Raport consolidat eveniment cibernetic

Malware NsppS

Descriere tehnică	**NsppS** este un troian de acces de la distanță (**RAT**), cu caracteristici de botnet. Codul său a fost scris în limbajul **Golang,** ceea ce îi conferă portabilitate și eficiență în execuție Atacul se desfășura folosind protocolul **HTTP**, pentru a trimite sau primi comenzi de la un server de comandă și control (C2).
Funcționalități principale	• **Acces la distanță:** Permite atacatorilor să execute comenzi pe sistemul compromis, oferind control complet asupra acestuia. • **Activități Proxy**: Configurează un server *SOCKS5* pe sistemul compromis, permițând atacatorilor să redirecționeze traficul de rețea prin acesta, facilitând activități de proxying și ascunderea originii traficului. • **Scanare de rețea:** Utilizează instrumente precum *Masscan* sau versiunea personalizată *"firewire"* pentru a scana rețeaua în căutarea altor sisteme vulnerabile, facilitând propagarea laterală. • **Exploatarea vulnerabilităților:** Profită de vulnerabilități cunoscute, cum ar fi *CVE-2019-19781* pentru a obține acces inițial la sisteme. • **Minerit de criptomonede:** Poate descărca și executa mineri de criptomonede, utilizând resursele sistemului compromis pentru a genera profit pentru atacatori. • **Evitarea detectării:** Se deghizează sub nume similare cu procese legitime, cum ar fi "*nsppe"*, pentru a induce în eroare administratorii de sistem. • **Persistență:** Își asigură persistența pe sistem prin diverse metode, inclusiv scripturi și modificări ale configurațiilor sistemului.
Similarități cu alte malware:	• **Kinsing:** scanarea rețelei pentru a detecta vulnerabilități, persistența prin cron-jobs sau scripturi de inițializare. • **Anchor:** abilitatea de a instala module suplimentare, persistența prin modificări în configurațiile sistemului. • **LemonDuck:** scanare agresivă a rețelei pentru a identifica noi ținte, exploatarea vulnerabilităților pentru propagare și utilizarea resurselor sistemului compromis pentru minerit. • **Tsunami:** exploatarea SSH pentru propagare, funcționalități extinse pentru control de la distanță. • **Mirai:** exploatarea porturilor și acreditărilor slabe, utilizarea fișierelor script pentru propagare.

Cele mai răspândite metode de infectare	• **Phishing and Social Engineering:** E-mailurile de phishing sunt una dintre cele mai comune metode utilizate pentru a livra NsppS. Prin diferite tactici de inginerie socială utilizatorii sunt înșelați să activeze macrocomenzi sau să ruleze fișierele executabil care le infectează sistemul. • **Explorarea vulnerabilităților:** Botnetul poate fi implimentat exploatând unele vulnerabilități ale sistemului (de ex. *CVE-2019-1978*). • **Scanare de rețea:** După compromiterea unui sistem, NsppS poate efectua scanări pentru a identifica alte dispozitive vulnerabile în rețea folosind *Masscan* sau versiuni personalizate precum „*firewire*”. La fel caută porturi și servicii vulnerabile, cum ar fi servere *SSH* sau interfețe de management. • **Exploatarea configurațiilor greșite**: NsppS vizează sistemele slab configurate sau expuse, cum ar fi servere fără parole puternice pentru *SSH*, dispozitive accesibile prin internet fără măsuri de securitate adecvate. • **Propagare laterală în rețea:** După compromiterea unui sistem, NsppS se poate răspândi la alte dispozitive din aceeași rețea • **Abuzarea funcțiilor integrate ale sistemelor compromise:** În unele cazuri, NsppS poate folosi funcții legitime ale sistemului pentru a facilita propagarea, cum ar fi folosirea utilitarelor standard (*ex.: scp, ssh*) pentru a accesa alte sisteme.
Recomandări generice pentru detectare	1. **Detectarea anomaliilor comportamentale:** Analizați activități neobișnuite, cum ar fi cereri *HTTP* suspecte, conexiuni *SSH* nereușite. 2. **Analiza traficului de rețea:** Folosiți instrumente precum *Wireshark* sau comanda *netstat* pentru a analiza anomaliile traficului cum ar fi conexiunile suspecte către serverele C2 sau trafic criptat pe porturi nesecurizate 3. **Scanare cu software specializat:** Utilizați soluții care includ detecție pentru malware scris în limbajul *Golang*. Integrați indicatorii de Compromitere (IoCs) în sistemele de monitorizare. Scrieți sau implementați reguli *YARA* pentru detectarea specifică a fișierelor malițioase. 4. **Scanarea fișierelor:** Căutați fișiere executabile neobișnuite în directoare temporare sau în locații sistem critice (*ex.: /tmp, /var, /usr/bin*). 5. **Scanarea și analizarea vulnerabilităților:** verificați dacă sistemele sunt expuse vulnerabilităților cunoscute, precum *CVE-2019-19781*. Utilizați un scanner de vulnerabilități, cum ar fi *Nessus* sau *OpenVAS*. Asigurați-vă că toate sistemele rulează la cele mai recente versiuni ale software-ului.

csi_rules.yara Kinsing/NSPPS malware	*rule Kinsing_Malware {* *meta:* *author = "Aluma Lavi, CyberArk"* *date = "22-01-2021"* *version = "1.0"* *hash = "d247687e9bdb8c4189ac54d10efd29aee12ca2af78b94a693113f382619a175b"* *description = "Kinsing/NSPPS malware"* *strings:* *$rc4_key = { 37 36 34 31 35 33 34 34 36 62 36 31 }* *$firewire = "./firewire -iL $INPUT --rate $RATE -p$PORT -oL $OUTPUT"* *$packa1 = "google/btree" ascii wide* *$packa2 = "kardianos/osext" ascii wide* *$packa3 = "kelseyhightower/envconfig" ascii wide* *$packa4 = "markbates/pkger" ascii wide* *$packa5 = "nu7hatch/gouuid" ascii wide* *$packa6 = "paulbellamy/ratecounter" ascii wide* *$packa7 = "peterbourgon/diskv" ascii wide* *$func1 = "main.RC4" ascii wide* *$func2 = "main.runTaskWithScan" ascii wide* *$func3 = "main.backconnect" ascii wide* *$func4 = "main.downloadAndExecute" ascii wide* *$func5 = "main.startCmd" ascii wide* *$func6 = "main.execTaskOut" ascii wide* *$func7 = "main.minerRunningCheck" ascii wide* *condition:* *(uint16(0) == 0x457F* *and not (elf.sections[0].size + elf.sections[1].size + elf.sections[2].size + elf.sections[3].size + elf.sections[4].size + elf.sections[5].size + elf.sections[6].size + elf.sections[7].size > filesize))* *and ($rc4_key* *or $firewire* *or all of ($packa*)* *or 4 of ($func*)* *)* *}*

Resurse externe

	https://www.ironnet.com/blog/malware-analysis-nspps-a-go-rat-backdoor
	https://trustedsec.com/blog/netscaler-honeypot