REPORT ANALISI MALWARE

Data analisi: 25 Agosto 2024

SHA256:
0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
Nome file: Jvczfhe.exe

COMPORTAMENTO OSSERVATO:

1. Catena di Infezione:

- Il malware viene scaricato tramite Firefox da GitHub
- Dopo l'esecuzione, il malware scarica e lancia un secondo file eseguibile (Muadnrd.exe)

2. Attività Sospette:

- Utilizzo di CMD.EXE per eseguire comandi
- Usa TIMEOUT.EXE per ritardare l'esecuzione
- I processi principali (Jvczfhe.exe e Muadnrd.exe) crashano dopo l'esecuzione
- Disabilita i log di tracciamento
- Lettura delle impostazioni di Internet Explorer
- Verifica delle impostazioni di sicurezza di Windows
- Connessioni a porte non standard (7702)

3. Comunicazioni di Rete:

- Connessione a dominio DuckDNS (egehgdehjbhjtre.duckdns.org:7702)
- Multiple richieste DNS sospette
- Connessioni HTTP/HTTPS a vari domini
- Tentativi di connessione tramite InstallUtil.exe

4. Persistenza:

- Modifica chiavi di registro
- Verifica delle impostazioni di sicurezza
- Lettura di chiavi di registro relative a Microsoft Office

5. Evasione:

- Utilizzo di .NET Reactor come protector
- Disabilitazione dei log di sistema
- Uso di timer per ritardare l'esecuzione

INDICATORI DI COMPROMISSIONE (IoC):

- Domain: egehgdehjbhjtre.duckdns.org
- IP: 91.92.253.47:7702
- File: Jvczfhe.exe (SHA256: 0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0)
- File: Muadnrd.exe (droppato durante l'esecuzione)

VALUTAZIONE RISCHI:

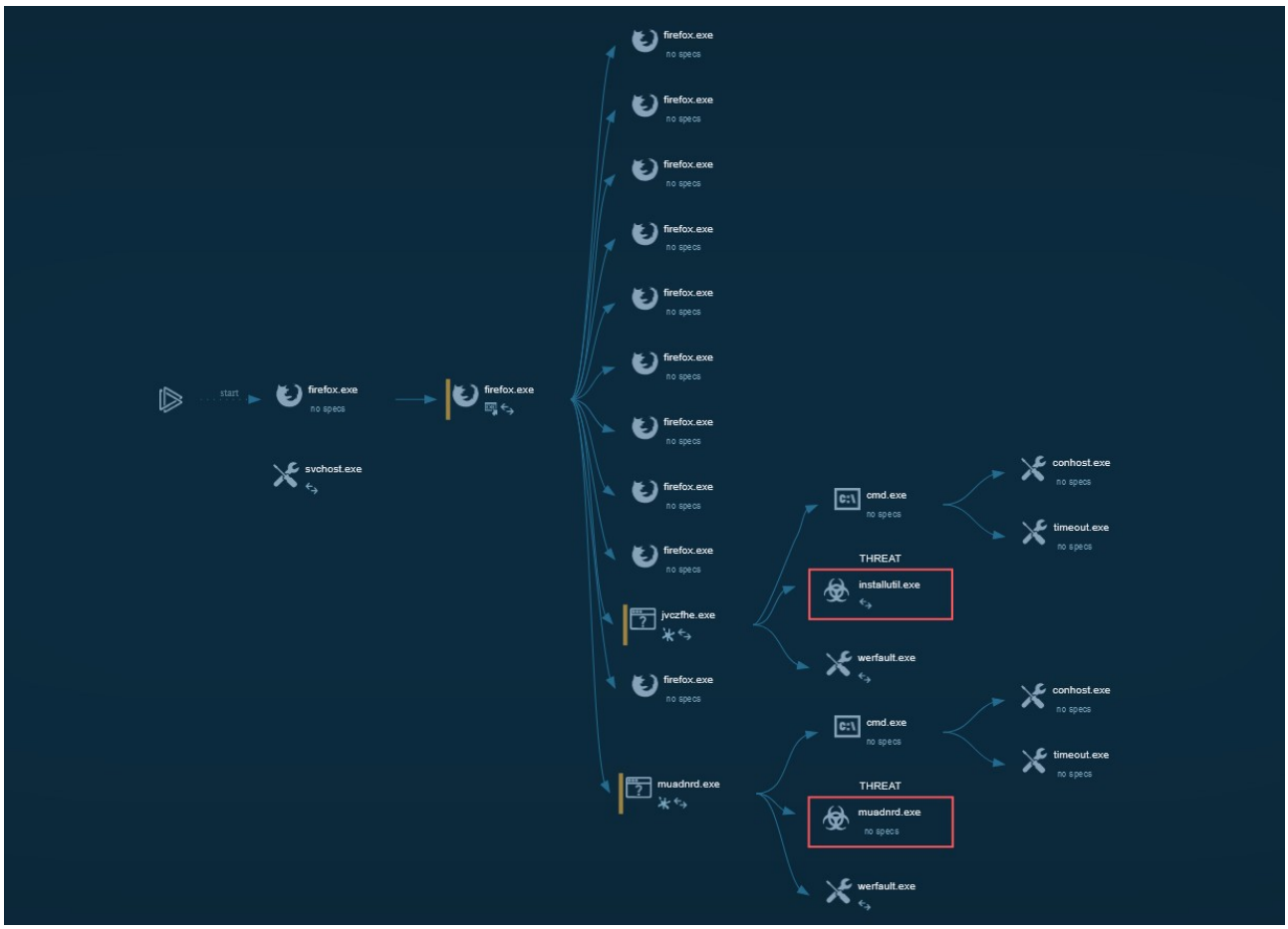
Il malware mostra caratteristiche di:

- Download e esecuzione di payload secondari
- Comunicazioni con C2 tramite DuckDNS
- Tentativi di persistenza nel sistema
- Tecniche anti-analisi e anti-debug
- Comportamento da dropper/downloader

RACCOMANDAZIONI:

1. Bloccare comunicazioni verso il dominio DuckDNS identificato
2. Monitorare attività sospette di InstallUtil.exe
3. Controllare modifiche al registro di sistema
4. Monitorare creazione di processi cmd.exe inattesi
5. Implementare regole di rilevamento basate sugli IoC identificati

Il comportamento osservato suggerisce che si tratta di un dropper/downloader utilizzato come primo stadio di un'infezione più complessa, probabilmente parte di una campagna di malware più ampia.


start
firefox.exe
no specs
firefox.exe
svchost.exe
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
jvczfhe.exe
firefox.exe
no specs
muadnrd.exe
cmd.exe
no specs
conhost.exe
no specs
timeout.exe
no specs
THREAT
installutil.exe
werfault.exe
cmd.exe
no specs
conhost.exe
no specs
timeout.exe
no specs
THREAT
muadnrd.exe
no specs
werfault.exe