Cornell University

IT Security @ Cornell

IT Security Office

Wyman Miles, Director ITSO

Glenn Larratt, Sr. Security Engineer

Dan Villanti, Sr. Security Engineer

Overview -- ITSO

- Part of the IT@Cornell organization
- 7 staff – CISO, Deputy, and 5 Sr. Security Engineers
- Works closely with IT Policy, Counsel, Audit, law enforcement, etc.
- Responsible for the security of Cornell information and for the operational stability of the IT ecosystem

IT @ Cornell

- Central: 270 employees
- Departments: 670 employees
- On any given day, 50000 devices active on campus
  - 25000 of those are on wireless

Security Incidents

- 2500 system compromises per year
  - ¾ are student systems on wireless
  - Almost all are drive-bys, heavily weighted towards Windows
  - Fortunately, very few put regulated data at risk
- Another 2000 password thefts per year
- Assorted web defacements, stolen devices, and other events account for 100 more incidents/yr

Threat Landscape

- Cybercrime
- Espionage – Industrial and National
- Hacktivisim
- Attacks *against* the university (50K/day, typically)
- Attacks *from* the university (???)
- Internal actors, direct and incidental

Regulatory Landscape

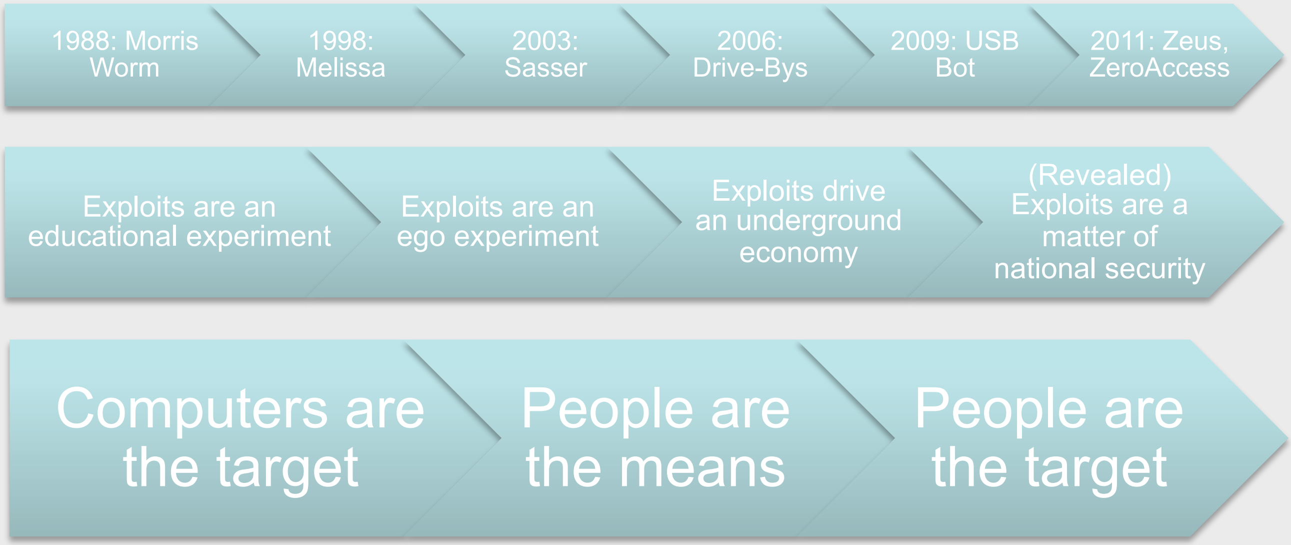
- We are a 30000 person city that runs its own bank, insurance company, medical clinic, refuse collection, power generation, potable water treatment, hotel, animal hospital, law enforcement agency, and hazmat team
- Oh, and the next Nobel Prize lurks somewhere within its 100 buildings and 2800 acres
- You name it, it applies: *FERPA, HIPAA/HITECH, PCI, SOX, GLBA, FISMA, FERC/NERC, …*

Guiding Principles: The Textbook

- Confidentiality, Integrity, and Availability
- Or, as most people think of it:
  - Secrecy
  - Get Security Out of the Way
  - Huh?
- Administrative, Technical, Physical
- Defense in Depth
- Least Privilege

Guiding Principles: Cornell

- Separation of Duties
- Minimal Access to Log Data, Zero Access to Content
- Data Stewardship
- *We are a cog in the risk management apparatus of the university*



1988: Morris Worm → 1998: Melissa → 2003: Sasser → 2006: Drive-Bys → 2009: USB Bot → 2011: Zeus, ZeroAccess

Exploits are an educational experiment → Exploits are an ego experiment → Exploits drive an underground economy → (Revealed) Exploits are a matter of national security

Computers are the target → People are the means → People are the target

The Objective is Data

Defending Cornell: Now

- Rudimentary network filtering across 80% of networks
- Network intrusion detection
  - FireEye
  - SIEM
  - Homegrown
- Log analysis
- Managed Antivirus
- Managed Encryption
- Vulnerability Scanning
- University Policy
  - Data classification and safeguards
  - Network registry
  - Accounts and access control
  - Data Governance

Defending Cornell: Future

- We need to shift to a preventative posture
  - *Risk Assessments, Risk Assessments, Risk Assessments*
  - *Re-align the program with FISMA, FedRAMP, and NIST*
  - *Application vulnerability management*
  - *Penetration testing*
  - Firewalls with Unified Threat Management
  - Increased management of desktops, laptops, tablets
  - Increased encryption
  - Data-loss prevention
- Policy re-aligned to meet new threats: espionage and cybercrime

(Hopefully) Interesting Reading, After the Sequester Lifts

- NIST-800:
  - http://csrc.nist.gov/publications/PubsSPs.html
- FISMA:
  - http://csrc.nist.gov/sec-cert/
- FedRAMP:
  - http://www.fedramp.gov

Shameless Plug

- The ITSO would like to hire a few students for closely supervised pen testing of high-value Cornell apps
- No sooner than Spring, 2014
- wm63@cornell.edu

