Inside a BBB Malware Scheme: Mapping and Dissecting Attacker Infrastructure

Prepared for FIRST 2008

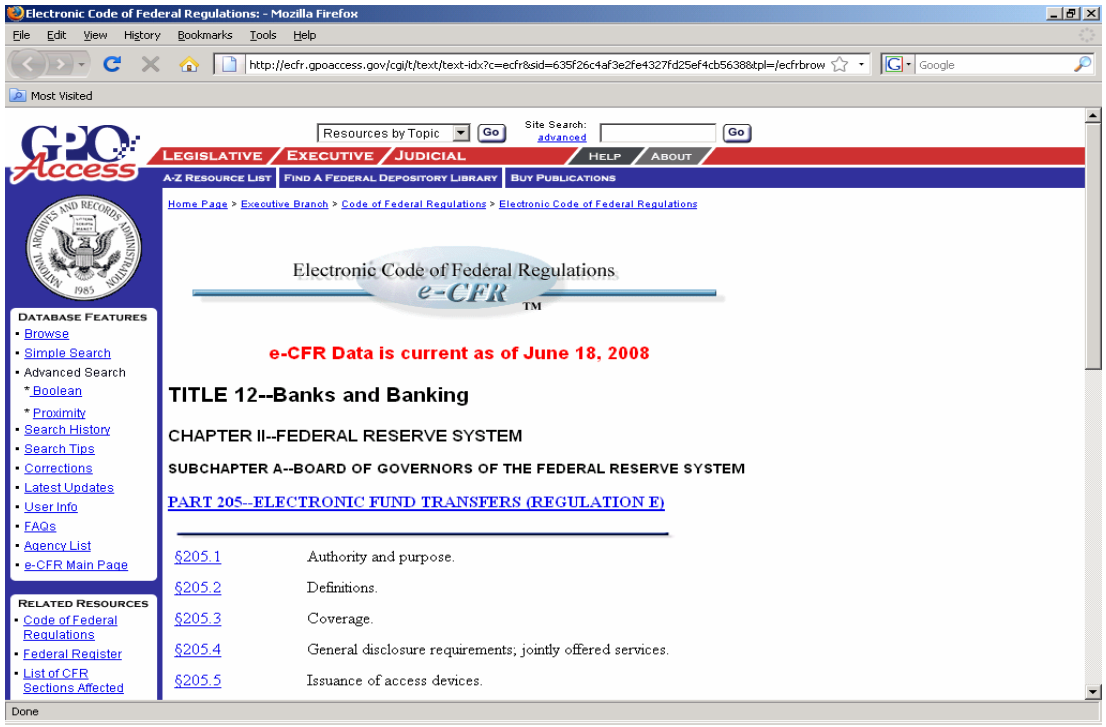
Michael La Pilla

VeriSign iDefense Malicious Code Operations Team

June 26, 2008

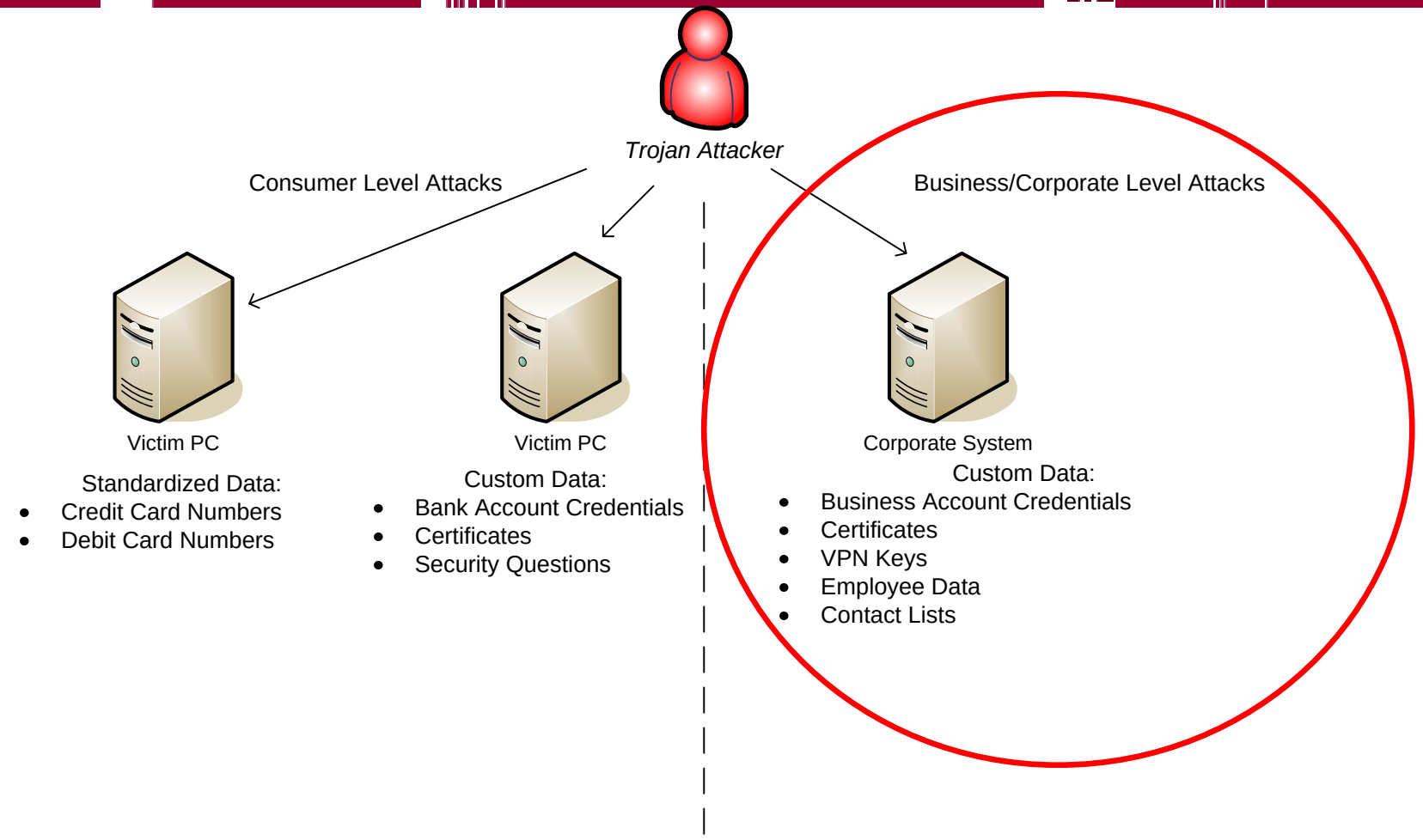
Why Should Incident Responders Care?

+ US Commercial Accounts (the current target) NOT covered by Regulation E (read http://www.gpoaccess.gov/ecfr/ for more details in US)
+ Businesses of all size losing money, not just the banks



