PROFILI I GRUPEVE RUSE TË HAKERAVE

Data: 05/07/2024

TLP-GREEN

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

PËRMBAJTJA

LISTA E FIGURAVE

TLP:GREEN

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

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

Krijimi i një profili mbi disa aktorë kërcënues të një shteti 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 grupet e hakerave "*State Sponsored Attackers"* dhe "*Advanced Persistent Threat"* (APT) të lidhur me një shtet. 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*. Këta tregues përfshijnë URL-të, emrat e forumeve ose burime të tjera që sugjerojnë përfshirjen e një shteti në aktivitetet kibernetike.

Faza e dytë:

Mbledhja e provave: Dokumentimi dhe ruajtja e provave përkatëse nga *DarkWeb*. Regjistrimi i pamjeve te 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 te mbledhur për të përcaktuar besueshmërinë dhe autenticitetin e profilit të *DarkWeb*. 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 te 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 shtetëror 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.

Adresa: Rruga "Papa Gjon Pali II" nr 3 Tiranë;
Tel./Fax: 04 2221

Në këtë raport do të listohet lista e grupeve të hakerave në Rusi të cilat mund të impaktojnë Republikën e Shqipërisë. Një pjesë e tyre ka bërë tentativa sulmesh DDoS kundrejt Infrastrukturave në Republikën e Shqipërisë.

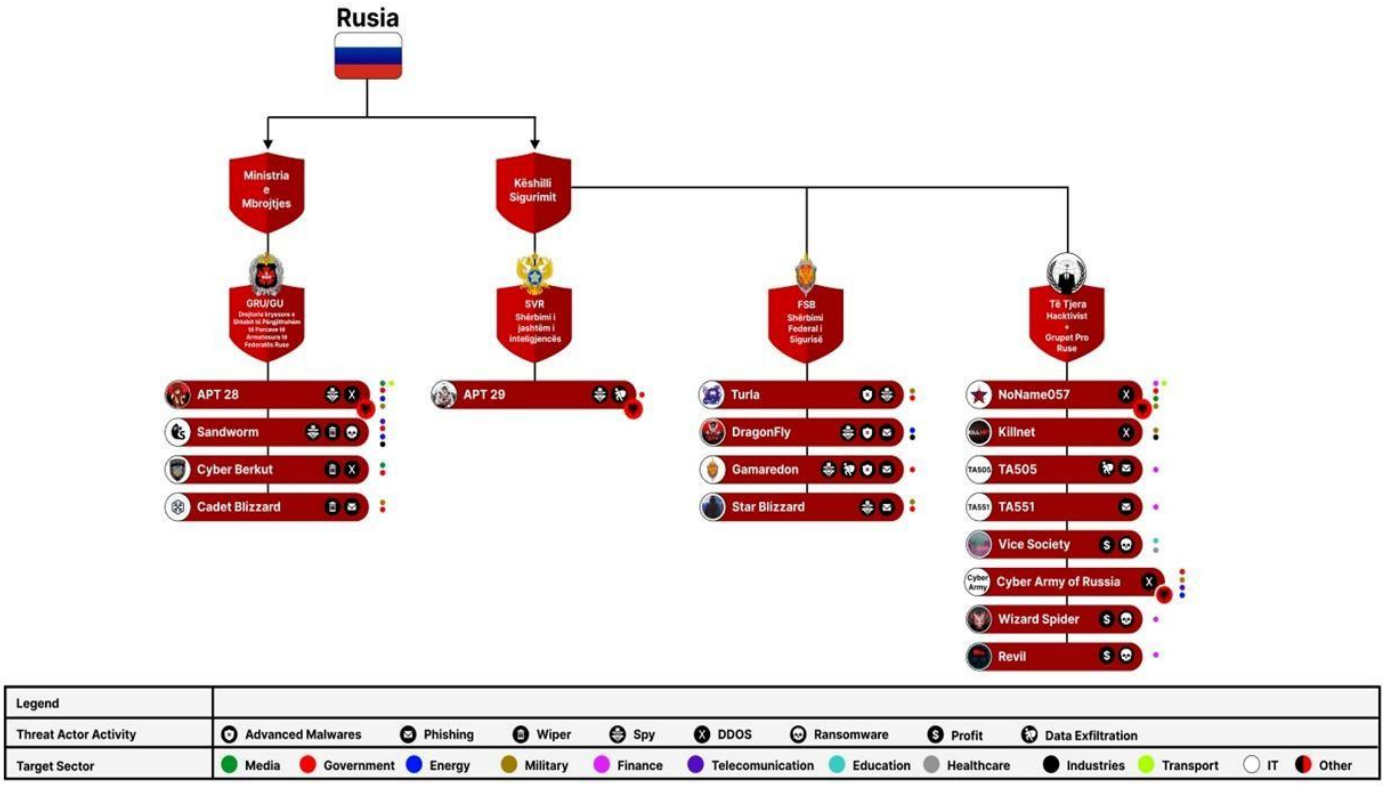

Figura 1: Harta e grupeve ruse

Grupi APT 28

APT28 (i njohur gjithashtu si FANCY BEAR, Pawn Storm, Sofacy, Strontium, Tsar Team dhe Iron Twilight) është një grup i mbështetur nga shteti rus që i atribuohet Drejtorisë së Përgjithshme të Zbulimit të Shtabit të Përgjithshëm të Forcave të Armatosura të Rusisë (GRU), Njësia 26165. Ky grup ka qenë aktiv që nga viti 2004 dhe kryen spiunazh kundër entiteteve të synuara për mbledhje informacioni dhe operacione të hakimit dhe rrjedhjes së informacionit (Operacione Informative - IO).

APT28 mban një ritëm të lartë operativ dhe shpesh synon entitete në Organizatën e Traktatit të Atlantikut të Veriut (NATO) dhe organizata partnere të NATO-s, si rezultat i interesave dhe aktiviteteve të kësaj aleance ushtarake në kufirin perëndimor të Rusisë, si dhe për të mbështetur objektivat e inteligjencës ushtarake ruse. APT28 gjithashtu ka synuar organizata në sektorët e aeronautikës dhe mbrojtjes, qeverisjes, mikpritjes, trupave ndërkombëtare sportive dhe mediave në fushatat e tyre të ndërhyrjeve. Disa nga fushatat e njohura të kryera nga APT28 përfshijnë një operacion ndërhyrjeje dhe shkatërrimi kundër medias franceze TV5Monde në vitin 2015, fushatat e hakimit dhe rrjedhjes kundër Komitetit

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

Kombëtar Demokratik (DNC) dhe Agjencisë Botërore të Antidopingut (WADA) në vitin 2016, dhe ndërhyrjet kundër institucioneve qeveritare gjermane në vitin 2015 dhe 2017.

APT28 kryen operacione të mbledhjes së kredencialeve dhe spearphishing direkt kundër objektivave të interesit ose, nëse këto objektiva janë mirë të mbrojtura, do të përpiqen të fitojnë qasje te partnerët e besuar si pikë fillestare e qasjes, nga e cila mund të nisin sulme të mëtejshme spearphishing. Grupi jo vetëm që ka përdorur një paketë mjetesh të personalizuara si XAgent, XTunnel, Zebrocy, DealersChoice, DownDelph, CredoMap, Graphite, Drovorub, Seduploader, Komplex/Complex, Coreshell dhe SkinnyBoy, por gjithashtu shpesh mbështetet në mjete me burim të hapur si Powershell Empire, Mimikatz dhe Responder.

Referimi dhe veprimi në bazë të Taktikave, Teknikave, dhe Procedureve MITRE ATT&CK' (TTPs).

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0010** Exfiltration	**T1566** Phishing
T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1204** User Execution	**T1033** System Owner/User Discovery
T1041 Exfiltration Over C2 Channel	**T1053.005** Scheduled Task	**T1057** Process Discovery	**T1082** System Information Discovery
T1204.002 Malicious File	**T1029** Scheduled Transfer	**T1007** System Service Discovery	**T1598.003** Spearphishing Link
T1562.004 Disable or Modify System Firewall	**T1564.001** Hidden Files and Directories	**T1053** Scheduled Task/Job	**T1055** Process Injection

Figura 2: Teknikat e Përdorua (APT28)

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

Hash/IP	Data
e9841e5c218611add64c07b6d6e8b2f2	14-06-2024
a6026867bfaf705bd8a58c14dcc9c301313962cec11002c6e1488a084798c5ca	14-06-2024
dfe7f4a66422420d6f73c57b64cd22225b4270963cbf00619c38d5f4c6e0a8a3	14-06-2024
9534205474098855513594 5b165e1840ba0ab93dd6ae9358dca1c203cc7080f0	13-05-2024
a1648e9432c1ed8da3bc51f75de824c4699034c7658a4eea57275025a601d237	13-05-2024
41a9784f8787ed86f1e5d20f9895059dac7a030d8d6e426b9ddcaf547c3393aa	13-05-2024
6b311c0a977d21e772ac4e99762234da852bbf84293386fbe78622a96c0b052f	13-05-2024
c60ead92cd376b689d1b4450f2578b36ea0bf64f3963cfa5546279fa4424c2a5	13-05-2024
7d51e5cc51c43da5deae5fbc2dce9b85c0656c465bb25ab6bd063a503c1806a9	13-05-2024
182[.]230[.]78[.]83	13-05-2024
351f10d7df282afed4558d765aa5018af0711fa4f37fa7eb82716313f4848a2f	13-05-2024
0873a19d278a7a8e8cff2dc2e7edbfddc650d8ea961162a6eb3cb3ea14665983	13-05-2024
07e539373177801e3fc5427bf691c0315a23b527d39e756daad6a9fc48e846bc	13-05-2024
2bd9591bea6b1f4128e4819e3888b45b193d5a2722672b839ad7ae120bf9af3d	13-05-2024
43ff178e428373512b83f85db32f364fc19c9a4ac7317835bd5089915b8727b5	13-05-2024
4f0f9a2076b0fd14124bed08f5fc939bada528e7a8163912a4ad1ec7687029a3	13-05-2024
34cabc0ff2f216830ffe217e8f8d0fa4b7d3a167576745aba48b7e62f546207b	13-05-2024
745cfce3e0242d0d5f6765b1f74608e9086d7793b45dbd1747f2d2778dec6587	13-05-2024
ae4e94c5027998f4ce17343e50b935f448e099a89266f9564bd53a069da2ca9a	13-05-2024
f348a0349fdec136c3ac9eaee9b8761da6bd33df82056e4dd792192731675b00	13-05-2024
ef67f20ff9184cab46408b27eaf12a5941c9f130be49f1c6ac421b546dac2bac	13-05-2024
e826dc4f5c16a1802517881f32f26061a4cbc508c3f7944540a209217078aa11	13-05-2024
949b0bd52a4ed47bc4a342e5a29bff2bcdb0169d2fbf0f052509b65229e19b6e	13-05-2024
ca700d44db08ad2ebd52278a3b303f8c13e44847a507fb317ea5dfb6cc924a76	13-05-2024
85f10d3df079b4db3a83ae3c4620c58a8362df2be449f8ce830d087ab41c7a52	13-05-2024
351f10d7df282afed4558d765aa5018af0711fa4f37fa7eb82716313f4848a2f	13-05-2024
642315d3091a3dfba6c0ed06f119fc40d21f3d84574b53e045baf8910e1fb38c	13-05-2024
0873a19d278a7a8e8cff2dc2e7edbfddc650d8ea961162a6eb3cb3ea14665983	13-05-2024
07e539373177801e3fc5427bf691c0315a23b527d39e756daad6a9fc48e846bc	13-05-2024
2bd9591bea6b1f4128e4819e3888b45b193d5a2722672b839ad7ae120bf9af3d	13-05-2024
750948489ed5b92750dc254c47b02eb595c6ffcefded6f9d14c3482a96a6e793	13-05-2024
745cfce3e0242d0d5f6765b1f74608e9086d7793b45dbd1747f2d2778dec6587	13-05-2024
5d2675572e092ba9aece8c8d0b9404b3adbd27db1312cd659ba561b86301fe73	13-05-2024
7c6689f591ce2ccd6713df62d5135820f94bdbf2e035ab70e6b3c6746865a898	13-05-2024

