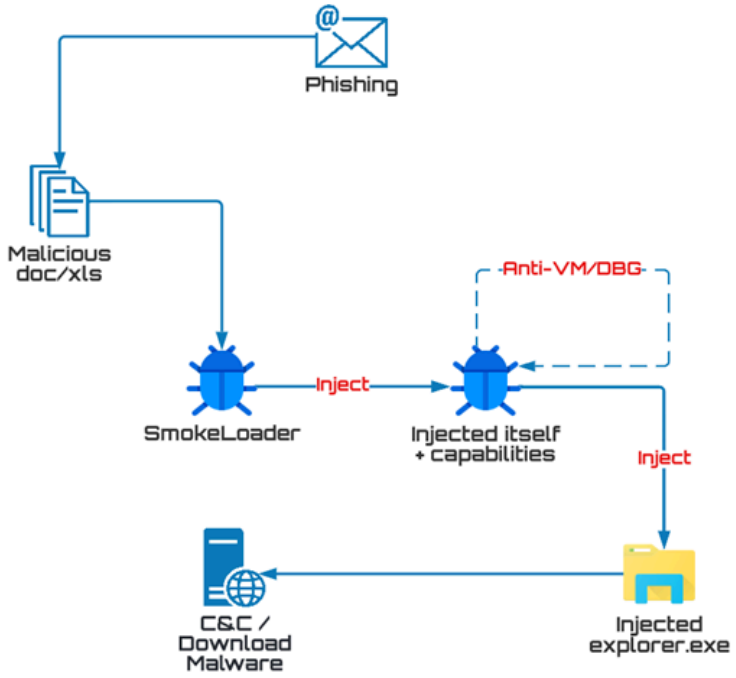
Raport consolidat eveniment cibernetic

Loader-ul Smoke

Loader-ul Smoke, cunoscut uneori și sub numele de **Dofoil**, este un malware modular utilizat în principal pentru a descărca alte viruși pe dispozitivele infectate. În ciuda naturii sale de loader, bot-ul Smoke Loader poate fi echipat cu o varietate de funcții malițioase. Majoritatea acestor funcții sunt orientate către furtul de date sensibile de la victime.

Smoke Loader a fost observat pentru prima dată în mediul sălbatic în 2011. A fost văzut fiind vândut pe portaluri subterane precum **grabberz[.]com și xaker[.]name** de un utilizator numit SmokeLdr. Funcționalitatea malware-ului variază de la un atac la altul și depinde de alegerea modulelor de către atacatori. Trebuie menționat că, după martie 2014, Smoke Loader este vândut doar atacatorilor vorbitori de limbă rusă.



Infectarea cu Loader Smoke

Informații sumare

TIP	***Loader-ul Smoke***
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
Identificare Smoke Loader	**1. Monitorizarea Traficului de Rețea :** Analizați și monitorizați traficul de rețea pentru activități suspecte, cum ar fi conexiuni frecvente către domenii cunoscute ca fiind malițioase (de exemplu, microsoft[.]com și adobe[.]com) sau către adrese IP suspecte. Utilizați soluții IDS/IPS pentru a detecta comunicările neobișnuite și pentru a bloca traficul către serverele C2. **2. Analiza Logurilor:** Examinați logurile de la servere, endpoint-uri și soluții de securitate pentru a identifica activități neobișnuite sau suspicioase. Căutați semne de execuție a fișierelor necunoscute sau modificări neașteptate în sistemele de fișiere și registre. **3. Scanări Antivirus și Antimalware:** Folosiți soluții de securitate actualizate pentru a efectua scanări complete ale sistemelor. Asigurați-vă că definițiile antivirus sunt la zi. Utilizați scanere dedicate pentru malware care pot identifica semnăturile specifice ale Smoke Loader. **4. Monitorizarea Proceselor și Activităților de Sistem:** Folosiți instrumente de monitorizare a sistemului pentru a urmări procesele active și pentru a detecta procesele injectate cum ar fi explorer.exe și rundll32.exe. Identificați și izolați procesele suspecte care rulează din locații neobișnuite, cum ar fi directoarele temporare.
Funcții principale	**Funcțiile principale ale Smoke Loader includ:** - Încărcarea și executarea a până la zece fișiere executabile. - Geo-țintirea victimelor pentru a direcționa atacurile către anumite țări. - Încărcarea fișierelor prin URL-uri. - Imitarea proceselor legitime. - Furnizarea de rezumate detaliate privind instalările și lansările. **Cele două module opționale** permit Smoke Loader să își extindă setul de caracteristici cu funcții de furt de informații. Acest lucru permite Dofoil să captureze parole din clienți de e-mail larg utilizați, clienți FTP și programe precum TeamViewer. Malware-ul poate trimite datele către C2 pentru atacator.
	MD5 - e6df0358d88a8286d96cba694588e74b - b8f70c9f9b3e385f78df360cf10b931d

