Grupi NoName057
Sulmet DDoS në Shqipëri

Version: 1.0
Data: 22/09/2023

Tabela e përmbajtjes

Ky dokument është hartuar nga Drejtoria e Analizës së Sigurisë Kibernetike, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike.

Krijimi i një profili mbi aktorin kërcënues ***NoName057(16)***, i cili përfshin një proces metodik dhe të kujdesshëm për të mbledhur dhe analizuar informacione nga burimet e fshehura të internetit. Qëllimi është të zbulohen dhe dokumentohen aktivitetet që lidhen me këtë grup aktivist me prejardhje Ruse. Si më poshtë janë ndjekur hapat për kryerjen e këtij raporti:

Faza e parë:

Identifikimi dhe zbulimi: Identifikimi i treguesve të mundshëm të pranisë së një aktori të kërcënimit shtetëror në *DarkWeb*.

Faza e dytë:

Mbledhja e provave: Dokumentimi dhe ruajtja e provave përkatëse nga *DarkWeb,* rrjeti social *Telegram, Burimet e hapura ("Osint")*. Regjistrimi i pamjeve të ekranit, regjistrimi i detajeve e komunikimit dhe taktikat, teknikat dhe procedurat e aktorit të kërcënimit (TTP).

Faza e tretë:

Analiza dhe verifikimi: Analizimi i informacionit të mbledhur për të përcaktuar besueshmërinë dhe autenticitetin e profilit të *DarkWeb dhe burimeve të hapura inteligjente ("Osint tools")*. Verifikimi i të dhënave me burime shtesë, platforma të inteligjencës së kërcënimeve për të zvogëluar rrezikun e keqinformimit.

Faza e katërt:

Vlerësimi i Ndikimit: Vlerësimi i ndikimit të mundshëm të aktiviteteve të aktorëve keqdashës, në entitetet ose industritë e synuara. Kuptimi i objektivave pas veprimeve të tyre, pavarësisht nëse ato përfshijnë spiunazh, vjedhje të dhënash, sabotim ose operacione të tjera kibernetike.

Faza e pestë:

Detajet teknike: Dokumentimi i informacionit teknik, të tilla si adresat IP, hash-et e malware dhe emrat e domenieve të përdorura nga aktori i kërcënimit. Këto detaje ndihmojnë në identifikimin dhe gjurmimin e aktiviteteve të tyre.

Faza e gjashtë:

Monitorimi i vazhdueshëm: Monitorimi i vazhdueshëm për çdo përditësim ose aktivitet të ri që lidhet me aktorin e kërcënimit, pasi taktikat e tyre mund të evoluojnë me kalimin e kohës.

Gjetjet e raportit bazohen në informacionin e disponueshëm gjatë kohës së hetimit dhe analizës. Nuk ka garanci në lidhje me ndryshime të mundshme apo përditësime të informacioneve të raportuara gjatë periudhës në vijim.

Grupi NoName057 (16)

Detajet e para: Mars 2022
Target: Ukraina dhe vendet e NATO
Sektorët: Çështjet e Jashtme, Transporti, Qeveria, Infrastruktura Kritike, Financat

Në datën 22/09/2023 pati një sulm i kategorisë: ***"DDoS"*** drejt disa faqeve të internetit të infrastrukturave të Shqipërisë. Ky sulm u mor përsipër nga **Grupi Rus NoName057(16) .**
Faqet që u sulmuan ishin:

- www.parlament.al,
- www.durresport.al,
- www.tirana.al,
- www.raiffeissen.al,
- www.uba.com.al,
- www.hekurudha.al.