TLP:GREEN

34cabc0ff2f216830ffe217e8f8d0fa4b7d3a167576745aba48b7e62f546207b	13-05-2024
52b8bfbd9ef8ecfd54e71c74a7131cb7b3cc61ea01bc6ce17cbe7aef14acc948	13-05-2024
4f0f9a2076b0fd14124bed08f5fc939bada528e7a8163912a4ad1ec7687029a3	13-05-2024
4001498463dc8f8010ef1cc803b67ac434ff26d67d132933a187697aa2e88ef1	13-05-2024
158d49cce44968ddd028b1ef5ebc2a5183a31f05707f9dc699f0c47741be84db	13-05-2024
38ae06833528db02cb3a315d96ad2a664b732b5620675028a8c5e059e820514f	13-05-2024
949b0bd52a4ed47bc4a342e5a29bff2bcdb0169d2fbf0f052509b65229e19b6e	13-05-2024
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364	13-05-2024
598a8b918d0d2908a756475aee1e9ffaa57b110d8519014a075668b8b1182990	13-05-2024
c8f5ca7f0c01ce9d967a6895d13402e2299fc62e8b94dee27b20e66f13cb1f4c	13-05-2024

Grupi APT 29

BlueBravo është një grup rus (APT) të njohur si APT29 dhe NOBELIUM. Operacionet e APT29 dhe NOBELIUM janë atribuuar më parë Shërbimit të Inteligjencës së Jashtme të Rusisë (SVR), një organizatë përgjegjëse për spiunazhin e jashtëm, masat aktive dhe mbikëqyrjen elektronike. SVR është përgjegjës për spiunazhin e jashtëm, masat aktive dhe mbikëqyrjen elektronike. Sipas raporteve të palëve të treta, APT29 ka qenë aktiv që nga të paktën viti 2008, duke u angazhuar në operacione spiunazhi kundër entiteteve të lidhura me sigurinë dhe mbrojtjen, politikën dhe kërkimin. Fillimisht, APT29 u vëzhgua duke mbikëqyrur organizata çeçene dhe disidente, dhe më vonë u zgjerua për të synuar entitete në Perëndim, si Pentagonin në vitin 2015, Komitetin Kombëtar Demokratik (DNC) dhe think tank-et amerikane në vitin 2016, qeverinë norvegjeze dhe disa ministri holandeze në vitin 2017, si dhe ishte përgjegjës për sulmin ndaj zinxhirit të furnizimit SolarWinds në vitin 2020, i cili gjithashtu ndikoi entitetet në qeverinë amerikane në nivelet shtetërore dhe federale.

BlueBravo ka përdorur një gamë të gjerë të skedarëve keqdashës dhe mjeteve open-source. Grupi gjithashtu ka përdorur skriptim PowerShell, komanda WMI dhe kontroll të komandës me shumë shtresa për të nxjerrë të dhëna nga rrjetet e synuara. Një aspekt i dukshëm është familjet e maluerëve të tyre që evoluojnë dhe praktikat e zhvillimit, të zhvilluara në gjuhë të ndryshme duke përfshirë Python, Go, PowerShell dhe Assembly. Grupi gjithashtu bën përdorim të mirë të mjeteve publike të disponueshme si Mimikatz dhe Cobalt Strike. Në vitin 2021, raportimet publike detajuan përdorimin nga BlueBravo të disa iteracioneve të një fushate phishing që imitonte entitete qeveritare. Fushatat e ndryshme dorëzonin skedarë ISO përmes metodave të tilla si përdorimi i URL-ve për të shkarkuar skedarin ISO dhe për të ekzekutuar një skedar LNK, dhe përdorimi i një skedari HTML në email për të nisur shkarkimin e një skedari ISO. Ky aktivitet u përdor për të vendosur NativeZone, një term ombrellë për ngarkuesit e tyre të personalizuar të Cobalt Strike. NativeZone zakonisht përdor rundll32.exe për të ngarkuar dhe ekzekutuar payload-et e mëtejshme. Në tetor 2022, Insikt Group vëzhgoi BlueBravo duke vendosur maluerin GraphicalNeutrino brenda një skedari ZIP keqdashës. Vendosja dhe shpërndarja e këtij skedari ZIP përputhet me droppper-in e përdorur më parë EnvyScout, përdorimi i të cilit është i lidhur me APT29 dhe NOBELIUM.

TLP:GREEN

Referimi dhe veprimi në bazë të Taktikave, Teknikave, dhe Procedureve MITRE ATT&CK' (TTPs).

TA0007 Discovery	TA0011 Command and Control	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
T1543.003 Windows Service	T1543 Create or Modify System Process	T1012 Query Registry	T1082 System Information Discovery
T1134 Access Token Manipulation	T1057 Process Discovery	T1007 System Service Discovery	T1027 Obfuscated Files or Information
T1070.004 File Deletion	T1070 Indicator Removal	T1055.003 Thread Execution Hijacking	T1055 Process Injection
T1083 File and Directory Discovery	T1071.001 Web Protocols	T1071 Application Layer Protocol	T1574.002 DLL Side-Loading
T1574 Hijack Execution Flow	T1566 Phishing	T1110 Brute Force	T1110.003 Password Spraying
T1566.002 Spearphishing Link	T1204.002 Malicious File	T1204 User Execution	

Figura 3: Teknikat e Përdorura (APT29)

TLP:GREEN

HOSTS/IP/HASH	Data
ovh-auth-desktop.test.dermloop.io	26 Mar 2024
status.dermloop.io	26 Mar 2024
help.nomadstays.com	26 Mar 2024
stayblog.nomadstays.com	26 Mar 2024
test.nomadstays.com	26 Mar 2024
wiki.nomadstays.com	26 Mar 2024
crm.prtgroup.eu	26 Mar 2024
digita.prtgroup.eu	26 Mar 2024
irendc.prtgroup.eu	26 Mar 2024
services.hce.prtgroup.eu	26 Mar 2024
www.mail.prtgroup.eu	26 Mar 2024
admin-dev.promosapp.es	26 Mar 2024
admin-uat.promosapp.es	26 Mar 2024
admin.promosapp.es	26 Mar 2024
api.promosapp.es	26 Mar 2024
api.uat.promosapp.es	26 Mar 2024
assets.promosapp.es	26 Mar 2024
dash.promosapp.es	26 Mar 2024
dash.uat.promosapp.es	26 Mar 2024
technomania.target.ba	26 Mar 2024
wizard.target.ba	26 Mar 2024
email.metadata.is	26 Mar 2024
jobtrigger.metadata.is	26 Mar 2024
malid.metadata.is	26 Mar 2024
profilemanager.metadata.is	26 Mar 2024
visit.metadata.is	26 Mar 2024
prototype.splice.call	26 Mar 2024
u0026array.prototype.splice.call	26 Mar 2024
m.indexof.call	26 Mar 2024
prototype.indexof.cal	26 Mar 2024
q.indexof.call	26 Mar 2024
r.indexof.call	26 Mar 2024
string.prototype.indexof.call	26 Mar 2024
uint8array.prototype.indexof.call	26 Mar 2024

TLP:GREEN

bj.prototype.map	26 Mar 2024
cj.prototype.map	26 Mar 2024
dj.prototype.map	26 Mar 2024
fe.prototype.map	26 Mar 2024
g.prototype.map	26 Mar 2024
gg.prototype.map	26 Mar 2024
hg.prototype.map	26 Mar 2024
id.prototype.map	26 Mar 2024
lg.prototype.map	26 Mar 2024
mg.prototype.map	26 Mar 2024
rj.prototype.map	26 Mar 2024
te.prototype.map	26 Mar 2024
ti.prototype.map	26 Mar 2024
ui.prototype.map	26 Mar 2024
vi.prototype.map	26 Mar 2024
ye.prototype.map	26 Mar 2024
zj.prototype.map	26 Mar 2024
a.prototype.ca	26 Mar 2024
ce.prototype.ca	26 Mar 2024
chrome.cast.media.h.prototype.ca	26 Mar 2024
d.prototype.ca	26 Mar 2024
gn.prototype.ca	26 Mar 2024
gv.prototype.ca	26 Mar 2024
kt.prototype.ca	26 Mar 2024
l.prototype.ca	26 Mar 2024
lf.prototype.ca	26 Mar 2024
m.prototype.ca	26 Mar 2024
me.cast.j.prototype.ca	26 Mar 2024
og.prototype.ca	26 Mar 2024
rb.prototype.ca	26 Mar 2024
rc.prototype.ca	26 Mar 2024
s.prototype.ca	26 Mar 2024
uj.prototype.ca	26 Mar 2024
w.prototype.ca	26 Mar 2024
yu.prototype.ca	26 Mar 2024

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

hostnameobject.prototype.hasownproperty.call	26 Mar 2024
a0f183ea54cb25dd8bdba586935a258f0ecd3cba0d94657985bb1ea02afd42c	26 Mar 2024
44ce4b785d1795b71cee9f77db6ffe1b	26 Mar 2024
5928907c41368d6e87dc3e4e4be30e42	26 Mar 2024
7a465344a58a6c67d5a733a815ef4cb7	26 Mar 2024
8bd528d2b828c9289d9063eba2dc6aa0	26 Mar 2024
e017bfc36e387e8c3e7a338782805dde	26 Mar 2024
efafcd00b9157b4146506bd381326f39	26 Mar 2024
fb6323c19d3399ba94ecd391f7e35a9c	26 Mar 2024
5b6b25012fa541a227e1c20d9f3004ce4e7d4aee	26 Mar 2024
a0f183ea54cb25dd8bdba586935a258f0ecd3cba0d94657985bb1ea02af8d42c	26 Mar 2024
0x3bd487.open	26 Mar 2024
siestakeying.com	26 Mar 2024
waterforvoiceless.org	26 Mar 2024
f32c04ad97fa25752f9488781853f0ea	26 Mar 2024
e0ac85f8dbda3a175a56e4355811a4284c880318	26 Mar 2024
116866708b5c22d643427203e7b0b023ccee8effeec8801638421bf96e569813	26 Mar 2024
d0a8fa332950b72968bdd1c8a1a0824dd479220d044e8c89a7dea4434b741750	26 Mar 2024
46299f696566a15638b4fdeffe91dc01ab1e4e07e980573c29531f1bc49d33f0	26 Mar 2024
dc79c213a28493bb4ba2c8e274696a41530a5983c7a3586b31ff69a5291754e6	26 Mar 2024
c7b01242d2e15c3da0f45b8adec4e6913e534849cde16a2a6c480045e03fbee4	26 Mar 2024
182.230.78.83	26 Mar 2024

Grupi Киберармия России (Russian Cyber Army)

Russian Cyber Army, e njohur gjithashtu si Ushtria Kibernetike e Popullit të Rusisë, është një organizatë kibernetike kriminale e njohur që ka qenë aktive të paktën që nga viti 2007. Ky grup është i njohur për kryerjen e sulmeve të ndryshme kibernetike, përfshirë sulmet DDoS, kundër entiteteve që i percepton si kundërshtarë të Rusisë.

