

Cyber Threat Intelligence Report

Event: MoCo

Generated on: Sun, 13 Jul 2025 21:56:41 GMT



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

1. Executive Summary

The 'MoCo' event indicates a critical and multifaceted threat targeting the 'monroe.in.us' domain and its associated infrastructure. Initial compromise likely involves the deployment of suspicious files, as evidenced by multiple file hashes linked directly to the 'co.monroe.in.us' domain and its related IPs. A key aspect of this threat is the apparent abuse of legitimate Microsoft cloud services (e.g., nexus.officeapps.live.com, www.microsoft.com, api.msn.com, windowsupdate.com) for potential command and control (C2) or data exfiltration, a common tactic to evade detection. Furthermore, the presence of numerous highly suspicious '.biz' and '.ru' domains, along with their associated IPs, points to dedicated malicious infrastructure used for C2 communication or hosting additional payloads. A separate cluster of indicators related to mobile applications and ad networks suggests either a broader campaign or a distinct mobile-specific attack vector. The overall threat level is assessed as Critical due to the targeted nature, the volume of malicious indicators, the blend-in-the-noise tactics, and the clear presence of C2 infrastructure, indicating a high probability of significant data compromise and operational disruption. Recommended actions include immediate isolation of affected systems, comprehensive network blocking of all identified malicious IPs and domains, thorough endpoint forensics and remediation, proactive threat hunting across the environment, enhanced monitoring of cloud service activity, and an urgent vulnerability assessment of the targeted infrastructure.

2. Actionable Recommendations

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

****Network Forensics:****

- * Immediately block all identified IPs (66.244.66.1, 66.244.66.13, 66.244.66.27, 66.244.66.30, 66.244.66.31, 66.244.66.100) at the network perimeter (firewall/IPS).
- * Block all identified domains (e.g., gw.monroe.smithvilledigital.net, vpn.co.monroe.in.us, co.monroe.in.us, www.monroe.in.us, mx2.co.monroe.in.us, test-2.smithvilledigital.net) at the DNS level and web proxy/filter.
- * Review firewall, proxy, and DNS logs for any historical and ongoing connections to/from the listed IPs and domains, identifying all internal source IPs.
- * Analyze network traffic logs (e.g., NetFlow/IPFIX) for unusual outbound connections to legitimate Microsoft cloud services (nexus.officeapps.live.com, www.microsoft.com, api.msn.com, windowsupdate.com) from internal hosts, focusing on volume, frequency, and associated processes.

****Host-Based Analysis:****

- * Search all endpoints and servers for the file hash `bfee7b955c02035b3668...e2a7d8e25089854`.
- * Isolate any systems found communicating with the identified malicious IPs/domains or hosting the suspicious file.
- * Perform full forensic imaging of identified compromised hosts for deeper analysis.
- * Examine endpoint logs (EDR, Sysmon, event logs) on compromised systems for process execution, network connections, file modifications, and persistence mechanisms related to the identified indicators.
- * Investigate the specific processes initiating connections to Microsoft cloud services on affected hosts.

****Intelligence & Threat Hunting:****

- * Submit the file hash `bfee7b955c02035b3668...e2a7d8e25089854` to public threat intelligence platforms (e.g., VirusTotal) to gather additional context, related samples, and known malware families.
- * Pivot on the listed IPs and domains (especially `smithvilledigital.net` and the `66.244.66.x` range) using OSINT tools (e.g., Passive DNS, WHOIS, Shodan) to identify any other associated infrastructure or campaigns.
- * Actively hunt for network connections to '.biz' and '.ru' domains across the environment, as the AI analysis indicates these are likely C2.
- * Research "MoCo" as a potential campaign identifier to find any public reporting or additional indicators.
- * Initiate an urgent vulnerability assessment of all `monroe.in.us` and `smithvilledigital.net` infrastructure, focusing on external-facing systems, to identify the initial compromise vector.

* If applicable, investigate mobile device management (MDM) logs and network traffic for indicators related to mobile applications and ad networks, as suggested by the AI analysis.

3. Attack Timeline (Key Indicators)

1 MAIN
MoCo

2 DOMAIN
co.monroe.in.us

3 FILE
bfee7b955c02035b36681cb969caad87f6b9d42a3bb195b85e2a7d8e25089854

4 FILE
3fe1f4be5e95b8b3af2bab2fbe265ebcd6cb906fdedb2e5d6ff40bab8ad8acc8

5 DOMAIN
nexus.officeapps.live.com

6 DOMAIN
cpclnad.biz

7 DOMAIN
iwnemfam.ru

8 IP
44.221.84.105

9 IP
74.134.111.120

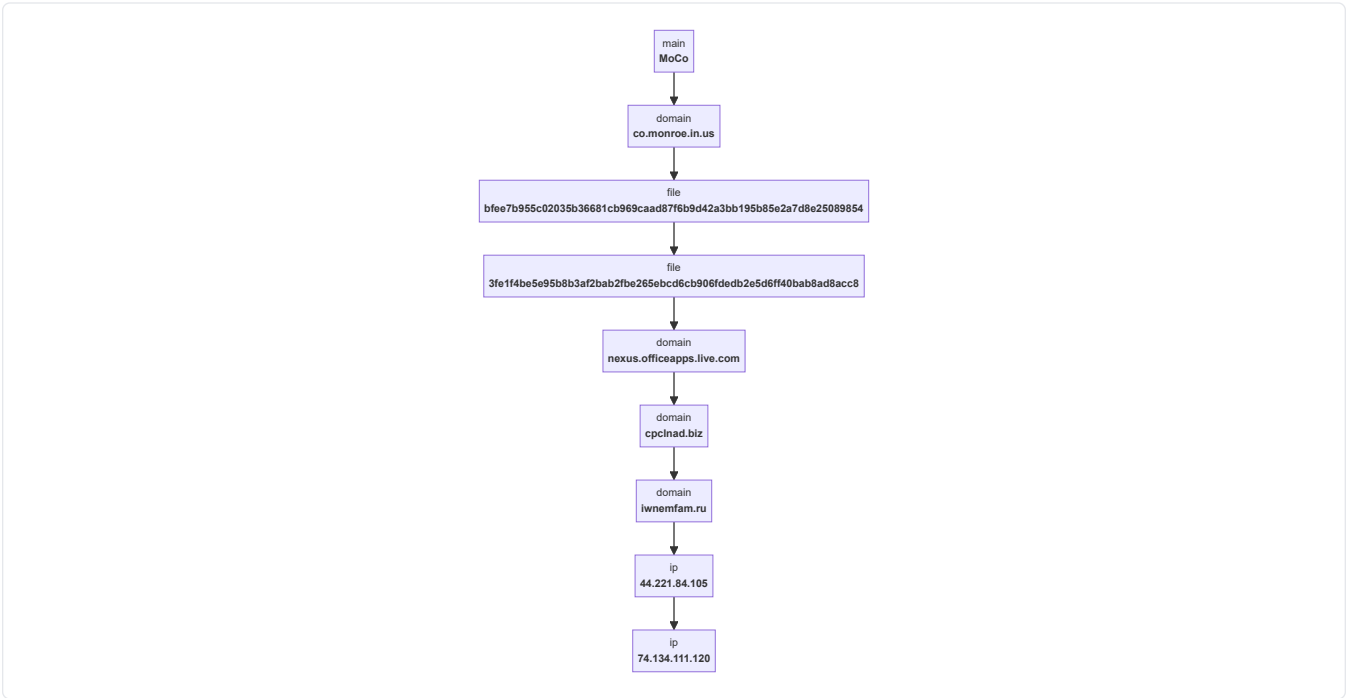
4. ATT&CK® Kill Chain

INITIAL ACCESS Phishing T1566	COMMAND AND CONTROL Application Layer Protocol T1071
JUSTIFICATION The presence of malicious file hashes and suspicious domains, alongside a legitimate-looking Microsoft domain, strongly suggests a phishing attempt to deliver malware or harvest credentials.	JUSTIFICATION The identified suspicious domains and IP address, along with the potential use of a legitimate domain for masquerading, are common indicators of command and control communications over application layer protocols.
EVIDENCE <div><div>📄 bfee7b955c02035b36681cb969ca...</div><div>📄 3fe1f4be5e95b8b3af2bab2fbe26...</div><div>🌐 cpclnad.biz</div><div>🌐 iwnefmam.ru</div><div>🌐 nexus.officeapps.live.com</div></div>	EVIDENCE <div><div>🌐 cpclnad.biz</div><div>🌐 iwnefmam.ru</div><div>📄 44.221.84.105</div><div>🌐 nexus.officeapps.live.com</div></div>

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									Application Layer Protocol		

6. Attack Flow Diagram



7. Detailed TTP Analysis


Initial Access

TA0001

Phishing (T1566)

The presence of malicious file hashes and suspicious domains, alongside a legitimate-looking Microsoft domain, strongly suggests a phishing attempt to deliver malware or harvest credentials.

RELATED INDICATORS:

-  bfee7b955c02035b36681cb969caad87f6b9d42a3bb195b85e2a7d8e25089854
-  3fe1f4be5e95b8b3af2bab2fbe265ebcd6cb906fdedb2e5d6ff40bab8ad8acc8
-  cpclnad.biz
-  iwnemfam.ru
-  nexus.officeapps.live.com





Command and Control

TA0011

Application Layer Protocol (T1071)

The identified suspicious domains and IP address, along with the potential use of a legitimate domain for masquerading, are common indicators of command and control communications over application layer protocols.

