Cyber Threat Intelligence Report

Event: we deserve better than this

Generated on: Sun, 13 Jul 2025 22:24:29 GMT

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

1. Executive Summary

The threat landscape indicates an active and potentially widespread phishing or malware distribution campaign, identified by the event 'we deserve better than this'. The primary initial access vector appears to be email-borne, as evidenced by a malicious file (hash: 023b0e0c7de16cfd5812...8f9a28c4486cd482) being executed by OUTLOOK.EXE. The campaign leverages a central domain, aflegal.org, and numerous subdomains, which resolve to a variety of IP addresses, suggesting a distributed infrastructure for hosting malicious content or command-and-control (C2) operations. Multiple other suspicious domains and associated IPs are also linked, indicating a broader network of malicious infrastructure. The presence of numerous unique file hashes further supports a malware distribution or data exfiltration objective. The potential threat level is High due to the clear initial access vector, the volume of associated malicious indicators, and the potential for widespread impact. Recommended actions include immediately blocking all identified malicious domains and IP addresses at the network perimeter (firewalls, DNS filters), implementing robust email filtering rules to detect and quarantine emails containing the identified file hashes or linking to the malicious domains, conducting endpoint scans for the specified file hashes, and enhancing user awareness training on phishing attacks. Furthermore, security teams should actively monitor network traffic for any connections to the identified indicators and investigate any internal systems showing compromise.

2. Actionable Recommendations

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

*   **Network Forensics:**
    *   Immediately implement network perimeter blocks for all identified domains (`aflegal.org`, `url3004.aflegal.org`, `forms.aflegal.org`, `events.aflegal.org`, `media.aflegal.org`) at DNS, proxy, and web filter levels.
    *   Immediately implement network perimeter blocks for all identified IP addresses (`157.230.68.71`, `188.114.96.2`, `188.114.97.2`, `172.64.80.1`, `68.183.207.241`, `151.101.194.159`, `172.67.131.170`, `104.21.4.48`, `34.102.136.180`) at firewall and network ACLs.
    *   Review firewall, proxy, and DNS logs for any past or ongoing connections to/from the identified domains and IP addresses across all network segments, going back at least 90 days.
    *   Analyze email gateway logs for messages containing the subject "we deserve better than this", attachments matching hash `023b0e0c7de16cfd5812...8f9a28c4486cd482`, or links to `aflegal.org` and its subdomains. Identify all recipients and senders.
    *   Deploy email filtering rules to quarantine or block emails matching the identified subject, file hash, or linking to `aflegal.org` and its subdomains.

*   **Host-Based Analysis:**
    *   Isolate any identified compromised hosts from the network immediately to prevent further lateral movement or data exfiltration.
    *   Initiate a full endpoint scan across all systems for the presence of the malicious file hash `023b0e0c7de16cfd5812...8f9a28c4486cd482`.
    *   For any endpoint where the file or related activity is detected, collect a full disk forensic image and volatile memory (RAM) dump.
    *   Examine process execution logs (e.g., EDR, Sysmon) on potentially affected systems for `OUTLOOK.EXE` spawning unusual child processes or making outbound network connections to the identified IPs/domains.
    *   Review registry keys, scheduled tasks, and startup folders on compromised hosts for persistence mechanisms.

*   **Intelligence & Threat Hunting:**
    *   Perform open-source intelligence (OSINT) on `aflegal.org` and its associated IP addresses (e.g., Whois, Passive DNS, SSL certificates, VirusTotal) to uncover registration details, hosting providers, and other associated infrastructure.
    *   Pivot on the identified IP addresses to discover other domains hosted on them or other malicious activity associated with those IPs, and identify their respective ASNs.
    *   Search internal and external threat intelligence platforms (e.g., MISP, industry sharing groups, commercial feeds) for the campaign name "we deserve better than this", the domain `aflegal.org`, and the identified file hash to gather further context, TTPs, and related

indicators.

* Submit the identified malicious file (hash: `023b0e0c7de16cfd5812...8f9a28c4486cd482`) to a secure sandbox environment for dynamic analysis to understand its full behavior, C2 communication patterns, and potential impact (e.g., data exfiltration, additional malware deployment).

* Develop and disseminate targeted user awareness training on current phishing tactics, specifically highlighting the characteristics of this campaign (e.g., subject lines, sender impersonation, suspicious links).

3. Attack Timeline (Key Indicators)

1 **MAIN**
`we deserve better than this`

2 **DOMAIN**
`aflegal.org`

3 **IP**
`157.230.68.71`

4 **FILE**
`023b0e0c7de16cfd581229cea5b3aa19ca47c012d62fa22e88f9a28c46595208`

5 **PROCESS**
`OUTLOOK.EXE`

6 **FILE**
`edb5a1c4bbf5092241ca...e17460e9b54851d`

7 **IP**
`167.89.118.83`

4. ATT&CK® Kill Chain

INITIAL ACCESS
Phishing
T1566

JUSTIFICATION
A 'main' indicator is linked to a file that interacts with OUTLOOK.EXE, strongly suggesting an initial compromise via an email-based attack such as a malicious attachment or link.

EVIDENCE

- `we deserve better than this`
- `023b0e0c7de16cfd581229cea5b3…`
- `OUTLOOK.EXE`

COMMAND AND CONTROL
Application Layer Protocol
T1071

JUSTIFICATION
A domain is observed resolving to an IP address and serving a file, indicating the use of standard web protocols for potential command and control communication or payload delivery.

