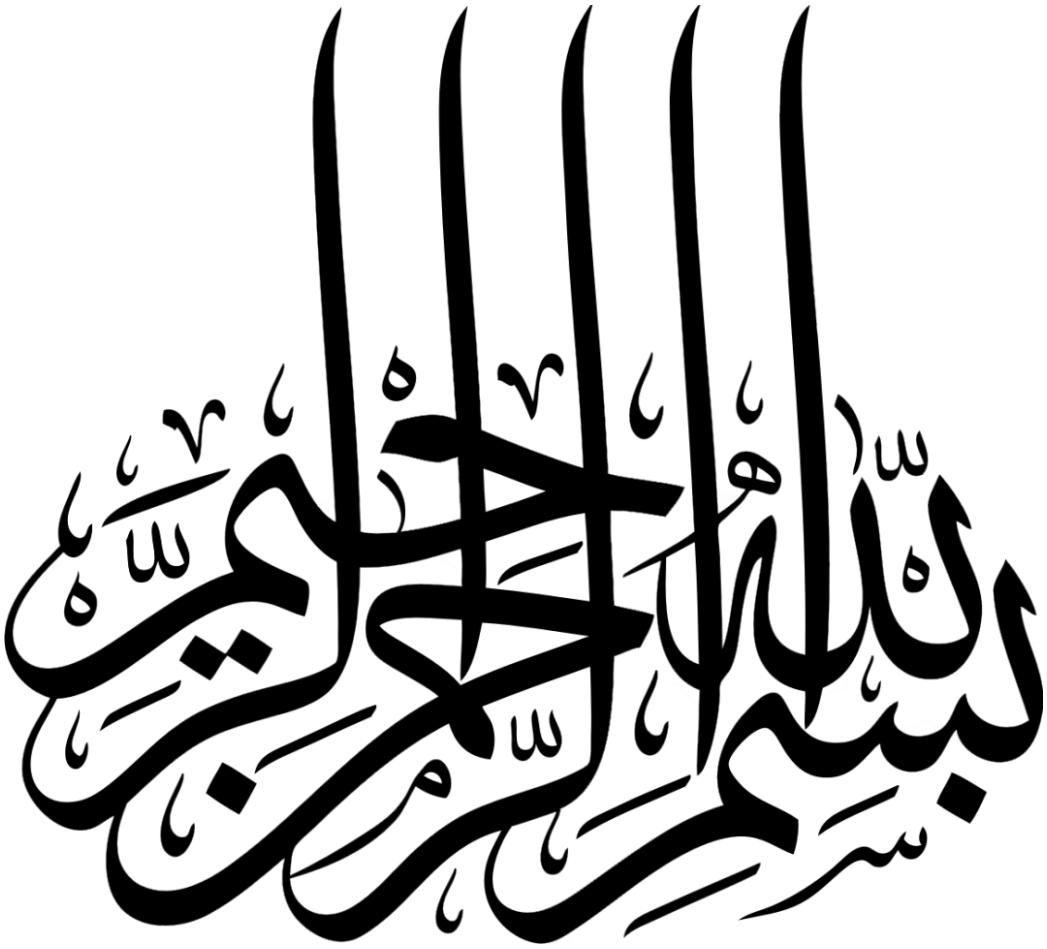

بسم الله الرحمن الرحیم

Ryuk in 5 Hours

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

مقدمه

تهدیدگران Ryuk از یک ایمیل فیشینگ به باج‌افزار در سطح دامنه در ۵ ساعت رسیدند. آنها با استفاده از Zerologon (CVE-2020-1472) کمتر از ۲ ساعت پس از فیشینگ اولیه، امتیازات خود را افزایش دادند. آنها از ابزارهایی مانند Cobalt Strike، AdFind، WMI و PowerShell برای رسیدن به هدف خود استفاده کردند.

Ryuk در چند سال گذشته یکی از ماهرترین گروه‌های باج‌افزاری بوده است، به طوری که اف‌بی‌آی ادعا می‌کند تا فوریه ۲۰۲۰، ۶۱ میلیون دلار به این گروه پرداخت شده است. اوایل امسال، گروه کمی ساکت شد، اما به نظر می‌رسد که این روند در چند هفته اخیر تغییر کرده است، با حوادثی مانند آنچه در بیمارستان‌های UHS رخ داد.

خلاصه پرونده

در پرونده قبلی Ryuk ما، دیدیم که تهدیدگرها از طریق بدافزار لودر Bazar به یک محیط دسترسی پیدا کردند. این بار، ما دیدیم که آنها هدف خود را سریع‌تر محقق کردند، اما تاکتیک‌ها و تکنیک‌های کلی بین حوادث مشابه remained می‌باشد.

Bazar دوباره از طریق تحویل ایمیل‌های فیشینگ وارد محیط شد. برای تجزیه و تحلیل عمیق این لودر، تحلیل توسط Roman Marshanski & Vitali Kremez را ببینید. مشاهده شد که Bazar، پس از اجرا، دوباره به explorer.exe، svchost.exe تزریق می‌شود و فرآیندهای command shell را ایجاد می‌کند.

از این لودر، ما نقشه‌برداری اولیه دامنه را با استفاده از ابزارهای داخلی ویندوز مانند Nltest دیدیم. با این حال، برخلاف پرونده قبلی، تهدیدگرها با یک کاربر با امتیاز پایین‌تر شروع کردند و به جای حرکت آهسته یا محتاطانه، از آسیب‌پذیری Zerologon (CVE-2020-1472) برای بازنشانی رمز عبور ماشین کنترل‌کننده دامنه اصلی استفاده کردند.

حرکت جانبی از طریق انتقال فایل SMB و اجراهای WMI از بیکن‌های Cobalt Strike آغاز شد. نشانگرهای شبکه مشابه کمپین قبلی بودند و توسط Kyle Ehmke در پاسخ به پست قبلی ما که بر اساس اطلاعات گزارش noted شدند. از تحلیل حافظه، همچنین توانستیم نتیجه بگیریم که بازیگران از یک نسخه آزمایشی Cobalt Strike با رشته EICAR موجود در پیکربندی شبکه برای بیکن استفاده می‌کردند. از بیکن‌های پرتابل اجرایی (portable executable) و DLL استفاده شد.

پس از حرکت جانبی به کنترل‌کننده دامنه ثانویه، تهدیدگر کشف دامنه بیشتری را از طریق Net و ماژول پاورشل اکتیو دایرکتوری آغاز کرد. از آنجا، به نظر می‌رسید تهدیدگرها از ماژول افزایش امتیاز named pipe پیش‌فرض روی سرور استفاده کردند. در این مرحله، تهدیدگرها با استفاده از حساب داخلی Administrator، از RDP برای اتصال از کنترل‌کننده دامنه ثانویه به کنترل‌کننده دامنه اول استفاده کردند.

هنگامی که در کنترل‌کننده دامنه اصلی قرار گرفتند، بیکن Cobalt Strike دیگری رها و اجرا گردید. سپس شناسایی دامنه بیشتری با استفاده از AdFind انجام شد. پس از اتمام این کار، در ساعت چهارم، تهدیدگرها برای هدف نهایی خود آماده بودند.

در ۴ ساعت و ۱۰ دقیقه، تهدیدگرها از نقطه حرکت (pivot) از کنترل‌کننده دامنه اصلی برای اتصال RDP به سرور پشتیبان استفاده کردند. سرورهای پشتیبان دوباره ابتدا هدف استقرار فایل اجرایی باج‌افزار

قرار گرفتند، و سپس سرورها و پس از آن ایستگاه‌های کاری. تهدیدگرها هدف خود را با اجرای باج‌افزار روی کنترل‌کننده دامنه اصلی به پایان رساندند و در ساعت ۵، حمله کامل شد.

در حالی که دفعه قبل در مورد زمان بین روز اول و دوم برای کمک به فعالیت‌های تشخیص و پاسخ اظهار نظر کردیم، این پرونده نشان می‌دهد که شما نمی‌توانید روی آن نوع بازه زمانی حساب کنید. شما باید آماده باشید تا در کمتر از یک ساعت اقدام کنید، تا مطمئن شوید که می‌توانید به طور مؤثر تهدیدگر را مختل کنید.

جدول زمانی


Ryuk in 5 hours
17:01 UTC Bazar malware executed
C2 3.137.182.114:443
19:34 Bazar injection spawns new explorer process
19:41 Domain discovery activity
19:48 Zerologon vulnerability exploited against primary domain controller
CVE-2020-1472
19:56 First lateral movement to secondary domain controller over SMB with WMI exec
20:03 Command and control established on secondary domain controller
Cobalt Strike beacon C2 88.119.171.94:443
20:07 Second Cobalt Strike beacon DLL executed new C2
5.2.64.174:443
20:12 discovery continues on domain controller
20:39 Lateral movement from secondary domain controller to primary domain controller via RDP
20:42 Cobalt Strike DLL executed on primary domain controller
C2 5.2.64.174:443
20:57 AdFind run on primary domain controller
20:09 Threat actor continues moving laterally to other domain joined systems via RDP
20:29 Ryuk executable is transfered over RDP connections and executed
21:03 Ryuk is ran on last system

دسترسی اولیه

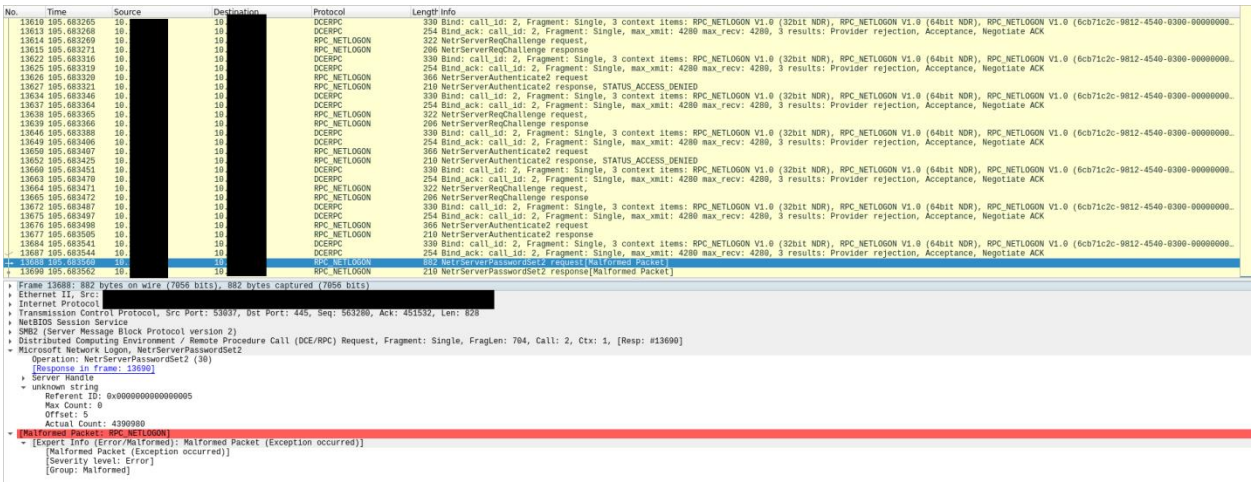
دسترسی با یک ایمیل فیشینگ آغاز شد که به فایل اجرایی بدافزار لودر Bazar منجر گردید.

اجرا

Bazar برای اجرا به اجرای فایل اجرایی توسط کاربر متکی است. این کاربر یک Domain User بود و هیچ مجوز دیگری نداشت.

افزایش دسترسی

از CVE-2020-1472 برای بازنشانی اعتبارنامه‌ها روی یکی از کنترل‌کننده‌های دامنه در محیط استفاده شد. پس از بازنشانی رمز عبور، تهدیدگرها سپس یک کنترل‌کننده دامنه دیگر را هدف قرار دادند، احتمالاً این کار به دلیل مختل شدن سرویس‌ها در اثر استفاده از اکسپلویت آنها صورت گرفته است.



بسته نشان‌دهنده رمز عبور صفر شده (zeroed out).

در یکی از کنترل‌کننده‌های دامنه ما شاهد استفاده از روش افزایش سطح دسترسی از طریق named pipe در Cobalt Strike بودیم.

C:\Windows\system32\cmd.exe /c echo 92d8cc45954 >; \\.\pipe\446b3c

فرار از شناسایی

در اولین کنترل‌کننده دامنه که تهدیدگرها پس از اتصال اولیه خود به آن متصل شدند، آنها یک فایل DLL را رها کرده (dropped) و آن را از طریق rundll32 اجرا کردند.

C:\Windows\system32\cmd.exe /C rundll32 C:\Windows\system32\SQL.dll, StartW

روی کنترل‌کننده دامنه، [فایل] از طریق RDP رها و از طریق rundll32 اجرا شد.

rundll32 C:\PerfLogs\arti64.dll, rundll

اندکی پس از آن، DLL دوباره از طریق regsvr32 فراخوانی شد.

regsvr32 C:\PerfLogs\arti64.dll

سپس یک DLL دوم به روشی مشابه روی کنترل‌کننده دامنه رها و اجرا شد.

rundll32 C:\\PerfLogs\\socks64.dll, rundll

کشف

روی میزبان beachhead اجرا شد.

nltest /domain_trusts /all_trusts

nltest /dclist:DOMAIN

net group "Domain admins" /DOMAIN

روی یک کنترل‌کننده دامنه اجرا شد.

net group "enterprise admins" /domain

nltest /domain_trusts /all_trusts

nltest /dclist:"DOMAIN"

ping DOMAINCONTROLLER

cmd.exe /C time

net user administrator /domain

سپس آنها ماژول پاورشل اکتیو دایرکتوری (PowerShell Active Directory module) را وارد کردند.

```
C:\\Windows\\System32\\W   powershell -nop -exec bypass -EncodedComman
indowsPowerShell\\v1.0\\   d SQBtAHAAbwByAHQALQBNAG8AZAB1AGwAZQAgAEEAY
powershell.exe             wB0AGkAdgBlAEQAaQByAGUAYwB0AG8AcgB5AA==
```

سپس آنها دستور زیر را برای جستجوی نام میزبان‌ها، سیستم‌عامل‌ها و تاریخ آخرین ورود (last logon dates) همه سیستم‌های Active Directory اجرا کردند.

C:\Windows\system32\cmd.exe /C Get-ADComputer -Filter {enabled -eq $true} -properties *|select Name, DNSHostName, OperatingS

پس از تکمیل کار کشف فوق و جابجایی (pivot) به کنترل‌کننده دامنه خود، تهدیدگرها برای شناسایی بیشتر دامنه به سراغ AdFind رفتند.

C:\Windows\Temp\adf\AdFind.exe

C:\Windows\Temp\adf\adf.bat

Contents of the script ran the following with AdFind.

