JORGE TESTA
Ciberseguridad

KILLING THE БЗАЯ

Malware y Cibercrimen organizado

GitBook

2022-05-01

"WE GET DIRTY
THE CLIENT STAYS CLEAN
THAT'S THE MISSION"

Índice de Contenidos

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus eget massa et metus dignissim molestie quis at sapien.

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

CAMPAÑAS

"Accellion FTA" (2021-02-24)

CVE: 4

A principios de enero de 2021, varios actores explotaron vulnerabilidades 0-day en Acellion'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*.

VULNERABILIDADES

Ransomware Vulnerabilities in 2021 (2022-04-30)

CVE: 44

Reporte sobre las vulnerabilidades más explotadas por operadores de Ransomware durante todo el 2021.

AMENAZAS

Lapsus$ (2022-04-29)

IPv4: 3 **URL:** 1 **Domain:** 1

Tácticas recientes de Lapsus$

Más información en *Killing The Bear*