SPYASTRA

CYBER CRIME INVESTIGATORS TOOLKIT : DEFENSIVE PURPOSE

VIRUSES

RANSOMWARE

TROJAN

DATA ENCRYPTOR

MALWARE

SYSTEM CRASHER

WE WILL NEUTRALIZE CRIMINAL ACTIVITY; ANY USE OF VIRUSES / TOOLS WILL BE STRICTLY LIMITED TO AUTHORIZED DEFENSIVE OPERATIONS CONDUCTED IN FULL COMPLIANCE WITH APPLICABLE LAWS AND ETHICAL STANDARDS.

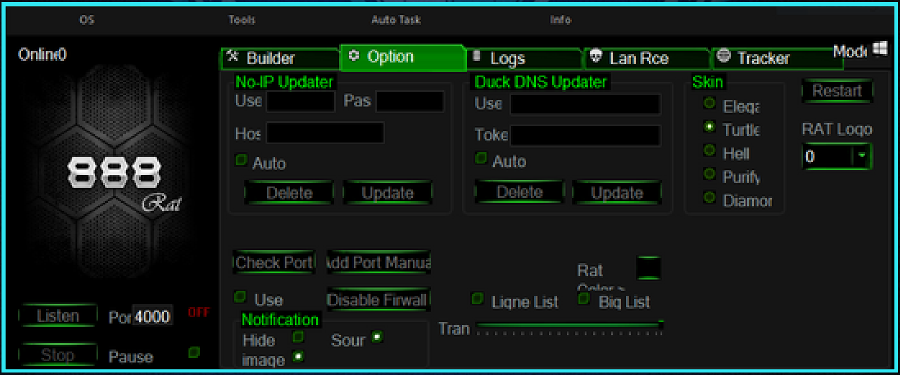
USE ONLY IN ISOLATED LAB ENVIRONMENTS FOR ETHICAL HACKING, RESEARCH, AND DEFENSIVE SIMULATIONS.

Purchase Now | ₹ 1499 /-

888 All in One RAT

CLICK HERE

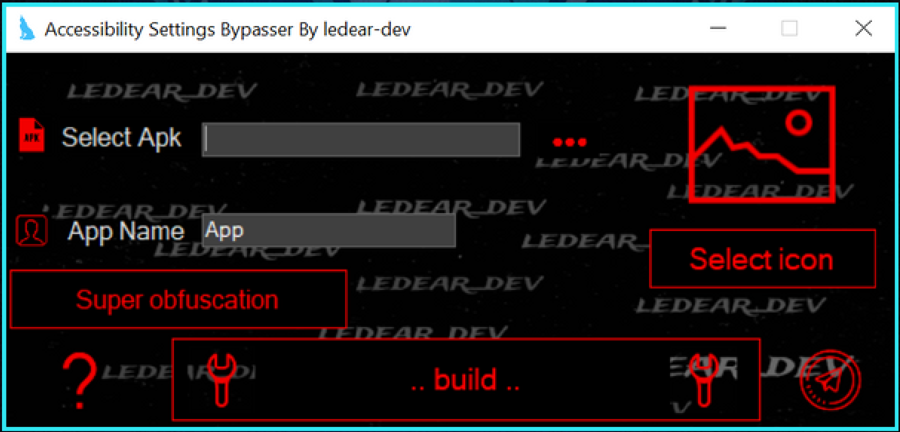
As a cyber-crime investigator: 888 RAT is a remote-access trojan that targets Android (and earlier Windows) devices — it exfiltrates device data, intercepts SMS/calls, records audio, takes screenshots, and gives attackers full remote control.



Accessibility Bypassed

CLICK HERE

As a cyber detective: an accessibility-bypass tool is malware that abuses Android's Accessibility Service to silently grant itself high privileges and automate UI actions — enabling stealthy credential theft, SMS interception, fraudulent transactions, and silent app installs.



