infinitum IT

Bunny Botnet

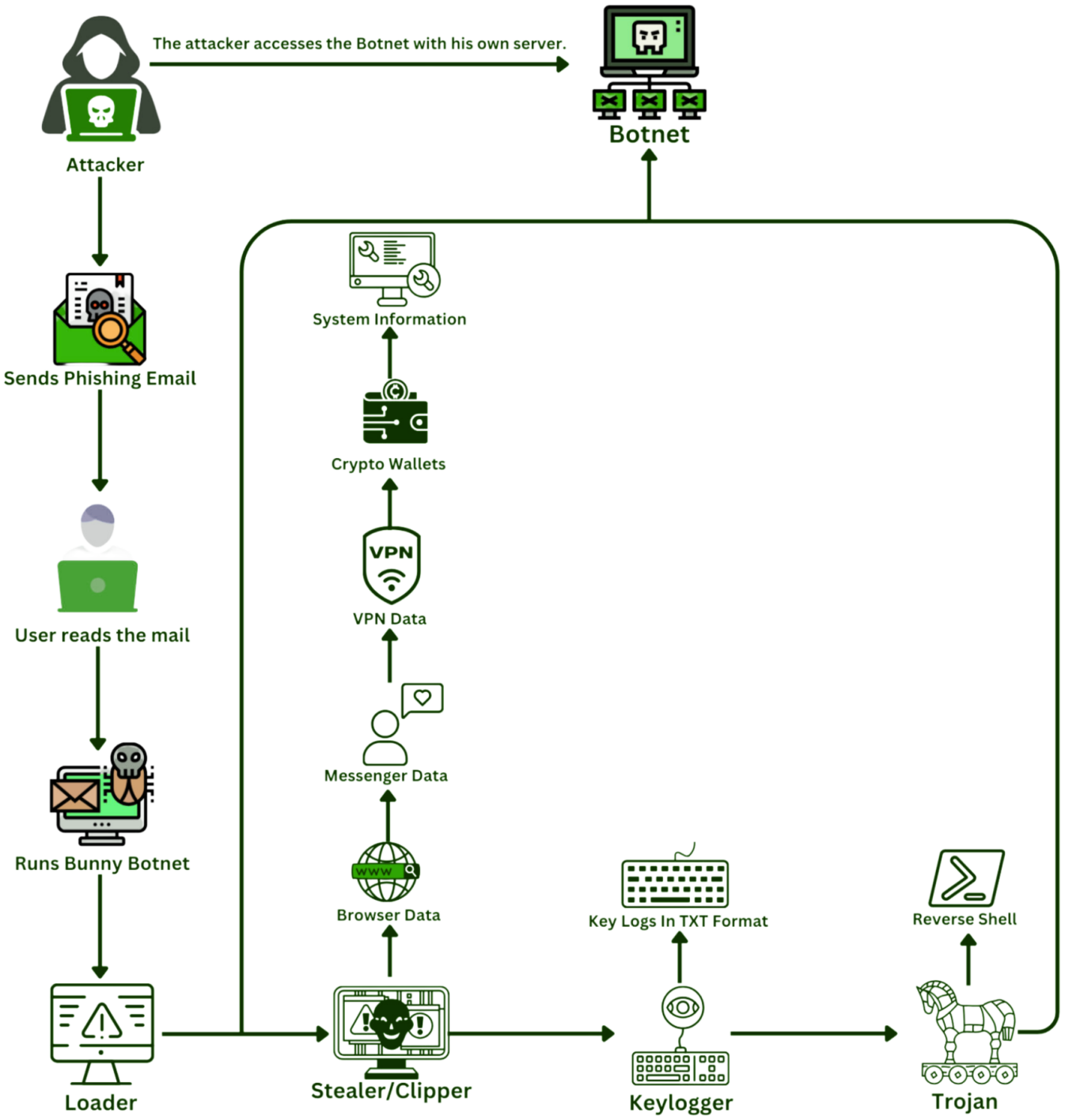
CTI Report

infinitumitlabs

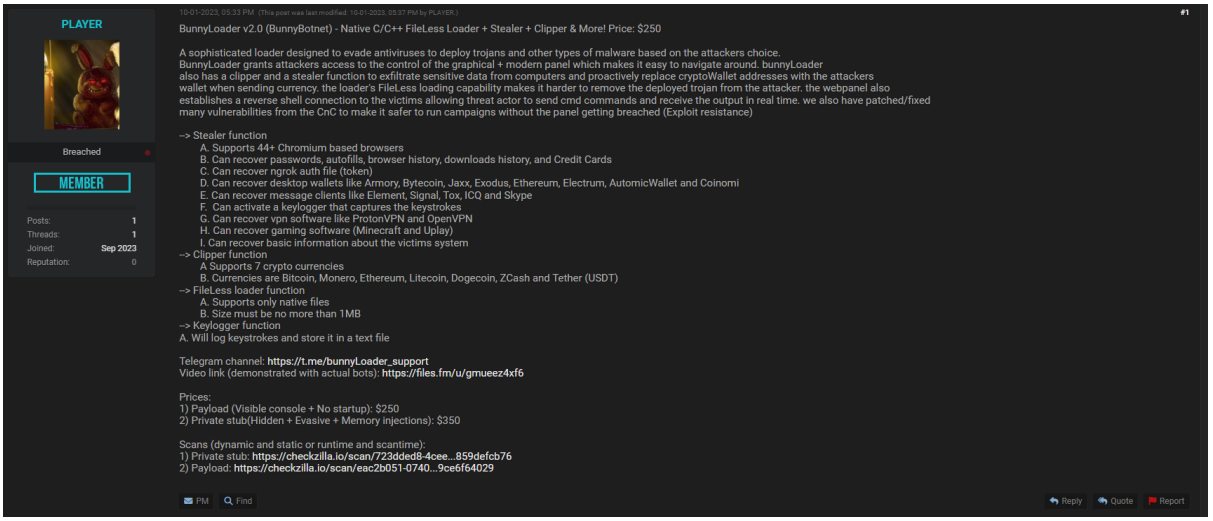
www.infinitumit.com.tr

Content

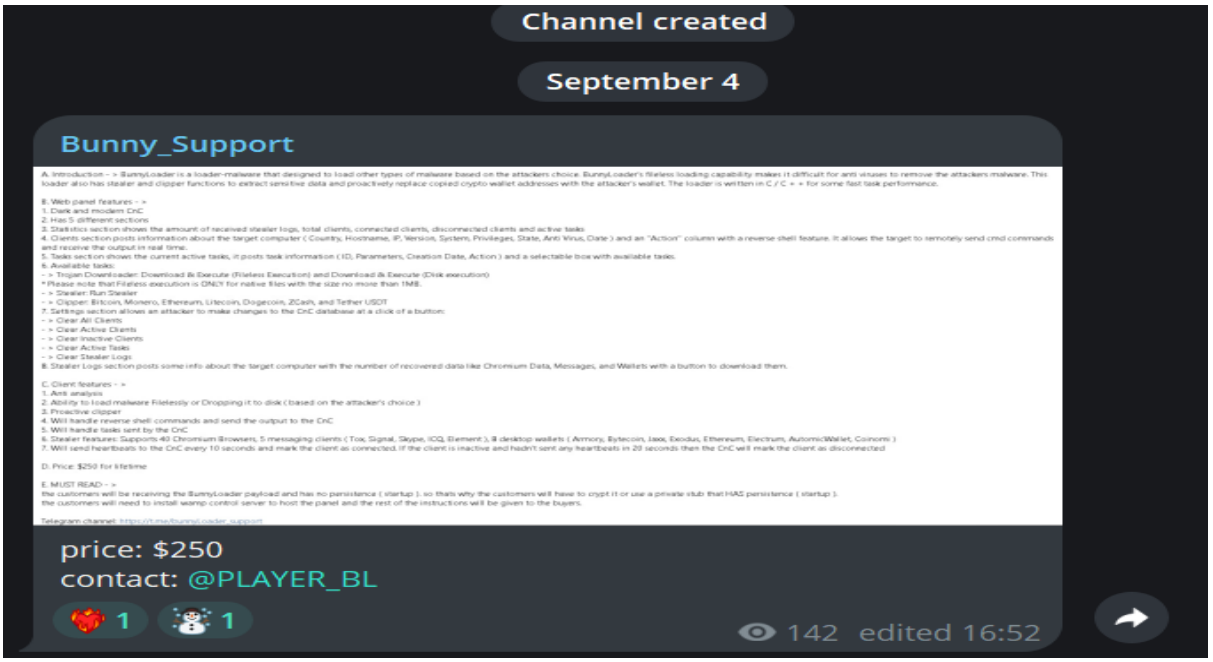
Attack Chain of Bunny Botnet



About Bunny Botnet



A new malware-as-a-service (MaaS) called 'BunnyBotnet' was first spotted on a dark web forum. The software has a low detection rate and incorporates many features. These can be summarized as follows: Botnet, Stealer, Botnet, Reverse Shell, Clipper, Keylogger. Each feature contains multiple capabilities.



The first version of “BunnyBotnet” also known as “BunnyBotnet” was published on September 4. And since then, the developer called “PLAYER_BL” publishes new features and it remains updated

.

Features of Bunny Botnet

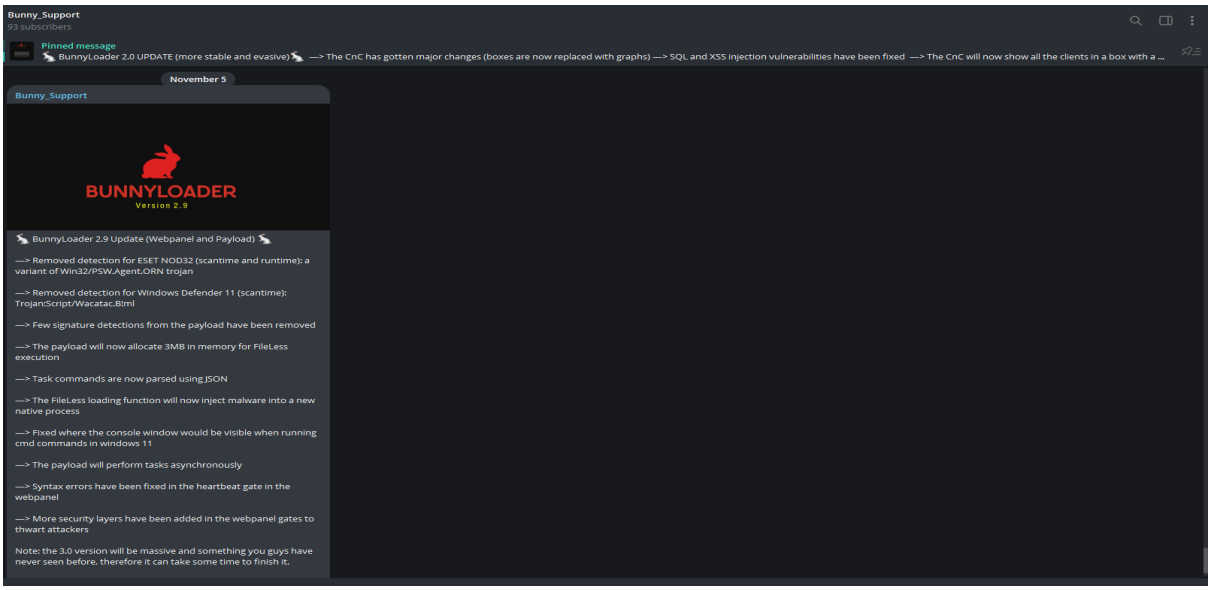
B. Web panel features - >
1. Dark and modern CnC
2. Has 5 different sections
3. Statistics section shows the amount of received stealer logs, total clients, connected clients, disconnected clients and active tasks
4. Clients section posts information about the target computer (Country, Hostname, IP, Version, System, Privileges, State, Anti Virus, Date) and an "Action" column with a reverse shell feature. It allows the target to remotely send cmd commands and receive the output in real time.
5. Tasks section shows the current active tasks, it posts task information (ID, Parameters, Creation Date, Action) and a selectable box with available tasks.
6. Available tasks:
- > Trojan Downloader: Download & Execute (Fileless Execution) and Download & Execute (Disk execution)
* Please note that Fileless execution is ONLY for native files with the size no more than 1MB.
- > Stealer: Run Stealer
- > Clipper: Bitcoin, Monero, Ethereum, Litecoin, Dogecoin, ZCash, and Tether USDT
7. Settings section allows an attacker to make changes to the CnC database at a click of a button:
- > Clear All Clients
- > Clear Active Clients
- > Clear Inactive Clients
- > Clear Active Tasks
- > Clear Stealer Logs
8. Stealer Logs section posts some info about the target computer with the number of recovered data like Chromium Data, Messages, and Wallets with a button to download them.

