Analiza malware TinkyWinkey – keylogger avansat pentru Windows cu persistență prin servicii

Arhitectura Malware și Componente	TinkyWinkey constă din două module modulare: • Tinky Service — un serviciu Windows malitios care: ✓ Instalează și gestionează via SCM (Service Control Manager). ✓ Rulează automat la pornirea sistemului, asigurând persistența. • Winkey Keylogger — componenta care: ✓ Poate rula ca executabil independent (winkey.exe) sau poate fi injectată ca DLL în procese de încredere (de ex. explorer.exe). ✓ Execută injecție DLL folosind metode de tip remote memory allocation și *LoadLibraryW*. Acest design dual îi oferă flexibilitate și stealth sporit.
Funcționalități Tehnice și Evaziune	❖ Keylogging și Reconnaissance: ✓ Instalează un hook la nivel scăzut (*WH_KEYBOARD_LL*) pentru intercepția tuturor tastărilor — inclusiv taste speciale, media keys, combinații, caractere Unicode și schimbări de layout. ✓ Monitorizează continuu fereastra activă (foreground window) pentru corelarea tastărilor cu aplicații specifice (browser, email, banking etc.). ❖ Profilare Sistem Realizează colectarea detaliată a informațiilor despre sistem folosind API-uri de nivel jos, inclusiv: ✓ *RtlGetVersion* (din ntdll.dll) — pentru identificarea corectă a versiunii OS; ✓ *__cpuid* și *GetSystemInfo()* — pentru detalii CPU (producător, model, arhitectură, număr nuclee); ✓ *gethostname*, *getaddrinfo* — pentru informații de rețea; ✓ *GlobalMemoryStatusEx()* — pentru dimensiunea RAM instalată. ❖ Logare și Persistență ✓ Datele sunt stocate într-un fișier text în codificare UTF-8, denumit *logs_tw.txt*, în directorul temporar al utilizatorului (temp). ✓ Persistența este asigurată prin serviciul "Tinky" configurat să pornească automat la boot.
IOCs	• Fișiere/artefacte cunoscute: ✓ *winkey.exe*, *tinky.exe* → executabile plasate în *%TEMP%*, *%APPDATA%*, *%ProgramData%*. ✓ *logs_tw.txt* → fișier text în *%TEMP%*, cu log-uri tastate, codificare UTF-8. • Chei de registru: ✓ *HKLM\SYSTEM\CurrentControlSet\Services\Tinky* → serviciu Windows creat pentru persistență. ✓ Modificări în *Run* sau *RunOnce* (HKCU/HKLM) dacă este injectat sub formă de DLL loader. • Procese/injectări: ✓ Prezența DLL-ului injectat în procese de încredere (explorer.exe, chrome.exe, winlogon.exe).

<table>
<tr><td></td><td>
✓ Procese cu nume similare celor legitime dar cu locație anormală (de ex. winkey.exe în %TEMP%).
<table>
<tr><th>Indicator</th><th>Type</th><th>Remarks</th></tr>
<tr><td>fe6a696e7012696f2e94a4d31b2f076f32c71d44e4c3cec69a6984ef0b81838a</td><td>Sha256</td><td>svc.exe</td></tr>
<tr><td>7834a64c39f85db5f073d76ddb453c5e23ad18244722d6853986934b750259fd</td><td>Sha256</td><td>winkey.exe</td></tr>
<tr><td>eb6752e60170199e4ce4d5de72fb539f807332771e1a668865aac1eee2c01d93</td><td>Sha256</td><td>keylogger.dll</td></tr>
</table>
</td></tr>
<tr><td>Posibil Impact în Organizații</td><td>
• Scoaterea din uz a EDR-urilor basic: metodele stealth îl fac dificil de detectat de soluții AV clasice.
• Furt de credențiale critice: parole VPN, RDP, domeniu Active Directory.
• Riscuri extinse: Escaladare laterală (lateral movement) după compromiterea inițială.
</td></tr>
<tr><td>Implicare și Recomandări</td><td>
• Amenințare ridicată în medii enterprise: TinkyWinkey este ideal pentru furt de credențiale și informații sensibile cu scop de spionaj.
• Metode de detecție recomandate:
✓ Monitorizarea serviciilor Windows noi/neobișnuite;
✓ Verificarea injectărilor DLL în procese legitime;
✓ Detectarea hook-urilor la nivel de tastatură și activități neobișnuite de logare în fișiere temporare.
• Mitigare:
✓ Limitarea privilegiației – evitarea executării cu drepturi administrative;
✓ Segmentarea și securizarea procesului de servicii și desktop;
✓ Politici stricte de control al aplicațiilor (WDAC, Application Control) și audit EDR sensibile la aceste tactici.
</td></tr>
<tr><td>Referință</td><td>
https://securityonline.info/tinkywinkey-a-stealthy-new-keylogger-is-hunting-for-credentials-on-windows/?utm_source=chatgpt.com
https://www.cyfirma.com/research/tinkywinkey-keylogger/?utm_source=chatgpt.com
</td></tr>
</table>