Sulmi kibernetik i 15 korrikut 2022 në Shqipëri

Një analizë e detajuar, sipas gjithë etapave që nga 15-16 korriku 2022

Microsoft DART (Detection and Response Team) dhe ekipi investigues i krimit kibernetik të FBI (Cyber Action Team), pas një investigimi, të detajuar, prej më shumë se 2 muajsh, që nga dita e sulmit kibernetik të 15-16 Korrikut 2022, që goditi shumë prej sistemeve qeveritare, të hostuara pranë AKSHI-t, me qëllim fshirjen e tyre të plotë, kanë hartuar dhe dorëzuar raportet e tyre përfundimtare.

Të dy ekipet e investigimit, kanë bashkëpunuar ngushtësisht me ekipet teknike të AKSHI-t, duke qenë të pranishëm edhe fizikisht pranë ambienteve të AKSHI-t për kryerjen e të gjitha investigimeve të tyre (Microsoft DART menjëherë, 1 javë pas sulmit dhe FBI CAT 2 javë pas sulmit). Ndërsa ka pasur në vijueshmëri të gjithë procesit një bashkëpunim në distancë edhe me CISA. Ka qenë tejet i domosdoshëm ky bashkëpunim dhe përfshirje aktive, e çdo dite, e ekipeve të AKSHI-t, pa të cilët ky investigim nuk do të kishte rezultuar dot kaq i plotë.

Bazuar në këto investigime, është arritur në konkluzionin se: data 21 Maj 2021, është data e parë e infiltrimit të aktorëve keqbërës, duke përdorur vulnerabilite të sistemit administrata.al. Ky sistem i prokuruar me fonde të IPA-s, nuk është implementuar, menaxhuar apo ndjekur nga AKSHI, por vetëm është hostuar fizikisht pranë Datacenter-it Qeveritar.

Për sa i përket sulmeve të fundit të 9 shtatorit 2022, ndaj sistemeve dhe infrastrukturave të Drejtorisë së Përgjithshme të Policisë së Shtetit, duhet theksuar se objektiv ka qenë një infrastrukturë krejt e veçantë (rrjet totalisht i pavarur, Active Directory e pavarur, Exchange – sistemi i email-it) i palidhur me infrastrukturat AKSHI-t.

Rrjedha e ngjarjeve të sulmit të 15 korrikut dhe kohëzgjatja që paraqitet në vijim nuk lidhen në asnjë formë me sulmin e 9 shtatorit ndaj sistemeve dhe infrastrukturave të Drejtorisë së Përgjithshme të Policisë së Shtetit, sikurse sqaruar më lart. Bëhet fjalë për dy sulme të ndryshme, me zanafilla të ndryshme, ndaj dy infrastrukturave të palidhura me njëra-tjetrën.

Në lidhje me kohëzgjatjen e një prezence, prej kohësh në mjedisin e brendshëm kibernetik të AKSHI-t duam të sqarojmë se:

Kohëzgjatja mesatare e identifikimit të penetrimit në sisteme për aktorët kërcënues është 287 ditë, sipas statistikës së firmës prestigjoze teknologjike IBM. Sulme të tilla, të cilat përdorin teknika kaq të sofistikuara dhe të dizenjuara për targetin specifik, kanë një kohëzgjatje të tillë pikërisht për të bërë që veprimet dhe lëvizjet e këtyre aktorëve keqdashës në mjediset e penetruara të duken sa më legjitime dhe normale. Në momentin që këta aktorë vendosin të fillojnë lëvizjet për të konkretizuar sulmin atëherë ata rezultojnë të dukshëm.

Më poshtë po paraqesim shtrirjen në kohë, si kanë ndodhur ngjarjet dhe cilat kanë qenë veprimet e menjëhershme, të ndërmarra nga AKSHI:

- **Kompromentimi i përdoruesit**

Platformat e sigurisë u sinjalizua për kompromentim të një prej përdoruesve me privilegje të veçanta. Menjëherë u izolua e u bë "disable" përdoruesi dhe ky incident iu raportua kontaktit të Microsoft-it për AKSHI-n.

Në pritje të rekomandimeve nga pika e kontaktit, ekipi i sigurisë së AKSHI-t investigoi mbi kompromentimin e kryer. Të gjithë loget dhe evidencat të cilat ishin pjesë e kompromentimit iu raportuan pikës së kontaktit.

AKSHI, bazuar tek incidenti i ndodhur kërkoi eskalimin e situatës pas aktivitetit keqdashës.

- **Incidenti u eskalua, duke krijuar "Security Case" në portalin e incidenteve kibernetike të Microsoft.**

"Security Case" si argument evidentoi:

- Kompromentimin e përdoruesit me privilegje të veçanta
- Webshells të detektuar në serverët Exchange.

Ekipi i sigurisë së AKSHI-t pas kontaktit me inxhinieret e Microsoft për "Security Case", duke zbatuar rekomandimet e tyre përgatiti loget dhe ia dërgoi për hetim ekipit të kundërpërgjigjes, për incidente kibernetike (CERT) të Microsoft.

- **Më 15/07/2022**

Në orën 13:00 u identifikua nga platformat e sigurisë fillimi i shpërndarjes së një sulmi Ransomware në rrjet, i cili preku një pjesë të përdoruesve fundore në institucione. Menjëherë pas identifikimit të këtij sulmi nisën bllokimet, në mënyrë që të mos përhapej me tutje dhe u hap gjithashtu një çështje me ekspertët e Microsoft në nivelin "Crisis Case" (niveli më i lartë i eskalimit të incidenteve kibernetike).

