

Innovations in Network Security

Michael Singer
April 18, 2012

Global Security Threats and Trends



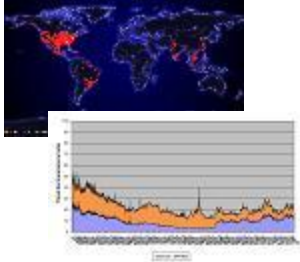
– Botnets –
System Control, Recruiting, DDoS, Spamming, Click-Fraud, Captcha Breaking
Fake Anti-Virus Scams, Account Theft

– Targeted Attacks –
Phishing, Spear Phishing, Whaling,
Advanced Persistent/Evasive Threat (APT/AET)

– Cybercrime Made Easy –
Hackers for Hire, Do-It-Yourself Kits



AT&T Approach to Network-Based Security



24x7 Situational Awareness function with near real-time analysis of security indicators:

- Internet and Intranet information
- Volumetric and behavioral algorithms
- Leverage output of malware, botnet and APT analysis



Embed security capabilities into the network itself

- Security Enforcement Nodes
- Managed Security Services



Cyber Intelligence Flash

Monday, April 16, 2012

Global Indicators

Homeland Security

(<http://www.dhs.gov/>)



SANS Internet Storm Center

(<http://isc.sans.org/infocon.php>)



AT&T Global IP Network Performance

(<http://ipnetwork.bqtmo.ip.att.net/pws/index.html>)

Latency: 35 ms Target: <= 37ms
Loss: 0.0% Target: < 0.05%

Top5 Scanned Ports

Scan Date: 04/15/2012

PROTOCOL	DESCRIPTION	% OF SOURCES	% OF PROBES
445/tcp	smb	49.0%	20.5%
1433/tcp	ms-sql	0.3%	17.0%
0:0/icmp	reply	26.1%	11.9%
80/tcp	http	1.0%	9.8%
3389/tcp	ms-term-serv	1.5%	4.2%
1105-others	1105-others	22.0%	36.6%

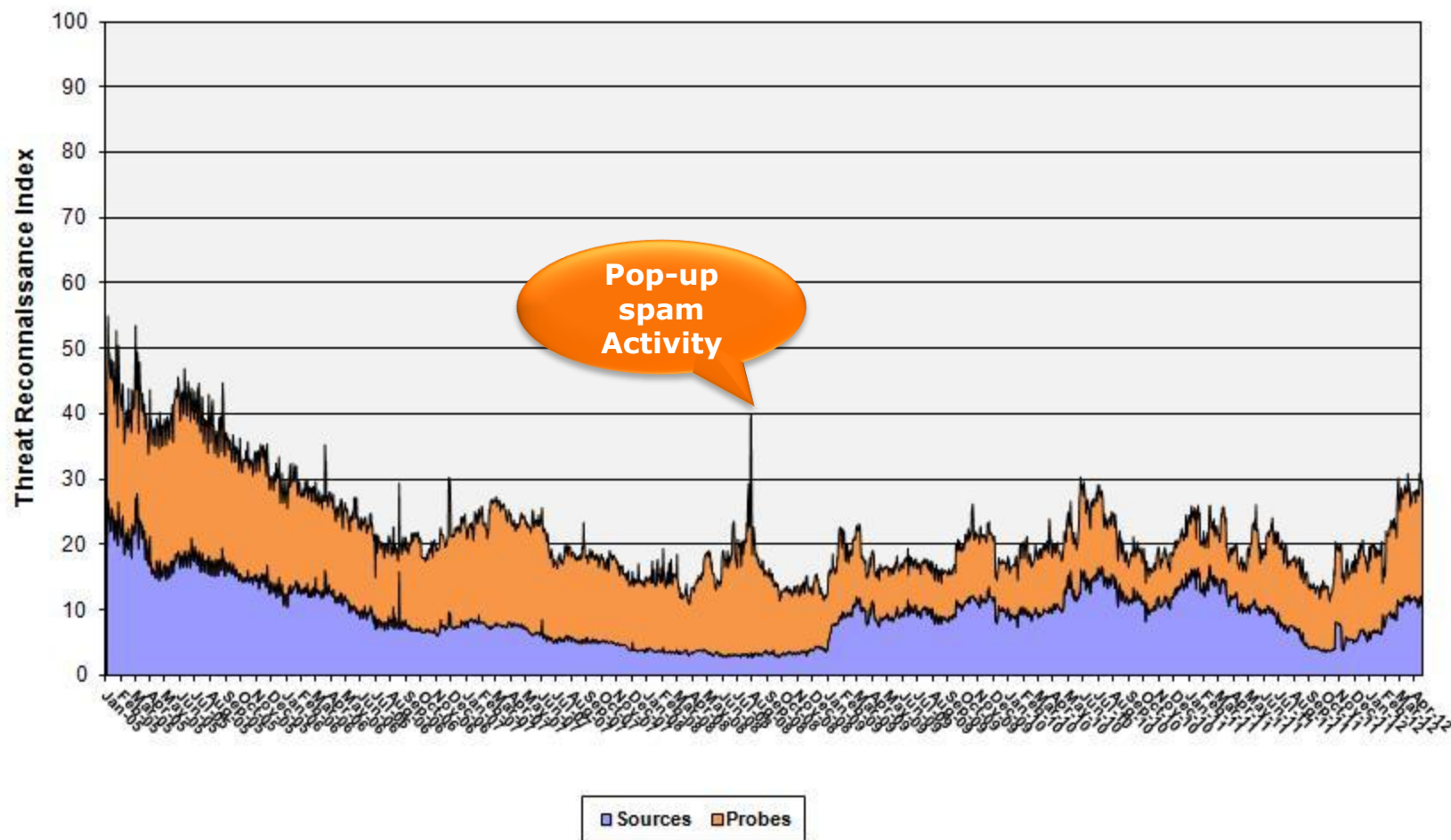
Daily Recon Index: 28
Weekly Recon Index: 29

04/15/2012

Critical	0
High	0
Medium	3 (C10051428-Closed)bm912x/Internal System Exhibiting Spyware Activity (C10051430-Closed)pg4857/Internal system showing signs of P2P software running (C10051431-Closed)rp4241/Internal system showing signs of P2P software running
Low	3 (C10051429-Closed)iPhone issue/non-vulnerability/Amber Bullard Kucera (C10051433-Closed)mk576n/Mobility VPN Botnet Detection (C10051432-Closed)Peggy McCanless/Phishing



Threat Reconnaissance Index



Active Botnets

HTTP-20120415-Members BotnetKoobface090724



Botnet Trends in Monetization

- DDoS'ing victims (as extortion)
- Spam email advertising
- Click fraud

Affiliate based Fake Anti-Virus software

Affiliate based programs of spreading Fake Anti-Virus software (scare ware) to victims generated hundreds of thousands of dollars of income for botnet operators (Koobface, Waledac, Conficker).