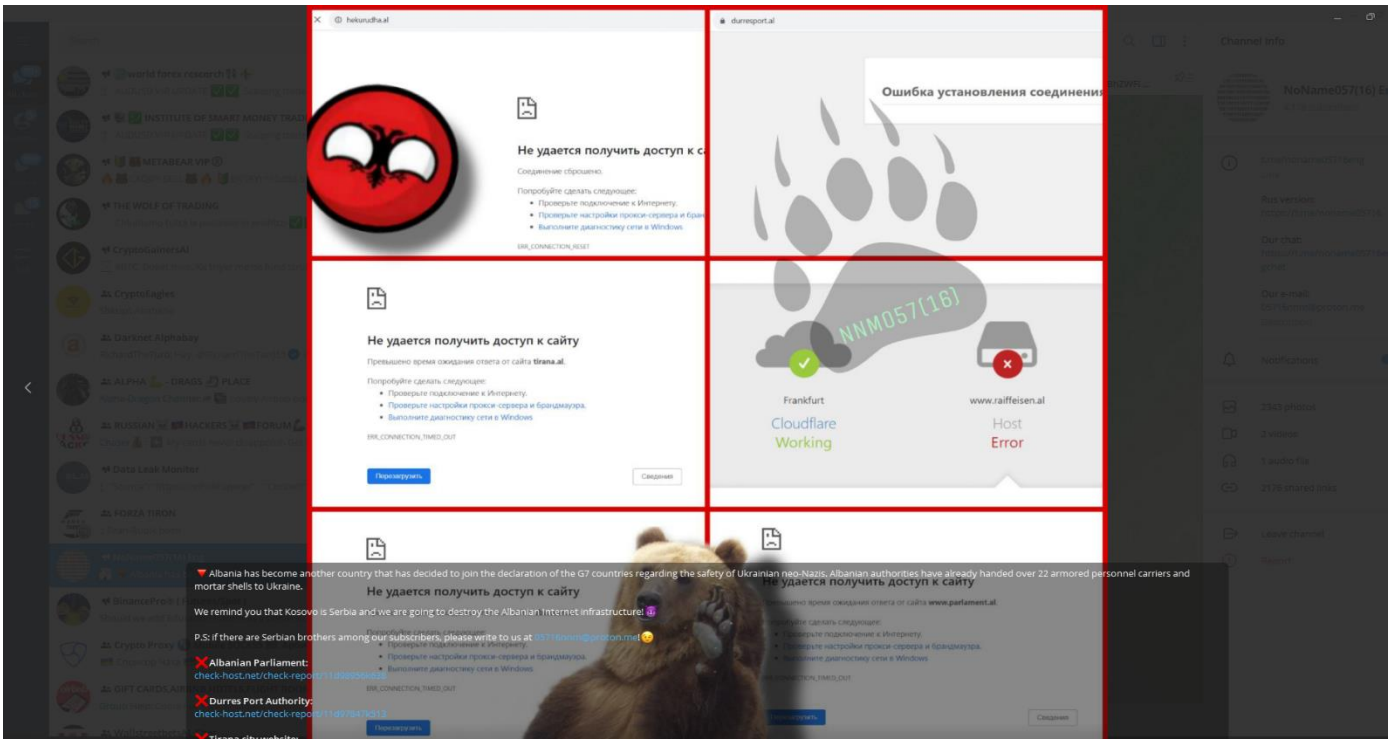

Figura 1: Njoftimi i grupit NoName057 në platformën Telegram

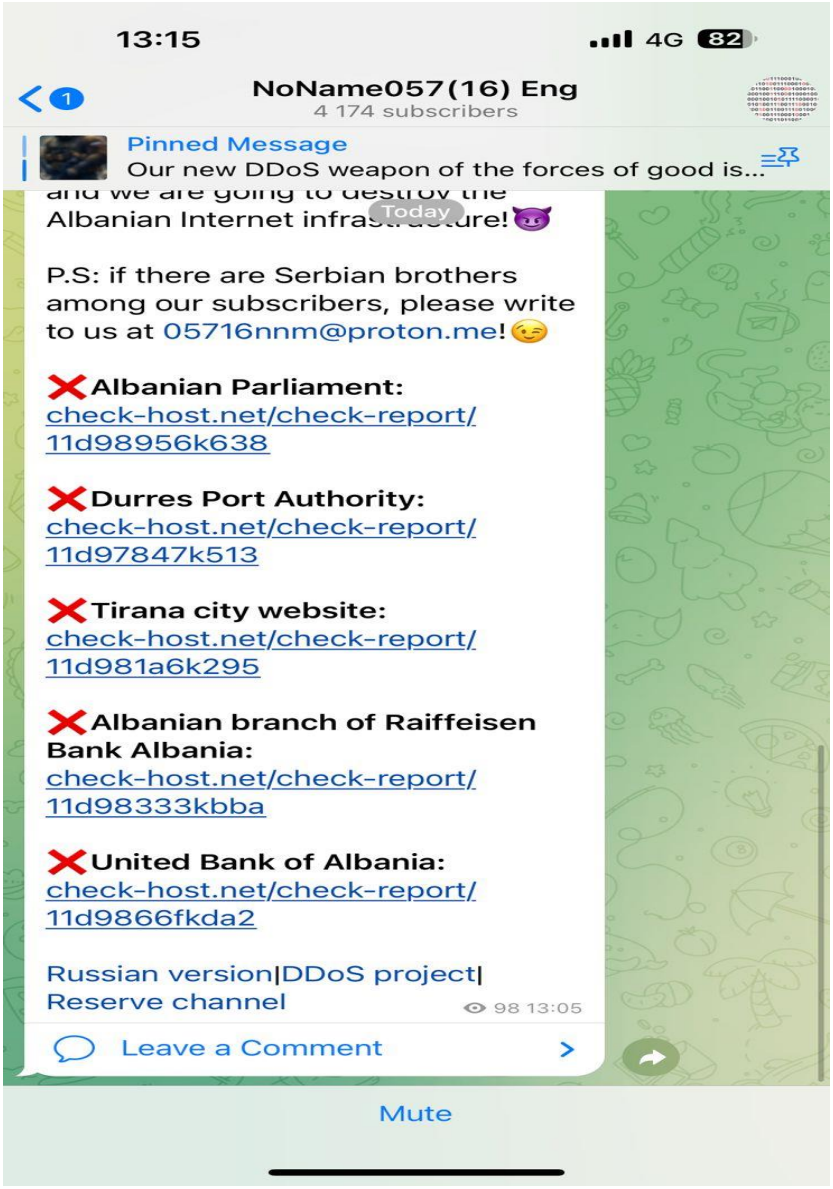

Figura 2: Njoftimi 2 në telegram, webfaqet e targetuara nga hakerat Rus

NoName057(16) është një grup haktivist pro-rus që ka kryer një fushatë sulmesh DDoS ndaj Ukrainës dhe organizatave të NATO-s që nga ditët e para të luftës në Ukrainë. Grupi ka shënjestruar organizatat qeveritare dhe infrastrukturën kritike dhe ka qenë përgjegjës për ndërprerjen e shërbimeve në të gjithë sektorin financiar të Danimarkës. U raportua gjithashtu se më 11 janar, NoName057(16) synoi faqet e internetit të kandidatëve për zgjedhjet presidenciale çeke të vitit 2023.

Motivimet e grupit përqendrohen kryesisht drejt faqeve web të cilat janë të rëndësishme për vendet kritike ndaj pushtimit rus në Ukrainë. Sulmet fillestare u përqendruan në faqet web ukrainase, por më vonë u zhvendosën edhe drejt NATO-s.

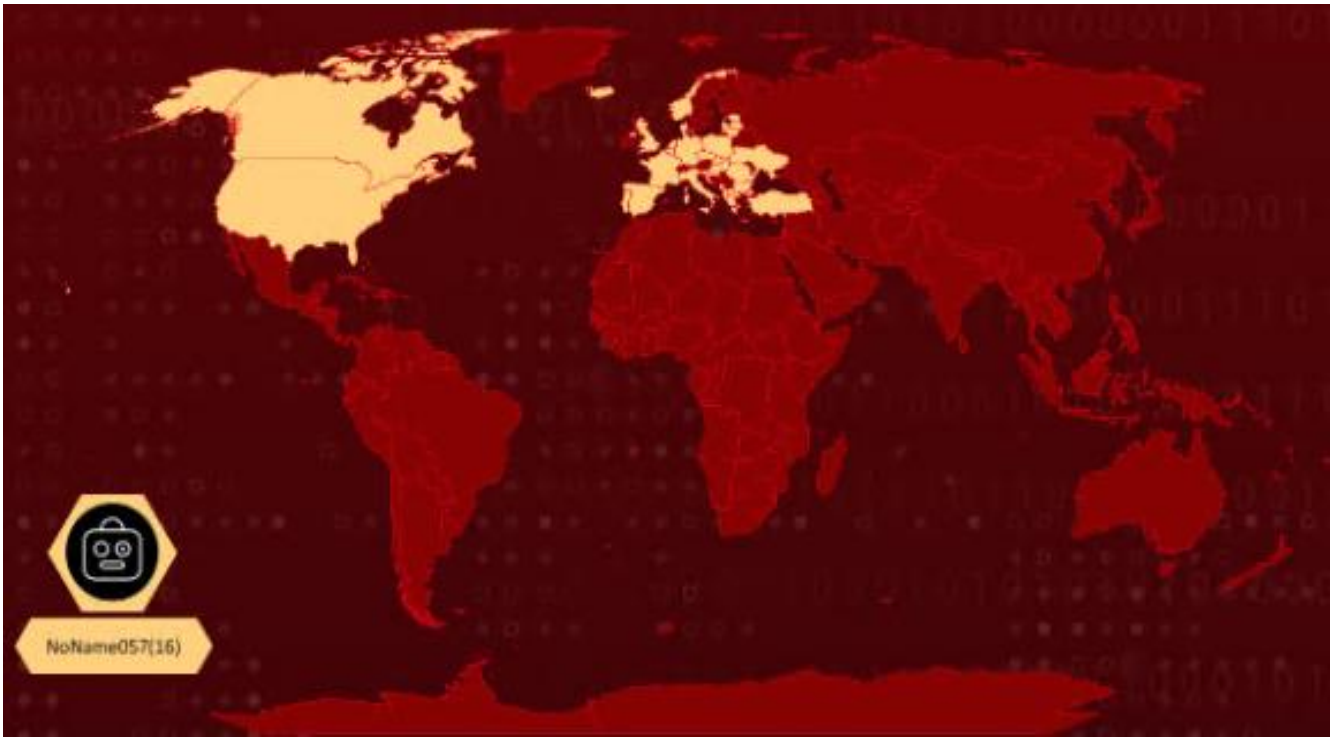

Figura 3: Harta e vendeve që janë target nga NoName057(16)

Detajet e aktorëve

NoName057(16), i njohur edhe si ***NoName05716, 05716nnm*** ose ***Nnm05716*** është një grup hakerash pro-rus që ka kryer një fushatë sulmesh DDoS në Ukrainë dhe vendet e NATO që në ditët e para të luftës në Ukrainë. Grupi ka synuar organizatat qeveritare dhe infrastrukturën kritike në shtete të ndryshme. Në dhjetor të vitit 2022, grupi ishte përgjegjës për ndërprerjen e faqes zyrtare të qeverisë polake. Siç është theksuar nga qeveria polake, incidenti ishte një përgjigje ndaj Republikës së Polonisë që e njohu zyrtarisht Rusinë si sponsor shtetëror të terrorizmit në mes të dhjetorit të vitit 2022. Ai është përgjegjës për ndërprerjen e shërbimeve në sektorin financiar të Danimarkës. Gjithashtu u raportua se më 11 janar, NoName057(16) sulmoi faqet e internetit të kandidatëve në zgjedhjet presidenciale të vitit 2023 në Çeki. Grupi operon përmes kanaleve të Telegramit, një toolkit që suporton disa sisteme operative dhe në GitHub.

