

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

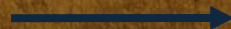


Hunt For eBPF

eBPF
syscall hooking

Hunt For eBPF

eBPF
syscall hooking



VoidLink



Hunt For eBPF



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

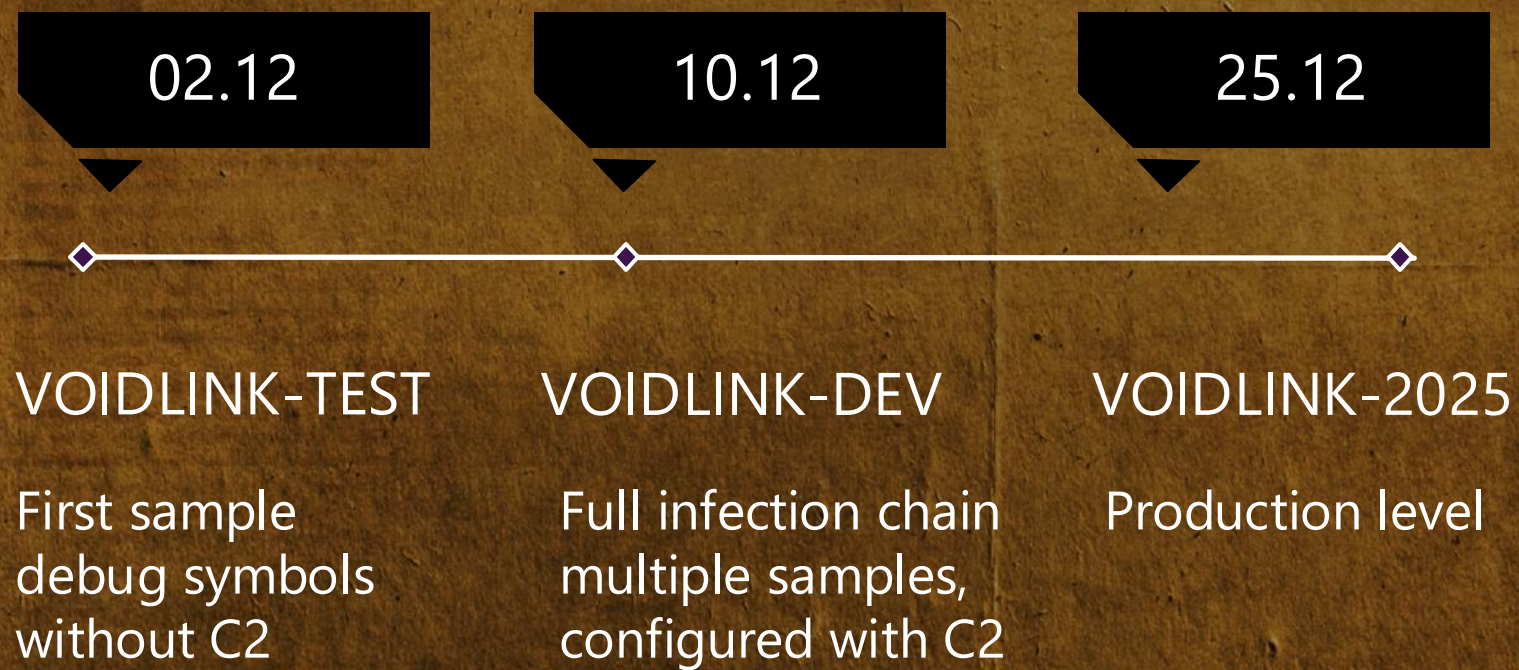
VOIDLINK-TEST

First sample
debug symbols
without C2

VOIDLINK-DEV

Full infection chain
multiple samples,
configured with C2

VoidLink Versions



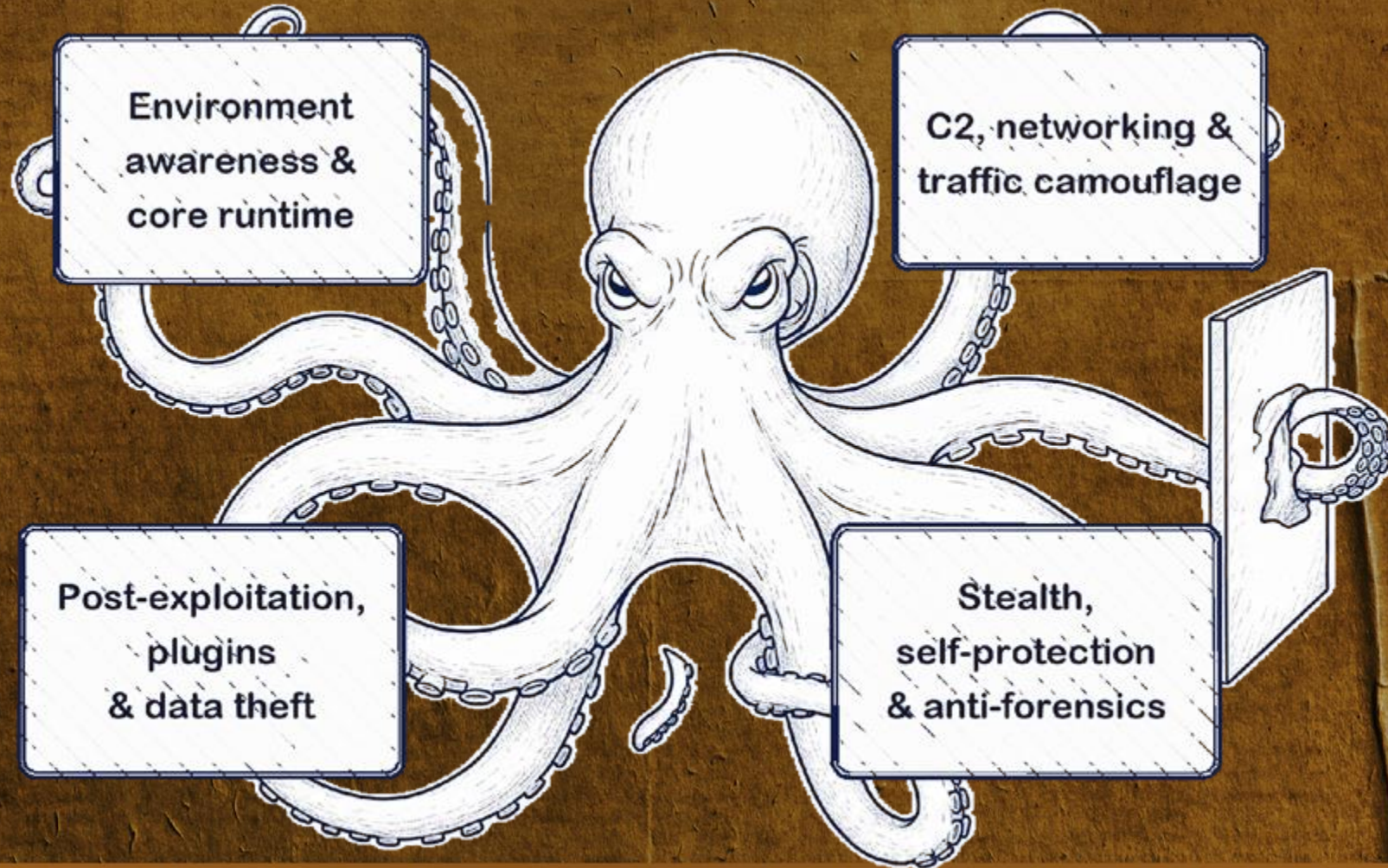
VoidLink Reemerges



THE MALWARE

BLUEHAT IL

VoidLink: Cloud-Native Malware

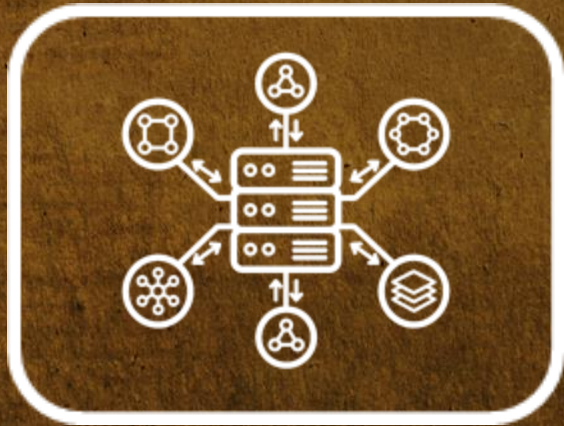


C2, Networking & Traffic Camouflage



Multi-Protocol C2

C2, Networking & Traffic Camouflage



Multi-Protocol C2



Traffic Disguise

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+0 ; "/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+0
; camouflage_http_camouflage_DEFAULT_USER_AGENTS[5]
camouflage_http_camouflage_DEFAULT_USER_AGENTS __u8 <offset __anon_16899, 6Fh>
; DATA XREF: .rodata:00000000010125A0+0 ; "Mozilla/5.0 (Windows NT 10.0; Win64; x64; ...
__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) AppleWebKit"...
__u8 <offset __anon_16909, 50h> ; "Mozilla/5.0 (Windows NT 10.0; Win64; x64"...
__u8 <offset __anon_16913, 54h> ; "Mozilla/5.0 (Macintosh; Intel Mac OS X "...
__anon_16959 dq offset __anon_16932 ; DATA XREF: .rodata:00000000010125B0+0
dq 6 ; "Accept"
dq offset __anon_16934 ; "application/json, text/plain, */*"
dq 21h ; "Accept-Language"
dq offset __anon_16941 ; "Accept-Language"
dq 0Fh ; "en-US,en;q=0.9"
dq offset __anon_16943 ; "Accept-Encoding"
dq 0Eh ; "Accept-Encoding"
dq offset __anon_16950 ; "Accept-Encoding"
dq 0Fh ; "gzip, deflate, br"
dq offset __anon_16952 ; "gzip, deflate, br"
dq 11h ; "Accept-Encoding"
; count u8 off_1012580
off_1012580 dq offset camouflage_http_camouflage_DEFAULT_API_PATHS
; DATA XREF: camouflage_http_camouflage_CamouflageConfig_default+F+0
dq 8 ; "application/json"
dq offset __anon_16894 ; "application/json"
dq 3 ; "application/json"
dq offset camouflage_http_camouflage_DEFAULT_USER_AGENTS
dq 5 ; "application/json"
dq offset __anon_16751 ; "application/json"
dq 10h ; "_ga"
dq offset __anon_16929 ; "_ga"
dq 3 ; "_ga"
dq offset __anon_16959 ; "_ga"
dq 3 ; "_ga"
```

API routes

User-Agents

Headers and Cookies

Stealth, Self-Protection & Anti-Forensics



Rootkit

Stealth, Self-Protection & Anti-Forensics



Anti-Analysis



Rootkit

Stealth, Self-Protection & Anti-Forensics



Anti-Analysis



Anti-Forensics



Rootkit

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 )
```