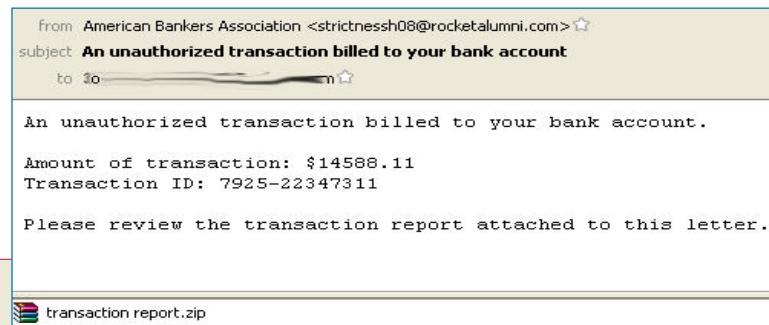
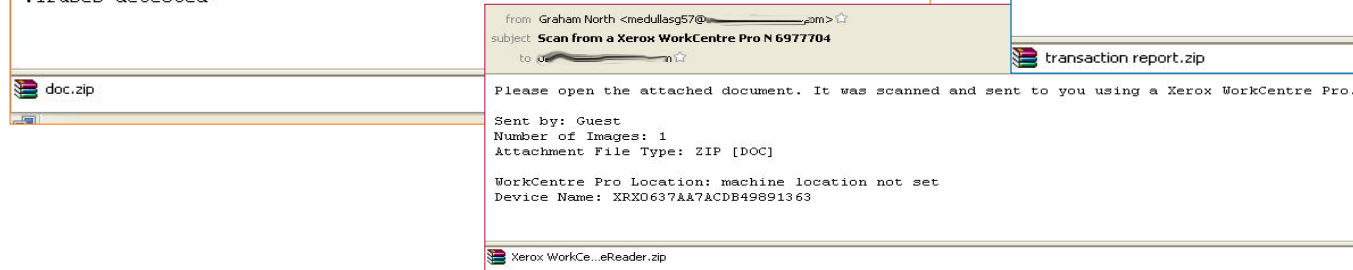
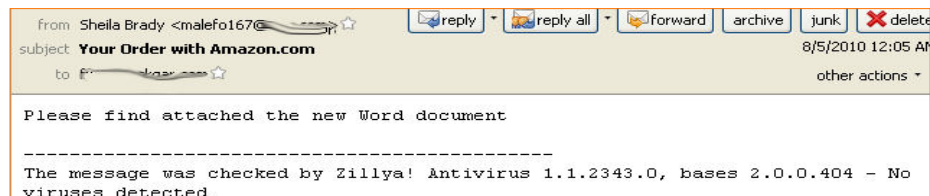
Active Botnets

HTTP-20120415-Members BotnetZeus090625



Zeus Propagation Methods

- The Zeus toolkit does not ship with a mechanism to infect victims. Buyers must pick their own method to spread.
- Most are spread via drive-by download and phishing.
 - Messages posted to [Facebook](#) and other social websites used to lure victims.
 - E-mail phishing lures are most common:



Zeus Modules and Pricing

- Zeus Kit for Version 1.3.4.x (\$3,000 to \$4,000)

- The Private Version of the Zeus Kit is running between \$3,000 and \$4,000. The latest private version of Zeus, as of this date, is 1.3.4.x.

- Backconnect \$1500

- The backconnect module allows an attacker to 'connect back' to the infected computer and make financial transactions from it. This way, banks that try to track where money transfers originate will always trace it back to the computer of the account holder.

- Firefox form grabber \$2000

- The Firefox form grabber module grabs data out of fields that are submitted using the Firefox web browser. This data can include personally identifiable information (PII) as well as usernames and passwords for bank accounts, trading accounts, online payment accounts, and anything else that would require the use of a username and password.

- Jabber (IM) chat notifier \$500

- The Jabber module allows an attacker to receive stolen data in "real time". If a bank account is being protected with a token that generates random numbers, then the attacker can access the victim's account in real time after the victim logs in using the token.

- VNC (Virtual Network Computing) private module \$10,000

- The VNC module is similar to the backconnect module, except that it allows you to establish a fully functioning virtual connection. The attacker can take control of the infected computer without the victim being aware of it. Essentially, the VNC provides the hacker with not just a Network Proxy but with a Total Presence Proxy (it is the total package), allowing the hacker to use all of the victim's hardware and software, including its browser, so as to avoid a bank's fraud detection systems.

