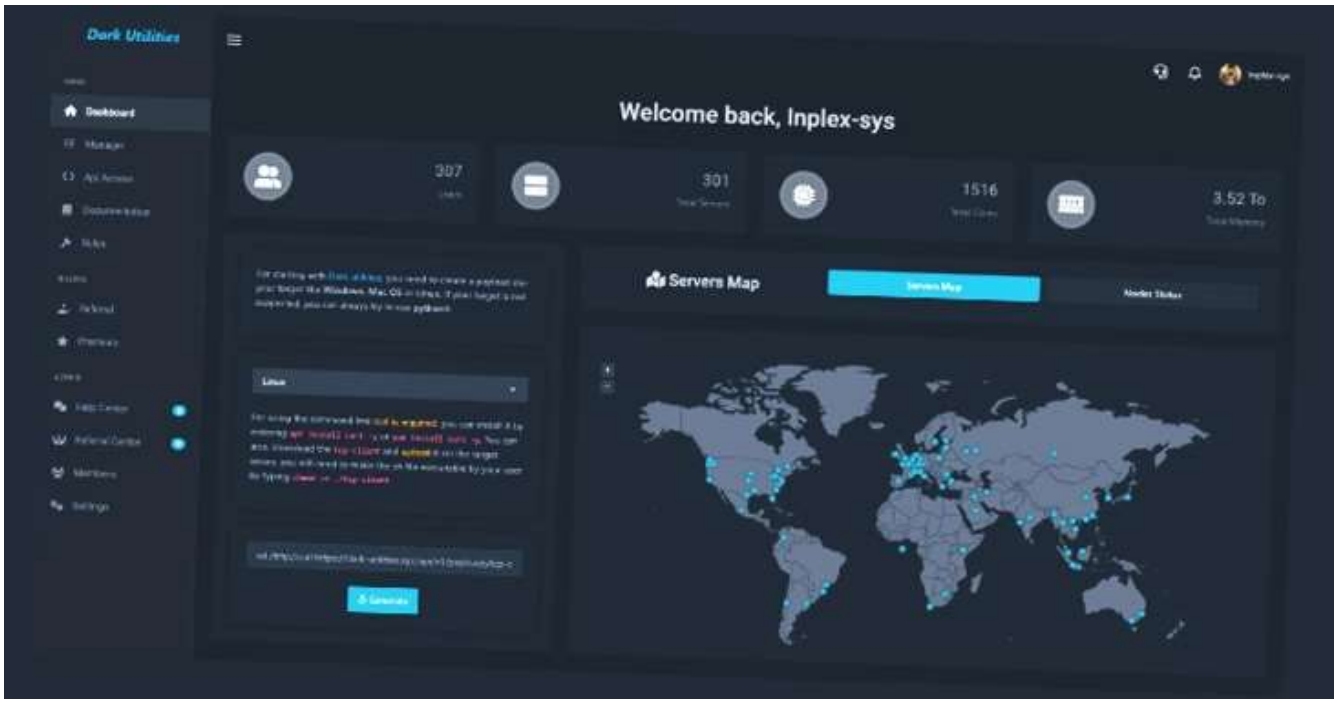
Cybersecurity – Cibersegurança - Ciberseguridad
Sharing information and best practices: that's the idea!
Compartilhar informações e boas práticas: essa é a idéia!
Compartir información y mejores prácticas: ¡esa es la idea!

Interesting News from around the Cybersecurity Community - Aug 5th, 2022



a) A Growing Number of Malware Attacks Leveraging Dark Utilities 'C2-as-a-Service' (Aug 05, 2022)

A nascent service called Dark Utilities has already attracted 3,000 users for its ability to provide command-and-control (C2) services with the goal of commandeering compromised systems.

"It is marketed as a means to enable remote access, command execution, distributed denial-of-service (DDoS) attacks and cryptocurrency mining operations on infected systems," Cisco Talos said in a report shared with The Hacker News.

Dark Utilities, which emerged in early 2022, is advertised as a "C2-as-a-Service" (C2aaS), offering access to infrastructure hosted on the clearnet as well as the TOR network and associated payloads with support for Windows, Linux, and Python-based implementations for a mere €9.99.

Authenticated users on the platform are presented with a dashboard that makes it possible to generate new payloads tailored to a specific operating system that can then be deployed and executed on victim hosts.

Additionally, users are provided an administrative panel to run commands on the machines under their control upon establishing an active C2 channel, effectively granting the attacker full access to the systems.

