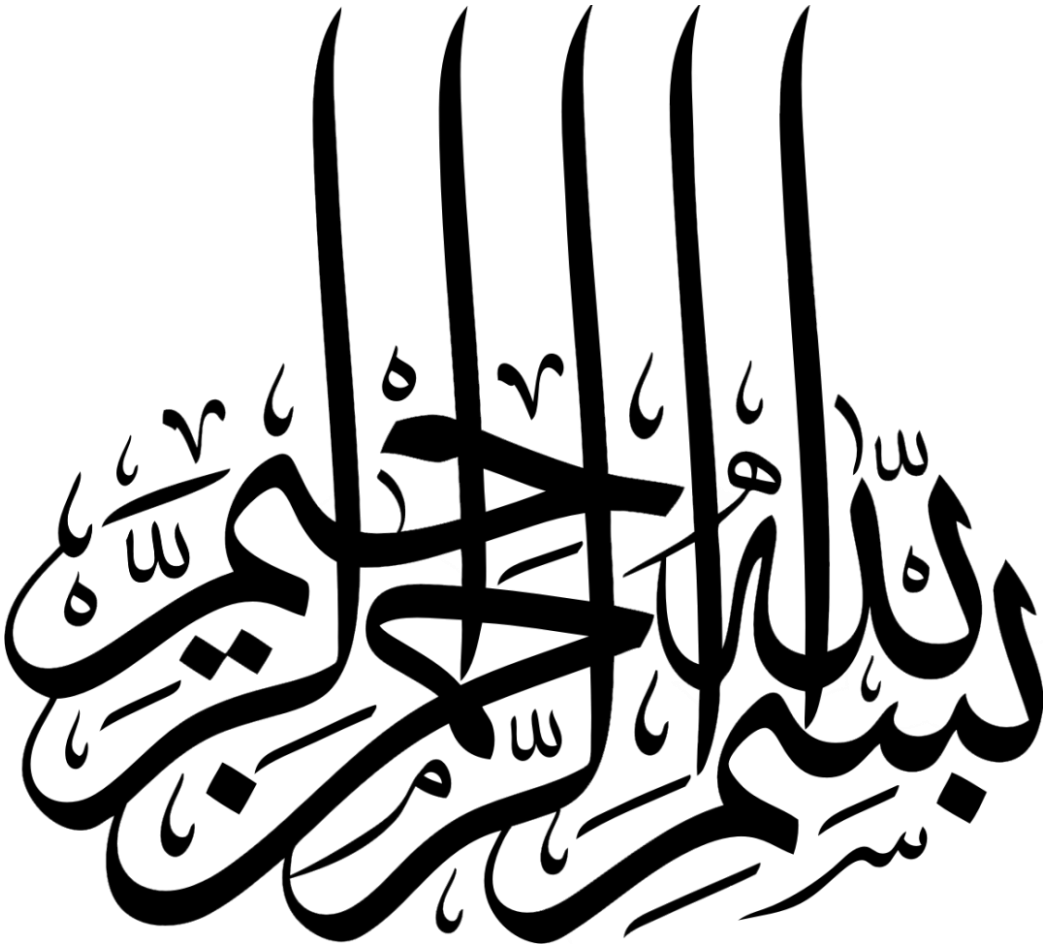

بسم الله الرحمن الرحیم

GoGoogle Ransomware

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

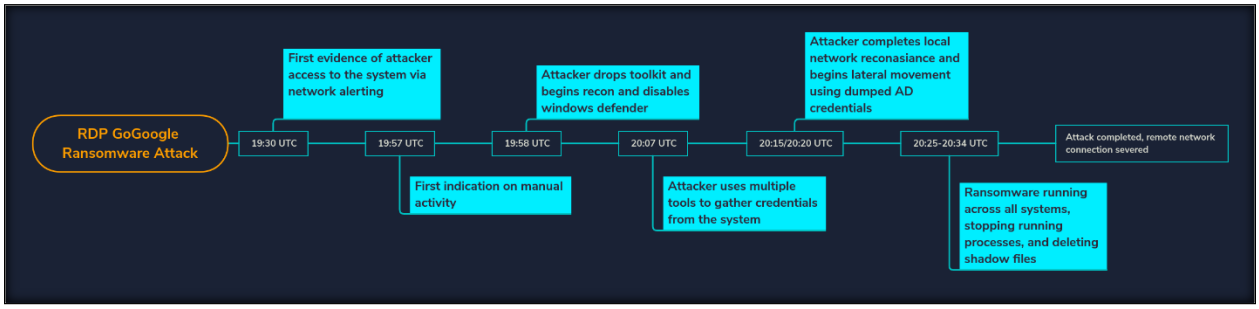
مقدمه

در سال‌های اخیر، باج‌افزارها به یکی از جدی‌ترین تهدیدهای امنیتی در سازمان‌ها تبدیل شده‌اند؛ حملاتی که اغلب نه با تکنیک‌های پیچیده، بلکه با سوءاستفاده از ضعف‌های رایج مثل دسترسی ناامن RDP، رمزهای عبور ضعیف و نبود نظارت کافی آغاز می‌شوند.