Detajet

Origjina	Motivi	Rajonet e synuara	Industritë e synuara
Rusia	Haktivizëm dhe Shkatërrim	Ukraina dhe NATO	Punët e Jashtme, Transporti, Qeveria, Infrastruktura Kritike, Financiare

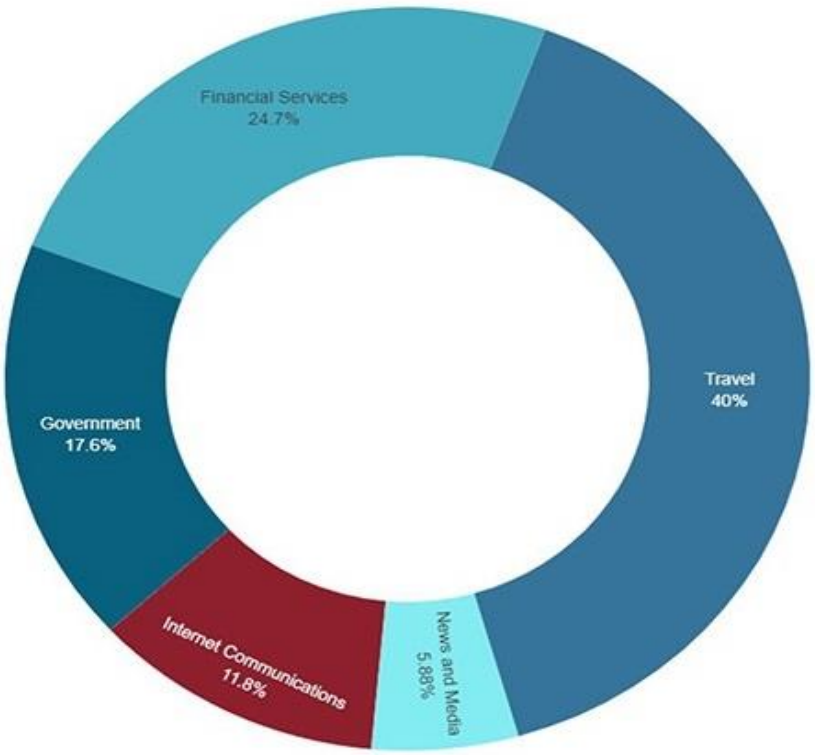

Figura 4: Sektorët e synuar nga NoName057(16)

Studiuesit e SOCRadar observuan se grupi drejton një total prej 5 kanalesh Telegrami:

1. NoName057(16) – përdoret për shpalljen e deklarimeve të tyre (më së shumti nëpërmjet screenshot-eve të sulmeve DDoS të tyre) në gjuhën ruse
2. NoName057(16) Eng – përmban të njëjtat postime si me kanalin kryesor të përkthyera në anglisht
3. NoName057(16) – një kanal bisedimi të cilën anëtarët e përdorin për të komunikuar
4. NoName057(16)_reserve – kanali backup i grupit
5. DDosia Project – kanali i komunikimit që kanë krijuar për mjetin Dosia që përdorin

Nga 8 Maj 2023 deri më 26 Qershor 2023, mjeti DDoSia i përmirësuar synon një sërë shtetesh, duke përfshirë: **Lituaninë, Ukrainën, Poloninë, Italinë, Republikën çeke, Danimarkën, Letoninë, Francën, Mbretërinë e Bashkuar dhe Zvicrën**.

Grupi është duke sulmuar Ukrainën dhe shtetet pjesëtare të NATO-s, si dhe mendohet se do të zgjerojnë sulmet dhe tek shtetet të cilat suportojnë Ukrainën gjatë luftës midis Ukrainës dhe Rusisë.

Duke parë deklarat e grupit në Janar, vihet re se më shumë se çereku i sulmeve kanë synuar Republikën çeke, dhe nuk japin më shumë arsye për sulmet përveç "Ruso-fobisë". Duke parë deklaratat në Shkurt, gati gjysma e sulmeve (42.5%) kishin synim Ukrainën dhe Suedinë, si dhe grupi sulmon disa sektorë të shteteve viktimë siç janë:

- Administrata publike
- Transporti dhe Magazinimi
- Financa dhe Sigurimet
- Siguria Kombëtare dhe Punët e Jashtme

- Telekomunikacioni
- Korrierët dhe Shërbimet e Dorëzimit Express
- Shërbimet komunale
- Bankimi Komercial

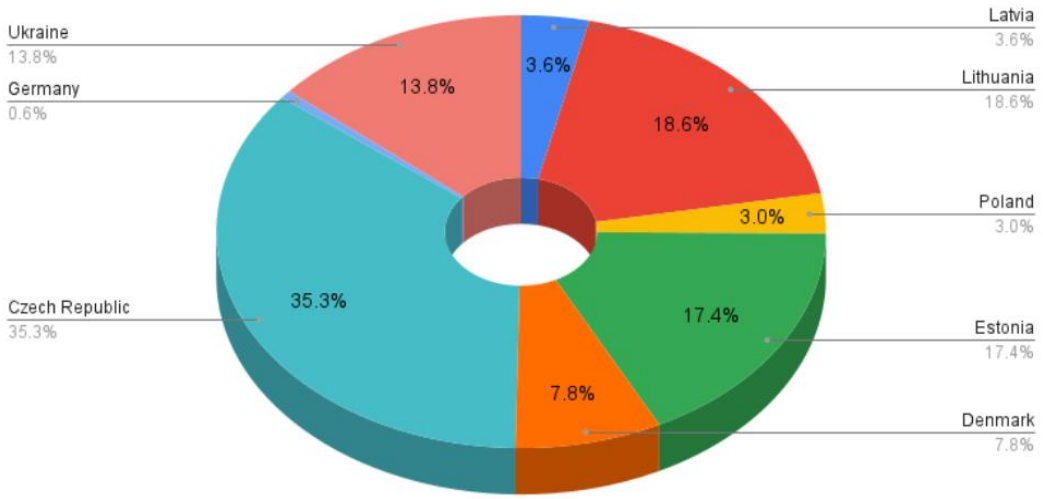

Figura 5: Shpërndarja në përqindje e sulmeve të grupit, gjatë muajit Janar nga shtetet e targetuara (Burimi: SOCRadar)

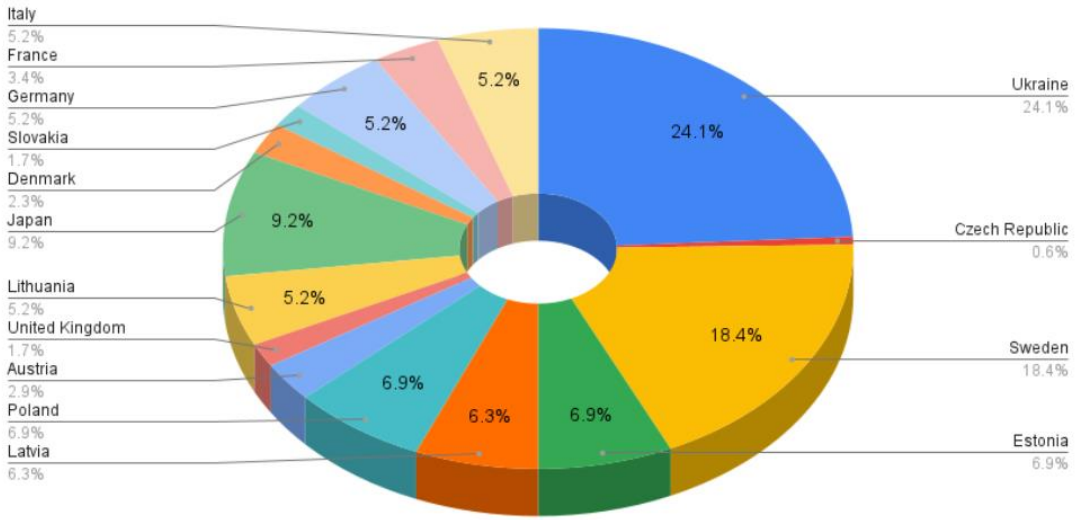

Figura 6: Shpërndaja në përqindje të sulmeve gjatë muajit Shkurt bazuar në vendet e targetuara

(Burimi: SOCRadar)

Në sulmet e fundit, **NoName057(16)** ka synuar sektorin financiar, kryesisht në institucionet financiare Ukrainase dhe Polake.

Institucionet financiare Ukrainase përfshijnë:

- Joint Stock Company “Bank Credit Dnepr,”
- State Savings Bank of Ukraine “Oshchadbank,”
- Joint Stock Company TASCOMBANK,
- Bank JSC “UNIVERSAL BANK,”
- Pravex-Bank,
- MTB Bank,
- Piraeus Bank,
- Bank JSB “CLEARING HOUSE,”
- IndustrialBank,
- Ukrsibbank BNP Paribas Group,
- Credit Agricole Bank.

Ndërsa në Poloni përfshihen:

- PKO Bank Polski,
- Bank Pekao,
- Plus Bank,
- Raiffeisen Bank,
- Polish Development Fund (PFR) Ventures, and another Polish Development Fund Group, PFR Towarzystwo Funduszy Inwestycyjnychhas been targeted by NoName057(16).

Metodat e sulmeve të grupit *NoName057(16)*

Metoda kryesore e sulmit të grupit është Distributed Denial of Service (DDoS). Për të kryer një sulm DDoS, nevojiten botnets. Grupi i hackerave deri më tani ka përdorur “***Redline Stealer botnet Bobik”***, një “***Remote Access Trojan (RAT)”*** për të operuar sulmet DDoS të tij.

