بررسی فایل Agenda.ISO

نویسنده: ابوالفضل کاظمی

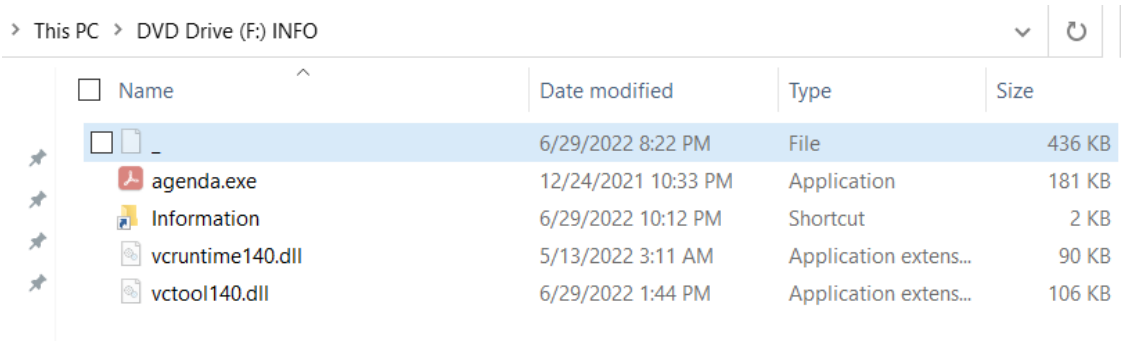
چندتا از تصاویر از گزارش PaloAlto گرفته شده‌اند.

نکته مهم: در تصاویر گزارش من ممکنه PIDهای مختلفی از یک پروسه ببینید. این مشکل به این دلیل رخ داد که ماشین مجازی تست خراب شد و مجبور به اجرای مجدد شدم! ولی علی رغم این ناهماهنگی، **ارتباط منطقی در گزارش و طرز کار بدافزار بوده** و از این بابت مشکلی نیست.

```
PS D:\> Get-FileHash .\Agenda.iso

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          347715F967DA5DEBFB01D3BA2EDE6922801C24988C8E6EA2541E370DED313C8B       D:\Agenda.iso
```

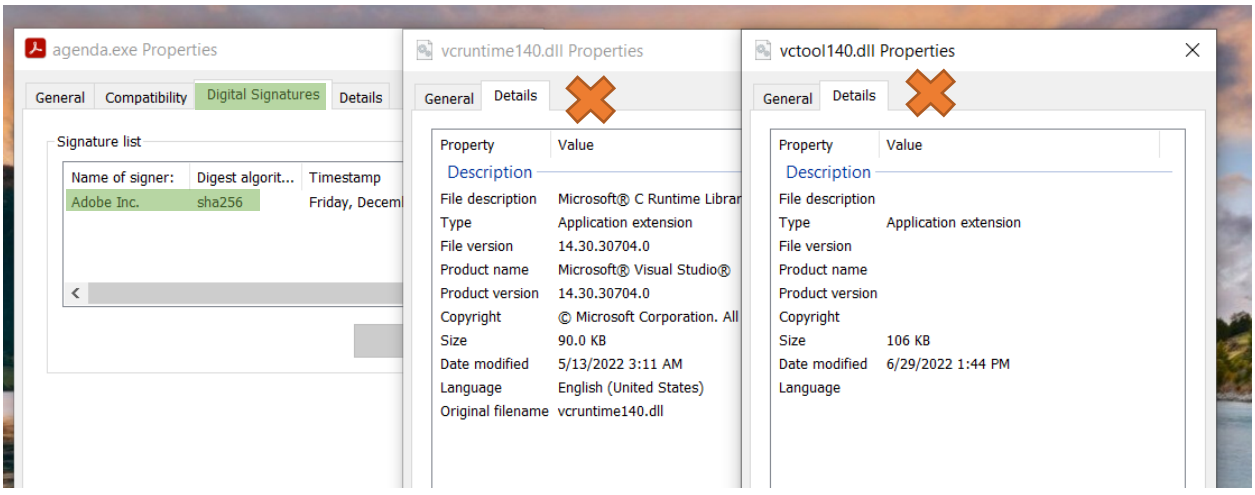
اجرای فایل ISO باعث mount شدن آن شده و فایل‌های زیر را نمایش می‌دهد که فقط فایل Information.lnk پیدا بوده و مابقی مخفی هستند.