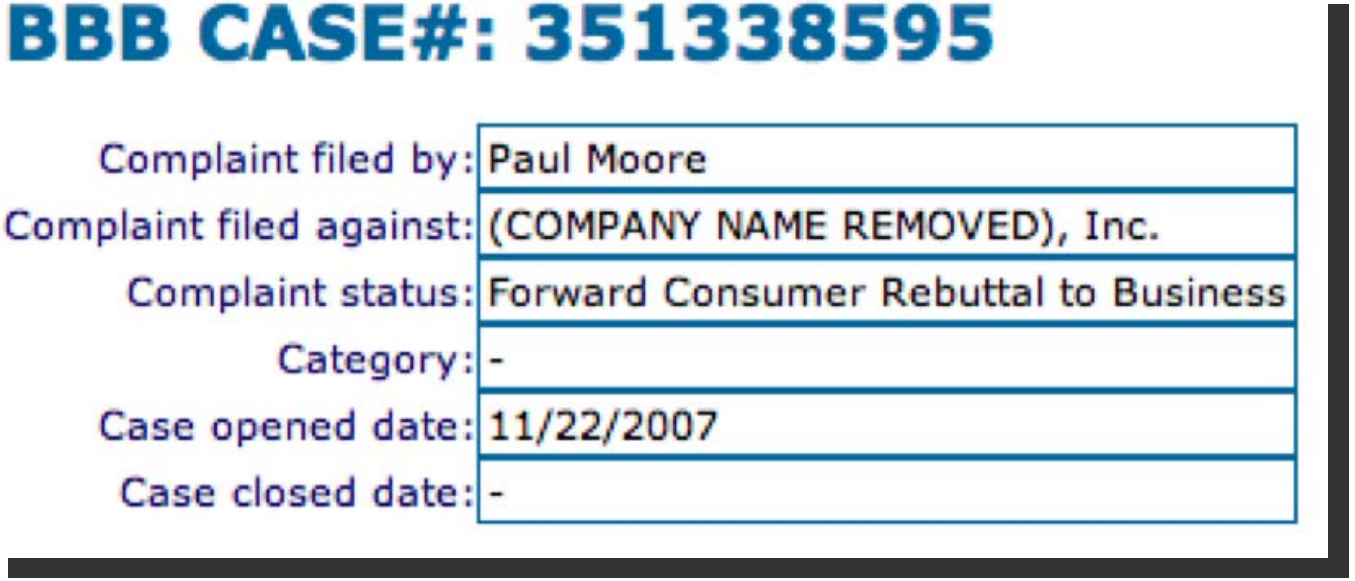
VeriSign®

Retail vs. Commercial



What is a “BBB Attack”

- Targeted e-mail using social engineering
- Coined after use of Better Business Bureau name
- “BBB Attack” is like saying “Storm Worm”
- 60+ documented attacks Feb 2007 – June 2008



BBB CASE#: 351338595

Complaint filed by:	Paul Moore
Complaint filed against:	(COMPANY NAME REMOVED), Inc.
Complaint status:	Forward Consumer Rebuttal to Business
Category:	-
Case opened date:	11/22/2007
Case closed date:	-

BBB Attacks - FTC

FEDERAL TRADE COMMISSION

Dear [redacted]

A complaint has been filled against you and the company you are affiliated to by Mr. George Hanson and sent to Federal Trade Comission by fax,in witch he's claiming that he has been cheated by you and your company in paying a greater ammount of money than the one appearing on the invoice you gave him for using your services.
The complaint states he contacted your company on MON,22 OCT 2007, trying to solve this situation without interference from any Governmental Institution , but your company refused to take action.
On WED,24 OCT 2007, the complaint was sent by fax to Federal Trade Commission and we forwarded it to Internal Revenue Service and Better Business Bureau.
Complaint was filled against :
Name : [redacted]
Company : - [redacted]
If you feel that this message has been sent to you in error or if you have any questions regarding the next steps of this process, please dl ownload the original complaint by clicking the link below :
http://ftc.gov/fraud/complaints/24_oct_2007_george_hanson.doc

Please take knowledge of the complaint's content and complete the form at the bottom of forward it to fraudcomplaint@ftc.gov.

Bruce Jameson
Complaint Officer
Federal Trade Commission,Fraud Department

VeriSign®

US Courts – April 14, 2008

From: United States District Court [mailto:subpoena@uscourts.com]
Sent: Monday, April 14, 2008 7:00 AM
To: CEO Name
Subject: Subpoena in case #27-830-IBM

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room
room 5217

Issuing officers name and address: O'Mevely & Meyers LLP; 400 South Hope Street, Los Angeles, CA 90071

Please download the entire document on this matter(follow this link) and print it for your record.

