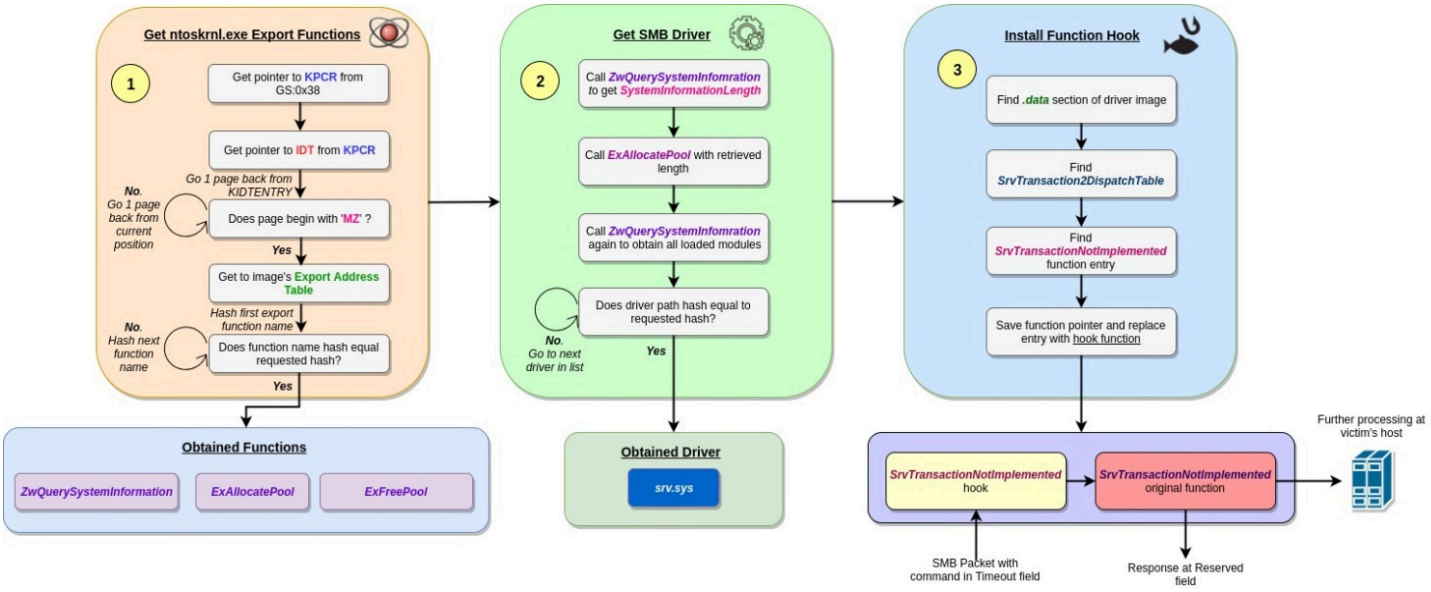
Raport consolidat eveniment cibernetic

Backdoor.DoublePulsar Malware

Backdoor.DoublePulsar Malware este un agent malițios care permite accesul la distanță prin exploatarea vulnerabilităților SMB (Server Message Block). Acesta a fost dezvăluit de scurgerile de informații ale Shadow Brokers în martie 2017 și a fost folosit în atacul ransomware WannaCry din mai 2017. Susține atât protocolul **SMB** cât și **RDP**.

Acesta rămâne persistent în sistem prin crearea de fișiere și modificări ale registrului și comunică pe **porturile 445/3389.**



