REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Raport mbi grupin Dark Storm Team

Versioni: 1.0

Datë: 24/04/2025

Tabela e përmbajtjes:

Tabela e figurave

1. Hyrje

Dark Storm Team është një ndër grupet që ka tërhequr vëmendjen më të madhe në arenën ndërkombëtare gjatë kohëve të fundit. Ky grup ka kombinuar teknikat tradicionale të haktivizmit me taktikat dhe strategjitë e luftës hibride. Kjo ka rezultuar në një seri incidentesh që kanë tronditur platforma globale, institucione shtetërore, media dhe sisteme kritike infrastrukturore.

Dark Storm Team nuk është thjesht një grup hakerash që veprojnë për qëllime personale. Përkundrazi, ky grup përfaqëson një kombinim kompleks të motivimeve gjeopolitike, ideologjike dhe financiare. Që nga krijimi i tij në shtator të vitit 2023, grupi është shfaqur në skenë si një strukturë e organizuar mirë, me një agjendë të qartë politike, që mbështet çështjet pro-palestineze dhe mban një qëndrim pro-rus. Kjo e vendos Dark Storm Team në një pozitë unike në krahasim me shumë grupe të tjera kibernetike që operojnë vetëm për motive financiare.

Sulmet e ndërmarra nga ky grup janë karakterizuar jo vetëm nga ndikimi i madh në shërbime dhe në reputacionin e objektivave të zgjedhur, por edhe nga mënyra e sofistikuar e realizimit. Dark Storm Team përdor një shumëllojshmëri të teknikave të avancuara, që nga DDoS masiv, deri te phishing, social engineering dhe shfrytëzimi i vulnerabiliteteve të panjohura (zero-day). Shqetësues është edhe përdorimi i *botnet*-eve, që e bëjnë të vështirë gjurmimin dhe ndalimin e tyre në kohë reale. Të gjithë këto elementë tregojnë për një nivel të lartë ekspertize teknike dhe një strategji të mirëmenduar.

Ky grup ka marrë përgjegjësinë për sulmet ndaj platformave si Twitter (X.com), Zoom, Spotify, si dhe institucioneve shtetërore në Kosovë, Shqipëri, Ukrainë, Francë, Izrael, Finlandë, Belgjikë dhe vende të tjera europiane. Madje, grupi ka shfaqur edhe interes për sektorë specifikë si transporti ajror, institucionet financiare dhe rrjetet e informacionit publik. Me një aktivitet që është rritur ndjeshëm në muajt e fundit, Dark Storm Team është kthyer në një rrezik të vërtetë për sigurinë kibernetike, jo vetëm në rajonin tonë, por edhe në nivel global.

2. Origjina dhe Strukturimi i Grupit

Grupi ***Dark Storm Team*** u formua në një kontekst të veçantë gjeopolitik dhe teknologjik, në shtator të vitit 2023, në një periudhë kur tensionet globale, veçanërisht në Lindjen e Mesme dhe Evropën Lindore, ishin në rritje. Ky grup nuk lindi si një organizatë klasike kriminale apo një rrjet i vogël hakerësh me qëllime të kufizuara. Përkundrazi, ai përfaqëson një shembull të ri të evolucionit të haktivizmit, ku përzihen ideologjia politike, instrumentet e luftës hibride, dhe interesat financiare.

Që nga fillimi, Dark Storm Team u identifikua si një strukturë e decentralizuar, ku mungesa e një udhëheqjeje të qartë hierarkike nuk është tregues i dobësisë, por një avantazh taktik. Në vend që të mbështeten në një qendër komanduese të vetme, anëtarët operojnë në mënyrë të shpërndarë, duke përdorur kanale të sigurta komunikimi dhe duke marrë vendime në mënyrë autonome. Ky model organizativ e bën të vështirë gjurmimin.

Anëtarët e Dark Storm Team besohet se vijnë nga një sërë vendesh, përfshirë Lindjen e Mesme, vende të Evropës Lindore (si Rusia, Moldavia) dhe vende të Azisë Qendrore. Profilizimi i tyre tregon për një përzierje të ekspertizës teknike me njohuri të thella të gjuhëve të programimit, teknologjive të rrjetit, sigurisë kibernetike dhe inxhinierisë sociale. Disa raporte kanë shprehur se pjesë të këtij grupi janë të përbëra nga ish-inxhinierë të IT-së, studentë të universiteteve teknologjike dhe individë të lidhur me organizata politike ose lëvizje ideologjike.

