RED OCTOBER

Sachin Vasant
Boston University


THE ATTACK
FROM
RED OCTOBER

Introduction

- Large scale cyber-espionage
- Targeted on diplomatic, governmental and research organizations
- Nations in Central Asia, Easter Europe and former members of USSR targeted
- Active since 2007.

Features

- Attacked various governmental agencies.
- Retrieved data used later in other attacks
- Network of command and control (C&C) servers (to control infected nodes). Mothership remains hidden.
- Multi-functional. Extendable feature-set for info-retrieval.
- Affected PCs, phones, n/w equipment, removable hard-drives, etc.

Anatomy

- Two stages of attack:
  - Initial infection:
    - Malicious files sent as emails to targets.
    - Files used existing exploits.
    - Downloads main program to communicate with C&C servers
  - Addition of modules
    - Main program then adds various spy modules.
    - Purpose of modules vary. For eg., modules to infect smartphones, modules for info-retrieval.

Infection phase

- Emails probably sent through:
  - Anonymous mailboxes by public free mailbox providers
  - Mailboxes of infected organizations
- The subject of mails varied with targets.
- Attached files contained the trojan dropper.

Infection phase-Exploits

- Exploit codes for three existing vulnerabilities used:
    - Exploiting Office documents
    - 'Rhino' Java Exploit
- These exploits were already in public domain from previous attacks.
- Only changed the trojan dropper executable from the document.

Infection phase-Vulnerabilities (An Example)

- Excel Featheader Record Memory Corruption CVE-2009-3129:
  - A remote code-execution vulnerability for upto MS Excel-2007 –SP2.
  - Vulnerability exists in the way a few specially crafted Excel docs are parsed (parsing those cause memory corruptions).
  - Exploit the vulnerability, to run any program in the system (with as much rights as the logged in user)

Infection phase-Trojan Dropper

- The trojan dropper extracts 3 files:
  - A batch file MSC.BAT that starts or removes the dropper file
  - A payload file: RC4 encrypted and compressed using zlib
  - A loader (svchost.exe) that decrypts the payload
- The decrypted payload is injected to system memory as a “backdoor” and is responsible for communication with C&C servers.

Infection phase-Communication

- The loader checks if the system is connected to internet. Done by connecting to 3 Microsoft hosts:
  - update.microsoft.com
  - www.microsoft.com
  - support.microsoft.com
- Once connected, loader executes main backdoor component.
- Backdoor components establish encrypted connections (different algos for send and recv)to one of the C&C servers.
- Over 60 registered C&C domains identified .
- 3 such servers hardcoded into the component.

Stage 2- Spy Modules

Once connected, backdoor component can add additional spy modules. These modules are of two types:

- Online: Doesn't exist on local disk. System memory only. No logs maintained on local disk. The results communicated with C&C servers. Used for one time tasks, like stealing saved passwords from browsers, system password, etc.
- Offline: Saved as files on local disks. Has its own registry keys and log files (saved in local disk). May communicate with C&C server. Used for more persistent tasks. One module waits for the connection removable hard-drives, to extract info.

Circumventing C&C takedowns

A module to circumvent C&C server takedowns:

- Exploits Adobe Reader and/or Microsoft Office
- Malicious document sent attached to mail.
- Attached documents don't contain exploit codes.
- When downloaded, module processes the document and starts the associated malicious application.
- For C&C takedowns, the application helps regain access to the infected machines.

