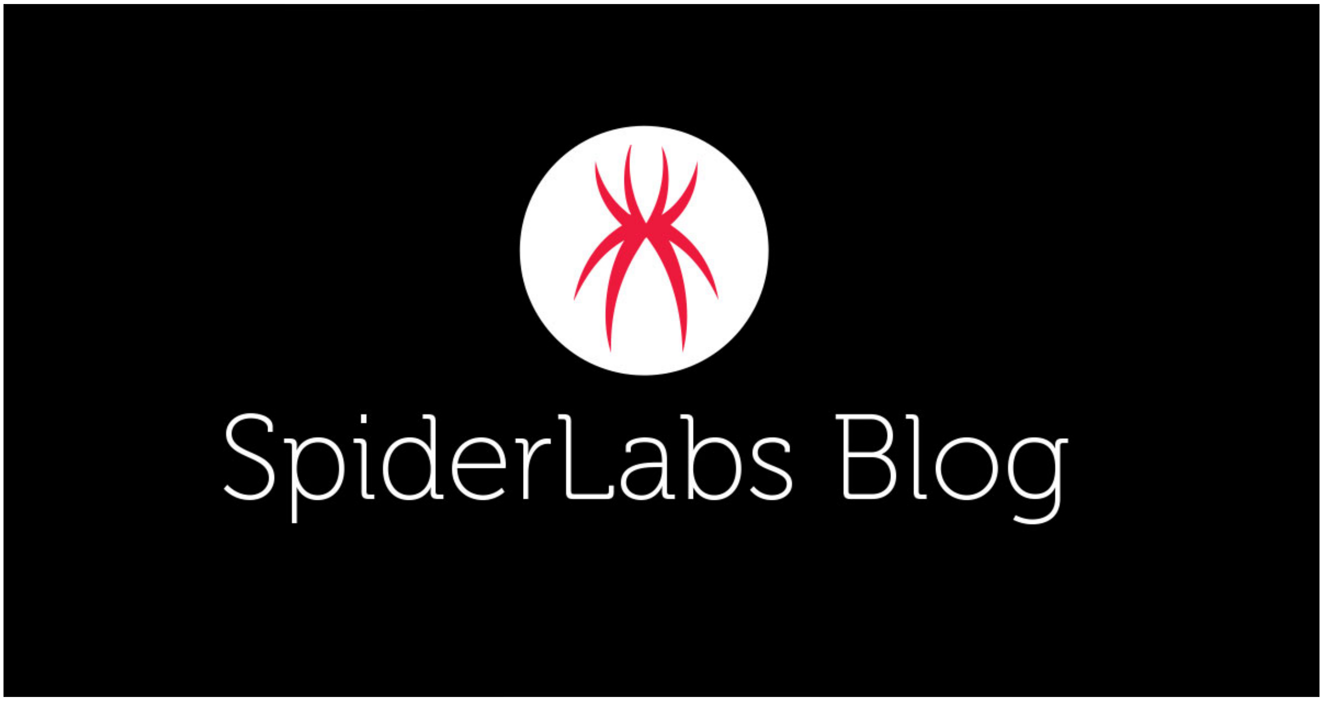
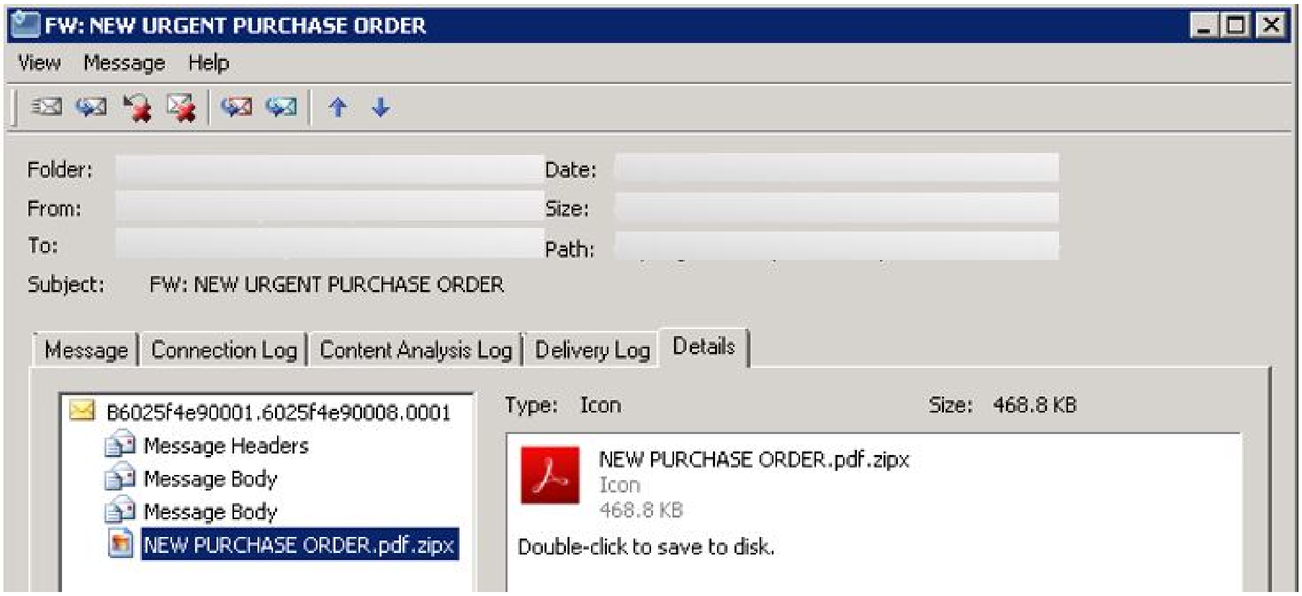
Image File Trickery Part II: Fake Icon Delivers NanoCore

