UNIVERSITATEA „CONSTANTIN BRÂNCUŞI” DIN TÂRGU - JIU

FACULTATEA DE ŞTIINŢE ECONOMICE

Domeniul: Cibernetică, Statistică și Informatică Economică

Program de studii: **Informatică Economică**

Top malware 2022 - Gh0st

Disciplina: Informatică Economică

STUDENT:

Udrescu Vlad-Mihai

Târgu Jiu, 2024

Cuprins

Introducere

În era digitală, tehnologia a evoluat rapid, oferind beneficii semnificative, dar aducând și riscuri sporite în materie de securitate cibernetică. Unul dintre aceste riscuri majore este reprezentat de malware, programe malefice care vizează compromiterea sistemelor informatice și furarea datelor sensibile. În anul 2022, peisajul securității cibernetice a fost marcat de apariția și răspândirea unui malware deosebit de periculos, cunoscut sub numele de Gh0st.

Gh0st, un troian de acces remote (RAT), și-a făcut simțită prezența ca o amenințare persistentă și sofisticată, reușind să evadeze sistemele de securitate convenționale și să compromită sisteme informatice la nivel global. Această prezentare se va concentra asupra descrierii succinte a acestui malware notoriu, evidențiind caracteristicile sale distinctive, modurile de răspândire și impactul devastator asupra securității cibernetice.

1. Descrierea Malware-ului Gh0st

Gh0st nu este doar un simplu program malefic; este un instrument de atac complex și rafinat, conceput pentru a prelua controlul complet al sistemelor infectate. A fost pentru prima dată identificat în 2008, și de atunci, a evoluat continuu, adaptându-se la tehnologiile de securitate în schimbare și devenind tot mai dificil de identificat și eliminat.

2. Caracteristici și Moduri de Răspândire

RAT-ul Gh0st utilizează diverse tactici pentru a se răspândi și a infecta sistemele. Atacatorii recurg frecvent la campanii de phishing, în care utilizatorii sunt induși în eroare pentru a descărca fișiere infectate, crezând că sunt legitime sau inofensive. De asemenea, exploatează vulnerabilitățile cunoscute ale software-ului neactualizat pentru a-și instala discret prezența.

3. Funcționalități Distructive

Gh0st este cunoscut pentru funcționalitățile sale extrem de distructive. Printre acestea se numără capturarea tastelor, monitorizarea activității pe ecran, accesul la camera web și microfon, precum și transferul de fișiere între sistemul infectat și serverul de comandă și control al atacatorilor. Aceste capabilități îi permit atacatorului să obțină control complet asupra sistemului și să acceseze informații sensibile fără cunoștința utilizatorului.

4. Măsuri de Protecție și Prevenție

Pentru a se apăra împotriva amenințărilor cauzate de Gh0st și malware-uri similare, organizațiile și utilizatorii trebuie să adopte măsuri preventive robuste. Acestea includ actualizarea regulată a software-ului, utilizarea soluțiilor de securitate avansate, educație și conștientizare în rândul utilizatorilor și implementarea unor politici stricte de securitate cibernetică.

Concluzie:

În concluzie, Gh0st se afirmă ca o amenințare persistentă în peisajul securității cibernetice din 2022, evidențiind necesitatea unei abordări proactive și comprehensive pentru protejarea datelor și sistemelor informatice. Acest malware, prin funcționalitățile sale sofisticate și modurile subtile de răspândire, subliniază importanța educației în privința securității cibernetice, implementării măsurilor de protecție avansate și menținerii unui ritm constant de actualizare a sistemelor.

Pentru a contracara amenințările continue ale malware-urilor precum Gh0st, organizațiile trebuie să investească în soluții de securitate inovatoare, să consolideze eforturile de conștientizare a utilizatorilor și să creeze strategii de gestionare a vulnerabilităților. Numai printr-o abordare holistică și colaborativă a securității cibernetice se pot asigura organizațiile și indivizii împotriva impactului devastator al acestor amenințări evolutive în peisajul tehnologic în continuă schimbare.

Bibliografie

- https://www.cisecurity.org/insights/blog/top-10-malware-december-2022
- https://en.wikipedia.org/wiki/Gh0st_RAT
- https://malpedia.caad.fkie.fraunhofer.de/details/win.ghost_rat
- https://medium.com/@huntressofthreats/unmasking-the-gh0st-a-comprehensive-guide-to-threat-hunting-e4ab7f1f3e5b
- https://cofense.com/blog/open-source-gh0st-rat-still-haunting-inboxes-15-years-after-release
- https://www.fortiguard.com/encyclopedia/ips/38503
- https://resources.infosecinstitute.com/topics/malware-analysis/gh0st-rat-complete-malware-analysis-part-1/