Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

March 7, 2012

Virginia Information Technologies Agency

ISOAG March 2012 Agenda

I.	Welcome & Opening Remarks	Michael Watson, VITA
II.	McAfee Threats Briefing	Dave Marcus, McAfee
III.	DNS Sinkhole	Eric Taylor, NG
IV.	Overview of Security Laws	Bob Baskette, VITA
V.	Shell Game	Bob Baskette, VITA
VI.	Upcoming Events & Other Business	Michael Watson, VITA
VII.	Partnership Update	Bob Baskette, VITA Mike Clark, & Moses Camacho, NG

McAfee Threats Briefing

Dave Marcus
Director, Advanced Research and Threat Intelligence
McAfee Labs

McAfee
An Intel Company

SAFE NEVER SLEEPS™

Key Trends

- Hacktivist activities increased particularly targeting global financial, military and other public sector enterprises
- Attacker attention turns from PCs to mobile devices, particularly Android
- Attacks on Android nearly quadrupled
- PC malware and FakeAV attacks declined significantly in Q4
- Reported data breaches have more than doubled in the last two years
- Network level attacks techniques are now led by attacks on Microsoft's Remote Procedure Call, SQL injection and cross site scripting

Hactivism Activities Accelerated in Q4

- Anonymous, in support of the Occupy Wallstreet movement, attempted to disrupt operations at both the NYSE and Toronto Stock Exchange via DDOS attack. Squabbles amongst Anonymous members mitigated the impact of the attacks.

- Anonymous announced it penetrated the network of US security consultant Stratfor. After stealing confidential client lists and mining more than 4,000 credit card numbers, passwords, and home addresses, the attackers used credit card information to make contributions to charitable organizations such as the American Red Cross and CARE.

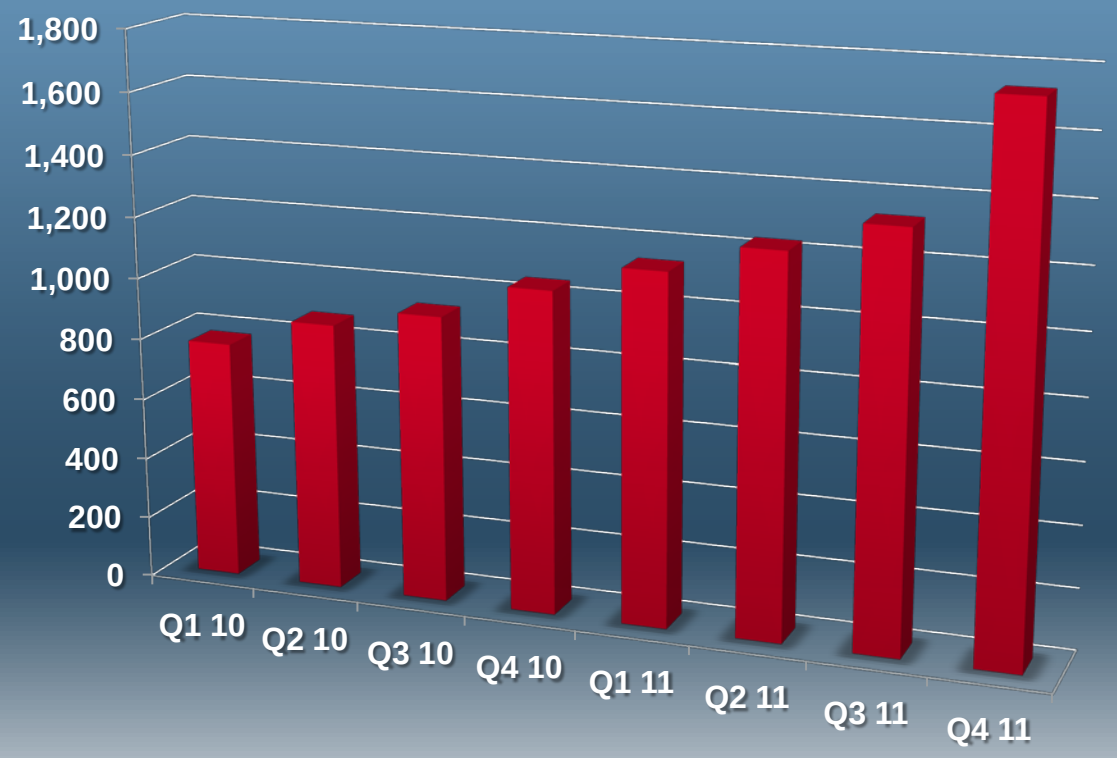
- The year ended with the operation #lulzxmas, described by Anonymous as a weeklong hacking campaign against sites related to global finance, militaries, and governments.

- “Doxing” activity (releasing photos of police and publishing personal and family details of police and other public figures) ramped as a popular hactivist activity.