RELATED INDICATORS:

-  cpclnad.biz
-  iwnemfam.ru
-  44.221.84.105
-  nexus.officeapps.live.com

Appendix

A.1 YARA Detection Rule



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

  strings:
    // No direct string patterns from file content are provided.
    // Filename indicators are interpreted as SHA256 hashes, which are checked in the condition section.

  condition:
    hash.sha256() == "bfcee7b955c02035b36681cb969caad87f6b9d42a3bb195b85e2a7d8e25089854" or
    hash.sha256() == "3fe1f4be5e95b8b3af2bab2f26e265ebcd6cb906fdebd2e5d6ff40bab8ad8acc8" or
    hash.sha256() == "1d3889846c78298de4e701b54bc58af3c7d41146fdef717eccc7c04123805a1a" or
    hash.sha256() == "da4a75ed01227a575db2b87423b2d3a09fa738886764df5d416ba67ee3ae2217" or
    hash.sha256() == "17ad9bb615ae018d4bc9e724663a6b124157c43f670237f4e71f1e7f2f081df9" or
    hash.sha256() == "0c2fedbe0423d14f6d48c8f802437771f413e1318c5d9fd9429eb58c00df37bf" or
    hash.sha256() == "30bdf413c08247b47fed3340a4fb7b897f91a45415896c2504bb6465ea5f7f5f" or
    hash.sha256() == "86d99f86390774790289752558eee73cdc5cca3d0e08f26f77dc4d7655dc0aa5" or
    hash.sha256() == "4d419290f9b22edd988addf09ee61bb7a4fad948041ead12adee880df13e059d" or
    hash.sha256() == "eb05f2ecc2cc310063284fffa0eca04107c38a1d13da57b5da02f6aab0f4b39d" or
    hash.sha256() == "c0f4221a34d5b32c79f63a6ccf5aa80541fc1174ccd61d285d7cdca52311de2f" or
    hash.sha256() == "8ee77b30d56cdcde4a89950a23c43ff10470fd2063cf436d68ff68b1f4b09a1c" or
    hash.sha256() == "29e550dfab69b3248ed65c58773d01073090c1f14db2f6522400f183ea3aa5ac" or
    hash.sha256() == "858a154a4223a59068c2a847aa088d9dfa47bc13ade2b4baa6c83faa0d244796" or
    hash.sha256() == "50948e64098b04a0eaea711ae4c3e9b91fa765e70696c1483cd1c0d63e11b57a" or
    hash.sha256() == "3f072dab60bed8886950f2127ae7c8d886ccc0550c74f0018202d9625017807a" or
    hash.sha256() == "7ee78939d4d6b50589a78b217796e471380996ef841058399ff9d8de8429a49a" or
    hash.sha256() == "d225dc131ce6a0adca96e02cf0a7101294626b55eeaa7465e9a83d3f66a713e" or
    hash.sha256() == "93b30a9e1aa6e71e5ec99dd207e4e4b322addf1f274c9785143573b943217b5a" or
    hash.sha256() == "464426386bd530d9ca0c00671c70abfe694a9e178582fbd6dc41ecca92c9eba" or
    hash.sha256() == "b761803bb96f50eb90ce3defce0549bb282f054e30fb913a9488b789cde734ee" or
    hash.sha256() == "0a4d7e4860afac36c43f2e5272678b7e267b46618ab46a596dd28dbc4c5915e3" or
    hash.sha256() == "22aa981f10e839fbf2c5c3a8f3de7caa2f9c3add7af4750420fd2b1a05be1709" or
    hash.sha256() == "452acb807a408b767ad4318d01e17053499521dc201aa502e47950726872c83" or
    hash.sha256() == "48e537902c03a3eee4790fc97ee072cddc7c1a90122702dd18243d8c12a0d99a" or
    hash.sha256() == "56d8f8af1e45eff640be34914a9dc332e6154108f194deec5853d66dac766496" or
    hash.sha256() == "6c1b1e6b7a1f5a9499a3f7c66939b933d89efd7bff818255f57cd182c7474650" or
    hash.sha256() == "71356358d9c1df71801f9bfbf5b040ab664a4b06e6c73d29e4801e23fe9f1f9f" or
    hash.sha256() == "7dfd9f131494d23952f4428b9a6d20f358910796729c7ac4815f76a14b3c643e" or
    hash.sha256() == "8b064ebb257b55ee09b619b791475058b4d9d2b90907ec727e70235e5b25b730" or
    hash.sha256() == "7dc546ebd1e2a40b2785df2e18d87058898ec87740aec8f4c1bf224987b7710" or
    hash.sha256() == "a48c02fd36302685b5fbb3691db0fb2c4aca77c0b3b1df9aa7ec6f154affa0a8" or
    hash.sha256() == "d1614ad99aded9f6f5c1be7fe7ffa5124bd04a526580da3818ea8a954e852aa6" or
    hash.sha256() == "dfbde381fde1a284c81a72d06a1a43faf49cd1c085c87234e34e50b881567806" or
    hash.sha256() == "ee9e288c3495fd548fd49095be08807f215fc0780064e179011098c0c7461a34" or
    hash.sha256() == "6230814bf5b2d554397580613e20681752240ab87fd354eccec188c1eabe0e97" or
    hash.sha256() == "c64ed5c2a323c00e84272ad3a701caebe1dcceb67231978de978042f09635fa7" or
    hash.sha256() == "e23040951e464b53b84b11c3466bbd4707a009018819f9ad2a79d1b0b309bc25" or
    hash.sha256() == "fa6f9722c1b9542271766681a939b53f7e0c2616155f41b72b6debb0e65aed6b" or
    hash.sha256() == "7dc5546ebd1e2a40b2785df2e18d87058898ec87740aec8f4c1bf224987b7710" or
    hash.sha256() == "01f15adfb4b3ba22946b914bfc50fcb2b746841511c9c69fd439bb971ba128df" or
    hash.sha256() == "c2ffecdc77fa99cdf56c81099958fbdca11a08d3b02e3b7ef238739b000404cfd" or
    hash.sha256() == "e4862e12edfe5bf0c85e57fe1d6e9828f2c76a4b98ffae1b801513899a27a404" or
    hash.sha256() == "1a724aa3ce05da87e26dc7b963ecc405234444eb71d9ae3a3930a7fb7ac0c042" or
    hash.sha256() == "3102cec0048148d22b5ba5628d744a7eae55efdae50a7dbb59070682fdb7d660" or
    hash.sha256() == "47bc56e666ab3a33cb3ada887d70e1d5484d34bcfa0d6061763034adbb4b4930" or
    hash.sha256() == "47f106f8f50a49a939e80187e23069f0e685907223832211dddcaddddef09184b" or
    hash.sha256() == "4847cdc9d0d8bb940dae76e5231cb46dda1334885afef4e6a5b257d03d026b" or
    hash.sha256() == "4909cc6023e1b633f3eb5398b6cce6790e5cc34fecb39d878cd9b26c4d56ea91" or
```

hash.sha256() == "4fd87aaddc9106bd8179adfc07a9e8fa0cefc3dcd9604712874af3376f0ea01" or
hash.sha256() == "5a41e0316f8c2fe59c084f861483457d62bf4977e3dc8e1aab8a07b160f3991" or
hash.sha256() == "5f7a674e1c6b0a3edb3532ee9276b8f5b694526a7f47597e7b972bbd197907fb" or
hash.sha256() == "6a290aac09aa391e4637fc34f1aba53da8428e458b2f0225c4a16199ce7a1c7" or
hash.sha256() == "6e9274c9c1acdf19ca64138163d1c5ea0ba78074a01bbc459e48469c597fff25" or
hash.sha256() == "7768dae586920feac88943b260caa4f9a26bd357603d81517431d38f5e026594" or
hash.sha256() == "7d590200863f6a0d93834ecf02c2367fe5ba24ff4145d6c89ad7840587e453a3" or
hash.sha256() == "89f2aca9a2d7d10117e9ed30fa99c700cdf2712995db3bbc7835a84a271418e1" or
hash.sha256() == "8d34fbc3eff2a634be965b2dcc3a5655bcc6f04f5ab7e9697e91d87874da185" or
hash.sha256() == "947075792a2af3817fbc27da5627f3d160b0d32d7a8f62a64c02abe5bcb46fef" or
hash.sha256() == "96175287d907186c92662735a29580dc151320582669c1e7984368534d87916a" or
hash.sha256() == "983ea6e2b83565788f4ffa6362260c9d8b51a07fed7892b65ce8ba4bd5d07247" or
hash.sha256() == "adca17f0bdf3c81269602b1c0c263f5688098b92daae69ea2c11d7db87c74872" or
hash.sha256() == "89f2aca9a2d7d10117e9ed30fa99c700cdf2712995db3bbc7835a84a271418e1" or
hash.sha256() == "000a35caeb27c4e8b9fdf455ab1991081138b857a0f347e521fc32563a49cc8c" or
hash.sha256() == "001cc58e88ee2bf06de698d629a888b0cc69e728eba3297d199f8a04770ae4d1" or
hash.sha256() == "001ea1697fff9db1d9891ee31677ef925240185d8204683bcd185459e2edb683" or
hash.sha256() == "00211659db8833b98618936d199ef1fffe7274d12a541de3d9d8fc6d7e21293c" or
hash.sha256() == "003af175b42dd165367c93a14b13eaa91016d637db484e01427d3b2e0ffa4a4f" or
hash.sha256() == "0046138927938ef7cd3aea09f7978a4201e6f6b7ed61bd8b6a1b381a3b4a9c1" or
hash.sha256() == "0052a3ef1b8f4463ff4cc19c783ba5db033e11d638b24d7219fcc3f3a430c5a4" or
hash.sha256() == "0053e31957446978773c7e5aa5ea81889b2f6d0f730ead502232419490aedaa3" or
hash.sha256() == "005abda499e24c08ef0f29143df57c7206e679edf7d4456e868a8665649cab7" or
hash.sha256() == "005ba00a46df16c0c31ce90f947eddae62997ce847a6d094dfb5a871a769aee2" or
hash.sha256() == "00730d58342c3d70d5060838997369e63f842acd91cee4b0c33ff8e728060131" or
hash.sha256() == "0075e3cbb63fb0b7d0548f3dc023c07e760247680f6e5340ead924f2ed52028e" or
hash.sha256() == "007d275f0491ddd9b36ee088ef6b3415d59a5cc9ba2ca8d4bbfac3496f91a852" or
hash.sha256() == "00875137c3a94523c74e6a9234b76174c8a7b573a3101514f34caba8344feae8" or
hash.sha256() == "008f18ac3976971ff90478974a98900f4d02005e8bb6c6503024b093ea9c101cc" or
hash.sha256() == "0093c863702ff2323f80eaf6ba00228ae3e6bd381dfc38b3cbb07f114b701c1c" or
hash.sha256() == "00b7aaef5c5c8768b498a4065707ddac6dcbe3585d5e33b96338423a60c390f3" or
hash.sha256() == "00c1b47c050dc2a09043d124cc11d6f5f0cf4aae573619c625e0b06b6e47104a7" or
hash.sha256() == "00d02a97c3efc2539f656663092f3fe981759a98ccdaedd4560358ee5a47a098" or
hash.sha256() == "ace43fc2b15725e28c9377542300ada8ce31e2ec51f44c3d59e006c467d491b5" or
hash.sha256() == "db01b514803c170f9668f6e6dc95fe2595a6dd5518acaf7eae45d4f82bc64d3" or
hash.sha256() == "caa419ae23ec1dd04b5d86496691550cffe8a872ff987405b4eded2bab874937c" or
hash.sha256() == "01e450aa49ba5be377be683cd1e007a992e0dc79f2fb34571667334c52f68ca9" or
hash.sha256() == "00c0bb960eae9ae9e49eb9ba9bee6c592c5d1374158cea09de80d45744d61c105" or
hash.sha256() == "190b219271c822b5499a42508bc5578914a3b54e8e220654f1405f9cb21d8dfa" or
hash.sha256() == "1c8d6d5830973d4cd4865f484f728f5556bc433cb9a5973b706eaf75c087807e" or
hash.sha256() == "1db0d69c233dd4975f4dbfab7cacf97f86481b87fa1b9c81cea5ee1a8d32de3f" or
hash.sha256() == "26cbdff92bbd91e4b33f970538dae8662133d97b28c3985394e64e708097ad41" or
hash.sha256() == "302545c98e225a1f0ddccbab3ffdd9f69bf91e51664f53bdfc2269042c55ede" or
hash.sha256() == "34c9d086c2af471a45e38428baf823f9112459854d2963f883a04d11d210f7fe" or
hash.sha256() == "52bb8e44ebd9ee0715f4490ad86f5c10ed8c4e71e3b51b9a7505cbdb3e88d7c7" or
hash.sha256() == "759c66e423c7c53c17b0be1456b336592ecc91fe440c0ff637f35830fd7f4869" or
hash.sha256() == "90937f087a01b79741d43b0140e19e5546d3ff6e86bc800f1c92a8a7fdbb771" or
hash.sha256() == "a99ca9f79d7e5c89865ce90fc1027d9fad6ec3b26f8fab5712af7e97ab40a26b" or
hash.sha256() == "b9cb434e82ac9204495deb6addc2707c5087aa1e416885f5b9de0be30a93f61d" or
hash.sha256() == "bb0c29c4f4d2f1721a6016b642195e98e5b1bb6f01e2f6d019ae58dd291a7fe9" or
hash.sha256() == "d02567dfc4e93b82b6f3164c6a32838b77457f7a879fa589f62b9f716e099874" or
hash.sha256() == "d0db7afbe28a845fa75aebfaccfe1d16e64f719d7c45f87a79165903a29315d7" or
hash.sha256() == "d434c7720a5eb9017527080c2f7dbdd07c881d5175812080d520a512f1a76d91" or
hash.sha256() == "de235889fcc37a882a93485741ae6520189774eed7f940064e8f731f7cae79a4" or
hash.sha256() == "f0fc2852843c27a813ac3bae288de70f311191148c863079dd6f1bfc40c566" or
hash.sha256() == "000000a512a847e8ed28fdaf433d6dd601a88d74e5dd7d71bd07817b1ce3a2a2" or
hash.sha256() == "0000014a634db98f85038b833a8dfc50d5fb13a464e0b25994e439aef830cd70" or
hash.sha256() == "00000238ff09aa0e0e0ce9fb075a62592f1b35c719986c3946db1e7fd5a6ab05" or
hash.sha256() == "000002869785aa152f0830368c0ae50653ec1f70aadfa665dea26bb201d49fd7" or
hash.sha256() == "00000428f03c4512a07d064719d8aa5d85462cac78e4d4c342b9818fb5e2121c" or
hash.sha256() == "000004393aafab2eaba9cda3dd56db0f8a6506d1fb9b566b37c70dcf0e5132ca" or
hash.sha256() == "00000439a3ffa123c3f9bc45e5e821351b1a5c276871b36447ab80c74261f354" or
hash.sha256() == "0000048d976a523a117a63cb21eab6c7d88bf510352cd9f9f27838475a1ec8ed" or
hash.sha256() == "0000064cacbf07d04bd4c5151f7fad673bffff4b5e803faaaf872cdcb355a18a" or
hash.sha256() == "0000067fbb4783bb96552304c7c9d0f33d89988621ccbdcc7a3654b99f49ce6" or
hash.sha256() == "00000722ff984d5cd9cd766d12c70eccc7a2ad7502999c5a99d582c79b92c1a6" or
hash.sha256() == "0000079dfb0c33717924384f3dcce65bf7656316467cc6de3735ac33fb8124b7" or
hash.sha256() == "000007b8271a49ecfcb407d34575f71b25dca41cab52f46068677dd89dc662af" or