Nga këndvështrimi teknologjik, Dark Storm Team është i pajisur me një arsenal të gjerë mjetesh dhe metodash për të ruajtur anonimitetin. Përdorimi i Dark Web, kanaleve të enkriptuara si Telegram, VPN, proxy serverëve ndërkombëtarë dhe botnet-eve janë vetëm disa nga teknikat që e bëjnë grupin pothuajse të paprekshëm. Botnet-et e tyre janë shpesh të përbërë nga pajisje të infektuara përmes *malware*-ve dhe *phishing*, të cilët përdoren për sulme DDoS.

Një aspekt tjetër i rëndësishëm i këtij grupi është dhe organizimi. Anëtarët nuk janë të gjithë njësoj, disa janë përgjegjës për planifikimin strategjik dhe përzgjedhjen e objektivave, të tjerë për zhvillimin e malware-ve specifikë, një pjesë merren me analizimin e dobësive (vulnerability research), dhe një pjesë tjetër fokusohet te propagandimi në rrjet dhe menaxhimi i komuniteteve në Telegram apo forume të errëta. Ky lloj funksionalizimi e rrit shumë efikasitetin operacional të grupit.

Kjo strukturë e organizuar i ka lejuar Dark Storm Team të bashkëpunojë në mënyrë fleksibël me aktorë të tjerë, përfshirë grupe të mirënjohura si KillNet, Anonymous Sudan, ose aktorë që dyshohet të jenë të lidhur me agjenci shtetërore të vendeve si Rusia. Në disa raste janë evidentuar sulme të sinkronizuara me grupe të tjera, që përkonin me zhvillime politike ndërkombëtare, gjë që tregon një koordinim të mundshëm në një nivel më të lartë strategjik.

Simbolet, logot, videot me muzikë dramatike dhe montazhe të sulmeve të suksesshme krijojnë një mitologji për grupin dhe tërheqin rekrutë të rinj që ndajnë të njëjtat bindje ideologjike apo që kërkojnë hakmarrje kibernetike ndaj një bote të cilën e shohin të padrejtë.

Së fundmi, është me rëndësi të theksohet edhe fakti që ky grup nuk është statik. Ai evoluon dhe përshtatet shpejt. Nëse një taktikë bëhet e paefektshme, grupi është i aftë të rikualifikojë anëtarët dhe të zhvillojë metoda të reja. Ky dinamizëm e bën Dark Storm Team një nga grupet më elastike dhe të rrezikshme në skenën globale të kërcënimeve kibernetike.

3. Sulmet

Gjatë veprimtarisë së tyre, Dark Storm Team ka marrë përgjegjësinë për disa nga sulmet më të spikatura dhe më të sofistikuara të viteve të fundit. Një nga goditjet më të fuqishme u regjistrua në mars 2025, kur grupi kreu një sulm masiv DDoS ndaj platformës sociale X (ish-Twitter), duke shkaktuar ndërprerje globale për disa orë dhe duke ekspozuar dobësitë e një prej rrjeteve më të përdorura botërore. Po ashtu, platforma të tjera me përdorim të gjerë si Zoom dhe Spotify u prekën nga sulmet e koordinuara të Dark Storm Team. Ndërkohë, një tjetër sulm i përmasave të mëdha u zhvillua në prill 2025 ndaj institucioneve kryesore të Republikës së Kosovës, ku ndër objektivat ishin Kryeministria, Ministria e Mbrojtjes, si dhe një sërë mediash kombëtare. Ky sulm masiv

synonte jo vetëm ndërprerjen e shërbimeve, por edhe dërgimin e një mesazhi politik në kontekstin e qëndrimeve të Kosovës ndaj luftës në Ukrainë dhe mbështetjes për vendet perëndimore.