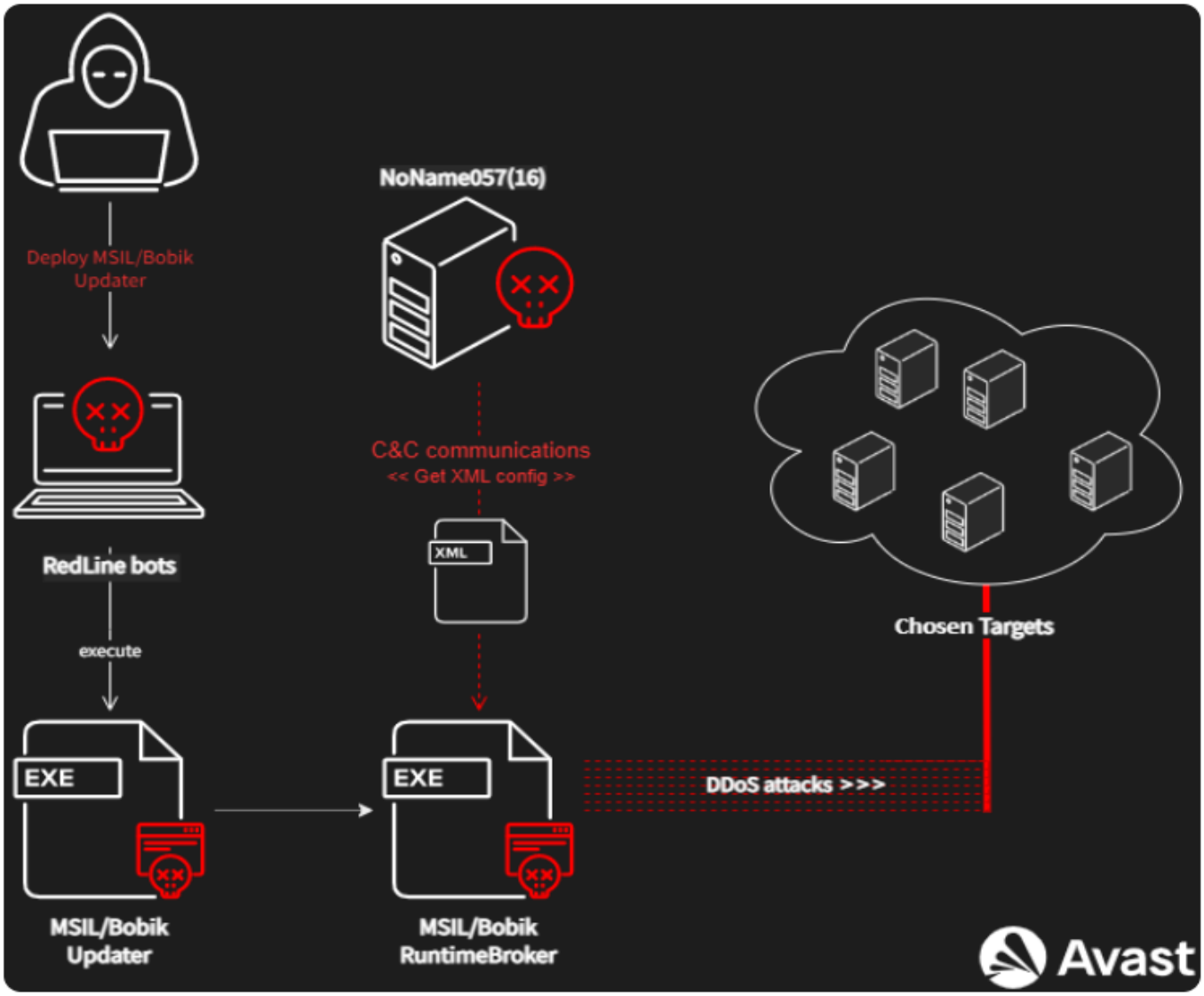

Figura 7: Vendosja e proçesit të Bobik e përdorur nga NoName057(16) (Burimi:Avast)

