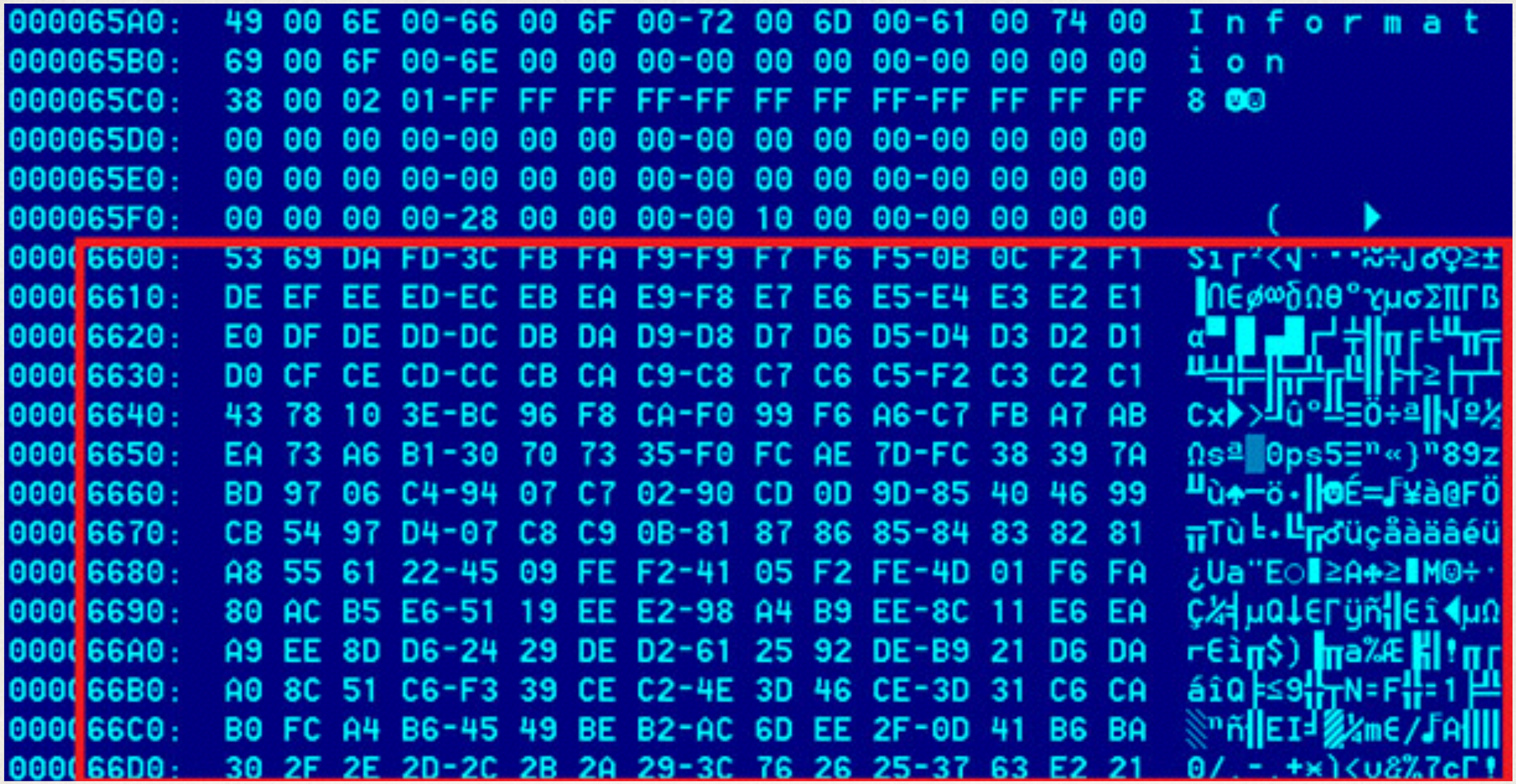


Red October and Its Reincarnation

Raymond Chavez | William Kranich | Alex Casella

Boston University | CS558 Network Security | April 30, 2015

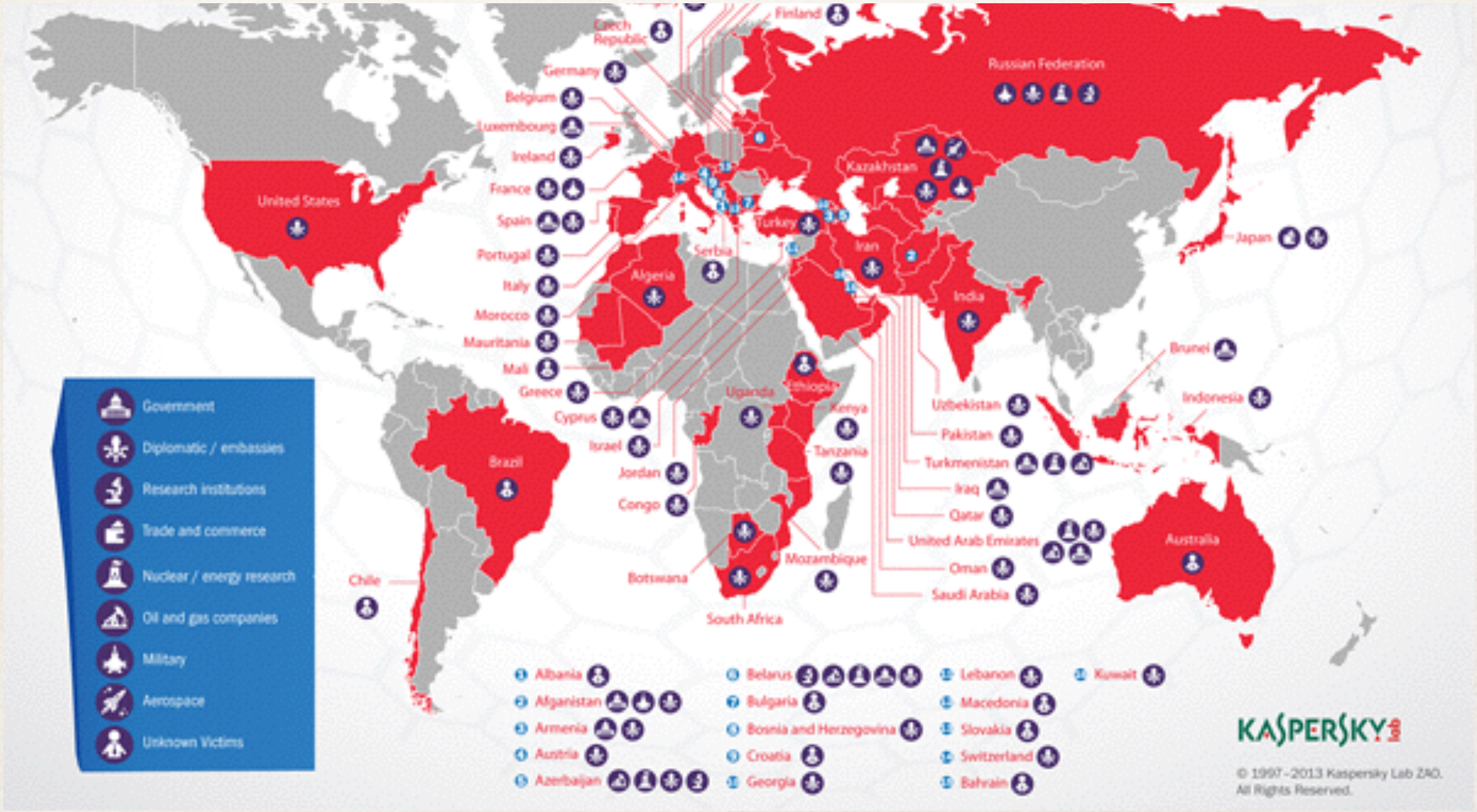
Overview

- 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.