در این گزارش از The DFIR Report با یک سناریوی کلاسیک اما بسیار آموزنده از باج‌افزار GoGoogle روبه‌رو می‌شویم؛ حمله‌ای که از یک ورود نسبتاً ساده (از طریق RDP) آغاز می‌شود و در مدت کوتاهی به تسلط بر شبکه و در نهایت رمزگذاری گسترده فایل‌ها ختم می‌گردد. مهاجم پس از ورود، ابتدا با غیرفعال‌کردن ابزارهای امنیتی و رهاسازی مجموعه‌ای از ابزارها روی سیستم، مرحله‌ی شناسایی را شروع می‌کند و خیلی سریع سراغ سرقت/استخراج گذرواژه‌ها با ابزارهایی مثل Mimikatz، LaZagne و مجموعه ابزارهای NirSoft می‌رود. سپس با تکیه بر اطلاعات به‌دست‌آمده، حرکت جانبی را سرعت می‌دهد، روی سیستم‌های بیشتری حضور پیدا می‌کند و در نهایت روی Domain Controller متمرکز می‌شود تا روند استقرار باج‌افزار را کامل کند.

نکته‌ی مهم این پرونده، «نمایش زنجیره‌ی کامل حمله» از دید ردپاها و آرتیفکت‌هاست: از اسکریپت‌ها و فایل‌های رهاشده برای جمع‌آوری کلمات عبور تا نحوه‌ی شناسایی سیستم‌ها و حتی نشانه‌هایی مثل پاک‌سازی لاگ‌ها و توقف سرویس‌ها قبل از رمزگذاری. این متن ترجمه‌شده، علاوه بر روایت مرحله‌به‌مرحله‌ی رخداد، به شما کمک می‌کند بفهمید مهاجم چه چیزهایی را روی میزبان‌ها باقی می‌گذارد و تیم‌های دفاعی دقیقاً باید دنبال چه علائمی بگردند—خصوصاً در محیط‌هایی که RDP، ذخیره‌ی رمز در فایل‌های .rdp یا کنترل ضعیف روی حساب‌ها و دسترسی‌ها وجود دارد.

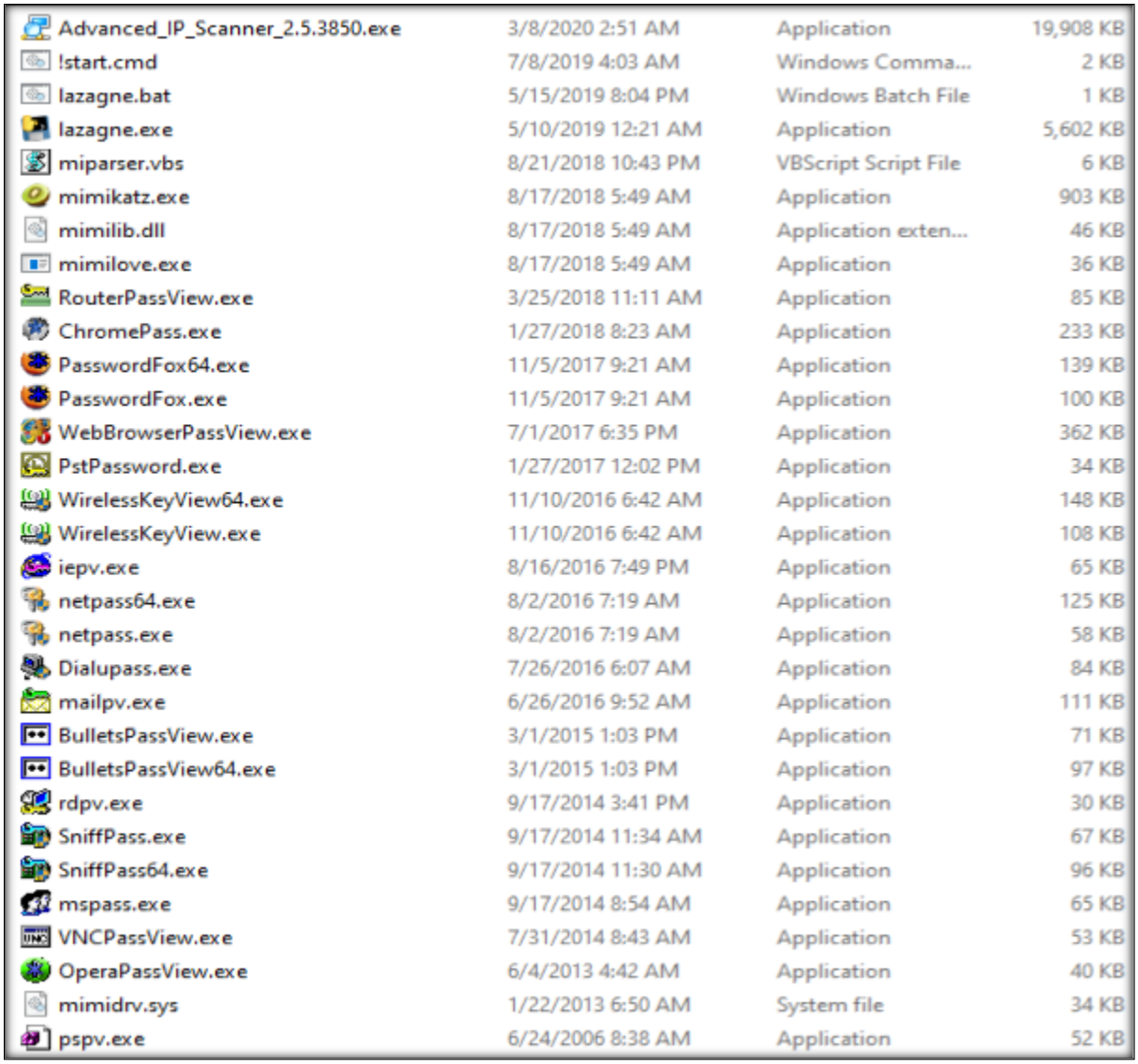
توضیحات اولیه



یک مهاجم از آدرس 93.174.95[.]73 وارد «هانی‌پات» شد، ابزارهای امنیتی را غیر فعال کرد، ابزارهای خودش را روی سیستم قرار داد و شروع به بررسی و شناسایی نمود. بعد از شناسایی، به سرعت از ابزارهایی برای دزدیدن رمز عبور مثل Mimikatz، Lazagne، rdpv و چند مورد دیگر استفاده کرد. پس از استخراج کلمات عبور، به کمک Network Port Scanner به چند سیستم دیگر دسترسی گرفته و کنترل آن‌ها را در دست گرفت. چند دقیقه بعد، مهاجم روی یک Domain Controller تمرکز کرد و شروع به اجرای باج‌افزار نمود.

نمونه های جالب

در طول این نفوذ، تعداد زیادی نمونه/ابزار (artifact) روی سیستم گذاشته شد. بیشتر این‌ها ابزارهای استخراج رمز عبور بودند، به جز !start.cmd و Advanced IP Scanner.



Advanced_IP_Scanner_2.5.3850.exe	3/8/2020 2:51 AM	Application	19,908 KB
!start.cmd	7/8/2019 4:03 AM	Windows Comma...	2 KB
lazagne.bat	5/15/2019 8:04 PM	Windows Batch File	1 KB
lazagne.exe	5/10/2019 12:21 AM	Application	5,602 KB
miparser.vbs	8/21/2018 10:43 PM	VBScript Script File	6 KB
mimikatz.exe	8/17/2018 5:49 AM	Application	903 KB
mimilib.dll	8/17/2018 5:49 AM	Application exten...	46 KB
mimilove.exe	8/17/2018 5:49 AM	Application	36 KB
RouterPassView.exe	3/25/2018 11:11 AM	Application	85 KB
ChromePass.exe	1/27/2018 8:23 AM	Application	233 KB
PasswordFox64.exe	11/5/2017 9:21 AM	Application	139 KB
PasswordFox.exe	11/5/2017 9:21 AM	Application	100 KB
WebBrowserPassView.exe	7/1/2017 6:35 PM	Application	362 KB
PstPassword.exe	1/27/2017 12:02 PM	Application	34 KB
WirelessKeyView64.exe	11/10/2016 6:42 AM	Application	148 KB
WirelessKeyView.exe	11/10/2016 6:42 AM	Application	108 KB
iepv.exe	8/16/2016 7:49 PM	Application	65 KB
netpass64.exe	8/2/2016 7:19 AM	Application	125 KB
netpass.exe	8/2/2016 7:19 AM	Application	58 KB
Dialupass.exe	7/26/2016 6:07 AM	Application	84 KB
mailpv.exe	6/26/2016 9:52 AM	Application	111 KB
BulletsPassView.exe	3/1/2015 1:03 PM	Application	71 KB
BulletsPassView64.exe	3/1/2015 1:03 PM	Application	97 KB
rdpv.exe	9/17/2014 3:41 PM	Application	30 KB
SniffPass.exe	9/17/2014 11:34 AM	Application	67 KB
SniffPass64.exe	9/17/2014 11:30 AM	Application	96 KB
mspass.exe	9/17/2014 8:54 AM	Application	65 KB
VNCPassView.exe	7/31/2014 8:43 AM	Application	53 KB
OperaPassView.exe	6/4/2013 4:42 AM	Application	40 KB
mimidrv.sys	1/22/2013 6:50 AM	System file	34 KB
pspv.exe	6/24/2006 8:38 AM	Application	52 KB

