McAfee Labs Threat Advisory

Operation Red October

January 18, 2013

Summary

"Red October" is a targeted attack and cyber espionage network that was discovered to be targeting Diplomatic and Government agencies. The threats that were used in this attack campaign have been known to be active since 2009. This targeted attack involves both MS-office and Java based exploits. The payloads used in the exploitation are mostly backdoors and password stealers that steal the user's information and send it in an encrypted form to the remote attacker.

Detailed information about the infection, its propagation, and mitigation are in the following sections:

- Infection and Propagation Vectors
- Characteristics and Symptoms
- Exploit HeatMap
- Restart Mechanism
- Getting Help from the McAfee Foundstone Services team

Infection and Propagation Vectors

The exploits used in the targeted attack are sent to the users through spear phishing e-mails that contain crafted malicious documents as attachments, and a malicious link embedded in the e-mail that leads to a compromised website.

Once the user opens the malicious document containing the embedded code, a malicious payload is dropped into the system. The dropped payload in turn communicates with the C&C servers. The payload receives additional modules from the C&C server to handle the infection on different types of devices and also could drop additional malware.

Characteristics and Symptoms

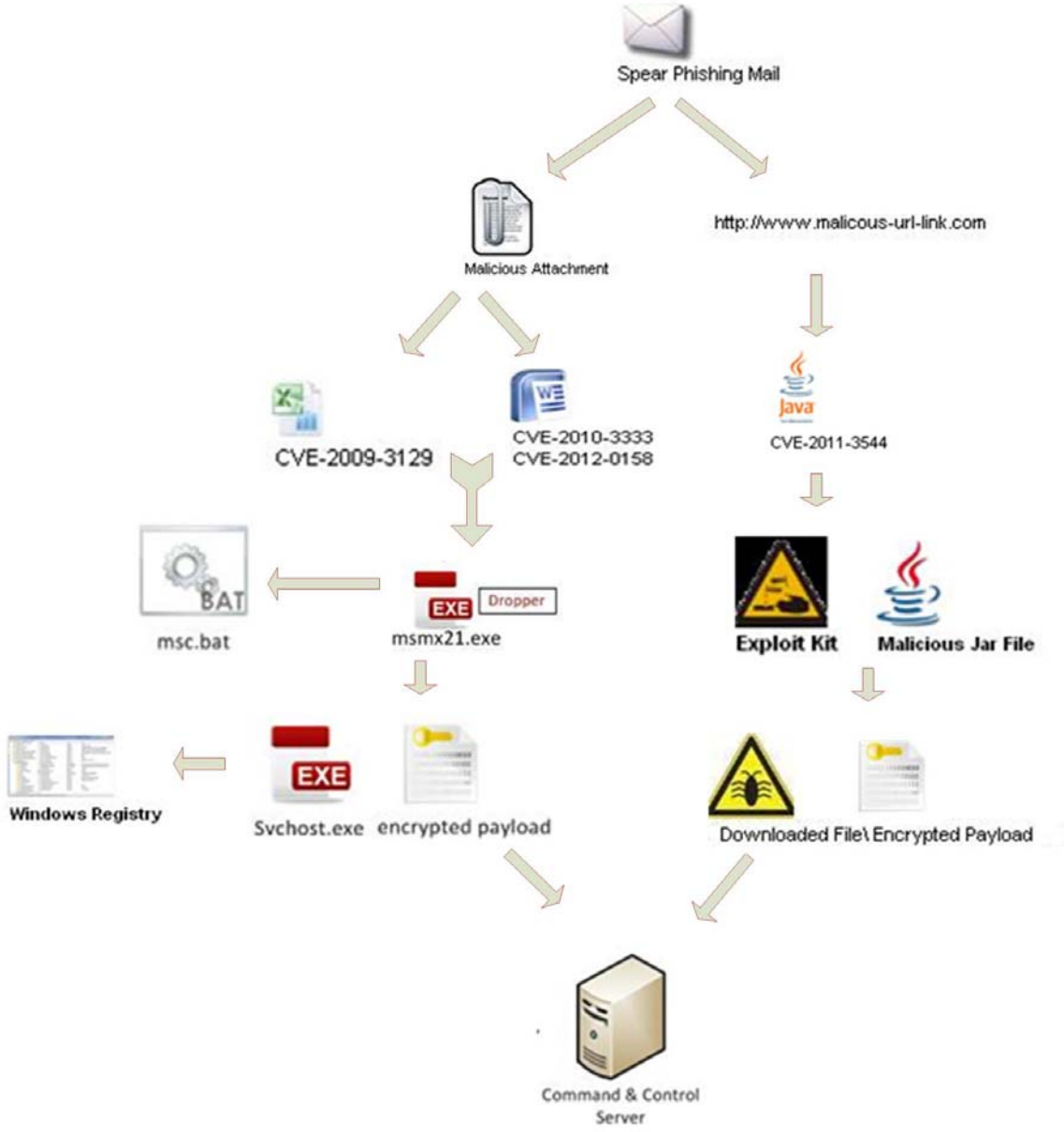
Description

There could be different combinations of Microsoft and Java exploits and payload in the wild to achieve this attack. We have used one of the MD5s (51EDEA56C1E83BCBC9F873168E2370AF) to do this analysis, which is a document file.

