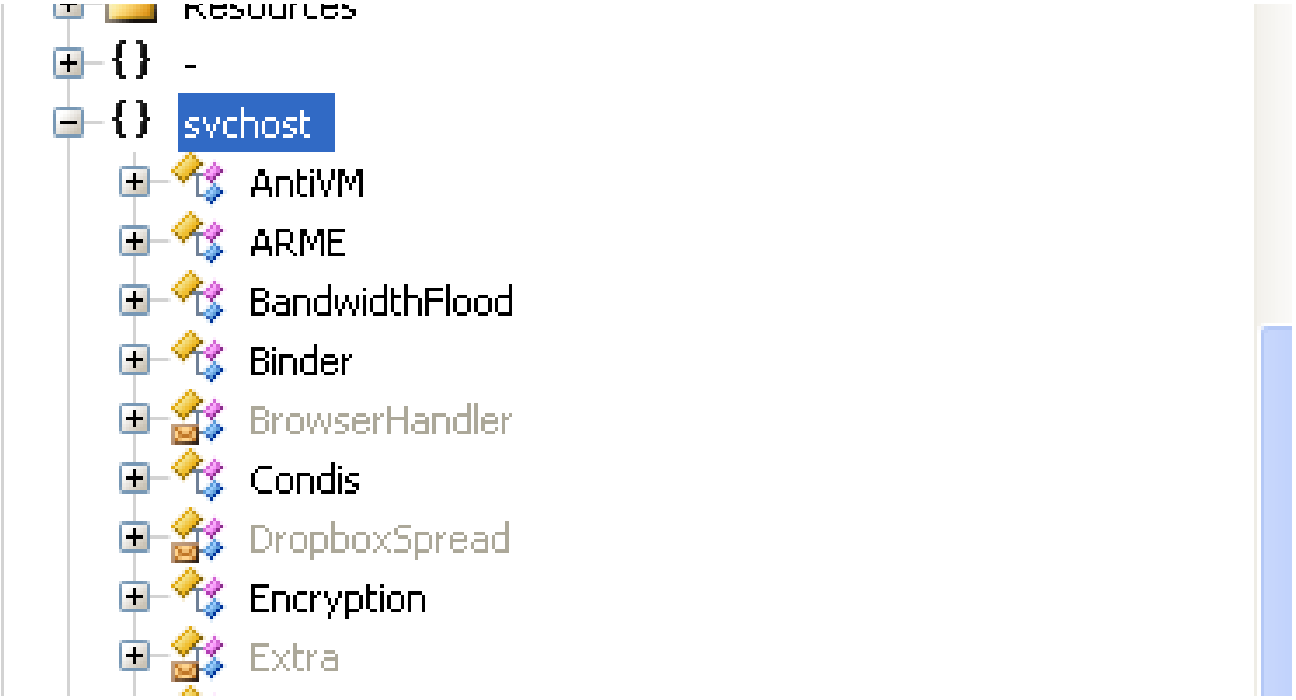
BlackNet RAT - When you leave the Panel unprotected

pwncode.io/2019/12/blacknet-rat-when-you-leave-panel.html



```
Resources
{} -
{} svchost
    AntiVM
    ARME
    BandwidthFlood
    Binder
    BrowserHandler
    Condis
    DropboxSpread
    Encryption
    Extra
```

BlackNET is a PHP based Web Panel which has a builder written in VB.NET. It is being actively used in-the-wild for malicious activities.

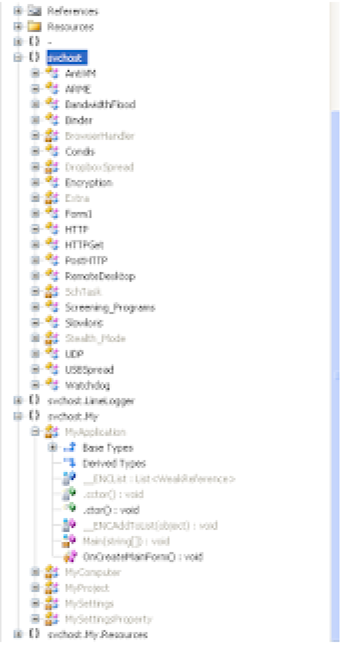
Recently, while analysing a malicious .NET Binary, I came across something interesting which caught my attention. Before I share those details, I will discuss a little bit about the capabilities of the payload, the project itself and then will present the discovery :)

MD5 hash of the sample discussed: 7e88ccc91e0f9a242c4723e43afa93ab

The .NET binaries used in-the-wild which leverage BlackNET panel are not obfuscated. At least the binaries I analysed so far are not protected or obfuscated. This makes the process of analysis straightforward.

