Advanced Persistent Validations to counter Advanced Persistent Threats

用高级持续的验证去应对高级持续的攻击威胁

Speaker：Amritam Putatunda

Position：Product Manager – Apps and Security

Date：2014/09/25

ISC 2014
中国互联网安全大会

360互联网安全中心

China Internet Security Conference 2014
2014中国互联网安全大会

Todays **IT CHALLENGES 今天IT面临的挑战**

More devices

Connecting from more places

Accessing more data

From more sources

salesforce
You Tube
hadoop
Google App Engine
amazon webservices

…and now its all moving

..and you can see less of it

And attacks continue to rise

And your users want it all now

And it has to be fast

And it has to work over wireless..always

The Planet of the Apps
"The internet is changing"

互联网是一个充满应用的世界，并且应用在时时变化

- Millions of different Apps with new one cropping up each day.
- Every other organization is adopting BYOD
- Applications access data differently
- Security implications magnify with attacks hidden within apps.

Mobile Malware -The fastest growing type of malware.

移动终端的恶意软件是增长最快的恶意软件类型

How does it change the threat landscape

- Millions of phones/tablets/PC’s accessing Data
- Until now Malware’s were still at the stage of Phishing, scamming.
- Expected to grow exponentially with Apps.
- OS security models are beginning to break.
- “**UI State Inference and Novel Android Attacks**”

Attackers becoming vicious each passing day

攻击者在过去的每一个天都在变化：形式更多样，更具威胁

- DDoS
- Malware
- APTs
- Botnets

TARGET

CLOUDFLARE.

JPMorganChase

Adobe

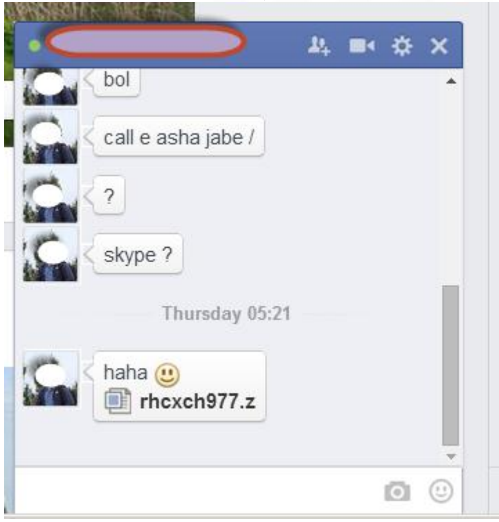
The New York Times

ADVANCED PERSISTENT THREAT – Propagation
APT的工作方式-传播

Porousness and inherent vulnerabilities in devices magnifying the viciousness of APTs

Infections through Social Media

通过社交媒体感染传播


[redacted]

bol

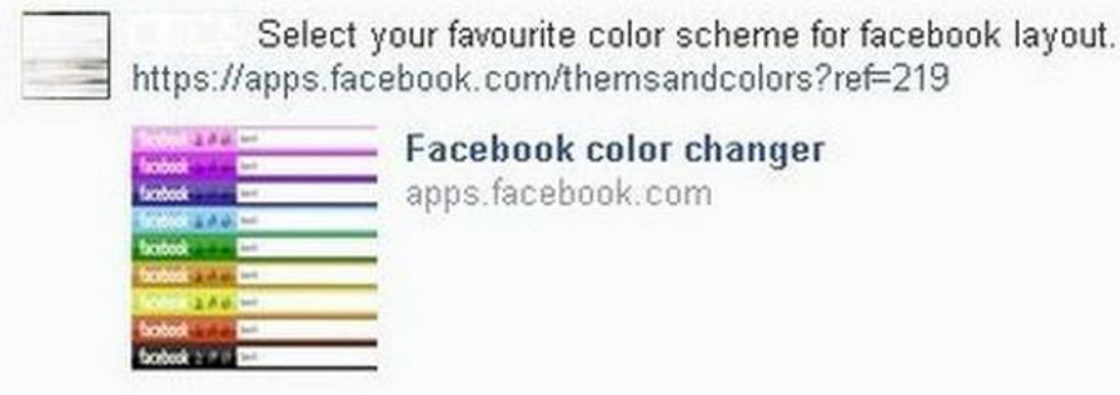
call e asha jabe /

?

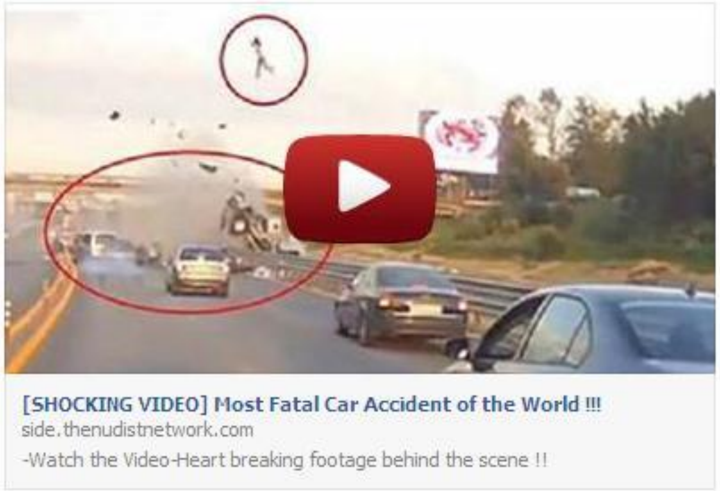
skype ?

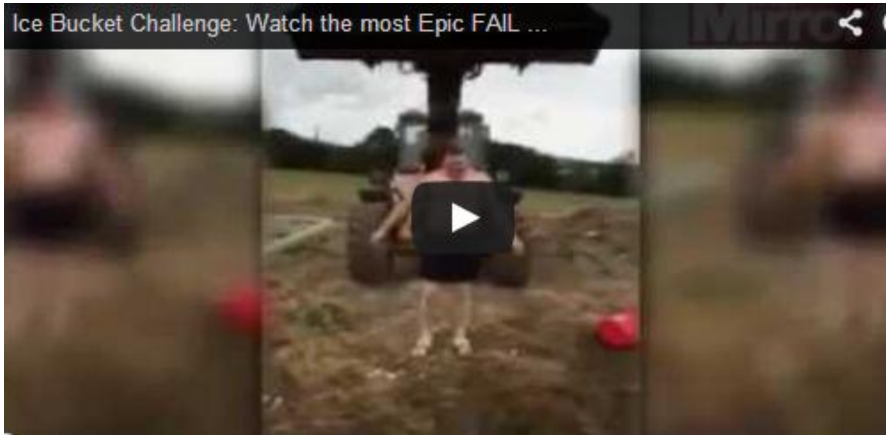
Thursday 05:21

haha 🙂
rhcxch977.z

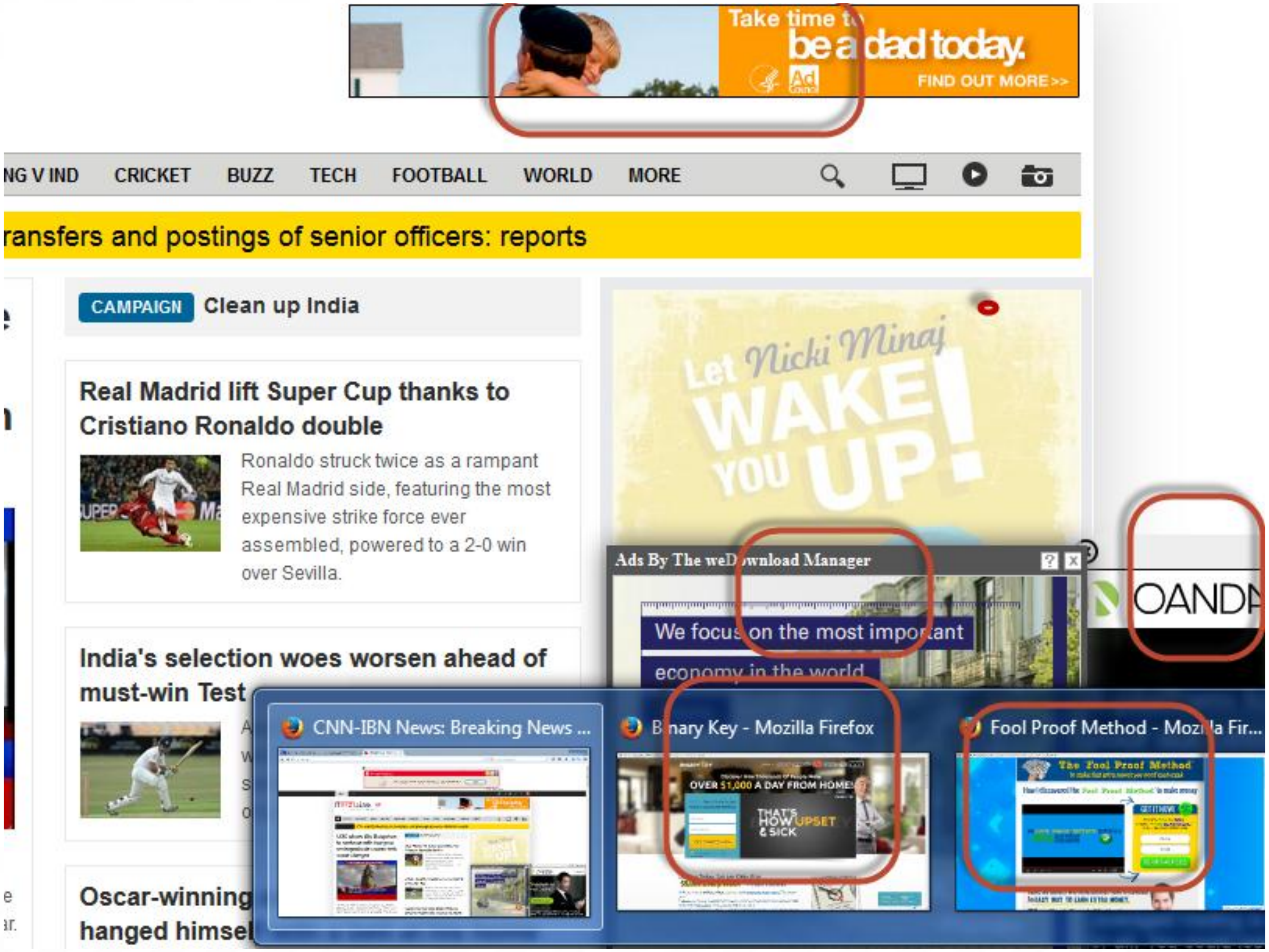

Select your favourite color scheme for facebook layout.
https://apps.facebook.com/themsandcolors?ref=219

Facebook color changer
apps.facebook.com


[SHOCKING VIDEO] Most Fatal Car Accident of the World !!!
side.thenudistnetwork.com
-Watch the Video-Heart breaking footage behind the scene !!


Ice Bucket Challenge: Watch the most Epic FAIL ...

Infection through Dodgy Websites
“Drive by Downloads”
通过欺诈网站感染传播



Take time to be a dad today.

FIND OUT MORE>>

NG V IND CRICKET BUZZ TECH FOOTBALL WORLD MORE

ransfers and postings of senior officers: reports

CAMPAIGN Clean up India

Real Madrid lift Super Cup thanks to Cristiano Ronaldo double

Ronaldo struck twice as a rampant Real Madrid side, featuring the most expensive strike force ever assembled, powered to a 2-0 win over Sevilla.

India's selection woes worsen ahead of must-win Test

Oscar-winning hanged himsel

Let Nicki Minaj WAKE YOU UP!

Ads By The weDownload Manager

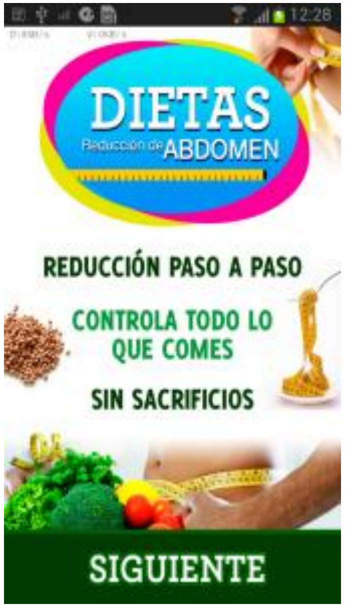
We focus on the most important economy in the world

OANDA

CNN-IBN News: Breaking News ...

Binary Key - Mozilla Firefox

Fool Proof Method - Mozilla Fir...



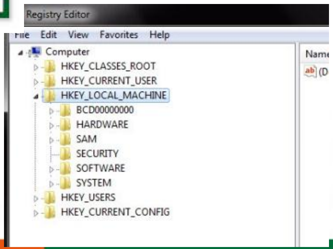
Sample example of Drive By Downloads

由于点击恶意链接而误下载各种恶意软件

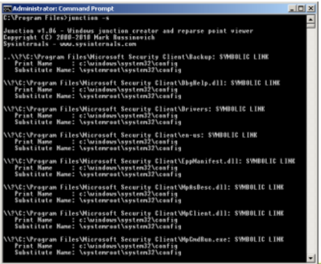
www.very_dodgy_url.com

www.xxx_123.com

www.porn_zxcv.com



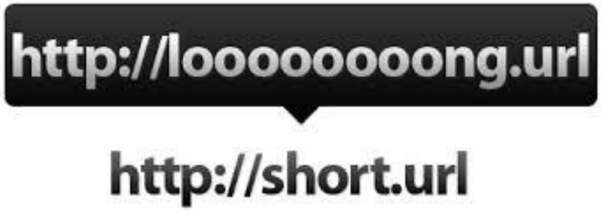
```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
  HKEY_USERS
  HKEY_CURRENT_CONFIG
```

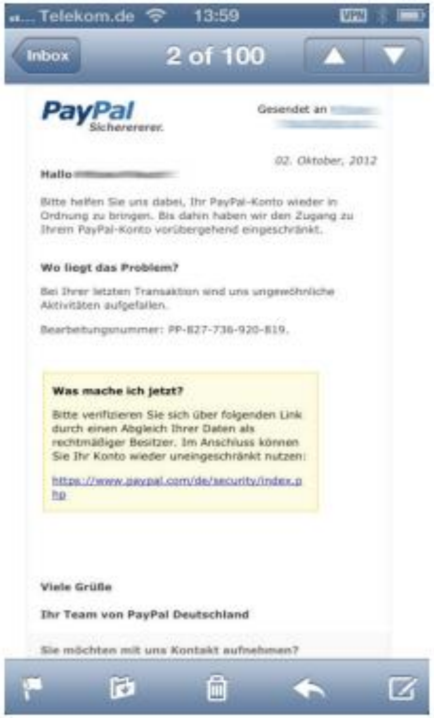


```
C:\Program Files>junction -s

Junction v1.06 - Windows junction creator and reparse point viewer
Copyright (C) 2000-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

..\\?\C:\Program Files\Microsoft Security Client\Backup: SYMBOLIC LINK
   Print Name     : c:\windows\system32\config
   Substitute Name: \systemroot\system32\config

\\?\C:\Program Files\Microsoft Security Client\DbgHelp.dll: SYMBOLIC LINK
   Print Name     : c:\windows\system32\config
   Substitute Name: \systemroot\system32\config

\\?\C:\Program Files\Microsoft Security Client\Drivers: SYMBOLIC LINK
   Print Name     : c:\windows\system32\config
   Substitute Name: \systemroot\system32\config

\\?\C:\Program Files\Microsoft Security Client\en-us: SYMBOLIC LINK
   Print Name     : c:\windows\system32\config
   Substitute Name: \systemroot\system32\config

\\?\C:\Program Files\Microsoft Security Client\EppManifest.dll: SYMBOLIC LINK
   Print Name     : c:\windows\system32\config
   Substitute Name: \systemroot\system32\config

\\?\C:\Program Files\Microsoft Security Client\MpAsDesc.dll: SYMBOLIC LINK
   Print Name     : c:\windows\system32\config
   Substitute Name: \systemroot\system32\config

\\?\C:\Program Files\Microsoft Security Client\MpClient.dll: SYMBOLIC LINK
   Print Name     : c:\windows\system32\config
   Substitute Name: \systemroot\system32\config

\\?\C:\Program Files\Microsoft Security Client\MpCmdRun.exe: SYMBOLIC LINK
   Print Name     : c:\windows\system32\config
   Substitute Name: \systemroot\system32\config
```

Drive By Downloads-Vicious in mobiles
移动终端上的恶意链接更隐蔽危害更大

- Url’s on phones are shortened
- Websites look different Mobile phones.
- SMS, Whatsapp, Viber, weibo messages
- One unmindful click enough for attackse





PayPal Sichererer.

Gesendet an [redacted]

02. Oktober, 2012

Hallo [redacted]

Bitte helfen Sie uns dabei, Ihr PayPal-Konto wieder in Ordnung zu bringen. Bis dahin haben wir den Zugang zu Ihrem PayPal-Konto vorübergehend eingeschränkt.

Wo liegt das Problem?

Bei Ihrer letzten Transaktion sind uns ungewöhnliche Aktivitäten aufgefallen.

Bearbeitungsnummer: PP-827-736-920-819.

Was mache ich jetzt?

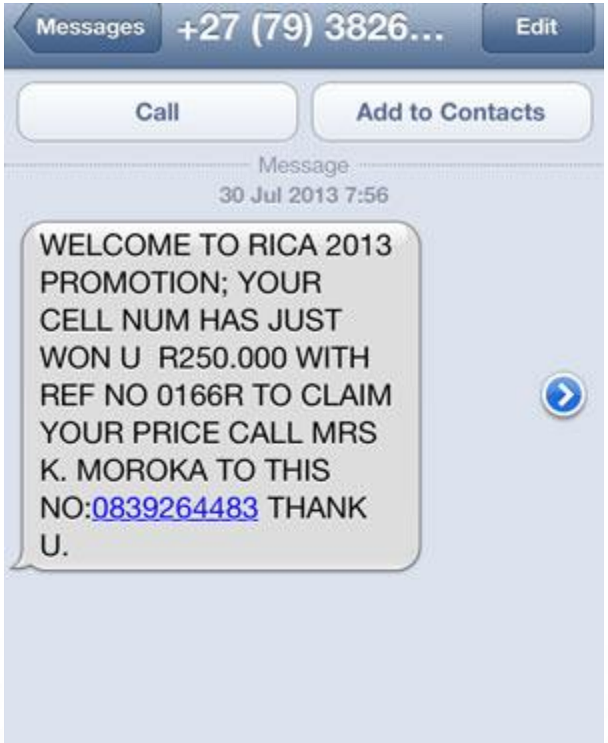
Bitte verifizieren Sie sich über folgenden Link durch einen Abgleich Ihrer Daten als rechtmäßiger Besitzer. Im Anschluss können Sie Ihr Konto wieder uneingeschränkt nutzen:

https://www.paypal.com/de/security/index.php

Viele Grüße

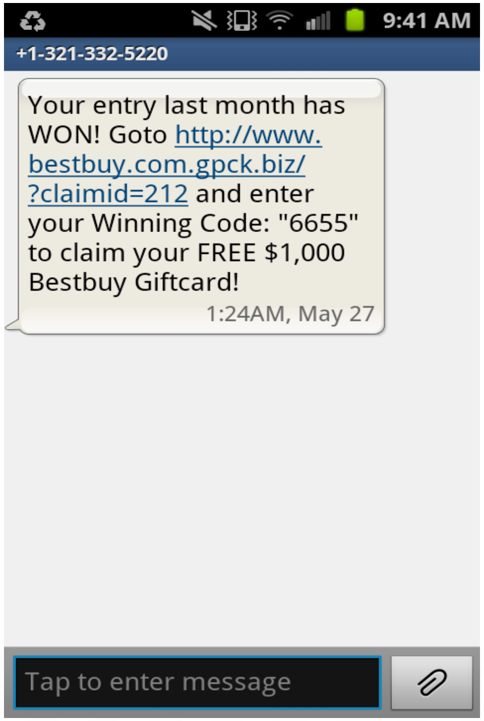
Ihr Team von PayPal Deutschland

Sie möchten mit uns Kontakt aufnehmen?



Message
30 Jul 2013 7:56

WELCOME TO RICA 2013 PROMOTION; YOUR CELL NUM HAS JUST WON U R250.000 WITH REF NO 0166R TO CLAIM YOUR PRICE CALL MRS K. MOROKA TO THIS NO:0839264483 THANK U.



+1-321-332-5220

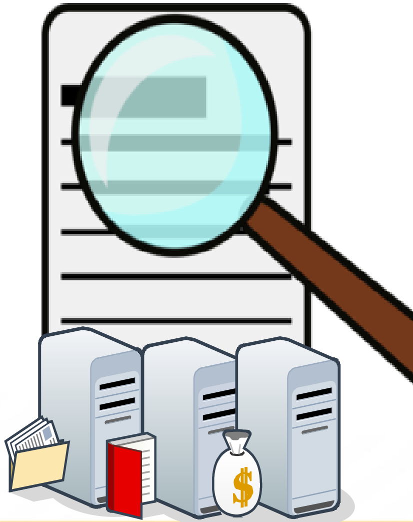
Your entry last month has WON! Goto http://www.bestbuy.com.gpck.biz/?claimid=212 and enter your Winning Code: "6655" to claim your FREE $1,000 Bestbuy Giftcard!

1:24AM, May 27

Successful Infection Always Follows Deeper Penetration

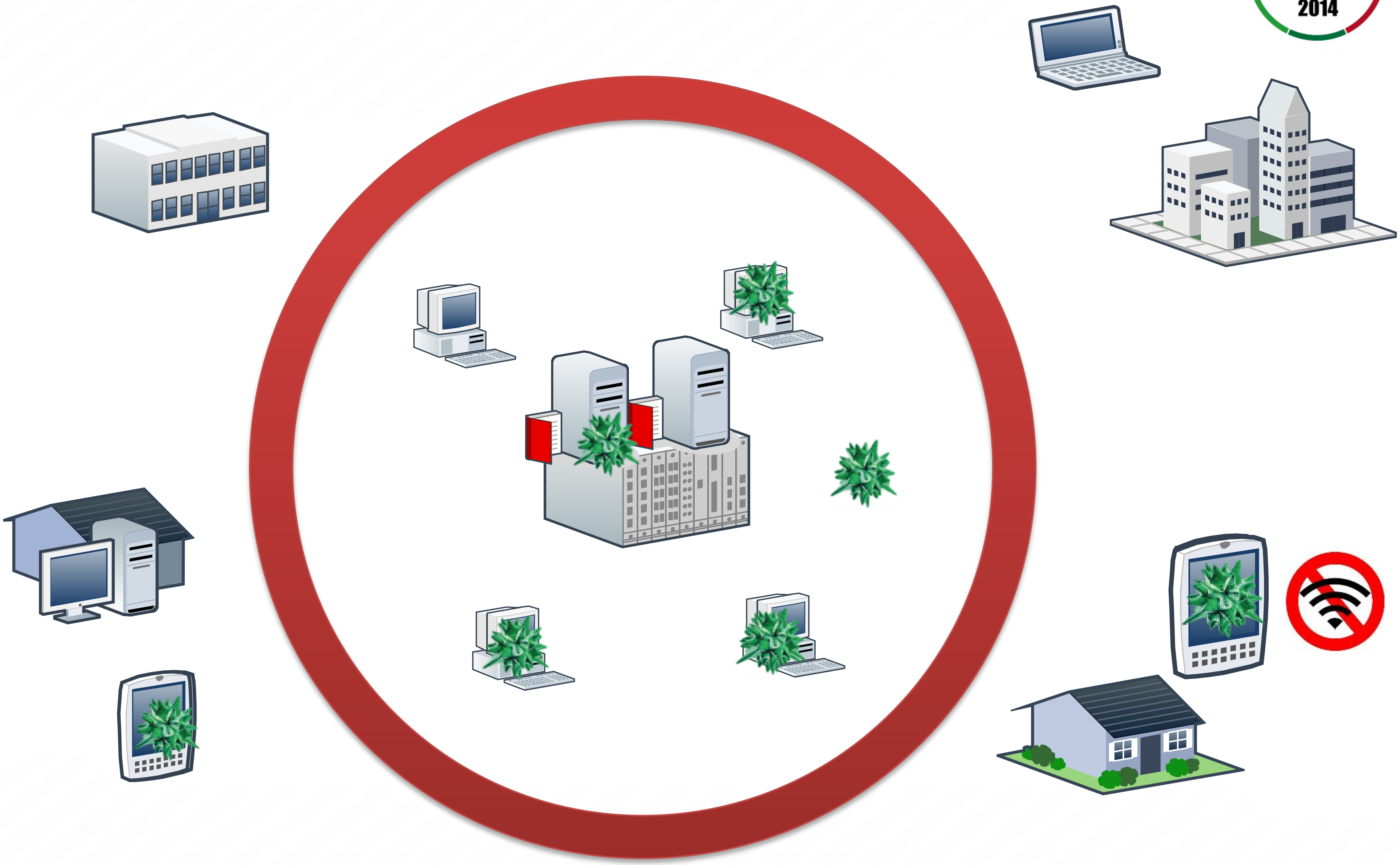
成功的感染植入后，紧接着的是进一步渗透

- Extract personal information
- Install Utilities, Malwares
- Dig Deeper into the system
- Corrupt/Encrypt or Hide Data
- Make a Bot and do nothing



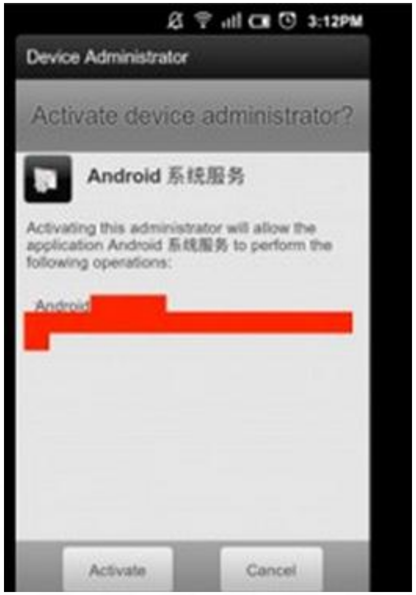
Attack Spread Dangers of a perimeter less world

BYOD让这种攻击传播的更快



Advanced Data Leakages
数据泄露问题

- Leakage through Video cams
- Recording Keystrokes/History
- Record meeting/call data
- SMS copiers, remote login utilities, rootkits



3:12PM

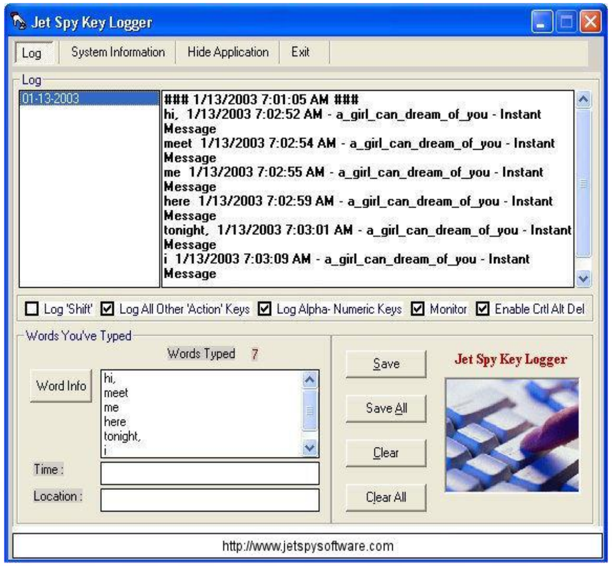
Device Administrator

Activate device administrator?

Android 系统服务

Activating this administrator will allow the application Android 系统服务 to perform the following operations:

[redacted]



```
### 1/13/2003 7:01:05 AM ###
hi,  1/13/2003 7:02:52 AM - a_girl_can_dream_of_you - Instant
Message
meet  1/13/2003 7:02:54 AM - a_girl_can_dream_of_you - Instant
Message
me  1/13/2003 7:02:55 AM - a_girl_can_dream_of_you - Instant
Message
here  1/13/2003 7:02:59 AM - a_girl_can_dream_of_you - Instant
Message
tonight,  1/13/2003 7:03:01 AM - a_girl_can_dream_of_you - Instant
Message
i  1/13/2003 7:03:09 AM - a_girl_can_dream_of_you - Instant
Message
```

☐ Log 'Shift' ☑ Log All Other 'Action' Keys ☑ Log Alpha- Numeric Keys ☑ Monitor ☑ Enable Crtl Alt Del

Words You've Typed

Words Typed 7

```
hi,
meet
me
here
tonight,
i
```

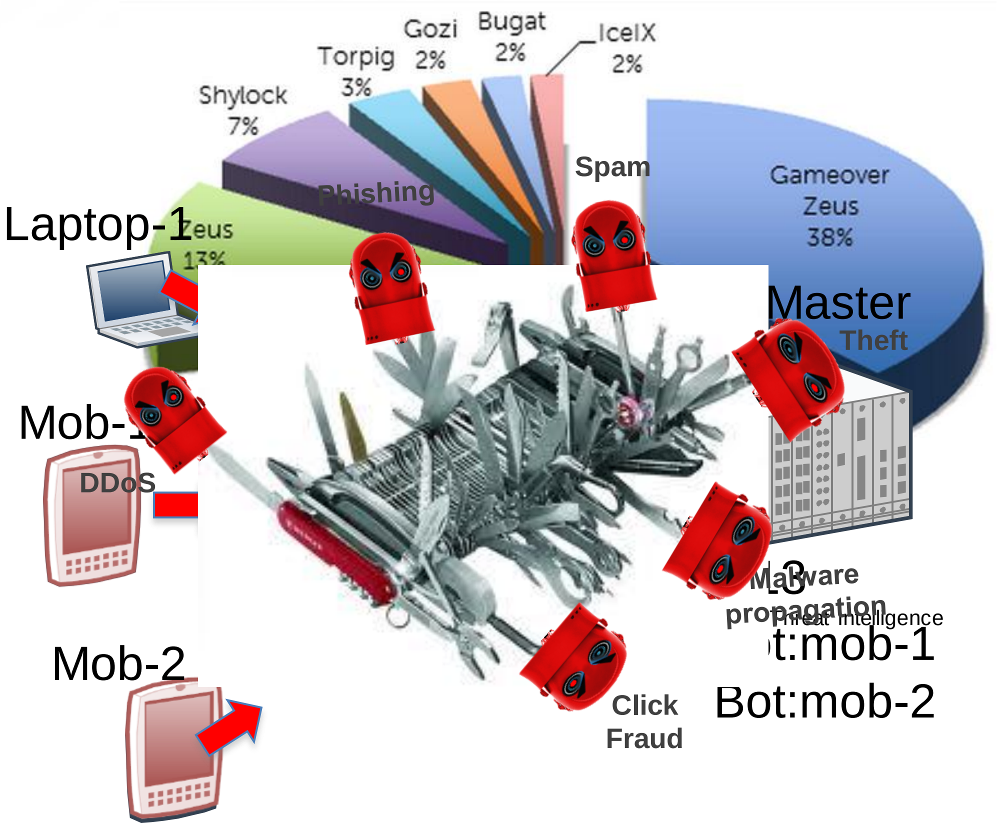
Time :

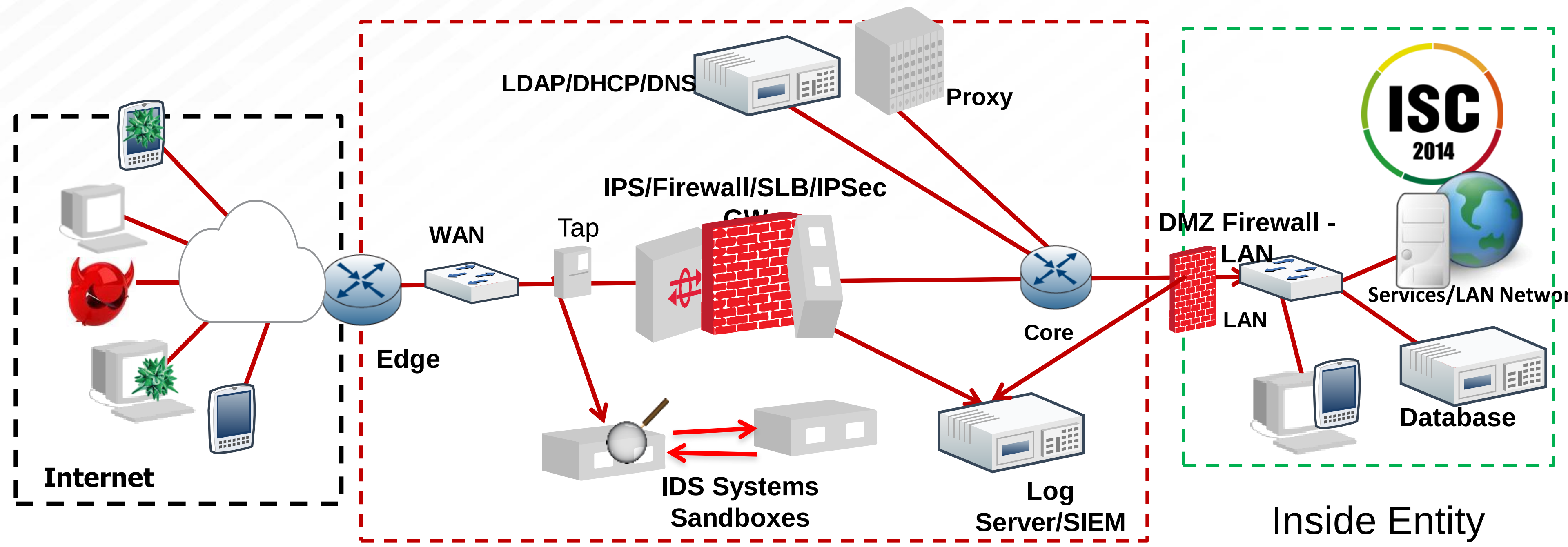
Location :

Modern APT breeding grounds of Large Botnet

APT可以产生大规模的僵尸网络

Sophisticated Botnets – The Swiss army knife of Attackers





Hardware Infrastructure

- DHCP
- VPN
- Web Proxy
- IDS/IPS
- Firewall/Router ACL
- IPSec Gateways
- HIDS/HIPS
- Endpoint Protections
- Redundant Hardware

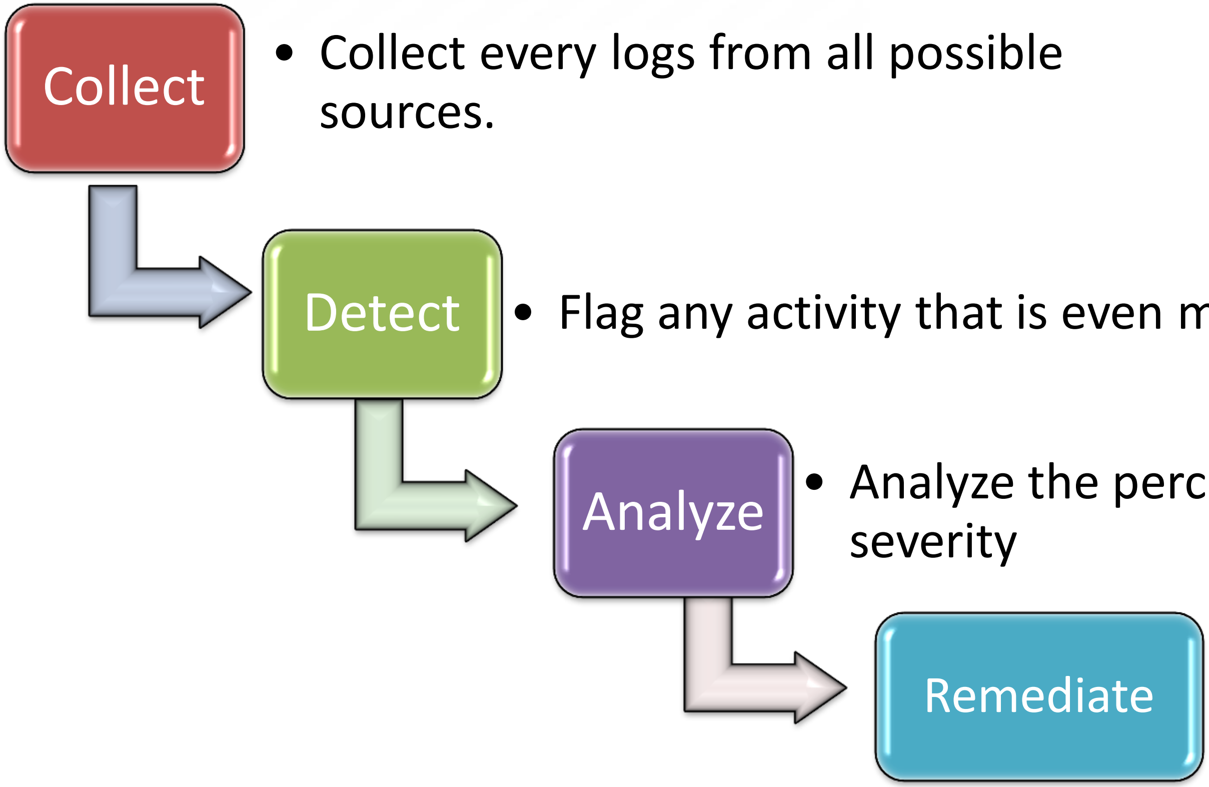
Forensic and Investigation

- Robust Logging
- Proxy Logs
- Authentication Logs
- IDS Alerts
- Host-based Logs
- Firewall Logs
- Full Content Traffic Captures
- Netflow
- Server Event Logs
- Workstation Event Logs

Efficient Network Design

- Proper Network Segmentation
- Well Defined DMZ
- Wifi and Wireless Zoning
- IP Address Schemas
- Public Facing device control
- Overview of NW Infrastructure

Stages in APT Mitigation
预防抵御APT攻击的不同阶段



Collect

- Collect every logs from all possible sources.

Detect

- Flag any activity that is even mildly suspicious

Analyze

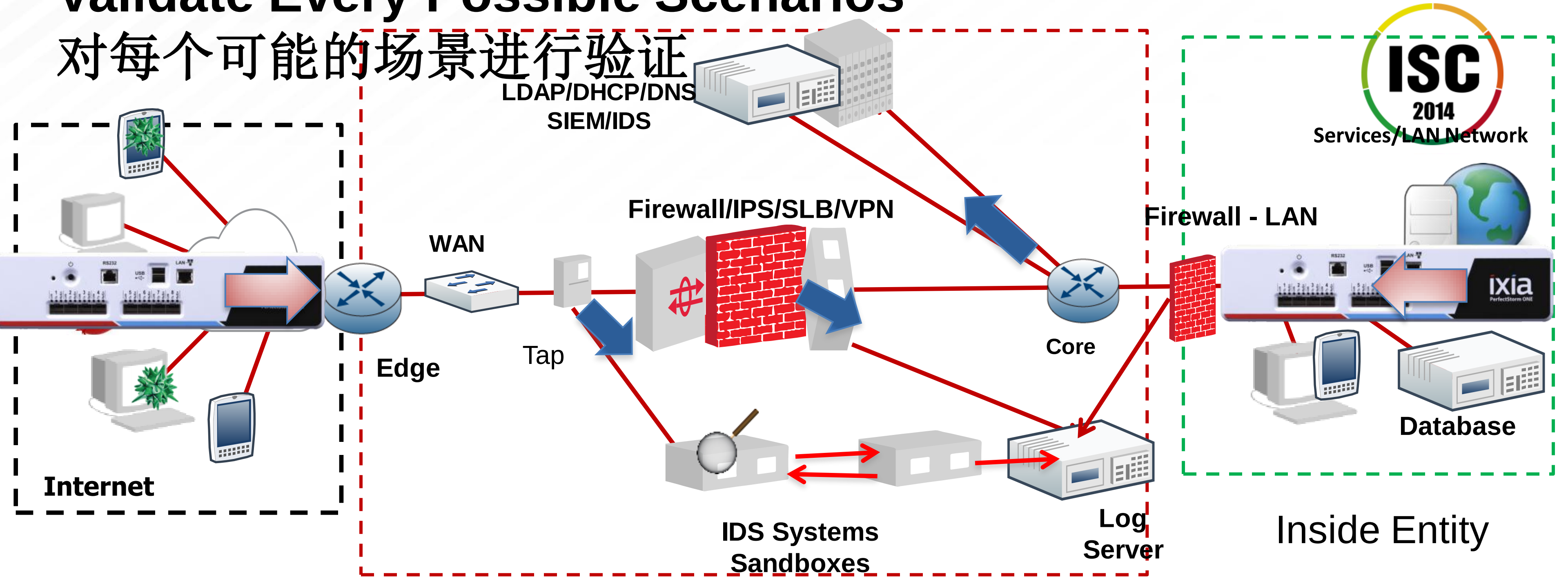
- Analyze the perceived threat severity

Remediate

- Take necessary actions

Validate Every Possible Scenarios

对每个可能的场景进行验证



Validation Techniques:

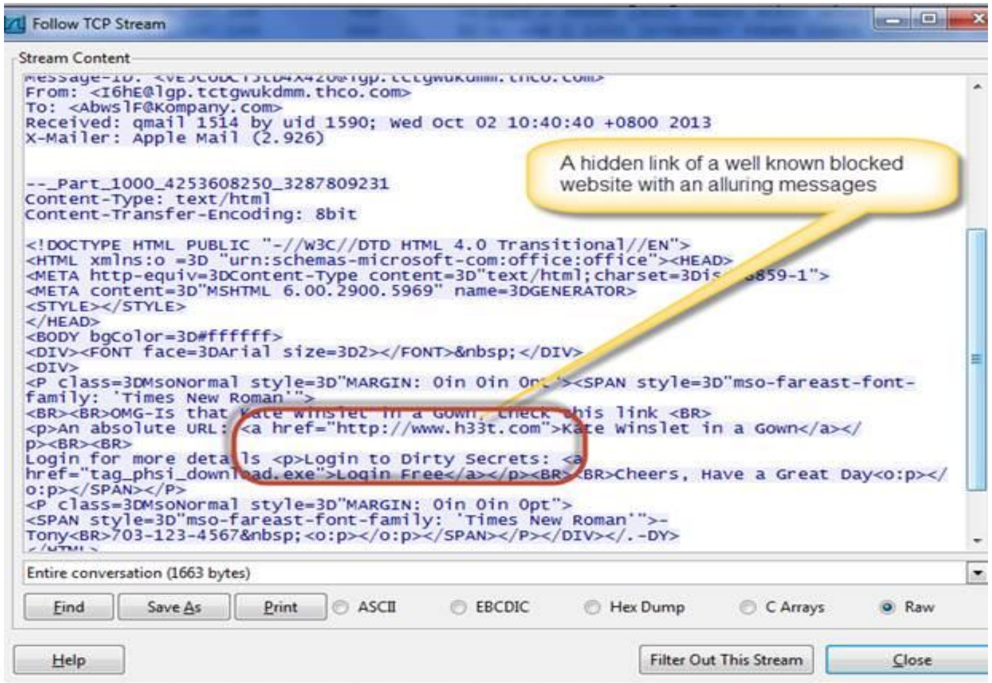
- Practice every stages of APT Mitigations
  - Phishing Attack
  - Malware Delivery
  - Data Ex-filteration
  - Lateral Movements
- Device validation and procurement best practices
- Continuously improve Attack Detection Time(ADT)
- Continuous practice of D.C.A.R cycle (Detect ->Collect -> Assess -> Remediate**)**

Validating Phishing and Spam Email detection/prevention mechanism

对钓鱼网站和垃圾邮件监测识别系统的验证

APT Step 1- Phishing and Spam email generation

- Generate different types of phishing emails.
- Create new variants-Pictured Spam, Scrambled Spam
- Extensive Phishing with more than hundred plus phishing techniques
- False positives assessments



```
From: <I6hE@lgp.tctgwukdmm.thco.com>
To: <AbwslF@Kompany.com>
Received: qmail 1514 by uid 1590; Wed Oct 02 10:40:40 +0800 2013
X-Mailer: Apple Mail (2.926)


--_Part_1000_4253608250_3287809231
Content-Type: text/html
Content-Transfer-Encoding: 8bit

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML xmlns:o =3D "urn:schemas-microsoft-com:office:office"><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html;charset=3Diso-8859-1">
<META content=3D"MSHTML 6.00.2900.5969" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV><FONT face=3DArial size=3D2></FONT>&nbsp;</DIV>
<DIV>
<P class=3DMsoNormal style=3D"MARGIN: 0in 0in 0pt"><SPAN style=3D"mso-fareast-font-
family: 'Times New Roman'">
<BR><BR>OMG-Is that Kate Winslet in a Gown, check this link <BR>
<p>An absolute URL: <a href="http://www.h33t.com">Kate Winslet in a Gown</a></
p><BR><BR>
Login for more details <p>Login to Dirty Secrets: <a
href="tag_phsi_download.exe">Login Free</a></p><BR><BR>Cheers, Have a Great Day<o:p></
o:p></SPAN></P>
<P class=3DMsoNormal style=3D"MARGIN: 0in 0in 0pt">
<SPAN style=3D"mso-fareast-font-family: 'Times New Roman'">-
Tony<BR>703-123-4567&nbsp;<o:p></o:p></SPAN></P></DIV></.-DY>
```

A hidden link of a well known blocked website with an alluring messages

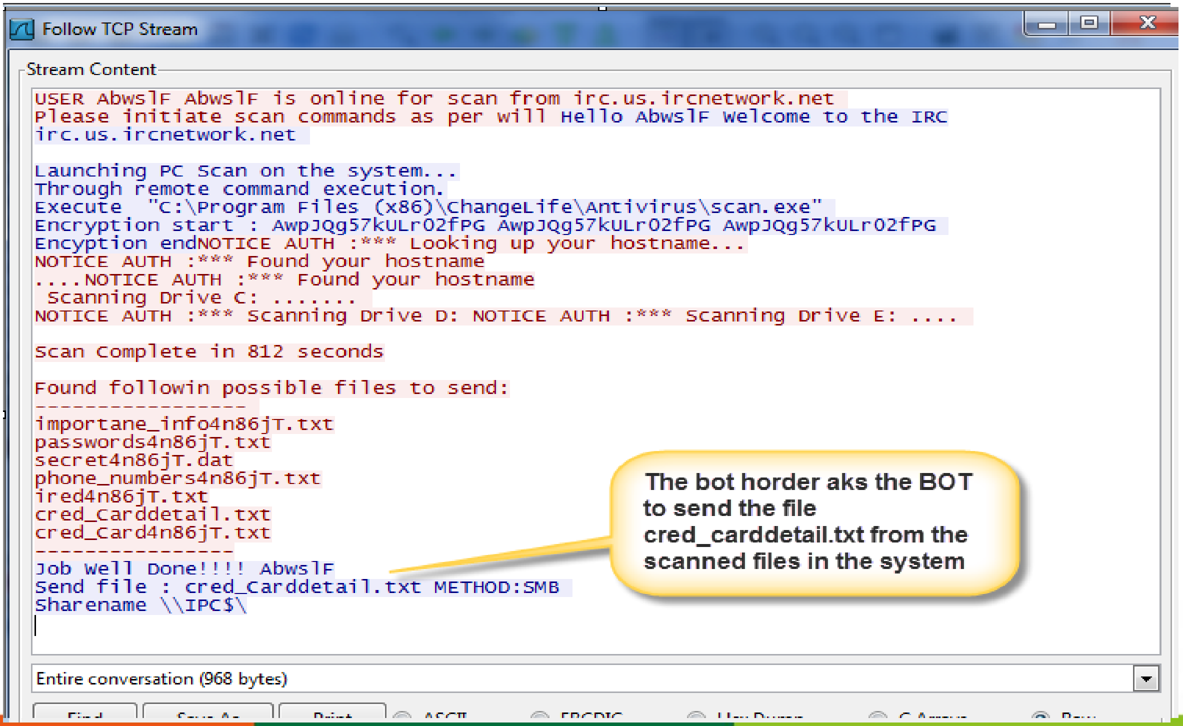
Entire conversation (1663 bytes)

Validate Malware/Exploit and Vulnerability delivery mitigation

对于病毒和漏洞攻击防御系统的验证

APT Step 2- User compromise and Bot to C&C message simulation

- Malware/Vulnerability delivery through various apps.
- Weibo, Gmail, SMTP every app/protocol can be a delivery vehicle.
- Simulate Bot to C&C communication.



```
USER AbwslF AbwslF is online for scan from irc.us.ircnetwork.net
Please initiate scan commands as per will Hello AbwslF Welcome to the IRC
irc.us.ircnetwork.net

Launching PC Scan on the system...
Through remote command execution.
Execute  "C:\Program Files (x86)\ChangeLife\Antivirus\scan.exe"
Encryption start : AwpJQg57kULr02fPG AwpJQg57kULr02fPG AwpJQg57kULr02fPG
Encyption endNOTICE AUTH :*** Looking up your hostname...
NOTICE AUTH :*** Found your hostname
....NOTICE AUTH :*** Found your hostname
 Scanning Drive C: .......
NOTICE AUTH :*** Scanning Drive D: NOTICE AUTH :*** Scanning Drive E: ....

Scan Complete in 812 seconds

Found followin possible files to send:
-----------------
importane_info4n86jT.txt
passwords4n86jT.txt
secret4n86jT.dat
phone_numbers4n86jT.txt
ired4n86jT.txt
cred_Carddetail.txt
cred_Card4n86jT.txt
----------------
Job Well Done!!!! AbwslF
Send file : cred_Carddetail.txt METHOD:SMB
Sharename \\IPC$\
```

Entire conversation (968 bytes)

The bot horder aks the BOT to send the file cred_carddetail.txt from the scanned files in the system

Validating Alarms, Loggings, Distraction and Decoy efficiency

验证报警、日志、反欺骗系统等系统的效率

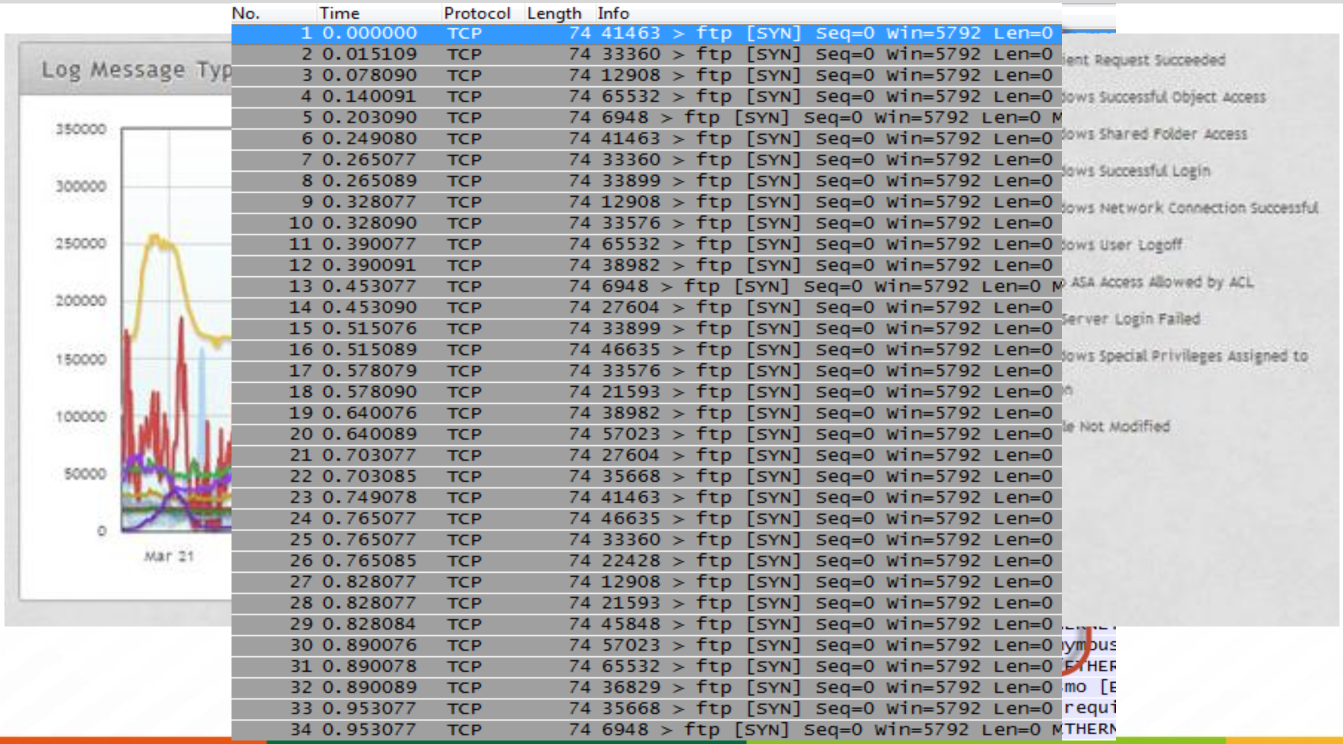
APT Step 3- Generation of Logs, Decoys and Distractions

•Generate extremely common and low-end attacks

•Generate different severity of Logs.

•Validate logging efficiency from each devices

•Generate volumetric DDOS Attacks.



```
No.   Time       Protocol Length Info
    1 0.000000   TCP          74 41463 > ftp [SYN] Seq=0 Win=5792 Len=0
    2 0.015109   TCP          74 33360 > ftp [SYN] Seq=0 Win=5792 Len=0
    3 0.078090   TCP          74 12908 > ftp [SYN] Seq=0 Win=5792 Len=0
    4 0.140091   TCP          74 65532 > ftp [SYN] Seq=0 Win=5792 Len=0
    5 0.203090   TCP          74 6948 > ftp [SYN] Seq=0 Win=5792 Len=0 M
    6 0.249080   TCP          74 41463 > ftp [SYN] Seq=0 Win=5792 Len=0
    7 0.265077   TCP          74 33360 > ftp [SYN] Seq=0 Win=5792 Len=0
    8 0.265089   TCP          74 33899 > ftp [SYN] Seq=0 Win=5792 Len=0
    9 0.328077   TCP          74 12908 > ftp [SYN] Seq=0 Win=5792 Len=0
   10 0.328090   TCP          74 33576 > ftp [SYN] Seq=0 Win=5792 Len=0
   11 0.390077   TCP          74 65532 > ftp [SYN] Seq=0 Win=5792 Len=0
   12 0.390091   TCP          74 38982 > ftp [SYN] Seq=0 Win=5792 Len=0
   13 0.453077   TCP          74 6948 > ftp [SYN] Seq=0 Win=5792 Len=0 M
   14 0.453090   TCP          74 27604 > ftp [SYN] Seq=0 Win=5792 Len=0
   15 0.515076   TCP          74 33899 > ftp [SYN] Seq=0 Win=5792 Len=0
   16 0.515089   TCP          74 46635 > ftp [SYN] Seq=0 Win=5792 Len=0
   17 0.578079   TCP          74 33576 > ftp [SYN] Seq=0 Win=5792 Len=0
   18 0.578090   TCP          74 21593 > ftp [SYN] Seq=0 Win=5792 Len=0
   19 0.640076   TCP          74 38982 > ftp [SYN] Seq=0 Win=5792 Len=0
   20 0.640089   TCP          74 57023 > ftp [SYN] Seq=0 Win=5792 Len=0
   21 0.703077   TCP          74 27604 > ftp [SYN] Seq=0 Win=5792 Len=0
   22 0.703085   TCP          74 35668 > ftp [SYN] Seq=0 Win=5792 Len=0
   23 0.749078   TCP          74 41463 > ftp [SYN] Seq=0 Win=5792 Len=0
   24 0.765077   TCP          74 46635 > ftp [SYN] Seq=0 Win=5792 Len=0
   25 0.765077   TCP          74 33360 > ftp [SYN] Seq=0 Win=5792 Len=0
   26 0.765085   TCP          74 22428 > ftp [SYN] Seq=0 Win=5792 Len=0
   27 0.828077   TCP          74 12908 > ftp [SYN] Seq=0 Win=5792 Len=0
   28 0.828077   TCP          74 21593 > ftp [SYN] Seq=0 Win=5792 Len=0
   29 0.828084   TCP          74 45848 > ftp [SYN] Seq=0 Win=5792 Len=0
   30 0.890076   TCP          74 57023 > ftp [SYN] Seq=0 Win=5792 Len=0 ymbus
   31 0.890078   TCP          74 65532 > ftp [SYN] Seq=0 Win=5792 Len=0 ETHER
   32 0.890089   TCP          74 36829 > ftp [SYN] Seq=0 Win=5792 Len=0 mo [E
   33 0.953077   TCP          74 35668 > ftp [SYN] Seq=0 Win=5792 Len=0 requi
   34 0.953077   TCP          74 6948 > ftp [SYN] Seq=0 Win=5792 Len=0 MTHERN
```

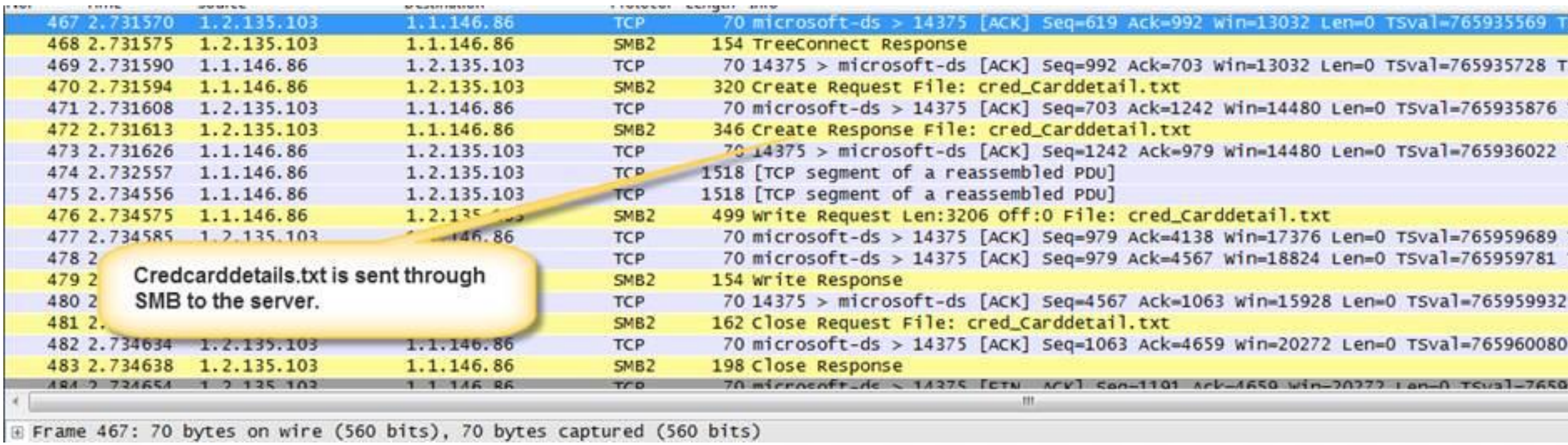
ient Request Succeeded
dows Successful Object Access
dows Shared Folder Access
dows Successful Login
dows Network Connection Successful
dows User Logoff
ASA Access Allowed by ACL
Server Login Failed
dows Special Privileges Assigned to
n
le Not Modified

Validate Data Leakage, Data Ex-filteration, Lateral Movements mitigation

验证防数据泄露系统

APT Step 4- Data Leakage and Persistency

- Leakage simulation through encrypted and non-encrypted apps.
- Data Leakage policy validation
- Lawful Interception efficiency assessments
- Validate multiple data leakage protection against multiple Vehicle and data types.

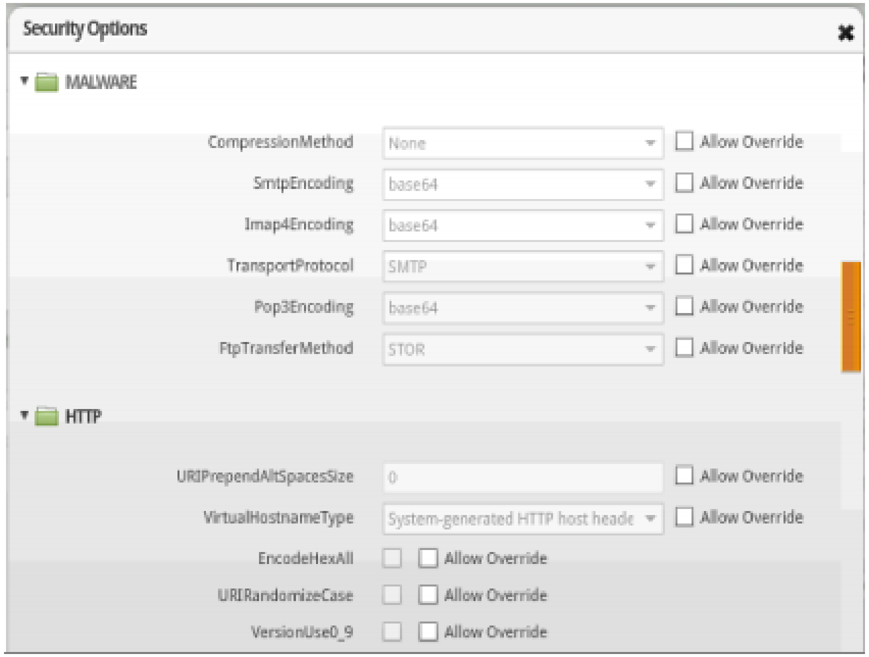


```
No.    Time      Source        Destination   Protocol Length Info
   467 2.731570  1.2.135.103   1.1.146.86    TCP        70 microsoft-ds > 14375 [ACK] Seq=619 Ack=992 Win=13032 Len=0 TSval=765935569 T
   468 2.731575  1.2.135.103   1.1.146.86    SMB2      154 TreeConnect Response
   469 2.731590  1.1.146.86    1.2.135.103   TCP        70 14375 > microsoft-ds [ACK] Seq=992 Ack=703 Win=13032 Len=0 TSval=765935728 T
   470 2.731594  1.1.146.86    1.2.135.103   SMB2      320 Create Request File: cred_Carddetail.txt
   471 2.731608  1.2.135.103   1.1.146.86    TCP        70 microsoft-ds > 14375 [ACK] Seq=703 Ack=1242 Win=14480 Len=0 TSval=765935876
   472 2.731613  1.2.135.103   1.1.146.86    SMB2      346 Create Response File: cred_Carddetail.txt
   473 2.731626  1.1.146.86    1.2.135.103   TCP        70 14375 > microsoft-ds [ACK] Seq=1242 Ack=979 Win=14480 Len=0 TSval=765936022
   474 2.732557  1.1.146.86    1.2.135.103   TCP      1518 [TCP segment of a reassembled PDU]
   475 2.734556  1.1.146.86    1.2.135.103   TCP      1518 [TCP segment of a reassembled PDU]
   476 2.734575  1.1.146.86    1.2.135.103   SMB2      499 Write Request Len:3206 Off:0 File: cred_Carddetail.txt
   477 2.734585  1.2.135.103   1.1.146.86    TCP        70 microsoft-ds > 14375 [ACK] Seq=979 Ack=4138 Win=17376 Len=0 TSval=765959689
   478 2                                     TCP        70 microsoft-ds > 14375 [ACK] Seq=979 Ack=4567 Win=18824 Len=0 TSval=765959781
   479 2                                     SMB2      154 Write Response
   480 2                                     TCP        70 14375 > microsoft-ds [ACK] Seq=4567 Ack=1063 Win=15928 Len=0 TSval=765959932
   481 2.                                    SMB2      162 Close Request File: cred_Carddetail.txt
   482 2.734634  1.2.135.103   1.1.146.86    TCP        70 microsoft-ds > 14375 [ACK] Seq=1063 Ack=4659 Win=20272 Len=0 TSval=765960080
   483 2.734638  1.2.135.103   1.1.146.86    SMB2      198 Close Response
   484 2.734654  1.2.135.103   1.1.146.86    TCP        70 microsoft-ds > 14375 [FIN, ACK] Seq=1191 Ack=4659 Win=20272 Len=0 TSval=7659

⊞ Frame 467: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
```

Credcarddetails.txt is sent through SMB to the server.

Validating Protection against Attack polymorphism
对于攻击各种变化形态的验证

Every Malware, Exploit and Vulnerability can be hidden through evasion techniques.



Security Options ✖

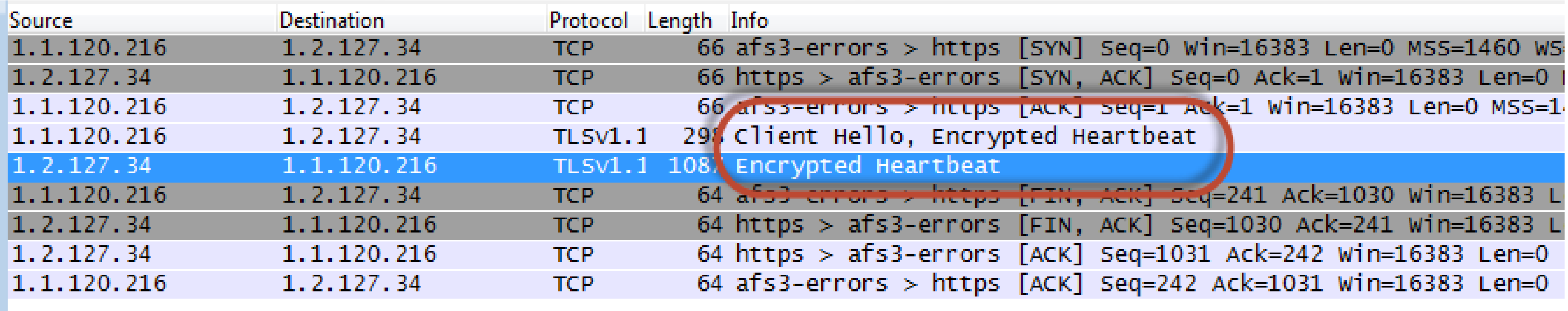
▾ MALWARE

CompressionMethod: None ▾ □ Allow Override
SmtpEncoding: base64 ▾ □ Allow Override
Imap4Encoding: base64 ▾ □ Allow Override
TransportProtocol: SMTP ▾ □ Allow Override
Pop3Encoding: base64 ▾ □ Allow Override
FtpTransferMethod: STOR ▾ □ Allow Override

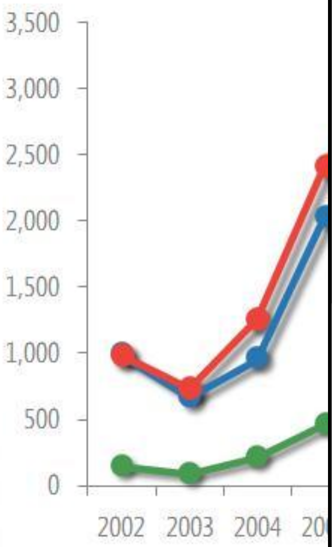
▾ HTTP

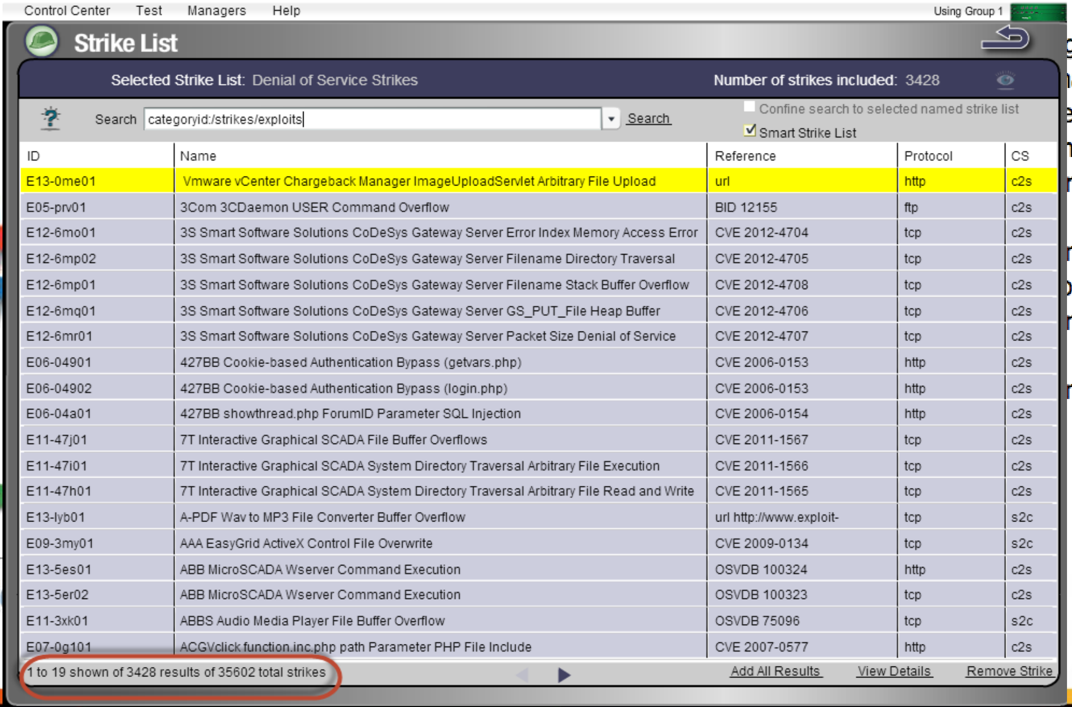
URIPrependAltSpacesSize: 0 □ Allow Override
VirtualHostnameType: System-generated HTTP host heade ▾ □ Allow Override
EncodeHexAll: □ □ Allow Override
URIRandomizeCase: □ □ Allow Override
VersionUse0_9: □ □ Allow Override

Validating Resiliency against Vulnerability Exploitatio
进行漏洞攻击的弹性验证



Source	Destination	Protocol	Length	Info
1.1.120.216	1.2.127.34	TCP	66	afs3-errors > https [SYN] Seq=0 Win=16383 Len=0 MSS=1460 WS
1.2.127.34	1.1.120.216	TCP	66	https > afs3-errors [SYN, ACK] Seq=0 Ack=1 Win=16383 Len=0
1.1.120.216	1.2.127.34	TCP	66	afs3-errors > https [ACK] Seq=1 Ack=1 Win=16383 Len=0 MSS=1
1.1.120.216	1.2.127.34	TLSv1.1	29	Client Hello, Encrypted Heartbeat
1.2.127.34	1.1.120.216	TLSv1.1	108	Encrypted Heartbeat
1.1.120.216	1.2.127.34	TCP	64	afs3-errors > https [FIN, ACK] Seq=241 Ack=1030 Win=16383 L
1.2.127.34	1.1.120.216	TCP	64	https > afs3-errors [FIN, ACK] Seq=1030 Ack=241 Win=16383 L
1.2.127.34	1.1.120.216	TCP	64	https > afs3-errors [ACK] Seq=1031 Ack=242 Win=16383 Len=0
1.1.120.216	1.2.127.34	TCP	64	afs3-errors > https [ACK] Seq=242 Ack=1031 Win=16383 Len=0





Selected Strike List: Denial of Service Strikes

Number of strikes included: 3428

Search categoryid:/strikes/exploits

□ Confine search to selected named strike list

☑ Smart Strike List

ID	Name	Reference	Protocol	CS
E13-0me01	Vmware vCenter Chargeback Manager ImageUploadServlet Arbitrary File Upload	url	http	c2s
E05-prv01	3Com 3CDaemon USER Command Overflow	BID 12155	ftp	c2s
E12-6mo01	3S Smart Software Solutions CoDeSys Gateway Server Error Index Memory Access Error	CVE 2012-4704	tcp	c2s
E12-6mp02	3S Smart Software Solutions CoDeSys Gateway Server Filename Directory Traversal	CVE 2012-4705	tcp	c2s
E12-6mp01	3S Smart Software Solutions CoDeSys Gateway Server Filename Stack Buffer Overflow	CVE 2012-4708	tcp	c2s
E12-6mq01	3S Smart Software Solutions CoDeSys Gateway Server GS_PUT_File Heap Buffer	CVE 2012-4706	tcp	c2s
E12-6mr01	3S Smart Software Solutions CoDeSys Gateway Server Packet Size Denial of Service	CVE 2012-4707	tcp	c2s
E06-04901	427BB Cookie-based Authentication Bypass (getvars.php)	CVE 2006-0153	http	c2s
E06-04902	427BB Cookie-based Authentication Bypass (login.php)	CVE 2006-0153	http	c2s
E06-04a01	427BB showthread.php ForumID Parameter SQL Injection	CVE 2006-0154	http	c2s
E11-47j01	7T Interactive Graphical SCADA File Buffer Overflows	CVE 2011-1567	tcp	c2s
E11-47i01	7T Interactive Graphical SCADA System Directory Traversal Arbitrary File Execution	CVE 2011-1566	tcp	c2s
E11-47h01	7T Interactive Graphical SCADA System Directory Traversal Arbitrary File Read and Write	CVE 2011-1565	tcp	c2s
E13-lyb01	A-PDF Wav to MP3 File Converter Buffer Overflow	url http://www.exploit-	tcp	s2c
E09-3my01	AAA EasyGrid ActiveX Control File Overwrite	CVE 2009-0134	tcp	s2c
E13-5es01	ABB MicroSCADA Wserver Command Execution	OSVDB 100324	http	c2s
E13-5er02	ABB MicroSCADA Wserver Command Execution	OSVDB 100323	tcp	c2s
E11-3xk01	ABBS Audio Media Player File Buffer Overflow	OSVDB 75096	tcp	s2c
E07-0g101	ACGVclick function.inc.php path Parameter PHP File Include	CVE 2007-0577	http	c2s

1 to 19 shown of 3428 results of 35602 total strikes

ge
ation
ervice
nething
raversal

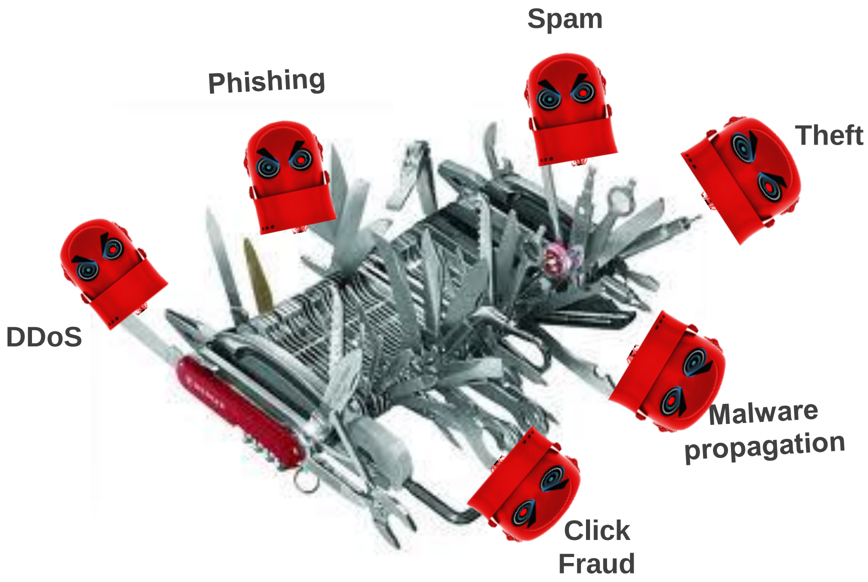
n
on
rruption

nse Splitting

Validations against Botnet Lifecycle Protections

对僵尸网络各环节保护能力进行验证

- ✓ Cutwail
- ✓ Zeus
- ✓ SpyEye
- ✓ ZeroAccess
- ✓ Duqu
- ✓ BlackEnergy
- ✓ TDL4
- ✓ PushDO
- ✓ TDW
- ✓ Customized Bot validation



Traditional DDOS Assessments

Layer 3 IP / ICMP
✓DDoS IP Frag Attack
✓DDoS ICMP Request Flood Attack
✓DDoS ICMP Response Flood Attack

Layer 4 UDP
✓LOIC UDP53 DoS Attack
✓DDoS UDP Fragmentation
✓DDoS Non-Spoofed UDP Flood
✓DDoS UDP Flood

Layer 4 TCP
✓DDoS SYN Flood
✓DDoS PSH-ACK Attack
✓DDoS Fake Session Attack
✓DDOS SYN-ACK Flood Attack
✓DDoS Rcv Wnd Size

Next Generation DDOS

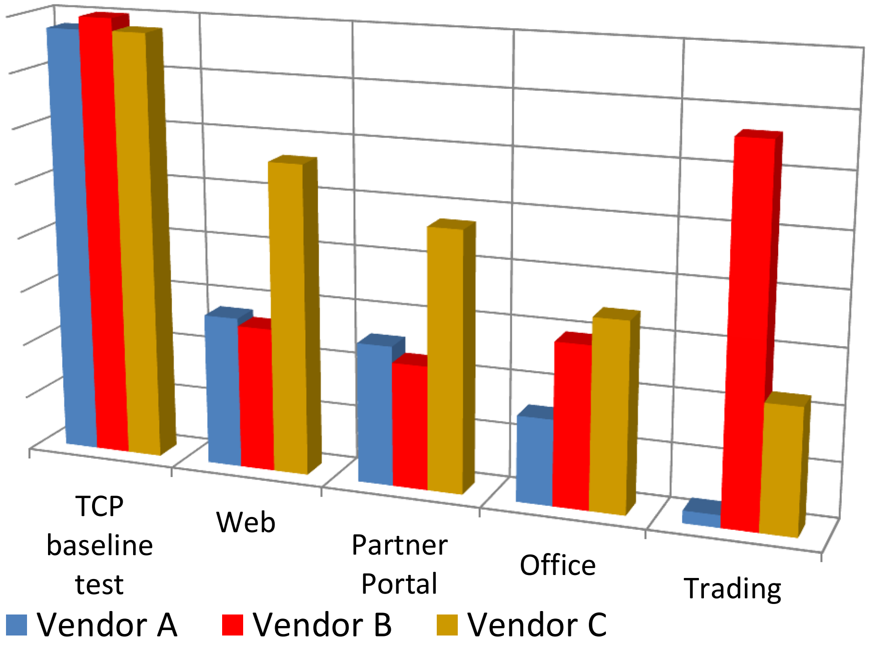
Layer 7 Apps
✓DDoS DNS Reflect - Attack
✓DDoS DNS Reflect - Zombie
✓LOIC HTTP DoS Attack
✓DDoS SIP Invite Flood
✓DDoS Redirect
✓DDoS DNS Flood
✓DDoS Excessive GET POST
✓DDoS Slow POST
✓DDoS Recursive GET
✓DDOS NTP
✓UE DDOS Generation

Unique
✓DDoS SlowLoris
✓DDoS Smurf Attack
✓DDoS TDL4 CC HTTP Flood
✓MultiVERB DDoS
✓RUDY DDoS
✓LOIC TCP8080 DoS Attack

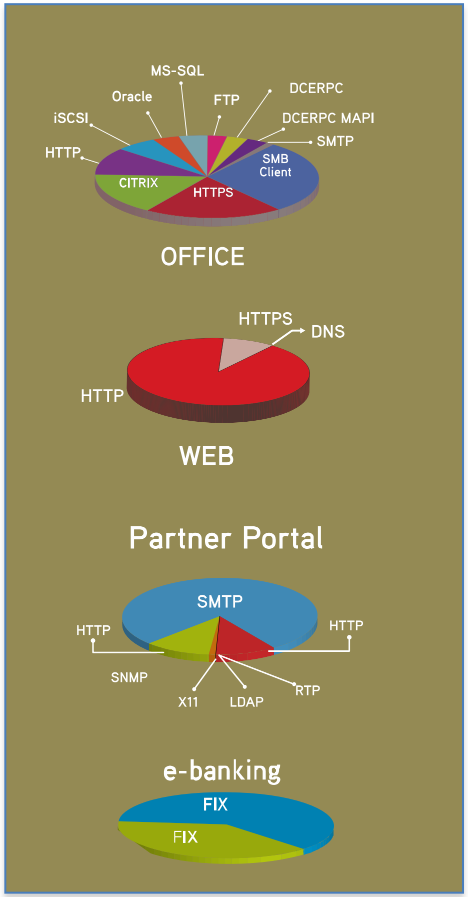
Application Performance Under Attack

在攻击下的应用业务性能

- Benchmarking performance of real network traffic
- Applications efficiency for attack mitigations
- Average Security Effectiveness



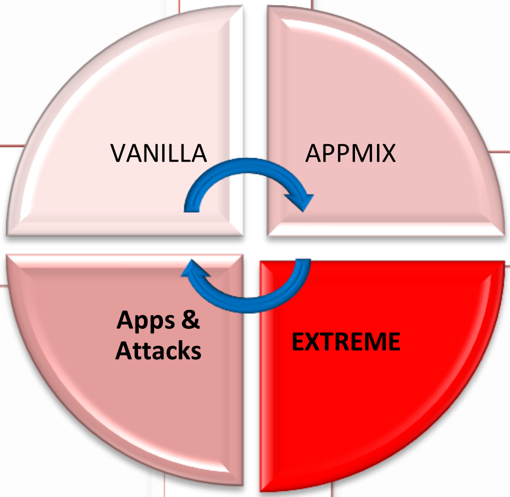
	Vendor A	Vendor B	Vendor C
Avg Sec effectiveness *	48%	52%	28%



Advanced Persistent Validations
高级的可持续验证

- TCP maximum concurrency
- TCP max connections per second
- TCP and UDP Max Throughput per second
- HTTP Page size max CC, CPS and TPS
- Max GTP performance
- RFC2544 & RFC3511

- Enterprise Mix
- Datacenter Mix
- Wireless Mix
- APAC/Europe/Americas
- Carrier Mix
- Organization specific Mix
- Customized

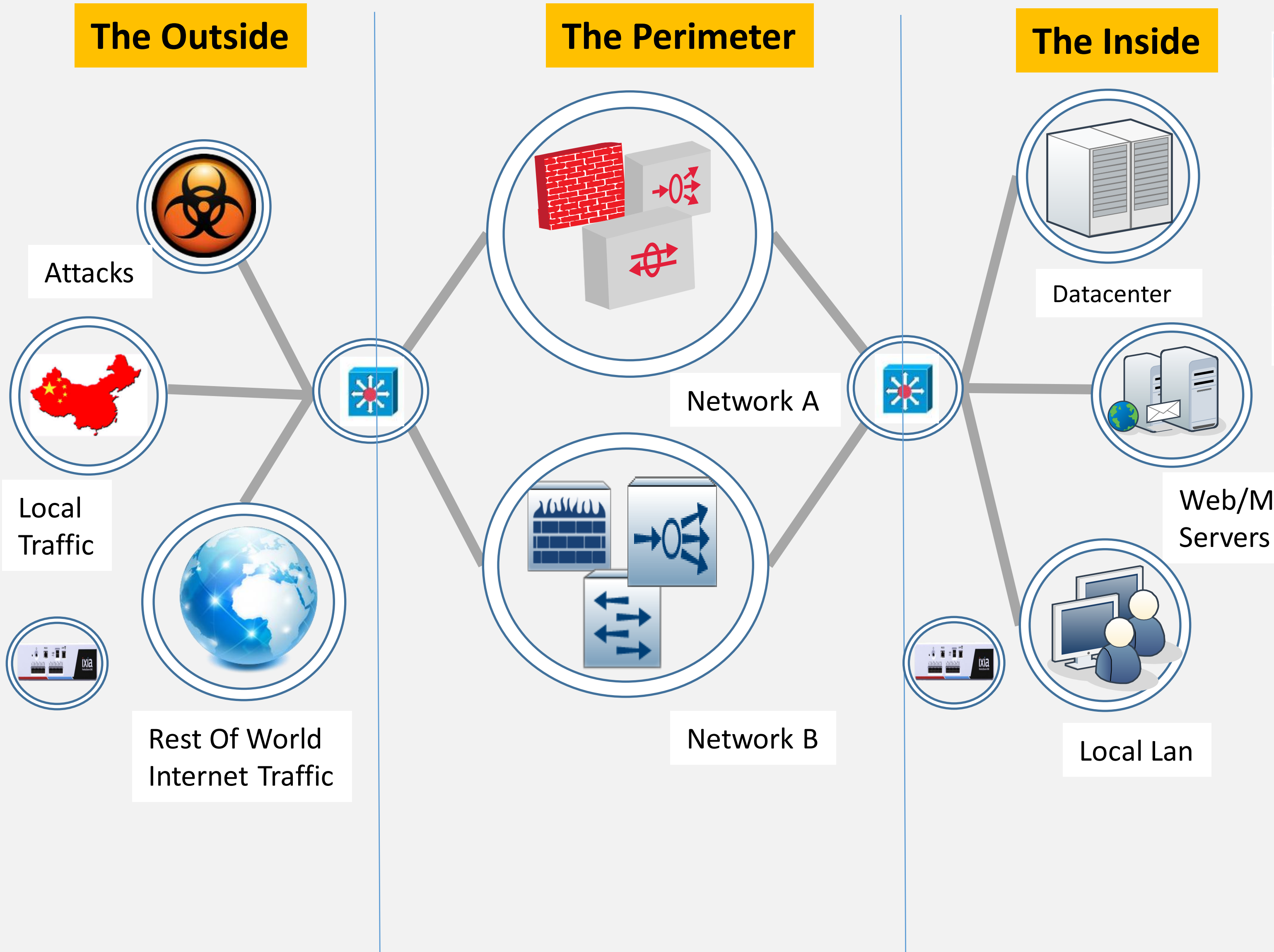


- Attack+ TCP performance
- Fuzzing + TCP/UDP Test
- Attack s+ AppMix
- Malwares within Attacks
- Apps + DOS
- Application + Vulnerabilities
- Botnet DDOS

- 100G DDOS
- Application DDOS
- Strikes + Apps + DDOS
- ADT efficiency
- Customized Application
- Data Generation
- Randomized behaviors
- Zero Days

NETWORK RESILIENCY VALIDATION

网络的弹性验证



Network Report Car

Category	Net-A	Net-B
Application Performance	B	B+
Security Effectiveness	C	B
Error Handling	A	A+
Min Latency	C+	B+
Overall Resiliency	C+	B+

Summary 小结

- The Internet, Applications and Attacks have changed
- Our defense in comparison have not changed.
- To counter newer attacks resilient networks are needed.
- **Advanced Validations** is the only way to assure network protection against attacks.