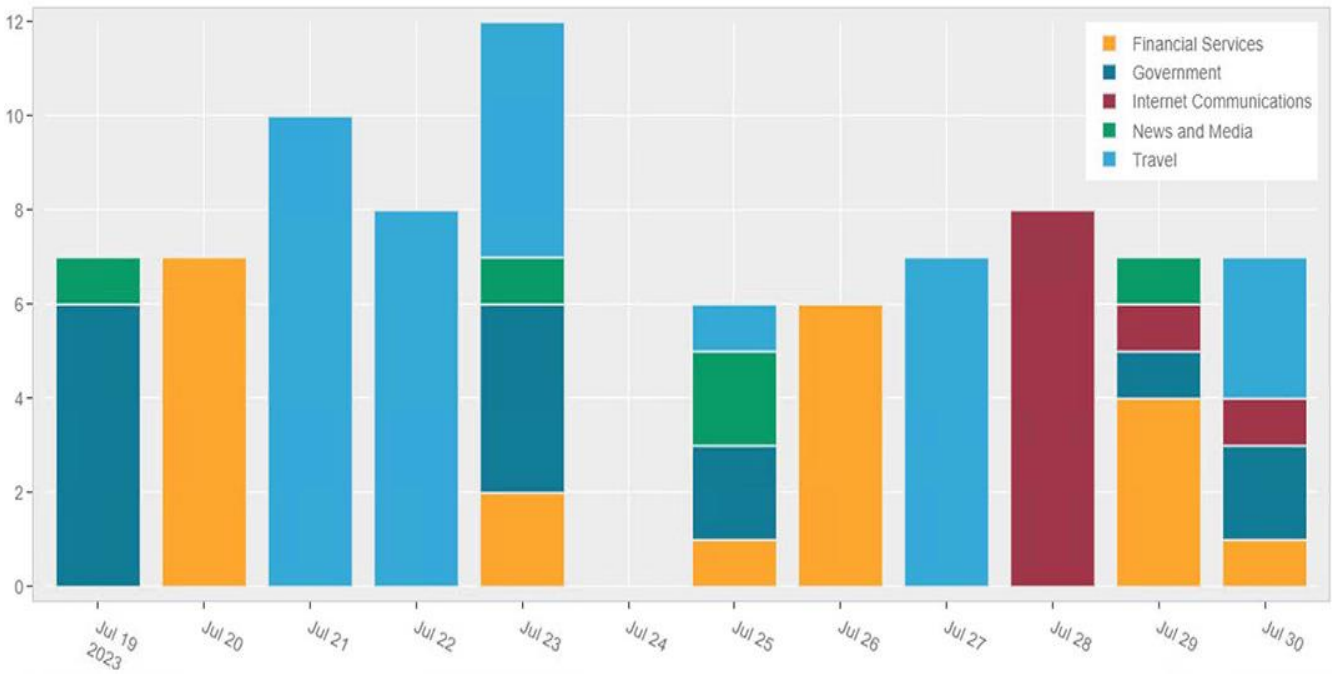

Figura 8: Sektorët e synuar në Korrik 2023

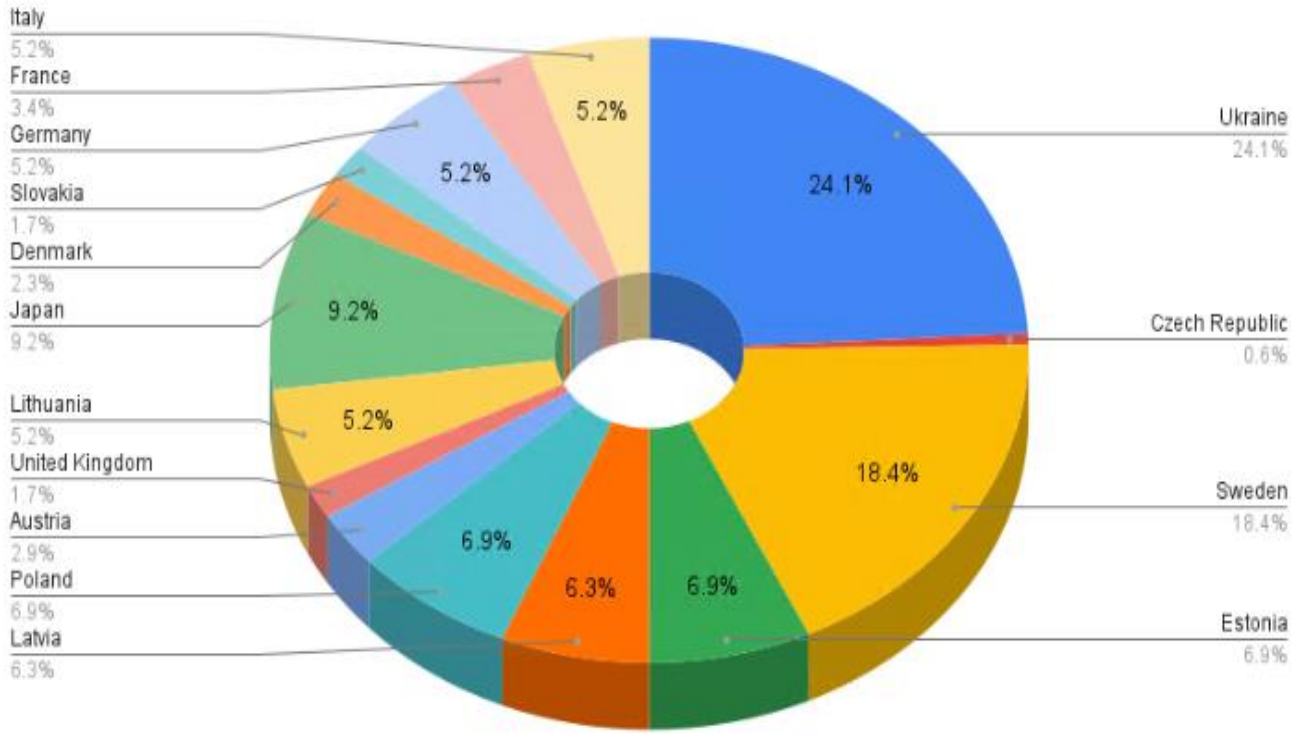

Figura 9: Shtetet e sulmuara më shumë në Korrik 2023

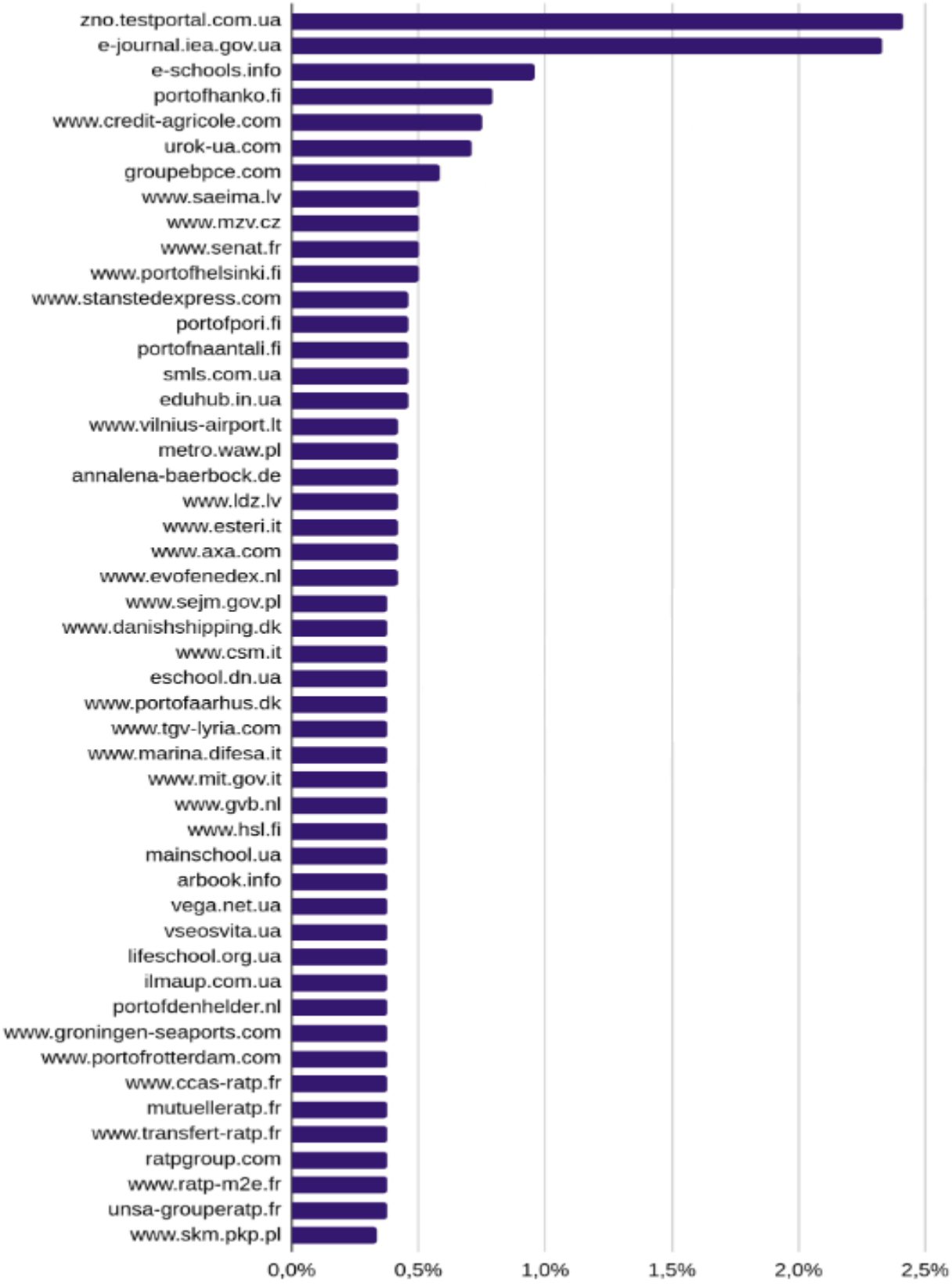

Figura 10: 50 faqet e internetit më të sulmuara nga NoName057(16)

Referimi dhe veprimi në bazë të Taktikave, Teknikave, dhe Procedureve MITRE ATT&CK' (TTPs) dhe Treguesve të Kompromentimit (IoC) të Grupit keqdashës Rus NoName057.

TA0011 Command and Control	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0007** Discovery
TA0040 Impact	**T1499** Endpoint Denial of Service	**T1498** Network Denial of Service	**T1049** System Network Connections Discovery
T1016 System Network Configuration Discovery	**T1547** Boot or Logon Autostart Execution	**T1071** Application Layer Protocol	

Figura 8: Teknikat, Taktikat dhe Procedurat e përdorura nga NoName057(16)

Datë 22/09/2023 nga bashkëpunimi shumë i mirë me AKEP dhe ISP (Internet Service Providers) si dhe të gjithë infrastrukturat e prekura shikohet që sulmi është eleminuar duke vendosur filtrat e duhura anti DdoS dhe 95% të kërkesave nuk kanë arritur të jenë të suksesshme.

