

OceanLotus组织的最新下载软件：KerrDown

[1671243993849594](#) / 2019-02-05 09:09:00 / 浏览数 1697 [技术文章](#) [翻译文章](#) [顶\(0\)](#) [踩\(0\)](#)

本文是翻译文章，文章来源：unit42.paloaltonetworks.com

原文地址：<https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/>

译文仅供参考，具体内容表达以及含义原文为准

一、简介

OceanLotus (AKA

APT32)组织来自东南亚，具有极高的攻击能力，在过去的几年里，许多安全研究人员对该组织的活动进行披露。对该组织使用的工具和策略进行了研究和跟踪。该组织主要

该博客主要探讨一款自定义下载的恶意软件，我们命名为“KerrDown”，自2018年初至今，OceanLotus组织一直在使用该软件。我们还展示了如何使用[jaccard-index](#)算法

KerrDown通过以下两种方法进行传播：1.使用带有恶意宏的Microsoft

Office文档。2.包含合法DLL文件的RAR压缩包。该压缩包文件名使用越南语，通过分析，我们认定该活动主要目标为越南。

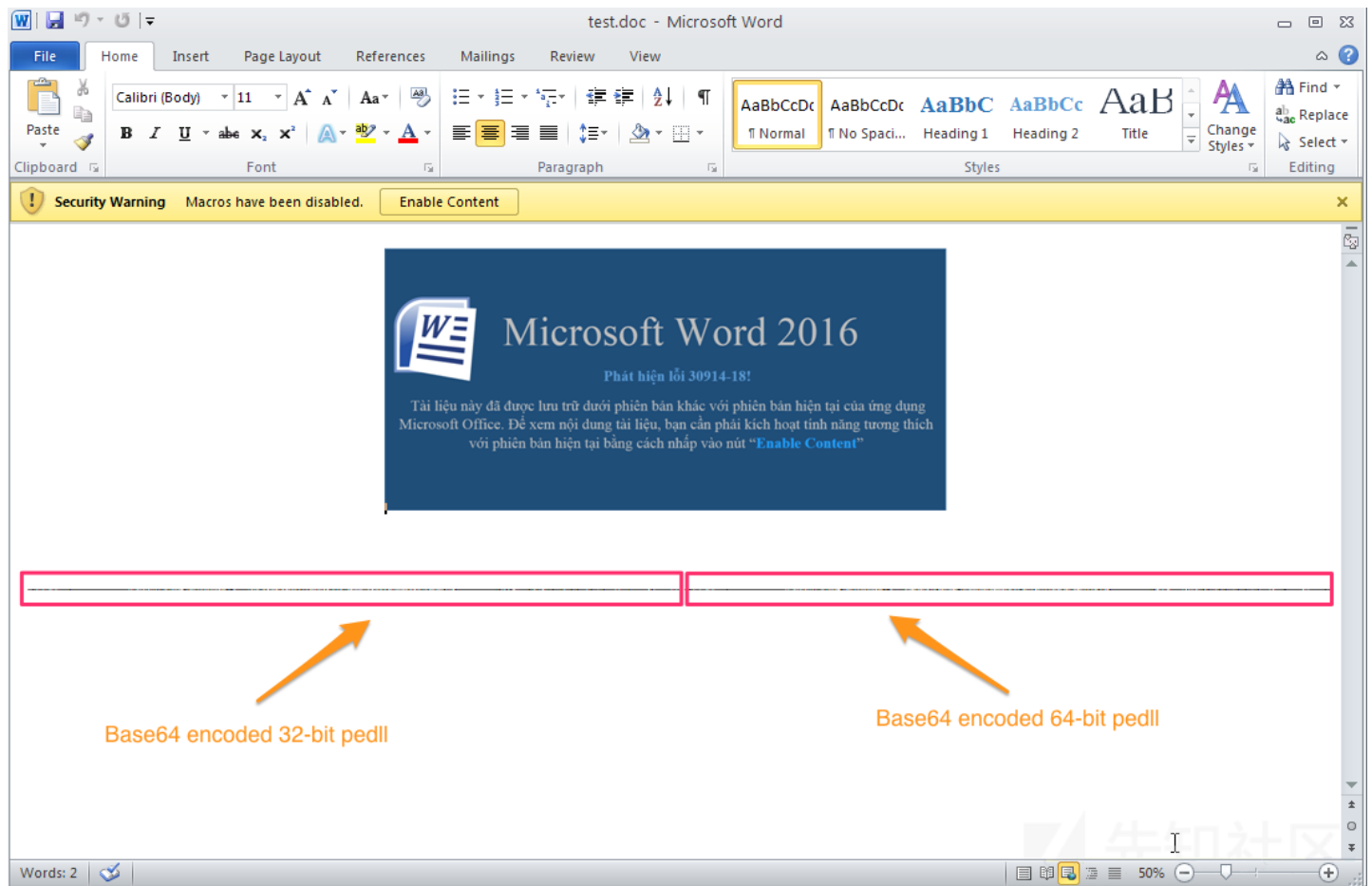
二、细节分析

恶意文档

我们的分析开始于一个邮件，OceanLotus组织曾经用过该传播方式，但该邮件包含了一个新的载荷：KerrDown，其哈希为：

(SHA256:89e19df797481ae2d2c895bcf030fe19e581976d2aef90c89bd6b3408579bfc3)