اسکریپت !start.cmd به نظر می‌رسد که از ابزارهای بالا برای برداشت رمزهای عبور از سیستم استفاده می‌کند. این اسکریپت طوری نوشته شده که هم سیستم‌های ۶۴ بیتی و هم ۳۲ بیتی را پشتیبانی کند، زیرا قبل از اجرای هر ابزار استخراج رمز، معماری پردازنده را بررسی می‌کند.

نیمه‌ی اول اسکریپت برنامه‌های زیر را اجرا می‌کند:

Mimikatz, Lazagne, BulletsPassView, netpass, PasswordFox, SniffPass, و WirelessKeyView.

نیمه‌ی دوم اسکریپت برنامه‌های زیر را اجرا می‌کند:

ChromePass, Dialupass, iepv, mailpv, mspass, OperaPassView, pspv, PstPassword, rdpv, RouterPassView, WebBrowserPassView و VNCPassView

و بعد از آن فایل‌های Mimikatz را حذف می‌کند.

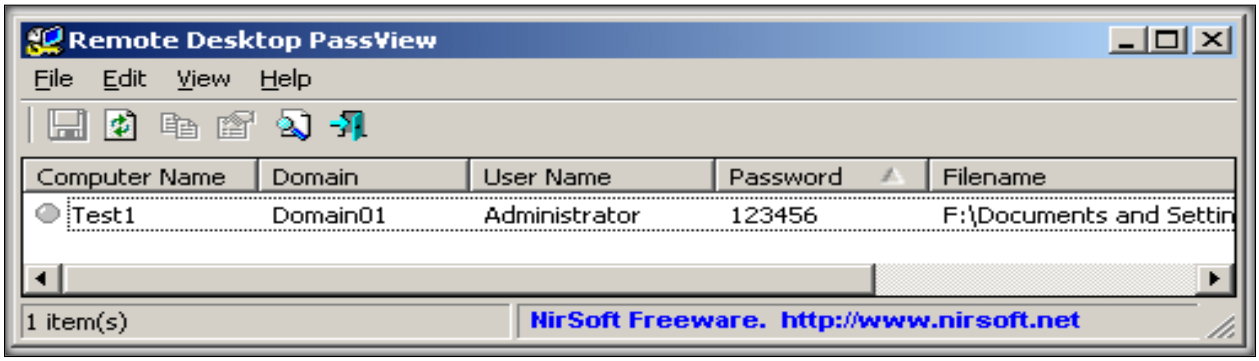
```
start .\passrecpk\ChromePass.exe
start .\passrecpk\Dialupass.exe
start .\passrecpk\iepv.exe
start .\passrecpk\mailpv.exe
start .\passrecpk\mspass.exe
start .\passrecpk\OperaPassView.exe
start .\passrecpk\pspv.exe
start .\passrecpk\PstPassword.exe
start .\passrecpk\rdpv.exe
start .\passrecpk\RouterPassView.exe
start .\passrecpk\VNCPassView.exe
start .\passrecpk\WebBrowserPassView.exe

REM del mimikatz.exe /F /Q
REM del mimidrv.sys /F /Q
REM del mimilib.dll /F /Q
REM del %0

REM @echo.
REM pause > nul
```

یک نکته که اینجا باید به آن توجه کرد، پوشه‌ای به نام passrecpk است. بعد از انجام کمی تحقیق بیشتر، ما معتقدیم این پوشه به احتمال زیاد مربوط به بسته ابزار رایگان NirSoft به نام passrecenc.zip است. بیشتر ابزارهای NirSoft که در بالا به آن‌ها اشاره شده است، داخل فایل passrecenc.zip قرار دارند.