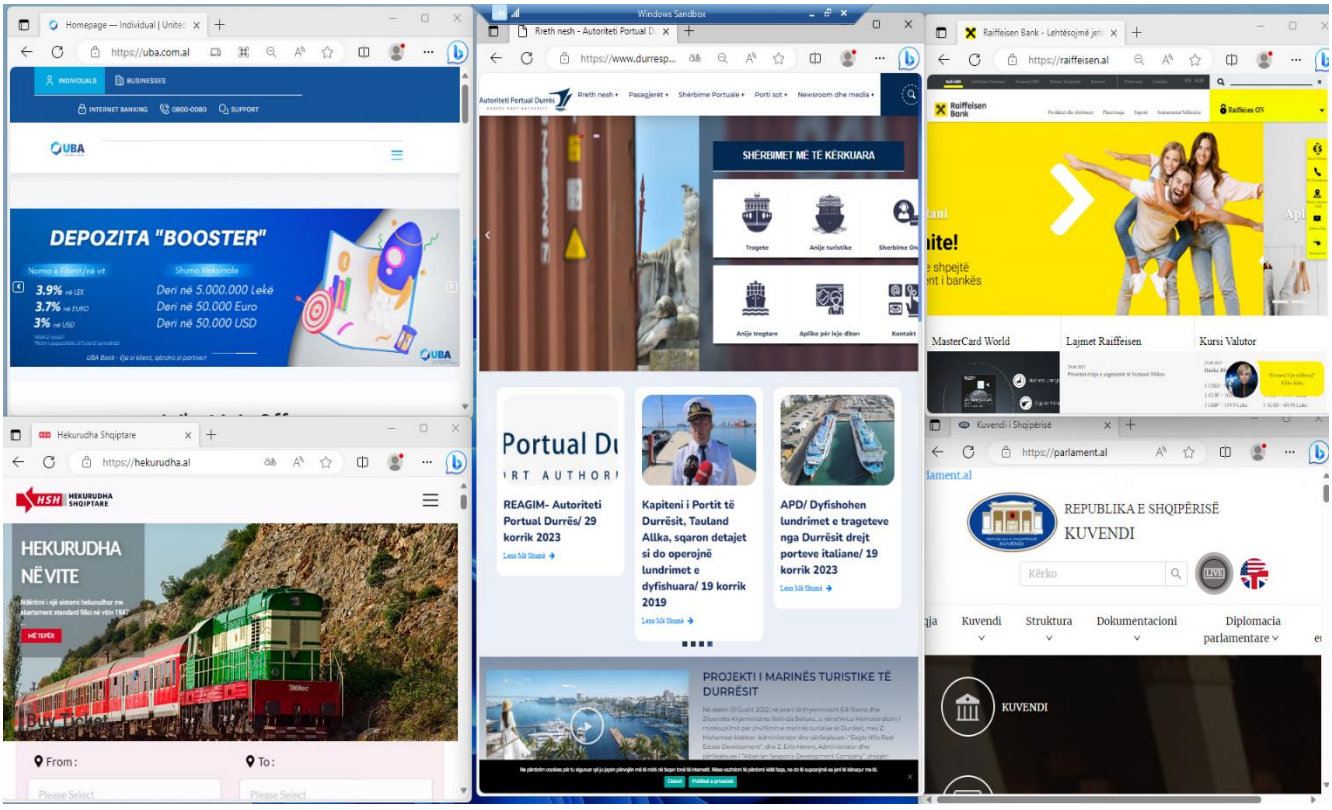

Figure 11: Problematikat e rregulluara

Indikatorët e kompromitetit (IOCs)

TIPI	Indikatorët e sulmeve
IPv4	94.140.114.239
IPv4	23.216.147.64
IPv4	20.99.184.37
IPv4	192.229.211.108
IPv4	114.114.114.114
IPv4	2.57.122.82
IPv4	2.57.122.243
IPv4	109.107.181.130
IPv4	77.91.122.69
IPv4	31.13.195.87
FileHash-SHA256	fae9b6df2987b25d52a95d3e2572ea578f3599be88920c64fd2de09d1703890a
FileHash-SHA256	f0fe30d33eeb8bb73f7d3ff4844ae632e3ed6a5f55f46ebc8b008c2f274f23e6
FileHash-SHA256	ee003e90d86ad027df9a10ba1d5cd34b0d806d8a31200bfbb472b3911e8a5934
FileHash-SHA256	ca60e1a24868136bc2ee27c7bf33e6605ea6bac297ef9c25cefed1902914dabf
FileHash-SHA256	c29f1c31ce2cb55e94274081e1db7a9b85d258bdd2d049259c1af33b2e5a5fc8
FileHash-SHA256	c1d24c5bbd80066a936e703805a8617deb96e86272ba71bcf540b574b1caa1dd
FileHash-SHA256	bbfefd38766c187f7e3903c4782804b7242673e7f72a40b1763896c73a17b630
FileHash-SHA256	a3b6b719ce886b1b47b5e1d94d5d017c6bd58d3732ee3d43e0557b6395a87401
FileHash-SHA256	9c95ab10c67c5ac8980a77eb838a30f168a6b9dc627489cd32041d02ef4e67f3
FileHash-SHA256	9a1f1c491274cf5e1ecce2f77c1273aafc43440c9a27ec17d63fa21a89e91715
FileHash-SHA256	99f0b2accef85843ea62935ac4bfefbd72eb2d5989a5440d52112b1d4d0f7b24
FileHash-SHA256	8eb708fb8f044596b841b47c2d75f6c02f878f5685b75008084c70752b961d15
FileHash-SHA256	8e1769763253594e32f2ade0f1c7bd139205275054c9f5e57fefd8142c75441f
FileHash-SHA256	848b47c55da850343ef365a367da5387673219f69ac6a0fa98a23527c886a350
FileHash-SHA256	7e12ec75f0f2324464d473128ae04d447d497c2da46c1ae699d8163080817d38
FileHash-SHA256	7bc0a27df5b8420ca23081fb973bb68729bab7b6229513c81019f7be76deb8e1
FileHash-SHA256	761075da6b30bb2bcbb5727420e86895b79f7f6f5cebdf90ec6ca85feb78e926
FileHash-SHA256	74ceb6eb99a71221a6c2e5408eac4a05878279a73021d97ab9dc87a0b13e8165
FileHash-SHA256	726c2c2b35cb1adbe59039193030f23e552a28226ecf0b175ec5eba9dbcd336e
FileHash-SHA256	66662654fddfabac6024e9026ec7a90109eb52ff710a0e24e02b004bc4e53cde
FileHash-SHA256	659ea2a2b93c8a51f66368aab6b8744aaa59894e147b236b9279d7f4a5e28d77
FileHash-SHA256	458844d1edad3253667e6eea0dc735a748e87ff784cbf12c80f05c15e96ec3d9
FileHash-SHA256	306b1ec94edc35a6de3bff359ed4c3eb397624a259622e517ee6cca5ec67ecb1
FileHash-SHA256	30200109a37b650d69ac118a0ed36010a6b857043e41a160496b51d12924528e
FileHash-SHA256	2e645745a77459be01fa26f5ba2bfe0c5bfee7f4a96263cfd335a10e65f17881
FileHash-SHA256	269504171aacb87e66f51cb6dc6353b371bde963aad8a406281862ed18b540ca
FileHash-SHA256	1e66c01d3e2c896aea6f9608ac121048bb93fc182a61d6554ed92052fa638fc8
FileHash-SHA256	04d56c6a8ad2167e6838dbac92a0407f1abe832768f0646a4fc503c269902994

FileHash-SHA1	f9274e33dc0ce645c108b277a6a4c016872bf58a
FileHash-SHA1	f8d735d2a6890849c8b5bed15eaf70d7c73a47a7
FileHash-SHA1	f4cd37128057701661f5b50d85a0d01f011f648f
FileHash-SHA1	dcf39d59cc58ee98f331871c7416a3cb4cda3271
FileHash-SHA1	bc5843dd36d4a8e2e500b217052379b33d26c768
FileHash-SHA1	9c4533416484b1449fa2052fb65ecbb1a9e68602
FileHash-SHA1	93a9f9ddc75ac2b8a0f5ec56a4e4194ecbe7bde4
FileHash-SHA1	56c3f841aa0459e8eb93df55eb6f7d5e3e4437a9
FileHash-SHA1	4f193dfeb7e71699ed9c38893dd7bdad6306ee11
FileHash-SHA1	4d02003d0030ed34d786f96e90d7131daebb45f5
FileHash-SHA1	3a6af84d1cd133c603eb66f15e082995ea03ca8f
FileHash-SHA1	2fc23bd2d7307a9dc3c10848342bc24ff45159d2
FileHash-SHA1	1a2803c5804ca9d68f6b59546493db6f95680d61
FileHash-SHA1	05c8b4534ac412240972bc807da48ac6e8a8ab4f
FileHash-SHA1	94d7653ff2f4348ff38ff80098682242ece6c407
FileHash-SHA1	e786c3a60e591dec8f4c15571dbb536a44f861c5
FileHash-SHA1	c86ae9efcd838d7e0e6d5845908f7d09aa2c09f5
FileHash-SHA1	e78ac830ddc7105290af4c1610482a41771d753f
FileHash-SHA1	09a3b689a5077bd89331acd157ebe621c8714a89
FileHash-SHA1	8f0b4a8c8829a9a944b8417e1609812b2a0ebbbd
FileHash-SHA1	717a034becc125e88dbc85de13e8d650bee907ea
FileHash-SHA1	ef7b0c626f55e0b13fb1dcf8f6601068b75dc205
FileHash-SHA1	b63ce73842e7662f3d48c5b6f60a47e7e2437a11
FileHash-SHA1	5880d25a8fbe14fe7e20d2751c2b963c85c7d8aa
FileHash-SHA1	78248539792bfad732c57c4eec814531642e72a0
FileHash-SHA1	1dfc6f6c35e76239a35bfaf0b5a9ec65f8f50522
FileHash-MD5	ea252a83f501a1fd293d4a649cce274a
FileHash-MD5	e6239ebafc69b135007413ac8f78b26e
FileHash-MD5	d4d180a05ecd3189628183793db2a8a6
FileHash-MD5	c7ea77da6e9c68fa54bbb11c1b12818b
FileHash-MD5	bd73f60ea81ac924a2e0b0b055f29d0f
FileHash-MD5	9c87eace72edffd50c4713ffa127e551
FileHash-MD5	9b9cdac0500794c369a3275624b37899
FileHash-MD5	7b68c2c502809e55cd43aa255825f1ad
FileHash-MD5	6e97d3248be719d62ab5371d03f5588b
FileHash-MD5	3725aee958df5c00797c44df003d4b70
FileHash-MD5	2c2802221441e510b67049f640224888
FileHash-MD5	1c91041a27becab88009f11b7d5e45cd
FileHash-MD5	0ffdf132cf201ab8b1bbf6e3e1d9333e
FileHash-MD5	014a15caca151701a316b09e75c5a2ff