下图为诱饵文件图片，当受害者打开诱饵文档，文档要求受害者启用宏以查看文件内容。仔细观察，还会发现页面包含两个base64编码的数据。并且字体大小为1。该方法可



对两段数据进行解码，会发现PE文件的MZ头，如下图所示：

<pre> TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAAQAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAEAEAAA4fug4AtAnNlbgBTM0hV GhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4ga W4gRE9TIG1vZGUuDUQ0KJAAAAAAAAAAqpnrWb scUhW7HFIVuxxSF2lvhWfHfIXaW+eFG8cUhdpb 5oV2xxSFVZkXhlfzHFIVVmRGEEdMcUhVWZEIR+x xSFZ7+HhW3HFIVuxxWFNccUhfYzHYRvxxSF/Jnrh W/HFIVux4OFb8cUhfYzFoRvxxSFUmljaG7HFIUA AAAAAAAAAAAAAAABQRRQ AATAEGAENVo1sAAAAAAAAAAOAAiELAQ4AAK IAAADu/ AEAAQA ADgBAA EAAAEAAAAAABAAAAAAAAAAAAAAAAAKQQAQ AoAAAAAMAEAEgCAAAAAAAAAAAAAAAAAAAAA AAAAANAELQNAADACQEAOAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAPgJAQBAAAAAA AAAAAAAAAAwAAAHAEAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAC5ZXh0AAAAC6EAAA AQAAAAogAAAAQAAAAAAAAAAAAAAAAACAA AGAucmRhdGEAAPHWAAAAwAAAAAFgAAACmAA </pre>	<pre> TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAAQAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAEAEAAA4fug4AtAnNlbgBTM0hV GhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4ga W4gRE9TIG1vZGUuDUQ0KJAAAAAAAAAAjFZU3Zxz 7ZGcc+2RnHPtk04AKZGMc+2TTgAhkEhz7ZNOAC WRqHPtkXEL4ZW8c+2RcQv5lftz7ZFxC/2V3HPtk bmRoZGQc+2RnHPpkORz7ZPV8mVmHPtk9UIE ZGYc+2RnHGxkZhz7ZPVC+WmHPtkUmljaGcc+2 QAAAAAAAAAAAAAAABQ RQAAZIYHAEVVo1sAAAAAAAAAAPAAliALag4AAJ CAAQA AAAAAA AAAAQA AAAAAAAAAAQAAAAAAAAAEAAAAAAAAAAAAAA QAAAAAAAAAAAAABoLwEAKAAAAACwBABIAg AAAJAEAKgMAAAAAAAAAAAAAADABAAMBgAA kCEBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAADQIQEAIAAAAAAAAAAAAAAAAALAAAE gCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAudGV4dAAAAPCdAAAEAAAAAJ4AAAAEAAA AAAAAAAAAAAAAAAgAABgLnJkYXRhAAAchwa </pre>
---	--

MZ@ !L!This program cannot be run in DOS mode.

下图为嵌入的宏代码，可以看出，通过iCheck变量检测是哪段数据，如果受害者的操作系统是64位，则iCheck为True，左侧的数据会被解码。32位操作系统则返回False。

```

45 Dim b As String
46 Dim a As String
47 Dim tableNew As Table
48 Set tableNew = ActiveDocument.Tables(1)
49 If (iCheck = True) Then
50     a = tableNew.Cell(1, 1).Range.Text
51     a = Left(a, Len(a) - 2)
52     b = Base64Decode(a)
53 Else
54     a = tableNew.Cell(1, 2).Range.Text
55     a = Left(a, Len(a) - 2)
56     b = Base64Decode(a)
57 End If

```

我们还观察到攻击者使用了Motobit发布的VBS解码功能。下图显示了宏代码中base64函数和Motobit发布的VBS base64解码器之间的比较情况。

```

86 Function Base64Decode(ByVal base64String) As String
87     Const Base64 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
88     Dim dataLength, sOut, groupBegin
89
90     base64String = Replace(base64String, vbCrLf, "")
91     base64String = Replace(base64String, vbTab, "")
92     base64String = Replace(base64String, " ", "")
93
94     dataLength = Len(base64String)
95     If dataLength Mod 4 <> 0 Then
96         Err.Raise 1, "Base64Decode", "Bad Base64 string."
97         Exit Function
98     End If
99
100    For groupBegin = 1 To dataLength Step 4
101        Dim numDataBytes, CharCounter, thisChar, thisData, nGroup, pOut
102        numDataBytes = 3
103        nGroup = 0
104
105        For CharCounter = 0 To 3
106
107            thisChar = Mid(base64String, groupBegin + CharCounter, 1)
108
109            If thisChar = "=" Then
110                numDataBytes = numDataBytes - 1
111                thisData = 0
112            Else
113                thisData = InStr(1, Base64, thisChar, vbBinaryCompare) - 1
114            End If
115            If thisData = -1 Then
116                Err.Raise 2, "Base64Decode", "Bad character In Base64 string."
117                Exit Function
118            End If
119
120            nGroup = 64 * nGroup + thisData
121        Next
122
123        nGroup = Hex(nGroup)
124
125        nGroup = String(6 - Len(nGroup), "0") & nGroup
126
127        pOut = Chr(CByte("&H" & Mid(nGroup, 1, 2))) + _
128                Chr(CByte("&H" & Mid(nGroup, 3, 2))) + _
129                Chr(CByte("&H" & Mid(nGroup, 5, 2)))
130
131        sOut = sOut & Left(pOut, numDataBytes)
132    Next
133
134    Base64Decode = sOut
135 End Function