- We expect them to turn attention to SCADA and Infrastructure attacks

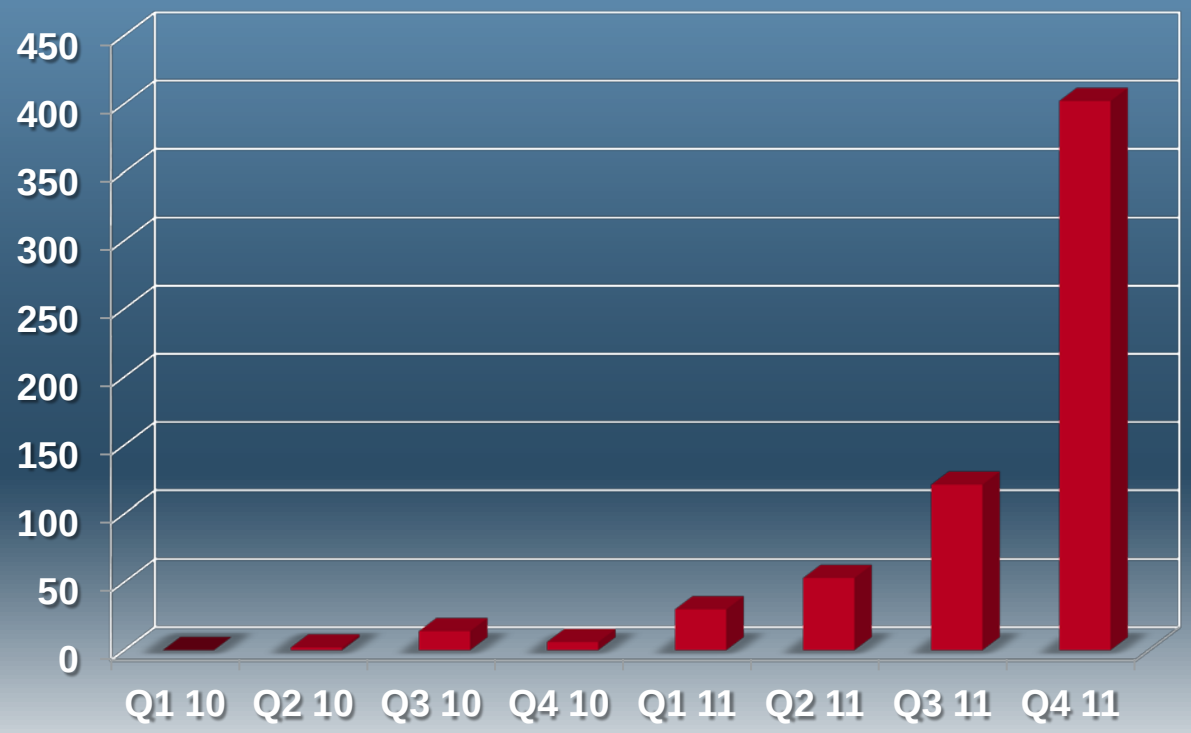
Mobile Malware - Cumulative

Mobile malware has now established itself as the fastest growing category as attackers continue to experiment with new attacks aimed primarily at the Android platform.



