

RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

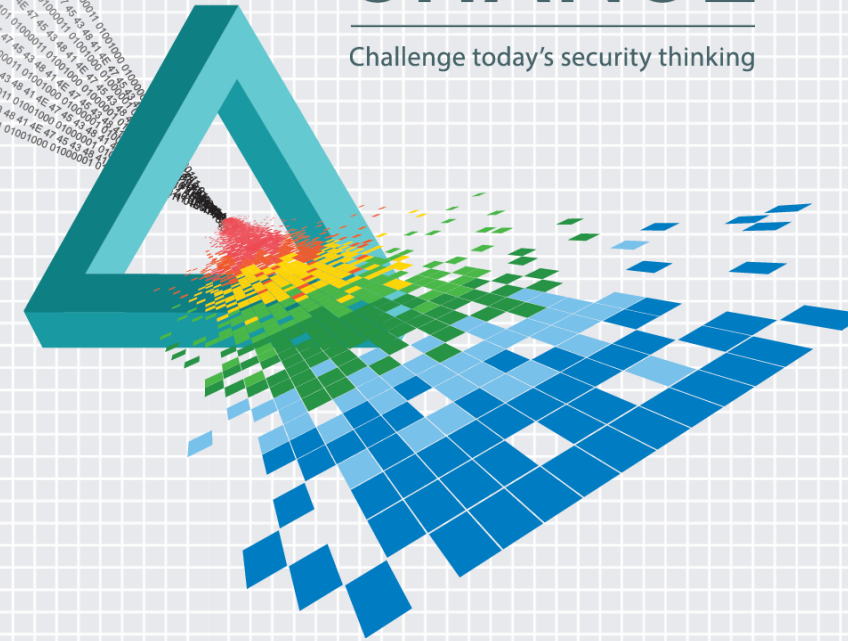
SESSION ID: EXP-T07

Hacking Exposed: LIVE Next Generation Threats

a.k.a. “Sophisticated” Attacks

CHANGE

Challenge today's security thinking

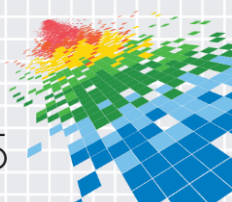


Stuart McClure and Brian Wallace

CEO and Sr. Researcher
Cylance, Inc

The Biggest Myth Running

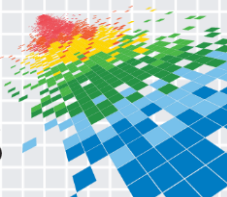
- ◆ “It’s all new and sophisticated, advanced”
- ◆ “Defenders Dilemma”
- ◆ “60% of all attacks don’t use malware”
 - ◆ We define malware as “malicious software” or anything that can run on an endpoint and do bad things. This includes scripts, interpreted code, PEs, DLLs, admin tools, PuPs, etc.
 - ◆ Authentication based and insider threat attacks? Yes but small percentage and only one step in the chain.
 - ◆ Complete in-memory attacks? Yes but small percentage and only one step in the chain.
- ◆ Prevention is not truly possible
- ◆ But let’s see what this means...



Agenda

- ◆ *Act 0: Destover/Wiper (setup)*
- ◆ *Act I: Operation Cleaver: LIVE*
- ◆ *Act II: Forever-days: LIVE*
- ◆ *Act III: Destover/Wiper: LIVE (grand finale)*

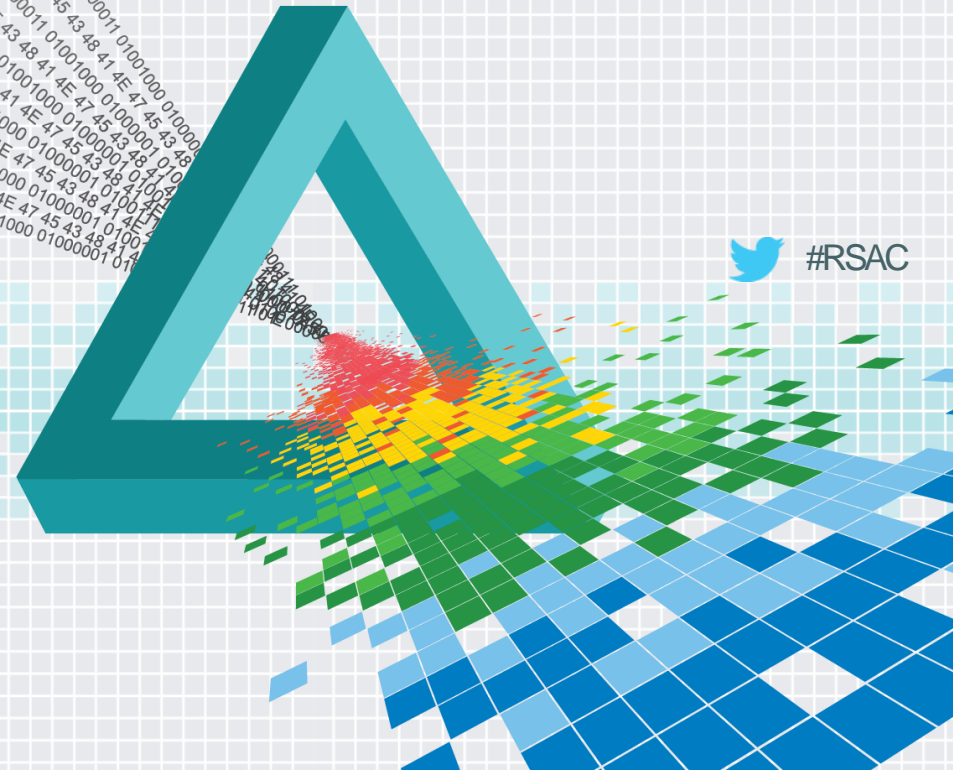
Throughout: Mitigations and Prevention



RSAConference2015

San Francisco | April 20-24 | Moscone Center

Act 0: Sony Attack *Setting the stage...*

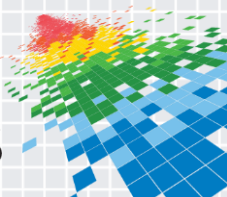


Wiper:

201a9c5fe6a8ae0d1c4312d07ef2066e5991b1462b68f102154bb9cb25bf59f9

Sleep(2700000) =
45minutes

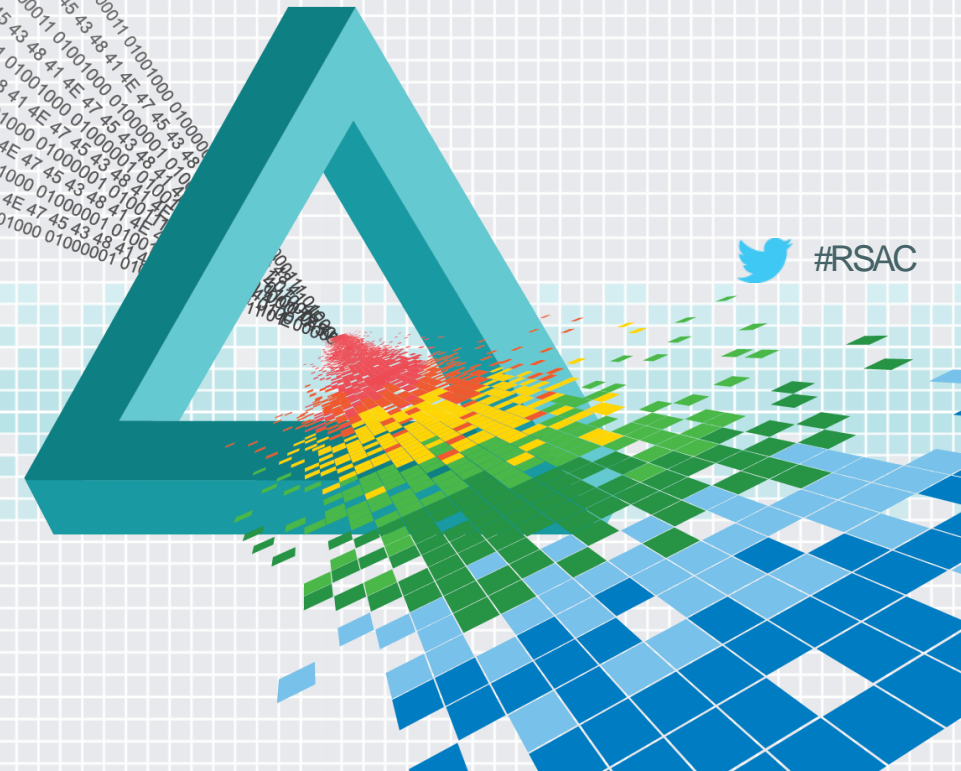
Ladies and Gentlemen, start your malware...



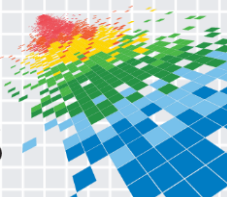
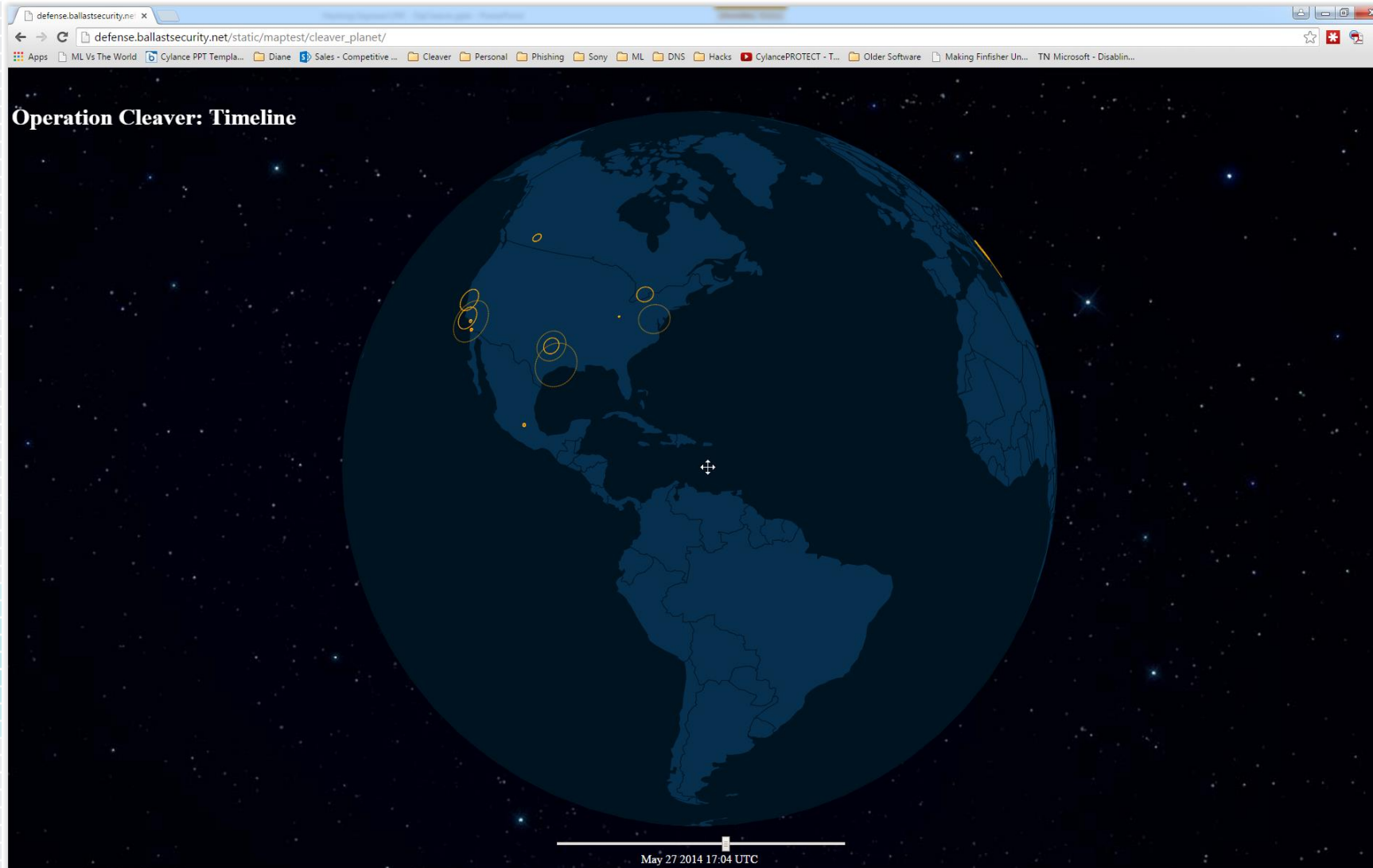
RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Act I – Scene I: Operation Cleaver *Global Impact*



http://defense.ballastsecurity.net/static/cleaver_planet/



OPERATION CLEAVER

- ◆ Rapid Growth of Skilled Hacking Starting 2012, **2010...2007**
- ◆ Targets: **Global Critical Infrastructure**
- ◆ Campaign Phase 1: **Initial Compromise**
- ◆ Campaign Phase 2: **Data Exfiltration and Persistence**
- ◆ Campaign Phase 3: TBD - **Sabotage???**
- ◆ Critical Discoveries:
 - ◆ Sources emanating from Iranian netblocks
 - ◆ **Tarh Andishan**, Zhoupin Exploit Team, **Operation Cleaver**
 - ◆ **Netafraz.com** Hosting (Esrahan, Iran)
 - ◆ Tools created to check for **Iranian IPs**
 - ◆ Malware named: **TinyZbot**
 - ◆ 50+ Victims Worldwide, 2 years+



SOURCING

Attribution back to Iran

GeoIP Location: Iran

Net block: 78.109.194.96 - 78.109.194.127

Owner: Tarh Andishan

Email: tarh.andishan(at)yahoo.com

Phone: +98-21-22496658

NIC-Handle: TAR1973-RIPE

Tarh Andishan – meaning “Innovators”, “Inventors”

