



HITCON '25

# The Evolving Bloodline: Revealing the Hidden Operations of BloodAlchemy

---

Suguru Ishimaru, ITOCHU Cyber & Intelligence Inc.

You Nakatsuru, Sophos

Kiyotaka Tamada, Sophos

# About Us



**Suguru Ishimaru**

Executive Cybersecurity Researcher

ITOCHU Cyber & Intelligence Inc.



**You Nakatsuru**

Principal Threat Researcher



**Kiyotaka Tamada**

Principal Threat Researcher

Counter Threat Unit, Sophos  
(Formerly Secureworks)

# Agenda

---

The Malicious Bloodline

---

Diving into DeedRAT and BloodAlchemy

---

Unveiling Additional Modules

---

Attack Campaigns Involving DeedRAT/BloodAlchemy

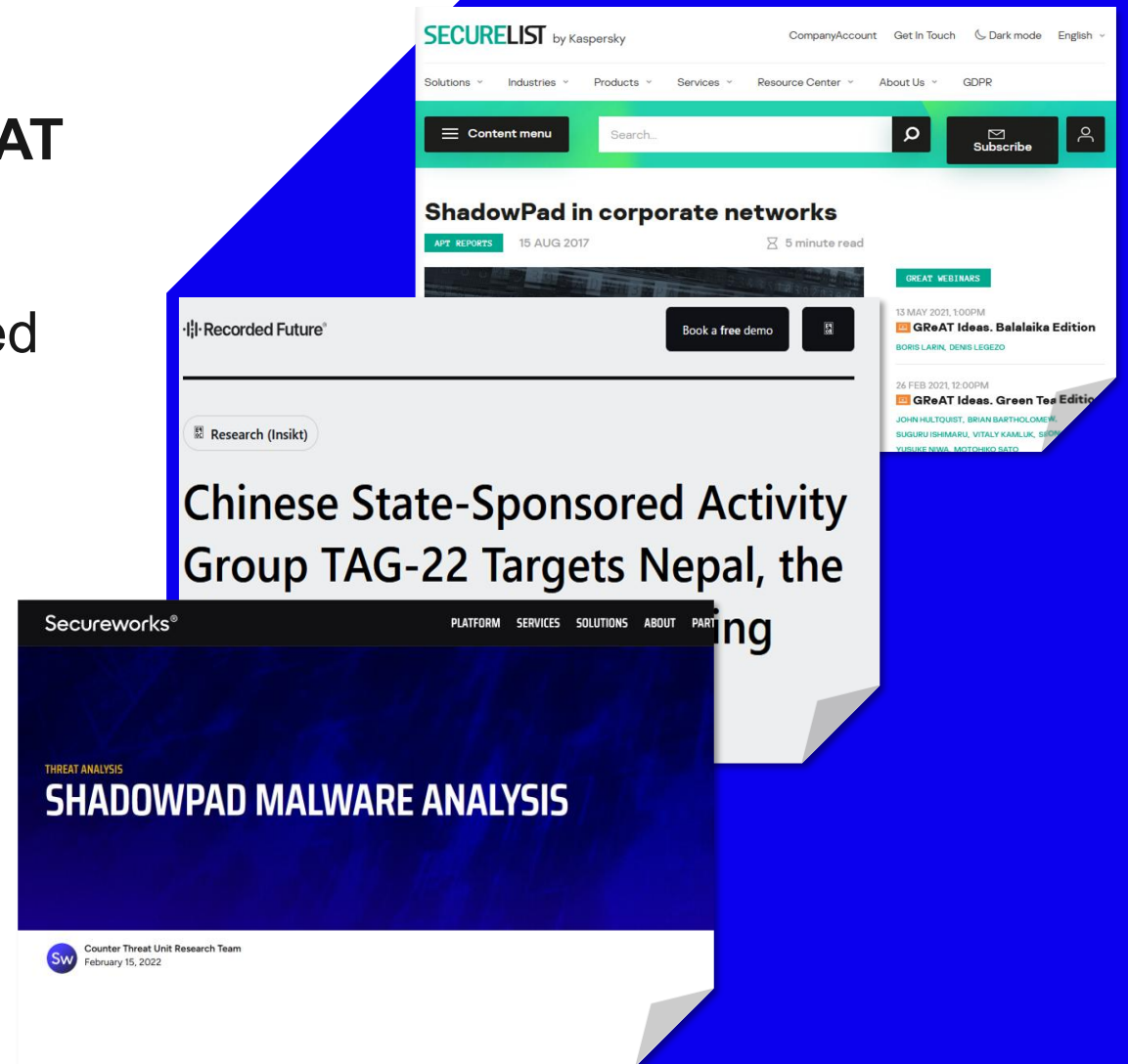
---

Conclusions

# The Malicious Bloodline

# Notorious Malware ShadowPad

- ShadowPad is a **sophisticated modular RAT**
- Discovered in a supply chain attack in 2017
- Since 2020, It has been reported as a shared malware by **multiple Chinese-speaking actors**:
  - BRONZE ATLAS (APT41)
  - BRONZE BUTLER (Tick)
  - Tonto
  - TropicTrooper
  - Etc...



# DeedRAT Overview

- DeedRAT (a.k.a SNAPPYBEE) is a **variant of ShadowPad**
- Published by Positive Technologies in 2022 and has been observed since 2019
- The name DeedRAT originates from the magic bytes **0xDEED**
- Used in several campaigns linked to Chinese-speaking actors

## Space Pirates: a look into the group's unconventional techniques, new attack vectors, and tools

PT EXPERT SECURITY CENTER 23 JULY 2023

### Analytics articles

9 November 2024

Cybersecurity threatscape for African countries: Q1 2023–Q3 2024

26 October 2024

Iran's cybersecurity threatscape for 2021-H1 2024

22 October 2024

India: cyberthreat landscape Q3 2023-Q3 2024



### Contents

- Introduction
- 1. Investigating the network infrastructure
- 2. Analysis of the malware and tools
  - 2.1. Deed RAT
  - 2.2. Voidoor
    - 2.2.1. Preparatory phase
    - 2.2.2. Talking to GitHub repositories
    - 2.2.3. Gaining persistence
    - 2.2.4. Talking to the voidtools forum
    - 2.2.5. GitHub-based C&C server
    - 2.2.6. Some facts about the developer of the tool
  - 2.3. Other tools
- Conclusion
- Applications

<https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/space-pirates-a-look-into-the-group-s-unconventional-techniques-new-attack-vectors-and-tools>

# BloodAlchemy Overview

- BloodAlchemy is **another variant** of DeedRAT/ShadowPad
- First reported by Elastic Security Labs in 2023
- It is **exceptionally rare to find**
- The name BloodAlchemy seems to originate from the magic number 0xAB too
- A C2 overlaps the IoCs of Earth Estries

Researcher Blog  
ITOCHU Cyber & Intelligence Inc.

Top About Us

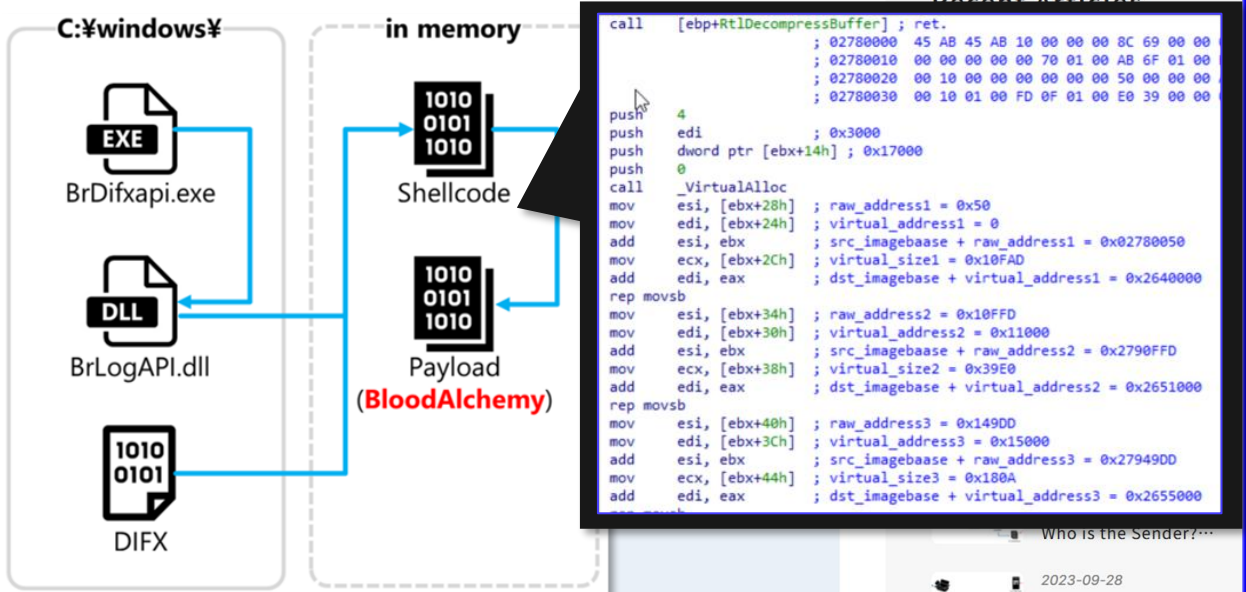
2024-05-23

## Malware Transmutation! - Unveiling the Hidden Traces of BloodAlchemy

Subscribe

Subscribe

Recent Articles



```
call [ebp+RtlDecompressBuffer] ; ret.  
; 02780000 45 AB 45 AB 10 00 00 00 8C 69 00 00  
; 02780010 00 00 00 00 00 70 01 00 AB 6F 01 00  
; 02780020 00 10 00 00 00 00 00 50 00 00 00  
; 02780030 00 10 01 00 FD 0F 01 00 E0 39 00 00  
  
push 4  
push edi ; 0x3000  
push dword ptr [ebx+14h] ; 0x17000  
push 0  
call _VirtualAlloc  
mov esi, [ebx+28h] ; raw_address1 = 0x50  
mov edi, [ebx+24h] ; virtual_address1 = 0  
add esi, ebx ; src_imagebase + raw_address1 = 0x02780050  
mov ecx, [ebx+2Ch] ; virtual_size1 = 0x10FAD  
add edi, eax ; dst_imagebase + virtual_address1 = 0x2640000  
rep movsb  
mov esi, [ebx+34h] ; raw_address2 = 0x10FFD  
mov edi, [ebx+30h] ; virtual_address2 = 0x11000  
add esi, ebx ; src_imagebase + raw_address2 = 0x2790FFD  
mov ecx, [ebx+38h] ; virtual_size2 = 0x39E0  
add edi, eax ; dst_imagebase + virtual_address2 = 0x2651000  
rep movsb  
mov esi, [ebx+40h] ; raw_address3 = 0x149DD  
mov edi, [ebx+3Ch] ; virtual_address3 = 0x15000  
add esi, ebx ; src_imagebase + raw_address3 = 0x27949DD  
mov ecx, [ebx+44h] ; virtual_size3 = 0x180A  
add edi, eax ; dst_imagebase + virtual_address3 = 0x2655000
```

Who is the Sender?

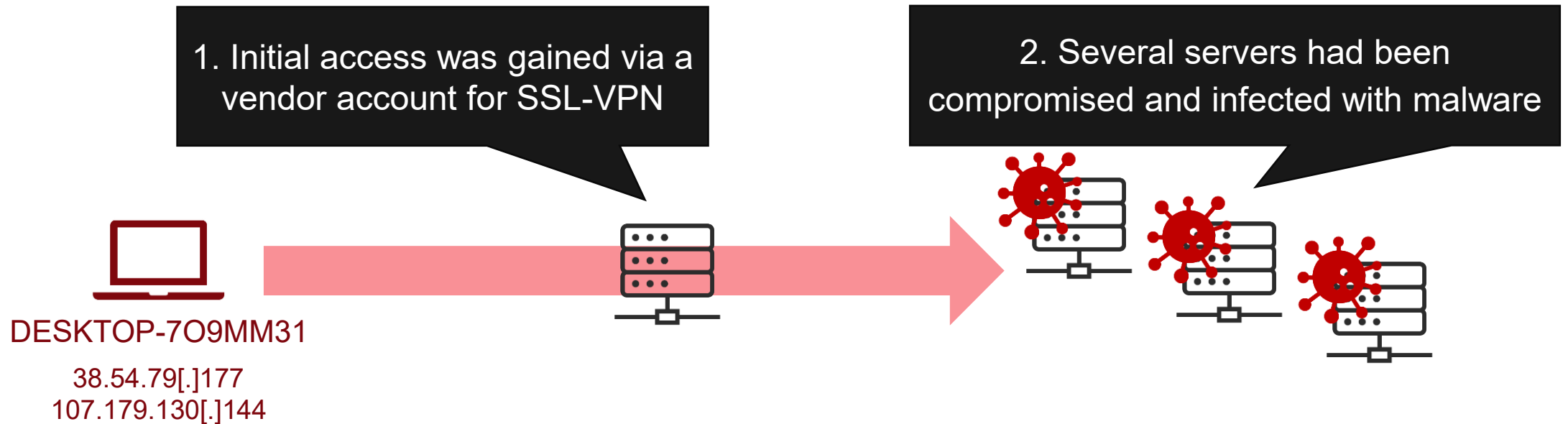
2023-09-28

<https://blog-en.itochuci.co.jp/entry/2024/05/23/090000>

# The Beginning of Our Investigation

Discovering the unknown entity called BloodAlchemy

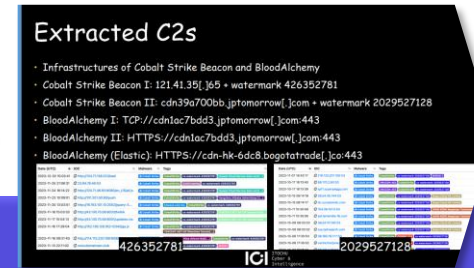
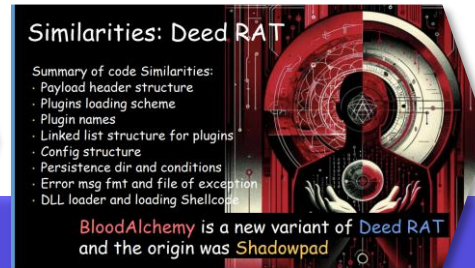
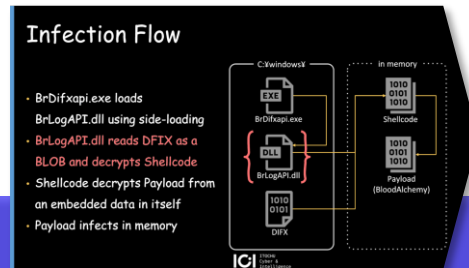
- In May 2023, we observed an APT activity and investigated it deeply
- **BloodAlchemy** was found from the one of the compromised servers



# Previous Research on BloodAlchemy

[https://www.botconf.eu/wp-content/uploads/formidable/2/BOTCONF2024-NiwaIshimaruSato-IntotheVapor\\_ICI.pdf](https://www.botconf.eu/wp-content/uploads/formidable/2/BOTCONF2024-NiwaIshimaruSato-IntotheVapor_ICI.pdf)

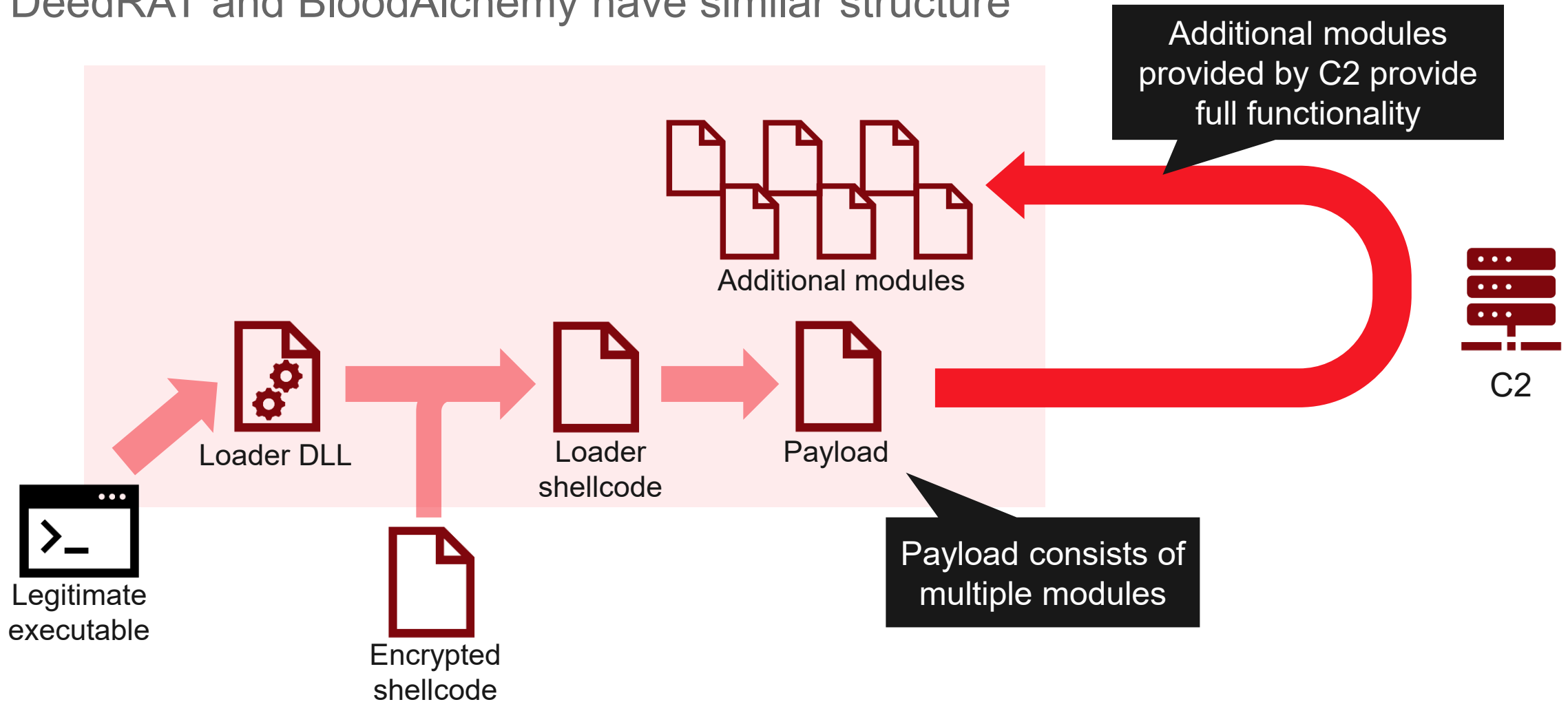
- The details of the initial infection vector
- Analyzed the features and characteristics of the BloodAlchemy
- Revealed it as a **variant of DeedRAT**, originally derived from **ShadowPad**
- Tracked the actor's infrastructures to identify potential C2 servers



# Diving into DeedRAT and BloodAlchemy

# ShadowPad Modular Malware

DeedRAT and BloodAlchemy have similar structure



# Known Similarities – Module Header, Code, etc.

See: <https://blog-en.itochuci.co.jp/entry/2024/05/23/090000>

## DeedRAT

| offset | descriptions                                                                                                                                                                                                                                                                                                                                                                                                                                             | data        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 0x00   | magic number                                                                                                                                                                                                                                                                                                                                                                                                                                             | 54 45 ED DE |
| 0x04   | plugin id                                                                                                                                                                                                                                                                                                                                                                                                                                                | 0x20        |
| 0x08   | entry point                                                                                                                                                                                                                                                                                                                                                                                                                                              | 0x1740      |
| 0x0c   | original base                                                                                                                                                                                                                                                                                                                                                                                                                                            | 0x400000    |
| 0x10   | <pre>// %ALLUSERSPROFILE%\error.log // fmt: // %4.4d-%2.2d-%2.2d %2.2d:%2.2d:%2.2d Exception Address: 0x%p, Code: 0x%8.8x int __stdcall c_write_error_log(_DWORD **a1)</pre>                                                                                                                                                                                                                                                                             |             |
| 0x14   | <pre>{ void (*v1)(void); // eax char v3[1024]; // [esp+0h] [ebp-418h] BYREF __int16 v4[8]; // [esp+400h] [ebp-18h] BYREF int v5[2]; // [esp+410h] [ebp-8h] BYREF</pre>                                                                                                                                                                                                                                                                                   |             |
| 0x18   | <pre> v5[0] = 0; v5[1] = 0; if ( getprocaddrbyhash(&amp;p_GetLocalTime, &amp;e_GetLocalTime) )     p_GetLocalTime(v4); dec(&amp;format_4_4d_2_2d); v1 = p_user32_wsprintfA(v3, v5[0], v4[0], v4[1], v4[3], v4[4], v4[5], v4[6], v1()); if ( getprocaddrbyhash(&amp;kernel32_OutputDebugStringA, &amp;e_outputdebugstringA) )     kernel32_OutputDebugStringA(v3); write_error_log(v3); // %ALLUSERSPROFILE%\error.log c_c_localfree(v5); return 0;</pre> |             |
| 0x1c   |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |             |

## BloodAlchemy

| offset | descriptions                                                                                                                                                                                                                                                                                                                                                                                                       | data        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 0x00   | magic number                                                                                                                                                                                                                                                                                                                                                                                                       | 45 AB 45 AB |
| 0x04   | plugin id?                                                                                                                                                                                                                                                                                                                                                                                                         | 0x10        |
| 0x08   | entry point                                                                                                                                                                                                                                                                                                                                                                                                        | 0x698c      |
| 0x0c   | original base?                                                                                                                                                                                                                                                                                                                                                                                                     | 0x400000    |
| 0x10   | <pre>// %ALLUSERSPROFILE%\error.log // fmt: // %4.4d-%2.2d-%2.2d %2.2d:%2.2d:%2.2d Exception Address: 0x%p, Code: 0x%8.8x int __stdcall c_write_error_log(int **arg0)</pre>                                                                                                                                                                                                                                        |             |
| 0x14   | <pre>{ int ModuleHandleA; // eax int v3; // [esp-4h] [ebp-424h] char v4[1024]; // [esp+4h] [ebp-41Ch] BYREF int a1[3]; // [esp+404h] [ebp-1Ch] BYREF __int16 v6[8]; // [esp+410h] [ebp-10h] BYREF</pre>                                                                                                                                                                                                            |             |
| 0x18   | <pre> memset(a1, 0, sizeof(a1)); dec_0(a1, &amp;format_4_4d_2_2d, 0x62u); p_kernel32_GetLocalTime(v6); j_memset(v4, 0, sizeof(v4)); v3 = **arg0; ModuleHandleA = kernel32_GetModuleHandleA(0, (*arg0)[3]); p_user32_wsprintfA(v4, a1[0], v6[0], v6[1], v6[3], v6[4], v6[5], v6[6], Module kernel32_OutputDebugStringA(v4, v3); write_error_log(v4); // %ALLUSERSPROFILE%\error.log j_memclear_localfree(a1);</pre> |             |
| 0x1c   |                                                                                                                                                                                                                                                                                                                                                                                                                    |             |

# Another Examples of Code Similarity

Initial  
code of  
C2 main  
routine

Module  
entry

## DeedRAT

```
lea ecx, [ebp+recv_data]
call aa_zeromemory_0
and [ebp+netsocket_class], 0
call aa_SetErrorMode_SEM_FAILCRITIC
call aa_SetErrorMode_SEM_FAILCRITIC
call aa_SetErrorMode_SEM_FAILCRITIC
call aa_check_working_hours
lea ecx, [edi+aa_network.c2_url] ;
mov edx, ebx ; lpString2
call aa_lstrcpyA_1
cmp [ebp+proxy], 0
jz short loc_20101E
mov edx, [ebp+proxy]
lea ecx, [edi+aa_network.proxy]
pu
ca
loc_1903F4: ; CODE XREF: aa_init_module
push offset aConfig ; "Config"
lea ecx, [ebp+lpString2]
mov [ebp+lpString2], esi
mov [ebp+var_4], esi
call aa_decode_string_0
mov edx, offset aLstrcpyw_0 ; "lstrcpyW"
mov ecx, offset lstrcpyW
call aa_get_proc_address_kernel32_0
test eax, eax
jz short loc_190426
push [ebp+lpString2] ; lpString2
push [ebp+lpString1] ; lpString1
call ds:lstrcpyW
loc_190426: ; CODE XREF: aa_init_module
lea ecx, [ebp+lpString2]
call aa_free_8
jmp short loc_190461
; -----
case_2: ; CODE XREF: aa_init_module
mov eax, [ebp+lpString1]
mov dword ptr [eax], 40h
jmp short loc_190461
; -----
case_1: ; CODE XREF: aa_init_module
mov eax, [ebp+lpString1]
mov ds:offset_aa_func_0, eax
mov ds:module_config_func_table.get_config, off
mov ds:module_config_func_table.get_reg_data, o
mov ds:module_config_func_table.exec_c2_command
```

## BloodAlchemy

```
mov esi, ds:SetErrorMode
push SEM_FAILCRITICALERRORS ; uMode
call esi ; SetErrorMode
push SEM_FAILCRITICALERRORS ; uMode
call esi ; SetErrorMode
push SEM_FAILCRITICALERRORS ; uMode
call esi ; SetErrorMode
call aa_check_working_hours
push 328h ; uBytes
push 40h ; '@' ; uFlags
call ds:LocalAlloc
mov esi, eax
test esi, esi
jz short loc_1F2388
call aa_init_module_list
mov [esi+aa_network.field_0], eax
test eax, eax
```

```
call ds:lstrcpyW
lea ecx, [ebp+lpString2]
call aa_free
jmp short loc_1F1EA1
; -----
loc_1F1E83: ; CODE XREF: aa_init_m
push 8
mov edx, offset aBaseapi ; "baseapi"
jmp short loc_1F1E5C
; -----
loc_1F1E8C: ; CODE XREF: aa_init_m
mov eax, [ebp+lpString1]
mov dword ptr [eax], 10h
jmp short loc_1F1EA1
; -----
loc_1F1E97: ; CODE XREF: aa_init_m
mov ds:baseapi_func_table, offset aa_exec
```

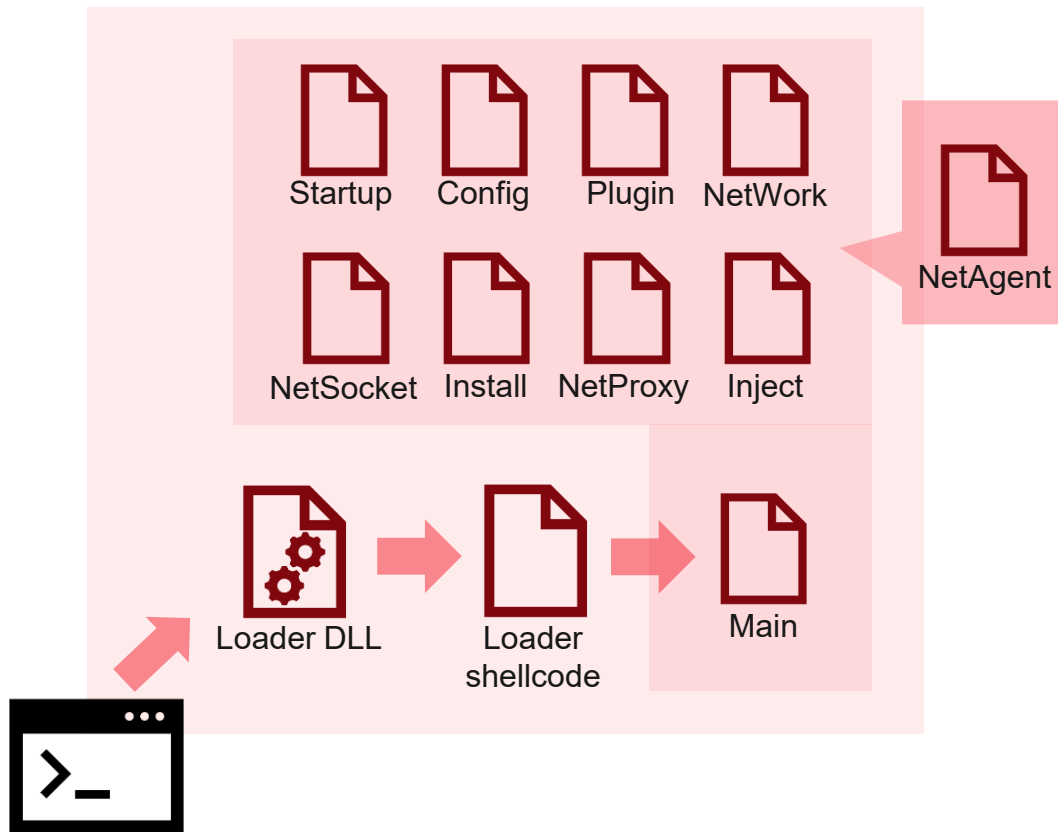
## ShadowPad

```
mov esi, ds:SetErrorMode
push edi
xor ebx, ebx
push SEM_FAILCRITICALERRORS ; uMode
mov [esp+1Ch+var_4], ebx
call esi ; SetErrorMode_0
push SEM_FAILCRITICALERRORS ; uMode
call esi ; SetErrorMode_0
push SEM_FAILCRITICALERRORS ; uMode
call esi ; SetErrorMode_0
mov eax, ds:aa_func_2
movzx esi, ds:word_297042
push SHADOWPAD_MODULE_ONLINE
mov [esp+1Ch+var_C], ebx
mov [esp+1Ch+var_8], ebx
call [eax+aa_func.get_module_data]
push ebx
```

