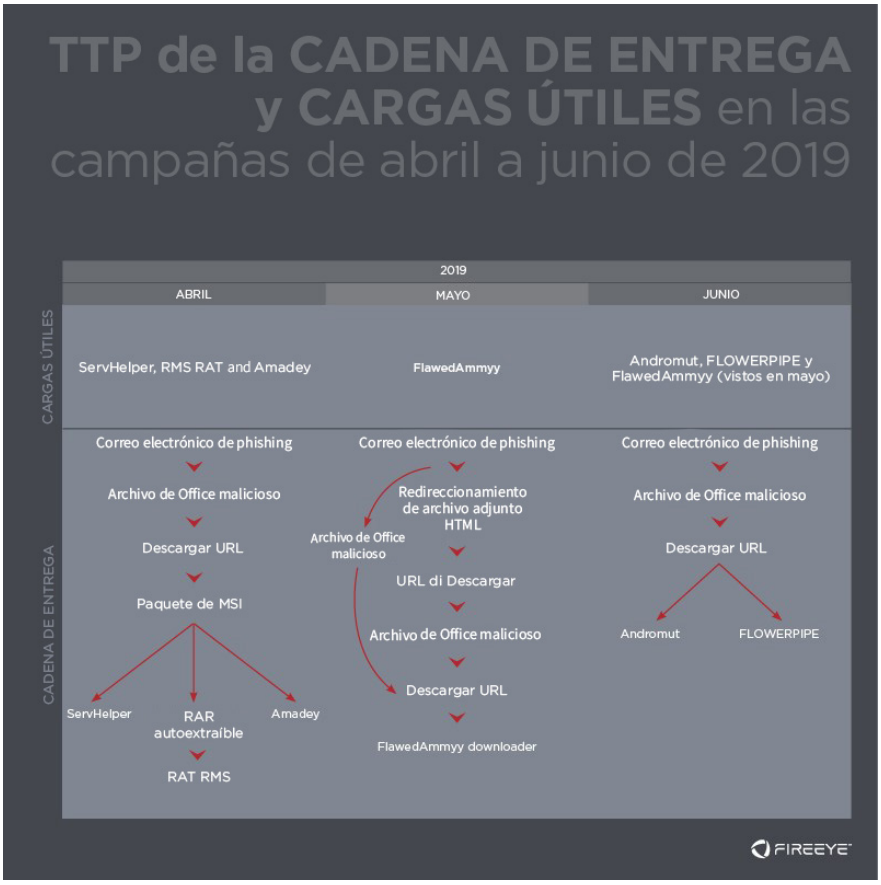


Figura 1.
Ejemplos de entrega de TTP observados desde abril hasta junio de 2019

Abril de 2019

En abril, FIN11 usó constantemente archivos adjuntos maliciosos de Office, incluidos .doc, .xls y .wiz, para descargar paquetes de Windows Installer (.msi). Durante la primera mitad del mes, estos paquetes entregaron ServHelper. Una campaña del 18 al 19 de abril también entregó ServHelper en algunos casos, pero proporcionó archivos RAR autoextraíbles que contenían RAT RMS en otros casos. Alrededor del 24 de abril, el grupo cambió la carga útil a Amadey. La información obtenida de fuentes sensibles indica que FlawedAmmyy y EMASTEAL se distribuyeron como cargas útiles secundarias de estas campañas, así como BARBWIRE, a un conjunto de víctimas más limitado.

Mayo de 2019

En mayo, FIN11 intentó entregar FlawedAmmyy a través de archivos adjuntos de Excel habilitados para macros o archivos adjuntos HTML que descargaban archivos de Excel desde las URL (Figura 2). También observamos campañas sospechosas de FIN11 a principios de mes que usaban archivos de Office maliciosos para entregar paquetes de Windows Installer que contenían cargas útiles de Amadey.

Figura 2.
Captura de pantalla del correo electrónico de FIN11 de mayo de 2019

Junio de 2019

Las operaciones de junio de FIN11 se basaron en técnicas observadas en mayo para entregar cargas útiles de FlawedAmmyy, pero también utilizaron archivos maliciosos de Office para entregar el cargador de AndroMut y la puerta trasera FLOWERPIPE. También observamos al grupo usando la utilidad de robo de credenciales de correo electrónico EMASTEAL: según la funcionalidad de la herramienta, es posible que FIN11 estuviera intentando recopilar direcciones de correo electrónico para utilizarlas en campañas futuras. Si bien no observamos que EMASTEAL se entregara en junio, anteriormente hemos observado que EMASTEAL se entrega a través de Amadey. Además, observamos campañas de FIN11 sospechosas que entregaron Amadey o ServHelper.

Agosto de 2019

En agosto de 2019, FIN11 se alejó de sus cargas útiles preferidas, el cargador sin nombre FlawedAmmyy y FlawedAmmyy. Se cree que este es el comienzo del uso grupal de MINEDOOR y FRIENDSPEAK, una combinación de FIN11 utilizada durante el otoño de 2019 y la primavera de 2020. FIN11 usó documentos de Word habilitados para macros para entregar cargadores empaquetados de MINEDOOR, que cargaban cargas útiles de FlawedAmmyy. Estas macros aprovecharon el código para descargar una carga útil codificada en XOR o iniciar msiexec para descargar un instalador MSI que contiene la carga útil. También observamos una campaña de FIN11 sospechosa a finales de agosto que parecía utilizar un prototipo de JavaScript del cargador FRIENDSPEAK para entregar FlawedAmmyy.

Campañas de septiembre de 2019 a junio de 2020

Desde septiembre de 2019 hasta junio de 2020, FIN11 realizó cambios incrementales en las técnicas utilizadas para entregar archivos de Office maliciosos, incluido el uso de servicios de acortamiento de URL, archivos adjuntos HTML e infraestructura comprometida. El grupo incorporó técnicas de entrega adicionales casi mensualmente, sin dejar de utilizar técnicas de campañas anteriores. La Figura 3 ilustra la introducción de estos TTP, centrándose en la cadena de entrega entre los correos electrónicos de phishing y los documentos maliciosos de Office. Los archivos de Office casi siempre usaban macros para entregar el inyector MINEDOOR y el cargador FRIENDSPEAK. FRIENDSPEAK parecía entregar sistemáticamente la puerta trasera MIXLABEL, a veces con un protocolo de transferencia segura de archivos PuTTY (PuTTY Secure File Transfer Protocol, PSFTP) legítimo, sin embargo, no siempre observamos la carga útil secundaria.

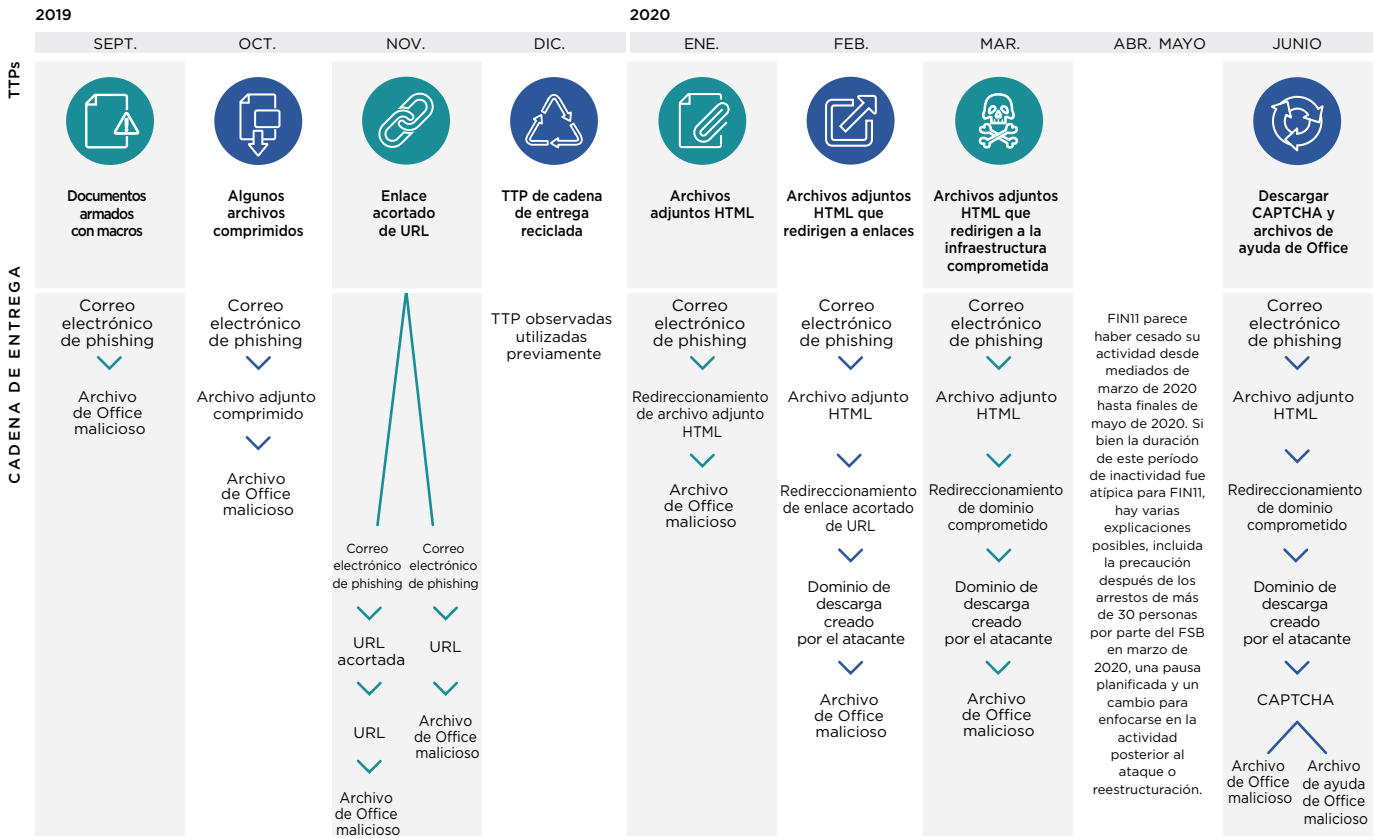


Figura 3.
TTP de entrega de FIN11 en las campañas FRIENDSPEAK de septiembre de 2019 a junio de 2020.

Septiembre de 2019

A partir de septiembre de 2019, FIN11 llevó a cabo campañas de phishing utilizando archivos de Office adjuntos, incluidos archivos adjuntos de Excel y Word, que aprovecharon macros maliciosos para distribuir MINEDOOR y FRIENDSPEAK. Continuamos observando FIN11 utilizando esta técnica mensualmente desde octubre de 2019 hasta diciembre de 2019, así como en marzo de 2020.

Octubre de 2019

Las campañas de octubre de 2019 aprovecharon el método de entrega de archivos adjuntos de documentos armados observado en el mes anterior. Observamos algunos casos en los que los archivos comprimidos adjuntos a los correos electrónicos de phishing contenían archivos de Excel habilitados para macros que entregaron FRIENDSPEAK y MINEDOOR. Los dominios de comando y control de FRIENDSPEAK y MIXLABEL utilizados en estas campañas disfrazados de entidades relacionadas con Microsoft y Windows. Observamos tipos similares de enmascaramiento en las campañas de diciembre y febrero.

Noviembre de 2019

En noviembre de 2019, FIN11 incorporó nuevos métodos de entrega que se basaban en gran medida en la incorporación de enlaces maliciosos en correos electrónicos de phishing. Una técnica observada utilizó servicios de URL abreviados, como is.gd y bit.do, que redirigían a un dominio de descarga creado por un atacante que distribuía archivos de Office maliciosos, que contenían cargas útiles de MINEDOOR y FRIENDSPEAK. FIN11 también usó enlaces integrados que llevaban directamente a descargar dominios. Los dominios de descarga a menudo usaban una redirección basada en scripts desde el identificador uniforme de recursos (Uniform Resource Identifier, URI) inicial a un recurso llamado download.php; este comportamiento no se limitó a noviembre de 2019, sino que también se observó en la mayoría de las campañas que usaban URL de descarga.

Diciembre de 2019

Las campañas de diciembre de 2019 aprovecharon los métodos de entrega anteriores para distribuir MINEDOOR y FRIENDSPEAK.

Enero de 2020

En enero de 2020, FIN11 aprovechó los archivos adjuntos HTML con redireccionamientos de JavaScript a sitios de descarga, a menudo disfrazados de servicios de intercambio de archivos que descargarían archivos Excel habilitados para macros entregando FRIENDSPEAK y MINEDOOR (Figura 4). Este mecanismo de entrega se utilizó junto con técnicas que observamos en campañas FIN11 anteriores, incluido el uso de enlaces de descarga maliciosos en correos electrónicos de phishing.

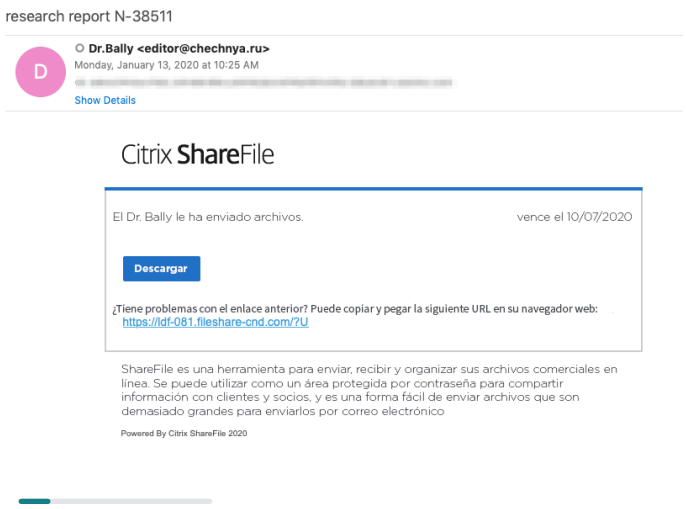


Figura 4.
Captura de pantalla del correo electrónico de FIN11 de enero de 2020

Febrero de 2020

Las campañas de febrero de 2020 también utilizaron archivos adjuntos HTML, pero se redirigieron a URL acortadas. Estos enlaces redirigían a dominios creados por FIN11, principalmente disfrazados de servicios de intercambio de archivos, que descargaban archivos de Excel maliciosos que distribuían MINEDOOR y FRIENDSPEAK. FIN11 utilizó varios servicios de acortamiento de URL, incluidos bit.do, is.gd, gg.gg, hec.su, tinyurl.com y chogoon.com.

Marzo de 2020

En marzo de 2020, FIN11 utilizó una variedad de métodos de entrega. Estos incluían archivos adjuntos HTML con redireccionamientos de JavaScript a la infraestructura comprometida que posteriormente se redirigían a un dominio de descarga controlado por el perpetrador. Algunos de los dominios comprometidos parecían utilizar el panel de control de Plesk, lo que sugiere que el grupo puede haber estado atacando sitios web que utilizan la plataforma de alojamiento web de Plesk. Además, el grupo usó URL de dominios comprometidos directamente en el cuerpo de los mensajes de correo electrónico y archivos adjuntos maliciosos de Excel.

