Cyber Threat Intelligence Report

Event: GRAPH-VT-20250518-01

Generated on: Sun, 13 Jul 2025 14:36:27 GMT

Castle Bravo Project
Open Code. Open Defense. Open Future.

1. Executive Summary

This MISP report, 'GRAPH-VT-20250518-01', reveals a highly active and distributed malware campaign. The threat landscape is characterized by multiple seemingly legitimate or compromised domains (e.g., 'forensics.umass.edu', 'secure.icaccops.com', 'secure.ep2p.us', 'cps.gridcop.com', 'feeble-industries.com') serving as command-and-control (C2) infrastructure or malware distribution points. These domains are associated with a significant number of unique IP addresses and a large volume of distinct file hashes, indicating a broad and potentially polymorphic malware family or multiple concurrent campaigns. The use of an educational domain ('forensics.umass.edu') suggests a possible compromise, which could be leveraged for increased credibility in phishing or other initial access vectors. The sheer scale of unique file hashes points to an adversary actively developing or acquiring new malware variants to evade detection. The potential threat level is assessed as Critical due to the extensive and resilient infrastructure, the high volume of associated malware samples, and the likely intent for widespread compromise. Security operations teams should immediately implement blocking rules for all identified domains and IP addresses at network perimeter defenses (firewalls, DNS filters, proxies). All associated file hashes must be deployed to endpoint detection and response (EDR) and antivirus solutions for proactive detection and prevention. Furthermore, a thorough threat hunt should be conducted across the environment to identify any historical or ongoing communications with these indicators and the presence of any of the associated malware files. Enhance user awareness training, particularly regarding phishing attempts that might leverage seemingly legitimate domains. All identified Indicators of Compromise (IOCs) should be shared with trusted threat intelligence partners.

2. Actionable Recommendations

Here are the specific, actionable recommendations for the next steps in the investigation:

*   **Network Forensics:**
    *   Immediately implement blocking rules for all identified domains (`forensics.umass.edu`, `secure.icaccops.com`, `secure.ep2p.us`, `cps.gridcop.com`, `feeble-industries.com`) and IP addresses (`128.119.240.95`, `50.229.189.110`) at network perimeter defenses (firewalls, DNS filters, proxies).
    *   Review firewall, proxy, and DNS logs for any historical or ongoing connections to the identified domains and IP addresses, extending the search window as far back as log retention allows.
    *   Analyze NetFlow or equivalent flow data for connections to/from these IPs and domains to identify potentially compromised internal systems or data exfiltration.

*   **Host-Based Analysis:**
    *   Deploy all provided file hashes (`fc0beb87553541eeb072...`, `04531596d3958b3a2f19...`, etc.) to EDR and antivirus solutions for proactive detection and prevention across all endpoints.
    *   Conduct a comprehensive threat hunt across all endpoints using EDR to search for the presence of any of the identified file hashes.
    *   For any systems found with the malware, collect forensic images, analyze process execution logs, registry changes, and persistence mechanisms.
    *   Examine system logs (e.g., Windows Event Logs, Sysmon) on potentially affected hosts for suspicious activities, such as unusual process creations, network connections, or privilege escalation attempts.

*   **Intelligence & Threat Hunting:**
    *   Perform WHOIS lookups and passive DNS queries on all identified domains and IP addresses to uncover additional associated infrastructure, historical records, and potential related entities (e.g., shared registrars, name servers, ASNs).
    *   Leverage external threat intelligence platforms (e.g., VirusTotal, Any.Run, OSINT tools) to pivot on the identified IOCs (domains, IPs, file hashes) to discover new malware variants, C2 patterns, and TTPs associated with this campaign.
    *   If malware samples are acquired, perform static and dynamic analysis to understand their functionality, C2 communication protocols, and any embedded IOCs.
    *   Share all identified Indicators of Compromise (IOCs) and findings with trusted threat intelligence partners and relevant sector-specific ISACs/ISAOs to contribute to collective defense.