The idea is to enable threat actors to target multiple architectures without requiring significant development efforts. Also extended to its customers are technical support and assistance through Discord and Telegram.

"Given the relatively low cost compared to the amount of functionality the platform offers, it is likely attractive to adversaries attempting to compromise systems without requiring them to create their own C2 implementation within their malware payloads," the researchers noted.

Source: https://thehackernews.com/2022/08/a-growing-number-of-malware-attacks.html

b) Un informe indica que la Fed no está lista para evitar la recopilación de datos por parte de China (July 26, 2022)

La Reserva Federal no cuenta con sistemas adecuados para contrarrestar un esfuerzo "malicioso" de China para reunir información interna sobre la economía y la política monetaria de Estados Unidos, según un informe que fue elaborado por el personal republicano del Comité de Seguridad Nacional del Senado, y que fue rápidamente rechazado por la Fed por considerarlo "imparcial, no fundamentado y no verificado."

El informe, que se publicó el martes, se basa en gran medida en la información proporcionada por el propio banco central estadounidense, que se remonta a una investigación interna de 2015 sobre lo que llegó a conocerse como la "Red P", un grupo de 13 personas en ocho departamentos regionales de la Fed cuyos patrones de "viajes al extranjero, correos electrónicos, detalles en los currículos y antecedentes académicos" suscitaron preocupación.

La Junta de Gobernadores de la Reserva Federal, con sede en Washington, y los 12 cuasi independientes bancos regionales emplean a miles de economistas, muchos de ellos procedentes de otros países, entre ellos China. Este enfoque de colaboración, según el informe del comité, mejora la capacidad de la Reserva Federal para comprender la economía y formular políticas.

Los incidentes citados en el documento, más que a la colaboración intelectual, apuntaban a "un esfuerzo sostenido de China, durante más de una década, para ganar influencia sobre la Reserva Federal", según el informe.

No está claro qué resultó de ello. El informe de la comisión ofrece estudios de casos detallados de cinco personas, cuatro de las cuales siguen siendo empleados de la Reserva Federal, y dice que, a pesar de sus conexiones con altos cargos y universidades chinas, la Reserva Federal no encontró ningún caso en el que se hubiera compartido información en violación de las políticas.

Informe:https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Report%20-%20China%20Threat%20to%20the%20Fed.pdf

Fuente: https://es-us.finanzas.yahoo.com/noticias/informe-indica-fed-lista-evitar-110317909.html

c) Phishing y vulnerabilidades de software, 7 de cada 10 incidentes cibernéticos (July 29, 2022)

De acuerdo con un nuevo informe de Palo Alto Networks, el intenso uso de vulnerabilidades de software coincide con el comportamiento oportunista de los actores de amenazas que buscan en internet vulnerabilidades y puntos débiles en los que concentrarse.

El Informe de respuesta a incidentes de 2022 de Unit 42 ofrece una variedad de conocimientos obtenidos por el trabajo de respuesta a incidentes (RI) de Unit 42 de Palo Alto Networks, aprovechando una muestra de más de 600 casos de RI recibidos, para ayudar a los CISO y equipos de seguridad a comprender los mayores riesgos de seguridad a los que se enfrentan y dónde priorizar los recursos para reducirlos.

En el informe, Unit 42 identificó que entre las industrias que recibieron el promedio más alto de solicitudes de rescate se encontraron las finanzas y los bienes raíces, con una demanda promedio de casi ocho millones y 5.2 millones de dólares, respectivamente.

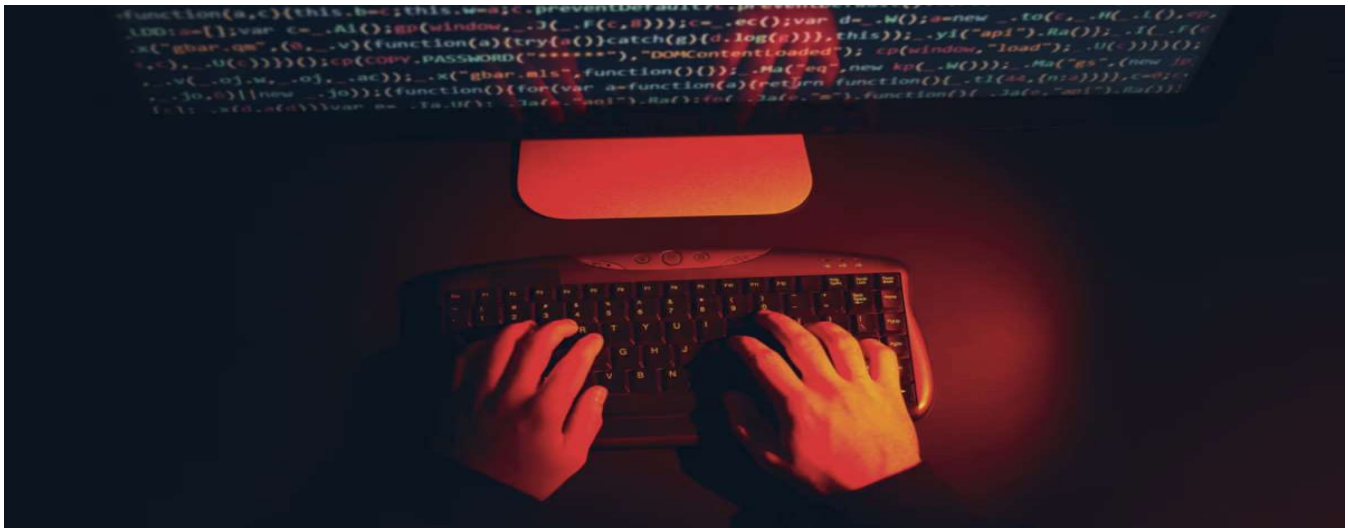
En general, el ransomware y el correo electrónico empresarial comprometido fueron los principales tipos de casos a los que atendió el equipo de respuesta a incidentes durante los últimos 12 meses, lo que representa aproximadamente el 70 % de los ataques.

Las tendencias clave cubiertas en el informe incluyen:

- Ransomware
- BEC (Business Email Compromise, por sus siglas en inglés)
- Industrias afectadas

Informe: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2022-unit42-incident-response-report-final.pdf

Fuente: https://reseller.com.mx/phishing-y-vulnerabilidades-de-software-7-de-cada-10-incidentes-ciberneticos/



d) Investigación austriaca revela spyware dirigido a bufetes de abogados e instituciones financieras (Aug 1st, 2022)

El gobierno austriaco dijo el viernes que estaba investigando a una empresa con sede en el territorio de la nación por supuestamente desarrollar software espía dirigido a bufetes de abogados, bancos y consultorías en al menos tres países.

La noticia llega días después de que el Threat Intelligence Center (MSTIC) de Microsoft dijo encontró malware llamado Subzero (CVE-2022-22047) implementado en 2021 y 2022.

Según el gigante tecnológico, Subzero fue desarrollado por la empresa DSIRF con sede en Viena (seguida por Microsoft con el nombre en clave KNOTWEED) y se implementó a través de una variedad de métodos, incluidas vulnerabilidades de día cero en Windows y Adobe Reader.

Por contexto, DSIRF opera bajo la apariencia de ayudar a las corporaciones multinacionales a realizar análisis de riesgo y recopilar inteligencia comercial.

Sin embargo, el aviso de Microsoft ha relacionado a la empresa con la venta de software espía utilizado para la vigilancia no autorizada.

“Las víctimas observadas hasta la fecha incluyen firmas de abogados, bancos y consultorías estratégicas en países como Austria, el Reino Unido y Panamá”, MTIC escribió.

“Es importante tener en cuenta que la identificación de objetivos en un país no significa necesariamente que un cliente de DSIRF resida en el mismo país, ya que la orientación internacional es común”.

Microsoft dijo que encontró múltiples vínculos entre DSIRF y las vulnerabilidades y el malware utilizado en estos ataques.

Informe: https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

Leer más: https://dearce.com.uy/investigacion-austriaca-revela-spyware-dirigido-a-bufetes-de-abogados-e-instituciones-financieras/

e) Estos hackers de ransomware se dieron por vencidos cuando llegaron a la autenticación multifactor (Jul 27, 2022)

Se evitó un ataque de ransomware simplemente porque la víctima prevista estaba usando autenticación multifactor (MFA) y los atacantes decidieron que no valía la pena el esfuerzo de intentar eludirlo.

A menudo se dice que usar MFA, también conocida como autenticación de dos factores (2FA), es una de las mejores cosas que puede hacer para ayudar a proteger sus cuentas y redes informáticas de los ataques cibernéticos porque crea una barrera efectiva, y ahora Europol lo ha visto. en acción mientras investiga bandas de ransomware.