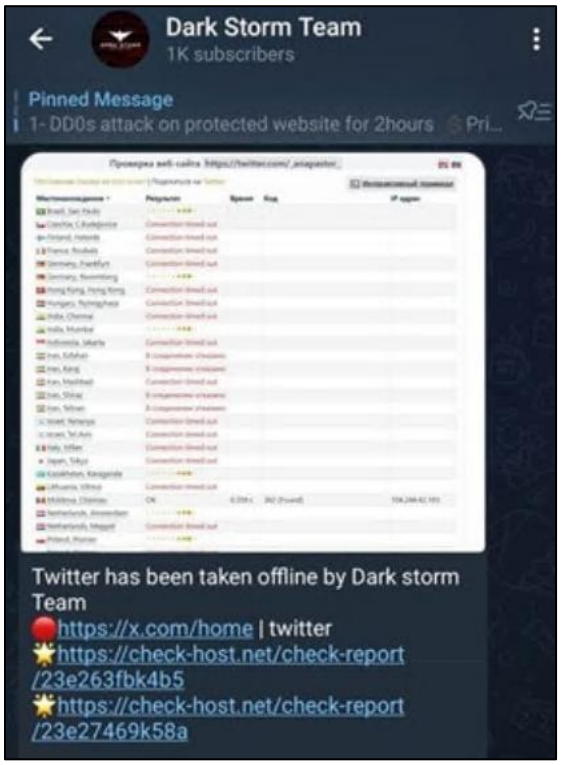

Figura 1: Sulmi ndaj platformës X

Figura 2: Sulmi ndaj platformës Zoom

Figura 3: Sulmet në Kosovë

Figura 4: Sulmet në Kosovë

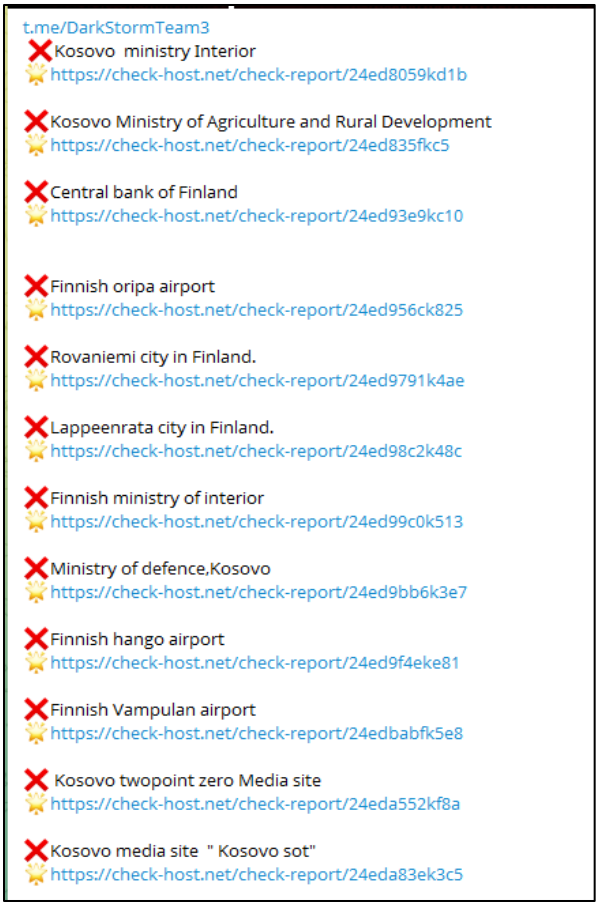

Figura 5: Sulmet në Kosovë

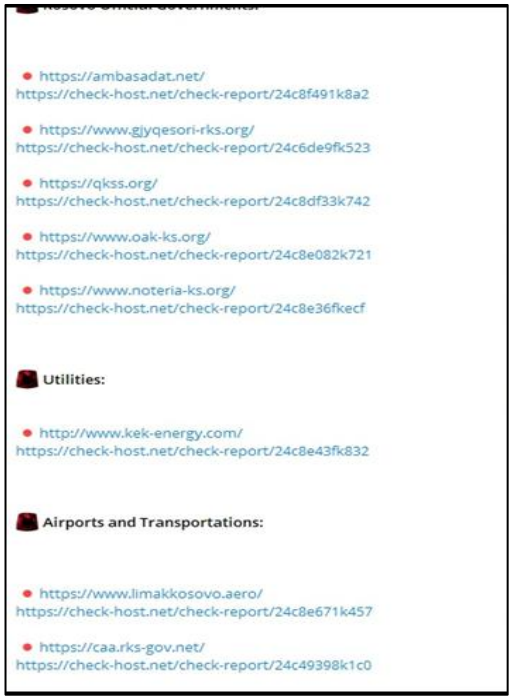

Figura 6: Sulmet në Kosovë

Institucionet e sulmuara në Kosovë ishin:

- Kryeministria
- Parlamenti
- Ministria e Mbrojtjes
- Ministria e Brendshme
- Ministria e Arsimit, Shkencës dhe Teknologjisë
- Ministria e Shëndetësisë
- Ministria e Financave
- Ministria e Agrokulturës dhe Zhvillimit Rural
- Faqja e Ambasadave
- Këshilli Gjyqësor i Kosovës
- Oda e Noterëve
- Korporata Energjetike e Kosovës
- Qendra Kosovare për studime të Sigurisë
- Aeroporti Ndërkombëtar i Prishtinës
- Autoriteti i Aviacionit Civil

- Banka BPB
- Lëvizja Vetëvendosja
- Media “Kosova Press”
- Media “Kosova Sot”
- Media “Zwri Info”
- Media “Koha”
- Media “Twopointzero”
- Portal pune në Kosovë
- Portali “ofertasuksesi”
- Shkolla Amerikane
- International Learning Group

4. Sulmet në Shqipëri

Në prill të vitit 2025, grupi Dark Storm Team publikoi një deklaratë në Telegram ku pretendonte se kishte sulmuar disa institucione të Republikës së Shqipërisë. Edhe pse pas një verifikimi të shpejtë nuk u evidentuan dëme të drejtpërdrejta në faqet apo sistemet e përmendura, deklarata e grupit mund të konsiderohet si një kërcënim serioz për sigurinë. Ky mund të jetë një mesazh paralajmërues për angazhimin e Shqipërisë në çështjet ndërkombëtare dhe pozicionimin e saj të hapur pro-perëndimor, veçanërisht në kontekstin e mbështetjes së Ukrainës dhe pjesëmarrjes në strukturat e NATO-s.

Figura 7: Sulmet në Shqipëri

5. Metodat e Sulmit

Dark Storm Team përdor një spektër të gjerë metodash dhe teknikash për të realizuar sulmet e tyre kibernetike, duke u përshtatur me natyrën dhe nivelin e mbrojtjes së objektivit. Më poshtë janë përshkruar metodat kryesore që grupi ka përdorur në mënyrë të dokumentuar ose që janë raportuar nga burime të inteligjencës kibernetike.

5.1 Sulmet DDoS (Distributed Denial of Service)

Një nga metodat më të përdorura nga Dark Storm Team janë sulmet DDoS, të cilat konsistojnë në dërgimin masiv të trafikut ndaj një serveri apo infrastrukture për ta mbingarkuar dhe për ta nxjerrë jashtë funksionit. Grupi përdor botnet të përbërë nga mijëra pajisje të kompromet uara që dirigjohen në mënyrë të sinkronizuar për të realizuar këto sulme. Këto operacione shpesh shënjestrojnë faqe qeveritare, media dhe rrjete sociale.

5.2 Phishing dhe Social Engineering

Një tjetër taktikë e zakonshme është phishing, dërgimi i mesazheve mashtruese me qëllim që përdoruesi të japë informacione sensitive, si kredenciale apo të dhëna personale. Dark Storm Team përdor email dhe faqe të rreme që imitojnë portale zyrtare, duke kombinuar teknika të inxhinierisë sociale për të bindur viktimat të veprojnë.

5.3 Shfrytëzim të dobësive Zero-Day

Grupi është i njohur për përdorimin e dobësive të paidentifikuara më parë (zero-day vulnerabilities). Në shumë raste, Dark Storm Team ka arritur të shfrytëzojë këto dobësi për të marrë akses në sistemet e organizatave, duke instaluar *backdoor* ose duke kompromet uar serverë kritikë. Kjo kërkon ekspertizë të lartë teknike dhe burime që zakonisht lidhen me aktorë të sponsorizuar nga shtetet.