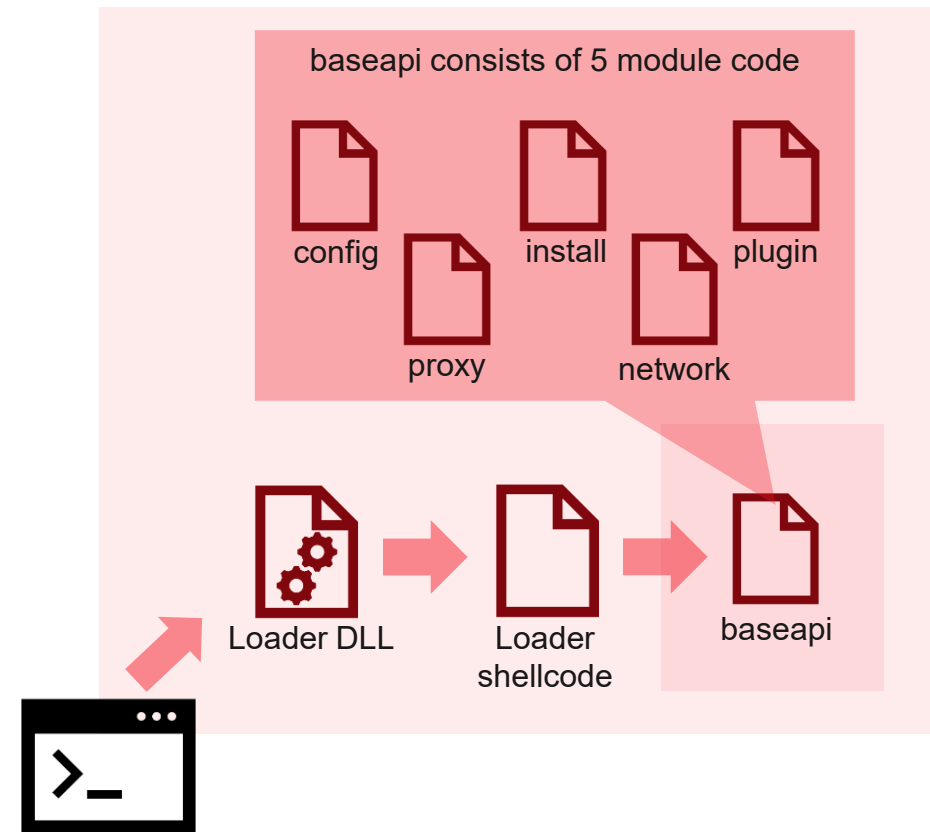
```
loc_2A110E: ; CODE XREF: aa_init_modul
push esi
push offset aConfig ; "Config"
lea eax, [ebp+var_10]
call aa_decode_string_1
push dword ptr [eax+8] ; lpString2
push [ebp+lpString1] ; lpString1
call aa_lstrcpyW_0
lea esi, [ebp+var_10]
call aa_free_2
pop esi
jmp short loc_2A1165
; -----
loc_2A1132: ; CODE XREF: aa_init_modul
mov eax, [ebp+lpString1]
mov dword ptr [eax], 66h
jmp short loc_2A1165
; -----
loc_2A113D: ; CODE XREF: aa_init_modul
mov eax, [ebp+lpString1]
mov ds:aa_func_0, eax
jmp short loc_2A1165
; -----
loc_2A1147: ; CODE XREF: aa_init_modul
mov ds:module_config_func_table.exec_command,
mov ds:module_config_func_table.get_current_co
```

# Multi-Module Payload v.s. Unified Payload

## DeedRAT



## BloodAlchemy



# Different Encoding for Module (Payload and Plugins)

Both can be easily decoded, and might be samples that use another methods

## DeedRAT

```
def decode_payload(ea):
    size = struct.unpack('>L', ida_bytes.get_bytes(ea, 4))[0]
    if size == 0:
        return None

    enc = ida_bytes.get_bytes(ea+4, size)
    key_num = struct.unpack('>L', enc[:4])[0]
    out = b''
    for c in enc:
        key_bytes = struct.pack('<L', key_num)
        k = 0
        for j in key_num:
            tmp = (0x401 * (k + j)) & 0xFFFFFFFF
            k = ((tmp >> 6) ^ tmp) & 0xFFFFFFFF

        key_num ^= (((((k * 9) & 0xFFFFFFFF) ^ (((k * 9) &
0xFFFFFFFF) >> 11) & 0xFFFFFFFF)) * 0x8001) & 0xFFFFFFFF)
        out += (c ^ (key_num & 0xFF)).to_bytes()
    return out
```

## BloodAlchemy

```
import lznt1

def custom_fnv1a_32_2(value):
    values = struct.pack('<H', value)
    hval = 0x811c9dc5
    for c in values:
        hval = ((hval ^ c) * 0x01000193) % 0x100000000
    tmp = (0x2001 * hval) & 0xFFFFFFFF
    tmp = (9 * (tmp ^ tmp >> 7)) & 0xFFFFFFFF
    return (33 * (tmp ^ ((tmp >> 17) & 0xFFFFFFFF))) & 0xFFFFFFFF

def decode_payload(ea, size):
    key = struct.unpack('<H', ida_bytes.get_bytes(ea, 2))[0]
    enc = ida_bytes.get_bytes(ea+2, size-2)
    out = b''
    for c in enc:
        key = (key ^ custom_fnv1a_32_2(key & 0xFFFF)) & 0xFFFFFFFF
        out += (c ^ (key & 0xFF)).to_bytes()
    out = lznt1.decompress(out)
    return out
```

# Different String Encoding

Most of hard-coded strings are encoded

## DeedRAT

```
def ror(c, n):
    return 0xff & ((c >> n) | (c << (8-n)))

def decode_string(enc_addr):
    out = ""
    c = ida_bytes.get_byte(enc_addr)
    for i in range(4096):
        c_1 = ida_bytes.get_byte(enc_addr+i+1)
        out += chr((c ^ c_1) & 0xFF)
        if c == c_1:
            break
        rol3 = rol(c, 3)
        c = (((c * c + rol3 * rol3) & 0xFF) ^
            ror((c * rol3) & 0xFF, 3)) + c) & 0xFF
    return out
```

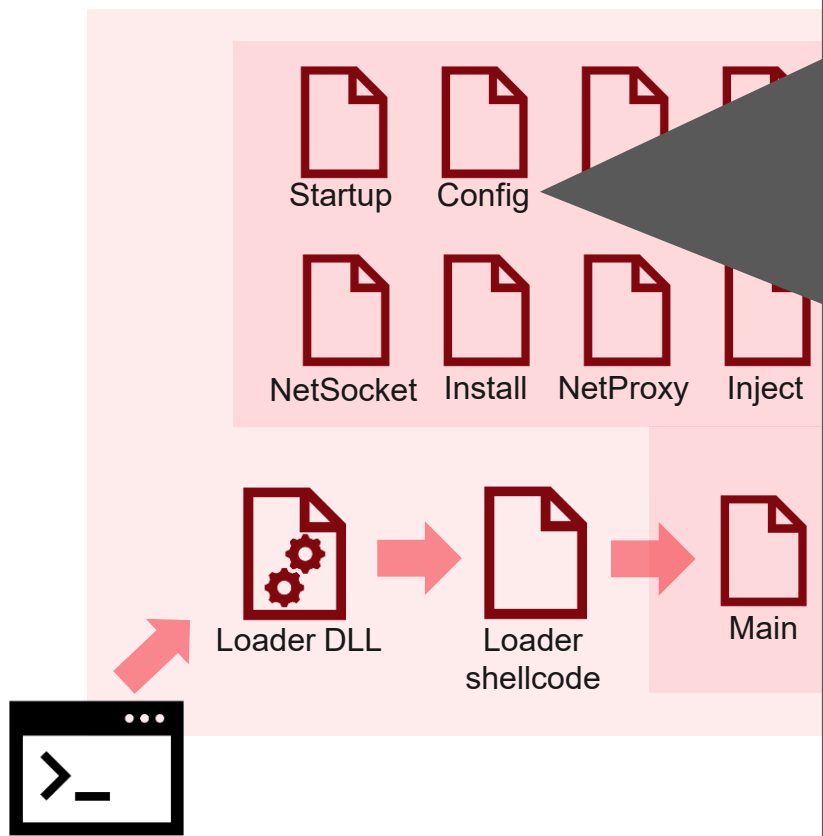
## BloodAlchemy

```
def rol(c, n):
    return 0xff & ((c << n) | (c >> (8-n)))

def decode_string(enc_addr):
    out = ""
    c = ida_bytes.get_byte(enc_addr)
    for i in range(4096):
        c_1 = ida_bytes.get_byte(enc_addr+i+1)
        if c_1 == 0:
            j = 1
            tmp_ea = enc_addr+i+1+j
            while ida_bytes.get_byte(enc_addr+i+1+j) == 0:
                j += 1
            if ida_xref.get_first_dref_to(enc_addr+i+1+j) !=
0xffffffffffffffff or j >= 4:
                break
            elif ida_xref.get_first_dref_to(enc_addr+i+1) !=
0xffffffffffffffff:
                break
            out += chr(c ^ c_1 & 0xFF)
            c = (c + rol(c, i%5+1)) & 0xFF
    return out
```

# DeedRAT Configuration

Unlike BloodAlchemy, it exists within the Config module, not the Loader



Startup Config NetSocket Install NetProxy Inject

Loader DLL Loader shellcode Main

```
193000 enc_config dd 879BBB6Eh
193000
193000
193000
193004 dd 6EBB9871h
193008 db 37h, 1Bh, 8Fh, 1, 0C0h, 0D9h, 82h, 0D9h, 19h, 9, 87h
193013 db 0Ch, 0A8h, 0B4h, 52h, 6Fh, 54h, 60h, 8, 0E1h, 0E4h
19301D db 2Dh, 0CAh, 0E9h, 6, 11h, 0B3h, 72h, 49h, 0E0h, 0A1h
193027 db 0E7h, 0E1h, 0A1h, 0BCh, 0F9h, 0CBh, 0B1h, 56h, 65h
193030 db 42h, 46h, 1, 03h, 8Bh, 0A1h, 72h, 0B4h, 22h, 6Dh, 83h
```

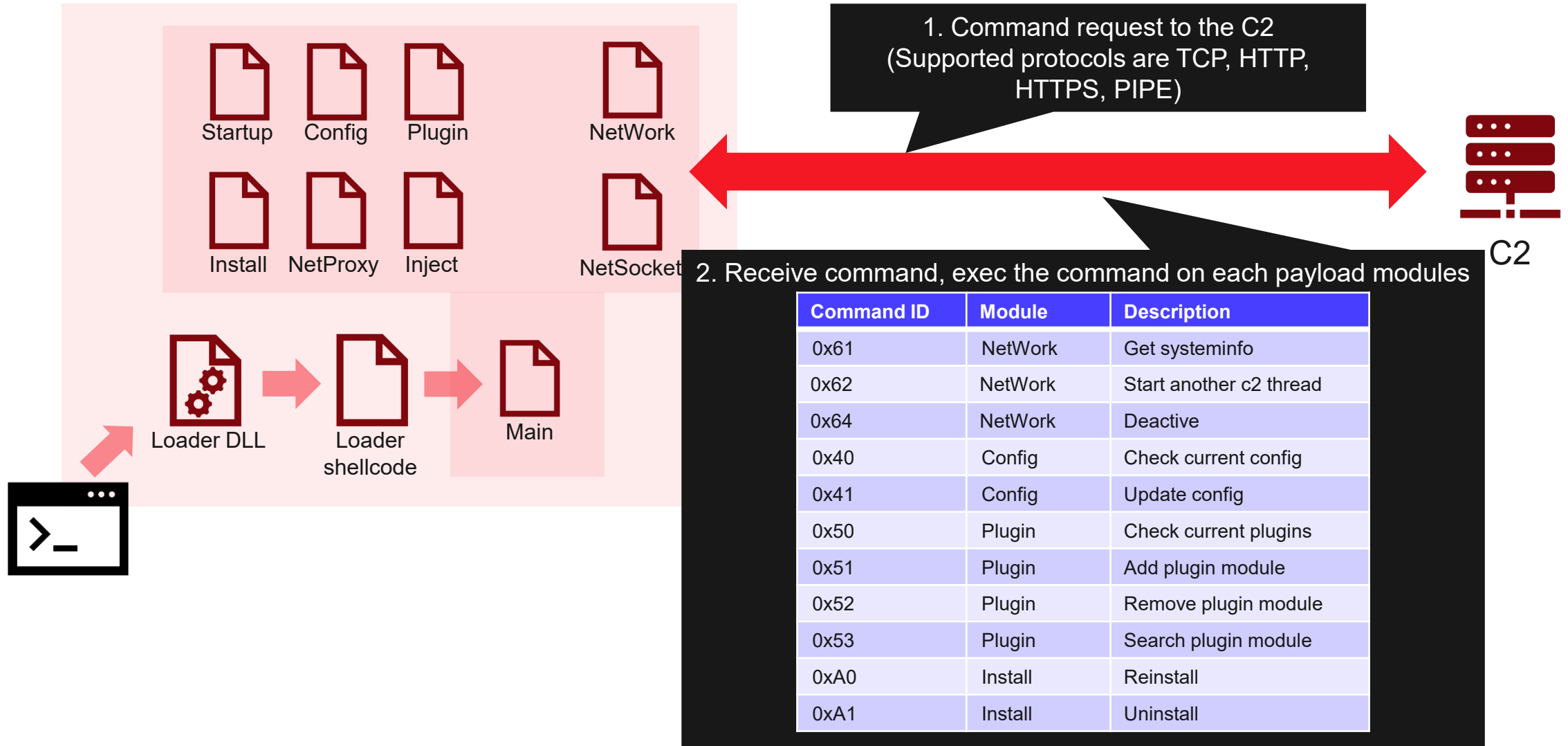
First 8 bytes are xor key (little endian) and xor-encoded size (big endian)

Decode as same as DeedRAT modules + Decode strings

```
dw offset aUplskh3hagroca - offset config_base ; "-UPLskH3HAGroCa3WvTI5I98vfV24Ijpg"
db 1
dw offset aProgramdataCur - offset config_base ; "%ProgramData"
dw offset aDbghelpDll - offset config_base ; "dbghelp.dll"
dw offset aDebugLog - offset config_base ; "debug.log"
dw offset aYanbrowser - offset config_base ; "YanBrowser"
dw offset aYandex - offset config_base ; "YanDex"
dw offset aYandex_0 - offset config_base ; "Yandex"
dw offset aSoftwareMicros_2 - offset config_base ; "SOFTWARE\\Microsoft\\Windows\\CurrentVe"
dw offset aYanbrowser_0 - offset config_base ; "YanBrowser"
db 1
dw offset aWindirSystem32 - offset config_base ; "%windir%\\system32\\WmiPrvSE.exe"
dw offset aWindirSystem32_0 - offset config_base ; "%windir%\\system32\\taskeng.exe"
dw offset aProgramfilesIn - offset config_base ; "%ProgramFiles%\\Internet Explorer\\iexp"
dw offset aWindirSystem32_1 - offset config_base ; "%windir%\\system32\\dwm.exe"
dw offset aAs - offset config_base ; "C:\\Program Files\\Internet Explorer\\iexplore.exe"
db 1
dw offset aTcp19813561974 - offset config_base ; "TCP://198.13.56.197:443"
dw offset aHttps198135619 - offset config_base ; "HTTPS://198.13.56.197:443"
dw offset aHttp1981356197 - offset config_base ; "HTTP://198.13.56.197:443"
```

