UPDATE ON SITUATIONAL ALERT

DATE: 08-Aug-2023

Executive summary:

This report serves as an update to the **'SITUATIONAL ALERT ON CYBER THREATS'** issued on 4th August. It provides an Indicator of Compromise (IOC) list which organizations may use for their preventive security measures.

Indicators of Compromise (IOCs)

Following IP addresses are observed to be used for potential DDoS attacks:

38.242.220[.]21
141.0.8[.]70
162.159.200[.]123
104.28.159[.]49
54.37.2[.]81
66.102.9[.]68
163.171.211[.]12
163.171.138[.]32
66.249.93[.]163
183.171.175[.]20
139.59.254[.]181
193.186.4[.]143
66.249.68[.]64

PHP web shell observed to be used by hacktivist groups:

All data type: SHA-256

Indicators	Description
1d645c3277c4c504b8b8efc4ccc0455e7de29a55981bb082c6d242bf3accf72d	PHP web shell
a9278983f6704dfbd0303be8c4a477dd42d9e8fa08d1fc78a2b32ccc4f5d658f	PHP web shell
f2b90ecc4519db4bfc5d355d8a0920ba63586933bea925fa9f560c0bc59ef708	PHP web shell
d581c842109bf3ca85b7b4dcc2f4bc45958cbee7393516707622a990c7b1e885	PHP web shell
fbcb496d9b45060860abdfc05193185fd57653c55851368567b34dfef213d71b	PHP web shell
78539a07f24bc63a0b7b310288e338597b54cdb8dff02baa981d9babff4b227b	PHP web shell
1e80d44200b74e9d6a8c9a623667aadec0086af4806ecffdceb29be4ba4d4d35	PHP web shell
303d0f0de552f9bbe750b92617f9682b74b3d77be0ddb5e7917c1acae55262e0	PHP web shell
ce2a8d2c41e66a7df6f76757b3209c40ebc4b1f342de332778ec04464b11f18b	PHP web shell
7c014aac33fef35956a64a3f574bc6b293c95f2f866ffabb7309930b7507c445	PHP web shell
3073496e684028e26fdd24e852ffcd2ec4c278d43facd69f2c7655737e8f8879	PHP web shell

Cypher RAT v5:

All data type: SHA-256

Indicators	Description
99102b94023a7b7a09ee9f0a457de9b70391a9c6d57332ebe647963fc745dd20	EXE (builder)
2e84c3f95013feb8ea9f9aec097997258f657cf5a64ca902d9b2726ec7c8c72e	RAR (builder)
79dfc775cec5baed761d39e33bb9a81db319b8b5212ebcd60b1fe2ebf22a2190	Zip (builder)
c765f7f82227b9f796f7d92ba3caef42af719c3dbcc320c21de06738fac032fa	RAR (builder)
b29993b87b1d0cd6be2da121684207cc8b03cab2cad561517752fe67ffc08abf	EXE (builder)
6356b3f4bfab5d64275eed1a3f8059c79e101a410db9d76abfcb7722a4553c7c	Zip (builder)
1925f8610b35a2c8d2272f304a4524ce64fcf9dfcf3d6e54d5fbcf01f68ef33f	Zip (builder)
1abf8ba9013e2ae59101cac2638e8e2c00bef2c7eeeb145a5497bf775a250302	EXE (builder)
e95d8eab67b595a89acda9bf36103909a2050c3b424583d4eb2b3578a58ca5b0	Zip (builder)
1876dc44f532e4c5fbec7b4b76b0b527bedacd1151db6d7fdf7f88e0354fdc57	RAR (builder)
b13763067f9bc942d9f436b884517ed1cb9df772a630089c7efbc567d7f7d208	Zip (builder)
ab2107e6ac18c5c2374d817deec090cbd16eb19b4d5aedffb04d1cea86817634	Zip (builder)
a06dd46bd32e85ea4b2b20dae4e77ae85a66a56a0a2d592aac53599d3749b6e0	EXE (builder)
b0bed92d135cd310715f477ac629e343fdd3bbd2f0001b8ce657eb334f3eea8f	Zip (builder)
2607f0a07bcbaa8c565fd77f364b58e7a9e51758fb73ee26eb6c1f75b3d7ae8a	Zip (builder)
f5a4a735fcd7b341c4376fcd8ed69aab25d5f403bd4b2cd465d64c9b64b4361b	Zip (builder)
40df1793f563a174c5eb1fdd7a62d35391a027d63ab0cbac12cdb77c7049680f	EXE (builder)
620f1b7890f0dca8ea52c6484e47881c8dc8c38c0def976727653d65d7b4c5f6	RAR (builder)
ac4310c16c117886b43c9064b0cff6ff4dfa6e0f85d4eeaf1ce744dfadf55aba	Malicious APK
b24d00614d80bd06fea99a69599fc9dadcf1d8b85af77dcf39723e34b963cb48	Malicious APK
a00519830db794ff8a12ad4949b5b376937059d5f43f1a4477e12cbaae60f113	Malicious APK
ca75901b9dc5391ee0e2847f24d41690aff30223b2ad90a1c526f49b23b7d93e	Malicious APK
87502e6ee73f2c038b850dec33cee546440788bfdce80131dfacaa4f58434cde	Malicious APK