3. Attack Timeline (Key Indicators)

1 **DOMAIN**
`forensics.umass.edu`

2 **DOMAIN**
`secure.icaccops.com`

3 **DOMAIN**
`secure.ep2p.us`

4 **DOMAIN**
`cps.gridcop.com`

5 **DOMAIN**
`feeble-industries.com`

6 **IP**
`128.119.240.95`

7 **IP**
`173.163.5.2`

8 **FILE**
`fc0beb87553541eeb072...4fe0a36fcc20639`

9 **FILE**
`3641cb93bf203ece865d...fc0234b2f1f51b5`

10 **FILE**
`c6acf614726fc8ee98ba...c4841325ac6e48b`

11 **FILE**
`de3f1c7ecd5d93ae1ab5...ec66d4a1514c112`

4. ATT&CK® Kill Chain

INITIAL ACCESS

Phishing

T1566

JUSTIFICATION

Multiple domains are observed delivering distinct malicious files, strongly indicating the use of phishing campaigns to gain initial access. These domains likely serve as distribution points for malware delivered via email or malicious links.

EVIDENCE

- forensics.umass.edu
- fc0beb87553541eeb072...4fe0a…
- secure.icaccops.com
- 3641cb93bf203ece865d...fc023…
- secure.ep2p.us
- c6acf614726fc8ee98ba...c4841…
- cps.gridcop.com
- de3f1c7ecd5d93ae1ab5...ec66d…

COMMAND AND CONTROL

Standard Application Layer Prot…

T1071.001

JUSTIFICATION

The observed relationships between multiple domains and IP addresses, along with domains hosting files, suggest the use of standard web protocols (HTTP/HTTPS) for command and control communication or malware delivery.

EVIDENCE

- forensics.umass.edu
- 128.119.240.95
- secure.icaccops.com
- 173.163.5.2
- feeble-industries.com
- secure.ep2p.us
- cps.gridcop.com

RESOURCE DEVELOPMENT

Acquire Infrastructure: Domains

T1583.001

JUSTIFICATION

The adversary acquired or compromised multiple distinct domains to support their malicious operations, including malware delivery and command and control.

EVIDENCE

- forensics.umass.edu
- secure.icaccops.com
- secure.ep2p.us
- cps.gridcop.com
- feeble-industries.com

RESOURCE DEVELOPMENT

Acquire Infrastructure: Virtual Pr…

T1583.003

JUSTIFICATION

The use of multiple IP addresses as hosting infrastructure for malicious domains suggests the acquisition of virtual private servers or similar hosting services by the adversary.

EVIDENCE

- 128.119.240.95
- 173.163.5.2

RESOURCE DEVELOPMENT

Develop Capabilities: Malware

T1587.001

JUSTIFICATION

The presence of four distinct file hashes, linked to various malicious domains, indicates that the adversary developed or acquired multiple malware samples for their campaigns.