TLP:GREEN

Aktivitetet e fundit në vitin 2024 kanë përfshirë sulmet ndaj impianteve të trajtimit të ujit në Shtetet e Bashkuara, Poloni dhe Francë. Këto sulme synonin të prishnin infrastrukturën kritike duke shfrytëzuar dobësitë në sistemet e teknologjisë operacionale (OT), veçanërisht duke përdorur protokollin VNC për të manipuluar ndërfaqet njeri-makinë (HMI). Grupi gjithashtu sulmoi Fondacionin Ekonomik të Japonisë me një sulm të madh DDoS, duke bërë që faqja e internetit e organizatës të dilte offline përkohësisht.

Taktikat e Ushtrisë Kibernetike përfshijnë shpesh mbushjen e faqeve të synuara me trafik, duke mbingarkuar kapacitetin e tyre për të funksionuar normalisht. Ky qasje ka qenë efektive në prishjen e operacioneve dhe në theksimin e aftësive dhe shtrirjes së grupit. Aktivitetet e grupit janë të lidhura ngushtë me strategjinë më të gjerë të luftës kibernetike të Rusisë, e cila përfshin si sulmet shkatërruese ashtu edhe fushatat afatgjata të dezinformimit.

Në Ballkan dhe konkretisht në Shqipëri, ka pasur disa raste të sulmeve kibernetike nga grupi rus i njohur si Russian Cyber Army. Këto sulme përfshijnë sulme të shpërndara të mohimit të shërbimeve (DDoS), të cilat kanë si qëllim të prishin funksionimin normal të faqeve të internetit dhe sistemeve të ndryshme.

FUSHATA NË SHQIPËRI:

Më datë 27.06.2024, Autoriteti Kombëtar për Sigurinë Kibernetike, nga analiza e kryer nëpëmjet mjeteve të Inteligjencës së Kërcënimeve Kibernetike bazuar në burime të hapura (OSINT), ka evidentuar një fushatë sulmesh *DDoS* drejt institucioneve të Republikës së Shqipërisë.

Ky sulm dyshohet të ketë ardhur si pasojë e thirrjeve të një prej lojtarëve të Shqipërisë në Kampionatin Europian 2024, si dhe vendimeve të qeverisë shqiptare për të mbështetur udhëzimet e Brukselit dhe Uashingtonit për luftën në Ukrainë dhe përsa i përket mosmarrëveshjeve territoriale mes Serbisë dhe Kosovës.

Figura 4; Postimi që tregon se janë kundër sjelljes së lojtarit

Në postimin e datës 21/06/2024 ata i quajnë serbët vëllezër, si dhe i bëjnë thirrje serbëve të bashkohen me rusët, sepse sipas tyre ata kanë një armik të përbashkët dhe se armiku i tyre po përparon kudo. Postimi

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

mbyllet me fjalinë: "*Ju mund të jeni të sigurt se armiqtë e vëllezërve tanë janë armiqtë tanë të përbashkët!"*.

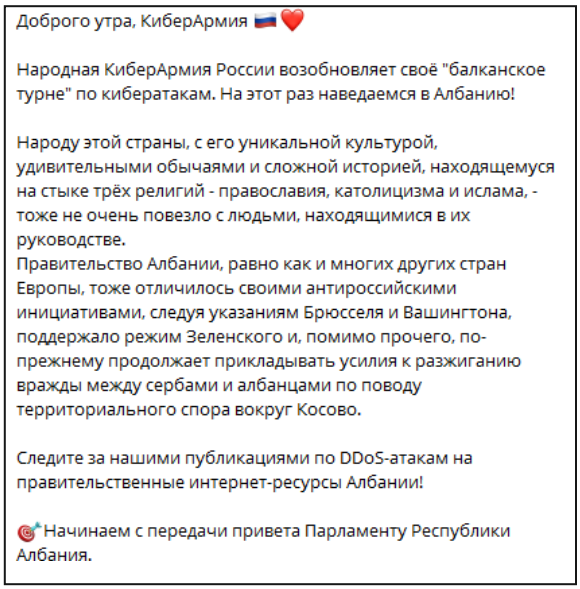

Figura 5: Postimi kundër vendimeve të qeverisë shqiptare

Në këtë postim shkruhet:
"*Njerëzit e këtij vendi, me kulturën e tyre unike, zakonet e mahnitshme dhe historinë komplekse, të vendosur në kryqëzimin e tre feve - Ortodokse, Katolike dhe Islame - nuk janë shumë me fat me njerëzit në udhëheqjen e tyre. Qeveria shqiptare, si shumë vende të tjera evropiane, është dalluar edhe me iniciativat e saj anti-ruse, duke ndjekur udhëzimet e Brukselit dhe Uashingtonit, duke mbështetur regjimin e Zelenskit dhe, ndër të tjera, vazhdon të bëjë përpjekje për të nxitur armiqësi mes serbëve dhe shqiptarëve. për mosmarrëveshjen territoriale për Kosovën*."

Analiza teknike

Nga analiza e kryer, u evidentuan se sulmet i përkasin kategorisë DDoS.
Sipas postimeve në kanalin e Telegram të "*Народная CyberАрмия (People's CyberArmy)",* sulmet janë të motivuar politikisht, si rezultat i mbështetjes pro-Ukrainës.

Adresa: Rruga "Papa Gjon Pali II" nr 3 Tiranë;
Tel./Fax: 04 2221

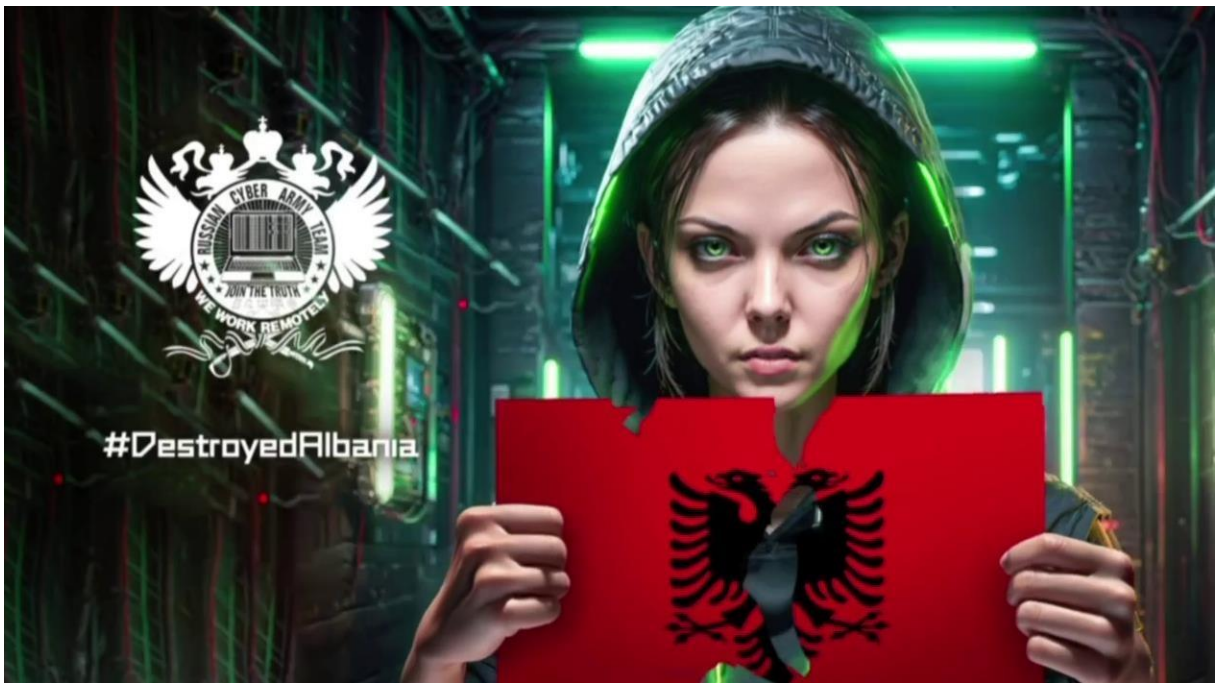

Figura 6: Imazh i krijuar me AI për sulmin ndaj Shqipërisë

Gjatë analizës *Threat Intelligence* shikohet se grupi "*Cyber Army Russia Reborn*" po bën sulme DDoS kundrejt infrstrukturave të Shqipërisë. Ky grup motivohet gjeopolitikisht rreth sulmeve në Ballkan, ku mund të përfshijë dhe aktorë të tjerë hakerash kibernetik si *CARRtel Hacknet, Noname057 (16), Cyber Dragon.*

Në postimin e këtij grupi shkruhet se ky grup po rifillon një fushatë drejt vendeve të Ballkanit.

Ky grup gjithashtu ka konfirmuar marrëveshjen me ***grupin NoName057(16),*** grup i cili ka sulmuar institucionet e Republikës së Shqipërisë në shtator 2023.

Adresa: Rruga "Papa Gjon Pali II" nr 3 Tiranë;
Tel./Fax: 04 2221

Figura 7: Publikimi për bashkëpunimin midis NoName057(16) dhe Cyber Army

Në vijim ky grup gjithashtu ka realizuar dhe tentative sulmesh DDoS ndaj institucioneve të Republikës së Shqipërisë. Të tre infrastrukturat për momentin janë nën kontroll dhe AKSK është në dispozicion të plotë për t'i suportuar në çdo moment.

Adresa: Rruga "Papa Gjon Pali II" nr 3 Tiranë;
Tel./Fax: 04 2221

NoName057 (16)

NoName057(16) është një grup kërcënues që ka kryer në mënyrë aktive sulme DDoS kundër organizatave të ndryshme në Ukrainë dhe vende të tjera pro Ukrainës.

Grupi synon një gamë të gjerë sektorësh, duke përfshirë administratën publike, transportin, financat, sigurinë kombëtare, telekomunikacionin, shërbimet, energjinë dhe bankat.

NoName057(16) ka shfrytëzuar shumë CVE, duke përfshirë CVE-2017-0143, CVE-2017-0147, CVE-2014-3153 dhe CVE-2017-0199, për të nisur sulmet e tyre.

Aktivitetet e grupit paraqesin një rrezik të konsiderueshëm të sigurisë kibernetike për organizatat në sektorët e synuar, pasi sulmet DDoS mund të ndërpresin veprimtarinë, të shkaktojnë humbje financiare dhe të dëmtojnë reputacionin.

People CyberArmy of Russia

Të dhënat tregojnë se People CyberArmy of Russia është një grup kërcënues. Megjithatë, nuk përmendet asnjë lloj grupi specifik, duke sugjeruar që aktivitetet dhe motivimet e grupit mund të mos jenë të mirëpërcaktuara ose të njohura publikisht.

Pikat kryesore:

Potencial për spiunazh kibernetik: Grupet e aktorëve të kërcënimit shpesh përfshihen në spiunazh kibernetik për të mbledhur informacione të ndjeshme për përfitime politike ose financiare.

Sulmet e synuara: Aktorët e kërcënimit mund të synojnë organizata ose individë të veçantë bazuar në vlerën ose cenueshmërinë e tyre.

Përdorimi i Malware: Aktorët e kërcënimit zakonisht përdorin malware për të kompromet uar sistemet, për të vjedhur të dhëna ose për të ndërprerë operacionet.

