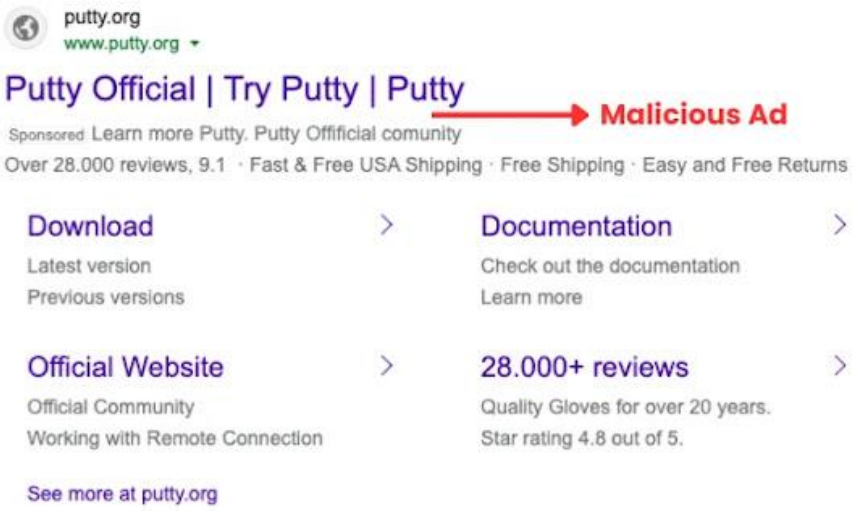
Versiuni Trojanizate ale PuTTY și WinSCP

Descriere	Recent, s-a descoperit că *versiuni compromise* ale aplicațiilor PuTTY și WinSCP sunt folosite de actori cibernetici pentru a obține acces la rețeaua internă. Vă rugăm să nu instalați aplicații din surse neoficiale, chiar dacă par a fi utile sau vă sunt recomandate într-un context de angajare. Contactați imediat echipa IT pentru verificare.	
Detalii tehnice	**Caracteristică**	**Descriere**
	Vector de atac	Inginerie socială – victimele sunt atrase prin campanii de recrutare IT și instruite să descarce versiuni modificate ale aplicațiilor
	Aplicații compromise	PuTTY și WinSCP (modificate)
	Comportament malițios	- Executarea unui shellcode - Comunicarea cu server C2 - Instalarea backdoor-ului AIRDRY.V2
	Payload final	AIRDRY.V2, un malware utilizat de Lazarus pentru control la distanță
	Metoda de execuție	Într-un fișier aparent benign este integrat un cod shell malițios care, odată executat, instalează malware-ul
	Persistență	Stabilită prin backdoor; permite comenzi de la distanță și persistă în sistem
	Tehnici de evitare a detecției	Obfuscare a codului, folosirea de aplicații legitime cu trojan, semnături valide aparent
Ținte vizate	• Profesioniști în domeniul IT • Companii din domenii strategice • Instituții sensibile • Persoane care caută locuri de muncă în domeniul IT (simulări de interviuri)	
IOCs	• Domenile trojanizate de evitat: ✓ puutty[.]org (typosquat PuTTY) ✓ puttyy[.]org, ✓ putyy[.]org, ✓ puttty[.]org ✓ winnscp[.]net, vvinscp[.]net ✓ updaterputty[.]com ✓ zephyrhype[.]com ✓ putty[.]run ✓ putty[.]bet • Fake PuTTY Hash MD5: f42dae36a47882391da920ce56f497b8, Signed by "GALVIN & ASSOCIATES LLC"	

Indicatorii la care tragem atenția	
Remediere	• Blocarea filtrarea DNS/Blocare imediată pe domeniile malițioase. • Blocare imediată a executabilelor malițioase. • Inventarierea instanțelor de PuTTY/WinSCP instalate. • Audit de conectări SSH/SCP din ultimele 30 zile. • Resetare parole SSH dacă s-a folosit credential harvesting. • Scanare endpointuri afectate (EDR, AV, manuală).