Theoretische analyse:

Onderzoek de belangrijkste doelen van hackers bij het inzetten van een Trojan:

Data exfiltratie, toegang verkrijgen en behouden, privilege escalatie, controle over systemen verkrijgen en behouden, financieel gewin, spionage, botnet creëren, educatief hacken.

Waarom en hoe worden Trojans gebruikt?

Er zijn verschillende soorten trojans hier zijn de meest voorkoomende met voorbeelden:

- Backdoor Trojan – Maakt het mogelijk voor een aanvaller om ongeautoriseerde toegang te krijgen tot een geïnfecteerd systeem via een achterdeur. (Vb. NetBus)
- Banker Trojan – Ontworpen voor gebruikers hun financiele accounts te stelen. Het Steelt bankgegevens zoals inloggegevens, pincodes of creditcardnummers. (Vb. ZeuS)
- Ransomware trojan – Encrypteert alle bestanden op een systeem om dan losgeld te vragen voor de decryptie sleutel. (Vb. wannaCry)
- Rootkit Trojan – Zorgt ervoor dat andere malware verborgen blijft door het besturingssysteem of antivirussoftware te manipuleren. (Vb. TDSS, ZeroAccess)
- Infostealing Trojan – Ontworpen om gevoelige gegevens zoals wachtwoorden, bestanden of browsergeschiedenis te stelen. (Vb. Emotet)
- Spy Trojan – ontworpen voor te spioneren op een systeem.
- Downloader Trojan - Ontworpen om andere kwaadaardige bestanden of malware van een externe server te downloaden en te installeren op een geïnfecteerd systeem. (Vb. Nemucod)
- DDoS Trojan - Maakt een geïnfecteerd systeem onderdeel van een botnet voor dan DDoS aanvallen uit te voeren. (Vb. Mirai)

[1]

Trojans kunnen verspreid worden door phishing emails, infected websites, malvertising, of infected USB-sticks. Trojans werken onopgemerkt omdat ze vaak gecamoufleerd zijn als legitieme software zoals een antivirus.

Wat is het verschil tussen een backdoor, een RAT (Remote Access Trojan), en een agent?

Backdoor: Een backdoor is een methode die standaard authenticatie of beveiligingsmaatregelen omzeilt om ongeautoriseerde toegang tot een systeem te krijgen. Het stelt aanvallers in staat om ongemerkt toegang te krijgen tot een systeem. [1]

RAT: Een RAT (remote access trojan) is een type malware dat een aanvaller op afstand volledige controle geeft over een geïnfecteerd systeem. Een RAT maakt het mogelijk om een besmette machine op afstand te besturen, vaak ongemerkt, voor spionage, gegevensdiefstal of andere aanvallen. [1]

Agent: Een agent is een softwarecomponent die specifieke taken uitvoert op een systeem. Een agent verzamelt gegevens, voert opdrachten uit en communiceert met een centrale server die instelt wat de agent moet doen en verzamelen. Een voorbeeld hiervan is de Wazuh agent die wordt gebruikt om end points te monitoren, het controleert op anomalieën en signatures voor intrusions te detecteren. Er zijn ook kwaadaardige agents zoals Cobalt strike beacon, deze agent meldt zich aan bij een C2 server, de aanvaller kan nu configuraties instellen voor de agent om bijvoorbeeld gegevens te stelen. [1]

Hoe past dit in een breder kader van hacking, zoals reconnaissance, privilege escalation, en exfiltratie?

Trojans worden gebruikt om informatie te verzamelen over het netwerk of de gebruiker, zoals IP-adressen of gebruikersnamen. Met een Trojan kan een aanvaller administratorrechten verkrijgen door

kwetsbaarheden te misbruiken. Trojans sturen gestolen gegevens terug naar een command-and-control server van de aanvaller, vaak via versleuteld verkeer. [1]

Technische analyse:

Naam van mijn Trojan: Glitch Gremlin

Maak een overzicht van hoe je Trojan (of Agent) er qua opbouw zal uitzien:

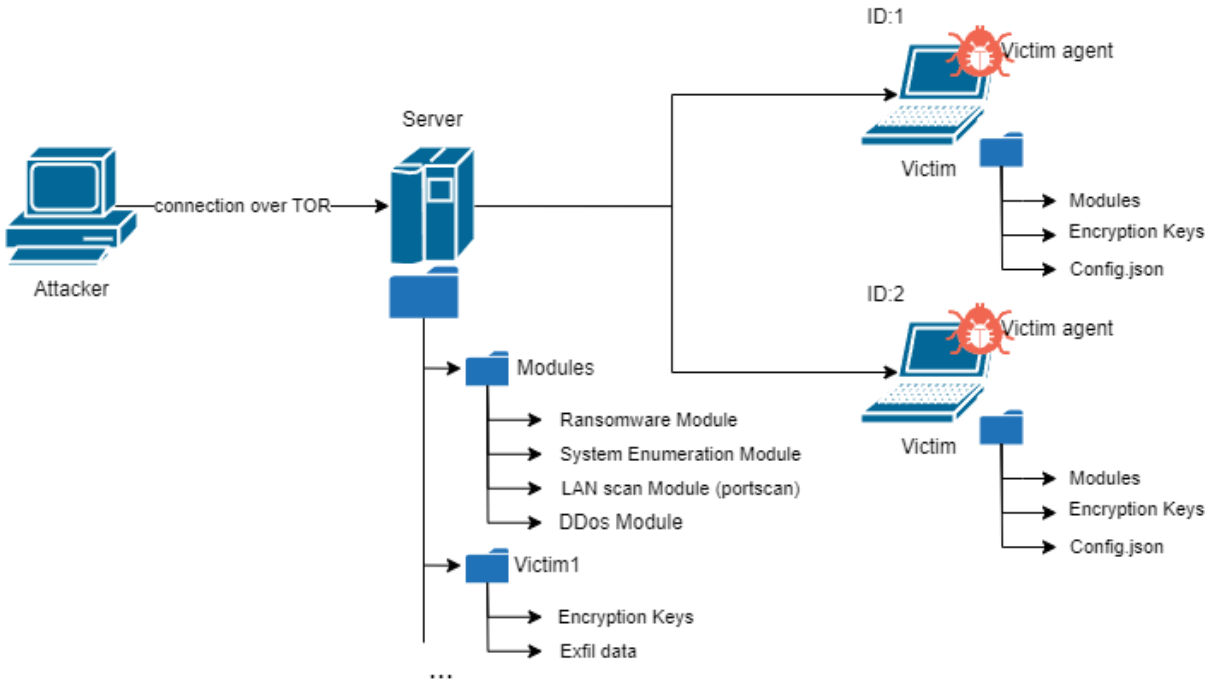

Fig 1.0 Eerste uitwerking Glitch Gremlin Trojan

Kies minimaal drie custom modules en licht toe, Welke functionaliteit hebben deze modules?

- Antivirus module – Een module dat antivirus detecteert
- Ransomware module – Encrypteert alle bestanden en vraagt een ransom voor decryptie
- Tor connect module – Een module dat via TOR connect voor extra stealthy configuratie.
- System Enumeration Module – Verzamelt systeem informatie
- Lan Scan Module – Verzamelt local area network informatie (e.g. voert poortscans uit, host discovery ect.)

Waarom kiezen hackers deze technieken?

Antivirus module: Hackers willen weten of hun malware wordt gedetecteerd door beveiligingssoftware. Door het antivirusprogramma te identificeren, kunnen ze:

- Antivirus omzeilen met specifieke technieken.
- Het gedrag van hun malware aanpassen (bijvoorbeeld het uitschakelen van bepaalde functies die detecteerbaar zijn).

Ransomware module: Het doel van ransomware is financieel gewin. Het versleutelen van bestanden en het eisen van een losgeldbetaling zorgt voor:

- Hoge impact: Slachtoffers hebben vaak geen toegang tot hun bestanden
- Drukmiddel: Hackers vergroten hun kansen op betaling door gevoelige of belangrijke bestanden te versleutelen.
- Hoge winstpotentie: Losgeld wordt vaak geeist in moeilijk traceerbare methodes zoals cryptocurrency (vooral Monero), wat anonimiteit waarborgt.

TOR module: TOR (The Onion Router) biedt anonimiteit en maakt het moeilijker om de aanvaller te traceren. Hackers gebruiken deze techniek om:

Enumeration module: Het verzamelen van informatie over het doelwit stelt hackers in staat om gerichte aanvallen uit te voeren. Deze module helpt bij:

- Begrijpen van de omgeving: Informatie zoals besturingssysteem, hardware, en actieve processen geeft inzicht in kwetsbaarheden.
- Keuze van exploits: Op basis van de verzamelde gegevens kunnen aanvallers exploits selecteren die specifiek zijn voor de omgeving.

LAN scan module: Het scannen van het lokale netwerk geeft hackers toegang tot meer potentiële doelen en informatie. Dit helpt om:

- Aanvalspad te vergroten: Door verbonden apparaten en diensten te identificeren, kunnen hackers meerdere zwakke punten uitbuiten.
- Laterale beweging mogelijk te maken: Aanvallers kunnen van het ene apparaat naar het andere bewegen binnen hetzelfde netwerk.
- Netwerktoegang te analyseren: Informatie over open poorten en actieve hosts geeft hackers strategische inzichten voor verdere aanvallen.

Hoe kunnen ze worden gebruikt in een ethical hacking context?

- Penetratietests: Gebruik de modules om zwakke plekken in antivirus, systeemconfiguraties, en netwerkbeveiliging te ontdekken.
- Red Team Oefeningen: Simuleer een echte aanval om de reactie van een organisatie te testen.
- Blue Team Training: Gebruik de modules om beveiligingsteams te trainen in het herkennen en reageren op aanvallen.

Bronnen

[1] https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus