AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Italia paralajmëron organizatat që të përgatiten për sulmet e ardhshme DDoS

Përmbajtja

Mashtrimi përmes mobile e-commerce

Niveli i cenueshmërisë: Serioz (kritik)

Ekipi italian i reagimit ndaj incidenteve të sigurisë kompjuterike (CSIRT) ka ngritur një alarm urgjent për të rritur ndërgjegjësimin për rrezikun e lartë të sulmeve kibernetike kundër subjekteve kombëtare.

Lloji i sulmit kibernetik të cilit i referohet organizata italiane është DDoS (distributed denial-of-service), i cili mund të mos jetë katastrofik, por megjithatë mund të shkaktojë dëme, financiare ose të tjera, për shkak të ndërprerjeve të shërbimit.

"Vazhdojnë të ketë shenja dhe kërcënime për sulme të mundshme të pashmangshme kundër subjekteve publike kombëtare, subjekteve private që ofrojnë shërbime publike ose subjekteve private imazhi i të cilëve identifikohet me shtetin e Italisë," shpjegon alarmi publik[1]. Sinjalet janë postime nga kanali Telegram i grupit Killnet, të cilat nxisin sulme 'masive dhe të paprecedentë' kundrejt Italisë.

Killnet është një grup haktivist pro-rus që sulmoi Italinë dy javë më parë[2], duke përdorur një metodë të vjetër, por ende efektive DDoS të njohur si 'Slow HTTP'. Ky sulm shoqërohet nga kundërmasa të natyrës mbrojtëse, të propozuara nga CSIRT. Gjithashtu përfshihen këshilla të ndryshme mbi praktikat e mira të sigurisë.

Operacioni Panopticon

Operacioni Panopticon u njoftua nga Killnet duke u bërë thirrje rreth 3000 ekspertëve kibernetikë për t'u ofruar vullnetarisht brenda 72 orëve.

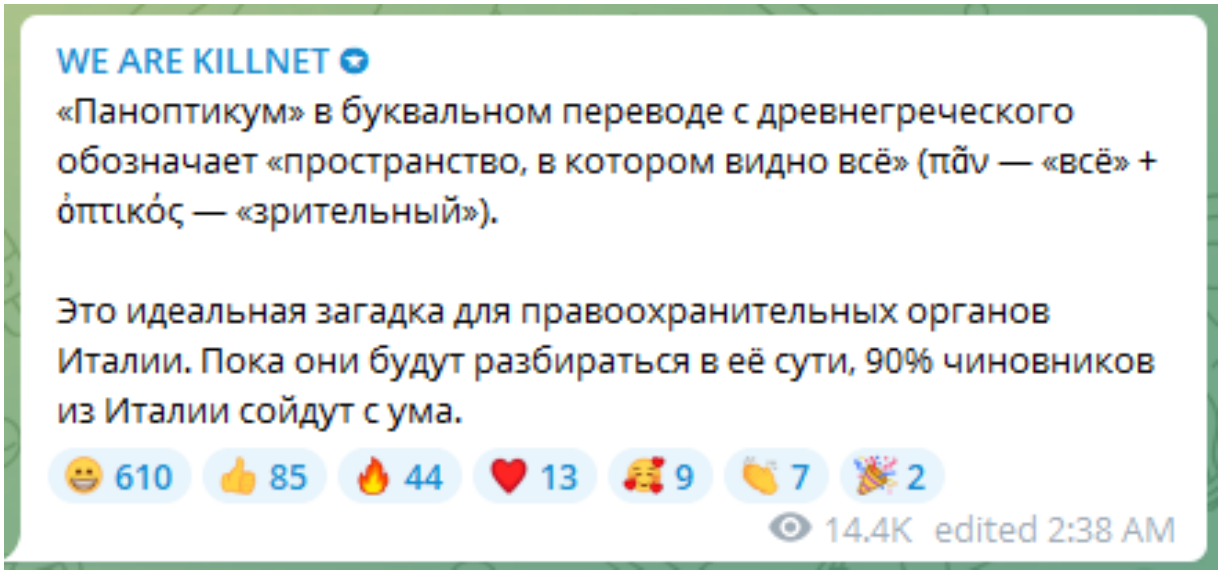
[1] https://www.csirt.gov.it/contenuti/rilevato-potenziale-rischio-di-attacco-informatico-ai-danni-di-enti-ed-organizzazioni-nazionali-al01-220529-csirt-ita

[2] https://www.bleepingcomputer.com/news/security/italian-cert-hacktivists-hit-govt-sites-in-slow-http-ddos-attacks/

Njoftimi i operacionit në Telegram

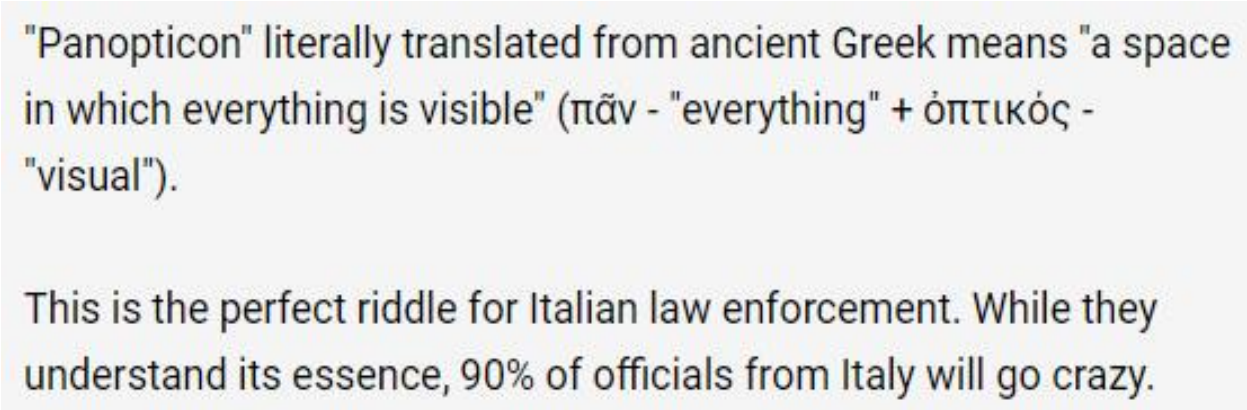
Vullnetarët të cilët u regjistruan plotësuan të dhënat për sistemin, origjinën, moshën dhe llogarinë e tyre në Telegram dhe ofruan mjetet e nevojshme për të nisur sulmet ndaj burimeve. Killnet planifikon të përdorë DDoS për të detyruar administratorët e sistemeve të merren me ndërprerjet e shërbimit në vend që të korrigjojnë sulmet aktive kibernetike.

Killnet dha një shpjegim etimologjik të fjalës Panopticon, duke dhënë sugjerime për rrjedhje të dhënash dhe duke paralajmëruar se 90% e zyrtarëve të vendit ‘do të çmenden’.



Një enigmë për autoritetet italiane

Teksti i mësipërm u përkthye si më poshtë:



Përplasje midis hakerave

Killnet që synon organizatat italiane është rezultat i grupit të shënjestruar kohët e fundit të subjekteve në disa vende, mes tyre edhe Italia, për mbështetjen e rezistencës së Ukrainës kundër Rusisë.

Kjo shkaktoi aksionin e Anonymous Italisë, të cilët filluan të godasin Killnet-in dhe të mashtrojnë disa prej anëtarëve të saj duke publikuar foto në rrjetet sociale. Si rezultat, Killnet u kundërpërgjigj. Në momentin e shkrimit, faqja e internetit e CSIRT Italia ishte e padisponueshme, me ndërprerje shërbimi, por nuk u vunë re probleme të gjata në aksesim.

Ka pasur gjithashtu raportime për Postën Italiane, ofruesi kombëtar i shërbimit postar të Italisë, që pësoi një ndërprerje disa orë.

Megjithatë, agjencia ka thënë për La Repubblica se kjo ndërprerje nuk ishte shkaktuar nga sulmet e Killnet, por për shkak të një përmirësimi të softuerit që nuk shkoi siç ishte planifikuar. Njoftimet e tjera të mediave vendase që ndjekin nga afër statusin e faqeve italiane raportojnë se sot të paaksesueshme shfaqen edhe portalet online të Policisë së Shtetit dhe Ministrisë së Jashtme dhe Mbrojtjes italiane.

Rekomandime

Rekomandime për parandalimin e sulmeve DDoS:

- Mos shkarkoni skedarë nga burime të dyshimta ose mos kliko në link-e të dyshimta.
- Mbroni pajisjet nga malware që mund të fshihen në postat elektronike.
- Sigurohuni që programet kompjuterike dhe pajisjet të jenë gjithmonë të përditësuara dhe perdorni pajisje që ofrojnë suport per software dhe hardware.
- Parandaloni përdoruesit të instalojnë aksidentalisht *malware* nga një email phishing, duke kufizuar llogaritë e administratorit, dhe duke i dhënë të drejta vetëm atyre që kanë nevojë. Përdoruesit me llogari administratori nuk duhet t'i përdorin këto llogari për të kontrolluar postën elektronike ose të shfletojnë në internet.
- Mbroni përdoruesit nga faqet e internetit me qëllim të keq. Shumica e shfletuesve të përditesuar bllokojne faqet e njohura të phishing dhe të malware-ve. Kjo nuk ndodh gjithmonë tek pajisjet mobile. Përdor shërbimin proxy në shtëpi ose në cloud, 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”.

- Shtoni siguri në procesin e hyrjes duke vendosur Autentifikimin me Dy Faktor (2FA), i cili gjithashtu quhet 'Dy Hapa në Verifikim' në disa shërbime në internet. Të kesh një faktor të dytë do të thotë që një sulmues nuk mund të hyjë në një llogari vetëm duke përdorur një fjalëkalim të vjedhur.
- Siguroni akses të privilegjuar vetëm për përdorues të kualifikuar. Rishikoni rregullisht dhe revokoni privilegjet nëse nuk janë më të nevojshme.
- Sigurohuni që përdoruesit të dinë paraprakisht se si mund të raportojnë incidente.

Referenca

[1] https://www.bleepingcomputer.com/news/security/italy-warns-organizations-to-brace-for-incoming-ddos-attacks/amp/

[2]https://www.csirt.gov.it/contenuti/rilevato-potenziale-rischio-di-attacco-informatico-ai-danni-di-enti-ed-organizzazioni-nazionali-al01-220529-csirt-ita

[3] https://www.bleepingcomputer.com/news/security/italian-cert-hacktivists-hit-govt-sites-in-slow-http-ddos-attacks/