BlueHat IL

VoidLink Internals

Inside a Chinese Commercial Grade Cloud Native Malware

Who Are We?

Yuval Sadowsky
Malware Researcher & APT Intelligence

David Driker
Malware Researcher & Reverse Engineer

Hunt For **eBPF**

eBPF
syscall hooking

BlueHat IL

Hunt For **eBPF**

eBPF
syscall hooking

BlueHat IL

Hunt For **eBPF**

eBPF
syscall hooking

- Cloud Native
- Modular
- Stealthy
- Rootkit
- Chinese

BlueHat IL

THREE Points Of View

Malware

Capabilities
Cloud Environment

Attacker

Operator Dashboards
OPSEC mistakes

Developer

The framework sources
AI written code

VoidLink Versions

02.12

VOIDLINK-TEST

First sample
debug symbols
without C2

VoidLink Versions

02.12

10.12

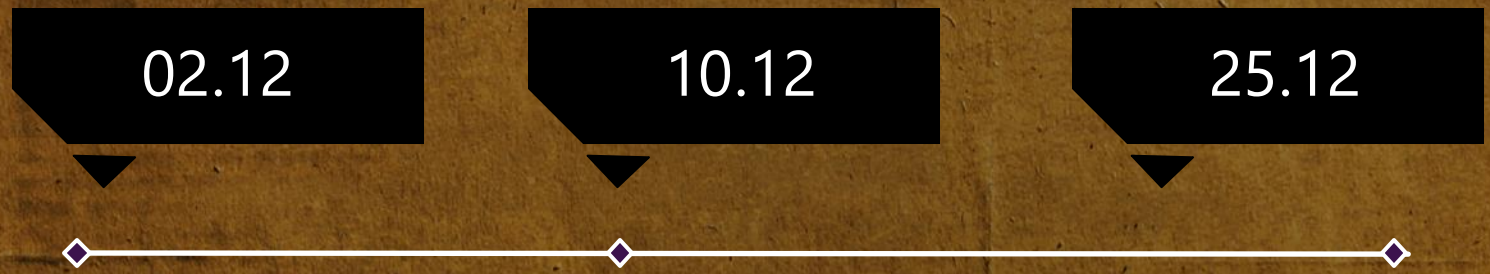
VOIDLINK-TEST

First sample
debug symbols
without C2

VOIDLINK-DEV

Full infection chain
multiple samples,
configured with C2

VoidLink Versions



VOIDLINK-TEST

First sample
debug symbols
without C2

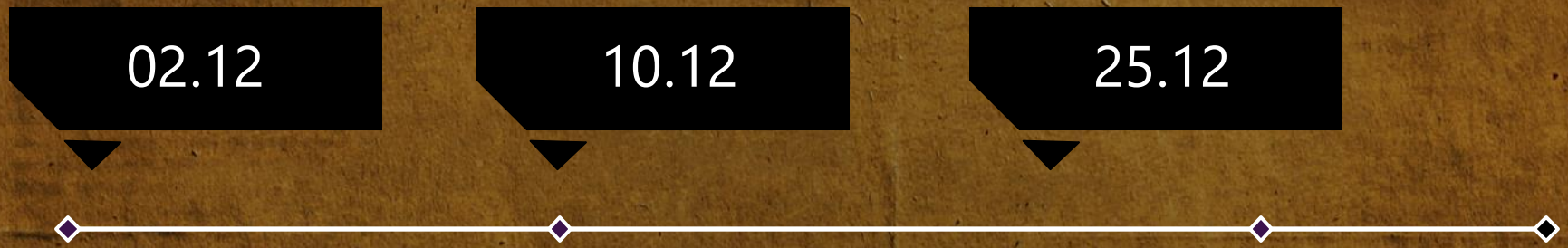
VOIDLINK-DEV

Full infection chain
multiple samples,
configured with C2

VOIDLINK-2025

Production level

VoidLink Reemerges



VOIDLINK-TEST

First sample
debug symbols
without C2

VOIDLINK-DEV

Full infection chain
multiple samples,
configured with C2

VOIDLINK-2025

Production level

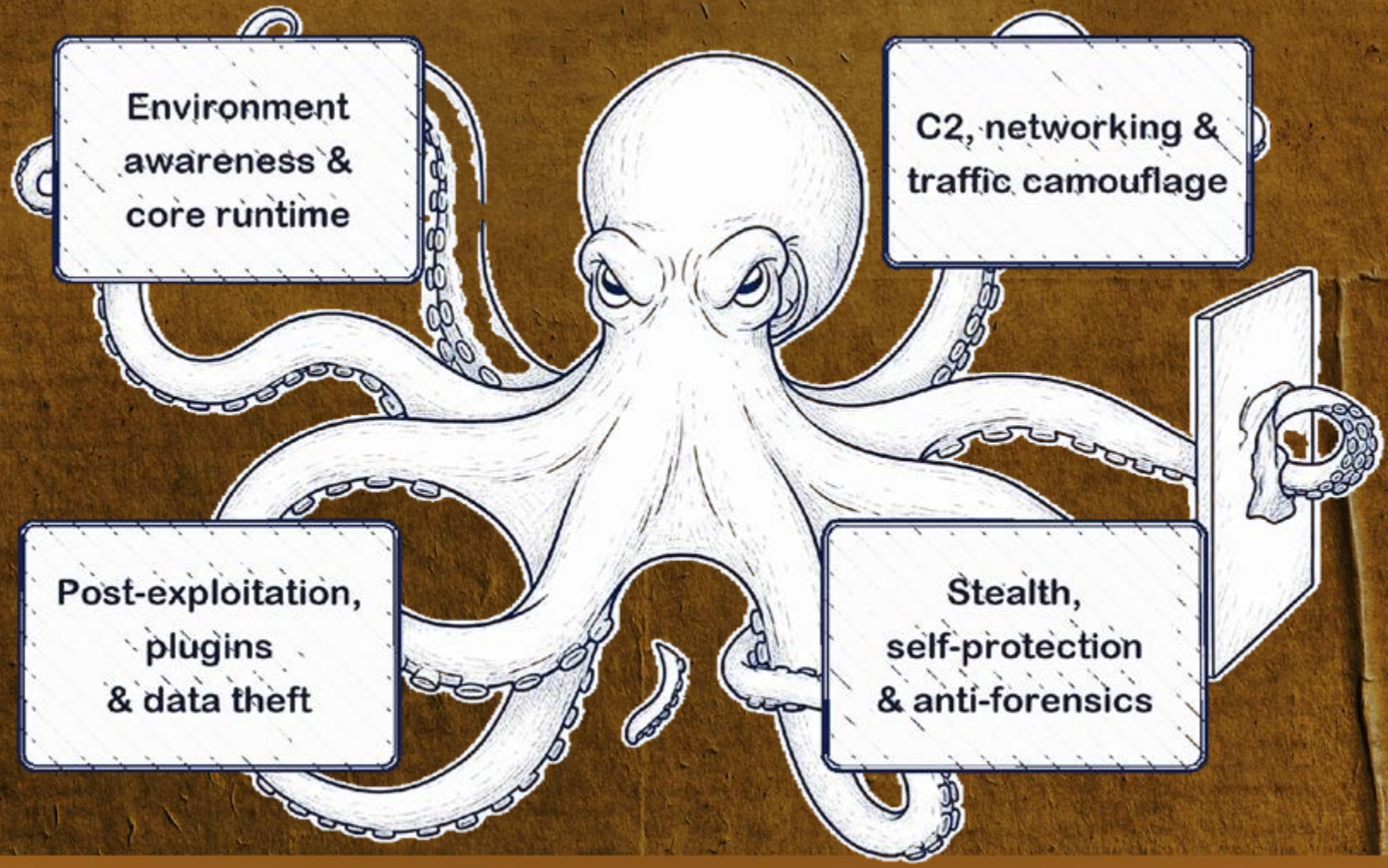
VOIDLINK-X

Voidlink reemerge

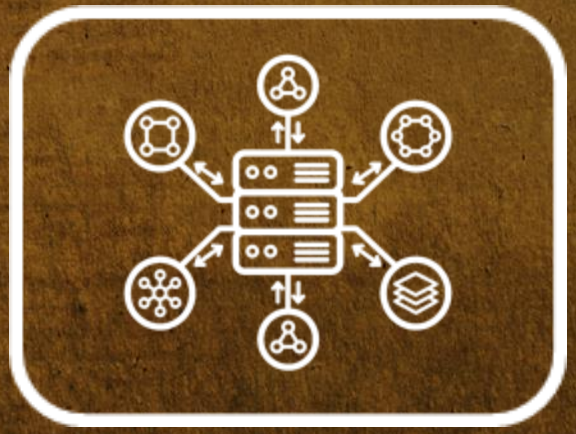
THE MALWARE

BlueHat IL

VoidLink: Cloud-Native Malware



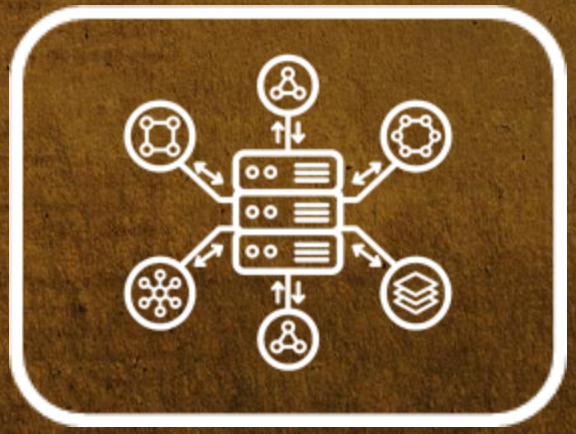
C2, Networking & Traffic Camouflage



Multi-Protocol C2

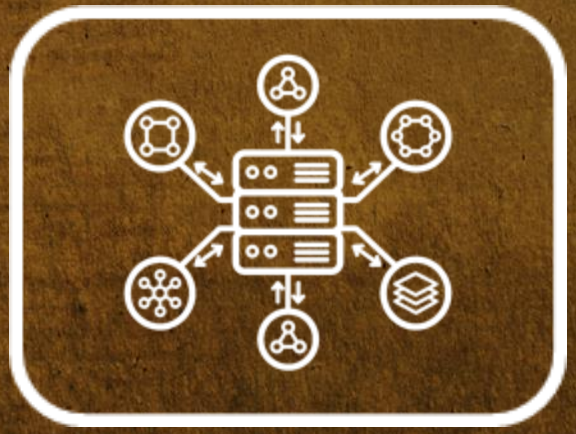
C2, Networking & Traffic Camouflage

Traffic Disguise



Multi-Protocol C2

C2, Networking & Traffic Camouflage



Multi-Protocol C2

Traffic Disguise

Mesh & Relays

C2, Networking & Traffic Camouflage

Advanced C2 Capabilities

Flexible, resilient, and hard to detect

```
; __u8 camouflage_http_camouflage_DEFAULT_API_PATHS[8]
camouflage_http_camouflage_DEFAULT_API_PATHS __u8 <offset __anon_16855, 15h>
                                        ; DATA XREF: .rodata:off_1012580↓o ; "/api/v1/users/profile"
                __u8 <offset __anon_16857, 15h>   "/api/v1/notifications"
                __u8 <offset __anon_16859, 10h>   "/api/v1/settings"
                __u8 <offset __anon_16861, 18h>   "/api/v1/analytics/events"
                __u8 <offset __anon_16863, 0Ch>   "/api/v2/sync"
                __u8 <offset __anon_16865, 11h>   "/api/v2/heartbeat"
                __u8 <offset __anon_16867, 11h>   "/api/health/check"
                __u8 <offset __anon_16869, 0Ch>   "/api/metrics"
__anon_16894    dq 20100h               ; DATA XREF: .rodata:0000000001012590↓o
; __u8 camouflage_http_camouflage_DEFAULT_USER_AGENTS[5]
camouflage_http_camouflage_DEFAULT_USER_AGENTS __u8 <offset __anon_16899, 6Fh>
                                        ; DATA XREF: .rodata:00000000010125A0↓o ; "Mozilla/5.0 (Windows NT 10.0; Win64; x6"...