C. Client features - >
1. Anti analysis
2. Ability to load malware Filelessly or Dropping it to disk (based on the attacker's choice)
3. Proactive clipper
4. Will handle reverse shell commands and send the output to the CnC
5. Will handle tasks sent by the CnC
6. Stealer features: Supports 40 Chromium Browsers, 5 messaging clients (Tox, Signal, Skype, ICQ, Element), 8 desktop wallets (Armory, Bytecoin, Jaxx, Exodus, Ethereum, Electrum, AutomicWallet, Coinomi)
7. Will send heartbeats to the CnC every 10 seconds and mark the client as connected. If the client is inactive and hadn't sent any heartbeats in 20 seconds then the CnC will mark the client as disconnected

D. Price: $250 for lifetime

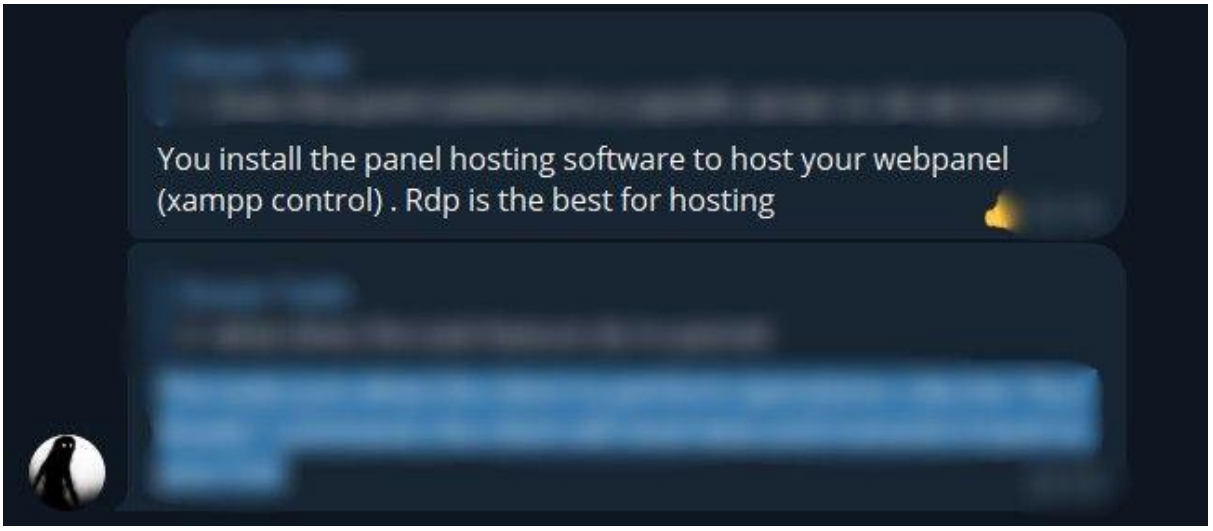
E. MUST READ - >
the customers will be receiving the BunnyLoader payload and has no persistence (startup). so thats why the customers will have to crypt it or use a private stub that HAS persistence (startup).
the customers will need to install wamp control server to host the panel and the rest of the instructions will be given to the buyers.

The software 'BunnyBotnet' has its own unique web panel. The features on the web panel include a distinctive dark mode design, 5 different sections, Trojan download capability, Stealer execution capability, Clipper feature, and a self-cleaning feature. On the client side, it offers anti-analysis, virus download either as fileless or through dropping, execution of reverse shell commands, execution of tasks sent from the panel, and reporting whether the infected system is connected or disconnected to the panel.

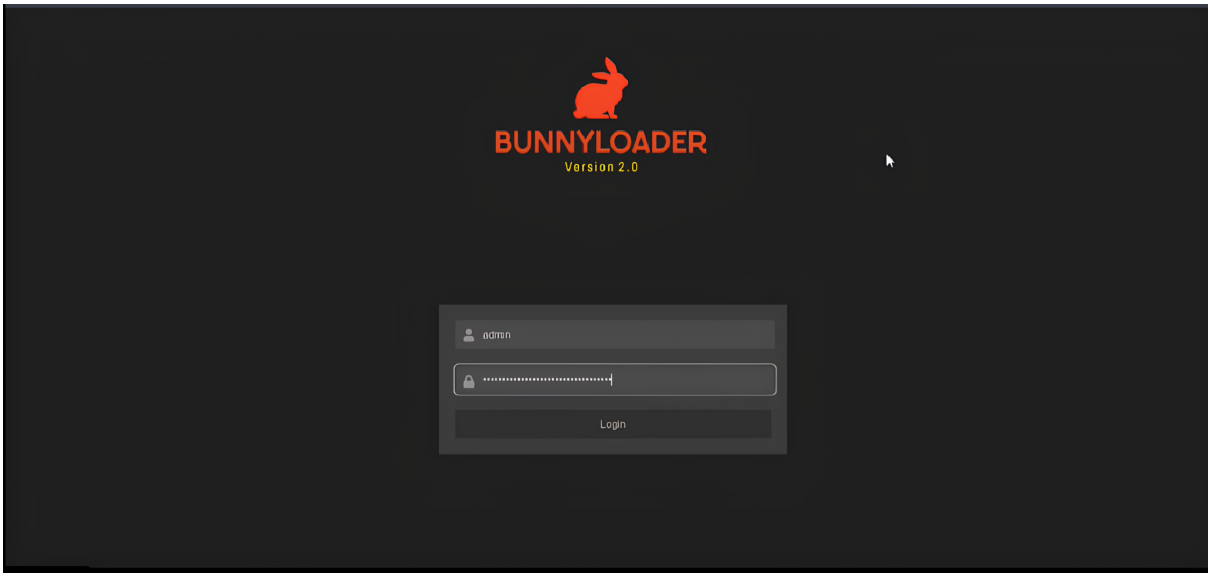


With the new versions, features continue to improve. In the latest version of 'BunnyBotnet,' measures have been taken against the detection of antivirus software like Eset NOD32 and Microsoft Defender, precautions have been implemented to prevent detection via signatures, the FileLess execution size has been increased, and software bugs have been resolved.

