JORGE TESTA
Ciberseguridad

KILLING THE БЗАЯ

Malware y Cibercrimen organizado

GitBook

2022-05-03

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

Índice de Contenidos

MALWARE

NJRat (2022-05-02)

FileHash-MD5: 1 | FileHash-SHA1: 1 | FileHash-SHA256: 1

Mirai (2022-05-02)

FileHash-MD5: 7 | FileHash-SHA1: 7 | FileHash-SHA256: 7

CAMPAÑAS

RIG Exploit Kit Redline

CVE: 1 | FileHash-MD5: 3 | IPv4: 2 | URL: 3 | Domain: 5 | Artículos: 3

Researchers have discovered a new malicious campaign that exploits an Internet Explorer vulnerability and deploys RedLine.

Campaign "Silent Chollima - Spying Operation" (2022-04-27)

CVE: 1 | FileHash-MD5: 4 | FileHash-SHA1: 4 | FileHash-SHA256: 28 | URL: 6 | Domain: 5

Espionage group focuses on obtaining classified or sensitive intellectual property that has civilian and military applications.

VULNERABILIDADES

Vulnerabilities linked to Mirai IoT (2022-01-25)

CVE: 13

https://intel471.com/blog/iot-cybersecurity-threats-mirai-botnet

Vulnerability linked to Enemybot (2022-04-13)

CVE: 1

https://www.evernote.com/shard/s724/sh/71c7f804-132c-4651-88a6-8e1d20f47ecf/9c04109edd8bcb76474f292c735e32d5

Vulnerabilities Cisco "Accusoft ImageGear" (2022-05-02)

CVE: 2

Vulnerabilities Daily (2022-05-03)

CVE: 6

Linux Kernel, D-LINK e IBM ICP4A

Vulnerabilities Cisa Summary Apr 25th (2022-05-03)

CVE: 328

AMENAZAS

Killing The Bear - Grupo emergente “Keksec”

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

Keksec está usando el malware EnemyBot y vulnerabilidades de vendedores como Seowon Intech y D-Link