                __u8 <offset __anon_16902, 75h> ;   Mozilla/5.0 (Macintosh; Intel Mac OS X "...
                __u8 <offset __anon_16905, 65h> ;   Mozilla/5.0 (X11; Linux x86_64) AppleWe"...
                __u8 <offset __anon_16909, 50h> ;   Mozilla/5.0 (Windows NT 10.0; Win64; x6"...
                __u8 <offset __anon_16913, 54h> ;   Mozilla/5.0 (Macintosh; Intel Mac OS X "...
__anon_16959    dq offset __anon_16932  ;
                                        ; "Accept"
                dq 6
                dq offset __anon_16934  ; "application/json, text/plain, */*"
                dq 21h
                dq offset __anon_16941  ; "Accept-Language"
                dq 0Fh
                dq offset __anon_16943  ; "en-US,en;q=0.9"
                dq 0Eh
                dq offset __anon_16950  ; "Accept-Encoding"
                dq 0Fh
                dq offset __anon_16952  ; "gzip, deflate, br"
                dq 11h
; const u8 off_1012580
off_1012580     dq offset camouflage_http_camouflage_DEFAULT_API_PATHS
                                        ; DATA XREF: camouflage_http_camouflage_CamouflageConfig_default+F↓o
                dq 8
                dq offset __anon_16894
                dq 3
                dq offset camouflage_http_camouflage_DEFAULT_USER_AGENTS
                dq 5
                dq offset __anon_16751  ; "application/json"
                dq 10h
                dq offset __anon_16929  ; "_ga"
                dq 3
                dq offset __anon_16959
                dq 3
```

API routes

User-Agents

Headers and Cookies

BlueHat IL

Stealth, Self-Protection & Anti-Forensics

Rootkit

Stealth, Self-Protection & Anti-Forensics

Anti-Analysis

Rootkit

Stealth, Self-Protection & Anti-Forensics

Anti-Analysis

Rootkit

Anti-Forensics

Stealth, Self-Protection & Anti-Forensics

Deep Stealth & Evasion

Anti-analysis & anti-forensics, by design

```
  // Select rootkit deployment method depending on environment
  v10 = stealth_stealth_manager_StealthManager_selectBestMethod(self);
switch ( (v10 + 4) & 7 )
{
  case 0:
    v8 = stealth_stealth_manager_StealthManager_activateLdPreload(self);
    if ( !v8 )
      goto LABEL_7;
    builtin_returnError();
    result = v8;
    break;
  case 1:
    v7 = stealth_stealth_manager_StealthManager_activateProcHide(self);
    if ( !v7 )
      goto LABEL_7;
    builtin_returnError();
    result = v7;
    break;
  case 2:
  case 3:
    debug_FullPanic__function__defaultPanic____memcpyAlias_0();
    return result;
  case 4:
    return 0;
  case 5:
  case 6:
    v6 = stealth_stealth_manager_StealthManager_activateEbpf(self, method);
    if ( !v6 )
      goto LABEL_7;
    builtin_returnError();
    result = v6;
    break;
  case 7:
    v9 = stealth_stealth_manager_StealthManager_activateLkm(self);
    if ( v9 )
```

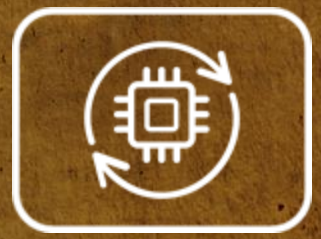
BlueHat IL

Environment & Core Runtime

Fingerprinting

Environment & Core Runtime

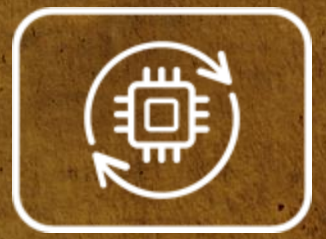
Fingerprinting



Adaptive

Environment & Core Runtime

Fingerprinting



Adaptive

Behavior

BlueHat IL

Environment & Core Runtime

Environment Awareness

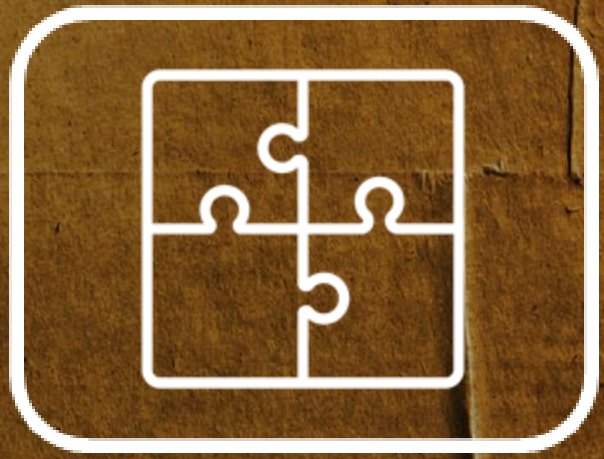
Understands and adapts to its surroundings

```
anyerror __cdecl adapter_cloud_detect_CloudDetector_fetchAWSMetadata(adapter_cloud_detect_CloudDetector *self)
{
  unsigned __int64 v1; // rsi
  __u8 v2; // r8
  __u8 v3; // r8
  __u8 v4; // r8
  u8 *path_4; // [rsp+38h] [rbp-48h]

  adapter_cloud_detect_CloudDetector_readCloudInitData(self);
  if ( *(_QWORD *)(v1 + 16) )
    return 0;
  path_4 = adapter_cloud_detect_CloudDetector_readEnvVar(self, (__u8)__PAIR128__("AWS_REGION", v1)).ptr;
  if ( path_4 )
  {
    adapter_cloud_detect_CloudMetadata_setRegion(
      (adapter_cloud_detect_CloudMetadata *)self,
      (__u8)__PAIR128__((unsigned __int64)path_4, v1 + 16));
  }
  else
  {
    v2.len = (usize)"/latest/meta-data/placement/region";
    v2.ptr = (u8 *)80;
    adapter_cloud_detect_CloudDetector_fetchMetadataHTTP(
      self,
      (__u8)__PAIR128__("169.254.169.254", v1),
      0xFu,
      v2,
      (__u8)0x22uLL);
    v3.ptr = (u8 *)80;
    v3.len = (usize)"/latest/meta-data/instance-id";
    adapter_cloud_detect_CloudDetector_fetchMetadataHTTP(
      self,
      (__u8)__PAIR128__("169.254.169.254", v1),
      0xFu,
      v3,
      (__u8)0x1DuLL);
    v4.ptr = (u8 *)80;
    v4.len = (usize)"/latest/meta-data/instance-type";
    adapter_cloud_detect_CloudDetector_fetchMetadataHTTP(
      self,
      (__u8)__PAIR128__("169.254.169.254", v1),
      0xFu,
      v4,
      (__u8)0x1FuLL);
  }
  return 0;
}
```

BlueHat IL

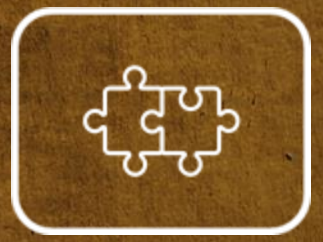
Post-Exploitation, Plugins & Data Theft



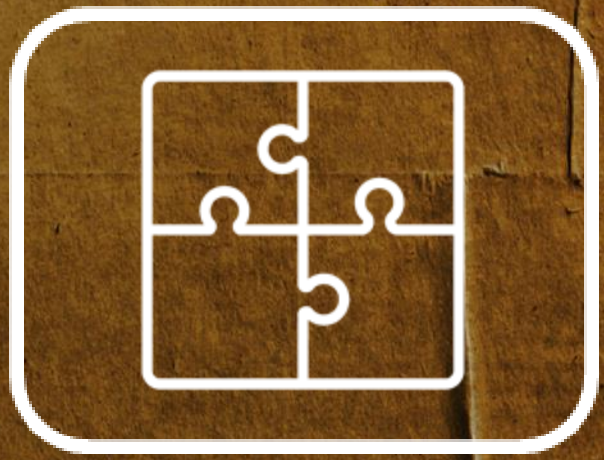
Modular

BlueHat IL

Post-Exploitation, Plugins & Data Theft



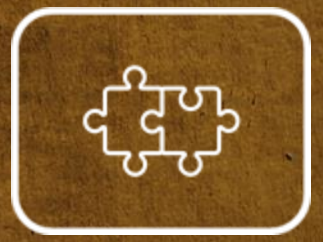
Plugins



Modular

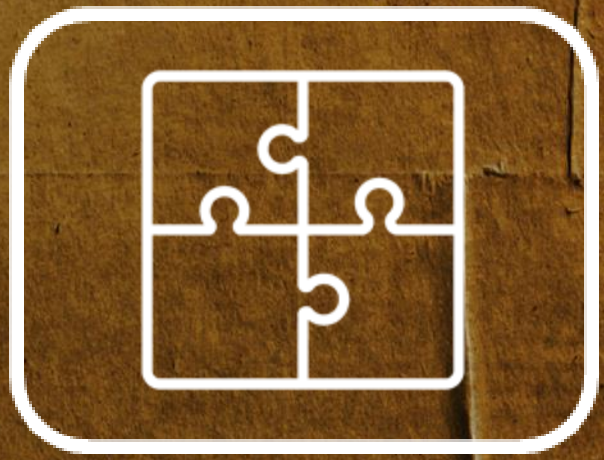
BlueHat IL

Post-Exploitation, Plugins & Data Theft



Plugins

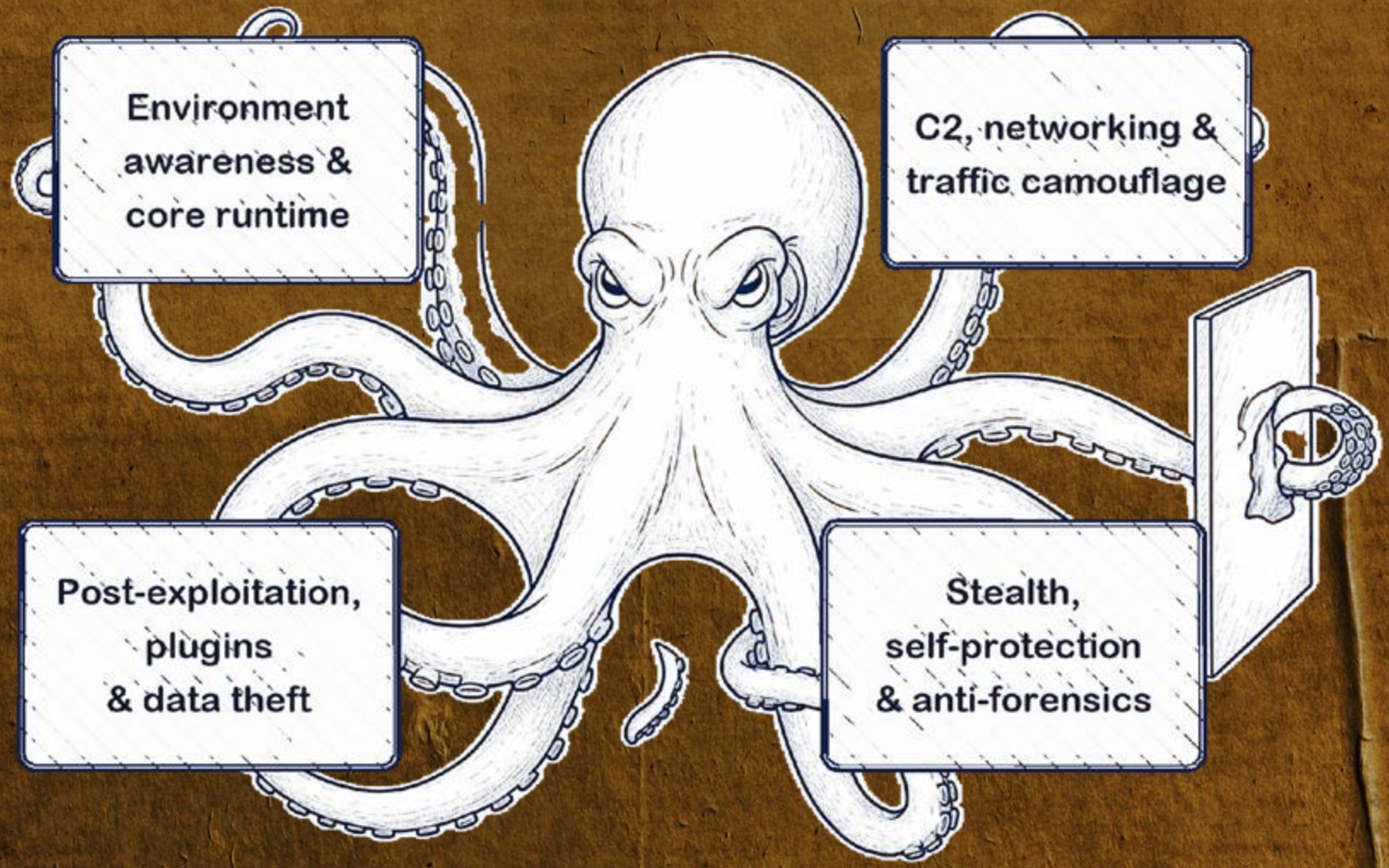
Exfiltration



Modular

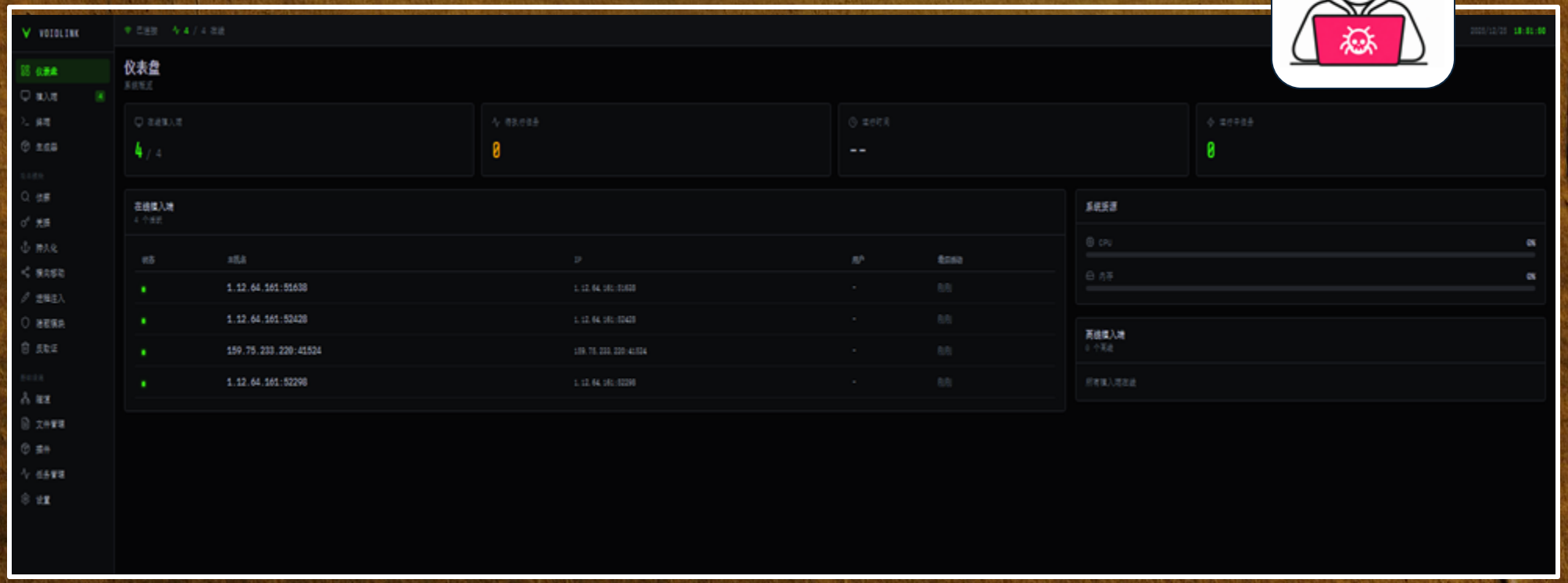
BlueHat IL

VoidLink: Cloud-Native Malware



THE ATTACKER

VoidLink - Attacker View



BlueHat IL

Dashboard - Three Panels