The Red October campaign is known to target the following mentioned vulnerabilities:

- CVE-2012-0158 (MS Word)
- CVE-2010-3333 (MS Word)
- CVE-2009-3129 (MS Excel)
- CVE-2011-3544 (Java Rhino Script Engine Vulnerability)

The following picture clearly shows how the targeted attack happens in the Red October Campaign.



Microsoft Document Exploitation (CVE-2012-0158, CVE-2010-3333, CVE-2009-3129):

The phishing email contains an attachment with the malicious office document. This file, when opened, exploits one of the above mentioned vulnerabilities and drops the payload file “msmx21.exe”.

Payload Information:

After successful exploitation of the vulnerability, the embedded executable file (msmx21.exe) is dropped in the %temp% folder.

msmx21.exe creates and executes the following files:

%Temp%\msc.bat
%ProgramFiles%\Windows NT\svchost.exe
%ProgramFiles%\Windows NT\wsdktr.ltp (Encrypted payload) -> random name

The dropped batch file has the following content:

```
chcp 1251
:Repeat
attrib -a -s -h -r "%DROPPER_FILE%"
del "%DROPPER_FILE%"
if exist "%DROPPER_FILE%" goto Repeat
del "%TEMP%\msc.bat"
```

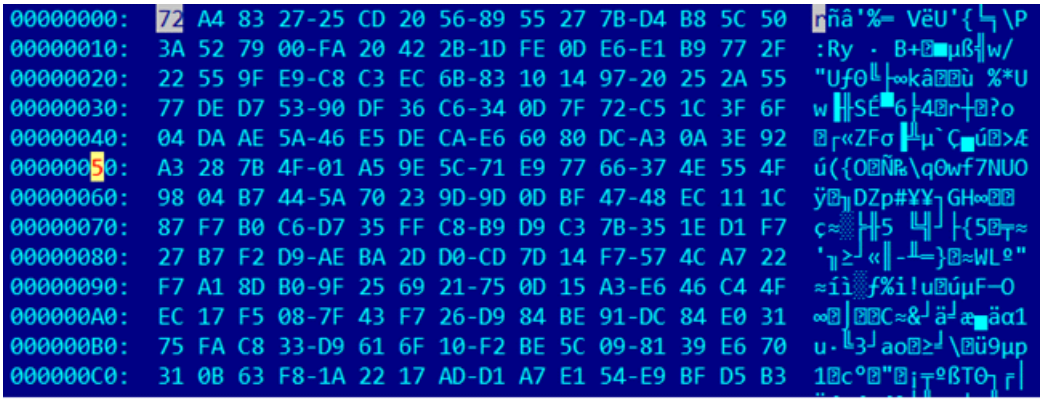
The use of “chcp 1251” in the batch file is to switch the codepage of an infected system to handle Cyrillic characters. This might suggest that either the attack originates from Russia or was also targeted towards government agencies in Russia.

Svchost.exe is an installer component that decrypts and loads the main backdoor (wsdktr.ltp). It connects to the following Microsoft hosts to check for a live Internet connection:

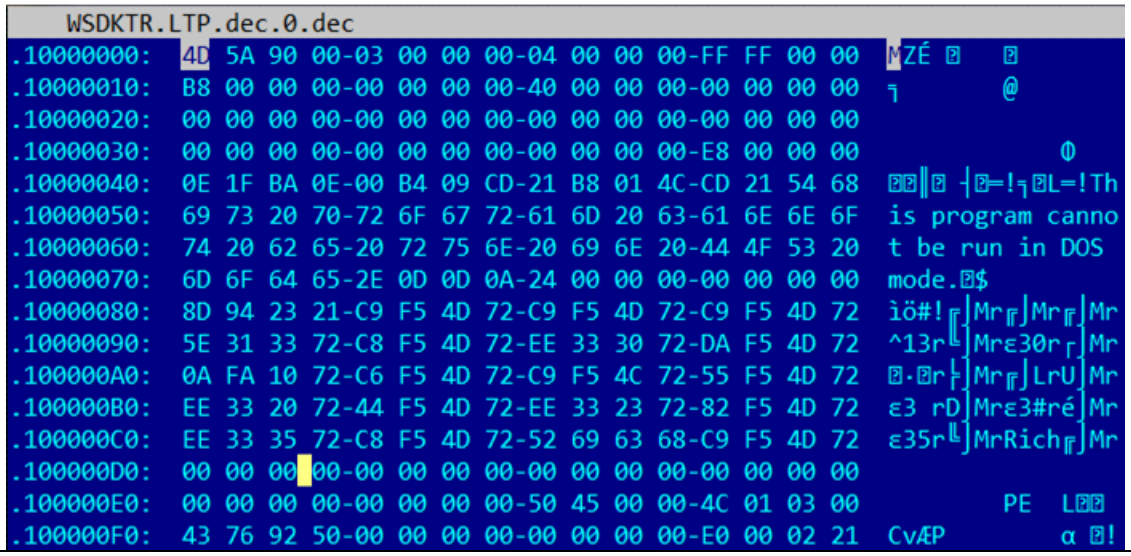
update.microsoft.com
www.microsoft.com
support.microsoft.com

