Cyber Threat Intelligence Report

Event: ep2p_a

Generated on: Sun, 13 Jul 2025 21:51:07 GMT

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

1. Executive Summary

The threat landscape centers around the 'ep2p.us' domain and its subdomains, which appear to serve as a central malicious infrastructure for malware distribution and Command and Control (C2) operations. The presence of numerous associated file hashes, some linked to internal IP addresses (e.g., 192.168.0.x), strongly indicates active compromise and potential lateral movement within affected networks. A specific URL, 'http://www.icaccops.com/filesem.zip', is identified as a direct download source for malicious payloads, suggesting a likely initial access vector such as phishing or drive-by download. The overall activity points to a well-established and active malicious campaign. The potential threat level is assessed as High due to the clear indicators of active malware distribution, C2 communications, and potential internal network compromise. Recommended actions for a security operations team include immediately blocking all identified 'ep2p.us' domains and subdomains, the 'icaccops.com' domain, and all associated malicious IP addresses at the perimeter. Furthermore, it is critical to deploy endpoint detection and response (EDR) rules for the identified file hashes and conduct thorough scans across the environment to identify and quarantine any compromised systems. Network traffic should be continuously monitored for any attempts to resolve or connect to these indicators.

2. Actionable Recommendations

Network Forensics
*   Immediately implement perimeter blocks for all identified `*.ep2p.us` domains, `icaccops.com`, and the IP addresses (50.229.189.100, 96.69.77.132, 173.163.4.108, 173.163.5.13, 50.254.196.145) at DNS, firewall, and proxy levels.
*   Review proxy, firewall, and DNS logs for any historical or ongoing connections to/from `*.ep2p.us` domains, `icaccops.com`, and the listed malicious IPs. Prioritize logs from the last 90 days.
*   Search network traffic logs (e.g., NetFlow, full packet capture if available) for any HTTP/S requests to `http://www.icaccops.com/filesem.zip` to identify potential initial access points.
*   Investigate internal network traffic for any communications originating from or destined for the identified malicious IPs, especially from internal IP ranges like 192.168.0.x, to identify lateral movement or internal C2.

Host-Based Analysis
*   Deploy EDR/antivirus rules for the file hash `017539edeeea6e318309...00919f6cb9ad12a` across all endpoints.
*   Initiate a full, enterprise-wide scan using the new EDR/antivirus rules to identify and quarantine any systems containing the malicious file.
*   For any identified compromised systems, isolate them from the network immediately.
*   On isolated systems, perform a detailed forensic analysis: examine process execution logs, registry modifications, file system changes, and network connections to understand the malware's behavior and persistence mechanisms.
*   Check browser history, download folders, and email clients on potentially affected user workstations for evidence of the `filesem.zip` download or related phishing attempts.

Intelligence & Threat Hunting
*   Utilize threat intelligence platforms (e.g., VirusTotal, AlienVault OTX, PassiveTotal) to pivot on the identified domains (`ep2p.us`, `icaccops.com`), IPs, and the file hash to uncover additional associated indicators, malware families, or TTPs.
*   Perform WHOIS lookups and passive DNS queries for `ep2p.us` and `icaccops.com` to identify registration details, associated infrastructure, or other domains hosted on the same IPs.
*   Investigate the Autonomous System Numbers (ASNs) associated with the malicious IPs to identify other potentially related infrastructure or common hosting providers used by the threat actor.
*   Search for public reports or advisories related to the `ep2p.us` infrastructure or the identified file hash to gain insights into the campaign's objectives, typical targets, and known attack chains.

3. Attack Timeline (Key Indicators)

1 **MAIN**
ep2p_a

2 **DOMAIN**
http://www.icaccops.com/filesem.zip

3 **DOMAIN**
secure.ep2p.us

4 **DOMAIN**
ep2p.us

5 **FILE**
017539edeeea6e318309...00919f6cb9ad12a

6 **FILE**
90506161ed789251b13d...44e46b0dd0066cc

7 **IP**
50.229.189.100

8 **IP**
192.168.0.3

4. ATT&CK® Kill Chain

INITIAL ACCESS

Phishing

T1566

JUSTIFICATION

The URL 'http://www.icaccops.com/filesem.zip' points to a compressed file, which is a common method for delivering malware via phishing emails.

EVIDENCE

- `http://www.icaccops.com/file…`

INITIAL ACCESS

User Execution

T1204

JUSTIFICATION

The presence of downloadable files (a .zip and two file hashes) implies that a user must interact with them (e.g., open, execute) for the compromise to proceed.

