RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Brothers In Arms: How the Financial Sector Fought the Brobot Attacks

SESSION ID: TRM-T07

Denise Anderson
Vice President, Financial Services ISAC

Agenda

- What is an ISAC?
- Overview of the FS-ISAC – How We Share
- Role of Intelligence – We Saw Them Coming
- Overview of the Attacks – Trends and Phases
- Information Sharing During the DDoS
- DDoS - Lessons Learned

What is an ISAC?

Why ISACs?

Why ISACs?

- Trusted entities established by CI/KR owners and operators.
- Comprehensive sector analysis aggregation/ anonymization
- Reach-within their sectors, with other sectors, and with government to share critical information.
- All-hazards approach
- Threat level determination for sector
- Operational-timely accurate actionable

ISACs

- Communications ISAC
- Defense Industrial Base ISAC
- Electricity ISAC
- Emergency Management & Response ISAC
- Financial Services ISAC
- Information Technology ISAC
- Maritime ISAC
- Multi-State ISAC

ISACs

- National Health ISAC
- Oil and Natural Gas ISAC (ONG)
- Over the Road & Motor Coach ISAC
- Public Transit ISAC
- Real Estate ISAC
- Research and Education ISAC
- Supply Chain ISAC
- Surface Transportation ISAC
- Water ISAC

Other Operational Sectors and Upcoming ISACs

- **Automotive**
- **Aviation**
- Food & Ag
- Nuclear
- Chemical
- Critical Manufacturing

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Overview of FS-ISAC

Example of a Successful Model for Sharing

MISSION: Sharing Timely, Relevant, Actionable Cyber and Physical Security Information & Analysis

- A nonprofit private sector initiative formed in 1999
- Designed/developed/owned by financial services industry
- Assist to mitigate recent cybercrime & fraud activity
- Process thousands of threat indicators per month
- 2004: 68 members;
- 2014: 5,000+ members
- Sharing information globally

FINANCIAL SERVICES ISAC

FS-ISAC Operations

Information Sources

GOVERNMENT SOURCES

- DHS
- Treasury & FS Regulators
- FBI, USSS, NYPD
- Other Intel Agencies

- iSIGHT Partners Info Sec
- Secunia Vulnerabilities
- Wapack Labs Malware Forensics
- NC4 PhySec Incidents
- MSA Phy Sec Analysis

FS-ISAC 24x7
Security Operations Center

Cross Sector (other ISACS)

Open Sources (Hundreds)

CROSS SECTOR SOURCES

Member Communications

- Information Security
- Physical Security
- Business Continuity/ Disaster Response
- Fraud Investigations
- Payments/ Risk

Alerts

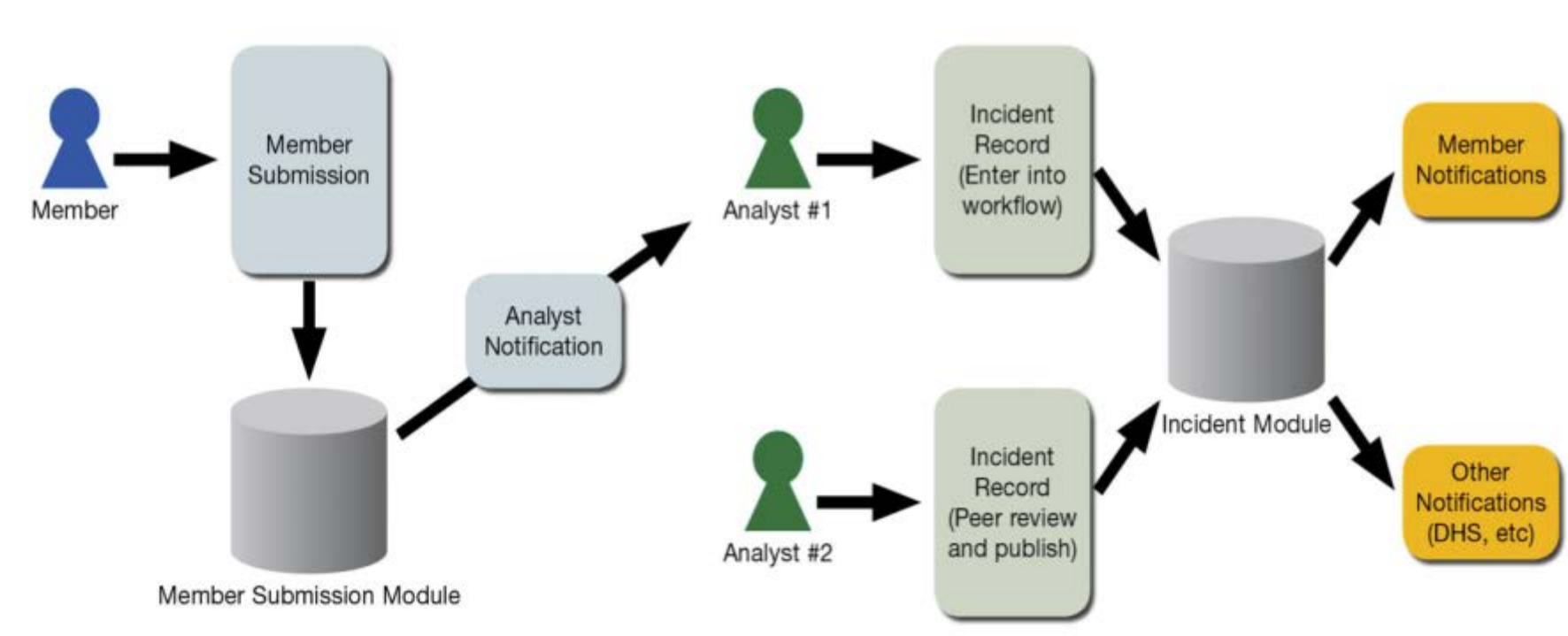
Member Submissions

Traffic Light Protocol (TLP)

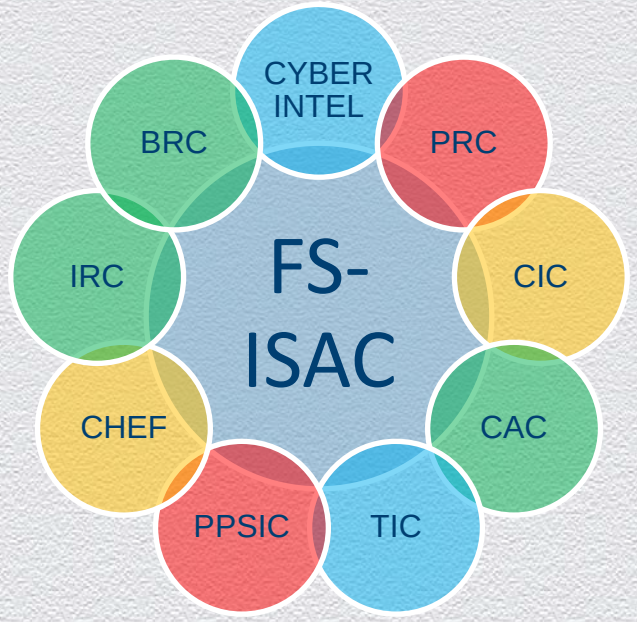
- Restricted to a defined group (e.g., only those present in a meeting.) Information labeled **RED** should not be shared with anyone outside of the group
- **AMBER** information may be shared with FS-ISAC members.
- **GREEN** Information may be shared with FS-ISAC members and partners (e.g., vendors, MSSPs, customers). Information in this category is not to be shared in public forums
- **WHITE** information may be shared freely and is subject to standard copyright rules

Member Submissions Via the Secure Portal

- **Anonymous or Attributed Submission Types: Cyber Incident, Physical Incident or Document Upload**



How FS-ISAC Works: Circles of Trust



- Clearing House and Exchange Forum (CHEF)
- Payments Risk Council (PRC)
- Payments Processor Information Sharing Council (PPISC)
- Business Resilience Committee (BRC)
- Threat Intelligence Committee (TIC)
- Community Institution Council (CIC)
- Insurance Risk Council (IRC)
- Compliance and Audit Council (CAC)
- Cyber Intelligence Listserv
- Education Committee
- Product and Services Review Committee
- Survey Review Committee
- Security Automation Working Group (SAWG)