IOC	**SHA-1** - 19c2f1461c0be9c7ecb75537ff52dc8d1431b0e1 - 97c63d4b34c1b9f96b3b8efdbecd3162d4d95e9f **SHA-256** - 7f5fbb1b9cf10e2075b0c4d0bc9d5a6f21d58b8fdb90a702620bb5b953e15c27 - 3401c49c8b47dc4d7f5c6a60420b9d02eec8f4a37b03faea8c9cba3dd1be56e1 **URL-uri și domenii** - grabberz[.]com - xaker[.]name - microsoft[.]com (utilizat pentru comunicații de tip C2) - adobe[.]com (utilizat pentru comunicații de tip C2) **Adrese IP suspecte** - 185.129.148.50 - 95.181.151.95 - 37.1.214.166 **Chei de registru** - **HKCU\Software\Microsoft\Windows\CurrentVersion\Run**
Procese și activități suspecte	- explorer.exe (cod malițios injectat) - rundll32.exe (utilizat pentru a încărca module malițioase) - crearea și execuția fișierelor .exe în directoare temporare
Tehnici de distribuție și execuție	- Documente Microsoft Office malițioase trimise prin campanii de email spam - Utilizarea ingineriei sociale pentru a păcăli victimele să activeze macro-urile - Injectarea codului malițios în procese legitime de sistem
	- Încărcarea și executarea fișierelor executabile malițioase - Geo-țintirea victimelor pentru atacuri direcționate

Funcționalități specifice	- Imitarea proceselor legitime pentru a evita detectarea - Furtul de informații din clienți de e-mail, FTP și aplicații de acces la distanță (ex. TeamViewer)
Comunicări de rețea	Realizarea de cereri HTTP către site-uri precum microsoft[.]com și adobe[.]com, în ciuda răspunsurilor HTTP 404, cu date ascunse în corpul răspunsului
Eliminare Smoke Loader	**1. Izolarea Sistemelor Afectate:** - Deconectați imediat sistemele infectate de la rețea pentru a preveni răspândirea malware-ului și pentru a întrerupe comunicarea cu serverele C2. - Utilizați VLAN-uri separate pentru a izola dispozitivele compromise. 2. **Eliminarea Manuală a Malware-ului:** - Identificați și ștergeți fișierele malițioase identificate în locații neobișnuite (de exemplu, %AppData%\SmokeLoader\smoke.exe). - Verificați și curățați cheile de registru suspecte, cum ar fi `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\SmokeLoader`. **3. Restaurarea Sistemelor:** - Reinstalați sistemul de operare pe dispozitivele afectate dacă nu se poate asigura eliminarea completă a malware-ului. - Restaurați datele din backup-uri sigure, asigurându-vă că acestea nu sunt infectate. **4. Actualizarea și Patching-ul Sistemelor:** - Asigurați-vă că toate sistemele și aplicațiile sunt actualizate cu cele mai recente patch-uri de securitate pentru a preveni exploatarea vulnerabilităților cunoscute. - Implementați măsuri de securitate suplimentare, cum ar fi controlul aplicațiilor și restricționarea macro-urilor în documentele Microsoft Office. **5. Educație și Conștientizare:** - Instruirea utilizatorilor în recunoașterea e-mailurilor de phishing și a altor tactici de inginerie socială. - Promovarea practicilor de securitate, cum ar fi verificarea sursei e-mailurilor și evitarea deschiderii atașamentelor necunoscute

Resurse externe

https://medium.com/@farghly.mahmod66/smoke-loader-analysis-1f1442809802