78.109.194.96/27 – Current – Afranet, Iran

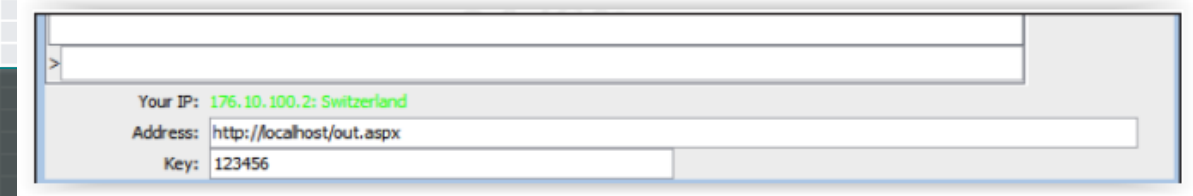
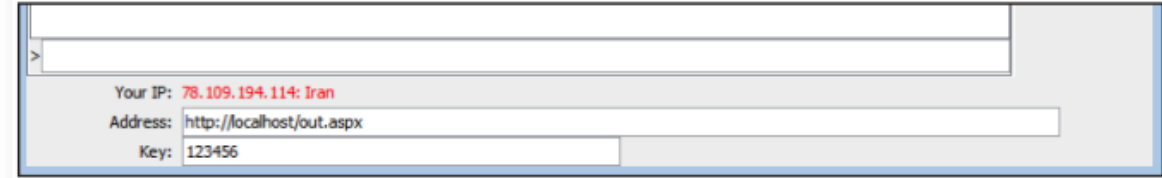
217.11.17.96/28 - 10/22/2014 – Afranet, Iran

81.90.144.104/29 - 10/5/2014 – Afranet, Middle East Oil, Iran

31.47.35.0/24 – 11/2012 – Afranet, Iran

Netafraz.com infrastructure in Iran

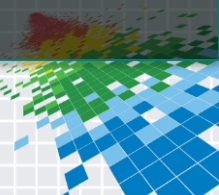
Persian hacker names: **Salman Ghazikhani, Bahman Mohebbi, Kaj, Parviz, Alireza**, etc.



The logger module binary's file description value is the following:
ye file khube DG. ba in ham kari nadashte bashin

Roughly translated from Persian, this text says:
DG is a good file, don't bother with this

**Starting Nmap 6.25 at 2012-08-17
09:18 Iran Daylight Time**

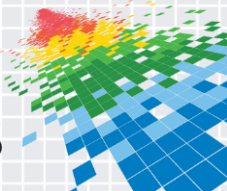


-
- The screenshot displays the Microsoft Forefront Threat Management Gateway 2010 (TMG) web interface. On the left is a navigation pane with options like Dashboard, Monitoring, Firewall Policy, Web Access Policy, E-Mail Policy, Intrusion Prevention System, Remote Access Policy (VPN), Networking, System, Logs & Reports, Update Center, and Troubleshooting. The main area is titled 'Reporting' and shows a table of log records. The selected record is highlighted in blue.
- | Log Time | Client IP | Destination IP | Destin... | Protocol | Action | NIS Scan Result | NIS ! |
|---------------------|---------------|----------------|-----------|----------|----------|-----------------|-------|
| 3/6/2013 9:19:25 AM | 10.100.178.13 | 10.1.40.77 | 443 | https | Allow... | Inspected | |
| 3/6/2013 9:19:25 AM | 10.100.178.13 | 10.1.40.77 | 443 | https | Allow... | Inspected | |
| 3/6/2013 9:19:26 AM | 10.100.178.13 | 10.1.40.77 | 443 | https | Allow... | Inspected | |
| 3/6/2013 9:19:26 AM | 10.100.178.13 | 10.1.40.77 | 443 | https | Allow... | Inspected | |
| 3/6/2013 9:19:29 AM | 10.100.178.13 | 10.1.40.77 | 443 | https | Allow... | Inspected | |
| 3/6/2013 9:19:30 AM | 10.100.178.13 | 10.1.40.77 | 443 | https | Allow... | Inspected | |
| 3/6/2013 9:19:30 AM | 10.100.178.13 | 10.1.40.77 | 443 | https | Allow... | Inspected | |
- Below the table, a detailed view of the selected log record is shown:
- Allowed Connection**
Log type: Web Proxy (Reverse)
Status: 200 OK
Rule: RDWeb RPC
- At the bottom, a network packet capture (PCAP) viewer shows details for a connection from 10.100.178.13 to 10.1.40.77 on port 443. The packet is identified as a Local Host (Microsoft) GET request for a folder.png file. The status is 200 OK. The viewer also shows the raw packet data in hexadecimal and ASCII.

The screenshot displays the Windows Server 2012 Remote Desktop Services Overview page. The main content area shows a deployment overview diagram for the RD Connection Broker server MCRDAP. The diagram illustrates the following components and their connections:

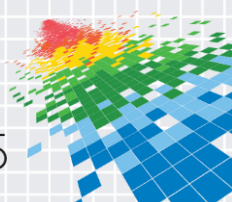
- RD Web Access** (represented by a globe icon) connects to the **RD Connection Broker**.
- RD Gateway** (represented by a green plus icon) connects to the **RD Connection Broker**.
- RD Licensing** (represented by a green plus icon) connects to the **RD Connection Broker**.
- The **RD Connection Broker** (represented by a gear icon) connects to both the **RD Virtualization Host** and the **RD Session Host**.
- The **RD Virtualization Host** (represented by a speech bubble icon) is connected to the **RD Session Host**.
- The **RD Session Host** (represented by a server rack icon) is highlighted with a blue box and has a "Refresh" button below it.

The right sidebar shows the deployment overview details, including the server name MCRDAP and the role RD Connection Broker. The "Refresh" button is also visible in the top right corner of the main content area.



CONCLUSIONS & SPECULATIONS

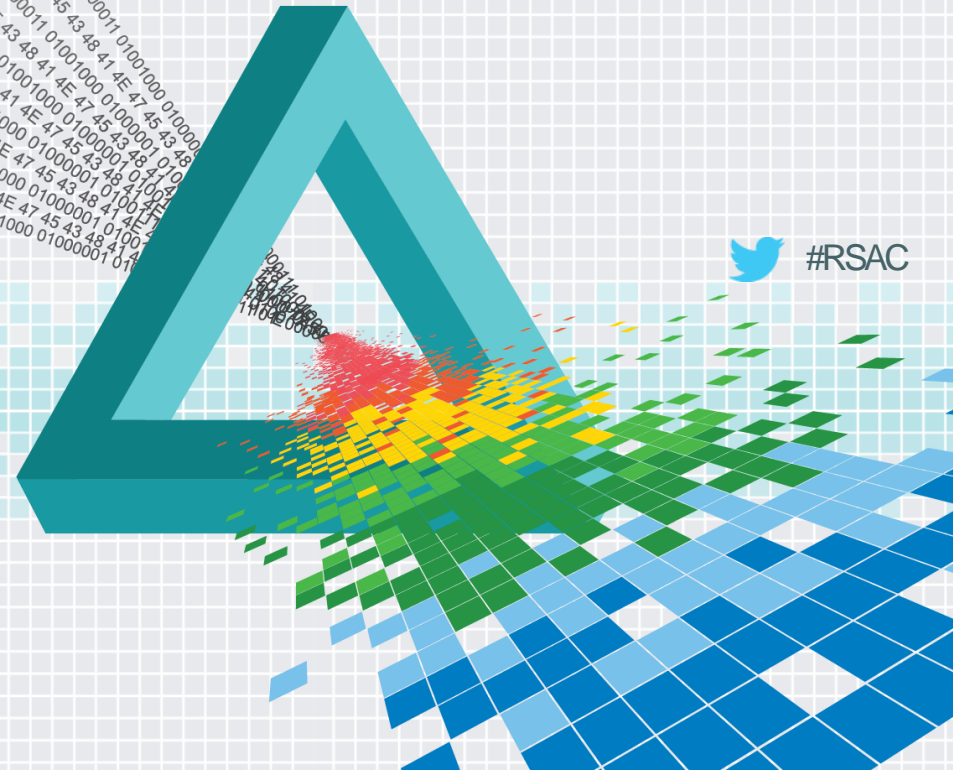
- ◆ Iran's technical capabilities **evolving quickly**, gained momentum after Stuxnet
- ◆ **Targeting Critical Infrastructure**, espionage leading to sabotage – at a minimum terroristic (no other obvious gain)
- ◆ The sheer breadth and depth of targeting, the repeated sourcing infrastructure, the consistent techniques, tools and tactics used, all lead us to a narrow conclusion: that **Iran is actively involved in and executing attacks against global critical infrastructure in an effort to negatively impact our physical world.**