FileHash-SHA256	00000254e6344d34a1e4ef157cb01d8b7efa65c22c996f9dfe85e7482c6c86ab
FileHash-SHA1	f336b50f5cca2ddc0341e2c4001b419a830d27a5
FileHash-MD5	ed5c771224fbd6f9b2c0cf1e8cce09b5
FileHash-SHA256	00044048f4bc537527adf1e3fb9bc161b3d8b0486093ceac87b6ae1946053a80
FileHash-SHA256	000000fa31dd212345f86e2129eef17b12d197742f60f90a90554a5f9ad2eee1
FileHash-SHA1	e33c69056cf6b827c5ec6d9e93330f3139dc1e81
FileHash-SHA1	5020b29393a3a694059f37c2b1084c798cfe928f
FileHash-MD5	ce8c21c534386baade5485f6136415cc
FileHash-MD5	a5a327539b6d98d869a01921f3fe0de8
FileHash-SHA256	69b9e0b2f38faf1b7b960db783bc67ffa2048bfd0e22ac455fd7441f3296d139
FileHash-SHA256	0004d986bb59ce995903d11c710c05f1d43af00047bebd5e277538ca57f57637
FileHash-SHA256	00047eca77dedf2d3b3213dc1cc94df713e58ceeb482a4b8a91ee216f53ae32c
FileHash-SHA256	000473eb7dd933b5e08929643bac0f9f28d62633ea0f8a061f276703478af67a
FileHash-SHA256	000460b2c275914268bac3e063b1ed16beef417fa60ee564ada978edfae2cb32
FileHash-SHA256	0004090cf180bbf33c61151cc16b2aa57ce52e6c4e62756d523917c461733dad
FileHash-SHA256	0003b82288fa18c42487e418e5e72c9b8e18b3579221e24472721150bcd1bd76
FileHash-SHA256	00036f6dfe1db2c67c3e57ab253b7b982d2e8e25e5b8576cf10498736966d5dd
FileHash-SHA256	000333138bb0f66d865c664b5b892b1f08211cdd42b1a5f8b7c6779b2fab8268
FileHash-SHA256	00033224b62564fa6a37bf6293d96dee6e70eb4820b70957023575ed15179076
FileHash-SHA256	00029f8882d72e5707fdbd3a76867db74ce6930db238ccf3e2ce9976feef123f
FileHash-SHA256	000273a58938b234595b390ef5752f166e8eecea6252cd6da07b72db23bec6e3
FileHash-SHA256	00023527df55454eb5044800a719fb8b15e2a83695830e5ed1a9615ddb8f8054
FileHash-SHA256	00020e01c2c1d1d166d31383674e12d282b3b71c8fa9df0aab553b27fd87e4aa
FileHash-SHA256	000206cf182dbd1d32efea3695bc2d43d11a6ab9bb9ca27aa0335a0b44fe9992
FileHash-SHA256	0001f69435b7b17dcfa01748218de8a9007bd79e5d9f5b1ce41600fc58becb26
FileHash-SHA256	0001efd7365502c22926de8489fd0a7a89b7fc2ecb51e26e682fe965d50f050d
FileHash-SHA256	0001e11c9115837a902f681ba689815b832bb8ec942bab73519e24aa10aabe17
FileHash-SHA256	0001a1b290a275a8dfcca188e05dac526d2d873c46ef55eac7dc2f872fae608e
FileHash-SHA256	00019a7e5767b044bfe8b9b442f3ba146011b3cc6168925b56b5160bed69e714
FileHash-SHA256	00018905aae75982cca94b4dbdaec00c99b5209fb96c28b2380e2c2fd6001617
FileHash-SHA256	000185f46ffe20eda6031b039672491a2de2459606c7a921cb1697f352527d86
FileHash-SHA256	0000c13be593cf025d699aefd506796a2e11b5190ab28870facd065297a55107
FileHash-SHA256	0000aa529de5773e5091c7ea250581289cf943d667522113c489f65cc6c7ac17
FileHash-SHA256	00007e19dedc3548e96acd9d1ba66532b29fd3a77d21af4e2c0844ff72951d6e
FileHash-SHA256	0000532f716af9fd8cb29a5e9a3f5ee8df552208509e291fc3078e5a5d613b9b
FileHash-SHA256	00004177f03c1c2c5de1883dae166ab9a8aff70028036760a009685b922e7488
FileHash-SHA256	00003e647fe39f379c90cad62bb72188efbd5110b94db73ffc5f4168c80b4623
FileHash-SHA256	00002f5b34595f5814dd8557d6b6a56be8b09fe89c22008f82dd2c1d86293b84
FileHash-SHA256	0000299dab00f4d54307b23aaae49ee99ed65a46d253696446005e074e7b7d36
FileHash-SHA256	0000198cb57a02f282e9298407d601a6be519773b6541f57d0a22eba00d369cd