“Hemos realizado investigaciones en las que se monitoreó a los delincuentes de ransomware. En ciertas investigaciones, vimos que intentaban acceder a las empresas, pero tan pronto como accedían a la autenticación de dos factores en este proceso, inmediatamente abandonaban a esta víctima y pasaban a la siguiente”, dijo Marijn Schuurbiers, jefa de operaciones del Centro Europeo de Delitos Cibernéticos (EC3) de Europol, hablando sobre un incidente no revelado que investigó la agencia.

Demuestra cuán útil puede ser MFA para prevenir ransomware y otros ataques cibernéticos. Incluso si el atacante tiene la contraseña legítima de la cuenta, ya sea porque la adivinó o porque se la robaron, el uso de MFA generalmente evita que pueda iniciar sesión.

Una alerta inesperada de una aplicación de autenticación MFA también puede notificar a la víctima prevista que algo anda mal y debe investigarse, lo que también puede ayudar a prevenir más ataques e incidentes.

Los ciberdelincuentes no solo pueden explotar cuentas pirateadas para obtener acceso inicial a la red e instalar ransomware, sino que el acceso que obtienen también se puede usar como parte de ataques de doble extorsión, donde los delincuentes roban información antes de cifrarla, con amenazas de publicar los datos si no se recibe un rescate.

Sin embargo, si los atacantes no pueden acceder a esos datos debido al uso de MFA, no pueden intentar explotarlos para extorsionarlos.

Leer más: https://es.postsus.com/negocio/861466.html

----------X----------

*The information contained in this newsletter, including any external links, is provided "AS IS," with no express or implied warranty, for informational purposes only.
*As informações contidas neste boletim, incluindo links externos, são fornecidas "COMO ESTÃO", sem garantia expressa ou implícita, apenas para fins informativos.
*La información contenida en este boletín, incluidos los enlaces externos, se proporciona "TAL CUAL", sin garantía expresa o implícita, solo con fines informativos.

Personal Cybersecurity Tip

Charity & Disaster Scams

August 3, 2022

Cyber criminals know that one of the best ways to rush people into making a mistake is by creating a heightened sense of urgency. And one of the easiest ways to create a sense of urgency is to take advantage of a crisis. This is why cyber criminals love it whenever there is a traumatic event with global impact. What most of us regard as a tragedy, cyber criminals view as an opportunity, such as the breakout of a war, a major natural disaster such as a volcanic explosion, and of course infectious disease breakouts like COVID- 19. When there is an immense amount of social media and news coverage about a certain event, cyber criminals know that is the time to strike.

They use this opportunity to create timely phishing emails or scams about the event, and then send that phishing email or launch the scam to millions of people around the world. For example, during a natural disaster, they may pretend to be a charity asking for donations to save children in need. Cyber criminals can often act within hours of a crisis or disaster, as they have all the technical infrastructure prepared and are ready ahead of time. How can we protect ourselves the next time there is a big crisis or disaster, and cyber criminals seek to exploit it?

How to Detect and Defend Against These Scams

The key to avoiding these scams is to be suspicious of anyone who reaches out to you. For example, do not trust an urgent email claiming to be from a charity that desperately needs donations, even if the email appears to be from a brand that you know and trust. Do not trust a phone call claiming to be a local food bank pressuring you to donate. The greater the sense of urgency, the more likely the request is an attack. Here are some of the most common indicators of a charity scam:

- Be very suspicious of any charity that requires that you donate via cryptocurrency, Western Union, wiring money, or gift cards.
- Cyber criminals can change their caller ID phone number to make their phone call look like it's from your local area code or from a trusted name. Caller ID cannot be relied upon these days.
- Some cyber criminals will use names and logos that sound or look like a real charity. This is one reason it pays to do some research before giving.
- Cyber criminals will often make lots of vague and sentimental claims about what they will do with your money but give no specifics about how your donation will be used.
- Some cyber criminals may try to trick you into donating to them by thanking you for a donation you made in the past when, in reality, you never donated to them.
- Do not assume pleas for help on crowdfunding sites such as GoFundMe or social media sites such as TikTok are legitimate, especially in the wake of a crisis or tragedy.
- Do not give out personal or financial information in response to any unsolicited request.

Source: https://www.sans.org/newsletters/ouch/charity-disaster-scams/?utm_medium=Email&utm_source=HL-GL&utm_content=1158315%20August3%20OUCH%20Newsletter%20button&utm_campaign=OUCH_Newsletter