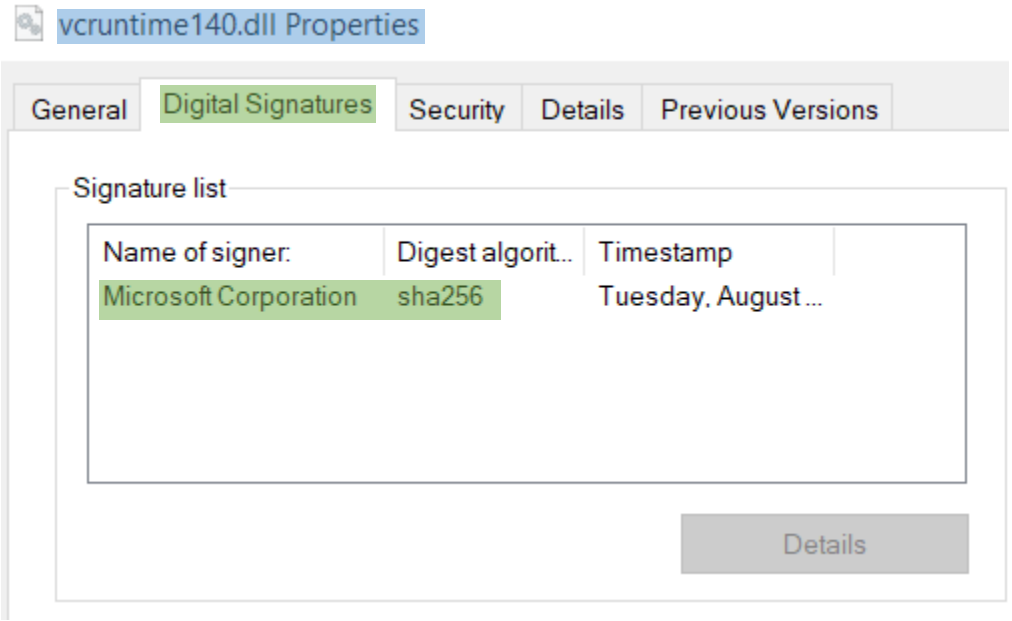
اگر Properties فایل lnk را ببینیم متوجه اجرای agenda.exe با دستور cmd.exe به صورت زیر می‌شویم:

```
%windir%/system32/cmd.exe /k start agenda.exe
```

اگر جزئیات فایل‌ها را مشاهده کنیم مشخص است که agenda.exe امضای رسمی Adobe را دارد ولی دو فایل DLL کنار آن امضای معتبری نداشته و vcruntime140.dll که مربوط به C++ Runtime است فقط جزئیاتی دارد که به نظر برسد فایل معتبری است و هدف آن انجام دادن DLL-Proxy می‌باشد.



برای اطمینان از اینکه vcruntime140.dll یک فایل معتبر مایکروسافت است می‌توانیم آنرا از C:\Windows\System32 باز کرده و امضای فایل را چک کنیم (این فایل با نصب کردن Visual C++ Redistributable For Visual Studio 2015 ایجاد می‌شود)



در مقاله‌ی ارائه شده توسط PaloAlto جزئیات فایل‌های داخل ISO به صورت زیر ارائه شده است:

File Name	SHA-256	Description
_	09F0EA9B239385EB22F794DCECAEC1273BE87F3F118A2DA067551778971CA677	File name is underscore. This is a compressed file (MSZIP) that is loaded by vctool140.dll
Information.lnk	32E1EEBF2AF8D36857B3A9EA3A2653E8E7AD6B6EAB8CA4665B252B5FB609D993	Windows shortcut file.
agenda.exe	E8E63F7CF6C25FB3B93AA55D5745393A34E2A98C5AEACBC42F1362DDF64EB0DA	Digitally Signed file by Adobe, Inc.
vcruntime140.dll	A018F4D5245FD775A17DC8437AD55C2F74FB6152DD4FDF16709A60DF2A063FFF	DLL loaded by agenda.exe
vctool140.dll	9230457E7B1AB614F0306E4AAAF08F1F79C11F897F635230AA4149CCFD090A3D	Actors DLL used to decompress and in-memory load payload

اگر فایل vcruntime140.dll موجود در فایل ISO آلوده را در PEBear باز کنیم مشاهده می‌کنیم که در بخش Import یک فایل dll اضافه نسبت به فایل اصلی دارد که همان vctool140.dll بوده و یک تابع از آن استفاده شده است.

Disasm | General | DOS Hdr | Rich Hdr | File Hdr | Optional Hdr | Section Hdrs | Exports | Imports | Resources | Exception | Security

فایل مخرب

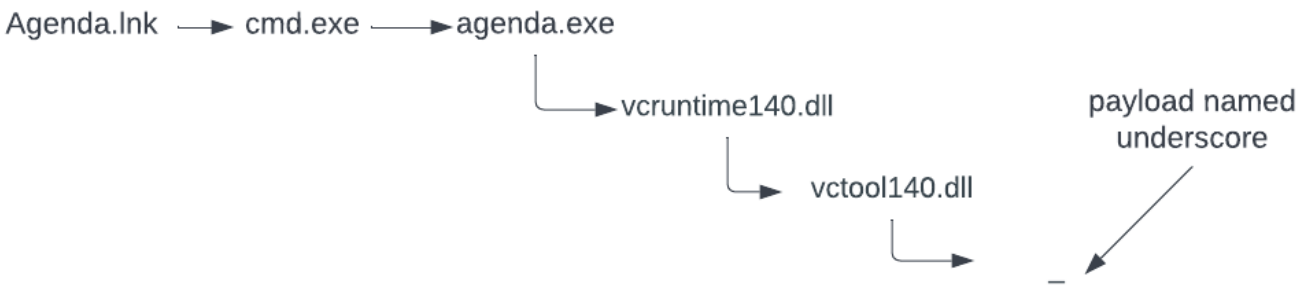
Offset	Name	Func. Count	Bound?	OriginalFirstThunk	TimeDateStamp	Forwarder	NameRVA	FirstThunk
16600	api-ms-win-crt-runtime-l1-1-0.dll	2	FALSE	14D28	0	0	14DE4	11148
16614	api-ms-win-crt-heap-l1-1-0.dll	3	FALSE	14D08	0	0	14E06	11128
16628	api-ms-win-crt-string-l1-1-0.dll	3	FALSE	14D50	0	0	14E26	11170
1663C	api-ms-win-crt-stdio-l1-1-0.dll	1	FALSE	14D40	0	0	14E48	11160
16650	api-ms-win-crt-convert-l1-1-0.dll	1	FALSE	14CF8	0	0	14E68	11118
16664	KERNEL32.dll	34	FALSE	14BE0	0	0	1514C	11000
16678	vctool140.dll	1	FALSE	1B0CD	0	0	1B0A0	1B0BD

Disasm | General | DOS Hdr | Rich Hdr | File Hdr | Optional Hdr | Section Hdrs | Exports | Imports | Resources | Exception | Security

فایل اصلی

Offset	Name	Func. Count	Bound?	OriginalFirstThunk	TimeDateStamp	Forwarder	NameRVA	FirstThunk
138E4	api-ms-win-crt-runtime-l1-1-0.dll	2	FALSE	14CB8	0	0	14D74	11148
138F8	api-ms-win-crt-heap-l1-1-0.dll	3	FALSE	14C98	0	0	14D96	11128
1390C	api-ms-win-crt-string-l1-1-0.dll	3	FALSE	14CE0	0	0	14DB6	11170
13920	api-ms-win-crt-stdio-l1-1-0.dll	1	FALSE	14CD0	0	0	14DD8	11160
13934	api-ms-win-crt-convert-l1-1-0.dll	1	FALSE	14C88	0	0	14DF8	11118
13948	KERNEL32.dll	34	FALSE	14B70	0	0	150DC	11000