Accessibility Settings Bypasser By ledear-dev

Select Apk

App Name: App

Akira Ransomware

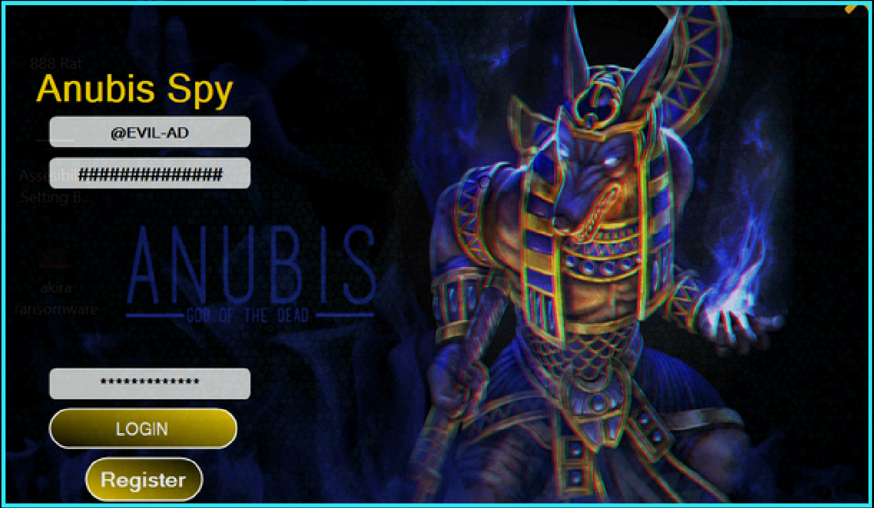
CLICK HERE

When a blackmailer blackmails someone by taking their personal data, then using this Akira Ransomware tool we can delete the victim's data from his system.

Anubis Spy Trojan

CLICK HERE

Investigative intent: preserve a full device forensic image, collect the malicious APK(s)/package names and Accessibility-enabled app list, extract overlay/UI artifacts, SMS/credentials databases and network/C2 indicators (domains, IPs, hashes) and correlate these with threat-intel for attribution and takedown



@EVIL-AD

##################

****

Ares RAT

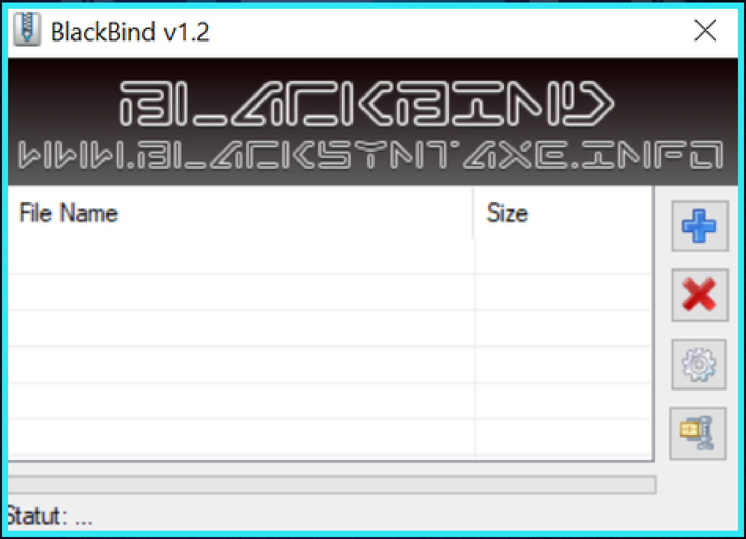
CLICK HERE

Ares RAT is a multi-platform remote-access trojan (open-source Python variants have been observed) that provides shell/command execution, file upload/download, screenshot capture and other backdoor capabilities used in targeted campaigns.