```

Base64 decoder excerpt from macro

```

Function Base64Decode(ByVal base64String)
'rfc1521
'1999 Antonin Foller, Motobit Software, http://Motobit.cz
Const Base64 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
Dim dataLength, sOut, groupBegin

'remove white spaces, if any
base64String = Replace(base64String, vbCrLf, "")
base64String = Replace(base64String, vbTab, "")
base64String = Replace(base64String, " ", "")

'The source must consists from groups with Len of 4 chars
dataLength = Len(base64String)
If dataLength Mod 4 <> 0 Then
    Err.Raise 1, "Base64Decode", "Bad Base64 string."
    Exit Function
End If

' Now decode each group:
For groupBegin = 1 To dataLength Step 4
    Dim numDataBytes, CharCounter, thisChar, thisData, nGroup, pOut
    ' Each data group encodes up To 3 actual bytes.
    numDataBytes = 3
    nGroup = 0

    For CharCounter = 0 To 3
        ' Convert each character into 6 bits of data, And add it To
        ' an integer For temporary storage. If a character is a '=', there
        ' is one fewer data byte. (There can only be a maximum of 2 '=' In
        ' the whole string.)
        thisChar = Mid(base64String, groupBegin + CharCounter, 1)

        If thisChar = "=" Then
            numDataBytes = numDataBytes - 1
            thisData = 0
        Else
            thisData = InStr(1, Base64, thisChar, vbBinaryCompare) - 1
        End If
        If thisData = -1 Then
            Err.Raise 2, "Base64Decode", "Bad character In Base64 string."
            Exit Function
        End If

        nGroup = 64 * nGroup + thisData
    Next

    'Hex splits the long To 6 groups with 4 bits
    nGroup = Hex(nGroup)

    'Add leading zeros
    nGroup = String(6 - Len(nGroup), "0") & nGroup

    'Convert the 3 byte hex integer (6 chars) To 3 characters
    pOut = Chr(CByte("&H" & Mid(nGroup, 1, 2))) + _
            Chr(CByte("&H" & Mid(nGroup, 3, 2))) + _
            Chr(CByte("&H" & Mid(nGroup, 5, 2)))

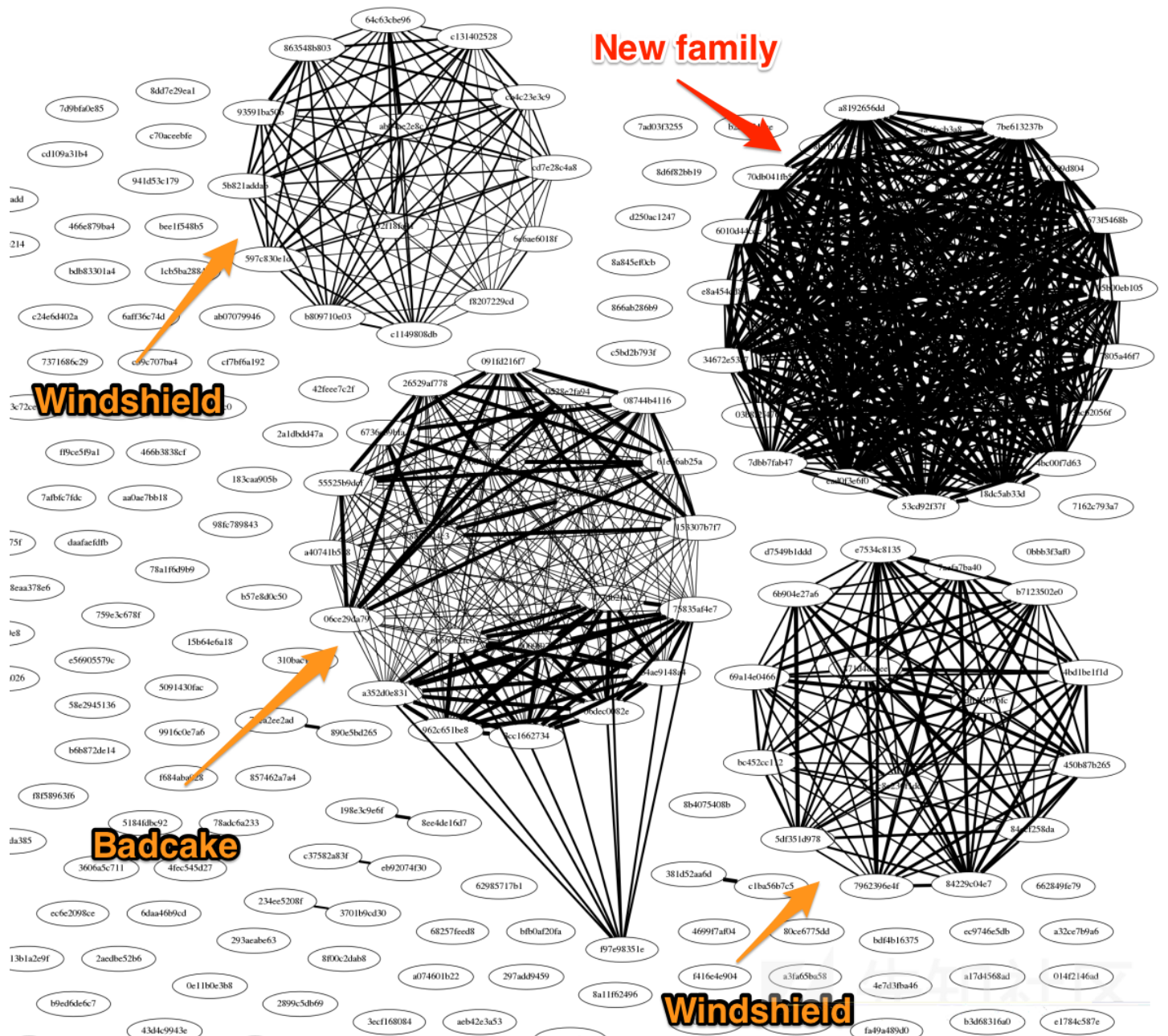
    'add numDataBytes characters To out string
    sOut = sOut & Left(pOut, numDataBytes)
Next

Base64Decode = sOut
End Function

```

Base64 decoder from Motobit

我们用[jaccard-index](#)来分析KerrDown样本的相似性，我们通过Jaccard索引来检测OceanLotus组织曾经使用过的恶意文件，我们没有发现任何匹配。我们使用KerrDown和



如上文所说，该恶意软件会根据不同的操作系统解码对应的dll文件，并将该文件命名为“main_background.png”。存放在“User\Administrator\AppData\Roaming”目录下。DLL文件被保存在系统中。下图显示了下载程序连接的URL。

OS Architecture	URL	User Agent
32 bit	https://syn.servebbs[.]com/kuss32.gif	Mozilla/5.0 (Windows NT 10.0; Win32; x32; rv:60.0)
64 bit	https://syn.servebbs[.]com/kuss64.gif	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0)