Taktikat në zhvillim: Aktorët e kërcënimit përshtatin vazhdimisht taktikat dhe teknikat e tyre për të shmangur zbulimin dhe kundërmasat.

FUSHATA NË SHQIPËRI:

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) .**

TLP:GREEN

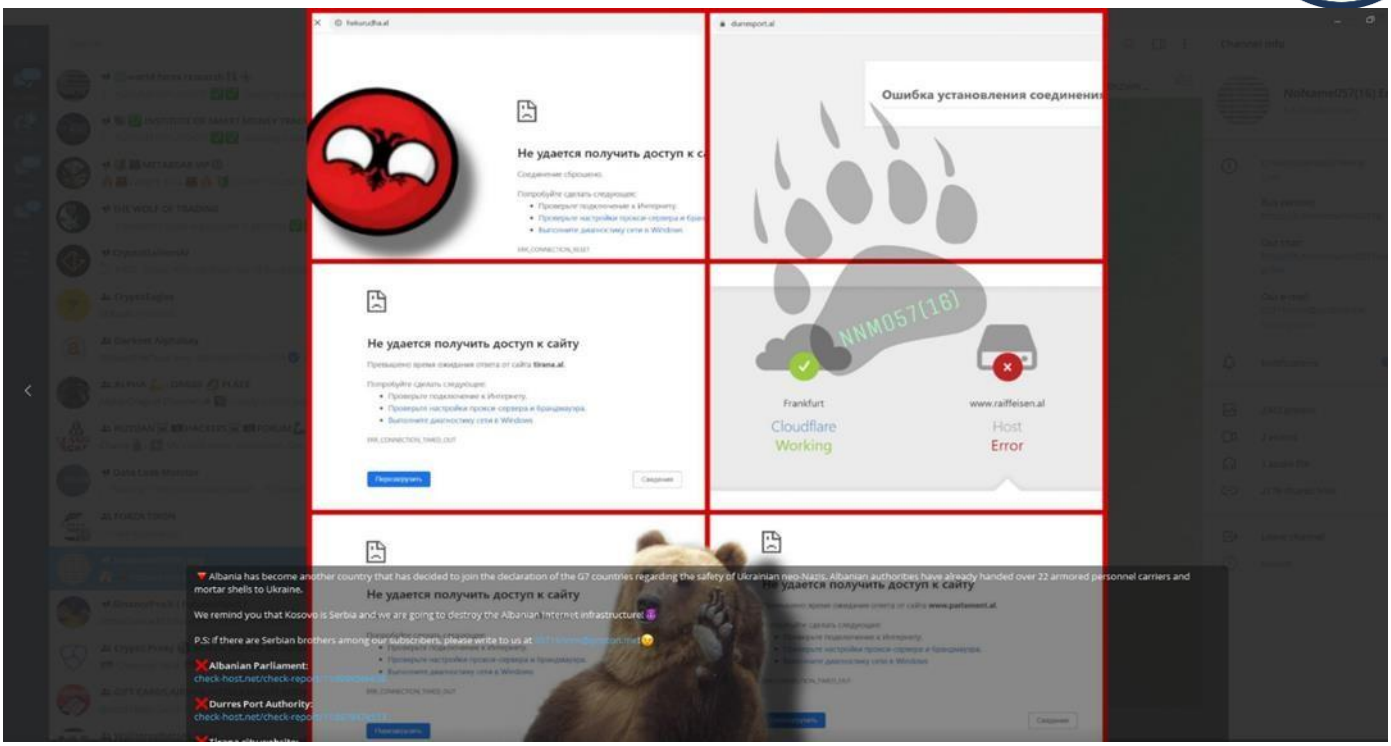

Figura 8: Njoftimi i grupit NoName057 në platformën Telegram

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.

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

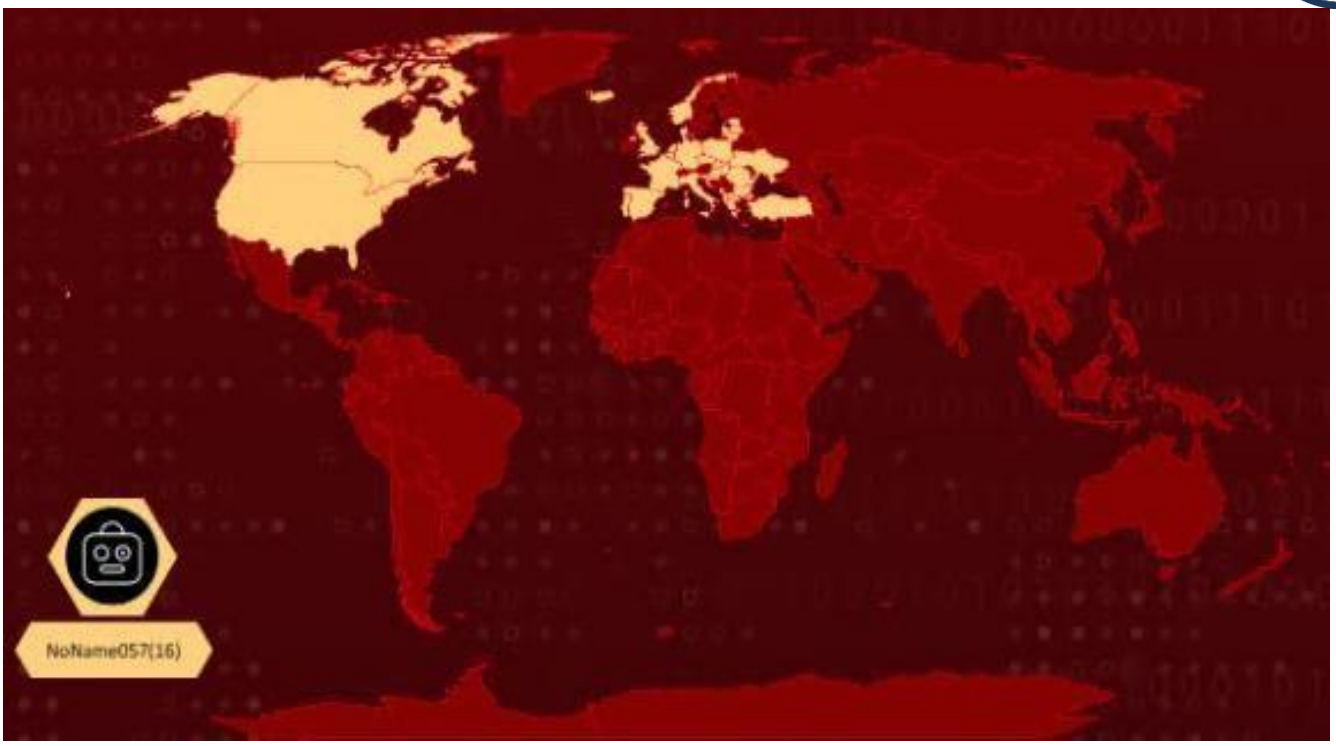

Figura 9: Harta e vendeve që janë target nga NoName057(16)

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.

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

Detajet

Tabela 1: Detaje rreth NoName

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

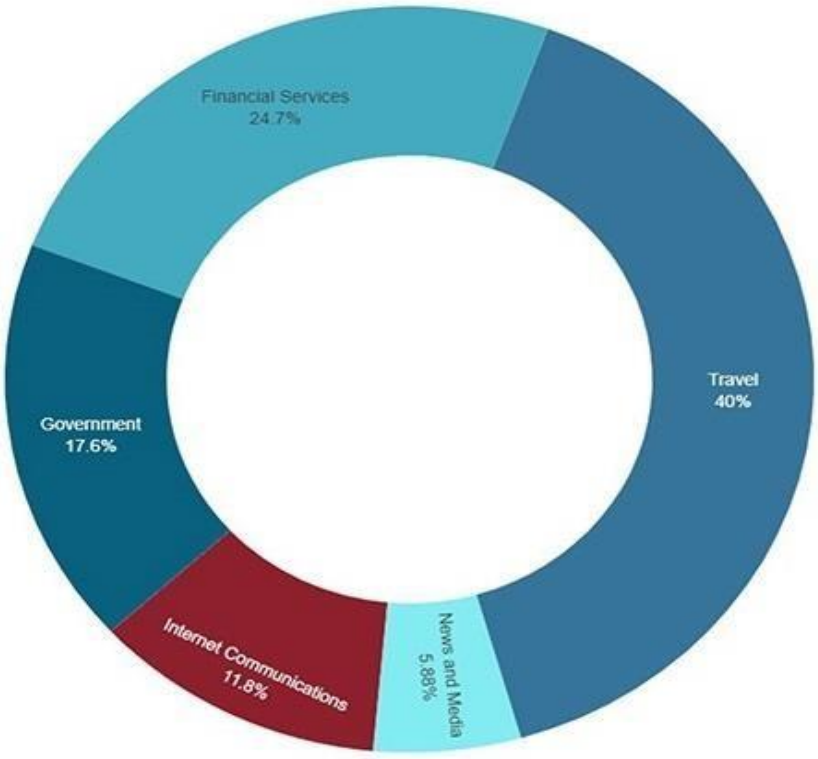

Figura 10: Sektorët e synuar nga NoName057(16)

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**.

TLP:GREEN

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

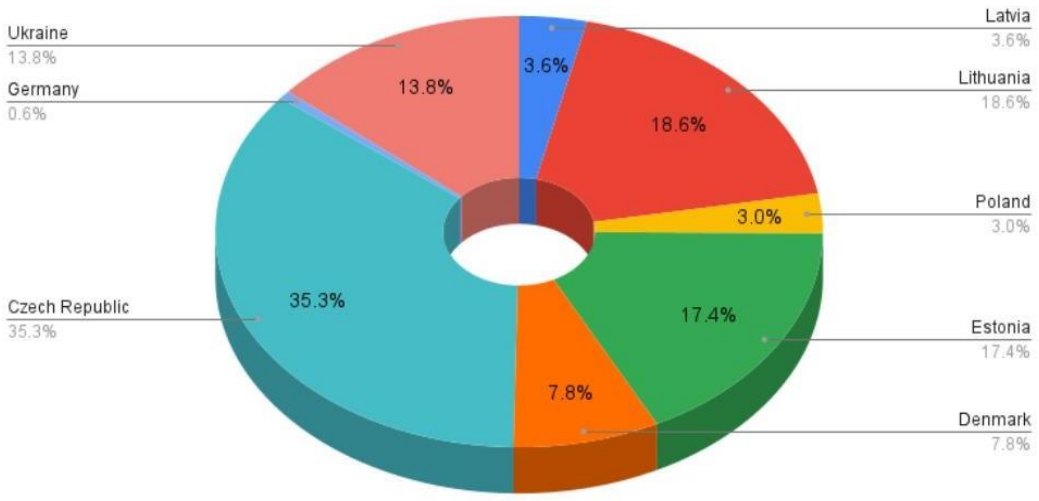

Figura 11: Shpërndarja në përqindje e sulmeve të grupit, gjatë muajit Janar nga shtetet e targetuara (Burimi: SOCRadar)

TLP:GREEN

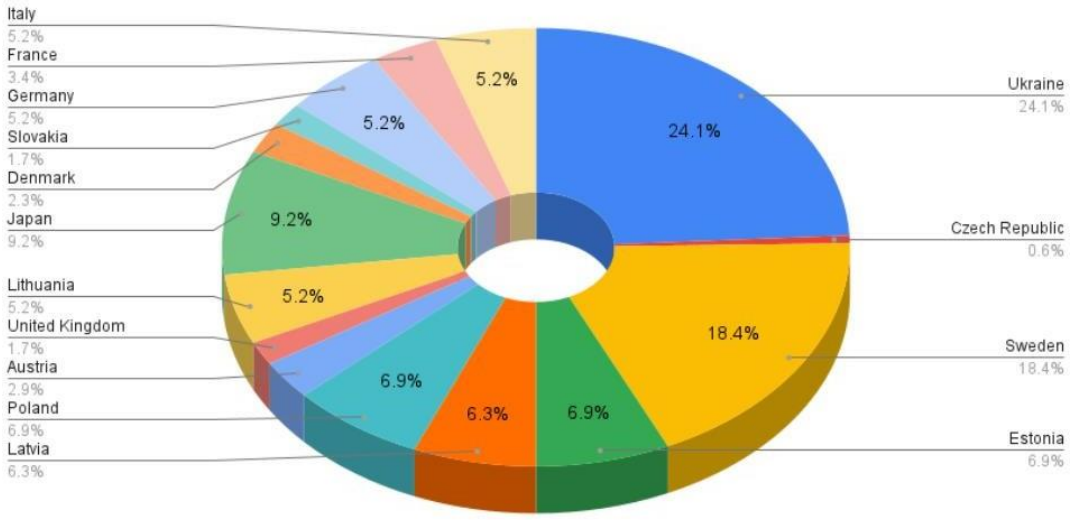

Figura 12: Shpërndarja në përqindje e sulmeve gjatë muajit Shkurt bazuar në vendet e targetuara

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).