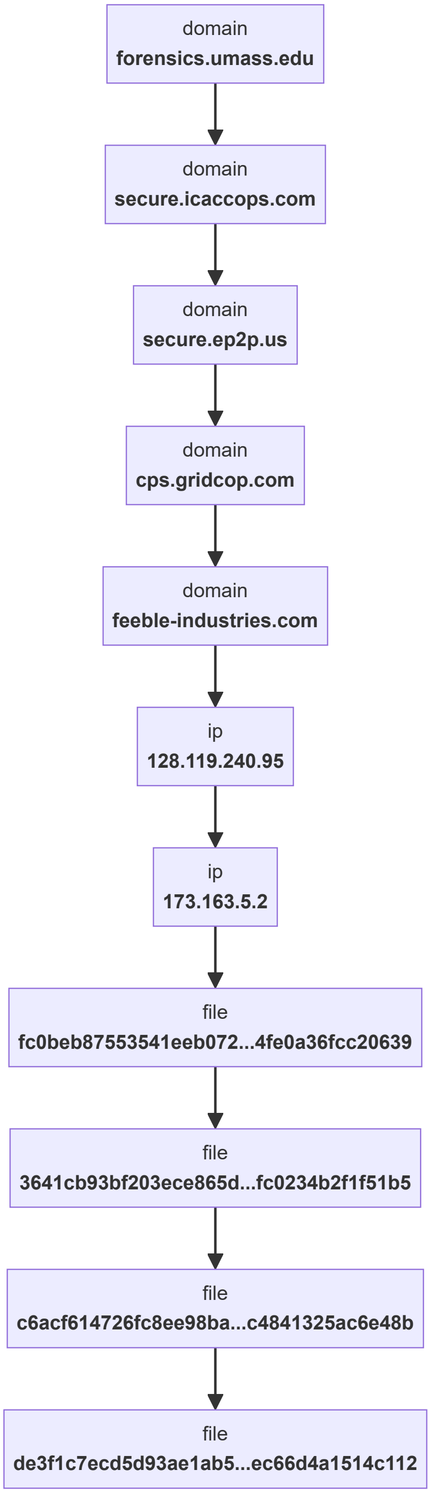
EVIDENCE

- fc0beb87553541eeb072...4fe0a…
- 3641cb93bf203ece865d...fc023…
- c6acf614726fc8ee98ba...c4841…
- de3f1c7ecd5d93ae1ab5...ec66d…

5. MITRE ATT&CK® Matrix Overview

Reconnaissa e	Resource Developme	Initial Acce	Execution	Persistenc	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command a Control	Exfiltratio	Impact
	Acquire Infrastructure Domains Acquire Infrastructure Virtual Privat Server Develop Capabilities: Malware	Phishing									Standard Application Layer Protoc Web Protoco		

6. Attack Flow Diagram



7. Detailed TTP Analysis

Initial Access

TA0001

Phishing (T1566)

Multiple domains are observed delivering distinct malicious files, strongly indicating the use of phishing campaigns to gain initial access. These domains likely serve as distribution points for malware delivered via email or malicious links.

RELATED INDICATORS:

- 🌐 `forensics.umass.edu`
- 📄 `fc0beb87553541eeb072...4fe0a36fcc20639`
- 🌐 `secure.icaccops.com`
- 📄 `3641cb93bf203ece865d...fc0234b2f1f51b5`
- 🌐 `secure.ep2p.us`
- 📄 `c6acf614726fc8ee98ba...c4841325ac6e48b`
- 🌐 `cps.gridcop.com`
- 📄 `de3f1c7ecd5d93ae1ab5...ec66d4a1514c112`

Command and Control

TA0011

Standard Application Layer Protocol: Web Protocols (T1071.001)

The observed relationships between multiple domains and IP addresses, along with domains hosting files, suggest the use of standard web protocols (HTTP/HTTPS) for command and control communication or malware delivery.

RELATED INDICATORS:

- 🌐 `forensics.umass.edu`
- 🗄 `128.119.240.95`
- 🌐 `secure.icaccops.com`
- 🗄 `173.163.5.2`
- 🌐 `feeble-industries.com`
- 🌐 `secure.ep2p.us`
- 🌐 `cps.gridcop.com`

Resource Development

TA0042

Acquire Infrastructure: Domains (T1583.001)

The adversary acquired or compromised multiple distinct domains to support their malicious operations, including malware delivery and command and control.

RELATED INDICATORS:

- forensics.umass.edu
- secure.icaccops.com
- secure.ep2p.us
- cps.gridcop.com
- feeble-industries.com

Acquire Infrastructure: Virtual Private Server (T1583.003)

The use of multiple IP addresses as hosting infrastructure for malicious domains suggests the acquisition of virtual private servers or similar hosting services by the adversary.

RELATED INDICATORS:

- 128.119.240.95
- 173.163.5.2

Develop Capabilities: Malware (T1587.001)

The presence of four distinct file hashes, linked to various malicious domains, indicates that the adversary developed or acquired multiple malware samples for their campaigns.