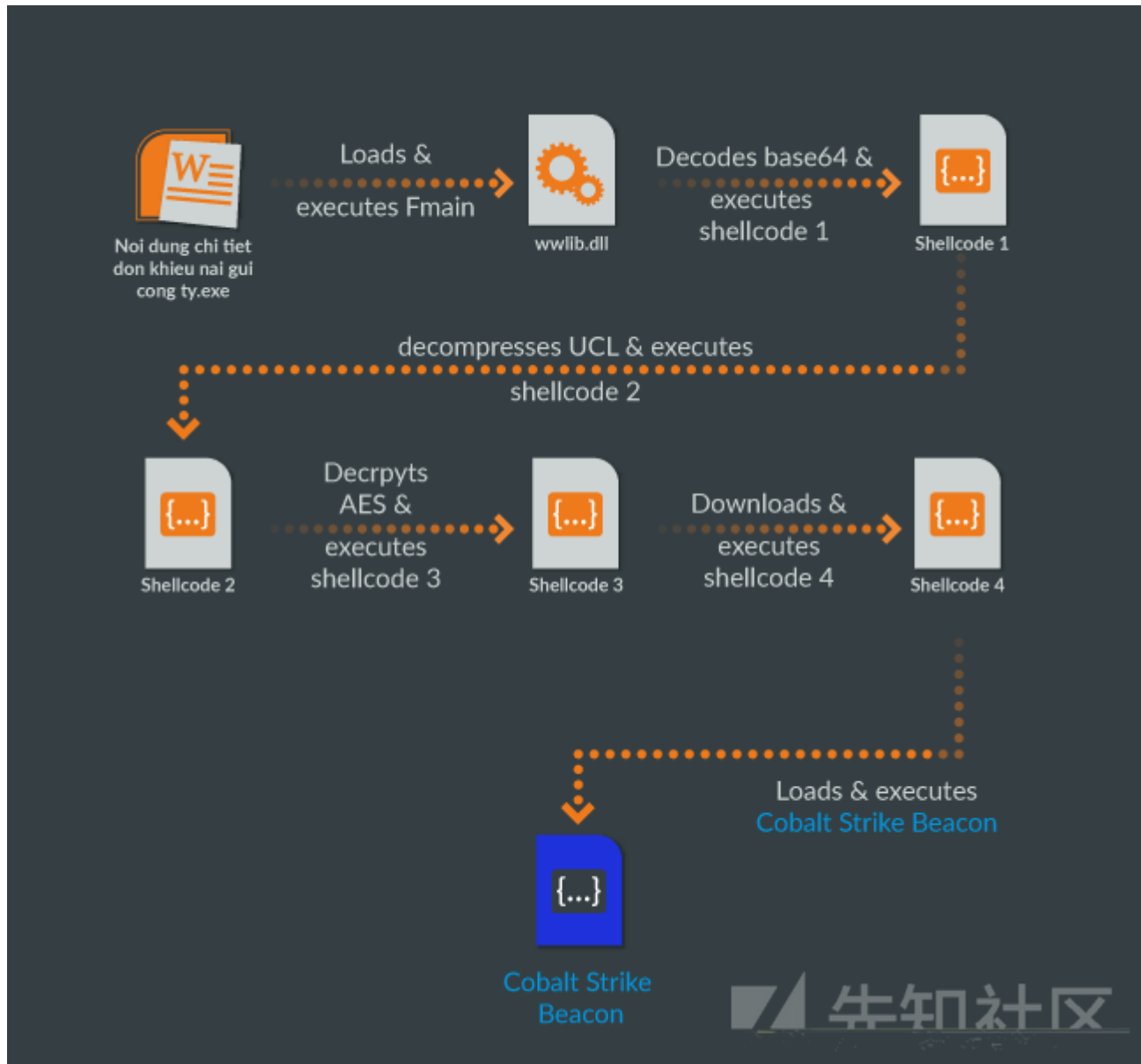
在分析期间，恶意载荷仍然有效，我们发现下载的文件是Cobalt Strike Beacon的变种。[Cybereason](#)在以前的攻击活动中使用Cobalt Strike。我们看到，该恶意软件的目的是在内存中下载并执行Cobalt Strike Beacon有效负载。虽然Cobalt Strike是一款商业渗透工具。但很多攻击者在活动中使用它。

在调查KerrDown时，我们发现了多个包含恶意软件的RAR文件。攻击者通过压缩和加密来隐藏攻击程序。RAR文件哈希如下：

(SHA256:040abac56542a2e0f384adf37c8f95b2b6e6ce3a0ff969e3c1d572e6b4053ff3)

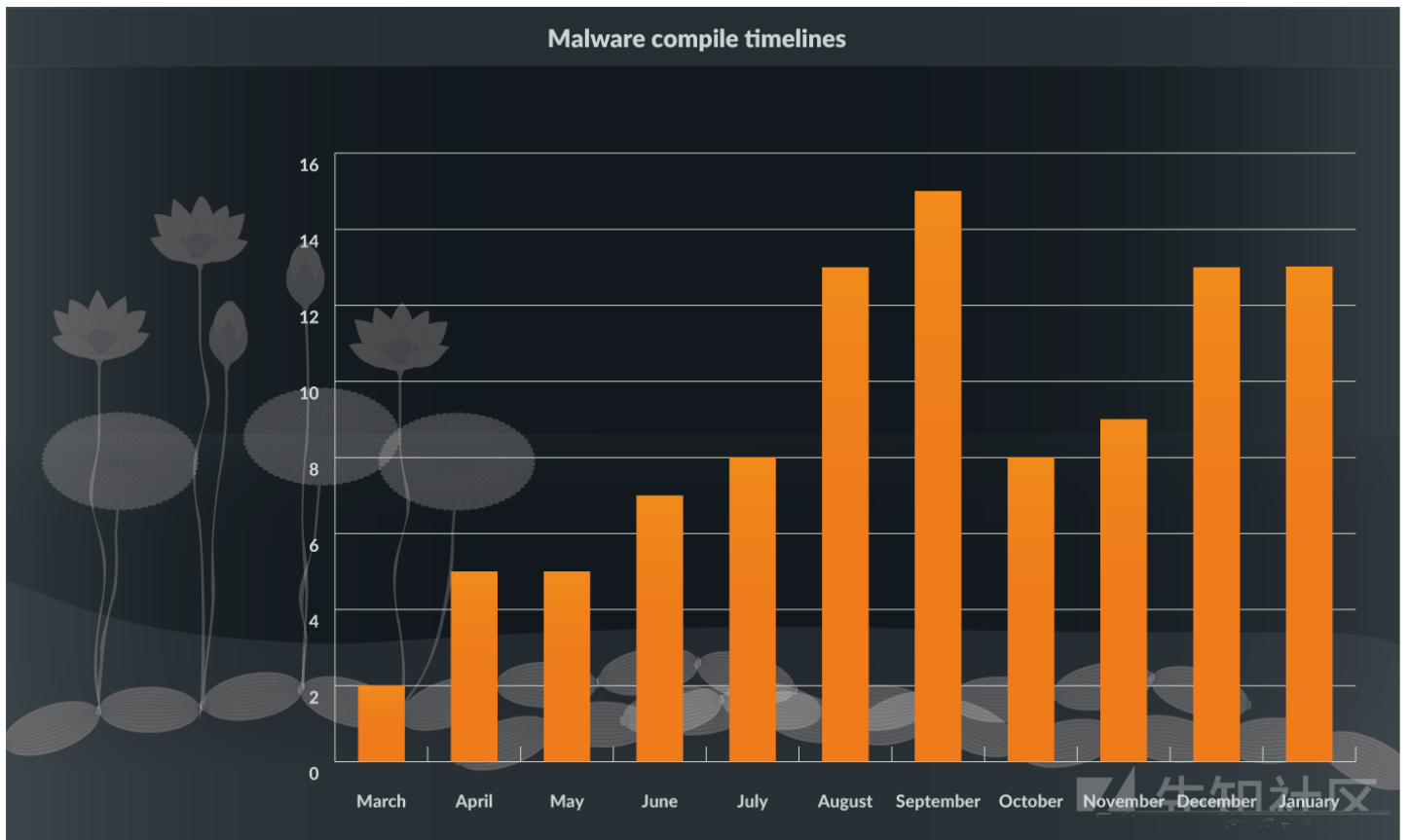
压缩文件的文件名用越南话书写，为“Don khieu nai.rar”，是“投诉信”的意思。该文件包含一个合法的旧版Microsoft Word (Microsoft Word 2007) 可执行文件，名为“Noi dung chi tiet don khieu nai gui cong ty.exe”，其含义是“了解贵公司更多信息”。攻击者加载该DLL。DLL执行多个shellcode，每段shellcode使用各种技术进行隐藏。具体步骤如下：

1. Microsoft Word exe将wwlib.dll加载到同一目录并执行DLL中的“FMain”功能。
2. DLL用base64解码shellcode并执行。
3. shellcode用开源代码UCL进行解压第二个shellcode并执行。
4. 第二个shellcode用AES解密第三个shellcode
5. 第三个shellcode从以下位置检索shellcode并执行：[https://cortanasyn\[.\]com/Avcv](https://cortanasyn[.]com/Avcv)
6. 第四个shellcode将嵌入的Cobalt Strike Beacon DLL加载到内存并执行。

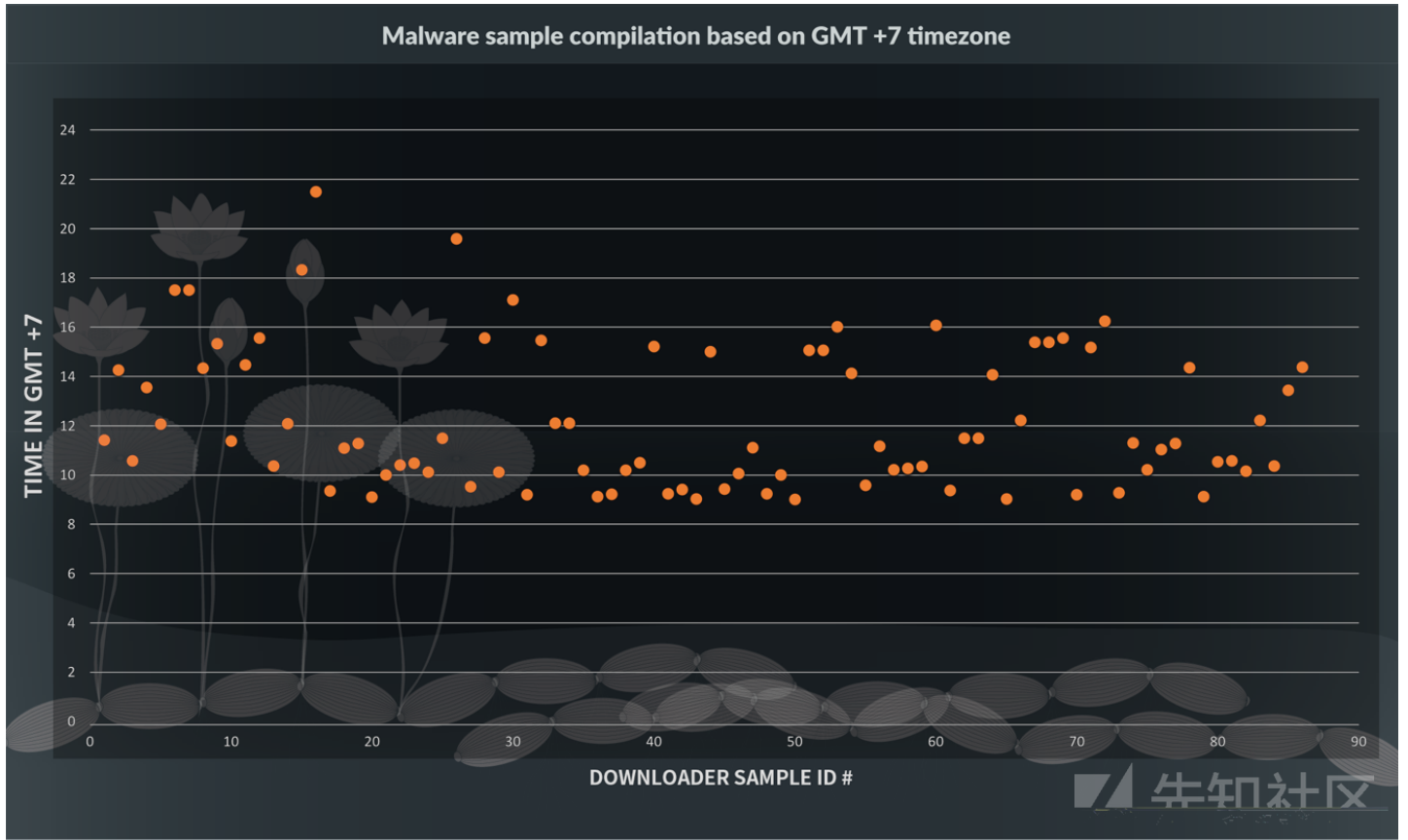


通过对KerrDown样本的时间戳进行分析，我们可以得出如下结论：

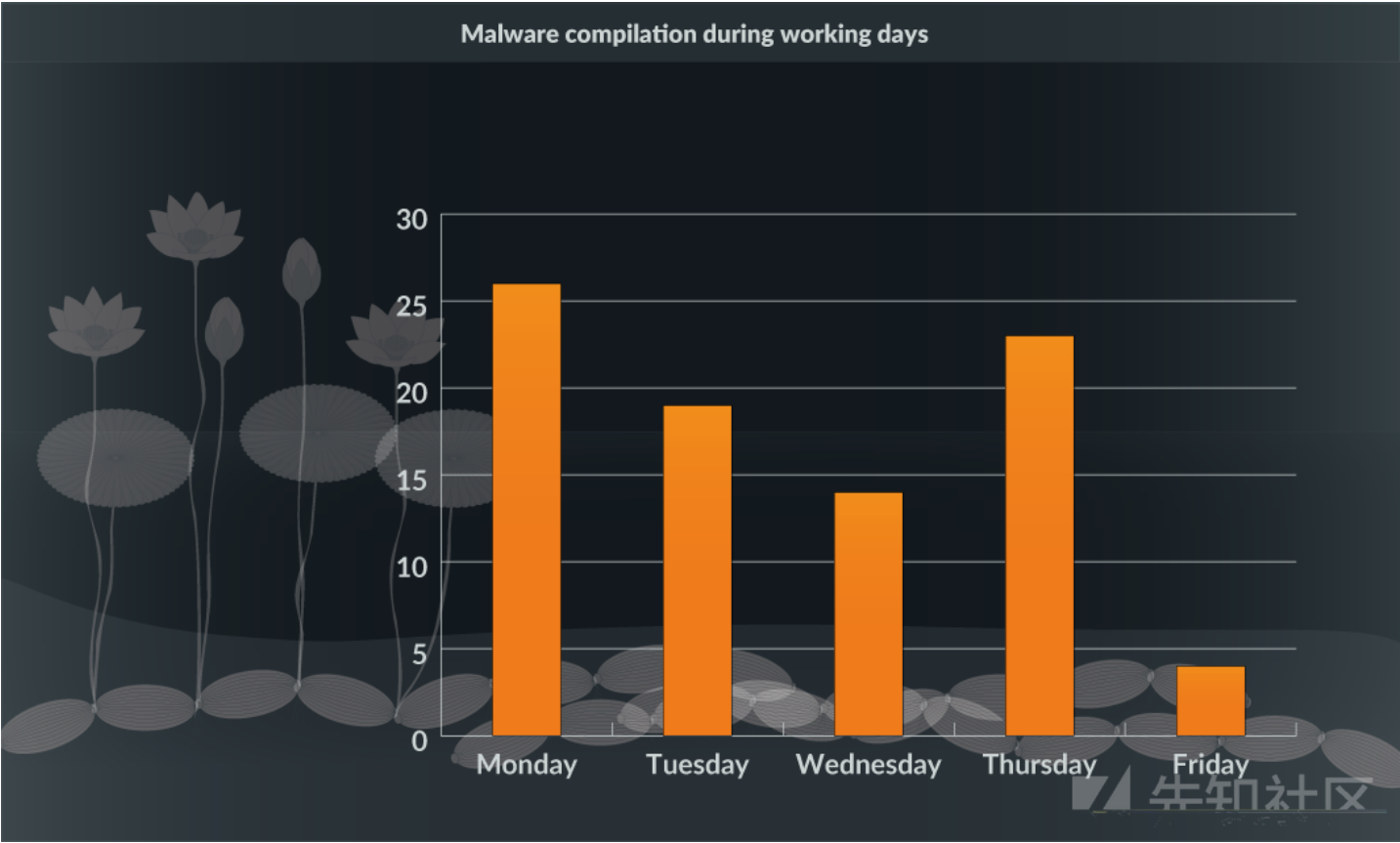
OceanLotus组织自2018年3月以来一直在其活动中使用该下载程序。并继续使用它。下图显示了KerrDown活动时间轴：



人们普遍认为OceanLotus组织来自越南，我们希望从我们的数据集中找到他们的工作模式，我们绘制了文件的编译时间，发现该组织工作时间为上午9点至下午6点。大部分



我们还观察到所有样本都是在工作日期间编译的：周一到周五。因此，OceanLotus组织在工作日工作，周末休息。下图是本周编译的样本。



三、总结

OceanLotus组织是亚太地区极具危险性的组织之一。正如我们在最近的活动中发现的KerrDown恶意软件。该组织在不断更新自己的技术和工具。所以，了解其运营和架构

四、IOC

Lure DOCS

73dcbcc47d6bd95dcf031ebbd34ac42301a20ee1143ac130b405e79b4ba40fc8
89e19df797481ae2d2c895bcf030fe19e581976d2aef90c89bd6b3408579bfc3
a4a066341b4172d2cb752de4b938bf678ceb627ecb72594730b78bd05a2fad9d
8bf22202e4fd4c005afde2266413cba9d1b749b1a2d75deac0c35728b5eb3af8
df8210d20c5eb80d44ba8fa4c41c26c8421dcb20168e4f796e4955e01ebc9e13
94fab926b73a6a5bc71d655c8d611b40e80464da9f1134bfce7b930e23e273ab
4321a9f95901a77b4acfbaf3596cf681712345e1cbd764873c6643fe9da7331

KerrDown DLLs

4a0309d8043e8acd7cb5c7cfca95223afe9c15a1c34578643b49ded4b786506b
4b431af677041dae3c988fcc901ac8ec6e74c6e1467787bf099c4abd658be5be
4bc00f7d638e042da764e8648c03c0db46700599dd4f08d117e3e9e8b538519b
4e2f8f104e6cd07508c5b7d49737a1db5eeba910adfdb4c19442a7699dc78cfc
4e791f2511c9bd3c63c8e37aa6625d8b590054de9e1cca13a7be2630bc2af9ce
539e8a53db3f858914cfe0d2132f11de34a691391ba71673a8b1e61367a963c7
53cd92f37ffd0822cc644717363ba239d75c6d9af0fa305339eaf34077edd22d
53efaac9244c24fab58216a907783748d48cb32dbdc2f1f6fb672bd49f12be4c
5c18c3e6f7ac0d0ac2b5fa9a6435ee90d6bd77995f85bed9e948097891d42ca2

5cda7d8294a8804d09108359dd2d96cdf4fdcf22ec9c00f0182d005afff76743
5f0db8216314da1f128b883b918e5ac722202a2ae0c4d0bf1c5da5914a66778e
6010d44cdca58cdec4559040e08798e7b28b9434bda940da0a670c93c84e33cd
60b65ebb921dca4762aef427181775d10bbffc30617d777102762ab7913a5aa1
6146aedfe47597606fb4b05458ec4b99d4e1042da7dc974fa33a57e282cd7349
6245b74b1cc830ed95cb630192c704da66600b90a331d9e6db70210acb6c7dfa
67cd191eb2322bf8b0f04a63a9e7cb7bc52fb4a4444fcb8fed2963884aede3aa
68f77119eae5e9d2404376f2d87e71e4ab554c026e362c57313e5881005ae79e
69e679daaaff3832c39671bf2b813b5530a70fb763d381f9a6e22e3bc493c8a9
6faa7deb1e1e0c3a7c62c2bb0ecd56b6e3ba4fe16971ec4572267ac70b9177
6fb397e90f72783adec279434fe805c732ddb7d1d6aa72f19e91a1bf585e1ea5
70db041fb5aad63c1b8ae57ba2699baa0086e9b011219dcebccbf632017992
7673f5468ba3cf01500f6bb6a19ce7208c8b6fc24f1a3a388eca491bc25cd9cd
77805a46f73e118ae2428f8c22ba28f79f7c60aeb6305d41c0bf3ebb9ce70f94
788265447391189ffc1956ebfec990dc051b56f506402d43cd1d4de96709c082
7be613237b57fbc3cb83d001efadeed9936a2f519c514ab80de8285bdc5a666c
7dbb7fab4782f5e3b0c416c05114f2a51f12643805d5f3d0cd80d32272f2731a
7ec77e643d8d7cc18cc67c123feceed91d10db1cc9fa0c49164cba35bb1da987
860f165c2240f2a83eb30c412755e5a025e25961ce4633683f5bc22f6a24ddb6
868ed69533fac80354a101410d3dd0a66f444385c6611cc85c5b0be49db2d6fd
89759e56d5c23085e47d2be2ce4ad4484dfdd4204044a78671ed434cec19b693
8b7fb1cd5c09f7ec57ccc0c4261c0b4df0604962556a1d401b9cbfd750df60ba
8d6e31c95d649c08cdc2f82085298173d03c03afe02f0dacb66dd3560149184f
942d763604d0aefdff10ce095f806195f351124a8433c96f5590d89d809a562f
98a5f30699564e6d9f74e737a611246262907b9e91b90348f7de53eb4cf32665
9e6011d6380207e2bf5105cde3d48e412db565b92cdc1b3c6aa15bd7bd4b099f
a106e0a6b7cc30b161e5ea0b1ec0f28ab89c2e1eb7ba2d5d409ddbabc3b037e6
a2b905c26e2b92e63de85d83e280249258cb21f300d8c4a3a6bdb488676e9bcf
a4a86e96f95f395fc0ceb6a74a2564f4ba7adbe1b40cc702b054427327a0399
a8192656dd1db0be4cec9d03b4d10e0529d9c52c899eda8d8e72698acfb61419
a8f776bd3a9593e963b567ce790033fec2804ea0afb40a92d40e21d8f33d066f
b4966f8febdba6b2d674afffc65b1df11e7565acbd4517f1e5b9b36a8c6a16ed
bb25f1a73d095d57b2c8c9ac6780e4d412ddf3d9eef84a54903cc8e4eae7c335
bc82bce004afb6424e9d9f9fc04a84f58edf859c4029eda08f7309dbeec67696
c30198e0b0e470d4ac8821bd14bb754466e7974f1c20be8b300961e9e89ed1ea
caabc45e59820a4349db13f337063eddede8a0847ae313d89a800f241d8556c8
d3ef6643ad529d43a7ec313b52c8396dc52c4daad688360eb207ee91a1caf7b2
e3c818052237bb4bb061290ab5e2a55c3852c8a3fef16436b1197e8b17de2e18

e56ffcf5df2afd6b151c24ddfe7cd450f9208f59b5731991b926af0dce24285a
e8704bf6525c90e0f5664f400c3bf8ff5da565080a52126e0e6a62869157dfe3
e8a454cd8b57a243f0abeec6945c9b10616cfdcc4abfb4c618bfc469d026d537
eac776c3c83c9db1a770ffaf6df9e94611c8293cbd41cb9257148603b8f2be0b
ead0f3e6f0ca16b283f09526d09e8e8cba687dab642f0e102e5487cb565bf475
f011a136996fa53fdbde944da0908da446b9532307a35c44ed08241b5e602cc9
f2a2f4fa2ed5b2a94720a4661937da97ab21aa198a5f8c83bb6895aa2c398d22
f62f21ee7e642f272b881827b45ceb643c999a742e1d3eac13d1ba014d1e7f67
f9f0973dc74716b75291f5a9b2d59b08500882563011d1def2b8d0b1b9bbb8ae

C2

theme[.].]blogsite[.]org

cortana[.]homelinux[.]com

word[.]webhop[.]info

work[.]windownoffice[.]com

cortanasyn[.]com

e[.]browsersyn[.]com

syn[.]servebbs[.]com

service[.]windown-update[.]com

check[.]homeip[.]net

outlook[.]updateoffices[.]net

mail[.]fptservice[.]net

office[.]windown-update[.]com

cortanazone[.]com

beta[.]officopedia[.]com

videos[.]dyndns[.]org

service[.]serveftp[.]org

syn[.]browserstime[.]com

check[.]webhop[.]org

ristineho[.]com

硬编码的配置信息，可以看到C2：[https:// b.cortanazone\[.\]com](https://b.cortanazone[.]com)。如下图所示：

▼	9a485c477c771b02ad3eb5c5a1f42426cf4495df90306c1f5ab327cf46053656
▼	CV Ly Anh Tu
	CV Thông tin cá nhân Ly Anh Tu - Phòng viên Tài chính - Ngân hàng - Chung khoan - 28-06-2018 .exe
	wwlib.dll
▼	03d0fc9af277bebc908338ae4ce9062a3a8faf80960ad61ce0207c27a19b7f2f
▼	Ban Co Yeu va sai pham thông tin trên website
	Ban Co Yeu va sai pham thông tin trên website.doc.exe
	wwlib.dll
▼	7a4b9e7db193ba7f57376cd6671617bbad34eb7ac7511030b7f60cb7826b0b25
▼	Tong Cuc Thue Viet Nam va sai pham thông tin trên website
	Tong Cuc Thue Viet Nam va sai pham thông tin trên website.exe
	wwlib.dll
▼	4e0ae56827852f96de0eff8ab8c2562fac9157b0440761579a95f30d8cc905cc
▼	Quang cao
	Lien he dat quang cao trên các trang báo của Công ty TNHH Truc tuyen Sai gon Kinh thuong 18_04_2018.exe
	wwlib.dll
▼	8fe79e805a0e516758bec37306c12aaed4d3598af4a91cc220ab0d8ef5e2e310
▼	Don cau cuu
	Nội dung chi tiết đơn cầu cứu gửi chỉ Nhung . Công hòa xã hội chủ nghĩa Việt Nam Doc lap tu do hanh phuc.exe
	wwlib.dll
▼	040abac56542a2e0f384adf37c8f95b2b6e6ce3a0ff969e3c1d572e6b4053ff3
▼	Don khieu nai
	Nội dung chi tiết đơn khiếu nại gửi công ty.exe
	wwlib.dll
▼	042f24da1ed77b66553d8a87bc471ef867f6fc1430762bbdb982afe41807f0ff
▼	Hình ảnh cần báo vi phạm
	Một số hình ảnh cần báo vi phạm kỹ luật.exe
	wwlib.dll
▼	497675d3825e977855dc6bac6240b92b11eca14fd16d05c1e5ef41f631ae0f85
▼	Thu moi tham du
	Thu moi tham du hội nghị toàn quốc. Công hòa xã hội chủ nghĩa Việt Nam - Doc lap tu do.exe
	wwlib.dll
▼	49f51e66b43c42a81821889437ac72923c0aa56d5e6e57c238e56a813578e881
▼	TocaoPageCongDongSinhVienHutech
	Hình ảnh chi tiết tạo page công đồng sinh viên hutech admin dat.exe
	wwlib.dll
▼	a5fd69f6337b61249eba5a6bf0035b39331c60314b296261a6627e408d442291
▼	Don cau cuu
	Nội dung chi tiết đơn cầu cứu gửi anh Thang. Công hòa xã hội chủ nghĩa Việt Nam Doc lap tu do hanh phuc.exe
	wwlib.dll
▼	c47e71f39ddb42ce546b19dd3cfeea137848507dafdeaff5cd421c9757e042cd
▼	Thu moi
	Thu moi tham du hội nghị toàn quốc. Công hòa xã hội chủ nghĩa Việt Nam - Doc lap tu do.exe.exe
	wwlib.dll
▼	cd7a0315e046e7d4e0912d9741694ef5ad790064dca3d54e6096f4bd0a71cc2e
▼	Don cau cuu
	Nội dung chi tiết đơn cầu cứu gửi Thay Diép . Công hòa xã hội chủ nghĩa Việt Nam Doc lap tu do hanh phuc.exe
	wwlib.dll
▼	fed8de1236e378a4d44d3a770048a12e3c102874f9903f94ad6e1f598031e0ca
▼	Don khieu nai
	Nội dung chi tiết đơn khiếu nại. Công hòa xã hội chủ nghĩa Việt Nam Doc lap tu do hanh phuc.exe
	wwlib.dll
▼	fa7b968c3f2aa2be9683db5c7d5632867c5d6cee3d2992e32c6be471ba4624c9
▼	Thu moi
	Thu moi tham du hội nghị và thông tin nội dung chi tiết về việc tổ chức hội nghị - Từ ngày 29-07-2018 - 30-07-2018.exe
	wwlib.dll
▼	d21d9c66e8b23946b022678c78db324e53b8ad70fd97907bdc0674b154c1e060
▼	Gui lai cho MS.MAI post content kaspersky
	Gui lai cho MS.MAI post and banner content kaspersky.exe
	wwlib.dll
▼	dacc4fc7c5bb740487d9ce5f0d6e0d110dc25992d8536b036245a9422f7e060a
▼	Thu moi
	Thu moi tham du hội nghị và thông tin nội dung chi tiết về việc tổ chức hội nghị - Từ ngày 09-09-2018 - 10-09-2018.exe
	wwlib.dll

点击收藏 | 0 关注 | 1

[上一篇：某CMS-5.0.190111后台...](#) [下一篇：利用DWORD SHOOT实现堆溢...](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)