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"(

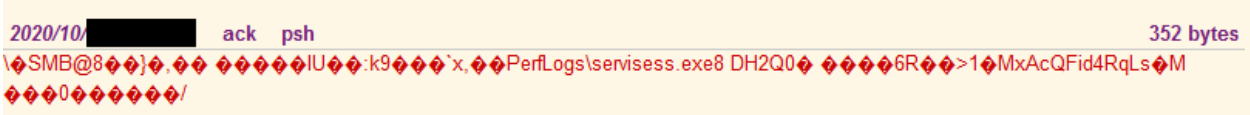
adfind.exe -gcb -sc trustdmp

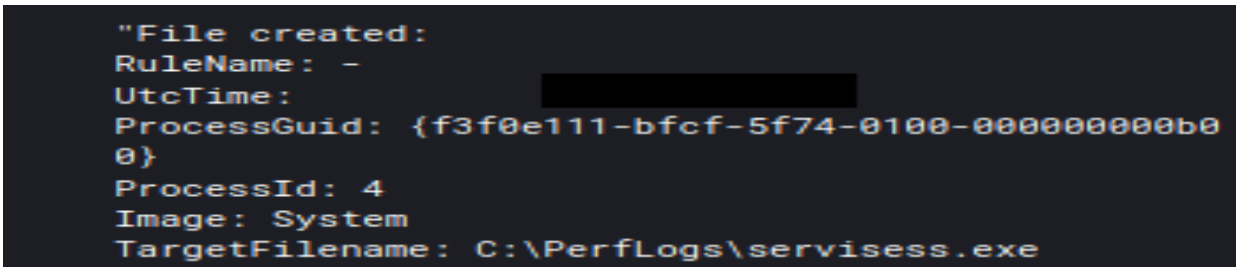
The threat actor then ran this command a few times.

nltest /domain_trusts /all_trusts

حرکت جانبی

اولین حرکت جانبی به سمت کنترل‌کننده دامنه‌ای انجام شد که تحت تأثیر استفاده از CVE-2020-1472 قرار نگرفته بود. یک فایل اجرایی از طریق SMB و با استفاده از یک حساب کاربری مدیر دامنه به آن منتقل شد.

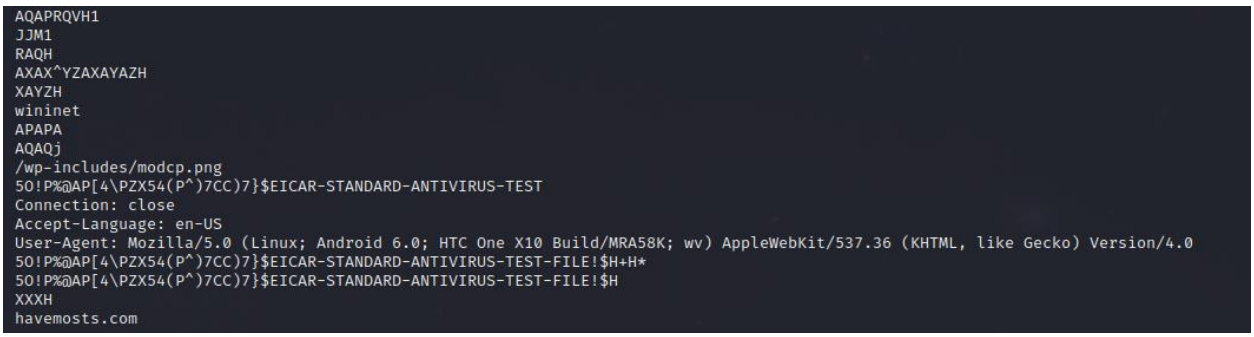




پس از انتقال فایل اجرایی، تهدیدگرها از WMI روی میزبان beachhead برای اجرای فایل استفاده کردند.

C:\Windows\system32\cmd.exe /C WMIC/node:"DC.DOMAIN.local" process call create "cmd /c C:\PerfLogs\servisess.exe"\

وجود رشته‌های EICAR نشان می‌دهد که از نرم‌افزار Cobalt Strike به عنوان یک نسخه آزمایشی استفاده شده است.



آنها به GPO دامنه دسترسی پیدا کردند، اما هیچ‌کدام اصلاح یا اضافه نشدند.

mmc.exe" "C:\Windows\System32\gpedit.msc"

اندکی پس از آن، ما شاهد انتقال یک فایل DLL مربوط به Cobalt Strike از طریق اتصال RDP بودیم.

```
"File created:
RuleName: technique_id=T1047,technique_name=File System Permissions Weaknes
s
UtcTime:
ProcessGuid: {1372730A-D516-5F74-6700-000000000F00}
ProcessId: 2656
Image: C:\Windows\Explorer.EXE
TargetFilename: C:\PerfLogs\arti64.dll
CreationUtcTime:
```

حرکت جانبی و تحویل payload

از RDP برای جابجایی (pivot) از کنترل‌کننده دامنه اصلی و توزیع payload نهایی باج‌افزار در سراسر سازمان استفاده شد.

فرماندهی و کنترل

پس از گزارش قبلی ما، @kyleehmke بر اساس گزارش قبلی Ryuk ما جابجا شد (pivot) و از داده‌های شبکه برای ارتباط دادن چندین دامنه از این دامنه‌ها استفاده کرد که ما در این پرونده مشاهده کردیم.

