Ransomware-taldea: BlackNevas Ransomware

Laburpen exekutiboa

BlackNevas ransomware emergentea da, 2024aren amaieran lehen aldiz behatua; **Ransomware-as-a-Service (RaaS)** gisa jarduten du, eta berehala finkatu da estortsio bikoitzeko talde gisa. Beste ransomware-familia moderno batzuek bezala, artxibo lokalak eta sareko artxiboak zifratzen ditu eta lapurtutako informazioa dark webeko atarietan argitaratzen du, biktimei presioa eginez erreskateak ordaintzera behartzeko eta datu sentikorrak filtratzea saihesteko.

BlackNevas-en **hasierako sarbideak** honako hauek izaten dira: **kredentzial** konprometituak, Interneten **esposiziopean jarritako zerbitzuen ustiapena**, eta, zenbait kasutan, **phishing**-kanpainak. Operatiboki, taldeak aurreko familien kodea eta metodologiak berrerabiltzen eta egokitzen ditu, **Trigonarekin antzekotasunak** erakutsiz, eta horrek kanpainak eskalatzeko eta ingurune korporatiboetara egokitzeko bide ematen du.

Teknikoki, malwareak zifratze-algoritmo sendoak erabiltzen ditu, **AES eta gako publikoko teknikak** konbinatzen dituztenak fitxategiak blokeatzeko, ia ezinezko bihurtuz erasotzailearen gakorik gabe berreskuratzea. Segurtasun-kopiak ezabatzeko eta leheneratzea eragozteko mekanismoak ere baditu, eta horrek handitzen du biktimei egiten zaien presioa.

Negozio ziberkriminalaren ereduaren ikuspegitik, BlackNevas-ek atari batzuk ditu dark webean **biktimen zerrendak eta lapurtutako datuen laginak eta ordaintzeko epeak** argitaratzeko, estortsio bikoitzaren ereduari jarraituz. BlackNevas ransomwarea agertu zenetik, hainbat enpresa global erregistratu dira biktima gisa, nazioartean jarduteko gaitasuna eta sektore kritiko eta korporatiboentzako arrisku gero eta handiagoa agerian jarriz.

Ransomware-taldea: BlackNevas

BlackNevas-ek **Ransomware-as-a-Service (RaaS)** eredu batekin jarduten du, afiliatuei **estortsio bikoitzeko** kanpainak egiteko tresnak, azpiegitura eta laguntza teknikoa eskainiz. Kanpaina horietan, konprometitutako sistemak zifratu egiten dira, eta, horrez gain, lapurtutako datuak esfiltratu eta ondoren webeko inguruneetan argitaratzen dira, biktimei egiten zaien presioa areagotzeko.

Talde horrek antzekotasunak ditu Trigona ransomwarearekin, eta beste talde ziberkriminal batzuekin lankidetzan aritzeko duen estrategiagatik bereizten da, hala nola Hunters International, DragonForce, Embargo Team... Eragiketetan zehar, BlackNevas-ek erreskate-ohar bat uzten du **“how_to_decrypt.txt”** izenarekin, eta bertan argibideak ematen dizkie biktimei ordainketa-prozesuari buruz. Eskatutako ordainketa jasotzen ez badu, lapurtutako informazioa filtrazio-plataformen bidez zabaltzeko mehatxua egiten du.

Eragindako herrialdeak eta sektoreak

BlackNevas-en jarduera globala da: Estatu Batuetan, Alemanian, Erresuma Batuan, Australian eta Europako hainbat herrialdetan berretsitako biktimak ditu.

Espainian, gutxienez 3 gorabehera dokumentatu dira, honako hauek barne:

- Undefasa (manufaktura-industria),
- Cartonajes Bernabeu SAU (manufaktura-industria)
- Cash and carry – Cosaen Grup (retail).

Eraso gehien dituzten sektoreen artean **finantzak, manufaktura, teknologia, osasuna eta hezkuntza** daude; jomugan dituzte, batez ere, datu kritikoak maneiatzen dituzten enpresa ertain eta handiak, estortsio bikoitza erabiliz presioa handitzeko eta ordaintzeko aukera maximizatzeko.

Analisi teknikoa

Ikuspegi teknikotik, BlackNevas-ek Trigonaren oinarri kriptografikoa heredatzen du, eta **zifratze hibridoa inplementatzen** du, AES-256, fitxategiak RSArekin batera zifratzeko, horrela deszifratzea ahalbidetzen duten gakoak zifratuz. Malwareak **sistema-arkitektura desberdinak** onartzen ditu, eta bertsio espezifikoak ditu **birtualizazio-inguruneetarako** (ESXi) eta **NAS gailuetarako**, kasu bakoitzerako parametro bereziekin. **Windows eta Linux sistema eragileetan**, operadoreek hainbat funtzionalitate erabil ditzakete, hala nola biktimaren gailutik datuak ezabatzea, artxiboak izena aldatu gabe zifratzea, exekutatzeko lehentasuna aldatzea edo zifratzearen ondoren makina itzaltzea. Gainera, ransomware honek iraunkortasuna sortzen du, eta aukera ematen du sareko baliabide partekatuetan (SMB) artxiboak bilatzeko eta zifratzeko.