5.4 Ransomware dhe Ekfiltrim i të Dhënave

Ndërsa DDoS përdoret për ndërprerje të menjëhershme, sulmet *ransomware* synojnë përfitimin financiar nëpërmjet enkriptimit të të dhënave dhe kërkesës për shpërblim. Dark Storm Team ka përdorur ransomware në disa raste për të mbyllur sistemet e viktimave dhe për të kërcënuar me publikimin e të dhënave të ndjeshme nëse nuk paguhet një shumë e caktuar kriptomonedhash. Në disa raste, ata i kanë përdorur këto të dhëna edhe për propagandë.

5.5 Shfrytëzimi i Infrastrukturës së Shpërndarë (Botnet Infrastructure)

Përveç sulmeve të drejtpërdrejta, Dark Storm Team përdor rrjete botnet që përfshijnë mijëra pajisje të infektuara. Këto pajisje i përdorin jo vetëm për DDoS, por edhe për fshirjen e gjurmëve, *tunneling* dhe ruajtje të të dhënave të kompromet uara. Botnetet e tyre janë dinamike dhe është e vështirë të zbulohen.

5.6 Desinformimi dhe Falsifikimi i Informacionit

Një taktikë shumë efektive, është përhapja e informacionit të rremë përmes Telegram. Dark Storm Team ka shpërndarë deklarata të rreme për të shkaktuar panik, për të dezinformuar publikun dhe për të ndikuar në narrativën e mediave. Kjo është një formë e luftës psikologjike që shoqëron shpesh sulmet teknike.

5.7 Përdorimi i AI dhe Automatizimit

Ka evidenca të fundit që sugjerojnë se grupi ka filluar të eksperimentojë me përdorimin e inteligjencës artificiale për të përmirësuar phishing, për të automatizuar përzgjedhjen e objektivave dhe për të analizuar mbrojtjet e rrjeteve. Automatizimi i analizës së dobësive dhe gjenerimi i *malware* të reja përmes AI përbën një kërcënim serioz për sistemet e mbrojtjes.

6. Ideologjia dhe Propaganda

Ideologjia dhe propaganda e Dark Storm Team përbëjnë një komponent thelbësor të funksionimit të grupit, duke shërbyer jo vetëm si motivim për anëtarët ekzistues, por edhe si mjet rekrutimi dhe legjitimimi për aktivitetet e tyre të paligjshme.

Një nga qëllimet kryesore të propagandës së Dark Storm Team është të përçojë idenë se ata janë një zë për të pafuqishmit dhe një armë kundër strukturave të padrejta të fuqisë globale. Për këtë qëllim, grupi i paraqet sulmet e veta si akte të drejtësisë shoqërore dhe jo si akte kriminale. Kjo qasje ka rezultuar efektive në tërheqjen e individëve të rinj që ndihen të zhgënjyer nga sistemet ekzistuese politike.

Telegrami është platforma kryesore për përhapjen e mesazheve të tyre. Ata krijojnë kanale dhe grupe ku postojnë jo vetëm rezultate të sulmeve, por edhe lajme të manipuluara, analiza politike dhe mesazhe që promovojnë aksione të mëtejshme.

Së fundi, propaganda e grupit nuk është vetëm ideologjike por edhe taktike. Ajo përdoret për të frikësuar objektivat e ardhshëm dhe për të çorientuar opinionin publik. Në këtë kuptim, propaganda është një armë psikologjike po aq e fuqishme sa edhe mjetet teknike që grupi përdor në sulmet e tij.

7. Analizimi dhe vlerësimi i rrezikut kibernetik kombëtar

Aktivitetet e rritura të grupit haker Dark Storm Team paraqesin një kërcënim serioz dhe të qëndrueshëm për sigurinë kibernetike të Shqipërisë dhe infrastrukturave të saj kritike. Si një shtet pro-perëndimor dhe anëtar i NATO-s, Shqipëria mund të konsiderohet si objektiv i mundshëm për sulme kibernetike me motive politike, të cilat synojnë destabilizimin e institucioneve shtetërore dhe ndërprerjen e shërbimeve publike.