IT Security Ops – Priorities / Customers

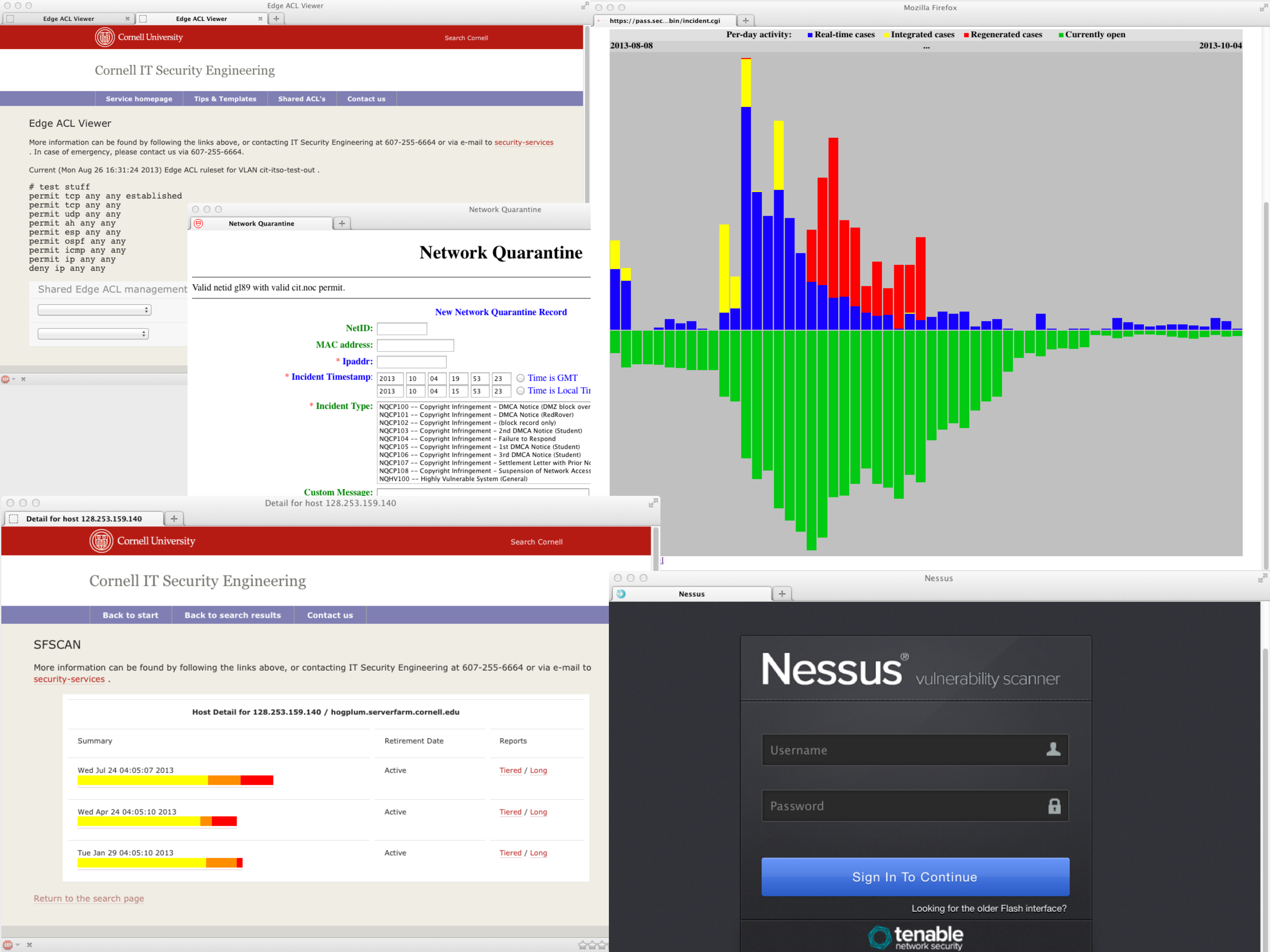
- “The Data” is our first priority
  - Networks designed based on data contained therein
  - First question we ask in incident response
  - Data types and data stewards
- Our customer base
  - End users
  - Netadmins / local Sysadmins
  - Investigative/administrative units within the University

IT Security Ops – Defense in Depth

- There is no, no, **NO** silver bullet
- Layered defense – one layer catches what another misses
- Firewalls, encryption, and AAA are obvious layers
- Less obvious layers include policy, detection, incident response, and trained analysts

IT Security – Services

- Antiphishing
- Network Quarantine / PASS
- Endpoint Protection
- Remote Access via VPN
- Full-disk and other encryption
- Edge ACL’s
- Proactive vulnerability scanning



Cornell IT Security Engineering

Edge ACL Viewer

More information can be found by following the links above, or contacting IT Security Engineering at 607-255-6664 or via e-mail to security-services . In case of emergency, please contact us via 607-255-6664.

Current (Mon Aug 26 16:31:24 2013) Edge ACL ruleset for VLAN cit-itso-test-out .

```
# test stuff
permit tcp any any established
permit tcp any any
permit udp any any
permit ah any any
permit esp any any
permit ospf any any
permit icmp any any
permit ip any any
deny ip any any
```

Shared Edge ACL management

Network Quarantine

Valid netid gl89 with valid cit.noc permit.

New Network Quarantine Record

NetID:	
MAC address:	
* Ipaddr:	
* Incident Timestamp:	2013 10 04 19 53 23 ○ Time is GMT 2013 10 04 15 53 23 ○ Time is Local Ti
* Incident Type:	NQCP100 -- Copyright Infringement – DMCA Notice (DMZ block over NQCP101 -- Copyright Infringement – DMCA Notice (RedRover) NQCP102 -- Copyright Infringement – (block record only) NQCP103 -- Copyright Infringement – 2nd DMCA Notice (Student) NQCP104 -- Copyright Infringement – Failure to Respond NQCP105 -- Copyright Infringement – 1st DMCA Notice (Student) NQCP106 -- Copyright Infringement – 3rd DMCA Notice (Student) NQCP107 -- Copyright Infringement – Settlement Letter with Prior No NQCP108 -- Copyright Infringement – Suspension of Network Access NQHV100 -- Highly Vulnerable System (General)
Custom Message:	

Detail for host 128.253.159.140
Detail for host 128.253.159.140
Cornell University
Search Cornell

Cornell IT Security Engineering

SFSCAN

More information can be found by following the links above, or contacting IT Security Engineering at 607-255-6664 or via e-mail to security-services .

Host Detail for 128.253.159.140 / hogplum.serverfarm.cornell.edu

Summary	Retirement Date	Reports
Wed Jul 24 04:05:07 2013	Active	Tiered / Long
Wed Apr 24 04:05:10 2013	Active	Tiered / Long
Tue Jan 29 04:05:10 2013	Active	Tiered / Long

Return to the search page

IT Security – SIEM

- Security Information/Event Management
- Listens to network traffic at the core
- Receives AAA, IDS, and other logs
- Correlation / Corroboration / Investigation

IT Security – Detection (Network)

- NetFlow – Server Farm and Border routers
  - Spike alerts
  - Traflog

- Tap on the network core, feeding:
  - Flow processor of our SIEM
  - FireEye IDS
  - Bro IDS

IT Security – Detection (logs)

- AAA logs from most systems on campus
  - Look for obvious patterns of compromise

- IDS logs from our several such systems
  - Postprocess, correlate, check with bad actor info

IT Security - Consulting

- “How do I use this service?”
- “Why doesn’t my network work as expected?”
- “Is this (old) firewall really giving me any value?”
- Security Assessments
- Security planning for new IT projects

IT Security – Incident Response

- Again – it’s the data
- What data was there?
- What capabilities did the attacker have?
- Analyze a large volume of technical data…