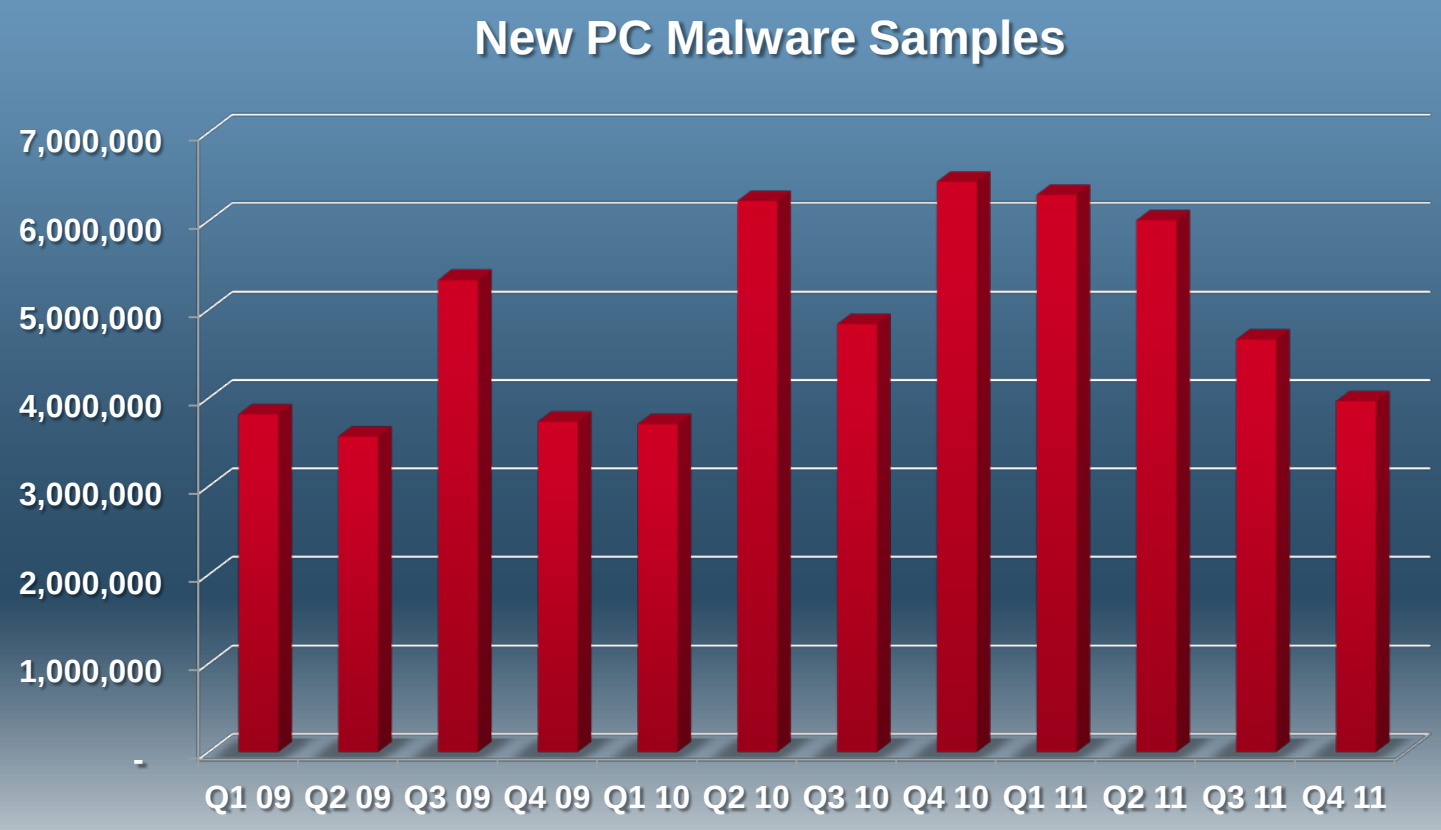
New Android Malware Samples by Quarter

Q4 2011 will be remembered as the point in time when Android malware creation went ballistic. New Android targeted malware samples nearly quadrupled. Much of the Android malware is now been for-profit SMS-sending Trojans, which benefit cybercriminals by hijacking phones to send messages that cost their owners money. Rooting Android devices has becoming easier with the availability of apps that combine vulnerability exploits.



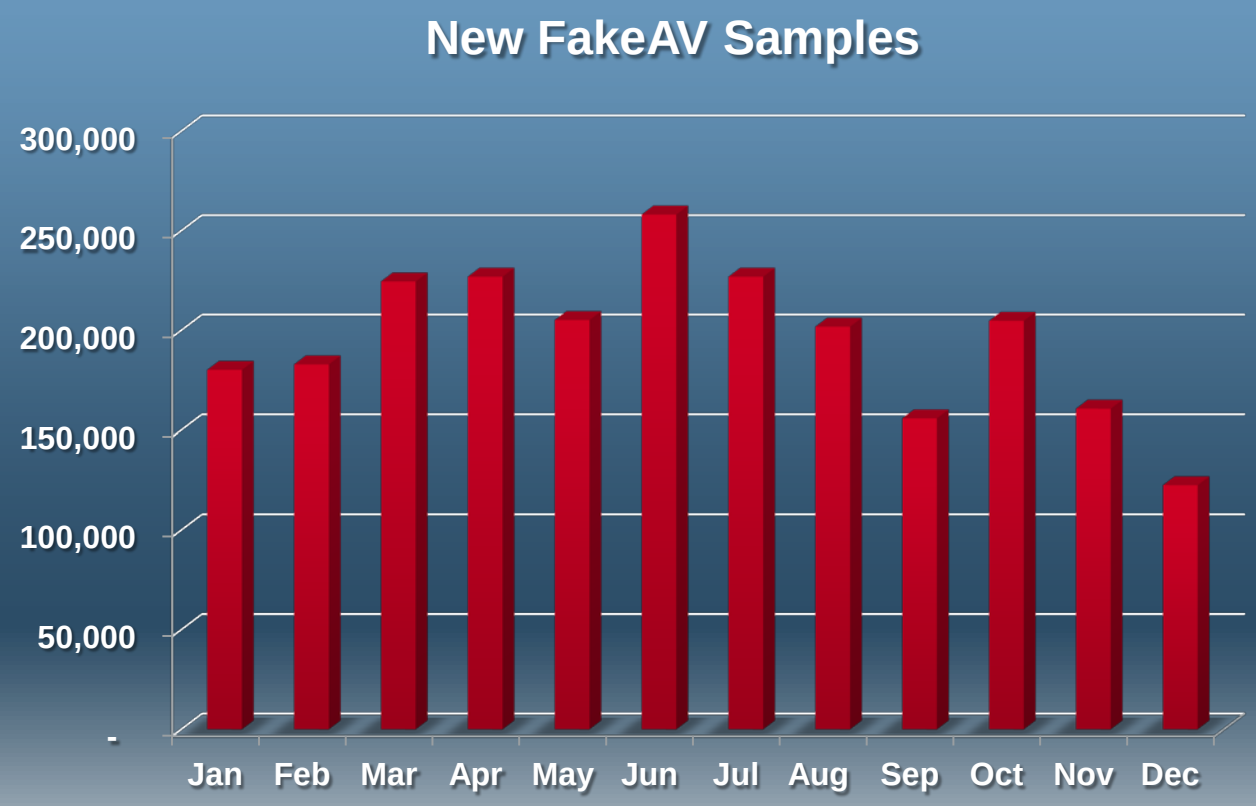
Key Trend: PC Malware Growth Slows

The overall growth of PC-based malware continued to decline throughout the quarter and is significantly lower than last year at this time. But don't get complacent. The cumulative number of unique malware samples in our collection still exceeds the 75 million mark, as we predicted in our last report.