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Act I – Scene II: Operation Cleaver *It's All About the Malware*



TTPs

Spearphishing: fake resume tool



TTPs

Spearphishing: Resume Submitter

Resume Submission Form

Contact Information

Job Objective

Education

Work Experience

Skills List

Submission

First Name :

E-Mail Address :

Phone Number :

Country :

State :

City :

Street :

Number :

Resume Submission Form

Contact Information

Job Objective

Education

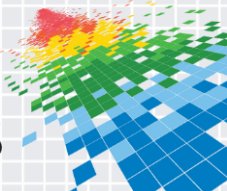
Work Experience

Skills List

Submission

UPLOAD PROGRESS

Submit



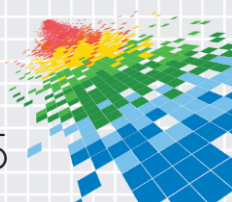
ESCALATION & PIVOTING

Tools & Toys ...

Public: Netcat, Cain & Abel, psexec, **Mimikatz**, WCE, Putty, Plink, nmap, xcmd, etc.

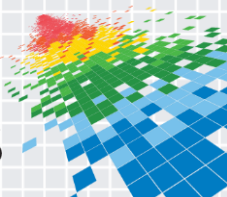
Custom: **TinyZbot**, NetC, ASPX **webshells**, SYN flooder, ARP poisoning, Csext, etc.

Exploits: MS08-067 (Conficker) and MS10-015 (KiTrap0D)



Hack Demo

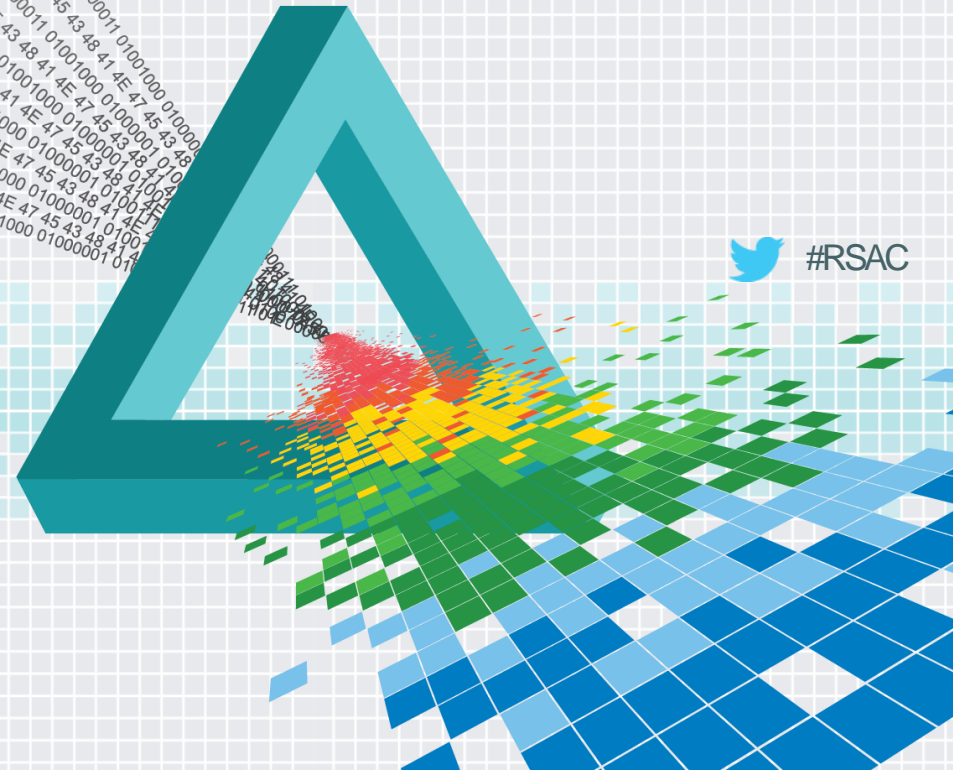
How they worked...



RSA[®]Conference2015

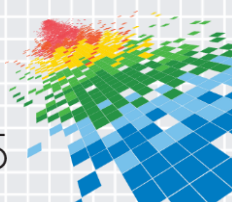
San Francisco | April 20-24 | Moscone Center

Act II – Scene I:
Forever-Days - SMB
a.k.a. “Beyond Malware”



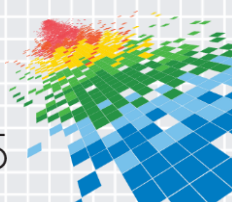
Scene I: SMB Credential Hoovering

- ◆ Discovered by Aaron Spangler in 1997
- ◆ Design flaw in Microsoft – it's a feature!!!
- ◆ The difference?
 - ◆ No need to send a file:// directive to trigger the SMB
- ◆ URLMon.dll
 - ◆ URLDownloadToFile
 - ◆ URLDownloadToCacheFile
 - ◆ URLOpenStream
 - ◆ URLOpenBlockingStream
- ◆ Embedded versions of Internet Explorer



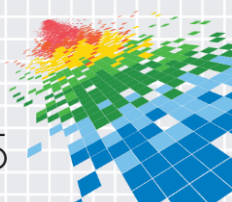
Countless Products Vulnerable

- ◆ Adobe Reader
- ◆ Internet Explorer
- ◆ Lunascape 6
- ◆ Arora Browser
- ◆ Windows Media Player
- ◆ Apple Software Update
- ◆ Microsoft Baseline Security Analyzer (MBSA)
- ◆ AVG Free
- ◆ Norton Security Scan
- ◆ BitDefender Free
- ◆ Comodo Antivirus
- ◆ Free Download Manager
- ◆ KMPlayer
- ◆ Github for Windows
- ◆ TeamViewer
- ◆ SketchUp Make 2014
- ◆ Maltego CE
- ◆ PyCharm
- ◆ PHP Storm
- ◆ RubyMine
- ◆ IntelliJ IDEA
- ◆ JDK 8u31
- ◆ GoPro Studio
- ◆ NetBeans
- ◆ .Net Reflector
- ◆ FBCIM
- ◆ Box Sync
- ◆ SMPlayer
- ◆ Seafile Client for Windows
- ◆ Excel 2010



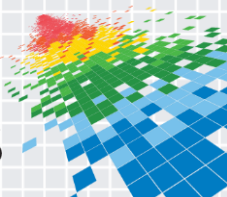
SMB Attack Demo

- ◆ ARP poisoning
- ◆ Launch re-direct SMB
- ◆ Crack credentials
- ◆ RDP or psexec to connect back to victim