RELATED INDICATORS:

- fc0beb87553541eeb072...4fe0a36fcc20639
- 3641cb93bf203ece865d...fc0234b2f1f51b5
- c6acf614726fc8ee98ba...c4841325ac6e48b
- de3f1c7ecd5d93ae1ab5...ec66d4a1514c112

Appendix

A.1 YARA Detection Rule ▼

```
import "hash"

rule Threat_Intel_Report_Rule {
    meta:
        description = "Detects files based on known malicious SHA256 hashes from a threat intelligence report."
        author = "Castle Bravo Project - Threat Intel Visualizer AI"
        date = "2025-07-13"

    strings:
        // The provided "filenames" are SHA256 hashes, and the "file hashes" are also SHA256 hashes.
        // For hash-based indicators of compromise, the most effective and standard YARA practice
        // is to calculate the hash of the scanned file and compare it against a list of known hashes.
        // This is achieved using the 'hash' module in the 'condition' section, rather than
        // attempting to find the hash string literally within the file content.
        // Therefore, this 'strings' section remains empty as per best practice for hash IOCs.

    condition:
        hash.sha256() in (
            "fc0beb87553541eeb072be57b96ec23ca46f4029975c597264fe0a36fcc20639",
            "04531596d3958b3a2f19eb05cf70a77c01427600369399d32c31fc10abd007e7",
            "277041078227413c4ae988dff6dc42e06abd9dfb51de47aef61432a08df1e610",
            "abc21e3c1f90a895b76e3b1c562600d4b113ab936ddae20689960ca84be07630",
            "77b0f741b1f7699c1e2c51eb7eb17c3d59dffe9f92ac40f325d298faa7c46229",
            "24459dd44143242d1ae2b7eb6e154b15170aba46d88dc6f6af82605ab21cbf57",
            "418de3fa8226cca095773920b2f9d0805de9eb8238b33d03dd71d282c1affc4b",
            "0a59acc5d026063b92032934d1c1b70b38307180ddff69f6dba45a6f7e7c0b03",
            "bb01ab5516793ed7ba6c4d0b3effc99569aed9adc8ad6fdf52f123776a066a4f",
            "df3ec414793491ce27c8dd3a918c4655b7db1cee67025482b0ed7ad286d22080",
            "3641cb93bf203ece865d02aa480a829a798ea86c0ff5dd51cfc0234b2f1f51b5",
            "a31cfca5ba78bca99b8731f196e330af5ce1ecf71b5fa021a89f027a3f5450b7",
            "0a6d8d01d00d7aecbe9b3a341f55521e4a6162272e82ca8f48d146686476e187",
            "35d6842856228adb7e8badcc12d035d17b12b17d14988b96e45c9d40a690b550",
            "90506161ed789251b13d8e8988ba02ac4218fcc1ff0cc8e2644e46b0dd0066cc",
            "017539edeeea6e318309307f640d06d56d59690733379ad2b00919f6cb9ad12a",
            "8086a04737e66df563fb4ca440f67d22103b22ec601c30a1009159dc67bb8982",
            "1366bef60db01f78949d3dfd150e0d696cc26ecf25248aab3b89ff6129535613",
            "9f6506cfc2cc321db15a2cc8d29653a9eae6754e05ac790e524d54628def646a",
            "bf1af55c81a02923b55fc1fad124bc5b086097d5e7bdcec7a5f3d0bca12f3540",
            "538d53a975285187a7f7067159c1c44b4943d02d57f4d00c40279c2347968209",
            "3998bc4e6956bd365191ea0093b34d8b55947a8854ccfa0f40ff7c752cd52228",
            "157b0edd9592722d33e332d51d49f50629c96ea05f501d42a26e77cc8eed666d",
            "5adc04667336657d221cc4ddb500b0bf794ff1e640ff190bc7ebbc13e1871fb8",
            "411a77b393dfe96312653819f831e7e52f5c5b5bee04775f8b8d1e60d1d42815",
            "c6acf614726fc8ee98bac5c0b5bd83b0bb529bc9d0afd3ecac4841325ac6e48b",
            "0c2be51a259f206a0ec68c7fc65cbac2a7cadcd7e1a8bb5e1bad9ae7f8f2baed",
            "c14201d7706da3ad1efdb99e799ee2809936fd20484be5b924a6a9a1dd87537c",