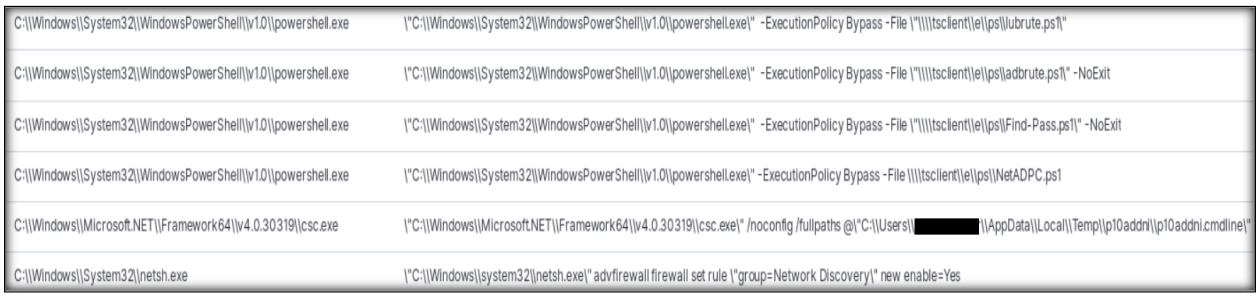
نمونه (artifact) بعدی یک Mimikatz parser است. هدف این اسکریپت این است که خروجی برنامه Mimikatz را پردازش و مرتب کند تا استفاده از رمزهای عبور یا NTLM برای مهاجم راحت‌تر شود. ما مشاهده کردیم که مهاجمان فایل Passwords.txt را باز کردند؛ فایلی که شامل نام کاربری و رمز عبور کاربران وارد شده به سیستم بود. این نمونه را می‌توان از اینجا دانلود کرد.

https://drive.google.com/file/d/1zr5-9WQB4K7LzioJbkoYv1PGUQXvPmn5/view?usp=sharing

یکی دیگر از نمونه‌های جالب، ابزار Remote Desktop PassView (rpv.exe) ساخته شرکت NirSoft است که رمزهای ذخیره‌شده در فایل‌های .rdp را نمایش می‌دهد. این یک مثال بسیار خوب است که نشان می‌دهد چرا نباید رمزهای عبور را داخل فایل‌های rdp ذخیره کنید.



مثالی از اسکریپت‌های PowerShell و سایر عناصر شناسایی و بررسی (recon) که اجرا شدند:



ما نتوانستیم این فایل‌ها را به دست بیاوریم، اما افکار و حدس‌های خودمان این‌هاست:

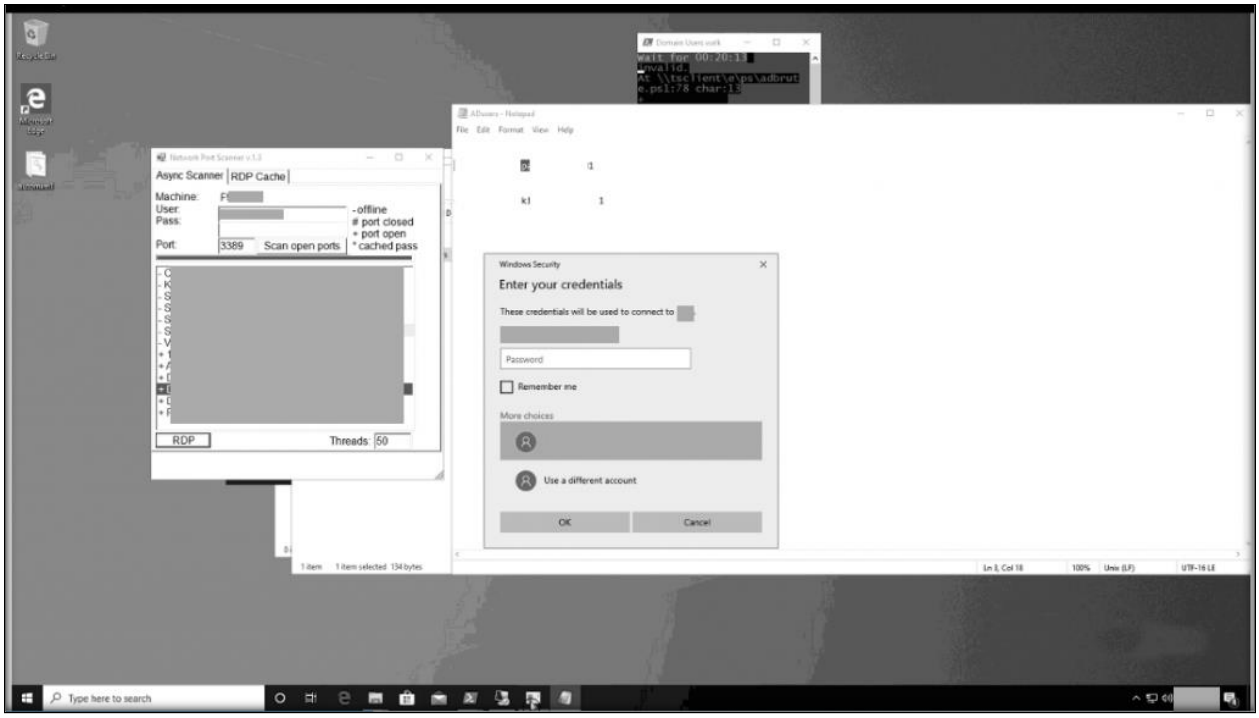
lubrute.ps1 – ما معتقدیم این اسکریپت برای حمله بروت فورس روی حساب‌های محلی (local accounts) استفاده شده است.