Black Binder

CLICK HERE

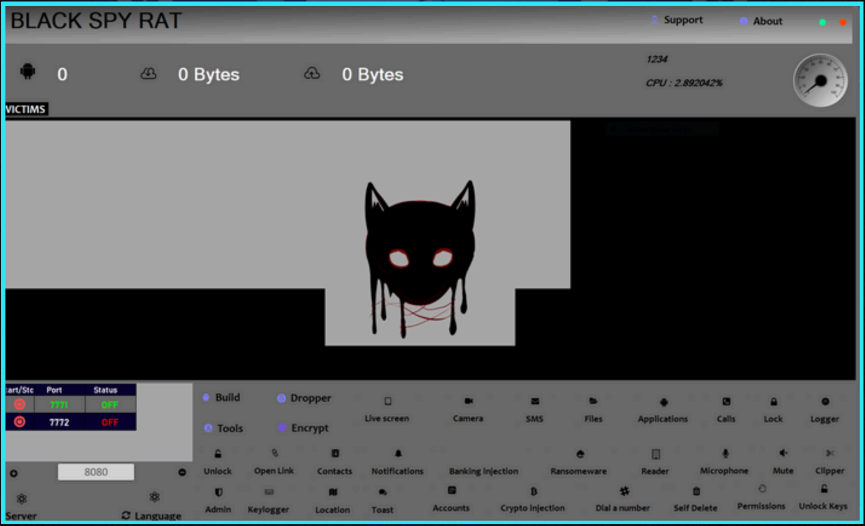
Black Binder is reported to offer file-merging capabilities—able to combine or concatenate files (potentially across formats) which attackers might use to hide or transport exfiltrated data.



Black Spy RAT

CLICK HERE

preserve a forensic image, collect the sample and hashes, document persistence and privilege-escalation artifacts, capture network/C2 indicators, and map behavior to MITRE ATT&CK for attribution and containment.

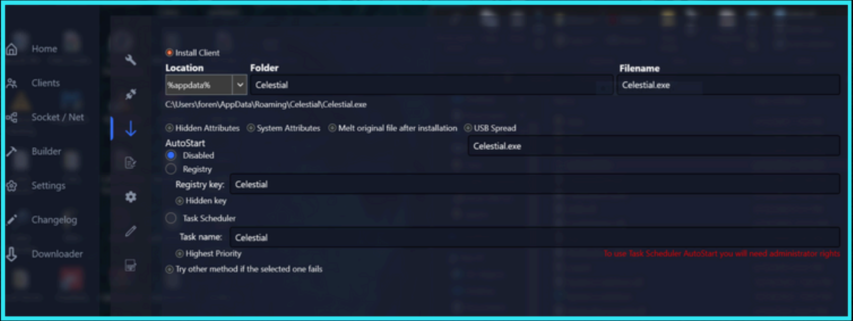


art/Stc	Port	Status
●	7771	OFF
●	7772	OFF

Celestial RAT

CLICK HERE

Celestial (Celestial Stealer / CelestialRAT) is a Malware-as-a-Service/Electron-or-NodeJS Windows infostealer/RAT observed in 2024–2025 that exfiltrates browser credentials, crypto-wallet data and system artifacts and exhibits persistence and C2 communication in sandbox reports.



● Install Client

Location: %appdata%
Folder: Celestial
Filename: Celestial.exe

C:\Users\foren\AppData\Roaming\Celestial\Celestial.exe

○ Hidden Attributes ○ System Attributes ○ Melt original file after installation ○ USB Spread

Celestial.exe

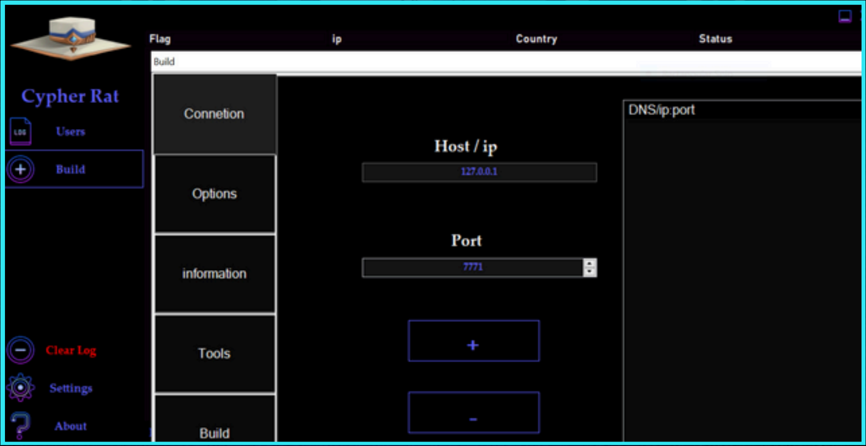
AutoStart
● Disabled
○ Registry
Registry key: Celestial
○ Hidden key
○ Task Scheduler
Task name: Celestial
○ Highest Priority
○ Try other method if the selected one fails