trustwave.com/en-us/resources/blogs/spiderlabs-blog/image-file-trickery-part-ii-fake-icon-delivers-nanocore/



The *.zipx* file extension is used to denote that the ZIP archive format is compressed using advanced methods of the WinZip archiver. In 2019, we published a blog about this file extension being abused to deliver Lokibot malware. In this blog, we outline another *.zipx* attachment we recently encountered with spam messages, and we will show the result of our investigation in comparison to the previous *.zipx* sample we observed.



FW: NEW URGENT PURCHASE ORDER

Folder: [redacted] Date: [redacted]
From: [redacted] Size: [redacted]
To: [redacted] Path: [redacted]
Subject: FW: NEW URGENT PURCHASE ORDER

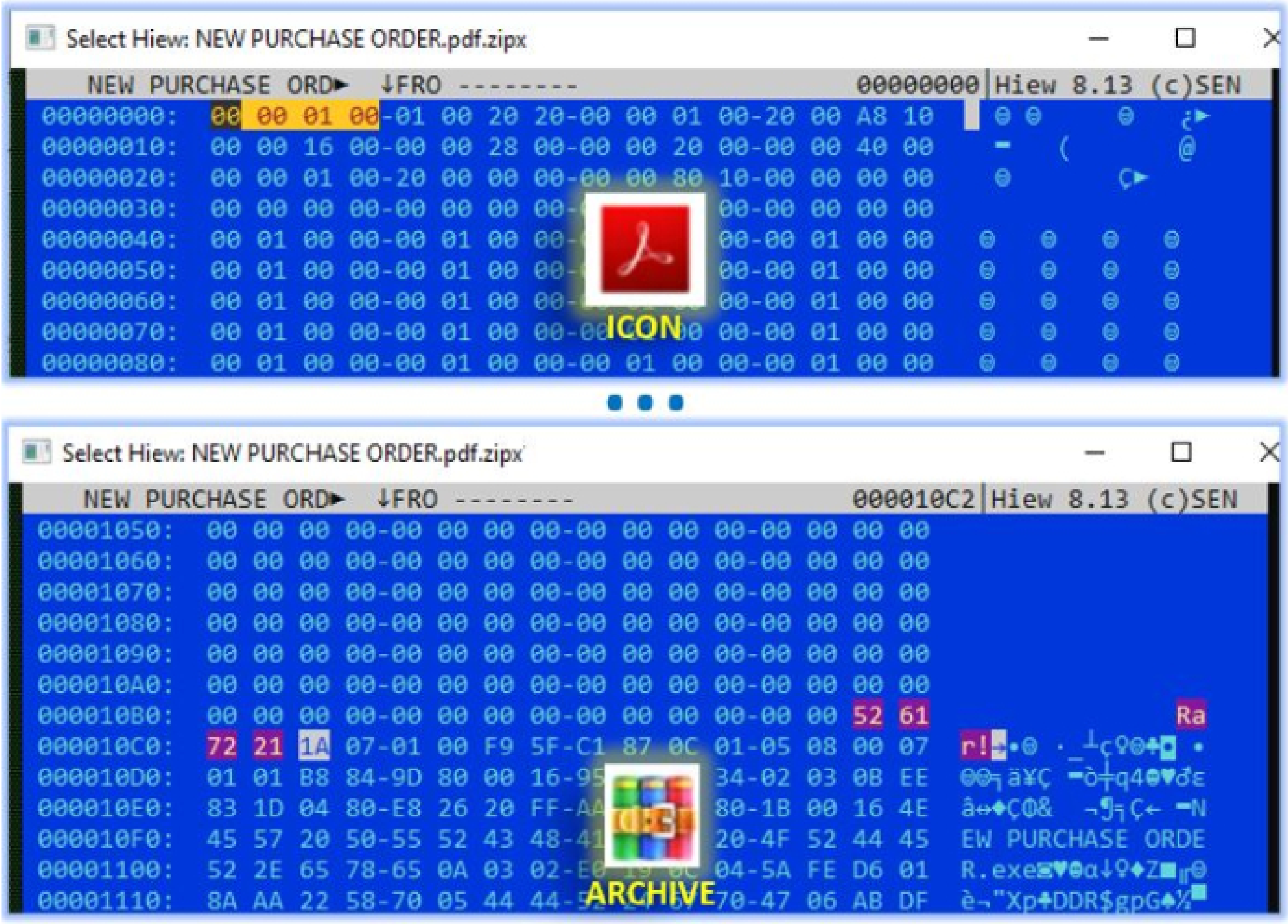
B6025f4e90001.6025f4e90008.0001
Message Headers
Message Body
Message Body
NEW PURCHASE ORDER.pdf.zipx

Type: Icon Size: 468.8 KB

NEW PURCHASE ORDER.pdf.zipx
Icon
468.8 KB
Double-click to save to disk.

Figure 1: The email sample containing a .zipx attachment

The emails, claiming to be from the Purchase Manager of certain organizations that the cybercriminals are spoofing, look like usual malspams except for their attachment. The attachments, which have a filename format “*NEW PURCHASE ORDER.pdf*.zipx”,* are actually image (Icon) binary files, with attached extra data, which happens to be RAR. This file format abuse is similar to what we have seen previously.

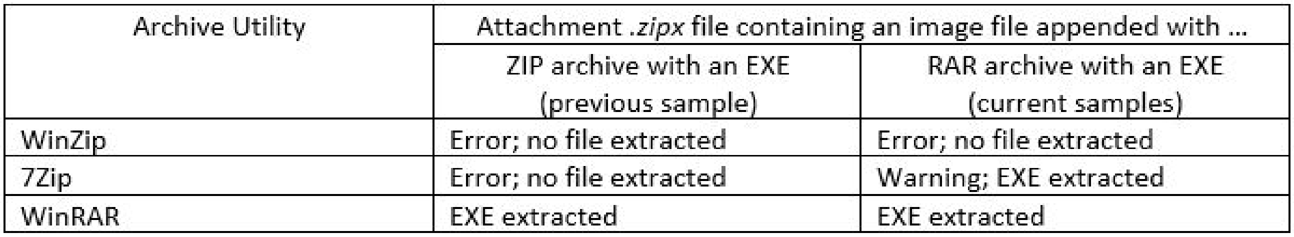


```
Select Hiew: NEW PURCHASE ORDER.pdf.zipx
   NEW PURCHASE ORD►  ↓FRO --------                      00000000|Hiew 8.13 (c)SEN
00000000:  00 00 01 00-01 00 20 20-00 00 01 00-20 00 A8 10   ☺ ☺     ☺   ¿►
00000010:  00 00 16 00-00 00 28 00-00 00 20 00-00 00 40 00    ▬   (       @
00000020:  00 00 01 00-20 00 00 00-00 00 80 10-00 00 00 00    ☺       Ç►
00000030:  00 00 00 00-00 00 00 00-           00-00 00 00 00
00000040:  00 01 00 00-00 01 00 00-           00-00 01 00 00   ☺   ☺   ☺   ☺
00000050:  00 01 00 00-00 01 00 00-           00-00 01 00 00   ☺   ☺   ☺   ☺
00000060:  00 01 00 00-00 01 00 00-           00-00 01 00 00   ☺   ☺   ☺   ☺
00000070:  00 01 00 00-00 01 00 00-00       00 00-00 01 00 00   ☺   ☺   ☺   ☺
00000080:  00 01 00 00-00 01 00 00-00 01 00 00-00 01 00 00   ☺   ☺   ☺   ☺
```

```
Select Hiew: NEW PURCHASE ORDER.pdf.zipx
   NEW PURCHASE ORD►  ↓FRO --------                      000010C2|Hiew 8.13 (c)SEN