754798d8bcca13fef642aba40dd69f05d7a910d82f3f868e4c09def07ac462f9	Malicious APK
2346b0d054711ebecf6619b2ef585eadf57ef3df5204b87521838b97c63944e0	Malicious APK
c90bcc318ad1407699d56e62d5640f6b9302cbb038d42747b2d8f3a52131e876	Malicious APK
d8dcb0e44437f427d0109598757d9746ecc7227ca940f6cf87dc12b2e1f125f1	Malicious APK
133409720e053c2e2f4555fe9b4067231955ac83eaac7677a4fdaf73bc789750	Malicious APK
53dd4c2e9e458b61d0e69022699077a749646be8a63c98c8ff30fff7cdcbefae	Malicious APK
fdcde341a9b615c71b55b474ddc5b4d2889c8d38f4b05e7a1a1dfa815dac7b44	Malicious APK
b944550b81e810fe3cd86ab3bb082467c4e7d3e877b6a07519b1d724da46c759	Malicious APK
9625a456e543ac7a9ffdb68d1e264fe5ade8567c1823bfe3e6da27db92a66fc6	Malicious APK
78258ae86bdd666d6b1b497bcef145d3e1644095640e4485f09af5a0974944f5	Malicious APK
99a4c54dda280aa0889fec55bb90a66487d8cf52785c1131e1d44ebb24b8afd0	Malicious APK
73823333a325ed1d3befaab7eba6bd5f71ab09cdff6d5d61064fa7d16317703b	Malicious APK
1144a4aabc68dd39907d2d70d9d6a09bf88c256af3b0e134ec3af16ac84260bd	Malicious APK
218f1693856e999ac0605d00d319b8e85c8d0991fb5640e19e7c5c7dc5ff30f5	Malicious APK
18b5ddf9f83946282c2a28c6153160ad4898be69b67866b2d682bd4d966cc76c	Malicious APK
8065297874bb9d369f1c478749e2e82e24aec398381109569c03cde9f70f05d4	Malicious APK

Crax RAT V3.0:

All data type: SHA-256

Indicators	Description
534756b486fd0a0981a5502d10d4dd549f19922364fd9dcef5baf126b7c0e590	RAR (builder)
23766c6df2ae7a72748e1c734c46fd1938864deaeab5dac12991c7b045efccca	EXE (builder)
1bf32c5dd0813e6f7fadb6525d8e00e185fb89b44243aba672ce753eee3a6973	Zip (builder)
a1ca2eff979c798c83cb159c84eb920014375c742b6158e2219173eb23a7dfa6	Malicious APK
2365ca22b471351c5874e83cf8312fc7d4f80ed5ba7f7a4e17cada7e74a23d5b	Malicious APK
db50c13dca6a9b7594f105f50c4eff3fc736cd78b1411e3b318229b49ebeafa0	Malicious APK
c9518e47060680aba7b6485a786881ba31767ca4a516b259055b3f55355d112e	Malicious APK
3537c8e37689ddb95f84f4ff4c9f7159892a5c66fbc1db86dc2d90571b279e63	Malicious APK
115e25786dace8450beaa355c6e8fcdbb371a39222c774673349af591d7c2798	Malicious APK
b5d0cfb51c6c672311e07cbccbebcb65a8109f9de6784102ee62b43a152ecd38	Malicious APK
5d757362c77df82d339fac3d78a4207bf8c4ce81f1ecaddef54c7370eef96783	Malicious APK
522637ee86a97482b74d640034916d62086ac5c736dbab55a093637f0b31d5a6	Malicious APK
05c9827d9fba03a6a663e127623a9cff8019bfd7ef32045ad3baf2b676859c23	Malicious APK
ab58abc21fa25be77232925361e6751d189250c1fdfc7c46ca081f70f6d97e8f	Malicious APK
370cd221952ec22216016d87a0f8ab05ea10d8f5d532469419da5c4c324c6f6d	Malicious APK
35adff0f1083df7a529fa86d0999bc8954bab704ed4e5d2dd603793588fdfc40	Malicious APK
2296b0c1fba50443bface32d5f7db91acc329fb971be9f63f0fce6bd9a48ecd4	Malicious APK
3b4fc694b4cd82f99084ce85d3716bf515a8e184d6d03eaa2815e4fdc19772bb	Malicious APK
cc5ec60f576138fab085714b054a00712220c8e7df1069763ce15c0c9f8f3120	Malicious APK
2ecf09946f91e0254c8cc7e0f8b7c42e15258f38537bd0741cfca4d80ac3f067	Malicious APK
7e4756497e2b9c54c4ca2b5cc0a9e9ddc6b585db16681a6e751fe20609f48f60	Malicious APK
12a69a2db7596ba820431789406656c767f6671ff4b4354580197f995f186a1a	Malicious APK
d0e044d60be996884f8dc0388c2466fc894e16b6f7ca16ca75247d9622b1ff7b	Malicious APK

407ba0e6637f56d574bd8aa9f54ec4ae8775417fa4081c3112f2f42519550657	Malicious APK
2581759a4dfd703952dcffccca00f9b971b0d9a9103a12d39233f53fa1e35266	Malicious APK
3cb9b9bced9daf82e28c69f1fa8aca07ea50b9b3c652c2d6f7fdf90168fff749	Malicious APK
06c4a302fe411b5ac78ad7fe64352b1a0578dfa630ab8cafbc81ad40127c4c14	Malicious APK
366d271377503cde54909db43409e0f21448f3f3e9b64a2eb2ca9f934229993e	Malicious APK
d37e1269c5060c6840ac73d6733365968fbdee0933f6ae00966a188ad41294f0	Malicious APK
3422a42624f187db00f63bfbde6ab96f4569bae43fba5f9851b3676eed2530d0	Malicious APK
7599f2cc798c8c67d240ea28c86276a3e421284d7d98d222d7e6ecdc9ea85ece	Malicious APK
abeb4aface0dd4e6c6a86992433fb39ae1412004ac46d8327cd0cfe5d38375e9	Malicious APK
04a9e0a0bed70d6cac0d88eb34fde5512480610a268d99f53b0876eddf72e662	Malicious APK
6431a77b46911620fdff3140411be20ce3d81d0f62fb665efe94547ee3b15918	Malicious APK
7757897b36393f104ac9d0438f33e3a9584523d15f359d81f178216ef5c94adf	Malicious APK
d2b32113f8be89598f142e892b7dcfb0aa88cc9774356a50436139a89dca006f	Malicious APK
87591001050b0dae8d9c2eefedae5dfa3c192327b33cb9c1b83beac82ae67b58	Malicious APK
2992aa9adffcd3fc5b7b1b9366774203642d4e2d6012dfda7dacd16425ba77df	Malicious APK
a67be614988f06641c61978b7f5ff8b07f75afd453e2d46bd34dae3544aaaa2a	Malicious APK
d79549476163001b3272f702637cc8169e4c3fb1b87e926ecbf6fd7af76d351a	Malicious APK
b13024b12fc5a013044d512141db7c1da0254fee738b2ba6187f7137200cb6f8	Malicious APK
73a50342b6694cd6dc51ff98dbd94c4a9c7acffc45c7de8622ce0de0ee5201f6	Malicious APK
c4f077193e8838add767b739dae1c0cfcc67eab6fa92edb55d90f6df1c7d8779	Malicious APK
2ff5041b93b9da7483ca4e42adbc808a14dc40dd021d355f6fac02996bf4ea55	Malicious APK
cc0d28ae37fe254b0c24f9d177b92433e1fd7b2ece60c7bddf2390db0bece37e	Malicious APK
59e97586f51a673985282f6f9b06243ebe9ffc103631c86364cae24136b6a606	Malicious APK
5c5b284626263dba3036ea0a62bdb30c480fe55f6ce86807b8e7a6104a5032fd	Malicious APK
0554aad65ff4876bcd2dd8b9b4881aa6efd00f8f3c3ef319dc509a3b81933573	Malicious APK