…to reach a simply-stated likelihood of data loss, for a committee of university executives

Incident Response

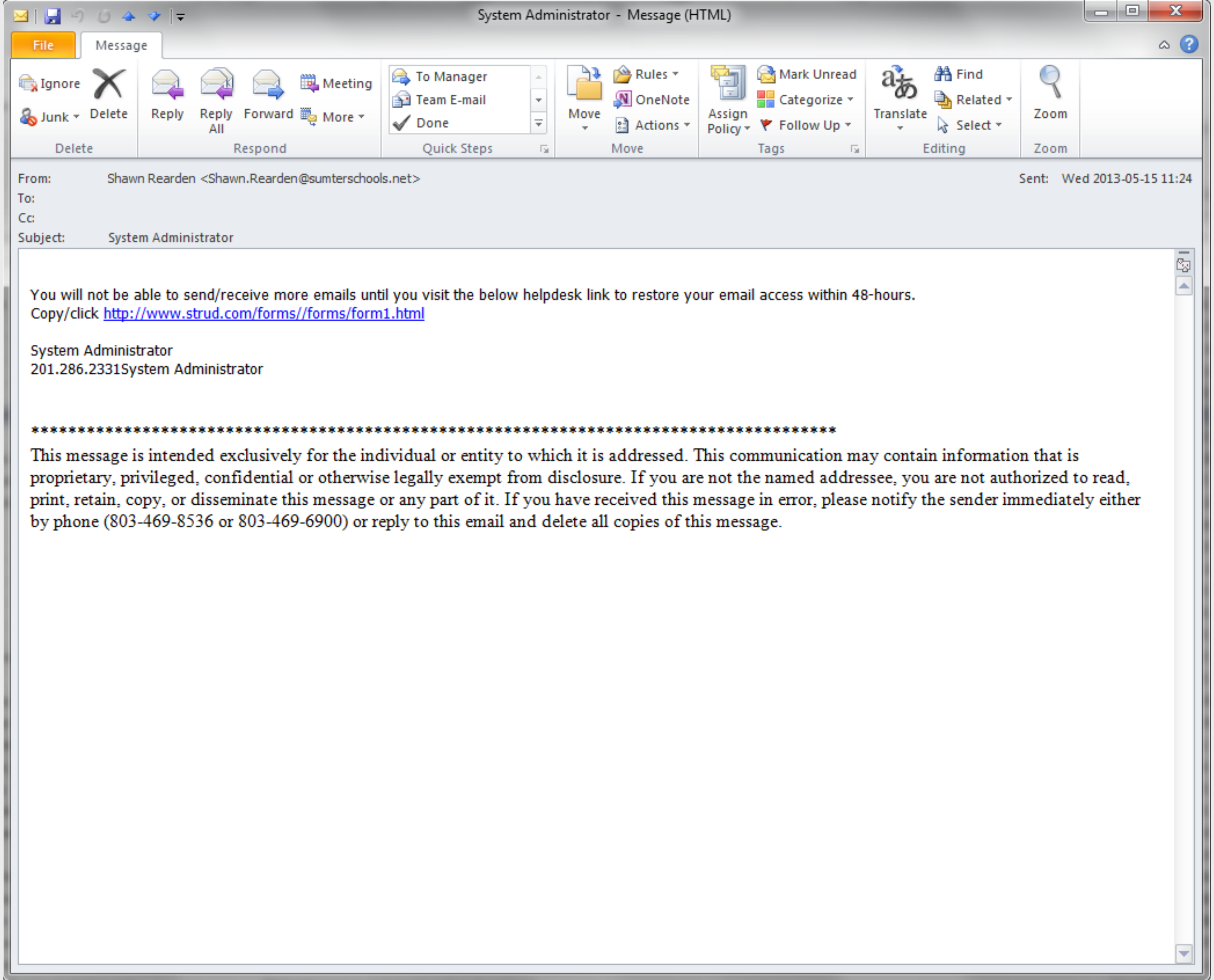
- Volatile data is important
- Modern malware is encrypted
- Acquire RAM and disk image
- Contain communications
- Restore user work environment

Threat Landscape

- Older
  - Trojan horses
  - Viruses
  - Worms (network, USB)
- Newer
  - Phishing
  - Drive-by downloads
  - Distributed Denial of Service (DDoS) attacks
  - Web application attacks

Phishing

- Trick the user into giving information (social engineering)
- Trick the user into executing malware
- Methods
  - URLs in
    - e-mail, instant messages, social media, SMS
  - Attachments
  - Phone calls



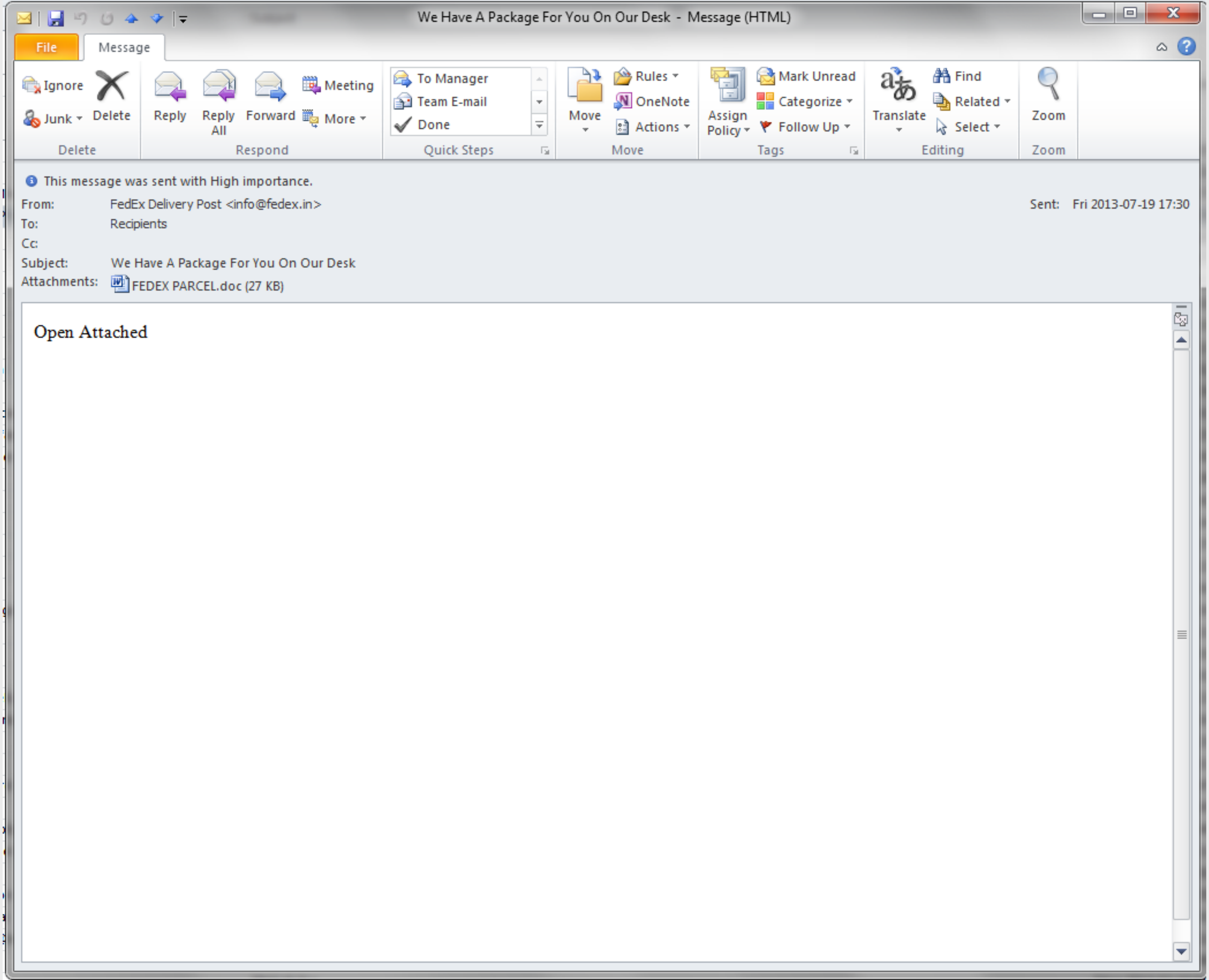
From: Shawn Rearden <Shawn.Rearden@sumterschools.net>
Sent: Wed 2013-05-15 11:24
To:
Cc:
Subject: System Administrator