wsdktr.ltp is an encrypted executable file (UPX packed dll) that is decrypted and loaded into memory by svchost.exe.

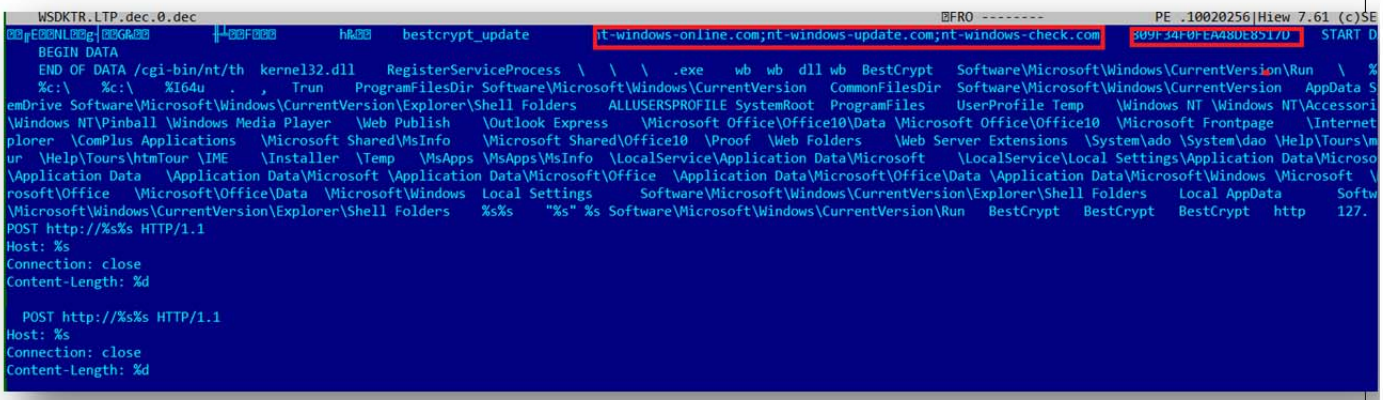
Encrypted wsdktr.ltp file:



Decrypted file:



The decrypted file is responsible for the communication between the infected machine and C&C server as shown in the following image.



The following domains are used for C&C :

nt-windows-online.com
nt-windows-update.com
nt-windows-check.com
csrss-check-new.com

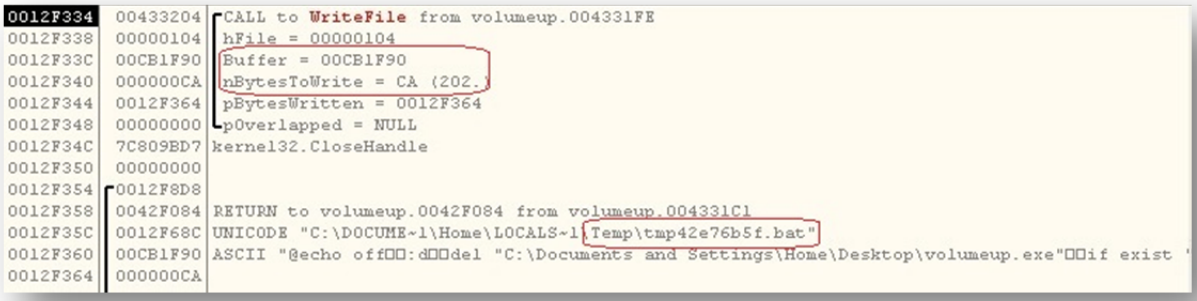
Exploitation Using Java (CVE-2011-3544):

In Java Rhino Script Engine Vulnerability, security manager is disabled during JavaScript execution, which would enable full permission to the system during its execution. When the user clicks the link that came through the spam mail, the exploit would be triggered on the vulnerable system.