Figura 5.
Captura de pantalla del correo electrónico de FIN11 de marzo de 2020

Junio de 2020

A principios de junio de 2020, FIN11 reanudó su actividad utilizando una cadena de infección casi idéntica a las observadas en marzo de 2020. Los correos electrónicos de phishing contenían archivos adjuntos HTML que redirigían a dominios comprometidos, que posteriormente se redirigían a un dominio de descarga controlado por un perpetrador que entregaba archivos de Office maliciosos. Las campañas posteriores utilizaron un dominio de descarga que llevaba a cabo una verificación CAPTCHA antes de entregar una hoja de cálculo de Excel típica cargada de macros o un archivo de ayuda de Office malicioso (.chm), lo que demuestra una evolución continua en la entrega de TTP.

Julio a septiembre de 2020

A lo largo del tercer trimestre de 2020, FIN11 continuó utilizando URL aparentemente comprometidas para redirigir los navegadores a fin de descargar dominios que entregaban archivos de Office maliciosos. El grupo utilizó tácticas de entrega previamente observadas, como incluir enlaces maliciosos dentro del cuerpo del mensaje o en un archivo adjunto HTML, pero introdujo pequeños cambios con regularidad. Por ejemplo, FIN11 varió la forma en que los archivos adjuntos HTML cargaban los enlaces maliciosos y realizó ligeras modificaciones en las macros de Office que entregaron FRIENDSPEAK. El cambio más significativo ocurrió en septiembre, cuando los perpetradores incorporaron técnicas de geovalla en las URL comprometidas para elegir selectivamente qué víctimas recibieron una carga útil maliciosa.

TTP de infraestructura

Antes de septiembre de 2019, las campañas de FIN11 utilizaban una infraestructura variada, incluidas las URL basadas en IP y la infraestructura probablemente comprometida, para alojar cargas útiles o para comando y control (C&C). Sin embargo, la infraestructura que respalda las campañas más recientes ha seguido patrones más predecibles. Desde septiembre de 2019, generalmente cada campaña empleaba varios dominios controlados por perpetradores para respaldar funciones como el alojamiento de documentos maliciosos y la infraestructura C&C de FRIENDSPEAK y MIXLABEL. La cantidad de tiempo que estos dominios permanecieron activos varió según su función. Por ejemplo, el alojamiento de documentos y los dominios C&C de FRIENDSPEAK generalmente permanecían "activos" durante horas o días para respaldar una sola campaña, mientras que la infraestructura de MIXLABEL puede permanecer activa durante semanas para respaldar varias campañas.

Macromodificaciones
Los archivos maliciosos de Office que se utilizan para entregar el cargador de FRIENDSPEAK han presentado cambios menores a lo largo del tiempo. Estos documentos contenían la DLL FRIENDSPEAK empaquetada en MINEDOOR incorporada como un objeto OLE. Una vez habilitado, el código de macro copiaría el archivo de Office a una ubicación temporal con una extensión ".zip". Luego, la macro ubicaría el archivo de objeto binario OLE dentro del archivo ZIP y extraería la DLL maliciosa, guardándola en una ubicación temporal con la extensión ".dll". La DLL extraída se iniciaría usando uno de los dos métodos siguientes:

- En ejemplos anteriores, el código de macro utilizaría llamadas directas a la función de la API de Windows kernel32.LoadLibraryW para cargar la DLL FRIENDSPEAK en la memoria. Luego llamaría directamente a una función exportada desde la DLL recién cargada para iniciar la funcionalidad de FRIENDSPEAK.
- En ejemplos posteriores, en lugar de usar la función LoadLibraryW y un paso separado para invocar una función exportada en particular, el código de macro usaría la función "CALL" de ExecuteExcel4Macro para iniciar la función exportada de la DLL.

Modificaciones como estas son casi con certeza un esfuerzo por evadir los mecanismos de detección, ya que las variaciones menores de los métodos utilizados para ejecutar el código pueden tener un impacto significativo en firmas a veces definidas de manera estricta diseñadas para detectar este tipo de actividad.

Actividad posterior a la explotación
A pesar de las campañas de phishing generalizadas de alto volumen del grupo, solo hemos observado evidencia de que FIN11 monetiza con éxito sus operaciones en un puñado de casos. A fines de 2018, Mandiant observó el intento de FIN11 de monetizar sus operaciones utilizando la herramienta de raspado de memoria de punto de venta (POS) BLUESTEAL en una organización de restaurantes. Desde entonces, FIN11 ha implementado el ransomware CLOP en una variedad de organizaciones e incorporado el robo de datos para aumentar la presión sobre las víctimas, a fin de que paguen tarifas de extorsión.

Raspado de POS
A finales de 2018, observamos el intento de FIN11 de utilizar la herramienta de raspado de memoria de POS BLUESTEAL en una víctima de la industria de restaurantes, que se presta a pagos frecuentes con tarjeta de crédito y débito.

- FIN11 instaló la puerta trasera BARBWIRE y reemplazó el ejecutable Sticky Keys con cmd.exe para establecer la persistencia en el entorno de la víctima durante aproximadamente tres días antes de implementar BLUESTEAL y una puerta trasera secundaria. Luego, el grupo intentó realizar el raspado de POS utilizando BLUESTEAL en varios hosts durante varios meses.

Ransomware

Entre finales de 2019 y principios de 2020, FIN11 implementó ransomware CLOP, una familia de malware que actualmente se cree que es exclusiva del grupo, para monetizar sus operaciones. Mandiant ha respondido a varias implementaciones de ransomware CLOP de FIN11 desde septiembre de 2019; sin embargo, consideramos que FIN11 ha estado implementando ransomware CLOP desde al menos principios de 2019.

- La primera referencia al ransomware CLOP parece ser un tweet del 8 de febrero de 2019 del investigador de seguridad Michael Gillespie.
- Entre febrero y mayo de 2019, identificamos los certificados de firma de código utilizados para firmar tanto las muestras de FlawedAmmyy utilizadas en las campañas FIN11 como las muestras de ransomware CLOP (Tabla 1). Uno de los certificados también se utilizó para firmar hojas de cálculo de Excel atribuidas a FIN11.

Tabla 1. Certificados utilizados para firmar CLOP y FlawedAmmyy

Nombre común (país)	MD5	Emisor	Fecha de inicio de validez	Fechas de compilación de CLOP	Fechas de compilación de FlawedAmmyy
COME AWAY FILMS LTD (GB)	e259a49a8f996e398d8d78b385fc8585	Sectigo Limited	23 de febrero de 2019	Variado, pero se cargaron muestras en un repositorio de malware entre marzo y abril de 2019 durante el período de validez del certificado.	Finales de febrero de 2019
VIEW DESIGN LIMITED (GB)	19b2nmDGUQrYT3in9Pr4YNqs46c6P7nK45	Thawte, Inc.	27 de mayo de 2019	Es probable que la muestra se haya modificado con el tiempo; sin embargo, se cargó en un repositorio de malware a fines de mayo de 2019 durante el período de validez del certificado.	Finales de mayo de 2019

Observamos los siguientes TTP durante las implementaciones de CLOP de FIN11:

- A los pocos días de la intrusión inicial, FIN11 instaló múltiples puertas traseras, intentó obtener privilegios de administrador de dominio y se desplazó lateralmente dentro de la red de la organización afectada. Si bien las puertas traseras utilizadas como puntos de apoyo iniciales (FlawedAmmyy y MIXLABEL) pueden ser exclusivas de FIN11, los perpetradores generalmente usaron herramientas comunes disponibles públicamente durante esta fase.
- Antes del despliegue de CLOP, los perpetradores utilizaron SALTLICK para desactivar Windows Defender.
- Luego los perpetradores utilizaron la herramienta de instalación e implementación NAILGUN para implementar CLOP, a veces atacando a cientos de sistemas. Con menos frecuencia, los perpetradores implementaron CLOP con objetos de la política de grupo.
- FIN11 a menudo ha sido rápido para volver a atacar los hosts en las organizaciones después de perder el acceso. Por ejemplo, una organización se vio atacada en varias campañas de phishing de FIN11 en cuestión de meses. En otra organización, varios servidores se infectaron con CLOP, se restauraron a partir de copias de seguridad y luego se volvieron a infectar. No es clara la forma en que FIN11 volvió a infectar estos sistemas.

Extorsión

Más recientemente, en 2020, FIN11 ha llevado a cabo ataques de extorsión híbridos, combinando ransomware con robo de datos para presionar a sus víctimas a aceptar las demandas de extorsión. En los casos en que observamos el robo de datos, los perpetradores accedieron a varias docenas de sistemas, almacenaron datos en archivos RAR, cargaron los archivos en los servidores MegaSync, implementaron el ransomware CLOP y luego enviaron un correo electrónico amenazando con publicar los datos. Los datos extraídos se publicaron más tarde en un sitio web oscuro llamado CL0P^ _– LEAKS. Dado que solo hemos observado CLOP distribuido por FIN11, consideramos que también mantienen este sitio.

CL0P^_– LEAKS: Nombrar y humillar

A fines de febrero de 2020, se creó un sitio web para compartir datos robados de víctimas asociados con incidentes de ransomware CLOP, una técnica cada vez más común diseñada para aumentar la presión sobre las víctimas de extorsión. (19-00021828). El sitio estaba mal configurado, lo que hacía que los registros y las copias de seguridad fueran accesibles y proporcionaba información sobre cómo ha cambiado el sitio con el tiempo.

- Los primeros datos de las víctimas se publicaron el 26 de febrero de 2020. Los perpetradores afirmaron que habían notificado a la empresa de una vulnerabilidad en su sitio web y luego publicaron los datos después de que la empresa se negó a proporcionar una "recompensa". No podemos verificar la afirmación de los perpetradores; sin embargo, sería notable si los perpetradores obtuvieran acceso a través de una vulnerabilidad o una mala configuración del servidor web, ya que el vector de infección normal de FIN11 son los correos electrónicos de phishing.
- Para mediados de mayo de 2020, los perpetradores habían filtrado datos asociados con al menos ocho empresas. En algunos casos, publicaron los datos en partes, probablemente para alentar a las víctimas a pagar el rescate antes de que se filtraran más datos potencialmente dañinos. En el archivo de recuento de páginas vistas se incluyó una novena empresa; sin embargo, no identificamos ningún dato asociado. Es posible que la víctima haya pagado el rescate y, por lo tanto, los datos no se publicaron o se eliminaron antes de la siguiente copia de seguridad.
- Mandiant respondió a una intrusión de primavera de 2020 en la que FIN11 no implementó el ransomware CLOP, sino que parecía depender únicamente de la extorsión por robo de datos. Los perpetradores exfiltraron cientos de gigabytes de datos, que se publicaron en el sitio CL0P Leaks después de que la compañía se negó a pagar decenas de millones de dólares en rescate. No está claro si los perpetradores habían planeado implementar CLOP eventualmente.
- Los perpetradores también han utilizado el sitio web para anunciar servicios de seguridad cibernética, aparentemente pruebas de penetración, por 250 000 dólares en bitcoins.

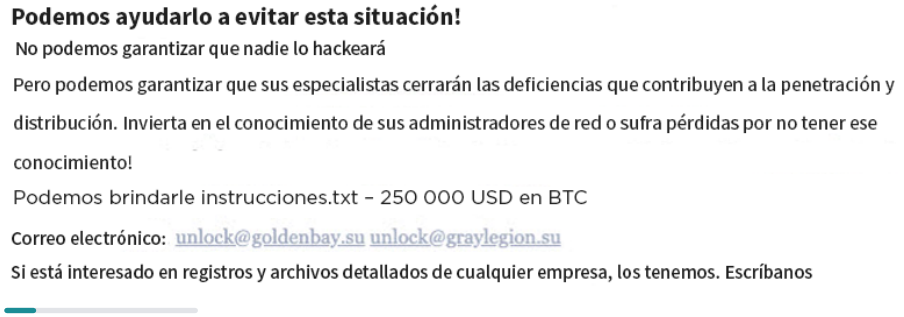
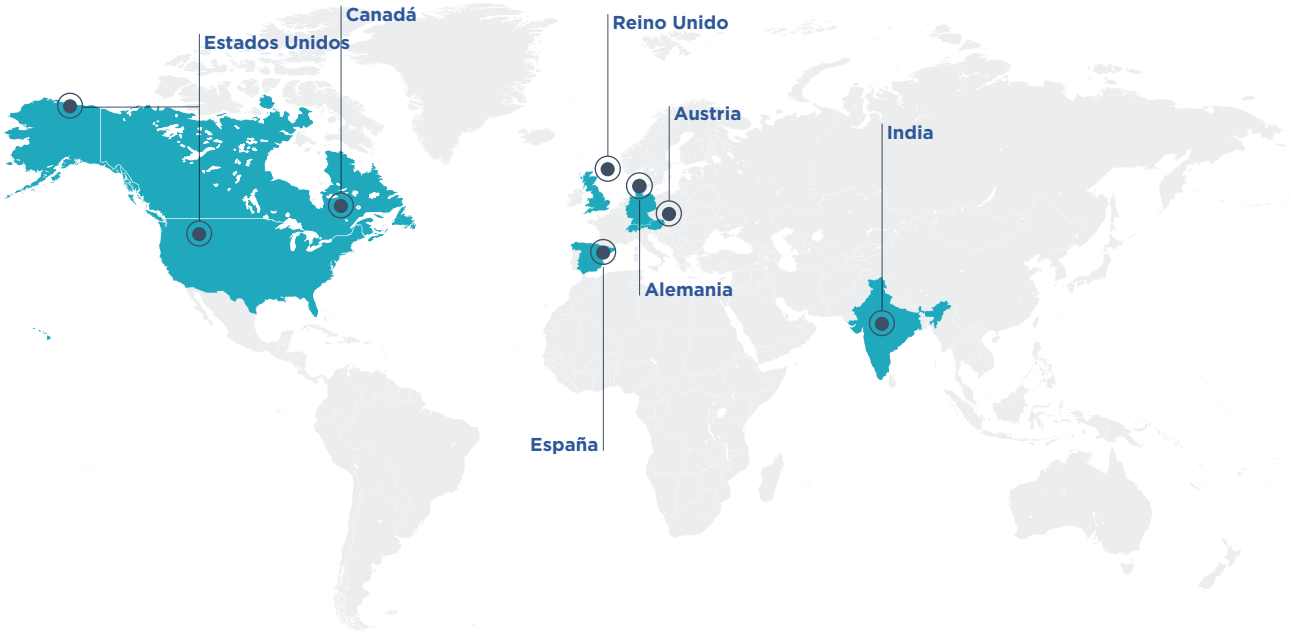


Figura 6.
Texto de la página de inicio de CL0P^ _–LEAKS

Las presuntas víctimas que aparecen en el sitio web CL0P^ _–LEAKS se han basado con mayor frecuencia en Europa (Figura 7); aproximadamente, la mitad de las organizaciones de víctimas tienen su sede en Alemania. Si bien estos datos están sesgados hacia aquellos que optaron por no aceptar las demandas de extorsión, FIN11 ha utilizado engaños en alemán en muchas de sus campañas de 2020, lo que sugiere que atacaron activamente a organizaciones que realizan negocios en alemán.

Figura 7.

Geolocalización de presuntas víctimas de CL0P^ _–LEAKS



En particular, durante la COVID-19, se publicó un mensaje en el sitio web de CL0P en el que se indicaba que no atacarían a organizaciones del sector sanitario o benéfico, pero que continuarían atacando organizaciones farmacéuticas comerciales que se benefician de la pandemia. Este mensaje es coherente con nuestras observaciones de empresas farmacéuticas que han sido objeto de campañas no deseadas de FIN11 a principios de 2020.

Pagos de rescate

A las víctimas del ransomware CLOP se les indica que se comuniquen con las direcciones de correo electrónico especificadas en las notas del ransomware, en lugar de ser dirigidas a un portal de pago como otras operaciones de ransomware. Las notas de rescate no especifican la demanda de rescate. La Figura 8 ilustra un ejemplo de nota de ransomware CLOP de FIN11.

Muestra de nota de rescate

```
-=-=REENVÍENOS EL ARCHIVO=-=-=

==CORREO ELECTRÓNICO DE CONTACTO==:
unlock@goldenbay.su
o
unlock@graylegion.su
Y
crescopute1985@protonmail.com

Cuanto más rápido escriba, menor será el precio.
Cl0p^_-
```

Figura 8.

Muestra de nota de rescate

Los informes públicos y los datos compartidos por la firma de remediación de ransomware Coveware sugieren que FIN11 ha exigido una amplia gama de pagos de rescate, entre unos pocos cientos de miles de dólares y hasta 10 millones de dólares.

- A mediados de noviembre de 2019, el Centro Hospitalario Universitario (CHU) de Rouen recibió una respuesta automática de los operadores de CLOP que indicaba que el rescate era de 40 bitcoins (aproximadamente 340 000 USD); el hospital indicó que no pagaría el rescate.
- A finales de diciembre de 2019, la Universidad de Maastricht pagó un rescate de 30 bitcoins (aproximadamente 220 000 USD). Los informes públicos no indican si la demanda inicial de rescate fue mayor.
- Durante la primera mitad de 2020, Coveware habría negociado pagos CLOP en nombre de varios clientes, donde la demanda inicial promedió 1,1 millones de dólares, aproximadamente; en ambos casos, se proporcionó un descifrador, la tasa de recuperación de datos fue extremadamente alta y los datos extraídos no fueron liberados por el perpetrador de la amenaza.
- En particular, en otro caso en 2020, Coveware declaró que la demanda inicial de rescate fue de 10 millones de dólares.

Es posible que FIN11 haya aumentado las demandas de rescate en respuesta a informes públicos de empresas que pagan grandes rescates. La demanda de rescate de 10 millones de dólares no solo es significativamente más alta que los pagos de rescate anteriores de CLOP, sino que también es alta en comparación con la mayoría de las otras implementaciones de ransomware posteriores al ataque. El drástico aumento podría estar relacionado con la introducción de la extorsión híbrida.

Los proveedores criminales habilitan las operaciones FIN11

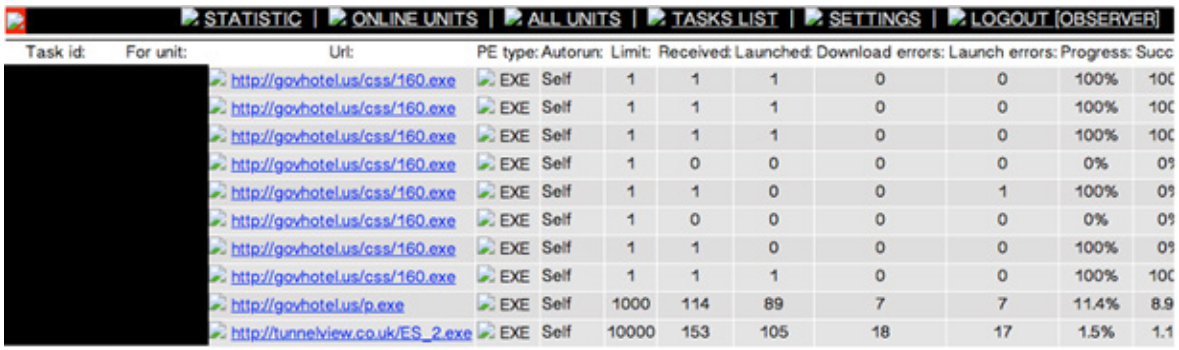
FIN11 aparentemente ha aprovechado varios proveedores delictivos, como los que brindan malware, registro de dominios y servicios de firma de códigos, para realizar sus operaciones (Figura 9). Su uso de proveedores delictivos es en gran medida consistente con otros grupos de amenazas motivados financieramente: es común que los perpetradores que se especializan en una sola fase del ciclo de vida del ataque ofrezcan sus servicios a la venta en los mercados de delitos cibernéticos. Los perpetradores pueden adquirir una amplia gama de servicios y herramientas en comunidades clandestinas, incluidas capacidades de malware privadas o semiprivadas, proveedores de alojamiento a prueba de balas, varios servicios relacionados con DNS (incluido el registro y las ofertas de DNS dinámico o de flujo rápido) y certificados de firma de código.

Figura 9.
Servicios utilizados por FIN11.

Implementación de malware de segunda etapa a través de Amadey

Durante la primavera y el verano de 2019, las muestras FlawedAmmyy, BARBWIRE y EMASTEAL atribuidas a FIN11 se distribuyeron como cargas útiles secundarias de Amadey. Amadey es un cargador que ha sido anunciado por el perpetrador de habla rusa "InCrease" en el foro Exploit desde octubre de 2018. (18-00017241). Con base en información obtenida de fuentes sensibles confiables, las cargas útiles secundarias de BARBWIRE se entregaron solo a un subconjunto de máquinas infectadas, lo que sugiere que FIN11 está perfilando a las víctimas para una mayor explotación.

- A los clientes de Amadey se les proporciona un panel que les permite emitir comandos a los hosts infectados con Amadey en un nivel granular (Figura 10).
- El análisis de una instancia de panel de Amadey asociada con un dominio atribuido a FIN11 reveló que las cargas útiles de FlawedAmmyy y EMASTEAL se entregaron a todas las víctimas como cargas útiles de segunda etapa de varias campañas FIN11 de Amadey. Además, en al menos un caso, BARBWIRE se entregó como carga útil de segunda etapa a solo un pequeño número de víctimas.
- El 24 de abril de 2019, una campaña de phishing atribuida a FIN11 entregó Amadey. Si bien no identificamos cargas útiles secundarias para esa URL específica de C&C de Amadey, observamos otra botnet de Amadey que entrega cargas útiles FlawedAmmyy y BARBWIRE el mismo día.
- Los informes públicos del Instituto de Seguridad Financiera (Financial Security Institute, FSI) de Corea del Sur sugieren que FIN11 pudo haber estado usando el mismo servidor en abril de 2019 para la gestión de botnets de Amadey, así como C&C para una herramienta de robo de credenciales de correo electrónico (EMASTEAL) utilizada por el grupo.



Task id:	For unit:	Url:	PE type:	Autorun:	Limit:	Received:	Launched:	Download errors:	Launch errors:	Progress:	Succ
[redacted]		http://govhotel.us/css/160.exe	EXE	Self	1	1	1	0	0	100%	100
		http://govhotel.us/css/160.exe	EXE	Self	1	1	1	0	0	100%	100
		http://govhotel.us/css/160.exe	EXE	Self	1	1	1	0	0	100%	100
		http://govhotel.us/css/160.exe	EXE	Self	1	0	0	0	0	0%	0%
		http://govhotel.us/css/160.exe	EXE	Self	1	1	0	0	1	100%	0%
		http://govhotel.us/css/160.exe	EXE	Self	1	0	0	0	0	0%	0%
		http://govhotel.us/css/160.exe	EXE	Self	1	1	0	0	0	100%	0%
		http://govhotel.us/css/160.exe	EXE	Self	1	1	1	0	0	100%	100
		http://govhotel.us/p.exe	EXE	Self	1000	114	89	7	7	11.4%	8.9
		http://tunnelview.co.uk/ES_2.exe	EXE	Self	10000	153	105	18	17	1.5%	1.1

Figura 10.
Ejemplo de panel de Amadey que muestra las instrucciones de entrega

Servicio de registro de dominio

Evaluamos con poca confianza que FIN11 ha utilizado dominios registrados a través de un servicio de registro de dominios anónimo. El registro de dominio es un proceso relativamente fácil y rápido. Sin embargo, la obtención de una infraestructura no facturable o errónea puede llevar mucho tiempo. Al subcontratar este trabajo a perpetradores que se especializan en el registro de dominios anónimos, los perpetradores pueden concentrarse en sus propias áreas de especialización.

Este supuesto servicio de registro de dominios ha proporcionado dominios a FIN11 y a otros perpetradores desde al menos 2014. Entre septiembre y octubre de 2019, observamos que varios dominios registrados por el servicio de registro de dominio sospechoso se utilizaban como dominios de descarga o C&C para las campañas de FIN11 que entregaron MINEDOOR y FRIENDSPEAK (Tabla 2).

Sospechamos que estos dominios están asociados con un servicio de registro según las diferencias entre las campañas que usan los dominios de este servicio, incluidas las herramientas utilizadas, los métodos de entrega, los ataques y los métodos de monetización. Por ejemplo, en octubre de 2019, observamos los dominios utilizados en las campañas atribuidas a FIN11, así como múltiples operaciones aparentemente no relacionadas, que incluyen:

- Campañas de FIN11 entregando MINEDOOR y FRIENDSPEAK a una variedad de víctimas potenciales
- Páginas de recopilación de credenciales disfrazadas de bancos irlandeses
- Correos electrónicos de phishing que contienen archivos PDF maliciosos dirigidos a víctimas en Australia y Nueva Zelanda.
- Correos electrónicos de phishing dirigidos a entidades alemanas enviados a través de la botnet Cutwail y probablemente entregando Dridex.

En particular, algunos de los dominios de FIN11 registrados en septiembre y octubre de 2019 no parecían estar asociados con este servicio de registro de dominios. Además, los dominios FIN11 registrados entre noviembre de 2019 y marzo de 2020 utilizaron la protección de privacidad de Eranet, por lo que se eliminaron los detalles del registrante. FIN11 puede haber descontinuado el uso del servicio de registro de dominios; sin embargo, también es plausible que el servicio brinde varias opciones de registro de dominio, para incluir datos de registrantes protegidos por privacidad.

Tabla 2. Ejemplos de registro de dominio

Dominio	Fecha de registro	Registrador	Información del registrante
windows-update-02-en.com	2 de setiembre de 2019	Registro de dominio público	Artak Gasparyan Shinararneri str. 43 Yerevan, YVN, AM whois-agent@gmx.com
office365-eu-update.com	13 de octubre de 2019	Registro de dominio público	Artak Gasparyan Shinararneri str. 43 Yerevan, YVN, AM whois-agent@gmx.com
windows-afx-update.com	15 de octubre de 2019	Registro de dominio público	Wiet Lee NO.1111 Chaoyang Road, Beijing, CN whois-protect@hotmail.com
windows-office365.com	24 de octubre de 2019	Registro de dominio público	Wiet Lee NO.1111 Chaoyang Road, Beijing, CN whois-protect@hotmail.com

Posible uso del servicio de firma de código

A lo largo de 2019, observamos que FIN11 utiliza con frecuencia certificados de firma de código válidos para firmar su malware, lo que probablemente aumentará la efectividad de sus campañas. Muchos de estos certificados comparten características comunes, como el uso de organizaciones con sede en el Reino Unido con direcciones físicas incorrectas como asunto del certificado. Al buscar superposiciones de certificados en las muestras, identificamos muchos casos en los que se firmó malware aparentemente no relacionado con certificados que compartían un tema en común. El uso de certificados de firma de código con características superpuestas por lo que parecen ser varios perpetradores no relacionados parece una coincidencia poco probable y sugiere que estos certificados se adquieren de una fuente común.

- Se asociaron varios certificados con la misma organización y, a menudo, los emitió la misma autoridad de certificación. En gran parte, las organizaciones parecían ser empresas pequeñas. Además, los certificados que contenían los nombres de estas organizaciones no incluían direcciones físicas precisas.
- Identificamos al menos ocho certificados distintos que comparten el valor de nombre común "ET HOMES LTD" (Tabla 3). Solo uno de estos certificados se utilizó para firmar muestras atribuidas a FIN11. Otras muestras firmadas por certificados que comparten el mismo valor de nombre común incluyen AZORult, GANDCRAB, GODZILLA LOADER y BETABOT.

Tabla 3. Superposición de certificados de nombre común ET HOMES LTD

MD5	familias de malware	Emitiendo CA	Clave pública MD5	Atribución
c94f47e8f25c3b41df97ecb3c23ccf5d	FlawedAmmyy, MINEDOOR	Thawte	24016bd5a1e0c03474cb97c1253a5dad	FIN11
a19ebe61347b91f997257cf3104b9621	AZORult, Godzilla, Remcos	Comodo	dfd53dd143e1d904d16fae05e929a8f9	Ninguna
87cf140238fd26a03b815bb229eef009	GANDCRAB	Comodo	89c9a36bb642b0b8dfb0cdc6ae9e5238	Ninguna
b7dfc43bdd46c560a3e32d6eaea25bc8a	AZORult, GANDCRAB, GODZILLA	Comodo	ce2b80abfbc72c0a74d3745ca3faedfe	Ninguna
491ef81a6f6f1849797b39091a6046de	AZORult	Comodo	024e15a4287dad10a8314d8c2c593651	Ninguna
6d3b27150b04d94ffa77441132f8f24a	AZORult	Comodo	c8439866c526ccd673f2aeed0be2f894	Ninguna
d2c06720c0896a50ecaa5a27633be1d3	AZORult	Comodo	10a54f36e3a95e802f5ff5a2773110c8	Ninguna
169b1841347ebb2d43a326417a6f05bd	AZORult, BETABOT	Comodo	7324e4ed9fbc1d157e8433fc30740b	Ninguna

El uso de certificados de firma de código para firmar malware no es una técnica nueva; sin embargo, sigue siendo popular entre los perpetradores, ya que puede hacer que el malware parezca más legítimo para los usuarios objetivo y puede evadir algunos mecanismos de protección de Windows. Los certificados de firma de código válidos generalmente se pueden obtener robando o comprometiendo certificados de organizaciones legítimas o adquiriéndolos de las autoridades de certificación utilizando información falsificada (20-00003595). Si bien históricamente el uso de certificados robados o comprometidos fue un enfoque empleado por perpetradores sofisticados, en los últimos años, Mandiant ha identificado múltiples proveedores en foros clandestinos que anuncian certificados de firma de código legítimos para la venta.

