Operation “Red October”:

Indicators of Compromise and Mitigation Data

Table of contents:

1. Background information
2. Indicators of compromise
3. Command and control domains
4. IPs used in the attack
5. Network traffic & snort rules
6. List of passwords and community names used to attack network devices
7. RC4 encryption keys
8. OpenIOC File
9. Vulnerabilities and patches
10. References
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\`
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
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
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-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
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
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 cssss-check-new.com"; content:"[01 00 00 01 00 00 00 00 00 00]"; depth:10; offset:2; content:"[04]cssss-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 cssss-update-new.com"; content:"[01 00 00 01 00 00 00 00 00 00]"; depth:10; offset:2; content:"[04]cssss-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 cssss-upgrade-new.com"; content:"[01 00 00 01 00 00 00 00 00 00]"; depth:10; offset:2; content:"[04]cssss-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;)

Whitepaper: Operation “Red October” - Indicators of Compromise and Mitigation Data
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;
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;
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain dll-update.com"; content:"[01 00 00 01 00 00 00 00 00 00]"; depth:10; offset:2; content:"[04]dll-update[04]com"; fast_pattern;
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;
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;
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;
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;
Whitepaper: Operation “Red October” - Indicators of Compromise and Mitigation Data

<table>
<thead>
<tr>
<th>Drivers Update Online</th>
<th>com</th>
</tr>
</thead>
</table>

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:111111125; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain genuine-servicecheck.com"; content:"[01 00 00 01 00 00 00 00 00 00]"; depth:10; offset:2; content:"[04]genuine-servicecheck[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 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:111111127; 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:111111128; 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_Cyber_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;
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;
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;
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;
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;
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;
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;

Whitepaper: Operation “Red October” - Indicators of Compromise and Mitigation Data
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;
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;
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain new-driver-update.com"; content:"[01 00 00 01 00 00 00 00 00 00]"; depth:10; offset:2; content:"[04]new-driver-update[04]com"; fast_pattern;
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;
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;
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;
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;
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-
Whitepaper: Operation “Red October” - Indicators of Compromise and Mitigation Data

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;
ber_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 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;
ber_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 shellupdate.com”; content:”|01 00 00 01 00 00 00 00 00 00|”; depth:10; offset:2;
content:”|04|shellupdate|04|com”; fast_pattern;
ber_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;
ber_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;
ber_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 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;
ber_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;
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:111111156; 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:111111157; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"DNS query for Red October domain windowsgenuine.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:111111158; 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:111111159; 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:111111160; 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;)

Whitepaper: Operation “Red October” - Indicators of Compromise and Mitigation Data
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;
ber_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 win-
update.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|winupdate-|
04|com"; fast_pattern;
ber_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 win-
updateonline.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|04|winupdateonline|04|com"; fast_pattern;
ber_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 win-
updateos.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|04|winupdateos|04|com"; fast_pattern;
ber_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;
ber_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 xpon-
lineupdate.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|04|xonlineupdate|04|com"; fast_pattern;
ber_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 ->
[141.101.239.225,178.162.129.237,178.162.182.42,178.63.208.49,188.40.19.247,31.184.234.1
8,31.41.45.9,37.235.54.48,46.4.202.86,77.72.133.161,78.46.173.15,88.198.30.44,88.198.85.16
1,88.198.85.162,92.53.105.40,95.168.172.69,31.41.45.139,91.226.31.40,178.63.208.63,31.41.4
5.119,176.9.241.254,31.41.45.179,176.9.189.36,92.53.105.214,188.40.19.244,85.25.104.57]
any (msg:"Red October C&C TCP Traffic"; flags:S;
ber_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;
cks_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;
cks_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;
cks_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;
cks_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;
cks_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;
cks_Investigation; classtype:trojan-activity; sid:2016219; rev:1;)

Whitepaper: Operation “Red October” - Indicators of Compromise and Mitigation Data
6. List of passwords and SNMP community names hardcoded in the Netscan plugin:

public, private, 1q2w3e, 1q2w3e4r, 1q2w3e4r5t, 1q2w3e4r5t6y, cscAstral, @5tr0Mon1, 1qazxsw23edc, 3edcxzaq12, 123ewqasdctx, !@#ewqASDctx, !QAZxcde32, qscxzse, 234rfcvexw, $3eTn27W#7, 010101, 03101974, 0392a0, 041309, 06051983, 080808, 0ublic, 1021947, 1100293, 111, 1211511polo, 1212x, 123, 123123321, 1234, 123456, 12345678, 123456789123456789, 12345678987654321, 123o321, 126ajm19kal51ma, 130601, 1324132442314231, 13244231, 13971852654, 162534, 17081, 170810, 1809B91G, 1940107, 1947102, 19841990, 199937, 19M1R20S, 105IRJIn69Q, 1q2w3e, 1q2w3e4r, 1q2w3e4r5t, 1q2w3e4r5t6y, 1qazxsw23edc, 2005, 21012008a, 212321a, 24021985, 240787, 2531821, 285468339, 29091972, 2read, 31sal999, 378dd6, 3DB5ZG, 3MC-Zuku-Rw, 43827207V, 4changes, 4udoju, 549yotok, 553322, 5bpwHeLu0a9Ab, 5zzkzp, 626fqs, 63Fd6DyhMnsjMNPk, 654321, 6551318, 693ygUgv, 722690, 77777777inchinas, 789456, 7917407, 794613, 7ntiR0, 7p1CcZvqY6T, 80244, 816836, 83L80N3, 8491, 8888888, 8ublic, 8urlib, <removed>, AKdGmjQQ, ANYCOM, Admin, Afoltz-PB, Allahu, Andrey131201, BI234353, C0de, C0mmunity[hez00a1, C0mmunity[hez00a2, C0mmunity[hez00a3, C0mmunity[hez00b1, C495y5m6T1, CISCO, CONSIP_MIB, CR52401, D1gIT, DNOT?ISTLE, DNOTHISTLE, E142BERLINO, EC IMCO, ET0021B7E49CC9, G1Mme1nf0, GINL!M3npEFF, GN0CR3AD, GSBTBMPLS!, GWAN_g.2b?i?m0nIt0r, GWAN gl0ba1??k??, GWAN_gl0bal_m0g0d0r, GWAN gl0bal_m0nIt0r, GWAN_gl0bal_mxJ76?v, GulNozMeh, HDDBEBLX, HİTMAN, IBM, ICE, ILMI, Intervec, Jede3e71, JoJo, KBRlog3CPRK, L#39YWh7N16w, Lcxu1d9, Mailbox, Manyasha, Mihnea@109, NURTENKREM, NoGaH$@!, OrigEquipMfr, P@SSWORD, PRIVATE, PUBLIC, Petrof`c, Petrof`ac, Petrofac, Petrofac, Private, Ptbnic, Ptcmic, PUbMic, Public, RM24655521, RcFnSsCo20m08R, RnfE63Mm, RoaringKat, SECRET, SECURITY, SINetMGT, SNMP, SNMP_trap, SPBranc1d-Rw, SUN, SWITCH, SYSTEM, SbchAiryq52, Secret, Security, Si4m2010AyzNkFe45L, Slay1987, Socr, Sr.h3Q6i, Switch, System, TENmanUFact0ryPOWER, TEST, TRD_VSAT, W1ld#Parr0ts, YDFWgSKh, YXaLmb15Ras, YsZpL5QMa76, Z123456z, Zxcvbnm123, `ublic, a1b2c3d4, absurdistan_81, access, adimn, adm, admin, admin1, adonis, agent, agent_stear, ahi, ajutorsoci, akjol1230, alfa239, alfa2390, alfred, all, all,
7. RC4 encryptions keys

Whitepaper: Operation “Red October” - Indicators of Compromise and Mitigation Data
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"2dl2043d4d043d4fd4j cfcsyn.pcs, sdfg45fhhh65fhhddshd5hjgccccds4waxxzhjy6yrr4dhjmmtr357643fbnffr frpdhry.hry, sfgrskyw5wqegd43564ytfdkgfngcxcagd6566igfsdr656867idfgkgdsdsdtt im6e4ex.ncs, jr89h5tr489fg954dewedwedweh845jhi54jlgjg5j3gj589gh489h2php io32.ocx, 38r7783fh374fh37fhf394fhf938fhf938fhf938fhf938fhf938fhf938f lhafdp.cgp, 3497888h8f943h8f943j893j893j893j893j893j893j893j893j893f lsc32i.cmp, 0641cn3473cn4732cyn43ycn43ycn43ycn43ycn43ycn43ycn43ycn43ycn ocxstate.dat, ldffn34fdrfflfvtfvlu3049u039utgf9vuxdf0gu0349ut34po5j34pakoew02o3ox opdocx.gtx, efkjgjfrut454329wehtdftrixcmgaf457edhajzq234yryfkkjseirjygtjfgks scccme.hrp, dkeeqwerfvgv467643ffffhf5434DGFRFRES2D455667QQEwrfgu45kj535kj534m5n scprdr.hrd, awrsrqqwerfvgv4676e34gdfthf5443DGFRFRES2D547967QQEwrfgu45kj535kj53we4u syncls.gxt, rtei458ghjdfkierutnawfondfrjwugfsrionher5409smcmbrhreqpjr5vjr538hr lgdke.swk, qwertjxazxcvnmklrue23458732wurfyghc4whcfggbjd3skdjkstfsf543ie sdxv.kv, ekbfhdfh34569382wqhdjvnmcndjlosjhdmaszplkeey4559382dkwuwieuwo rfsccp.pck, dfrey56euy3939g45ncv43jhrmpoyulqawert65hfjtreowo26kkfjle9532je scpkrp.gmx, a6749328347569483ryedtcbcsjxqopehffr4bdjwhse945hshdrgswkjw2354sheg3472s synhpf.pck, ldfn34fdldslfivlu4tu3049u039utgf9vuxdf0gu0349ut34po5j34pakoew02o3ox wsdktlr.ltp, dfdedkwe3322eoiotdkjdeio39e9edkjdwasddcmvdasalwpoeryg7534hvn5wewse QSDTPL.RCP, eerkxlbs4783dtgwetpqwov33wktkasdgadgakti3eqtjowjwoeidgiddfgo lsmpdr.vcs, erhgg548rhglfr4932vng56832hdffnjrcnqjpmrjdrewdjanzrow321hfrjska38rue MBDSEC.SDX, hyjrti458jeusertkcbnvn44cjthweewqkdsdjklorpwjkdfj5i4wos894230d SCPESC.ECS, dfwjdth45683jismcmt9539qhdhertlnmbgfjjwpaj438271jdrh4hdsbqplm34hs ksklrd.srl, dfmsgdjjwinerqkwdgohjsdfokgboi5290348t0dfjgbsjr65jopokfj34j4dfgsd

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:
Whitepaper: Operation “Red October” - Indicators of Compromise and Mitigation Data

- 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:


10. References:

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

Whitepaper: Operation “Red October” - Indicators of Compromise and Mitigation Data
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](http://www.AlienVault.com) or follow us on [Twitter](http://Twitter).