```

hash.sha256() == "000007cb124a92fd3c6553ca4d61ed432887736f33825d8239db72fafdebd5be" or
hash.sha256() == "00000893d37db36ef14c3922141928a04f92d27360ceba9af43d6d003d471bc7" or
hash.sha256() == "00000944c9e053f1c545ef1b4b21bfbf6f07265b6449bfffdeb4b761c78416e6e" or
hash.sha256() == "00000a7d66dc4e9ff3f21f544341cddc0259bdba2ccf95523119d68ee919c17d" or
hash.sha256() == "00000a8c4d72a3818c10e4fbb578b8923ba3754021e50b627f3eb87b9d1d9f81" or
hash.sha256() == "00000a8d83184e8f603b6a2682439deab7d9935c7414add6961fb919e86ecacd" or
hash.sha256() == "00000af7e147252a9838e0694eec2cbd5fdd3482bf8eeee7eaae8c0cc5969c61" or
hash.sha256() == "211bdf19381949eb8115d9b099670d0277e91531afea23e23a11879d9a29f87d" or
hash.sha256() == "24d6742653761510338bb242f67a627d03a7ccf98f0ab8d21292034f9bb3bd34" or
hash.sha256() == "5845a3a9aa81f92f4a2ea69f6353d9096b89b186befffd1c81788ccc8edf0bf15" or
hash.sha256() == "a1cce8a43ef384aa3e44fbc222f3d99a869ae2078872f514e5ad8f383568a8b9" or
hash.sha256() == "bf34420ca94118eb47dad3f01abfe68433534295268e66207a2e7a7889be5148" or
hash.sha256() == "e11eb59cf535da90ef6617ac9256138659a8420b47afbe8749a8076fbdc29bc" or
hash.sha256() == "226c926cb2beb6b4cbbb7a42f5e860b1da02530cdc402e6b6145170ef7b3eb3f" or
hash.sha256() == "291bf6745bb5a406186261a5b916b831c0230c877db267731f0a3ab431649038" or
hash.sha256() == "62e03c94f568196ad4e5fd181ef60cf3e2c03f73ec336faf10bba0a15a96182d" or
hash.sha256() == "d1d308e355e4cff921461c9c015f4f3ac88ea29736a46e5a28c04d8822e132e6" or
hash.sha256() == "d85bdad87177cc72973c0ffca03166c0739f36f394c58915575e51f94ed61388" or
hash.sha256() == "f3137b0da2063617a279b8cdf1438b4ac083eed1982fe65d7e293eff626b8b66" or
hash.sha256() == "f4b7c8b9553e0b1c9a77da6e94750099923570ad14d966c739eace5e17a2e399" or
hash.sha256() == "3d04ecde07280474cc7e73f6e547a558ebea6d61555b2fccd62ad2c7e8441954"
}

```

A.2 All Indicators of Compromise (IOCs)



INDICATOR VALUE	TYPE
66.244.66.30	Ip
gw.monroe.smithvilledigital.net	Domain
66.244.66.13	Ip
bfee7b955c02035b3668...e2a7d8e25089854	File
66.244.66.27	Ip
vpn.co.monroe.in.us	Domain
27.66.244.66.monroe...illedigital.net	Domain
mx2.co.monroe.in.us	Domain
66.244.66.31	Ip
66.244.66.1	Ip
66.244.66.100	Ip
co.monroe.in.us	Domain
www.monroe.in.us	Domain
test-2.smithvilledigital.net	Domain
www.smithvilledigital.net	Domain
monroe.in.us	Domain

INDICATOR VALUE	TYPE
15.197.183.30	Ip
209.43.47.37	Ip
66.244.66.20	Ip
gis.co.monroe.in.us	Domain
gisserver.co.monroe.in.us	Domain
helpdesk.co.monroe.in.us	Domain
gistest.co.monroe.in.us	Domain
ftp.co.monroe.in.us	Domain
legacy.co.monroe.in.us	Domain
mercury.co.monroe.in.us	Domain
docs.co.monroe.in.us	Domain
cms.co.monroe.in.us	Domain
mx1.co.monroe.in.us	Domain
webmail.co.monroe.in.us	Domain
mail.co.monroe.in.us	Domain
autodiscover.co.monroe.in.us	Domain
www.co.monroe.in.us	Domain
3fe1f4be5e95b8b3af2b...ff40bab8ad8acc8	File
1d3889846c78298de4e7...cc7c04123805a1a	File
da4a75ed01227a575db2...16ba67ee3ae2217	File
17ad9bb615ae018d4bc9...71f1e7f2f081df9	File
0c2fedbe0423d14f6d48...29eb58c00df37bf	File
30bdf413c08247b47fed...4bb6465ea5f7f5f	File
86d99f86390774790289...7dc4d7655dc0aa5	File
4d419290f9b22edd988a...dee880df13e059d	File
eb05f2ecc2cc31006328...a02f6aab0f4b39d	File
c0f4221a34d5b32c79f6...d7cdca52311de2f	File
8ee77b30d56cdcde4a89...8ff68b1f4b09a1c	File
29e550dfab69b3248ed6...400f183ea3aa5ac	File

INDICATOR VALUE	TYPE
858a154a4223a59068c2...6c83faa0d244796	File
50948e64098b04a0eaea...cd1c0d63e11b57a	File
3f072dab60bed8886950...202d9625017807a	File
7ee78939d4d6b50589a7...ff9d8de8429a49a	File
d225dc131ce6a0adca96...e9a83d3f66a713e	File
93b30a9e1aa6e71e5ec9...43573b943217b5a	File
464426386bd530d9ca0c...dc41ecca92c9eba	File
b761803bb96f50eb90ce...488b789cde734ee	File
nexus.officeapps.live.com	Domain
52.111.229.47	Ip
52.111.236.24	Ip
52.111.236.25	Ip
52.111.243.25	Ip
52.111.243.26	Ip
0a4d7e4860afac36c43f...dd28dbc4c5915e3	File
22aa981f10e839fbf2c5...0fd2b1a05be1709	File
452acbf807a408b767ad...e47950726872c83	File
48e537902c03a3eee479...8243d8c12a0d99a	File
56d8f8af1e45eff640be...853d66dac766496	File
6c1b1e6b7a1f5a9499a3...57cd182c7474650	File
71356358d9c1df71801f...4801e23fe9f1f9f	File
7dfd9f131494d23952f4...15f76a14b3c643e	File
8b064ebb257b55ee09b6...e70235e5b25b730	File
97da3c982874ec87dcba...179b82fa0014346	File
a48c02fd36302685b5fb...7ec6f154affa0a8	File
d1614ad99aded9f6f5c1...8ea8a954e852aa6	File
dfbde381fde1a284c81a...34e50b881567806	File
ee9e288c3495fd548fd4...11098c0c7461a34	File
204.79.197.203	Ip

INDICATOR VALUE	TYPE
89.35.237.180	Ip
6230814bf5b2d5543975...cf188c1eabe0e97	File
c64ed5c2a323c00e8427...978042f09635fa7	File
e23040951e464b53b84b...a79d1b0b309bc25	File
204.89.253.55	Ip
66.244.66.44	Ip
fa6f9722c1b954227176...b6debb0e65aed6b	File
7dc5546ebd1e2a40b278...c1bf224987b7710	File
01f15adfb4b3ba22946b...439bb971ba128df	File
c2ffecd77fa99cdf56c8...38739b000404cfd	File
e4862e12edfe5bf0c85e...01513899a27a404	File
www.microsoft.com	Domain
1a724aa3ce05da87e26d...930a7fb7ac0c042	File
3102cec0048148d22b5b...9070682fdb7d660	File
47bc56e666ab3a33cb3a...63034adbb4b4930	File
47f106f8f50a49a939e8...ddcadddef09184b	File
4847cdc9d0d8bb940da...6a5b257d03d026b	File
4909cc6023e1b633f3eb...cd9b26c4d56ea91	File
4fd87aaddc9106bd8179...874af3376f0ea01	File
5a41e0316f8c2fe59c08...ab8a07b160f3991	File
5f7a674e1c6b0a3edb35...b972bbd197907fb	File
6a290aacc09aa391e463...c4a16199ce7a1c7	File
6e9274c9c1acdf19ca64...e48469c597fff25	File
7768dae586920feac889...431d38f5e026594	File
7d590200863f6a0d9383...ad7840587e453a3	File
89f2aca9a2d7d10117e9...835a84a271418e1	File
8d34fbe3eff2a634be96...7e91d87874da185	File
947075792a2af3817fbc...c02abe5bcb46fef	File
96175287d907186c9266...84368534d87916a	File

INDICATOR VALUE	TYPE
983ea6e2b83565788f4f...ce8ba4bd5d07247	File
adca17f0bfd3c8126960...c11d7db87c74872	File
130.163.182.133	Ip
130.163.184.43	Ip
130.163.190.78	Ip
192.168.0.17	Ip
209.43.1.143	Ip
209.43.1.226	Ip
209.43.100.212	Ip
209.43.101.219	Ip
209.43.102.155	Ip
209.43.104.189	Ip
209.43.104.23	Ip
209.43.109.117	Ip
209.43.110.129	Ip
209.43.110.207	Ip
209.43.114.16	Ip
209.43.114.58	Ip
209.43.115.37	Ip
209.43.118.135	Ip
209.43.118.174	Ip
209.43.12.127	Ip
business.bing.com	Domain
bzib.nelreports.net	Domain
edge-mobile-static.azureedge.net	Domain
edgedl.me.gvt1.com	Domain
13.107.6.158	Ip
23.215.55.139	Ip
23.215.55.144	Ip

INDICATOR VALUE	TYPE
239.255.255.250	Ip
34.104.35.123	Ip
2fbffdiny3hekzgye5g3...grqyon.dns0.org	Domain
vjzwub55z3yhqebokmhr...423pop.dns0.org	Domain
yhk225bv63wg5d25qiy...lg5m14.dns0.org	Domain
vjzwub55z3yhqebokmhr...423pop.dns0.org	Domain
pwlv2vaddy147jxv5qet...t89f7n.dns0.org	Domain
vjzwub55z3yhqebokmhr...423pop.dns0.org	Domain
alt1.edgedl.me.gvt1.com	Domain
alt3.edgedl.me.gvt1.com	Domain
alpmuggj5cxnm7o46f...n9cr2u.dns0.org	Domain
ir5nm1k2ukxbhhtonr6i...c97qc1.dns0.org	Domain
i7n6s23mey3wrd2ro5tf...facahr.dns0.org	Domain