Distribución de correo electrónico a través de Necurs
Si bien no hemos confirmado de forma independiente el uso de Necurs por parte de FIN11, vale la pena señalar que la actividad de TA505 informada públicamente sugirió que el grupo usó la botnet Necurs para distribuir un correo electrónico de phishing desde al menos 2016. Desde entonces y hasta 2018, hubo reducciones en la actividad de TA505 que se correspondían directamente con pausas en la actividad de Necurs. Estas interrupciones se observaron desde diciembre de 2016 a marzo de 2017 y de enero a febrero de 2018. Esta correlación sugiere que Necurs fue el vector de distribución principal de TA505. En particular, Proofpoint informó una campaña atribuida a TA505 que utilizó Necurs para entregar FlawedAmmyy en marzo de 2018, aunque la colaboración entre TA505 y Necurs pareció terminar en 2018.

- En marzo de 2020, Microsoft anunció la interrupción coordinada de la botnet de Necurs. Necurs había estado activo desde 2012 y probablemente sus operadores lo alquilaron a varios ciberdelincuentes que aprovecharon la botnet para enviar correos electrónicos maliciosos. Durante estos años, Necurs permitió varios tipos de actividad maliciosa, incluida la distribución de malware, las estafas románticas y las estafas del tipo "inflar y vender".

Desafíos de atribución
La subcontratación de herramientas y servicios asociados con varias partes del ciclo de vida del ataque a través de proveedores de servicios criminales puede frustrar los esfuerzos de atribución. Los analistas pueden mezclar accidentalmente la actividad entre proveedores de servicios y clientes e implicar un vínculo entre grupos dispares basados en indicadores y TTP que son atribuibles a un proveedor de servicios común. Un ejemplo principal que causa confusión con la actividad de FIN11 y TA505 es el uso de malware compartido, especialmente porque a menudo hay un retraso entre la identificación del malware y el descubrimiento de que es proporcionado por un servicio y utilizado por varios clientes.

- TA505 se ha combinado comúnmente con los "operadores Locky" o los "operadores Dridex (Evil Corp)". Si bien TA505 puede haber distribuido estas dos familias, es importante tener en cuenta que se cree que Locky y Dridex operan bajo un modelo de afiliados. Según este modelo de negocio, un afiliado sería responsable de la distribución del malware, ya sea directamente él mismo o mediante la contratación de otro tercero.
- Los investigadores han identificado múltiples similitudes entre FIN11 y TEMP.TruthTeller (también conocido como Silence Group), principalmente agrupadas en torno al uso de variantes TRUEBOT (también conocido como Silence.Downloader) y SLOWROLL (también conocido como Silence. Mainmodule). Según la evidencia disponible en el momento del análisis, no está claro si estas superposiciones son el resultado de una afiliación comercial, un proveedor compartido o una conexión más cercana, como un miembro común o varios. Consulte el Apéndice B para obtener más información.

De manera similar, el uso potencial de FIN11 de un servicio de registro de dominio y un proveedor de certificado de firma de código compartido podría potencialmente conducir a la atribución de una actividad no relacionada.

- Se cree que el servicio de registro utilizado por FIN11 en 2019 se remonta a 2013 y está asociado con actividad y malware no atribuidos a FIN11.
- Los certificados de firma de código FIN11 utilizados en 2019 probablemente fueron proporcionados por un servicio: se han utilizado certificados con los mismos nombres comunes para firmar muestras de malware no atribuidas al grupo.

Inyectores compartidos

Desde el otoño de 2019, FIN11 ha utilizado FORKBEARD, SPOONBEARD y MINEDOOR para inyectar una variedad de cargas útiles. Los informes públicos no distinguen entre estos inyectores, ya que son bastante similares y podrían ser variantes de la misma familia de malware. De hecho, hay al menos un desempaquetador disponible públicamente que funciona bien en todas las variaciones que hemos observado. La comparación de muestras representativas de cada una de estas variantes identificó una gran superposición con algunas diferencias clave.

- El flujo de ejecución siguió un patrón muy similar de decodificación y ejecución de shellcode que a su vez decodificaría y ejecutaría un binario integrado en todas las variantes.
- Si bien las familias utilizaron diferentes algoritmos de decodificación, las operaciones de apoyo fueron muy similares, incluido el uso de argumentos y variables similares para indexar distancias específicas en matrices que contienen datos codificados.
- Las características distintivas entre cada variación incluyeron cambios menores en algoritmos de codificación específicos, el almacenamiento y manejo de claves XOR que soportan esos algoritmos, y la inclusión de funciones adicionales en shellcode por lo demás extremadamente similar.

Según las similitudes identificadas, sospechamos que se utilizó un desarrollador común con diferentes opciones, configuraciones o capacidades polimórficas para crear estos inyectores. Sin embargo, elegimos rastrear estas variaciones por separado porque existen diferencias, aunque menores, en sus mecanismos de codificación, y parece haber patrones en cuanto a cuándo o cómo se han utilizado.

- La variante de MINEDOOR ha inyectado el cargador de FRIENDSPEAK y, en un pequeño número de casos, FlawedAmmyy.
- La variante FORKBEARD se ha utilizado casi exclusivamente para inyectar BARBWIRE, pero también lo hemos observado inyectando FlawedAmmyy.
- La variante SPOONBEARD se ha utilizado para inyectar una amplia variedad de cargas útiles de FIN11, como AndroMut, BARBWIRE, CLOP, EMASTEAL, FlawedAmmyy, FLOWERPIPE y SALTLICK.

Es posible que estos inyectores, o el desarrollador utilizado para crearlos, no sean exclusivos de FIN11 debido a varias instancias en las que han lanzado malware normalmente asociado con otros grupos de amenazas (Tabla 4). No hemos identificado si se comparten los inyectores ni cómo; sin embargo, esto podría indicar que un desarrollador utilizado para generar los inyectores se ofrece en foros clandestinos o que FIN11 tiene membresía superpuesta con otros grupos de amenazas.

Tabla 4. Familias de malware asociadas con inyectores de FIN11
(el * denota actividad sospechosa de estar asociada con un grupo de amenazas diferente)

Inyector	Familias inyectadas	Notas
SPOONBEARD	Amadey AndroMut AZORult* BARBWIRE CLOP EMASTEAL FlawedAmmyy FLOWERPIPE JESTBOT* POPFLASH SALTLICK SCRAPMINT* SLOWROLL* TINYMET VIDAR*	• En mayo de 2019, se cargó una muestra de SCRAPMINT con SPOONBEARD en VirusTotal. SCRAPMINT se asocia típicamente con FIN6; sin embargo, según varios casos de respuesta ante incidentes de Mandiant, creemos que SCRAPMINT ha sido utilizado por varios perpetradores para realizar operaciones de malware en POS. • Entre agosto y diciembre de 2019, identificamos muestras de SPOONBEARD que entregaron malware de robo de credenciales AZORult o VIDAR. Es creíble que FIN11 haya utilizado a estos ladrones de credenciales; sin embargo, tanto AZORult como VIDAR se han comercializado en foros clandestinos y son utilizados por varios perpetradores. • A finales de 2019 y principios de 2020, identificamos muestras SPOONBEARD que entregaron SLOWROLL y JESTBOT respectivamente. SLOWROLL es una puerta trasera asociada con la actividad posterior al ataque de TEMP.TruthTeller. JESTBOT comparte algunas similitudes en funcionalidad y estructura de código con los malware TRUEBOT y SLOWROLL, los cuales se han utilizado en campañas TEMP.TruthTeller; sin embargo, carecemos de evidencia suficiente para atribuir esta actividad al grupo de amenazas (20-00003380).
FORKBEARD	BARBWIRE FlawedAmmyy SHORTBENCH* Meterpreter*	Observamos a FORKBEARD inyectando SHORTBENCH y meterpreter en una intrusión de abril de 2020. FIN11 ha utilizado estas herramientas relacionadas con Metasploit; sin embargo, actualmente no disponemos de pruebas suficientes para atribuir esta intrusión a FIN11. SHORTBENCH y meterpreter son utilizados por una variedad de perpetradores, por lo que esta actividad posiblemente fue realizada por otro grupo de amenazas.
MINEDOOR	FlawedAmmyy FRIENDSPEAK MINEBRIDGE*	En enero de 2020, Mandiant identificó campañas de phishing que usaban MINEDOOR para entregar la puerta trasera MINEBRIDGE (20-00001525). La superposición limitada en los TTP entre estas campañas y las campañas de FIN11 contemporáneas puede sugerir que MINEDOOR no es exclusivo de FIN11.

Origen potencial de CEI

Evaluamos con moderada confianza que FIN11 probablemente esté operando fuera de la Comunidad de Estados Independientes (CEI) según los metadatos de archivos en idioma ruso, la evitación de implementaciones de CLOP en países de la CEI y la observancia del Año Nuevo Ruso y el período de vacaciones de la Navidad ortodoxa.

Figura 11.
Países fundadores y miembros de la Comunidad de Estados Independientes (CEI)

Metadatos
Varios archivos de FIN11 contienen metadatos que sugieren que los operadores están usando un idioma con alfabeto cirílico.

- Algunos de los ejecutables portátiles FLAWEDAMMY y WOOLLYBEAR de FIN11 contienen archivos de recursos en ruso.
- Numerosos archivos de Word y Excel en los correos electrónicos de phishing selectivo del grupo tienen la página de código cirílico 1251. Algunos de estos documentos se crearon en diciembre de 2018 y se utilizaron en campañas de phishing posteriores en abril de 2019. Sin embargo, desde noviembre de 2019 en adelante, FIN11 cambió la página de códigos en sus documentos a Latin 1 1252.

CLOP no ataca a las víctimas de la CEI
Las muestras de ransomware CLOP comprueban las distribuciones del teclado comúnmente utilizadas en los países de la CEI y el conjunto de caracteres rusos (204) antes de la ejecución. Si tanto la distribución del teclado como los caracteres sugieren que el anfitrión está en un país de la CEI, CLOP se eliminará.

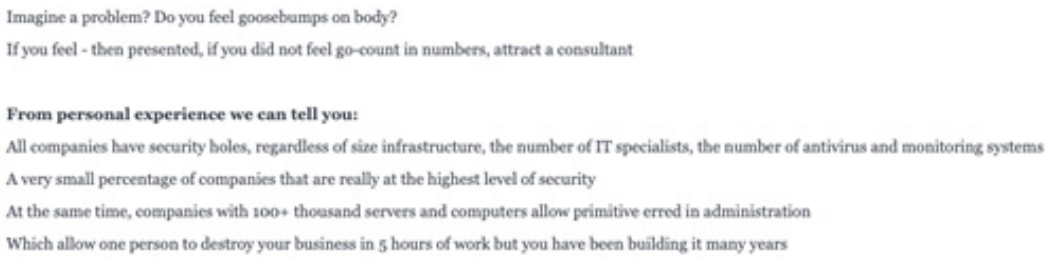
- Distribuciones del teclado evitadas: 1049, 1058, 1059, 1064, 1076, 1087, 1090, 2092, 2115
- Conjunto de caracteres de texto 204: RUSSIAN_CHARSET

Interrupción en las vacaciones rusas
La actividad de FIN11 parece disminuir drásticamente durante las vacaciones del Año Nuevo ruso y la Navidad ortodoxa, que ocurren entre el 1 y el 8 de enero de cada año.

- No hemos observado campañas de correo electrónico durante este período desde 2017.
- Solo hemos observado que uno de los ejecutables portátiles del grupo, un inyector MIXLABEL (MD5: e0ea63ace0b8efb4ebba9115f91dfef5), tiene un tiempo de compilación que cae dentro del período de vacaciones.

Hablantes de inglés no nativos
Aunque no es indicativo de un país específico donde se encuentra FIN11, el grupo también parece estar formado por hablantes no nativos de inglés. Algunos de sus engaños de correo electrónico han sido redactados de manera extraña o contienen errores tipográficos, lo que sugiere errores en las traducciones o el uso de un servicio de traducción.

- Una campaña de septiembre de 2019 dirigida a países africanos tenía uno de los temas como "necesidad de aprobación".
- Una campaña de enero de 2020 enumeró al remitente como "secretaría" y al asunto como "secretaría ha compartido un archivo con usted". Si bien secretaría se puede utilizar para referirse a una oficina administrativa del gobierno, suponemos que pretendían decir "secretaria".
- El mensaje de la página de inicio de CL0P^ _–LEAKS está escrito en un inglés deficiente con errores gramaticales que sugieren un autor no nativo en inglés (Figura 12).


Imagine a problem? Do you feel goosebumps on body?
If you feel - then presented, if you did not feel go-count in numbers, attract a consultant

From personal experience we can tell you:
All companies have security holes, regardless of size infrastructure, the number of IT specialists, the number of antivirus and monitoring systems
A very small percentage of companies that are really at the highest level of security
At the same time, companies with 100+ thousand servers and computers allow primitive erred in administration
Which allow one person to destroy your business in 5 hours of work but you have been building it many years

Figura 12.
Extracto del sitio CL0P^ _–LEAKS

Perspectiva e implicaciones

Las frecuentes campañas de phishing de alto volumen de FIN11 son probablemente un intento de lanzar una red amplia en lugar de un reflejo de las capacidades del grupo para monetizar un número creciente de víctimas de forma simultánea. Incluso si las campañas tienen una tasa de éxito relativamente baja, es poco probable que FIN11 tenga los recursos para monetizar cada intrusión antes de ser detectada. FIN11 puede elegir de forma selectiva a las víctimas para seguir explotando en función de criterios como su ubicación geográfica, sector o postura de seguridad percibida. Este costo de oportunidad perdido podría hacer que los perpetradores de FIN11 busquen asociaciones dentro de la comunidad delictiva cibernética. Por ejemplo, Mandiant ha informado recientemente sobre otros perpetradores con acceso a una gran cantidad de organizaciones a través de botnets que se están reclutando para brindar el acceso inicial a los equipos que implementan ransomware. Varias posibilidades de asociación podrían existir en el horizonte de FIN11, incluido el reclutamiento de comprobadores de penetración para implementar CLOP dentro de entornos infectados por FIN11, proporcionar CLOP para que otros lo distribuyan o brindar acceso a las víctimas de FIN11 para que otros exploten. La colaboración con otros perpetradores permitiría potencialmente a FIN11 multiplicar sus ingresos, aunque probablemente aumente la exposición del grupo en términos de seguridad operativa. Independientemente de estas oportunidades de asociación, Mandiant espera que las campañas no deseadas de FIN11 continúen en el futuro inmediato y, salvo que se tomen medidas con las fuerzas de seguridad, con una diversificación continua en las tácticas de entrega.

Apéndice A: Orígenes de TA505

TA505 definido

TA505, informado por primera vez gracias a Proofpoint en 2017, supuestamente data del 28 de julio de 2014, con el inicio de una campaña de Dridex 125. Desde entonces, este grupo motivado financieramente ha entregado una variedad de familias de códigos, incluyendo Dridex con varios ID de afiliados, Locky ransomware, TrickBot, FlawedAmmyy y otros.

FIN11 como un subconjunto de TA505

FIN11 es un subconjunto del TA505 informado públicamente basado en las motivaciones financieras de ambos grupos, las TTP superpuestas, las operaciones de phishing expansivas y el uso de malware. Si bien estas similitudes son convincentes, Mandiant no pudo verificar de forma independiente que toda la actividad TA505 informada fuera realizada por FIN11 u otro conjunto de intrusión único.