- Windows 7 Support \$2000

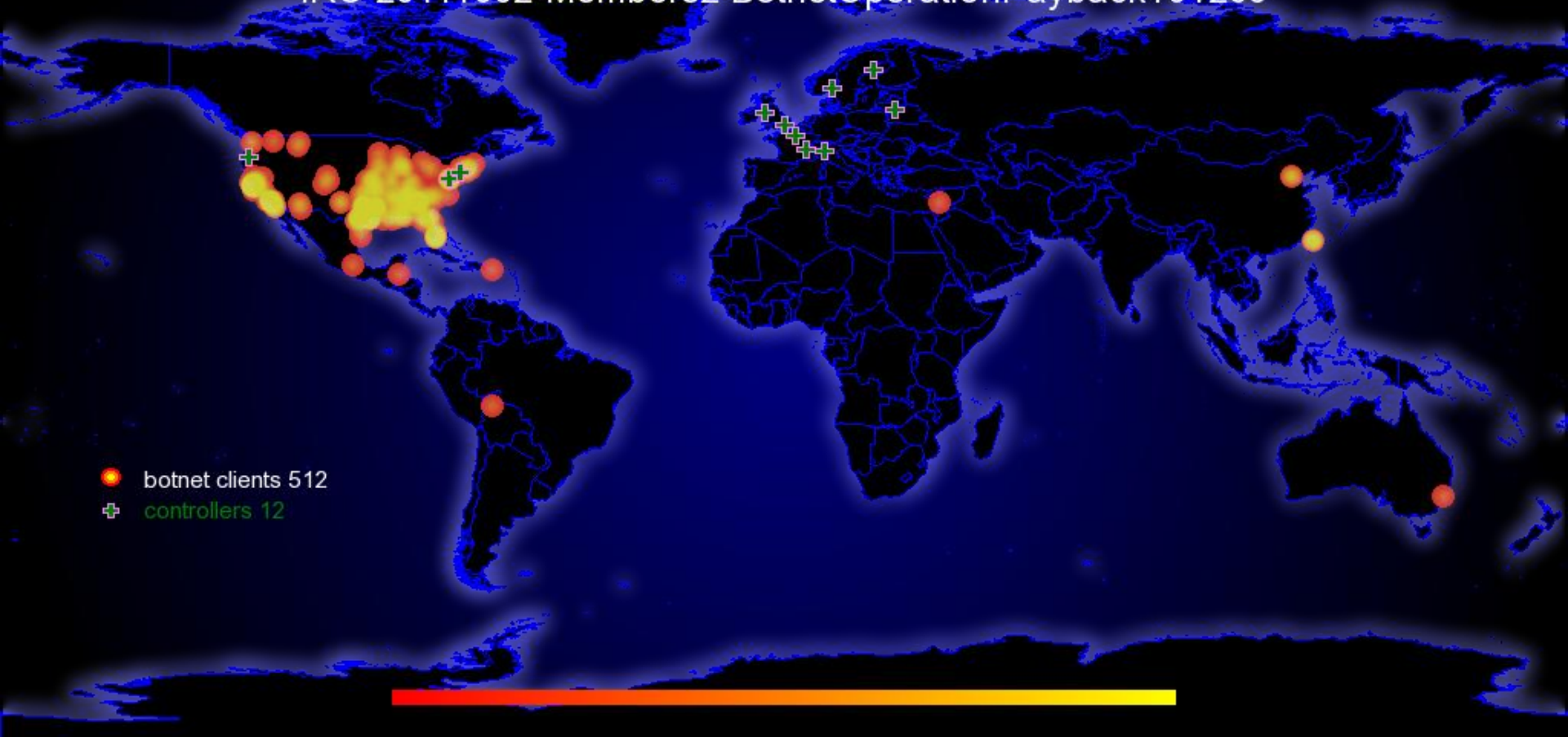
- This module allows the Zeus trojan to infect these Windows 7 and Vista systems. Without it, the botnet controller is limited to Windows XP systems.