You will not be able to send/receive more emails until you visit the below helpdesk link to restore your email access within 48-hours.
Copy/click http://www.strud.com/forms//forms/form1.html

System Administrator
201.286.2331System Administrator

****

This message is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged, confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy, or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately either by phone (803-469-8536 or 803-469-6900) or reply to this email and delete all copies of this message.



This message was sent with High importance.

From: FedEx Delivery Post <info@fedex.in>

Sent: Fri 2013-07-19 17:30

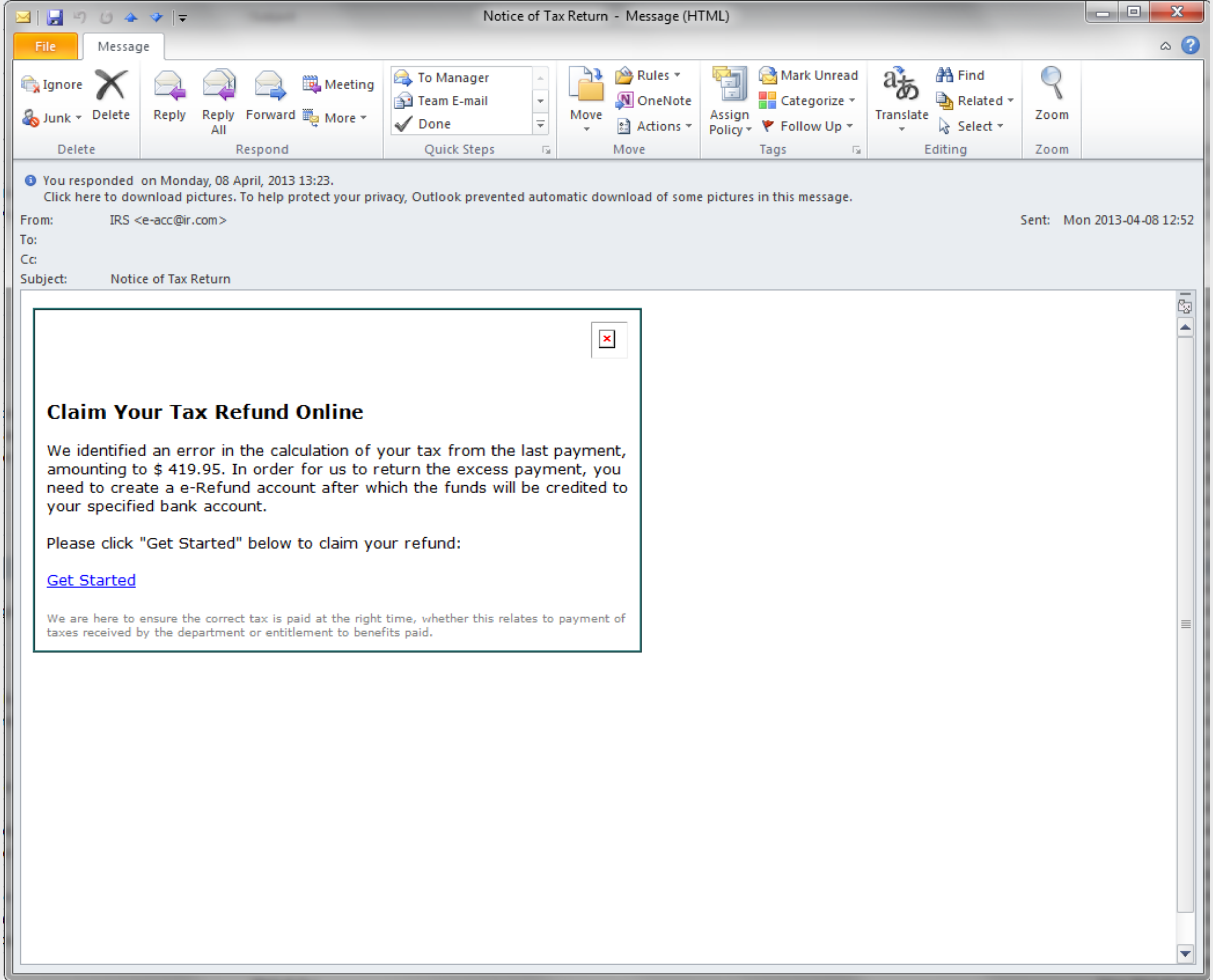
To: Recipients

Cc:

Subject: We Have A Package For You On Our Desk

Attachments: FEDEX PARCEL.doc (27 KB)

Open Attached



You responded on Monday, 08 April, 2013 13:23.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: IRS <e-acc@ir.com>
Sent: Mon 2013-04-08 12:52
To:
Cc:
Subject: Notice of Tax Return

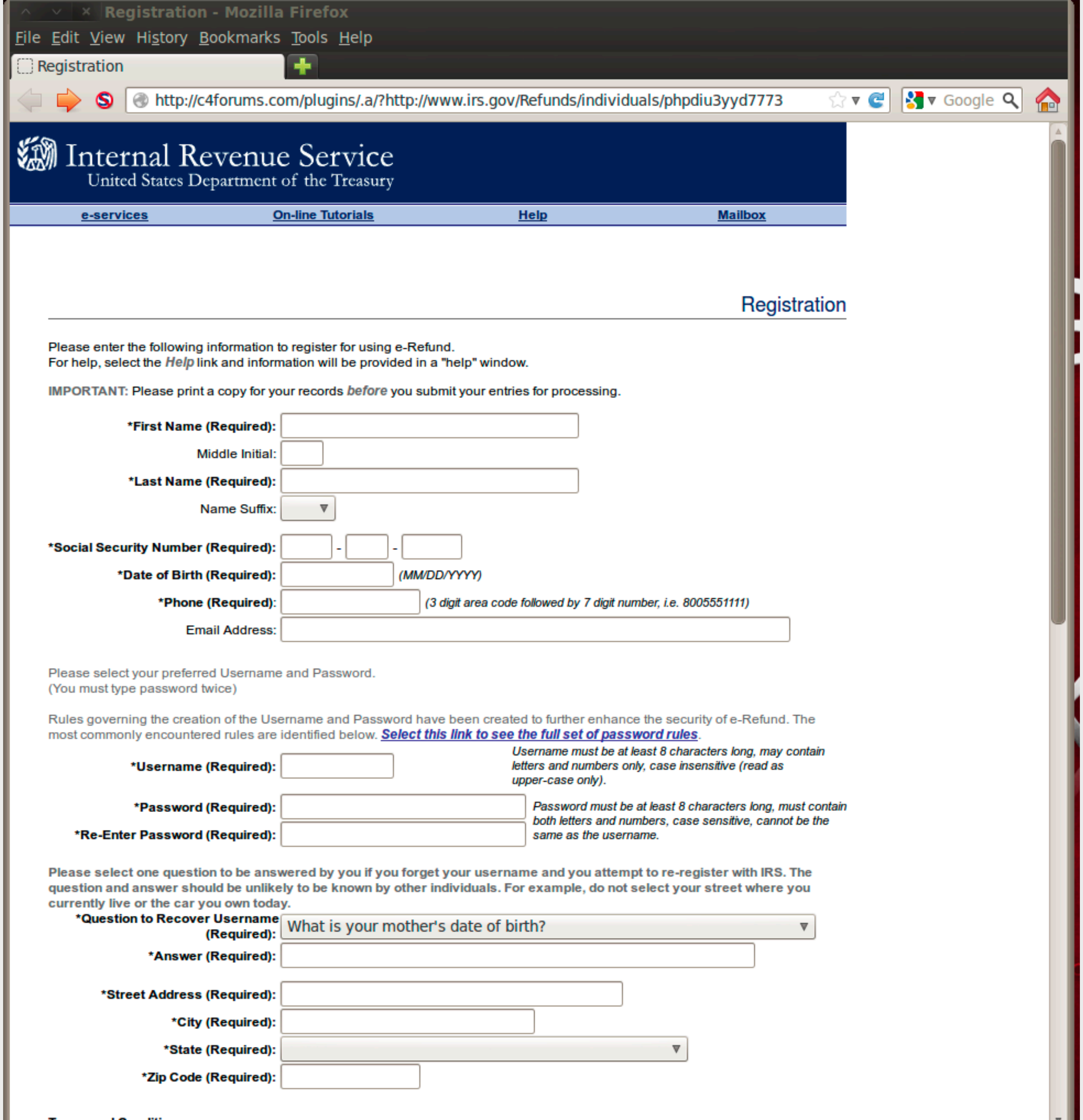
Claim Your Tax Refund Online

We identified an error in the calculation of your tax from the last payment, amounting to $ 419.95. In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

We are here to ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.


Registration - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Registration
Google

http://c4forums.com/plugins/.a/?http://www.irs.gov/Refunds/individuals/phpdiu3yyd7773

Internal Revenue Service
United States Department of the Treasury

e-services On-line Tutorials Help Mailbox

Registration

Please enter the following information to register for using e-Refund.
For help, select the *Help* link and information will be provided in a "help" window.

IMPORTANT: Please print a copy for your records *before* you submit your entries for processing.

***First Name (Required):**

Middle Initial:

***Last Name (Required):**

Name Suffix:

***Social Security Number (Required):** - -

***Date of Birth (Required):** *(MM/DD/YYYY)*

***Phone (Required):** *(3 digit area code followed by 7 digit number, i.e. 8005551111)*

Email Address:

Please select your preferred Username and Password.
(You must type password twice)

Rules governing the creation of the Username and Password have been created to further enhance the security of e-Refund. The most commonly encountered rules are identified below. ***Select this link to see the full set of password rules***.

***Username (Required):** *Username must be at least 8 characters long, may contain letters and numbers only, case insensitive (read as upper-case only).*

***Password (Required):**

***Re-Enter Password (Required):** *Password must be at least 8 characters long, must contain both letters and numbers, case sensitive, cannot be the same as the username.*

Please select one question to be answered by you if you forget your username and you attempt to re-register with IRS. The question and answer should be unlikely to be known by other individuals. For example, do not select your street where you currently live or the car you own today.