TLP:GREEN

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.

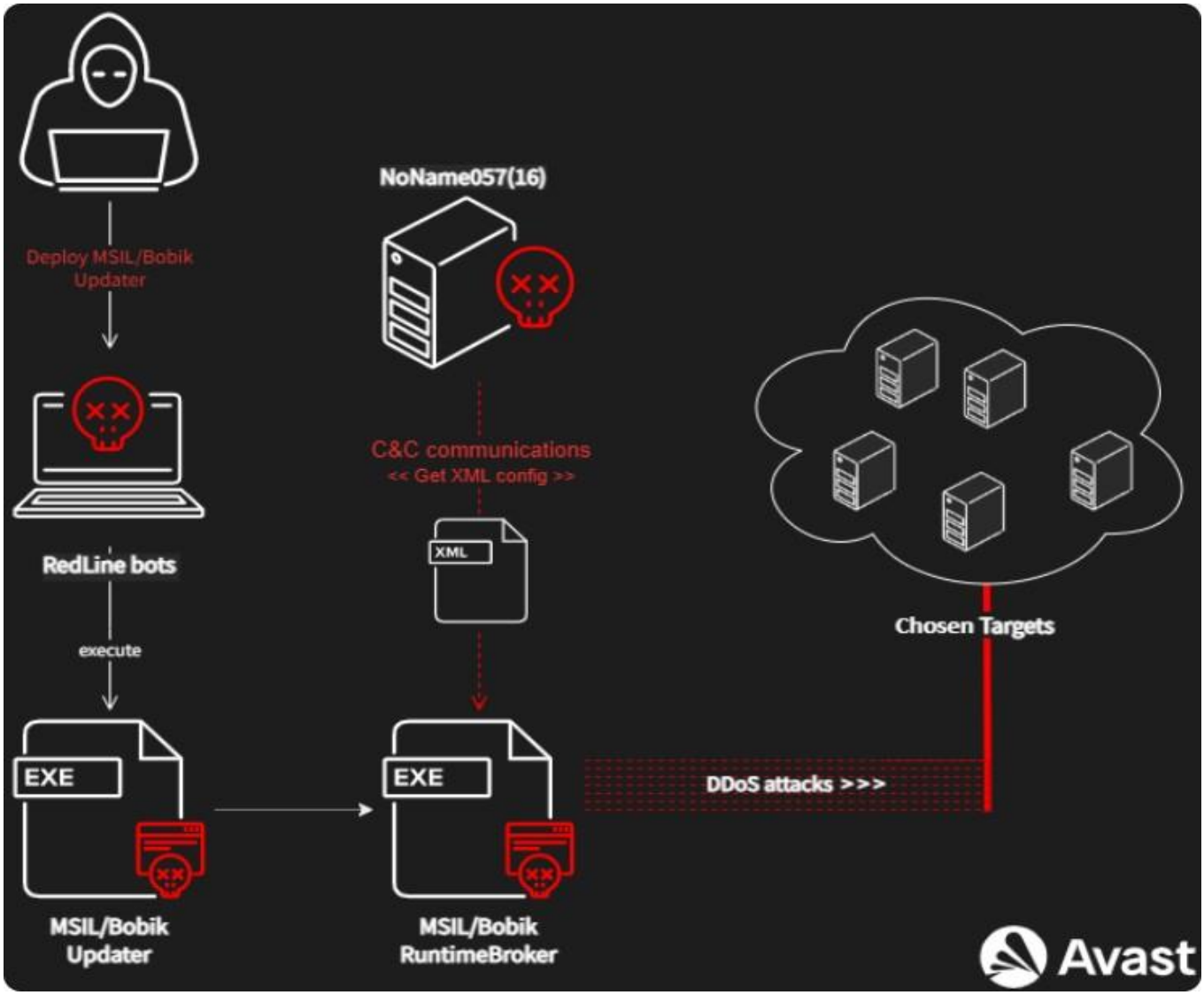

Figura 13: Vendosja e proçesit të Bobik e përdorur nga NoName057(16) (Burimi:Avast)

