Distribuirea malware-ului Noodlophile Stealer & XWorm prin site-uri AI false

<table>
<tr><td>Descriere</td><td colspan="4">Gruparea APT denumită ViciousTrap desfășoară o campanie avansată de spionaj cibernetic prin compromiterea routerelor expuse public. Atacatorii transformă aceste dispozitive în honeypot-uri false, simulate pentru a atrage trafic legitim și a intercepta comunicații. Metoda implică manipularea serviciilor de rețea și a configurațiilor DNS fără a instala malware tradițional, ceea ce îngreunează detecția. Scopul principal este monitorizarea activităților rețelelor vizate și colectarea de date sensibile într-un mod discret și persistent.</td></tr>
<tr><td>Etapele atacului</td><td colspan="4">• Scanarea routerelor expuse public – folosind motoare ca Shodan pentru a găsi dispozitive slab securizate.
• Acces inițial – exploatarea vulnerabilităților cunoscute sau parole implicite.
• Manipularea traficului – configurarea routerului pentru a intercepta și redirecționa traficul spre infrastructura controlată de atacator.
• Crearea honeypot-urilor false – se simulează servere sau servicii legitime pentru a atrage anumiți utilizatori sau atacatori reali.
• Colectarea datelor – capturi de trafic, date de autentificare, comportamente de rețea.</td></tr>
<tr><td rowspan="8">Vulnerabilități și Versiuni Software Vizate</td><td>Vendor</td><td>Model/Platformă</td><td>Versiuni afectate (exemplu)</td><td>Vulnerabilitate relevantă</td></tr>
<tr><td>MikroTik</td><td>RouterOS</td><td>< 6.49.7</td><td>CVE-2018-14847 (Winbox), CVE-2023-32154 (WebFig RCE)</td></tr>
<tr><td>TP-Link</td><td>Archer C50 / WR841N / alte modele SOHO</td><td>firmware < 2022</td><td>Diverse RCE și bypass-uri de autentificare (CVE-2021-41653, CVE-2021-31755)</td></tr>
<tr><td>Netgear</td><td>R6700, R7000, Nighthawk series</td><td>firmware < v1.0.9.88</td><td>CVE-2020-26919, CVE-2021-34991 – Auth Bypass și buffer overflow</td></tr>
<tr><td>Cisco (Linksys Small Business)</td><td>RV Series, E900, EA2700</td><td>firmware < 1.0.07.02</td><td>CVE-2022-20825, CVE-2020-3297 (comandă la distanță fără autentificare)</td></tr>
<tr><td>D-Link</td><td>DIR-600, DIR-816, alte SOHO</td><td>firmware < 2021</td><td>CVE-2020-25078, CVE-2021-21807 – DNS hijacking și backdoor</td></tr>
<tr><td>Huawei</td><td>HG532, EchoLife</td><td>firmware pre-2019</td><td>Exploatare Telnet/FTP activ implicit, CVE-2017-17215</td></tr>
<tr><td>Zyxel</td><td>USG/ZyWALL, NBG, VMG</td><td>firmware < 4.60 sau < V5.21(ABWC.0)</td><td>CVE-2020-29583, CVE-2022-30525 – Pre-auth RCE</td></tr>
<tr><td rowspan="4">Atribuție și Context Grup</td><td colspan="2">Secțiune</td><td colspan="2">Informație</td></tr>
<tr><td colspan="2">Nume grup</td><td colspan="2">ViciousTrap</td></tr>
<tr><td colspan="2">Tip atacatori</td><td colspan="2">APT (Advanced Persistent Threat) necatalogat anterior</td></tr>
<tr><td colspan="2">Obiectiv primar</td><td colspan="2">Spionaj cibernetic și monitorizare prin infrastructură de rețea compromisă</td></tr>
</table>

Distribuirea malware-ului Noodlophile Stealer & XWorm prin site-uri AI false

	Ținte posibile	Organizații guvernamentale, companii din energie, telecom, apărare, *ISP*
	Geolocalizare probabilă	Neatribuit public, dar se suspectează regiuni cu infrastructură Eurasia/Sud-Est Asiatică
	Tactică principală	Compromiterea routerelor pentru a transforma dispozitivele în honeypot-uri false
	Scop	Supraveghere, interceptare trafic, culegere de informații
	Dispozitive țintite	Routere vulnerabile (inclusiv modele *SOHO*)
	Tehnici folosite	Manipularea *DNS*, rerutarea traficului, spoofing de servicii (ex: *SSH, FTP, HTTP*), uneori fără implicarea *malware*
	Persistență	Se mențin prin modificarea configurațiilor la nivel de firmware sau rutare
	Indicatori activitate	Routerele încep să servească pagini web false, să redirecționeze traficul sau să răspundă la porturi neobișnuite
Vectori de acces și Tehnici MITRE ATT&CK	**Tactică**	**Tehnică MITRE ATT&CK**
	Inițializare acces	[T1190] Exploit Public-Facing Application
	Persistență	[T1053.005] Scheduled Task/Job: Embedded Script sau [T1547.001] Boot or Logon Autostart Execution
	Evitarea detecției	[T1027] Obfuscation of configuration, [T1036] Masquerading
	Colectare informații	[T1040] Network Sniffing
	Exfiltrare	[T1041] Exfiltration Over C2 Channel
	Command and Control	[T1071.001] Web Protocols sau [T1090.003] Multi-hop Proxy (folosind routere drept relay)
Indicatori de Compromitere (IoCs)	**Tip**	**Exemplu**
	IP C2 suspect	***185.203.118.22***
	Hostname fals	***router-management.ddns.net***
	Servicii emulate	SSH (port 22), HTTP (port 80), Telnet (port 23), FTP (port 21)
	DNS modificat	DNS server setat spre ***203.0.113.55*** în routerele compromise
	Hashes (fișiere injectate)	***SHA256: bdf56eaa...*** (simulat)
Măsuri de protecție	• Actualizarea firmware-ului tuturor routerelor. • Dezactivarea serviciilor WAN inutile (ex: administrarea la distanță). • Schimbarea parolelor implicite și implementarea autentificării multifactor. • Monitorizarea activă a configurației DNS și a rutelor dinamice. • Implementarea de IDS/IPS pentru detecția rerutărilor neautorizate.	
Referință	https://securityonline.info/vicioustrap-new-cyber-espionage-group-hijacks-routers-for-honeypot-surveillance/	