00001050:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00001060:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00001070:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00001080:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00001090:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000010A0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000010B0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 52 61                 Ra
000010C0:  72 21 1A 07-01 00 F9 5F-C1 87 0C 01-05 08 00 07   r!→•☺ ·_┴ç♀☻♣◘ •
000010D0:  01 01 B8 84-9D 80 00 16-95       34-02 03 0B EE   ☺☺╕ä¥Ç ▬ò╪q4☻♥♂ε
000010E0:  83 1D 04 80-E8 26 20 FF-AA       80-1B 00 16 4E   â↔♦ÇΦ& ¬╕╗Ç← ▬N
000010F0:  45 57 20 50-55 52 43 48-41       20-4F 52 44 45   EW PURCHASE ORDE
00001100:  52 2E 65 78-65 0A 03 02-E0       04-5A FE D6 01   R.exe◙♥☻α↓♀♦Z■╓☺
00001110:  8A AA 22 58-70 05 44 44-5        70-47 06 AB DF   è¬"Xp♣DDR$gpG♠½▀
```

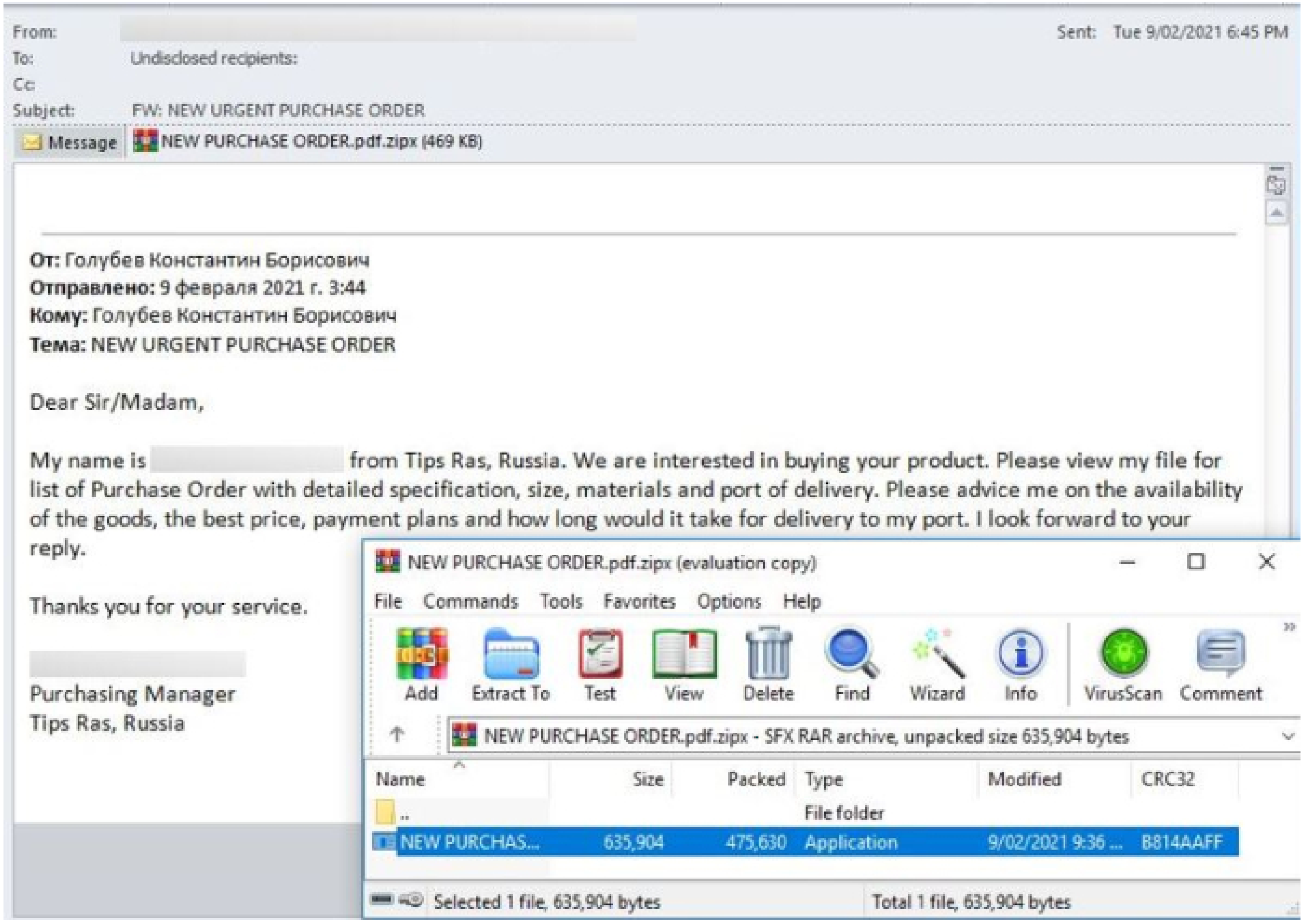
Figure 2: The attachment’s contents viewed in the Hiew tool

If the attachment successfully evades any scanning email gateways, the next hurdle is the victim’s machine, which needs to have an unzip tool that can extract the executable file inside the attachment. We tried using the same tools from the previous blog to extract the EXE file and here is the result:



Archive Utility	Attachment .*zipx* file containing an image file appended with …	
	ZIP archive with an EXE (previous sample)	RAR archive with an EXE (current samples)
WinZip	Error; no file extracted	Error; no file extracted
7Zip	Error; no file extracted	Warning; EXE extracted
WinRAR	EXE extracted	EXE extracted

The archive utility WinZip and WinRAR yield similar results when extracting the EXE file from the previous and current *.zipx* files. WinZip does not support unzipping either of samples whereas WinRAR managed to extract the EXE file contained in both samples.



From: [redacted]
To: Undisclosed recipients:
Cc:
Subject: FW: NEW URGENT PURCHASE ORDER
Sent: Tue 9/02/2021 6:45 PM

Message | NEW PURCHASE ORDER.pdf.zipx (469 KB)

От: Голубев Константин Борисович
Отправлено: 9 февраля 2021 г. 3:44
Кому: Голубев Константин Борисович
Тема: NEW URGENT PURCHASE ORDER

Dear Sir/Madam,

My name is [redacted] from Tips Ras, Russia. We are interested in buying your product. Please view my file for list of Purchase Order with detailed specification, size, materials and port of delivery. Please advice me on the availability of the goods, the best price, payment plans and how long would it take for delivery to my port. I look forward to your reply.

Thanks you for your service.

[redacted]
Purchasing Manager
Tips Ras, Russia

NEW PURCHASE ORDER.pdf.zipx (evaluation copy)

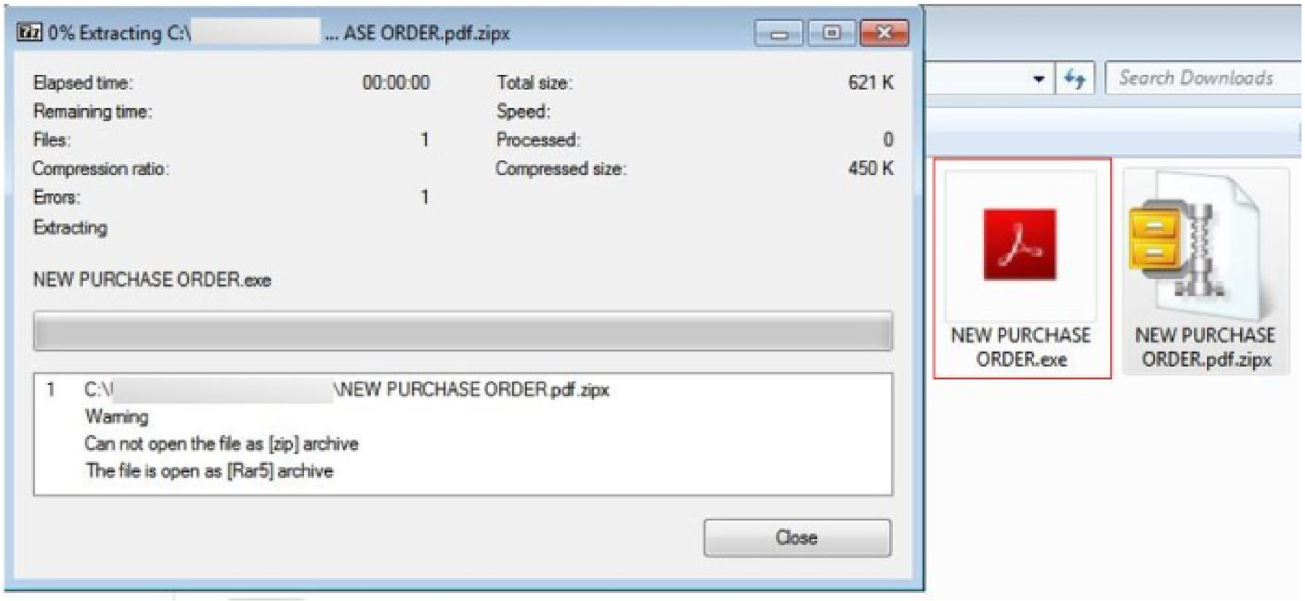
NEW PURCHASE ORDER.pdf.zipx - SFX RAR archive, unpacked size 635,904 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
NEW PURCHAS...	635,904	475,630	Application	9/02/2021 9:36 ...	B814AAFF

Selected 1 file, 635,904 bytes | Total 1 file, 635,904 bytes

Figure 3: The executable contained in the attachment NEW PURCHASE ORDER.pdf.zipx is recognized by WinRAR

Interestingly, 7Zip can also extract the content of the latest *.zipx* sample. 7Zip initially tries to open the files as a ZIP archive and fails, but afterward, 7Zip recognizes the *.zipx* files as Rar5 archives and can get their contents unpacked. Unlike in the previous blog, there is no need for the extension of the recent attachments to be renamed to something else other than *.zipx* or *.zip* just for their executables to be extracted using 7Zip.



0% Extracting C:\ [redacted] ... ASE ORDER.pdf.zipx

```
Elapsed time:          00:00:00    Total size:          621 K
Remaining time:                    Speed:
Files:                        1    Processed:               0
Compression ratio:                 Compressed size:     450 K
Errors:                       1
Extracting

NEW PURCHASE ORDER.exe
```

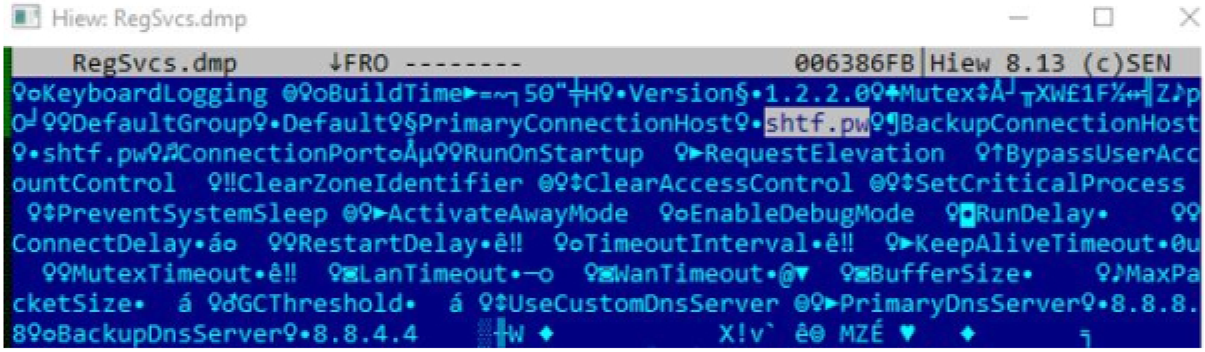
```
1   C:\ [redacted] \NEW PURCHASE ORDER.pdf.zipx
    Warning
    Can not open the file as [zip] archive
    The file is open as [Rar5] archive
```