Adresa: Rruga "Papa Gjon Pali II" nr 3 Tiranë;
Tel./Fax: 04 2221

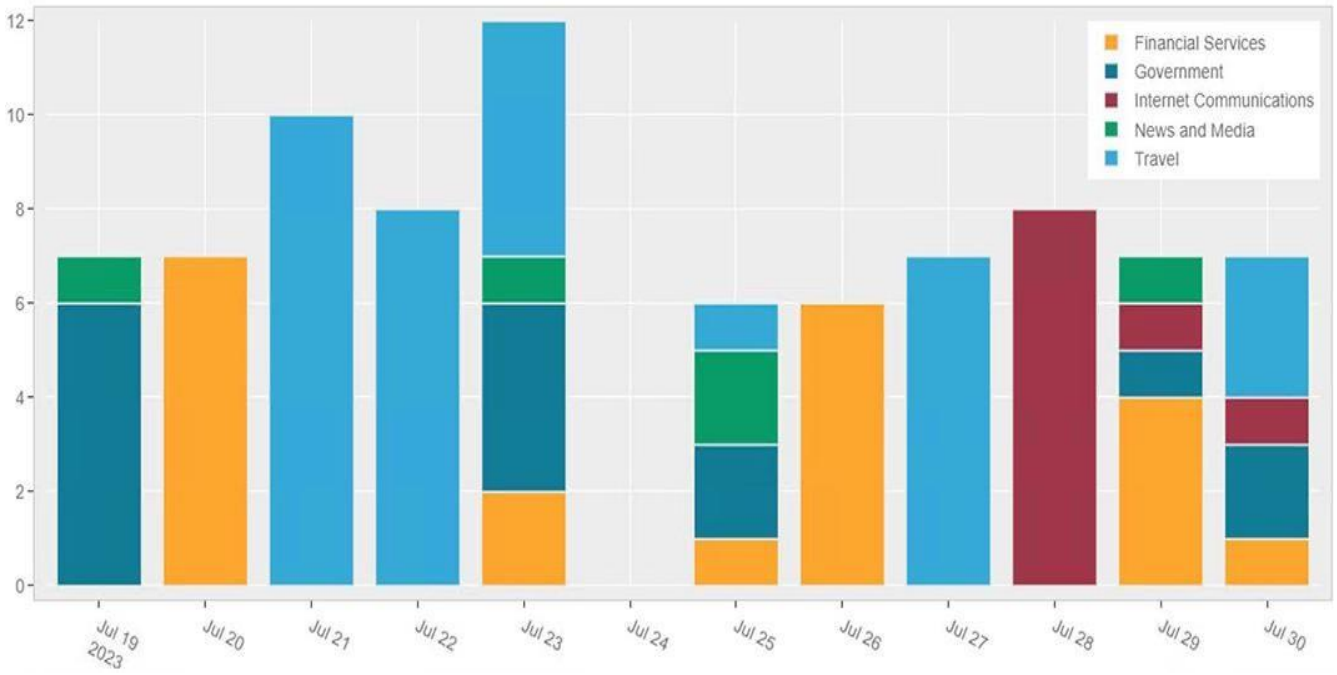

Figura 14: Sektorët e synuar në Korrik 2023

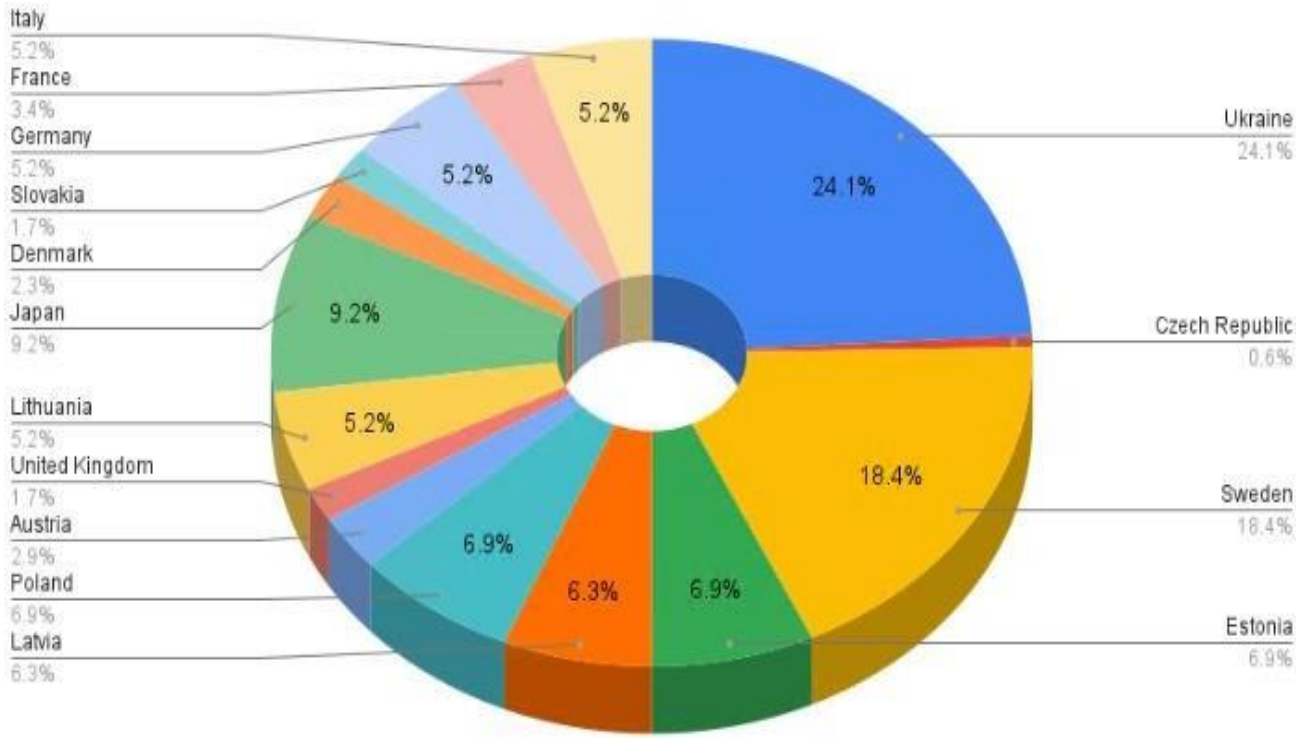

Figura 15: Shtetet e sulmuara më shumë në Korrik 2023

TLP:GREEN

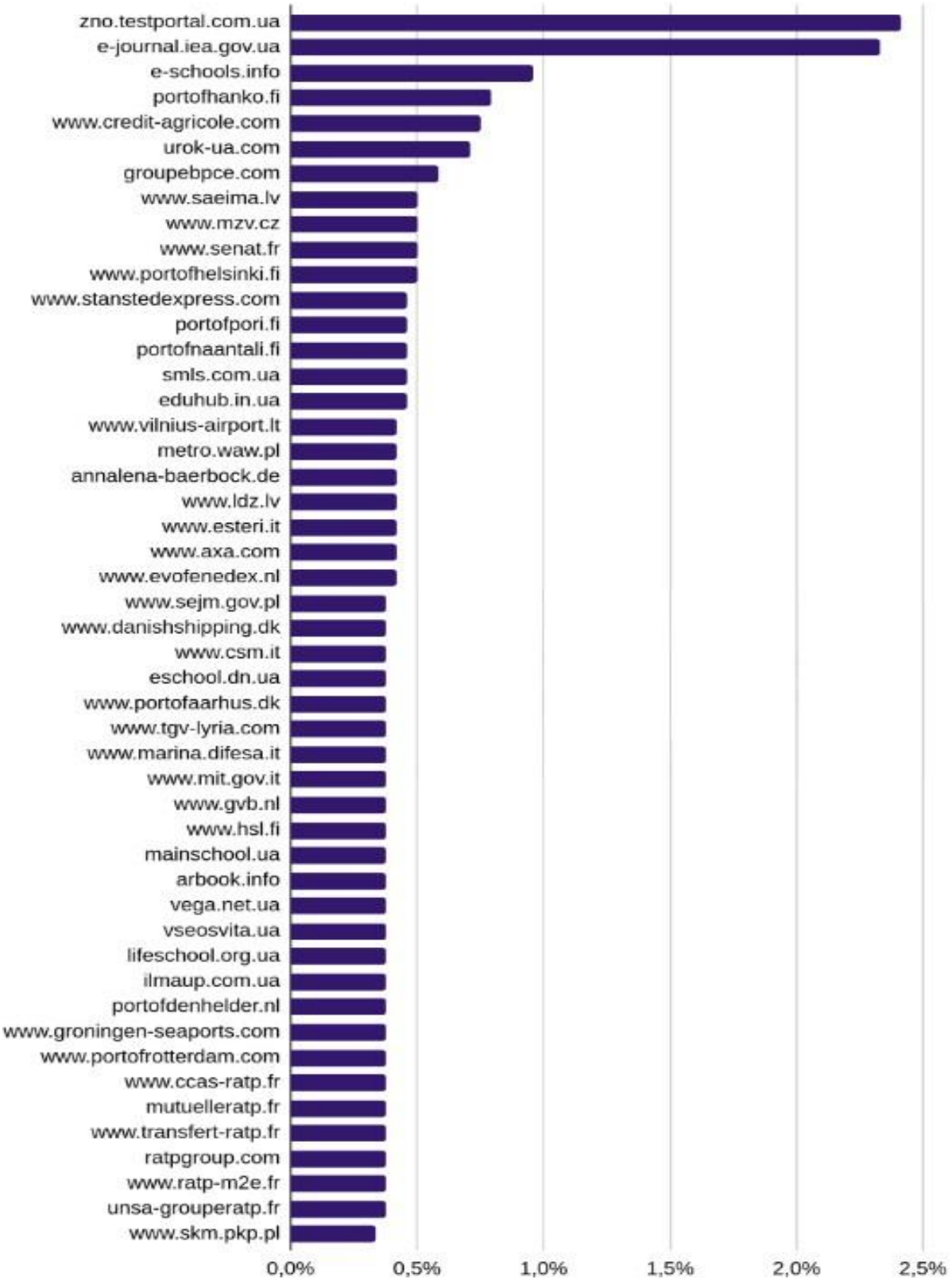

Figura 16: 50 faqet e internetit më të sulmuara nga NoName057(16)

TLP:GREEN

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

Figura 17: Teknikat, Taktikat dhe Procedurat e përdorura nga NoName057(16)

Indikatorët e kompromentimit (IOCs)

Tabela 2: Indikatorët e Kompromentimit

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

TLP:GREEN

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

TLP:GREEN

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

TLP:GREEN

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

TLP:GREEN

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

TLP:GREEN

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

Metodat e operimit – Telegram Channel

NoName057(16) operon përmes Telegramit për të marrë përgjegjësinë për sulmet e tyre, për të bërë kërcënime dhe në përgjithësi për të arsyetuar veprimet e tyre si një grup.

Kanali gjithashtu poston meme pro-ruse, postime motivuese dhe përditësime të përgjithshme. Aktiviteti i evidentuar në Telegram e bën të qartë se grupi e konsideron veten si një aktor kryesor rus në kërcënim, ndërsa në realitet impakti i sulmeve të tyre DDoS është një ndërprerje e shkurtër me pasoja të vogla.