711fb4be5cf9d0b2c06ca5fc4264406eeb5917529461387420be8bcb29278995	Malicious APK
fd83f704b9baecd7b03653d8524f013baebda23b60f1c515c605b44fc14cad70	Malicious APK
555b2efc675b2ff41feeb073117b16bd65eea8536233f509bd135a447b0f2b53	Malicious APK
54b9d824d990f9a224c305d781457b694d22f006bb387586c7ffd9222c72662f	Malicious APK
5050698a5c6e1d932acc3370ebb1011094d605010f844b73f6da122aa1d6fb0e	Malicious APK
3b02abbad9153527ccd1bc52e799301b7a1fd46fbe80142c7ef42ec84b22a1c8	Malicious APK
01874744630d62f500a77c4824d7868ca607a6e94f5cf635255ebc9ee2fe576d	Malicious APK
a7fc333ed2aa854cae4f46efecbde27622e4291e4c94cc560526ebf134388eab	Malicious APK
c2337e75e7ae85e82a7d62d8931f679e4afa46b8d8680f1d8061d12dd300e1d4	Malicious APK
7a123cb2061051c99bc360ad61bed681cc29bf1cb1bbab3b20be0b19dee352e0	Malicious APK
087725a3605498a7a39a856ed847afdbc8454cb0ed5aa0f2e2830d95d624e320	Malicious APK
b79c60d8c56f022db73217738e2ef90af678b6f583b2a4e826e4287255ece0bc	Malicious APK
0841b7bcc56ff8e42869289468e472104b68a299d7b745466131a41e47d140e0	Malicious APK
cf993fb25bbf09bc2cedf8989a144ced2d0604d53fc3d6be4ea039a3b63917b7	Malicious APK
d9792cffec5d8bd28045ddd17ae9a1782972614db8972e6e6116d7a0c5c29329	Malicious APK
e99bed7388293a36e77c6d2a39dd98339c8991e92fc3de506e8d3f6ce7e2a426	Malicious APK
20dc82ad4e2f7f84f9ef509e6359912675ccff2ced271cda8769abcbb4326c79	Malicious APK
6aee097330dcdf2f7180664277bf9527cdaa8e32c6d87fc715c97ebf02dc070d	Malicious APK
0fcfd49b00a7ee1069fe1928f4a5d7efb2255d30788c7dc25f5915b4d9f01fdd	Malicious APK
dee908862526ff5e05cb9017ac3b3c0561a2d50e7e8cbc1600f9af7037456083	Malicious APK
91c69ad8f668bb5c71d0974260d297433f661f197def3b29271e89a8a411f1ec	Malicious APK
a12a2347664c1aac21e1cafaa7f18d4929d7790209ce776d4e04ae1393410c95	Malicious APK
7b7fb79d8dcb96536d835005c00794f29bb4a3518e642d0330d2e2f263242d47	Malicious APK
55dac5f3fd137030a92ac725c3b913c206541a5e051c064be03f3ee75be17f76	Malicious APK
1ccf6289195861c4444aa020b4fcfbfe6fa10799c9afde5652f26add289c7767	Malicious APK

