Raport consolidat eveniment cibernetic

Informații suplimentare

Denumire	**BABAR**
Tip	Remote Access Trojan
Grup asociat	EvilBunny SNOWBALL
Descriera	Barbar este un RAT (Troian Acces de la Distanță) cu caracteristici comune pentru acest tip de malware ca: • code execution • code injection • furtul de fișiere. Cu toate acestea el mai are și caracteristici suplimentare: • key logger pentru a înregistra cheilor de rigistru • furtul conținutul clipboard (frecvent utilizat pentru a stoca parole) • asculte conversațiilor și înregistrarea lor utilizând bibliotecile dsound și winmm. Datele sunt stocate, de obicei, în fişier: **%COMMON_APPDATA%\MSI\update.msi.**
Simptomele	• Performanță lentă • Prezența fișierelor adăugate sau modificate • Modificări ale setărilor desktop • Congelare sau cracare • Spațiu de depozitare diminuat
MITRE ATT&CK techniques	• T0834 - Native API • T0842 - Network Sniffing • T0846 - Remote System Discovery • T0802 - Automated Collection

Etapele de instalare	1. Malware-ul utilizează în principal **code injection**, care permit rularea codului în contextul de încredere al unui alt proces. 2. Odată instalat, Barbar încearcă să modifice modul de gestionare a erorilor al procesului pentru a putea trata următoarele tipuri de erori: **SEM_NOOPENFILEERRORBOX SEM_NOGPFAULTERBLOCK, SEM_FAILCRITICALRORS.** Astfel, dacă apare oricare dintre erori el se autodistruge. 3. Următoarea etapă este tentaivă de a obține privilegii de depanare și verifică. Dacă versiunea este >= **Windows Vista** și ID-ul platformei este **VER_PLATFORM_WIN32_NT** malware încearcă să creeze un fișier numit **event.log** în folderul **%ALLUSERSPROFILE**. care duce la crearea următorului fișier: **C:\ProgramDataevent.log** Dacă nu încearcă să obțină calea folderului local **AppData**. Aceste date sunt utilizate pentru a crea următoarele fișiere: **C:\Users\AppData\Roaming\Microsoft\wmimgnt.dll C:\Users\AppData\Roaming\Microsoft\wmimgnt.exe** 4. Malware încearcă să șteargă orice urmă prin ștergerea intrărilor din următoarele chei de registru: **HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache\ HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache** 5. La final se creează un proces suspendat de Internet Explorer și injectează DLL-ul de sarcină utilă prin metoda **CreateRemoteThread()**.
IOC	**IP**: De obicei IP dinamice, care se schimbă frecvent. **URL:** De obicei folosește domenii temporare sau domenii generice pentru a evita detecția rapidă. **Porturi:** De obicei folosește porturile standarde pentru HTTP și HTTPS
Identificarea originii și caracteristicilor	• Eroare tipografică comisă de autorii este ca în loc să folosească șirul MSIE (MicroSoft Internet Explorer), malware-ul folosește șirul **MSI**. • ID-ul de limbă al resursei de informații despre versiune este **1036**, care înseamnă limba franceză. • Interfața de comandă și control este în limba engleză, dar alegerea cuvintelor nu este tipică pentru un vorbitor nativ de limba engleză. Exemplu: !**!!EXTRAGE EROARE!!!File Does Not Exists->[%s]** • Barbar utilizează obfuscarea API pentru a face analiza mai complicată. Scopul este de a executa un Microsoft Windows API fără a-l numi. Atunci când malware-ul trebuie să execute o funcție externă utilizează un **“HASH”** în loc să utilizeze numele funcției. “HASH”-ul este furnizat unei funcții interne, această funcție stabilește relația dintre “HASH” și adresa funcției. La final, adresa este executată.