تا الان مشخص است که به ترتیب cmd باعث اجرا شدن agenda.exe شده و سپس فایل vcruntime140.dll بارگذاری شده و از طریق آن فایل vctool140.dll بارگذاری می‌شود. از این تحلیل اینکه فایل _ چیست و چطور بارگذاری می‌شود مشخص نیست ولی احتمالا توسط vctool140.dll بارگذاری می‌شود. در مستند تحلیل PaloAlto تصویر زیر برای ترتیب اجرا مشخص شده است که در ادامه دقیق‌تر بررسی می‌کنیم.



من فایل را اجرا کرده و با Process Monitor رویدادهای زیر را Capture کردم:

Process Name	PID	Operation	Path	Result	Detail
agenda.exe	496	Process Start		SUCCESS	Parent PID: 4496, Command line: agenda.exe , Current directory: F:\, ...
agenda.exe	496	QueryDirectory	F:*	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: *, 2: _
agenda.exe	496	QueryDirectory	F:\	SUCCESS	FileInformationClass: FileBothDirectoryInformation, 1: agenda.exe, 2: ...
agenda.exe	496	Load Image	F:\vcruntime140.dll	SUCCESS	Image Base: 0x7ffee6da0000, Image Size: 0x1c000
agenda.exe	496	Load Image	F:\vctool140.dll	SUCCESS	Image Base: 0x7ffedc820000, Image Size: 0x1f000
agenda.exe	496	Thread Create		SUCCESS	Thread ID: 3928
agenda.exe	496	Thread Create		SUCCESS	Thread ID: 8708
agenda.exe	496	ReadFile	F:_	SUCCESS	Offset: 0, Length: 446,179, Priority: Normal
agenda.exe	496	Thread Create		SUCCESS	Thread ID: 6048
agenda.exe	496	Thread Create		SUCCESS	Thread ID: 9372
agenda.exe	496	Load Image	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2205.7-0\MpOAV.dll	SUCCESS	Image Base: 0x7ffee2380000, Image Size: 0x7b000
agenda.exe	496	Load Image	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2205.7-0\MpClient.dll	SUCCESS	Image Base: 0x7ffee3cd0000, Image Size: 0x12d000
agenda.exe	496	CreateFile	C:\Users\Abolfazl\AppData\Roaming	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open R...
agenda.exe	496	CreateFile	F:\agenda.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sequenti...
agenda.exe	496	CreateFile	C:\Users\Abolfazl\AppData\Roaming\agenda.exe	SUCCESS	Desired Access: Generic Read/Write, Delete, Write DAC, Disposition...
agenda.exe	496	CreateFile	F:_	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sequenti...
agenda.exe	496	CreateFile	C:\Users\Abolfazl\AppData\Roaming_	SUCCESS	Desired Access: Generic Read/Write, Delete, Write DAC, Disposition...
agenda.exe	496	CreateFile	F:\vcruntime140.dll	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sequenti...
agenda.exe	496	CreateFile	C:\Users\Abolfazl\AppData\Roaming\vcruntime140.dll	SUCCESS	Desired Access: Generic Read/Write, Delete, Write DAC, Disposition...
agenda.exe	496	QueryEaInformationFile	F:\vctool140.dll	SUCCESS	EaSize: 0
agenda.exe	496	CreateFile	C:\Users\Abolfazl\AppData\Roaming\vctool140.dll	SUCCESS	Desired Access: Generic Read/Write, Delete, Write DAC, Disposition...
agenda.exe	496	ReadFile	C:\Users\Abolfazl\NTUSER.DAT	SUCCESS	Offset: 909,312, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Sy...
agenda.exe	496	TCP Connect	DESKTOP-3B7EU10.localdomain:49749 -> fra16s50-in-f10.1e100.net:https	SUCCESS	Length: 0, mss: 1460, sackopt: 0, tsopt: 0, wsopt: 0, rcvwin: 64240, rcvw...
agenda.exe	496	Thread Create		SUCCESS	Thread ID: 7516
agenda.exe	496	TCP Send	DESKTOP-3B7EU10.localdomain:49749 -> fra16s50-in-f10.1e100.net:https	SUCCESS	Length: 125, startime: 629302, endtime: 629302, seqnum: 0, connid: 0
agenda.exe	496	TCP Receive	DESKTOP-3B7EU10.localdomain:49749 -> fra16s50-in-f10.1e100.net:https	SUCCESS	Length: 5, seqnum: 0, connid: 0
agenda.exe	496	Process Exit		SUCCESS	Exit Status: 1, User Time: 0.2343750 seconds, Kernel Time: 0.2187500...
agenda.exe	496	TCP Disconnect	DESKTOP-3B7EU10.localdomain:49749 -> fra16s50-in-f10.1e100.net:https	SUCCESS	Length: 0, seqnum: 0, connid: 0

