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 - Jul 29th, 2022

a) US Cyber Command Says Malware Indicators Targeting Ukraine (Jul 21, 2022)

A barrage of cyberattacks targeting Ukraine led the U.S. military to publicly disclose a slew of malware indicators in a bid to stymie hackers and underline America's close relationship with Kyiv.

U.S. Cyber Command in coordination with the Security Service of Ukraine on Wednesday disclosed 20 novel indicators of malware infections.

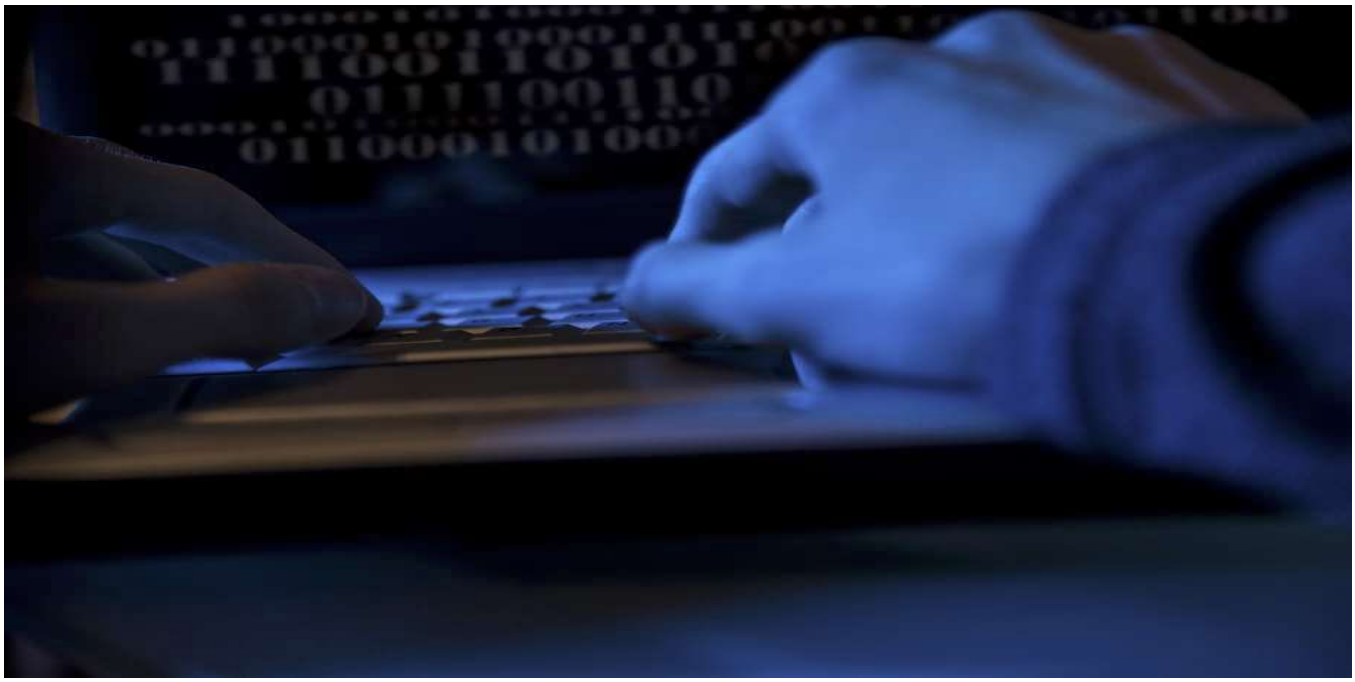
"Our Ukrainian partners are actively sharing malicious activity they find with us to bolster collective cybersecurity, just as we are sharing with them. We continue to have a strong partnership in cybersecurity between our two nations," U.S. Cyber Command says.

The military command has acknowledged working side by side with Ukrainian Cyber Command to identify vulnerabilities and spot hackers. The United States has aided Ukrainian defense through weapons transfers and humanitarian aid. In June, President Joe Biden announced $1 billion in additional security assistance for the Eastern European country, the twelfth delivery of U.S. arms since August 2021.

Ukrainian cyberspace went into red alert following Russia's February invasion as defenders mobilized to fend off an arsenal of wipers and other digital attacks. (see: *Major Takeaways: Cyber Operations During Russia-Ukraine War*).