Czech Republic
Germany
Belgium
Luxembourg
Ireland
France
Spain
Portugal
Italy
Morocco
Mauritania
Mali
Greece
Cyprus
Israel
Jordan
Congo
Botswana
South Africa
Mozambique
Chile
Brazil
United States
Finland
Russian Federation
Kazakhstan
Turkey
Serbia
Algeria
Iran
India
Japan
Brunei
Indonesia
Uzbekistan
Pakistan
Turkmenistan
Iraq
Qatar
United Arab Emirates
Oman
Saudi Arabia
Uganda
Ethiopia
Kenya
Tanzania
Australia
Government
Diplomatic / embassies
Research institutions
Trade and commerce
Nuclear / energy research
Oil and gas companies
Military
Aerospace
Unknown Victims
Albania
Afganistan
Armenia
Austria
Azerbaijan
Belarus
Bulgaria
Bosnia and Herzegovina
Croatia
Georgia
Lebanon
Macedonia
Slovakia
Switzerland
Bahrain
Kuwait
KASPERSKY lab
© 1997-2013 Kaspersky Lab ZAO.
All Rights Reserved.

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?

2007-2013

- 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

Example Spear Phish file

Diplomatic car for sale

MODEL: Mazda 323- 1998 **DISPLACEMENT:** 1800 cc

TRANSMISSION: Automatic **FUEL:** Benzin

MILEAGE: 145.000 km

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

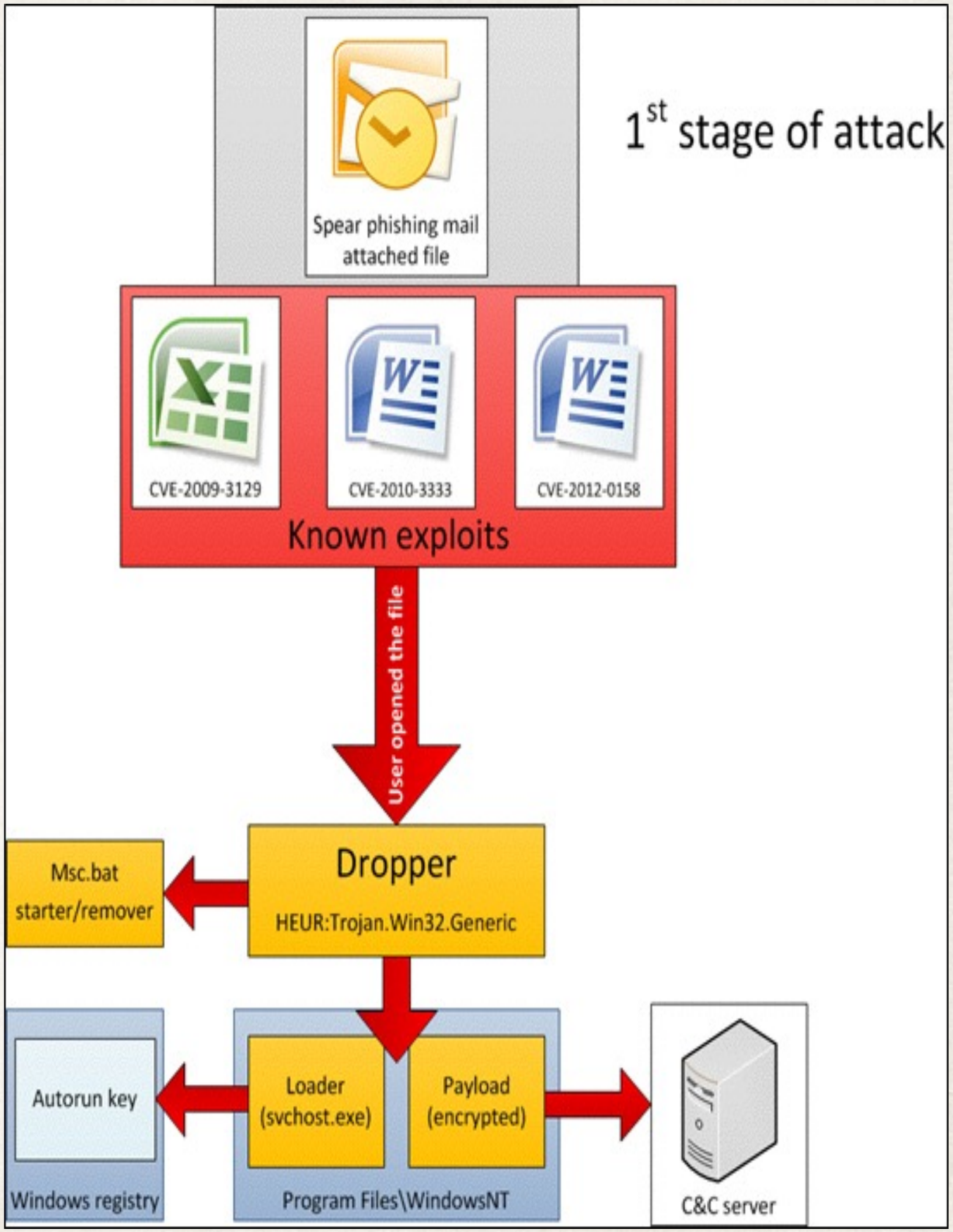
PRICE: 2.700 $ (USD)

