Operation “Red October”:

Indicators of Compromise and Mitigation Data

Version 1.4

Table of contents:

1. Background information

On January 14, 2013, Kaspersky Lab announced the discovery of “Red October”, a high-level cyber-espionage campaign that has been active for over 5 years. (https://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies). This campaign has successfully infiltrated computer networks at diplomatic, governmental and scientific research organizations, gathering data and intelligence from mobile devices, computer systems and network equipment.

This document is aimed at CERTs and system administrators, to allow the detection and mitigation of the threat.

2. Indicators of compromise

An indicator of compromise is a forensic artifact that can identify pieces of an intrusion on a host or network. OpenIOC is a framework developed by Mandiant to share intelligence about security breaches including technical characteristics, methodologies or other evidences. This information can be used by security professionals to quickly search and identify security breaches.

The loader, most common known path/names:

%PROGRAMFILES%\Windows NT\svchost.exe
%PROGRAMFILES%\Windows NT\svclogon.exe

Note: the malware dropper writes **“svchost.exe”** or **“svclogon.exe”** into the first available path from the list:

%ProgramFiles%\Windows NT
%APPDATA%\Microsoft
%ProgramFiles%\Windows NT\Accessories
%ProgramFiles%\Windows NT\Pinball
%ProgramFiles%\Windows Media Player
%ProgramFiles%\Web Publish
%ProgramFiles%\Outlook Express
%ProgramFiles%\Microsoft Office\Office10\Data
%ProgramFiles%\Microsoft Office\Office10
%ProgramFiles%\Microsoft Frontpage
%ProgramFiles%\Internet Explorer
%ProgramFiles%\ComPlus Applications

%ProgramFiles%\WindowsUpdate
%CommonProgramFiles%\Microsoft Shared\MsInfo
%CommonProgramFiles%\Microsoft Shared\Office10
%CommonProgramFiles%\Proof
%CommonProgramFiles%\Web Folders
%CommonProgramFiles%\Web Server Extensions
%CommonProgramFiles%\System\ado
%CommonProgramFiles%\System\msadc
%SystemDrive%\Documents and Settings\LocalService\Application Data\Microsoft
%SystemDrive%\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft
%ALLUSERSPROFILE%\Application Data
%windir%\Installer
%windir%\Help\Tours\mmTour
%windir%\Help\Tours\htmTour
%windir%\Help\Tours\WindowsMediaPlayer
%windir%\IME
%windir%\MsApps
%windir%\MsApps\MsInfo
%windir%\inf
%ALLUSERSPROFILE%\Application Data\Microsoft
%ALLUSERSPROFILE%\Application Data\Microsoft\Office
%ALLUSERSPROFILE%\Application Data\Microsoft\Office\Data
%ALLUSERSPROFILE%\Application Data\Microsoft\Windows
%HOMEPATH%\Local Settings
%APPDATA%
%APPDATA%\Microsoft\Office
%APPDATA%\Microsoft\Office\Data
%APPDATA%\Microsoft\Windows
%windir%\Temp
%TMP%
%TEMP%

To correctly identify an infected system, we recommend checking all these paths.

Main backdoor encrypted body, known filenames (same location on disk as “the loader”):

fsmgmtio32.msc
cfsyn.pcs
frpdhry.hry
ime64ex.ncs
io32.ocx
lhafd.gcp

lsc32i.cmp
ocxstate.dat
opdocx.gxt
sccme.hrp
scprd.hrd
syncls.gxk
lgdrke.swk
sdlvk.acx
wsdktr.ltp
synhfr.pkc
scpkrp.gmx
rfkscp.pck
qsdtlp.rcp

Stolen data and logs:

%TMP%\SSDPserv32\ssdtrbs%08x%.sys.%d%
"%TMP%\smrdprev\smrdprev_%p_%p.tmp

Scheduler module:

%APPDATA%\Microsoft\RtkN32Gdi.exe

Encrypted configuration data:

%ALLUSERSPROFILE%\adt.dat
%LOCALAPPDATA%\adt.dat

Nokia module log:

"%TMP%\adobe_upd_imhbfex_%p_%p.dat"

Windows Mobile module:

"%TMP%%\tmp_m.%p.%p.dat"