IOCs from Ukrainian networks: https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/

Source: https://www.govinfosecurity.com/us-cyber-command-reveals-malware-indicators-targeting-ukraine-a-19619



b) How the cyberwar between Iran and Israel has intensified (July 25, 2022)

In late June, Iran's state-owned Khuzestan Steel Co. and two other steel companies were forced to halt production after suffering a cyberattack. A hacking group claimed responsibility on social media, saying it targeted Iran's three biggest steel companies in response to the "aggression of the Islamic Republic."

Israel's defense secretary then ordered an investigation into leaked video showing the damage to the steel plants, citing "operational events in a manner that violates Israel's ambiguity policy." This incident came close on the heels of a statement by the Israeli Security Agency, or Shin Bet, claiming a May cyberoperation by Iran was intended to generate actions outside of the cyber-domain.

Both incidents show how the cyberconflict between the two countries has grown increasingly public in the past two years. While Israel traditionally sticks to ambiguous responses, these latest examples and others suggest that may be changing. Iran also broke its silence and chose to publicly discuss some of these incidents.

Why are Israel and Iran going public about these cyberoperations? Here are three things to know about the not-so-covert cyberconflict between Israel and Iran.

Cyber-actions are becoming less covert

Iran and Israel have long engaged in mutual offensive covert cyber-actions, although neither government took credit for them in public. More than a decade ago, Iranian officials discovered the Stuxnet malware in the uranium enrichment centrifuges in one of Iran's nuclear facilities, marking the first public evidence of the use of cyberweapons against Iran. But the alleged cyberattacks and intrusions between Iran and Israel have intensified, gaining global attention and coverage, giving a new public dimension to the ongoing covert conflict.

Read more at: https://www.washingtonpost.com/politics/2022/07/25/iran-israel-cyber-war/

c) Cyberattack Affects Albanian Government E-Services: Report (July 18, 2022)

Albania's pivot to digital delivery of government services is being disrupted by a cyberattack that resulted in the shutdown of the national e-services portal.

A Monday statement attributed to the prime minister's office by local media says the government detected the attack Friday afternoon. It appeared at first to be ransomware but has its real goal was to take Albania's government offline, says a copy of the statement posted by the Albanian Daily News.

On Sunday, London-based internet traffic monitor NetBlocks tweeted it observed government online services being taken offline Saturday night.

As of publication, the prime ministerial and parliament websites are offline, as is government portal e-Albania.

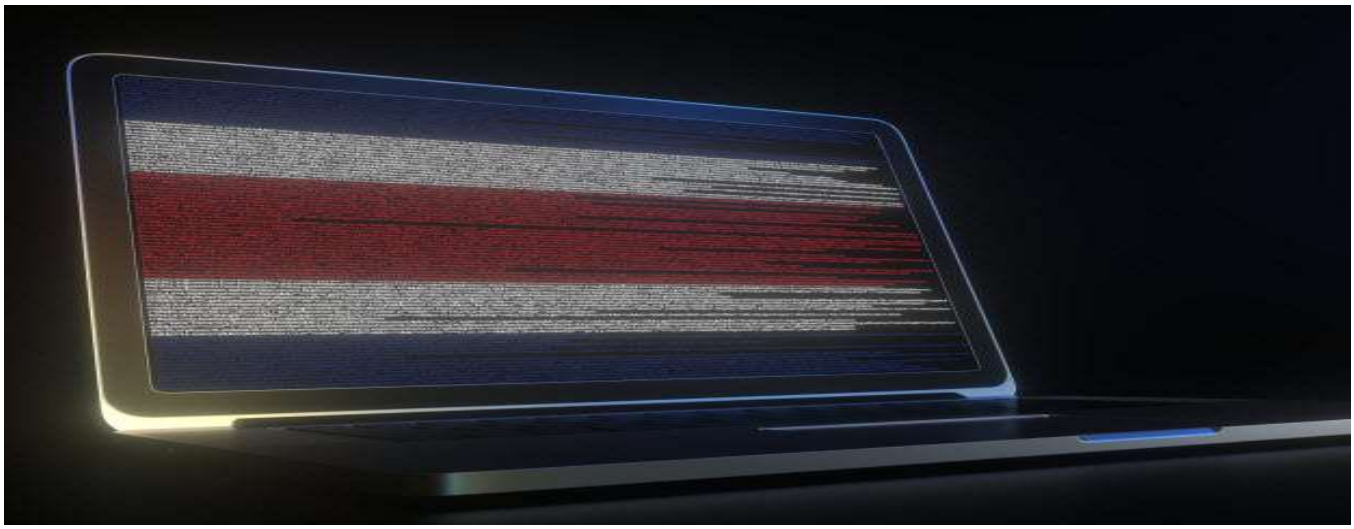
"Government systems are all backed up and secure," the prime minister's office says.