Member Reports Incident to Cyber Intel list, or via anonymous submission through portal

Members respond in real time with initial analysis and recommendations

SOC completes analysis, anonymizes the source, and generates alert to general membership

Collaboration

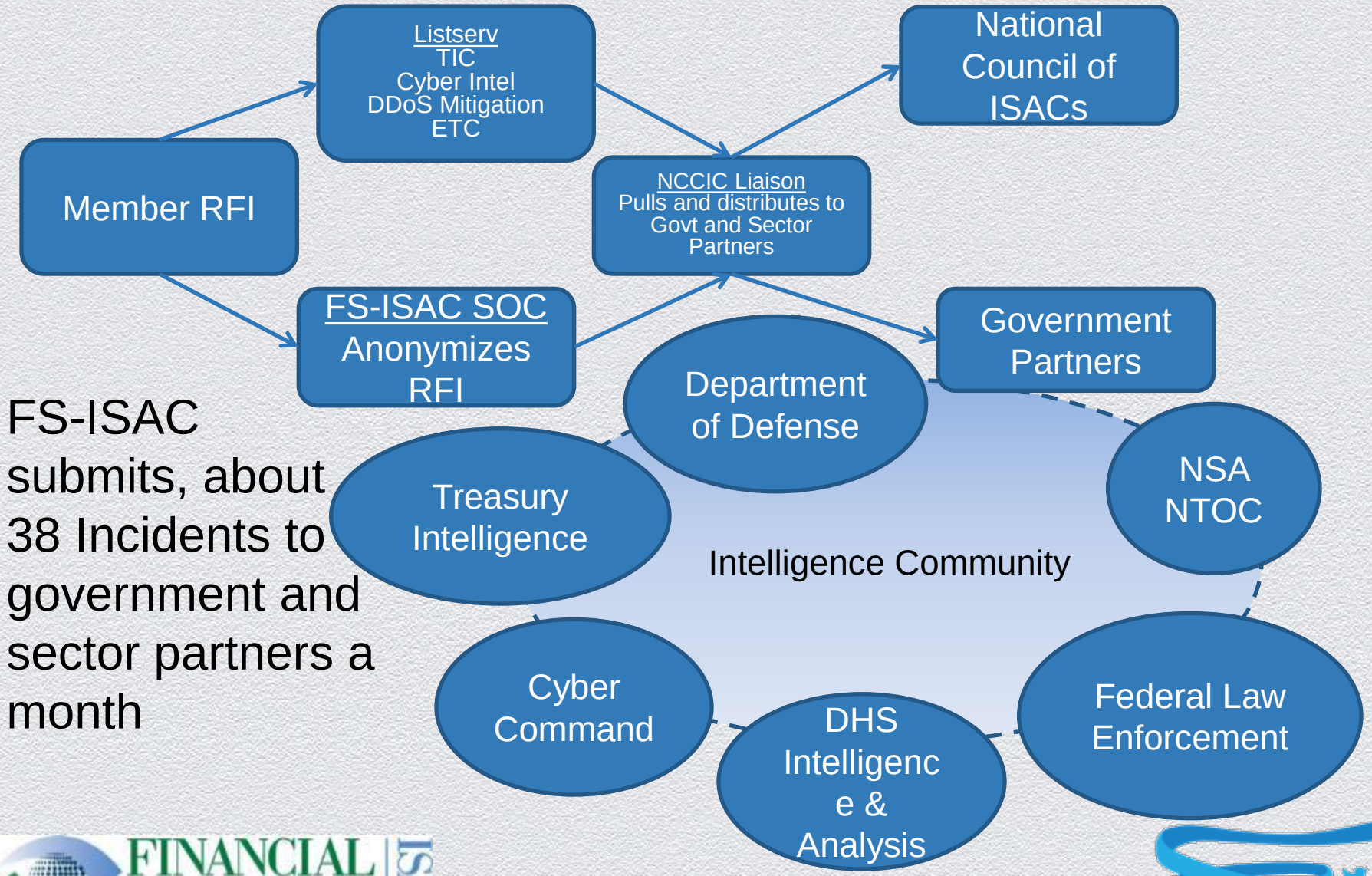
- **Cyberintel List**:

  700+ individuals / 179 companies

- **TIC**

  54 individuals / 26 companies

Information Sharing Flow - External



FS-ISAC submits, about 38 Incidents to government and sector partners a month

Information Sharing Statistics

Alert Statistics			
Alert Type	Jan-14	Feb-14	Mar-14
CISCP (Cyber Information Sharing & Collaboration Program)	91	88	68
Collective Intelligence	92	78	81
Cyber Incident	60	70	71
Cyber Threat	42	45	34
Cyber Vulnerability	104	119	133
Physical Incident	3	7	5
Physical Threat	4	8	2
PORTAL TOTAL	397	417	394
LISTSERV POST TOTAL	400	298	269
Bi-Weekly Threat Call Attendance	**301/251/293**	**279/276**	**277/284**
Heartbleed Mitigation Member Call (4/17/2014)	**800**		

- Portal versus Listserv

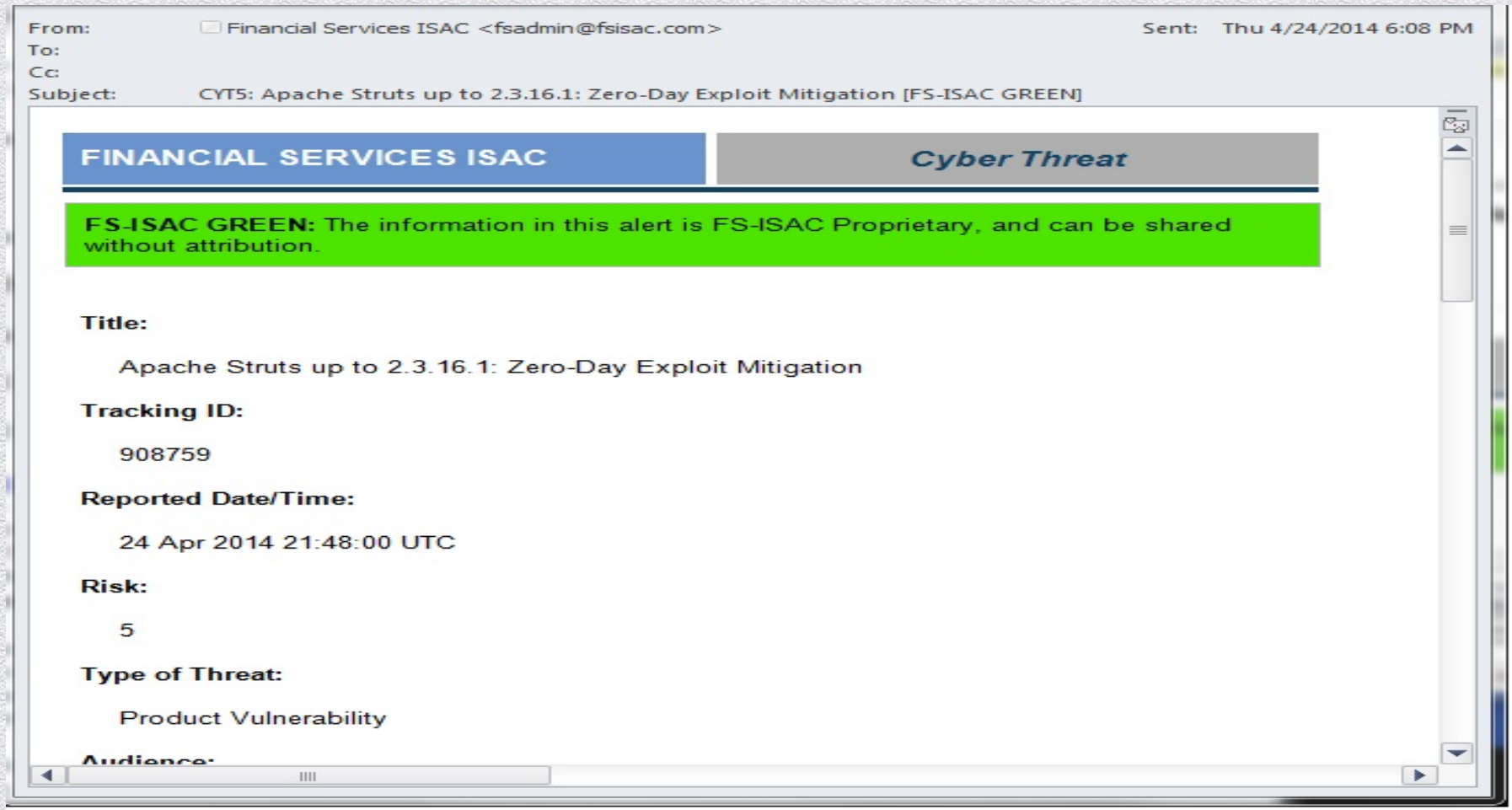
Types of Information Shared

- Denial of Service Attacks
- Malicious Emails: Phishing/Spearphishing Campaigns
- Software Vulnerabilities
- Malicious Software
- Malicious Sites