Ezaugarri tekniko nagusiak:

- **Eredu operatiboa:** Trigona ransomwarearen aldaera, modu independentean eta RaaS ezaugarriekin jarduten duena.
- **Zifratzea:** AES-256 eta RSA erabiltzen ditu artxiboak blokeatzeko eta gakoak babesteko, berreskuratzea eragotziz.
- **Eragindako sistemak:** Windows, Linux, NAS eta ESXi zerbitzariak erasotzen ditu.
- **Hasierako sarbidea:** Phishingaren, adabakirik gabeko kalteberatasunen eta esposiziopeko urruneko zerbitzuen bidez.
- **Esfiltrazioa:** Datuak lapurtzen eta argitaratzen ditu dark webean duen filtrazioen gunean, biktimei estortsioa egiteko.

MITRE ATT&CK teknikak

Taktika	Teknika erabiliena
Initial Access	**T1190** — Exploitation of Public-Facing Application **T1566** — Phishing **T1078** — Valid Accounts
Execution	**T1059** — Command and Scripting Interpreter **T1203** — Exploitation for Client Execution
Persistence	**T1547** — Boot/Logon Autostart **T1547.001** — Registry Run Keys/Startup Folder
Privilege Escalation	**T1068** — Exploitation for Privilege Escalation
Defense Evasion	**T1070** — Indicator Removal on Host **T1027** — Obfuscated Files or Information **T1562** — Impair Defenses
Discovery	**T1135** — Network Share Discovery **T1012** — Query Registry **T1083** — File and Directory Discovery
Command and Control	**T1071** — Application Layer Protoco
Impact	**T1486** — Data Encrypted for Impact **T1561.001** — Disk Content Wipe

Arintze-neurriak

Proaktiboak

- ❑ Segurtasun-adabakiak aplikatzea, zerbitzu publikoak suebakiarekin/WAFekin babestea, faktore anitzeko autentifikazioa inplementatzea eta prestakuntza phishingaren aurrean. (T1566 – Phishing, T1190 – Exploit Public-Facing Application, T1078 – Valid Accounts)

- ❑ Sinatu gabeko scriptak eta makroak mugatzea, PowerShell edo CMD bezalako interpreteen erabilera kontrolatzea eta hasiera automatikoko gakoak eta karpetak monitorizatzea. (T1203 – Exploitation for Client Execution , T1059 – Command and Scripting Interpreter, T1547 – Boot or Logon Autostart Execution)

- ❑ Pribilegioak dituzten kontuak mugatzea, sistema eguneratuta mantentzea eta ezabatzeen aurrean logak babestea. (T1068 – Exploitation for Privilege Escalation, T1070 – Indicator Removal, T1562 – Impair Defenses)

- ❑ Pribilegio minimoaren printzipioa aplikatzea, sarea segmentatzea eta baliabide partekatuetarako sarbideak monitorizatzea. (T1083 – File and Directory Discovery, T1135 – Network Share Discovery)

- ❑ Offline segurtasun-kopiak mantentzea, aldizkako leheneratzeak probatzea, irteerako trafikoa iragaztea eta komunikazio-patroi susmagarriak detektatzea. (T1486 – Data Encrypted for Impact, T1561.001 – Disk Wipe: Disk Content Wipe, T1071 – Application Layer Protocol):

Erreaktiboak

- ❑ Antibirusak AMSIrekin erabiltzea, ASR arauak aplikatzea eta erabiltzaileei prestakuntza ematea fitxategi lausotuak blokeatzeko. (T1027 - Obfuscated Files or Information)

Ondorioak eta gomendioak

BlackNevas-ek entzute handia lortu du 2025eko ransomware-aldaerarik aktiboenetako bat izanik, eta egokitzeko duen gaitasunagatik eta hainbat sektore eta eskualdetan sortzen duen inpaktuagatik nabarmentzen da. Bere jarduerak ondo egituratutako jarduna erakusten du, hedapen global azkarrarekin eta Europan, Asian eta Amerikan biktimen kopuruaren gorakadarekin –tartean Espainiako hainbat enpresa–; horrek bere nazioarteko irismena berresten du.

Taldeak **Trigona ransomware familiarekin loturak** dituela dirudi, zifratze-teknikak eta estortsio bikoitzeko taktikak partekatzen baitituzte, nahiz eta modu independentean eta baliabide propioekin jarduten duen. Joera horrek ransomwarearen ekosistemaren dibertsifikazioa islatzen du, non hainbat familiak azpiegiturak eta erremintak partekatzen dituzten haren eraginkortasuna maximizatzeko.

BlackNevas-ekiko arriskua murrizteko, gomendatzen da **MFArekin** urruneko sarbideak indartzea, sistemak **eguneratuta eta segmentatuta** mantentzea, segurtasun-kopiak offline babestea eta balizko gorabeheren aurrean **monitorizazioa eta erantzun azkarra** izatea.