CONTACT: &&&&&&&& - &&&&&&&&&

THE CAR IS IN A VERY GOOD CONDITIONS

Infection

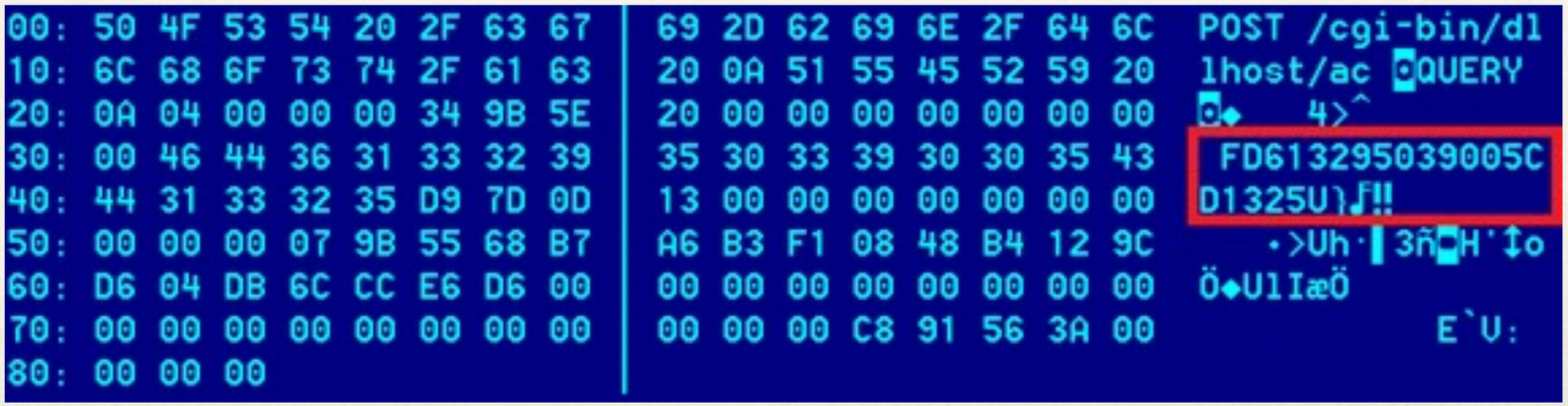
- After opening malicious file, victim's machine is infected using a malware dropper
- Main component is installed and communication with command and control server is established through backdoor module
- Encrypted communication between victim machine and C&C server
- More than 60 different domains 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



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"