Sample of Listserv Sharing

- File: Shipment Label.exe
- Size: 49152
- MD5: BE636DEE8447C0EFF8985747108F351C
- URL: hxxp://tokobukuislamionline.com/wp-content/hunt.php?d_info=882_373246286
- Network connections / Bot communications
- GET /2D8AE3D34A40FD3FAD57567FB63670215CDD634290413F6345A973622CAE682CAC00722E289B78BBEC9BA46F830CD99D2216FC226B9B631108520D733412667432E0308CFFC12DC423DD20FD104090 HTTP/1.1
- 88.191.139.235

Sample Alert



From: Financial Services ISAC <fsadmin@fsisac.com> Sent: Thu 4/24/2014 6:08 PM
To:
Cc:
Subject: CYT5: Apache Struts up to 2.3.16.1: Zero-Day Exploit Mitigation [FS-ISAC GREEN]

FINANCIAL SERVICES ISAC | *Cyber Threat*

FS-ISAC GREEN: The information in this alert is FS-ISAC Proprietary, and can be shared without attribution.

Title:

Apache Struts up to 2.3.16.1: Zero-Day Exploit Mitigation

Tracking ID:

908759

Reported Date/Time:

24 Apr 2014 21:48:00 UTC

Risk:

5

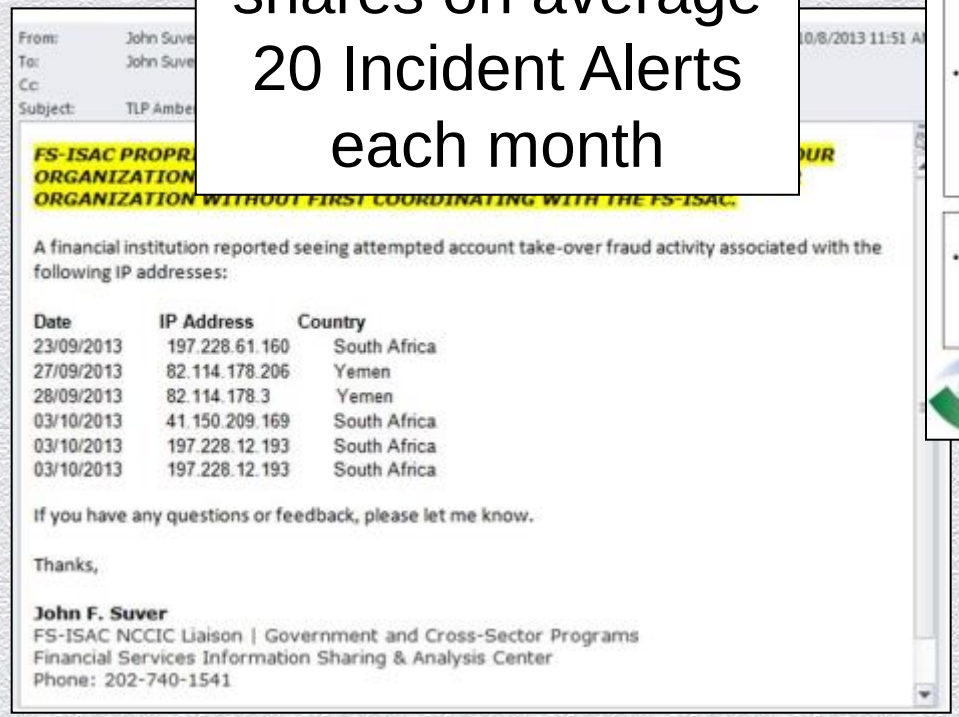
Type of Threat:

Product Vulnerability

Audience:

FS-ISAC Products

FS-ISAC Incident Alert: FS-ISAC shares on average 20 Incident Alerts each month



From: John Suve
To: John Suve
Cc:
Subject: TLP Ambe

FS-ISAC PROPR... ...OUR ORGANIZATION
ORGANIZATION WITHOUT FIRST COORDINATING WITH THE FS-ISAC.

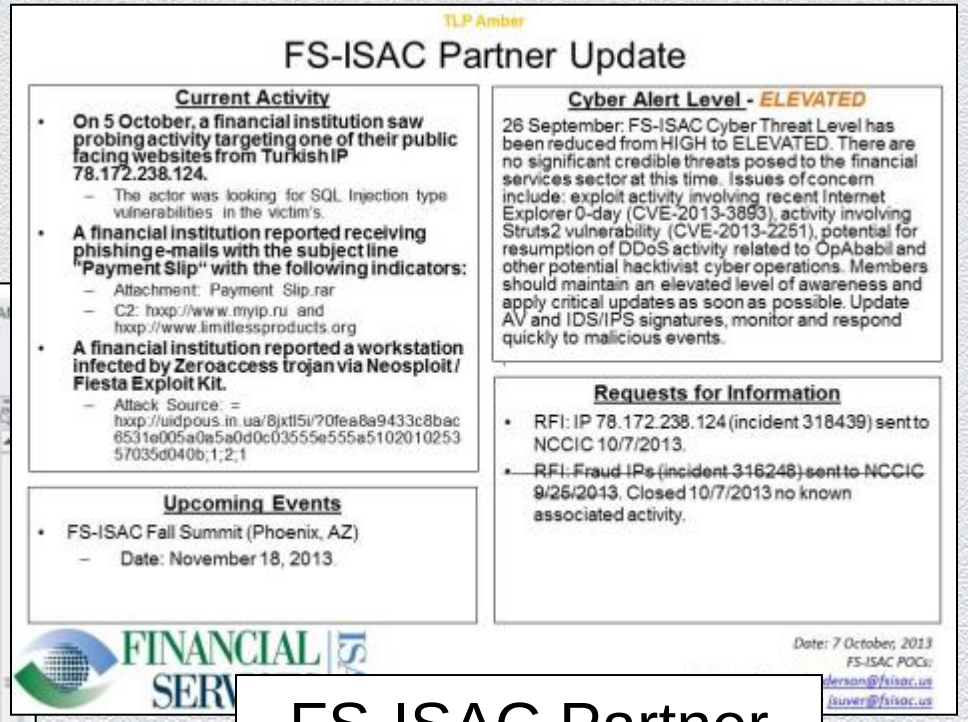
A financial institution reported seeing attempted account take-over fraud activity associated with the following IP addresses:

Date	IP Address	Country
23/09/2013	197.228.61.160	South Africa
27/09/2013	82.114.178.206	Yemen
28/09/2013	82.114.178.3	Yemen
03/10/2013	41.150.209.169	South Africa
03/10/2013	197.228.12.193	South Africa
03/10/2013	197.228.12.193	South Africa

If you have any questions or feedback, please let me know.

Thanks,

John F. Suver
FS-ISAC NCCIC Liaison | Government and Cross-Sector Programs
Financial Services Information Sharing & Analysis Center
Phone: 202-740-1541



TLP Amber

FS-ISAC Partner Update

Current Activity

- **On 5 October, a financial institution saw probing activity targeting one of their public facing websites from Turkish IP 78.172.238.124.**
  - The actor was looking for SQL Injection type vulnerabilities in the victim's.
- **A financial institution reported receiving phishing e-mails with the subject line "Payment Slip" with the following indicators:**
  - Attachment: Payment Slip.rar
  - C2: hxxp://www.myip.ru and hxxp://www.limitlessproducts.org
- **A financial institution reported a workstation infected by Zeroaccess trojan via Neosploit / Fiesta Exploit Kit.**
  - Attack Source: = hxxp://uidpous.in.ua/8jxtl5i/?0fea8a9433c8bac6531e005a0a5a0d0c03555e555a510201025357035d040b;1;2;1

Upcoming Events

- FS-ISAC Fall Summit (Phoenix, AZ)
  - Date: November 18, 2013

Cyber Alert Level - *ELEVATED*

26 September: FS-ISAC Cyber Threat Level has been reduced from HIGH to ELEVATED. There are no significant credible threats posed to the financial services sector at this time. Issues of concern include: exploit activity involving recent Internet Explorer 0-day (CVE-2013-3893), activity involving Struts2 vulnerability (CVE-2013-2251), potential for resumption of DDoS activity related to OpAbabil and other potential hacktivist cyber operations. Members should maintain an elevated level of awareness and apply critical updates as soon as possible. Update AV and IDS/IPS signatures, monitor and respond quickly to malicious events.

Requests for Information

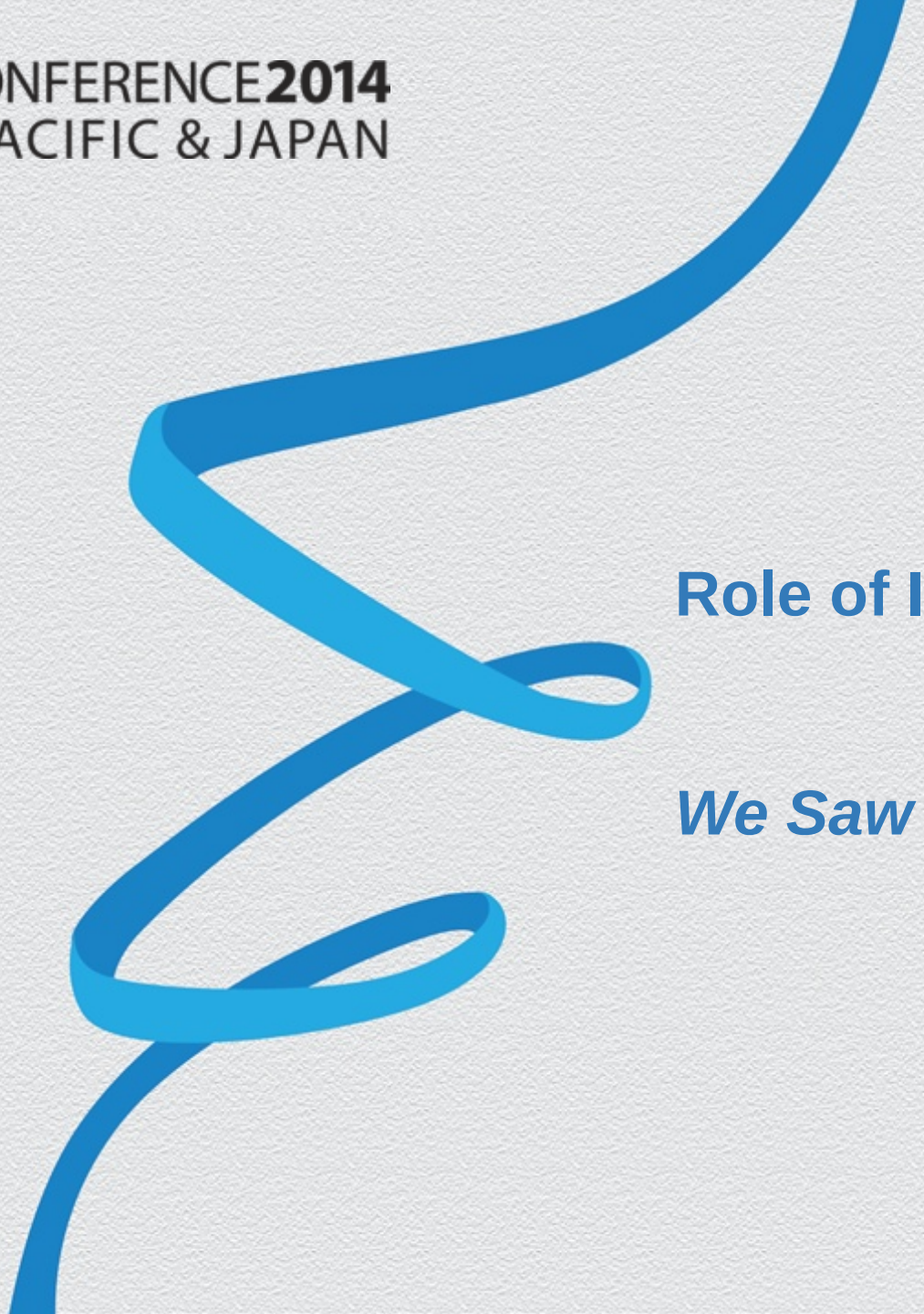
- RFI: IP 78.172.238.124 (incident 318439) sent to NCCIC 10/7/2013.
- ~~RFI: Fraud IPs (incident 316248) sent to NCCIC 9/25/2013~~. Closed 10/7/2013 no known associated activity.

FINANCIAL SERV...

Date: 7 October, 2013
FS-ISAC POCs:
...erson@fsisac.us
...suver@fsisac.us

FS-ISAC Partner Update: FS-ISAC shares on average 21 Partner Update Slides each month

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN



Role of Intelligence

We Saw Them Coming

We Saw Them Coming….

- Monitoring DDoS activity with similar technical characteristics observed against sector since late 2011/early January.
- Based on activity – developed and distributed updated DDoS Threat Viewpoint. Revision will be available August 2013.
- Reconnaissance – Alerts on known tool signatures
- Monitoring activity against other sectors and sharing partners. Held briefings as appropriate.

We Saw Them Coming….

- **Ability to see scripts loaded onto Bot nodes, alerted banks being targeted**
- Active collaboration between targeted FS-ISAC members and US Govt including Joint Indicator Bulletins (JIBs) and Early Warning Indicator Notifications (EWINs) to targeted institutions and to membership under AMBER.
- Ongoing monitoring of intelligence and collaboration with private sector and government partners for analysis

Overview of the Attacks

Trends and Phases

Phase I – Op Ababil

- **Dates of Activity: 9/18/2012 to 10/18/2012**
- **Announcement**
  - In Sept threats actors announced attacks/targets on Pastebin/Blogspot.
  - General announcements were seen in all phases (via Pastebin on Tuesdays that attacks would occur) but the actual calling out of specific targets was only seen in Phase 1.
- **Targeting**
  - Generally One FI at a time.

Phase I – Op Ababil

- **Timing**
  - Tuesday, Wednesday, Thursday.
  - 10am-6pm although residual traffic into the night and next day(s).
- **Attack Capacity**
  - Started slowly 3-4 GBPS in first wave.
  - Second wave later in the day ramps up.
  - Peaked up to 80 GBPS and packets 70 MPPS.

Phase I - Op Ababil

- **Steps in attack:**
  - Port 80 SYN Flood with some UDP to overwhelm network bandwidth if possible.
  - Attack DNS Servers with malformed UDP/TCP packets.
  - Attack DNS ports on web servers.
  - Attack SSL Connections.
  - URLs (latest tactic) switch from main site to secondary sites.
  - HTTP/HTTPS Post attacks (Search functions).
  - Ports 80/443/53

Phase I - Op Ababil

- **Tools**
  - Most of the tools known (Kamikaze and Brobot) but customized. *Itsoknoproblembro*
- **Attackers were adaptive**
  - Significant volume (Bandwidth/Packets) constant morphing (Port/Protocol).
  - On the fly customization of attacks to address mitigation.
  - Ability to compromise and then utilize malware-infected servers with high bandwidth connections.
  - Ability to add to bots and add new clients to evade IP filters/blacklists.

Phase II - Op Ababil

- **Dates of Activity:** 12/11/2012 to 1/24/2013
- **Announcement**
  - General announcements were seen via Pastebin on Tuesdays that attacks would occur.
- **Targeting**
  - Number of targets and attacked on average 6 to 13 FI's in a day
  - On 24 Jan, QCF targeted 23 FIs

Phase II - Op Ababil

- Targets included Fis both on and off of the top 50 holdings list
- 23 new targets were added
- 127 unique attacks
- **Timing**
  - Tuesday, Wednesday, Thursday.
  - Attack started at random times in the morning and afternoon. Seen in multiple waves.
  - General attack duration was reduced from phase one

Phase II - Op Ababil

- **Attack Capacity**
  - Peaks up to 85 Gbps
- **Tools**
  - Most of the tools known (Kamikaze and Brobot) but customized. *Itsoknoproblembro*
  - Traffic Seen Over Ports 80, 443, 53, 1800
- **Attackers Adapt - new tactics:**
  - PDF Downloads - L7 attacks against PDFs – PDF Downloads
  - Logins Jammed

Phase II - Op Ababil

- URL Strings and patterns
- New traffic pattern consisting of SYN-PUSH-ACK packet types.
- Increase in new, unique targeting IPs,
- AQCF tried low and slow attacks, and they've also been observed to attempt POST against login portals.
- Ability to increase Bot size rapidly

Phase III - Op Ababil

- **Dates of Activity:** 3/5/2013 to 5/2/2013
- **Anouncement**
  - General announcements were seen via Pastebin on Tuesdays that attacks would occur.
  - On Monday, 25 February, AQCF targeted 22 Financial institutions; Phase three attacks started 8 days later.
- **Targeting**
  - Number of targets ranged from 3 to 12 FI's in a day
  - Targets included Fis both on and off of the top 50 holdings list

Phase III - Op Ababil

- 8 New targets added
- FS-ISAC saw a total of 38 institutions attacked during Phase III
- There were a total of 195 unique attacks.

- **Timing**
  - Tuesday, Wednesday, Thursday.
  - Attack started at random times in the morning and afternoon. Seen in multiple waves.
  - General attack duration was reduced from phase two

Phase III - Op Ababil

- **Tools**
  - Most of the tools known (Kamikaze and Brobot) but customized. *Itsoknoproblembro*
  - Traffic Seen Over Ports 80, 443, 53, 1800
- **Attackers Adapt - new tactics:**
  - increase in targeted number of URLs, giving the attacker a broader attack spectrum against a single institution

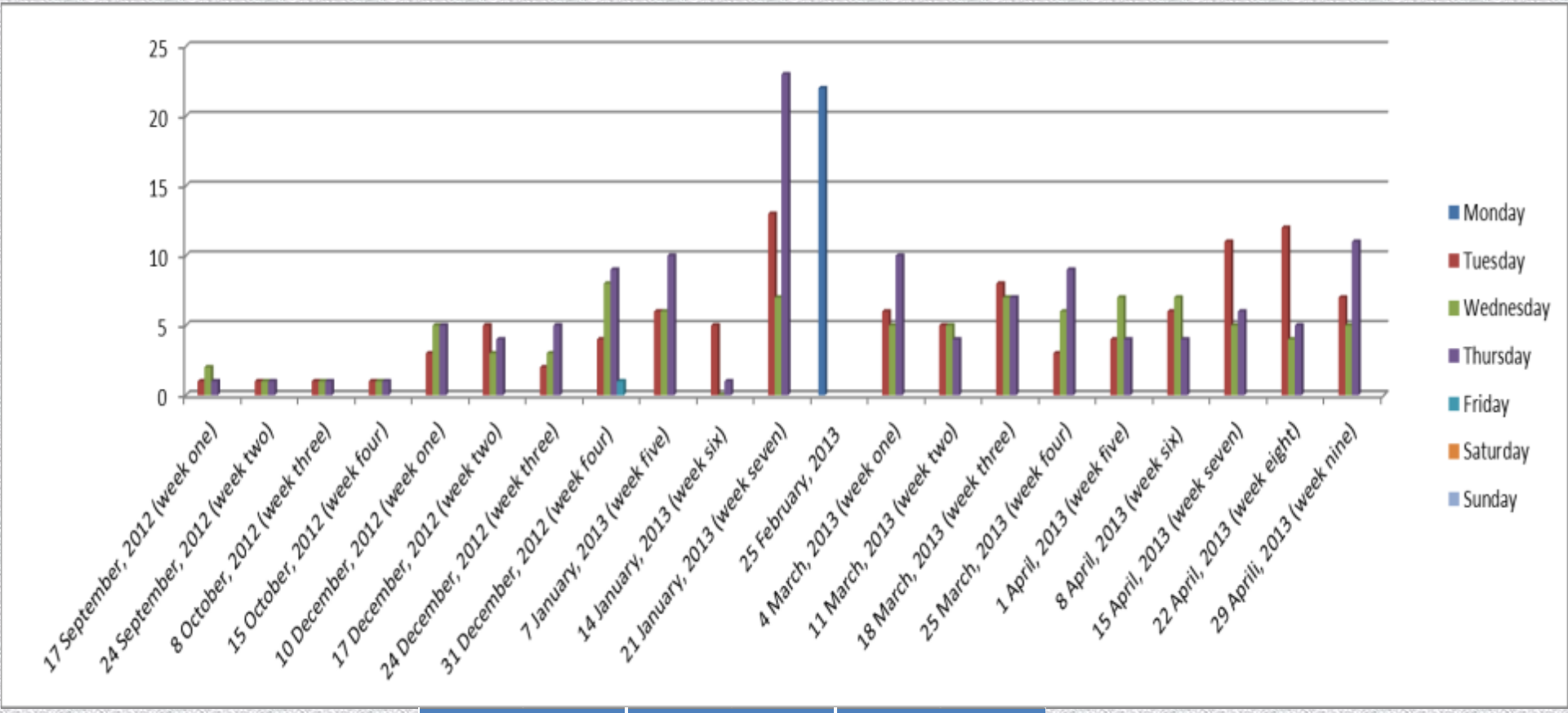
Phase III - Op Ababil

- Increased number of attack scripts:
  - Kamikaze/Toxin
  - Brobot
  - Vertigo
  - Assasin
  - KongFu
  - Kamina
  - Upchagi
  - Dragonkiss
  - Terminator

Comparison Summary of Phases

Indicator	Phase I – 9/18/2012 to 10/18/2012	Phase II – 12/11/2012 to 1/24/2013	Phase III – 3/5/2013 to 5/2/2013
Announcement	Yes for most	No	No
Number of Unique FI attacked	11	33	38
Number of Unique Attacks	13	129	195
Number of FIs/day	1	5 (max 23)	6 (max 12)
Days of Attack	T-TH	T-TH	T-TH
Attack Times	10:30am-5:00pm	Random morning and afternoon waves	Random morning and afternoon waves
Attack Duration (average)	7 hours (average)	4 hours (average)	3 hours (average)
Peak Traffic	80GBS	85GBS	162GBS
New Targets	11	23	8
Break After Phase	7 Weeks	5 Weeks	Currently 6 Weeks
Floods	Yes	Yes	Yes
Logins Jammed	-	Yes	Yes
PDF Download	-	Yes	Yes
Search Function	Yes	Yes	Yes
URL Strings	-	Yes	Yes
Low Slow Attacks	-	-	Yes
Blended Attack Scripts	-	-	Yes

Attacks Per Week



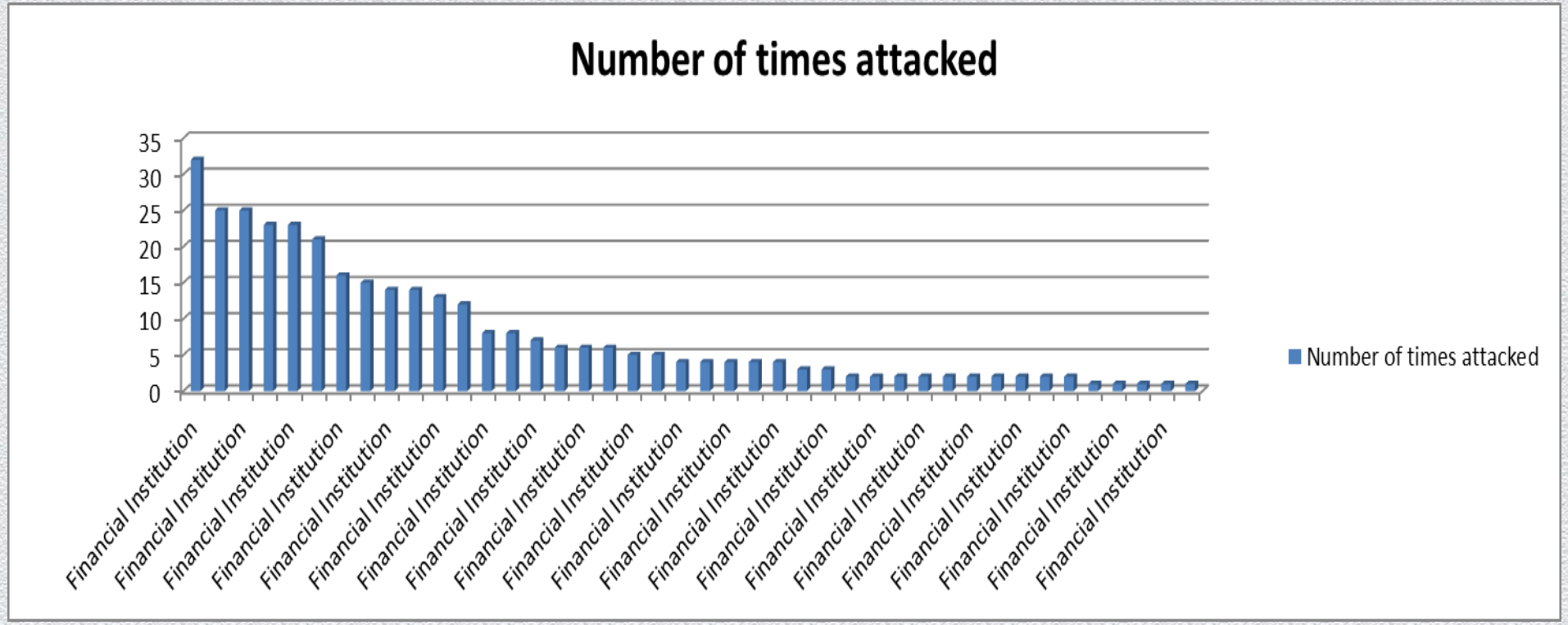
Phase I – 17 Sep to 15 Oct	Phase II – 10 Dec to 21 Jan	Phase III – 4 Mar to 29 Apr

- **335** 'distributed denial-of-service' attacks against banks 9/17/12 to 5/2/2013
- **42** unique banks victimized – up to **23** per day.

FINANCIAL SERVICES ISAC

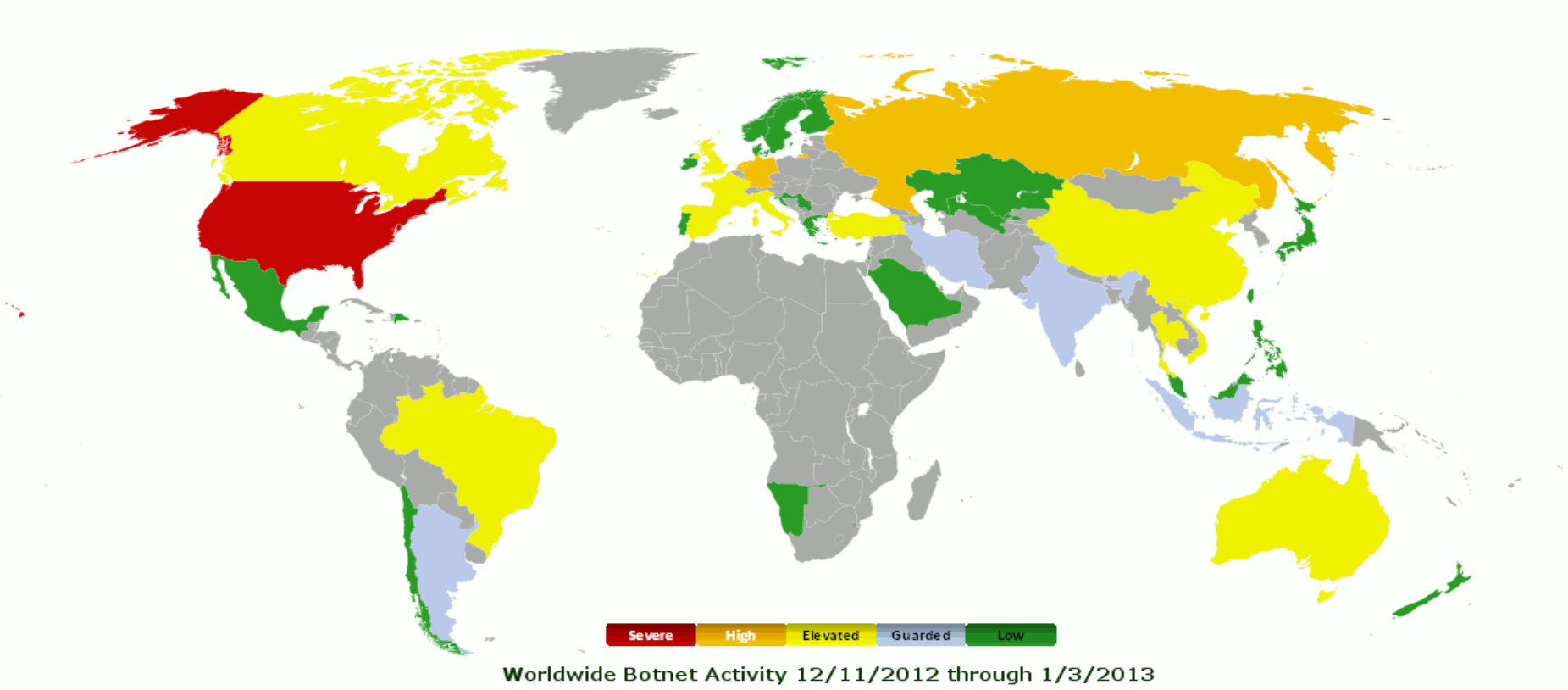
Attacks Per Institution

- **From 9/17/12 to 5/2/2013 attacks ranged from 32 to 1**



Brobot Size

- **Highly** distributed network of compromised servers
- December 2012: ~**2,500** bots grew to ~**28,887** active URLs in April 2013



Worldwide Botnet Activity 12/11/2012 through 1/3/2013

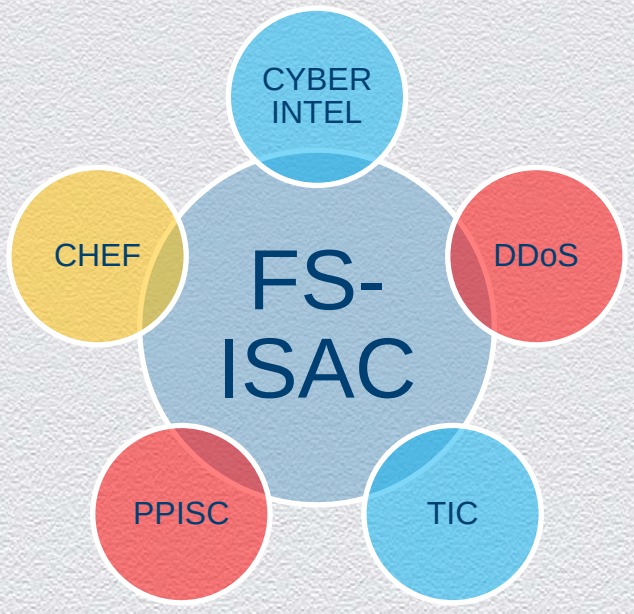
RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Sharing During the DDoS Attacks

Together We Stand

#RSAC

How FS-ISAC Works: Circles of Trust



- DDoS Mitigation Group
- 133 Individuals
- 36 Companies

Member being attacked reports to DDoS group

Members respond in real time with initial analysis and recommendations

FS-ISAC staff anonymizes the source, and generates alert to general membership, government partners and cross-sector partners.

Type of Information Shared

Denial of Service Attacks

Start time/Stop time
Internet Protocol (IP) Addresses
Type of Attack ie. *SYN Flood, UDP GET Flood, Port(s) 443, 80 and 53*
Script Type ie. *Kamikaze/Toxin; Brobot, Kamina, Dragonkiss, Umagi, King Kong, Vertigo, Assasin*
Bandwidth ie. *Mbps or Gbps*
Packets per second and packet size
Effect on Financial Institution if any

Sample of Sharing Thread

I am attaching our current IP blocklist As I've mentioned previously, this list is blocking more than 99.9% of the bad traffic.

At 9:00 am ET today, 46.10 million sessions were denied over the last one hour period. That number is down from 83.06 million 24 hours prior. Still sounds pretty high to me though for "residual traffic".

We continue to see DDoS attack traffic. All being dropped at moment…..

At 1:07pm, an iRule to block PDFs was implemented..sharing…

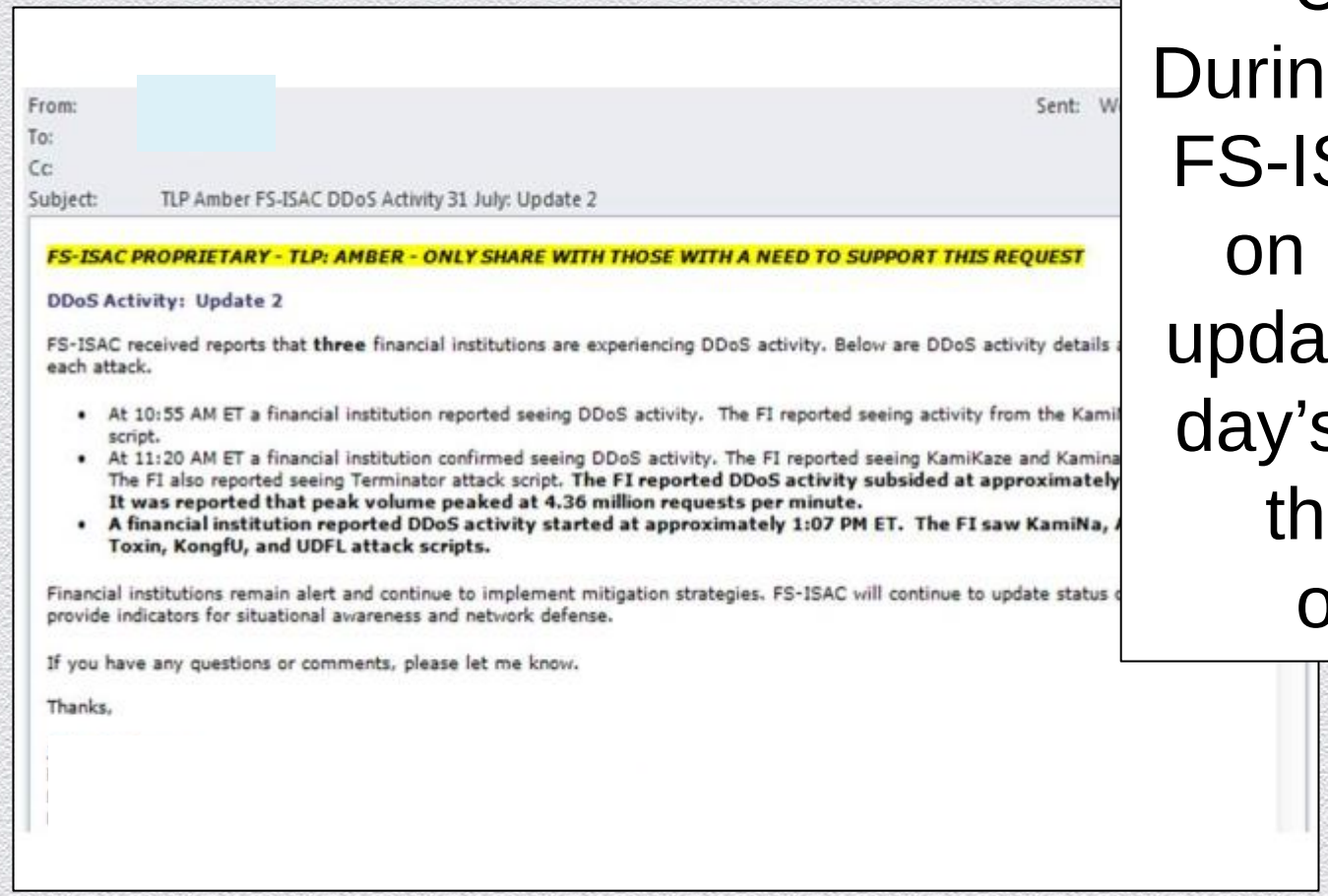
START iRules
"//50e" := "block",

Sharing with Partners and Government

FS-ISAC has received **four** reports of DDoS activity.

- A financial institution reported seeing DDoS activity from 8:15 AM ET to 8:45 AM ET. The FI reported seeing traffic reaching X Gbps. **The FI reported activity resumed at approximately 10:40 AM ET.**
- A financial institution reported seeing DDoS activity beginning around 9:15 AM ET. The FI reported seeing UDP floods to port 443. The FI reported peak volume at roughly X. **The FI reported activity targeted login fields over HTTPS.**
- **At approximately 11:10 AM ET a financial institution reported seeing DDoS activity. The FI reported seeing TCP floods to 443 and PDF GETS. Traffic volume reached approximately X Gbps.**
- **A financial institution reported seeing SYN 443 floods from approximately 10:30 AM ET and lasting for about 25 minutes.**

Example of Reporting



From:
To:
Cc:
Subject: TLP Amber FS-ISAC DDoS Activity 31 July: Update 2

Sent: W

FS-ISAC PROPRIETARY - TLP: AMBER - ONLY SHARE WITH THOSE WITH A NEED TO SUPPORT THIS REQUEST

DDoS Activity: Update 2

FS-ISAC received reports that **three** financial institutions are experiencing DDoS activity. Below are DDoS activity details
each attack.

- At 10:55 AM ET a financial institution reported seeing DDoS activity. The FI reported seeing activity from the Kami
script.
- At 11:20 AM ET a financial institution confirmed seeing DDoS activity. The FI reported seeing KamiKaze and Kamina
The FI also reported seeing Terminator attack script. **The FI reported DDoS activity subsided at approximately**
It was reported that peak volume peaked at 4.36 million requests per minute.
- **A financial institution reported DDoS activity started at approximately 1:07 PM ET. The FI saw KamiNa,**
Toxin, KongfU, and UDFL attack scripts.

Financial institutions remain alert and continue to implement mitigation strategies. FS-ISAC will continue to update status
provide indicators for situational awareness and network defense.

If you have any questions or comments, please let me know.

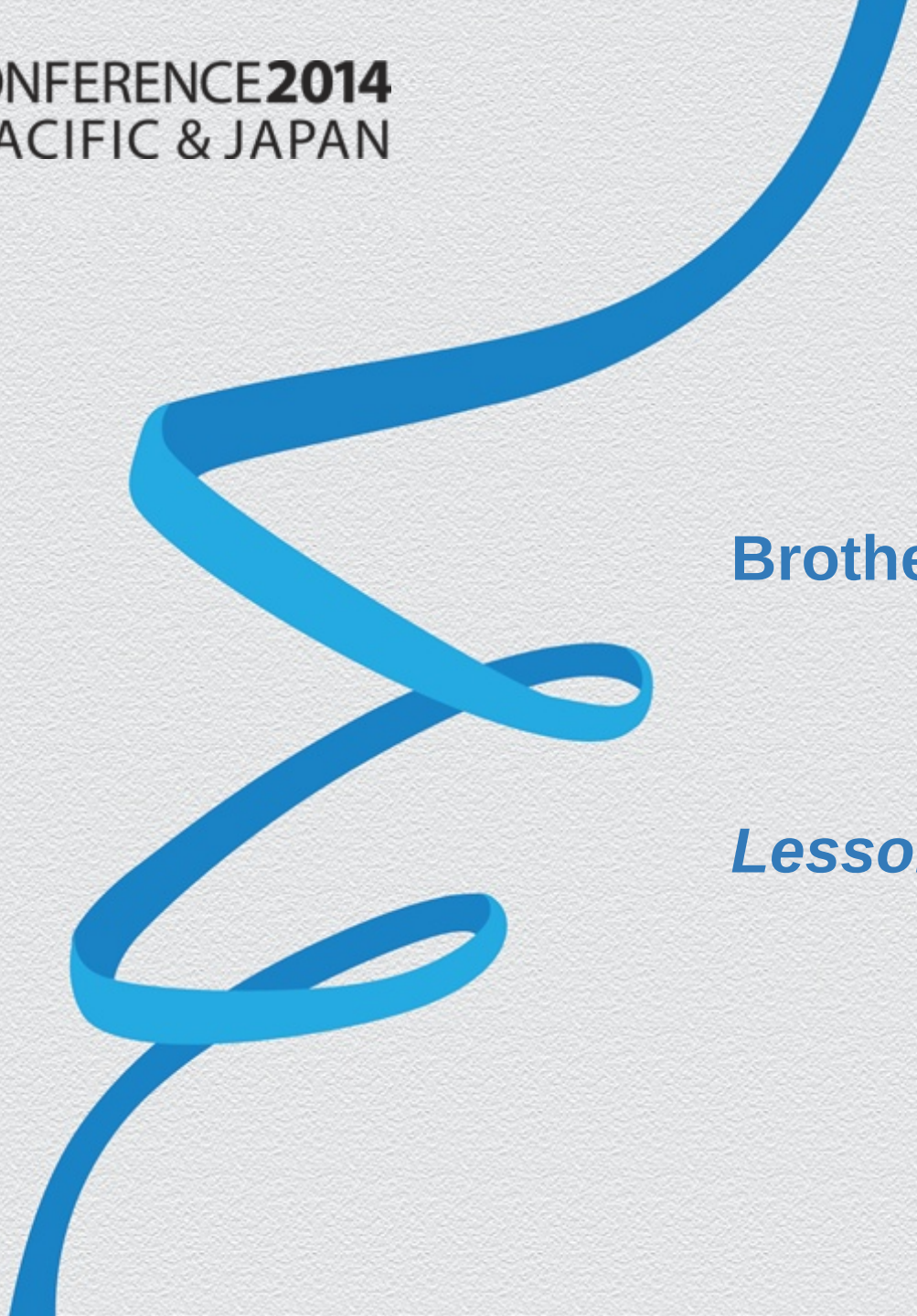
Thanks,

Operational Updates:
During Op Ababil, FS-ISAC shared on average 4 updates for each day's activity, as the activity occurred

Operation Ababil

"none of the U.S banks will be safe from our attacks"

Phase 1	Phase 2	Phase 3	Other
Sep 12 2012 – Mid Oct	Dec 12, 2012 – Jan 24	March 5 2013 – May 2	July 23, 2013 – Aug 15
• 12 Attack Days • Average alerts to partners: 1.5 • Total alerts shared: 18	• 21 Attack Days • Average alerts to partners: 3 • Total alerts shared: 63	• 28 Attack Days • Average alerts to partners: 3 • Total alerts shared: 84	• 4 Attack Days • Average alerts to partners: 2.75 • Total alerts shared: 11



Brothers In Arms

Lessons Learned

Technical Tools

- **The primary DDoS types launched by AQCF include:**
  - UDP Flooding
  - TCP Flooding
  - Search function attacks
  - Large file GET
  - Infrastructure-level attacks
  - Authentication portal attacks

Technical Tools

- **The primary tools used to mitigate:**
  - Carrier rate limiting
  - Carrier blocklists
  - Carrier blackholing of the destination or protocol
  - F5 iRules or other Load Balancer rules
  - Web Application Firewalls
  - Third party BGP-based scrubbing
  - Third party DNS-based scrubbing
  - IPS rules
  - Network blocks based on Layer 3 or 4 characteristics
  - On-premises DDoS detection/mitigation gear
  - Geo blocking at the carriers

DDoS is Back; 3 Banks Attacked

Experts Analyze Whether There's an al-Qassam Connection

By Tracy Kitten, July 30, 2013. Follow Tracy @FraudBlogger

Credit Eligible | Email | Tweet | Like | Share | Get Permission

A week after the self-proclaimed hacktivist group **Izz ad-Din al-Qassam Cyber Fighters** announced plans to launch a fourth phase of attacks against U.S. banks it's still not clear whether the group has resumed its **distributed-denial-of-service** activity.

DDoS attacks appear to have targeted three banks July 24 through July 27, according to Keynote, an online and mobile cloud testing and traffic monitoring provider, and other sources. But security vendors that track attacks linked to al-Qassam's botnet, known as Brobot, say they're uncertain exactly who was behind those attacks. While some attack evidence suggested a link to Brobot, nothing was definitive.

The online banking sites of JPMorgan Chase, U.S. Bancorp and Regions Financial Corp. all experienced intermittent outages last week, Keynote says, and the outages appear to

RELATED CONTENT

- DDoS Attacks: Worst Yet to Come?

FINANCIAL SERVICES ISAC

#RSAC

RSACONFERENCE2014 ASIA PACIFIC & JAPAN

Lessons Learned

- Communications:
  - Have a clear communications plan for your institution and ensure C-suite and media relations are primed with talking points and with not what to say.
  - Bring in the other teams, Risk, Fraud etc.
  - Stream Bridge Lines – have separate lines for technical team (soldiers in the trenches) versus everyone else.
- Monitor – Twitter feeds and other public forums for “chatter”
- Streamline decision making: Limit decision makers. Organizations should obtain pre-approvals for invoking the mitigation service so as not to delay invocation once the attack starts. Know team roles ahead of time.

Lessons Learned

- Close collaboration and sharing critical!!!!
- Know your network end to end. Assess your inventory.*
- Traffic:
  - Baseline Activity – Know your baselines for log-ins, transactions, connections, and users, mindful of traditionally high volume transaction days. Marketing Staff may hold this knowledge.
  - Have plan for triaging traffic, know what you need to keep up and what you can drop
  - Have a plan for prioritizing customers
  - Separate incoming web/customer traffic from outgoing corporate traffic using segmentation.

Lessons Learned

- Understand what mitigation will do to your apps/customers.**
- Be prepared to sacrifice some functions on your website that can be subject to POST attacks (search etc).
- Limit non-critical activities – Halting non-critical scanning activity as well as non-essential applications to reduce noise/resources
- Server initiated DDoS can stress even the most capable organizations. Consider having your Internet DNS infrastructure externally managed or utilizing multiple DDoS mitigation service/DNS providers.

Lessons Learned

- Have a hardened disposal site ready to default to
- Mobile applications should be part of testing
- Test, Test, Test
- Playbook, Playbook, Playbook
- And Test the Playbook
- Be prepared to handle lots of data. Have a strategy for vetting/deploying blacklists.
- Capture as much data as possible, not just IPs but also date/time stamps for forensics.

Bottom Line

- While it might not seem so, the attackers have done us a favor:
  - Exercised sector response to targeted network attacks.
  - Ironed bugs out of processes that had not been exercised in this manner.
  - Validated peer to peer information sharing model
  - Validated FS-ISAC consolidation and coordination role for sharing more broadly with membership and partners
- This will not go away – this actor or others.
- Information sharing and partnering both amongst targets institutions, within the sector and the public/private partnership works!

Questions?