SECURITY BULLETIN

Týždeň 23. 08. 2017 – 29. 08. 2017

No: B20170829-01V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure – Joint Technical Alert

Popis

FBI (Federal Bureau of Investigation) a DHS (Department of Homeland Security) vydala tzv. spojené technické upozornenie (joint Technical Alert), ktoré poukazuje na technické detaily a nástroje, ktoré sú používané pri kybernetických útokoch zo strany Severnej Kórei s cieľom ovplyvňovať médiá, finančnú sféru a kritickú infraštruktúru v Spojených štátoch amerických, ako aj v globálnej rovine.

FBI spolu s DHS odhalili IP adresy a protokoly, cez ktoré komunikuje DeltaCharlie, typ malvéru, používaný na infikovanie zariadení pripojených na sieť a ich následné zapojenie do botnetu, ktorý Severná Kórea využíva na DDoS útoky. Správa obsahuje rôzne IOC (Indicators of Compromise).

Od roku 2009 sa predstavitelia skupiny HIDDEN COBRA zameriavajú na kompromitáciu veľkej škály obetí, pričom niektoré útoky viedli k exfiltrácii dát alebo narušeniu prostredia u obete. Komerčné spravodajstvo poukazovalo v týchto prípadoch na skupiny ako Lazarus Group a Guardians of Peace, ktoré sú taktiež spájané s vládou v Severnej Kórei.

FBI a DHS zhodnotili, že predstavitelia skupiny HIDDEN COBRA budú aj naďalej využívať kybernetické operácie na podporu vojenských a strategických cieľov vlády v Severnej Kórei. Preto svojou správou chcú vyzvať všetkých analytikov a pracovníkov, pôsobiacich v oblasti kybernetickej bezpečnosti, aby skontrolovali a monitorovali škodlivé aktivity v sieti.

Nástroje a postupy, ktoré sú najčastejšie používané skupinou HIDDEN COBRA, zahŕňajú DDoS boty, keylogery, nástroje RAT na vzdialený prístup a wiper malvér. Najčastejšími variantami sú Destover, Wild Positron / Duuzer a Hangman. Takisto sa u tejto skupiny vyskytujú aj nástroje server message block (SMB).

HIDDEN COBRA sa väčšinou zameriava na systémy, ktoré používajú staršie nepodporované verzie operačných systémov od spoločnosti Microsoft. Takisto využívajú aj zraniteľnosti v neaktualizovaných verziách softvéru Adobe Flash Player.

CVE

Činnosť Hidden Cobra sa zameriava na zneužívanie zraniteľností pod CVE:

- CVE-2015-6585: Hangul Word Processor Vulnerability
- CVE-2015-8651: Adobe Flash Player 18.0.0.324 and 19.x Vulnerability
- CVE-2016-0034: Microsoft Silverlight 5.1.41212.0 Vulnerability
- CVE-2016-1019: Adobe Flash Player 21.0.0.197 Vulnerability
- CVE-2016-4117: Adobe Flash Player 21.0.0.226 Vulnerability

Zasiahnuté systémy

Sieťové systémy

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*

SK-CERT
Naša značka:

IOC (Indicators of Compromise)
Kompletný list IOC nájdete na tomto odkaze: https://www.us-cert.gov/sites/default/files/publications/TA-17-164A_csv.csv

MAR (Malware analysis report)
Kompletný MAR nájdete na tomto odkaze: https://www.us-cert.gov/sites/default/files/publications/MAR-10132963.pdf

Technická analýza
DeltaCharlie je nástroj DDoS, ktorý používa HIDDEN COBRA, schopný spustiť útoky na DNS (Domain Name System), útoky na NTP (Network Time Protocol) a útoky typu NAT (CGN). Malware funguje na systéme botov ako služba založená na svchost a je schopná prevziať spustiteľné súbory, zmeniť vlastnú konfiguráciu, aktualizovať svoje vlastné binárne súbory, ukončiť svoje vlastné procesy a aktivovať a ukončiť DDoS útoky.