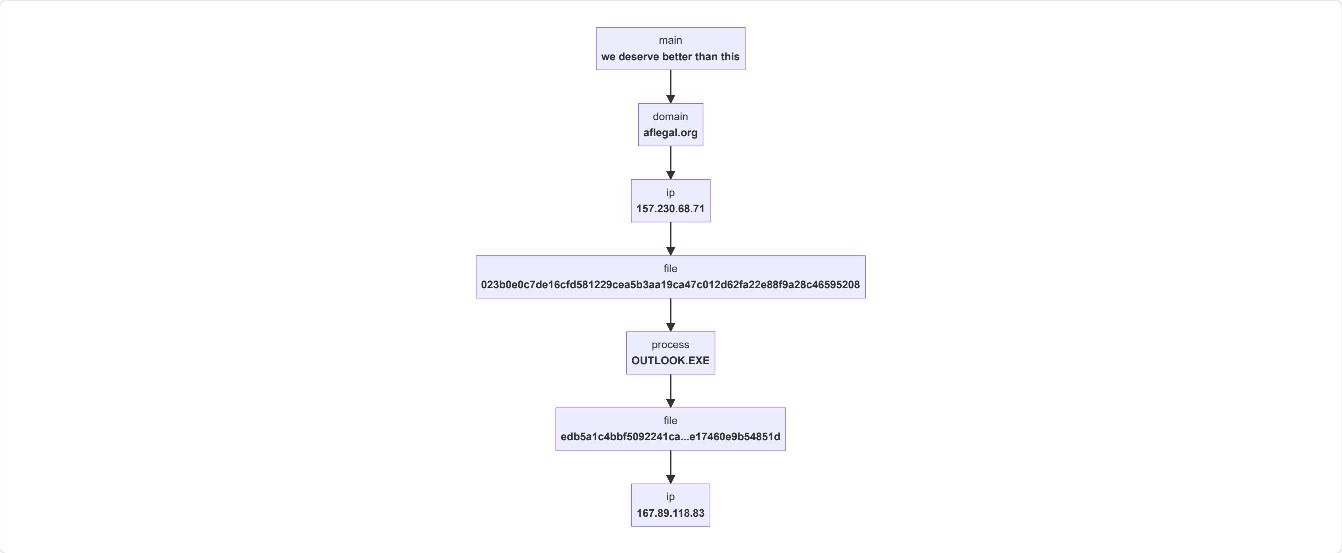
EVIDENCE

- `aflegal.org`
- `157.230.68.71`
- `edb5a1c4bbf5092241ca...e1746…`

5. MITRE ATT&CK® Matrix Overview

Reconnaissan e	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		Phishing									Application Layer Protocol		

6. Attack Flow Diagram


main
we deserve better than this
domain
aflegal.org
ip
157.230.68.71
file
023b0e0c7de16cfd581229cea5b3aa19ca47c012d62fa22e88f9a28c46595208
process
OUTLOOK.EXE
file
edb5a1c4bbf5092241ca...e17460e9b54851d
ip
167.89.118.83

7. Detailed TTP Analysis

Initial Access

TA0001

Phishing (T1566)

A 'main' indicator is linked to a file that interacts with OUTLOOK.EXE, strongly suggesting an initial compromise via an email-based attack such as a malicious attachment or link.

RELATED INDICATORS:

- `we deserve better than this`
- `023b0e0c7de16cfd581229cea5b3aa19ca47c012d62fa22e88f9a28c46595208`
- `OUTLOOK.EXE`

Command and Control

TA0011

Application Layer Protocol (T1071)

A domain is observed resolving to an IP address and serving a file, indicating the use of standard web protocols for potential command and control communication or payload delivery.

RELATED INDICATORS:

- `aflegal.org`
- `157.230.68.71`
- `edb5a1c4bbf5092241ca...e17460e9b54851d`

Appendix

A.1 YARA Detection Rule

▼

```
rule Threat_Intel_Report_Rule {
  meta:
    description = "Detects files based on a list of known malicious filenames (which are SHA256 hashes) and their correspondi
    author = "Castle Bravo Project - Threat Intel Visualizer AI"
    date = "2025-07-13"
    rule_version = "1.0"
    threat_name = "FileHash_Filename_IOCs"

  strings:
    // Filename indicators (treated as strings that might appear in file content)
    $s_filename_1 = "6a05c044ac57c3d7c6f7db824ee55064668ea6f39e255fac5038645a00252716" ascii nocase
    $s_filename_2 = "edb5a1c4bbf5092241ca0552fde09f2a66cc8898e0c27507be17460e9b54851d" ascii nocase
    $s_filename_3 = "8287421b42d5632c79f3df52bcd0e6a85effc61c1812ac6db327d2cff2e2d3ab" ascii nocase
    $s_filename_4 = "4dbbdcdb3c14fe645f9b78f3b377c7c931ece10a151226ea507b2a782f650e79" ascii nocase
    $s_filename_5 = "07a108f206c99cb6f60933c5fc3075a4d5184ba17548876f308e54a72210f8ea" ascii nocase
    $s_filename_6 = "bb3b532ad1560ca643f98e3f5461181d016714a3077afdcc4b3220edc8248740" ascii nocase
    $s_filename_7 = "38dd6cf332158bef51f92c65536a3c57e3e456cf89658978704d8161919d8324" ascii nocase
    $s_filename_8 = "ae6abfff5a02cf0d39aaeb7497be3a6a01b6f3694c72525f207ec0b64942c8ab" ascii nocase
    $s_filename_9 = "15646aca0d8996e6fc162a46b1b9b2bd2c446531f0cd5d29cf4bdaff47785062" ascii nocase
    $s_filename_10 = "f8ff68de65b082c19638d639de002b991f7e4e1e325a0750ad7fd2aa3dd292b5" ascii nocase
    $s_filename_11 = "5a11485b74d1f1bfab5b97641dd4723dd172df5ce19bc539ce0560e6c281dba2" ascii nocase
    $s_filename_12 = "fe55d260b363890e8de25dcc271e527ca994e4db350ce2b958d72eb68129bb6b" ascii nocase
    $s_filename_13 = "044a1e432d3aefa85e902531f906b7f672fc2d515af943db7b267fb247d650b9" ascii nocase
    $s_filename_14 = "451ad6ba887a8aa9c80d90466eff8dc680060c9cda88349b677da27d07b0af72" ascii nocase
    $s_filename_15 = "13db9d0c5955a014b00fa33254246b3e5231b8b16916fcb43509003544d09f1c" ascii nocase
    $s_filename_16 = "11fb0103d6c8f9586e0caf61f54c4f37d660c8df2f0dffa53b8c5a46f1ae24cb" ascii nocase
    $s_filename_17 = "a1efee1ebf6efbacb43cdd28c2ef18c22d1fc5e4908bda2c8af003e827ee80ea" ascii nocase
    $s_filename_18 = "779ef4d968fa2a5c8b812e1b59f9e3ac491cf784bd24994dd6046b87134110b4" ascii nocase
    $s_filename_19 = "c1a9c7d8ff2fbcda8b114a41e6b81b8ff87a0932471af4d669b181da5ebc572a" ascii nocase
    $s_filename_20 = "0afbbd7e73cb4ace9dc8b4204591ec3bd3da488d6e8d4fdd201a17f1b4a80a38" ascii nocase
    $s_filename_21 = "0968477fe2b0ad304dca383e0017d3d44a0138b23ef34b5513f8b822f2af7084" ascii nocase
    $s_filename_22 = "102c7c49f99d62fb794f9cc80cbb38c28219f39e9c1951193ffeb1c7f0bf3a6a" ascii nocase
    $s_filename_23 = "2b3b2a0f55936f8e01d9c95f40cc14a6b43c91638f54499ef3258d5ec937c4d7" ascii nocase
    $s_filename_24 = "310396c12326c155eb1b984438671fc9221adc6c024d1db508551af9d78b5c37" ascii nocase
    $s_filename_25 = "5cb1a8a5a93cd649496652afda61374894995ac841251b21bab51cb8b15db7ca" ascii nocase
    $s_filename_26 = "843a9822f3b458a5eb5d0fe3cad9a09240629da902aa30dea60f607d2ddb050d" ascii nocase
    $s_filename_27 = "a0aec2bdec638b39ad14899e3303f68863fccf88330c83f4d0bd1669da6b94bb" ascii nocase
    $s_filename_28 = "e0096e9170a4754a2178f9f8d2db9913e7ea13fb91b290a93677229f89d9be11" ascii nocase
    $s_filename_29 = "81ff65efc4487853bdb4625559e69ab44f19e0f5efbd6d5b2af5e3ab267c8e06" ascii nocase
    $s_filename_30 = "0d153e9b74bf32951a653580558fbfce639fb2800199f0441400c895d2fb5dc4" ascii nocase
    $s_filename_31 = "1163902298804aed26ac518d710bce19fc81bc06f9be8eb3ecf0bb03367d1a6a" ascii nocase
    $s_filename_32 = "00173656adc31643e612d50ccdf0c7b544f92b972f9418ecaf8c503143b12c7f" ascii nocase
    $s_filename_33 = "0020aafe558012576734b1c2a33c7f77772f7d25b79e0ecd1915e026661e1aae" ascii nocase
    $s_filename_34 = "016e13379b95b8b17a45e98bcf2409f89d6ae19d07e9fbb7445afcf8b8cb3106" ascii nocase
    $s_filename_35 = "019a51363a9169bb3862c61b55fcbe3976cf63f06ec44841a4c920ff4c1816fd" ascii nocase
    $s_filename_36 = "019a9691ce5762c566cd8c5b199fbbe496bad41fa0e01474b191b752664aa776" ascii nocase
    $s_filename_37 = "01a4ff9efb99dc84f47a7210496d00f91c5fa3ccb9e87502929a3eb7d67ccce1" ascii nocase
    $s_filename_38 = "01c4cd441ec04e859283fcf5181f11326cfba0f7475561fe8ccf8b014c28a483" ascii nocase
    $s_filename_39 = "02101568a534c097881ed9d6559b093a8ded1436c3e8087f869e63fc8d34cd27" ascii nocase
    $s_filename_40 = "0223ab27ac2d8bd3c12874ffc32ac9ba51c278eabd7563e9387fbc5b69023896" ascii nocase
    $s_filename_41 = "023b0e0c7de16cfd581229cea5b3aa19ca47c012d62fa22e88f9a28c46595208" ascii nocase
    $s_filename_42 = "025c82b31c24c459717f1643b3803a47df3e050299b9d7eaee190799b3a4525d" ascii nocase
    $s_filename_43 = "0267fc8c52c3d3d9951eb8a4f135837c7e487b5f2c763d3f2fda89744833d20f" ascii nocase
    $s_filename_44 = "0282ff2ef03e71d48524040621a1dcb3cf0e701ced9807aaa136a896174e42c7" ascii nocase
    $s_filename_45 = "02b38929d67941f4227ad01f62b69a895d94c63bc0ebbcc8f211bdee68f3d8f3" ascii nocase
