LevelBlue - Open Threat Exchange

By PetrP.73

Archived: 2026-04-05 19:46:04 UTC

- 161 Subscribers

Author Url

Oz Batch: 50 IOCs (avg BDE: 85)

FileHash-MD5: 1 | **FileHash-SHA256:** 1 | **Domain:** 1 | **Hostname:** 10

OTX Pulse Description: Cobalt Infrastructure Detection Our latest findings indicate a notable collection of indicators associated with the Cobalt threat actor, encompassing 50 IOCs including IPs, domains, SHA256, and MD5 hashes. This infrastructure is linked to various C2 frameworks such as ValleyRAT, Mirai, ClearFake, and Cobalt Strike, with an average BDE (Big Data analytics Energy) Score of 85, highlighting its malicious potency. Security teams should prioritize monitoring for these indicators and implement defenses against techniques outlined in the MITRE ATT&CK framework, including T1071 (Application Layer Protocol) and T1203 (Exploitation for Client Execution). Detection timestamp: [insert timestamp here].

- 152 Subscribers

Author Url

ThreatFox Hunt: Cobalt Strike IOCs - 2026-02-16

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

Automated ThreatFox hunt for Cobalt Strike indicators. 114 IOCs collected via Pattern 49 intelligence streaming. MITRE ATT&CK: T1071.001, T1059.001, T1055, T1105, T1027. Reference: https://analytics.dugganusa.com

- 152 Subscribers

Author Url

ThreatFox Hunt: Cobalt Strike IOCs - 2026-02-16

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

Automated ThreatFox hunt for Cobalt Strike indicators. 116 IOCs collected via Pattern 49 intelligence streaming. MITRE ATT&CK: T1071.001, T1059.001, T1055, T1105, T1027. Reference: https://analytics.dugganusa.com

- 152 Subscribers

Author Url

Oz Batch: 50 IOCs (avg BDE: 85)

Hostname: 10

Pulse Description: This pulse identifies 50 indicators consisting of IPs and domains associated with known Cobalt infrastructure, leveraging multiple command-and-control (C2) frameworks such as ValleyRAT, ClearFake, Mirai, Sliver, DeimosC2, and Cobalt Strike. The average Behavioral Detection Energy (BDE) Score is 85, indicating a significant threat level. Given the attribution to the Cobalt adversary, security teams should prioritize monitoring for these indicators and consider implementing defensive measures aligned with MITRE ATT&CK techniques like T1071 (Application Layer Protocol) and T1203 (Exploitation for Client Execution). BDE (Big Data analytics Energy) Score: 85. Detection Timestamp: [Insert Timestamp Here].

- 152 Subscribers

- 35 Subscribers

Author Url

Oz Batch: 36 IOCs (avg BDE: 85)

Hostname: 5

Pulse Description: This finding highlights 36 indicators, including domains, IPs, and URLs associated with Cobalt infrastructure, leveraging sophisticated C2 frameworks such as ClearFake, Sliver, and Cobalt Strike. The average BDE score of 85 indicates high-risk activity. Given the attribution to the Cobalt adversary, organizations should monitor for these signatures and consider implementing defensive measures against MITRE ATT&CK techniques like Credential Dumping (T1003) and Remote Access Tools (T1219). BDE (Big Data analytics Energy) Score: 85, detected on [current timestamp].

- 152 Subscribers

 Author Url

Oz Batch: 50 IOCs (avg BDE: 85)

FileHash-MD5: 1 | **FileHash-SHA256:** 1 | **Hostname:** 9

Pulse Description: Cobalt Infrastructure Detection This pulse identifies 50 indicators associated with Cobalt infrastructure, including domains, IPs, and hashes linked to various C2 frameworks such as ClearFake, ValleyRAT, and Cobalt Strike. The average BDE (Big Data analytics Energy) Score is 85, indicating a high threat level. Notable MITRE ATT&CK techniques include Tactics related to Remote Access Tools (RATs) and C2 communications. Given the adversarial attribution to Cobalt, security teams should prioritize monitoring and blocking these indicators to mitigate potential threats. Detection timestamp: [insert timestamp]. BDE Score: 85.

- 152 Subscribers

 Author Url

ThreatFox Hunt: Cobalt Strike IOCs - 2026-02-16

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

Automated ThreatFox hunt for Cobalt Strike indicators. 120 IOCs collected via Pattern 49 intelligence streaming. MITRE ATT&CK: T1071.001, T1059.001, T1055, T1105, T1027. Reference: https://analytics.dugganusa.com

- 152 Subscribers

 Author Url

ThreatFox Hunt: Cobalt Strike IOCs - 2026-02-16

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

Automated ThreatFox hunt for Cobalt Strike indicators. 120 IOCs collected via Pattern 49 intelligence streaming. MITRE ATT&CK: T1071.001, T1059.001, T1055, T1105, T1027. Reference: https://analytics.dugganusa.com

- 152 Subscribers

Author Url

ThreatFox Hunt: Cobalt Strike IOCs - 2026-02-16

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

Automated ThreatFox hunt for Cobalt Strike indicators. 120 IOCs collected via Pattern 49 intelligence streaming. MITRE ATT&CK: T1071.001, T1059.001, T1055, T1105, T1027. Reference: https://analytics.dugganusa.com

- 152 Subscribers

Author Url

ThreatFox Hunt: Cobalt Strike IOCs - 2026-02-16

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

Automated ThreatFox hunt for Cobalt Strike indicators. 120 IOCs collected via Pattern 49 intelligence streaming. MITRE ATT&CK: T1071.001, T1059.001, T1055, T1105, T1027. Reference: https://analytics.dugganusa.com

- 152 Subscribers

Author Url

ThreatFox Hunt: Cobalt Strike IOCs - 2026-02-16

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

Automated ThreatFox hunt for Cobalt Strike indicators. 120 IOCs collected via Pattern 49 intelligence streaming. MITRE ATT&CK: T1071.001, T1059.001, T1055, T1105, T1027. Reference: https://analytics.dugganusa.com

- 152 Subscribers

Author Url

Oz Batch: 50 IOCs (avg BDE: 85)

FileHash-MD5: 1 | **FileHash-SHA256:** 1 | **Hostname:** 9

OTX Pulse Description: Cobalt Infrastructure Detection We have identified a significant collection of indicators associated with Cobalt infrastructure, including 50 distinct IOCs such as domains and IPs utilized by various C2 frameworks including ClearFake, ValleyRAT, and Cobalt Strike. The average BDE (Big Data analytics Energy) Score for these indicators is 85, indicating a high level of threat potency. This attribution to the Cobalt adversary aligns with known tactics, techniques, and procedures (TTPs) documented under MITRE ATT&CK, particularly T1071.001 (Application Layer Protocol: Web Protocols). Detection Timestamp: [Insert timestamp here].

- 152 Subscribers

Oz Batch: 50 IOCs (avg BDE: 85)

FileHash-MD5: 1 | **FileHash-SHA256:** 1 | **Hostname:** 9

OTX Pulse Description: Cobalt Infrastructure Detection This pulse identifies a significant Cobalt infrastructure with 50 associated indicators, encompassing domains, IPs, SHA256, and MD5 hashes. The detected command and control (C2) frameworks include notable variants such as ClearFake, ValleyRAT, and Cobalt Strike, suggesting coordinated malicious activities. The adversary linked to these indicators is attributed to Cobalt, a known threat actor with a record of sophisticated cyber operations. BDE (Big Data analytics Energy) Score: 85, Detection Timestamp: [Insert Timestamp Here].

- 152 Subscribers

Oz Batch: 50 IOCs (avg BDE: 85)

FileHash-MD5: 1 | **FileHash-SHA256:** 1 | **Hostname:** 9

Pulse Description: This finding reveals a total of 50 indicators associated with Cobalt infrastructure, including domains, IPs, and hashes (MD5, SHA256). The indicators are linked to various C2 frameworks such as ClearFake, ValleyRAT, and Cobalt Strike, indicating a sophisticated adversary actively deploying malware. Notably, the average BDE (Big Data analytics Energy) Score is 85, highlighting the potential threat level of this infrastructure. Detection Timestamp: [Insert Timestamp Here]

- 152 Subscribers

Oz Batch: 50 IOCs (avg BDE: 85)

FileHash-MD5: 3 | **FileHash-SHA256:** 3 | **Domain:** 8 | **Hostname:** 11

Pulse Description: Cobalt Infrastructure Detection This pulse identifies 50 indicators linked to the Cobalt adversary, including SHA256 and MD5 hashes, IP addresses, and domains associated with various C2 frameworks such as SystemBC, XWorm, Remcos, and Cobalt Strike. The high average BDE Score of 85 indicates significant threat potential. Security teams should investigate these indicators to mitigate risks associated with known techniques from the MITRE ATT&CK framework, particularly T1071.001 (Application Layer Protocol). **BDE (Big Data analytics Energy) Score: 85** **Detection Timestamp: [insert timestamp]**

- 152 Subscribers

OSINT Volley 2026-02-15 - Cobalt Strike/Vidar/ClearFake

URL: 52 | **Domain:** 17 | **Hostname:** 49

Automated OSINT sweep from ThreatFox. Top malware: Cobalt Strike(107), Vidar(78), ClearFake(66), AsyncRAT(45), Unknown malware(42). Source: abuse.ch ThreatFox API. SSL enriched: 33 IPs with HTTPS, 28 self-signed (C2 candidates). Pattern 54: sweep→volley automation.

- 152 Subscribers

ThreatFox Hunt: Cobalt Strike IOCs - 2026-02-15

FileHash-MD5: 2 | **FileHash-SHA256:** 2 | **Hostname:** 3

Automated ThreatFox hunt for Cobalt Strike indicators. 125 IOCs collected via Pattern 49 intelligence streaming. MITRE ATT&CK: T1071.001, T1059.001, T1055, T1105, T1027. Reference: https://analytics.dugganusa.com

- 152 Subscribers

OSINT Volley 2026-02-15 - Cobalt Strike/Vidar/ClearFake

URL: 51 | **Domain:** 17 | **Hostname:** 48

Automated OSINT sweep from ThreatFox. Top malware: Cobalt Strike(107), Vidar(78), ClearFake(66), AsyncRAT(45), Unknown malware(40). Source: abuse.ch ThreatFox API. SSL enriched: 36 IPs with HTTPS, 29 self-signed (C2 candidates). Pattern 54: sweep→volley automation.

- 152 Subscribers