Case number: 27-830-IBM
United States District Court

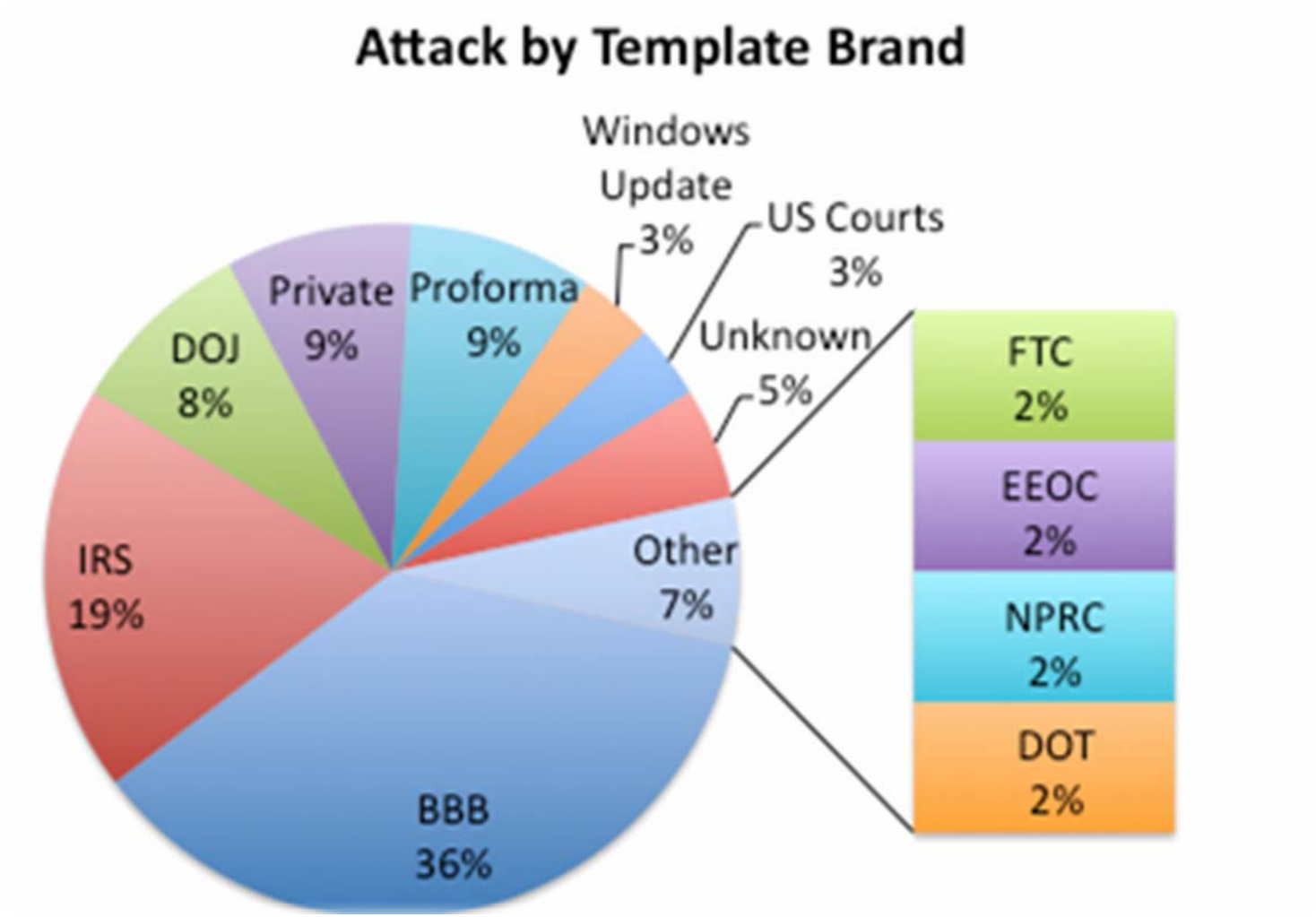
YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specifiied below.

