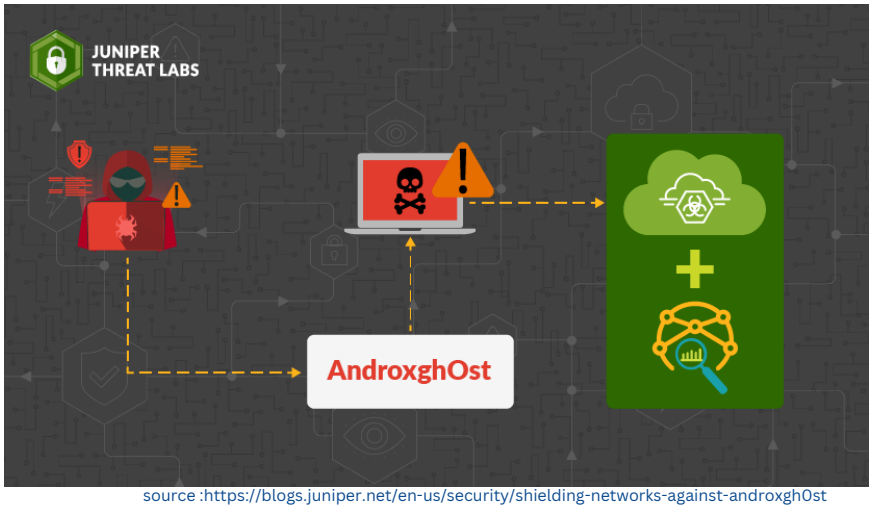
Raport consolidat eveniment cibernetic

AndroxGh0st malware



source :https://blogs.juniper.net/en-us/security/shielding-networks-against-androxgh0st

Informații suplimentare

Descriere tehnică	**AndroxGh0st** este un malware script Python conceput pentru a viza fișierele **.env** care conțin informații sensibile în aplicațiile web. Acest malware face parte dintr-o operațiune de tip botnet care are ca scop în primul rând să fure credențialele și să abuzeze de alte funcții, cum ar fi Simple Mail Transfer Protocol (SMTP), interfețele de programare a aplicațiilor (API), implementarea web shell, lansarea atacurilor DDoS și chiar pentru a implementa ransomware. Malware-ul AndroxGh0st adesea abuzează vulnerabilitățile cunoscute, cum ar fi: • **CVE-2017-9841** - Vulnerabilitate permite adversarilor să execute comenzi arbitrare în serviciul web țintă prin trimiterea de cereri HTTP POST rău intenționate către PHPUnit. • **CVE-2018-15133** - Vulnerabilitatea permite adversarilor să execute comenzi arbitrare de la distanță utilizând valori XSRF. • **CVE-2021-41773** - Vulnerabilitatea permite atacatorilor neautentificați să execute cod arbitrar și să dezvăluie informații sensibile despre sistemele vulnerabile. Întrucât vulnerabilitatea poate fi exploatată de la distanță și nu necesită un administrator sau un cont privilegiat, gravitatea acesteia este critică.

File Samples:	• f6f240dc2d32bfd83b49025382dc0a1cf86dba587018de4cd96df16197f05d88 • 3b04f3ae4796d77e5a458fe702612228b773bbdefbb64f20d52c574790b5c81a • 23fc51fde90d98daee27499a7ff94065f7ed4ac09c22867ebd9199e025dee066 • 6b5846f32d8009e6b54743d6f817f0c3519be6f370a0917bf455d3d114820bbc • bb7070cbede294963328119d1145546c2e26709c5cea1d876d234b991682c0b7 • ca45a14d0e88e4aa408a6ac2ee3012bf9994b16b74e3c66b588c7eabaaec4d72 • 0df17ad20bf796ed549c240856ac2bf9ceb19f21a8cae2dbd7d99369ecd317ef
Practici bune pentru protejarea împotriva amenințărilor împotriva AndroxGh0st	1. **Actualizări regulate:** Asigurați-vă că toate sistemele de operare sunt actualizate. 2. **Patching prioritar:** Concentrați-vă pe patch-urile vulnerabilităților exploatate cunoscute în sistemele de internet, inclusiv ***CVE-2017-9841, CVE-2018-15133 și CVE-2021-41773.*** 3. **Dezactivați modul Debug:** Asigurați-vă că aplicațiile Laravel nu sunt în modul de depanare sau testare, care poate expune informații sensibile. 4. **Eliminați acreditările Cloud:** Eliminați toate acreditările cloud din fișierele ***.env*** și revocați-le. Utilizați metode mai sigure furnizate de furnizorii de cloud pentru acreditări temporare. 5. **Criptarea informațiilor sensibile:** Criptarea informațiilor sensibile, cum ar fi ***cheile API*** și acreditările, în special în fișiere precum .env. 6. **Îmbunătățiți securitatea contului:** Implementați autentificarea cu mai mulți factori (MFA) pentru a îmbunătăți securitatea contului. 7. **Securitatea rețelelor**: Implementați măsuri robuste de securitate a rețelei, inclusiv ***IDS,*** pentru a detecta și a bloca activitățile rău intenționate. 8. **Firewall-uri:** Utilizați firewall-uri pentru a monitoriza și controla traficul de rețea de intrare și de ieșire pe baza unor reguli de securitate predeterminate. 9. **Scanările sistemului:** Scanați în mod regulat sistemul de fișiere al serverului pentru fișiere PHP necunoscute, în special în folderul ***/vendor/phpunit/phpunit/src/Util/PHP.*** 10. **Monitorizați cererile de ieșire:** Examinați solicitările GET de ieșire către site-uri de găzduire a fișierelor, cum ar fi ***GitHub, Pastebin*** etc., în special atunci când accesați un fișier .php.

Detectarea AndroxGh0st	1. **Activitate de rețea anormală:** ◦ Creșteri masive de trafic ieșit sau modele de trafic neobișnuite către IP-uri sau domenii necunoscute. ◦ Conexiuni externe neașteptate inițiate de dispozitive. 2. **Comportament suspect al dispozitivelor:** ◦ Consumul anormal de resurse (CPU, memorie) pe dispozitive IoT. ◦ Dispozitive care se repornesc frecvent sau prezintă comportamente neobișnuite. 3. **Încercări de acces neautorizat:** ◦ Atacuri brute-force asupra serviciilor precum Telnet, SSH sau interfețe web. 4. **Analiza jurnalelor (logs):** ◦ Jurnale care indică multiple eșecuri de autentificare sau conexiuni către IP-uri suspicioase.

Resurse externe

	https://www.lacework.com/blog/androxghost-the-python-malware-exploiting-your-aws-keys
	https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/androxgh0st-malware-everything-you-need-to-know/