            "a5706d8f621b337f212b7007a26a145d8601faf92e386e8cd79b25a2c4bb6582",
            "8693b5f9f91a1d86f46939163326e3db4bb210de4f2b20a7582cffe40f5cdc82",
            "b0e7cc4aef2bf48bf9c76a3b4c28978818a97094c20c820e6478a9e63b000a74",
            "f6f46cae6b70af0119a528ce5719622afbda3cfaa481985e45baea1dd04138d8",
            "de3f1c7ecd5d93ae1ab5ec0f6284b8ffe910f75bf0d82a183ec66d4a1514c112",
            "d1b8429fabed6e134d4f010d2c0a7361b73f2225f496918a97f39dcf0d45151a",
            "8f712a9625b2700c6cb8a34e34167a4961cc9efa0d6c88be2a5ea9ec9fb5f6f8",
            "7e093bcc6615679be2fcc5aa8d4c2116ebf0c78fbf710ee86ea0ef233d90fe9a",
            "acc5949dbe7e4e9e383b8d9c23037a5ab5cacb1ae692c8660d496259a5e896b5",
            "64e3cf0324fbe4cc6caaffac3dfe874493182401e20ee51f5847c05dcab88158",
            "afb7207f4a4f1b045fa096ce621c1125e5c65fef50989293f66abaef3df3196f",
            "e4481f6741ebe1005e43459038b5297dd93aadf35352b182204f4b99ee2567a1",
            "52001718f01fba1778d5f857d7202805552de21fb74ccd05393d2a2b93d3b720",
            "51567e8f9b17dcc8160804b3f93847e0f4b4d1cca8a9e8a5184ebdb20423feda",
            "f7ba75d81fae7ef77b06dfa6001ac3ecbf29635510ee01b246a6b087e6449b76",
            "0d1c9bcbda71dc3306fd3bc59ccf7e1160ef156bfa0ff8efc9de6e1843e0b200",
            "6e52e8d38679bd2f28b203666d6d3fe222d40be4836315f112ffad83bf42fd88",
            "ea246121345a6a19fa3980cd57ccf555f1e941e509f5b25c4a0083bf664943db",
            "c92a9760bc4464f59881b19543e352bb6657a27c93c1fa81586c1ec60163b697",
            "633fd3662df3a254a9fdf0dcf5e637e41ff96b0c8cb127a1dde3c16f6a1231ac",
            "7a7af6f08cbf13e3da2f9e3fbbdcef317651867a27e8082dbf9ba14826ef112e",
            "37751817558ae91e6473c2faf5b2c62505c1241bd4b08f4981963850efd77f26",
            "29db1a047802158781c02d6000d94c0c45b6ef831f1dc13e85bae05c42c43aa6",
            "0333732b7253a5970829782c9d4effa1364e295208f2cf09f832cc79fcaa87d4",
            "26f606a3396b0fb971dc88d9da2240f8c65e6f10b97e11d397c093d3ffe158d9",
            "367246f60eaf19f38ea0ebb3052778f27f2a38c46fa9388059c66fd560ee7aee",
            "51e7e9d824e8630a62df6be85e8b9415fcaa5b6e526859e5879685d97350c228",
            "5650791e31627fdda21e9711e76972df44f9b0f28d95d3c50bff06d881ac5421",
            "674f5a69c30e8e202148673c97bee8db721e637f8cb8ebb0cfe09ed02f17b897",
            "70abb222cab3e3a5faf7b61bf33a4976f9706ba77e828165fcd1792529958c5c",
            "71146cb7d745b03eadf5f123fdb9e1db8381d7cb7a91df5482845ea0a1267f12",
            "a34fb073e7b63394df2614cd34b6b4eca47edad7b759ae8e3d6dec7b4fe66992",
            "af04f732878c60308c1246e664c0277daefc40a585da1380b6a69a69c6345d3f",
            "c1ba165b90825a7a15662585d14bf0f548eecba11decf7c27ce039009c583900",
            "d0bf77a8310afe1be68239ee7d8cf3d51922b430f8fad8f002207c5d3cc1bd0c",
            "d1b979b121d86b1fbee23cbaf55161feef9edd18e181659e75bf93de27f7fbed",
            "da003e3c1ee98d983502654c17d3a7fdc364520f55ffa30a41c6847aa634cae5",
            "e82d326cfc5e273804887e8a246c4f1d06ab2c42f9b4e79c23cf03c97185854d",
            "ef7a46e8f8472c4b45d409003924360257f74842ebd11fc9bd10a1f364cf28dc",
            "f0988cb5cde328d71f98f3c8da43aac5eae3939448c3319ede9045e55966b30d",
            "f868b1bf5ca0661db466dc31cfcb2a597fc8db24d942ad64410000198921c6d7"
        )
}
```