How to identify whether this is related to BlackNET?

When you decompile the binary, the list of .NET methods are sufficient to correlate and understand that they have used the BlackNET project. In our case, after decompiling the .NET binary, we can see the list of methods as shown below:



```
References
Resources
{} -
{} svchost
    AntiVM
    ARME
    BandwidthFlood
    Binder
    BrowserHandler
    Conds
    DropboxSpread
    Encryption
    Extra
    Form1
    HTTP
    HTTPGet
    PostHTTP
    RemoteDesktop
    SchTask
    Screening_Programs
    Slowloris
    Stealth_Mode
    UDP
    USBSpread
    Watchdog
{} svchost.LimeLogger
{} svchost.My
    MyApplication
        Base Types
        Derived Types
        __ENCList : List<WeakReference>
        .cctor() : void
        .ctor() : void
        __ENCAddToList(object) : void
        Main(string[]) : void
        OnCreateMainForm() : void
    MyComputer
    MyProject
    MySettings
    MySettingsProperty
{} svchost.My.Resources
```

The names of the methods are self explanatory however for the purpose of brevity, I will mention below some of the capabilities:

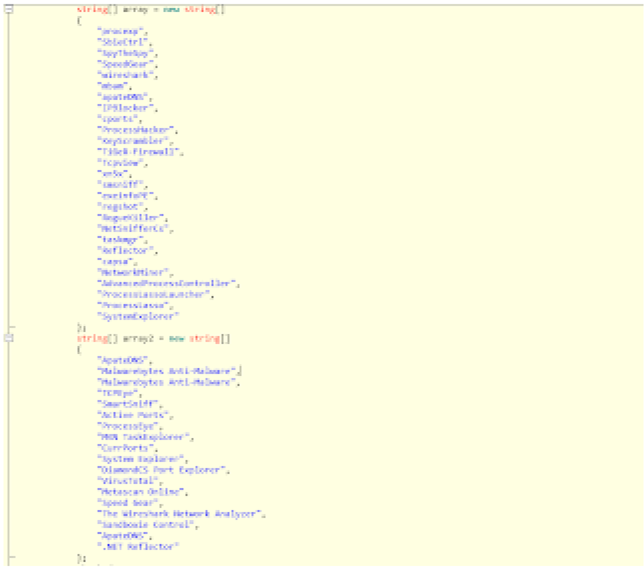
AntiVM: It has the ability to detect a Virtual Machine by checking for the presence of the DLL files, **vmGuestLib.dll** and **vboxmrxnp.dll** on the file system. If it finds these files, then it will delete them.

It also tries to load the DLL, **SbieDll.dll** to check for the presence of Sandboxie (a very common method).

DDoS: Various methods of DDoS are supported by this binary which include: ARME, Slowloris, UDP, TCP, HTTP GET and HTTP POST request based. The attacker can specify the host address they want to perform the DDoS attack against using the BlackNET Panel. They can also select the DDoS method as can be seen here

LimeLogger: This is the key logging module which leverages LowLevelKeyboardProc() function along with SetWindowsHookEx() to do keylogging.

Screening_Programs: This method checks for the presence of analysis tools used by Malware Researchers. It performs checks using both the process names as well as the Window Titles as shown below:



```
string[] array = new string[]
{
    "procexp",
    "SbieCtrl",
    "SpyTheSpy",
    "SpeedGear",
    "wireshark",
    "mbam",
    "apateDNS",
    "IPBlocker",
    "cports",
    "ProcessHacker",
    "KeyScrambler",
    "TiGeR-Firewall",
    "Tcpview",
    "xn5x",
    "smsniff",
    "exeinfoPE",
    "regshot",
    "RogueKiller",
    "NetSnifferCs",
    "taskmgr",
    "Reflector",
    "capsa",
    "NetworkMiner",
    "AdvancedProcessController",
    "ProcessLassoLauncher",
    "ProcessLasso",
    "SystemExplorer"
};
string[] array2 = new string[]
{
    "ApateDNS",
    "Malwarebytes Anti-Malware",
    "Malwarebytes Anti-Malware",
    "TCPEye",
    "SmartSniff",
    "Active Ports",
    "ProcessEye",
    "MKN TaskExplorer",
    "CurrPorts",
    "System Explorer",
    "DiamondCS Port Explorer",
    "VirusTotal",
    "Metascan Online",
    "Speed Gear",
    "The Wireshark Network Analyzer",
    "Sandboxie Control",
    "ApateDNS",
    ".NET Reflector"
};
```

I have included the list in Appendix which can be used as a reference by you to harden your Virtual Machine while analyzing malwares in future.

