(U) Financial Sector Cyber Security

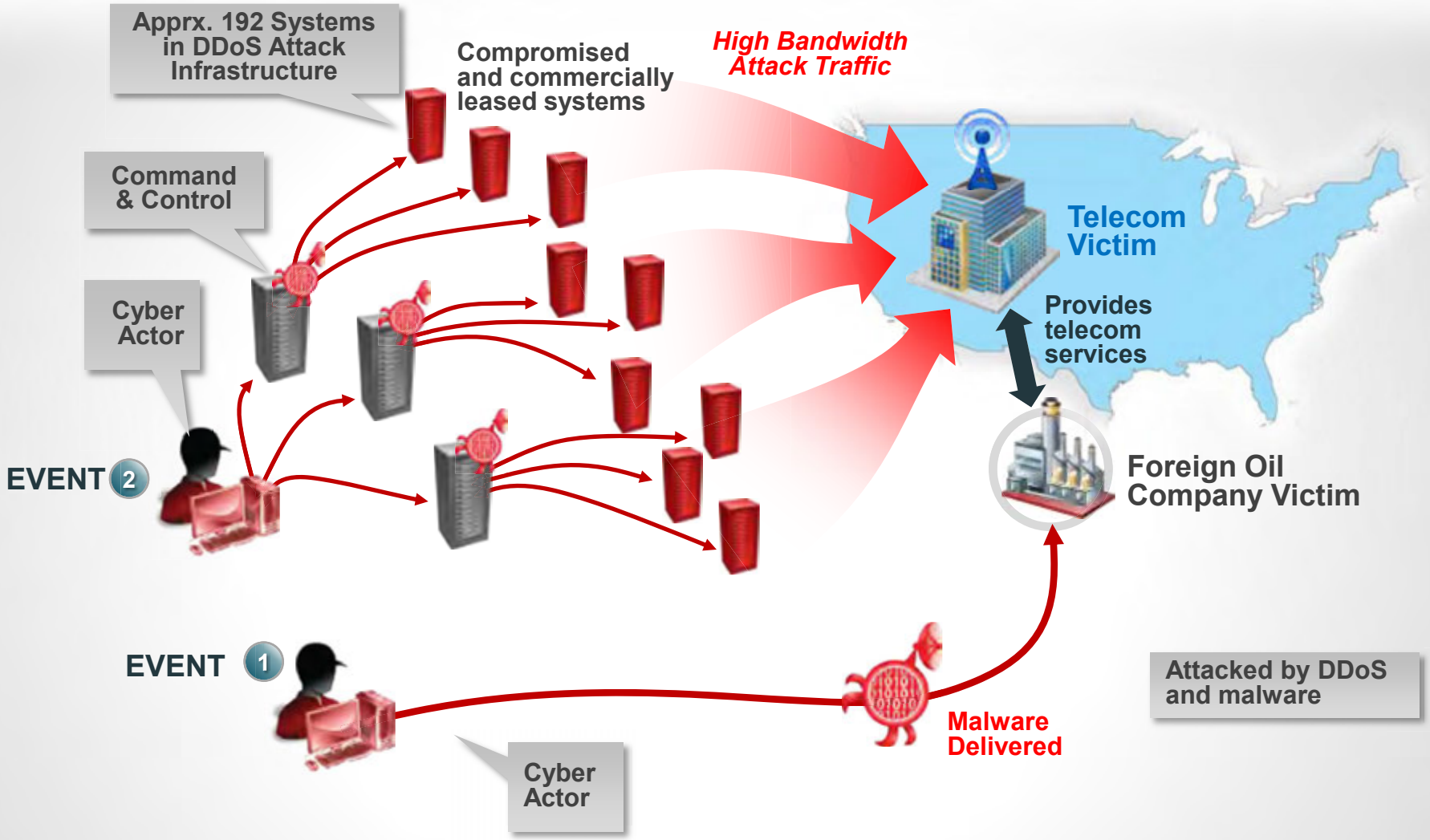
(U) Cyber Event:

(U) 15 August – Foreign cyber actors targeted a **foreign oil company** *in a large-scale coordinated cyber attack, incidentally attacking a* **major US telecom company** *that provides business services to the primary target; (no effect on actual oil production)*

US TELECOM
- ► Impaired services
- ► DDoS lasted 9 hours

FOREIGN OIL COMPANY
- ► 30,000 + computer systems infected
- ► Critical data destroyed on all infected systems
- ► Operations offline for 8 days

(U) How: Anatomy of the First Cyber Event



(U) Malware Attack

- (U) Shamoon Virus
- (U) Comprised of four files
  - trksrv.exe: initial infection agent
  - Netint.exe: communication with remote host
  - Drdisk.sys: provides raw access to disk
  - Dnslookup.exe: wiper component

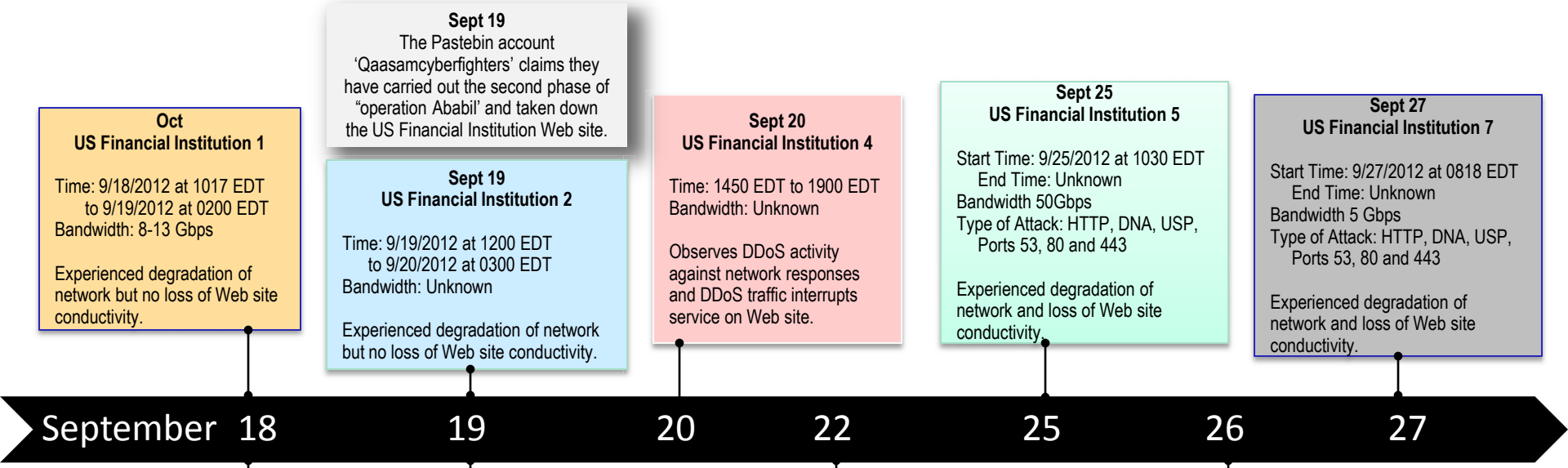
(U) US Financial Institutions Attacked

(U) 18 September – 11 October – Foreign cyber actors targeted 10 **US Financial Institutions** *with a coordinated cyber attack*

US FINANCIAL INSTITUTIONS

- ►DDoS targeted 10 institutions
- ►Degradation of networks
- ►Disruption to or Loss of Web site conductivity for at least 4 institutions

(U) Timeline of Events: Financial Sector



Oct
US Financial Institution 1

Time: 9/18/2012 at 1017 EDT
to 9/19/2012 at 0200 EDT
Bandwidth: 8-13 Gbps

Experienced degradation of network but no loss of Web site conductivity.

Sept 19
The Pastebin account 'Qaasamcyberfighters' claims they have carried out the second phase of "operation Ababil' and taken down the US Financial Institution Web site.

Sept 19
US Financial Institution 2

Time: 9/19/2012 at 1200 EDT
to 9/20/2012 at 0300 EDT
Bandwidth: Unknown

Experienced degradation of network but no loss of Web site conductivity.

Sept 20
US Financial Institution 4

Time: 1450 EDT to 1900 EDT
Bandwidth: Unknown

Observes DDoS activity against network responses and DDoS traffic interrupts service on Web site.

Sept 25
US Financial Institution 5

Start Time: 9/25/2012 at 1030 EDT
End Time: Unknown
Bandwidth 50Gbps
Type of Attack: HTTP, DNA, USP, Ports 53, 80 and 443

Experienced degradation of network and loss of Web site conductivity.

Sept 27
US Financial Institution 7

Start Time: 9/27/2012 at 0818 EDT
End Time: Unknown
Bandwidth 5 Gbps
Type of Attack: HTTP, DNA, USP, Ports 53, 80 and 443

Experienced degradation of network and loss of Web site conductivity.

Sept 18
US Financial Institution 2

Time: 1130 EDT to1500 EDT
Bandwidth: Unknown

Experienced degradation of network but no loss of Web site conductivity.

Sept 18
Group calling itself the Cyber Fighters of Izz Ad-Din Al-Qassam claim on Pastebin they will attack two US Financial Institutions in retaliation for the posting of the anti-Islamic video on Youtube.

Sept 19
US Financial Institution 3

Time: 9/19/2012 1600 EDT
to 9/20/2012 0700 EDT
Type of Attack; TCP, UDP, Ports 53, 80, and 443
Bandwidth: Unknown

DDoS results in loss of Web site conductivity.

Sept 19
US Financial Institution 4

One hour attack
Type of Attack: UDP, Ports 53
Bandwidth: Unknown

Experienced degradation of network but no loss of Web site conductivity.

Sept 22
US Financial Institution 3

Time: 9/22/2012 at 1700 EDT
End Time: Unknown
Type of attack: UDP, Port 53
Bandwidth: 1 Mbps

Web site experiences slight DDoS activity. No disruptions.

Sept 26
US Financial Institution 6

Start Time: 9/26/2012 at 0930 EDT
End Time: Unknown
Bandwidth 25 Gbps
Type of Attack: HTTP, DNA, USP, Ports 53, 80 and 443

Experienced degradation of network and loss of Web site conductivity.

(U) Timeline of Events: Financial Sector

Oct 9
US Financial Institution 8

Time: 10/09/2012 at 1111 EDT
to 10/09/2012 at 1500 EDT
Bandwidth: As high as 8 Gbps
Type

Experienced degradation of network but no loss of Web site conductivity.

Oct 11
US Financial Institution 10

Start Time: 10/11/2012 at 1045 EDT
End Time: Unknown
Bandwidth: about 5.7Gbps
Type of Attack: Unknown

Experienced degradation of network. There was no reported loss in Web site connectivity.

Oct 10
US Financial Institution 9

Time: 10/10/2012 at 1000 EDT
End Time: 10/10/2012 at 1600 EDT
Bandwidth: Max 77 Gbps
Type of Attack: Unknown

Some Web sites affected. There was no "hard down." Main customer page never went offline.

The FBI provided advanced notice to three US Financial Institutions on October8th.

(U) Distributed Denial of Service Attack Network Indicators

- UDP Port 53 traffic with packet lengths ~1,400 bytes in size and padded with “A”
- UDP Port 80 traffic padded with “/http1”
- A Port 53 TCP SYN flood
- A Port 80 TCP SYN flood
- HTTP GET Flood directed at default Web pages

(U) Distributed Denial of Service Attack Network Indicators

- (U) Attacking Hosts
  - Compromised Web servers
    - Joomla and cPanel vulnerabilities
  - Attack scripts uploaded to a hidden directory
    - Indx.php
    - Stcp.php
    - Stph.php

(U) FBI Investigative and Operational Capabilities

- Investigative Interviews
- Evidence Collection
- Electronic Surveillance
- Network Traffic Analysis
- Digital Forensics through Computer Analysis Response Team (CART)
- Malware analysis through the Binary Analysis, Characterization, and Storage System (BACSS)
- Cyber Action Team (CAT) Deployment
- Legal Attaché Support
- USIC coordination through the NCIJTF
- Indict/Arrest Authority
- Review Current Field Office Collections and Investigations.

(U) Questions