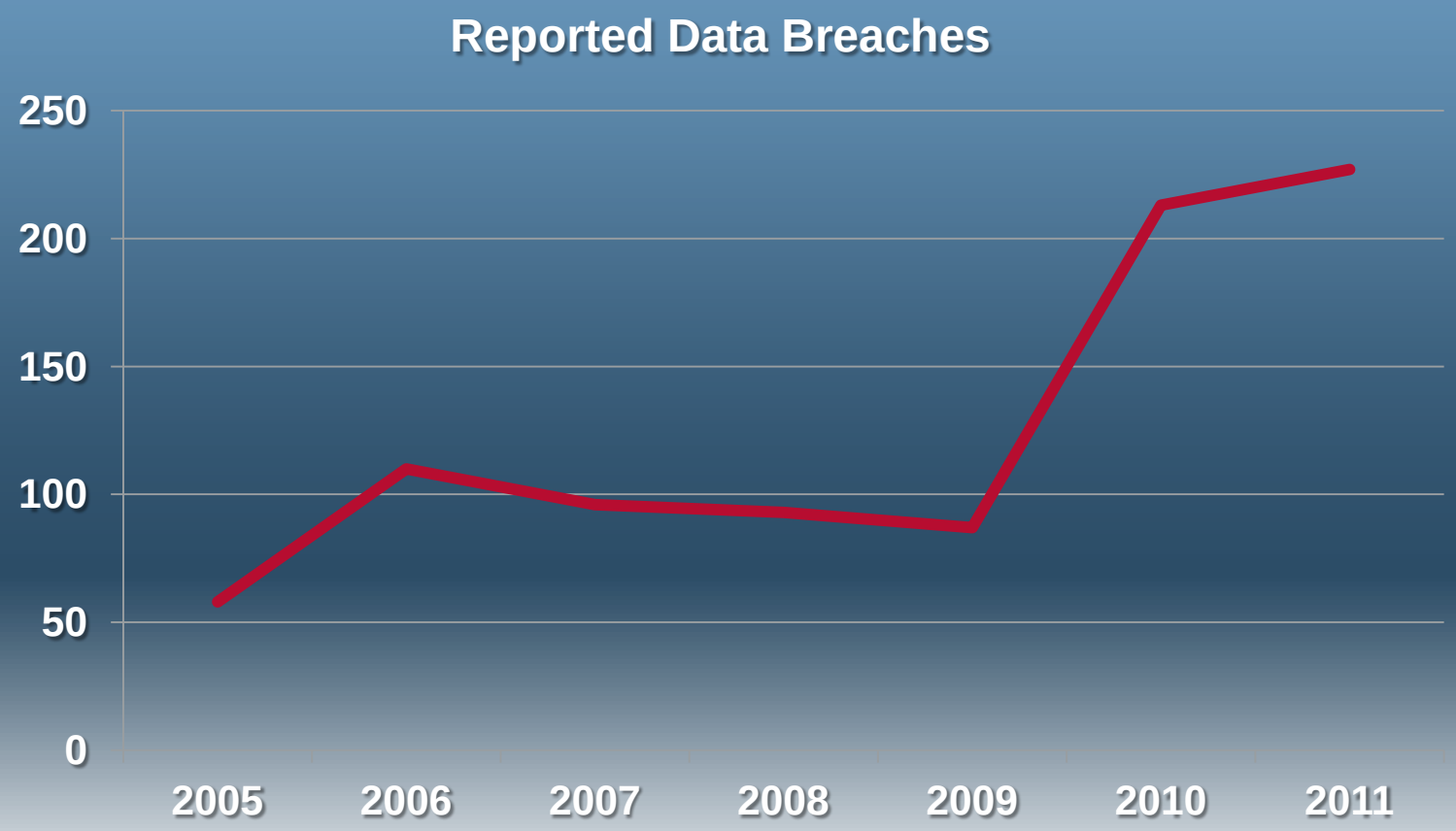
Fake AV Continues to Decline

New FakeAV activity declined 15%+ from Q3 and continued to suffer from ongoing law enforcment activities and (presumably) smaller returns owing to user education campaigns.