IP	Active	Confirmed Malicious	Location	Hosting
141.101.239.225	Oct-12	Yes	Russia	Leadertelecom Ltd.
178.63.208.49	Oct-12	Yes	Germany	Nuremberg Hetzner Online Ag
188.40.19.247	Oct-12	Yes	Germany	Nuremberg Hetzner Online Ag
37.235.54.48	Oct-12	Yes	-unclear- ? Austria / UK /Spain	Edis Gmbh
78.46.173.15	Oct-12	Yes	Germany	Nuremberg Hetzner Online Ag
88.198.30.44	Oct-12	Yes	Germany	Nuremberg Hetzner Online Ag
88.198.85.161	Oct-12	Yes	Germany	Nuremberg Hetzner Online Ag
92.53.105.40	Oct-12	Yes	Russia	Ooo Lira-s
31.41.45.119	Nov-12	Yes	Russia	Relink Ltd
176.9.241.254	Nov-12	Yes	Germany	Nuremberg Hetzner Online Ag

IP	Date	Confirmed malicious	Country	ISP
31.41.45.139	Oct-12	Yes, mini-mothership	Russia	Relink Ltd.
91.226.31.40	Oct-12	Yes, mini-mothership	Russia	i7 Ltd
178.63.208.63	Oct-12	Yes, mini-mothership	Germany	Nuremberg Hetzner Online Ag