    $s_filename_46 = "02b8e83f3895f781308d545b5b2ba18c11e4c70f1a3352b7424b800d108bb984" ascii nocase
    $s_filename_47 = "02e02f043fd3069fb1246eaf1eedad4687fbaa3747cefd6edb9e6c95ddf358e8" ascii nocase
    $s_filename_48 = "02ebbdfb6407201a65c9a28a5f78f587fa49374f4382bdee02bb5ccd58ea8bc2" ascii nocase
    $s_filename_49 = "02fe0e0db3fac72999f25e5c0c8899eb35d59dfb7ae6b51283a3d15f5e2a23b2" ascii nocase
    $s_filename_50 = "03225672c3385ebe65fd6d99309f9e7115c973e03553c84b1c9d39b2402c5f07" ascii nocase
    $s_filename_51 = "032a5646d6969def7f2a85ab1de2309a46bbaf14ffb087c7b7c0cb3f85d8fc3a" ascii nocase
```

```
condition:
  // Match by SHA256 hash of the file content
  hash.sha256() in (
    "6a05c044ac57c3d7c6f7db824ee55064668ea6f39e255fac5038645a00252716",
    "edb5a1c4bbf5092241ca0552fde09f2a66cc8898e0c27507be17460e9b54851d",
    "8287421b42d5632c79f3df52bcd0e6a85effc61c1812ac6db327d2cff2e2d3ab",
    "4dbbdcdb3c14fe645f9b78f3b377c7c931ece10a151226ea507b2a782f650e79",
    "07a108f206c99cb6f60933c5fc3075a4d5184ba17548876f308e54a72210f8ea",
    "bb3b532ad1560ca643f98e3f5461181d016714a3077afdcc4b3220edc8248740",
    "38dd6cf332158bef51f92c65536a3c57e3e456cf89658978704d8161919d8324",
    "ae6abfff5a02cf0d39aaeb7497be3a6a01b6f3694c72525f207ec0b64942c8ab",
    "15646aca0d8996e6fc162a46b1b9b2bd2c446531f0cd5d29cf4bdaff47785062",
    "f8ff68de65b082c19638d639de002b991f7e4e1e325a0750ad7fd2aa3dd292b5",
    "5a11485b74d1f1bfab5b97641dd4723dd172df5ce19bc539ce0560e6c281dba2",
    "fe55d260b363890e8de25dcc271e527ca994e4db350ce2b958d72eb68129bb6b",
    "044a1e432d3aefa85e902531f906b7f672fc2d515af943db7b267fb247d650b9",
    "451ad6ba887a8aa9c80d90466eff8dc680060c9cda88349b677da27d07b0af72",
    "13db9d0c5955a014b00fa33254246b3e5231b8b16916fcb43509003544d09f1c",
    "11fb0103d6c8f9586e0caf61f54c4f37d660c8df2f0dffa53b8c5a46f1ae24cb",
    "a1efee1ebf6efbacb43cdd28c2ef18c22d1fc5e4908bda2c8af003e827ee80ea",
    "779ef4d968fa2a5c8b812e1b59f9e3ac491cf784bd24994dd6046b87134110b4",
    "c1a9c7d8ff2fbcda8b114a41e6b81b8ff87a0932471af4d669b181da5ebc572a",
    "0afbbd7e73cb4ace9dc8b4204591ec3bd3da488d6e8d4fdd201a17f1b4a80a38",
    "0968477fe2b0ad304dca383e0017d3d44a0138b23ef34b5513f8b822f2af7084",
    "102c7c49f99d62fb794f9cc80cbb38c28219f39e9c1951193ffeb1c7f0bf3a6a",
    "2b3b2a0f55936f8e01d9c95f40cc14a6b43c91638f54499ef3258d5ec937c4d7",
    "310396c12326c155eb1b984438671fc9221adc6c024d1db508551af9d78b5c37",
    "5cb1a8a5a93cd649496652afda61374894995ac841251b21bab51cb8b15db7ca",
    "843a9822f3b458a5eb5d0fe3cad9a09240629da902aa30dea60f607d2ddb050d",
    "a0aec2bdec638b39ad14899e3303f68863fccf88330c83f4d0bd1669da6b94bb",
    "e0096e9170a4754a2178f9f8d2db9913e7ea13fb91b290a93677229f89d9be11",
    "81ff65efc4487853bdb4625559e69ab44f19e0f5efbd6d5b2af5e3ab267c8e06",
    "0d153e9b74bf32951a653580558fbfce639fb2800199f0441400c895d2fb5dc4",
    "1163902298804aed26ac518d710bce19fc81bc06f9be8eb3ecf0bb03367d1a6a",
    "00173656adc31643e612d50ccdf0c7b544f92b972f9418ecaf8c503143b12c7f",
    "0020aafe558012576734b1c2a33c7f77772f7d25b79e0ecd1915e026661e1aae",
    "016e13379b95b8b17a45e98bcf2409f89d6ae19d07e9fbb7445afcf8b8cb3106",
    "019a51363a9169bb3862c61b55fcbe3976cf63f06ec44841a4c920ff4c1816fd",
    "019a9691ce5762c566cd8c5b199fbbe496bad41fa0e01474b191b752664aa776",
    "01a4ff9efb99dc84f47a7210496d00f91c5fa3ccb9e87502929a3eb7d67ccce1",
    "01c4cd441ec04e859283fcf5181f11326cfba0f7475561fe8ccf8b014c28a483",
    "02101568a534c097881ed9d6559b093a8ded1436c3e8087f869e63fc8d34cd27",
    "0223ab27ac2d8bd3c12874ffc32ac9ba51c278eabd7563e9387fbc5b69023896",
    "023b0e0c7de16cfd581229cea5b3aa19ca47c012d62fa22e88f9a28c46595208",
    "025c82b31c24c459717f1643b3803a47df3e050299b9d7eaee190799b3a4525d",
    "0267fc8c52c3d3d9951eb8a4f135837c7e487b5f2c763d3f2fda89744833d20f",
    "0282ff2ef03e71d48524040621a1dcb3cf0e701ced9807aaa136a896174e42c7",
    "02b38929d67941f4227ad01f62b69a895d94c63bc0ebbcc8f211bdee68f3d8f3",
    "02b8e83f3895f781308d545b5b2ba18c11e4c70f1a3352b7424b800d108bb984",
    "02e02f043fd3069fb1246eaf1eedad4687fbaa3747cefd6edb9e6c95ddf358e8",
    "02ebbdfb6407201a65c9a28a5f78f587fa49374f4382bdee02bb5ccd58ea8bc2",
    "02fe0e0db3fac72999f25e5c0c8899eb35d59dfb7ae6b51283a3d15f5e2a23b2",
    "03225672c3385ebe65fd6d99309f9e7115c973e03553c84b1c9d39b2402c5f07",
    "032a5646d6969def7f2a85ab1de2309a46bbaf14ffb087c7b7c0cb3f85d8fc3a",
    "211bdf19381949eb8115d9b099670d0277e91531afea23e23a11879d9a29f87d",
    "529139c00f218f0a2077853ab017c1057eb76c875c44fca465806410d61b7e69",
    "637d06de23cc8f9feb728801c02636746acb238cfcd19d8c5832ace4486cd482",
    "94ff773f44ba8f65a1a77496a942aca8111051c23a674ab353c9c9a3e90c2116",
    "a7ecc6fc2808df859893520585b5ee10cb3e5f9cd35df7efd3ccb3b998930b08",
    "ad27039abac3252c3b397bfe925afa85e1484f1af826849f277261441137ede5",
    "d99691338dcc96efa74ee46656448b7bd9c7a3777b90d12ff1ae3ba93fd7a06f",
    "ff06e38f3d807ad79ed526829ca7c01bfeec1421b99ce67195e7cbce78ce4364"
  )
  // OR match if any of the filename hash strings are present in the file content
```

```
    or any of ($s_filename_*)
}
```