Environment & Core Runtime

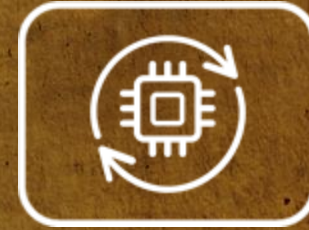


Fingerprinting

Environment & Core Runtime



Fingerprinting

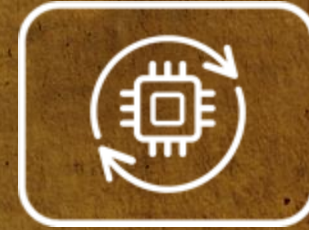


Adaptive

Environment & Core Runtime



Fingerprinting



Adaptive



Behavior

Environment & Core Runtime



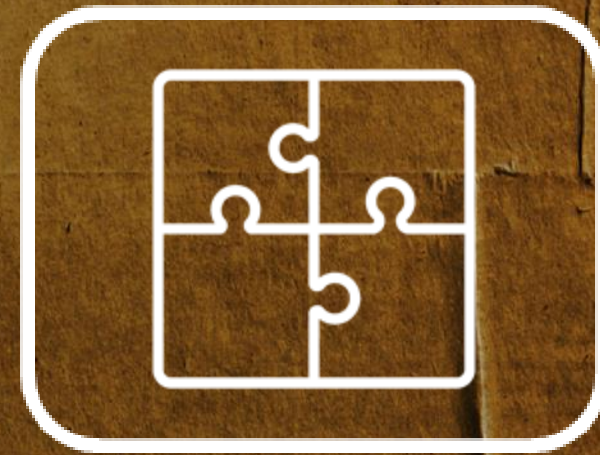
Environment Awareness

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;
}
```

Post-Exploitation, Plugins & Data Theft

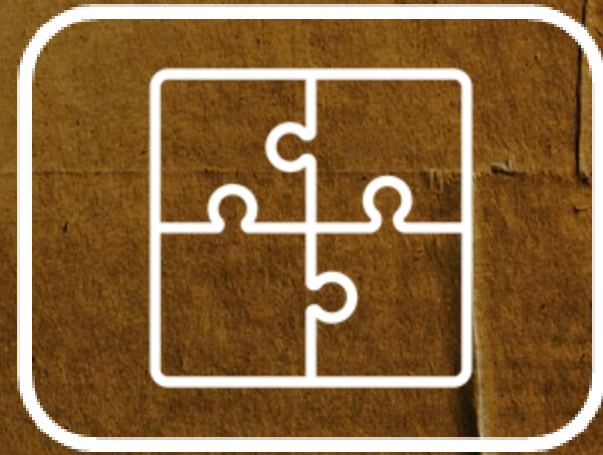


Modular

Post-Exploitation, Plugins & Data Theft



Plugins



Modular

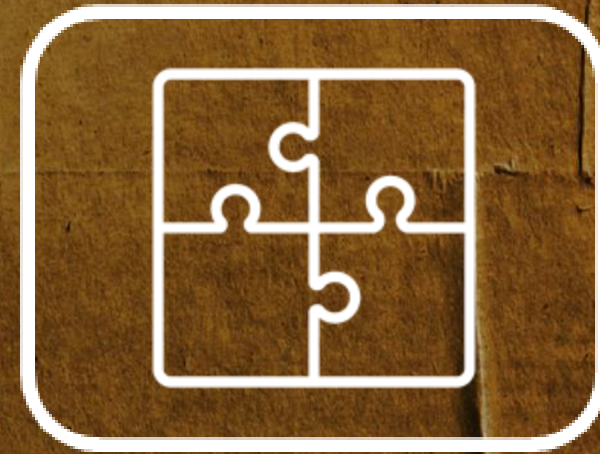
Post-Exploitation, Plugins & Data Theft



Plugins

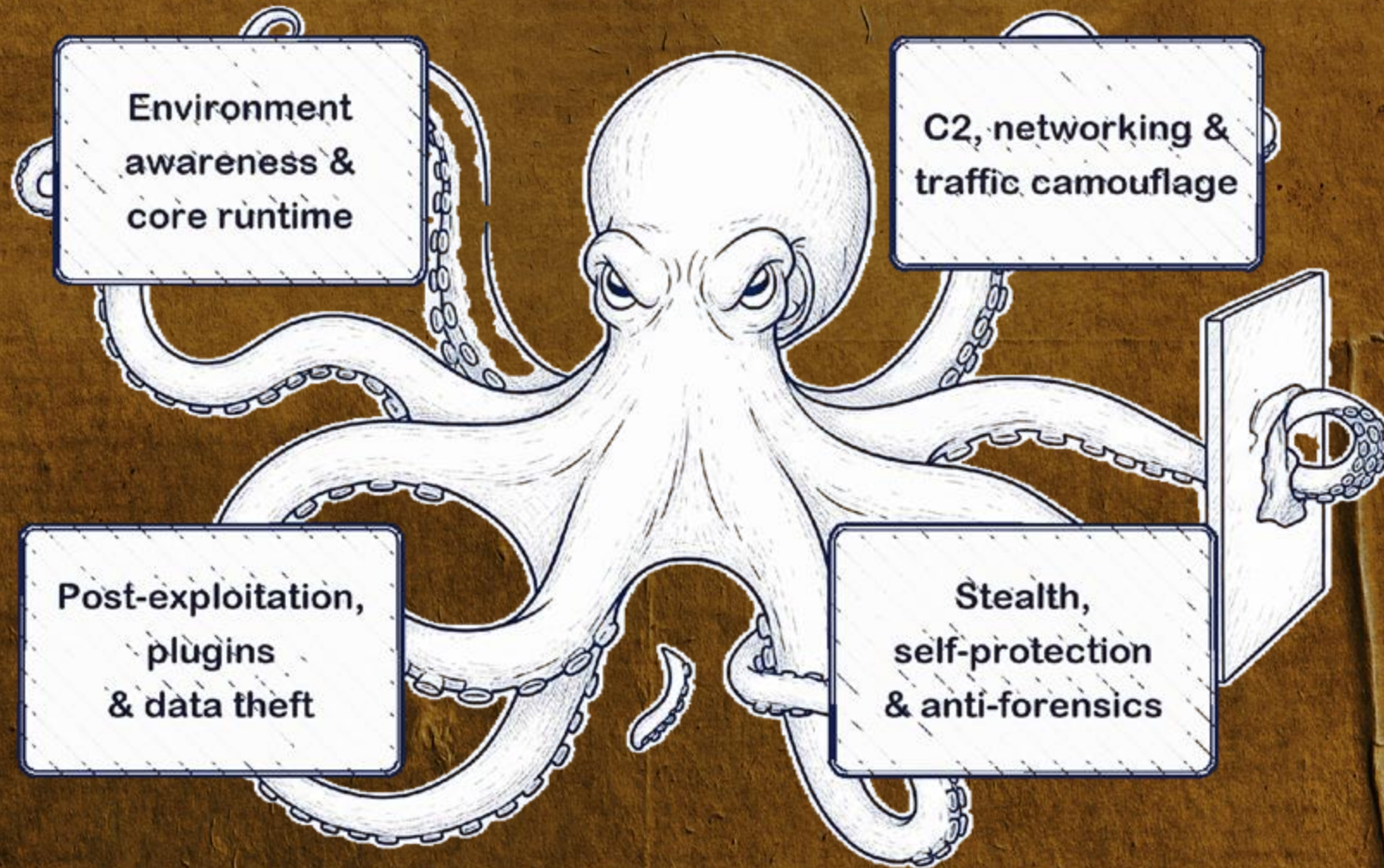


Exfiltration



Modular

VoidLink: Cloud-Native Malware



THE ATTACKER

BLUEHAT IL

VoidLink - Attacker View



VOIDLINK 已连接 4 / 4 连接

仪表盘

系统概览

- 在线主机: 4 / 4
- 僵尸主机: 0
- 僵尸进程: --
- 僵尸任务: 0

在线主机

4 个主机

主机	地址	IP	用户	端口
●	1.12.64.161-51638	1.12.64.161:51638	-	关闭
●	1.12.64.161-52428	1.12.64.161:52428	-	关闭
●	159.75.231.220-41524	159.75.231.220:41524	-	关闭
●	1.12.64.161-52296	1.12.64.161:52296	-	关闭

系统资源

- CPU: 0%
- 内存: 0%

离线主机

0 个主机

所有主机均离线

2023-10-23 18:01:00

Dashboard - Three Panels

Dashboard

Attack

Infrastructure

The screenshot shows the VOIDLINK dashboard interface. The top navigation bar includes the VOIDLINK logo and a status indicator showing '已连接' (Connected) with '4 / 4' devices online. The main content area is divided into three sections, each highlighted with a pink border:

- Dashboard Panel:** Contains a sidebar menu with '仪表盘' (Dashboard) selected, '接入点' (Access Points), '终端' (Terminals), and '生成器' (Generators).
- Attack Panel:** Contains a sidebar menu with '侦察' (Reconnaissance), '光谱' (Spectrum), '持久化' (Persistence), '横向移动' (Lateral Movement), '逻辑注入' (Logic Injection), '池数据流' (Pool Data Flow), and '反取证' (Anti-Forensics).
- Infrastructure Panel:** Contains a sidebar menu with '设备管理' (Device Management), '文件管理' (File Management), '操作' (Operations), '任务管理' (Task Management), and '设置' (Settings).

The main content area displays the '仪表盘' (Dashboard) section, which includes a '系统概览' (System Overview) card showing '4 / 4' devices online, and a table titled '在线接入点' (Online Access Points) with 4 entries:

状态	主机名
●	1.12.64.161:51638
●	1.12.64.161:52428
●	159.75.233.220:41524
●	1.12.64.161:52298

Dashboard

✓ VOIDLINK

☰ dashboard

☒ Implant

>_ Terminal

📦 Generator

Dashboard - Builder

Features:

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

```
One word generator.  
Generate an implant-in-one-sent-on command
```

Building a configuration

TARGET

Bundle (完整包) ▾

COMMUNICATION CONFIGURATION

AGREEMENT

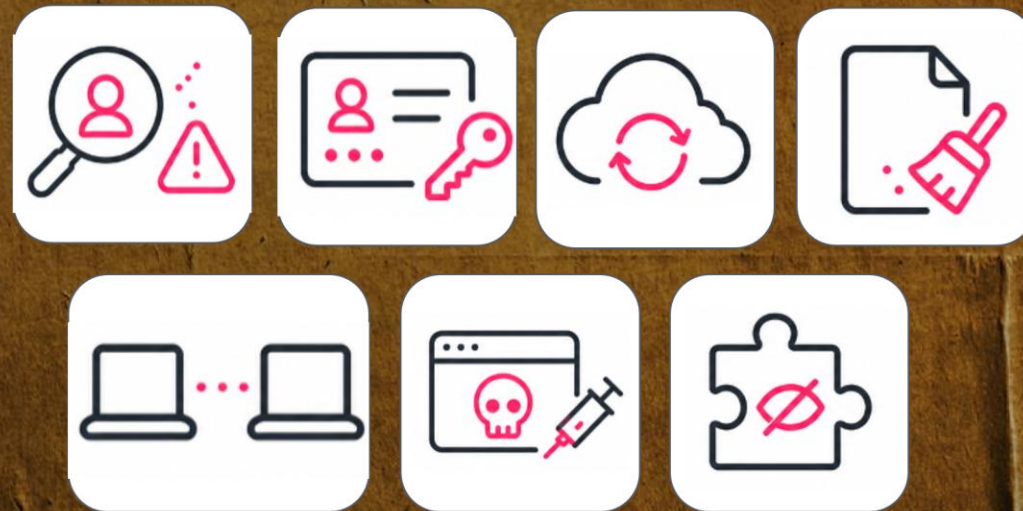
自动选择 ▾

HEART RATE INTERVAL (SECONDS) 60 ⚙

SHAKE (SECONDS) 15 ⚙

Dashboard - Attack

- ATTACK MODULE
- 🔍 Reconnaissance
 - 🔑 Evidence
 - ⚓ Persistence
 - 🔗 Horizontal movement
 - 💉 Process injection
 - 🛡️ Concealed Modules
 - 🗑️ Counter-evidence



Dashboard - Rootkit



ATTACK MODULE

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

Concealed Modules

LKM · eBPF · Process/Port/File Hide

Selecting the target... ▾

Overview **Quickly hidden.** EDR Scanner

Hidden port

Hide from netstat/ss output

Port number (such as 443)

The Hidden Process

Hiding from ps/top output

PID (as in 1234)

Hiding the file

Hiding from the ls/find output

/path/to/file

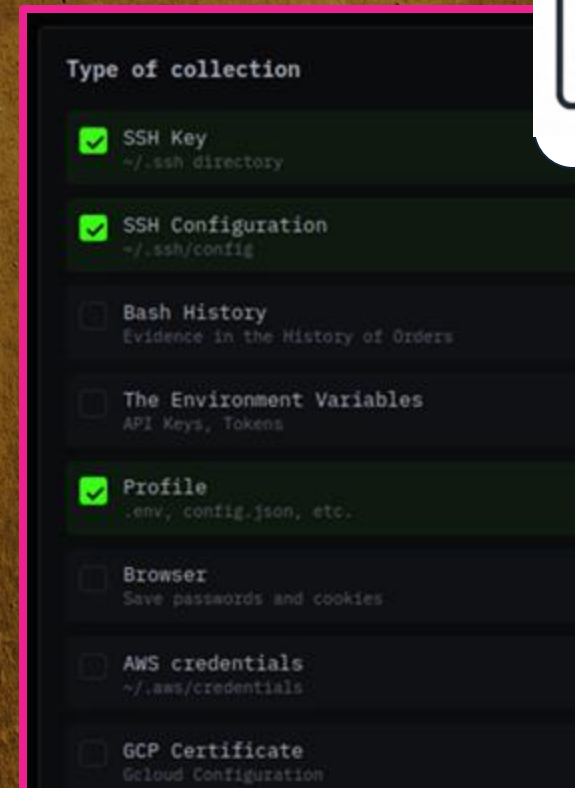
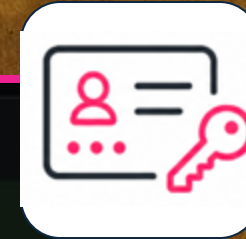
Hiding an executable file

Hide the /proc/PID/exe symbolic link

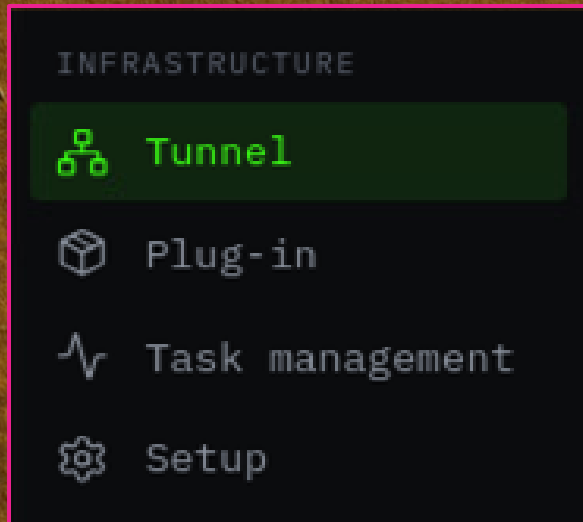
/path/to/binary

Dashboard - Credentials

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



Dashboard - Infrastructure



Plugins



Plug - in management
37 Plugins · Distribution · Execute

GENERAL PLUG-IN 37 NUMBER OF UPLOADS 38 NUMBER OF DOWNLOADS 0

Q Search for the plug-in...

1.0.0	42.4 KB	1.0.0	39.5 KB	1.0.0	45.8 KB
RECONNAISSANCE (8)					
@ net_ifconfig_v3 1.0.0 83.1 KB	@ user_enum_v3 1.0.0 42.9 KB	@ proc_list_v3 1.0.0 71.1 KB	@ service_enum_stealth_ 1.0.0 16.2 KB	@ sys_info_v3 1.0.0 161.5 KB	
@ net_topology_v3 1.0.0 66.5 KB	@ port_scanner_v3 1.0.0 56.9 KB	@ service_enum_v3 1.0.0 46.9 KB			
COUNTER-EXAMINATION (3)					
@ history_wipe_v3 1.0.0 37.8 KB	@ timestomp_v3 1.0.0 30.8 KB	@ log_wiper_v3 1.0.0 33.8 KB			
PACKAGING (3)					
@ k8s_exec_v3	@ docker_escape_v3	@ k8s_privesc_v3			

Plugins

Recon



net topology

port scanner

user enum

sys info

proc list

net ifconfig

service enum stealth

service enum

mount info

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



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



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



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



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



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

Task Management



0x0010 completed

✔ Task Details # 61 ✕

Agent 78422d09-0f7d-5638-b3b2-5c24b361fd2f	Type/Opcode 0x0010
state completed	Creation time 12/25 03:14:09

parameter