SMB Credential Hoovering Attack Demo

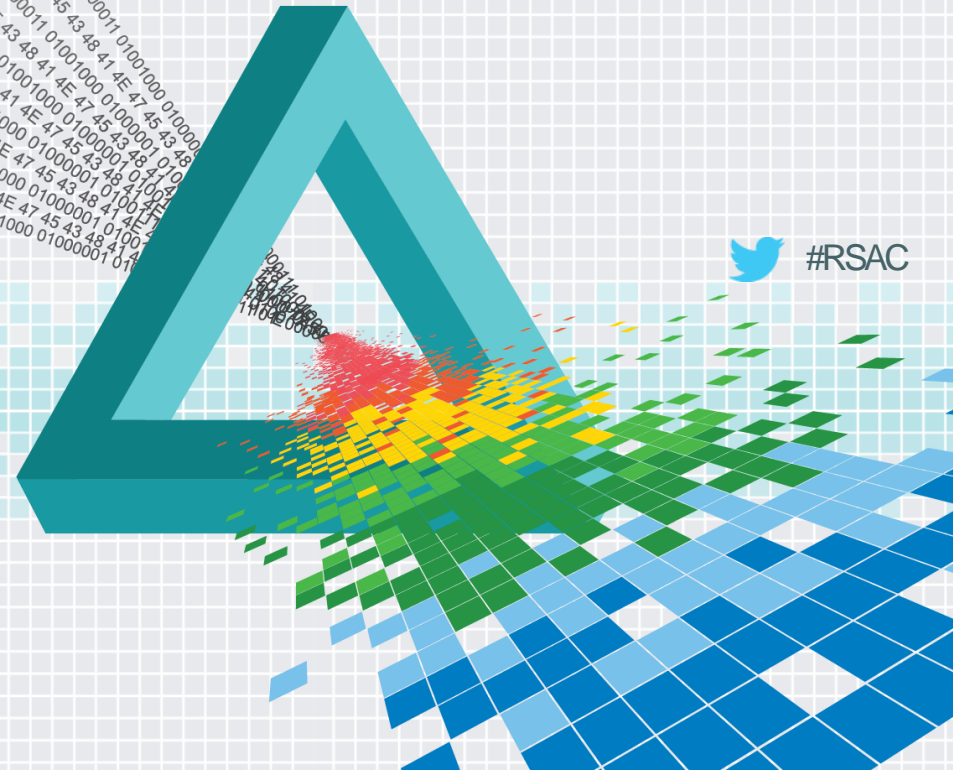
Beyond Malware



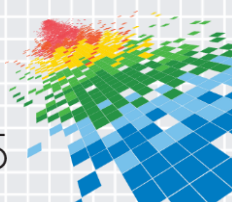
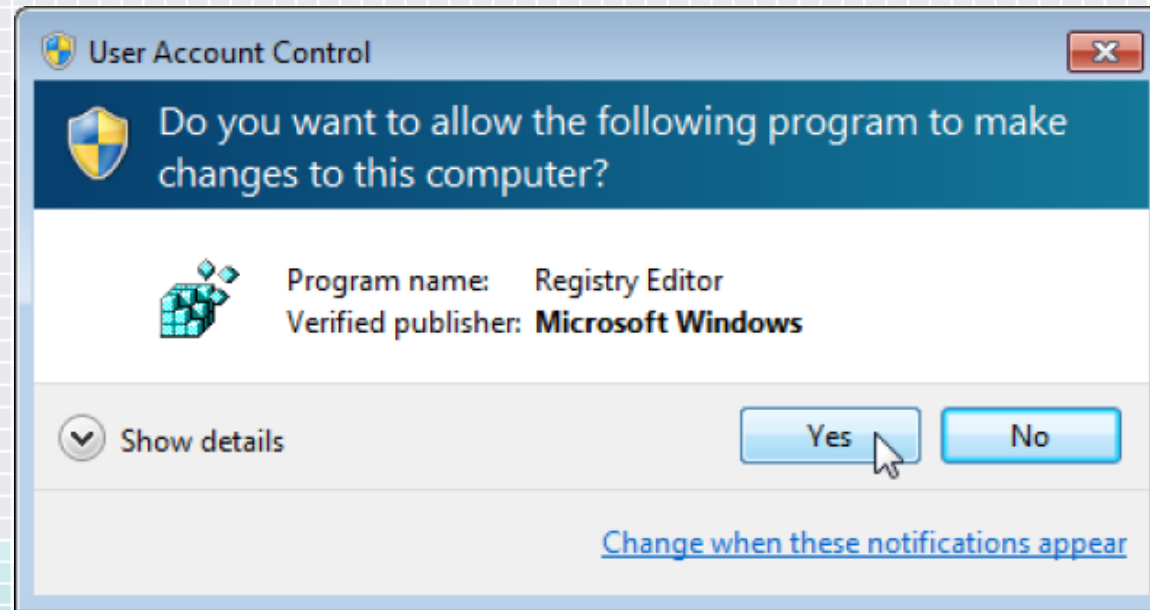
RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

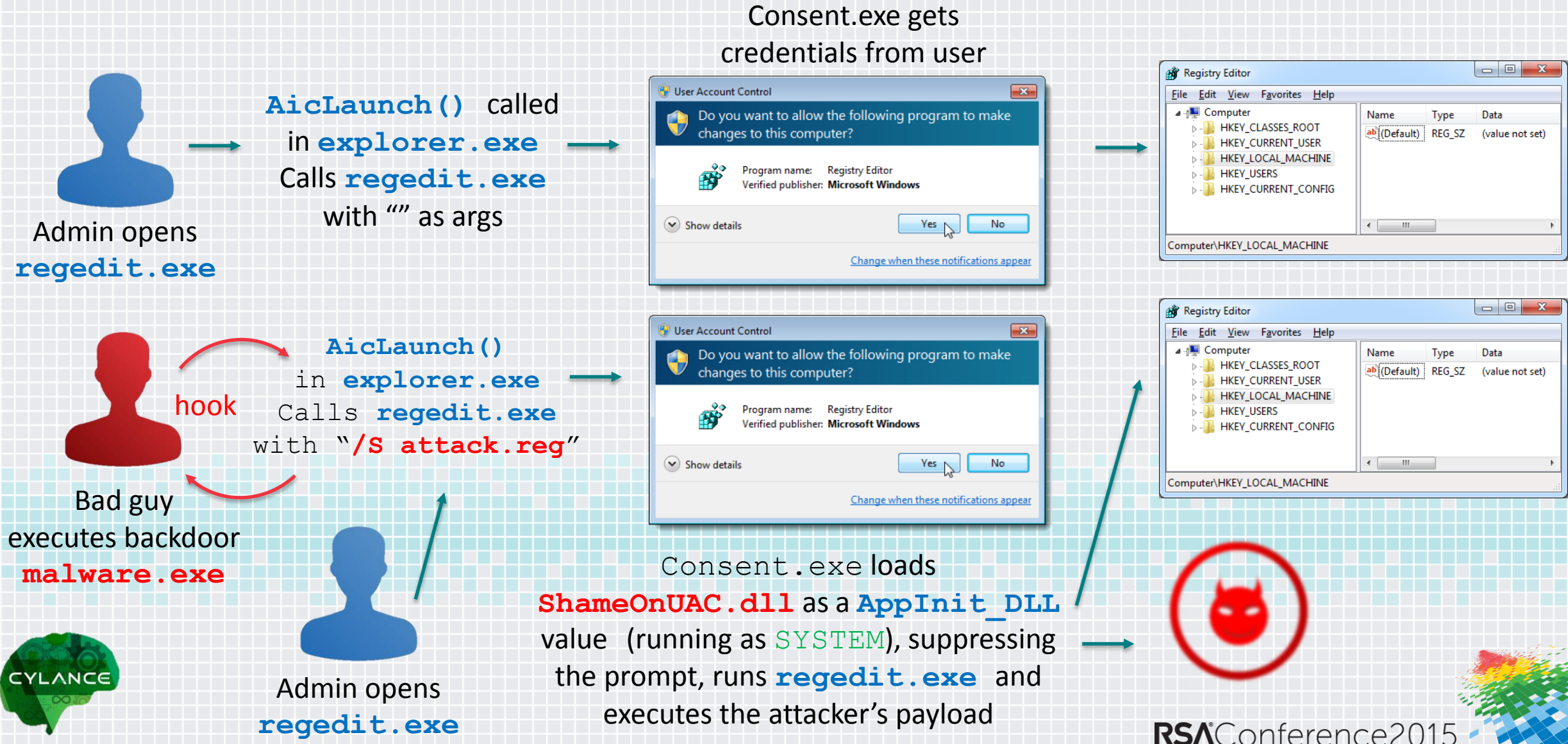
Act II – Scene II: Forever Days – ShameOnUAC *a.k.a. – “Beyond Malware”*



UAC – User Account Control

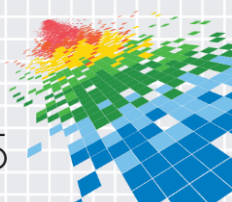


ShameOnUAC



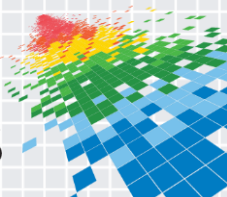
“Beyond Malware”

- ◆ Run ShameOnUAC backdoor
- ◆ Trigger UAC on victim
- ◆ Cached credential dumping = keys to the kingdom!!!
- ◆ Connect back
- ◆ Game is over...



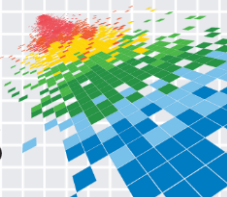
ShameOnUAC Attack Demo

Beyond Malware



ShameOnUAC Mitigations

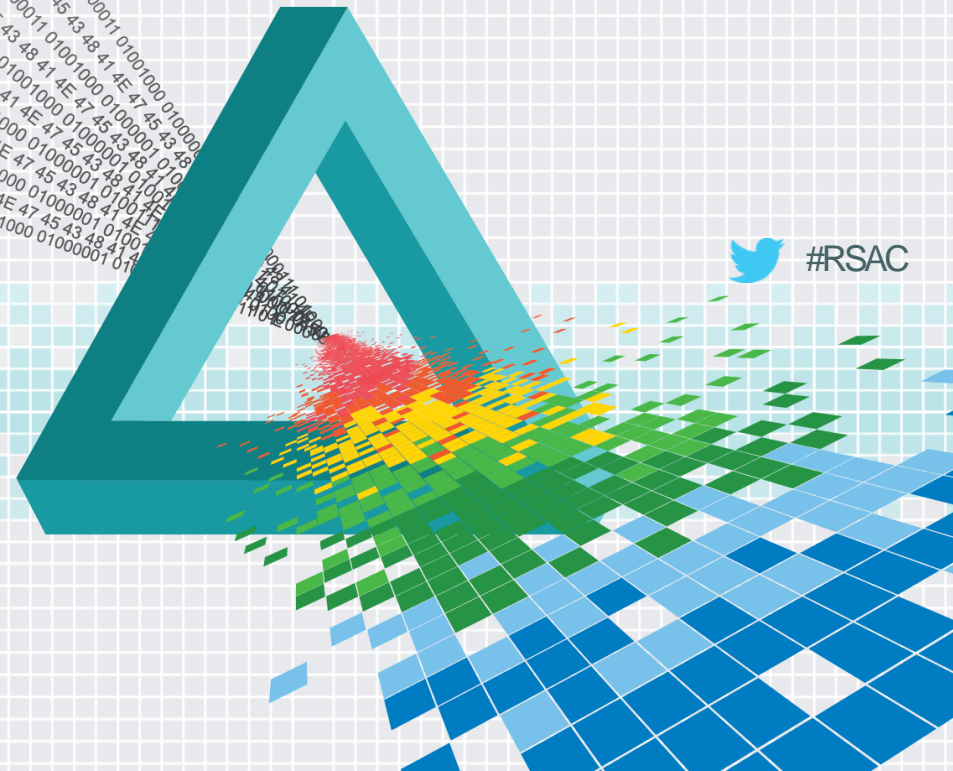
- ◆ None really.
- ◆ It's a feature!



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Act III – Sony Attack *“Hacking Exposed” style*



Sony Speculation

- ◆ Spearphishing
- ◆ Credential Harvesting
- ◆ Remote access
- ◆ Launch leveraging harvested credentials



--Warninig--

We've already warned you, and this is just a beginning.

We continue till our request be met.

We've obtained all your internal data including your secrets and top secrets.

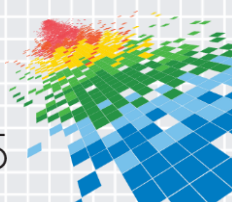
If you don't obey us, we'll release data shown below to the world.

Determine what will you do till November the 24th, 11:00 PM(GMT).

Post an email address and the following sentence on your twitter and facebook,
and we'll contact the email address.

!°Thanks a lot to Godi'sApstls contributing your great effort to peace of the world.i±
And even if you just try to seek out who we are, all of your data will be released at once.

Best Regards



Spearphishing

Normal Mail View Hex View Properties View Message Header

From : Apple <no-reply@apple.com>
To :
Cc :
Bcc :
Subject : [Verify your Apple ID](#)
Attachments :

From : iCloud ID <apple@ioscareteam.com> **Date Time** : 9/18/2014 11:18:38 PM

To : [REDACTED]
Cc :
Bcc :
Subject : Your iCloud Account Under Review
Attachments :

PayPal™

Login attempt from unknown device.

a little while ago to ask for your help
 e with your account

blem?

n on your account appears to be missing or incorrect.

Date Time : 9/18/2014 11:18:38 PM

: iCloud ID <apple@ioscareteam.com>

[REDACTED]

:

:

: Your iCloud Account Under Review

For more information, see
 Thanks,
 Apple Customer Support

How to certify my AppleID and remove the suspension?
 Just proceed to the highlighted URL below to validate your iCloud/Apple ID. Log-in
 in using your Apple/iCloud login and password, then follow the prompts.

[>Certify My Apple/iCloud ID](#)

While using Apple devices and services, you'll still login with your main email
 address as your Apple ID.

If you have queries and want help, visit the AppleID Care website.

Untitled - Notepad

File Edit Format View Help

http://tercumburosu.info.tr/tercume/wp-cor


Untitled - Notepad

File Edit Format View Help

http://ioscareteam.net/account/?email=[REDACTED]@spe.sony.com

ty page c

<http://update.information.elitesparadise.com/>





Spearphishing

Lookup the Hosting History of a Domain

IP Address History

Event Date	Action	Pre-Action IP	Post-Action IP
2014-09-11	New	-none-	85.233.160.22
2014-10-02	Not Resolvable	85.233.160.22	-none-

Note: The current IP location and IP Whois may not be the same as it was on the event date.

Registrar History

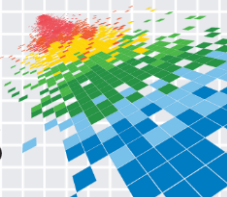
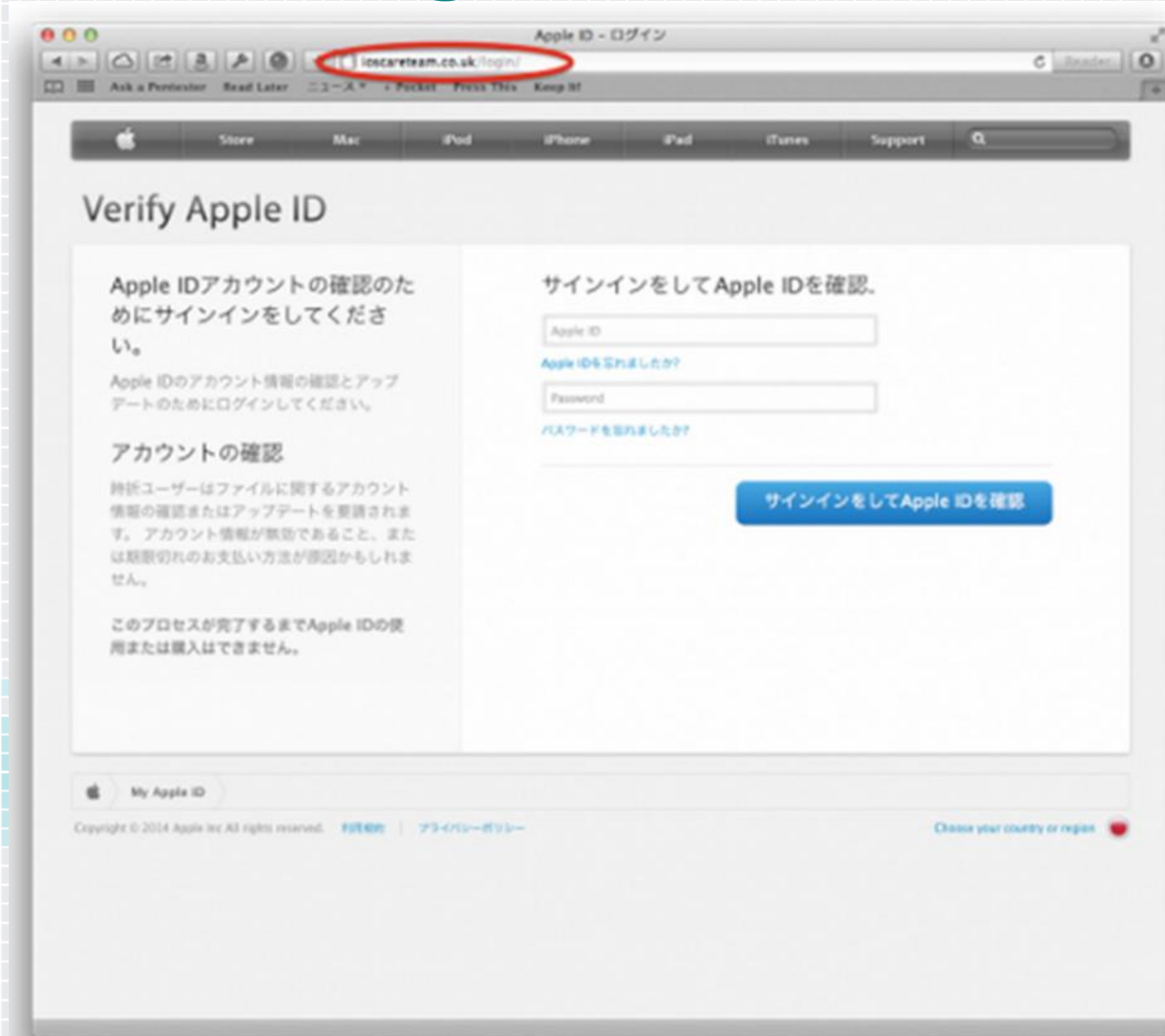
Date	Registrar
2014-09-19	Register.it SPA

Name Server History

Event Date	Action	Pre-Action Server	Post-Action Server
2014-09-11	New	-none-	Phase8.net
2014-09-20	Delete	Phase8.net	-none-
2014-12-19	New	-none-	123-reg.co.uk
2014-12-20	Delete	123-reg.co.uk	-none-

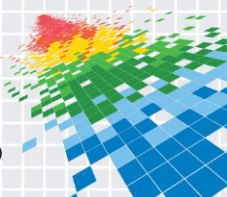


Credential Harvesting



Remote Access

- ◆ VPN
- ◆ RDP
- ◆ Remote mail

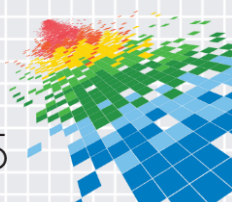


Launching

- ◆ First hand accounts
 - ◆ “Someone on the IT team screwed up and ran something wrong.”
 - ◆ “Some people think it was someone from the inside”

SCCM 2007 Central Administration Site in Chandler - ACT (Chris Monti)

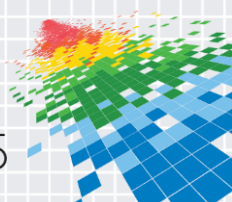
- ◆ SCCM distribution
 - ◆ Looked like an insider
 - ◆ Easy distribution to everything!
 - ◆ Would take weeks to figure it out.