A.2 All Indicators of Compromise (IOCs)

INDICATOR VALUE	TYPE
aflegal.org	Domain
157.230.68.71	Ip
188.114.96.2	Ip
188.114.97.2	Ip
172.64.80.1	Ip
68.183.207.241	Ip
151.101.194.159	Ip
172.67.131.170	Ip
104.21.4.48	Ip
34.102.136.180	Ip
url3004.aflegal.org	Domain
forms.aflegal.org	Domain
events.aflegal.org	Domain
media.aflegal.org	Domain
wokewagon.aflegal.org	Domain
ftp.aflegal.org	Domain
tracker.aflegal.org	Domain
test.aflegal.org	Domain
wordpress.aflegal.org	Domain
www.aflegal.org	Domain
6a05c044ac57c3d7c6f7...038645a00252716	File
edb5a1c4bbf5092241ca...e17460e9b54851d	File
8287421b42d5632c79f3...327d2cff2e2d3ab	File
4dbbdcdb3c14fe645f9b...07b2a782f650e79	File
07a108f206c99cb6f609...08e54a72210f8ea	File

INDICATOR VALUE	TYPE
bb3b532ad1560ca643f9...b3220edc8248740	File
38dd6cf332158bef51f9...04d8161919d8324	File
ae6abfff5a02cf0d39aa...07ec0b64942c8ab	File
15646aca0d8996e6fc16...f4bdaff47785062	File
f8ff68de65b082c19638...d7fd2aa3dd292b5	File
5a11485b74d1f1bfab5b...e0560e6c281dba2	File
fe55d260b363890e8de2...8d72eb68129bb6b	File
044a1e432d3aefa85e90...b267fb247d650b9	File
451ad6ba887a8aa9c80d...77da27d07b0af72	File
13db9d0c5955a014b00f...509003544d09f1c	File
11fb0103d6c8f9586e0c...b8c5a46f1ae24cb	File
a1efee1ebf6efbacb43c...af003e827ee80ea	File
779ef4d968fa2a5c8b81...6046b87134110b4	File
c1a9c7d8ff2fbcda8b11...9b181da5ebc572a	File
0afbbd7e73cb4ace9dc8...01a17f1b4a80a38	File
45.56.70.215	Ip
104.21.14.51	Ip
172.67.157.217	Ip
104.21.34.35	Ip
172.67.167.218	Ip
167.89.115.52	Ip
167.89.115.28	Ip
167.89.115.56	Ip
167.89.118.95	Ip
167.89.115.61	Ip
167.89.118.128	Ip
167.89.118.120	Ip
167.89.118.52	Ip
167.89.118.109	Ip

INDICATOR VALUE	TYPE
167.89.118.83	Ip
167.89.115.120	Ip
167.89.115.150	Ip
62.210.90.237	Ip
62.210.90.238	Ip
68.70.205.3	Ip
68.70.205.4	Ip
68.70.205.1	Ip
68.70.205.2	Ip
8.8.8.8	Ip
acroipm2.adobe.com	Domain
0968477fe2b0ad304dca...3f8b822f2af7084	File
102c7c49f99d62fb794f...ffeb1c7f0bf3a6a	File
2b3b2a0f55936f8e01d9...3258d5ec937c4d7	File
310396c12326c155eb1b...8551af9d78b5c37	File
5cb1a8a5a93cd6494966...ab51cb8b15db7ca	File
843a9822f3b458a5eb5d...60f607d2ddb050d	File
a0aec2bdec638b39ad14...0bd1669da6b94bb	File
e0096e9170a4754a2178...677229f89d9be11	File
81ff65efc4487853bdb4...af5e3ab267c8e06	File
baystatebollard.com	Domain
www.wrap.com	Domain
wrap.com	Domain
www.vettedbreeders.com	Domain
cardiackrock.com	Domain
www.annapolistdclub.com	Domain
vettedbreeders.com	Domain
annapolistdclub.com	Domain
battlegroundjiujitsu.com	Domain

INDICATOR VALUE	TYPE
kathleenannstarr.com	Domain
www.kathleenannstarr.com	Domain
flatcreekfrm.com	Domain
graffgrown.com	Domain
mbariorancho.com	Domain
scheerandmontgomery.com	Domain
comuga.com	Domain
voltrix.com.au	Domain
hubble-vpn.encapture.com	Domain
bwwealthmanagement.com	Domain
estuaryhealth.ca	Domain
0d153e9b74bf32951a65...400c895d2fb5dc4	File
1163902298804aed26ac...cf0bb03367d1a6a	File
13.248.243.5	Ip
76.223.105.230	Ip
50.63.202.4	Ip
184.168.221.29	Ip
50.63.202.24	Ip
50.63.202.33	Ip
173.236.251.254	Ip
208.113.171.129	Ip
151.101.66.159	Ip
149.154.59.7	Ip
15.197.225.128	Ip
3.33.251.168	Ip
15.197.142.173	Ip
3.33.152.147	Ip
69.175.15.202	Ip
107.180.48.169	Ip

INDICATOR VALUE	TYPE
69.172.206.24	Ip
208.89.53.106	Ip
76.223.113.161	Ip
104.143.9.211	Ip
104.143.9.210	Ip
72.52.179.175	Ip
3.33.130.190	Ip
15.197.148.33	Ip
184.168.221.59	Ip
100.24.208.97	Ip
184.168.131.241	Ip
132.148.15.143	Ip
208.109.191.62	Ip
185.230.63.171	Ip
185.230.63.186	Ip
185.230.63.107	Ip
34.224.10.110	Ip
52.11.37.152	Ip
104.16.111.239	Ip
104.16.110.239	Ip
104.16.109.239	Ip
104.16.112.239	Ip
104.16.108.239	Ip
184.168.221.76	Ip
184.168.221.91	Ip
167.68.37.150	Ip
00173656adc31643e612...f8c503143b12c7f	File
0020aafe558012576734...915e026661e1aae	File
016e13379b95b8b17a45...45afcf8b8cb3106	File

INDICATOR VALUE	TYPE
019a51363a9169bb3862...4c920ff4c1816fd	File
019a9691ce5762c566cd...191b752664aa776	File
01a4ff9efb99dc84f47a...29a3eb7d67ccce1	File
01c4cd441ec04e859283...ccf8b014c28a483	File
02101568a534c097881e...69e63fc8d34cd27	File
0223ab27ac2d8bd3c128...87fbc5b69023896	File
023b0e0c7de16cfd5812...8f9a28c46595208	File
025c82b31c24c459717f...e190799b3a4525d	File
0267fc8c52c3d3d9951e...fda89744833d20f	File
0282ff2ef03e71d48524...136a896174e42c7	File
02b38929d67941f4227a...211bdee68f3d8f3	File
02b8e83f3895f781308d...24b800d108bb984	File
02e02f043fd3069fb124...b9e6c95ddf358e8	File
02ebbdfb6407201a65c9...2bb5ccd58ea8bc2	File
02fe0e0db3fac72999f2...3a3d15f5e2a23b2	File
03225672c3385ebe65fd...c9d39b2402c5f07	File
032a5646d6969def7f2a...7c0cb3f85d8fc3a	File
cantgetabreak12222223.ca	Domain
url3571.wowzi.co	Domain
url8684.update.ai	Domain
url5148.redisage.eu	Domain
url7393.ibyndmail.com	Domain
url.orenascimentodainternet.com	Domain
tj-link.greatbigbeautifuladventures.com	Domain
mail-links.compology.com	Domain
url9796.gmshop.in	Domain
sg1.greenhillscm.com	Domain
url9258.mktdisrupt-ct.com.br	Domain
url2710.ronin-edge.com	Domain

INDICATOR VALUE	TYPE
send.rodighierogioielli.com	Domain
coretech2565.t.honeycrmapp.net	Domain
url5089.reviewmgr.com	Domain
startechcompcom14970.t.honeycrmapp.net	Domain
emails.zlvs.co	Domain
url6653.musiciansabroad.com	Domain
url5978.elite-lawpartners.io	Domain
url4826.whitewhale.ai	Domain
167.89.123.90	Ip
167.89.123.124	Ip
167.89.118.62	Ip
167.89.123.204	Ip
167.89.123.54	Ip
167.89.123.62	Ip
167.89.123.58	Ip
167.89.123.89	Ip
167.89.118.61	Ip
167.89.125.30	Ip
52.39.173.225	Ip
44.245.147.253	Ip
44.228.207.192	Ip
aflegal.org	Domain
157.230.68.71	Ip
188.114.96.2	Ip
188.114.97.2	Ip
172.64.80.1	Ip
68.183.207.241	Ip
151.101.194.159	Ip
172.67.131.170	Ip

INDICATOR VALUE	TYPE
104.21.4.48	Ip
34.102.136.180	Ip
url3004.aflegal.org	Domain
forms.aflegal.org	Domain
events.aflegal.org	Domain
media.aflegal.org	Domain
wokewagon.aflegal.org	Domain
ftp.aflegal.org	Domain
tracker.aflegal.org	Domain
test.aflegal.org	Domain
wordpress.aflegal.org	Domain
www.aflegal.org	Domain
6a05c044ac57c3d7c6f7db824ee55064668ea6f39e255fac5038645a00252716	File
edb5a1c4bbf5092241ca0552fde09f2a66cc8898e0c27507be17460e9b54851d	File
8287421b42d5632c79f3df52bcd0e6a85effc61c1812ac6db327d2cff2e2d3ab	File
4dbbdcdb3c14fe645f9b78f3b377c7c931ece10a151226ea507b2a782f650e79	File
07a108f206c99cb6f60933c5fc3075a4d5184ba17548876f308e54a72210f8ea	File
bb3b532ad1560ca643f98e3f5461181d016714a3077afdcc4b3220edc8248740	File
38dd6cf332158bef51f92c65536a3c57e3e456cf89658978704d8161919d8324	File
ae6abfff5a02cf0d39aaeb7497be3a6a01b6f3694c72525f207ec0b64942c8ab	File
15646aca0d8996e6fc162a46b1b9b2bd2c446531f0cd5d29cf4bdaff47785062	File
f8ff68de65b082c19638d639de002b991f7e4e1e325a0750ad7fd2aa3dd292b5	File
5a11485b74d1f1bfab5b97641dd4723dd172df5ce19bc539ce0560e6c281dba2	File
fe55d260b363890e8de25dcc271e527ca994e4db350ce2b958d72eb68129bb6b	File
044a1e432d3aefa85e902531f906b7f672fc2d515af943db7b267fb247d650b9	File
451ad6ba887a8aa9c80d90466eff8dc680060c9cda88349b677da27d07b0af72	File
13db9d0c5955a014b00fa33254246b3e5231b8b16916fcb43509003544d09f1c	File
11fb0103d6c8f9586e0caf61f54c4f37d660c8df2f0dffa53b8c5a46f1ae24cb	File
a1efee1ebf6efbacb43cdd28c2ef18c22d1fc5e4908bda2c8af003e827ee80ea	File

INDICATOR VALUE	TYPE
779ef4d968fa2a5c8b812e1b59f9e3ac491cf784bd24994dd6046b87134110b4	File
c1a9c7d8ff2fbcda8b114a41e6b81b8ff87a0932471af4d669b181da5ebc572a	File
0afbbd7e73cb4ace9dc8b4204591ec3bd3da488d6e8d4fdd201a17f1b4a80a38	File
45.56.70.215	Ip
104.21.14.51	Ip
172.67.157.217	Ip
104.21.34.35	Ip
172.67.167.218	Ip
167.89.115.52	Ip
167.89.115.28	Ip
167.89.115.56	Ip
167.89.118.95	Ip
167.89.115.61	Ip
167.89.118.128	Ip
167.89.118.120	Ip
167.89.118.52	Ip
167.89.118.109	Ip
167.89.118.83	Ip
167.89.115.120	Ip
167.89.115.150	Ip
62.210.90.237	Ip
62.210.90.238	Ip
68.70.205.3	Ip
68.70.205.4	Ip
68.70.205.1	Ip
68.70.205.2	Ip
8.8.8.8	Ip
acroipm2.adobe.com	Domain
0968477fe2b0ad304dca383e0017d3d44a0138b23ef34b5513f8b822f2af7084	File

