PyXie (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-02 10:39:13 UTC

PyXie

aka: PyXie RAT

Full-featured Python RAT compiled into an executable.

PyXie RAT functionality includes:
* Man-in-the-middle (MITM) Interception
* Web-injects
* Keylogging
* Credential harvesting
* Network Scanning
* Cookie theft
* Clearing logs
* Recording video
* Running arbitrary payloads
* Monitoring USB drives and exfiltrating data
* WebDav server
* Socks5 proxy
* Virtual Network Connection (VNC)
* Certificate theft
* Inventorying software
* Enumerating the domain with Sharphound

References

2022-05-17 · Trend Micro ·
Ransomware Spotlight: RansomEXX
LaZagne Cobalt Strike IcedID MimiKatz PyXie RansomEXX TrickBot

2022-05-03 · Cluster25 · Cluster25
The Strange Link Between A Destructive Malware And A Ransomware-Gang Linked Custom Loader: IsaacWiper Vs Vatet
Cobalt Strike IsaacWiper PyXie

2021-11-01 · FBI · FBI

PIN Number 20211101-001: Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims

DarkSide RansomEXX DarkSide PyXie RansomEXX

2021-02-26 · CrowdStrike · Eric Loui, Sergei Frankoff

Hypervisor Jackpotting: CARBON SPIDER and SPRITE SPIDER Target ESXi Servers With Ransomware to Maximize Impact

DarkSide RansomEXX Griffon Carbanak Cobalt Strike DarkSide IcedID MimiKatz PyXie RansomEXX REvil

2021-02-23 · CrowdStrike · CrowdStrike

2021 Global Threat Report

RansomEXX Amadey Anchor Avaddon BazarBackdoor Clop Cobalt Strike Conti Cutwail DanaBot DarkSide DoppelPaymer Dridex Egregor Emotet Hakbit IcedID JSOutProx KerrDown LockBit Mailto Maze MedusaLocker Mespinoza Mount Locker NedDnLoader Nemty Pay2Key PlugX Pushdo PwndLocker PyXie QakBot Quasar RAT RagnarLocker Ragnarok RansomEXX REvil Ryuk Sekhmet ShadowPad SmokeLoader Snake SUNBURST SunCrypt TEARDROP TrickBot WastedLocker Winnti Zloader Evilnum OUTLAW SPIDER RIDDLE SPIDER SOLAR SPIDER VIKING SPIDER

2021-02-02 · · CRONUP · Germán Fernández

De ataque con Malware a incidente de Ransomware

Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DanaBot Dharma Dridex Egregor Emotet Empire Downloader FriedEx GootKit IcedID MegaCortex Nemty Phorpiex PwndLocker PyXie QakBot RansomEXX REvil Ryuk SDBbot SmokeLoader TrickBot Zloader

2020-11-06 · Palo Alto Networks Unit 42 · CRYPSIS, Drew Schmitt, Ryan Tracey

Next Up: “PyXie Lite”

Defray PyXie

2020-11-06 · Palo Alto Networks Unit 42 · CRYPSIS, Drew Schmitt, Ryan Tracey

Linking Vatet, PyXie and Defray777

PyXie RansomEXX

2020-11-06 · Palo Alto Networks Unit 42 · CRYPSIS, Drew Schmitt, Ryan Tracey

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

PyXie RansomEXX

2020-11-06 · Palo Alto Networks Unit 42 · CRYPSIS, Drew Schmitt, Ryan Tracey

Last, but Not Least: Defray777

PyXie RansomEXX

2020-11-06 · Palo Alto Networks Unit 42 · CRYPSIS, Drew Schmitt, Ryan Tracey

Indicators of Compromise related to Cobaltstrike, PyXie Lite, Vatet and Defray777

Cobalt Strike PyXie RansomEXX

2020-01-01 · Secureworks · SecureWorks

GOLD DUPONT

Cobalt Strike Defray PyXie GOLD DUPONT

2019-12-02 · Cylance · Ryan Tracey

Meet PyXie: A Nefarious New Python RAT

PyXie

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.pyxie