- **Më 15/07/2022 - Aktivizim i opsioneve ekstra të sigurisë, pas sulmi 23:30**

Pas komunikimit të vazhdueshëm nga ekipi i sigurisë, për sulmin e kryer me inxhinierët e ekipit të kundërpërgjigjes për incidentet kibernetike, u rekomandua nga ata aktivizimi i opsionit ekstra në raste sulmesh kibernetike.

- **16/07/2022 - Wiper Attack**

Aktivizimi i opsionit ekstra të sigurisë në raste sulmesh kibernetike detektoi aktorët kërcënues, të cilët kishin penetruar në sistem. Pas evidentimit nga ana e tyre dhe bllokimit të përhapjes së aktiviteteve keqdashëse, ata ndryshuan metodologjinë e sulmit duke tentuar përmbushjen e objektivit final: fshirjen e të gjithë sistemeve digjitale. Menjëherë pasi u detektua procesi i fshirjes, nga AKSHI u mor masa drastike e izolimit të të gjitha sistemeve, me qëllim parandalimin e zgjerimit te aktivitetit.

- **Angazhim i ekipeve të Microsoft-it: DART, CRSP, MAT**

DART Team u angazhua për hetimin e sulmit kibernetik dhe higjienizimin nga aktorët kërcënues. Për ringritjen e sistemeve në mënyrë të sigurt u angazhua ekipi i Compromise Recover Security Team (CRSP) i Microsoft. Ndërkohë "Modernisation and Transformation Team" (MAT) është angazhuar aktualisht për transformimin e strukturës aktuale.

Në gjithë këto kohë ka pasur një keqinterpretim e keqinformim se AKSHI-t i kanë munguar elementet e sigurisë qe pasqyrohen ne këto rekomandime. Por fakti është se këto rekomandime janë standard i CISA-s dhe FBI-së, i përdorur në raporte për të gjitha organizatat. Siç qartësisht cilësohet ne raportin e mëposhtëm të AKSHI-t , këto janë rekomandime të CISA-s dhe FBI-së për të gjitha organizatat për të zbatuar "best practices" https://www.cisa.gov/uscert/ncas/alerts/aa22-264a për të ulur riskun e kompromentimit.

Në një link tjetër https://www.cisa.gov/uscert/ncas/alerts/aa22-257a për infrastrukturat amerikane që janë goditur nga IRGDC, jepen rekomandime të ngjashme, sikurse paraqiten edhe në raportin e FBI-së për Shqipërinë, lidhur me sulmet e kryera nga aktorët iranianë ndaj infrastrukturave amerikane (Policia, Aerospace dhe kompanitë e transportit).

Raporti i Microsoft-it faktoi **sponsorizimin e qeverisë iraniane** ndaj këtij sulmi kibernetik, të strukturuar dhe koordinuar nga MOIS (Ministria e Inteligjencës Iraniane) dhe Garda Revolucionare Iraniane. Buxheti i kësaj të fundit është sa gjysma e GDP-së së Shqipërisë (7 miliardë EUR, nga 14.4 miliardë EUR që është GDP-ja e Shqipërisë për vitin 2021).

Raporti tregoi qartë se pavarësisht përpjekjeve dhe sofistikimit të sulmit, qëllimi i keqdashësve për fshirjen e gjithë sistemeve qeveritare dhe të dhënave të tyre nuk është përmbushur. Arritën të preken nga procesi i fshirjes **vetëm 10% e sistemeve të cilat janë rikthyer tërësisht falë politikave të backup-it dhe rikuperimit nga fatkeqësia, brenda javës së parë.** Dokumenti saktësoi se pas analizave të kryera mbi metodologjinë e përdorur, pavarësisht mekanizmave të ndryshme, objektiv i sulmeve të të njëjtëve aktorë kanë qenë edhe Izraeli, Jordania, Kuvajti, Arabia Saudite dhe Turqia.

Ruajtja e të dhënave dhe kthimi në normalitet, brenda një afati rekord, u bë falë reagimit të shpejtë të sistemeve mbrojtëse si dhe bashkëpunimit të ngushtë të ekipit të AKSHI-t me Microsoft-in, CRSP (Compromise Recovery Security Practice) dhe Modernization and Transformation Team. Partnerët ndërkombëtarë na kanë mundësuar mbështetje dhe investigim të plotë, rezultatet e të cilave, janë tashmë të hartuara në raporte.

Duhet theksuar se edhe për sa i përket sulmeve të fundit të 9 Shtatorit 2022, ndaj sistemeve dhe infrastrukturave të Drejtorisë së Përgjithshme të Policisë së Shtetit, raporti evidenton se objektiv ka qenë një infrastrukturë krejt e veçantë (rrjet totalisht i pavarur, Active Directory e pavarur, Exchange – sistemi i email-it) i palidhur me infrastrukturat AKSHI-t.

Sulmet kibernetike të kryera drejt 2 infrastukturave të vecanta, pronë të qeverise shqiptare, të përbashkët kanë vetëm metodologjinë e tij dhe atribuimin e aktorëve kërcënues. Sulmi i datës 15 korrik me atë të 9 shtatorit janë sulme të ndryshme, vektorët e shfrytëzuar dhe kohëzgjatja e tyre janë po ashtu të ndryshëm.