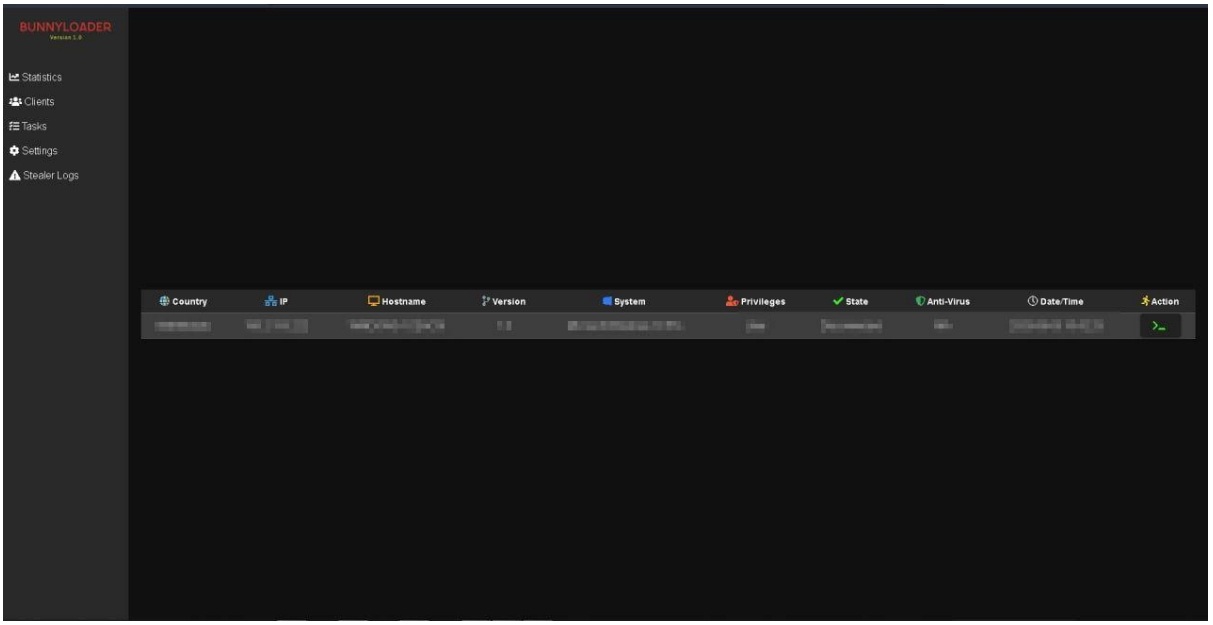
Bunny Botnet From The Eyes Of Attackers



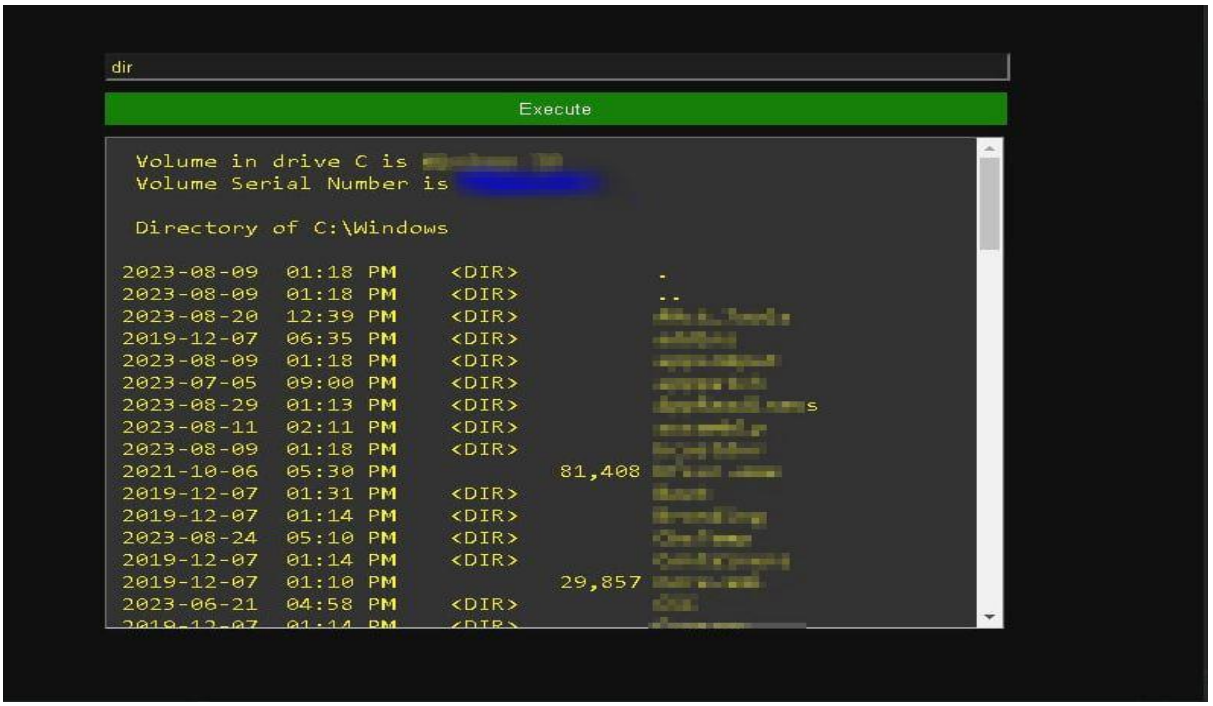
The "BunnyBotnet" software does not have its own specific server or panel. After purchasing the software, the user is provided with a tool to set up the panel, and the panel is installed on the user's server.