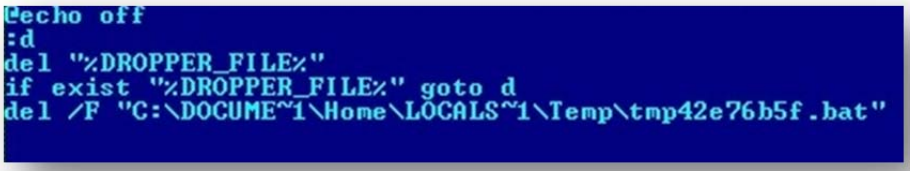
The downloaded payload creates and executes the following files:

%Temp%\ tmp42e76b5f.bat -> random name
%Application Data%\Keucot\ qagi.exe -> random name
%Application Data%\ Okurp \ dezaa.ufy-> random name (encrypted content)

The *following debugged code shows the batch being created while execution.*



The batch file has the following content:



The payload injects itself to the running system processes in the machine. They also monitor the browser activities in the targeted browsers (Chrome, Firefox, Safari, and IE).

```
user_pref("network.cookie.cookieBehavior", 0);
user_pref("privacy.clearOnShutdown.cookies", false);
user_pref("security.warn_viewing_mixed", false);
user_pref("security.warn_viewing_mixed.show_once", false);
user_pref("security.warn_submit_insecure", false);
user_pref("security.warn_submit_insecure.show_once", false);
```

The above picture shows the changes made to the configuration file so that cookies won't be cleared when the user shuts down the system. Also warning messages won't be displayed when the user visits the malicious or insecure pages.

Malicious threads injected to the processes monitor the user's activities and collect the information about the Outlook contacts and browser cookies, along with the system information. The collected information is stored as an encrypted content and sent to the command & control server. Some of these exploits download Ransomware and Zbot payloads.

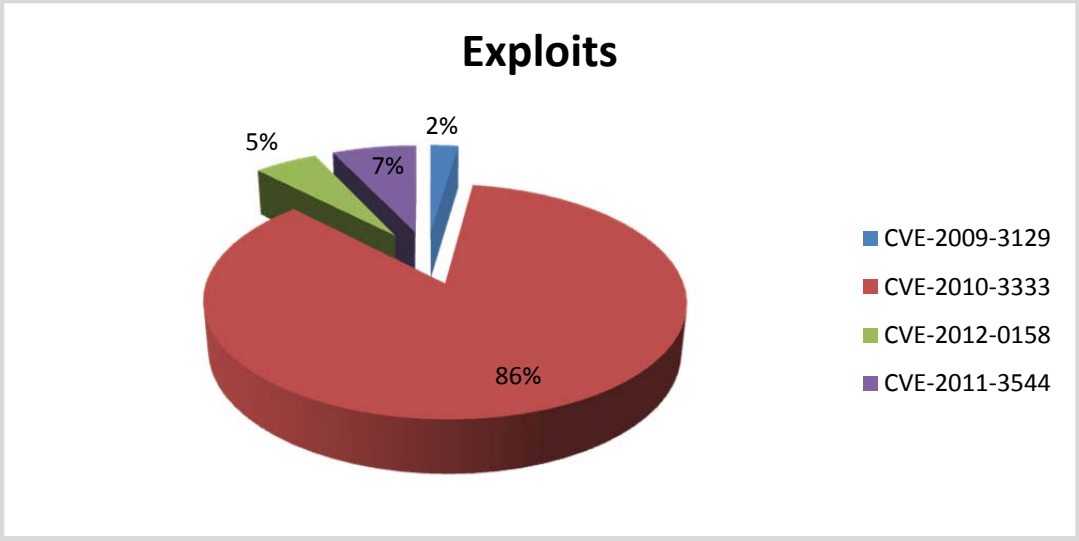
C&C Server:

29f2aad01fee3663.com

McAfee has coverage for this exploit CVE-2011-3544 and detects the downloaded payload used in the targeted attack as BackDoor-FJJ.

Exploit Heat Map

The following statistics show the usage of the vulnerabilities in the targeted attack in the last quarter.



Exploits Statistics Targeted on Companies and Government Organizations (Aug 2012 – Dec 2012).

Restart Mechanism

Description

The following registry entry would enable the Trojan to execute every time when Windows starts.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon "Userinit" "C:\WINDOWS\system32\userinit.exe,""C:\WINDOWS\system32\userinit.exe, C:\Program Files \WindowsNT\svchost.exe"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Zeemav: ""C:\Documents and Settings\Home\Application Data\Keucot\qagi.exe""

Mitigation

Users are requested to exercise caution while opening unsolicited emails and unknown links. Users are advised to update Windows and third-party application security patches and virus definitions on a regular basis and have proper filtering rules.

- Use Access Protection Rules from accessing such run keys.
- Please keep your anti-virus updated.
- Keep software up-to-date with the latest available patches.
- It is advisable to use your firewall to monitor unusual traffic.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives.

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx