Red October and Its Reincarnation

Raymond Chavez | William Kranich | Alex Casella
Overview

- Scale and Victims
- Red October Initial Infection
- Technical details
- Reincarnation as Cloud Atlas
- Prevention
Scale

- High level cyber espionage campaign
- Second most complicated malware in history as of 2013
- Infiltrated networks around the world
  - 39+ countries
  - Hundreds of high profile victims
Scale Cont.
8 Main Groups of Victims

- Government
- Embassies and diplomatic agencies
- Universities and research firms
- Commercial organizations
- Nuclear energy labs
- Oil and gas companies
- Aerospace institutions
- Military
Goal

- Steal classified information
- Obtain geopolitical intelligence
- Backed by nation states?
- Sell info on black markets?
Active for 5+ years

Discovered in late 2012 by Russian cyber security research firm Kaspersky Labs and partners
  Noted possible attribution to Russian-speaking attackers

Ended in January 2013 after Kaspersky Labs published findings in late 2012
Red October: Initial Infection

- Spear Phishing - directed at a specific target or organization based on known information

- Utilized known Microsoft Office, PDF, and Java vulnerabilities
  
  - CVE-2009-3129, CVE-2010-3333, CVE-2012-0158
  
  - Java ~ Rhino exploit (CVE-2011-3544)
  
  - Code from original exploit by Chinese hackers
Diplomatic car for sale

MODEL: Mazda 323- 1998  
TRANSMISSION: Automatic  
MILEAGE: 145,000 km

DISPLACEMENT: 1800 cc  
FUEL: Benzin

Power Steering – Electric Windows - AM/FM Stereo- 
Electric Mirrors - Air Conditioning - Remote central 
locking with Alarm - Extra snow tires.

PRICE: 2,700 $ (USD)


THE CAR IS IN A VERY GOOD CONDITIONS
Infection

- After opening malicious file, victim’s machine is infected using a malware dropper
- Main component is installed and communication with command and control server is established through backdoor module
- Encrypted communication between victim machine and C&C server
- More than 60 different domains hardcoded in malware code to communicate with C&C servers
- Malware contains components that infect machines on the same local network without the initial phishing attack
Infection

- Malware assigns each machine its own unique ID
  - This allows attackers to learn specific information about the user and tailor their attacks

- Malware installs PDF and Office plugins that allow attackers to regain communication with a machine even if the malware has been uninstalled

![Image of computer code and hexadecimal data]
Command and Control

- Kaspersky attempted to locate the command and control server
- The domains were pointing to IP addresses that ended up just being proxies
  - Requests forwarded over port 40080 using `socat` tool: relay for bidirectional data transfer
- Confirmed 10 different proxy servers, pointing to 3 different “mini-motherships”

<table>
<thead>
<tr>
<th>IP</th>
<th>Active</th>
<th>Confirm Malicious</th>
<th>Location</th>
<th>Hosting</th>
</tr>
</thead>
<tbody>
<tr>
<td>141.101.239.225</td>
<td>Oct-12</td>
<td>Yes</td>
<td>Russia</td>
<td>Leadertelemcom Ltd.</td>
</tr>
<tr>
<td>178.63.208.49</td>
<td>Oct-12</td>
<td>Yes</td>
<td>Germany</td>
<td>Nuremberg Hetzner Online Ag</td>
</tr>
<tr>
<td>188.40.19.247</td>
<td>Oct-12</td>
<td>Yes</td>
<td>Germany</td>
<td>Nuremberg Hetzner Online Ag</td>
</tr>
<tr>
<td>37.235.54.48</td>
<td>Oct-12</td>
<td>Yes</td>
<td>Ukraine / UK</td>
<td>Edis GmbH</td>
</tr>
<tr>
<td>78.46.173.15</td>
<td>Oct-12</td>
<td>Yes</td>
<td>Germany</td>
<td>Nuremberg Hetzner Online Ag</td>
</tr>
<tr>
<td>88.198.30.44</td>
<td>Oct-12</td>
<td>Yes</td>
<td>Germany</td>
<td>Nuremberg Hetzner Online Ag</td>
</tr>
<tr>
<td>88.198.85.161</td>
<td>Oct-12</td>
<td>Yes</td>
<td>Germany</td>
<td>Nuremberg Hetzner Online Ag</td>
</tr>
<tr>
<td>92.53.105.40</td>
<td>Oct-12</td>
<td>Yes</td>
<td>Russia</td>
<td>Ooo Lira-s</td>
</tr>
<tr>
<td>31.41.45.119</td>
<td>Nov-12</td>
<td>Yes</td>
<td>Russia</td>
<td>Reink Ltd</td>
</tr>
<tr>
<td>176.9.241.254</td>
<td>Nov-12</td>
<td>Yes</td>
<td>Germany</td>
<td>Nuremberg Hetzner Online Ag</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP</th>
<th>Date</th>
<th>Confirmed Malicious</th>
<th>Country</th>
<th>ISP</th>
</tr>
</thead>
<tbody>
<tr>
<td>31.41.45.139</td>
<td>Oct-12</td>
<td>Yes, mini-mothership</td>
<td>Russia</td>
<td>Reink Ltd.</td>
</tr>
<tr>
<td>91.226.31.40</td>
<td>Oct-12</td>
<td>Yes, mini-mothership</td>
<td>Russia</td>
<td>17 Ltd</td>
</tr>
<tr>
<td>178.63.208.63</td>
<td>Oct-12</td>
<td>Yes, mini-mothership</td>
<td>Germany</td>
<td>Nuremberg Hetzner Online Ag</td>
</tr>
</tbody>
</table>
• Requesting the index page of the “mini-motherships” returns the following:

```html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<title>BBC - Homepage</title>
<meta http-equiv="REFRESH"
content="0;url=http://www.bbc.com/">
</head>
</html>
```

• Requesting the HTTP “HEAD” of each server reveals that the “Last Modified” date is exactly the same, indicating that these servers are probably proxies themselves
Kaspersky was unable to determine if these “mini-motherships” were the actual end points or if they were proxies themselves.
Modules

- Entirely modular

- Consists of several categories:
  - Recon
  - Password
  - Email
  - USB Drive
  - Keyboard
  - Persistence
  - Spreading
  - Mobile
  - Exfiltration
Cloud Atlas

- Red October operation was shut down in 2013 after Kaspersky announcement.

- Network of C&Cs was dismantled.

- Highly complex operations such as this don’t just disappear, however:
  - In August 2014, Kaspersky discovered the Cloud Atlas malware when it found a very familiar spear phish file: DiplomaticCarSale.doc
  - This same file was used in the Red October operation.
  - Researchers believe the same group may be behind both campaigns, based on similarities in tactics, tools and targets.
The attackers use accounts at Swedish cloud provider CloudMe to communicate with compromised machines.

Attackers upload data to this account, which is then downloaded by the implant, decrypted, and interpreted.

The malicious files were uploaded by the malware and contain various things, such as system information, running processes and current username.
Similarities with Red October

- Rely on a similar construct:
  - Share the same LZMA (lossless) compression algorithm, which is used to compress the logs and to decompress the decrypted payload from the C&C servers.
  - Compiled using the same version of Visual Studio and same build number, using a very similar project configuration.
Similarities with Red October

- Same primary target nations:
  - Russia, Kazakhstan, India, Czech Republic

- Both Red October and CloudAtlas have targeted the same victims. Not just the same organizations, but some of the same machines. In one case, a machine was attacked twice in the last two years, once by Red October and once by CloudAtlas.
## Similarities with Red October

<table>
<thead>
<tr>
<th>Cloud Atlas</th>
<th>RedOctober</th>
</tr>
</thead>
</table>

### Cloud Atlas: Chevrolet Optra
- **Model:** 2007
- **Color:** Silver metallic
- **Engine:** 1.5L, LSE
- **Transmission:** Automatic
- **Mileage:** 8,000 km
- **Equipment:** Air-conditioning, Electric windows, very good condition, new batteries, always serviced

### RedOctober: Mazda 323
- **Model:** 1998
- **Displacement:** 1,800 cc
- **Transmission:** Automatic
- **Fuel:** Premium
- **Mileage:** 145,000 km
- **Features:** Power steering, Electric windows, AM/FM stereo, Electric Mirrors, Air Conditioning, Remote central locking with Alarm, Extra snow tires
- **Price:** 2,700 USD
- **Contact:** &__________ - &__________

The car can be viewed and tested at the German Embassy, Ulga Hofmoodsey 10, 116335 Moscow. In order to arrange an appointment please contact Mr. Paul Rechsteiner. Tel: +7 392 396 4500 (mobile) or +7 406 397 9500 ext. 423. E-mail: paul.rechsteiner@gmu.de

**THE CAR IS IN A VERY GOOD CONDITIONS**
Prevention

- Update Microsoft Office, Windows OS, PDF Software, and Java version.
- Be more aware of the types of emails that are opened and the attachments that are downloaded.
References


- https://securelist.com/blog/research/68083/cloud-atlas-redoctober-apt-is-back-in-style/


References