Bazar:

Report_Print.exe

۳.۱۳۷.۱۸۲.۱۱۴:۴۴۳

cstr3.com

Cobalt Strike:

servisses.exe

۸۸.۱۱۹.۱۷۱.۹۴:۴۴۳

Certificate 86:77:d8:5e:51:69:ac:e2:08:07:2e:b0:dc:6c:10:9e:25:80:70:a6

Not Before 2020/10/06 13:33:55 UTC

Not After 2021/10/06 13:33:55 UTC

Issuer Org lol

Subject Common havemosts.com

Subject Org lol

Public Algorithm rsaEncryption

JA3: 57f3642b4e37e28f5cbe3020c9331b4c

JA3s: e35df3e00ca4ef31d42b34bebaa2f86e

SQL.dll

۵.۲.۶۴.۱۷۴:۴۴۳

Certificate 36:d5:68:f9:be:2a:34:e1:76:3d:89:78:e5:62:4d:fc:ae:02:97:ad

Not Before 2020/10/02 16:45:57 UTC

Not After 2021/10/02 16:45:57 UTC

Issuer Org lol

Subject Common quwasd.com

Subject Org lol

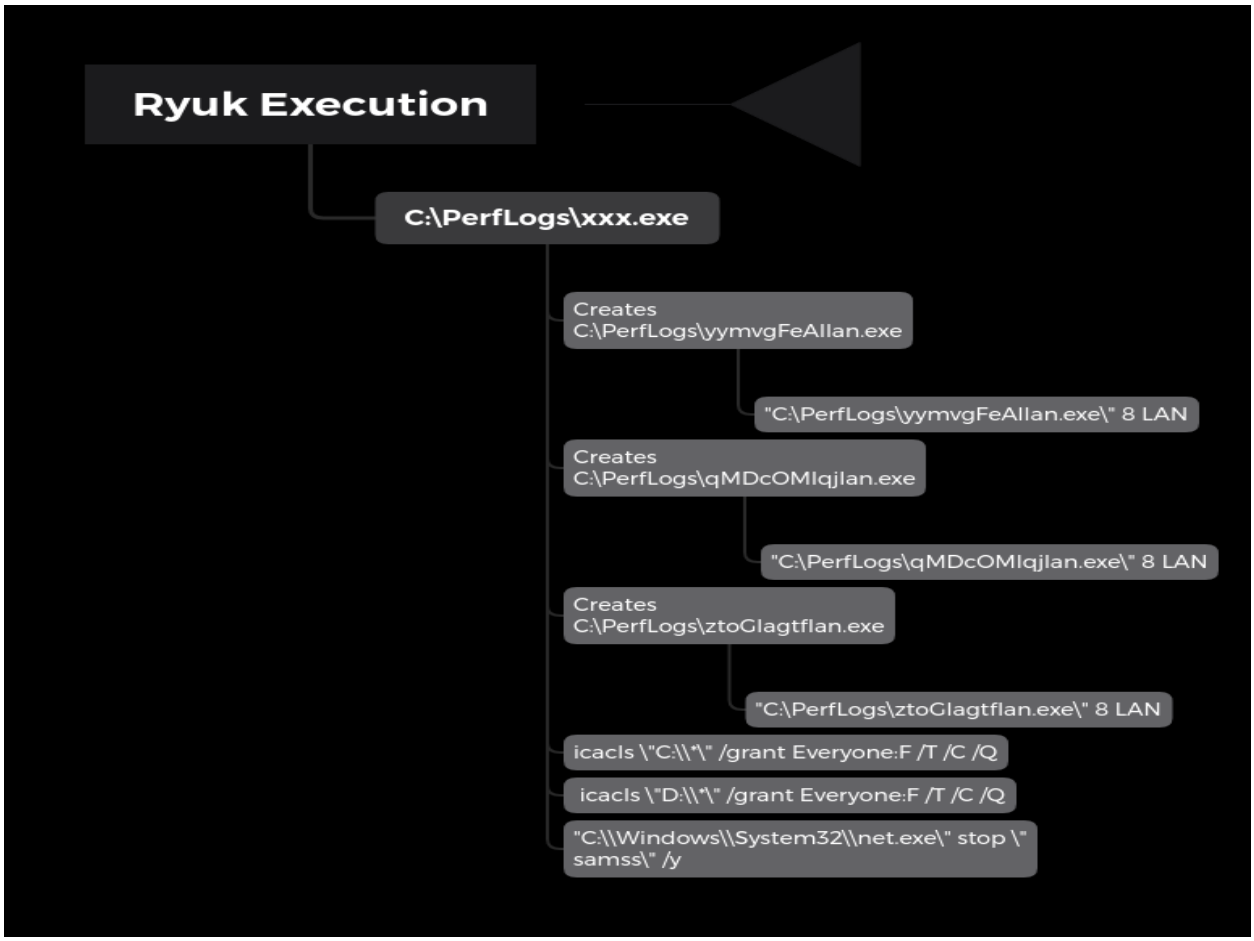
Public Algorithm rsaEncryption

JA3: a0e9f5d64349fb13191bc781f81f42e1

JA3s: ae4edc6faf64d08308082ad26be60767

تأثیر

حدود ۴.۵ ساعت پس از اجرای بدافزار اولیه Bazar، تهدیدگران Ryuk به اهداف نهایی خود عمل کردند و اتصالات RDP را از کنترل‌کننده دامنه‌ای که قبلاً مورد بهره‌برداری قرار گرفته بود، به بقیه محیط آغاز کردند. این بار آنها ابتدا باج‌افزار را روی کنترل‌کننده دامنه ثانویه (اولین نقطه جابجایی خود) اجرا کردند و فایل اجرایی Ryuk را از طریق اتصال RDP منتقل کردند.