A.2 All Indicators of Compromise (IOCs)

INDICATOR VALUE	TYPE
forensics.umass.edu	Domain
128.119.240.95	Ip
fc0beb87553541eeb072...4fe0a36fcc20639	File
04531596d3958b3a2f19...c31fc10abd007e7	File
277041078227413c4ae9...61432a08df1e610	File
abc21e3c1f90a895b76e...9960ca84be07630	File
77b0f741b1f7699c1e2c...5d298faa7c46229	File

INDICATOR VALUE	TYPE
24459dd44143242d1ae2...f82605ab21cbf57	File
418de3fa8226cca09577...d71d282c1affc4b	File
0a59acc5d026063b9203...ba45a6f7e7c0b03	File
bb01ab5516793ed7ba6c...2f123776a066a4f	File
df3ec414793491ce27c8...0ed7ad286d22080	File
secure.icaccops.com	Domain
50.229.189.110	Ip
173.163.5.2	Ip
50.254.196.129	Ip
64.8.3.9	Ip
3641cb93bf203ece865d...fc0234b2f1f51b5	File
a31cfca5ba78bca99b87...89f027a3f5450b7	File
0a6d8d01d00d7aecbe9b...8d146686476e187	File
35d6842856228adb7e8b...45c9d40a690b550	File
90506161ed789251b13d...44e46b0dd0066cc	File
017539edeeea6e318309...00919f6cb9ad12a	File
8086a04737e66df563fb...09159dc67bb8982	File
1366bef60db01f78949d...b89ff6129535613	File
9f6506cfc2cc321db15a...24d54628def646a	File
bf1af55c81a02923b55f...5f3d0bca12f3540	File
538d53a975285187a7f7...0279c2347968209	File
3998bc4e6956bd365191...0ff7c752cd52228	File
157b0edd9592722d33e3...26e77cc8eed666d	File
5adc04667336657d221c...7ebbc13e1871fb8	File
411a77b393dfe9631265...b8d1e60d1d42815	File
secure.ep2p.us	Domain

INDICATOR VALUE	TYPE
50.229.189.100	Ip
96.69.77.132	Ip
173.163.4.108	Ip
173.163.5.13	Ip
50.254.196.145	Ip
c6acf614726fc8ee98ba...c4841325ac6e48b	File
0c2be51a259f206a0ec6...bad9ae7f8f2baed	File
c14201d7706da3ad1efd...4a6a9a1dd87537c	File
a5706d8f621b337f212b...79b25a2c4bb6582	File
8693b5f9f91a1d86f469...82cffe40f5cdc82	File
b0e7cc4aef2bf48bf9c7...478a9e63b000a74	File
f6f46cae6b70af0119a5...5baea1dd04138d8	File
cps.gridcop.com	Domain
104.22.24.229	Ip
104.22.25.229	Ip
172.67.23.75	Ip
172.67.188.148	Ip
104.21.19.194	Ip
38.130.240.160	Ip
38.130.240.157	Ip
38.130.240.151	Ip
38.130.240.153	Ip
38.130.240.155	Ip
209.170.91.66	Ip
209.170.91.70	Ip
209.170.91.72	Ip

INDICATOR VALUE	TYPE
209.170.91.68	Ip
209.170.91.77	Ip
4.30.22.205	Ip
208.22.99.18	Ip
de3f1c7ecd5d93ae1ab5...ec66d4a1514c112	File
d1b8429fabed6e134d4f...7f39dcf0d45151a	File
8f712a9625b2700c6cb8...a5ea9ec9fb5f6f8	File
7e093bcc6615679be2fc...ea0ef233d90fe9a	File
acc5949dbe7e4e9e383b...d496259a5e896b5	File
64e3cf0324fbe4cc6caa...847c05dcab88158	File
afb7207f4a4f1b045fa0...66abaef3df3196f	File
e4481f6741ebe1005e43...04f4b99ee2567a1	File
52001718f01fba1778d5...93d2a2b93d3b720	File
51567e8f9b17dcc81608...84ebdb20423feda	File
f7ba75d81fae7ef77b06...6a6b087e6449b76	File
0d1c9bcbda71dc3306fd...9de6e1843e0b200	File
6e52e8d38679bd2f28b2...2ffad83bf42fd88	File
ea246121345a6a19fa39...a0083bf664943db	File
c92a9760bc4464f59881...86c1ec60163b697	File
633fd3662df3a254a9fd...de3c16f6a1231ac	File
7a7af6f08cbf13e3da2f...f9ba14826ef112e	File
37751817558ae91e6473...1963850efd77f26	File
29db1a047802158781c0...5bae05c42c43aa6	File
0333732b7253a5970829...832cc79fcaa87d4	File
26f606a3396b0fb971dc...7c093d3ffe158d9	File
367246f60eaf19f38ea0...9c66fd560ee7aee	File

INDICATOR VALUE	TYPE
51e7e9d824e8630a62df...79685d97350c228	File
5650791e31627fdda21e...bff06d881ac5421	File
674f5a69c30e8e202148...fe09ed02f17b897	File
70abb222cab3e3a5faf7...cd1792529958c5c	File
71146cb7d745b03eadf5...2845ea0a1267f12	File
a34fb073e7b63394df26...d6dec7b4fe66992	File
af04f732878c60308c12...6a69a69c6345d3f	File
c1ba165b90825a7a1566...ce039009c583900	File
d0bf77a8310afe1be682...2207c5d3cc1bd0c	File
d1b979b121d86b1fbee2...5bf93de27f7fbed	File
da003e3c1ee98d983502...1c6847aa634cae5	File
e82d326cfc5e27380488...3cf03c97185854d	File
ef7a46e8f8472c4b45d4...d10a1f364cf28dc	File
f0988cb5cde328d71f98...e9045e55966b30d	File
f868b1bf5ca0661db466...10000198921c6d7	File
www.feeble-industries.com	Domain
direct.feeble-industries.com	Domain
feeble-industries.com	Domain
www.icaccops.com	Domain
icaccops.com	Domain
forensics.umass.edu	Domain
128.119.240.95	Ip
fc0beb87553541eeb072be57b96ec23ca46f4029975c597264fe0a36fcc20639	File
04531596d3958b3a2f19eb05cf70a77c01427600369399d32c31fc10abd007e7	File
277041078227413c4ae988dff6dc42e06abd9dfb51de47aef61432a08df1e610	File
abc21e3c1f90a895b76e3b1c562600d4b113ab936ddae20689960ca84be07630	File

INDICATOR VALUE	TYPE
77b0f741b1f7699c1e2c51eb7eb17c3d59dffe9f92ac40f325d298faa7c46229	File
24459dd44143242d1ae2b7eb6e154b15170aba46d88dc6f6af82605ab21cbf57	File
418de3fa8226cca095773920b2f9d0805de9eb8238b33d03dd71d282c1affc4b	File
0a59acc5d026063b92032934d1c1b70b38307180ddff69f6dba45a6f7e7c0b03	File
bb01ab5516793ed7ba6c4d0b3effc99569aed9adc8ad6fdf52f123776a066a4f	File
df3ec414793491ce27c8dd3a918c4655b7db1cee67025482b0ed7ad286d22080	File
secure.icaccops.com	Domain
50.229.189.110	Ip
173.163.5.2	Ip
50.254.196.129	Ip
64.8.3.9	Ip
3641cb93bf203ece865d02aa480a829a798ea86c0ff5dd51cfc0234b2f1f51b5	File
a31cfca5ba78bca99b8731f196e330af5ce1ecf71b5fa021a89f027a3f5450b7	File
0a6d8d01d00d7aecbe9b3a341f55521e4a6162272e82ca8f48d146686476e187	File
35d6842856228adb7e8badcc12d035d17b12b17d14988b96e45c9d40a690b550	File
90506161ed789251b13d8e8988ba02ac4218fcc1ff0cc8e2644e46b0dd0066cc	File
017539edeeea6e318309307f640d06d56d59690733379ad2b00919f6cb9ad12a	File
8086a04737e66df563fb4ca440f67d22103b22ec601c30a1009159dc67bb8982	File
1366bef60db01f78949d3dfd150e0d696cc26ecf25248aab3b89ff6129535613	File
9f6506cfc2cc321db15a2cc8d29653a9eae6754e05ac790e524d54628def646a	File
bf1af55c81a02923b55fc1fad124bc5b086097d5e7bdcec7a5f3d0bca12f3540	File
538d53a975285187a7f7067159c1c44b4943d02d57f4d00c40279c2347968209	File
3998bc4e6956bd365191ea0093b34d8b55947a8854ccfa0f40ff7c752cd52228	File
157b0edd9592722d33e332d51d49f50629c96ea05f501d42a26e77cc8eed666d	File
5adc04667336657d221cc4ddb500b0bf794ff1e640ff190bc7ebbc13e1871fb8	File
411a77b393dfe96312653819f831e7e52f5c5b5bee04775f8b8d1e60d1d42815	File

INDICATOR VALUE	TYPE
secure.ep2p.us	Domain
50.229.189.100	Ip
96.69.77.132	Ip
173.163.4.108	Ip
173.163.5.13	Ip
50.254.196.145	Ip
c6acf614726fc8ee98bac5c0b5bd83b0bb529bc9d0afd3ecac4841325ac6e48b	File
0c2be51a259f206a0ec68c7fc65cbac2a7cadcd7e1a8bb5e1bad9ae7f8f2baed	File
c14201d7706da3ad1efdb99e799ee2809936fd20484be5b924a6a9a1dd87537c	File
a5706d8f621b337f212b7007a26a145d8601faf92e386e8cd79b25a2c4bb6582	File
8693b5f9f91a1d86f46939163326e3db4bb210de4f2b20a7582cffe40f5cdc82	File
b0e7cc4aef2bf48bf9c76a3b4c28978818a97094c20c820e6478a9e63b000a74	File
f6f46cae6b70af0119a528ce5719622afbda3cfaa481985e45baea1dd04138d8	File
cps.gridcop.com	Domain
104.22.24.229	Ip
104.22.25.229	Ip
172.67.23.75	Ip
172.67.188.148	Ip
104.21.19.194	Ip
38.130.240.160	Ip
38.130.240.157	Ip
38.130.240.151	Ip
38.130.240.153	Ip
38.130.240.155	Ip
209.170.91.66	Ip
209.170.91.70	Ip

INDICATOR VALUE	TYPE
`209.170.91.72`	Ip