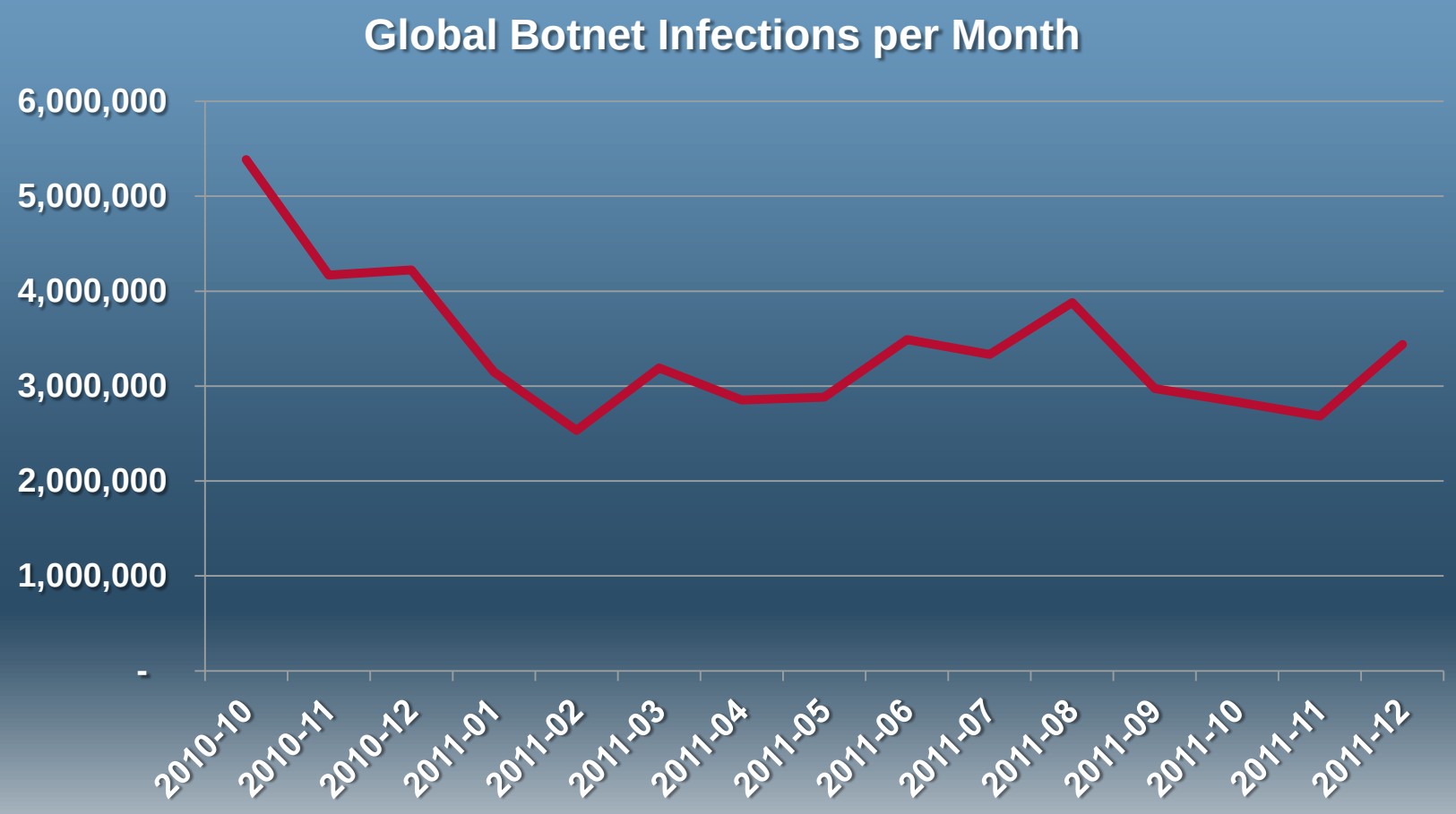
Reported Data Breaches Accelerate

The number of reports of data breaches via hacking, malware, fraud, and insiders has more than doubled since 2009. In the Q4 2011 alone we saw more than 40 breaches publically reported. Although the last three months are not the record holder in this area, data breach events continue to increase.



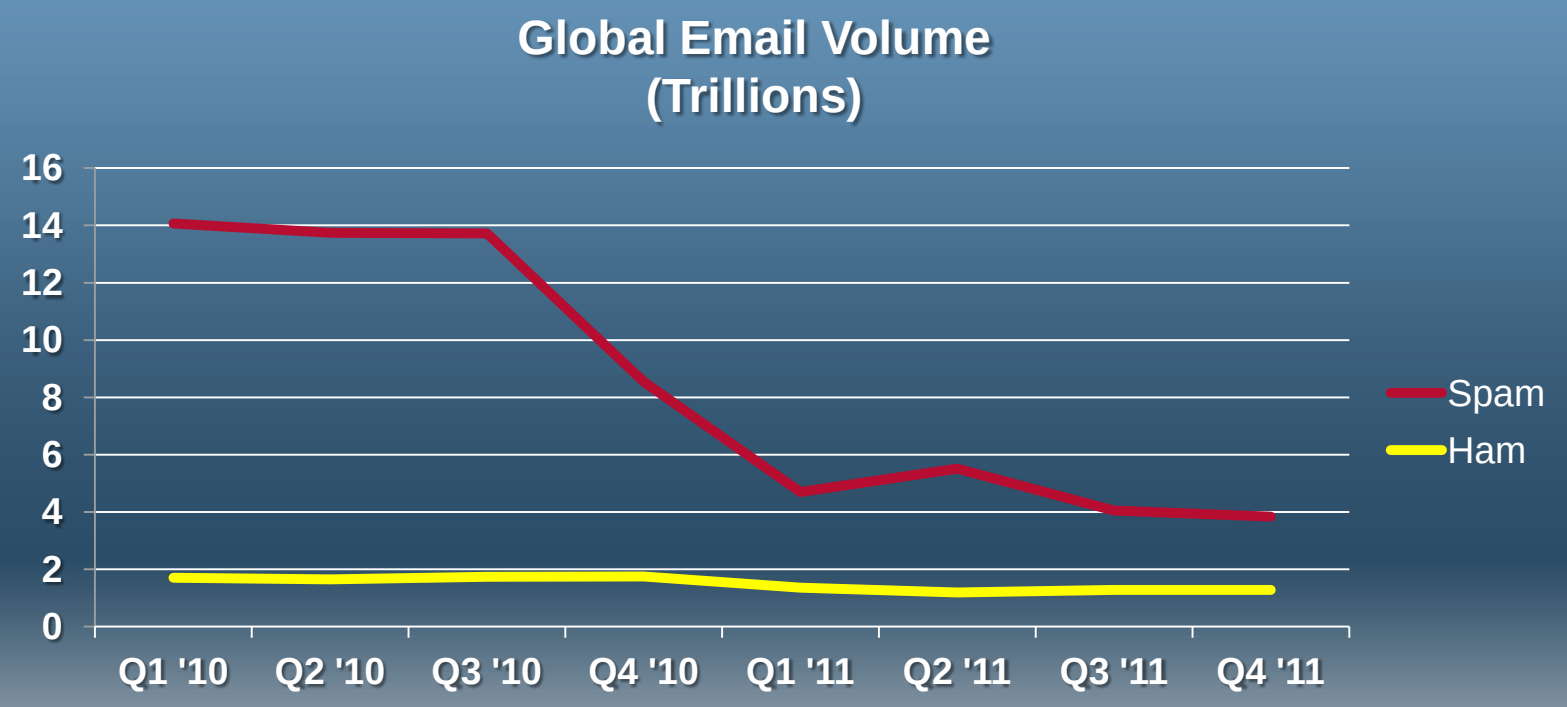
Key Trend: Botnet Infections Recover

Botnet infections rebounded strongly in December, but is still no where near its historic peak. Brazil, Belarus, Columbia, India, Spain, Turkey, and the United States saw significant increases.



