LokiRAT

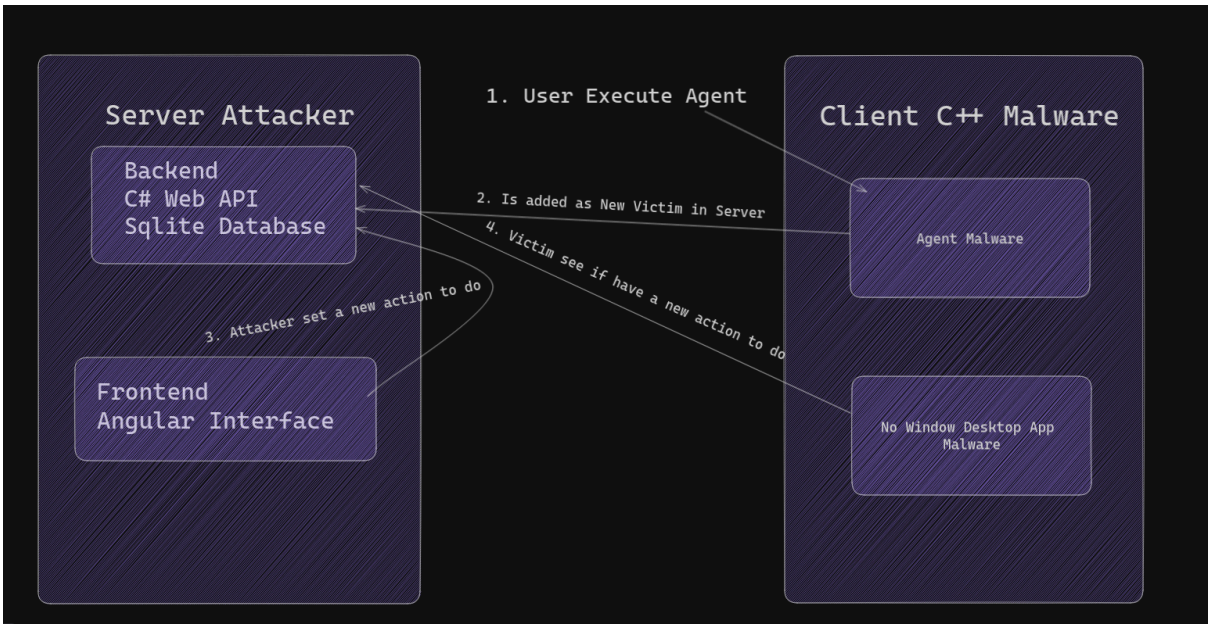
Technologies

- C# Web API (Server Backend)
- Angular Web Client
- Sqlite Database (Backend)
- Agent
- C++ Malware (Victim/Client EXE)
- Victim malware GUI app without window

FlowCode

User create in angular web panel a agent (EXE) to execute for first time in victim PC.
Victim execute the EXE agent in her Windows OS.
A new victim is stored in Backend Database and visible in attacker web panel.
Now you have the victim captured, you can order any action in victim OS.
The victim is constantly searching if they need to do a new action.

Excalidraw:



Features

For sure:

- Hide Files & Directories from **explorer.exe**
- Hide Services
- Hide Processes from **Task Manager**
- Hide Registries from **regedit.exe**
- Undetectable Network Connection
- TimeStomping

- Windows Defender Killer
- Create Scheduled Tasks
- DLL Injection
- List Processes
- Command Execution
- System Enumeration
- Find RWX Memory Regions
- PEB Parameter Manipulation
- PEB Module Manipulation
- Shellcode Execution with NinjaInjector (without VirtualAlloc + CreateRemoteThread)
- Encrypt Memory Addresses with SystemFunction033
- Decrypt Memory Addresses with SystemFunction033
- Set No Access to Memory Region
- Create New Process with PPID Spoofer
- Downloader (Encrypt network file packet)
- Execute Function in Remote Process (rtlremotecall)
- Install a EXE as Service
- Persistence to RAT Process
- Persistence to Remote Process
- Keylogger
- Dump lsass.exe
- Privilege Escalation (Execute EXE as Administrator)
- Shellcode Encryption
- Shellcode Decryption
- File Transfer
- CMD Spoofing
- Unhook AV hooks (Perun Farts) in Remote Process
- Patch ETW in Remote Process
- File Hider with ADS (https://medium.com/@s12deff/file-hider-c-malware-development-class-60942f012051)
- Hide Trace
- rdp credential stealer https://github.com/S12cybersecurity/RDPCredentialStealer
- Security Solutions Detector

I wish:

- Remote Desktop
- Screenshot taker
- Threat Hijacking with predefined payloads to execute setted as CTX context
- Fake UAC to phishing user password

Evasion

- Unhook AV Hooks (Perun Farts)
- ETW Patch
- VirtualAlloc Function Evaded (https://medium.com/@s12deff/my-own-virtualalloc-implementation-using-module-stomping-technique-bdb3559490af)
- CreateRemoteThread Function Evaded (Threat Hijacking: or - Enum Functions)
- CMD Spoofing
- PPID Spoofing
- PEB Manipulation (Parameters + Modules)
- Entropy
- Signature
- AntiDebugging
- Anti VM & Sandbox
- String Crypter
- IAT Evasion
- Firewall Evasion
- Windows Defender Evasion
- AV Evasion
- EDR Evasion

Entity Relationship Diagram

Timeline

1 feature at day = **60 days = 2 months**

12 february - 25 april = 73 total days

49 days (no Friday, Saturday, Sunday)

Less than 1 feature for day.

Is missing Web Client with Angular