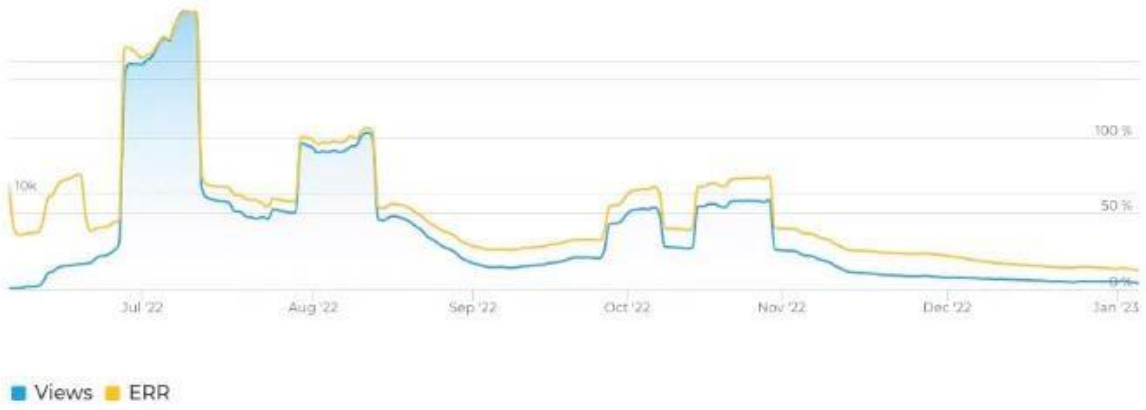

Figura 18: Aktiviteti i NoName057(16) gjatë vitit të parë

Adresa: Rruga "Papa Gjon Pali II" nr 3 Tiranë;
Tel./Fax: 04 2221

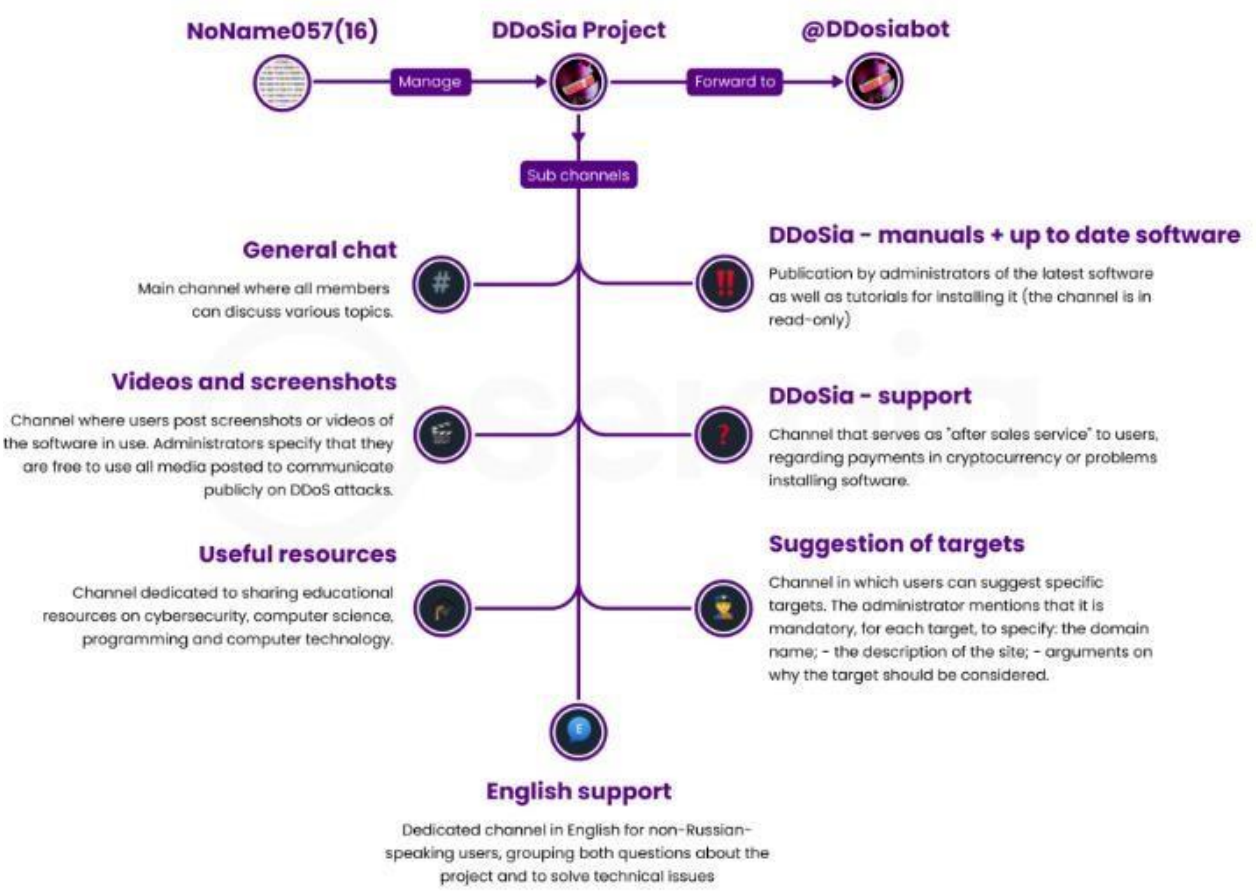

Figura 19: Aktiviteti në Telegram

TLP:GREEN

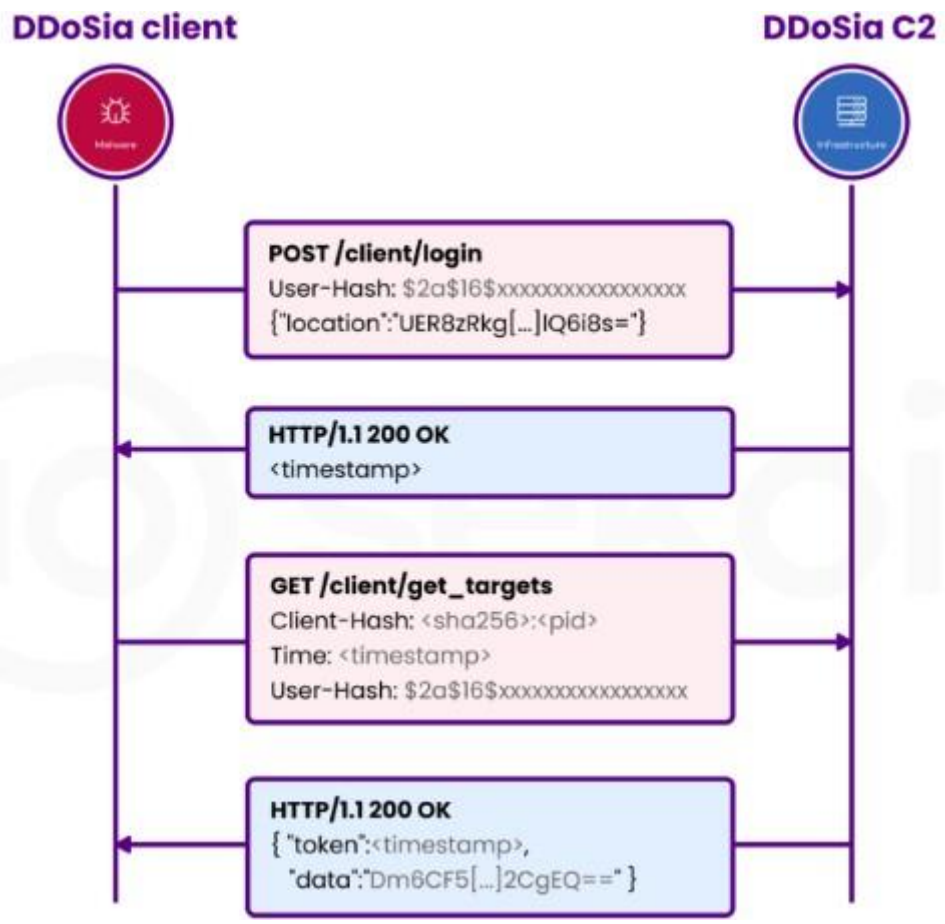

Figura 20: Lidhja midis klientit dhe C2

Kur malware ekzekutohet, krijon kërkesë POST në url hxxp://[IP]/client/login për tu lidhur me C2. Fusha "User-Hash"korespondon me përmbajtjen e "client_id.txt" , skedari që fillon me $2a$16$.

POST /client/login HTTP/1.1
Host: " hosti ku shënjestrohet "
User-Agent: Go-http-client/1.1
Content-Length: 251
Client-Hash: xxxxxxxxxxxxxxxxxxxxxxxxxxxxx:xxxx
Content-Type: application/json
User-Hash: $2a$16$xxxxxxxxxxxxxxxxx
Accept-Encoding: gzip
{“location“: “UER8zRkg[…]lQ6i8s=”}

Më tej C2 konfirmon autentifikimin dhe krijon një Token drejt klientit si më poshtë :

HTTP/1.1 200 OK

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 25 Apr 2023 19:04:09 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 19
Connection: keep-alive
Vary: Origin
Access-Control-Allow-Origin:
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Link
1682xxxxxxxxxxxxx

Vazhdimisht, klienti dërgon kërkesë GET tek C2 hxxp://[IP]/client/get_targets, ku rifreskon vlerat:

GET /client/get_targets HTTP/1.1
Host: hosti
User-Agent: Go-http-client/1.1
Client-Hash: xxxxxxxxxxxxxxxxxxxxxxxxxxxx:xxxx
Content-Type: application/json
Time: 1682xxxxxxxxxxxx
User-Hash: $2a$16$xxxxxxxxxxxxxxxxx
Accept-Encoding: gzip

Më tej C2 rikthen Token në formatin JSON:

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 25 Apr 2023 19:04:15 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 69595
Connection: keep-alive
Vary: Origin
Access-Control-Allow-Origin:
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Link
{“token“: 1682xxxxxxxxxxxxx, “data“: “Dm6CFMc9Lk4wrY2[…]XW2ZqF2CgzTboVEQ==”}

Tools i hostuar në Github

Grupi ka përdorur gjithashtu GitHub për një sërë aktivitetesh të paligjshme. Kjo përfshin përdorimin e GitHub Pages për të hostuar faqen e tyre të internetit për tools e DDoS në dddosia.github[.]io. Dy profilet

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

e GitHub janë dddosia dhe kintechi341. Postimet e para në ddos_config janë bërë me emrin "Роман Омельченко".

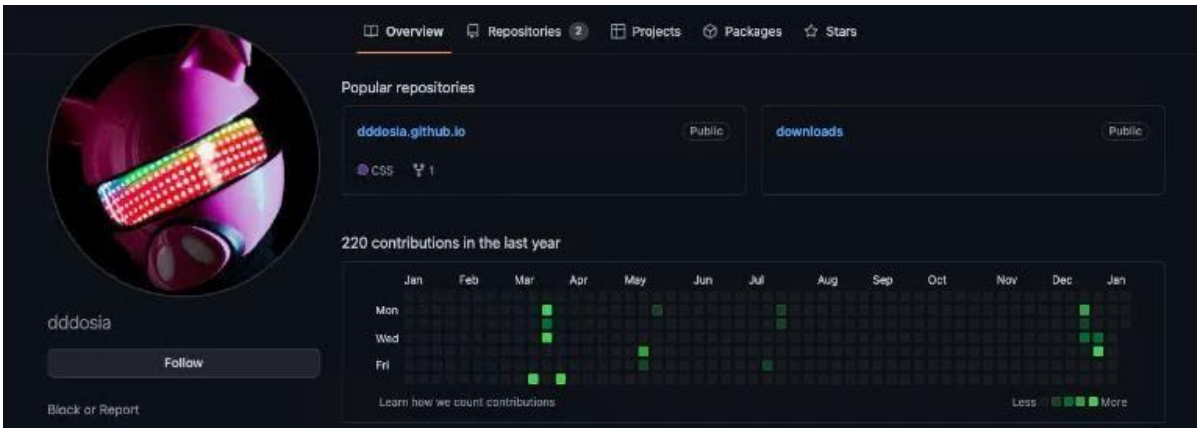

Figura 21: Profili i NoName057(16) në Github

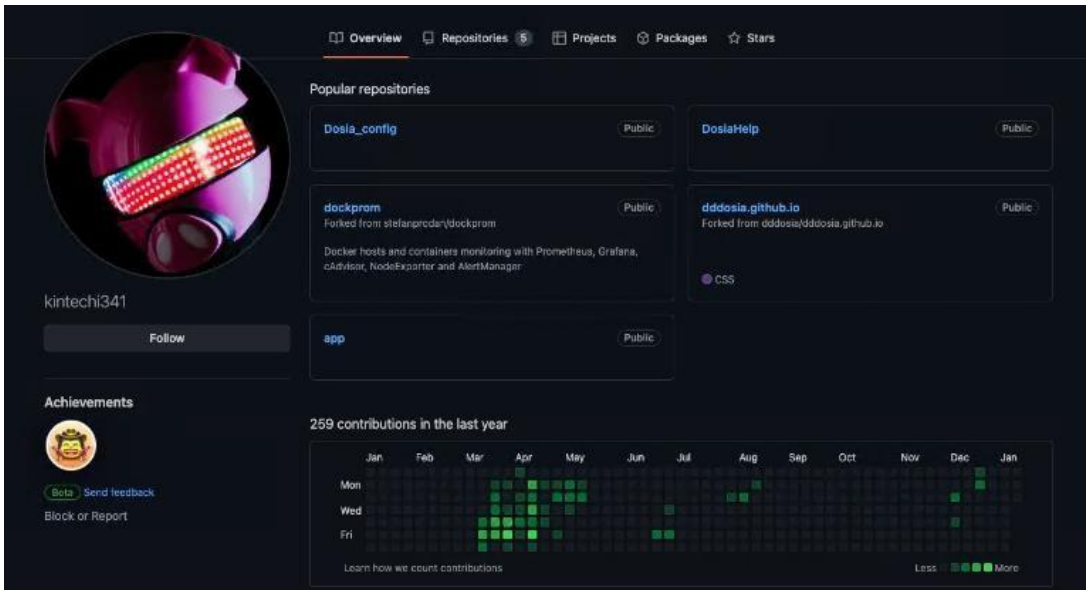

Figura 22: Profili 2 i NoName057(16) në Github

Network

Shërbimet C2 janë hostuar përmes Neterra, që është një organizatë e telekomunikacioneve bullgare, por gjithashtu përdoren shërbimet No-IP Dynamic DNS. Serveri C2 aktual është zig35m48zur14nel40[.]myftp.org në adresën IP 31.13.195.87.

TLP:GREEN

Target

Të gjitha sulmet e grupit NoName057(16) lidhen me Ukrainën dhe vendet anëtare të NATO. Organizatat që janë synuar janë zakonisht sektorët e infrastrukturës kritike, të cilët operojnë në mënyrë të rëndësishme për vendin e synuar.

Seleksionimi i objekteve të sulmit ndryshon në përputhje me ngjarjet politike. Siç është theksuar më herët, qeveria polake ishte një objektiv në dhjetor pasi Sejmi i Republikës së Polonisë e njohu zyrtarisht Rusinë si sponsor shtetëror të terrorizmit në mes të dhjetorit të vitit 2022. Në fillim të janarit 2023, u theksua shumë në sulmet ndaj organizatave lituaneze, kryesisht në sektorët e cargo dhe transportit.

Attack toolkit

NoName057(16) ka përdorur tools të ndryshme për të kryer sulmet e tyre. Në shtator 2022, Avast raportoi se ky grup kishte përdorur botnetin Bobik për të kryer sulmet e tyre DDoS. Megjithatë, grupi kërkon kryesisht pjesëmarrjen vullnetare përmes tools DDOSIA - të quajtura gjithashtu nga zhvilluesi i tyre si Dosia dhe Go Stresser, në varësi të versionit.

Janë analizuar dy raste të ndryshme të DDOSIA: një implementim në Python dhe një implementim në Golang.

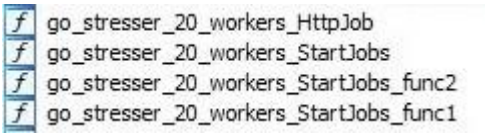

Figura 23: DDOSIA reference

DDOSIA është një aplikacion që kryen sulme denial-of-service ndaj faqeve të internetit duke dërguar kërkesa të vazhdueshme në rrjet. DDOSIA lëshon kërkesat sipas udhëzimeve të një skedari konfigurimi që malware merr nga një server C2 në momentin e nisjes. Skedari konfigurimit është në format JSON dhe ndodhet në path **/client/get_targets** në serverin C2.

Për çdo faqe të synuar, skedari konfigurimit specifikon:

- Një identifikues të veçantë të synimit në fushën **id**.
- Informacionin për të dhënat e targetizuara në rrjet në fushat host, adresë, dhe port - një emër hosti, një adresë IP, dhe një port.
- Një kombinim lloj/synimi dhe mënyrë të kërkesave në fushat **type** dhe **method**. DDOSIA dhe skedarët konfigurues më poshtë tregojnë se malware mbështet llojet e kërkesave **http**, **http2**, dhe **tcp**, dhe mënyrat e kërkesave - metodat HTTP - GET dhe POST (për llojet e kërkesave http ose http2) dhe syn (për llojin e kërkesave tcp). Bazuar në llojin dhe mënyrën e konfiguruar, DDOSIA ndërton paketa e rrjetit HTTP ose TCP (kërkesa) për t'i dërguar në faqen e synuar.