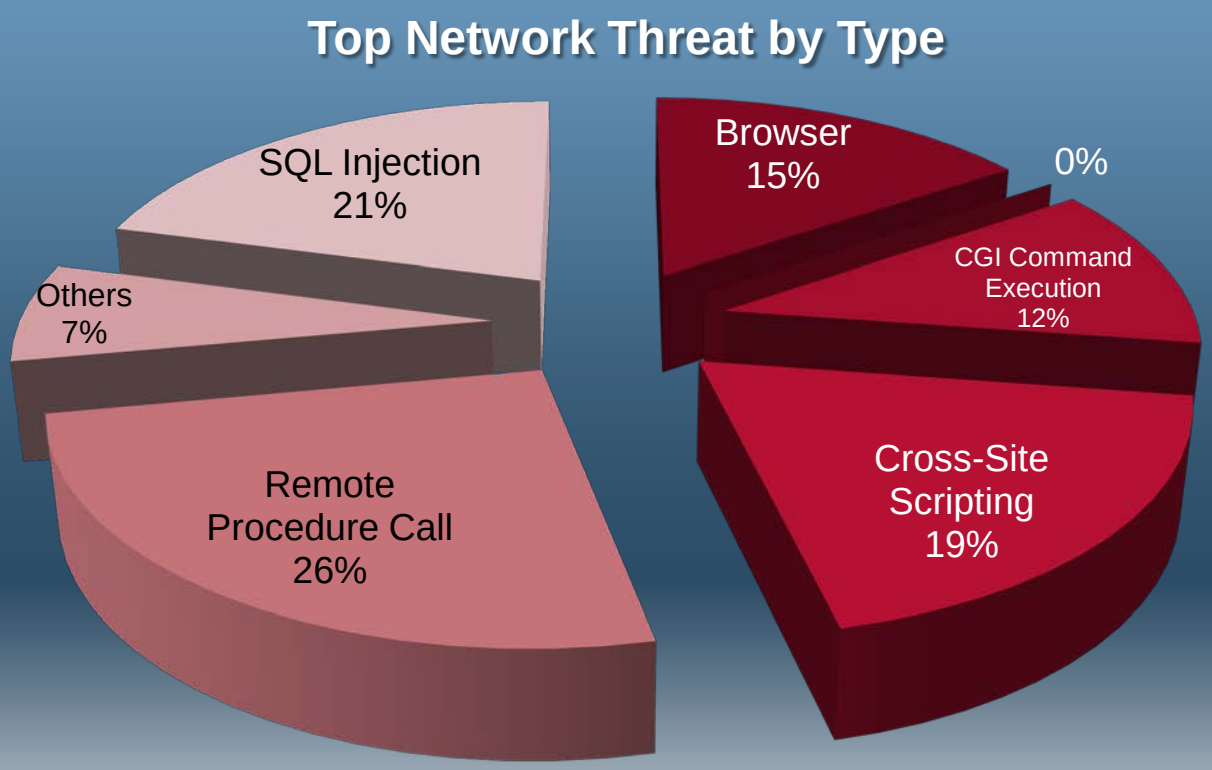
Spam Volume Fails to Recover

Despite the recovery of botnet activity, spam volume did not recover from the “Crash of ’10”. Global spam volume remains at an historic low…or at least a recent historic low. Those historically perpetrating volume spam attacks are now utilizing targeted phishing techniques to propagate their scams which remain a material risk.



Network Threat Trends

The leading network threat this quarter came via Microsoft remote procedure calls. This was followed by a very close race between SQL-injection and cross-site scripting attacks. These two attacks are very much remote in nature, meaning they can be launched at selected targets around the globe.