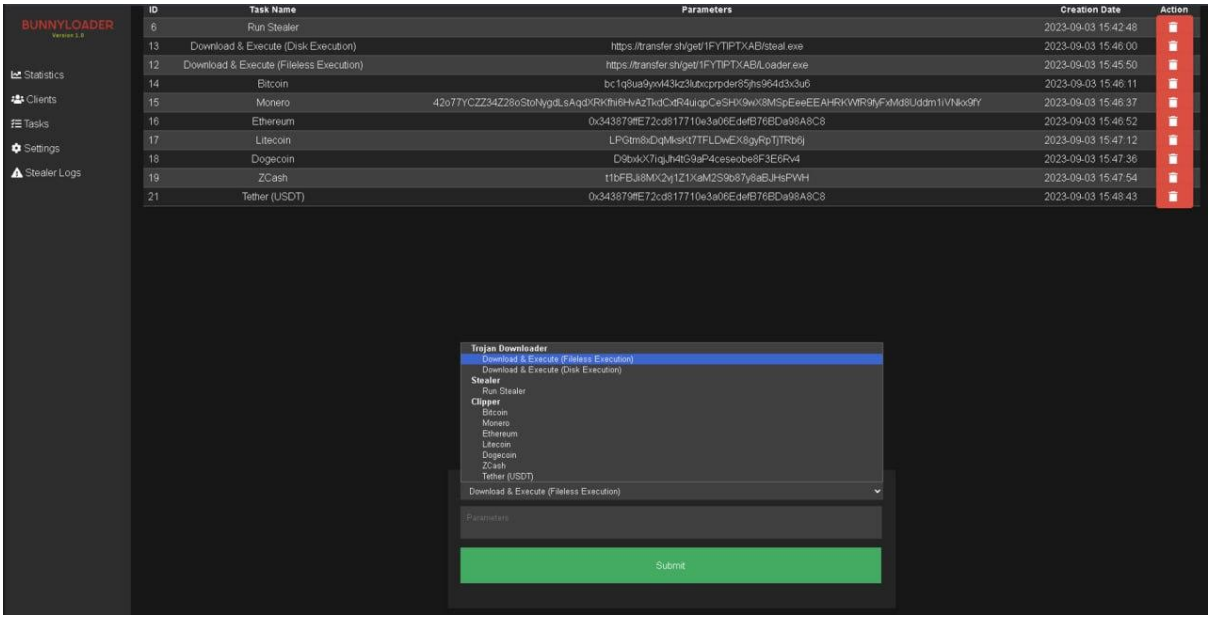
Access to the BunnyBotnet software's panel can be obtained after the panel software is installed.



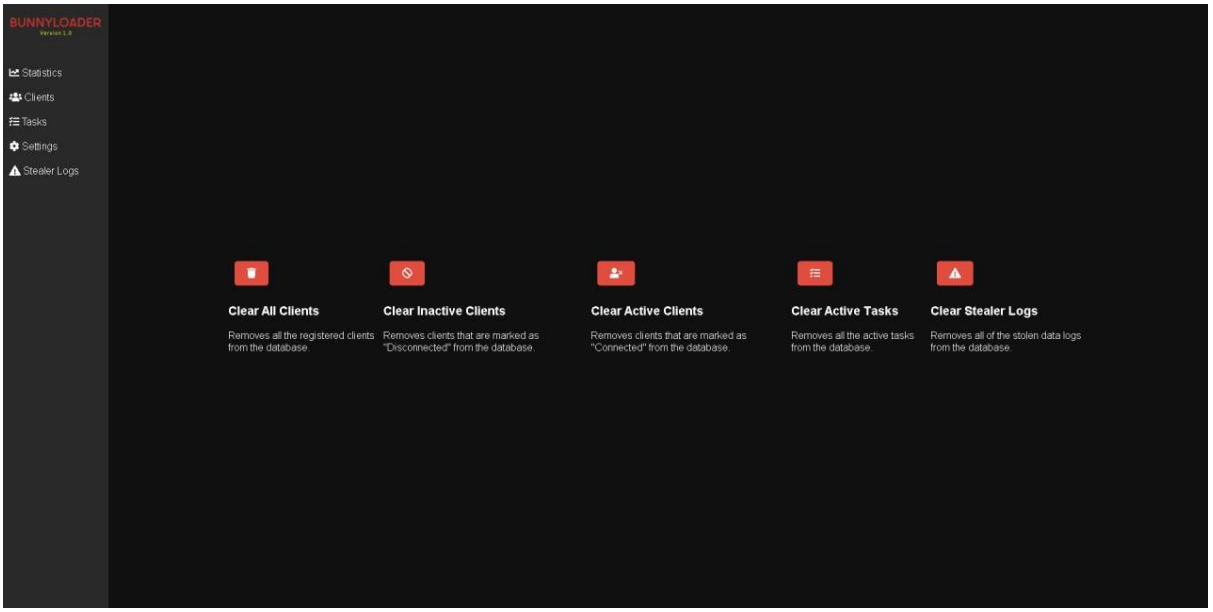
The “Clients” feature gives the information of Country, IP, Hostname, Version, System, Privilege, Status, Antivirus, Date Time and Action.



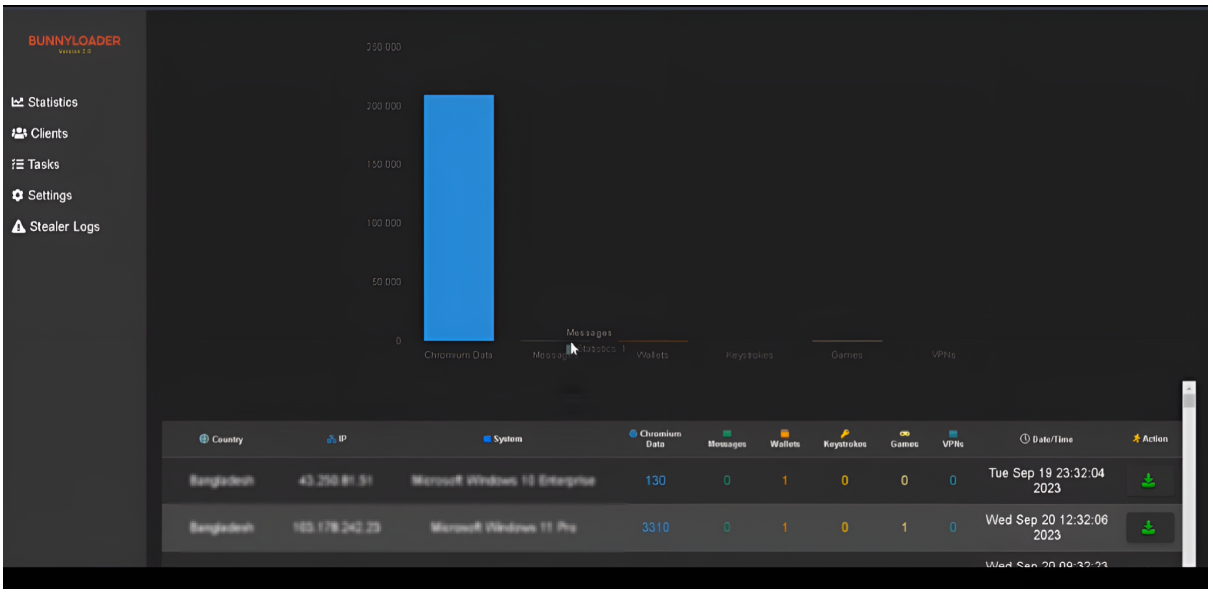
The “Action” part allows the “BunnyBotnet” user to run commands on the victim PC. This is the reverse shell feature of “BunnyBotnet”



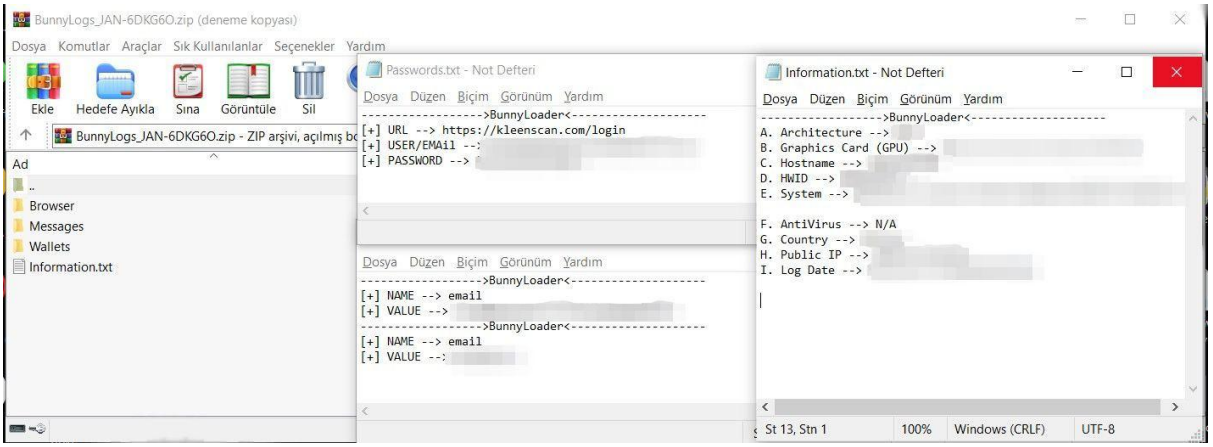
The tasks allow the client to perform operations. Like the "Run Stealer" command, the client will steal data and transmit it back to user's CnC



The Settings allows the client to clear all clients, inactive clients, active clients, active tasks and stealer logs

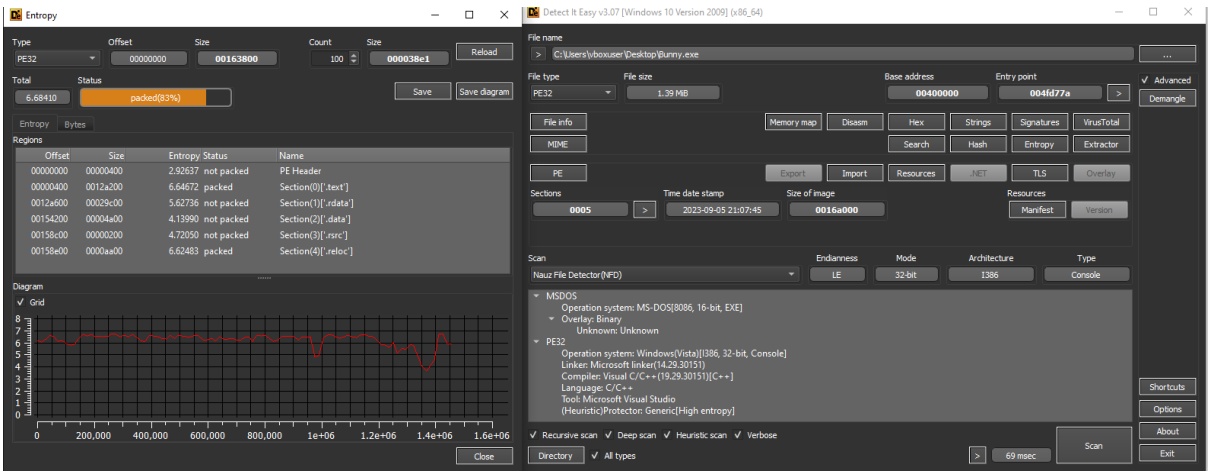


The Stealer Logs allows the client to manage stealer logs that have been arrived from the client PC.

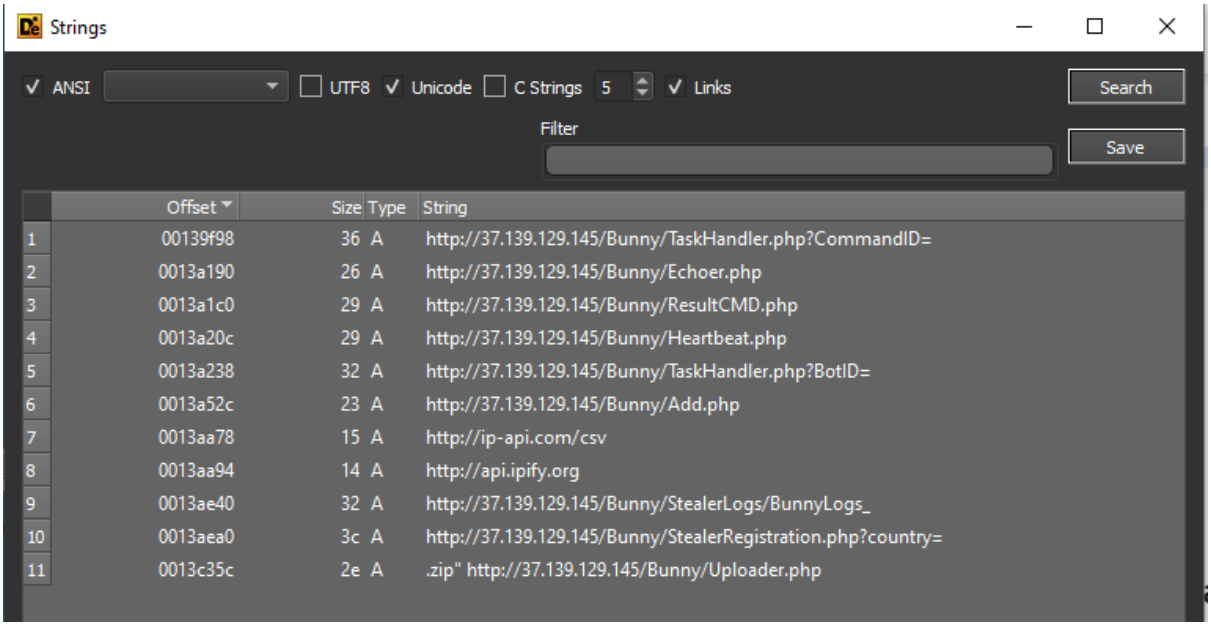


All stealer logs can be downloaded on the local PC. “Information.txt” logs information about system. The “Browser” directory contains “Passwords.txt”,”Autofills.txt”. The “Passwords.txt” logs password information stored on the victim’s browser and “Autofills.txt” logs autofill keyboard inputs.