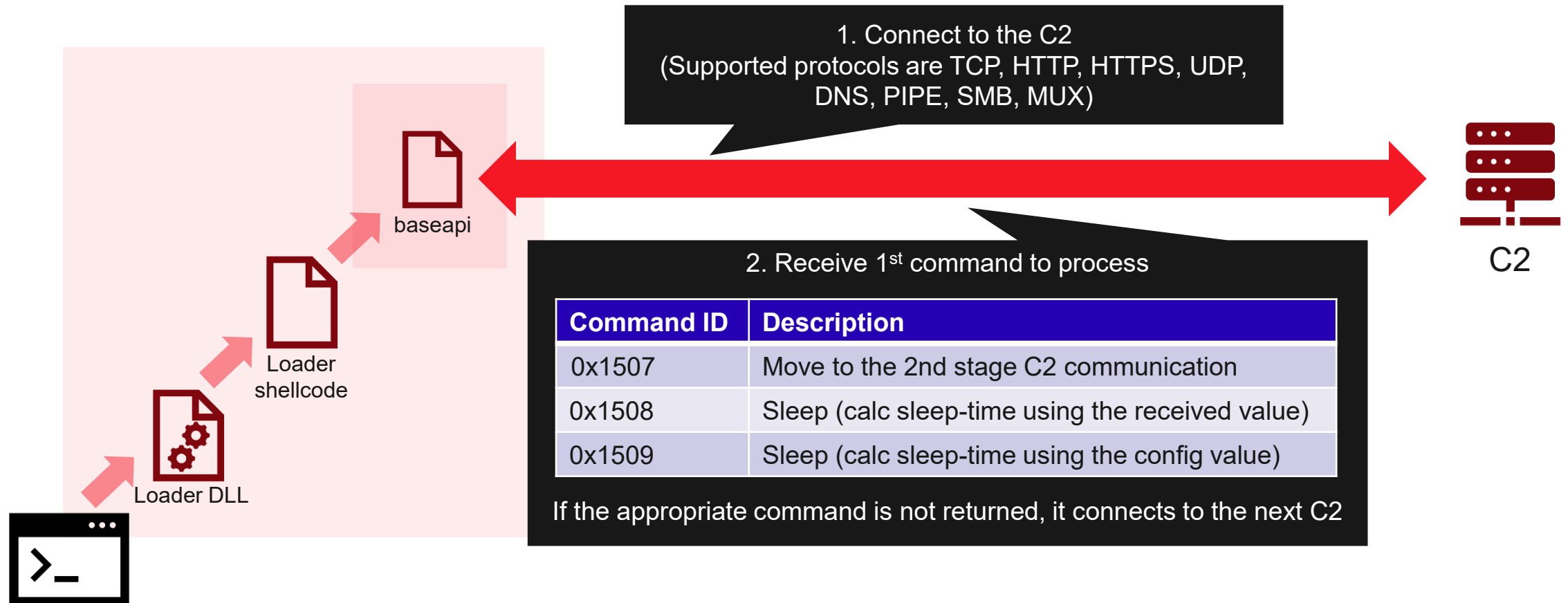
The entries are similar to BloodAlchemy

# DeedRAT Command & Control



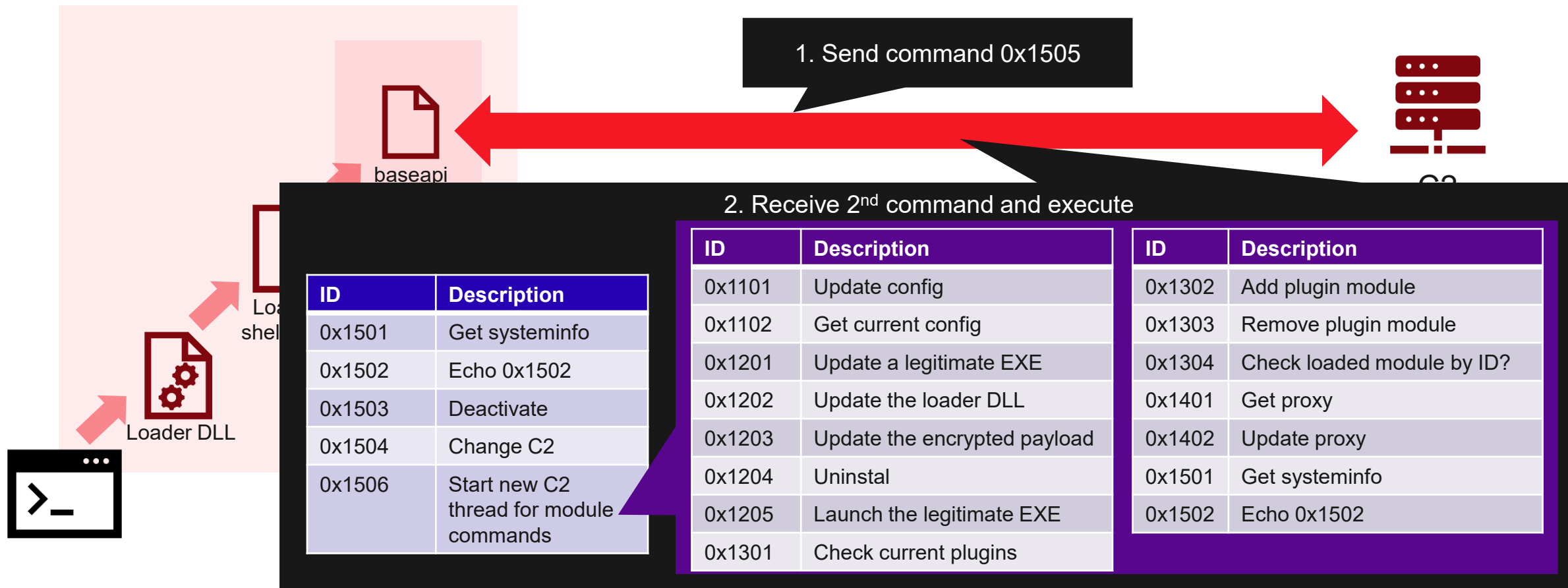
# BloodAlchemy Command & Control

1st stage – preprocessing?



# BloodAlchemy Command & Control

2nd stage – main command and control



# In-depth Comparison Summary

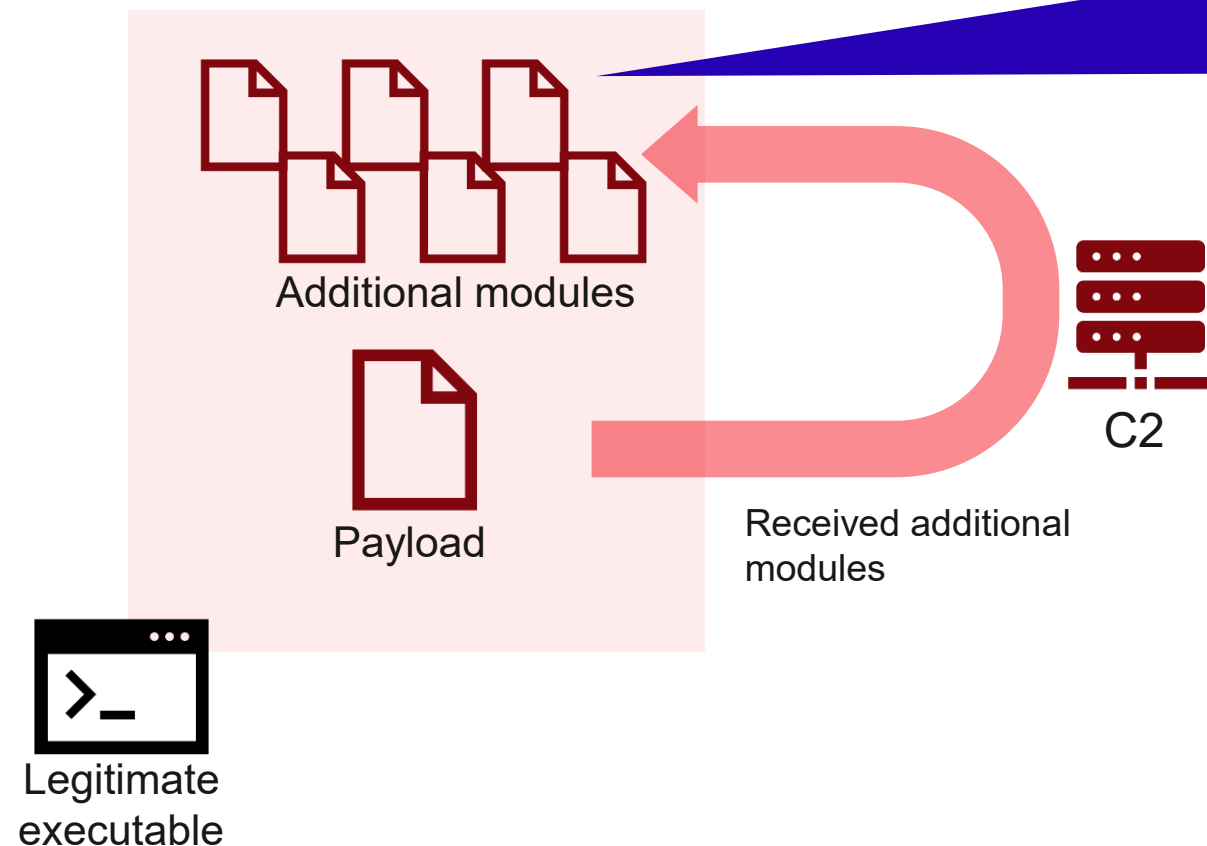
This suggests that there is a relationship between all the shadows

|                              | ShadowPad (Casper sample)                                                                       | DeedRAT                                                                                                                                                                                                                                          | BloodAlchemy                                                                              |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
|------------------------------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|------|--------------|-------------|-----------|------|-------------|--------|---------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|------|--------------|-------------|------------|------|-------------|--------|----------------|----------|
| Payload style                | Multi-module payload                                                                            | Multi-module payload                                                                                                                                                                                                                             | Unified payload                                                                           |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| Payload modules              | Root (0x64), Plugins (0x65), Online (0x68), Config (0x66), Install (0x67), HTTP (0xC9)          | Main (0x20), Startup (0x30), Config (0x40), Install (0xA0), Inject (0xB0), NetWork (0x60), NetSocket (0x70), Plugin (0x50), NetAgent (0x80), NetProxy (0x90)                                                                                     | baseapi(0x10), config (0x11), install (0x12), plugin (0x13), proxy (0x14), network (0x15) |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| Payload/plugin module header | <ul style="list-style-type: none"><li>Original module header</li><li>Also supports PE</li></ul> | <table><tr><th>descriptions</th><th>data</th></tr><tr><td>magic number</td><td>54 45 ED DE</td></tr><tr><td>plugin id</td><td>0x20</td></tr><tr><td>entry point</td><td>0x1740</td></tr><tr><td>original base</td><td>0x400000</td></tr></table> | descriptions                                                                              | data | magic number | 54 45 ED DE | plugin id | 0x20 | entry point | 0x1740 | original base | 0x400000 | <table><tr><th>descriptions</th><th>data</th></tr><tr><td>magic number</td><td>45 AB 45 AB</td></tr><tr><td>plugin id?</td><td>0x10</td></tr><tr><td>entry point</td><td>0x698c</td></tr><tr><td>original base?</td><td>0x400000</td></tr></table> | descriptions | data | magic number | 45 AB 45 AB | plugin id? | 0x10 | entry point | 0x698c | original base? | 0x400000 |
| descriptions                 | data                                                                                            |                                                                                                                                                                                                                                                  |                                                                                           |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| magic number                 | 54 45 ED DE                                                                                     |                                                                                                                                                                                                                                                  |                                                                                           |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| plugin id                    | 0x20                                                                                            |                                                                                                                                                                                                                                                  |                                                                                           |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| entry point                  | 0x1740                                                                                          |                                                                                                                                                                                                                                                  |                                                                                           |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| original base                | 0x400000                                                                                        |                                                                                                                                                                                                                                                  |                                                                                           |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| descriptions                 | data                                                                                            |                                                                                                                                                                                                                                                  |                                                                                           |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| magic number                 | 45 AB 45 AB                                                                                     |                                                                                                                                                                                                                                                  |                                                                                           |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| plugin id?                   | 0x10                                                                                            |                                                                                                                                                                                                                                                  |                                                                                           |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| entry point                  | 0x698c                                                                                          |                                                                                                                                                                                                                                                  |                                                                                           |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| original base?               | 0x400000                                                                                        |                                                                                                                                                                                                                                                  |                                                                                           |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| Anti-analysis                | None                                                                                            | None                                                                                                                                                                                                                                             | Sandbox detection<br>Debug detection                                                      |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| Supported C2 protocol        | TCP, HTTP, UDP, DNS, HTTPS, SSL                                                                 | TCP, HTTP, HTTPS, PIPE                                                                                                                                                                                                                           | TCP, HTTP, HTTPS, UDP, DNS, PIPE, SMB, MUX                                                |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| C2 flow                      | Single stage communication                                                                      | Single stage communication                                                                                                                                                                                                                       | Multi stages communication                                                                |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |
| Known algorithms used        | QuickLZ                                                                                         | RSA, AES, LZNT1, ChaCha20                                                                                                                                                                                                                        | RSA, AES, LZNT1, FNV-1A                                                                   |      |              |             |           |      |             |        |               |          |                                                                                                                                                                                                                                                    |              |      |              |             |            |      |             |        |                |          |

# Unveiling Additional Modules

# Additional Modules of ShadowPad Families

Received additional modules for enhanced



<https://vms.drweb.com/virus/?i=21995049>

The algorithm for loading additional modules is also similar to **BackDoor.ShadowPad.1**; however, there are new modules in this has 16 modules in total. A list of their names with codes and timestamps is provided in the following table:

| Module name                     | Code  | Timestamp           |
|---------------------------------|-------|---------------------|
| Config                          | 0x66  | 2019-05-06 08:33:07 |
| Disk                            | 0x12C | 2019-05-06 08:29:55 |
| ImpUser                         | 0x6A  | 2019-05-06 08:33:18 |
| Install                         | 0x67  | 2019-05-06 08:33:34 |
| KeyLogger                       | 0x132 | 2019-05-06 08:30:26 |
| Online                          | 0x68  | 2019-05-06 08:33:13 |
| PIPE                            | 0xCF  | 2019-05-06 08:29:11 |
| Plugins                         | 0x65  | 2019-05-06 08:33:02 |
| Process                         | 0x12D | 2019-05-06 08:30:00 |
| RecentFiles                     | 0x13D | 2019-05-06 08:31:23 |
| Register                        | 0x12F | 2019-05-06 08:30:10 |
| Screen                          | 0x133 | 2019-05-06 08:30:31 |
| Servcie (the original spelling) | 0x12E | 2019-05-06 08:30:05 |
| Shell                           | 0x130 | 2019-05-06 08:30:15 |
| TCP                             | 0xC8  | 2019-05-06 08:28:45 |
| UDP                             | 0xCA  | 2019-05-06 08:28:56 |

For each loadable module a structure is formed that is added to the list that modules can use to call each other's functions. To w other auxiliary tasks, the `Root` module exports the function table.