EVIDENCE

- `http://www.icaccops.com/file…`
- `017539edeeea6e318309...00919…`
- `90506161ed789251b13d...44e46…`

DEFENSE EVASION

Obfuscated Files or Information

T1027

JUSTIFICATION

The use of generic file hashes for the malicious payloads suggests that the files may be obfuscated or packed to evade signature-based detection.

EVIDENCE

- `017539edeeea6e318309...00919…`
- `90506161ed789251b13d...44e46…`

COMMAND AND CONTROL

Application Layer Protocol

T1071

JUSTIFICATION

The domains 'secure.ep2p.us' and 'ep2p.us' resolving to a public IP '50.229.189.100' and hosting malicious files indicate the use of standard application layer protocols (e.g., HTTP/HTTPS) for C2 communication.

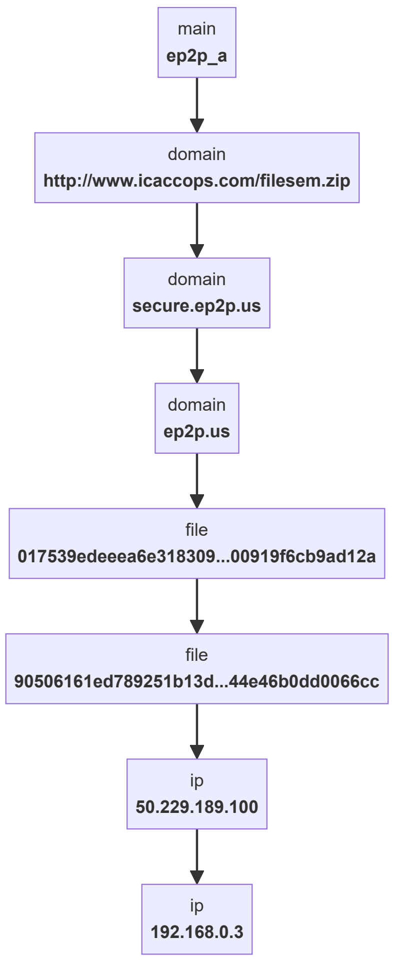
EVIDENCE

- `secure.ep2p.us`
- `ep2p.us`
- `50.229.189.100`

5. MITRE ATT&CK® Matrix Overview

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		Phishing				Obfuscated Files or Information					Application Layer Protocol		
		User Execution											

6. Attack Flow Diagram


main
ep2p_a
domain
http://www.icaccops.com/filesem.zip
domain
secure.ep2p.us
domain
ep2p.us
file
017539edeeea6e318309...00919f6cb9ad12a
file
90506161ed789251b13d...44e46b0dd0066cc
ip
50.229.189.100
ip
192.168.0.3

7. Detailed TTP Analysis

Initial Access

TA0001

Phishing (T1566)

The URL 'http://www.icaccops.com/filesem.zip' points to a compressed file, which is a common method for delivering malware via phishing emails.

RELATED INDICATORS:

🌐 `http://www.icaccops.com/filesem.zip`

User Execution (T1204)

The presence of downloadable files (a .zip and two file hashes) implies that a user must interact with them (e.g., open, execute) for the compromise to proceed.

RELATED INDICATORS:

🌐 `http://www.icaccops.com/filesem.zip`

🗎 `017539edeeea6e318309...00919f6cb9ad12a`

🗎 `90506161ed789251b13d...44e46b0dd0066cc`

Defense Evasion

TA0005

Obfuscated Files or Information (T1027)

The use of generic file hashes for the malicious payloads suggests that the files may be obfuscated or packed to evade signature-based detection.

RELATED INDICATORS:

- `017539edeeea6e318309...00919f6cb9ad12a`
- `90506161ed789251b13d...44e46b0dd0066cc`

Command and Control

TA0011

Application Layer Protocol (T1071)

The domains 'secure.ep2p.us' and 'ep2p.us' resolving to a public IP '50.229.189.100' and hosting malicious files indicate the use of standard application layer protocols (e.g., HTTP/HTTPS) for C2 communication.

RELATED INDICATORS:

- `secure.ep2p.us`
- `ep2p.us`
- `50.229.189.100`

Appendix

A.1 YARA Detection Rule ▼

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

    strings:
        // No byte strings are defined here as the detection relies solely on file hashes.
        // YARA's 'hash' module functions are used directly in the condition section.

    condition:
        // Match if the SHA256 hash of the scanned file matches any of the provided hashes.
        hash.sha256("017539edeeea6e318309307f640d06d56d59690733379ad2b00919f6cb9ad12a") or
        hash.sha256("c6acf614726fc8ee98bac5c0b5bd83b0bb529bc9d0afd3ecac4841325ac6e48b") or
        hash.sha256("0c2be51a259f206a0ec68c7fc65cbac2a7cadcd7e1a8bb5e1bad9ae7f8f2baed") or
        hash.sha256("c14201d7706da3ad1efdb99e799ee2809936fd20484be5b924a6a9a1dd87537c") or
        hash.sha256("90506161ed789251b13d8e8988ba02ac4218fcc1ff0cc8e2644e46b0dd0066cc") or
        hash.sha256("8086a04737e66df563fb4ca440f67d22103b22ec601c30a1009159dc67bb8982") or
        hash.sha256("9f6506cfc2cc321db15a2cc8d29653a9eae6754e05ac790e524d54628def646a") or
        hash.sha256("bf1af55c81a02923b55fc1fad124bc5b086097d5e7bdcec7a5f3d0bca12f3540") or
        hash.sha256("a5706d8f621b337f212b7007a26a145d8601faf92e386e8cd79b25a2c4bb6582") or
        hash.sha256("8693b5f9f91a1d86f46939163326e3db4bb210de4f2b20a7582cffe40f5cdc82") or
        hash.sha256("538d53a975285187a7f7067159c1c44b4943d02d57f4d00c40279c2347968209") or
        hash.sha256("35d6842856228adb7e8badcc12d035d17b12b17d14988b96e45c9d40a690b550") or
        hash.sha256("24459dd44143242d1ae2b7eb6e154b15170aba46d88dc6f6af82605ab21cbf57") or
        hash.sha256("77b0f741b1f7699c1e2c51eb7eb17c3d59dffe9f92ac40f325d298faa7c46229") or
        hash.sha256("f6f46cae6b70af0119a528ce5719622afbda3cfaa481985e45baea1dd04138d8") or
        hash.sha256("b0e7cc4aef2bf48bf9c76a3b4c28978818a97094c20c820e6478a9e63b000a74") or
        hash.sha256("78b844361e94290bbd30a95654f78b4c59bdb3fb9d80b4576664815961bf4a5d") or
        hash.sha256("2131dfee80294e4d927d3dbacac5247b2e1251c5eea11cf0d042611944bed801") or
        hash.sha256("3641cb93bf203ece865d02aa480a829a798ea86c0ff5dd51cfc0234b2f1f51b5") or
        hash.sha256("0a6d8d01d00d7aecbe9b3a341f55521e4a6162272e82ca8f48d146686476e187") or
        hash.sha256("f7897ad701a9a6e22ce4682af75b56b50bee820d34a5d9aed9dc299ee1efd3e8") or
        hash.sha256("8fee5981fc81b93f0cb961e9598e34cfdaa07c0c317e255b0a1959046474e710") or
        hash.sha256("cee161f236efa77c0861c95ad8e00f9026c245a71e9c6b71eee1cb32440425a5") or
        hash.sha256("86e35b41c40abd5dc1f9bbc1a978c403fb46293f7b31d174d3cabf570b49107f") or
        hash.sha256("802e86f28075b411f1dce7288fcc4fb56a8b3ba44577019b52e1efc955bad304") or
        hash.sha256("a9dd6f0f38909be6224e5e2939a51d595d2bab4e6125e3769cd6cee88f4ad7ba") or
        hash.sha256("16a0d09032e4af5623be25cfd19a7e8287d8d891422415878fd0e81fdc3d5ac7") or
        hash.sha256("4a8774bccad5090ccf56ed986120205dba4de1b4e08c62d2960b2b81147ad82d") or
        hash.sha256("74826431fcdd6be0b623d28e41bcefd0a32fa83be95f60a806f0cd46bff4f475") or