Mutexes:

dfgber7t8234ytfndfugh5vndfuvh4
dfgbsdfjvabufqgwiffuvh4
208D2C60-3AEA-1069-A2D7-08002B30309D

huiofwhfiowjcpowjkcwcophwvurweionwopmcvopwkvpwjnhopv
sysvolumecheckasdfg

3. Command and control domains

To receive instructions from the attackers and to exfiltrate data, Red October uses a complex infrastructure which relies on multiple domains and servers distributed around the world. The following Command and Control domains have been observed in the attacks:

bb-apps-world.com
blackberry-apps-world.com
blackberry-update.com
csrss-check-new.com
csrss-update-new.com
csrss-upgrade-new.com
dailyinfonews.net
dll-host.com
dll-host-check.com
dll-host-udate.com
dll-host-update.com
dllupdate.info
drivers-check.com
drivers-get.com
drivers-update-online.com
genuine-check.com
genuineservicecheck.com
genuineupdate.com
hotinfonews.com
microsoftcheck.com
microsoft-msdn.com
microsoftosupdate.com
mobile-update.com
msgenuine.net
msinfoonline.org
msonlinecheck.com
msonlineget.com
msonlineupdate.com
ms-software-check.com
ms-software-genuine.com
ms-software-update.com
new-driver-upgrade.com

nt-windows-check.com
nt-windows-online.com
nt-windows-update.com
osgenuine.com
os-microsoft-check.com
os-microsoft-update.com
security-mobile.com
shellupdate.com
svchost-check.com
svchost-online.com
svchost-update.com
update-genuine.com
win-check-update.com
windowscheckupdate.com
windows-genuine.com
windowsonlineupdate.com
win-driver-upgrade.com
wingenuine.com
wins-driver-check.com
wins-driver-update.com
wins-update.com
winupdateonline.com
winupdateos.com
world-mobile-congress.com
xponlineupdate.com

4. IPs used in the attack.

The Red October infrastructure relied on several command and control servers, proxies and superproxies. Here's a list of known IPs associated with the attackers:

141.101.239.225
178.162.129.237
178.162.182.42
178.63.208.49
188.40.19.247
31.184.234.18
31.41.45.9
37.235.54.48
46.4.202.86
77.72.133.161

78.46.173.15
88.198.30.44
88.198.85.161
88.198.85.162
92.53.105.40
95.168.172.69
31.41.45.139
91.226.31.40
178.63.208.63
31.41.45.119
176.9.241.254
31.41.45.179
176.9.189.36
92.53.105.214
188.40.19.244
85.25.104.57

5. Network traffic

Snort rules based on server ETags of known motherships:

#this catches most of the traffic
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Possible Red October proxy CnC 1"; flow:to_client,established; content:"ETag|3a 20 22|**8c0bf6-ba-4b975a53906e4**|22|"; http_header; classtype:trojan-activity; sid:2016224; rev:2;)

#traffic handled by the 2nd mothership server
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Possible Red October proxy CnC 2"; flow:to_client,established; content:"ETag|3a 20 22|**1c824e-ba-4bcd8c8b36340**|22|"; http_header; classtype:trojan-activity; sid:2016225; rev:1;)

#traffic handled by the 3rd mothership server
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Possible Red October proxy CnC 3"; flow:to_client,established; content:"ETag|3a 20|W/|22|**186-1333538825000**|22|"; http_header; classtype:trojan-activity; sid:2016226; rev:1;)

Snort rules to match the C&C domains:

alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain bb-apps-world.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|bb-apps-world|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111111; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain blackberry-apps-world.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|blackberry-apps-world|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111112; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain blackberry-update.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|blackberry-update|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111113; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain csrss-check-new.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|csrss-check-new|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111114; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain csrss-update-new.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|csrss-update-new|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111115; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain csrss-upgrade-new.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|csrss-upgrade-new|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111116; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain dailyinfonews.net"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|dailyinfonews|04|net"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111117; rev:1;)

alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain dll-host.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|dll-host|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111118; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain dll-host-check.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|dll-host-check|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111119; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain dll-host-udate.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|dll-host-udate|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111120; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain dll-host-update.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|dll-host-update|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111121; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain dllupdate.info"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|dllupdate|04|info"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111122; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain drivers-check.com "; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|drivers-check|04|com "; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111123; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain drivers-get.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|drivers-get|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111124; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain drivers-update-online.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;

content:"|04|drivers-update-online|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111125; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain genuine-check.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|genuine-check|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111126; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain genuineservicecheck.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|genuineservicecheck|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111127; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain genuineupdate.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|genuineupdate|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111128; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain hotinfonews.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|hotinfonews|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111129; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain microsoftcheck.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|microsoftcheck|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111130; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain microsoft-msdn.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|microsoft-msdn|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111131; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain microsoftosupdate.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|microsoftosupdate|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cy

ber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111132; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain mobile-update.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|mobile-update|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111135; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain msgenuine.net"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|msgenuine|04|net"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111136; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain msinfoonline.org"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|msinfoonline|04|org"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111137; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain msonlinecheck.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|msonlinecheck|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111138; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain msonlineget.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|msonlineget|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111139; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain msonlineupdate.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|msonlineupdate|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111140; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain ms-software-check.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|ms-software-check|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111141; rev:1;)

alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain ms-software-genuine.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|ms-software-genuine|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111142; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain ms-software-update.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|ms-software-update|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111143; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain new-driver-upgrade.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|new-driver-upgrade|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111144; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain nt-windows-check.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|nt-windows-check|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111145; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain nt-windows-online.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|nt-windows-online|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111146; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain nt-windows-update.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|nt-windows-update|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111147; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain osgenuine.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|osgenuine|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111148; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain os-microsoft-check.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|os-

microsoft-check|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111149; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain os-microsoft-update.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|os-microsoft-update|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111150; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain security-mobile.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|04|security-mobile|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111151; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain shellupdate.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|04|shellupdate|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111152; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain svchost-check.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|svchost-check|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111153; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain svchost-online.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|svchost-online|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111154; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain svchost-update.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|04|svchost-update|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111155; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain update-genuine.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|04|update-genuine|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cy

ber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111156; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain win-check-update.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|win-check-update|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111157; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain windowscheckupdate.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|windowscheckupdate|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111158; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain windows-genuine.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|windows-genuine|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111159; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain windowsonlineupdate.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|windowsonlineupdate|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111160; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain win-driver-upgrade.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|win-driver-upgrade|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111161; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain wingenuine.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|wingenuine|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111162; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain wins-driver-check.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|wins-driver-check|04|com"; fast_pattern;
reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111163; rev:1;)

alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain wins-driver-update.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|wins-driver-update|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111164; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain wins-update.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|wins-update|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111165; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain winupdateonline.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|winupdateonline|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111166; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain winupdateos.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|winupdateos|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111167; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain world-mobile-congress.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|world-mobile-congress|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111168; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain xponlineupdate.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|xponlineupdate|04|com"; fast_pattern; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; classtype:bad-unknown; sid:111111169; rev:1;)

Snort rules to match the C&C ip addresses:

alert tcp $HOME_NET any -> [141.101.239.225,178.162.129.237,178.162.182.42,178.63.208.49,188.40.19.247,31.184.234.18,31.41.45.9,37.235.54.48,46.4.202.86,77.72.133.161,78.46.173.15,88.198.30.44,88.198.85.161,88.198.85.162,92.53.105.40,95.168.172.69,31.41.45.139,91.226.31.40,178.63.208.63,31.41.45.119,176.9.241.254,31.41.45.179,176.9.189.36,92.53.105.214,188.40.19.244,85.25.104.57]

any (msg:"Red October C&C TCP Traffic"; flags:S; reference:url,www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; threshold: type limit, track by_src, seconds 60, count 1; classtype:misc-attack; flowbits:set,ET.Evil; flowbits:set,ET.CompIP; sid:111111170; rev:1;)

Snort rules to detect the HTTP traffic (from Emerging Threats):

/etc/snort/rules/emerging_pro-trojan.rules:alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Red October/Win32.Digitalia Checkin cgi-bin/nt/th"; flow:established,to_server; content:"POST"; nocase; http_method; content:"/cgi-bin/nt/th"; urilen:14; content:!"User-Agent|3a| "; http_header; reference:url,www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation; classtype:trojan-activity; sid:2016214; rev:1;)
/etc/snort/rules/emerging_pro-trojan.rules:alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Red October/Win32.Digitalia Checkin cgi-bin/nt/sk"; flow:established,to_server; content:"POST"; nocase; http_method; content:"/cgi-bin/nt/sk"; urilen:14; content:!"User-Agent|3a| "; http_header; reference:url,www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation; classtype:trojan-activity; sid:2016215; rev:1;)
/etc/snort/rules/emerging_pro-trojan.rules:alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Red October/Win32.Digitalia Checkin cgi-bin/dllhost/ac"; flow:established,to_server; content:"POST"; nocase; http_method; content:"/cgi-bin/dllhost/ac"; urilen:19; content:!"User-Agent|3a| "; http_header; reference:url,www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation; classtype:trojan-activity; sid:2016216; rev:4;)
/etc/snort/rules/emerging_pro-trojan.rules:alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Red October/Win32.Digitalia Checkin cgi-bin/ms/check"; flow:established,to_server; content:"POST"; nocase; http_method; content:"/cgi-bin/ms/check"; urilen:17; content:!"User-Agent|3a| "; http_header; reference:url,www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation; classtype:trojan-activity; sid:2016217; rev:1;)
/etc/snort/rules/emerging_pro-trojan.rules:alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Red October/Win32.Digitalia Checkin cgi-bin/ms/flush"; flow:established,to_server; content:"POST"; nocase; http_method; content:"/cgi-bin/ms/flush"; urilen:17; content:!"User-Agent|3a| "; http_header; reference:url,www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation; classtype:trojan-activity; sid:2016218; rev:1;)
/etc/snort/rules/emerging_pro-trojan.rules:alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Red October/Win32.Digitalia Checkin cgi-bin/win/wcx"; flow:established,to_server; content:"POST"; nocase; http_method; content:"/cgi-bin/win/wcx"; urilen:16; content:!"User-Agent|3a| "; http_header; reference:url,www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation; classtype:trojan-activity; sid:2016219; rev:1;)

/etc/snort/rules/emerging_pro-trojan.rules:alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Red October/Win32.Digitalia Checkin cgi-bin/win/cab"; flow:established,to_server; content:"POST"; nocase; http_method; content:"/cgi-bin/win/cab"; urilen:16; content:!"User-Agent|3a| "; http_header; reference:url,www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation; classtype:trojan-activity; sid:2016220; rev:1;)

6. List of passwords and SNMP community names hardcoded in the Netscan plugin:

public, private, 1q2w3e, 1q2w3e4r, 1q2w3e4r5t, 1q2w3e4r5t6y, cscAstral, @5tr0Mon1, 1qazxsw23edc, 3edcxzaq12, 123ewqasdcxz, !@#ewqASDcxz, !QAZxcde32, qsczse, 234rfvcxsw, $3eTn27W#7, 010101, 03101974, 0392a0, 041309, 06051983, 080808, 0ublic, 1021947, 1100293, 111, 112511polo, 1212x, 123, 123123321, 1234, 123456, 12345678, 123456789123456789, 1234567899876543 21, 123o321, 126ajm19kal51ma, 130601, 1324132442314231, 13244231, 13971852654, 162534, 17081-, 170810, 1809BGD11, 1940117, 1947102, 19841990, 199397, 19M1R20S, 1Q5IRJmg9Q, 1q2w3e, 1q2w3e4r, 1q2w3e4r5t, 1q2w3e4r5t6y, 1qazxsw23edc, 2005, 21012008a, 212321a, 24021985, 240787, 2531821, 280d1a03, 285468339, 29091972, 2read, 31sal999, 378dd6, 3DB5ZG, 3MC-Zuku-Rw, 43827207V, 4changes, 4udoju, 549yotok, 553322, 5bpbpyHeLu0a9Ab, 5zzkzp, 626fqs, 63Fd6dYhMnsjMNPk, 654321, 6551318, 693ygUgv, 722690, 7777777inchinas, 789456, 7917407, 794613, 7nsi20, 7p1cCcZvqY6T, 80244, 816836, 83L80N3, 8491, 8591, 8888888, 8ublic, 8urlib, <removed>, AKdGmjQO, ANYCOM, Admin, Afoltz-PB, Allahu, Andrey131201, Bl234353, C0de, C0mmunity[hezt00a1, C0mmunity[hezt00a2, C0mmunity[hezt00aa3, C0mmunity[hezt00b1, C495y5m6T1, CISCO, CONSIP_MIB, CR52401, D1g!T, DNOT?ISTLE, DNOTHISTLE, E142BERLINO, EC_IMCO, ET0021B7E49CC9, G1Mme1nf0, GINL-!M3npEFF, GN0CR3AD, GSBTBMPLS!, GWAN_g,2b?l?m0nit0r, GWAN_gl0baL??k??, GWAN_gl0bal_m0gid0r, GWAN_gl0bal_m0nit0?, GWAN_gl0bal_m0nit0r, GWAN_gl0bal_mxJ?6?v, GulNozMeh, HDDBELBXL, HITMAN, IBM, ICE, ILMI, Intermec, Jedeee71, JoJo, KBRlog3CPRK, L#39YWh7N16w, Lcxuidtg, Mailbox, Manyasha, Mihnea@109, NURTENEKREM, NoGaH$@!, OrigEquipMfr, P@SSW0RD, PRIVATE, PUBLIC, Petr0f`c, Petr0fac, Petr0fac?, Petrofac, Private, Ptbnic, Ptcmic, PuBMic, Public, RM24655521, RcFnsSnCo20m08R, RnfE36mM, RoaringKat, SECRET, SECURITY, SINetMGT, SNMP, SNMP_trap, SPBranc1d-Rw, SUN, SWITCH, SYSTEM, SbcihAiryq52, Secret, Security, Si4m2010AyZnFkDe45L, Slay1987, Soco, Sr.h3Q6i, Switch, System, TENmanUFactOryPOWER, TEST, TRD_VSAT, W1ld#Parr0ts, YDFWgSKh, YXaLmb1t5Ras, YsZpL5RqMa76, Z123456z, Zxcvbnm123, `ublic, a1b2c3d4, absurdistan_81, access, adimn, adm, admin, admin1, adonis, agent, agent_steal, ahi, ajutorsoci, akjol1230, alfa239, alfa2390, alfred, all, all,

all, alpha, amBa3#wsx, amsterdam2003, andrey240787, antoniu, apc, arbor, assistant2007, astalavista, at.prague, at@szat, aublic, auok12, avsvMda, baborasa1234, backb00r, backupauto, badarsul, badarsul86, bandwidth, bar789, bathclnet, batru_ro, benj2023, benjaminfranklin, bintec, blue, boksha, br0adwhy, bratan, breakpoint, bumblebee, bunnia2010, c20176, cable-d, cable-docsis, canon_admin, ccrthwtd, cde32wsxzaq1, chelyabinsk, chera98888, chiaro, chumburidze, cisco, cisco-adsl, clingendael, cme_1823, commread, community, commwrite, control, corba, core, correyvba, cp8S52aA, cpecwr99, cpecww99, cs1bhS8W, csi-rain, cucurigu, da123456, dasakirov, debug, deeplomat, default, dilbert, diver, dk0208, dollys, drazen024, efimerida, elchin2491, elen24, eman72, embassy, enable, f6PF3T9T, fabian, fake2011, fastanefnd1, field, field-service, finance, forescout, fourthmile, freekevin, fubar, fwrocmn, fwwrcmn, g0v53vM3, germanos, gestione, gsoficom14, gu#3Gst., guest, gulbalam, gwendal, hello, henrygiz, hp_admin, i6666, ibm, icces, ilmi, intelligence, intermec, internal, ipko, ipxint, itorocmn, jessica, jg214327, jimaguas, jozefina, jpiworldwide, karZer, kazeem, kbiway2007, kbiway2008, kerrek, kittec, kokale, kokale1980, koko, konsulro, korablik, korona, krakoziabra, kuwait, kyw.u61, lapublic, laura, lebanon, lfcadoot, lhlyy0320, linda, louvain, loveme, macedonia, makbank23, manager, manuel, mariam, marius, martin, mary1964, meerim0909, merlin62, mesurucu, metiha, mfa123MFA, mfa6789, mfalOVAL, mimoza, mirella, mirella26091978, mitrkq1w2e3, mmat1230, mmat1987, mngt, mofa, mohammed, moni4man, monitor, monitoring, mq5Kg9iG, mrtg, ms03101974, msnadm, mudrost999, nasasiet, nasawr1, nature, netman, netman2002, network, nina180754, none, noppes, norformin, notprivate, notpublic, notpulic, nr.490315, ntnhflm, nurtenbay, nvaiaJC4, okoloamaraa, openview, oyeneye, p0l!@#nms, p3j4nt4n, p5blic, p9EGn25D, pUbhic, parrral, pass, password, pgnred, picpu, polaris, polmrtg, polsnmp, porneste, post, pounette, power222, ppb(260685), pqblic, pqpq-1957, pr1ap1014, pr1v4t3, priemnaja, privat, provision, proxy, prtgmail, pu6lik, pu?hi?, pu?l, pu?l)c, pu?l`b, pu?lib, pu?lic, pu?lik, pu?lyc, puBlic, pu`lic, pub?ic, pubdic, pubhic, publ, publ)c, publ1c, publ?3, publac, publhc, publi#, publi+, publi?, publia, publib, public!!!, public1, public2, public3, public?, publig, publik, publio, publis, publiw, publkB, publkc, publmc, publoc, publxc, publyc, publ{C, publ{c, pubmi?, pubmia, pubmic, pubn, pubn)c, pubni?, pubni?", pubnib, pubnic, pubpc1, pucliC, puclic, puclic?, puclik, pucmic, pufl, puflic, pufli{, pufmyc, puglic, pujlic, pur-i?, pur??1, purlic, purlig, pusac, pwbli#, pwblic, pwjlic, p}1??1, qazwsx, qazxcdew, qubl?3, qwedcxza, qwer1234, qwerty, qwerty123456, qwertyu, qwertyui, r0snmp$tr1ng, r23771, rainbow, rbnpublic, rccm-map, read, read-only, read-write, readonly, readwrite, red, regional, rekzi, richka, rm5tbd23, rmon, rmon_admin, ro4orion, ro81qnp4, roembil, romania2, root, router, rusinfonet, rw4orion, rwa, rwcfcmp1s, s3cr3t, sabonis, safara, salvaje07, san-fran, sanfran, sayyara, scotty, seCtion

7. RC4 encryptions keys

The Red October main backdoor module is stored on disk in the form of a zlib compressed and RC4-encrypted executable.

Here's a list of known module names with their respective RC4 encryption keys:

fsmgmtio32.msc, rkef09erf90kerf9k34fo3kfo3ekdf2[l'2dl2043dl4d03ld34fkf4j
cfsyn.pcs, sdfg45fyhh656ffhjfddsd5hkjfgccdxs4waaxzhjjy6yrre4dhjmmtr357643fbnffr
frpdhry.hry, sfgsrykw5rwqedg43564ytdfbgkfgnxczagsd6566igfsdr656867idffghkgdsdsdtd
ime64ex.ncs, jr89h5tr489fg954dewdwedwehg845jhgi54jgljg54j3gj589gh489h2php
io32.ocx, 384r783fh374fh37hf349hf9348hf938fh3894hf893h4f89h3489fh3894f8
lhafd.gcp, 3497888hf8943hf89j389fj8934jf9843jf983j489fjjj43ghkjnbsdfjhsdf8374
lsc32i.cmp, 0641cn34873cn47832cyn43ycn43yo5c4n5ynyynyn324y5c324yn5c3yn5c
ocxstate.dat, ldfn34fdldsflivfu4tu3049u039utgf9vuxdf0gu0349ut34po5j432pakoew02o3ox
opdocx.gxt, efkggjfrut454329wehdfgtriwnxcmgf457edhajzq234yr4fkkdjsheirtyjghfgks
sccme.hrp, dkeerqwerfgvg467643fffdffhf5443DGFRESD2455667QQEwrfgu45kj535kj534m5n
scprd.hrd, awsrrqwerfgvg4676e34gfdffhf5443DGFRESD2547967QQEwrfgu45kj535kj53we4u
syncls.gxk, rtei458ghfjdkeirutnawqpondfrjuwgsfroinher5409srncbdhreqpodjrv5438hr
lgdrke.swk, qwertfhsjazxbcvnmkdlruwe23458732wuryfjghc4whcfggbjd3skdjfksfsf543ie
sdlvk.acx, ekrjdfh56urti34569382wqhdjfvncmdjqlosjhdfmazplkeey4559382dkwuueiowo
rfkscp.pck, dfr45e6uyt39gth45ncv43fjhrmlpotyiulqawert65hfjtrewow62krifje9532j3e
scpkrp.gmx, a6749328347569483ryedfbcsjqopehf4rbdjwhse945hsdrgskwjr2354sheg3472s
synhfr.pkc, ldfn34fdldsflivfu4tu3049u039utgf9vuxdf0gu0349ut34po5j432pakoew02o3ox
wsdktr.ltp, dfdedkwe3322oeitodkdjeio3e9ekdjwasddcncmvjdasalwpeoryg7534hvn5wewse
QSDTLP.RCP, eerklxcbs4783dtglwetpoqweo33wketkasdlgasdjgakti3eqtojqwoiedgoiddfgo
lsmpdr.vcs, erhg548rhgflri4932nvg56832hdfjcnrlsjqpmdrewjdhaznrow321hfrjska38rua
MBDSEC.SDX, hyjtri458ejshertkcbnvbn44cjfthweeowqksdjfklgorpwwjkdfj5i4wos89423od
SCPESC.ECS, dfwjdh45683jsmcnrt5938qjdhertlmncbfgtjwpaj438271jdhr4hdbsuqplmk34hs
klsldr.slr, dfgsdgjweerqkwdgofjsdfokgbjoi5290348t0dfjgbsjr65jopofkaj345j4tdfgsd