* Source: *Secureworks*, <http://www.secureworks.com/research/threats/zeus>

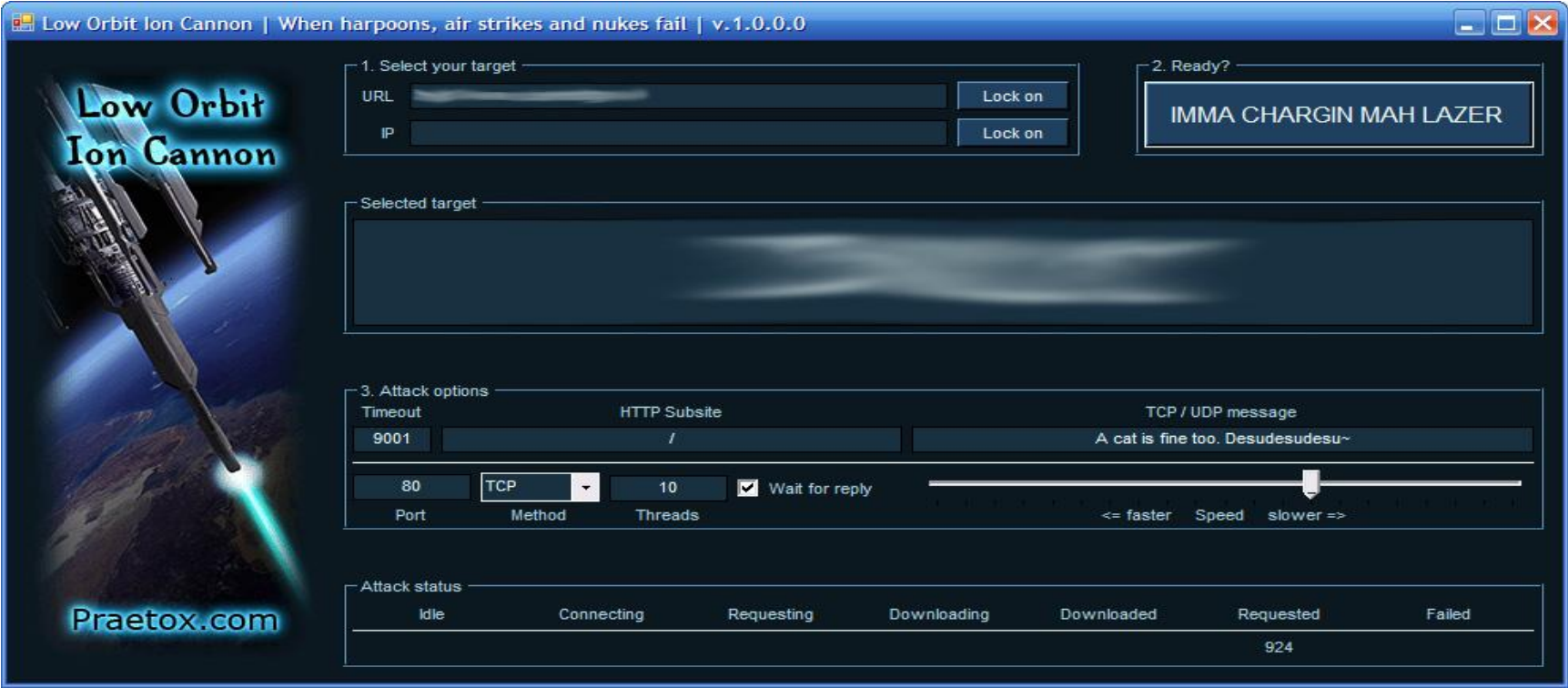


Active Botnets

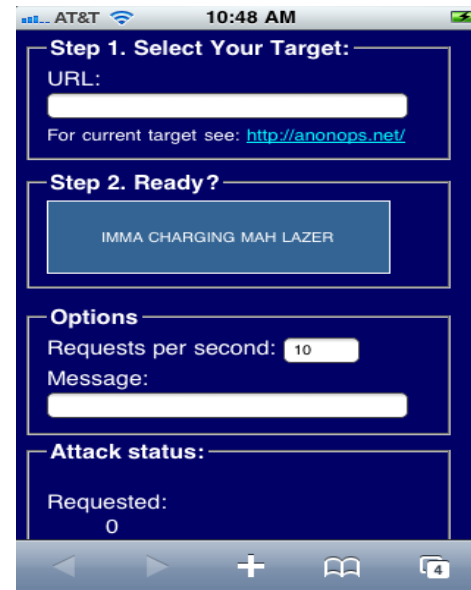
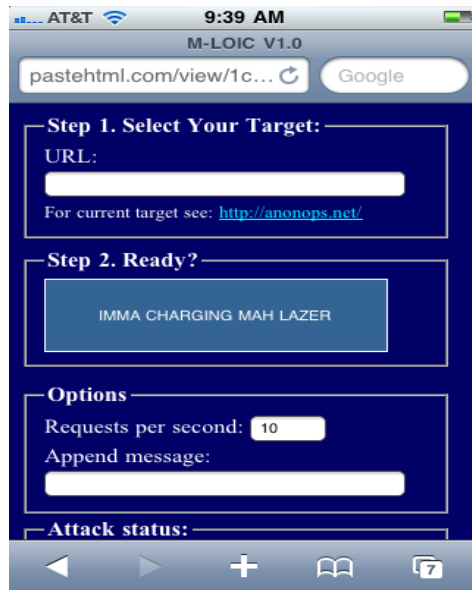
IRC-20111002-Members2 BotnetOperationPayback101209



DDOS Tool - Java Version



DDOS Tool - Mobile App



Timeline:

Javascript LOIC

Dec 9th 12:06 AM

M-LOIC 1.0

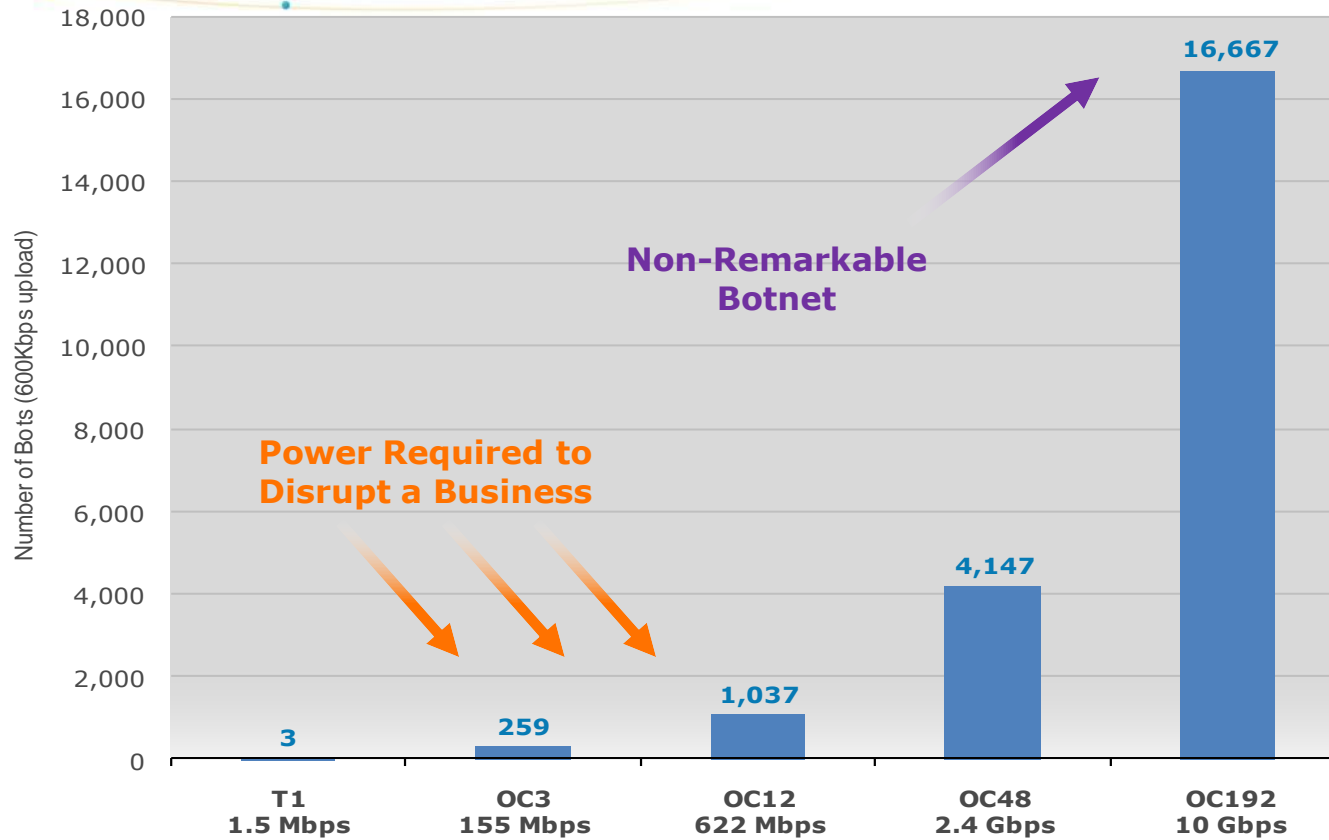
Dec 9th 11:38 AM

M-LOIC 1.4

Dec 9th 3:54 PM



Illustrative Power of Botnets



AT&T Botnet Defense Initiatives



Improving Detection Algorithms



DDoS Defense Service



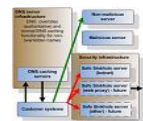
Spam Source Blocking



Submitting Malware Samples



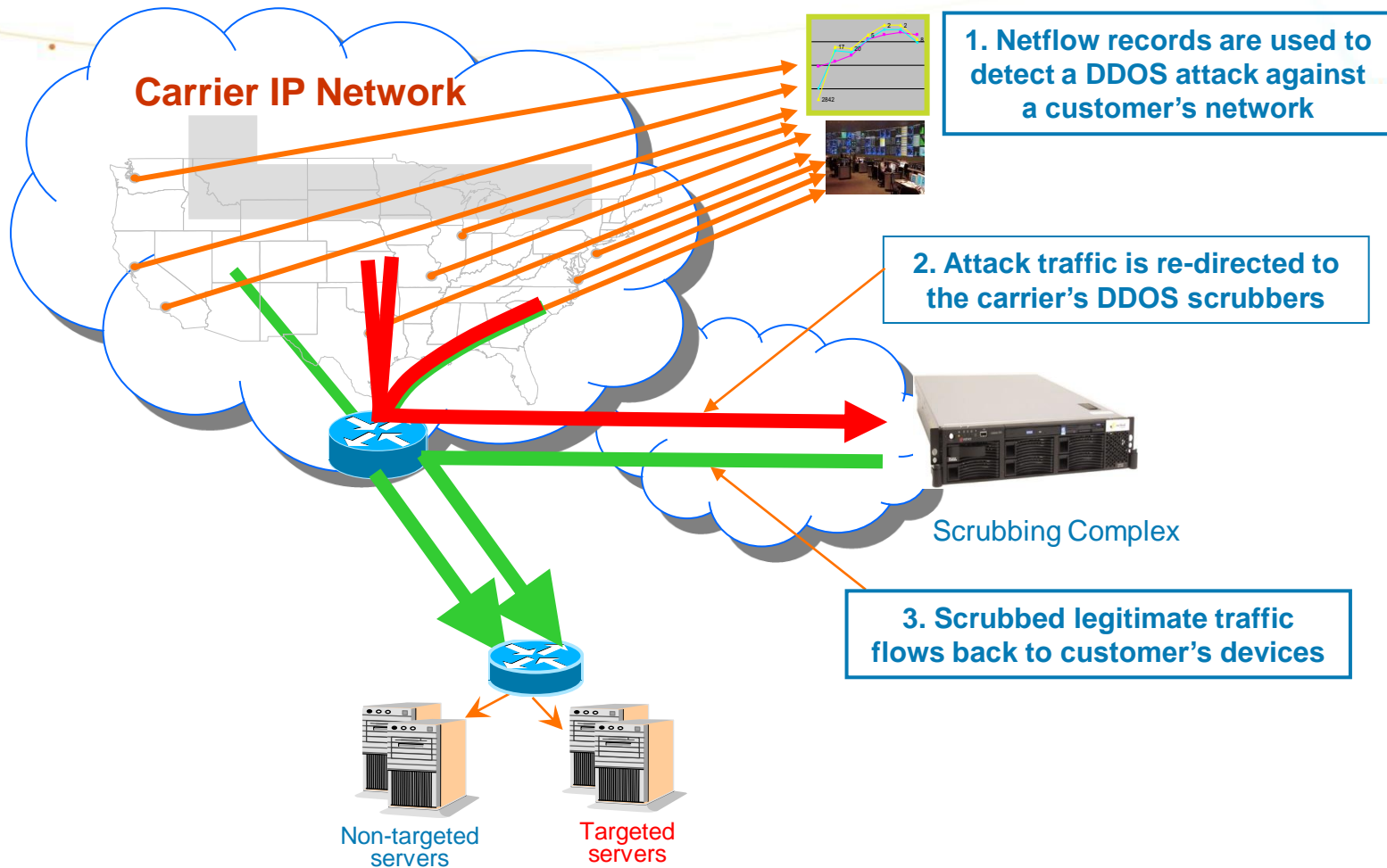
Customer bot Check





Botnet Aware Network



DDOS Defense Diversion Overview



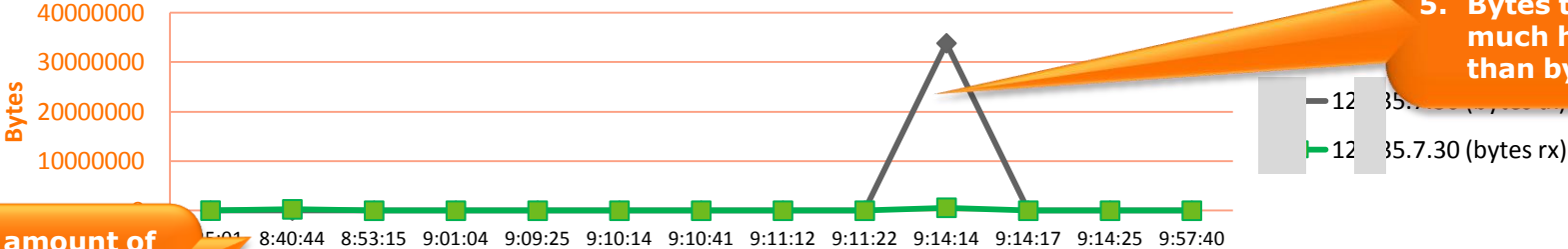
Advanced Persistent Threats (APT)

	Victim Targeting	Size	Stealth
Botnets and Worms 	Not specific	Large # victims	Generally noisy (spamming, scanning, DDoSing, frequent C&C check-in), somewhat detectable.
Advanced Persistent Threats 	Specific victims	Small # victims per target	Quiet, low-and-slow, fairly undetectable.



Exfiltration Event Victim Discovery

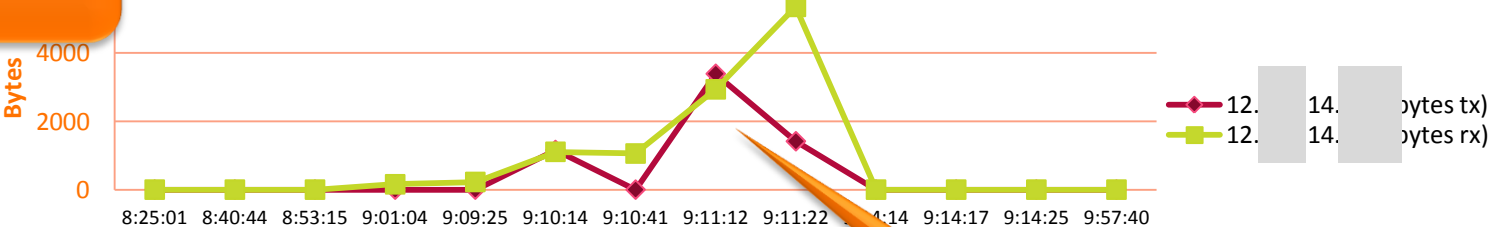
bytes tx/rx from victim to exfiltration drop site



