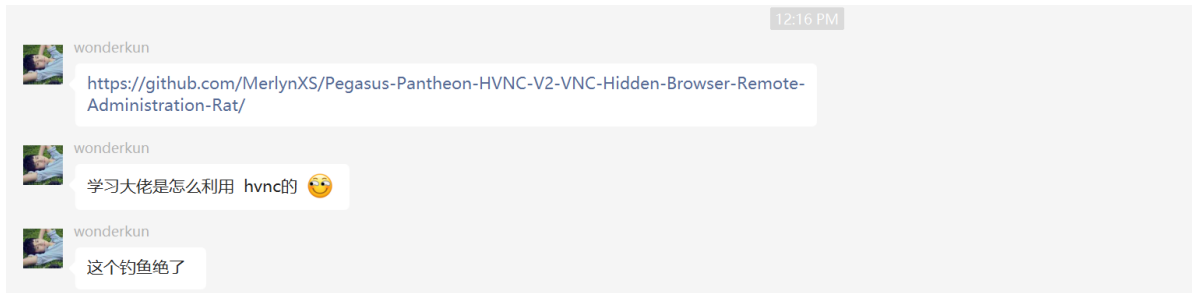
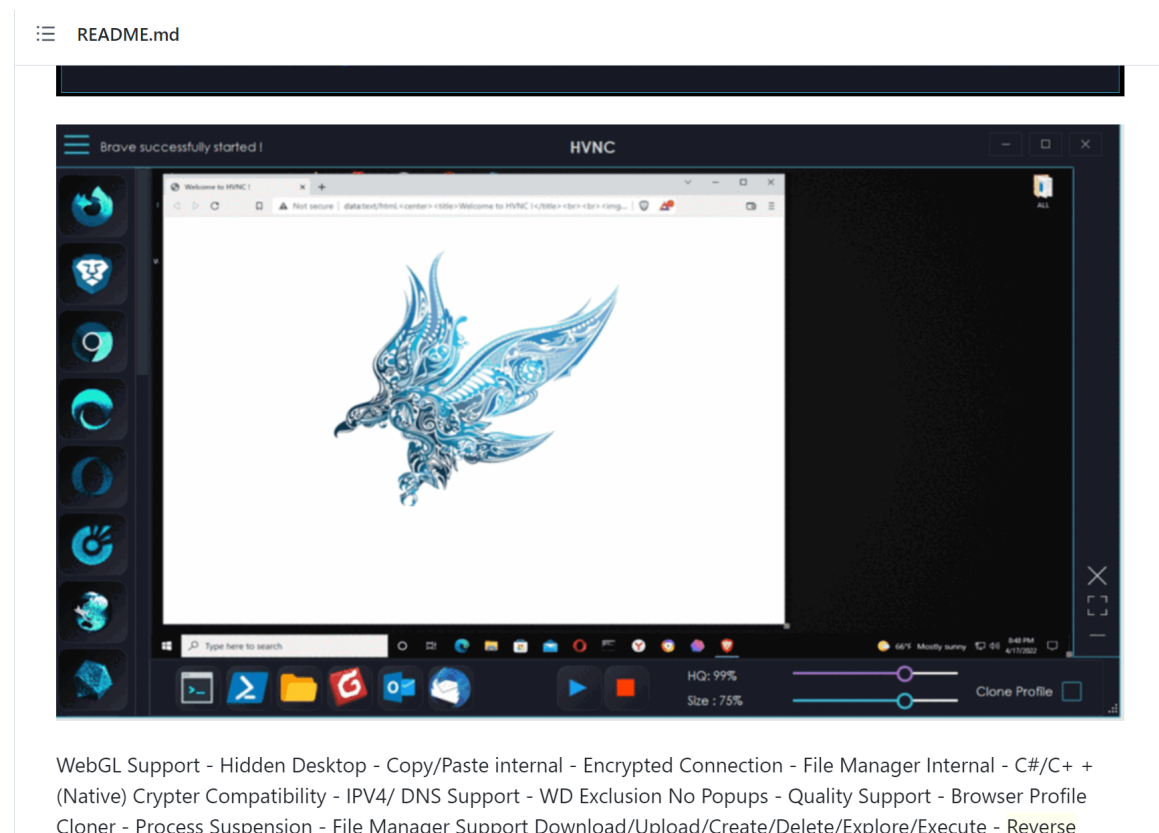