The government of Albanian Prime Minister Edi Rama earlier this year told citizens that nearly all public administration services would be shifted online May 1 while in-person facilities would be shut down. It shows that 72% of Albania's population as of 2020 can access the internet.

The government says the cyberattack is similar in pattern to attacks observed in Ukraine, Germany and other European countries earlier this year. There has been an uptick in cyberattacks in these places following Russia's invasion of Ukraine (see: Russia-Ukraine War: Cyberattack Escalation Risk Continues).

The National Agency for Information Society, or AKSHI, is working with Microsoft and the national security consultancy Jones Group International, the prime minister's office says. AKSHI did not immediately respond to ISMG's request for comment.

Source: https://www.govinfosecurity.com/cyberattack-affects-albanian-government-e-services-report-a-19582



d) Detalles de cómo se produjo el ataque del ransomware Conti a Costa Rica (Jul 22, 2022)

El ciberataque del ransomware Conti a organismos gubernamentales de Costa Rica en abril de 2022 tuvo gran repercusión por el alcance y las consecuencias del incidente. Y si bien hasta el momento no se habían publicado detalles de cómo fue que se produjo el ataque que terminó afectando al menos a ocho entidades y que derivó en que se declare la emergencia nacional en el país, investigadores revelaron detalles de cómo fue que Conti logró acceso a la red del Ministerio de Hacienda y los pasos que dieron los criminales hasta ejecutar el ransomware, extorsionar al gobierno y acceder a las redes de otros organismos.

Vale la pena mencionar que los mecanismos utilizados por Conti en este ataque son los mismos que viene utilizando desde hace bastante tiempo. Esto demuestra que los actores maliciosos seguirán recurriendo a las mismas estrategias hasta que las organizaciones no tomen nota de las técnicas y herramientas que utilizan estos grupos, pero también sirve como ejemplo para cuestionar esta idea que muchos tienen de que los cibercriminales siempre utilizan métodos y técnicas sofisticadas para comprometer a sus víctimas.

En un reporte publicado esta semana por AdvIntel, investigadores afirmaron que fue un proceso de cinco días (comenzó el 11 de abril) desde que los atacantes lograron el acceso inicial a la red, realizaron tareas de reconocimiento y exfiltración de información, hasta finalmente ejecutar el código maliciosos.

Un miembro del grupo, denominado MemberX, logró acceder a la red del Ministerio de Hacienda y obtener permisos de administrador de dominio utilizando credenciales previamente comprometidas de una conexión VPN. El robo de estas credenciales se logró a través de la instalación de una forma cifrada de la herramienta de pentesting legítima Cobalt Strike en una sub red del organismo.

Una vez dentro de la red utilizaron la herramienta de línea de comando nltest para obtener una lista de los controladores de dominio del organismo y la relación de confianza entre ellos. Luego, escanearon la red en busca de información sensible a través de la utilidad ShareFinder y AdFind para finalmente descargar en su máquina local el resultado de la herramienta File Share a través de un canal de CobaltStrike.

Report: https://www.advintel.io/post/anatomy-of-attack-truth-behind-the-costa-rica-government-ransomware-5-day-intrusion

Leer más: https://www.welivesecurity.com/la-es/2022/07/22/detalles-como-produjo-ataque-conti-organismos-costa-rica/

e) Este malware infecta su placa base y es casi imposible de eliminar (Jul 26, 2022)

Los investigadores han descubierto malware que ha estado infectando en secreto sistemas con placas base Asus y Gigabyte durante al menos seis años.

Desde 2016, los hackers de habla china se han estado infiltrando en las máquinas con el malware CosmicStrand, según un informe de Bleeping Computer.

En particular, una vez que se ha distribuido el código malicioso, permanece en gran medida sin ser detectado dentro de las imágenes de firmware para ciertas placas base. Este método particular de orientación de imágenes de firmware se clasifica como un rootkit de interfaz de firmware extensible unificada (UEFI).

La cepa fue nombrada CosmicStrand por investigadores que trabajan para la firma de ciberseguridad Kaspersky. Sin embargo, una versión anterior del malware, denominada Spy Shadow Trojan, fue descubierta inicialmente por analistas de Qihoo360.