2012 Threat Predictions and Expectations

McAfee
An Intel Company

SAFE NEVER SLEEPS™

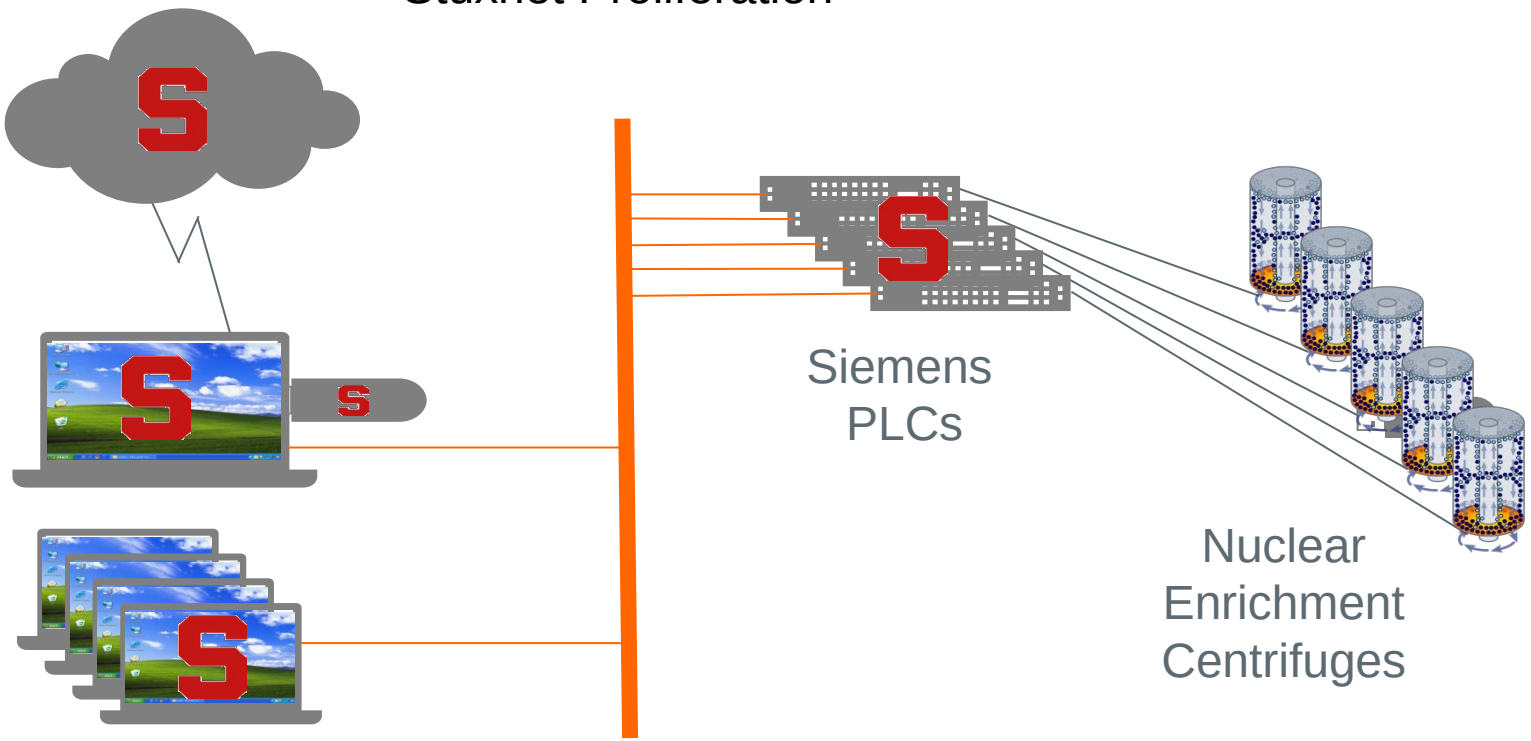
Threat Radar for 2012

- Industrial Threats Will Mature
- Hacktivism: Reboot or Marginalize
- Virtual Currency Attacks
- Windows 8: BIOS and Hardware Attacks
- Mobile Botnets and Rootkits
- Rogue CERTs: Rooting Trust

Industrial Attacks Will Mature

Stuxnet proved that malicious code can create a real world, kinetic response. Recent incidents directed at water utilities in the United States show that these facilities are of increasing interest to attackers. The more attention is focused on SCADA and infrastructure systems, the more insecurity seems to come to light. We expect to see this insecurity lead to greater threats through exploit toolkits and frameworks as well as the increased targeting of utilities and energy ICS systems in particular.

Stuxnet Proliferation



Get to know SHODAN

www.shodanhq.com/search?q=admin%2B1234+country%3AKR

Trojan.Boxnet Imported

Main Exploits Research Videos Anniversary Promotion

SHODAN admin+1234 country:KR Search

Home Search Directory Data Analytics/ Exports Developer Center Labs

Add to Directory Export Data

Results 1 -

121.162.52.11
Added on 22.01.2012
Seoul
Details

HTTP/1.0 401 Unauthorized
Server: GoAhead-Webs
Date: Sun Jan 22 23:50:15 2012
WWW-Authenticate: Basic realm="Default: admin/1234"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html

121.134.83.67
Added on 22.01.2012
Seoul
Details

HTTP/1.0 401 Unauthorized
Server: GoAhead-Webs
Date: Mon Jan 23 01:18:10 2012
WWW-Authenticate: Basic realm="Default: admin/1234"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html

