Tehnica ClickFix Captcha în Campanii de Ransomware

Context General	• O nouă metodă de livrare malware, denumită *ClickFix Captcha*, a fost observată recent în campanii active de ransomware. • Această tehnică implică utilizarea pagini false de tip *CAPTCHA* pentru a păcăli utilizatorii să dea clic și să ruleze executabile malițioase. • A fost observată în special în atacuri de tip *drive-by download*, în cadrul unor site-uri compromise sau clonate.
Modul de funcționare al ClickFix Captcha	**1. Scenariu de atac:** • Utilizatorul accesează un site compromis. • Este întâmpinat cu o pagină *CAPTCHA* falsă, ce afișează un mesaj gen: • "***Click 'Allow' to verify you're not a robot***" sau "ClickFix required for browser compatibility." • Clicul declanșează descărcarea unui fișier executabil (ex: ***.scr***, ***.exe*** sau ***.js***) care conține loader-ul ransomware. • *Malware*-ul este executat fie imediat, fie printr-o secvență scriptată *JavaScript* sau *PowerShell*, pentru a ocoli protecțiile browserului. 2. **Tehnici implicate:** • Obfuscare *JavaScript* • Bypass *SmartScreen* / *Defender* prin renumire fișier, loader cu delay sau folosirea ***mshta.exe*** • Living off the land binaries (LOLBins) pentru execuție silențioasă
Tipuri de ransomware asociate	**1.** Observate în combinație cu familii ransomware cunoscute: • STOP/Djvu • Phobos • BlackCat (ALPHV) în unele cazuri mai sofisticate **2.** Ransomware-ul criptează fișiere locale și de rețea, apoi afișează o notă de răscumpărare (.txt sau HTML)
IOC	**1.** Domenii folosite pentru CAPTCHA fake: • ***verify-me.clickfix[.]site*** • ***captcha-fix[.]top*** **2.** Hashuri fișiere: • ***2a14fbe3198c43f2e9d6c0ed2c7cc02a (MD5)*** **3.** Căi de execuție comune: • ***%APPDATA%\clickfix.exe*** • ***%TEMP%\fixverify.scr***
Comportament post-infectare	După infectarea cu loader-ul ransomware, sunt frecvent observate acțiuni automate precum: **1.** Ștergerea shadow copies cu comenzi gen: • ***vssadmin delete shadows /all /quiet*** **2.** Dezactivarea *Windows Defender* sau modificarea politicilor cu *PowerShell*

	3. Persistență prin *Registry Run keys* (***HKCU\Software\Microsoft\Windows\CurrentVersion\Run***). **4.** Căutare și criptare a fișierelor în directoare: • ***Desktop***, ***Documents***, ***Downloads***, rețele mapate (***Z:***, ***\\fileserver\...)***
Detecție în medii enterprise (SIEM & EDR)	**1.** Loguri și evenimente suspecte: • Execuție ***.scr*** din ***%TEMP%*** • ***mshta.exe*** sau ***rundll32.exe*** apelând URL-uri externe • Activități PowerShell cu obfuscare ***(-w hidden -enc ...)*** • Conectivitate către domenii necunoscute imediat după clic **2.** Se pot seta alerte personalizate în SIEM pentru: • Programe care rulează imediat după eveniment click în browser • Fișiere necunoscute executate la câteva secunde după descărcare
Checklist de protecție rapidă	**1.** Filtrare DNS și blocare domenii suspecte **2.** Dezactivare .scr ca extensie executabilă (prin GPO) **3.** Limitarea execuției din %TEMP%, %APPDATA% **4.** Implementare EDR cu rulesets MITRE T1059 și T1204 **5.** Back-up offline zilnic/verificat
Redomandări	https://cybersecuritynews.com/clickfix-captcha-technique-ransomware/