Figure 4: Opening the attachment NEW PURCHASE ORDER.pdf.zipx using the 7Zip tool

The executables we gathered have a similar name to that of the *.zipx* attachment, “*NEW PURCHASE ORDER*.exe*”. Also, the icon at the start of the *.zipx* files is actually the icon used on the EXE files within the archive.

Analyzing the EXE files indicates that they are samples of NanoCore RAT version 1.2.2.0. This RAT create copies of itself at the AppData folder and inject its malicious code at RegSvcs.exe process. The data stolen by this RAT is sent to the command and control servers listed below:

- shtf[.]pw
- uyeco[.]pw



Hiew: RegSvcs.dmp

```
   RegSvcs.dmp       ↓FRO --------                 006386FB│Hiew 8.13 (c)SEN
♀○KeyboardLogging ☻♀○BuildTime►=~┐5Θ"╪H♀•Version§•1.2.2.0♀♣Mutex‡Å┘┬XW£1F%↔╢Z♪p
O┘♀♀DefaultGroup♀•Default♀§PrimaryConnectionHost♀•shtf.pw♀¶BackupConnectionHost
♀•shtf.pw♀♫ConnectionPort○Åµ♀♀RunOnStartup  ♀►RequestElevation  ♀↑BypassUserAcc
ountControl  ♀‼ClearZoneIdentifier ☻♀‡ClearAccessControl ☻♀‡SetCriticalProcess
 ♀‡PreventSystemSleep ☻♀►ActivateAwayMode  ♀○EnableDebugMode  ♀■RunDelay•    ♀♀
ConnectDelay•áo  ♀♀RestartDelay•ê‼  ♀○TimeoutInterval•ê‼  ♀►KeepAliveTimeout•0u
  ♀♀MutexTimeout•ê‼  ♀◙LanTimeout•─o  ♀◙WanTimeout•@▼  ♀◙BufferSize•    ♀♪MaxPa
cketSize•  á ♀♂GCThreshold•  á ♀‡UseCustomDnsServer ☻♀►PrimaryDnsServer♀•8.8.8.
8♀○BackupDnsServer♀•8.8.4.4     ▒╪W ♦            X!v` ê☻ MZÉ ♥   ♦       ╕
```

Figure 5: Memory dump of RegSvcs processes where NanoCore malware is injected

Summary

The recent malspams have the same goal like the ones we investigated almost two years ago and that is to effectively hide the malicious executable from anti-malware and email scanners by abusing the file format of the “*.zipx*” attachment, which in this case is an Icon file with added surprises. In a slight twist, enclosing the executable into a RAR archive instead of a ZIP file, the content of the *.zipx* attachment can be extracted by another popular archiving tool, 7Zip. If the end-user uses 7Zip or WinRAR, the NanoCore malware could be installed onto the system, if the user decides to run and extract it. It all works because various archive utilities try their darndest to find something to unzip within files. You might even argue they try too hard!

The Trustwave Secure Email Gateway flagged the messages as malicious and detected this threat.

IOCs

Attachment:

NEW PURCHASE ORDER.pdf.zipx (480092 bytes) SHA1:
DF46A893B51D8ADE0CCDEF7E375FB387E2560720
New Purchase Order.pdf (2).zipx (403050 bytes) SHA1:
C93FBA54357E90235202F58DA1FEFF7AB1142F65

NanoCore RAT:

NEW PURCHASE ORDER.exe (635904 bytes) SHA1:
E99F6B9BD787679666F8C54B9A834D6ACECFA622
New purchase order (3).exe (431104 bytes) SHA1:
FD958C365B6BFA5EF34779831773EC92C041A5D5