8. OpenIOC File

You can download the "ioc" file from here:

https://github.com/jaimeblasco/AlienvaultLabs/blob/master/malware_analysis/RedOctober/48290d24-834c-4097-abc5-4f22d3bd8f3c.ioc

9. Vulnerabilities and patches:

The "Red October" attacks used five known attack vectors:

- CVE-2009-3129 (in XLS files)
- CVE-2010-3333 (in DOC files)
- CVE-2012-0158 (in DOC files)
- CVE-2011-3544 (online, via malicious web pages)
- CVE-2008-4250 (to attack other computers in the local network)

For patches, apply:

- Microsoft Security Bulletin MS09-067 – Important - Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652) - http://technet.microsoft.com/en-us/security/bulletin/MS09-067
- Microsoft Security Bulletin MS10-087 – Critical - Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930) - http://technet.microsoft.com/en-us/security/bulletin/MS10-087
- Microsoft Security Bulletin MS12-027 – Critical - Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2664258) - http://technet.microsoft.com/en-us/security/bulletin/ms12-027
- Microsoft Security Bulletin MS08-067 – Critical - Vulnerability in Server Service Could Allow Remote Code Execution (958644) - http://technet.microsoft.com/en-us/security/bulletin/ms08-067

10. References:

1. The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies:
https://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies
2. The OpenIOC WebSite: http://www.openioc.org/
3. 'snort' website: http://www.snort.org/
4. Emerging Threats website: https://www.emergingthreats.net/
5. "Red October" OpenIOC file:
https://github.com/jaimeblasco/AlienvaultLabs/blob/master/malware_analysis/RedOctober/48290d24-834c-4097-abc5-4f22d3bd8f3c.ioc
6. Red October: Java Exploit Delivery Vector Analysis -
https://www.securelist.com/en/blog/208194086/Red_October_Java_Exploit_Delivery_Vector_Analysis
7. "Red October" part 2 – the modules:
https://www.securelist.com/en/blog/208194091/Red_October_part_two_the_modules

About Kaspersky Lab:

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users*. Throughout its 15-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for consumers, SMBs and Enterprises. The company currently operates in almost 200 countries and territories across the globe, providing protection for over 300 million users worldwide. Learn more at www.kaspersky.com.

About AlienVault:

AlienVault's **Unified Security Management**™ platform (AV-USM™) provides a fast and cost-effective way for organizations with limited security staff and budget to address compliance and threat management needs. With all of the essential security controls built-in, the AV-USM puts enterprise-class security visibility within fast and easy reach of smaller security teams who need to do more with less. AlienVault's **Open Threat Exchange™**, a system for sharing threat intelligence among **OSSIM** users and AlienVault customers, ensures AV-USM always stays ahead of threats. AlienVault is a privately held company headquartered in Silicon Valley and backed by Kleiner Perkins Caufield & Byers, Sigma, Trident Capital and Adara Venture Partners. For more information visit **www.AlienVault.com** or follow us on **Twitter**.