i7n6s23mey3wrd2ro5tf...facahr.dns0.org	Domain
aegpojpvpa7fxwmgft7r...aczlku.dns0.org	Domain
edgedl.me.gvt1.com.1...30c5.roksit.net	Domain
z6d2564z6noxcltkl3n...ebkqy.dns0.org	Domain
edgedl.me.gvt1.com.9...c5e0.roksit.net	Domain
108.177.119.101	Ip
108.177.119.94	Ip
13.107.253.38	Ip
142.251.31.95	Ip
172.217.218.84	Ip
172.217.218.94	Ip
23.205.109.82	Ip
23.205.109.91	Ip
74.125.128.94	Ip
config.edge.skype.com	Domain
00054c77269f53ed4b8d...d601bf940c4937f	File

INDICATOR VALUE	TYPE
000a35caeb27c4e8b9fd...1fc32563a49cc8c	File
001cc58e88ee2bf06de6...99f8a04770ae4d1	File
001ea1697fff9db1d989...d185459e2edb683	File
00211659db8833b98618...9d8fc6d7e21293c	File
003af175b42dd165367c...427d3b2e0ff4a4f	File
0046138927938ef7cd3a...6a1b381a3b4a9c1	File
0052a3ef1b8f4463ff4c...9fcc3f3a430c5a4	File
0053e31957446978773c...232419490aadaa3	File
005abda499e24c08ef0f...68a86665649cab7	File
005ba00a46df16c0c31c...fb5a871a769aee2	File
00730d58342c3d70d506...33ff8e728060131	File
0075e3cbb63fb0b7d054...ad924f2ed52028e	File
007d275f0491ddd9b36e...bfac3496f91a852	File
00875137c3a94523c74e...34caba8344feae8	File
008f18ac3976971ff904...24b093ea9c101cc	File
0093c863702ff2323f80...bb07f114b701c1c	File
00b7aaef5c5c8768b498...338423a60c390f3	File
00c1b47c050dc2a09043...5e0bdb6e47104a7	File
00d02a97c3efc2539f65...60358ee5a47a098	File
http://www.if.ee/	Domain
https://api.msn.com/...4900de4d1baf000	Domain
http://download.wind...504821cdbd8.cab	Domain
20.82.32.45	Ip
199.232.214.172	Ip
www.if.ee	Domain
if.ee	Domain
216.9.137.80	Ip
ace43fc2b15725e28c93...9e006c467d491b5	File
http://74.134.111.120/default.htm	Domain

INDICATOR VALUE	TYPE
http://77.122.245.30/welcome.htm	Domain
http://77.122.245.30/start.htm	Domain
163.com	Domain
163mx00.mxmail.netease.com	Domain
163mx01.mxmail.netease.com	Domain
163mx02.mxmail.netease.com	Domain
163mx03.mxmail.netease.com	Domain
1646639377.mail.outlook.com	Domain
1974151189.mail.outlook.com	Domain
2d7633219391c9403033...ail.outlook.com	Domain
323805130.mail.outlook.com	Domain
394364422.mail.outlook.com	Domain
44uit.hm	Domain
4dorganising.co.uk	Domain
6og5ln.us	Domain
ad.state.mi.us	Domain
adinet.com.uy	Domain
ag.state.oh.us	Domain
ag.state.oh.us.s9a1.psmtip.com	Domain
ag.state.oh.us.s9a2.psmtip.com	Domain
ag.state.oh.us.s9b1.psmtip.com	Domain
ag.state.oh.us.s9b2.psmtip.com	Domain
0.0.0.0	Ip
1.70.154.156	Ip
10.1.10.3	Ip
106.10.165.51	Ip
106.10.166.54	Ip
108.59.49.249	Ip
108.59.49.250	Ip

INDICATOR VALUE	TYPE
110.45.136.134	Ip
110.45.136.135	Ip
110.45.215.15	Ip
112.127.57.38	Ip
114.108.154.167	Ip
114.108.154.181	Ip
114.108.154.199	Ip
114.108.154.208	Ip
114.108.154.231	Ip
114.108.154.234	Ip
114.108.154.241	Ip
115.114.58.13	Ip
115.114.58.15	Ip
77.122.245.30	Ip
74.134.111.120	Ip
db01b514803c170f9668...ae45d4f82bc64d3	File
caa419ae23ec1dd04b5d...eded2bab874937c	File
iwnemfam.ru	Domain
jilvoqsi.ru	Domain
taosiram.ru	Domain
01e450aa49ba5be377be...667334c52f68ca9	File
0c0bb960eae9ae9e49eb...80d45744d61c105	File
190b219271c822b5499a...1405f9cb21d8dfa	File
1c8d6d5830973d4cd486...06eaf75c087807e	File
1db0d69c233dd4975f4d...ea5ee1a8d32de3f	File
26cbdf92bbd91e4b33f9...4e64e708097ad41	File
302545c98e225a1f0ddc...fc2269042c55ede	File
34c9d086c2af471a45e3...3a04d11d210f7fe	File
52bb8e44ebd9ee0715f4...505cbdb3e88d7c7	File

INDICATOR VALUE	TYPE
759c66e423c7c53c17b0...7f35830fd7f4869	File
90937f087a01b79741d4...c92a8aa7fdbb771	File
a99ca9f79d7e5c89865c...2af7e97ab40a26b	File
b9cb434e82ac9204495d...9de0be30a93f61d	File
bb0c29c4f4d2f1721a60...9ae58dd291a7fe9	File
d02567dfc4e93b82b6f3...62b9f716e099874	File
d0db7afbe28a845fa75a...9165903a29315d7	File
d434c7720a5eb9017527...520a512f1a76d91	File
de235889fcc37a882a93...e8f731f7cae79a4	File
f0fc2852843c27a813ac...d6f1bfcca40c566	File
000000a512a847e8ed28...d07817b1ce3a2a2	File
0000014a634db98f8503...4e439aef830cd70	File
00000238ff09aa0e0e0c...6db1e7fd5a6ab05	File
000002869785aa152f08...ea26bb201d49fd7	File
00000428f03c4512a07d...2b9818fb5e2121c	File
000004393aafab2eaba9...7c70dcf0e5132ca	File
00000439a3ffa123c3f9...7ab80c74261f354	File
0000048d976a523a117a...27838475a1ec8ed	File
0000064cacbf07d04bd4...872cdccb355a18a	File
0000067fbb4783bb9655...7a3654b99f49ce6	File
00000722ff984d5cd9cd...9d582c79b92c1a6	File
0000079dfb0c33717924...735ac33fb8124b7	File
000007b8271a49ecfcb4...8677dd89dc662af	File
000007cb124a92fd3c65...9db72fafdebd5be	File
00000893d37db36ef14c...43d6d003d471bc7	File
00000944c9e053f1c545...b4b761c78416e6e	File
00000a7d66dc4e9ff3f2...119d68ee919c17d	File
00000a8c4d72a3818c10...f3eb87b9d1d9f81	File
00000a8d83184e8f603b...61fb919e86ecacd	File

INDICATOR VALUE	TYPE
00000af7e147252a9838...aae8c0cc5969c61	File
http://bestsmartfind...SUZZeU1GQkVSbDA	Domain
104.21.3.95	Ip
http://connectivityc...om/generate_204	Domain
https://googleads.g...k-core-v40.html	Domain
http://www.microsoft...s.aspx?id=30709	Domain
http://www.gstatic.com/generate_204	Domain
http://www.gstatic.c...sdk-core-v40.js	Domain
http://int.dpool.sin...php?format=json	Domain
http://count.lingte...rs=Android&ss=1	Domain
http://hmma.baidu.com/app.gif	Domain
http://sdk.wiipay.cn/cn/prefetch.do	Domain
http://imgsx.lingte...droid&version=1	Domain
http://900igr.net/	Domain
http://ww1.900igr.ne...x8=&opnslfp=1&	Domain
http://ww1.900igr.net/favicon.ico	Domain
http://ww1.900igr.net/	Domain
http://ww1.wcrypt.com/	Domain
http://ww1.wcrypt.com/px.js?ch=2&abp=1	Domain
http://ww1.wcrypt.com/px.js?ch=1&abp=1	Domain
http://googleads.g.d...k-core-v40.html	Domain
http://googleads.g.d...loader.appcache	Domain
http://googleads.g.d...e-v40-loader.js	Domain
http://alog.umeng.com/app_logs	Domain
http://topdata.downl...linone.callerid	Domain
http://android.downl..._hot_app&page=1	Domain
http://app.loveitsom...r&version=4.0.0	Domain
http://app.loveitsom...om.ayamob.video	Domain
http://topdata.downl...type=daily_info	Domain

INDICATOR VALUE	TYPE
http://topdata.downl...ype=weekly_info	Domain
https://gomovies.to/...0/watching.html	Domain
http://topdata.downl...om.ayamob.video	Domain
http://www.google.com/gen_204	Domain
https://pagead2.goog...aio.downloader	Domain
http://app.loveitsom...pp.batterysaver	Domain
http://android.downl...soft.accovenant	Domain
http://topdata.downl...upload_info.php	Domain
https://www.youtube...h?v=t0Y_5bPG4xY	Domain
http://topdata.downl...?type=base_info	Domain
http://topdata.downl...fo_from_aio.php	Domain
http://topdata.downl...fo_from_aio.php	Domain
http://app.loveitsom...app.cleanmaster	Domain
http://hiphotos.baid...ef41ad53a73.jpg	Domain
http://hiphotos.baid...dc451da3fa0.jpg	Domain
http://kg.plapk.com/...jjmsjktvcb.html	Domain
http://hiphotos.baid...9dbb7fd3ceb.jpg	Domain
http://hiphotos.baid...bef76099b35.jpg	Domain
http://hiphotos.baid...f51f2de66f1.jpg	Domain
http://hiphotos.baid...6246a60afe4.jpg	Domain
http://hiphotos.baid...bedaa641ba4.jpg	Domain
http://hiphotos.baid...9f9d62aa036.jpg	Domain