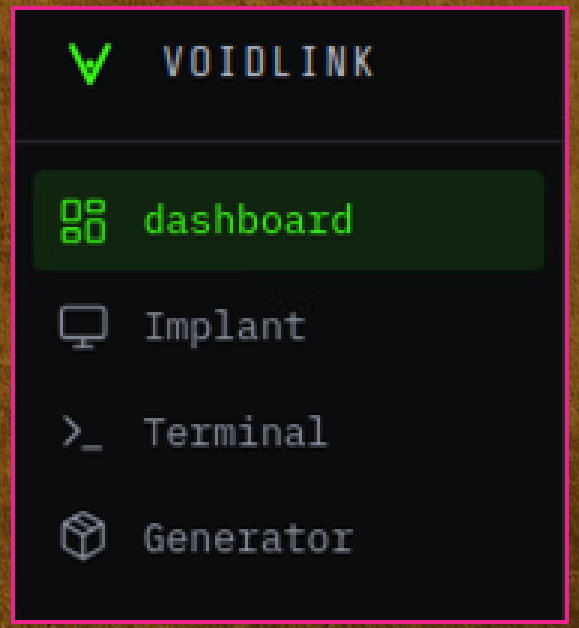
Dashboard

Attack

Infrastructure

BlueHat IL

Dashboard



Dashboard - Builder

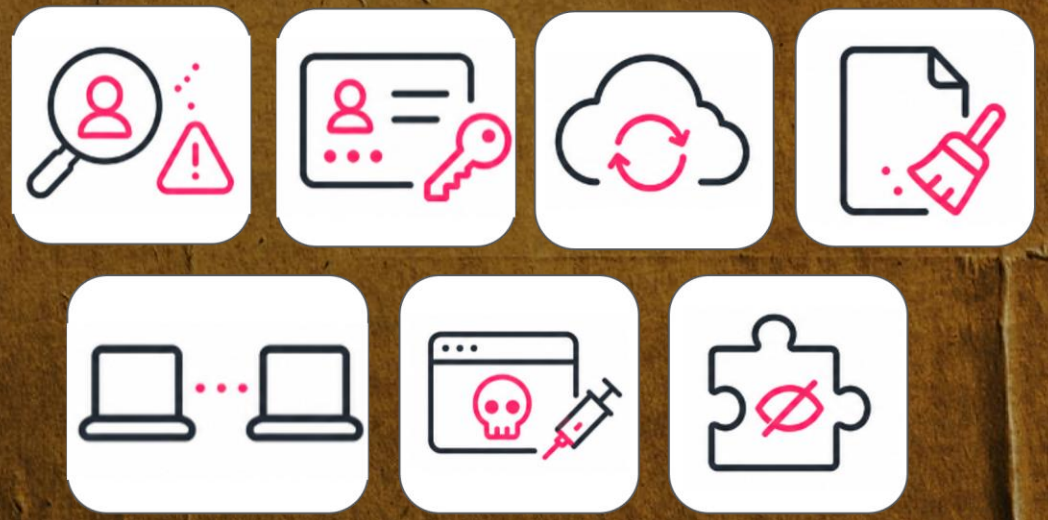
Features:

- Bundle\Implant\Stage1\Loader
- Evasion Level
  - Code Integrity
  - SMC
  - Anti sandbox
- Communication protocol
- Build options:
  - One time link
  - Symbols
  - Ignore cache

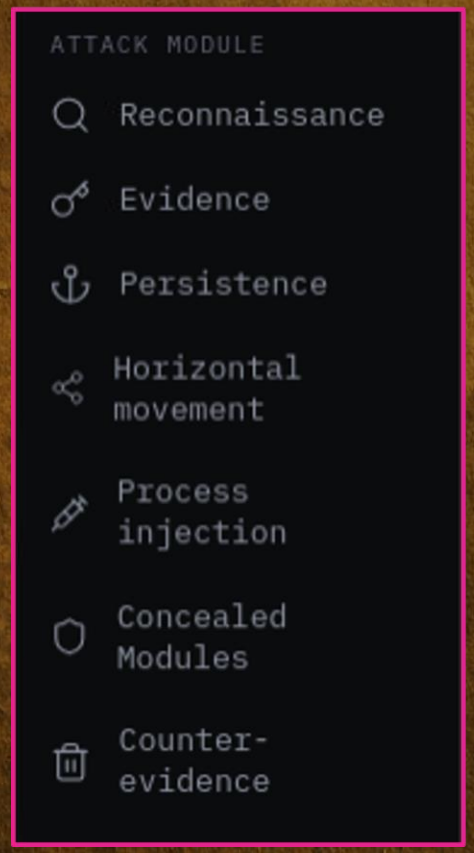
Dashboard - Attack

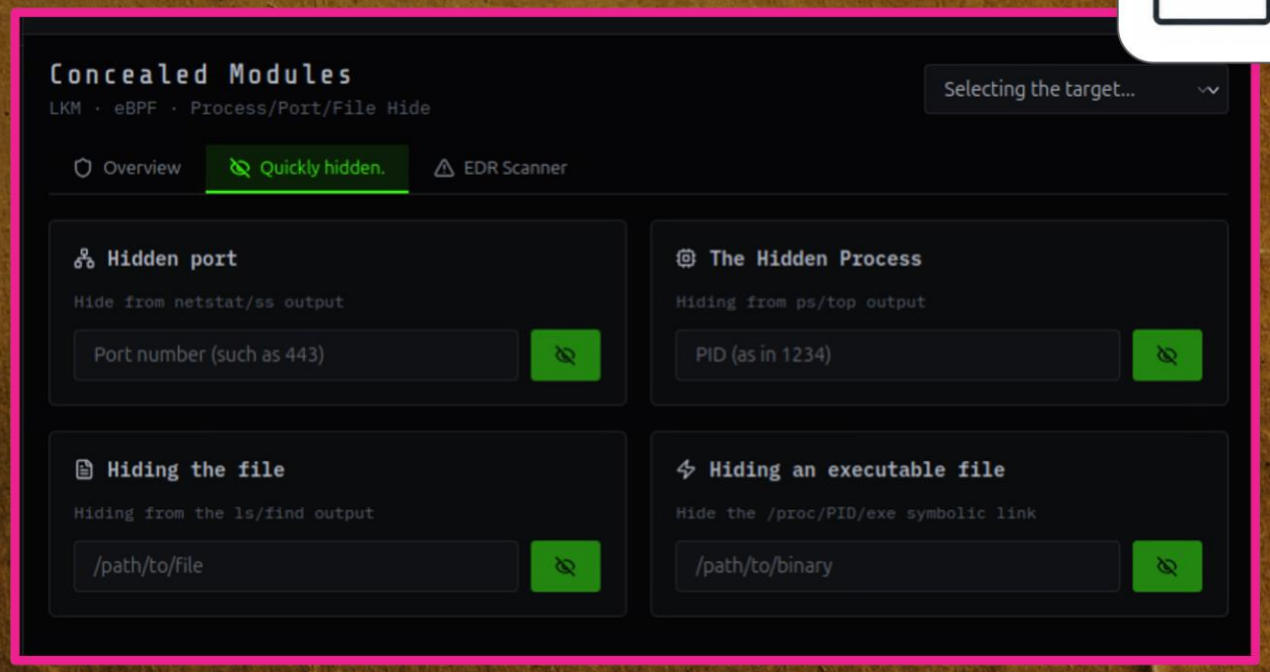
ATTACK MODULE

- Reconnaissance
- Evidence
- Persistence
- Horizontal movement
- Process injection
- Concealed Modules
- Counter-evidence