DoublePulsar backdoor installation stages

Informații sumare

TIP	***Backdoor.DoublePulsar Malware***
Instrumente pentru analiză	• **Pentru scanarea rețelei** – Wireshark, TCPDUMP, Angry IP Scanner • **Pentru scanarea de viruși și malware** – Software antivirus existente • **Anliză și detectare** -NMAP:SMB-DOUBLE-PULSAR-BACKDOOR.NSE, Lordpe, Sysmon , Procces Hacker
Detectare	1. Scanează sistemele pentru prezența fișierelor malware specifice, cum ar fi **kbv.dat** plasat în folderul **%TEMP%** de către DoublePulsar. 2. Monitorizează activitatea rețelei în căutarea unor conexiuni externe neobișnuite, în special către servere C&C utilizate de botnet. 3. Verifică lista proceselor și porturile deschise pentru procese/porturi suspecte ca **445/139** utilizate de DoublePulsar pentru C&C. 4. Examinează registrele și sistemul de fișiere pentru artefacte precum intrări modificate în **Run/RunOnce, autorun.inf** modificat etc. 5. Analizează traficul de rețea capturat cu Wireshark pentru a decoda și identifica comunicările specifice. 6. Controlează dacă sunt vulnerabile versiunile SMB exploatate, de ex. **SMBv1**. 7. Efectuează o analiză avansată a memoriei sistemelor suspecte pentru a depista cod injectat sau alte semne de infecție activă. 8. Utilizați https://github.com/countercept/doublepulsar-detection-script script în Python, ce detectează dacă mașina pe care se rulează este infectată.
NMAP:SMB-DOUBLE-PULSAR-BACKDOOR.NSE	**Example of usage** nmap -p 445 <target> --script=smb-double-pulsar-backdoor **Script Output** | smb-double-pulsar-backdoor: | VULNERABLE: | Double Pulsar SMB Backdoor | State: VULNERABLE | Risk factor: HIGH CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) | The Double Pulsar SMB backdoor was detected running on the remote machine. | | Disclosure date: 2017-04-14 | References: | https://isc.sans.edu/forums/diary/Detecting+SMB+Covert+Channel+Double+Pulsar/22312/ | https://github.com/countercept/doublepulsar-detection-script |_ https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation

Măsuri de tratare post incident	• **Izolarea dispozitivului compromis** -Identificați dispozitivul sau sistemele suspecte și izolați-le de rețeaua principală. Izolarea poate fi efectuată prin : deconectarea fizică a dispozitivelor sau restricționarea accesului acestora la rețea. • **Întreruperea comunicării cu serverul de comandă și control (C&C)** - Blocați traficul de ieșire către adresele IP cunoscute asociate cu serverele de comandă și control, le găsiți în descrierea din Anexă. Pentru aceasta utilizați firewall-uri sau soluții de filtrare a traficului. • **Actualizarea software-ului și a sistemelor (patch &update)** - Asigurați-vă că toate dispozitivele și sistemele din rețea sunt actualizate la cele mai recente versiuni, inclusiv sistemele de operare, aplicațiile și software-ul de securitate. Acest lucru ajută la remedierea vulnerabilităților cunoscute și la prevenirea reinfectării. • **Scanarea și curățarea dispozitivelor compromise** - Utilizați un antivirus actualizat și soluții anti-malware pentru a scana toate dispozitivele compromise în căutarea amenințărilor. Eliminați sau izolați fișierele și programele malware identificate. • **Resetarea dispozitivelor la starea implicită** - În cazul dispozitivelor care nu pot fi curățate sau încredințate, luați în considerare resetarea acestora la setările implicite de fabrică. Asigurați-vă că după resetare toate parolele implicite sunt schimbate și actualizate. • **Analiza log-urilor -** Analizați log-urile de securitate pentru a identifica activitatea suspectă și modelele de atac. Astfel puteți afla dacă unele porturi au rămas deschise sau sunt configurate greșit, iar remedierea acestor vulnerabilități va ajuta la creșterea nivelului de securitate din rețeaua locală. • **Reevaluarea securității rețelei** - Evaluați în mod regulat securitatea rețelei și revizuiți politicile de securitate pentru a vă asigura protecția continuă împotriva amenințărilor.

Resurse externe

	*https://isc.sans.edu/forums/diary/Detecting+SMB+Covert+Channel+Double+Pulsar/22312/*
	*https://github.com/countercept/doublepulsar-detection-script*