Additional modules of Shadowpad have already been reported as above, but additional modules for DeedRAT and BloodAlchemy have not been reported yet

# Storage Location of Additional Modules

Additional modules from C2 were encrypted and stored into the registry

- BloodAlchemy's baseapi command 0x1302 loads an additional module received from the C2
- Encrypts and compresses the data from C2, then stores the encrypted data into **the registry**

```
seg000:026437E4      loc_26437E4:
seg000:026437E4      mov     ecx, edi
seg000:026437E4 8B CF      call    extract_recvdata
seg000:026437E6 E8 C2 FB FF FF  mov     ecx, edi
seg000:026437E8 8B CF      call    cmp_data
seg000:026437ED E8 64 FC FF FF  test    eax, eax
seg000:026437F2 85 C0      jnz     short loc_2643807
seg000:026437F4 75 11

seg000:026437F6 8B 55 F8      mov     edx, [ebp+var_8]
seg000:026437F9 51           push    ecx
seg000:026437FA 8B 4D F4      mov     ecx, [ebp+var_C]
seg000:026437FD E8 3C FE FF FF  call    c_decFNv1_rtldecompressbuffer_check_magicnum_loadPlugins
seg000:02643802 59           pop     ecx
seg000:02643803 8B F0      mov     esi, eax
seg000:02643805 EB 05      jmp     short loc_264380C

seg000:0264380C      loc_264380C:
seg000:0264380C      ; 1
seg000:0264380C 83 3D 60 26 65 02 00  cmp     ds:update_conf_flag?, 0
seg000:02643813 74 20      jz      short loc_2643835

seg000:02643815 6A 10      push    10h
seg000:02643817 8D 45 CC      lea     eax, [ebp+var_34]
seg000:0264381A 50           push    eax
seg000:0264381B 57           push    edi
seg000:0264381C FF 15 DC 1F 65 02  call    ds:p_gen_string_calc_FNV1a_from_MachineGuid ; 0x26402A8
seg000:02643822 FF 75 F8      push    [ebp+var_8]
seg000:02643825 8D 45 CC      lea     eax, [ebp+var_34]
seg000:02643828 FF 75 F4      push    [ebp+var_C]
seg000:0264382B 50           push    eax
seg000:0264382C FF 15 E4 1F 65 02  call    ds:p_c_enc_data_regsetvalue ; 0x26404CE
seg000:02643832 83 C4 18      add     esp, 18h
```

# Hunting Additional Modules of BloodAlchemy

Three encrypted modules were discovered from the registry

| Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Store |                  |            |                                           |
|------------------------------------------------------|------------------|------------|-------------------------------------------|
| Computer                                             | Name             | Type       | Data                                      |
| Computer                                             | (Default)        | REG_SZ     | (value not set)                           |
| HKEY_CLASSES_ROOT                                    | BUJprDaooFNALtLj | REG_BINARY | b0 f4 08 57 8d 5d 04 4f 35 d0 7e 59 5e 96 |
| HKEY_CURRENT_USER                                    | jaYORssmSGDMgVjn | REG_BINARY | e8 1a 1f a7 b5 8b 98 ea 3c e5 e0 91 7c 5c |
| HKEY_LOCAL_MACHINE                                   | oonvCJdkzIEFXmWV | REG_BINARY | 59 3a 8f de c4 56 e2 d8 f8 41 df 8c 50 ed |
| BCD00000000                                          |                  |            |                                           |
| DRIVERS                                              |                  |            |                                           |

Decompress & decrypt

|      |             |    |          |             |             |
|------|-------------|----|----------|-------------|-------------|
| 0000 | 45 AB 45 AB | 40 | 00 00 00 | 2E 17 00 00 | 00 00 40 00 |
| 0010 | 00 00 00 00 | 00 | 70 00 00 | 51 4F 00 00 | 4C 71 00 00 |
| 0020 | 00 00 00 00 | 00 | 00 00 00 | 50 00 00 00 | 95 41 00 00 |
| 0030 | 00 00 00 00 | 00 | 00 00 00 | 84 02 00 00 | 00 60 00 00 |
| 0040 | 00 00 00 00 | 00 | 00 00 00 | 8D 4B 00 00 | 14 04 00 00 |
| 0050 | 55 8B EC 81 | EC | 04 05 00 | 00 53 56 57 | 68 04 01 00 |

Magic number of BloodAlchemy

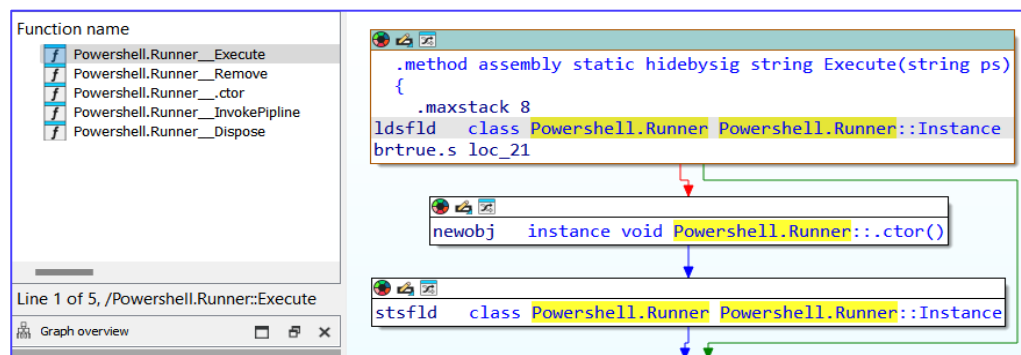
Module ID

| Module ID | Name   |
|-----------|--------|
| 0x20      | stdapi |
| 0x40      | netapi |
| 0x50      | impapi |

# BloodAlchemy's Additonal Module: stdapi (0x20)

stdapi enable the RAT capabilities

- File operations
  - List, move, copy, and execute files/directories
- Shell execution
  - Remote command-line access via anonymous pipes and WMI
- Payload execution
  - Execute received or embedded .NET PEs (e.g., a tiny PowerShell runner)



| Command ID | Description                                                 |
|------------|-------------------------------------------------------------|
| 0x2101     | Send drive information                                      |
| 0x2102     | Send files/directories list                                 |
| 0x2103     | Send recursive file/directory list                          |
| 0x2104     | Move or copy files/directories                              |
| 0x2105     | Execute a file                                              |
| 0x2106     | Read data from specified offset of a file                   |
| 0x2108     | Receive data from C2 and save it as a file                  |
| 0x210A     | Create directories                                          |
| 0x210B     | Resolve environment path                                    |
| 0x210C     | Change file creation time                                   |
| 0x210D     | Change file access time                                     |
| 0x210E     | Change file write time                                      |
| 0x210F     | Send list of network resources (e.g. shared folders)        |
| 0x2110     | Connect to network resource (e.g. shared folders) with auth |
| 0x2201     | Start interactive shell via anonymous pipe                  |
| 0x2301     | Start interactive shell via console (WMI)                   |
| 0x2401     | Execute received .NET PE from C2                            |
| 0x2402     | Execute embedded .NET PE (a tiny Powershell runner)         |

# BloodAlchemy's Additional Module: netapi (0x40)

This module provides network reconnaissance features

- Network scanner
  - Use scanners to map the local network and identify open ports
- Manipulate traffic
  - Act as a bridge/proxy to forward network traffic
- Capture data
  - Sniff network packets and send the captured data to the C2 server

| Command ID | Description                                             |
|------------|---------------------------------------------------------|
| 0x4101     | Start TCP communication to an URL received from C2      |
| 0x4103     | Start UDP bridge                                        |
| 0x4201     | Start TCP communication to IP and port received from C2 |
| 0x4202     | Connect named pipe and communication                    |
| 0x4203     | Start UDP communication to IP and port received from C2 |
| 0x4204     | Start MUX communication to IP and port received from C2 |
| 0x4401     | Send list of adapter ipv4 and netmasks to C2            |
| 0x4402     | Start ARP sweeping                                      |
| 0x4404     | Start TCP port scanner                                  |
| 0x4501     | Get IP address which resolved by localhost              |
| 0x4502     | Start for network capture and save them into a file     |
| 0x4503     | Stop network capture and delete the file                |
| 0x4504     | Send network captured data                              |
| 0x4601     | Send list of port transfer session to C2                |
| 0x4602     | Manage udp/tcp port transfer session                    |
| 0x4603     | Close session                                           |

# BloodAlchemy's Additonal Module: impapi (0x50)

impapi specializes in the impersonation of user session

- Impersonate user sessions
  - Execute with another user's privileges via CreateProcessAsUserW
- Manage sessions
  - Control processes across all user sessions, both active and disconnected
- Establish persistence
  - Ensure the malware runs for all users, regardless of their session state

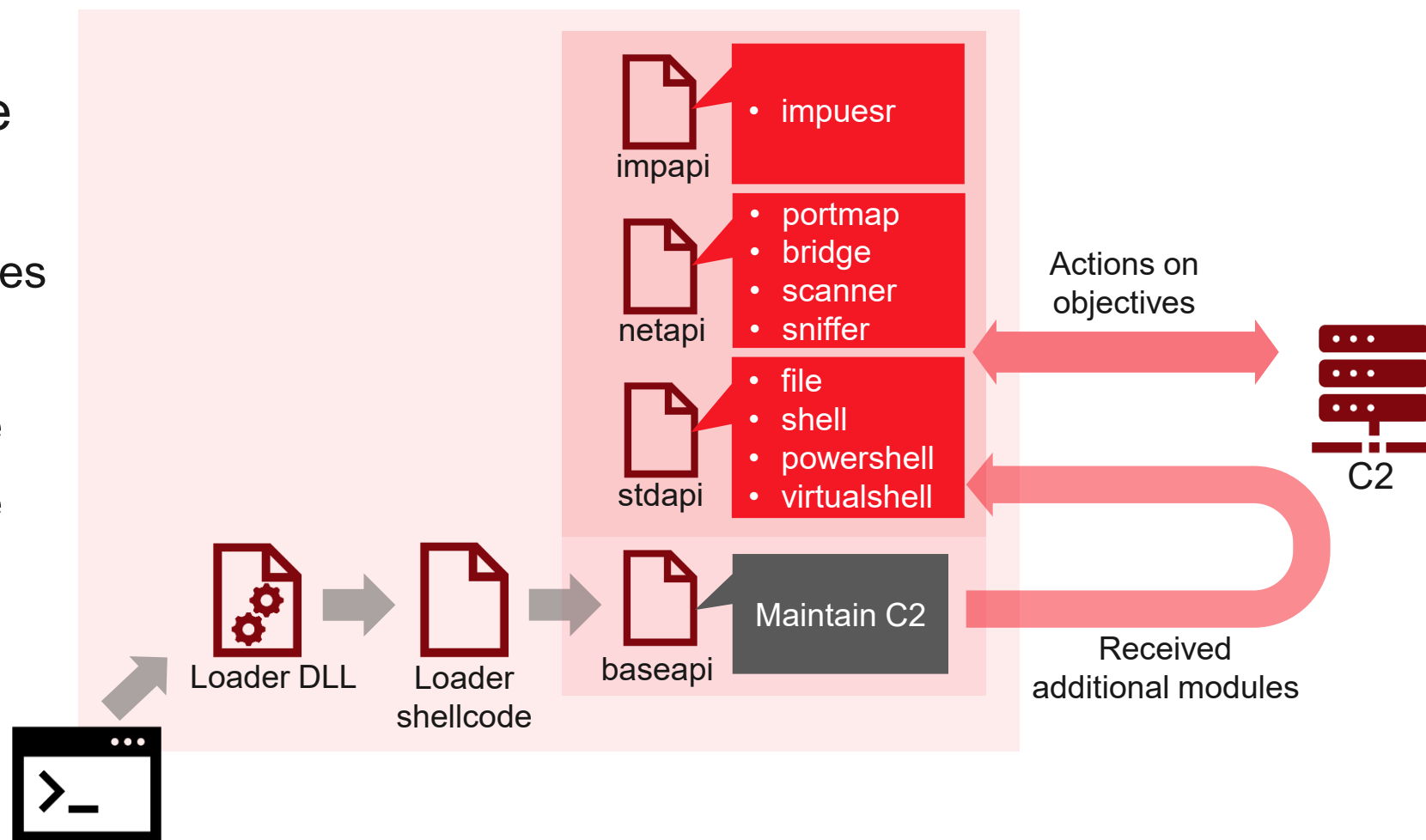
| Command ID | Description                                              |
|------------|----------------------------------------------------------|
| 0x5101     | Send impersonated list of user session information to C2 |

```
13 active = kernel32_WTSGetActiveConsoleSessionId();
14 if ( active != -1 )
15 {
16     if ( hProcess )
17     {
18         if ( active )
19         {
20             kernel32_TerminateProcess(hProcess, 0);
21             kernel32_CloseHandle(hProcess);
22             j_msvcrt_memset(&hProcess, 0, 284);
23             dword_E221A0 = -1;
24         }
25     }
26     if ( !c_CreateProcessAsUserW(v2) )
27         return 0x643;
28     hProcess = v2[0];
29     dword_E221A0 = active;
30     dword_E2219C = v2[2];
31     kernel32_CloseHandle(v2[1]);
```

# BloodAlchemy's Complete Form

C2-delivered modules turn it into a full-featured RAT

- baseapi is root module
  - manage and load for each additional modules
  - Hot-swap additional modules based on the purpose and use case



# Capabilities and Obstacles



## Flexible functionality

Additional modules from C2 enable expanded capabilities



## Analysis difficulty

The complex interdependencies between modules make analysis difficult



## Evasive countermeasures

Since modules are only deployed during the post-exploitation stage, they are hard to acquire, making investigation challenging

# Attack Campaigns Involving DeedRAT/BloodAlchemy

# Developer Speculation

- In 2017, Microsoft complaint alleges that Barium (subgroup of BRONZE ATLAS (APT41)) deployed ShadowPad <sup>\*1</sup>
  - At the time, ShadowPad was used only by Barium
  - They also have special version of ShadowPad
- The DOJ indictments allege that Chengdu 404 (attributed to BRONZE ATLAS) deployed ShadowPad <sup>\*2</sup>
- Tan Dailin (Wicked Rose, member of Barium) and whg (author of PlugX) played a major role in developing important tools leading up to the ShadowPad <sup>\*3</sup>