VeriSign®

US Courts – April 14, 2008

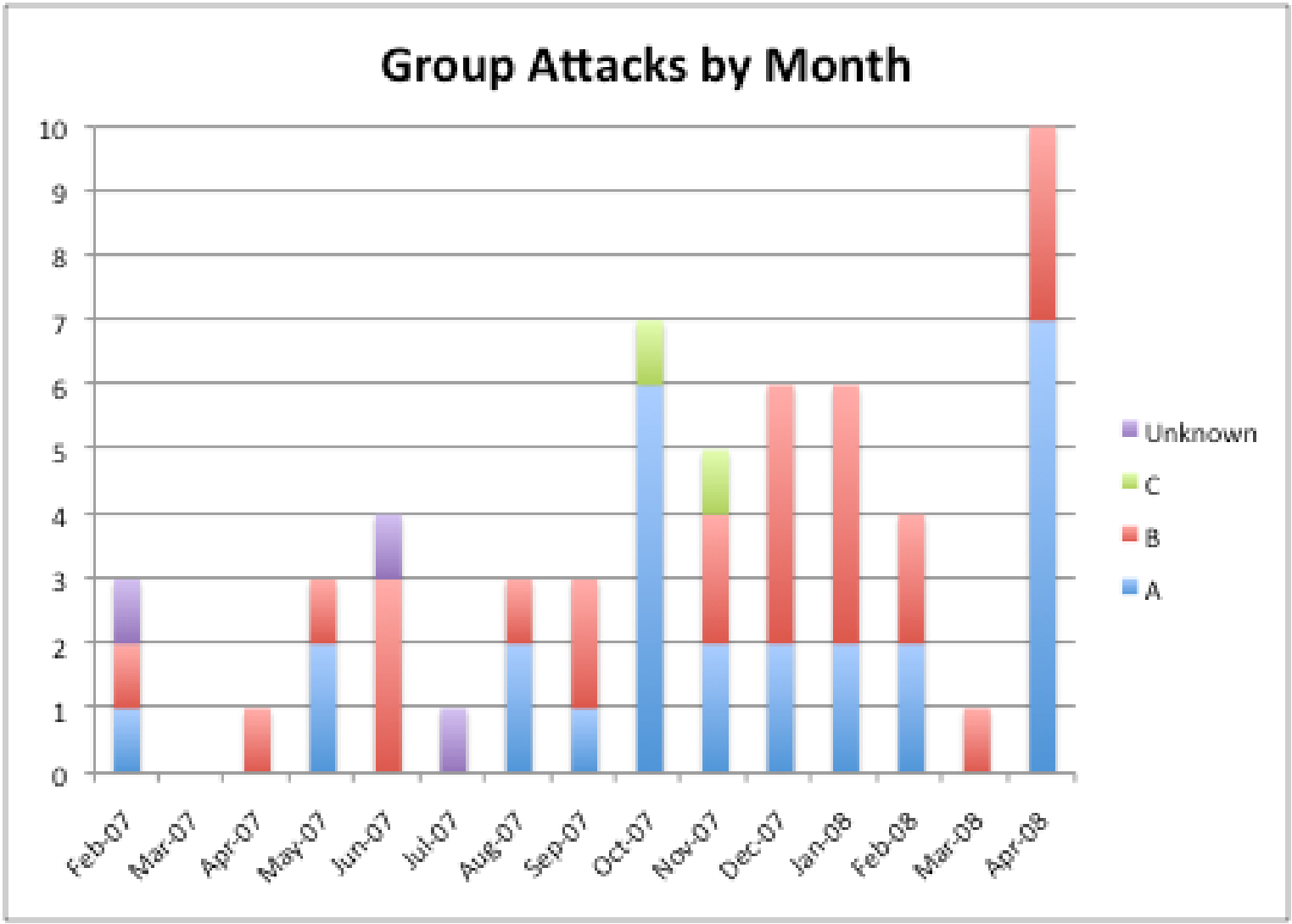
US Courts – April 14, 2008

Not Just BBB



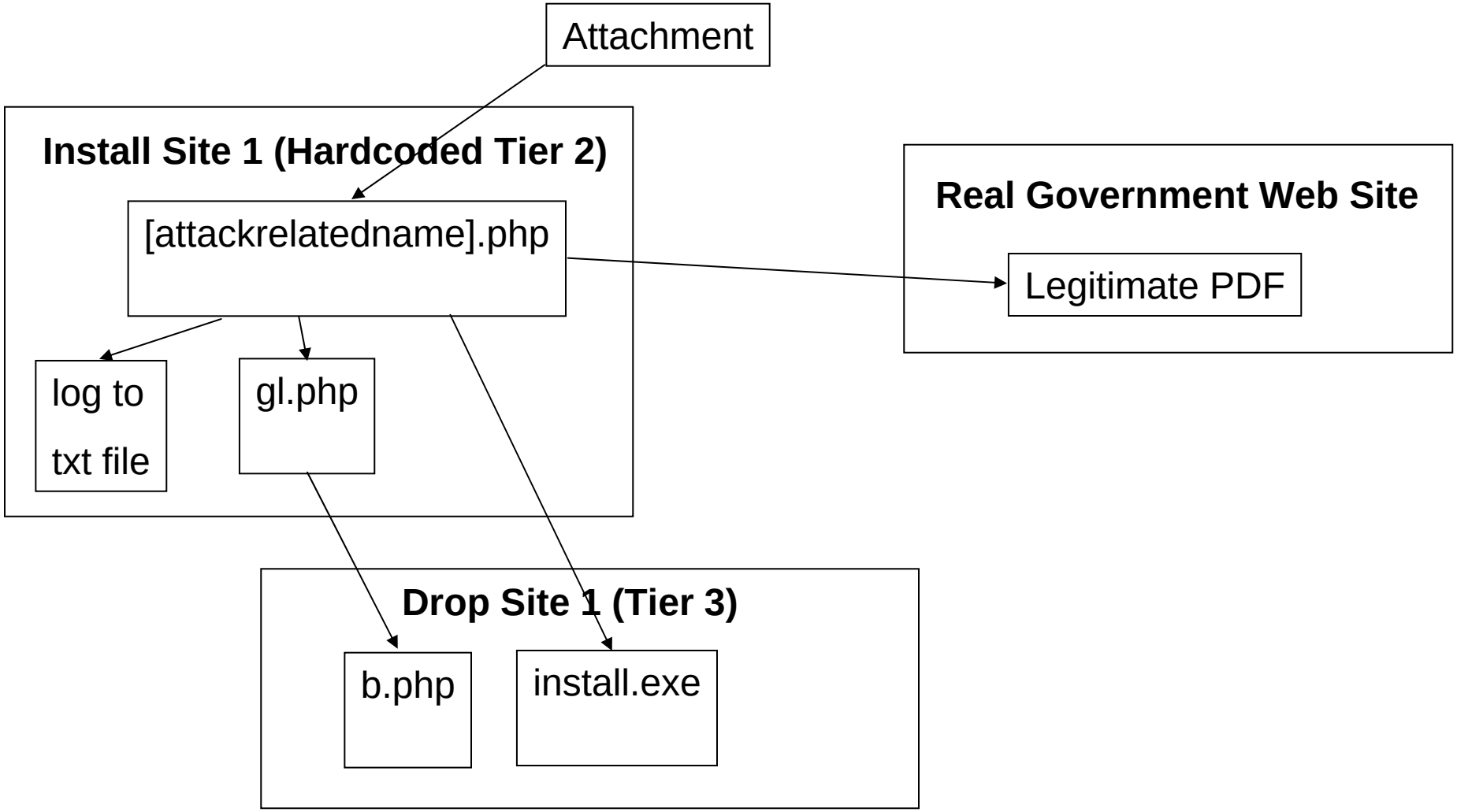
VeriSign®

Multiple Attackers, Different Infrastructures



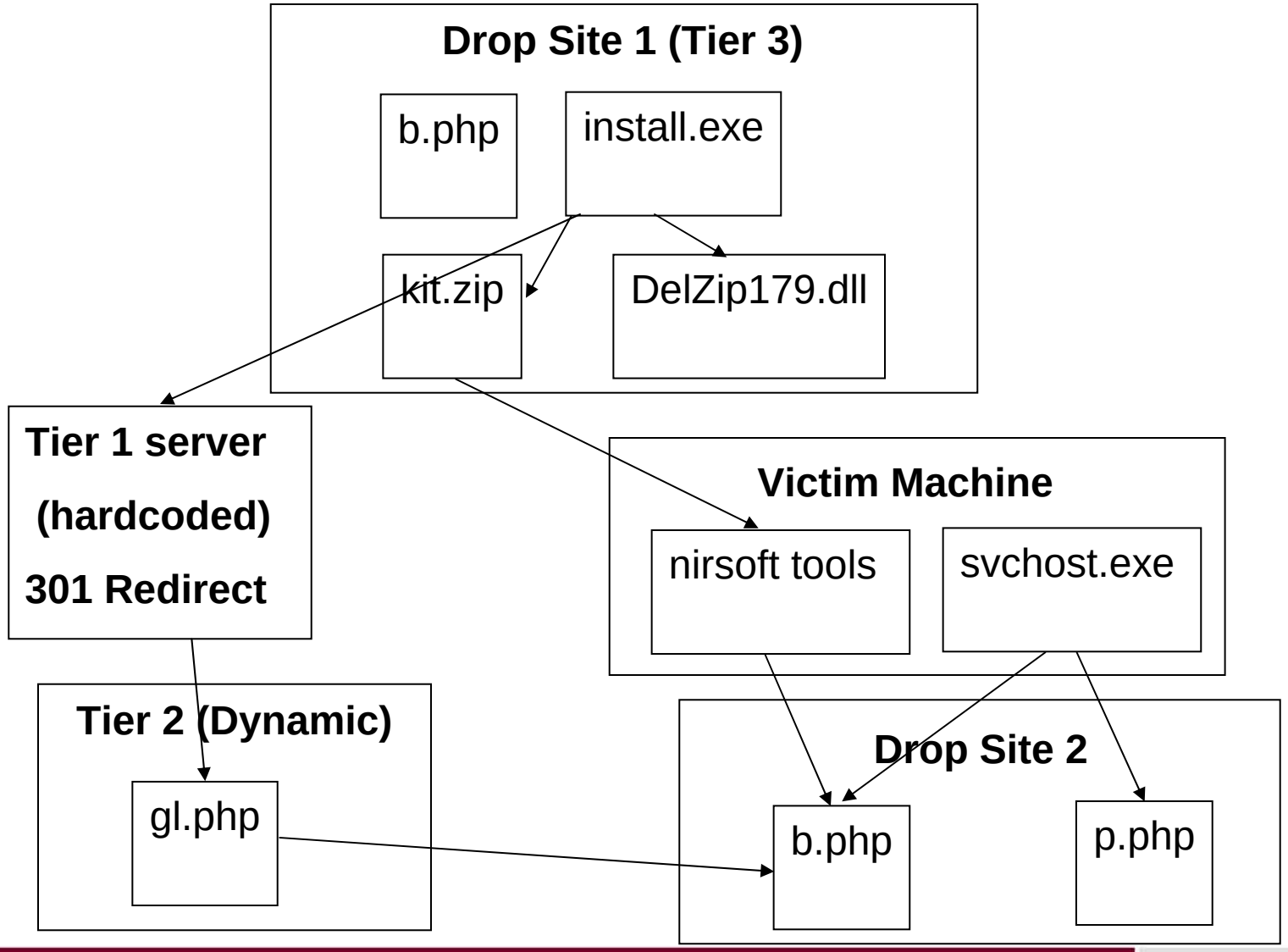
VeriSign®

The “A” Approach



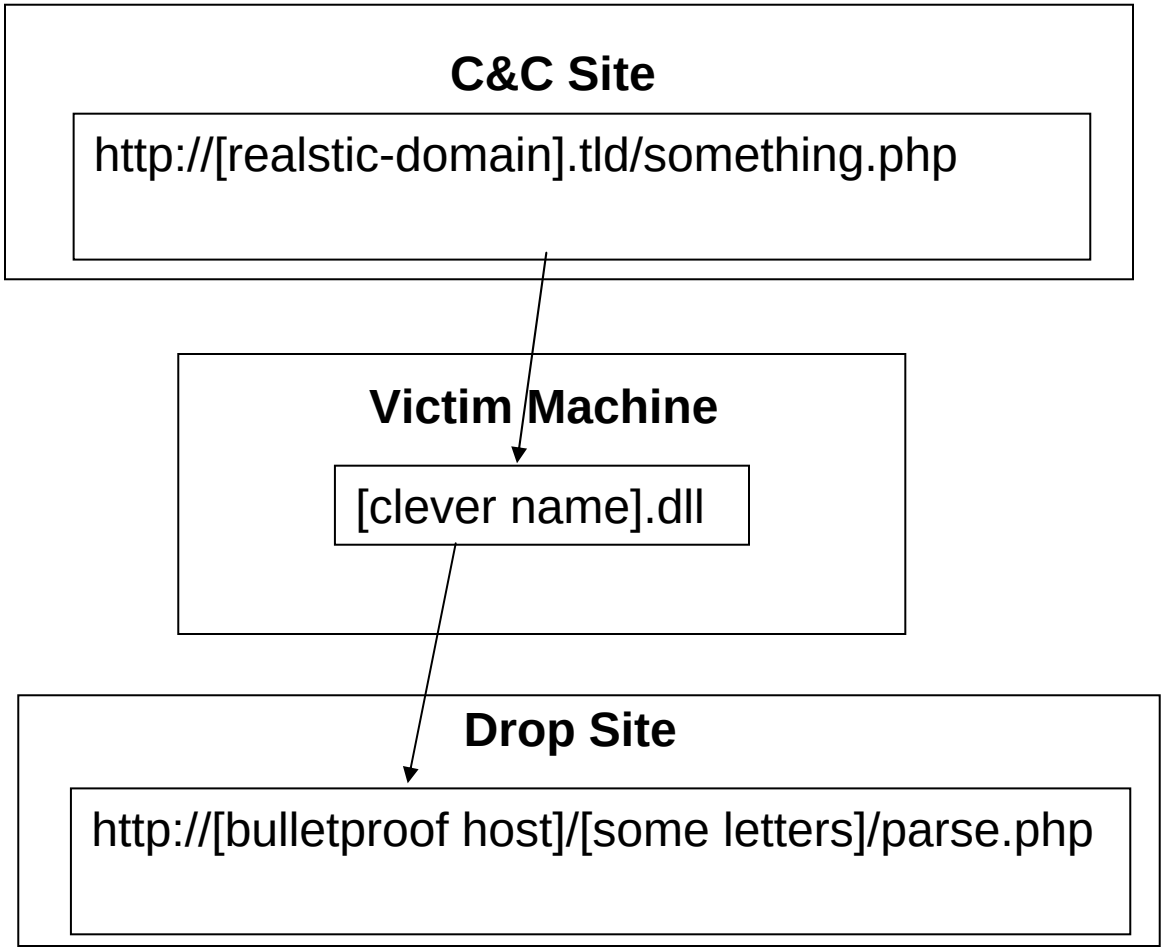
VeriSign®

The “A” Approach (continued)



VeriSign®

The “B” Approach



VeriSign®

