LevelBlue - Open Threat Exchange

By CyberHunter_NL

Archived: 2026-04-05 17:57:03 UTC

- 841 Subscribers

- 49 Subscribers

- 841 Subscribers

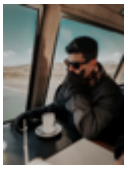
RansomEXX

CVE: 6 | **FileHash-MD5:** 13 | **FileHash-SHA1:** 13 | **FileHash-SHA256:** 22 | **URL:** 4 | **Domain:** 2 | **Hostname:** 3

The full text of the key characters for the TSPY-Trojan malware, which has now been identified as the "backdoor", can be seen here: Â£1.

- 354 Subscribers

- 72 Subscribers



RansomExx Renner

RansomExx is a ransomware family that targeted multiple companies starting in mid-2020. It shares commonalities with Defray777.

- 72 Subscribers

- 7 Subscribers

- 3 Subscribers

GoldMax

The full list ofSHA-256 and GoldFInder

- 130 Subscribers

- 431 Subscribers

HYPERVISOR JACKPOTTING: ANONYMOUS TARGETS ON ESXI SERVER WITH RANSOMWARE

SPRITE SPIDER is an eCrime actor that conducts low-volume Big Game Hunting ransomware campaigns using the Defray777 ransomware. Other tools used by SPRITE SPIDER include the Vatet loader and the PyXie remote access tool (RAT). The adversary has established initial access by exploiting vulnerable Citrix Application Delivery Controllers, as well as by using LUNAR SPIDER's BokBot trojan. To avoid detection, SPRITE SPIDER often stages payloads on internal servers within a victim network and uses in-memory-only deployments of its later-stage tooling. SPRITE SPIDER uses both PyXie and Cobalt Strike to move laterally within a victim environment after obtaining initial access.

- 250 Subscribers

New Ransomware Tactic: Adversaries Target ESXi Servers

FileHash-MD5: 2 | **FileHash-SHA1:** 2 | **FileHash-SHA256:** 2

Targeted large-scale ransomware campaigns, referred to as big game hunting (BGH), remained the primary eCrime threat to organizations across all sectors in 2020. The relentless volume and pace of these campaigns mean that some sophisticated BGH actors have not attracted much attention. While ransomware for Linux has existed for many years, BGH actors have not historically targeted Linux, much less the ESXi hypervisor specifically. This likely reflects the overwhelming dominance of the Windows operating system in businesses and large

organizations. However, in the second half of 2020, SPRITE SPIDER and CARBON SPIDER began deploying Linux versions of Defray777 and Darkside, respectively, designed specifically to affect ESXi.

- 373,955 Subscribers

- 551 Subscribers

[When Threat Actors Fly Under the Radar: Vatet, PyXie, and Defray777]

FileHash-MD5: 42 | **FileHash-SHA1:** 42 | **FileHash-SHA256:** 72 | **Domain:** 12 | **Hostname:** 1

We first noticed that there may be a relationship between the Vatet loader, PyXie Remote Access Tool (RAT) and Defray777 ransomware when there were remnants and/or detections of all three in various Incident Response and Managed Threat Hunting engagements. After digging deep into each malware family, it became apparent that Vatet, PyXie and Defray777 are all associated with the same financially motivated threat group that has been operating since as early as 2018. That threat group, sometimes referred to as PyXie by BlackBerry Cylance and

GOLD DUPONT by SecureWorks, has been actively conducting successful ransomware operations that have impacted organizations in a number of sectors including healthcare, education, government and technology while remaining under the radar.

- 373,955 Subscribers

- 1,344 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:defray777