از این خلاصه‌ی اجرا موارد زیر مشخص است:

- فایل agenda.exe پس از اجرا ماژول‌های dll کنار خود را بارگذاری کرده، یکسری نخ ایجاد می‌کند.
- در پروسه‌ی اجرا شده درایو ISO برای یک فایل به اسم _ جستجو می‌شود.
- فولدر C:\Users\[USERNAME]\AppData\Raoming مورد دسترسی قرار گرفته شده و 4 فایل موجود در ISO در آن کپی می‌شوند.
- اطلاعات کاربر از جمله NTUSER.DAT که برای پروفایل کاربران در ویندوز است خوانده می‌شود.
- ارتباط شبکه‌ای TLS با آدرس fra16s50-in-f10.1e100.net برقرار شده و داده‌هایی ارسال و دریافت می‌شود.

من برای کمتر بودند رویدادها، **رویدادهای رجیستری** را غیرفعال کردم. با فعال کردن آن موارد زیر دیده می‌شود که در تصویر صفحه‌ی بعد مشخص است:

- پس از باز کردن فایل _ یکسری کلید در مورد NetFramework. مورد دسترسی قرار گرفته‌اند و لود شدن یکسری DLL مرتبط با آن دیده می‌شود که این احتمال را می‌دهد که فایل _ یک باینری Net.ای است.
- به یکسری فایل و کلید رجیستری در مورد AMSI, Defender دسترسی انجام گرفته که احتمالا برای بحث Evasion است.
- مسیر برنامه پس از کپی شدن در Roaming در کلید Run رجیستری با نام AgendaE قرار گرفته است که در هر بار reboot ویندوز مجدد اجرا شود.
- اطلاعات شبکه از طریق رجیستری خوانده شده است که احتمالا به همراه اطلاعات کاربر جمع‌آوری و ارسال شود.
- به کتابخانه‌های Cryptography ویندوز دسترسی انجام گرفته است که شاید برای ارتباط با سرور و Encrypt کردن داده‌های جمع‌آوری شده از آن‌ها استفاده شود.
- برنامه تلاش کرده است که Tracing را برای خودش غیر فعال کند.

تصویر زیر خلاصه‌ی رویدادهای مرتبط با رجیستری را نمایش می‌دهد:

Operation	Path	Detail
Process Start		Parent PID: 1500, Command line: agenda.exe , Current directory: F:\, Environment: =::=::\=F:=F:\...
Load Image	F:\agenda.exe	Image Base: 0x7ff69c4c0000, Image Size: 0x30000
ReadFile	F:_	Offset: 0, Length: 446,179, Priority: Normal
RegOpenKey	HKLM\Software\Microsoft\.NETFramework\Policy\	Desired Access: Read
RegOpenKey	HKLM\Software\Microsoft\.NETFramework	Desired Access: Read
RegCloseKey	HKLM\SOFTWARE\Microsoft\AMSI	
CreateFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2205.7-0\MpOAV.dll	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Dir...
CreateFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2205.7-0\MpClient.dll	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n...
RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows Defender	Desired Access: Query Value
RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Desired Access: Read/Write
RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AgendaE	Type: REG_SZ, Length: 94, Data: "C:\Users\Abolfazl\AppData\Roaming\agenda.exe"
ReadFile	C:\Users\Abolfazl\NTUSER.DAT	Offset: 897,024, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Pri...
RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	
RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList	Desired Access: Read
RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 024	Desired Access: Read
RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 024\Name	Type: REG_SZ, Length: 108, Data: Microsoft Enhanced RSA and AES Cryptographic Provider
RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced RSA and AES Cryptographic Provider	Desired Access: Read
RegOpenKey	HKLM\Software\Policies\Microsoft\Cryptography	Desired Access: Read
RegOpenKey	HKLM\Software\Microsoft\Cryptography	Desired Access: Read
RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid	Type: REG_SZ, Length: 74, Data: a0ddd2b1-0516-482a-ad3f-58b1db471b87
RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces	Desired Access: Read
RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Hostname	Type: REG_SZ, Length: 32, Data: DESKTOP-3B7EU10
RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{a5ed5c9d-6b04-4c53-9ceb-2d3de85db98e}\Dh...	Type: REG_SZ, Length: 28, Data: 192.168.126.2
RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Hostname	Type: REG_SZ, Length: 32, Data: DESKTOP-3B7EU10
RegCreateKey	HKLM\Software\Microsoft\Tracing\agenda_RASAPI32	Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY
RegOpenKey	HKLM\Software\Microsoft\Tracing	Desired Access: Read
RegSetValue	HKLM\SOFTWARE\Microsoft\Tracing\agenda_RASAPI32\EnableFileTracing	Type: REG_DWORD, Length: 4, Data: 0
RegSetValue	HKLM\SOFTWARE\Microsoft\Tracing\agenda_RASAPI32\EnableConsoleTracing	Type: REG_DWORD, Length: 4, Data: 0
RegSetValue	HKLM\SOFTWARE\Microsoft\Tracing\agenda_RASAPI32\ConsoleTracingMask	Type: REG_DWORD, Length: 4, Data: 4294901760
RegSetValue	HKLM\SOFTWARE\Microsoft\Tracing\agenda_RASAPI32\MaxFileSize	Type: REG_DWORD, Length: 4, Data: 1048576
RegSetValue	HKLM\SOFTWARE\Microsoft\Tracing\agenda_RASAPI32\FileDirectory	Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\tracing
RegCreateKey	HKLM\Software\Microsoft\Tracing	Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY

و اما برسیم به بررسی لاگ‌های ثبت شده توسط Sysmon و اینکه از این لاگ‌ها چه چیزهایی می‌توان متوجه شد. کار را با ایجاد پروسه و بارگذاری فایل‌های DLL شروع کرده و سپس ادامه می‌دهیم.

۱. در اولین قدم پروسه‌ی cmd.exe اجرا شده و agenda.exe را اجرا می‌کند:

```
Process Create:
RuleName: -
UtcTime: 2022-07-27 06:52:29.928
ProcessGuid: {a0ddd2b1-e0ad-62e0-5802-000000001700}
ProcessId: 4496
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.19041.1 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "C:\Windows\system32\cmd.exe" /k start agenda.exe
CurrentDirectory: F:\
User: DESKTOP-3B7EU10\Abolfazl
LogonGuid: {a0ddd2b1-c831-62e0-c332-070000000000}
LogonId: 0x732C3
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA256=1B041F4DEEFB7A3D0DDC0CBE6FFCA70AE9C1FF88CBBD09F26492886DE649ACFD
ParentProcessGuid: {a0ddd2b1-c833-62e0-8800-000000001700}
ParentProcessId: 5272
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
ParentUser: DESKTOP-3B7EU10\Abolfazl
```

```
Process Create:
RuleName: -
UtcTime: 2022-07-27 06:52:30.149
ProcessGuid: {a0ddd2b1-e0ae-62e0-5a02-000000001700}
ProcessId: 496
Image: F:\agenda.exe
FileVersion: 21.11.20039.0
Description: Adobe Create PDF plug-in listener for Chrome
Product: Adobe Create PDF
Company: Adobe Systems Inc.
OriginalFileName: WCChromeNativeMessagingHost.exe
CommandLine: agenda.exe
CurrentDirectory: F:\
User: DESKTOP-3B7EU10\Abolfazl
LogonGuid: {a0ddd2b1-c831-62e0-c332-070000000000}
LogonId: 0x732C3
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA256=E8E63F7CF6C25FB3B93AA55D5745393A34E2A98C5AEACBC42F1362DDF64EB0DA
ParentProcessGuid: {a0ddd2b1-e0ad-62e0-5802-000000001700}
ParentProcessId: 4496
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe" /k start agenda.exe
ParentUser: DESKTOP-3B7EU10\Abolfazl
```

۲. پس از اجرا شدن **agenda.exe** فایل‌های **DLL** بارگذاری می شوند:

```
Image loaded:
RuleName: -
UtcTime: 2022-07-27 06:52:30.332
ProcessGuid: {a0ddd2b1-e0ae-62e0-5a02-000000001700}
ProcessId: 496
Image: F:\agenda.exe
ImageLoaded: F:\vcruntime140.dll
FileVersion: 14.30.30704.0 built by: vcwrkspc
Description: Microsoft® C Runtime Library
Product: Microsoft® Visual Studio®
Company: Microsoft Corporation
OriginalFileName: vcruntime140.dll
Hashes: SHA256=A018F4D5245FD775A17DC8437AD55C2F74FB6152DD4FDF16709A60DF2A063FFF
Signed: false
Signature: -
SignatureStatus: Unavailable
User: DESKTOP-3B7EU10\Abolfazl


Image loaded:
RuleName: -
UtcTime: 2022-07-27 06:52:30.332
ProcessGuid: {a0ddd2b1-e0ae-62e0-5a02-000000001700}
ProcessId: 496
Image: F:\agenda.exe
ImageLoaded: F:\vctool140.dll
FileVersion: -
Description: -
Product: -
Company: -
OriginalFileName: -
Hashes: SHA256=9230457E7B1AB614F0306E4AAAF08F1F79C11F897F635230AA4149CCFD090A3D
Signed: false
Signature: -
SignatureStatus: Unavailable
User: DESKTOP-3B7EU10\Abolfazl
```

۳. پس از این مراحل کپی شدن فایل‌ها در مسیر **Roaming** کاربر جاری مشاهده می شود:

```
File created:
RuleName: -
UtcTime: 2022-07-27 06:52:30.534
ProcessGuid: {a0ddd2b1-e0ae-62e0-5a02-000000001700}
ProcessId: 496
Image: F:\agenda.exe
TargetFilename: C:\Users\Abolfazl\AppData\Roaming\agenda.exe
CreationUtcTime: 2022-07-27 06:52:30.534
User: DESKTOP-3B7EU10\Abolfazl

File created:
RuleName: -
UtcTime: 2022-07-27 06:52:30.550
ProcessGuid: {a0ddd2b1-e0ae-62e0-5a02-000000001700}
ProcessId: 496
Image: F:\agenda.exe
TargetFilename: C:\Users\Abolfazl\AppData\Roaming\_
CreationUtcTime: 2022-07-27 06:52:30.550
User: DESKTOP-3B7EU10\Abolfazl

File created:
RuleName: -
UtcTime: 2022-07-27 06:52:30.550
ProcessGuid: {a0ddd2b1-e0ae-62e0-5a02-000000001700}
ProcessId: 496
Image: F:\agenda.exe
TargetFilename: C:\Users\Abolfazl\AppData\Roaming\vcruntime140.dll
CreationUtcTime: 2022-07-27 06:52:30.550
User: DESKTOP-3B7EU10\Abolfazl

File created:
RuleName: -
UtcTime: 2022-07-27 06:52:30.550
ProcessGuid: {a0ddd2b1-e0ae-62e0-5a02-000000001700}
ProcessId: 496
Image: F:\agenda.exe
TargetFilename: C:\Users\Abolfazl\AppData\Roaming\vctool140.dll
CreationUtcTime: 2022-07-27 06:52:30.550
User: DESKTOP-3B7EU10\Abolfazl
```

۴. سپس فایل **agenda.exe** در مسیر **Run** رجیستری قرار می‌گیرد که در هر بار **reboot** مجدد اجرا شود:

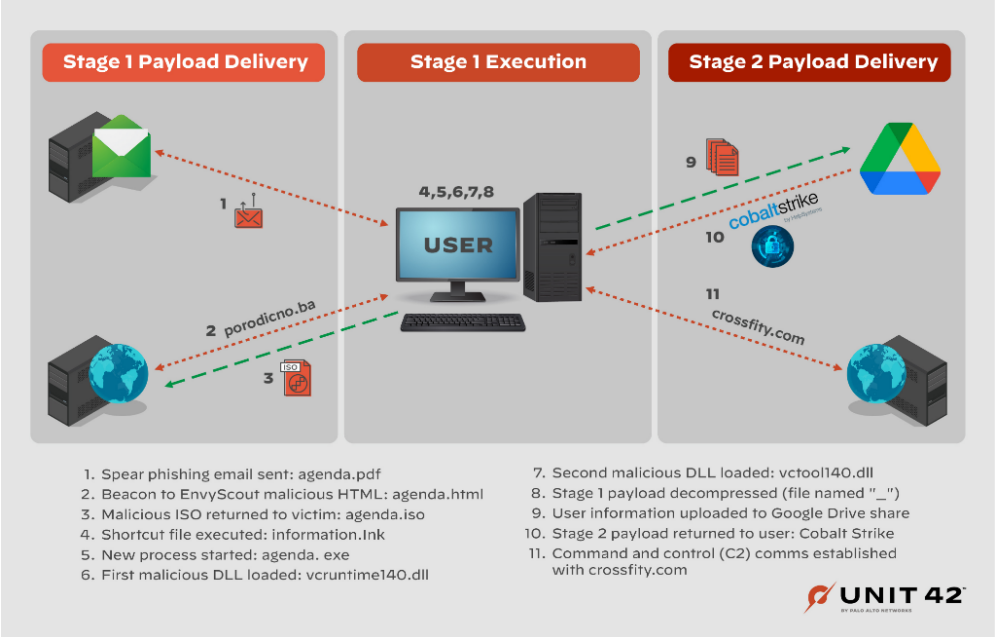
```
Registry value set:
RuleName: -
EventType: SetValue
UtcTime: 2022-07-27 06:52:30.550
ProcessGuid: {a0ddd2b1-e0ae-62e0-5a02-000000001700}
ProcessId: 496
Image: F:\agenda.exe
TargetObject: HKU\S-1-5-21-3588128041-3985369634-1347814394-
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AgendaE
Details: "C:\Users\Abolfazl\AppData\Roaming\agenda.exe"
User: DESKTOP-3B7EU10\Abolfazl
```

۵. در گزارش PaloAlto ذکر شده بود که داده‌های جمع‌آوری شده به GoogleDrive ارسال می‌شوند که در لاگ زیر دسترسی DNSای به api گوگل و ارتباط شبکه‌ای با آن مشاهده می‌شود.

```
Dns query:
RuleName: -
UtcTime: 2022-07-27 06:52:31.063
ProcessGuid: {a0ddd2b1-e0ae-62e0-5a02-000000001700}
ProcessId: 496
QueryName: oauth2.googleapis.com
QueryStatus: 0
QueryResults: ::ffff:142.250.185.138;
Image: F:\agenda.exe
User: DESKTOP-3B7EU10\Abolfazl


Network connection detected:
RuleName: -
UtcTime: 2022-07-27 06:52:31.167
ProcessGuid: {a0ddd2b1-e0ae-62e0-5a02-000000001700}
ProcessId: 496
Image: F:\agenda.exe
User: DESKTOP-3B7EU10\Abolfazl
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.126.130
SourceHostname: DESKTOP-3B7EU10.localdomain
SourcePort: 49749
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 142.250.185.138
DestinationHostname: -
DestinationPort: 443
DestinationPortName: https
```

تصویر زیر از مستند PaloAlto خلاصه‌ی تمامی مراحل اجرا را در بر دارد:



Read More:

https://cluster25.io/2022/05/13/cozy-smuggled-into-the-box/