http://hiphotos.baid...b134954777f.jpg	Domain
http://hiphotos.baid...bcb0b46d40e.jpg	Domain
http://hiphotos.baid...f3e660952f2.jpg	Domain
http://hiphotos.baid...52ac75cb74f.jpg	Domain
http://hiphotos.baid...6246a60afe9.jpg	Domain
http://hiphotos.baid...51f94ca5f6a.jpg	Domain
http://hiphotos.baid...933c9950dc1.jpg	Domain

INDICATOR VALUE	TYPE
https://collector.mobile.cnzz.com/	Domain
http://hiphotos.baid...744eaf8ac70.jpg	Domain
http://img.snaptube...b99598ba9af.png	Domain
http://dl-plugin.mb-..._Job-844321.apk	Domain
http://api.snaptube...all_vc=70960810	Domain
http://img.snaptube...a19398c43b5.png	Domain
http://img.snaptube...6d38f24777.webp	Domain
http://dl-plugin.mb-..._Job-291515.apk	Domain
http://img.snaptube...9f944f1e26d.png	Domain
http://img.snaptube...84be1583d8c.png	Domain
http://api.snaptube...t=18&os=32&gaid	Domain
http://push.snaptube...all_vc=70960810	Domain
http://img.snaptube...b9695e8ca_.webp	Domain
http://img.snaptube...5c631026981.png	Domain
http://api.snaptube...all_vc=70960810	Domain
http://api.snaptube...tube_snaptubeiq	Domain
http://dl-plugin.mb-..._Job-880817.apk	Domain
http://img.snaptube...e565ba6569.webp	Domain
http://cpclnad.biz/sqbg	Domain
http://przvgke.biz/oqtvksqovr	Domain
http://wluwplyh.biz/k	Domain
http://fjumtfnz.biz/kkagvl	Domain
http://pywolnvd.biz/ttwmuxbrjog	Domain
http://tltxn.biz/pbghs	Domain
http://iuzpxe.biz/akblcki	Domain
http://gjogvvpsf.biz/nnewl	Domain
http://znwbnskf.biz/y	Domain
http://jdhhs.biz/utkexuiy	Domain
http://brsua.biz/vicbjsp	Domain

INDICATOR VALUE	TYPE
http://mgmsclkyu.biz/txaanc	Domain
http://fwiwk.biz/iswwpilhmhubS	Domain
http://yunalwv.biz/ykbqmcddujdtttmp	Domain
http://uphca.biz/jiijeg	Domain
http://nqwjmb.biz/am	Domain
http://pywolwnvd.biz/lhpacigcdmexqkv	Domain
http://ftxlah.biz/tfrqkafmtryxcs	Domain
http://rffxu.biz/lyargql	Domain
http://haguicj.biz/iopxrjhnan	Domain
https://ws.ksmobile...ull&append=null	Domain
http://ufs.adkmob.co...e3aacc68f95229b	Domain
https://ups.ksmobile...ions.php?v=null	Domain
http://ads.mopub.com...2e8ca7349&dnt=0	Domain
http://ufs.adkmob.co...1df18b8ee1a17ed	Domain
http://us.st.dp.ksmo...1&calc=74393850	Domain
http://127.0.0.1:41646/ping	Domain
http://up.cm.ksmobil...ig/main_cfg.ini	Domain
http://help.pc120.co...calc=2028860295	Domain
https://bp.adkmob.co...aid=&lv=4.3.4.5	Domain
https://cmdts.ksmobile.com/c/	Domain
http://unconf.adkmob...&v=22&sdkv=3.12	Domain
https://ads.flurry.com/v14/getAds.do	Domain
https://pegasus.cmc.com/offer/	Domain
http://up.cm.ksmobil...er/CloudCfg.php	Domain
http://up.cm.ksmobil...otification.ini	Domain
http://unconf.adkmob...&v=22&sdkv=3.12	Domain
http://infoc2.duba.net/c/	Domain
http://ads.mopub.com...ba55cfeb4&dnt=0	Domain
199.59.243.227	Ip

INDICATOR VALUE	TYPE
34.94.160.21	Ip
34.211.97.45	Ip
172.234.222.138	Ip
18.208.156.248	Ip
3.254.94.185	Ip
47.129.31.212	Ip
44.221.84.105	Ip
35.91.124.102	Ip
34.246.200.160	Ip
13.251.16.150	Ip
208.100.26.245	Ip
54.244.188.177	Ip
wluwplyh.biz	Domain
tltxn.biz	Domain
cpclnad.biz	Domain
gjogvpsf.biz	Domain
hagujcj.biz	Domain
fjuntfnz.biz	Domain
znwbniskf.biz	Domain
ftxlah.biz	Domain
rffxu.biz	Domain
mgmsclkyu.biz	Domain
uphca.biz	Domain
brsua.biz	Domain
fwiwk.biz	Domain
jdhhbs.biz	Domain
pywolwnvd.biz	Domain
yunalwv.biz	Domain
iuzpxe.biz	Domain

INDICATOR VALUE	TYPE
przvgke.biz	Domain
nqwjmb.biz	Domain
66.244.66.30	Ip
gw.monroe.smithvilledigital.net	Domain
66.244.66.13	Ip
bfee7b955c02035b36681cb969caad87f6b9d42a3bb195b85e2a7d8e25089854	File
66.244.66.27	Ip
vpn.co.monroe.in.us	Domain
27.66.244.66.monroe.smithvilledigital.net	Domain
mx2.co.monroe.in.us	Domain
66.244.66.31	Ip
66.244.66.1	Ip
66.244.66.100	Ip
co.monroe.in.us	Domain
www.monroe.in.us	Domain
test-2.smithvilledigital.net	Domain
www.smithvilledigital.net	Domain
monroe.in.us	Domain
15.197.183.30	Ip
209.43.47.37	Ip
66.244.66.20	Ip
gis.co.monroe.in.us	Domain
gisserver.co.monroe.in.us	Domain
helpdesk.co.monroe.in.us	Domain
gistest.co.monroe.in.us	Domain
ftp.co.monroe.in.us	Domain
legacy.co.monroe.in.us	Domain
mercury.co.monroe.in.us	Domain
docs.co.monroe.in.us	Domain

INDICATOR VALUE	TYPE
cms.co.monroe.in.us	Domain
mx1.co.monroe.in.us	Domain
webmail.co.monroe.in.us	Domain
mail.co.monroe.in.us	Domain
autodiscover.co.monroe.in.us	Domain
www.co.monroe.in.us	Domain
3fe1f4be5e95b8b3af2bab2fbe265ebcd6cb906fdedb2e5d6ff40bab8ad8acc8	File
1d3889846c78298de4e701b54bc58af3c7d41146fdef717eccc7c04123805a1a	File
da4a75ed01227a575db2b87423b2d3a09fa738886764df5d416ba67ee3ae2217	File
17ad9bb615ae018d4bc9e724663a6b124157c43f670237f4e71f1e7f2f081df9	File
0c2fedbe0423d14f6d48c8f802437771f413e1318c5d9fd9429eb58c00df37bf	File
30bdf413c08247b47fed3340a4fb7b897f91a45415896c2504bb6465ea5f7f5f	File
86d99f86390774790289752558eee73cdc5cca3d0e08f26f77dc4d7655dc0aa5	File
4d419290f9b22edd988addf09ee61bb7a4fad948041ead12adee880df13e059d	File
eb05f2ecc2cc310063284fffa0eca04107c38a1d13da57b5da02f6aab0f4b39d	File
c0f4221a34d5b32c79f63a6ccf5aa80541fc1174ccd61d285d7cdca52311de2f	File
8ee77b30d56cdcde4a89950a23c43ff10470fd2063cf436d68ff68b1f4b09a1c	File
29e550dfab69b3248ed65c58773d01073090c1f14db2f6522400f183ea3aa5ac	File
858a154a4223a59068c2a847aa088d9dfa47bc13ade2b4baa6c83faa0d244796	File
50948e64098b04a0eaea711ae4c3e9b91fa765e70696c1483cd1c0d63e11b57a	File
3f072dab60bed8886950f2127ae7c8d886ccc0550c74f0018202d9625017807a	File
7ee78939d4d6b50589a78b217796e471380996ef841058399ff9d8de8429a49a	File
d225dc131ce6a0adca96e02cf0a7101294626b55eeaa7465e9a83d3f66a713e	File
93b30a9e1aa6e71e5ec99dd207e4e4b322addf1f274c9785143573b943217b5a	File
464426386bd530d9ca0c00671c70abfe694a9e178582fbdb6dc41ecca92c9eba	File
b761803bb96f50eb90ce3defce0549bb282f054e30fb913a9488b789cde734ee	File
nexus.officeapps.live.com	Domain
52.111.229.47	Ip
52.111.236.24	Ip

INDICATOR VALUE	TYPE
52.111.236.25	Ip
52.111.243.25	Ip
52.111.243.26	Ip
0a4d7e4860afac36c43f2e5272678b7e267b46618ab46a596dd28dbc4c5915e3	File
211bdf19381949eb8115d9b099670d0277e91531afea23e23a11879d9a29f87d	File
22aa981f10e839fbf2c5c3a8f3de7caa2f9c3add7af4750420fd2b1a05be1709	File
24d6742653761510338bb242f67a627d03a7ccf98f0ab8d21292034f9bb3bd34	File
452acb807a408b767ad4318d01e17053499521dc201aa502e47950726872c83	File
48e537902c03a3eeee4790fc97ee072cddc7c1a90122702dd18243d8c12a0d99a	File
56d8f8af1e45eff640be34914a9dc332e6154108f194deec5853d66dac766496	File
5845a3a9aa81f92f4a2ea69f6353d9096b89b186beffd1c81788ccc8edf0bf15	File
6c1b1e6b7a1f5a9499a3f7c66939b933d89efd7bff818255f57cd182c7474650	File
71356358d9c1df71801f9bfbf5b040ab664a4b06e6c73d29e4801e23fe9f1f9f	File
7dfd9f131494d23952f4428b9a6d20f358910796729c7ac4815f76a14b3c643e	File
8b064ebb257b55ee09b619b791475058b4d9d2b90907ec727e70235e5b25b730	File
97da3c982874ec87dcb39e8ae9e8c8df8acd4e06f360a8a4179b82fa0014346	File
a1cce8a43ef384aa3e44fbc222f3d99a869ae2078872f514e5ad8f383568a8b9	File
a48c02fd36302685b5fbb3691db0fb2c4aca77c0b3b1df9aa7ec6f154affa0a8	File