Behavior

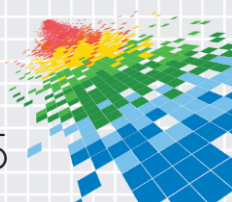
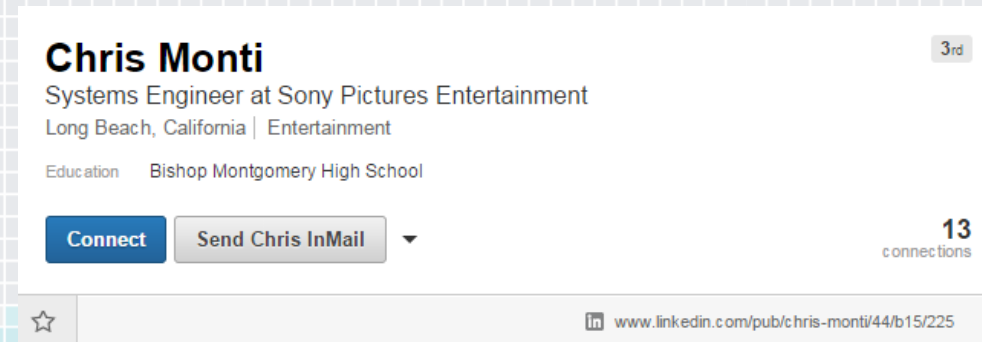
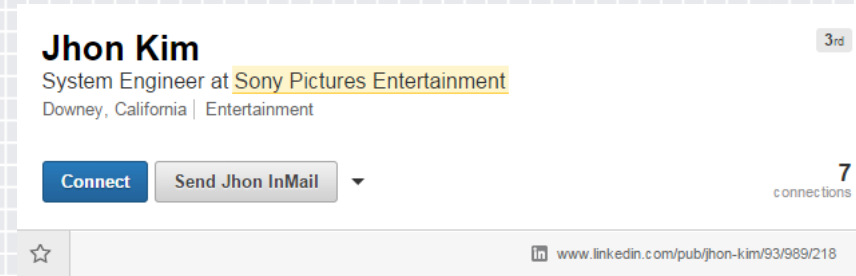
2618dd3e5c59ca851f03df12c0cab3b8 diskpartmg16.exe
. b80aa583591eaf758fd95ab4ea7afe39 igfxtrayex.exe
. 6aeac618e29980b69721158044c2e544 elrawdsk.sys
. 86e212b7fc20fc406c692400294073ff elrawdsk64.sys
. 612ae17dcac2248503d3b935f70a6838 (BMP) walls.bmp
. 7e5fee143fb44fdb0d24a1d32b2bd4bb ams.exe
. cc79a406d1a6c3d187319e8afb9a2901 kph.sys (kprocesshacker.sys)
. 844440e88f482c0b03f31cd7e1f9590d (TXT, long credentials/hosts list)

d1c27ee7ce18675974edf42d4eea25c6 diskpartmg16.exe
. 760c35a80d758f032d02cf4db12d3e55 igfxtrayex.exe
. 6aeac618e29980b69721158044c2e544 elrawdsk.sys
. 86e212b7fc20fc406c692400294073ff elrawdsk64.sys
. e1864a55d5ccb76af4bf7a0ae16279ba iissvr.exe
. 3a6bd9a5aa6eb760ec90df03499a5cb3 (HTML)
. 84942918a6c2da814b3c086bfbbd5987 (JPEG) back.jpg
. 942e076776e31a5646efe032b3f0c7e5 (WAV) index.wav
. 3769626c4734d5de074d7c9b53f66c15 (TXT, short
credentials/hosts list)



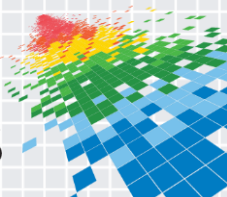
Credentials

- ◆ spe\jhkim-1|DE\$Ktop12
- ◆ spe\dhenderson-1|(Ba773l35)
- ◆ SPE\cmonti-1|Minion#1 -- SCCM administrator?
- ◆ SPE\Dayals-1|London13!
- ◆ SPE\JHKim4-1|!Tomorrow33
- ◆ SPE\KManku-1|M@nday77
- ◆ SPE\MMcLean3-1|@Smiley91
- ◆ SPE\ADutta2-1|P@ssw0rd123



Sleep(2700000) =

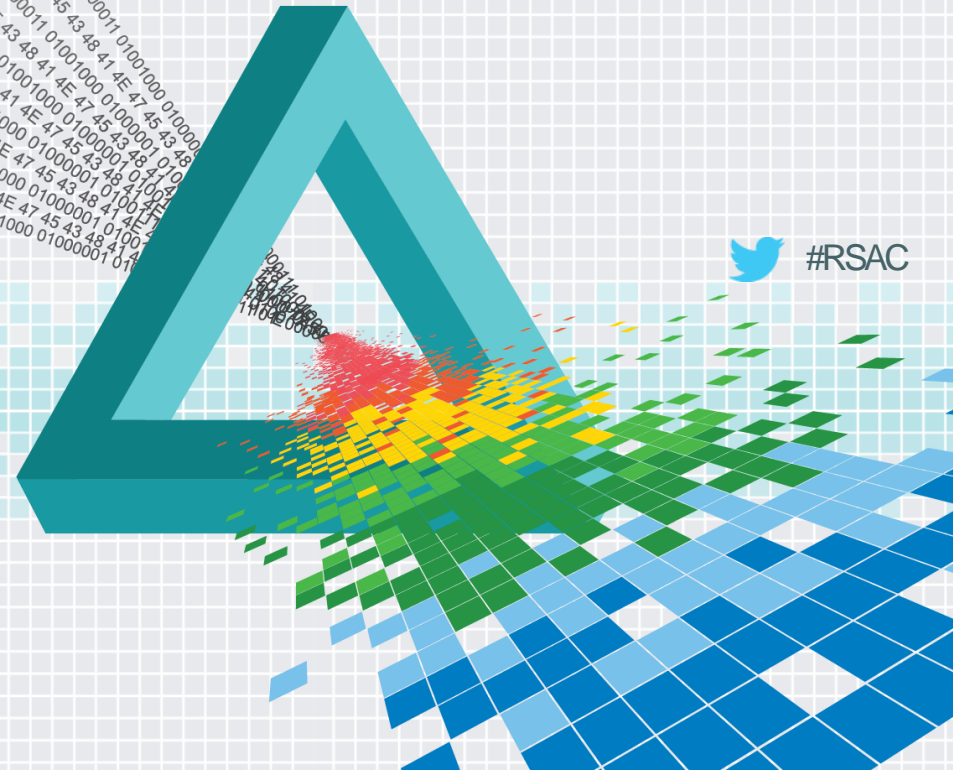
45minutes now?
Let's check on it!



RSA[®]Conference2015

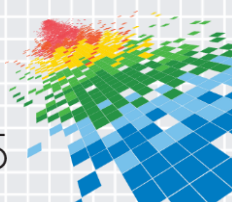
San Francisco | April 20-24 | Moscone Center

Destover/Wiper Malware LIVE demo



Mitigation

0. Protect your endpoints!
1. Success auditing of domain administrator logins, and failure auditing of all logins.
2. Central collection of Service Control Manager Event 7045 ("A service was installed in the system"). Catches kernel mode driver service creations too.
3. Prevent remote service creation (would also stop PsExec), and prevent process launch via remote WMI.
4. Use modern versions of Windows and make use of their security controls (UAC), grant domain admin only sparingly, and disable default shares and cached credentials whenever possible.
5. Protect your passwords! 2FA, One Time Passwords, CyberArk, KeyPass, LastPass*, etc.



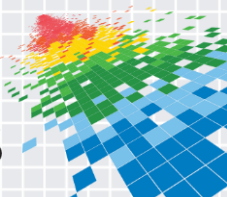
Bonus Demo?

How could any victim could have been protected?

Do we have time?

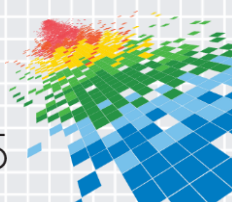
Yes, we've cracked the code!

If no time then go to the Cylance Booth or
Come to Children's Creativity Museum @ 5pm



Resources

- ◆ Cylance on Youtube (Cylance Inc)
- ◆ Cylance on Twitter (CylanceInc)
- ◆ “Hacking Exposed” on Twitter (@hackingexposed)
- ◆ www.cylance.com
- ◆ Come to our booth!
- ◆ Come to our VIP party @ 5pm @ Children’s Creativity Museum!
 - ◆ Tell them we invited you at the Hacking Exposed LIVE talk.



Thank you!

Reminder to submit your feedback!