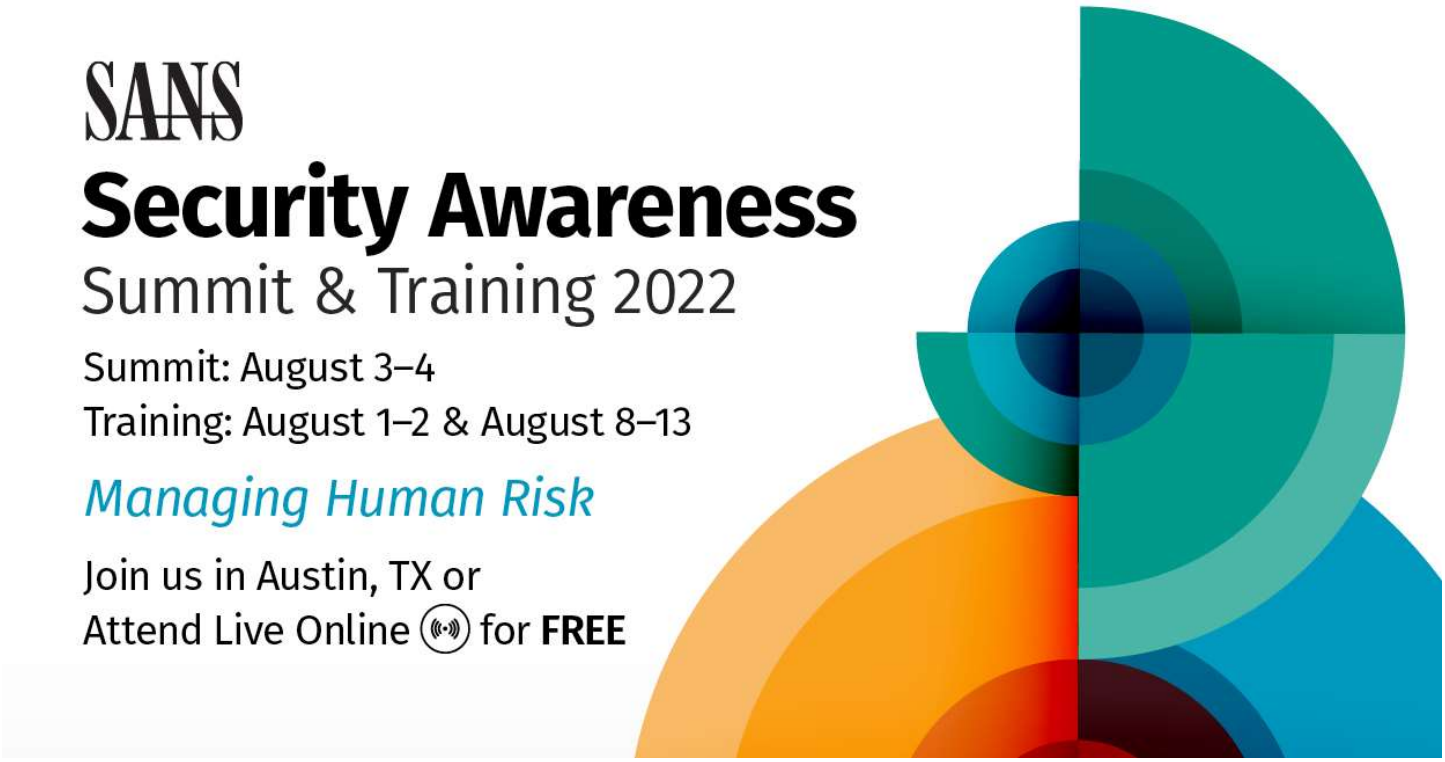
Como referencia, UEFI es una aplicación importante que conecta un sistema operativo con el firmware del propio hardware. Como tal, el código UEFI es lo que se ejecuta cuando una computadora se inicia inicialmente, incluso antes de cualquier medida de seguridad del sistema.

Como resultado, el malware que se ha colocado en la imagen del firmware UEFI es extremadamente efectivo para evadir las medidas de detección. Sin embargo, lo más preocupante es el hecho de que el malware no se puede eliminar técnicamente operando una reinstalación limpia del sistema operativo. Ni siquiera puede deshacerse de él reemplazando la unidad de almacenamiento.

Leer más: https://es.digitaltrends.com/computadoras/malware-infectando-sistemas-placas-bases-asus-gigabyte/

----------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.

Events



Link: https://www.sans.org/cyber-security-training-events/security-awareness-summit-2022/