



JORGE TESTA
Ciberseguridad

KILLING THE БЗАРЯ

Malware y Cibercrimen organizado

I GET DIRTY
THE CLIENT STAYS CLEAN
THAT'S THE MISSION

Índice de Contenidos



Malware

Wipers. Entre ellos Hermetic, Isaac y Caddy. Qakbot y ultimos IOCs de Emotet (E4)



Campañas

Vista atrás de la campaña Accellion FTA de 2021. Un repaso de los ataques a VMware ESXi y últimos movimientos de Rusia-Ucrania



Vulnerabilidades

44 Vulnerabilidades más usadas por operadores de Ransomware. 3 Vulnerabilidades críticas de Synology NAS y 5 vulnerabilidades bajas-medias de IBM y Linux Kernel



Amenazas

Un breve repaso a las TTPs e IOCs más recientes de Lapsus\$. NB65 y el supuesto ataque a Qiwi y una nueva encuesta de la siguiente víctima de Stormous.



MALWARE

Generic Malware (2022-04-29)

CIDR: 1 FileHash-MD5: 13 FileHash-SHA1: 12 FileHash-SHA256: 192 IPv4: 52 URL: 13
Domain: 37 Hostname: 32

HermeticWiper & IsaacWiper (2022-04-29)

FileHash-MD5: 33 FileHash-SHA1: 5 FileHash-SHA256: 7 YARA: 4

CaddyWiper (2022-04-29)

FileHash-MD5: 6 FileHash-SHA1: 1 FileHash-SHA256: 1 YARA: 1

Hermetic Wiper (2022-04-29)

FileHash-MD5: 58 FileHash-SHA1: 13 FileHash-SHA256: 13 SSLCertFingerprint: 3 YARA: 1

Emotet (2022-04-30)

FileHash-MD5: 5 FileHash-SHA1: 1 FileHash-SHA256: 1 IPv4: 61 URL: 74 Domain: 12 Email: 5
Hostname: 2

Qakbot (2022-04-30)

FileHash-SHA256: 4 IPv4: 136 URL: 159 Domain: 3

Emotet (2022-05-02)

FileHash-MD5: 1 FileHash-SHA1: 1 FileHash-SHA256: 3



CAMPAÑAS

"Accellion FTA" (2021-02-24)

CVE: 4

A principios de enero de 2021, varios actores explotaron vulnerabilidades 0-day en Accellion's legacy File Transfer Appliance (FTA) para instalar una webshell llamada ["Dewmode"](#)

"Hypervisor Jackpotting" (2022-04-29)

CVE: 1 FileHash-MD5: 2 FileHash-SHA1: 2 FileHash-SHA256: 2

Carbon Spider y Sprite spider son sospechosos de llevar a cabo una campaña contra ESXi (producto de VMWare) para propagar ransomware.

Timeline de la campaña en [Killing The Bear](#).

Russia-Ukraine War

Artículos: 5

Un repaso a los últimos acontecimientos del pasado mes de Abril.



VULNERABILIDADES

Ransomware Vulnerabilities in 2021 (2022-04-30)

CVE: 44

[Reporte](#) sobre las vulnerabilidades más explotadas por operadores de Ransomware durante todo el 2021.

Vulnerabilities Synology NAS (2022-05-02)

CVE: 3

Vulnerabilidades críticas

Vulnerabilities IBM and Kernel (2022-05-02)

CVE: 5

Vulnerabilidades de severidad baja y media en IBM y Linux Kernel



AMENAZAS

Lapsus\$ (2022-04-29)

IPv4: 3 URL: 1 Domain: 1

Tácticas recientes de Lapsus\$

Emotet (2022-05-01)

Artículos: 1

Emotet se adapta ante el movimiento de Microsoft de desactivar las macros VBA por defecto.

NB65 Allegedly get 10.5TB Qiwi.ru (2022-05-01)

Tweets: 1

NB65 asegura tener más de 10TB de Qiwi.ru

Stormous new pool (2022-05-01)

Tweets: 1

Nueva supuesta encuesta de Stormous para elegir nueva víctima