```
{"capture_stderr":false,"capture_stdout":false,"command":"crontab -l 2>/dev/null | head -5 || echo NO_CRONTAB","command_id":18,"environment":null,"process_name":"bash","shell":"bash","timeout":10,"working_d
```

✔ Execution result

```
* /5 * * * * flock -xn /tmp/stargate.lock -c '/usr/local/qcloud/stargate/admin/start.sh > /dev/null 2>&1 &'
```

0x0160 completed

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

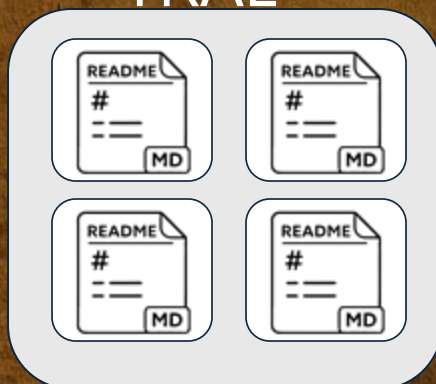


Bash History



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
```

THE DEVELOPER

BLUEHAT IL

AI At The Core Of VoidLink



AI-Generated



1 Dev + AI



< 1 Week

Who's That Coding Agent?



CODEX



CLAUDE Code



???

TRAE

BLUEHAT IL

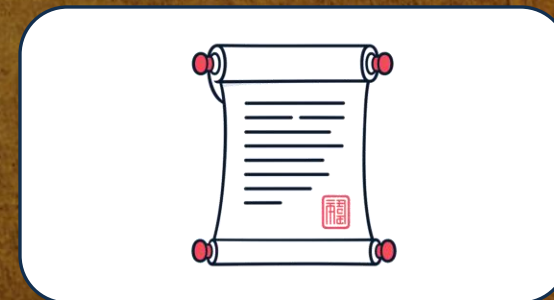
TRAE Traces



Leaked Files



AI Prompts



Chinese Doc

The Main Prompt & Spec-Driven Development



Seed

The Main Prompt & Spec-Driven Development



Seed

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

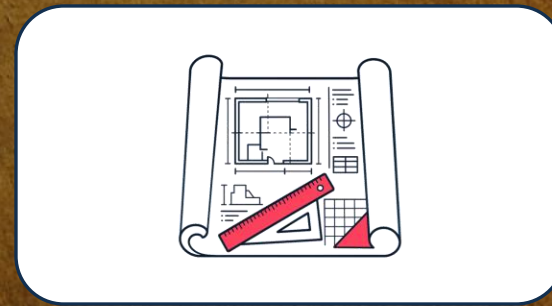
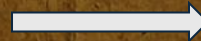
## Data Acquisition
- Please copy `c2_architecture.txt` to the working directory and
paste key sections here (table of contents, module descriptions,
specifications).
- I will parse the text in read-only mode to extract structured
data.