***Question to Recover Username (Required):** What is your mother's date of birth?

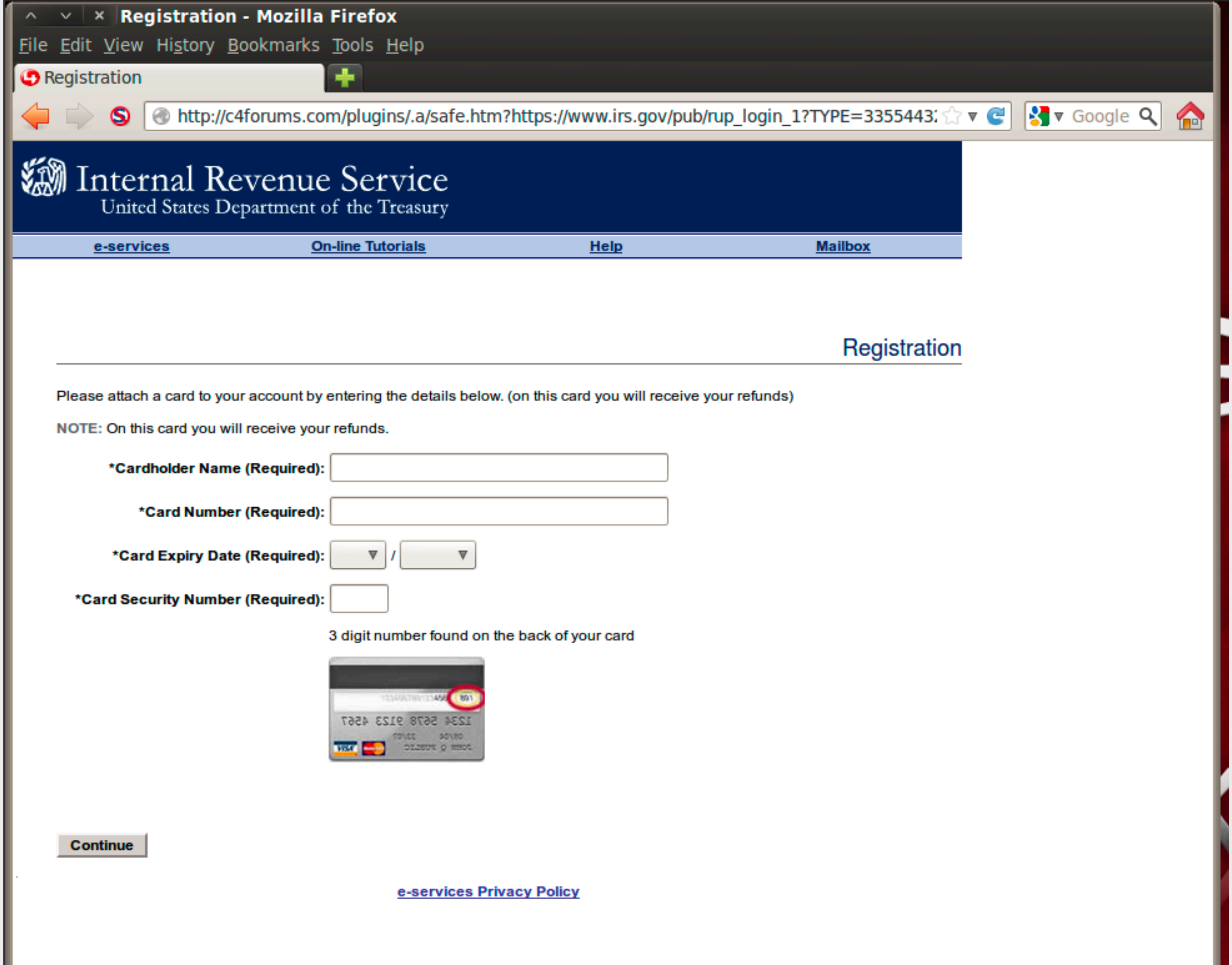
***Answer (Required):**

***Street Address (Required):**

***City (Required):**

***State (Required):**

***Zip Code (Required):**


Registration - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Registration
Google
e-services
On-line Tutorials
Help
Mailbox
Continue

http://c4forums.com/plugins/.a/safe.htm?https://www.irs.gov/pub/rup_login_1?TYPE=3355443

Internal Revenue Service
United States Department of the Treasury

Registration

Please attach a card to your account by entering the details below. (on this card you will receive your refunds)

NOTE: On this card you will receive your refunds.

***Cardholder Name (Required):**

***Card Number (Required):**

***Card Expiry Date (Required):** /

***Card Security Number (Required):**

3 digit number found on the back of your card

e-services Privacy Policy

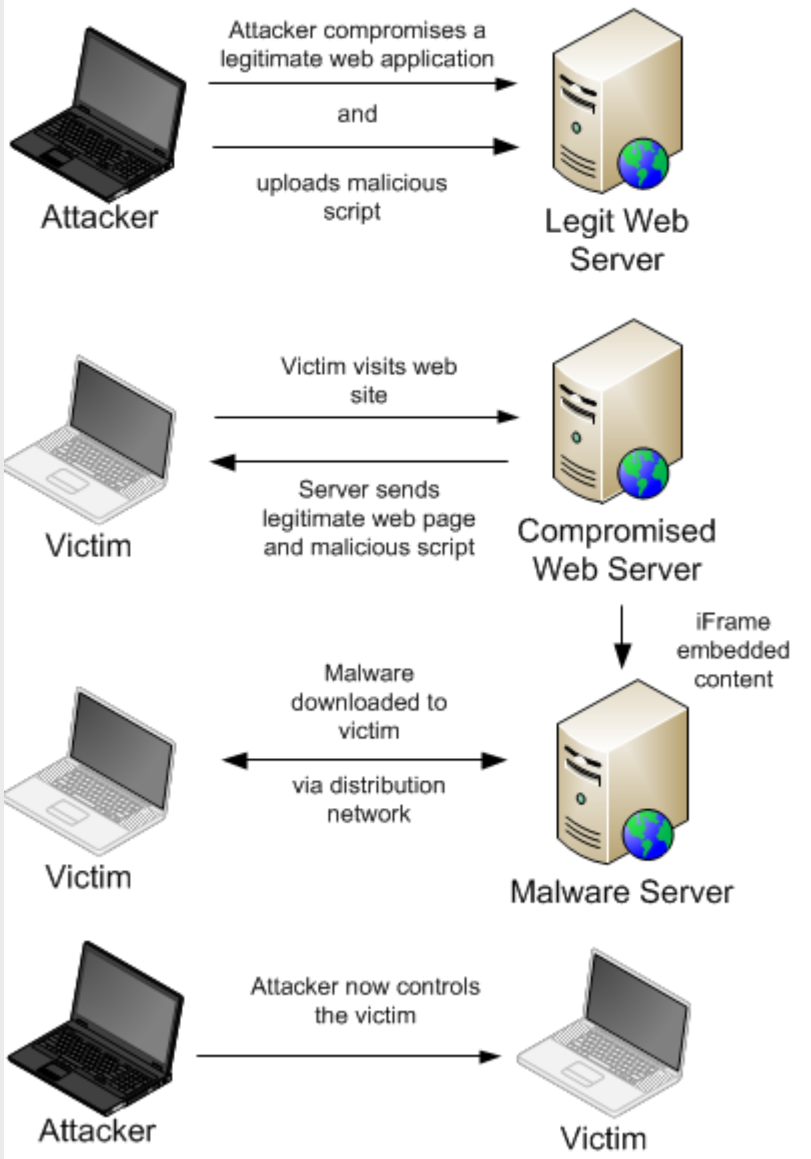
Drive-by Downloads

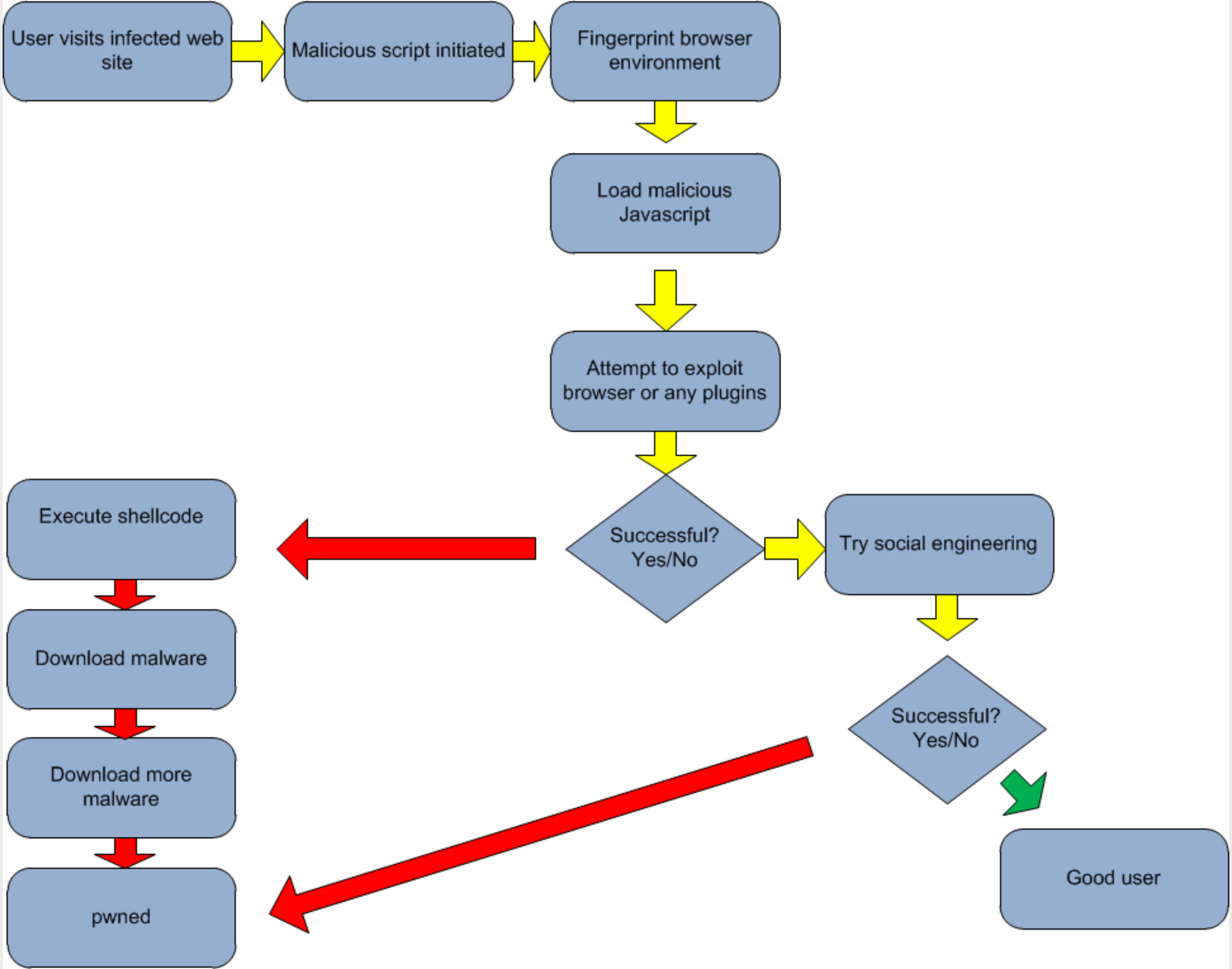
- Installs malicious software without user’s knowledge or consent
- Vector typically is a compromised web site or malicious advertisement
- Goal: exploit a vulnerable system and execute a “dropper” that downloads malware du jour

How do they work?

- Web-based exploit kits
- Hidden iFrame or redirect to malicious Javascript, usually obfuscated
- JS determines environment
  - OS platform, browser version, plugins installed
- Delivers tailored exploits based on results
- Exploits typically attack
  - Web browser
  - Plugins
    - Java
    - Adobe Flash
    - Adobe Reader

Typical Drive-By Download Attack





User visits infected web site

Malicious script initiated

Fingerprint browser environment

Load malicious Javascript

Attempt to exploit browser or any plugins

Successful? Yes/No

Execute shellcode

Download malware

Download more malware

pwned

Try social engineering

Successful? Yes/No

Good user

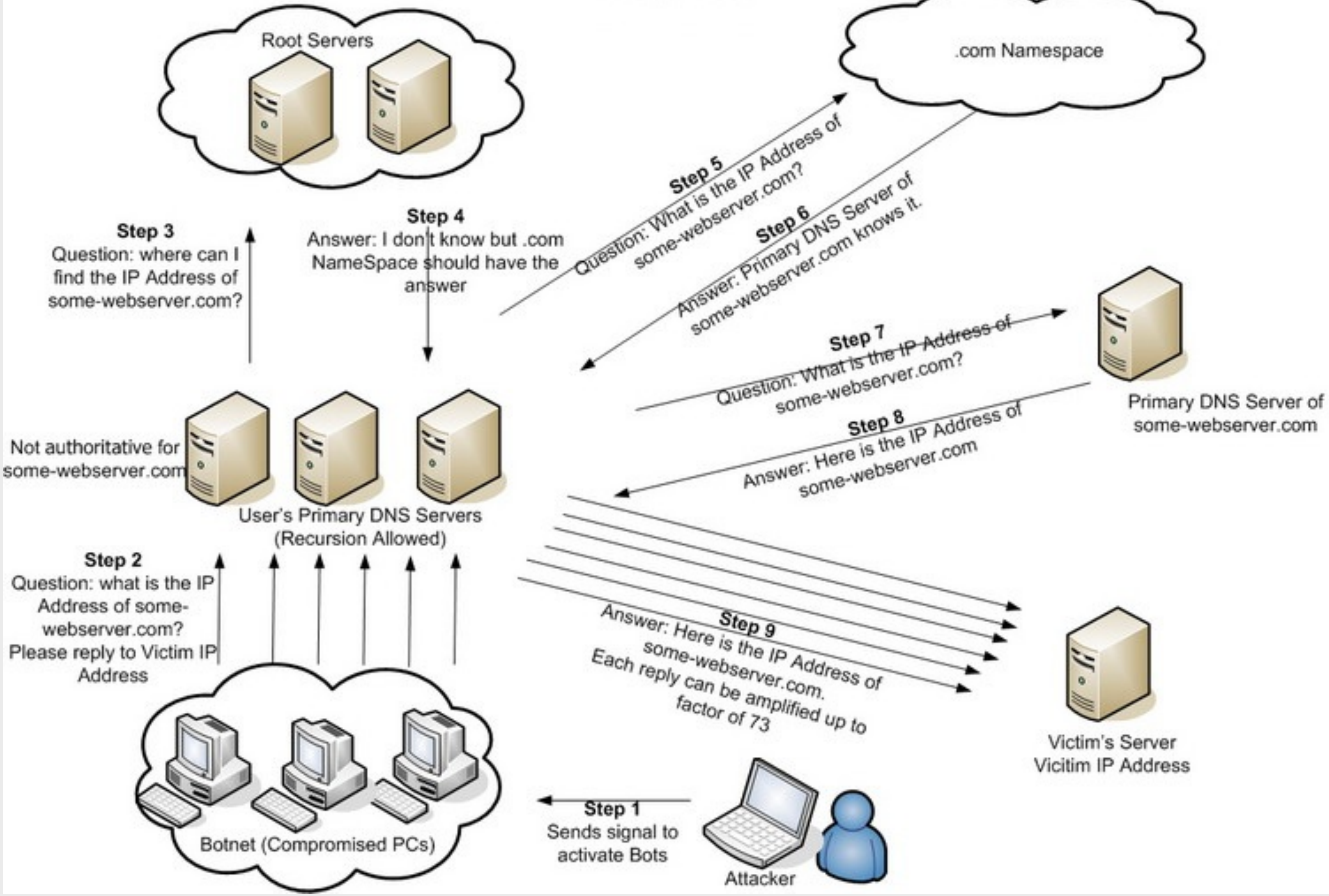
Popular Malware on Campus

- Fake anti-virus
- FBI ransomware
- ZBot
- ZeroAccess
- Flashback

DDoS

- Use voluminous resources around the Internet to conduct attack
- Source can be
  - Botnet
  - Open or insecure services
    - DNS
    - SNMP

DNS Amplification Attack



Root Servers

.com Namespace

Step 3
Question: where can I find the IP Address of some-webserver.com?

Step 4
Answer: I don't know but .com NameSpace should have the answer

Step 5
Question: What is the IP Address of some-webserver.com?

Step 6
Answer: Primary DNS Server of some-webserver.com knows it.

Step 7
Question: What is the IP Address of some-webserver.com?

Step 8
Answer: Here is the IP Address of some-webserver.com

Primary DNS Server of some-webserver.com

Not authoritative for some-webserver.com

User's Primary DNS Servers (Recursion Allowed)

Step 2
Question: what is the IP Address of some-webserver.com? Please reply to Victim IP Address

Step 9
Answer: Here is the IP Address of some-webserver.com. Each reply can be amplified up to factor of 73

Victim's Server
Vicitim IP Address

Botnet (Compromised PCs)

Step 1
Sends signal to activate Bots

Attacker

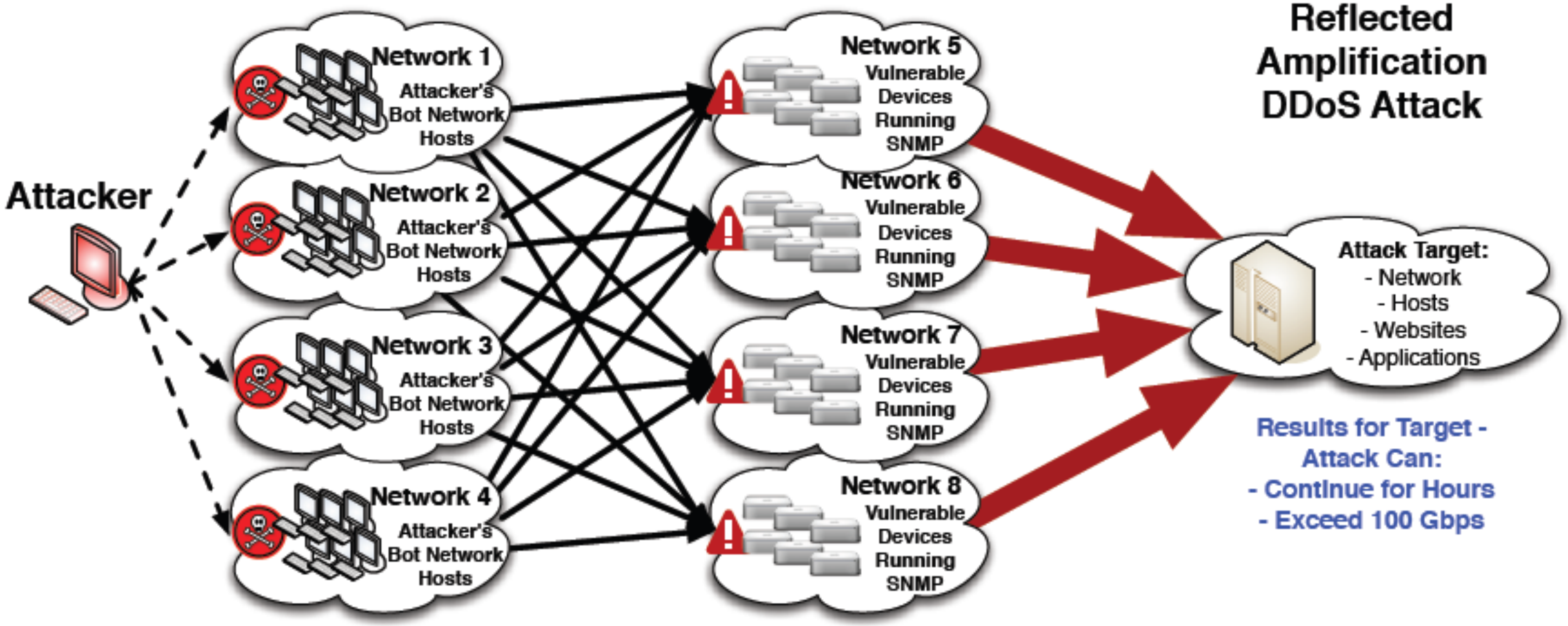
Case: SpamHaus

- Largest DDoS reported in history
- Estimated that over 30,000 resolvers were used
- Each 36 byte query resulted in a 3 kilobyte response (100x amplifier)
- Over 90 Gb/s smashed SpamHaus servers
  - More than 300 Gb/s at Tier 1 and 2 providers

***Distribution*:**
Attacker's Botnet Hosts

***Reflection*:**
SNMP Vulnerability

***Target*:**
Hit With
Reflected
Amplification
DDoS Attack



Attacker

Network 1
Attacker's
Bot Network
Hosts

Network 2
Attacker's
Bot Network
Hosts

Network 3
Attacker's
Bot Network
Hosts

Network 4
Attacker's
Bot Network
Hosts

Network 5
Vulnerable
Devices
Running
SNMP

Network 6
Vulnerable
Devices
Running
SNMP

Network 7
Vulnerable
Devices
Running
SNMP

Network 8
Vulnerable
Devices
Running
SNMP

Attack Target:
- Network
- Hosts
- Websites
- Applications

Results for Target -
Attack Can:
- Continue for Hours
- Exceed 100 Gbps

Step 1:
Attacker Sends
Command to
Botnet
"Send Forged
SNMP Query
to All Bots"
at ISPs 1 - 4

Step 2:
Bots Send
SNMP Queries
to All SNMP
Devices at
ISPs 5 - 8,
Using Forged
IP Address of
Target

Step 3:
Vulnerable Devices
Respond to Forged
Queries, Replying
En Masse to Target

Web Application Attacks

- OWASP
- Common attacks
  - SQLi
  - XSS
  - CSRF
- Common goals
  - database access
  - credential stealing
  - malware hosting
  - spam hosting

Prevention

- It’s all about the layers
  - Nextgen firewall
  - Endpoint protection
  - Patch management
  - Vulnerability management
  - Awareness training
- OS protection
  - ASLR
  - DEP
  - EMET (Windows)
- Penetration Testing