Demo #1 - BBBMapper.py

Attack Mitigation Strategies

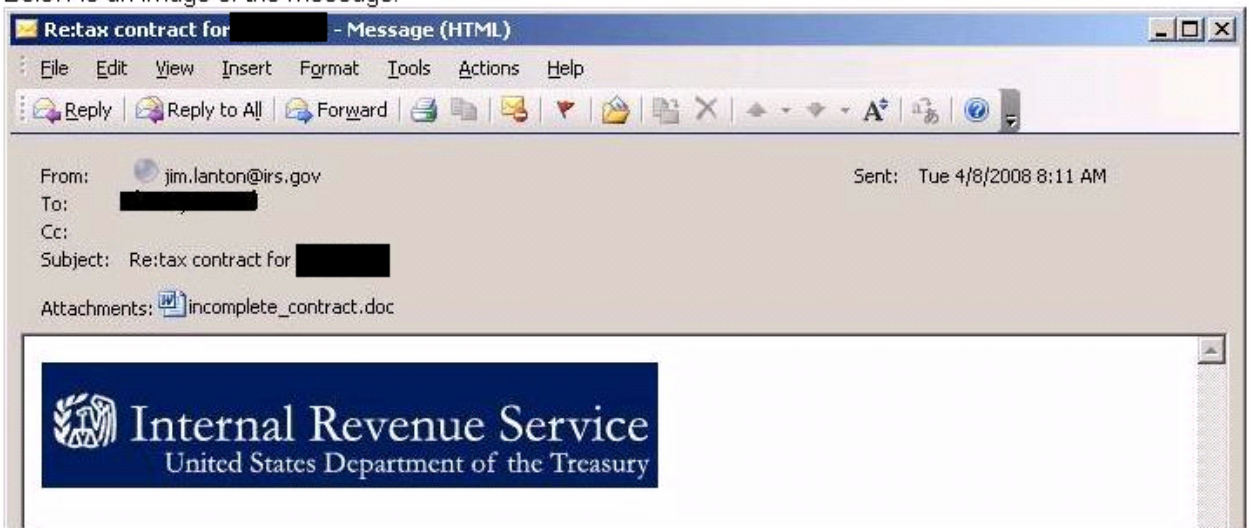
+ Variations on MFA
+ Transaction Verification
+ Server-side Detection
+ Credential Recovery / Victim IP Flagging
+ User Education
+ Transaction Fraud Detection
+ IDS/IPS Exploiting Lack of Attacker Innovation

User Education…Really?

+ Never 100 percent, but many success stories
+ Explain the situation, potential variations, and give a picture
+ Water-cooler effect in action

Several [redacted] users have received an email claiming to be from the IRS. If you receive this email, **please delete it immediately**. Under any circumstances, **do not open the attached word document**; it contains a virus that is currently not detected by the [redacted] anti-virus application.

Below is an image of the message:



Snort Sigs For FIRST Member Organizations

+ Available via e-mail for any members, can be shared with entire list if posting signatures to list is permissible

Demo #2 – The Real Payload

Q&A

Special Thanks

+ Matt Richard
+ FIRST SC and Members
+ The kind folks from Conference & Publication Services, LLC

  for dealing with all our last minute changes

Michael La Pilla

mlapilla@idefense.com

VeriSign iDefense Malicious Code Operations Team