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

The Main Prompt & Spec-Driven Development

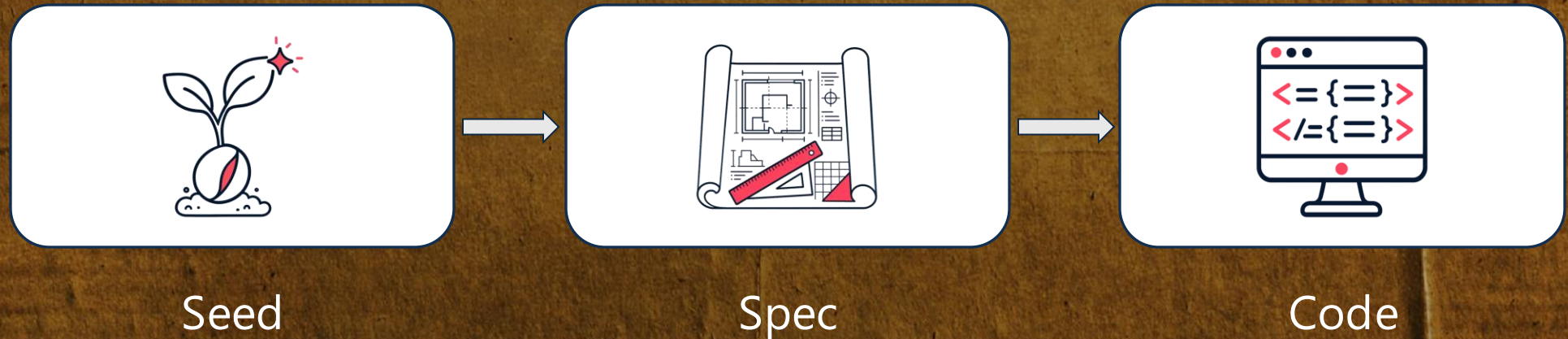


Seed



Spec

The Main Prompt & Spec-Driven Development



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...

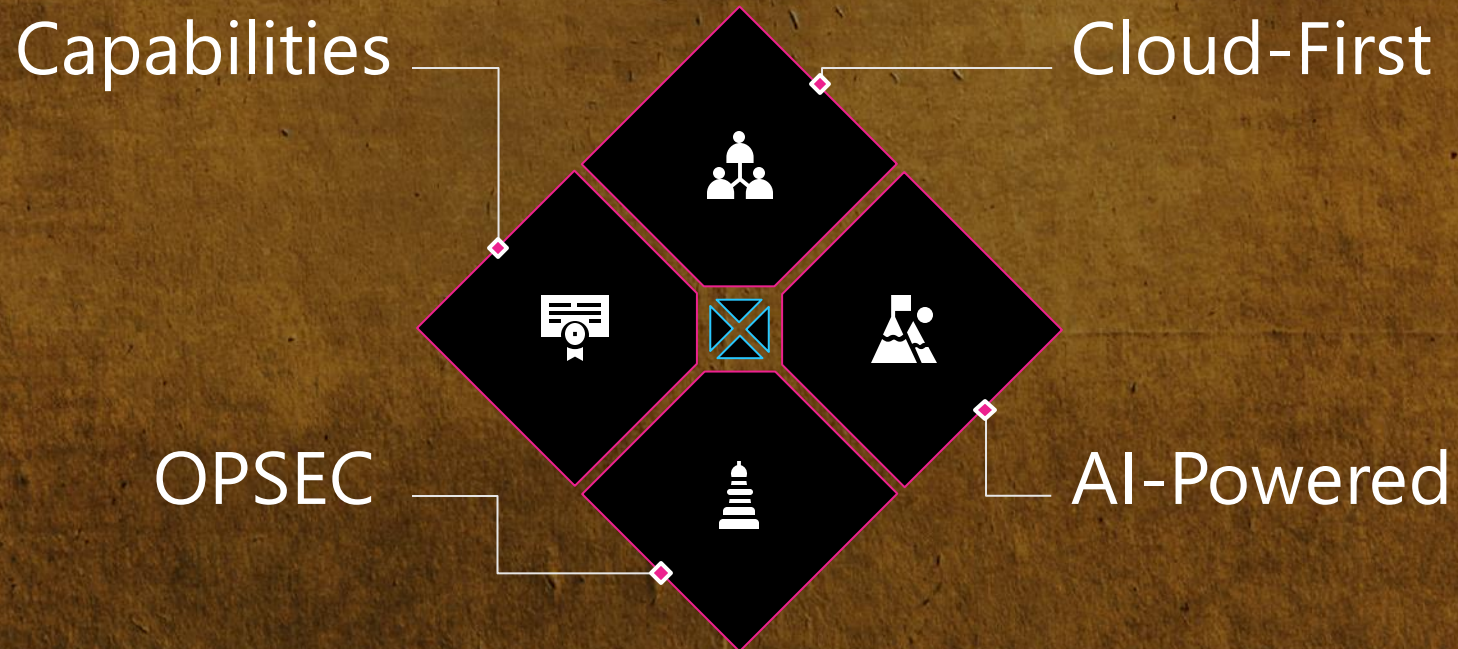
Additional Capabilities

Commands, Exploits, Plugins

Windows implant

same code base

Summary



THANK YOU

cp<r>

BLUEHAT IL