INDICATOR VALUE	TYPE
102c7c49f99d62fb794f9cc80cbb38c28219f39e9c1951193ffeb1c7f0bf3a6a	File
2b3b2a0f55936f8e01d9c95f40cc14a6b43c91638f54499ef3258d5ec937c4d7	File
310396c12326c155eb1b984438671fc9221adc6c024d1db508551af9d78b5c37	File
5cb1a8a5a93cd649496652afda61374894995ac841251b21bab51cb8b15db7ca	File
843a9822f3b458a5eb5d0fe3cad9a09240629da902aa30dea60f607d2ddb050d	File
a0aec2bdec638b39ad14899e3303f68863fccf88330c83f4d0bd1669da6b94bb	File
e0096e9170a4754a2178f9f8d2db9913e7ea13fb91b290a93677229f89d9be11	File
211bdf19381949eb8115d9b099670d0277e91531afea23e23a11879d9a29f87d	File
529139c00f218f0a2077853ab017c1057eb76c875c44fca465806410d61b7e69	File
637d06de23cc8f9feb728801c02636746acb238cfcd19d8c5832ace4486cd482	File
81ff65efc4487853bdb4625559e69ab44f19e0f5efbd6d5b2af5e3ab267c8e06	File
94ff773f44ba8f65a1a77496a942aca8111051c23a674ab353c9c9a3e90c2116	File
a7ecc6fc2808df859893520585b5ee10cb3e5f9cd35df7efd3ccb3b998930b08	File
ad27039abac3252c3b397bfe925afa85e1484f1af826849f277261441137ede5	File
d99691338dcc96efa74ee46656448b7bd9c7a3777b90d12ff1ae3ba93fd7a06f	File
ff06e38f3d807ad79ed526829ca7c01bfeec1421b99ce67195e7cbce78ce4364	File
baystatebollard.com	Domain
www.wrap.com	Domain
wrap.com	Domain
www.vettedbreeders.com	Domain
cardiackrock.com	Domain
www.annapolistdclub.com	Domain
vettedbreeders.com	Domain
annapolistdclub.com	Domain
battlegroundjiujitsu.com	Domain
kathleenannstarr.com	Domain
www.kathleenannstarr.com	Domain
flatcreekfrm.com	Domain
graffgrown.com	Domain

INDICATOR VALUE	TYPE
mbariorancho.com	Domain
scheerandmontgomery.com	Domain
comuga.com	Domain
voltrix.com.au	Domain
hubble-vpn.encapture.com	Domain
bwwealthmanagement.com	Domain
estuaryhealth.ca	Domain
0d153e9b74bf32951a653580558fbfce639fb2800199f0441400c895d2fb5dc4	File
1163902298804aed26ac518d710bce19fc81bc06f9be8eb3ecf0bb03367d1a6a	File
13.248.243.5	Ip
76.223.105.230	Ip
50.63.202.4	Ip
184.168.221.29	Ip
50.63.202.24	Ip
50.63.202.33	Ip
173.236.251.254	Ip
208.113.171.129	Ip
151.101.66.159	Ip
149.154.59.7	Ip
15.197.225.128	Ip
3.33.251.168	Ip
15.197.142.173	Ip
3.33.152.147	Ip
69.175.15.202	Ip
107.180.48.169	Ip
69.172.206.24	Ip
208.89.53.106	Ip
76.223.113.161	Ip
104.143.9.211	Ip

INDICATOR VALUE	TYPE
104.143.9.210	Ip
72.52.179.175	Ip
3.33.130.190	Ip
15.197.148.33	Ip
184.168.221.59	Ip
100.24.208.97	Ip
184.168.131.241	Ip
132.148.15.143	Ip
208.109.191.62	Ip
185.230.63.171	Ip
185.230.63.186	Ip
185.230.63.107	Ip
34.224.10.110	Ip
52.11.37.152	Ip
104.16.111.239	Ip
104.16.110.239	Ip
104.16.109.239	Ip
104.16.112.239	Ip
104.16.108.239	Ip
184.168.221.76	Ip
184.168.221.91	Ip
167.68.37.150	Ip
00173656adc31643e612d50ccdf0c7b544f92b972f9418ecaf8c503143b12c7f	File
0020aafe558012576734b1c2a33c7f77772f7d25b79e0ecd1915e026661e1aae	File
016e13379b95b8b17a45e98bcf2409f89d6ae19d07e9fbb7445afcf8b8cb3106	File
019a51363a9169bb3862c61b55fcbe3976cf63f06ec44841a4c920ff4c1816fd	File
019a9691ce5762c566cd8c5b199fbbe496bad41fa0e01474b191b752664aa776	File
01a4ff9efb99dc84f47a7210496d00f91c5fa3ccb9e87502929a3eb7d67ccce1	File
01c4cd441ec04e859283fcf5181f11326cfba0f7475561fe8ccf8b014c28a483	File

INDICATOR VALUE	TYPE
02101568a534c097881ed9d6559b093a8ded1436c3e8087f869e63fc8d34cd27	File
0223ab27ac2d8bd3c12874ffc32ac9ba51c278eabd7563e9387fbc5b69023896	File
023b0e0c7de16cfd581229cea5b3aa19ca47c012d62fa22e88f9a28c46595208	File
025c82b31c24c459717f1643b3803a47df3e050299b9d7eaee190799b3a4525d	File
0267fc8c52c3d3d9951eb8a4f135837c7e487b5f2c763d3f2fda89744833d20f	File
0282ff2ef03e71d48524040621a1dcb3cf0e701ced9807aaa136a896174e42c7	File
02b38929d67941f4227ad01f62b69a895d94c63bc0ebbcc8f211bdee68f3d8f3	File
02b8e83f3895f781308d545b5b2ba18c11e4c70f1a3352b7424b800d108bb984	File
02e02f043fd3069fb1246eaf1eedad4687fbaa3747cefd6edb9e6c95ddf358e8	File
[illegible]	[illegible]