        hash.sha256("3d7f09330411e6e7a5c5addc9b679312c85afb7aed988c0a03de1e2e8119a767") or
        hash.sha256("33bde433533e628e7f7e95790caf59d295928c51cfcf2a788d6c43dae429f1ea") or
        hash.sha256("ef8c6fc2b3dad7388deb889d48fa2dedd9aace4ad1f88f8203a5131a62705746")
}
```

A.2 All Indicators of Compromise (IOCs) ▼

INDICATOR VALUE	TYPE
secure.ep2p.us	Domain
ep2p.us	Domain
50.229.189.100	Ip

INDICATOR VALUE	TYPE
96.69.77.132	Ip
173.163.4.108	Ip
173.163.5.13	Ip
50.254.196.145	Ip
mail.ep2p.us	Domain
query.ep2p.us	Domain
query2.ep2p.us	Domain
query3.ep2p.us	Domain
query4.ep2p.us	Domain
www.ep2p.us	Domain
017539edeeea6e318309...00919f6cb9ad12a	File
c6acf614726fc8ee98ba...c4841325ac6e48b	File
c14201d7706da3ad1efd...4a6a9a1dd87537c	File
90506161ed789251b13d...44e46b0dd0066cc	File
9f6506cfc2cc321db15a...24d54628def646a	File
a5706d8f621b337f212b...79b25a2c4bb6582	File
8693b5f9f91a1d86f469...82cffe40f5cdc82	File
24459dd44143242d1ae2...f82605ab21cbf57	File
f6f46cae6b70af0119a5...5baea1dd04138d8	File
b0e7cc4aef2bf48bf9c7...478a9e63b000a74	File
50.254.196.146	Ip
173.163.5.12	Ip
20.99.132.105	Ip
23.216.147.56	Ip
192.168.0.64	Ip
20.99.133.109	Ip
23.55.140.42	Ip
http://www.icaccops.com/filesem.zip	Domain
72.21.81.200	Ip

INDICATOR VALUE	TYPE
192.168.0.3	Ip
23.216.147.76	Ip
13.107.253.70	Ip
131.253.33.203	Ip
151.101.22.172	Ip
192.168.0.61	Ip
20.99.185.48	Ip
20.99.186.246	Ip
23.213.37.172	Ip
23.221.103.220	Ip
23.49.140.110	Ip
192.229.211.108	Ip
20.99.184.37	Ip
96.69.77.131	Ip
20.42.73.29	Ip
20.101.57.9	Ip
52.163.118.68	Ip
192.229.221.95	Ip
104.45.18.177	Ip
51.140.65.84	Ip
13.89.190.88	Ip
51.105.208.173	Ip
13.65.245.138	Ip
23.216.147.78	Ip
69.164.0.128	Ip
13.65.88.161	Ip
13.86.101.172	Ip
51.137.137.111	Ip
168.61.215.74	Ip

INDICATOR VALUE	TYPE
8.252.65.254	Ip
52.173.193.166	Ip
51.145.123.29	Ip
sbzf1aunkq6vugp.west...udapp.azure.com	Domain
time.windows.com	Domain
llap-12060252-9e21.s...projecthilo.net	Domain
msedge.f.tlu.dl.deli...p.microsoft.com	Domain
akadns.net	Domain
a2525.g2.akamai.net	Domain
fp2e7a.wpc.2be4.phicdn.net	Domain
arc.msn.com	Domain
a665.g2.akamai.net	Domain
time.microsoft.akadns.net	Domain
a4836.g2.akamai.net	Domain
a258.y43806g.akamai.net	Domain
a2786.g2.akamai.net	Domain
a5347.g2.akamai.net	Domain
a1905.g2.akamai.net	Domain
dynmsg.modpim.com	Domain
fp2e7a.wpc.phicdn.net	Domain
saipem.it	Domain
ni.scene7.com	Domain
a1143.g2.akamai.net	Domain
a2209.g2.akamai.net	Domain
iris-de-prod-azsc-v2...udapp.azure.com	Domain
download.xbox.com	Domain
scalet404211216t2116...zuresynapse.net	Domain
a852.g2.akamai.net	Domain
arc-west.msn.com	Domain

INDICATOR VALUE	TYPE
prod-streaming-video...m.akamaized.net	Domain
t0.ssl.ak.dynamic.tiles.virtualearth.net	Domain
download.windowsupdate.com	Domain
g.bing.com	Domain
fp-global-cdn.akamaized.net	Domain
discovertakeoneschedule.com	Domain
tse1.mm.bing.net	Domain
fd.api.iris.microsoft.com	Domain
walletprotection.com	Domain
microsoft.akadns.net	Domain
mlcssltestid2lez.wes...udapp.azure.com	Domain
arc.trafficmanager.net	Domain
secure.ep2p.us	Domain
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
mail.ep2p.us	Domain
