Utilizarea unei versiuni trojanizate KeePass pentru livrarea Cobalt Strike

<table>
<tr><td>Descriere</td><td colspan="2">O campanie recentă de tip malware a vizat utilizatorii aplicației KeePass, distribuind o versiune trojanizată care, odată executată, lansează un beacon Cobalt Strike și începe furtul de credențiale. Atacul exploatează încrederea în aplicația de tip password manager și vizează obținerea accesului inițial în infrastructura victimelor.</td></tr>
<tr><td rowspan="6">Informație tehnică</td><td>Categorie</td><td>Detalii</td></tr>
<tr><td>Aplicație compromisă</td><td>KeePass (versiune falsificată/trojanizată).</td></tr>
<tr><td>Tip de malware</td><td>Trojan + Cobalt Strike beacon.</td></tr>
<tr><td>Tehnici utilizate</td><td>Executabil trojanizat, injectare în memorie, C2.</td></tr>
<tr><td>Framework post-exploatare</td><td>Cobalt Strike.</td></tr>
<tr><td>Metodă de livrare</td><td>Descărcare de pe surse neoficiale, inginerie socială.</td></tr>
<tr><td>Persistență</td><td>Posibilă injectare în proces legitim / execuție la pornirea sistemului.</td></tr>
<tr><td>Etapele de exploatare</td><td colspan="2">1. Distribuție: Victima descarcă aplicația KeePass falsificată de pe o sursă neoficială.
2. Execuție: La rulare, interfața aparent legitimă a KeePass este lansată pentru a nu ridica suspiciuni.
3. Injecție Cobalt Strike: În fundal, este injectat un beacon Cobalt Strike în memorie.
4. Comunicare C2: Sistemul infectat comunică cu infrastructura atacatorului, oferind control de la distanță.
5. Exfiltrare: Se extrag credențiale, token-uri și alte date sensibile.</td></tr>
<tr><td>Metode de detectare</td><td colspan="2">1. Analiza comportamentală - Observarea activităților neobișnuite ale KeePass.exe.
2. Verificare integritate fișiere - Compararea semnăturilor și hash-urilor cu versiunile oficiale.
3. Monitorizare trafic de rețea - Detectarea conexiunilor către infrastructură C2 necunoscută.
4. EDR/AV - Semnale de injectare în memorie, activități de tip beacon.
5. YARA scan - Reguli specifice pentru detectarea Cobalt Strike</td></tr>
<tr><td rowspan="4">Indicatori de Compromitere (IoC)</td><td>Tip</td><td>Valoare (exemple)</td></tr>
<tr><td>Hash SHA256</td><td>e3a53c8d3e05d5a7b7f0dc84f2c10b3f4cfa2d8d1d44df1c4ea2e718adb8d479</td></tr>
<tr><td>Domeniu C2</td><td>update-soft[.]cc, kee-access[.]xyz</td></tr>
<tr><td>IP C2</td><td>45.67.231.98, 185.225.74.34</td></tr>
<tr><td></td><td>Nume fișier</td><td>KeePass-Setup.exe, KeePassPortable.exe</td></tr>
<tr><td>Componentele compromise</td><td colspan="2">• Proces suspect: KeePass.exe rulează concomitent cu procese de tip rundll32.exe, powershell.exe, sau mshta.exe.
• Persistență: Scriere de chei în HKCU\Software\Microsoft\Windows\CurrentVersion\Run.</td></tr>
</table>

Utilizarea unei versiuni trojanizate KeePass pentru livrarea Cobalt Strike

	• **Memorie:** Activitate reflectivă (Reflective DLL Injection) detectată în proces *KeePass*. • **Fișiere temporare**: Drop de fișiere în *%TEMP%* sau *%APPDATA%*.
Măsuri de remediere	1. Descărcați aplicațiile doar de pe site-uri oficiale. 2. Verificați semnătura digitală a fișierelor executabile. 3. Implementați soluții EDR/XDR pentru detectarea comportamentelor de tip post-exploit. 4. Blocați la firewall domeniile și IP-urile necunoscute legate de activități C2. 5. Izolați stațiile compromise și efectuați analiza criminalistică (forensics). 6. Educați utilizatorii privind riscurile de descărcare de aplicații neoficiale.
Vulnerabilități exploatabile ulterior	• CVE-2021-40444 – Microsoft MSHTML Remote Code Execution • CVE-2022-30190 – Follina RCE (Microsoft Support Diagnostic Tool) • CVE-2023-23397 – Outlook Privilege Escalatio
Referință	https://securityonline.info/trojanized-keepass-used-to-deploy-cobalt-strike-and-steal-credentials/ https://github.com/Yara-Rules/rules