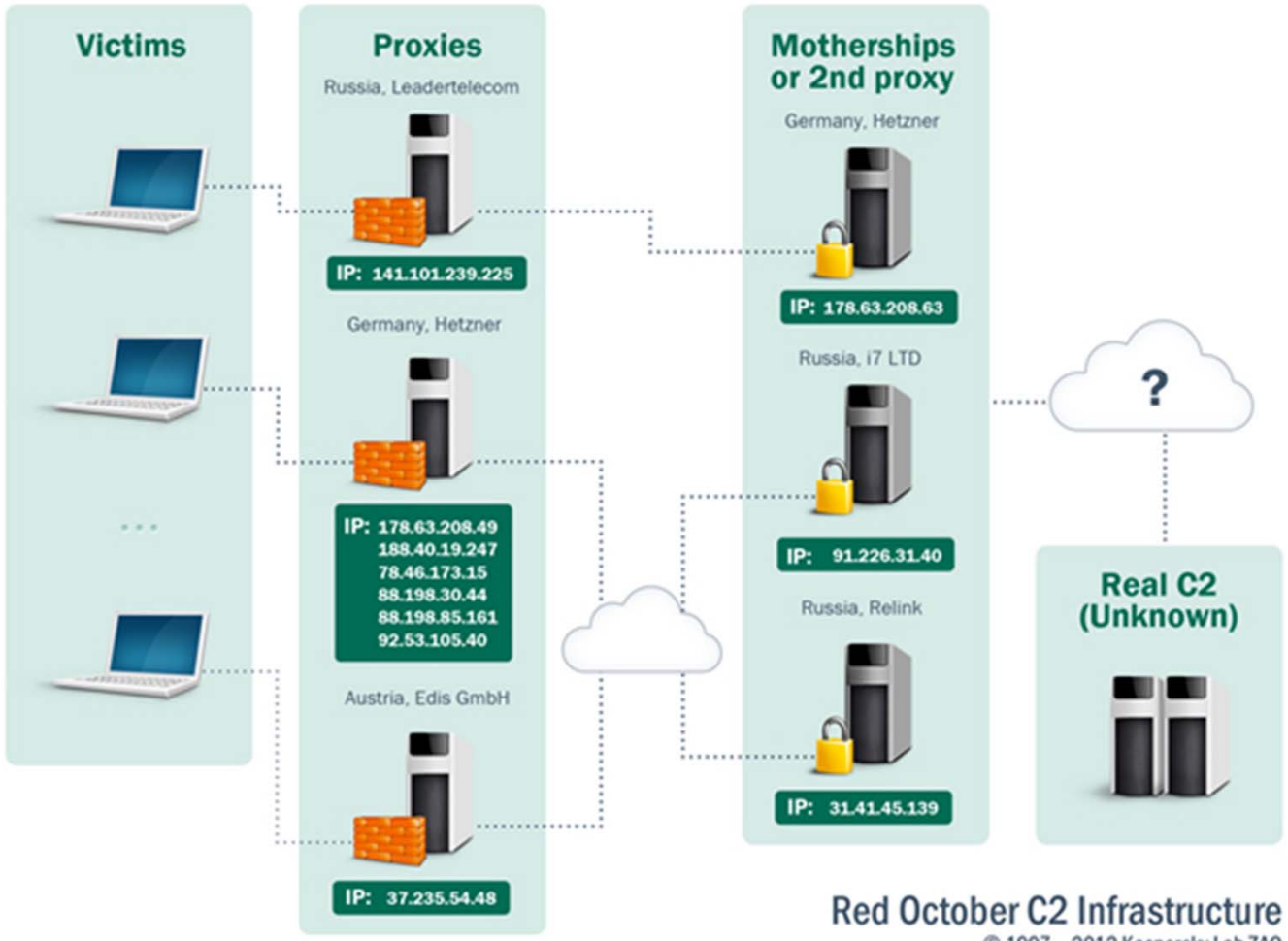
C&C Servers - Kasperky's Investigation

- Uncovered over 60 domains (possibly through their AV network)
- Identified victims using their existing AV network and by sinkholing (a fake DNS server for those URLs) a few of the unregistered malicious domains.
- On monitoring the domains, they observed about 10 servers with “confirmed” “malicious” behaviour.

C&C Servers - Kasperky's Investigation

- On obtaining an image of one of these C&C servers, they found it was merely forwarding to another server on port 40080.
- They scanned the network for servers with the port open, and identified three servers.
- They were able to obtain the index files of these servers.
- Identified that all three of these servers were last modified at the exact same time.
- This leads them to believe the existence of another mothership controlling these servers.

C&C's Suspected Architecture



Red October C2 Infrastructure

Summary – Design Considerations

- Why was it undetected for this long?:
  - Use of already known exploits (thus, even if detected, would be mistaken as an older virus).
  - The self-deletion of trojan dropper.
  - Use of online modules, in case of one-time work. (Again self deleting programs).
  - New modules were dropped no sooner than once in 3 days. Hence, communication with C&C wasn't as frequent. (to hoodwink the Sys Admins)
  - Modules were possibly specific to targets (each target was assigned a specific ID).
  - Use of multiple C&C proxies (tracing malicious communication becomes harder).

Summary – Design Considerations

- Large number of modules. “Swiss army knife of cyber-espionage”.
- Large number of modules → variety of infected devices (mainly done using offline modules).
- Possibly hard to find the mothership. Strength in numbers, and possibly because of the hierarchy.

Thank You!!

References

1. Kaspersky, '*"Red October" Diplomatic Cyber Attacks Investigation*', Url: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation

2. CVE-2009-3129, National Vulnerabilities Database, url: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3129

3. Microsoft Security Bulletin MS09-067 – Important, Microsoft url: http://technet.microsoft.com/en-us/security/bulletin/MS09-067

4. CVE-2010-3333, National Vulnerabilities Database, url: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3333

5. CVE-2012-0158, National Vulnerabilities Database, url: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0158

6. CVE-2011-3544, National Vulnerabilities Database, url: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3544

7. Arstechnia, Why Red October is the Swiss Army knife of Cyber Espionage, url: http://arstechnica.com/security/2013/01/why-red-october-malware-is-the-swiss-army-knife-of-espionage/

Sinkhole (source: Wikipedia)

- An entity in the DNS lookup chain (for ease : think of it as a DNS server).
- Hands out non-routable addresses for the domains in its list.
- Generally used to block the operation of Botnets.
- For our purpose, it only is used to identify the victims (since they'll communicate with this server).