Sieťové signatúry
alert tcp any any -> any any (msg:"DPRK_HIDDEN_COBRA_DDoS_HANDSHAKE_SUCCESS"; dsize:6; flow:established,to_server; content:"|18 17 e9 e9 e9 e9|"; fast_pattern:only; sid:1; rev:1;) alert tcp any any -> any any (msg:"DPRK_HIDDEN_COBRA_Botnet_C2_Host_Beacon"; flow:established,to_server; content:"|1b 17 e9 e9 e9 e9|"; depth:6; fast_pattern; sid:1; rev:1;)

HBR (Host-Based Rules)
Kompletný výpis HBR (v tomto prípade YARA) pravidiel nájdete na tomto odkaze: https://www.us-cert.gov/ncas/alerts/TA17-164A

Následky
Dočasná alebo trvalá strata citlivých alebo chránených informácií, Zneprístupnenie služby, narušenie pravidelnej prevádzky

Detekcia
DHS a FBI odporúčajú administrátorom siete, aby skontrolovali IP adresy, hash súbory, sieťové podpisy a YARA pravidlá a pridali IP adresy, uvedené v IOC súbore vyššie, do svojho monitorovacieho zoznamu, aby zistili, či bola v ich organizácii pozorovaná škodlivá aktivita. Pri kontrole sieťových protokolov a logov z perimetrov siete môžu administrátori nájsť početné prípady podozrivých IP adries, ktoré sa pokúšajú pripojiť k určitým systémom. Pri kontrole komunikácie z týchto IP adries správcovia systému môžu zistiť, že určité prenosy zodpovedajú škodlivým aktivitám a niektorým legitímnym aktivitám. Správcom systémov sa tiež odporúča, aby spustili nástroj YARA na akomkoľvek systéme, o ktorom majú podozrenie, že boli predmetom útoku zo strany HIDDEN COBRA.

Odporúčania

Administrátorom siete sa odporúča, aby uplatňovali nasledujúce odporúčania, ktoré môžu zabrániť až v 85 percentách cieleným kybernetickým útokom:

1. Aktualizácia aplikácií a operačných systémov - Väčšina útočníkov sa zameriava na zraniteľné aplikácie a operačné systémy. Skutočnosť, že aplikácie a operačné systémy sú vždy aktualizované najnovšími aktualizáciami, výrazne znižuje možnosť využiť zraniteľnosti týchto systémov. Používajte osvedčené postupy pri aktualizácii softvéru pomocou oficiálnych aktualizácií iba z overených lokalít od dodávateľov.
2. Používanie „whitelistov“ – Whitelist v rovine určenia povolení pri spúšťaní programov a služieb je jednou z najlepších stratégií zabezpečenia, pretože umožňuje spustiť iba špecifikované programy, pričom zablokuje všetky ostatné vrátane škodlivého softvéru.
3. Obmedziť privilégiá pre správcov - útočníci sa čoraz viac zameriavajú na získanie legitímnych oprávnení, najmä spojených s vysoko privilegovanými účtami. Upravte preto privilégiá administrátorov len na potrebnú úroveň s obmedzeným prístupom do iných úrovní.
4. Rozdeľte svoju sieť a vytvorte rôzne úrovne zabezpečenia - Segmentujte siete do logických štruktúr a obmedzte komunikačné cesty medzi jednotlivými sieťami. To pomáha chrániť citlivé informácie a kritické služby a obmedzuje poškodenia pri narušení siete.
5. Overovanie prístupov - verifikácia prístupov je metóda filtrácie nedôveryhodných vstupov používateľmi webových aplikácií. Implementácia verifikácie môže chrániť pred bezpečnostnými chybami webových aplikácií výrazným znížením pravdepodobnosti úspešného zneužitia. Typy útokov, ktoré možno odvrátiť, zahŕňajú útoky SQL injection, XSS a iné, na webové aplikácie zamerané útoky.
6. Použitie prísnych nastavení dôveryhodnosti súborov – Nastavte si najmä antivírusové systémy na také nadstavenie, ktoré dovoľuje spustiť len naozaj dôveryhodné programy a aplikácie.
7. Používajte firewall - Firewall pomáha vytvárať bezpečné prostredie a takisto slúži na minimalizáciu možností zaútočiť na váš systém.

Zdroje

https://www.us-cert.gov/ncas/alerts/TA17-164A