FileHash-SHA256	0000168b62a47fd2a418490547019f5ba14d2e1b92e7a35257031313a0121e66
FileHash-SHA256	000011248cbea867ea1eb2c7a3c89404c2d798894df67498c6edd665deac38e0
FileHash-SHA256	00000ab418c53abe095fca6ba9c460a63c980435814f70edf4c9fccb16a91837
FileHash-SHA256	00000a4a004c92576382a1ebd671de96e67a715c0ac0793aa7e3fa45b131e958
FileHash-SHA256	00000a2f3e178a4f2002ccf6b867365cbe25d43c92f64f1ac902baf9dce4146e
FileHash-SHA256	000008d822b0e7388cb0592b85642795acfd63057362d51d64c1e5af3e0bc0c9
FileHash-SHA256	000007c75c101dc83c52cfa7b08bbb6cc55a093cdd6fc73b1a1643689e800298
FileHash-SHA256	0000071efd2b97475dda89c6442a10bc6c6800a02903bbcb0ba89fef7a2aad33
FileHash-SHA256	00000607bb57653704fcda4e081dae3ab9d2ae3e886529d2e8a3d658ae5de63d
FileHash-SHA256	000005ccf6f4b68d12350a4d2791d1fc23c039ea5db1a357ab8d8c4c07e84d6e
FileHash-SHA256	00000569f28e2819050a27ecfbb9b03daa74d167b0121dba29ad39481d7b6ead
FileHash-SHA256	000005427fbe8d0b914fc56eec86ca6ee480a3a44b5fb5cb19eaeec29c21240e
FileHash-SHA256	0000039c1449f55a0825b566a4bdf728b398022c5af6cffb5786d1c0e7fdd1b2
FileHash-SHA256	0000036208b5ff68e26c338ff6d112b5d1c746091552031690286ad6cec26ac0
FileHash-SHA256	000002f1558a89f29984934d511289491032f9e96a249c12f2f6d42678264114
FileHash-SHA256	000002b4264441f39074ca5d48693ab72a2e35ade1cb9b30a18b388fb45c7603
FileHash-SHA256	000002a2558f34a0ebba13e90b7396af19d09d33268ae3aae7092fe81209278f
FileHash-SHA256	0000028f80066ad99544cc7a79caa649ee72eca2711b1b1128df61ffd13b0657
FileHash-SHA256	0000025ebd4ecf2fb52e8cbd8d4c72f2fb070c33e8ad24a1f12f74f30ac03119
FileHash-SHA256	000002305f386d9f7223c3bbf47164ca6f09f947dcd83b54c657594c54c6a359
FileHash-SHA256	0000021a70776a8d6968b58d128f35f01024f0ab590e709d970076e560250b04
FileHash-SHA256	000001ea2ae617d6de171f648d2683ff43b52cc01bc077f131cfd1be7549704a
FileHash-SHA256	000001e41599558a88da7cf4549285f6bab7bc348f4fd780aaaf27df8552fb02
FileHash-SHA256	000001e0650c8c94a9896862b1a02909936b9a8c0b9c0a8ac668fc622d3db177
FileHash-SHA256	0000017430387fa4d5e0bcff6bd02c8d521fb0ee4c44b6a3511b2b08fab5ebcb
FileHash-SHA256	0000012ea6fe3418b78446902fdf6b2959bb6324671f7ccc000a9ca6b15da31a
FileHash-SHA256	0000012e0dcff68425fd5e43ed3d668e74362a47fc93695cdf84696450d1df3a
FileHash-SHA256	000000e19cec622a01eee714629a0e641aae0264a41d19fcf240a0e911af700d
FileHash-SHA256	000000c30bd1247c9088ff83758a335a9d1aeffa89ec8757fc7de2f6ac563080
FileHash-SHA256	000000c1a823b0dbd22efbcb933b00e6d01fa62cfcb9a52d87e13948128f40a6
FileHash-SHA256	00000078afd5c2441b0a4ca628c1b7bcc961a68f2b779d281af6d2af405b5f1a
FileHash-SHA256	00000077553a5b27a610ac98f29563bbd6e0decc020c2d49e4fa0d89197e7fd8
FileHash-SHA256	00000075d77e227cdb2d386181e42f42b579eb16403143dc54cd4a3d17fc8622
FileHash-SHA256	000000627a55405cf609a534f2bd38ab2b74a50b17b4db5c271ef3305e38c830
FileHash-SHA256	00000048b1c9e60c14a6619f0292dea96df7f10c11cfa9ae28693219c0ae844b
FileHash-SHA1	ec715fe20231cb1cbe5ecf0eb1a33e33f9cf2c20
FileHash-SHA1	def92cd1a39062567e89304472236725d1cf8ebd
FileHash-SHA1	d45fbc0e01ddd64b18bd2f5f171f41ca3bcb88c0
FileHash-SHA1	b22a89d74e687d438724afef529ff54cf03671cb
FileHash-SHA1	a6186d98e4579f6802b4e4bee551833da2f3f302

FileHash-SHA1	8082df2822e1c4432eac87e51a5e70349f986f0c
FileHash-SHA1	776c5c5f005b0dc899586caa44815bfe48ceaf1d
FileHash-SHA1	5997ff10da5ce10ac28be2fa2941dccb3929d63c
FileHash-SHA1	4f67925c85b5cff98929083a3dd3c8b4bae87c1f
FileHash-SHA1	4bd827294f0ad2826d0c929563e621fe3b20997e
FileHash-SHA1	39d39d2ef7c05d8afc2848e8ae2a08e55ca422a3
FileHash-SHA1	0a6d717d33329bbc794ac3d608d197e276654228
FileHash-MD5	de498cf7be31ded3dd436f4623d1572f
FileHash-MD5	d041c6e0156b87978a54ab6a49f66593
FileHash-MD5	cc17c4e2805306984a614f5dcb3915e7
FileHash-MD5	b457518a80a0ce3c3c9558ec2e73602c
FileHash-MD5	7da21749854b2f0bd9a4a460484af2da
FileHash-MD5	7c64c189856caf65f2e0dafe5fef4d47
FileHash-MD5	7265719c94c5ffbcdbb5f71228d8ca68
FileHash-MD5	704a435ba88091baadc3b0dc86074b46
FileHash-MD5	6f673469206fa5120de6b175b0977904
FileHash-MD5	6421ff7c627288d69609a7c404de03de
FileHash-MD5	4db0c5b6b17665ad8245bdb93094d03d
FileHash-MD5	3be20f8b614703c1a0fe8c8b1e8caf17
Domain	tom56gaz6poh13f28[.]myftp.org
Domain	zig35m48zur14nel40[.]myftp.org
Domain	05716nnm@proton[.]me
Domain	dddosia
Domain	[.]github.io
URL	hxxps://t[.]me/noname05716
URL	hxxps://t[.]me/nn05716chat
URL	hxxps://github[.]com/dddosia
URL	hxxps://github[.]com/kintechi341

Rekomandime

Disa nga masat që rekomandohen për infrastrukturat për të parandaluar sistemet dhe rrjetet e tyre nga sulmet kibernetike:

AKCESK rekomandon infrastrukturat të zbatojnë praktikat më të mira të mëposhtme për të zvogëluar rrezikun ndaj sulmeve të këtyre aktorëve keqdashës.

- Sigurohuni që aplikacioni antivirus dhe anti-malware të jetë i aktivizuar dhe përkufizimet e nënshkrimeve të përditësohen rregullisht dhe në kohën e duhur. Antivirusi i mirëmbajtur mund të parandalojë përdorimin e mjeteve të sulmeve kibernetike të vendosura zakonisht, të cilat shpërndahen përmes spear-phishing.
- Nëse organizata juaj po përdor lloje të caktuara aplikacionesh dhe pajisjesh të cënueshme ndaj dobësive dhe ekspozimeve të zakonshme të njohura (CVE), sigurohuni që këto aplikacione të jenë të përditësuara në *patch e fundit*.
- Kontrolloni indikacionet e bazuara në host, duke përfshirë *webshells* në rrjetin tuaj.
- Mbani dhe testoni një plan reagimi ndaj incidenteve.
- Konfigurimi siç duhet i pajisjeve të rrjetit që përballen me internetin.
- Mos ekspozimi i ndërfaqeve të menaxhimit në internet.
- Çaktivizimi i portave dhe protokolleve të rrjetit të papërdorura ose të panevojshme.
- Çaktivizimi i shërbimeve dhe pajisjeve të rrjetit të cilat nuk janë më në përdorim.
- Miratimi i parimit dhe arkitekturës së besimit *Zero-Trust.*
- Bllokimi i IOCs-ve të sulmuesve të sipërpërmendura.

Rekomandime që mund të funksionojnë si një masë paraprake kundër DDoS:

- Detektimi: Nëse po evidentoni shumë kërkesa hyrëse në webserver logs, ose bandwidth të mbushur, kjo mund të tregojë një sulm i cili po përpiqet të bllokojë shërbimin tuaj në internet. Kuptoni asetet tuaja kritike, identifikoni shërbimet ndaj të cilave jeni ekspozuar në internet dhe dobësitë e këtyre shërbimeve.
- Implementimi i zgjidhjeve/shërbimeve të zvogëlimit të sulmeve DDOS për infrastrukturën kritike.
- Izolim i trafikut hyrës vetëm për shtetin Shqiptar, vendosni limite/sekond ose "*lower the threshold*" në rast Sulmi DDoS.
- Kontrolloni numrin e shkarkimeve nga një adresë IP e vetme.
- Zbatoni sistemet ***captcha*** në forma publike pa autentifikim.
- Sigurohuni që përdoruesit të dinë paraprakisht se si mund të raportojne incidente.
- Edukimi i punonjësve dhe paleve të interesuara mbi sulmet DDOS dhe strategjitë e zvogelimit.
- Aplikimin e proxy servers për të ridrejtuar trafikun. Përdorni shërbimin proxy , për të bllokuar çdo përpjekje për të lundruar në faqet e internetit, të cilat janë identifikuar si faqe që përmbajnë malware ose janë pjesë e fushatave "phishing".
- Implementoni filtra Network DDoS Protection, Application DDoS Protection, Website DDoS Protection.
- Monitorim i vazhdueshëm i logeve në sistemet tuaja kritike.

Gjithashtu, ju bëjmë me dije se AKCESK, mbetet në dispozicion të vazhdueshëm 24/7 për çdo support të mundshëm.

Përsa më sipër, lutemi mbi raportimin e menjëhershëm pranë AKCESK çdo aktivitet të dyshimtë ne infrastrukturat tuaja, me qëllim reagimin në kohë dhe trajtimin e tyre!