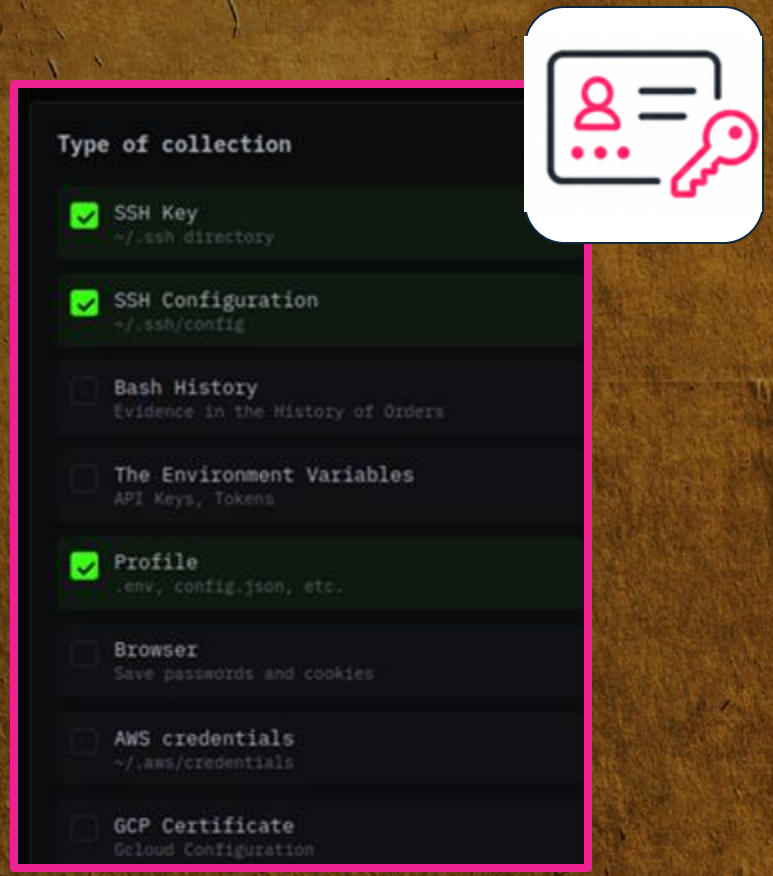
Dashboard - Rootkit



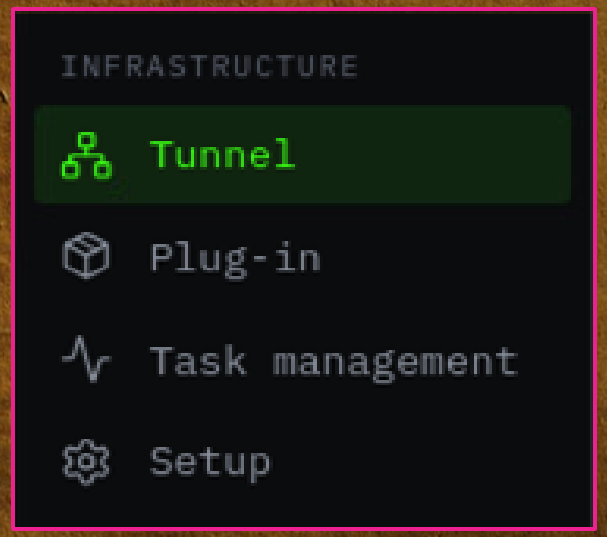


Dashboard - Credentials

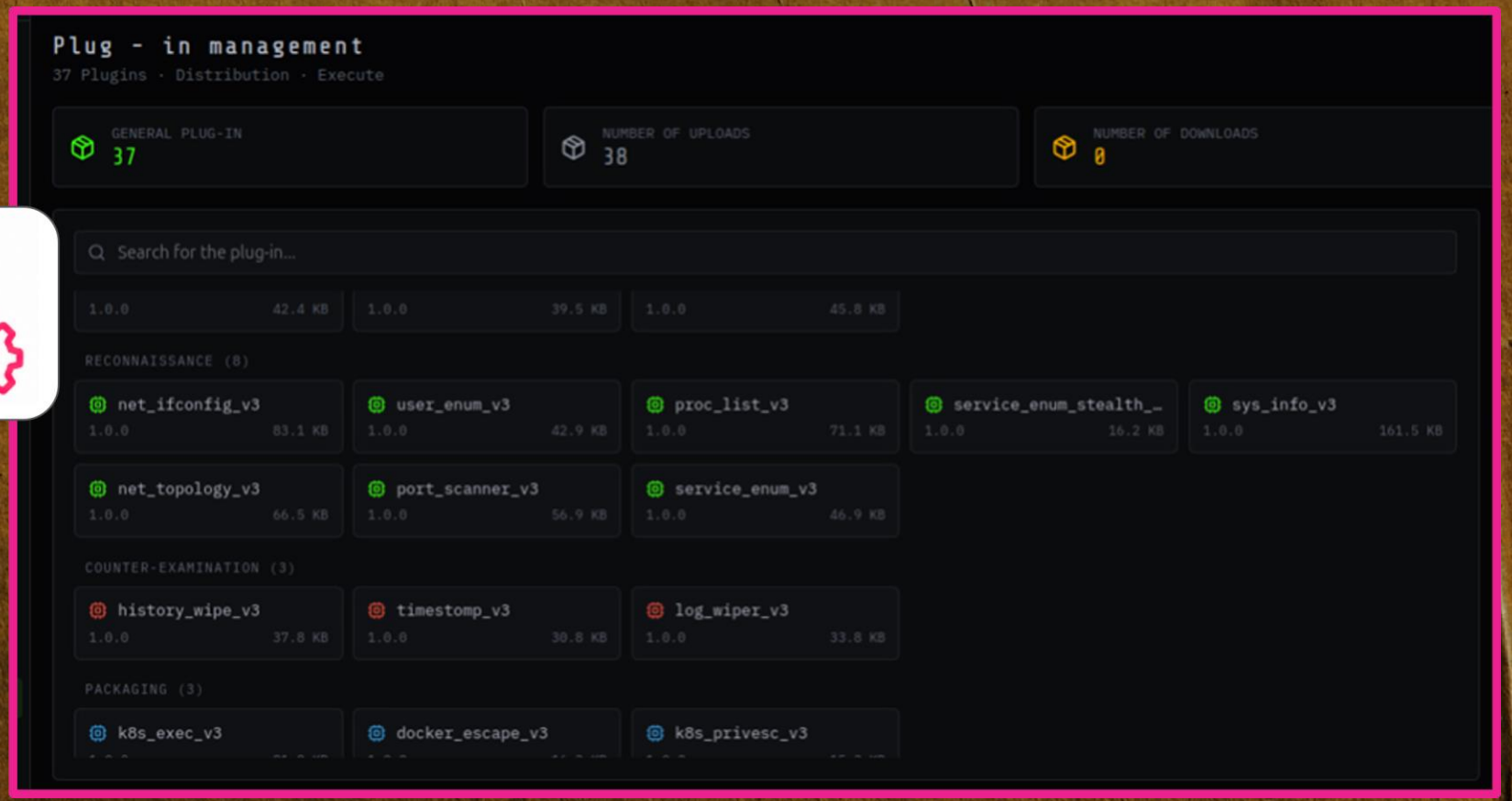
- SSH:
  - Key
  - Configs
- System:
  - Bash history
  - Environment
- Cloud:
  - AWS
  - GCP