bf34420ca94118eb47dad3f01abfe68433534295268e66207a2e7a7889be5148	File
d1614ad99aded9f6f5c1be7fe7ffa5124bd04a526580da3818ea8a954e852aa6	File
dfbde381fde1a284c81a72d06a1a43faf49cd1c085c87234e34e50b881567806	File
e11eb59cf535da90ef6617ac9256138659a8420b47afbe8749a8076fbdc29bc	File
ee9e288c3495fd548fd49095be08807f215fc0780064e179011098c0c7461a34	File
204.79.197.203	Ip
89.35.237.180	Ip
226c926cb2beb6b4cbbb7a42f5e860b1da02530cdc402e6b6145170ef7b3eb3f	File
291bf6745bb5a406186261a5b916b831c0230c877db267731f0a3ab431649038	File
6230814bf5b2d554397580613e20681752240ab87fd354ecec188c1eabe0e97	File
62e03c94f568196ad4e5fd181ef60cf3e2c03f73ec336faf10bba0a15a96182d	File

INDICATOR VALUE	TYPE
c64ed5c2a323c00e84272ad3a701caebe1dcceb67231978de978042f09635fa7	File
d1d308e355e4cfff921461c9c015f4f3ac88ea29736a46e5a28c04d8822e132e6	File
d85bdad87177cc72973c0ffca03166c0739f36f394c58915575e51f94ed61388	File
e23040951e464b53b84b11c3466bbd4707a009018819f9ad2a79d1b0b309bc25	File
f3137b0da2063617a279b8cdf1438b4ac083eed1982fe65d7e293eff626b8b66	File
f4b7c8b9553e0b1c9a77da6e94750099923570ad14d966c739eace5e17a2e399	File
204.89.253.55	Ip
66.244.66.44	Ip
fa6f9722c1b9542271766681a939b53f7e0c2616155f41b72b6debb0e65aed6b	File
7dc5546ebd1e2a40b2785df2e18d87058898ec87740aec8f4c1bf224987b7710	File
01f15adfb4b3ba22946b914bcf50fcb2b746841511c9c69fd439bb971ba128df	File
c2ffecd77fa99cdf56c81099958fbdc411a08d3b02e3b7ef238739b000404cfd	File
e4862e12edfe5bf0c85e57fe1d6e9828f2c76a4b98ffae1b801513899a27a404	File
www.microsoft.com	Domain
1a724aa3ce05da87e26dc7b963ecc405234444eb71d9ae3a3930a7fb7ac0c042	File
3102cec0048148d22b5ba5628d744a7eae55efdae50a7dbb59070682fdb7d660	File
3d04ecde07280474cc7e73f6e547a558ebea6d61555b2fccd62ad2c7e8441954	File
47bc56e666ab3a33cb3ada887d70e1d5484d34bcfa0d6061763034adbb4b4930	File
47f106f8f50a49a939e80187e23069f0e685907223832211dddcaadddef09184b	File
4847cdcfd9d0d8bb940dae76e5231cb46dda13348855afef4e6a5b257d03d026b	File
4909cc6023e1b633f3eb5398b6cce6790e5cc34fecb39d878cd9b26c4d56ea91	File
4fd87aaddc9106bd8179adfc07a9e8fa0cefc3dcd9604712874af3376f0ea01	File
5a41e0316f8c2fe59c084f861483457d62bf4977e3dcb8e1aab8a07b160f3991	File
5f7a674e1c6b0a3edb3532ee9276b8f5b694526a7f47597e7b972bbd197907fb	File
6a290aacc09aa391e4637fc34f1aba53da8428e458b2f0225c4a16199ce7a1c7	File
6e9274c9c1acd719ca64138163d1c5ea0ba78074a01bbc459e48469c597fff25	File
7768dae586920feac88943b260caa4f9a26bd357603d81517431d38f5e026594	File
7d590200863f6a0d93834ecf02c2367fe5ba24ff4145d6c89ad7840587e453a3	File
89f2aca9a2d7d10117e9ed30fa99c700cdf2712995db3bbc7835a84a271418e1	File

INDICATOR VALUE	TYPE
8d34fbe3eff2a634be965b2dcc3a5655bcec6f04f5ab7e9697e91d87874da185	File
947075792a2af3817fbc27da5627f3d160b0d32d7a8f62a64c02abe5bcb46fef	File
96175287d907186c92662735a29580dc151320582669c1e7984368534d87916a	File
983ea6e2b83565788f4ffa6362260c9d8b51a07fed7892b65ce8ba4bd5d07247	File
adca17f0bfd3c81269602b1c0c263f5688098b92daae69ea2c11d7db87c74872	File
130.163.182.133	Ip
130.163.184.43	Ip
130.163.190.78	Ip
192.168.0.17	Ip
209.43.1.143	Ip
209.43.1.226	Ip
209.43.100.212	Ip
209.43.101.219	Ip
209.43.102.155	Ip
209.43.104.189	Ip
209.43.104.23	Ip
209.43.109.117	Ip
209.43.110.129	Ip
209.43.110.207	Ip
209.43.114.16	Ip
209.43.114.58	Ip
209.43.115.37	Ip
209.43.118.135	Ip
209.43.118.174	Ip
209.43.12.127	Ip
business.bing.com	Domain
bzib.nelreports.net	Domain
edge-mobile-static.azureedge.net	Domain
edgedl.me.gvt1.com	Domain

INDICATOR VALUE	TYPE
13.107.6.158	Ip
23.215.55.139	Ip
23.215.55.144	Ip
239.255.255.250	Ip
34.104.35.123	Ip
2fbffddiny3hekzgye5g3iuftqoihc5dw.ormysby.1.0.scwbmwdp7owtf2jcwvrry53jzu.tgrqyon.dns0.org	Domain
vjzwub55z3yhqebokmhrxm6k2lخورqo.zfylc7y.1.0.o6uwrffj6r6um5vy5peylvkeou.v423pop.dns0.org	Domain
yhk225bv63wg5d25qiy7wxyt4ve5txp.3bzvcrl.1.0.komu5z3k5rbhaj4tv35hqifd1tclwe57dyk7jda.mlg5m14.dns0.org	Domain
vjzwub55z3yhqebokmhrxm6k2lخورqo.zfylc7y.1.0.ktgw73z2l74ngye4hpy2l7puwy.v423pop.dns0.org	Domain
pwl2vaddy147jxv5qetruqzkojlxknk.dsggjuq.1.0.w7n343f15kxd6pa3baz6nt7254.ft89f7n.dns0.org	Domain
vjzwub55z3yhqebokmhrxm6k2lخورqo.zfylc7y.1.0.hw1amqv2pv5hw626j7xucgzbe.v423pop.dns0.org	Domain
alt1.edgedl.me.gvt1.com	Domain
alt3.edgedl.me.gvt1.com	Domain
alapmuggj5cxnm7o46fwsgzpoiiazca6.fxoxczq.1.0.orekkhngov3r4uk2hjlwpfe56m.on9cr2u.dns0.org	Domain
ir5nm1k2ukxbhhtonr6izprlpyvxf32.2cvvfua.1.0.chdcvmahr6lmfe4a55a35ko7li.nc97qc1.dns0.org	Domain
i7n6s23mey3wr2ro5tfw44seyp2maeb.ro667xa.1.0.66sk2rdc7dmpoawhmbnnv3qxi.xfacahr.dns0.org	Domain
i7n6s23mey3wr2ro5tfw44seyp2maeb.ro667xa.1.0.ekjtyswb6ldeyalnb6brp3rzyq.xfacahr.dns0.org	Domain
aegpojpvpa7fxwmgt7rq2lxi5klitogo.cs2l7jq.1.0.l4poaainq32gussq7p4ofcjrfr.2aczlku.dns0.org	Domain
edgedl.me.gvt1.com.1.1.1cc430c5.roksit.net	Domain
z6d2564z6noxcltkl3nakydjhmvztx.mxqca5q.1.0.ao44474wcn2vczh7fc4y7glqni.4ebkqy.dns0.org	Domain
edgedl.me.gvt1.com.91.1.2e60c5e0.roksit.net	Domain
108.177.119.101	Ip
108.177.119.94	Ip
13.107.253.38	Ip
142.251.31.95	Ip
172.217.218.84	Ip
172.217.218.94	Ip
23.205.109.82	Ip
23.205.109.91	Ip

INDICATOR VALUE	TYPE
74.125.128.94	Ip
config.edge.skype.com	Domain
00054c77269f53ed4b8db889132bde7dfdfc3358f4940459d601bf940c4937f	File
000a35caeb27c4e8b9fdf455ab1991081138b857a0f347e521fc32563a49cc8c	File
001cc58e88ee2bf06de698d629a888b0cc69e728eba3297d199f8a04770ae4d1	File
001ea1697fff9db1d9891ee31677ef925240185d8204683bcd185459e2edb683	File
00211659db8833b98618936d199ef1fffe7274d12a541de3d9d8fc6d7e21293c	File
003af175b42dd165367c93a14b13eaea91016d637db484e01427d3b2e0ff4a4f	File
0046138927938ef7cd3aea09f7978a4201e6f6fb7ed61bd8b6a1b381a3b4a9c1	File
0052a3ef1b8f4463ff4cc19c783ba5db033e11d638b24d7219fcc3f3a430c5a4	File
0053e31957446978773c7e5aa5ea81889b2f6d0f730ead502232419490aadaa3	File
005abda499e24c08ef0f29143df57c7206e679edf7d4456e868a86665649cab7	File
005ba00a46df16c0c31ce90f947eddae62997ce847a6d094dfb5a871a769aee2	File
00730d58342c3d70d5060838997369e63f842acd91cee4b0c33ff8e728060131	File
0075e3cbb63fb0b7d0548f3dc023c07e760247680f6e5340ead924f2ed52028e	File
007d275f0491ddd9b36ee088ef6b3415d59a5cc9ba2ca8d4bbfac3496f91a852	File
00875137c3a94523c74e6a9234b76174c8a7b573a3101514f34caba8344faeae8	File
008f18ac3976971ff90478974a98900f4d02005e8bbc6503024b093ea9c101cc	File
0093c863702ff2323f80eaf6ba00228ae3e6bd381dfc38b3cbb07f114b701c1c	File
00b7aaef5c5c8768b498a4065707ddac6dcbe3585d5e33b96338423a60c390f3	File
00c1b47c050dc2a09043d124cc11d6f5f0cf4aae573619c625e0bdbb6e47104a7	File
00d02a97c3efc2539f656663092f3fe981759a98ccdaedd4560358ee5a47a098	File
http://www.if.ee/	Domain
https://api.msn.com/v1/News/Feed/Windows?apikey=qrUeHGGYvVowZJuHA3XaH0uUvg1ZJ0GUZnXk3mxxPF&ocid=windows-windowsShell-feeds&osLocale=en-US&CheckEnable=true&activityId=D5B7E70E-9CFE-4E34-8109-3390F8BC6826&user=m-de33484272fc4903a4900de4d1baf000	Domain
http://download.windowsupdate.com/d/msdownload/update/others/2015/05/17930914_a3b333eff1f0428f5a2c87724c542504821cddb8.cab	Domain