Megjithëse ende nuk janë raportuar dëme të drejtpërdrejta nga kërcënimet e Dark Storm Team ndaj institucioneve shqiptare, përfshirja e Shqipërisë në fjalorin e këtij grupi është një shenjë alarmi për dobësitë e mundshme në infrastrukturat kritike të vendit. Duke marrë parasysh aftësitë e grupit për të sulmuar platforma globale dhe sisteme të avancuara teknologjike, rreziku për sektorë kyç si energjia, transporti, financat dhe infrastruktura publike dixhitale është real dhe kërkon masa të menjëhershme.

Për këtë arsye, është e nevojshme një angazhim i koordinuar dhe afatgjatë për të forcuar sigurinë kibernetike të Shqipërisë, përmes investimeve në teknologji të avancuara, trajnimeve të specializuara dhe bashkëpunimit ndërkombëtar në fushën e sigurisë kibernetike.

8. Përfundim dhe Rekomandime

Analiza e detajuar e grupit Dark Storm Team tregon qartë se kemi të bëjmë me një aktor të sofistikuar, që operon me strategji të mirëpërcaktuara dhe që përfaqëson një kërcënim real për sigurinë kibernetike në nivel global. Përdorimi i teknologjive të përparuara, përfshirja e motivimeve ideologjike dhe kapaciteti për të koordinuar sulme të gjera dhe të sinkronizuara e bëjnë këtë grup një objektiv kritik për strukturat mbrojtëse të çdo vendi.

Përfundime Kryesore:

1. **Dark Storm Team është një grup hibrid:** Ai përzien motivimin ideologjik me interesin financiar.
2. **Veprimtaria e tyre ka ndikim ndërkombëtar:** Grupet e synuara përfshijnë jo vetëm shtete të konfliktit si Izraeli apo Ukraina, por edhe vende të NATO-s dhe të BE-së.
3. **Kapacitetet teknike janë në rritje:** Grupi është duke përdorur teknika gjithnjë e më të sofistikuara, përfshirë AI dhe dobësi zero-day, gjë që e bën të vështirë parandalimin dhe mbrojtjen.
4. **Përdorimi i mediave sociale dhe kanaleve si Telegram është pjesë e strategjisë së tyre:** Kjo i mundëson jo vetëm përhapjen e propagandës por edhe koordinimin e sulmeve.

Rekomandime Strategjike:

Forcimi i inteligjencës kibernetike (Cyber Threat Intelligence): Shtetet dhe organizatat duhet të investojnë në njësi të specializuara që monitorojnë aktivitetin e këtyre grupeve, me theks të veçantë në OSINT dhe infiltrimin e kanaleve të komunikimit të tyre.

Rritja e bashkëpunimit ndërkombëtar: Dark Storm Team nuk njeh kufij kombëtarë. Prandaj, bashkëpunimi ndërmjet agjencive të sigurisë së vendeve të ndryshme, ndarja e informacionit dhe krijimi i protokolleve të përbashkëta janë thelbësore.

Fuqizimi i infrastrukturës kritike: Aeroportet, rrjetet energjetike, sistemet financiare dhe institucionet shtetërore duhet të auditojnë dhe përmirësojnë mbrojtjen e tyre kibernetike.

Trajnimi i vazhdueshëm i stafit dhe edukimi i publikut: Për të zvogëluar suksesin e sulmeve të bazuara në inxhinieri sociale si phishing, është thelbësor trajnimi i punonjësve dhe fushata informuese për qytetarët.

Monitorimi dhe rregullimi i rrjeteve sociale dhe platformave të komunikimit: Telegram, forume të errëta dhe rrjete të tjera duhen monitoruar vazhdimisht për përmbajtje që lidhet me planifikimin e sulmeve, rekrutimin e anëtarëve të rinj apo shpërndarjen e propagandës.

Promovimi i bashkëpunimit me sektorin privat: Shumë prej infrastrukturave që sulmohen janë në pronësi private. Bashkëpunimi me kompanitë e teknologjisë, ofruesit e internetit dhe platformat e mëdha është thelbësor për një mbrojtje efektive.

Ndërtimi i qëndrueshmërisë nëpërmjet planeve të reagimit ndaj incidenteve: Çdo organizatë duhet të ketë një plan të detajuar për reagimin ndaj incidenteve dhe të realizojë simulime të rregullta për të testuar efektivitetin e këtij plani.