1. Small amount of https traffic from victim to exfiltration server.

4. Victim transmits ~32MB to drop site.
5. Bytes tx is much higher than bytes rx

bytes tx/rx from exfiltration drop site to unknown host



2. Host makes an RDP connection to an unknown host.
3. Then connects to it over https (443/tcp) briefly



APT Tracking Tools Developed

ExfilTracker and AptTracker

ExfilTracker

Mozilla Firefox

File Edit View History Bookmarks Tools Help

att.com https://anlport.tsic.cso.att.com:9443/db

Most Visited Getting Started Latest Headlines John's Page

https://anlport.tsic.cso.att.com/Summary.html

Alarmed due to DNS change activity within past 10 days

Resolution change detected! 20110427 03:01:52

Resolution change detected! 20110427 00:57:51

Resolution change detected! 20110426 22:59:26

Resolution change detected! 20110426 21:12:06

Resolution change detected! 20110426 14:52:47

Resolution change detected! 20110426 12:55:09

Resolution change detected! 20110425 10:45:26

Resolution change detected! 20110425 08:43:28

Resolution change detected! 20110425 00:41:31

AptTracker

Mozilla Firefox

File Edit View History Bookmarks Tools Help

att.com https://anlport.tsic.cso.att.com:9443/db/mirror/fromAnl/AuroraTracker/20110426/20110426-194.106

Most Visited Getting Started Latest Headlines John's Page

https://anlport.tsic.cso.att.com/Summary.html

Protocol	# flows	# pkts	# bytes
UDP	0	0	0
ICMP	0	0	0
Other	0	0	0

*** Layer 7 Protocol activity by hour for 20110426 ***

Layer 7 Protocol	TOTAL	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
HTTP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IRC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DNS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HTTPS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SMB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SMTP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SSH	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TELNET	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FTP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RDP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Note: HTTPS, SMB, SMTP, SSH, Telnet and FTP are speculative and based solely on port/protocol matching in flows.
SMB is 135/tcp, 135/udp, 137/tcp, 137/udp, 138/tcp, 138/udp, 139/tcp, 445/tcp, 445/udp.
SMTP is 25/tcp. SSH is 22/tcp. Telnet is 23/tcp. FTP is 20/tcp and 21/tcp. RDP is 3389/tcp.
HTTP, IRC, DNS are based on actual Narus LS protocol decodes and counts are expressed as # recs. All other protocols are # fl

References to k, m, b, t, q are thousand, million, billion, trillion, quadrillion (base 1000)



Example: Spear Phish Email

Email

From real employee at one company

To real employees at another company

Targets

Similar roles in a common industry.

Live in the same general region.

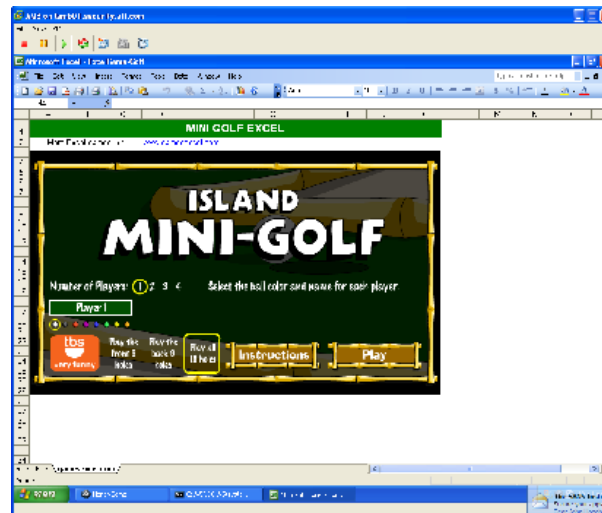
They are likely acquaintances

Malware

Content includes working spreadsheet-based game

Game retrieves malware, rootkits, sets-up to run on reboot, phones home

IP address that originated email is known contributor to this attack activity



Customer contacted and notified



Example: Exfiltrated Data Event Discovery

Event

AT&T ExfilTracker observed a 7MB .rar archive shuttled between one known exfiltration drop server to another known exfiltration drop server.

Contents

Contained recent email and documents.

Email subjects and filenames appear to be highly sensitive.

Targets

CEO and 4 VP's in a large International corporation.

```
$ rar v ./data.rar | more
RAR 3.93 Copyright (c) 1993-2010 Alexander Roshal 15 Mar 2010
Shareware version Type RAR -? for help

SFX Archive ./data.rar

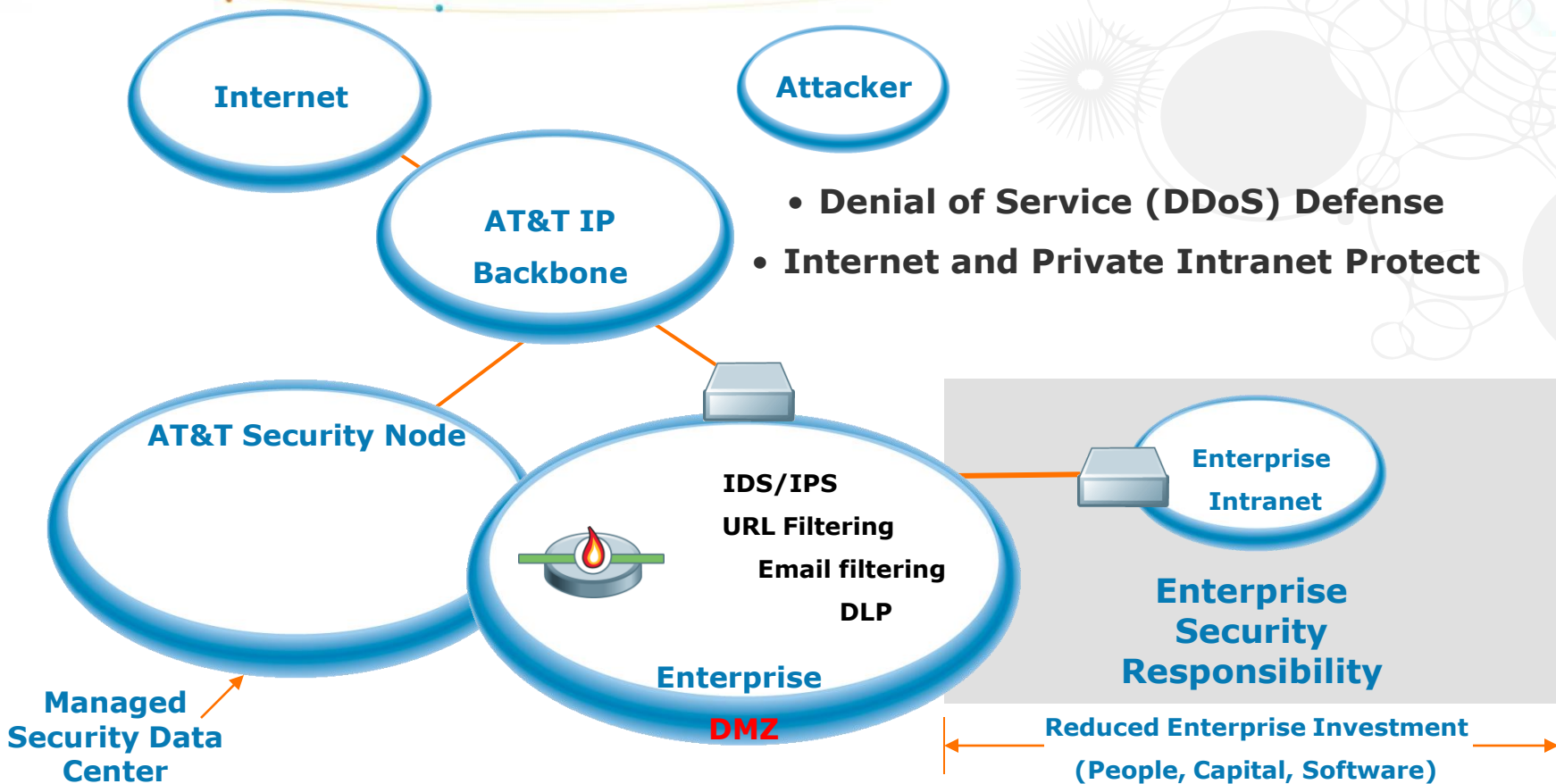
Pathname/Comment      Size   Packed Ratio  Date   Time   Attr   CRC   Meth Ver
-----
*windows/temp/t/mail/username/1/mail.txt
    6387    2352   36% 22-02-11 12:21   ....A.   9A0896A1 m3g 2.9
  windows/temp/t/mail/username/1
        0         0    0% 22-02-11 13:02
*windows/temp/t/mail/username/10-mail.txt
    6209    2496   40% 22-02-11 12:22
*windows/temp/t/mail/username/100/mail.txt
    9873    4144   41% 22-02-11 12:30
  windows/temp/t/mail/username/100
        0         0    0% 22-02-11 13:01
*windows/temp/t/mail/username/101-mail.txt
    2580    1024   39% 22-02-11 12:30
*windows/temp/t/mail/username/102-mail.txt
    2290    1056   46% 22-02-11 12:30
*windows/temp/t/mail/username/103-mail.txt
    2292    1072   46% 22-02-11 12:30
*windows/temp/t/mail/username/104/mail.txt
    4078    1680   41% 22-02-11 12:31
```



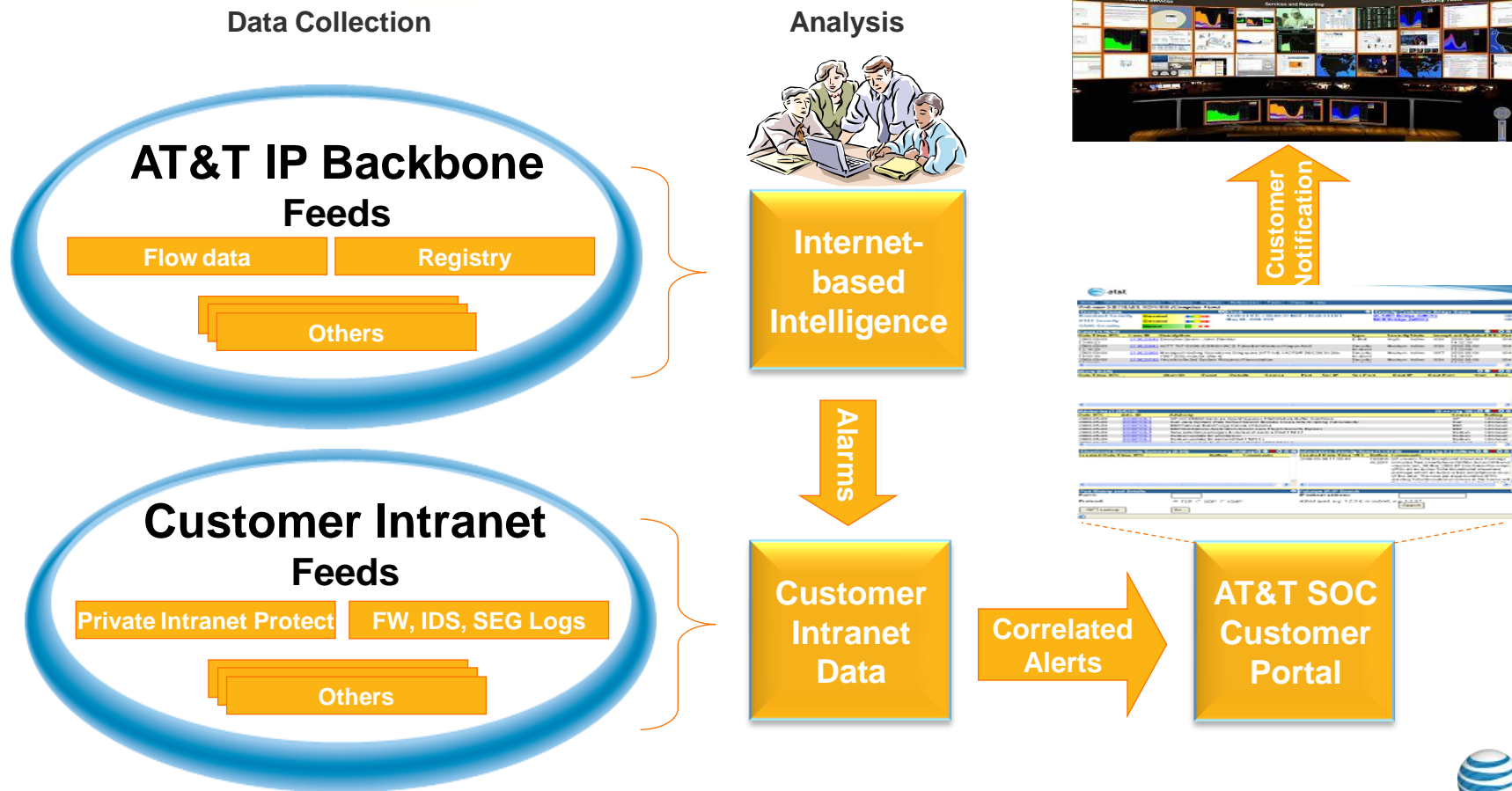
Customer contacted and notified



Network-Based Security Platform



Managed Security Service Information Flow



MTIPS Service

AT&T Government Solutions

Managed Trusted Internet Protocol Service (MTIPS)

Secure Public Internet Access for Federal Agencies

Challenge

Federal agencies are expected to comply with the Office of Management and Budget (OMB) Trusted Internet Connections Initiative – Memorandum 08-05 – which requires federal agencies to reduce the number of public Internet connections and secure their IP traffic to and from the public Internet.

By limiting the number of Internet connections across the Federal Government, the Trusted Internet Connections (TIC) Initiative reduces the security risk to federal agencies and enables the application of enhanced security management to the Internet connections that link federal agencies' IT infrastructure to public Internet.

Solution

AT&T offers a new TIC-compliant service, Managed Trusted Internet Protocol Service (MTIPS) on our Networkx contract. We are the first Networkx contract holder to be awarded the MTIPS from the General Services Administration.

Service components for MTIPS include:

- TIC portals providing secure connections to the public Internet
- Security Operations Center (SOC) for 24x7 surveillance of the TIC portals
- Transport from the agency locations to the TIC portal

Why should you buy AT&T MTIPS now?

We are the first Networkx contract holder to be awarded MTIPS from the General Services Administration.

How do you benefit from AT&T MTIPS?

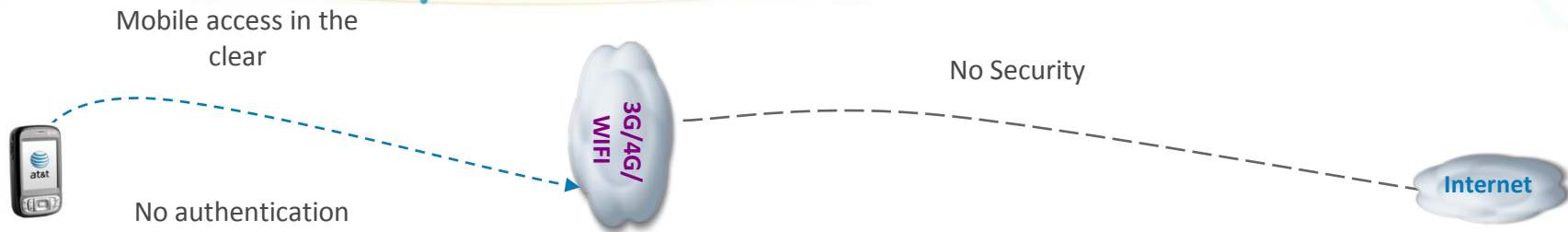
- **Comply with the OMB's Trusted Internet Connections (TIC) Initiative, a component of the Comprehensive National Cybersecurity Initiative (CNCI)**
- **Reduce the number of vulnerabilities using fewer external Internet connections, which are protected by a managed comprehensive security solution**
- **Enable a secure DMZ by integrating a managed firewall at the agency premise into the MTIPS service**
- **Leverage the security experience, and domestic and international network coverage of AT&T**

Service Elements

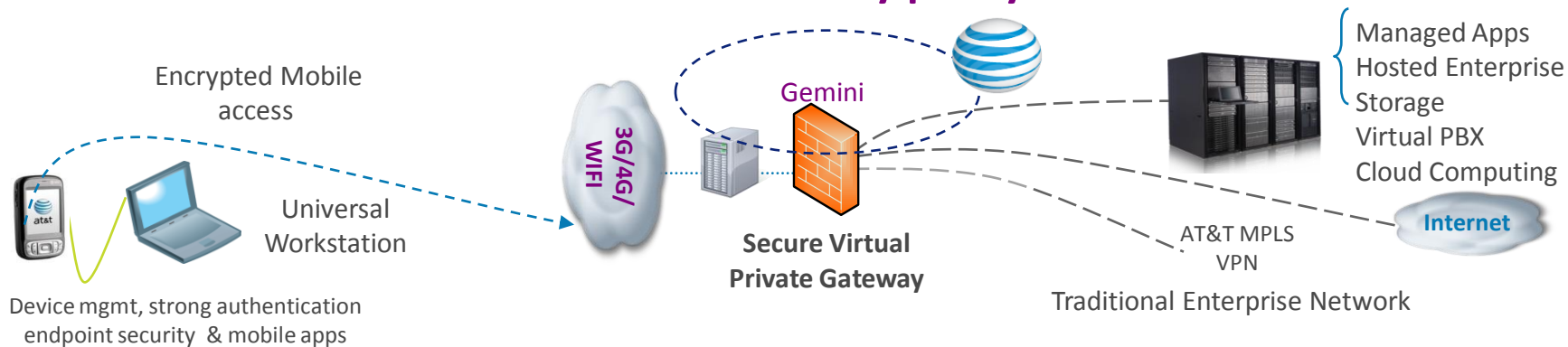
AT&T MTIPS combines new secure IP service offerings with existing AT&T security services offered through Networkx. You can choose from the following Basic Services and Optional Features:



Next Generation AT&T Mobile Security



AT&T Mobile Security provides Cloud Security with Botnet, Virus mitigation and secure encrypted transport to security node and enforces security policy



Cyber Threat Report – techchannel.att.com

The screenshot shows a web browser window displaying the AT&T Tech Channel website. The browser's address bar shows the URL <http://techchannel.att.com/>. The website's header features the AT&T logo and the text "AT&T Tech Channel". Below the header is a navigation bar with links for "HOME", "OUR SHOWS", and "ABOUT US", along with a search bar. The main content area displays a video player for a "Cyber Threat Report" dated "04/05/2012". The video title is "04/05/2012 - LeNa, Mass Code Injection, Flashback, Zeus, Internet Weather Report". The video player shows a blue background with the text "CYBER THREAT REPORT" and four video thumbnails of men. A large play button is centered over the thumbnails. Below the video player, there is a text box that reads "Questions or Feedback: CyberThreat@list.att.com".

Cyber Threat Report : 04/05/2012 - LeNa, Mass Code Injection, Flashback, Zeus, Internet Weather - Microsoft Internet Explorer p

<http://techchannel.att.com/>

Cyber Threat Report : 04/05/2012 - LeNa, Mass C...

AT&T Tech Channel

HOME | OUR SHOWS | ABOUT US

Search

Cyber Threat Report
04/05/2012 - LeNa, Mass Code Injection, Flashback,
Zeus, Internet Weather Report

CYBER THREAT REPORT

Questions or Feedback:
CyberThreat@list.att.com



Rethink Possible