Nuestra definición de FIN11 se caracteriza principalmente por el uso del grupo de FlawedAmmyy desde 2017 y FRIENDSPEAK/MINEDOOR desde 2019. Como se ilustra en la Figura 13, el uso de FlawedAmmyy, ServHelper, FRIENDSPEAK/MINEDOOR y TTP similares sugieren superposiciones entre la actividad de TA505 en 2018 y 2019 y FIN11.

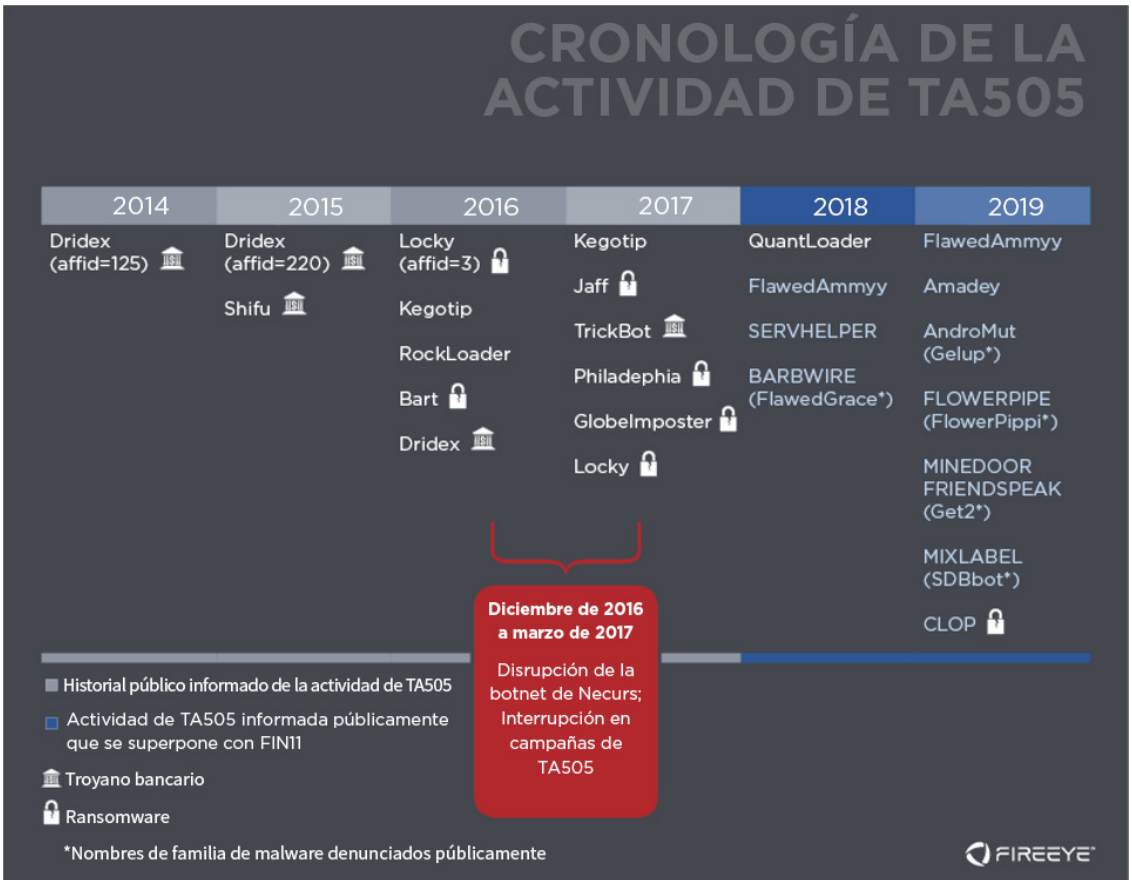


Figura 13.
Cronología de la actividad informada de TA505

Similitudes y diferencias

Hay superposiciones notables entre lo que rastreamos como FIN11 y la actividad TA505 informada públicamente. Estas superposiciones incluyen TTP, segmentación y uso de malware similares. Sin embargo, las primeras operaciones de TA505 y las familias de ransomware utilizadas no se pudieron confirmar como de parte de FIN11, y advertimos que no se crea que los dos grupos de actividad son sinónimos.

Similitudes

- A fines de 2018, se informó que TA505 estaba dirigido a organizaciones minoristas, de comestibles y de restaurantes con FlawedAmmyy. Durante este tiempo, también observamos a FIN11 utilizando FlawedAmmyy contra objetivos similares, junto con la herramienta de raspado de memoria de punto de venta BLUESTEAL.
- Un sello distintivo de las caracterizaciones de TA505 y FIN11 es el alto volumen de campañas de phishing para cada grupo. Se sabe que ambos grupos envían miles de correos electrónicos de phishing contra una variedad de industrias en un solo día.
- Algunos de los TTP de phishing de TA505 se superponen con nuestras observaciones de FIN11. Ambos grupos utilizan títulos de engaños de phishing relacionados con las finanzas similares, pero genéricos, como: “factura”, “solicitud”, “recibo” y más. Si bien no es exclusivo de ninguno de los grupos, ambos han intentado suplantar a organizaciones e individuos en los nombres para mostrar del correo electrónico.
- Además, hay superposiciones de metadatos de documentos entre los grupos. Algunos de los archivos adjuntos de Word enumeran la página de códigos como cirílico 1251 y “1” fue el último autor guardado.
- De manera similar, muchos de los indicadores atribuidos a FIN11 se atribuyen públicamente a TA505. Esto es especialmente cierto en las familias de malware FlawedAmmyy, FRIENDSPEAK y MINEDOOR.

Diferencias

- Una diferencia clave entre los grupos es el uso temprano de varias familias de ransomware. Aunque creemos que FIN11 implementa CLOP, no pudimos confirmar el uso de GlobeImposter, Filadelfia y otras familias de ransomware supuestamente utilizadas por TA505 durante operaciones anteriores.
- El historial de TA505 indica que el grupo ha distribuido los ID 125, 220, 223, 7200 e ID 7500 de la botnet Dridex a lo largo de los años. En particular, nuestro análisis en 2017 complementado con informes de código abierto, sugiere que estos ID de botnet no están asociados con un único grupo de afiliados sospechosos. Como no verificamos de forma independiente las campañas del historial de Dridex de TA505, y evaluamos que Dridex opera bajo un modelo de afiliados, no incluimos dicha actividad en nuestra definición de FIN11.

Apéndice B: Superposiciones notables con otros grupos de amenazas

TEMP.TruthTeller

Mandiant ha identificado varias superposiciones entre FIN11 y la actividad que atribuimos o sospechamos que fue realizada por TEMP.TruthTeller (también conocido como Silence Group). Estas superposiciones tienen un alcance limitado; la mayoría de las similitudes se agrupan en torno a variantes de TRUEBOT (también conocidas como Silence. Downloader) y SLOWROLL (también conocidas como Silence.Mainmodule). Según la evidencia disponible en el momento del análisis, no está claro si estas superposiciones son el resultado de una afiliación comercial, un proveedor compartido o una conexión más cercana, como un miembro común o varios.

Superposición de certificados

Se utilizaron al menos dos certificados de firma de código para firmar FlawedAmmyy y una variante de TRUEBOT (Tabla 5). El emisor y el código de país del asunto son consistentes con los certificados de firma de código que sospechamos que FIN11 adquirió de un servicio de certificados: se cree que el servicio haya emitido el mismo certificado a varios clientes.

Tabla 5. Certificados utilizados para firmar TRUEBOT y FlawedAmmyy

Nombre común (país)	MD5	Emisor	Fecha de inicio de validez	Fechas de compilación de TRUEBOT	Fechas de compilación de FlawedAmmyy
DIGI MICROSERVICE LIMITED (GB)	6fcefd24c81c340f568faa492d592c77	Comodo CA Limited	13 de junio de 2018	Agosto de 2018	Junio a julio de 2018
ITGS Consultancy Ltd (GB)	2026975b1bbccc903e3ff56116fcea33	Comodo CA Limited	10 de octubre de 2018	Finales de diciembre de 2018	Principios de diciembre de 2018

Superposición de nombres de archivo

FIN11 ha utilizado el nombre de archivo wsus.exe para una variedad de malware, incluidos BARBWIRE, FlawedAmmyy y TINYMET. El nombre de archivo, que se hace pasar por Windows Server Update Services, no es particularmente único; sin embargo, el malware que usa ese nombre solo se ha atribuido a FIN11, un clúster FIN11 sospechoso y dos clústeres TEMP.TruthTeller sospechosos. Las muestras sospechosas de TEMP.TruthTeller que usaban el nombre wsus.exe eran TRUEBOT.

Superposiciones de inyectores/cargadores

Los informes de código abierto de Group-IB han sugerido que el cargador de FlawedAmmyy y TRUEBOT fueron desarrollados por la misma persona. Los diseños y capacidades generales de los cargadores son similares; sin embargo, actualmente no hay evidencia suficiente para apoyar la afirmación de que un desarrollador escribió ambas herramientas.

- La implementación del algoritmo de cifrado RC4 no es completamente idéntica; el cargador FlawedAmmyy usa una variable global para la clave RC4, mientras que TRUEBOT pasa la clave como un argumento de función.
- El cargador de FlawedAmmyy construye un comando de autoeliminación a través de tres llamadas a la API, mientras que TRUEBOT usa una cadena de formato para crear su comando de autoeliminación.
- Ambos cargadores verifican que el tamaño del archivo descargado exceda los 4000 bytes, pero toman diferentes pasos cuando falla la verificación. El cargador de FlawedAmmyy se autoelimina y sale inmediatamente, mientras que TRUEBOT solo se autoelimina y sale si la respuesta del servidor contiene KILL. De lo contrario, esperará dos minutos antes de intentar volver a conectarse al servidor C&C.

Mandiant Threat Intelligence mencionó anteriormente que sospechamos que el inyector SPOONBEARD no es exclusivo de FIN11 porque también ha eliminado malware aparentemente no relacionado, como SLOWROLL y JESTBOT.

- Sospechamos que una instancia de SLOWROLL eliminada por SPOONBEAD e identificada en 2019 se distribuyó como parte de una campaña TEMP. TruthTeller basada en el uso establecido del malware por parte del grupo: el conocimiento limitado de las primeras etapas de esta campaña nos impide atribuir la actividad al grupo de amenazas en este momento.
- Una campaña de phishing de febrero de 2020 entregó muestras de SPOONBEARD que arrojaron JESTBOT, un cargador que comparte algunas similitudes en funcionalidad y estructura de código con el malware TRUEBOT y SLOWROLL.
  - Aunque TEMP.TruthTeller ha utilizado TRUEBOT y SLOWROLL, esta campaña utilizó TTP de entrega que son inconsistentes con las campañas de TEMP. TruthTeller y FIN11.
  - Además, algunos de los correos electrónicos de esta campaña no utilizaron el inyector SPOONBEARD, sino que utilizaron documentos GREENKIT para recuperar la misma carga útil de JESTBOT contenida en una imagen PNG esteganográfica.

Superposición de infraestructuras

El dominio trictac.com alojaba tanto una carga útil SLOWROLL como un documento malicioso utilizado en una supuesta campaña de phishing selectivo de FIN11 que entregó malware Amadey.

- El 18 de junio de 2019, la presunta campaña de phishing de FIN11 entregó un archivo adjunto HTML que usaba una metaactualización para descargar un documento de Word malicioso desde una URL de trictac.com. El documento de Word contenía una macro que, si se habilitaba, descargaría el cargador de Amadey desde una URL por separado.
- Una URL separada de trictac.com alojaba una carga útil SLOWROLL con una fecha de compilación del 28 de junio de 2019. La última fecha de modificación del sitio web sugiere que la carga útil se cargó el 19 de julio de 2019 o antes.

Ataques superpuestos

Durante algunas intrusiones que Mandiant Threat Intelligence atribuye a FIN11, hemos identificado actividad contemporánea asociada con otros grupos de amenazas, como FIN6 y FIN7. Evaluamos previamente que FIN11 entregó el acceso a estos grupos, posiblemente proporcionando su presencia como servicio. Si bien todavía es creíble que FIN11 tenga relaciones con otros grupos de amenazas, identificamos inconsistencias en el tiempo y la actividad posterior al ataque, lo que sugiere que las superposiciones también podrían ser una coincidencia.

- Si FIN11 estuviera proporcionando acceso a otro grupo, hubiéramos esperado que FIN11 fuera el primer grupo observado en el entorno. Si bien los datos de respuesta ante incidentes a menudo tienen brechas en la visibilidad, en la mayoría de los ataques, la evidencia disponible colocó al otro grupo de amenazas en el entorno antes que a FIN11. Es poco probable que la falta de visibilidad pueda explicar todos los casos en los que FIN11 no fue el primer grupo de amenazas observado.
- Además, no esperaríamos que FIN11 lleve a cabo una actividad de monetización adicional después de proporcionar acceso al otro grupo. En cambio, esperaríamos ver al segundo grupo de amenazas monetizando el acceso.
  - En un caso, FIN7 y FIN11 implementaron diferentes raspadores de tarjetas de crédito al mismo tiempo.
  - En otras interacciones, no observamos ninguna actividad de monetización adicional.

Perpetradores norcoreanos

El informe de código abierto ha sugerido que los perpetradores que implementan software malicioso SWIFT en nombre de Corea del Norte pueden haber obtenido acceso a las víctimas del sector financiero de FIN11. Mandiant ha identificado casos en los que tanto FIN11 como perpetradores afiliados a Corea del Norte han atacado a la misma víctima; sin embargo, las intrusiones no se superpusieron y no hubo evidencia que sugiera que hubo una transferencia entre estos dos grupos. Se sabe que ambos grupos apuntan a organizaciones financieras, lo que hace posible que los ataques superpuestos fueran una coincidencia.

Apéndice C: Ciclo de vida de un ataque

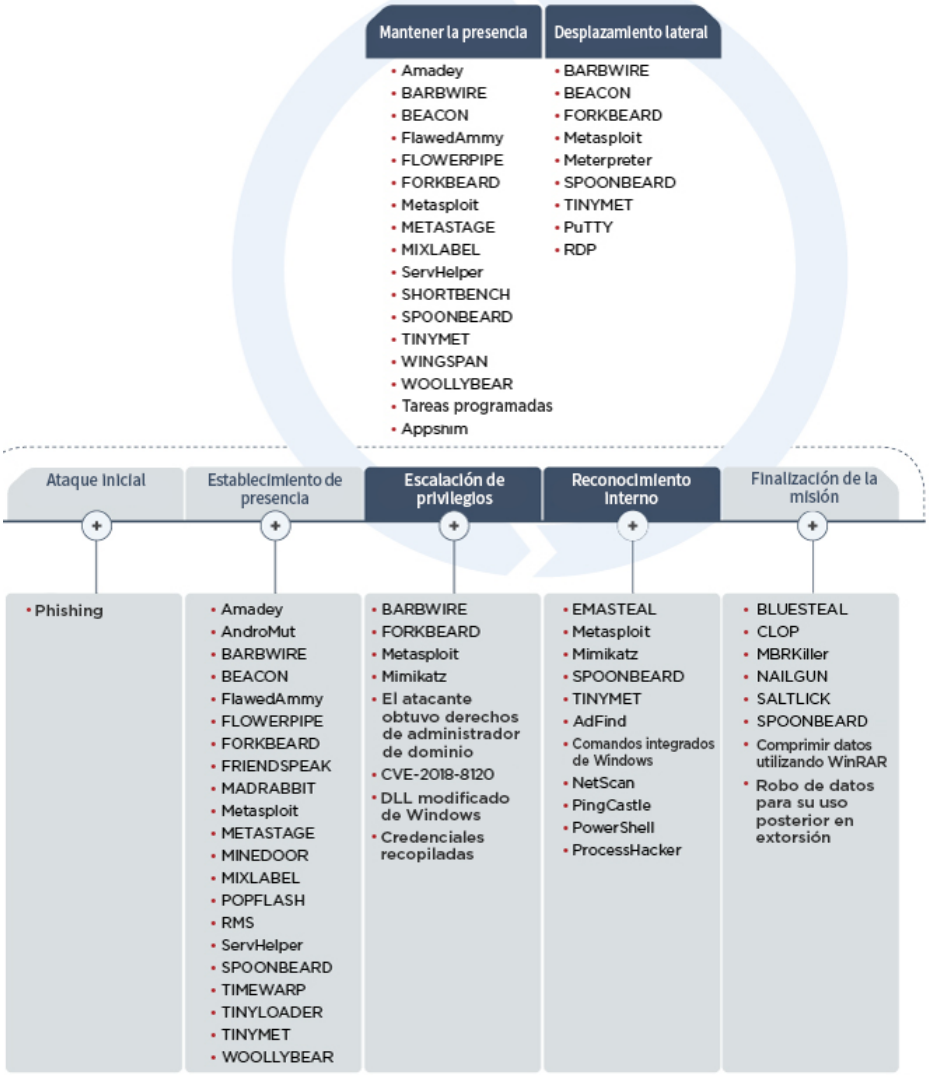


Figura 14.
Ciclo de vida de un ataque de FIN11

Ataque inicial

FIN11 se basa en el uso de simples correos electrónicos de phishing para atacar inicialmente a sus víctimas. El grupo ha realizado pequeños cambios en el mecanismo de entrega inicial utilizado para entregar sus cargas útiles finales a lo largo de sus operaciones. Desde al menos el otoño de 2018, FIN11 generalmente distribuye correos electrónicos de phishing simples que contienen URL o archivos adjuntos integrados para, en última instancia, entregar archivos maliciosos de Office. Los detalles de los cambios observados a lo largo del tiempo se pueden encontrar en la sección Evolución de las TTP en las campañas.

Establecimiento de presencia

Desde 2016, el grupo ha utilizado una variedad de malware y herramientas, tanto públicas como exclusivas del grupo, para establecer una presencia en el entorno de la víctima. El malware y las herramientas disponibles públicamente incluyen Amadey, BEACON, TIMEWARP, METASPLOIT, METASTAGE, RMS y TINYMET. El malware aparentemente no público ha incluido AndroMut, BARBWIRE, FlawedAmmyy, FLOWERPIPE, FORKBEARD, FRIENDSPEAK, MADRABBIT, MINEDOOR, MIXLABEL, ServHelper, SPOONBEARD, WOOLLYBEAR, POPFLASH y TINYLOADER. En muchos casos, estas cargas útiles se han firmado mediante certificados de firma de código válidos. Además, se utilizaron empaquetadores como MINEDOOR, FORKBEARD y SPOONBEARD para empaquetar algunas de las familias utilizadas para esta fase, pero no realizan individualmente funciones de establecimiento de base.

Escalación de privilegios

FIN11 aprovechó un binario que explota CVE-2018-8120 para escalar privilegios dentro de los entornos de las víctimas. El archivo, llamado wsus.exe, es un binario empaquetado que parece estar basado en un módulo Metasploit disponible públicamente o en el POC subyacente disponible públicamente. El exploit afecta a Windows 2008, Windows 7 y Windows Server 2008 R2. FIN11 también ha aprovechado BARBWIRE, MIMIKATZ y METASPLOIT para la escalación de privilegios.

FIN11 ha utilizado la técnica documentada públicamente de aplicar parches a versiones legítimas de 32 bits y 64 bits de WinSCard.dll, WinSCard64.dll y SCardSvr.dll para permitir la manipulación de tokens en sesiones de Protocolo de Escritorio Remoto (Remote Desktop Protocol, RDP). Las versiones modificadas de WinSCard.dll y WinSCard64.dll permiten que las sesiones de RDP accedan y utilicen el token seguro, al que se supone que se accede localmente. Si bien esta técnica podría haberse utilizado para la escalación de privilegios, no tenemos pruebas de que FIN11 la haya utilizado con éxito para este propósito.

Movimiento lateral

FIN11 utilizó las credenciales recopiladas por Mimikatz para iniciar sesión en varios sistemas remotos dentro de la red de la organización. Mimikatz contiene la funcionalidad para recolectar credenciales y permitir la suplantación de otro usuario. FIN11 utilizó ocasionalmente sesiones de RDP para el desplazamiento lateral. También ha utilizado PowerShell y PsExec para iniciar servicios en otros sistemas. También ha aprovechado BARBWIRE, BEACON, METASPLOIT, METERPRETER y TINYMET para el desplazamiento lateral.

Mantener la presencia

FIN11 ha aprovechado las tareas y los servicios programados en varios sistemas para garantizar la persistencia de los shells inversos FlawedAmmyy, BARBWIRE y METERPRETER después de reiniciar el sistema. Se instalaron varias puertas traseras, como BEACON, FLOWERPIPE, METASPLOIT, METASTAGE, MIXLABEL, SERVHELPEER, TINYMET y WOOLLYBEAR, en cada sistema, potencialmente para permitir el acceso redundante. FORKBEARD se utilizó para empaquetar BARBWIRE en esta fase y no contribuye individualmente a mantener la presencia.

Desde al menos septiembre de 2019 hasta febrero de 2020, FIN11 abusó de las shims de compatibilidad de aplicaciones para su persistencia e inyección. Se crearon shims de compatibilidad de aplicaciones para permitir la compatibilidad con versiones anteriores; sin embargo, también se pueden utilizar de forma maliciosa.

- FIN11 creó una base de datos de shims maliciosas en C:\Windows\AppPatch\Custom\Custom64\ y en C:\Windows\Temp\ que luego se registró en el proceso actualizado services.exe.
- La instalación de la base de datos de shims maliciosa permite al atacante lograr la persistencia a través de un services.exe parcheado que lee el archivo malicioso de la base de datos de shims y carga en la memoria la puerta trasera MIXLABEL que FIN11 colocó en un registro.

FIN11 ha realizado ocasionalmente varias campañas de phishing para mantener su presencia en el entorno.

Reconocimiento interno

FIN11 ha aprovechado las herramientas de línea de comandos de Windows (ping.exe, find.exe, ipconfig, hostname, systeminfo) y herramientas disponibles públicamente (PingCastle, METASPLOIT, MIMIKATZ, adfind, Process Hacker, SoftPerfect Network Scanner, TINYMET) para el reconocimiento interno.

Finalización de la misión

FIN11 ha intentado monetizar el acceso recopilando datos de tarjetas de pago de la Pista 1 y 2 con BLUESTEAL, implementando ransomware tradicional (CLOP) y exfiltrando y publicando datos en un esquema de extorsión híbrido.

FIN11 ha utilizado la herramienta de raspado de memoria de POS BLUESTEAL para intentar robar los datos de la tarjeta de pago de la Pista 1 y 2.

- FIN11 ha utilizado SALTLICK para deshabilitar Windows Defender en los sistemas infectados modificando el registro HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real- Time Protection\DisableRealtimeMonitoring. FIN11 luego usó NAILGUN o un objeto de política de grupo (GPO) malicioso para implementar el ransomware CLOP.
- En algunos casos, FIN11 usó MBRKILLER en los hosts, haciéndolos imposibles de arrancar. MBRKILLER está diseñado para interrumpir el sistema y sobrescribir el registro de arranque maestro y las duplicaciones de cada disco y sus particiones.
- En marzo de 2020, FIN11 comenzó a exfiltrar datos de víctimas para su uso posterior en extorsión antes de implementar CLOP. El grupo utilizó los datos robados como un beneficio adicional para alentar a las víctimas a pagar el rescate, amenazando con revelar la información confidencial de la víctima. FIN11 utilizó la herramienta WinRAR disponible públicamente para comprimir los datos específicos en una serie de archivos, los cargó en el sitio MegaSync y luego implementó el ransomware CLOP. El grupo envió correos electrónicos a las víctimas con líneas de asunto “CLOP UNLOCK FILES” para notificarles de la extorsión y, posteriormente, publicó enlaces a los datos en su sitio para nombrar y humillar, CL0P^_–LEAKS.
- Para obtener más información, consulte la sección Actividad posterior a la explotación.

Apéndice D: Asignaciones de MITRE ATT&CK

Acceso inicial

- t1192 Enlace de phishing selectivo
- t1193 Adjunto de phishing selectivo

Ejecución

- t1047 Instrumental de Administración de Windows
- t1086 PowerShell
- t1053 Tareas programadas
- t1064 Scripting
- t1059 Interfaz de línea de comandos
- t1035 Ejecución del servicio
- t1204 Ejecución de usuario

Persistencia

- t1133 Servicios remotos externos
- t1053 Tareas programadas
- t1060 Claves de ejecución del registro/carpeta de inicio
- t1015 Características de accesibilidad
- t1138 Suplementación de aplicación
- t1004 DLL de Winlogon Helper
- t1050 Servicio nuevo
- t1078 Cuentas válidas
- t1108 Acceso redundante

Escalación de privilegios

- t1138 Suplementación de aplicación
- t1055 Inyección de proceso
- t1015 Características de accesibilidad
- t1050 Servicio nuevo
- t1053 Tareas programadas
- t1078 Cuentas válidas
- t1086 Explotación para la escalación de privilegios

Evasión de defensa

- t1055 Inyección de proceso
- t1045 Empaquetado de software
- t1107 Eliminación de archivos
- t1064 Scripting
- t1116 Firma de código
- t1112 Modificar el registro
- t1070 Eliminación de indicadores en el host
- t1027 Archivos o información confusa
- t1202 Ejecución indirecta de comandos
- t1090 Proxy de conexión
- t1078 Cuentas válidas
- t1140 Desofuscar/decodificar archivos o información
- t1108 Acceso redundante

Acceso a credenciales

- t1003 Volcado de credenciales

Descubrimiento

- t1082 Descubrimiento de información del sistema
- t1057 Descubrimiento de procesos
- t1063 Descubrimiento del software de seguridad
- t1082 Descubrimiento de información del sistema
- t1057 Descubrimiento de procesos
- t1063 Descubrimiento del software de seguridad

Desplazamiento lateral

- t1021 Servicios remotos
- t1076 Protocolo de escritorio remoto
- t1105 Copia remota de archivos

Recopilación

- t1125 Captura en video
- t1113 Captura de pantalla
- t1119 Recopilación automatizada
- t1005 Datos del sistema local

Comando y control

- t1090 Proxy de conexión
- t1071 Protocolo estándar de la capa de aplicaciones
- t1094 Comando personalizado y protocolo de control
- t1105 Copia remota de archivos
- t1032 Protocolo criptográfico estándar
- t1043 Puerto utilizado comúnmente
- t1065 Puerto no utilizado comúnmente
- t1219 Herramientas remotas de acceso

Exfiltración

- t1002 Datos comprimidos
- t1022 Datos cifrados
- t1041 Exfiltración sobre el canal de mando y control
- t1048 Exfiltración sobre protocolo alternativo

Impacto

- t1486 Datos cifrados para el impacto
- t1529 Apagado/reinicio del sistema
- t1485 Destrucción de datos
- t1488 Eliminación de contenido del disco
- t1489 Detención del servicio

Apéndice E: familias de malware

Tabla 6. Familias de malware

Malware	Descripción	Detectado como
AMADEY	Amadey es un descargador/cargador compatible con MinGW que tiene la capacidad de descargar y ejecutar ejecutables y DLL. Amadey también emplea mecanismos para evitar la detección cuando abre ejecutables descargados de Internet, puede mantener la persistencia en el host infectado y envía un beacon cada minuto para verificar si hay nuevos archivos para descargar.	FE_Downloader_Win32_AMADEY_1 Downloader.Win.AMADEY Trojan.Amadey Trojan.Win.AMADEY FE_Trojan_Win32_AMADEY_1 Downloader.Amadey
ANDROMUT	AndroMut es un cargador que contiene varias comprobaciones antianálisis y usa objetos JSON encriptados para comunicarse con un servidor C&C codificado. Las cargas útiles contenidas dentro de un objeto de respuesta JSON recibido del servidor C&C se guardan en el directorio %TEMP% y se ejecutan.	Downloader.AndroMut Trojan.AndroMut Trojan.Win.Andromut FE_Trojan_Win32_AndroMut_1
BARBWIRE	BARBWIRE es una puerta trasera que se conecta a un servidor C&C mediante un protocolo binario personalizado. El C&C se obtiene de un archivo de configuración. En caso de que no exista ningún archivo de configuración, el malware utilizará un respaldo integrado. La puerta trasera admite una variedad de capacidades, incluida la actualización del malware, el robo de contraseñas, la ejecución de scripts y la eliminación automática. El malware también tiene la capacidad de hacer que el host de la víctima no pueda arrancar sobrescribiendo el comienzo del disco duro físico que contiene el sistema operativo con datos aleatorios.	Backdoor.Win.BARBWIRE FE_Trojan_Win_BARBWIRE_1 FE_Trojan_Win_BARBWIRE_2 FE_Trojan_Win32_BARBWIRE_1 FE_Backdoor_Win32_BARBWIRE_1 FE_Backdoor_Win32_BARBWIRE_2

Tabla 6. Familias de malware (continuación)

Malware	Descripción	Detectado como
BEACON	El malware BEACON es una puerta trasera que está disponible comercialmente como parte de la plataforma de software Cobalt Strike, comúnmente utilizada para entornos de red de prueba de penetración. El malware admite varias capacidades, como inyectar y ejecutar código arbitrario, cargar y descargar archivos y ejecutar comandos de shell.	Backdoor.BEACON.Staging Backdoor.BEACON COBALT STRIKE (PUERTA TRASERA) BEACON A (FAMILIA) MaliciousSSLCert.CobaltStrike Trojan.CobaltStrike FE_Backdoor_Win_BEACON_1 FE_Trojan_PS1_BEACON_1 FE_Loader_JS_BEACON_1 FE_Loader_VBS_BEACON_ FE_Loader_PS1_ BEACON_1 Backdoor.Win.BEACON Backdoor.BEACON.Netbios.URI.FB Backdoor.BEACON.Netbios.Cookie.FB Backdoor.BEACON.B64.URI.FB Backdoor.BEACON.B64.FB Backdoor.BEACON.B64.POST.Cookie.FB Backdoor.BEACON.B64u.URI.FB Backdoor.BEACON.MetasploitStager.FB Backdoor.BEACON.Netbios.POST.Payload.FB Backdoor.BEACON.B64.GET.Cookie.FB Backdoor.BEACON.B64u.Cookie.FB Backdoor.BEACON.Netbios.Header.FB Backdoor.BEACON.Default.URI.FB Backdoor.BEACON.B64u2.URI.FB Suspicious.Backdoor.BEACON Backdoor.BEACON.DNS FE_Launcher_Win_BEACO Backdoor.BEACON.CERT Backdoor.BEACON.FEC2 FE_Backdoor_Win32_BEACON_2 Backdoor.BEACON.SMB FE_Backdoor_Beacon, FE_Backdoor_Beacon2 Backdoor.Methodology.CobaltStrike. BeaconDLL.Encoded Backdoor.Beacon.Download FE_Backdoor_Win_BEACON_3 FE_Backdoor_Win32_BEACON_1 FE_Backdoor_Win_BEACON_2 FE_Backdoor_Win32_BEACON_3 FE_APT_Loader_Win_BEACON_1 FE_APT_Loader_Win_BEACON_2 FE_APT_Loader_Win32_BEACON_4 FE_APT_Loader_Win32_BEACON_5

Tabla 6. Familias de malware (continuación)

Malware	Descripción	Detectado como
BLUESTEAL	BLUESTEAL es una utilidad de extracción de memoria de POS que se utiliza para buscar datos de las pistas 1 y 2 de tarjetas de pago en la memoria de proceso. En particular, BLUESTEAL verifica que el primer dígito del número de la tarjeta sea: 3, 4, 5 o 6. Además, BLUESTEAL comprueba si el número de la tarjeta tiene entre 13 y 16 dígitos y utiliza el algoritmo LUHN para verificar el número de la tarjeta de crédito. El malware almacena los resultados en archivos que utilizan varias extensiones preestablecidas de archivo en un recurso compartido SMB remoto.	APTFIN.POS.Win.BLUESTEAL FE_APTFIN_POS_PS1_BLUESTEAL_1 FE_APTFIN_POS_Win_BLUESTEAL_2 FE_APTFIN_POS_Win32_BLUESTEAL_1
CLOP	CLOP es un ransomware que cifra tipos de archivos seleccionados en un sistema infectado. Luego del cifrado, los nombres de archivo se añaden con una extensión ".Clop", ".Ciop" o ".Cl0p". La instrucción del pago se escribe en un archivo de texto que se coloca en todas las carpetas enumeradas como "CLOPREADME.TXT" o "CIOPREADME.TXT".	FE_Ransomware_Win_CLOP_1 FE_Ransomware_Win32_CLOP_1
COBALT	COBALT es un cargador que intenta descargar y ejecutar una DLL codificada desde su servidor C&C.	FE_APT_COBALT_Cert_A APT.COBALT.Cert.A Trojan.APT.COBALT Trojan.Cobalt.DNS FE_APT_COBALT_Cert FE_APT_COBALT_Cert_B FE_APT_COBALT_Cert_C FE_APT_COBALT_Cert_D FE_APT_COBALT_Cert_F FE_APT_COBALT_Cert_G FE_APT_COBALT_Cert_H FE_APT_COBALT_Cert_I Trojan.Cobalt Malicious.SSL.Cobalt
EMASTEAL	EMASTEAL es un malware que intenta robar las credenciales de correo electrónico del sistema infectado. También recopila direcciones de correo electrónico almacenadas en determinados formatos de archivo como .txt, .xml, .class, .py, entre otros. Los datos robados luego se envían en un texto sin formato con formato JSON a su servidor C&C a través de HTTP POST.	InfoStealer.Win.EMASTEAL FE_InfoStealer_Win32_EMASTEAL_1
EMPIRE	Empire es un marco posterior a la explotación de PowerShell disponible públicamente que permite a los usuarios ejecutar agentes de PowerShell sin el uso de powershell. exe. PowerShell Empire también permite a los perpetradores ejecutar varios tipos de módulos posteriores a la explotación y realizar comunicaciones adaptables mientras evitan la detección.	EMPIRE RAT (PUERTA TRASERA) Backdoor.EMPIRE Trojan.Empire Trojan.APT.EMPIRE Downloader.EMPIRE FE_Backdoor_EMPIRE FE_Trojan_ObfuscatedEmpire_Downloader FE_Backdoor_EMPIRE_B FE_Downloader_PS1_EMPIRE_1 FE_Downloader_PS1_EMPIRE_2 Backdoor.Methodology.Empire.Downloader MaliciousSSLCert.PowerShellEmpire

Tabla 6. Familias de malware (continuación)

Malware	Descripción	Detectado como
FLAWEDAMMYY	FlawedAmmyy es una modificación de la herramienta de acceso remoto AmmyyAdmin que implementa comandos adicionales, incluida la capacidad de ejecutar un shell de comando canalizado, recopilar información del sistema y del usuario, incluida la detección de la presencia de una tarjeta inteligente (que podría indicar un sistema POS), iniciar un módulo Mimikatz para habilitar el robo de credenciales, actualizarse y reiniciar el sistema host.	RAT.FlawedAmmyy Trojan.FlawedAmmyy Trojan.FlawedAmmyRAT Downloader.FlawedAmmyRAT APTFIN.Backdoor.Win.FLAWEDAMMYY FE_APTFIN_Backdoor_Win_ FLAWEDAMMYY_1 FE_APTFIN_Backdoor_Win32_ FLAWEDAMMYY_1
FLOWERPIPE	FLOWERPIPE es una puerta trasera que se comunica con un servidor C&C codificado. Sus capacidades incluyen la descarga y ejecución de archivos, la generación de un shell inverso y la eliminación automática. También conocido como FlowerPippi.	Trojan.Win.FLOWERPIPE FE_Trojan_Win32_FLOWERPIPE_1
FORKBEARD	FORKBEARD es un inyector en memoria que primero decodifica su código de shell y luego decodifica y pone en marcha su carga útil en la memoria reemplazando el binario original en el proceso. Finalmente, el shellcode invoca el punto de entrada de la carga útil. Hemos observado que FORKBEARD se usa como inyector para FlawedAmmyy.	FE_Loader_Win32_FORKBEARD_1 FE_Loader_Win32_FORKBEARD_2 FE_Loader_Win32_FORKBEARD_3
FRIENDSPEAK	FRIENDSPEAK es un cargador HTTP que normalmente se encuentra dentro de un cargador MINEDOOR. El cargador recupera archivos ejecutables de un servidor C&C remoto, los guarda en el directorio TEMP y los ejecuta.	Downloader.Win.FRIENDSPEAK
MADRABBIT	MADRABBIT es un cargador que descifra y lanza el código shell que recupera de un servidor C&C codificado. Este malware también contiene una serie de comprobaciones antianálisis que intentan identificar si se está ejecutando en un entorno virtualizado o en una caja de arena automatizada antes de descargar su carga útil alojada de forma remota.	FE_APT_Loader_Win_MADRABBIT_1 FE_APT_Loader_Win_MADRABBIT_2 FE_APT_Loader_Win64_MADRABBIT_1 APT.Downloader.Win.MADRABBIT
MBRKILLER	MBRKILLER es una herramienta de interrupción ejecutable compilada por scripts de NSIS que intenta sobrescribir sectores en MBR, VBR y sus espejos para cada disco y sus particiones presentes en el sistema.	FEC_Wiper_NSIS_MBRKILLER_1
METASTAGE	METASTAGE es un pequeño binario de shellcode del kit de herramientas Metasploit conocido como “reverse_https stager”. METASTAGE generalmente se descomprime mediante un ejecutable principal, que se empaqueta en varias etapas. La capa exterior del archivo principal contiene cadenas y algo de código para que parezca una aplicación de prueba inocua. El archivo principal descomprime el código de shell METASTAGE y lo ejecuta, lo que descarga una carga útil secundaria que se carga en la memoria y se ejecuta.	Trojan.METASTAGE
METASPLOIT	Metasploit es un marco de pruebas de penetración popular que incluye módulos disponibles públicamente como METASTAGE y Meterpreter.	*Consulte los módulos Metasploit individuales.*

Tabla 6. Familias de malware (continuación)

Malware	Descripción	Detectado como
METERPRETER	METERPRETER es una carga útil multifacética disponible públicamente que opera mediante inyección de dll y está incorporada en Metasploit Framework.	FE_Hacktool_Meterpreter_Ultimet FE_Trojan_Win_Meterpreter_1 Trojan.Meterpreter Backdoor.APT.Meterpreterd Trojan.Meterpreter.Mapadubu Backdoor.Meterpreter Methodology.Backdoor.Meterpreter Meterpreter Traffic Trojan.Unk.Meterpreter Malicious.SSL.Meterpreter Backdoor.Meterpreter.SSL
MIMIKATZ	Mimikatz es una herramienta de auditoría de seguridad de Windows desarrollada por el investigador de seguridad Benjamin Delpy. Mimikatz se puede utilizar para robar códigos hash de contraseñas y volcar contraseñas de texto sin formato extraídas de la memoria. Mimikatz puede volcar credenciales de LSASS, así como contraseñas de Kerberos. Los sistemas Linux y Unix almacenan las credenciales de Kerberos en un archivo de caché, que Mimikatz también puede extraer.	HackTool.Win.Mimikatz FE_HackTool_Win_MIMIKATZ_1 FE_HackTool_Win_MIMIKATZ_2 FE_HackTool_Win_MIMIKATZ_3 FE_HackTool_Win_MIMIKATZ_4 FE_HackTool_PW_Mimikatz FE_HackTool_PS1_InvokeMimikatz FE_Trojan_PS1_InvokeMimikatz_1
MINEDOOR	MINEDOOR es un cargador empaquetado, visto anteriormente con un cargador HTTP integrado, FRIENDSPEAK.	FE_Loader_Win32_MINEDOOR_1 FE_Loader_Win64_MINEDOOR_1 FE_Loader_Win64_MINEDOOR_2
MIXLABEL	MIXLABEL es una puerta trasera simple que se comunica mediante un protocolo binario personalizado y puede crear un shell inverso, cargar y descargar archivos y enumerar y eliminar archivos.	APTFIN.Backdoor.Win.MIXLABEL FE_APTFIN_Backdoor_Win64_MIXLABEL_1 FE_APTFIN_Dropper_Win32_MIXLABEL_1 FE_APTFIN_Dropper_Win32_MIXLABEL_2 FE_APTFIN_Dropper_Win32_MIXLABEL_3 FE_APTFIN_Dropper_Win64_MIXLABEL_1
NAILGUN	NAILGUN es una herramienta de instalación/implementación que toma una carga útil dada en la línea de comando junto con una lista de hosts y otras configuraciones más para implementar malware.	APTFIN.HackTool.Win.NAILGUN

Tabla 6. Familias de malware (continuación)

Malware	Descripción	Detectado como
POPFLASH	POPFLASH es un cargador compatible con Wow64 que carga un complemento DLL integrado para manejar todas las comunicaciones de red. Las comunicaciones C&C se envían y reciben a una dirección IP de C&C codificada de forma rígida a través del DNS en el puerto UDP 53 con el tipo de consulta 19 (protocolo X25) utilizando un protocolo binario personalizado. POPFLASH parece capaz de descargar y ejecutar cargas útiles/complementos adicionales y actualizar su configuración de C&C.	APT.Downloader.Win.POPFLASH FE_APT_Downloader_Win32_POPFLASH_1
RMS	RMS es un paquete de software de administración remota disponible públicamente conocido como Sistema de manipulación remota (RMS).	Trojan.Bizzana Trojan.RemoteManipulator
SALTLICK	SALTLICK es una utilidad que deshabilita Windows Defender en un host modificando las claves de registro.	FE_HackTool_Win32_SALTLICK_1 HackTool.Win.SALTLICK.MVX
SERVHELPER	ServHelper tiene una variante de tunelizador y de cargador. La variante de tunelizador intenta agregar una nueva cuenta de usuario y reconfigurar el sistema afectado para permitir el acceso al escritorio remoto a través de esa cuenta. El tunelizador utiliza "OpenSSH para Windows" para configurar y administrar túneles SSH a través de los cuales se reenvía el tráfico del Protocolo de escritorio remoto. También está disponible la ejecución arbitraria de comandos remotos a través del shell de comandos. En contraste, la variante del cargador de ServHelper admite la descarga de cargas útiles, pero no contiene las capacidades de escritorio remoto y tunelización de la variante del tunelizador. La comunicación del cargador con su servidor de comando y control se realiza a través del puerto TCP 443 usando SSL.	Backdoor.Win.SERVHELPER Trojan.ServHelper FE_Backdoor_Win32_SERVHELPER_1 FE_Backdoor_Win32_SERVHELPER_2 Downloader.ServHelper MaliciousSSL.ServHelper Malicious.SSL.ServHelper
SHORTBENCH	SHORTBENCH es un cargador de shellcode generado por Metasploit que usa cadenas integradas para intentar disfrazarse como la aplicación válida ApacheBench. El malware comienza ejecutando un búfer de shellcode integrado que se conecta a un servidor C&C para descargar y ejecutar shellcode adicional.	FE_SHORTBENCH_Packer

Tabla 6. Familias de malware (continuación)

Malware	Descripción	Detectado como
SPOONBEARD	SPOONBEARD es un empaquetador/inyector que se utiliza para eliminar numerosas familias de malware, incluidos Amadey, CLOP, EMASTEAL, SALTLICK, FlawedAmmyy, TINYMET y AndroMut.	FE_Dropper_Win32_SPOONBEARD_2 FE_Dropper_Win32_SPOONBEARD_3
TIMEWARP	TIMEWARP es una herramienta de inyección de DLL. Puede cargar una DLL en su propio proceso o en otro proceso.	FE_APTFIN_Loader_Win64_TIMEWARP_1
TINYLOADER	Se ha observado que TINYLOADER se utiliza como cargador de malware de POS, incluido AbaddonPOS. Puede tener efectos más acumulativos en un entorno de base financiera.	FE_APTFIN_Downloader_Win32_TINYLOADER_1 FE_APTFIN_Downloader_Win64_TINYLOADER_1 FE_APTFIN_Downloader_Win64_TINYLOADER_2 FE_APTFIN_Downloader_Win32_TINYLOADER_2
TINYMET	El malware era un stager Meterpreter disponible públicamente que Mandiant rastreó con el nombre de TINYMET. El malware admite varios protocolos Meterpreter (también conocidos como “transportes”), que se pueden especificar durante el tiempo de ejecución: • 0: Shell inverso a través de TCP • 1: Shell inverso a través de HTTP • 2: Shell inverso a través de HTTPS • 3: Unión a puerto TCP	FE_Backdoor_Win32_TINYMET_1 Backdoor.Win.TINYMET.MVX

Tabla 6. Familias de malware (continuación)

Malware	Descripción	Detectado como
WINGSPAN	WINGSPAN es un cargador básico que recupera y ejecuta shellcode almacenado en una clave de registro codificada. El código de shell cargado por WINGSPAN generalmente se ha diseñado para ejecutar una carga útil de DLL PE integrada y comprimida.	FE_APTFIN_Loader_Win_WINGSPAN_1 FE_APTFIN_Loader_Win_WINGSPAN_2 FE_APTFIN_Loader_Win_WINGSPAN_3 FE_APTFIN_Loader_Win32_WINGSPAN_1 FE_APTFIN_Loader_Win64_WINGSPAN_1
WOOLLYBEAR	WOOLLYBEAR es una puerta trasera HTTP que puede ejecutar comandos proporcionados como respuesta HTTP a su servidor de comando y control. Se ha observado con poca frecuencia y la mayoría de las veces se instala utilizando otra puerta trasera.	APTFIN.Backdoor.Win.WOOLLYBEAR FE_APTFIN_Backdoor_Win32_WOOLLYBEAR_1

Apéndice F: Reglas de cacería

Las siguientes reglas no están diseñadas para ser utilizadas en sistemas de producción o para informar reglas de bloqueo sin haber sido validadas primero a través de los propios procesos de prueba internos de una organización para asegurar un desempeño apropiado y limitar el riesgo de falsos positivos. Estas reglas están destinadas a servir como punto de partida para los esfuerzos de cacería a fin de identificar los documentos descritos en este informe; sin embargo, los usuarios deben tener en cuenta que esta regla puede necesitar ser actualizada si los perpetradores actualizan sus técnicas o modifican las estructuras de sus documentos.