Basic Analysis of Bunny Botnet



“BunnyBotnet” has developed and compiled in C++. The stub has 1.39MB of file size which is quite large for a malware. By default it comes without being packed.



The strings of the malicious file contain visible URLs. However, there is no specific IP address for the C2 panel; the user sets it up on their own server. Therefore, this IP belongs to the personal server of the developer using the alias "PLAYER_BL."
Also, it can be observed that “BunnyBotnet” uses APIs from the URLs, ***http://ip-api.com/csv*** and ***http://api.ipify.org*** in the links displayed in the strings.

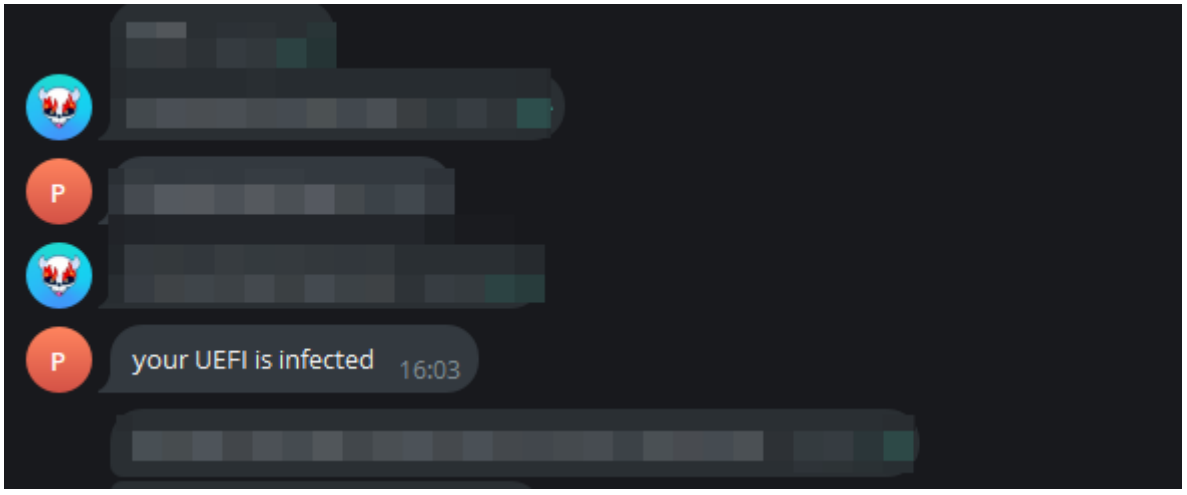
Whois Server	whois.ripe.net
IP Address	37.139.129.145

```
% Abuse contact for '37.139.128.0 - 37.139.130.255' is ' abuse@neterra.net '

inetnum:        37.139.128.0 - 37.139.130.255
netname:        BG-NETERRAIP-20180613
country:        BG
org:            ORG-NL38-RIPE
admin-c:        ND621-RIPE
tech-c:         Nc2110-RIPE
status:         ALLOCATED PA
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         MNT-NETERRA
created:        2023-10-23T07:28:33Z
last-modified:  2023-10-23T07:28:33Z
source:         RIPE

organisation:   ORG-NL38-RIPE
org-name:       Neterra Ltd.
country:        BG
org-type:       LIR
address:        9 Vitoshki Kambani Street, Kambanite Green Offices, Fl. 3
address:        1756
address:        Sofia
address:        BULGARIA
phone:          +359 2 974 3311
fax-no:         +359 2 975 3436
e-mail:         nmt-ip@neterra.net
```

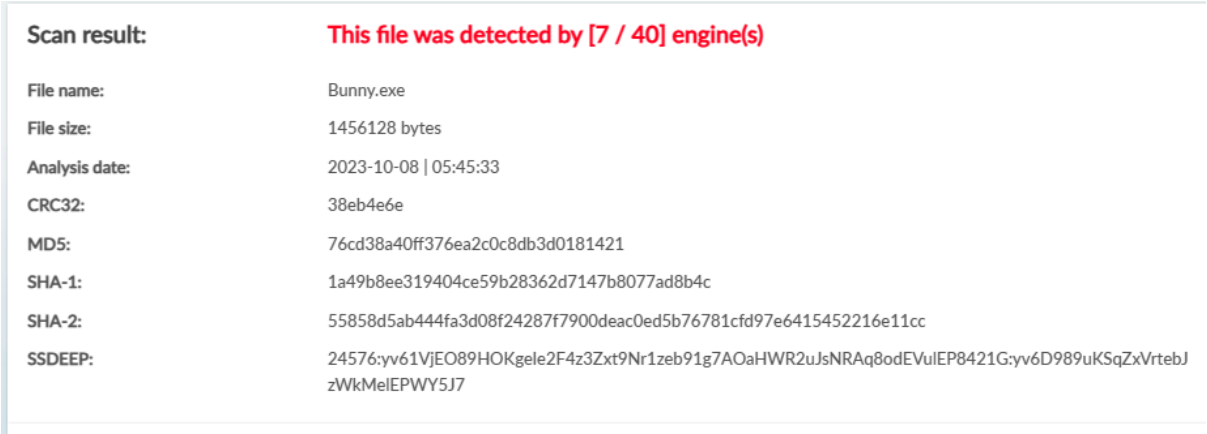
In the whois lookup of 37.139.129.145, it is displayed that the IP address belongs to the telecommunication company named NETERRA. NETERRA provides VDS servers through data centers.