adbrute.ps1 – ما معتقدیم این اسکریپت برای حمله بروت فورس روی حساب‌های Active Directory (AD accounts) استفاده شده است.

Find-Pass.ps1 – ما معتقدیم این اسکریپت برای اجرای Mimikatz و سایر ابزارهای استخراج رمز عبور استفاده شده است.

NetADPC.ps1 – ما معتقدیم این اسکریپت Network Port Scanner را اجرا کرده و در اتصال‌های RDP کمک کرده است.

باج‌افزار به صورت دستی اجرا شد و نیاز داشت مهاجم با RDP به هر سیستمی که Network Port Scanner پیدا کرده بود وصل شود.



فایل اجرایی، خاص به نظر جدید می‌رسد و در حال حاضر توسط id-ransomware به عنوان GoGoogle شناسایی شده است.

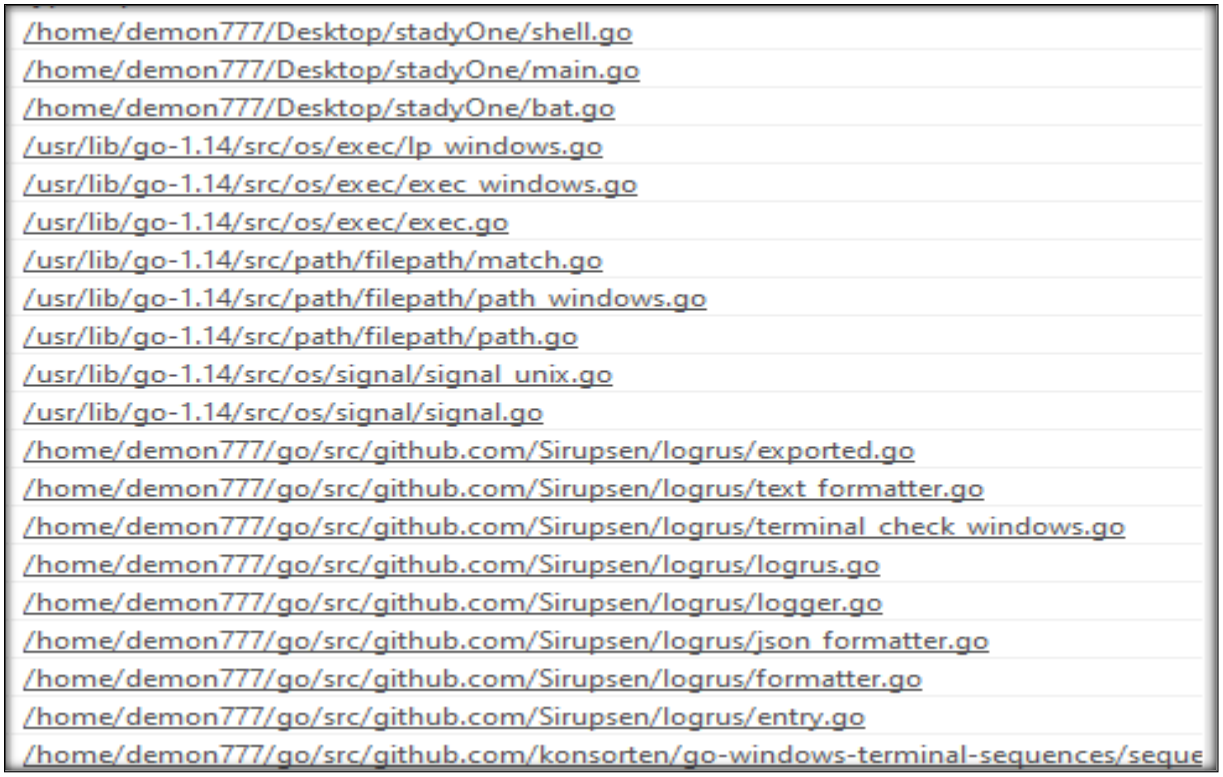
bild.exe|9330544a69b499f9b2ea79fd5a57bccc