YARA

```
rule Dropper_Win32_MIXLABEL_1
{
   strings:
      $op_load1 = { 8B 55 ?? 83 C2 ?? 89 55 ?? 83 7D [2] 7D ?? C7 45 [5] 8B 45 ?? 0F AF 45 ?? 03 45 ?? 89 45 ?? EB ?? 8B 4D ?? 89 4D ?? 83 7D [2] 74 ?? 8B 55 ?? 0F B7 02 3D [4] 75 ?? 8B 4D ?? 8B 51 ?? 8B 45 ?? 81 3C 10 [4] 75 ?? 8B 45 ?? E9 [4] C7 45 [5] 8D 4D ?? 89 4D ?? 8D 55 }
      $op_load2 = { 81 7D [5] 7D ?? C7 85 [8] C7 85 [8] 8B 8D [4] 83 C1 ?? 8B 85 [4] 99 F7 F9 89 85 [4] 8B 8D [4] 83 C1 ?? 8B 85 [4] 99 F7 F9 0F AF 85 [4] 89 85 [4] 8D 95 [4] 89 95 [4] 8B 85 [4] 8B 8D [4] 0F AF 08 8B 95 [4] 2B D1 89 95 [4] E9 [4] E8 [4] 89 45 ?? E8 [4] 50 E8 [4] 83 C4 }
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x010B) and all of them
}

rule Dropper_Win32_MIXLABEL_2
{
   strings:
      $op_load = { 8B 4D ?? 51 68 [4] 8B 55 ?? 52 E8 [4] 83 C4 ?? 83 7D [2] 0F 84 [4] 8B 45 ?? 0F B7 08 81 F9 [4] 75 ?? 8B 55 ?? 8B 42 ?? 8B 4D ?? 81 3C 01 [4] 75 ?? 8B 45 ?? E9 [4] C7 45 [5] C7 45 [5] 8B 55 ?? 3B 55 ?? 74 ?? C7 45 [5] 8B 45 ?? 0B 45 ?? 03 45 ?? 03 45 ?? 89 45 ?? EB ?? C7 45 [5] C7 45 [5] 8B 4D ?? 83 C9 ?? 03 4D ?? 0F AF 4D ?? 89 4D ?? 8B 55 ?? 03 55 ?? 0F AF 55 ?? 89 55 ?? C7 45 [5] 8B 45 ?? 23 45 ?? 03 45 ?? 0F AF 45 ?? 89 45 ?? 83 7D [2] 75 ?? E8 }
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x010B) and all of them
}
```

```
rule Dropper_Win32_MIXLABEL_3
{
   strings:
      $op_load = { 83 7D [2] 7D ?? C7 45 [5] 8D 55 ?? 89 55 ?? 8B 45 ?? 8B 4D ?? 03 08 03 4D ?? 89 4D ?? C7 45 [5] C7 45 [5] 8B 55 ?? 0B 55 ?? 03 55 ?? 8B 45 ?? 2B C2 89 45 ?? EB ?? 83 7D [2] 74 ?? 8B 4D ?? 0F B7 11 81 FA [4] 75 ?? 8B 45 ?? 8B 48 ?? 8B 55 ?? 81 3C 0A [4] 75 ?? 8B 45 ?? EB ?? C7 45 [5] 8B 45 ?? 50 68 [4] 8B 4D ?? 51 E8 [4] 83 C4 ?? 8B 55 ?? 81 EA [4] 89 55 ?? EB ?? C7 45 [5] C7 45 [5] 8B 4D ?? 83 C1 ?? 8B 45 }
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x010B) and all of them
}

rule Backdoor_Win64_MIXLABEL_1
{
   strings:
      $backdoor = { FF 15 [4] 48 [2] 48 [4] 45 33 C9 C7 44 [6] 48 [2-10] 45 8D [2] FF 15 [4] 83 F8 [1] 74 }
      $shell = { 48 C7 44 [2] 00 00 00 00 48 C7 44 [6] 48 C7 44 [2] 00 00 00 00 [0-10] 48 C7 [2] 00 00 00 00 C7 [2] 00 00 00 00 48 C7 [2] 05 00 00 00 48 C7 [2] 00 00 00 00 C7 [2] 01 01 00 00 [0-10] FF 15 [4] 85 C0 74 }
      $str1 = "createprocess" ascii nocase wide
      $str2 = "getcurrentprocessid" ascii nocase wide
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x020B) and all of them
}

rule Win32_CLOP_1
{
   strings:
      $a1 = { 6A 00 6A 00 50 8D 85 [4] 50 6A 00 6A 00 8D 85 [4] 50 FF 15 [4] 85 C0 }
      $a2 = { 8D 85 [4] 50 8D 85 [4] 50 6A ?? 68 00 80 00 00 FF B5 [4] 8D 85 [4] 50 6A 08 6A 01 FF 15 [4] 85 C0 74 ?? 68 00 00 00 F0 6A 01 6A 00 6A 00 8D 85 [4] 50 FF 15 [4] 85 C0 74 ?? 8D 85 [4] 50 6A 00 6A 00 6A 00 FF B5 [4] 6A 01 FF B5 [4] FF 15 [4] 85 C0 }
      $a3 = { 6A 75 8D 85 [4] C7 85 [4] 75 00 00 00 50 6A 00 6A 00 6A 01 6A 00 FF B5 [4] C7 85 [4] 75 00 00 00 FF 15 [4] 85 C0 }
      $a4 = "CryptStringToBinaryA"
      $a5 = "CryptDecodeObjectEx"
      $a6 = "CryptAcquireContextW"
      $a7 = "CryptImportPublicKeyInfoEx"
      $a8 = "CryptEncrypt"
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x010B) and all of them
}
```

```
rule Win_CLOP_1
{
   strings:
      $a1 = "%s\\ClopReadMe.txt" ascii wide
      $a2 = "%s%s.Clop" ascii wide
      $a3 = "Clop^_-" ascii wide
      $b1 = ".Clop" ascii wide
      $b2 = "%s%s.Clop" ascii wide
      $b3 = "Clop^_-" ascii wide
      $b4 = "ClopReadMe.txt" ascii wide
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and ( all of ($a*) or all of ($b*) )
}

rule Loader_Win32_MINEDOOR_1
{
   strings:
      $s1 = { 55 8B EC 51 C7 45 ?? 00 00 00 00 8B 45 ?? 33 45 ?? 89 45 ?? C1 45 ?? 04 8B 4D ?? 81 C1 78
77 77 77 89 4D ?? 8B 45 ?? 8B E5 5D C3 }
   condition:
      filesize < 1MB and uint16(0) == 0x5A4D and any of them
}

rule Loader_Win64_MINEDOOR_1
{
   strings:
      $alloc = { 41 B9 40 00 00 00 41 B8 00 30 00 00 [4-12] FF 15 }
      $decrypt = { C1 [2] 89 84 [3-6] 8B [3-6] 8B [3-6] 33 ?? 8B ?? 89 [4-6] 48 63 [4-6] 48 8B [3-6] 8B [3-
6] 89 [1-3] E9 }
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18)
== 0x020B) and all of them
}

rule Loader_Win64_MINEDOOR_2
{
   strings:
      $s1 = { 48 63 [6] 48 8D [5] 8B [2] 89 [6] 8B [5] 8B [6] 33 C8 8B C1 89 [6] 8B [6] C1 C0 07 89 }
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18)
== 0x020B) and all of them
}
```

```
rule Loader_Win32_FORKBEARD_1
{
   strings:
      $sb1 = { 55 8B EC 83 EC ?? 8B 45 08 35 [4] 89 45 F? B8 08 00 00 00 }
      $sb2 = { 6A 40 68 00 30 00 00 [0-12] 8B [2-16] FF 15 [4] 8B E5 5D C3 }
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18)
== 0x010B) and (filesize > 400KB) and (#sb1 == 1) and (#sb2 == 1)
}

rule Loader_Win32_FORKBEARD_2
{
   strings:
      $sb1 = { 8B ?? 08 03 ?? 10 8B ?? 0C 03 ?? 10 8A ?? FF 88 ?? FF 8B ?? 10 83 ?? 01 89 ?? 10 EB ?? 8B E5
5D C3 }
      $sb2 = { 6A 40 68 00 30 00 00 [0-12] 8B [2-16] FF 15 [4] 8B E5 5D C3 }
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18)
== 0x010B) and (filesize > 400KB) and (#sb1 == 1) and (#sb2 == 1)
}

rule Loader_Win32_FORKBEARD_3
{
   strings:
      $sb1 = { 8B [2] 8B [2] 8A 14 01 8B [2] 88 ?? 06 83 C0 01 8B }
      $sb2 = { 8A 3? 0? 28 ?? 8B [3] 88 ?? 0? [8-32] 83 C0 01 }
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18)
== 0x010B) and (filesize > 400KB) and (#sb1 == 1) and (#sb2 == 1)
}

rule Win32_SPOONBEARD_1_Beta
{
   strings:
      $f1 = { 73 7D 8B [2] 8B [2] 8B [2] 89 }
      $f2 = { 83 [2] 89 [2] 8B [5] 33 [5] 89 [5] 8B }
      $f3 = { 89 [2] C1 [6] 8B [5] 33 [5] 89 [5] 8B [2] 8B [2] 8B [5] 89 [2] E9 ?? FF FF FF }
   condition:
      (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) ==
0x010B) and filesize < 20MB and all of them
}
```

```
rule Dropper_Win32_SPOONBEARD_2
{
   strings:
      $dec1 = { C7 45 [5] C7 45 ?? 00 00 00 00 C7 45 ?? 00 00 00 00 EB ?? 8B [2] 83 ?? 01 89 [2] 8B [2]
C1 ?? 02 39 [2] 73 }
      $dec2 = { 8B [2] 8B [2] 8B [2] 89 [2-5] ( 8B ?? | A1 ) [4] 89 [2-5] 8B [2-5] 2B [2] 89 [2-5] 8B [2] 83
[2] 89 [2] 8B [2-5] 33 [2-5] 89 [2-5] 8B [2] ( 81 ?? | 2D ) [2] 00 00 89 [2] C1 [2-5] 07 8B [2-5] 33 [2-5] 89
[2-5] 8B [2] 8B [2] 8B [2-5] 89 [2] E? }
   condition:
      ((uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18)
== 0x010B)) and $dec1 and $dec2 and (@dec1[1] < @dec2[1])
}

rule Dropper_Win32_SPOONBEARD_3
{
   strings:
      $dec1 = { 81 7D ?? 84 03 00 00 73 ?? 8B ?? ?? 8B ?? ?? 8B ?? ?? 89 [7-11] 89 [2-5] 8? [2-5] 2B [2] 89
[2-5] 8B [2] 83 ?? 50 89 [2] 8B [2-5] 33 [2-5] 89 [2-5] 8B [3-4] E8 03 00 00 89 [2] C1 [2-5] 07 }
   condition:
      ((uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18)
== 0x010B)) and $dec1
}

rule Loader_Win_WINGSPAN_1
{
   strings:
      $sb1 = { FF 15 [4-5] 85 C0 [2-64] E8 [4] B? [4-5] 8? [1-3] E8 [4] B? [4-5] 8? [1-3] E8 [4] B? [4-5] 8?
[1-3] E8 [4] B? [4-5] 8? [1-3] E8 [4] B? [4-5] 8? [1-3] E8 [5-8] 8D [5-16] FF [16-64] 19 00 02 00 }
      $sb2 = { C7 44 24 [3] 00 00 [4-24] FF [1-5] 85 C0 7? [8-64] FF [1-5] 85 C0 7? [1-16] FF }
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and all of them
}

rule Loader_Win_WINGSPAN_2
{
   strings:
      $sb1 = { C1 C? 0D [0-8] 80 E? 61 [0-8] 80 F? 19 }
      $sb2 = { 83 ?? 01 7? ?? 83 ?? 03 [4-80] FF 15 [4-5] 85 C0 [2-64] E8 [4-16] B? [4-5] 8? [1-3] E8 [4-16]
B? [4-5] 8? [1-3] E8 [4-16] B? [4-5] 8? [1-3] E8 [4-16] B? [4-5] 8? [1-3] E8 [4-16] B? [4-5] 8? [1-3] E8 }
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and all of them
}
```

```
rule Loader_Win_WINGSPAN_3
{
   strings:
      $sb1 = { C1 C? 0D [0-8] 80 E? 61 [0-8] 80 F? 19 }
      $sb2 = { 2E 7? [1-16] 01 74 7? [1-16] 02 65 7? [1-16] 03 78 7? [1-16] 04 74 7? [1-16] 05 00 }
   condition:
      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and all of them
}
```

Snort

```
alert tcp $HOME_NET any -> any any ( msg:"MIXLABEL"; dsize:4; flow:to_server; content:"|00 00 de c0|";
offset:0; depth:4; fast_pattern; content:!"GET "; content:!"POST "; sid:99999999; rev:4; )
```

```
alert tcp any any -> any any ( msg:"FRIENDSPEAK"; flow:to_server; content:"&D="; depth:3; fast_pattern;
content:"&U="; distance:0; content:"&OS="; content:"&PR="; distance:0; content:!"Cookie:"; content:!"Referer";
sid:99999999; rev:3; )
```

```
alert tcp any any -> any [139,445] ( msg:"NAILGUN.[swaqp.exe]"; content:"|fe 53 4d 42 40|"; content:"|73 00 77
00 61 00 71 00 70 00 2e 00 65 00 78 00 65 00|"; classtype:methodology; priority:2; gid:666; sid:99999999;
rev:1; )
```

Para obtener más información acerca de Mandiant Solutions, visite:
www.FireEye.com/mandiant

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

M-EXT-SR-US-EN-000324-02

Acerca de Mandiant Solutions
Mandiant Solutions reúne la experiencia de información sobre amenazas y de primera línea más importante del mundo con una validación de la seguridad continua a fin de armar a las organizaciones con las herramientas necesarias para aumentar la eficacia de la seguridad y reducir el riesgo comercial.

MANDIANT®