Dashboard - Infrastructure



Plugins



BlueHat IL

Plugins

Recon

net topology

port scanner

user enum

sys info

proc list

net ifconfig

service enum stealth

service enum

mount info

BlueHat IL

Plugins

Recon

net topology

port scanner

user enum

sys info

proc list

net ifconfig

service enum stealth

service enum

mount info

Credentials

browser stealer stealth

browser stealer

gpg keys

ssh harvester stealth

ssh_harvester

mimi penguin lite

passwd_dump

keyring dump

BlueHat IL

Plugins

Recon

net topology

port scanner

user enum

sys info

proc list

net ifconfig

service enum stealth

service enum

mount info

Credentials

browser stealer stealth

browser stealer

gpg keys

ssh harvester stealth

ssh_harvester

mimi penguin lite

passwd_dump

keyring dump

Anti Forensics

log wiper

timestomp

history wipe

BlueHat IL

Plugins

Recon

net topology

port scanner

user enum

sys info

proc list

net ifconfig

service enum stealth

service enum

mount info

Credentials

browser stealer stealth

browser stealer

gpg keys

ssh harvester stealth

ssh_harvester

mimi penguin lite

passwd_dump

keyring dump

Anti Forensics

log wiper

timestomp

history wipe

Lateral Movement

port fwd

smb exec

ssh worm

ssh tunnel

BlueHat IL

Plugins

Recon

net topology

port scanner

user enum

sys info

proc list

net ifconfig

service enum stealth

service enum

mount info

Credentials

browser stealer stealth

browser stealer

gpg keys

ssh harvester stealth

ssh_harvester

mimi penguin lite

passwd_dump

keyring dump

Anti Forensics

log wiper

timestomp

history wipe

Lateral Movement

port fwd

smb exec

ssh worm

ssh tunnel

Cloud

k8s exec

k8s privesc

docker escape

BlueHat IL

Plugins

Recon

net topology

port scanner

user enum

sys info

proc list

net ifconfig

service enum stealth

service enum

mount info

Credentials

browser stealer stealth

browser stealer

gpg keys

ssh harvester stealth

ssh_harvester

mimi penguin lite

passwd_dump

keyring dump

Anti Forensics

log wiper

timestomp

history wipe

Lateral Movement

port fwd

smb exec

ssh worm

ssh tunnel

Cloud

k8s exec

k8s privesc

docker escape

Persistence

cron persist

ld preload

systemd persist

BlueHat IL

Plugins

Recon

net topology

port scanner

user enum

sys info

proc list

net ifconfig

service enum stealth

service enum

mount info

Credentials

browser stealer stealth

browser stealer

gpg keys

ssh harvester stealth

ssh_harvester

mimi penguin lite

passwd_dump

keyring dump

Anti Forensics

log wiper

timestomp

history wipe

Lateral Movement

port fwd

smb exec

ssh worm

ssh tunnel

Cloud

k8s exec

k8s privesc

docker escape

Persistence

cron persist

ld preload

systemd persist

Tools

env vars

file mgr

term pty

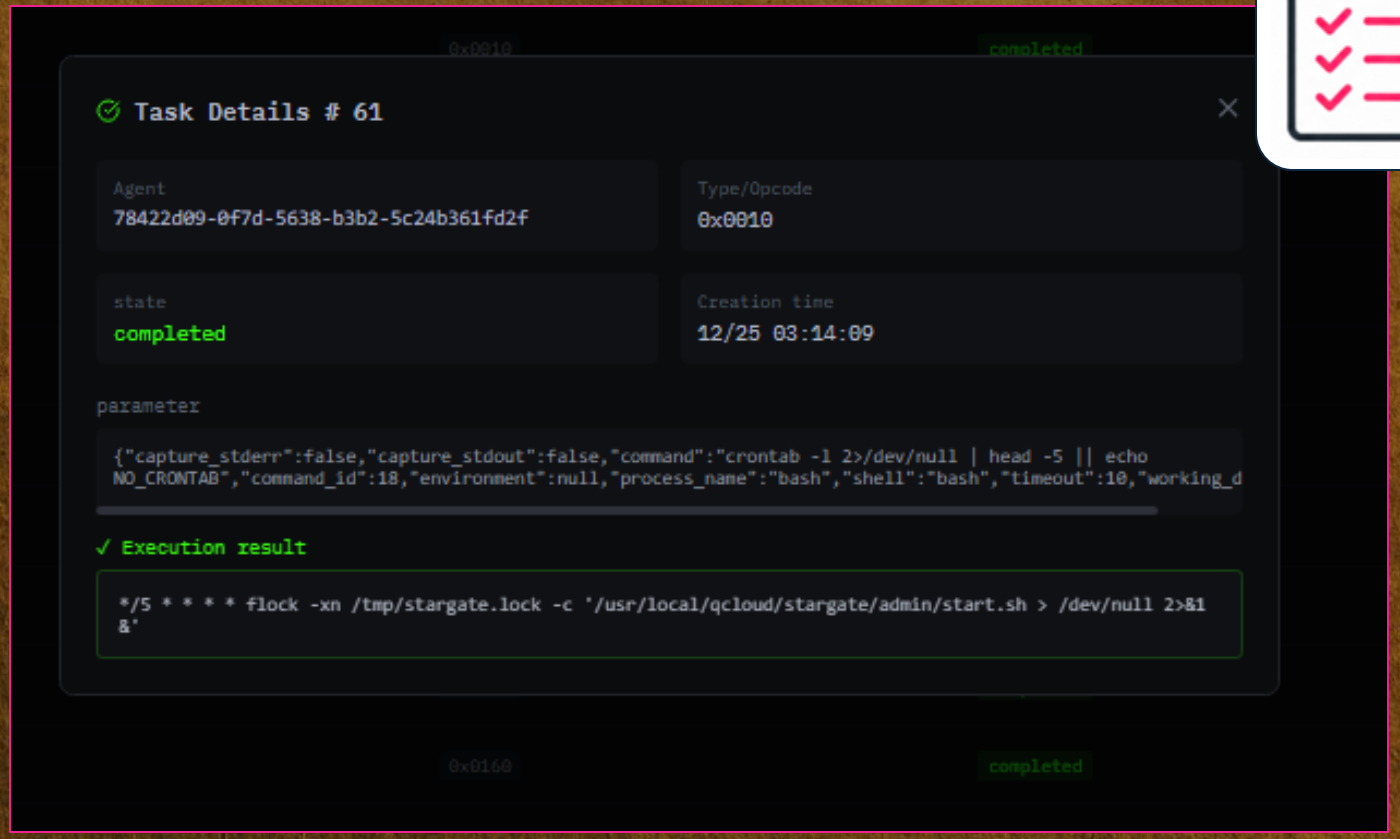
exploit dirty pipe

hello plugin

simple test

BlueHat IL

Task Management



BlueHat IL

OpenDir

Index of /.

- _common
- _frontend
- _persistence
- .font-unix/
- .ICE-unix/
- .implant_started
- .revproxy_debug
- .socks_debug.log
- .Test-unix/
- .ws_debug
- .X11-unix/
- .XIM-unix/
- agent.log
- agent_id.txt
- AliyunAssistClientSingleLock.lock
- backend_update/
- backend_update.tar.gz
- build_resp.json
- bundle_result.json
- bundle_test
- c2-server
- c2-server-debug
- c2-server-debug2
- c2-server-final
- c2-server-fixed
- c2-server.log
- c2.log
- c2_multipart_test.txt

- c2-server
- c2-server-debug
- c2-server-debug2
- c2-server-final
- c2-server-fixed
- c2-server.log
- c2.log
- c2_multipart_test.txt

- c2_update/
- c2_update.tar.gz

OpenDir

Sources

Implant

Backend

Frontend

OpenDir

Logs

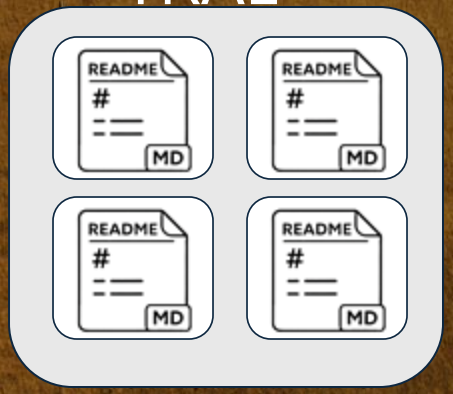
Malware

SSH

Bash History

OpenDir - TRAE

TRAE



VoidLink-2025 文档索引

当前进度: Week 14 (持久化 + 容器逃逸)

目录结构

```
docs/
├── 开发计划/          # 开发计划（仅主计划 + 进度）
│   ├── 当前进度.md                          ← 查看当前任务
│   ├── VoidLink-2025-统一开发计划-v3.1-30周-完整版.md  ← 主计划
│   └── _archive/                           ← 旧版本归档
├── 设计文档/          # 架构设计与模块设计
├── 规范文档/          # 编码规范、接口规范
├── 技术方案/          # 技术实现方案
├── 分析报告/          # 架构分析、功能对照
└── 进度报告/          # 开发进度报告
```