The IP of api.ipify.org is 173.231.16.77. Although it is not mandatory, this ip address can be blocked by the local system user. If blocked, even if the BunnyBotnet software infects the system, the IP and related information of the local system user cannot be transferred to the C2 panel of the BunnyBotnet software. But it should be remembered that this system can also be used by non-malicious software. In this case, if non-malicious software is using this system, problems may occur in the operation of that software.

The IP address of ip-api.com is 208.95.112.1. This IP also can be blocked by the system user but it should be remembered that these kinds of systems can be used by non-malicious software. In case of blocking this IP can cause inability to function properly of non-malicious software.



The stub also is being infected on UEFI. This means that even if a system that's been infected by the BunnyBotnet formats the PC, the malicious software will still be infected on the system.



Scan result:	This file was detected by [7 / 40] engine(s)
File name:	Bunny.exe
File size:	1456128 bytes
Analysis date:	2023-10-08 | 05:45:33
CRC32:	38eb4e6e
MD5:	76cd38a40ff376ea2c0c8db3d0181421
SHA-1:	1a49b8ee319404ce59b28362d7147b8077ad8b4c
SHA-2:	55858d5ab444fa3d08f24287f7900deac0ed5b76781cfd97e6415452216e11cc
SSDEEP:	24576:yv61VjEO89HOKgele2F4z3Zxt9Nr1zeb91g7AOaHWR2uJsNRAq8odEVulEP8421G:yv6D989uKSqZxVrtebJzWkMelEPWY5J7

The stub has a notably low detection rate. It maintains a detection rate of 7/40 even without being packed, and it is capable of bypassing widely used antivirus programs such as Kaspersky, Microsoft Defender, Comodo, Sophos, McAfee, Avast, IKARUS, Eset NOD32 and more.

IOCs

IP:

IOC Type	IOC
IPV4	37.139.129[.]145
IPV4	188.241.240[.]172

HASH:

IOC Type	IOC
SHA256	55858d5ab444fa3d08f24287f7900deac0ed5b76781cfd97e6415452216e11cc
SHA256	bbee98e1a45df6a04ff8f8c0de0550ad0baa91d873165bc20ce907302dba2c25
SHA256	9ac43068071a2bca79ca02b68f3bdf1b6e432881af22d441361b3d54b1fbdc37
SHA256	c15dbdd05315741d4099dc04f37e03f788ab65e4890b371016b8505fa6267558
SHA256	fe325af53d8e401b7c8202e2e1d7638167341a68f70843c87d3ceff3d2bc5fba
SHA256	3a1ccb42cbb712b9e6ca63ee9c4543b2c01907c068a0e199db7f2d864bee2b44
SHA256	3a1ccb42cbb712b9e6ca63ee9c4543b2c01907c068a0e199db7f2d864bee2b44

Categorization of Bunny Botnet

Malware Family	APT Group	Threat Category
Bodegun	No APT group	Trojan

All the **services** you need to keep your **business** secure

Secure your business effectively against cyber threats and attacks

In **InfinitumIT** we provide

Risk and Threat Analysis

Penetration Testing

Managed Security

Digital Forensics

Consultancy

Services at a glance

consultancy

- Continuous Cyber Security Consultancy
- Continuous Vulnerability Analysis Service
- Managed Detection and Response (MDR) Service
- SOC (Security Operations Center) Service

Managed Security

- Managed Detection and Response (MDR) Service
- SOC (Security Operations Center) Service
- Cyber Incident Response (SOME) Service
- SIEM / LOG Correlation Services

Risk & Threat Analysis

- Cyber Risk and Threat Analysis Service
- Ransomware Risk Analysis Service
- APT Detection & Cyber Hygiene Analysis Service
- Purple Teaming Service

Penetration Testing

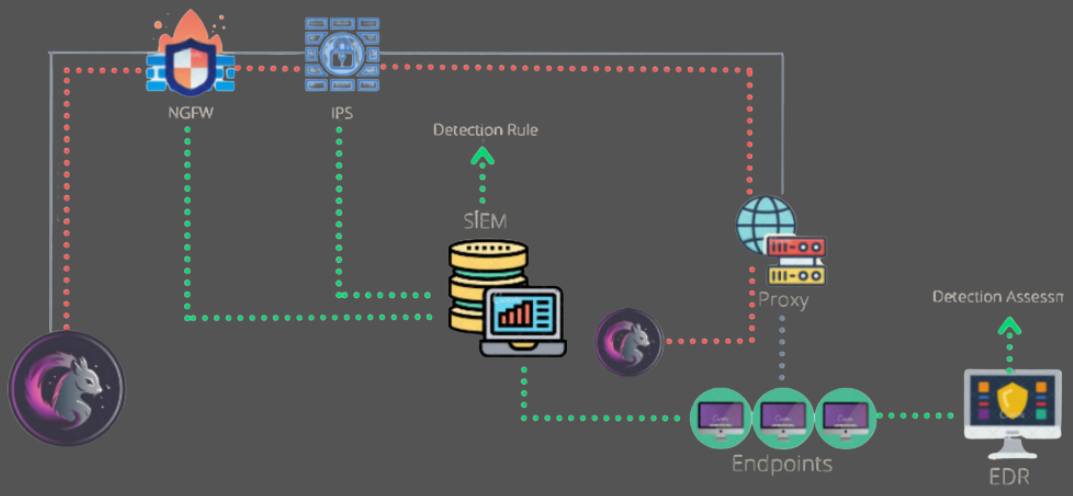
- Penetration Testing
- Red Teaming Service
- Source Code Analysis Service

Forensics

- Network Forensic Service
- Digital Forensic Service
- Mobile Forensic Service

Threatblade

Attack Simulation platform ThreatBlade simulates cyber attacks against your organization's network and systems.



Endpoint Risk Assessment

- Evaluate the security posture of individual endpoints, identify vulnerabilities, and mitigate risks by conducting endpoint-specific scenarios.

Network Risk Assessment

- Continuously monitor the network security posture using network specific attack scenarios, produce trend reports, and improve network security posture.

Identify Weaknesses

- Identify potential weaknesses in an organization's cybersecurity infrastructure and provide actionable insights for improvement purposes.

infinitum IT

"Power of Integrated Security"

Your Business's Weaknesses Do you know?

Contact us now to find out

Check Your MDR Healthcheck For Free

@infinitumitlabs *@infinitumitlabs* *@infinitumitlab1*