<https://www.fbi.gov/wanted/cyber/apt-41-group>

Barium or associates may have developed DeedRAT/Blood Alchemy from ShadowPad

2007  
NCPH Remote  
Control Software

2008  
PlugX

2015  
ShadowPad

2019  
DeedRAT

2023  
BloodAlchemy

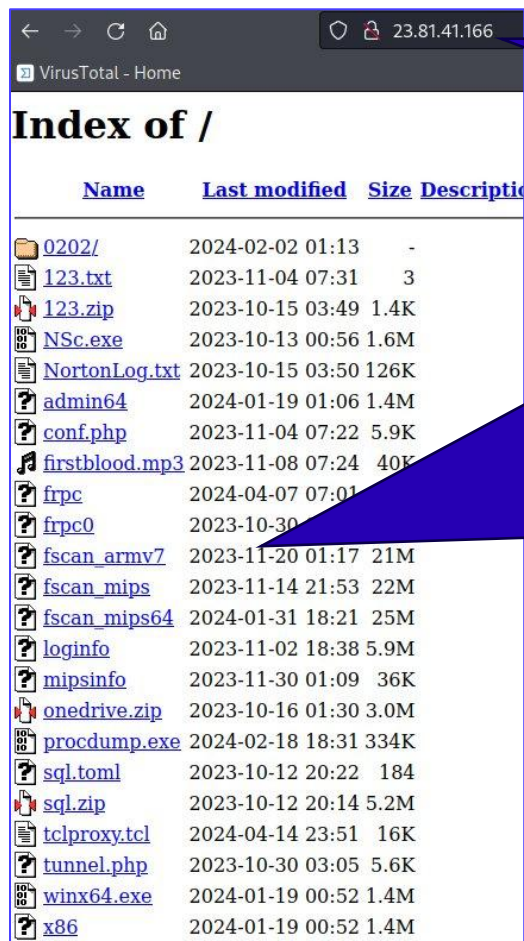
<sup>\*1</sup> [https://www.noticeofpleadings.net/barium/files/COMPLAINT\\_AND\\_SUMMONS/Complaint.pdf](https://www.noticeofpleadings.net/barium/files/COMPLAINT_AND_SUMMONS/Complaint.pdf)

<sup>\*2</sup> <https://www.fbi.gov/wanted/cyber/apt-41-group>

<sup>\*3</sup> <https://assets.sentineline.com/c/Shadowpad?x=P42eqA>

# New DeedRAT Intrusion Set Exposed in Apr 2024

<https://x.com/banthisguy9349/status/1788981985810972904>



| Name           | Last modified    | Size | Description |
|----------------|------------------|------|-------------|
| 0202/          | 2024-02-02 01:13 | -    |             |
| 123.txt        | 2023-11-04 07:31 | 3    |             |
| 123.zip        | 2023-10-15 03:49 | 1.4K |             |
| Nsc.exe        | 2023-10-13 00:56 | 1.6M |             |
| NortonLog.txt  | 2023-10-15 03:50 | 126K |             |
| admin64        | 2024-01-19 01:06 | 1.4M |             |
| conf.php       | 2023-11-04 07:22 | 5.9K |             |
| firstblood.mp3 | 2023-11-08 07:24 | 40K  |             |
| frpc           | 2024-04-07 07:01 |      |             |
| frpc0          | 2023-10-30       |      |             |
| fscan_armv7    | 2023-11-20 01:17 | 21M  |             |
| fscan_mips     | 2023-11-14 21:53 | 22M  |             |
| fscan_mips64   | 2024-01-31 18:21 | 25M  |             |
| loginfo        | 2023-11-02 18:38 | 5.9M |             |
| mipsinfo       | 2023-11-30 01:09 | 36K  |             |
| onedrive.zip   | 2023-10-16 01:30 | 3.0M |             |
| procdump.exe   | 2024-02-18 18:31 | 334K |             |
| sql.toml       | 2023-10-12 20:22 | 184  |             |
| sql.zip        | 2023-10-12 20:14 | 5.2M |             |
| tclproxy.tcl   | 2024-04-14 23:51 | 16K  |             |
| tunnel.php     | 2023-10-30 03:05 | 5.6K |             |
| winx64.exe     | 2024-01-19 00:52 | 1.4M |             |
| x86            | 2024-01-19 00:52 | 1.4M |             |

23.81.41[.]166  
Leaseweb Japan K.K

Hosted China related  
malware/tools:

- 2 DeedRAT sets
- ProxyTool
  - Stowaway
  - FRP
- ScanTool
  - Fscan
- Webshell (HTTP Tunneling)
  - Neo-Regeorg



fscan

English

1. 简介

一款内网

支持主机

息、web

Neo-reGeorg

简体中文 | English

Neo-reGeorg 是一个旨在积极重构 reGeorg 的项目, 目的是:

- 提高可用性, 避免特征检测
- 提高 tunnel 连接安全性
- 提高传输内容保密性

# FRP Server Address Linked to ShadowPad C2

The C2 was attributed to Barium (BRONZE ATLAS, APT41) by 3<sup>rd</sup> party

[https://github.com/stamparm/maltrail/blob/master/trails/static/malware/apt\\_barium.txt](https://github.com/stamparm/maltrail/blob/master/trails/static/malware/apt_barium.txt)

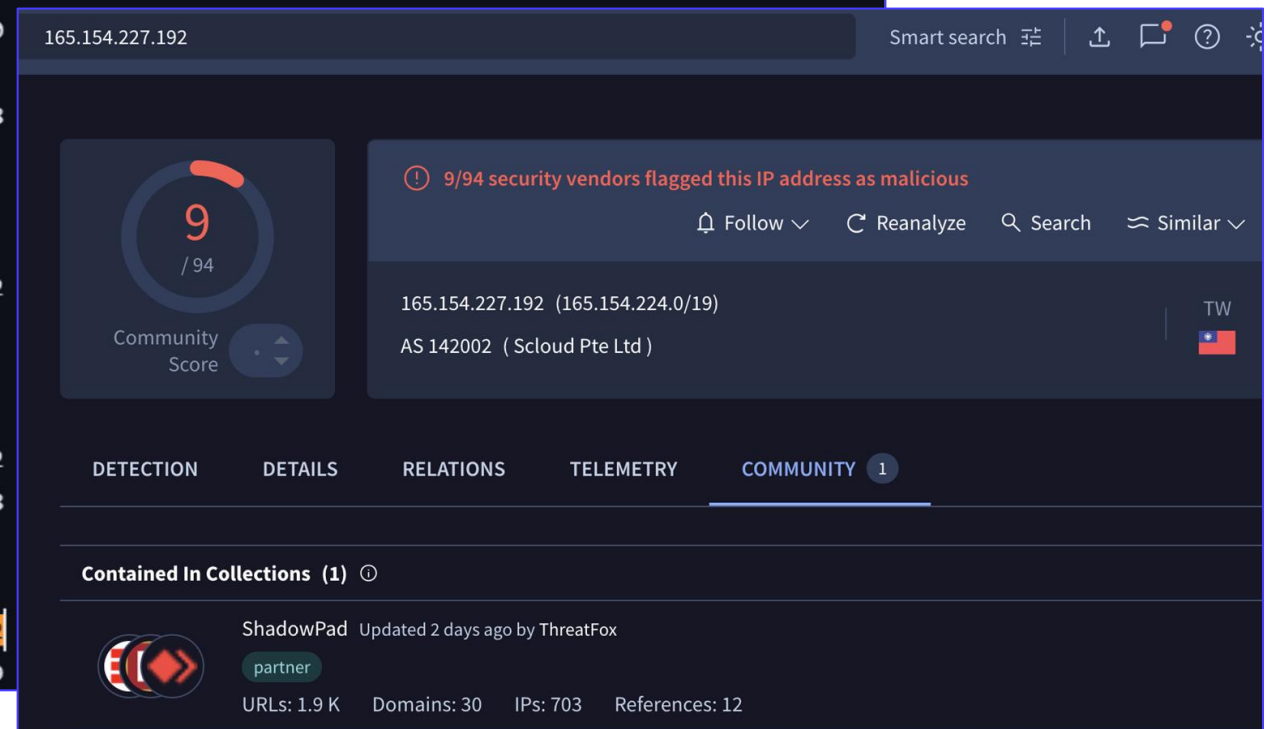
```
serverAddr = "165.154.227.192"
serverPort = 7000

[[proxies]]
name = "plugin_socks5"
type = "tcp"
remotePort = 6005
[proxies.plugin]
type = "socks5"
username = "abc"
password = "abc"
```

FRP configuration file

# Reference: <https://threatfox.abuse.ch/browse/malware/win.shadowpad/> (# 2023-10-26)

http://103.158.190.167  
http://103.255.118.149  
http://103.255.118.150  
http://103.51.110.5  
http://104.194.129.178  
http://104.233.167.99  
http://118.193.56.234  
http://124.126.116.7  
http://139.180.193.182  
http://149.202.45.103  
http://149.28.157.235  
http://149.88.75.49  
http://156.236.114.202  
http://158.247.202.188  
http://158.247.203.58  
http://158.247.213.14  
http://165.154.227.192  
http://167.179.108.149



<https://www.virustotal.com/gui/ip-address/165.154.227.192/community>

# Hostname Listed on The DeedRAT C2 Certificate Linked to BRONZE PRESIDENT (Earth Preta)

**Basic Information**

Routing 103.75.190.0/24 via GIGABIT-MY Gigabit Hosting Sdn Bhd, MY (AS55720)

OS Microsoft Windows

Services (9) 135/DCERPC, 5633/UNKNOWN 49153/DCERPC, 49154/DCERPC

DCERPC 135/TCP

Software

microsoft windows

Details

Could Bind True

Could Query Epm True

UNKNOWN 5633/TCP

Details

TLS

Handshake

Version Selected TLSv1\_2

Cipher Selected TLS\_ECDHE\_RSA\_WITH\_A

Certificate

Fingerprint 2f17b164f498d3325a8

Subject CN=WIN-9JJA076EVSS

Issuer CN=WIN-9JJA076EVSS

| Attribute                                                   | Value               |
|-------------------------------------------------------------|---------------------|
| services.banner                                             |                     |
| services.banner_hashes                                      | sha256:e3b0c44298f  |
| services.discovery_method                                   | PREDICTIVE_METHOD   |
| services.extended_service_name                              | WINRM               |
| services.observed_at                                        | 2024-11-15T14:41:00 |
| services.parsed.winrm.auth_types                            | Negotiate           |
| services.parsed.winrm.ntlm_info.encryption_56bit_supported  | true                |
| services.parsed.winrm.ntlm_info.encryption_128bit_supported | true                |
| services.parsed.winrm.ntlm_info.ntlm1_supported             | true                |
| services.parsed.winrm.ntlm_info.ntlm2_supported             | true                |
| services.parsed.winrm.ntlm_info.always_sign_supported       | true                |
| services.parsed.winrm.ntlm_info.challenge_type              | 3                   |
| services.parsed.winrm.ntlm_info.target_name                 | WIN-9JJA076EVSS     |
| services.parsed.winrm.ntlm_info.netbios_computer_name       | WIN-9JJA076EVSS     |
| services.parsed.winrm.ntlm_info.netbios_domain_name         | WIN-9JJA076EVSS     |
| services.parsed.winrm.ntlm_info.dns_server_name             | WIN-9JJA076EVSS     |
| services.parsed.winrm.ntlm_info.dns_domain_name             | WIN-9JJA076EVSS     |

<https://search.censys.io/hosts/103.75.190.73>

February 1, 2024

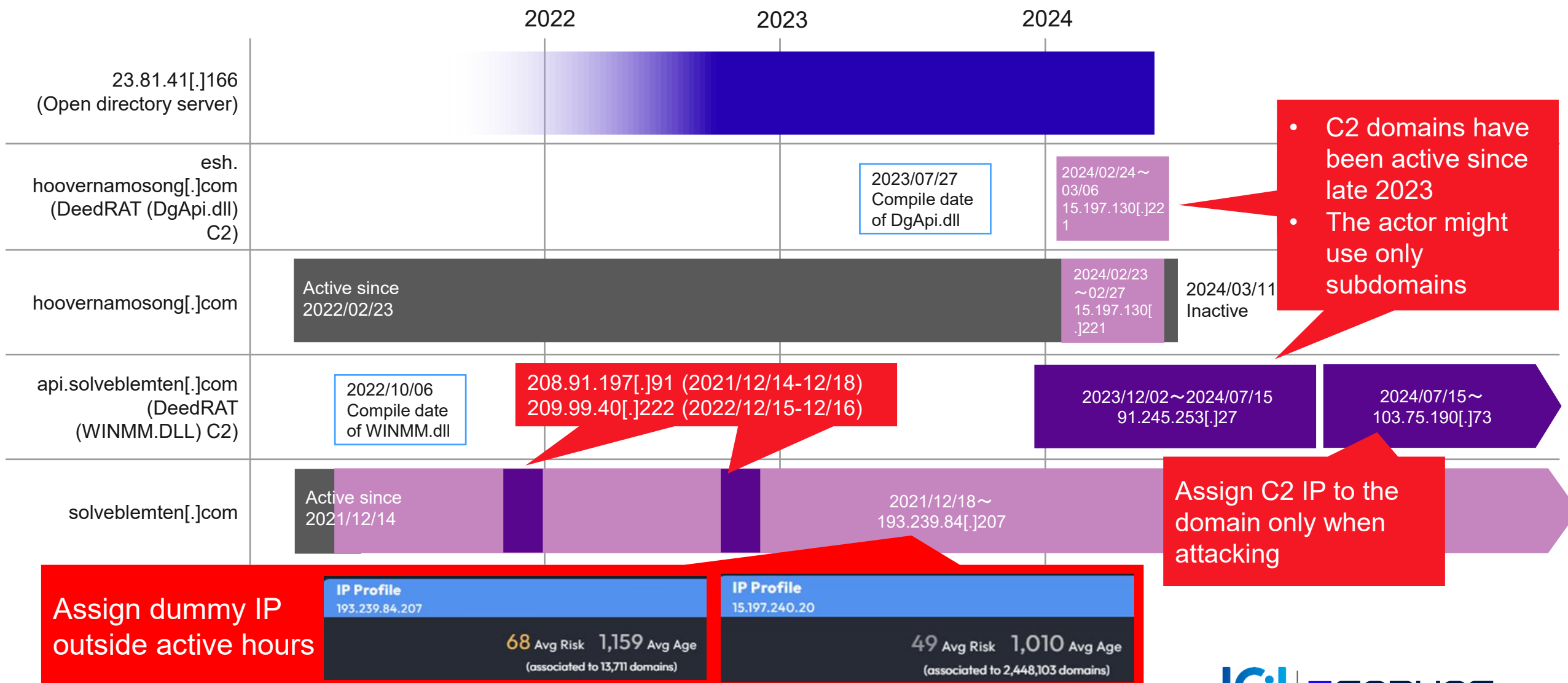
## Stately Taurus Continued – New Information on Cyberespionage Attacks against Myanmar Military Junta

On January 23rd, CSIRT-CTI [published a blogpost](#) describing a pair of campaigns believed to be launched by Stately Taurus (alias Bronze President, Camaro Dragon, Earth Preta, Mustang Panda, Red Delta, TEMP.Hex and Luminous Moth) against the Myanmar military junta. Subsequently, additional observations were made by [Palo Alto Networks's Unit 42](#), suggesting that the ubiquity of the campaigns targeting Myanmar may have been more extensive than originally delineated. In a joint effort with Unit 42, CSIRT-CTI continued its Stately Taurus investigation to uncover and describe five additional campaigns likely to be run against targeted entities in Myanmar.