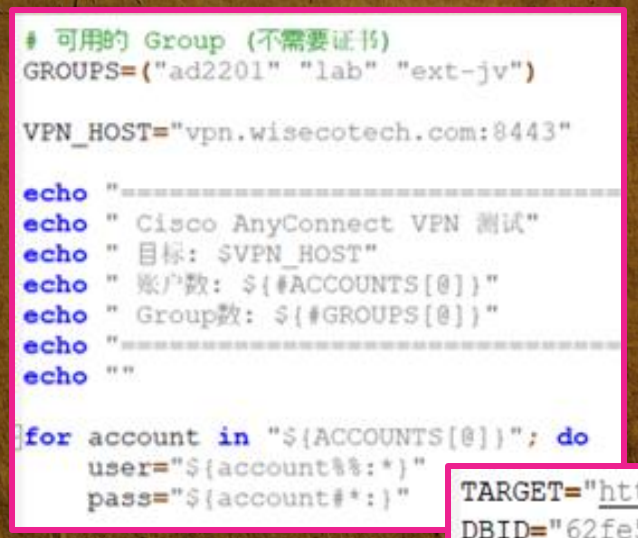
开发计划 (3 份有效)

文档	说明
当前进度.md	⭐ 当前任务 (Week 14)
Week14-30详细任务清单.md	⭐ Week 14-30 详细任务、函数签名、验收标准
VoidLink-2025-统一开发计划-v3.1-30周-完整版.md	⭐ 主计划 (30 周总览)

APT-Commercial-Research?

Real Attacks:

- Custom Scripts to exploit attacks:
  - OWA
  - Cisco VPN
  - RDP
  - Redis
- Other Backdoors:
  - VShell
  - CobaltStrike (old version)
- Targets are Chinese Tech organizations



```
# 可用的 Group (不需要证书)
GROUPS=("ad2201" "lab" "ext-jv")

VPN_HOST="vpn.wisecotech.com:8443"

echo "=================================="
echo " Cisco AnyConnect VPN 测试"
echo " 目标: $VPN_HOST"
echo " 账户数: ${#ACCOUNTS[@]}"
echo " Group数: ${#GROUPS[@]}"
echo "=================================="
echo ""

for account in "${ACCOUNTS[@]}"; do
    user="${account%%:*}"
    pass="${account#*:}"
```

```
TARGET="http://jd.xhytech.com/k3cloud"
DBID="62fe5f222b2a91"

echo "=== K3Cloud SQL 注入测试 ==="

echo "=== 1. ValidateUser SQL 注入 ==="
# 测试用户名参数
```

BlueHat IL

THE DEVELOPER

BlueHat IL

AI At The Core Of VoidLink

AI-Generated

1 Dev + AI

< 1 Week

BlueHat IL

Who's That Coding Agent?

CODEX

CLAUDE Code

???

BlueHat IL


TRAC
BlueHat IL

TRAE Traces

Leaked Files

AI Prompts

Chinese Doc

The Main Prompt & Spec-Driven Development

Seed

BlueHat IL

The Main Prompt & Spec-Driven Development

Seed

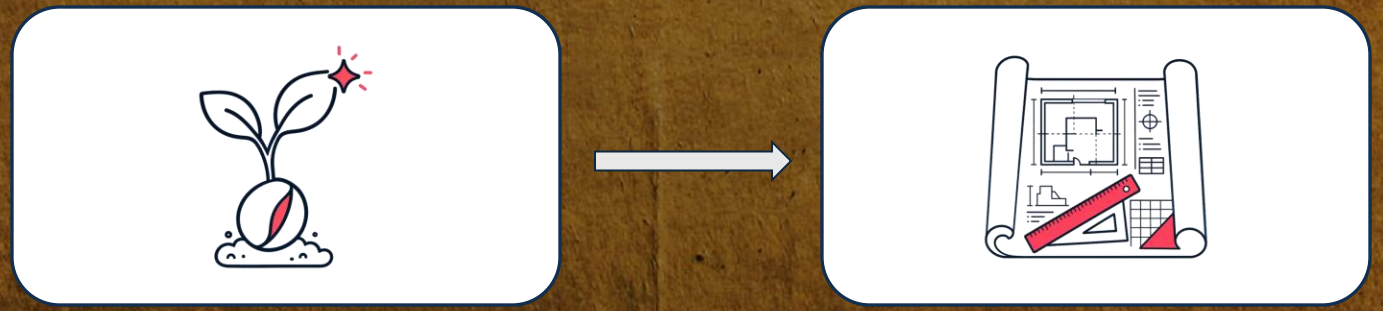
```
## Goals
- Only perform architecture review, security risk analys
- Do not provide or implement technical details of adver
penetration/evasion.

## Data Acquisition
- Please copy `c2_architecture.txt` to the working direc
paste key sections here (table of contents, module descr
specifications).
- I will parse the text in read-only mode to extract str

## Architecture Organization
- Identify high-level components: `Controller/Server/Age
Scheduling/Encryption Module`.
- Draw data flow and call relationships: Task dispatch,
callback, logging and auditing.
- Communication protocols and encryption: Channel types,
rotation strategies, replay and integrity protection.
- Reliability and robustness: Failure retry, reconnectio
limits.
```

BlueHat IL

The Main Prompt & Spec-Driven Development



Seed

Spec

BlueHat IL

The Main Prompt & Spec-Driven Development

Seed

Spec

Code

BlueHat IL

Markdown Residue: AI-Written Plans & Sprints

.md Collection

3 Virtual Teams

Sprint Planning

Specs = Code

Voidlink Reemerges

Written in RUST
But compiled in zig environment

Similar Classes
beacon\relay\comm\evasion…

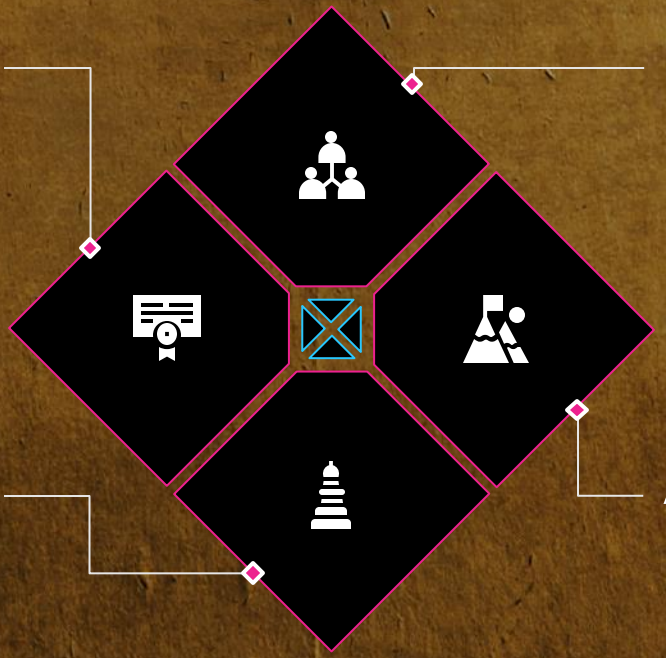
Additional Capabilities
Commands, Exploits, Plugins

Windows implant
same code base

Summary

Capabilities

Cloud-First



OPSEC

AI-Powered

THANK YOU

cp<r>

BlueHat IL