f52bbf29695206c9f45300d2031b7b4a4d7d9dfad9060e609445a74942319a08	Malicious APK
644cda84fffe2a78d4b38453409a64713a4aa1e030ee15174e0951b7e8cd109c	Malicious APK
5d9b5286d8b3807c77a83fee79dd34f754f4bbbafd6ef1db76b6e67e021d8495	Malicious APK
b11b00861caca081bcd8df7fe13c77b5c30eb6ba33af36fc566160e991470c3b	Malicious APK
8c9386bfe2b966b162747199815f88e37288b3e80a520d09d159732d07612415	Malicious APK
0d76ef5a1d0ff42b2dfdc5fb94238829521466138f31a87d2b346a673b4a9c30	Malicious APK
78e992ef0ea6847ebe4f988ba6be9b573f1b91d716e473c5ee0e0b6bb56cdc22	Malicious APK
0361c698c0ffc82e6171d4329e40338dd6e4bddb89018c670ac06f4ee616ec84	Malicious APK
aa7aac59bc01c73e21a886dd95d99bbee1643cba0bd6a5de33b2713287c92239	Malicious APK
2363310f6a94a36b4ff3ee8f1a0e86d8e6c9df6dbb23510fc43f8efac342da0c	Malicious APK
b516fc34abfdf2138116ec7e5889b4250aa7ea832b3d76cf96d8a20810acca9d	Malicious APK
ab00da303a37c510f3dca53e39614adbfc62d046961883beffbae45ca9b56ae5	Malicious APK
8079845361384c5c4c48df6825299fbc8f94c1c0b602e28072c469761a6ca1d0	Malicious APK
a8c41ec1d55b9a4332d7a862f845d7f92f7ae0f0a1a9f009c90702aefecee347	Malicious APK
883b3552379425f7b9e1d7604ee09ec7c20eabdb01737e15e60db544d50c0847	Malicious APK
7d0ba6e7ca20e9a71ad554c02ac1e2e63f9fe668e3966e6f55da99839d79e419	Malicious APK
4d7768879e29daa2fb2d26ce76b0e752de20204ea9cd8c338ef4502c394f2eab	Malicious APK
0ff1f9bf89806d4e7669f5ff4790ecb6582e607605ba56d14709a63c0c2746b7	Malicious APK
6ee5b8b06227a5e16ef2dcb44c9701cd5931738f704a3767007985faaf8fa606	Malicious APK
53eb53802218b3dd2f9aa3cde807e4b4e6a83709b7615bac5c0610e1983c5a11	Malicious APK

Recommendations:

1. Implement 24/7 strict network and user activity monitoring, especially during non-office hours, to promptly detect any signs of data exfiltration.

2. Minimize the attack surface by applying appropriate access controls based on a need-to-know basis.

3. Utilize the identified Indicators of Compromise (IOCs) to update network security tools and firewalls, effectively blocking communication with malicious IPs.

4. Ensure high availability and resilience by deploying load balancer solutions to distribute traffic evenly and prevent server overload during potential attacks.

5. Enhance the security posture with a Web Application Firewall (WAF) that analyzes incoming traffic, filtering out malicious requests and patterns associated with DDoS attacks.

6. Prioritize input validation and sanitation to mitigate risks of malicious code injection, such as SQL injection and Cross-Site Scripting, which could lead to web defacement.

7. Conduct thorough security assessments to check for missing security headers and implement recommended practices to prevent threat actors from exploiting vulnerabilities, as outlined by resources like OWASP Secure Headers guidelines.

8. Maintain regular backups of website content and databases to enable swift restoration in the event of defacement or other incidents.

9. Strengthen data protection by enforcing HTTPS with SSL/TLS encryption on the website, safeguarding data during transmission and preventing tampering by attackers.

10. Stay vigilant about security updates and patches for web server software, content management systems (CMS), plugins, and other components to mitigate known vulnerabilities.

11. Adhere to the latest OWASP guidelines and best practices while configuring and hardening web applications to fortify defenses against potential cyber threats.