Adresa: Rruga "Papa Gjon Pali II" nr 3 Tiranë;
Tel./Fax: 04 2221

- Një URL path dhe request body në fushat **path** dhe **body** për kërkesat e rrjetit të llojit **http** ose **http2**. Nëse fushat path dhe/ose body kanë vlera, DDOSIA ndërton dhe adreson kërkesa me request body të konfiguruar në rrugën e URL-së të konfiguruar në faqen e synuar.

```
if self._method == "syn":
    src_ip = os.urandom(4)
    src_port = random.randint(1025, 65535)
    ip_version = 4
    ip_hdr_len = 20
    ip_dsfield = 0
    ip_len = 0
    ip_id = 1
    ip_flags = 0
    ip_ttl = 64
    ip_proto = socket.IPPROTO_TCP
    ip_checksum = 0
    ip_header = struct.pack(
        '!BBHHHBBH4s4s',
        (ip_version << 4) + (ip_hdr_len // 4),
        ip_dsfield,
        ip_len,
        ip_id,
        ip_flags,
        ip_ttl,
        ip_proto,
        ip_checksum,
        src_ip,
        self._dst_ip)
    [...]
```

Figura 24: Implementimi i DDOSIA

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

```
p_http_Request = (http_Request *)runtime_newobject(&RTYPE_http_Request);
[...]
v105 = fmt_Sprintf((unsigned int)"%s%s:%v%s", 9, (unsigned int)&v112, 4, 4, v55, v56, v57, v58, v89, v94);
v106 = (url_URL *)net_url_Parse(v105, 9, v59, 4, 4, v60, v61, v62, v63, v90, v95);
if ( a15 == 4 && *(_DWORD *)target_method == 'TSOP' )
{
  if ( a18 == 6 && *(_DWORD *)a17 == 'irts' && *(_WORD *)(a17 + 4) == 'gn' )
  {
    [...]]
    v71 = (char **)net_http_NewRequestWithContext(
                     (unsigned int)go_itab__context_emptyCtx_context_Context,
                     context_background,
                     (_DWORD)target_method,
                     4,
                     v105,
                     9,
                     (unsigned int)go_itab__bytes_Reader_io_Reader,
                     (_DWORD)p_bytes_Reader,
                     v70,
                     v92,
                     v97,
                     v99);
    [...]
```

Figura 25: Implementimi i DDOSIA

DDOSIA zëvendëson substrings **${number}** të specifikuara në skedarin konfigurues me vlera të rastit që malware krijon kur ndertohet nje kerkese ne rrjet. Në një skedar konfigurimi DDOSIA, nënstringjet **${number}** zakonisht vendosen në **path**. Implementimi në Python i DDOSIA përdor template të përcaktuara në fushën **randoms** në skedarin konfigurues për të krijuar vlera të rastit në formë string-esh të ndryshme.

Një skedar konfigurimi DDOSIA specifikon path URL dhe request bodies që janë të vlefshme në faqet e internetit të synuara. Ky fakt tregon se operatorët e DDOSIA ndërtojnë skedarët konfigurues duke eksploruar fillimisht faqet e internetit të objekteve të tyre të cilat janë në target.

Ka veçori shtesë të DDOSIA përveç atyre të përmendura më lart që një skedar konfigurimi mund të udhëzojë malware të aktivizojë. Për shembull, fusha **use_random_user_agent** udhëzon DDOSIA-n të zgjedhë në mënyrë të rastësishme një agent përdoruesi nga një listë e agjentëve të paracaktuar të përdoruesve kur ndërton një kërkesë HTTP. Po ashtu, fushat **activate_by_schedule**, **started_at** dhe **finished_at** tregojnë se një sample DDOSIA të cilat mund të konfigurohen për të planifikuar dërgimin e kërkesave e rrjetit në intervale të caktuara kohore.

DDOSIA është në zhvillim të vazhdueshëm dhe është nën ndryshime të shpeshta.

Për shembull, implementimet e DDOSIA në Golang, mbështesin llojin e kërkesës të rrjetit http2, ndërsa ato në Python nuk e përdorin këtë mënyrë.

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

```
user_agents = [
    [...]
    "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:77.0) Gecko/20190101 Firefox/77.0",
    "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:77.0) Gecko/20100101 Firefox/77.0",
    "Mozilla/5.0 (X11; Linux ppc64le; rv:75.0) Gecko/20100101 Firefox/75.0",
    "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/75.0",
    "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.10; rv:75.0) Gecko/20100101 Firefox/75.0",
    "Mozilla/5.0 (X11; Linux; rv:74.0) Gecko/20100101 Firefox/74.0",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/73.0",
    "Mozilla/5.0 (X11; OpenBSD i386; rv:72.0) Gecko/20100101 Firefox/72.0",
    [...]
]
```

Figura 26: Agjentët e DDOSIA

Për më tepër, implementimet e DDOSIA në Golang autentikohen tek serverat C2 duke dërguar një kërkesë HTTP POST në rrugën e URL-së /login_new tek serverat dhe ndërrohen nëse autentikimi dështon. Implementimet e DDOSIA në Python që kemi analizuar nuk mbështesin këtë veçori.

```
if ( models_target_type_len == 5
    && *(_DWORD *)models_target_type == 'ptth'
    && *(_BYTE *)(models_target_type + 4) == '2' )
  {
    p_http2_Transport = (http2_Transport *)runtime_newobject
    (&RTYPE_http2_Transport);
    [...]
```

Figura 27: Implementimi i kërkesave http2

DDOSIA dërgon statistika mbi veprimin dhe normën e suksesit të tij - malware numëron totalin dhe numrin e kërkesave rrjetore të suksesshme të dërguara në çdo faqe të synuar. Në kontekstin e kërkesave rrjetore të llojit **http** ose **http2**, një kërkesë konsiderohet e suksesshme nëse faqja e targetizuar kthen kodin HTTP 200 (OK).

```
v48 = ((__int64 (__golang *)(_DWORD,[...] __int64))go_stresser_20_models_Login)(
        (unsigned int)"/login_new",
        10,
        (_DWORD)main_BackendLink,
        [...]
if ( v48 )
{
  v109[0] = &RTYPE_string;
  v109[1] = &off_7E2E80;
  [....]
}
else
{
  [...]
  time_Sleep(0xF8475800, 1, v56, v44, (unsigned int)&off_7E2E70, v57, v58, v59, v60, v88);
  v55 = os_Exit(1, 1, v61, v44, (unsigned int)&off_7E2E70,
  v62, v63, v64, v65, v89);
}
```

```
aAvtorizaIProid db 'Авторизация пройдена успешно
```

Figura 28: DDOSIA autentifikon veten në një server C2

DDOSIA dërgon statistika në serverin C2 në intervale kohore të rregullta - kjo informon operatorët e DDOSIA mbi progresin dhe suksesin e përgjithshëm të fushatës denial-of-service që malware kryen. Kjo është e lidhur me mënyrën se si grupi përdor një program të sponsorizuar nga vullnetarët. Ata shpërndajnë kriptovalutë tek kontribuesit më të mirë të sulmeve DDoS, duke inkurajuar njerëzit të japin më shumë burime teknike për një sulm më të fuqishëm.

Adresa: Rruga “Papa Gjon Pali II” nr 3 Tiranë;
Tel./Fax: 04 2221

Cyber Army of Russia Reborn

Të dhënat tregojnë ekzistencën e një grupi kërcënimi të njohur si *Cyber Army of Russia Reborn*. Ky grup nuk klasifikohet në një lloj specifik, duke bërë që aktivitetet dhe motivimet e tij mund të mos jenë të mirëpërcaktuara ose të njohura publikisht.

Pikat kryesore:

Potenciali për spiunazh kibernetik: Aktorët e kërcënimit me motivime të panjohura mund të përfshihen në spiunazh kibernetik për të mbledhur informacione të ndjeshme për qëllime të ndryshme, si përfitime politike ose ekonomike.

Rreziku i shkeljeve të të dhënave: Aktorët e paidentifikuar të kërcënimit mund të synojnë organizatat për të vjedhur të dhëna të ndjeshme, duke përfshirë informacionin financiar ose të dhënat e klientëve.

Vendosja e malware: Aktorët e kërcënimit mund të përdorin malware për të kompromentuar sistemet, për të ndërprerë operacionet ose për të vjedhur të dhëna. Familjet specifike të malware të lidhura me këtë grup nuk dihen, por ato mund të paraqesin rreziqe të konsiderueshme.

Potenciali për bashkëpunim: Aktorët e kërcënimit mund të bashkëpunojnë me grupe ose individë të tjerë për të rritur aftësitë e tyre dhe për të rritur ndikimin e sulmeve të tyre.

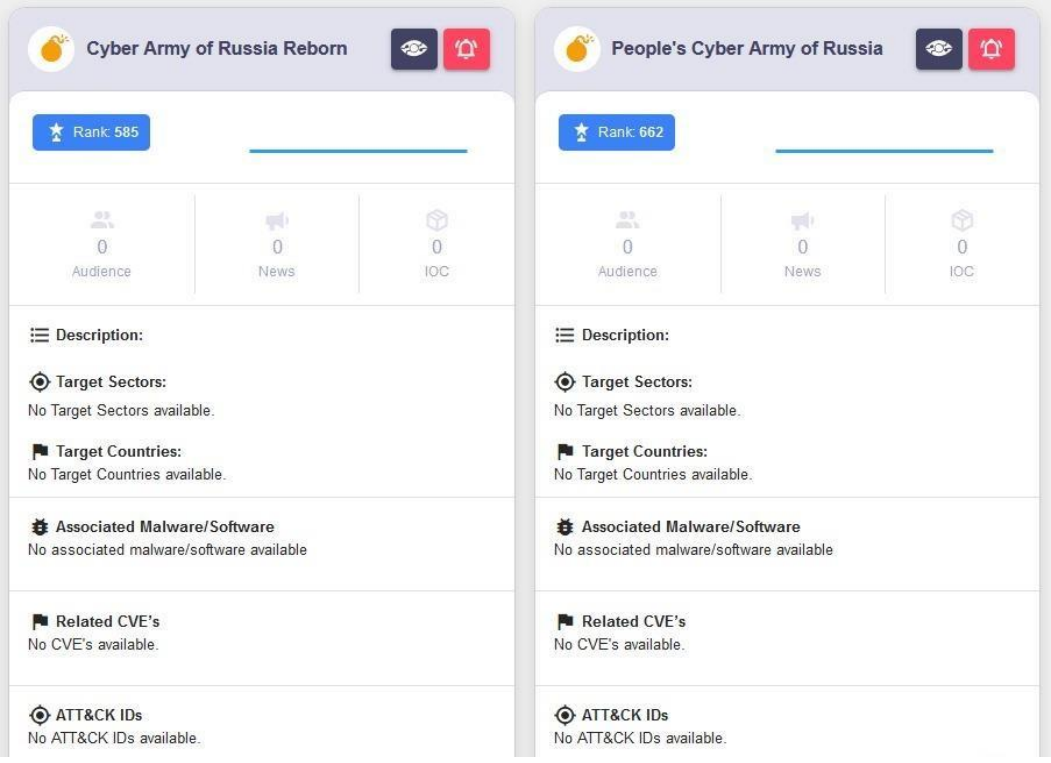

Figura 29: Renditja e Grupit Cyber Army of Russia

TLP:GREEN

Rekomandime

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

AKSK rekomandon organizatat 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.

TLP:GREEN

- Monitorim i vazhdueshëm i logeve në sistemet tuaja kritike.

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

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

TLP:GREEN