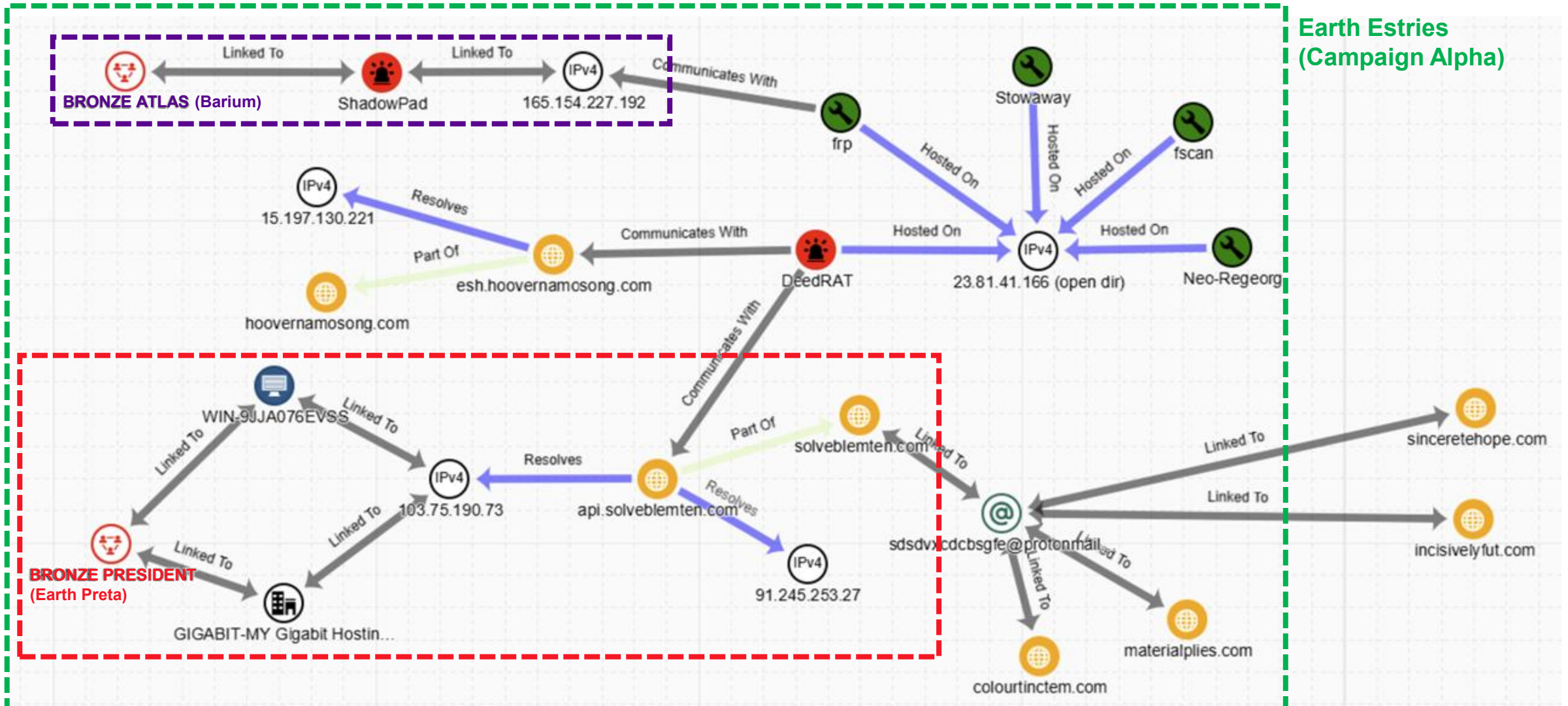
All newly discovered campaigns have taken place in between the originally discussed campaigns on November 9th, 2023 and January 17th, 2024. Employment of previously seen techniques such as DLL Search Order Hijacking and leveraging publicly documented malware such as PUBLOAD show a consistent intrusion set. However, deviations like the use of Cobalt Strike beacons and infostealers showcase variability in modus operandi. Key Indicators of Compromise (IOCs) involve IP addresses, standard magic bytes, autorun keys and created directories, with the certificate Common Name **"WIN-9JJA076EVSS"** consistently associated with C2 servers the malware communicates with. While attribution to Stately Taurus is made with confidence, it is advised to monitor adequately, as the mentioned variability might affect the effectiveness of rule-based detection using the disclosed IOCs.

<https://csirt-cti.net/2024/02/01/stately-taurus-continued-new-information-on-cyberespionage-attacks-against-myanmar-military-junta/>

# Timeline Analysis of Network Indicators



# Summary – Linking to 3 Chinese-Speaking Groups



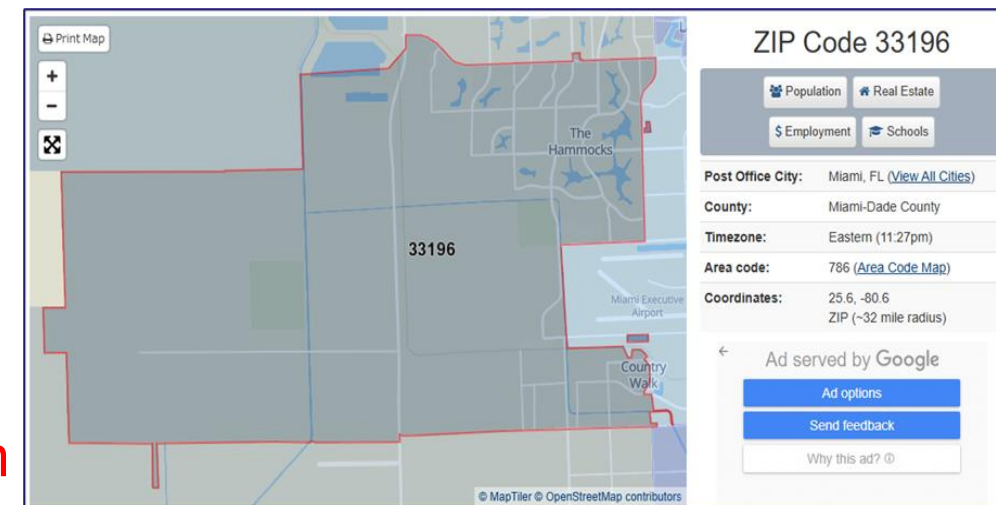
# Whois Info about DeedRAT C2

Non-existent address, with mismatched phone area code

- Registrant Name: Tommie Arnold
- Registrant Organization:
- Registrant Street: 1729 Marigold Lane
- Registrant City: Miami
- Registrant State/Province: FL
- Registrant Postal Code: 33196
- Registrant Country: US
- Registrant Phone: **+1.9852975116**
- Registrant Phone Ext:
- Registrant Fax:
- Registrant Fax Ext:
- Registrant Email: **sdsvxcdcbgfe@protonmail.com**

No presence in Miami

985: Louisiana area code



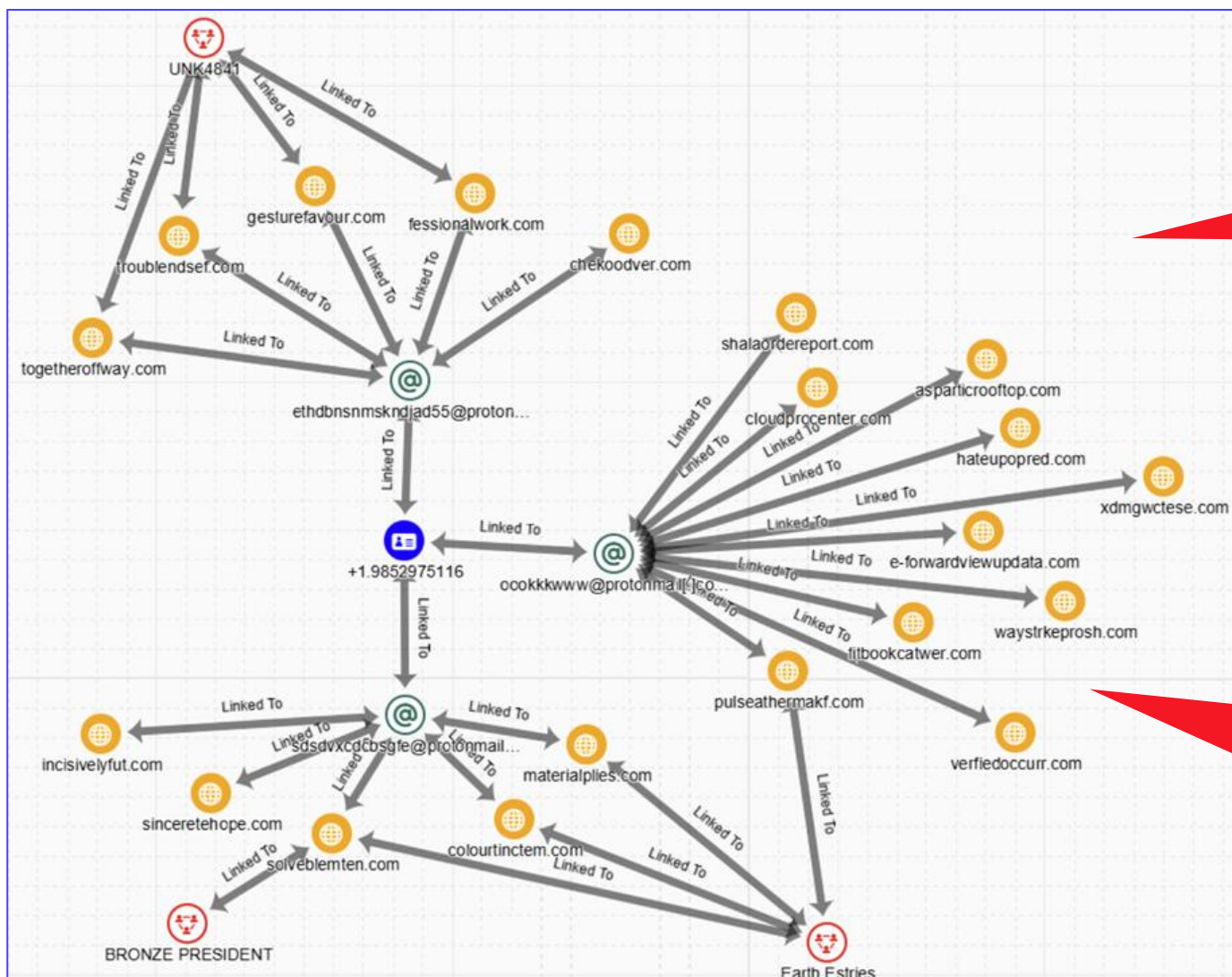
# Suspicious Domains Linked to +1-985-297-5116

Identified a cluster of suspicious domains with similar Whois info

```
Domain Name: PULSEATHERMAKF.COM
Registry Domain ID: 2691698178_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2025-06-06T06:07:38Z
Creation Date: 2022-04-25T05:14:27Z
Registrar Registration Expiration Date: 2025-04-25T05:14:27Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: REDEMPTIONPERIOD https://icann.org/epp#redempt
Registry Registrant ID: Not Available From Registry
Registrant Name: Shawn Francis
Registrant Organization:
Registrant Street: 4858 Agriculture Lane
Registrant City: Miami
Registrant State/Province: FL
Registrant Postal Code: 33141
Registrant Country: US
Registrant Phone: +1.9852975116
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: oookkkwww@protonmail.com
```

```
Domain Name: chekoodver.com
Registry Domain ID: 2979386712_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.discount-domain.com
Registrar URL: http://www.onamae.com
Updated Date: 2025-04-30T18:31:33Z
Creation Date: 2025-04-30T09:31:29Z
Registrar Registration Expiration Date: 2026-04-30T09:31:29Z
Registrar: GMO Internet, Inc.
Registrar IANA ID: 49
Registrar Abuse Contact Email: abuse@gmo.jp
Registrar Abuse Contact Phone: +81.337709199
Domain Status: clientTransferProhibited https://icann.org/epp
Registry Registrant ID: Not Available From Registry
Registrant Name: Geralyn Pickens
Registrant Organization: N A
Registrant Street: 1957 Trails End Road
Registrant City: Miami
Registrant State/Province: FL
Registrant Postal Code: 33131
Registrant Country: US
Registrant Phone: +1.9852975116
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: ethdbnsnmskndjad55@protonmail.com
```

# Linking Known IoCs and Domains



Several domains are linked to total three Chinese-Speaking groups

Other domains:

- May have been used in unconfirmed past attacks
- Will be used in future attacks

# Domains Related sdsdvxcdcbgfe@protonmail.com

| Domain                                                                                                         | Registrar info                                                                                                        | DNS records                                                                                                                                                                                                                           | Known links                                                       |
|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| solveblemten[.]com<br><a href="#">api.solveblemten[.]com</a>                                                   | 2021/12/14 Domain Activated<br>2021/12/14 GMO INTERNET, INC.<br>2022/12/17 PDR Ltd. d/b/a<br>PublicDomainRegistry.com | 208.91.197.91 (2021/12/14-12/18)<br>209.99.40.222 (2022/12/15-12/16)<br><a href="#">91.245.253.27 (2023/12/2-2024/6/29)</a><br><a href="#">103.75.190.73 (2024/7/20-11/27)</a><br>193.239.84.207 and 15.197.240.20 and 35.186.223.180 | <a href="#">BRONZE PRESIDENT</a><br><a href="#">Earth Estries</a> |
| materialplies[.]com<br><a href="#">pop3.materialplies[.]com</a>                                                | 2021/12/15 Domain Activated<br>2021/12/15 GMO INTERNET, INC.<br>2022/12/17 PDR Ltd. d/b/a<br>PublicDomainRegistry.com | 209.99.40.222 (2022/12/15-12/16)<br>208.91.112.55 (2023/2/27-2/28)<br><a href="#">103.159.133.251 (2023/9/1- )</a><br>193.239.84.207 and 15.197.240.20                                                                                | <a href="#">Earth Estries</a>                                     |
| colourtinctem[.]com<br><a href="#">news.colourtinctem[.]com</a><br><a href="#">service.colourtinctem[.]com</a> | 2021/12/14 Domain Activated<br>2021/12/14 GMO INTERNET, INC.<br>2022/12/17 PDR Ltd. d/b/a<br>PublicDomainRegistry.com | 208.91.197.91 (2021/12/14-12/18)<br>209.99.40.222 (2022/12/15-12/16)<br><a href="#">103.91.64.214 (2024/8/19-11/28)</a><br><a href="#">123.253.34.49 (2024/3/25-11/25)</a><br>193.239.84.207 and 15.197.240.20                        | <a href="#">Earth Estries</a>                                     |
| sinceretehope[.]com<br><a href="#">api.sinceretehope[.]com</a><br><a href="#">web.sinceretehope[.]com</a>      | 2021/12/14 Domain Activated<br>2021/12/14 GMO INTERNET, INC.<br>2022/12/16 PDR Ltd. d/b/a<br>PublicDomainRegistry.com | 209.99.40.222 (2022/12/15-12/16)<br><a href="#">172.107.240.4 (2024/7/16- )</a><br><a href="#">202.59.10.157 (2025/3/25- )</a><br>193.239.84.207 and 15.197.240.20                                                                    | No                                                                |
| incisivelyfut[.]com<br><a href="#">pop3.incisivelyfut[.]com</a>                                                | 2021/12/14 Domain Activated<br>2021/12/14 GMO INTERNET, INC.<br>2022/12/17 PDR Ltd. d/b/a<br>PublicDomainRegistry.com | 208.91.197.91 (2021/12/14-12/18)<br>209.99.40.222 (2022/12/14-12/15)<br><a href="#">103.75.189.170 (2024/7/6- 2024/7/7)</a><br><a href="#">193.56.255.210 (2025/4/9- )</a><br>193.239.84.207 and 15.197.240.20                        | No                                                                |