ما همچنین فایل‌های pcap، فایل‌ها، تصاویر حافظه، و بسته‌های Kape و Redline را در اینجا در دسترس داریم.

IOCs

https://misppriv.circl.lu/events/view/80223&

https://otx.alienvault.com/pulse/5f8cce76f5614d9b220181b6

Network

۳.۱۳۷.۱۸۲.۱۱۴:۴۴۳

cstr3.com

۸۸.۱۱۹.۱۷۱.۹۴:۴۴۳

havemosts.com

۵.۲.۶۴.۱۷۴:۴۴۳

quwasd.com

File

servisses.exe

d971827d974effedaeaf7d62b619b1dd

c3a846eb04e2fe765e56fa15a0d5c1eb650ccba3

۱d8b7faf5f290465cc742e07abca78fac419135b191071cc77912263cd1dde1d

socks64.dll

۸۹۰۲۰۶f0c506366d480e02fc9fed988a

ba1542d9b55fff21bda9495ed884404b0436cff2

feb8c2bcb71da02dbbeecb999869e053cf96af8cce6f9705cadca4338133d3b5

SQL.dll

۳۷۸۵d87f6995b4b95d9b55f8d2556237

۹b44a8f0bb2d65fb19e7ca7bbd85b36c176f3d60

d67461ba45a4edf3b2a69b3e64303fda8130bd1fc7a1173f35c1fe67b40c9639

arti64.dll

۳۷۸۵d87f6995b4b95d9b55f8d2556237

۹b44a8f0bb2d65fb19e7ca7bbd85b36c176f3d60

d67461ba45a4edf3b2a69b3e64303fda8130bd1fc7a1173f35c1fe67b40c9639

xxx.exe

۵b8b66ddbbf1fd67211e9a4bf78c1700

cdb042dd8e9dc17f677c991b386f4cd242f2628d

ccde47a0d315dcd4740fccfe8e8110fbb1fd85bb305734fec409f52051790c98

Detections

Network

GPL NETBIOS SMB-DS IPC$ share access

ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Movement

ET POLICY SMB2 NT Create AndX Request For an Executable File

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_powershell_suspicious_parameter_variation.yml

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

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: 2020-10-13
Identifier: Case 1006 Ryuk
Reference: https://thedfirreport.com/
/*
*/Rule Set/* ----------------------------------------------------------------------
imort "pe"
rule ryuk_1006_servisses_procdump}
            meta:
            description = "files - file servisses-procdump.exe"
            author = "The DFIR Report"
```

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

date = "2020-10-13"

hash1 = "387894a0b404c67e722799308b12ff2be31d2e8ce798aa53d971f0c13805d54d"

strings:

$s1 = "c:/crossdev/src/winpthreads-svn6233/src/mutex.c" fullword ascii

$s2 = "mutex_global_shmem" fullword ascii

$s3 = "mutex_global_static_shmem" fullword ascii

$s4 = "_pthread_key_dest_shmem" fullword ascii

$s5 = "_pthread_key_sch_shmem" fullword ascii

$s6 = "_pthread_key_max_shmem" fullword ascii

$s7 = "_pthread_key_lock_shmem" fullword ascii

$s8 = "cannot find name of executable" fullword ascii

$s9 = "tiles32.png" fullword ascii

$s10 = "GetModuleFileName: %s" fullword ascii

$s11 = "IP_DEST_HOST_UNREACHABLE (11003)" fullword ascii

$s12 = "This program requires Windows NT!" fullword ascii

$s13 = "SNMP INVALID_SESSION" fullword ascii

$s14 = "SNMP TRAP_ERRORS" fullword ascii

$s15 = "SNMP SELECT_FDERRORS" fullword ascii

$s16 = "Some different radices: %d %x %o %#x %#o " fullword ascii

$s17 = "c:/crossdev/src/winpthreads-svn6233/src/rwlock.c" fullword ascii

$s18 = "_pthread_tls_shmem" fullword ascii

$s19 = "IP_DEST_PORT_UNREACHABLE (11005)" fullword ascii

$s20 = "pthr_root_shmem" fullword ascii

condition:

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

)pe.imphash() == "a90d500745a1ce2417c01fecefbc2851" or 8 of them(

{ rule ryuk_1006_files_socks64}

meta:

description = "files - file socks64.dll"

author = "The DFIR Report"

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

date = "2020-10-13"

hash1 = "feb8c2bcb71da02dbbeecb999869e053cf96af8cce6f9705cadca4338133d3b5"

strings:

$x1 = "C:\\Users\\Izidu\\Desktop\\2019\\WindowsSDK7-Samples-master\\WindowsSDK7-Samples-master\\winui\\pictures\\acquisitionplugin\\x64" ascii

$s2 = "C:\\Users\\Izidu\\Desktop\\2019\\WindowsSDK7-Samples-master\\WindowsSDK7-Samples-master\\winui\\pictures\\acquisitionplugin\\x64" ascii

$s3 = "PluginSample.dll" fullword ascii

$s4 = "AppPolicyGetProcessTerminationMethod" fullword ascii

$s5 = "luginSample.pdb" fullword ascii

$s6 = "rundll" fullword ascii

$s7 = "AcquireSamplePlugin::DisplayConfigureDialog" fullword wide

$s8 = "AppPolicyGetThreadInitializationType" fullword ascii

$s9 = "`template-parameter-" fullword ascii

$s10 = "operator<=>" fullword ascii

$s11 = "operator co_await" fullword ascii

$s12 = "AppPolicyGetWindowingModel" fullword ascii

$s13 = "Transfer Completed Successfully!" fullword wide

$s14 = "AppPolicyGetShowDeveloperDiagnostic" fullword ascii

$s15 = "noexcept" fullword ascii

$s16 = "Read-Only Photo Acquire Plugin" fullword wide

$s17 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide

$s18 = "Software\\Microsoft\\Windows\\CurrentVersion\\Photo Acquisition\\Plugins\\%ws" fullword wide

$s19 = ".?AUIUserInputString@@" fullword ascii

$s20 = "g0DVNrB\"Rtf#" fullword ascii

condition:

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

)pe.imphash() == "0fd22f187f22ab4ec2eb55f91ccefa7a" and (pe.exports("SGeruIUrgVdfMaxMccIKRh") and pe.exports("rundll")) or (1 of ($x*) and 4 of them ((

{ rule ryuk_1006_Report_Print}

meta:

description = "files - file Report_Print.exe"

author = "The DFIR Report"

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

date = "2020-10-13"

hash1 = "23ac461f9b5128841cafabb4282432252ea7b57874595cf6fe8457fc1ac65007"

strings:

$s1 = "kErNel32.Dll" fullword wide

$s2 = "DOOKOL.exe" fullword ascii

$s3 = "c:/crossdev/src/winpthreads-svn6233/src/mutex.c" fullword ascii

$s4 = "hmutex" fullword ascii

$s5 = "._FindPESectionExec" fullword ascii

$s6 = "mutex_global_shmem" fullword ascii

$s7 = "processthreadsapi.h" fullword ascii

$s8 = "mutex_global_static_shmem" fullword ascii

$s9 = "TargetIp" fullword ascii

$s10 = "c:\\crossdev\\gccmaster\\build-tdm64\\gcc\\x86_64-w64-mingw32\\libgcc" fullword ascii

$s11 = "h:\\crossdev\\gccmaster\\build-tdm64\\runtime\\mingw-w64-crt" f

ullword ascii

$s12 = "J__mingw_winmain_lpCmdLine" fullword ascii

$s13 = "GNU C 4.8.1 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuilding-libgcc -fno-stack-protector" fullword ascii

$s14 = "GNU C 4.8.1 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuilding-libgcc -fno-stack-protector -fno-exceptions" fullword ascii

$s15 = "GNU C 4.8.1 -m64 -mtune=generic -march=x86-64 -g -O2 -std=gnu99" fullword ascii

$s16 = "GNU C 4.8.1 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuilding-libgcc -fno-stack-protector -fexceptions" fullword ascii

$s17 = "9lpszCommandLine" fullword ascii

$s18 = "=__mingw_GetSectionForAddress" fullword ascii

$s19 = "__mingw_winmain_lpCmdLine" fullword ascii

$s20 = "%Target" fullword ascii

condition:

uint16(0) == 0x5a4d and filesize < 3000KB and

pe.imphash() == "8f0088451a1156246379abc67514cacf" and pe.exports("CSBhvSWCvFRvfCfAoJdoFuAUmK") or 8 of them)

{ rule ryuk_1006_files_xxx}

meta:

description = "files - file xxx.exe"

author = "The DFIR Report"

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

date = "2020-10-13"

hash1 = "ccde47a0d315dcd4740fccfe8e8110fbb1fd85bb305734fec409f52051790c98"