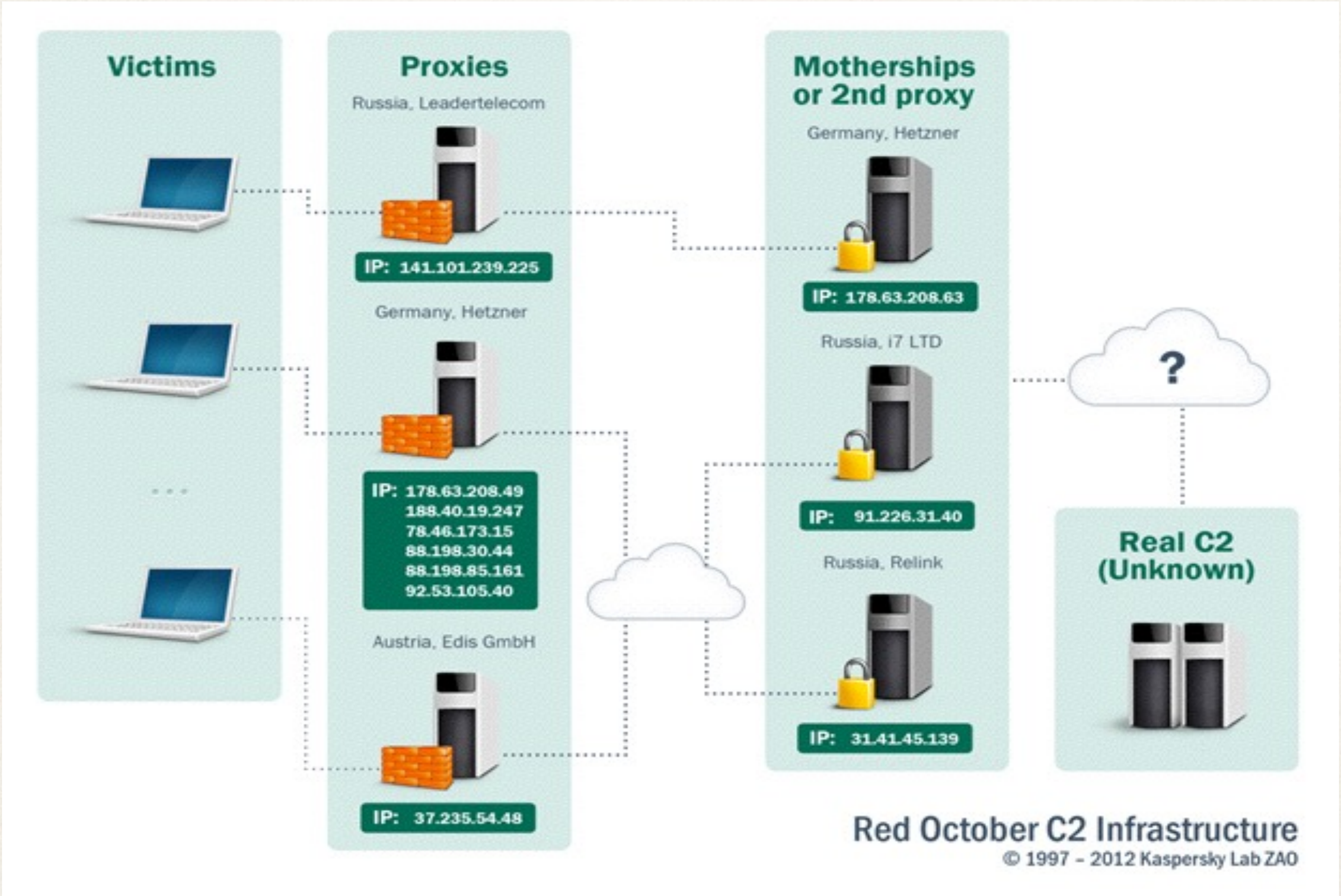
Command and Control

- Requesting the index page of the “mini-motherships” returns the following:

```
<!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

№	Name	Group			Size (Kb)	Summary
1	RegConn	Recon			~160	Query system software environment
2	WnHttp	Recon			~142	Get external IP and send to the C&C
3	SysInfo	Recon			~503	Get browser history,usb drives,processes,disks,...
4	GetWebFtp	Recon			~157	Get browser history,http/ftp credentials
5	AuthInfo	Recon			~660	Get file manager,browser,ftp,mail client credentials
6	Logic	Recon			~160	Get general information about current Windows machine and available remote network shares
7	lLogic	Recon			~150	Grab Internet Explorer URL history from the local system
8	Repeat2	Recon			~150	Get listing from remote shares available in Windows network neighborhood
9	Reference	Recon			~150	Grab directory/file listings of all drives attached to the local system
10	PswSuperMailru	Password			230-260	Steal Mail.ru account info and Outlook attachments
11	PswOutlook	Password			~31	Steal Outlook account info
12	MSHash	Password			400-550	Steal Windows account hashes
13	MAPIClient	Email			418-440	Steal e-mail data using local MAPI
14	POP3Client	Email			1100-1200	Steal e-mail data from POP3 server
15	USBContainer	USB drive			649-690	Loads and runs embedded USBStealer
16	USBRestore	USB drive			372-376	Recover and steal deleted files on USB drives
17	USBStealer	USB drive			448-504	Steal interesting files from USB drives
18	Keylogger	Keyboard			300-312	Makes screenshots, records keystrokes
19	Scheduler	Persistence			~620	Run various tasks from spec folders
20	DocBackdoor	Persistence			75-88	Runs an embedded module from MSOffice/PDF doc
21	OfficeBDInstaller	Persistence			~286	Installs DocBackdoor plugin in MS Office
22	AdobeBDInstaller	Persistence			~218	Installs DocBackdoor plugin in Adobe Reader
23	FilePutExec	Spreading			~305	Extract and run an embedded file locally or remotely
24	Netscan	Spreading			~315	Port scanner, vuln. scanner, Cisco cfg dumper
25	MSExploit	Spreading			~1200	Infect target host using MS08-067 exploit
26	DASvcInstall	Spreading			~276	Infect target host using admin credentials
27	Frog	Spreading			~102	Initial backdoor, used in MSExploit/DASvcInstall
28	iPhone	Mobile			329-331	Steals data from locally attached iPhone
29	Nokia	Mobile			~337	Steals data from locally attached Nokia phone
30	Winmobile	Mobile			~400-700	Infect locally attached Windows Mobile phones with a native backdoor/updater modules
31	Winmobile	Mobile			~7-100	Native mobile backdoor/utilites