- Some domains registered a C2 IP only for a short period
- They also used subdomains

# Infrastructure Overlaps Revealing Attack Links

Attacks using DeedRAT and BloodAlchemy shared the same infra with other attacks

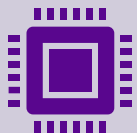
| Date     | Possible Actor                                    | Malware                        | Infrastructures              | Targets                         |
|----------|---------------------------------------------------|--------------------------------|------------------------------|---------------------------------|
| 2022/10~ | UNK4841                                           | CVE-2023-2868                  | +1.9852975116, Miami, FL, US | Around the world                |
| 2023/10  | BRONZE ATLAS                                      | ShadowPad                      | 165.154.227[.]192            | Unknown                         |
| 2023/10~ | BRONZE ATLAS / BRONZE PRESIDENT / Earth Estries ? | DeedRAT                        | 165.154.227[.]192            | Unknown                         |
|          |                                                   |                                | WIN-9JJA076EVSS AS55720      |                                 |
|          |                                                   |                                | +1.9852975116, Miami, FL, US |                                 |
| 2024/01  | BRONZE PRESIDENT / Earth Preta                    | PUBLOAD                        | WIN-9JJA076EVSS AS55720      | South Asia                      |
| 2023/XX  | Earth Estries                                     | Hemigate Zingdoor              | 3280132818 @ qq[.]com        | Asia, South Africa, Germany, US |
| 2023/05  | Earth Estries ?                                   | BloodAlchemy Cobalt Strike     | 3280132818 @ qq[.]com        | Asia                            |
| 2023/XX  | Earth Estries                                     | Zingdoor DeedRAT Cobalt Strike | 38.54.71[.]140               | Asia, South Africa, Germany, US |
| 2024/XX  | Earth Estries                                     | DEMODEX                        | +1.9852975116, Miami, FL, US | Southeast Asia                  |

# Attribution Summary



Multiple Chinese-speaking groups linked to DeedRAT/BloodAlchemy

At least four groups have been identified  
Suggests the existence of organizations like i-Soon that share these malware



Subdomains assigned to C2 IPs only during attacks

To avoid detection and response as much as possible



OPSEC failures observed, with shared infrastructure

Hostnames, email addresses, phone numbers

Highlights the importance of sharing threat intelligence to promote public attribution

# Conclusions

# The Evolving Bloodline

## The APT activities involving DeedRAT or BloodAlchemy

- Targeted regions include Russia and Asia, including Japan
- Detection and intelligence collection are both difficult due to limited reporting and samples

## Unraveling DeedRAT and BloodAlchemy

- Both share many similarities despite differences like encoding methods
  - Likely evolution: ShadowPad → DeedRAT → BloodAlchemy
- BloodAlchemy's additional modules show its full capabilities
  - DeedRAT's additional modules are still missing

## Multiple groups are sharing malware and infrastructure

- Possible entity behind preparing and distributing these resources
- Collaborative intelligence sharing is vital for uncovering these threats

# IOCs – DeedRAT / BloodAlchemy

| Path                    | SHA256                                                           | Description                                                   |
|-------------------------|------------------------------------------------------------------|---------------------------------------------------------------|
| DIFX                    | fe29c70611cdbb86457cf06087f33c1e1ce83c448f4cbbbbe180fd61f8a545d3 | Encrypted BloodAlchemy payload (cdn1ac7bdd3.jptomorrow[.]com) |
| N/A                     | 25268bc07b64d0d1df441eb6f4b40dc44a6af568be0657533088d3bfd2a05455 | BloodAlchemy payload                                          |
| BrLogAPI.dll            | e14ee3e2ce0010110c409f119d56f6151fdca64e20d902412db46406ed89009a | BloodAlchemy loader                                           |
| BrDifxapi.exe           | 1b26db32651074ec40606d94811353b358eec4127efad8a5576e2e19134a0a6d | Legitimate EXE file                                           |
| debug.log               | 67f7faf0161fdac7ebb619a2aa0c73a4a08def05d7752dfdd698d24410d9989e | Encrypted DeedRAT payload (198.13.56[.]197)                   |
| dbghelp.dll             | b6860214fcc1ef17937e82b1333672afa5fcf1c1b394a0c7c0447357477fe7c9 | DeedRAT loader                                                |
| browser_diagnostics.exe | a1885a930589c20aeede98d730222bb0b0b6574234fd2072a7709e4fc90ecbaf | Legitimate EXE file                                           |
| SBAMRES.DLL.CC          | 2d9107edad9f674f6ca1707d56619a355227a661163f18b5794326d4f81a2803 | Encrypted DeedRAT payload (luckybear669.kozow[.]com)          |
| SBAMRES.DLL             | 99a0b424bb3a6bbf60e972fd82c514fd971a948f9cedf3b9dc6b033117ecb106 | DeedRAT loader                                                |
| MicRun.exe              | e356dbd3bd62c19fa3ff8943fc73a4fab01a6446f989318b7da4abf48d565af2 | Legitimate EXE file                                           |

# IOCs – DeedRAT Discovered in Open Directory

| Path              | SHA256                                                           | Description                                              |
|-------------------|------------------------------------------------------------------|----------------------------------------------------------|
| 0202¥dbindex.dat  | 1a38303fb392ccc5a88d236b4f97ed404a89c1617f34b96ed826e7bb7257e296 | Encrypted DeedRAT payload (esh.hoovernamosong[.]com:443) |
| 0202¥DgApi.dll    | b2b617e62353a672626c13cc7ad81b27f23f91282aad7a3a0db471d84852a9ac | DeedRAT loader                                           |
| 0202¥imfsbDll.dll | 05840de7fa648c41c60844c4e5d53dbb3bc2a5250dcb158a95b77bc0f68fa870 | Legitimate DLL file of IObit malware fighter             |
| 0202¥imfsbSvc.exe | 5b88f7d36fe435cd6944bda05f1758f64c7d5136a5f529a58522ac3b0dc9743a | Legitimate EXE file of IObit malware fighter             |
| 123.zip           | b70ebdcfb01e5aa211c504eb15757794cc5bb17d7607512a22672c7782792c45 | Include WINMM.dll                                        |
| NortonLog.txt     | fba149eb5ef063bc6a2b15bd67132ea798919ed36c5acda46ee9b1118b823098 | Encrypted DeedRAT payload (api.solveblemten[.]com:8080)  |
| WINMM.dll         | fc3be6917fd37a083646ed4b97ebd2d45734a1e154e69c9c33ab00b0589a09e5 | DeedRAT loader                                           |
| NSc.exe           | d74dccb0a4856e8059eafe5954f90e2ab48fe2fc5e3f82790c941dc58b8c6252 | Legitimate EXE file of Symantec Norton                   |

# IOCs – Tools Discovered in Open Directory

| Path           | SHA256                                                           | Description                                                                                                                                                                                                                                  |
|----------------|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fscan_armv7    | 9f9675403c2be03232b1c3abe344bf0f4188454955ba89592be52ef77add4a39 | fscan, <a href="https://github.com/shadow1ng/fscan">https://github.com/shadow1ng/fscan</a>                                                                                                                                                   |
| fscan_mips     | aa12c40bc0ef87b1b706f1e9062d72d8c67c3b4b3347741efb38cf71817777d2 | fscan, <a href="https://github.com/shadow1ng/fscan">https://github.com/shadow1ng/fscan</a>                                                                                                                                                   |
| fscan_mips64   | ebaa36db295f1c3a7d59e460ce6813221d0097f3c12ce26e818d4d4ac83c0919 | fscan, <a href="https://github.com/shadow1ng/fscan">https://github.com/shadow1ng/fscan</a>                                                                                                                                                   |
| loginfo        | f34bd1d485de437fe18360d1e850c3fd64415e49d691e610711d8d232071a0b1 | fscan, <a href="https://github.com/shadow1ng/fscan/">https://github.com/shadow1ng/fscan/</a>                                                                                                                                                 |
| mipsinfo.txt   | 34b5a500afd6e3d383375d78643c0d19dfd8a6130ae31e2e1598531784d1fbb3 | Logfile of downloading fscan_mips from the following URL on 2023-11-30 01:09:29<br><a href="https://github.com/shadow1ng/fscan/releases/download/1.8.3/fscan_mips">https://github.com/shadow1ng/fscan/releases/download/1.8.3/fscan_mips</a> |
| frpc           | bbadd7a8d1f24d39f4fcc65b6fd5cbe22904c049ae3a6fee8b510ce6352d59ef | FRP reverse proxy, <a href="https://github.com/fatedier/frp">https://github.com/fatedier/frp</a>                                                                                                                                             |
| frpc0          | 7514ae1ed274d7ea5cd6c3e76f6845f5317dc6f61fc441ac8112c8219ca26132 | FRP reverse proxy, <a href="https://github.com/fatedier/frp">https://github.com/fatedier/frp</a>                                                                                                                                             |
| sql.exe        | 400278da13d6dee4a8d79151e643126bb9cdea61dae0ed8d45bf701db460b489 | FRP reverse proxy, <a href="https://github.com/fatedier/frp">https://github.com/fatedier/frp</a>                                                                                                                                             |
| sql.toml.txt   | ce638cf14d91a3ece6d5c593ecbae0c94f2669d5a8684fa9df0b506cf1bf4019 | FRP configuration file                                                                                                                                                                                                                       |
| x86            | 45d375871a1eb311af5d7b7179ca5cc060bce353292d1912fb766a5025f3d6aa | Stowaway proxy tool, <a href="https://github.com/ph4ntonn/Stowaway/tree/master">https://github.com/ph4ntonn/Stowaway/tree/master</a>                                                                                                         |
| winx64.exe     | a78d737f30e03d166d4e3e3b2dca71d54f1cbf582206dfe16a1e717ce3dc0ef7 | Stowaway proxy tool, <a href="https://github.com/ph4ntonn/Stowaway/tree/master">https://github.com/ph4ntonn/Stowaway/tree/master</a>                                                                                                         |
| admin64        | e4864472f1813776e19fd3468495cfce9745fe9c0270b85c6df4365028ce9fb6 | Stowaway proxy tool, <a href="https://github.com/ph4ntonn/Stowaway/tree/master">https://github.com/ph4ntonn/Stowaway/tree/master</a>                                                                                                         |
| sql.exe        | 400278da13d6dee4a8d79151e643126bb9cdea61dae0ed8d45bf701db460b489 | FRP reverse proxy, <a href="https://github.com/fatedier/frp">https://github.com/fatedier/frp</a>                                                                                                                                             |
| conf.php.txt   | f8db15375c14be16654323b422bafc992a97914740eb64e251c494447f52d075 | Neo-Regeorg, <a href="https://github.com/L-codes/Neo-reGeorg">https://github.com/L-codes/Neo-reGeorg</a>                                                                                                                                     |
| tunnel.php.txt | fc69784283251fe385411a546e9ba3ccdb771b36283ff123ff87856689c2b87c | Neo-Regeorg, <a href="https://github.com/L-codes/Neo-reGeorg">https://github.com/L-codes/Neo-reGeorg</a>                                                                                                                                     |
| onedrived.ps1  | 2fd4a49338d79f4caee4a60024bcd5ecb5008f1d5219263655ef49c54d9acdec | Powershell dropper                                                                                                                                                                                                                           |

# IOCs – IP&Domain, Hostname, Email Address

| IOCs                         | Description                                                                             |
|------------------------------|-----------------------------------------------------------------------------------------|
| 38.54.79[.]177               | VPN connection from TA (BloodAlchemy 2024/05)                                           |
| 107.179.130[.]144            | VPN connection from TA (BloodAlchemy 2024/05)                                           |
| 121.41.35[.]65               | Cobalt Strike C2 (BloodAlchemy 2024/05)                                                 |
| cdn39a700bb.jptomorrow[.]com | Cobalt Strike C2, Linked to Earth Estries's used domain (BloodAlchemy 2024/05)          |
| cdn1ac7bdd3.jptomorrow[.]com | BloodAlchemy C2, Linked to Earth Estries's used domain (BloodAlchemy 2024/05)           |
| cdn-hk-6dc8.bogotatrade[.]co | BloodAlchemy C2 (BloodAlchemy 2024/05)                                                  |
| 198.13.56[.]197              | DeedRAT C2 (debug.log)                                                                  |
| esh.hooveramosong[.]com      | DeedRAT C2 (dbindex.dat)                                                                |
| 15.197.130[.]221             | Associated to esh.hooveramosong[.]com                                                   |
| api.solveblemten[.]com       | DeedRAT C2 (NortonLog.txt)                                                              |
| 91.245.253[.]27              | Associated to api.solveblemten[.]com                                                    |
| 103.75.190[.]73              | Associated to api.solveblemten[.]com                                                    |
| 23.81.41[.]166               | Opendir                                                                                 |
| 165.154.227[.]192            | frp server IP, Linked to Barium's ShadowPad C2                                          |
| WIN-9JJA076EVSS              | TLS certificate CN of 103.75.190[.]73, Linked to BRONZE PRESIDENT's used certificate CN |
| 3280132818@qq[.]com          | Registrar email of jptomorrow[.]com, Linked to Earth Estries's used domain              |

# IOCs – IP&Domain, Hostname, Email Address

| IOCs                      | Description                                                                        |
|---------------------------|------------------------------------------------------------------------------------|
| troublendsef[.]com        | Domain linked to ethdbnsnmskndjad55@protonmail[.]com, +1.9852975116, Miami, FL, US |
| gesturefavour[.]com       |                                                                                    |
| chekoodver[.]com          |                                                                                    |
| fessionalwork[.]com       |                                                                                    |
| togetheroffway[.]com      |                                                                                    |
| pulseathermakf[.]com      | Domain linked to ookkkkwww@protonmail[.]com, +1.9852975116, Miami, FL, US          |
| cloudprocenter[.]com      |                                                                                    |
| fitbookcatwer[.]com       |                                                                                    |
| shalaordereport[.]com     |                                                                                    |
| asparticrooftop[.]com     |                                                                                    |
| e-forwardviewupdata[.]com |                                                                                    |
| waystrikeprosh[.]com      |                                                                                    |
| verfiedoccurr[.]com       |                                                                                    |
| hateupopred[.]com         |                                                                                    |
| xdmgwctese[.]com          |                                                                                    |

# IOCs – IP&Domain, Hostname, Email Address

| IOCs                | Description                                                                   |
|---------------------|-------------------------------------------------------------------------------|
| solveblemten[.]com  | Domain linked to sdsdvxcdcbgfe@protonmail[.]com, +1.9852975116, Miami, FL, US |
| materialplies[.]com |                                                                               |
| colourtinctem[.]com |                                                                               |
| sinceretehope[.]com |                                                                               |
| incisivelyfut[.]com |                                                                               |