a69b499f9b2ea79fd5a57bccc۹۳۳۰۵۴۴

cf9b71e0f8cf3068977c670499ed816e1b65ab۱۷

ce23c95a5049ca6d9678f419848b3ace3f1a0cdd36d3867d7d827ab5f4e8۸۸۰۵

با بررسی خود فایل باینری می‌توانیم ببینیم که بخش زیادی از کد با زبان Go نوشته شده و سازنده از نام demon777 استفاده کرده است.



قبل از اینکه باج‌افزار فایل‌ها را رمزگذاری کند، از ابزارهای مختلف ویندوز مانند WMI, taskkill, WEVTUTIL و net.exe استفاده می‌کند تا فرآیندها را متوقف کرده و لاگ‌ها را از سیستم پاک کند.

مثالی از لاگ‌هایی که پاک شدند:

C:\\Windows\\System32\\wevtutil.exe	WEVTUTIL CL \"Microsoft-Windows-EventLog-WMIProvider/Debug\"
C:\\Windows\\System32\\wevtutil.exe	WEVTUTIL CL \"Microsoft-Windows-WMI-Activity/Debug\"
C:\\Windows\\System32\\wevtutil.exe	WEVTUTIL CL \"Microsoft-Windows-WMI-Activity/Operational\"
C:\\Windows\\System32\\wevtutil.exe	WEVTUTIL CL \"Microsoft-Windows-WMI-Activity/Trace\"
C:\\Windows\\System32\\wevtutil.exe	WEVTUTIL CL \"SmbWmiAnalytic\"
C:\\Windows\\System32\\wevtutil.exe	wevtutil.exe cl \"Microsoft-Windows-EventLog-WMIProvider/Debug\"
C:\\Windows\\System32\\wevtutil.exe	wevtutil.exe cl \"Microsoft-Windows-WMI-Activity/Debug\"
C:\\Windows\\System32\\wevtutil.exe	wevtutil.exe cl \"Microsoft-Windows-WMI-Activity/Operational\"
C:\\Windows\\System32\\wevtutil.exe	wevtutil.exe cl \"Microsoft-Windows-WMI-Activity/Trace\"
C:\\Windows\\System32\\wevtutil.exe	wevtutil.exe cl \"SmbWmiAnalytic\"

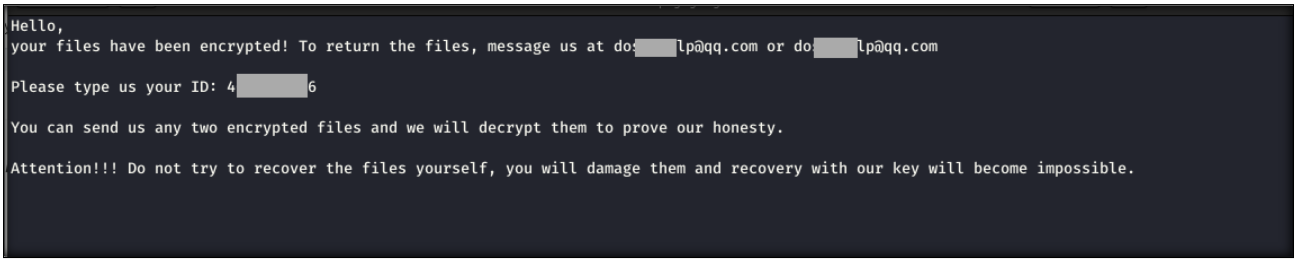
مثالی از فرآیندهایی که متوقف شدند:

C:\\Windows\\System32\\net1.exe	C:\\Windows\\system32\\net1 stop MSExchangePOP3BE
C:\\Windows\\System32\\net.exe	net stop MSExchangeRepl
C:\\Windows\\System32\\net1.exe	C:\\Windows\\system32\\net1 stop MSExchangeRepl
C:\\Windows\\System32\\net.exe	net stop MSExchangeRPC
C:\\Windows\\System32\\net1.exe	C:\\Windows\\system32\\net1 stop MSExchangeRPC
C:\\Windows\\System32\\net.exe	net stop MSExchangeServiceHost
C:\\Windows\\System32\\net1.exe	C:\\Windows\\system32\\net1 stop MSExchangeServiceHost
C:\\Windows\\System32\\net.exe	net stop MSExchangeSubmission
C:\\Windows\\System32\\net1.exe	C:\\Windows\\system32\\net1 stop MSExchangeSubmission
C:\\Windows\\System32\\net.exe	net stop MSExchangeThrottling
C:\\Windows\\System32\\net1.exe	C:\\Windows\\system32\\net1 stop MSExchangeThrottling
C:\\Windows\\System32\\net.exe	net stop MSExchangeTransport

در اینجا لیست طولانی‌ای از سرویس‌ها آورده شده که قبل از شروع فرآیند رمزگذاری باج‌افزار متوقف شدند:

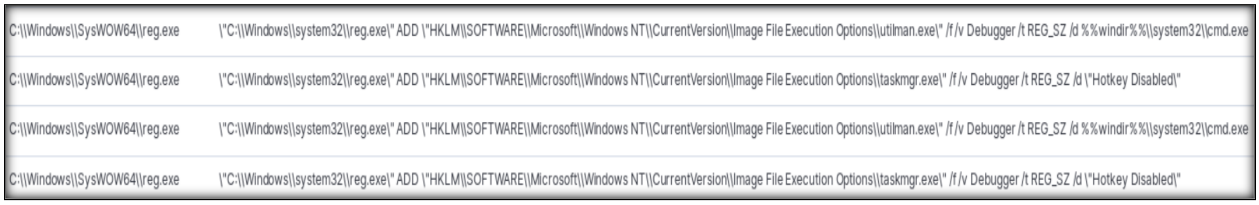
(سرویس‌ها:
AcronisActiveProtectionService,AcronisAgent,AcronisMonitoringService,AcronisZmqGw,AcrSch2Svc,Ado
(beActiveFileMonitor10.0,AdobeARMservice,AdobeFlashPlayerUpdateSvc,AdobeUpdateServi

یادداشت باج (Ransom Note) که باقی گذاشته شد، شامل یک ID بود و از یک آدرس ایمیل برای تماس با مهاجمان استفاده می‌کرد که سرویس qq.com بود.



تماس با مهاجم باج‌افزار برقرار شد و آن‌ها درخواست ۲ بیت‌کوین (حدود ۱۳،۴۰۰ دلار در زمان نوشتن گزارش) کردند. ممکن است این مبلغ برای هر دستگاهی که رمزگذاری شده بود باشد، اما آزمایشگاه تنها با یک یادداشت باج جمع‌آوری شده قبل از حذف شاخص‌ها (indicators) بازنشانی شد.

در حین گذاشتن یادداشت باج، به نظر می‌رسد که مهاجمان توانایی بازگشت در آینده را ایجاد کرده‌اند، اگر سیستم‌ها به‌طور کامل پاک نشوند، با استفاده از در پشتی Utilman.exe که امکان دسترسی به خط فرمان سیستم (cmd) در صفحه ورود را فراهم می‌کند.



خلاصه:

این مهاجمان خیلی سریع عمل کردند و توانستند از هیچ دسترسی تا نصب باج‌افزار روی ۵ دستگاه یا بیشتر را فقط در کمی بیش از یک ساعت انجام دهند.

تعداد زیادی نمونه/ابزار (artifacts) توسط این مهاجم گذاشته شد که بیشتر آن‌ها ابزارهای NirSoft بودند، اما مهاجمان چند اسکریپت مخصوص خودشان هم داشتند.

مهاجمان چند دستور اجرا کردند که ممکن است به راحتی قابل شناسایی باشد، مثل:

- فعال کردن کشف شبکه (network discovery)
- جایگزینی Utilman با cmd
- پاک کردن لاگ‌ها
- متوقف کردن تعداد زیادی سرویس مثل TeamViewer1

منبع:

https://thedfirreport.com/2020/04/04/gogoogle-ransomware/