32	WnFtpScan	Exfiltration			~209	Steals files from local FTP server
33	GetFileReg	Exfiltration			~340	Steals files from local/network disks
34	FileInfo	Exfiltration			339-340	Uploads various collected files to the C&C

- "online" module: all data is sent to the C&C; no local files created;
- "offline" module; no network communication; all data is stored locally;
- module with embedded script/config in resource named "AAA";
- module with all values hardcoded.

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.

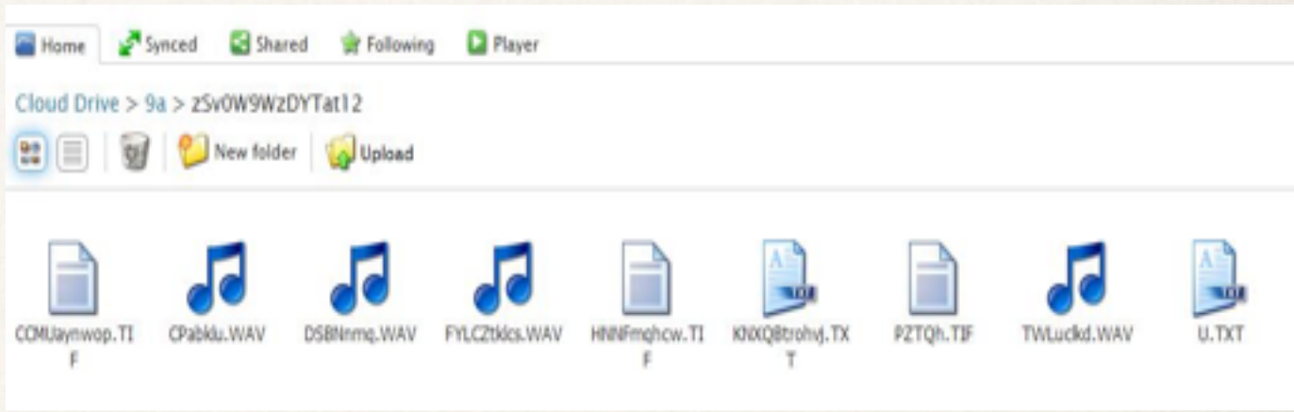
  - Researchers believe the same group may be behind both campaigns, based on similarities in tactics, tools and targets.

C&C Infrastructure

- 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

Cloud Atlas	RedOctober
	

Diplomatic Car for Sale

ChevroletOptra

rice 3500 Euro

Year of manufacture: 2007
Color: silver-metallic
Engine: 109 HP, 1.6 l, Petrol
Transmission: manual
Mileage: 82000 km
Equipment: Air-conditioner, Radio, electric windows, very good condition, new
battery, always serviced in the German Embassy Car Service

The car can be viewed and test driven at the German Embassy. Ulitsa Mosfilmovskaya 56,
119285 Moscow. In order to arrange an appointment please contact Mr. Paul Reschke
Tel.: +7 926 596 4909 (mobile) or +7 495 937 9500 ext. 425
E-Mail: paul.reschke@gmx.de

Diplomatic car for sale

MODEL: Mazda 323- 1998 **DISPLACEMENT:** 1800 cc

TRANSMISSION: Automatic **FUEL:** Benzin

MILEAGE: 145.000 km

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 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

- http://www.bbc.com/news/technology-21013087
- http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide
- https://securelist.com/blog/research/68083/cloud-atlas-redoctober-apt-is-back-in-style/
- https://threatpost.com/red-october-attackers-return-with-cloudatlas-apt-campaign/109806
- https://threatpost.com/inside-1000-red-october-cyberespionage-malware-modules-011713/77419

References

- http://www.tomshardware.com/news/red-october-malware-cloud-atlas,28220.html
- http://appleinsider.com/articles/14/12/11/massive-sophisticated-inception---cloud-atlas-malware-infects-windows-and-android-but-cant-exploit-apples-ios-without-jailbreak
- http://securelist.com/blog/incidents/57645/red-october-part-two-the-modules/
- http://securelist.com/blog/incidents/57647/the-red-october-campaign/
- https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/
- http://www.dailymail.co.uk/sciencetech/article-2263322/Operation-Red-October-revealed-The-astonishing-hacker-attack-infiltrated-55-000-high-level-government-computers.html