To use Task Scheduler AutoStart you will need administrator rights

Cypher RAT

CLICK HERE

As a cyber-detective: CypherRAT is an Android-focused MaaS remote-access trojan/infostealer sold to multiple operators — it steals credentials, SMS/media and leverages Accessibility/overlay abuse for stealthy persistence and exfiltration.



Host / ip: 127.0.0.1

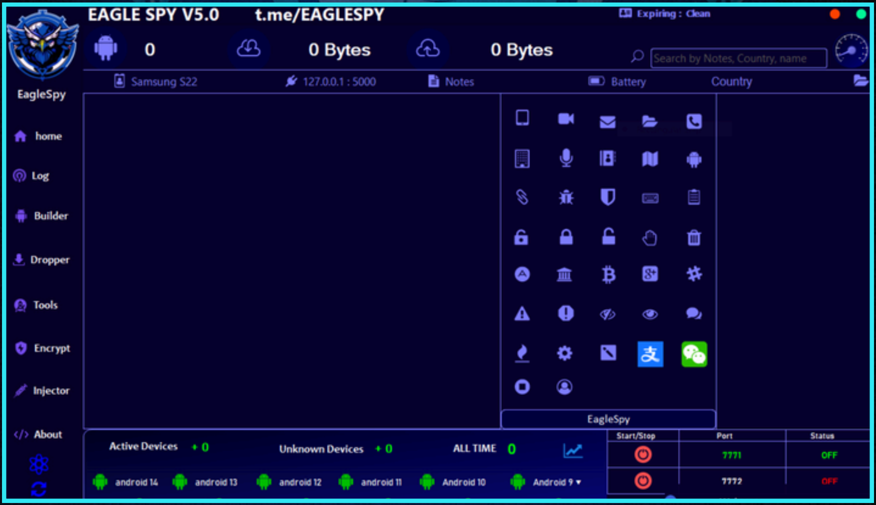
Port: 7771

DNS/ip:port

Eagle Spy RAT

CLICK HERE

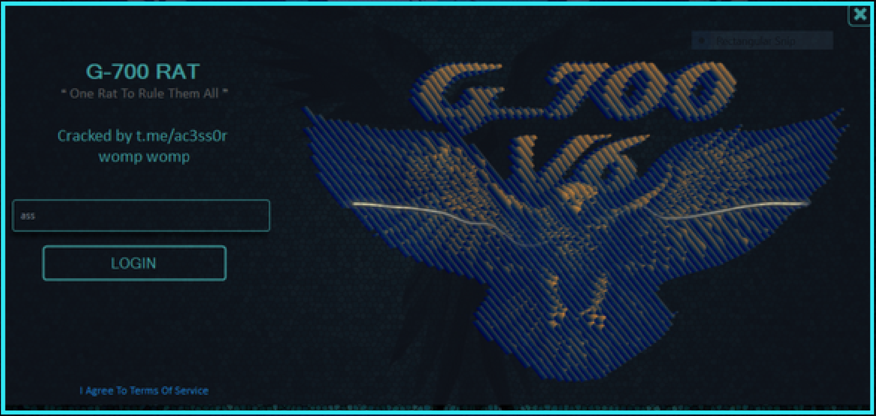
As a cyber-detective: EagleSpy (Eagle Spy RAT) is an Android remote-access trojan (recently marketed as “EagleSpy v5”) that targets Android 9–15, abuses Accessibility/overlay techniques to bypass protections and can steal credentials, 2FA codes, SMS, and other device data (some builds also advertise banking injection and additional payloads).



G-700 RAT

CLICK HERE

As a cyber-detective: G-700 (G700) is a CraxsRAT-family Android remote-access trojan that abuses Accessibility/overlay features and malicious APK installers to steal SMS, credentials (notably crypto wallets), intercept 2FA, and perform stealthy remote control and privilege escalation.



G-700 RAT

" One Rat To Rule Them All "

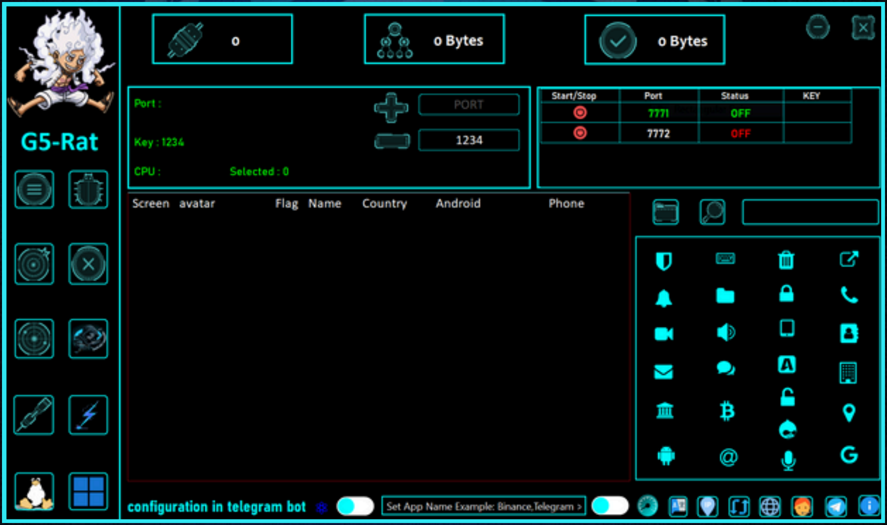
Cracked by t.me/ac3ss0r
womp womp

ass

I Agree To Terms Of Service

G5 RAT

CLICK HERE



Port :

Key : 1234

CPU : Selected : 0

PORT

1234

Start/Stop	Port	Status	KEY
●	7771	OFF	
●	7772	OFF	

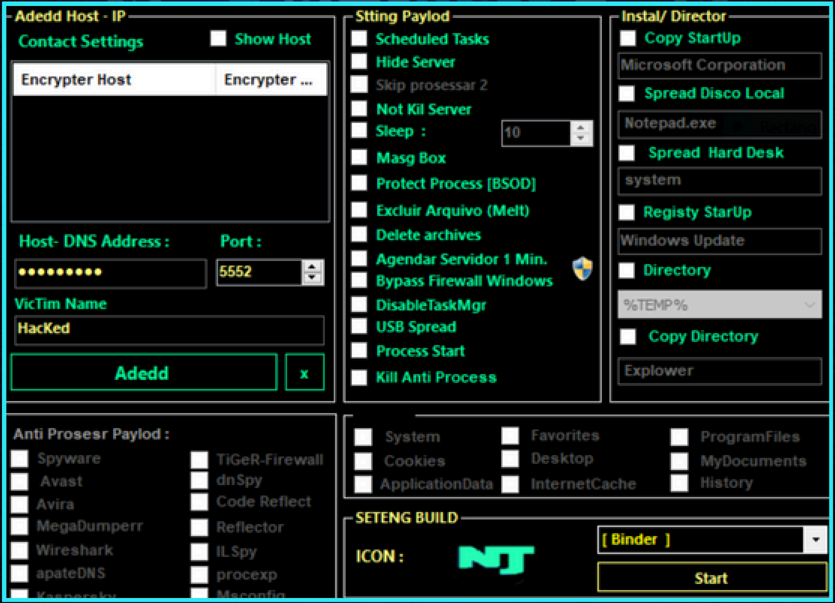
Screen	avatar	Flag	Name	Country	Android	Phone

configuration in telegram bot
Set App Name Example: Binance,Telegram >

NJ-RAT

CLICK HERE

njRAT (aka Bladabindi) is a longstanding Windows remote-access trojan that gives operators backdoor control — keystroke logging, camera/microphone access, file upload/download, shell/command execution and credential/coin-wallet theft; recent variants keep appearing and even use novel C2 channels.



Adedd Host - IP

Contact Settings □ Show Host

Encrypter Host	Encrypter ...

Host- DNS Address : ••••••••••

Port : 5552

VicTim Name: HacKed

Adedd | x

Stting Paylod

□ Scheduled Tasks
□ Hide Server
□ Skip prosessar 2
□ Not Kil Server
□ Sleep : 10
□ Masg Box
□ Protect Process [BSOD]
□ Excluir Arquivo (Melt)
□ Delete archives
□ Agendar Servidor 1 Min.
□ Bypass Firewall Windows
□ DisableTaskMgr
□ USB Spread
□ Process Start
□ Kill Anti Process

Instal/ Director

□ Copy StartUp: Microsoft Corporation
□ Spread Disco Local: Notepad.exe
□ Spread Hard Desk: system
□ Registy StarUp: Windows Update
□ Directory: %TEMP%
□ Copy Directory: Explower

Anti Prosesr Paylod :

□ Spyware
□ Avast
□ Avira
□ MegaDumperr
□ Wireshark
□ apateDNS
□ Kaspersky
□ TiGeR-Firewall
□ dnSpy
□ Code Reflect
□ Reflector
□ ILSpy
□ procexp
□ Msconfig

□ System
□ Cookies
□ ApplicationData
□ Favorites
□ Desktop
□ InternetCache
□ ProgramFiles
□ MyDocuments
□ History

SETENG BUILD

ICON : NJ

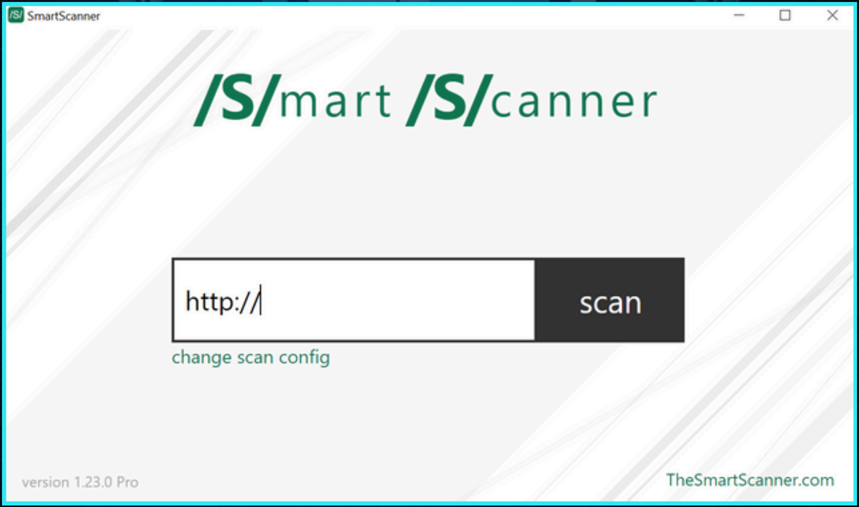
[Binder]

Start

Smart Scanner Pro

CLICK HERE

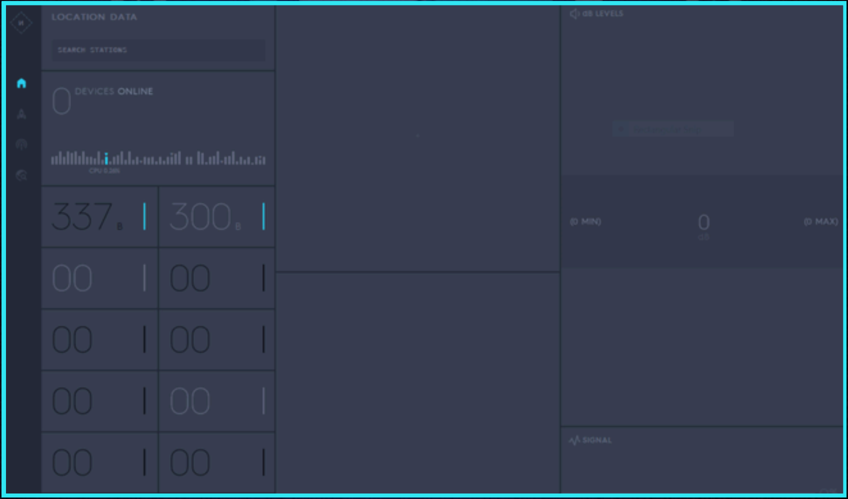
the AI-driven web vulnerability scanner that transforms testing with its reliability and simplicity.



Spy Note RAT

CLICK HERE

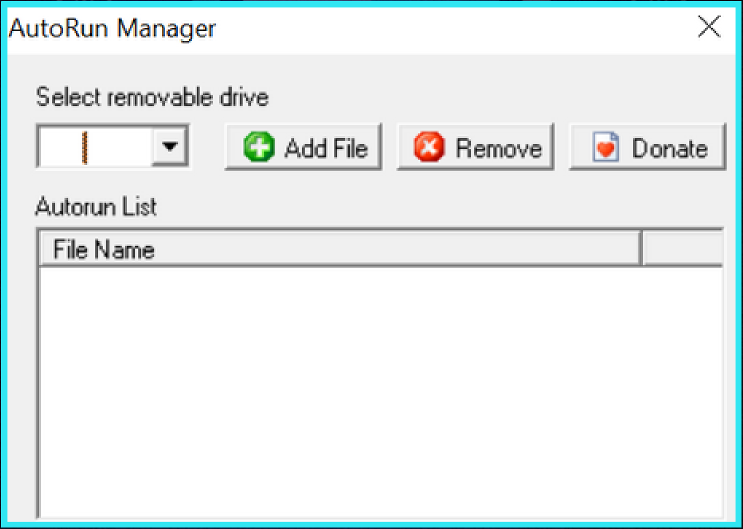
SpyNote is an Android RAT/spyware (builder leaked 2016)—commonly spread via smishing or fake apps—and abuses Accessibility/overlay to capture SMS/calls, mic/camera, location, install APKs and exfiltrate credentials and crypto data.



USB Auto Runner

CLICK HERE

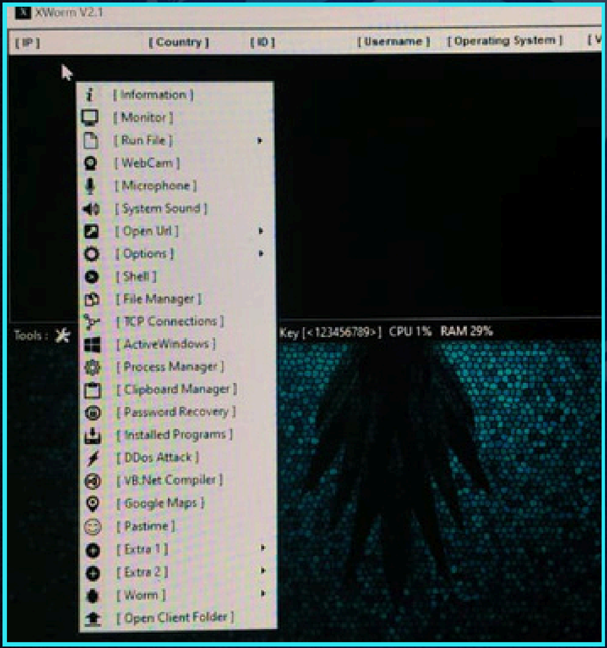
USB Auto-Runner refers to techniques/malware that leverage removable media autorun mechanisms (or deceptive LNK/macros/executables on USBs) to execute payloads when a drive is connected — used to drop backdoors, steal data, or stage lateral movement.



X-Worm RAT

CLICK HERE

XWorm (xWorm) is a modular, malware-as-a-service remote-access trojan commonly delivered via phishing, trojanized installers or obfuscated loaders; operators use it to steal credentials (including crypto wallets), hijack sessions, execute commands and sometimes drop ransomware.

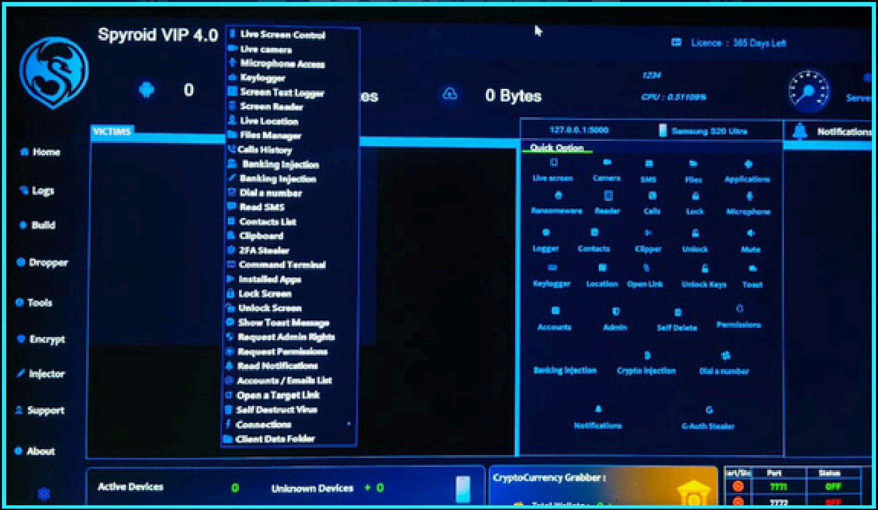


Key [<123456789>] CPU 1% RAM 29%

Spyroid VIP RAT

CLICK HERE

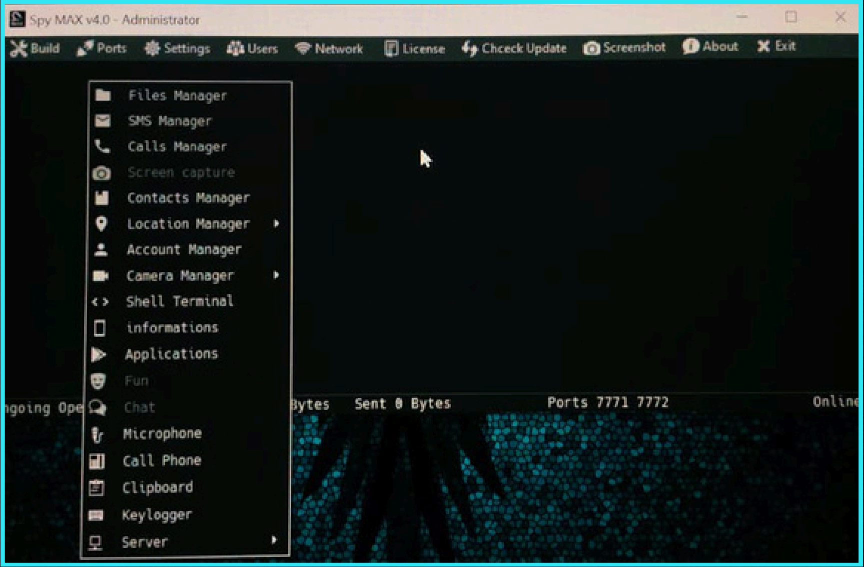
Spyroid VIP is an Android remote-access trojan marketed for full device control (keylogging, SMS/2FA interception, screen/mic access, app install/uninstall and crypto-app targeting) used by multiple operators.



Spy Max RAT

CLICK HERE

SpyMax is an Android RAT/spyware (SpyNote/CypherRat family) delivered via fake apps and phishing (Telegram/wedding-invite lures) that abuses Accessibility/overlay to exfiltrate messages, credentials, media and provide remote control.



Spy MAX v4.0 - Administrator
Build
Ports
Settings
Users
Network
License
Chceck Update
Screenshot
About
Exit
Files Manager
SMS Manager
Calls Manager
Screen capture
Contacts Manager
Location Manager
Account Manager
Camera Manager
Shell Terminal
informations
Applications
Fun
Chat
Microphone
Call Phone
Clipboard
Keylogger
Server
ngoing Ope
Bytes
Sent 0 Bytes
Ports 7771 7772
Online