strings:

$s1 = "DOOKOL.exe" fullword ascii

$s2 = "c:/crossdev/src/winpthreads-svn6233/src/mutex.c" fullword ascii

$s3 = "hmutex" fullword ascii

$s4 = "mutex_global_shmem" fullword ascii

$s5 = "processthreadsapi.h" fullword ascii

$s6 = "mutex_global_static_shmem" fullword ascii

$s7 = "fake_get_output_format" fullword ascii

$s8 = "&rvaTarget" fullword ascii

$s9 = "h:\\crossdev\\gccmaster\\build-tdm64\\runtime\\mingw-w64-crt" fullword ascii

$s10 = "c:\\crossdev\\gccmaster\\build-tdm64\\gcc\\x86_64-w64-mingw32\\32\\libgcc" fullword ascii

$s11 = "E__mingw_winmain_lpCmdLine" fullword ascii

$s12 = "GNU C 4.8.1 -m32 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuilding-libgcc -fno-stack-protector" fullword ascii

$s13 = "GNU C 4.8.1 -m32 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuilding-libgcc -fno-stack-protector -fno-exceptions" fullword ascii

$s14 = "GNU C 4.8.1 -m32 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuilding-libgcc -fno-stack-protector -fexceptions" fullword ascii

$s15 = "GNU C 4.8.1 -m32 -mtune=generic -march=x86-64 -g -O2 -std=gnu99" fullword ascii

$s16 = "__mingw_winmain_lpCmdLine" fullword ascii

$s17 = "Npthread_getspecific" fullword ascii

$s18 = "__gthread_getspecific" fullword ascii

$s19 = "=__mingw_GetSectionForAddress" fullword ascii

$s20 = "4lpszCommandLine" fullword ascii

condition:

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

(pe.imphash() == "00f3261b5b33a9b1e8b6003f4056a885" and pe.exports("CSBhvSWCvFRvfCfAoJdoFuAUmK") or 8 of them)

{ rule ryuk_1006_servisses}

meta:

description = "files - file servisses.exe"

author = "The DFIR Report"

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

date = "2020-10-13"

hash1 = "1d8b7faf5f290465cc742e07abca78fac419135b191071cc77912263cd1dde1d"

strings:

$s1 = "DOOKOL.exe" fullword ascii

$s2 = "c:/crossdev/src/winpthreads-svn6233/src/mutex.c" fullword ascii

$s3 = "mutex_global_shmem" fullword ascii

$s4 = "mutex_global_static_shmem" fullword ascii

$s5 = "_pthread_key_dest_shmem" fullword ascii

$s6 = "_pthread_key_max_shmem" fullword ascii

$s7 = "_pthread_key_sch_shmem" fullword ascii

$s8 = "_pthread_key_lock_shmem" fullword ascii

$s9 = "cannot find name of executable" fullword ascii

$s10 = "tiles32.png" fullword ascii

$s11 = "GetModuleFileName: %s" fullword ascii

$s12 = "IP_DEST_HOST_UNREACHABLE (11003)" fullword ascii

$s13 = "This program requires Windows NT!" fullword ascii

$s14 = "SNMP INVALID_SESSION" fullword ascii

$s15 = "SNMP TRAP_ERRORS" fullword ascii

$s16 = "SNMP SELECT_FDERRORS" fullword ascii

$s17 = "Some different radices: %d %x %o %#x %#o " fullword ascii

$s18 = "c:/crossdev/src/winpthreads-svn6233/src/rwlock.c" fullword ascii

$s19 = "_pthread_tls_shmem" fullword ascii

$s20 = "IP_DEST_PORT_UNREACHABLE (11005)" fullword ascii

condition:

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

)pe.imphash() == "a90d500745a1ce2417c01fecefbc2851" and pe.exports("KADWEGAFSTWUATQFFFFkxcEEF") or 8 of them(

{ rule ryuk_1006_files_SQL}

meta:

description = "files - file S

QL.dll"

author = "The DFIR Report"

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

date = "2020-10-13"

hash1 = "d67461ba45a4edf3b2a69b3e64303fda8130bd1fc7a1173f35c1fe67b40c9639"

strings:

$s1 = ".data$_ZN12_GLOBAL__N_110fake_mutexE" fullword ascii

$s2 = ".data$_ZZN12_GLOBAL__N_116get_static_mutexEvE4once" fullword ascii

$s3 = "DOOKOL.dll" fullword ascii

$s4 = "_ZN12_GLOBAL__N_110fake_mutexE" fullword ascii

$s5 = "_ZZN12_GLOBAL__N_116get_static_mutexEvE4once" fullword ascii

$s6 = ".data$_ZN12_GLOBAL__N_115emergency_mutexE" fullword ascii

$s7 = ".data$_ZN12_GLOBAL__N_1L12static_mutexE" fullword ascii

$s8 = "__shmem_winpthreads_grabber_mutex_global_shmem" fullword ascii

$s9 = "__shmem_winpthreads_init_mutex_global_shmem" fullword ascii

$s10 = "__shmem_winpthreads_ptr_mutex_global_shmem" fullword ascii

$s11 = "c:/crossdev/src/winpthreads-svn6233/src/mutex.c" fullword ascii

$s12 = "pthread_mutex_lock_intern" fullword ascii

$s13 = "__shmem_winpthreads_init_mutex_global_static_shmem" fullword ascii

$s14 = "__shmem_winpthreads_grabber_mutex_global_static_shmem" fullword ascii

$s15 = "__shmem_winpthreads_ptr_mutex_global_static_shmem" fullword ascii

$s16 = "_Z7ExecutePv" fullword ascii

$s17 = "hmutex" fullword ascii

$s18 = "._FindPESectionExec" fullword ascii

$s19 = "_ZN9__gnu_cxx17__recursive_mutex6unlockEv" fullword ascii

$s20 = ".text$_ZN9__gnu_cxx17__recursive_mutex6unlockEv" fullword ascii

condition:

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

)pe.imphash()=="d16819dafefb97404d0d0e42adb82e5c"and (

pe.exports("CSBhvSWCvFRvfCfAoJdoFuAUmK") and pe.exports("StartW")) or 8 of them(

{If you have detections you would like to add to this section, please contact us and we will credit you.

MITRE

Spearphishing Link – T1192

Remote Desktop Protocol – T1076

Remote File Copy – T1105

Windows Management Instrumentation – T1047

Command-Line Interface – T1059

Domain Trust Discovery – T1482

Remote System Discovery – T1018

System Time Discovery – T1124

Data Encrypted for Impact – T1486

Commonly Used Port – T1043

Standard Application Layer Protocol – T1071

Standard Cryptographic Protocol – T1032

User Execution – T1204

Valid Accounts – T1078

Exploitation for Privilege Escalation – T1068

Signed Binary Proxy Execution – T1218

Rundll32 – T1085

Regsvr32 – T1117

منبع:

https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/