针对开发人员的钓鱼

下午看到 @wonderkun 分享了一个项目：



此时我还没意识到这个项目的问题，在 clone 之后，Readme.md 的介绍是相当的给力，我想看看它是如何实现的。



总之看起来非常强大，有 gif ,还有支持的功能列表，就和所有的开源 RAT 一样。

Name	Date modified	Type	Size
Pantheon V2	6/3/2022 1:16 PM	File folder	
Properties	6/3/2022 1:16 PM	File folder	
Server	6/3/2022 1:16 PM	File folder	
Pantheon V2 HVNCrcs..sln	6/3/2022 1:16 PM	Screen saver	800 KB

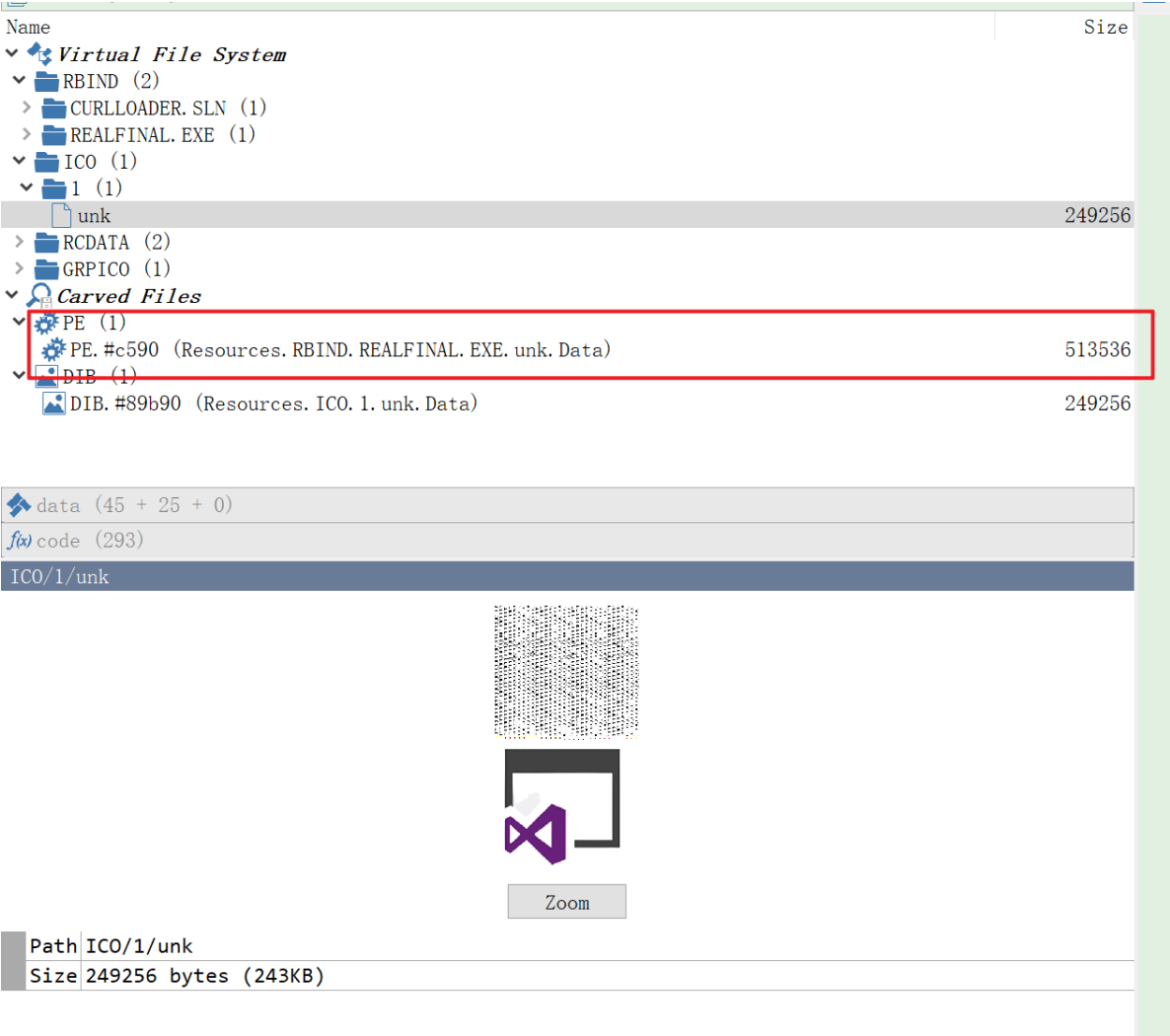
究竟是什么？

图标看过去是正常的，看上去和正常 VS 的项目文件一样。

在经过提醒之后，发现这个 VS 的项目文件有点奇怪，Type 为 `Screen saver`，文件的后缀名为 `..sln`。

Screen saver 为 Windows 屏幕保护程序，在用户不活动时，将会触发 屏幕保护程序。

这个文件实际上就是一个 PE，就是一个可执行文件。



并且伪装了图标。

如何伪装的后缀？

还有一个疑问，它是如何伪装后缀的呢？将文件名复制出来后，完整的文件名是：

```
1 | Pantheon v2 HVNCrcs..sln
```

复制出来的时候发现无法选择到 `rcs..` 的位置，@wonderkun 说明为 ununicode 反转字符。

参考：[不要让“它”迷惑了你的双眼——UNICODE反转字符串](#)

由于插入 Unicode的RLO,导致文本反向排列。

在文本框输入要处理的Unicode或Ascii字符：

Pantheon V2 HVNCrcs.sln

中文汉字转Unicode

Unicode转中文汉字

ASCII转换Unicode

Unicode转换ASCII

中文转换&#XXXX

\u0050\u0061\u006e\u0074\u0068\u0065\u0066\u006e\u0020\u0056\u0032\u0020\u0048\u0056\u004e\u0043\u0020\u006e\u006c\u0073\u002e\u002e\u0073\u0063\u0072

这里的 0x202e 就是 RLO.删除该编码，重新解析：

在文本框输入要处理的Unicode或Ascii字符：

\u0050\u0061\u006e\u0074\u0068\u0065\u0066\u006e\u0020\u0056\u0032\u0020\u0048\u0056\u004e\u0043\u0020\u006e\u006c\u0073\u002e\u002e\u0073\u0063\u0072

中文汉字转Unicode

Unicode转中文汉字

ASCII转换Unicode

Unicode转换ASCII

中文转换&#XXXX

Pantheon V2 HVNCnls.scr

参考：<http://tools.jb51.net/transcoding/chinese2unicode>

真实的的文件名为：

1 | Pantheon V2 HVNCnls..scr

执行效果是啥？

沙箱跑一下，emmm，这个绕过方式有点奇怪，但是有效。




Pantheon V2 HVNCnls.scr

Win7 32 bit Complete

MD5: 98D7999986D63FBD914BDDC3D7B7ECF9

Start: 03.06.2022, 15:29 Total time: 60 s

+ Add tags

Indicators:   

Get sample IOC MalConf ^{new} Restart

Text report Process graph ATT&CK™ matrix Export ▼

CPU RAM

Processes Filter by PID or name ☒ Only important

- 3076 Pantheon V2 HVNCnls.scr.exe PE
 - 389 719 47
 - 3816 REALFINAL.EXE PE
 - 847 223 68
 - 3668 cmd.exe /c timeout /nobreak /t 20
 - 218 17 14
 - 1588 timeout.exe /nobreak /t 20
 - 38 6 16
 - 2056 cmd.exe /c timeout 40
 - 92 16 13
 - 3916 timeout.exe 40
 - 33 6 16

8:29 AM

PCAP Content

扔下 VT :

55 / 69

55 security vendors and 4 sandboxes flagged this file as malicious

144a026bb63a29b36a3437094c4f53cf1cb135edcbe15ab06e35fb8759129bfc
144a026bb63a29b36a3437094c4f53cf1cb135edcbe15ab06e35fb8759129bfc.sample

799.50 KB Size 2022-06-01 17:14:52 UTC 1 day ago

cve-2011-1889 detect-debug-environment direct-cpu-clock-access executes-dropped-file exploit long-sleeps peexe runtime-modules

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

C2AE 9

Network Communication

HTTP Requests

- https://discord.com:443/api/webhooks/930517839058731038/wxqMQna6kAtTNVhmGukOHlrW-WHQkRPOYSzWz2dfuTv9WOf8jk0mo11B08FfEQzBLB
 - HTTP Method POST
 - Response code 204
- https://filebin2.aws.at-sign.cloud:443/93i3on1d3fta8ijh/dc_crypt.exe
 - HTTP Method GET
 - Response code 200

IP Traffic

还是有沙箱检查到了动作：

后续的分析摸了。

好吧，我分析不出来。。。。

小结：

- Unicode 使用 RLO 反转字符串
- 反转的字符串使用 scr，非 exe 降低警觉
 - IDA 直接打开会无法找到文件(也是一个点吧)
- 项目描述的非常真实，包括 gif,图片，
- 修改图标，降低警觉
- 猜测内部的动作
 - 反沙箱，比如使用 cmd 进程来了不断 sleep
 - 反调试。。
 - 使用 discord 和 aws 托管 下一步的 payload （从名字就知道是加密的）
 - 。。。。