20.82.32.45	Ip
199.232.214.172	Ip
www.if.ee	Domain

INDICATOR VALUE	TYPE
if.ee	Domain
216.9.137.80	Ip
ace43fc2b15725e28c9377542300ada8ce31e2ec51f44c3d59e006c467d491b5	File
http://74.134.111.120/default.htm	Domain
http://77.122.245.30/welcome.htm	Domain
http://77.122.245.30/start.htm	Domain
163.com	Domain
163mx00.mxmail.netease.com	Domain
163mx01.mxmail.netease.com	Domain
163mx02.mxmail.netease.com	Domain
163mx03.mxmail.netease.com	Domain
1646639377.mail.outlook.com	Domain
1974151189.mail.outlook.com	Domain
2d7633219391c9403033086ca3c6e1.mail.outlook.com	Domain
323805130.mail.outlook.com	Domain
394364422.mail.outlook.com	Domain
44uit.hm	Domain
4dorganising.co.uk	Domain
6og5ln.us	Domain
ad.state.mi.us	Domain
adinet.com.uy	Domain
ag.state.oh.us	Domain
ag.state.oh.us.s9a1.psmtip.com	Domain
ag.state.oh.us.s9a2.psmtip.com	Domain
ag.state.oh.us.s9b1.psmtip.com	Domain
ag.state.oh.us.s9b2.psmtip.com	Domain
0.0.0.0	Ip
1.70.154.156	Ip
10.1.10.3	Ip

INDICATOR VALUE	TYPE
106.10.165.51	Ip
106.10.166.54	Ip
108.59.49.249	Ip
108.59.49.250	Ip
110.45.136.134	Ip
110.45.136.135	Ip
110.45.215.15	Ip
112.127.57.38	Ip
114.108.154.167	Ip
114.108.154.181	Ip
114.108.154.199	Ip
114.108.154.208	Ip
114.108.154.231	Ip
114.108.154.234	Ip
114.108.154.241	Ip
115.114.58.13	Ip
115.114.58.15	Ip
77.122.245.30	Ip
74.134.111.120	Ip
db01b514803c170f9668fbe6dc95fe2595a6dd5518acafc7eae45d4f82bc64d3	File
caa419ae23ec1dd04b5d86496691550cff8a872ff987405b4eded2bab874937c	File
iwnemfam.ru	Domain
jilvoqsi.ru	Domain
taosiram.ru	Domain
01e450aa49ba5be377be683cd1e007a992e0dc79f2fb34571667334c52f68ca9	File
0c0bb960eae9ae9e49eb9ba9bee6c592c5d1374158cea09de80d45744d61c105	File
190b219271c822b5499a42508bc5578914a3b54e8e220654f1405f9cb21d8dfa	File
1c8d6d5830973d4cd4865f484f728f5556bc433cb9a5973b706eaf75c087807e	File
1db0d69c233dd4975f4dbfab7cacf97f86481b87fa1b9c81cea5ee1a8d32de3f	File

INDICATOR VALUE	TYPE
26cbdf92bbd91e4b33f970538daee8662133d97b28c3985394e64e708097ad41	File
302545c98e225a1f0ddccbab3fdd9f69bf91e51664f53bdefc2269042c55ede	File
34c9d086c2af471a45e38428baf823f9112459854d2963f883a04d11d210f7fe	File
52bb8e44ebd9ee0715f4490ad86f5c10ed8c4e71e3b51b9a7505cbdb3e88d7c7	File
759c66e423c7c53c17b0be1456b336592ecc91fe440c0ff637f35830fd7f4869	File
90937f087a01b79741d43b0140e19e5546d3fff6e86bc800f1c92a8aa7fdbb771	File
a99ca9f79d7e5c89865ce90fc1027d9fad6ec3b26f8fab5712af7e97ab40a26b	File
b9cb434e82ac9204495deb6addc2707c5087aa1e416885f5b9de0be30a93f61d	File
bb0c29c4f4d2f1721a6016b642195e98e5b1bb6f01e2f6d019ae58dd291a7fe9	File
d02567dfc4e93b82b6f3164c6a32838b77457f7a879fa589f62b9f716e099874	File
d0db7afbe28a845fa75aebfaccfe1d16e64f719d7c45f87a79165903a29315d7	File
d434c7720a5eb9017527080c2f7dbdd07c881d5175812080d520a512f1a76d91	File
de235889fcc37a882a93485741ae6520189774eed7f940064e8f731f7cae79a4	File
f0fc2852843c27a813ac3bae288de70f311191148c863079dd6f1bfcca40c566	File
000000a512a847e8ed28fdaf433d6dd601a88d74e5dd7d71bd07817b1ce3a2a2	File
0000014a634db98f85038b833a8dfc50d5fb13a464e0b25994e439aef830cd70	File
00000238ff09aa0e0e0ce9fb075a62592f1b35c719986c3946db1e7fd5a6ab05	File
000002869785aa152f0830368c0ae50653ec1f70aadfa665dea26bb201d49fd7	File
00000428f03c4512a07d064719d8aa5d85462cac78e4d4c342b9818fb5e2121c	File
000004393aafab2eaba9cda3dd56db0f8a6506d1fb9b566b37c70dcf0e5132ca	File
00000439a3ffa123c3f9bc45e5e821351b1a5c276871b36447ab80c74261f354	File
0000048d976a523a117a63cb21eab6c7d88bf510352cd9f9f27838475a1ec8ed	File
0000064cacbf07d04bd4c5151f7fad673bfff4b5e803faaaf872cdccb355a18a	File
0000067fbb4783bb96552304c7c9d0f33d899888621ccbdcc7a3654b99f49ce6	File
00000722ff984d5cd9cd766d12c70eccc7a2ad7502999c5a99d582c79b92c1a6	File
0000079dfb0c33717924384f3dcce65bf7656316467cc6de3735ac33fb8124b7	File
000007b8271a49ecfcb407d34575f71b25dca41cab52f46068677dd89dc662af	File
000007cb124a92fd3c6553ca4d61ed432887736f33825d8239db72fafdebd5be	File
00000893d37db36ef14c3922141928a04f92d27360ceba9af43d6d003d471bc7	File

INDICATOR VALUE	TYPE
00000944c9e053f1c545ef1b4b21bf6f07265b6449bffdeb4b761c78416e6e	File
00000a7d66dc4e9ff3f21f544341cddc0259bdba2ccf95523119d68ee919c17d	File
00000a8c4d72a3818c10e4fbb578b8923ba3754021e50b627f3eb87b9d1d9f81	File
00000a8d83184e8f603b6a2682439deab7d9935c7414add6961fb919e86ecacd	File
00000af7e147252a9838e0694eec2cbd5fdd3482bf8eeee7eaae8c0cc5969c61	File
http://bestsmartfind.com/population/angular.dGlua2VyYmVsbCBwaXhpZSBob2xsb3cgZ2FtZXMgbXA0IG1vdm1lIGRvd25sb2FkIGluIDl4NgdG1?delaware=failover?juleps=ZG93bmxxvYWR8aHo1wVRaNVVueDhNVFkxT0RJeE9UUTNM3g4TWpVNU1IeDhLRTBwSUZkdMntUndjbVZ6Y3lCYldFMU1VbEJESUZZeUlGQkVSbDA	Domain
104.21.3.95	Ip
http://connectivitycheck.gstatic.com/generate_204	Domain
	Domain
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40.html	Domain
http://www.microsoft.com/de-de/download/details.aspx?id=30709	Domain
http://www.gstatic.com/generate_204	Domain
	Domain
http://www.gstatic.com/afma/sdk-core-v40.js	Domain
http://int.dpool.sina.com.cn/iplookup/iplookup.php?format=json	Domain
http://count.lingte.cc/IsInterface.php?ri=sxm_n_FU780&op=install&mac=263179622839&vs=1.0&tm=1350549060201&key=e9e21c05b57ba9c4418913c9f90ddeae&dq={"ret":1,"start":-1,"end":-1,"country":"\u6cd5\u56fd","province":"","city":"","district":"","isp":"","type":"","desc":""}&sc=480.0*800.0&os=4.0.4&jrs=Android&ss=1	Domain
http://hmma.baidu.com/app.gif	Domain
http://sdk.wiipay.cn/cn/prefetch.do	Domain
http://imgsx.lingte.cc/MTProject/MTContr?action=MTUpdate&terminalType=android&version=1	Domain
http://900igr.net/	Domain
http://ww1.900igr.net/?fp=QMux8K4rN0T0n4R62lxa1ys0okz7ZrKdDrn8pIuUDm1Fs6Fsd013W+rygBNvyjwwmJd/I8mFUGCoR1d73+hua2rNHckrNADbRghhrlDeCZ381ZD8jklVsn7xDvATFiBnyNqpzNF/zVbQ5GKBc8cUcLUPCtTY30Tm7myhA0rMWZH+MwYYk2zW5QB11v0VQfRckiI3rmyRCmJxtQiFSW1tfeeJEeATA94M2rNlQk4yrBYyy7BiVwwkPDIKpJkkdoxd0y2zeoS9LSP1QcJ0BspsA==&poru=uIQLvTgztNgmE1JPRyHueaN/9we dU5Gpyq+PPQdeDx8=&_opns1fp=1&	Domain
http://ww1.900igr.net/favicon.ico	Domain
http://ww1.900igr.net/	Domain
http://ww1.wcrypt.com/	Domain
http://ww1.wcrypt.com/px.js?ch=2&abp=1	Domain
http://ww1.wcrypt.com/px.js?ch=1&abp=1	Domain

INDICATOR VALUE	TYPE
http://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40.html	Domain
http://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache	Domain
http://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.js	Domain
http://alog.umeng.com/app_logs	Domain
http://topdata.downloadatoz.com/atoz_statistics_info/market/ga_stat.php?type=alltype&action=/matrix/shortcut/caller/f/com.aio.downloader/t/com.allinone.callerid	Domain
http://android.downloadatoz.com/_201409/market/app_list_more_test.php?tab=aio_hot_app&page=1	Domain
http://app.loveitsomuch.com/gonglue_xilie/ping.php?id=com.aio.downloader&version=4.0.0	Domain
http://app.loveitsomuch.com/_manage/proc/get_android_info.php?id=com.ayamob.video	Domain
http://topdata.downloadatoz.com/atoz_statistics_info/market/post_info_data.php?type=daily_info	Domain
http://topdata.downloadatoz.com/atoz_statistics_info/market/post_info_data.php?type=weekly_info	Domain
https://gomovies.to/film/adult-life-skills-19690/watching.html	Domain
http://topdata.downloadatoz.com/atoz_statistics_info/market/ga_stat.php?type=alltype&action=/matrix/shortcut/YouTube/f/com.aio.downloader/t/com.ayamob.video	Domain
http://www.google.com/gen_204	Domain
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps&action=no_ads_fallback&js=4452070.10298000&os=4.4.2&api=19&flow=mobile_ads_settings&appid=com.aio.downloader	Domain
http://app.loveitsomuch.com/_manage/proc/get_android_info.php?id=com.axapp.batterysaver	Domain
http://android.downloadatoz.com/_201409/market/recommend_list_more.php?id=com.ubisoft.accovenant	Domain
http://topdata.downloadatoz.com/atoz_statistics_info/market/api/get_last_upload_info.php	Domain
https://www.youtube.com/watch?v=t0Y_5bPG4xY	Domain
http://topdata.downloadatoz.com/atoz_statistics_info/market/post_info_data.php?type=base_info	Domain
http://topdata.downloadatoz.com/atoz_statistics_info/market/api/get_app_info_from_aio.php	Domain
http://topdata.downloadatoz.com/atoz_statistics_info/market/api/get_last_request_app_info_from_aio.php	Domain
http://app.loveitsomuch.com/_manage/proc/get_android_info.php?id=com.evzapp.cleanmaster	Domain
http://hiphotos.baidu.com/exp/pic/item/9304c888d43f8794f76723cfd31b0ef41ad53a73.jpg	Domain
http://hiphotos.baidu.com/exp/pic/item/86d5bac27d1ed21b90f70df5ac6eddc451da3fa0.jpg	Domain
http://kg.plapk.com/html/zjjmsjktvcb.html	Domain
http://hiphotos.baidu.com/exp/pic/item/d35a10f41bd5ad6ee6982d4880cb39dbb7fd3ceb.jpg	Domain
http://hiphotos.baidu.com/exp/abpic/item/a005b3345982b2b7b082fc7b30adcbef76099b35.jpg	Domain
http://hiphotos.baidu.com/exp/pic/item/e6508eef76c6a7ef523b4cc5fcfaaf51f2de66f1.jpg	Domain

INDICATOR VALUE	TYPE
http://hiphotos.baidu.com/exp/pic/item/0db2c9ca7bcb0a467e1627dc6b63f6246a60afe4.jpg	Domain
http://hiphotos.baidu.com/exp/pic/item/ac0acf1373f082027d180d674afbfbeda641ba4.jpg	Domain
http://hiphotos.baidu.com/exp/pic/item/f76575600c338744773195ab500fd9f9d62aa036.jpg	Domain
http://hiphotos.baidu.com/exp/pic/item/e1bf8725bc315c6077b467818cb1cb134954777f.jpg	Domain
http://hiphotos.baidu.com/exp/pic/item/476217f79052982232fad367d6ca7bcb0b46d40e.jpg	Domain
http://hiphotos.baidu.com/exp/abpic/item/964b2e4e251f95cada7c29c7c8177f3e660952f2.jpg	Domain
http://hiphotos.baidu.com/exp/pic/item/148f28d3d539b600e38c594de850352ac75cb74f.jpg	Domain
http://hiphotos.baidu.com/exp/pic/item/0db2c9ca7bcb0a469d0a08df6b63f6246a60afe9.jpg	Domain
http://hiphotos.baidu.com/exp/pic/item/83cab81ea8d3fd1fdcb60e8314e251f94ca5f6a.jpg	Domain
http://hiphotos.baidu.com/exp/pic/item/34bbf8cd7b899e511734a11943a7d933c9950dc1.jpg	Domain
https://collector.mobile.cnzz.com/	Domain
http://hiphotos.baidu.com/exp/pic/item/0b07ec1fbe096b6331f40ac20c338744eaf8ac70.jpg	Domain
http://img.snaptube.app/image/em-video/26dcc42faaf8141b8691bb99598ba9af.png	Domain
http://dl-plugin.mb-cdn.com/release2/snaptube/gitlab/plugins/video_search_engine/video_search_engine_1.4.29_noarch_Job-844321.apk	Domain
	Domain
	Domain
http://api.snaptube.app/v1/video/details/rules?v=7.09.0.70960810&vc=70960810&u=1c855ebf336f46d858a69f2f2cc61c96&ch=tube_snaptubeiq&last_ch=tube_snaptubeiq&pn=com.snaptube.premium&lang=en®ion=GZ&networkCountryIso=&locale=en_US&apiVersion=12&installDays=0&lastInstallDays=0&random_id=88&ytb=true&bucket=18&os=32&gaid&install_vc=70960810	Domain
http://img.snaptube.app/image/em-video/ffaeda59ab215ed4c6127a19398c43b5.png	Domain
http://img.snaptube.app/image/em-video/316600cc3cbda7c89631786d38f24777.webp	Domain
	Domain
http://dl-plugin.mb-cdn.com/release2/snaptube/gitlab/plugins/ffmpeg/ffmpeg_3.0.2_armeabi_Job-291515.apk	Domain
http://img.snaptube.app/image/em-video/7ea350989e15de49f8d359f944f1e26d.png	Domain
http://img.snaptube.app/image/em-video/37e992ca143b3a36bc5d284be1583d8c.png	Domain
http://api.snaptube.app/region?v=7.09.0.70960810&vc=70960810&u=1c855ebf336f46d858a69f2f2cc61c96&ch=tube_snaptubeiq&last_ch=tube_snaptubeiq&pn=com.snaptube.premium&lang=en®ion=&networkCountryIso=&locale=en_US&apiVersion=12&installDays=0&lastInstallDays=3650&random_id=88&ytb=true&bucket=18&os=32&gaid	Domain
http://push.snaptube.app/push/token/v1/upsert?v=7.09.0.70960810&vc=70960810&u=1c855ebf336f46d858a69f2f2cc61c96&ch=tube_snaptubeiq&last_ch=tube_snaptubeiq&pn=com.snaptube.premium&lang=en®ion=GZ&networkCountryIso=&locale=en_US&apiVersion=12&installDays=0&lastInstallDays=3650&random_id=88&ytb=true&bucket=18&os=32&gaid&install_vc=70960810	Domain
http://img.snaptube.app/image/em-video/2d6343d2dc2af105121af2ab9695e8ca_.webp	Domain

INDICATOR VALUE	TYPE
http://img.snaptube.app/image/em-video/89d67c1e8ffd81d2b352b5c631026981.png	Domain
http://api.snaptube.app/region?v=7.09.0.70960810&vc=70960810&u=1c855ebf336f46d858a69f2f2cc61c96&ch=tube_snaptubeiq&last_ch=tube_snaptubeiq&pn=com.snaptube.premium&lang=en®ion=&networkCountryIso=&locale=en_US&apiVersion=12&installDays=0&lastInstallDays=3650&random_id=88&ytb=true&bucket=18&os=32&gaid&install_vc=70960810	Domain
	Domain
http://api.snaptube.app/v2/upgrade?manifestMd5=219da4be3467f536c64fbd741151f4f3&apkMd5=b08d3306d6523f7078992e5ef8e16ac3&manufacturer=unknown&v=7.09.0.70960810&vc=70960810&u=1c855ebf336f46d858a69f2f2cc61c96&last_ch=tube_snaptubeiq&pn=com.snaptube.premium&lang=en®ion=GZ&networkCountryIso=&locale=en_US&apiVersion=12&installDays=0&lastInstallDays=0&random_id=88&ytb=true&bucket=18&os=32&gaid&install_vc=70960810&ch=tube_snaptubeiq	Domain
http://dl-plugin.mb-cdn.com/release2/snaptube/gitlab/plugins/site_extractor/site_extractor_2.24.261_noarch_Job-880817.apk	Domain
http://img.snaptube.app/image/em-video/3184b2745c6052bb4eb649e565ba6569.webp	Domain
http://cpclnad.biz/sqbg	Domain
http://przvgke.biz/oqtvksqovr	Domain
http://wluwplyh.biz/k	Domain
http://fjumtfnz.biz/kkagv1	Domain
http://pywolnvd.biz/ttwmuxbrjog	Domain
http://tltxn.biz/pbghs	Domain
http://iuzpxe.biz/akblcki	Domain
http://gjogvvpsf.biz/nwew1	Domain
http://znwbnskf.biz/y	Domain
http://jdhhbs.biz/utkexuiy	Domain
http://brsua.biz/vicbjsp	Domain
http://mgmsclkyu.biz/txaanc	Domain
http://fwiwk.biz/iswwpilhmhubs	Domain
http://yunalwv.biz/ykbqmcddujdtttp	Domain
http://uphca.biz/jiijeg	Domain
http://nqwjmb.biz/am	Domain
http://pywolnvd.biz/lhpacigcdmexqkv	Domain
http://ftxlah.biz/tfrqkafmtryxcs	Domain
http://rffxu.biz/lyargql	Domain
http://hagujcj.biz/iopxrjhnan	Domain

INDICATOR VALUE	TYPE
https://ws.ksmobile.net/api/GetCloudMsgAdv?lan=zh_CN&apkversion=2.7.4&channelid=100000&osversion=4.4.4&mcc=460&device=Lenovo_A360t&resolution=764*480&mem_size=1006&pkg=com.rhmsoft.fm&version=1&aid=92841014150fc3fd&branch=Lenovo&mnc=00&gaid=null&net=1&dpi=0.75&hunter_v=null&append=null	Domain