query.ep2p.us	Domain
query2.ep2p.us	Domain
query3.ep2p.us	Domain
query4.ep2p.us	Domain
www.ep2p.us	Domain
017539edeeea6e318309307f640d06d56d59690733379ad2b00919f6cb9ad12a	File
c6acf614726fc8ee98bac5c0b5bd83b0bb529bc9d0afd3ecac4841325ac6e48b	File
0c2be51a259f206a0ec68c7fc65cbac2a7cadcd7e1a8bb5e1bad9ae7f8f2baed	File
c14201d7706da3ad1efdb99e799ee2809936fd20484be5b924a6a9a1dd87537c	File

INDICATOR VALUE	TYPE
90506161ed789251b13d8e8988ba02ac4218fcc1ff0cc8e2644e46b0dd0066cc	File
8086a04737e66df563fb4ca440f67d22103b22ec601c30a1009159dc67bb8982	File
9f6506cfc2cc321db15a2cc8d29653a9eae6754e05ac790e524d54628def646a	File
bf1af55c81a02923b55fc1fad124bc5b086097d5e7bdcec7a5f3d0bca12f3540	File
a5706d8f621b337f212b7007a26a145d8601faf92e386e8cd79b25a2c4bb6582	File
8693b5f9f91a1d86f46939163326e3db4bb210de4f2b20a7582cffe40f5cdc82	File
538d53a975285187a7f7067159c1c44b4943d02d57f4d00c40279c2347968209	File
35d6842856228adb7e8badcc12d035d17b12b17d14988b96e45c9d40a690b550	File
24459dd44143242d1ae2b7eb6e154b15170aba46d88dc6f6af82605ab21cbf57	File
77b0f741b1f7699c1e2c51eb7eb17c3d59dffe9f92ac40f325d298faa7c46229	File
f6f46cae6b70af0119a528ce5719622afbda3cfaa481985e45baea1dd04138d8	File
b0e7cc4aef2bf48bf9c76a3b4c28978818a97094c20c820e6478a9e63b000a74	File
78b844361e94290bbd30a95654f78b4c59bdb3fb9d80b4576664815961bf4a5d	File
2131dfee80294e4d927d3dbacac5247b2e1251c5eea11cf0d042611944bed801	File
3641cb93bf203ece865d02aa480a829a798ea86c0ff5dd51cfc0234b2f1f51b5	File
0a6d8d01d00d7aecbe9b3a341f55521e4a6162272e82ca8f48d146686476e187	File
50.254.196.146	Ip
f7897ad701a9a6e22ce4682af75b56b50bee820d34a5d9aed9dc299ee1efd3e8	File
8fee5981fc81b93f0cb961e9598e34cfdaa07c0c317e255b0a1959046474e710	File
cee161f236efa77c0861c95ad8e00f9026c245a71e9c6b71eee1cb32440425a5	File
86e35b41c40abd5dc1f9bbc1a978c403fb46293f7b31d174d3cabf570b49107f	File
173.163.5.12	Ip
20.99.132.105	Ip
23.216.147.56	Ip
802e86f28075b411f1dce7288fcc4fb56a8b3ba44577019b52e1efc955bad304	File
a9dd6f0f38909be6224e5e2939a51d595d2bab4e6125e3769cd6cee88f4ad7ba	File
192.168.0.64	Ip
20.99.133.109	Ip
23.55.140.42	Ip

INDICATOR VALUE	TYPE
http://www.icaccops.com/filesem.zip	Domain
72.21.81.200	Ip
192.168.0.3	Ip
23.216.147.76	Ip
13.107.253.70	Ip
131.253.33.203	Ip
151.101.22.172	Ip
192.168.0.61	Ip
20.99.185.48	Ip
20.99.186.246	Ip
23.213.37.172	Ip
23.221.103.220	Ip
23.49.140.110	Ip
192.229.211.108	Ip
20.99.184.37	Ip
96.69.77.131	Ip
16a0d09032e4af5623be25cfd19a7e8287d8d891422415878fd0e81fdc3d5ac7	File
4a8774bccad5090ccf56ed986120205dba4de1b4e08c62d2960b2b81147ad82d	File
74826431fcdd6be0b623d28e41bcefd0a32fa83be95f60a806f0cd46bff4f475	File
3d7f09330411e6e7a5c5addc9b679312c85afb7aed988c0a03de1e2e8119a767	File
33bde433533e628e7f7e95790caf59d295928c51cfcf2a788d6c43dae429f1ea	File
ef8c6fc2b3dad7388deb889d48fa2dedd9aace4ad1f88f8203a5131a62705746	File
20.42.73.29	Ip
20.101.57.9	Ip
52.163.118.68	Ip
192.229.221.95	Ip
104.45.18.177	Ip
51.140.65.84	Ip
13.89.190.88	Ip

INDICATOR VALUE	TYPE
51.105.208.173	Ip
13.65.245.138	Ip
23.216.147.78	Ip
69.164.0.128	Ip
13.65.88.161	Ip
13.86.101.172	Ip
51.137.137.111	Ip
168.61.215.74	Ip
8.252.65.254	Ip