Unprotected Web Panels

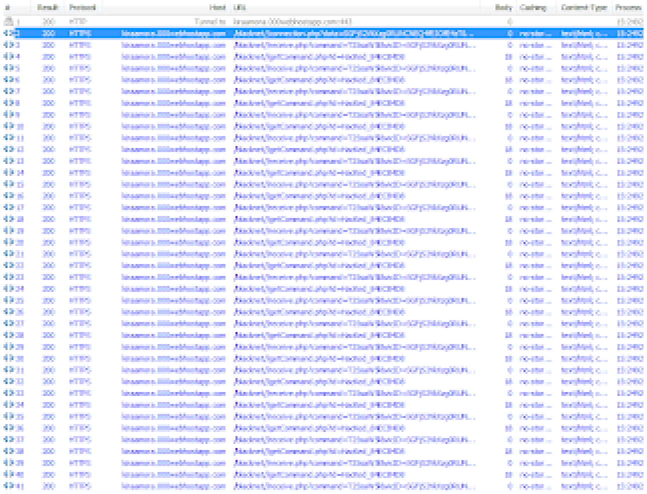
These web panels are easy to deploy. Just get a web hosting, upload the PHP scripts, run the Installation script which sets up the database and the Panel is ready to use.

I noticed that most users of BlackNET Web Panel are leveraging the hosting provided by 000webhostapp.com

One such example is the binary we are discussing in this article.

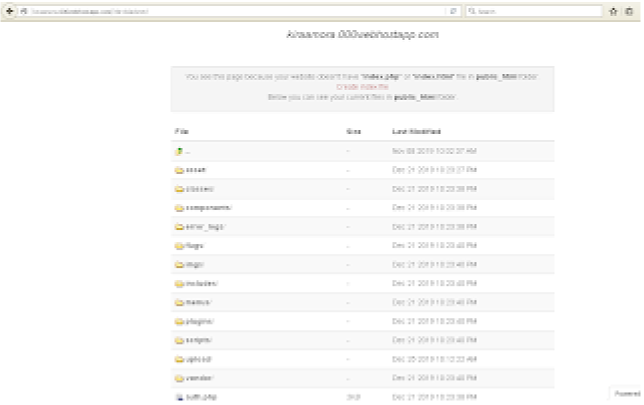
Once the sample is executed on the machine, it will gather basic details from the machine, send them in an HTTP GET request to the BlackNET panel and register the machine. For each victim's machine, an ID is generated in the format: Hacked_<ID>

Below is an example of the HTTP GET requests initiated by the binary:



Web Panel is located at: kiraamora.000webhostapp.com/blacknet

If we visit the hosting, we notice that there is no index.php script present. As a result of it, directory listing is enabled as shown below:



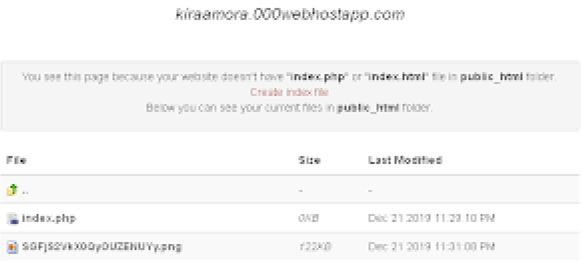
kiraamora.000webhostapp.com

You see this page because your website doesn't have "index.php" or "index.html" file in public_html folder.
Create index file
Below you can see your current files in public_html folder.

File	Size	Last Modified
..	-	Nov 08 2019 10:02:37 AM
assets/	-	Dec 21 2019 10:20:27 PM
classes/	-	Dec 21 2019 10:20:38 PM
components/	-	Dec 21 2019 10:20:38 PM
error_logs/	-	Dec 21 2019 10:20:38 PM
flags/	-	Dec 21 2019 10:20:40 PM
imgs/	-	Dec 21 2019 10:20:40 PM
includes/	-	Dec 21 2019 10:20:40 PM
menus/	-	Dec 21 2019 10:20:40 PM
plugins/	-	Dec 21 2019 10:20:40 PM
scripts/	-	Dec 21 2019 10:20:40 PM
upload/	-	Dec 25 2019 10:12:22 AM
vendor/	-	Dec 21 2019 10:20:40 PM
auth.php	3KB	Dec 21 2019 10:20:38 PM

There is an upload directory in which the information captured from the machines is stored. Inside the upload directory, there is a directory for each victim's machine with the name in the format: Hacked_<ID>

There is one directory of specific interest as shown below:

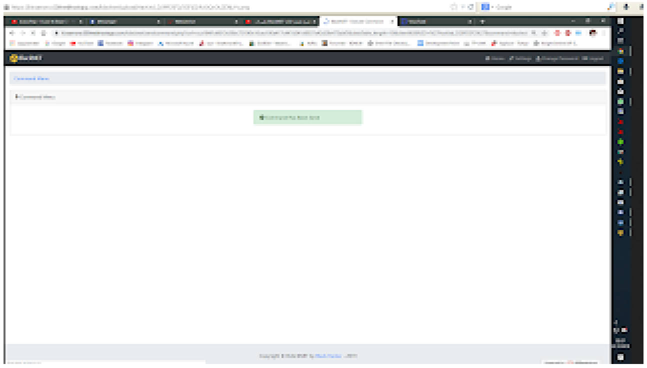


kiraamora.000webhostapp.com

You see this page because your website doesn't have "index.php" or "index.html" file in public_html folder.
Create index file
Below you can see your current files in public_html folder.

File	Size	Last Modified
..	-	-
index.php	0KB	Dec 21 2019 11:28:10 PM
SGFjS2VkX0QyOUZENUYy.png	122KB	Dec 21 2019 11:31:08 PM

The JPG file there is the screenshot taken from the machine. If we check the screenshot, we notice that it is the screenshot taken from the BlackNET panel's admin machine itself as shown below:



If we check the URL in the address bar in screenshot above, we can see that the command:

tkschot was used to capture the screenshot from the machine.

The command itself is defined in the code here

This could be the result of the admin verifying whether the panel is working properly by taking a screenshot of their machine. However, they forgot to delete the screenshot from the panel to clear any traces.

Below are some more MD5 hashes of .NET binaries using the BlackNET Panel:

d25ee82934bec167345502a1e7e3c931
3d28dc46e048daee4974dc5e2fe08bfd
1fd19fcca59ed976ee57640dafba5518
601b4e3b04069beed78e8ce1d2859d4a
c736fcdba9c96eb9b7d8f65e6ab8a4c9
52cd657b18efdbd92f7347d439016c6b
6e36e783324800952f4c0ebea2262fb9
e829cf7a744547e5f1aca6f53061a7b7
2033caac6e8064bd845004d4d628ebe3
8ea79fb698558a8fbed892a8297f3f4b
8d72b32f0d9796443218f1363324f731
281a4bbd61d5e5e310c407b10dafb78c
cd1084d9755db2a38402df2171f25948
83614ce163a71a04fb450f5cd55bfb9f
4a9102b122d9a8dcfe693693f4d91910
8c7e485a40ba5f1881801e56ca298eb0
6fa52977cb3aef5606900cd7a11df4da
6947014e2a2b60445860bfaf5ba35dc6
bdfa464369c660fabff9ec700c49bab9
9b4402ac464744fd4ed118c956752bbc
dc4cf73a81f74f4aa3ec5224ba2cee91
31dc0a5c441b531e029a4158354a1529
6d34058315b46deb297c3d7f712f7451
53c1d9cbf7ca1147880de072d64980dd
d45bac3b009058b11cabc7a9b4048c8d

More Web Panels:

hxxp://davidescu.000webhostapp.com/BlackNET Panel/
hxxps://imdavidfree.000webhostapp.com//BlackNET%20Panel
hxxps://impieselfree.000webhostapp.com/blacknet
hxxp://homedeco.id/
hxxps://davidbotnet.000webhostapp.com/blacknet
hxxp://piratashost.top:82/panel/

Appendix:

List of Process Names Checked:

procexp
SbieCtrl
SpyTheSpy
SpeedGear
wireshark
mbam
apateDNS
IPBlocker
cports
ProcessHacker
KeyScrambler
TiGeR-Firewall
Tcpview
xn5x
smsniff
exeinfoPE
regshot
RogueKiller
NetSnifferCs
taskmgr
Reflector
capsa
NetworkMiner
AdvancedProcessController
ProcessLassoLauncher
ProcessLasso
SystemExplorer

List of Window Titles Checked:

ApateDNS
Malwarebytes Anti-Malware
TCPEye
SmartSniff
Active Ports
ProcessEye
MKN TaskExplorer
CurrPorts
System Explorer
DiamondCS Port Explorer

VirusTotal
Metascan Online
Speed Gear
The Wireshark Network Analyzer
Sandboxie Control
.NET Reflector

c0d3inj3cT