112.162.233.49
Added on 21.01.2012
Seoul
Details

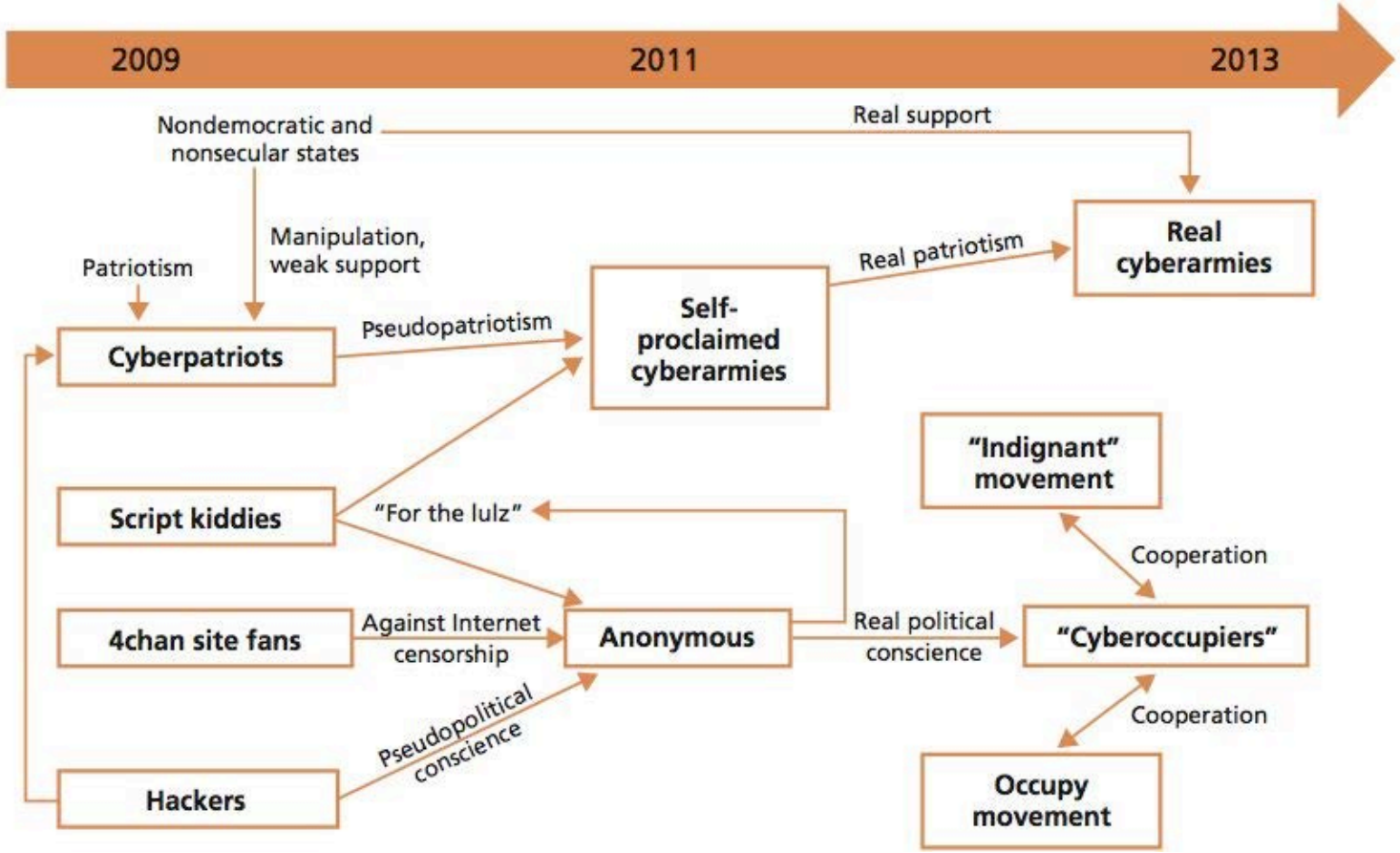
HTTP/1.0 401 Unauthorized
Server: GoAhead-Webs
Date: Sun Jan 22 07:34:15 2012
WWW-Authenticate: Basic realm="Default: admin/1234"
Pragma: no-cache

Hacktivism Networks Will Evolve

McAfee believes the historical “Anonymous” syndicate will reinvent itself for die out. The people leading digital disruptions will become better engaged with the people leading physical demonstrations. For political and ideological ends, the private lives of public figures—politicians, industry leaders, judges, and law-enforcement and security officers—will be disclosed this year more than in the past. Some hacktivists will operate along the same lines as the various “cyberarmies” that primarily flourish in nondemocratic or nonsecular states

.

.



Anonymous + SCADA

#US #SCADA #IDIOTS

SCADA EXPLOITS - Hex00010 - Water - Power Plant

BY: A GUEST | JAN 30TH, 2012 | SYNTAX: NONE | SIZE: 1.21 KB | HITS: 2,238 | EXPIRES: NEVER

Severity	Time	Source	Message
Critical	19/08/2011 6:50:12.965...	NH.Water Plant.GST Low Lvl	State changed to Low Level, value is 1 (Current data)
High	2/09/2011 2:11:47.491 AM	NH.Water Plant.GST High Lvl	State changed to High level, value is 1 (Current data)
High	29/06/2011 9:34:14.084...	NH.Water Plant.WW1 ETM Current Hr	State changed to Underrange, value is -6500 Hr (Current data)
High	18/05/2011 10:38:13.755...	NH.Water Plant.GenSet Tank	State changed to Underrange, value is -4.59 inches (Current data)
High	16/02/2011 10:24:51.516...	NH.Water Plant.Utility power	State changed to Power Failure, value is 1 (Current data)
High	19/01/2011 8:16:24.888...	NH.Water Plant.WW Flow Alarm	State changed to Failed, value is 1 (Current data)
High	27/04/2009 2:02:21.738...	NH.Water Plant.Drought Stage 1	State changed to Stage 1, value is 1 (Current data)
High	24/02/2009 4:33:44.578...	NH.MasterRTU	Communications state - Failed (Unable to connect to TCP/IP port)

```
9.  I was able to open up metasploit ans start sniffing the network then running the auto
    further access - i was able to  install and hide my detection
10.
11.
```

Anonymous Doxing

PASTEBIN | #1 PASTE TOOL SINCE 2002 CREATE

PASTEBIN Follow @pastebin

CREATE NEW PASTE TRENDING PASTES

Dox of MPAA CEO Chris Dodd, Powerful Lobbyist for SOPA/PIPA

BY: A GUEST | JAN 18TH, 2012 | SYNTAX: NONE | SIZE: 5.27 KB | HITS: 12,961 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE

249 810

Like Tweet

```
1. Chris Dodd is the Chairman and CEO of the Motion Picture Association of America, one of the largest and
most significant supporters of SOPA and PIPA, the Internet censorship bills in the United States
Congress. The MPAA, under the guidance of Chris Dodd, has lobbied Congress with enormous sums of money
while trying to rush these dangerous bills through Congress. Just this past year, the former Senator who
preached "No lobbying, no lobbying" just before leaving his position, did just that
[http://bit.ly/dgJ1NA]. He joined one of the most powerful lobbies in the country, lobbying for two of
the most controversial bills in recent memory: SOPA and PIPA.
2.
```

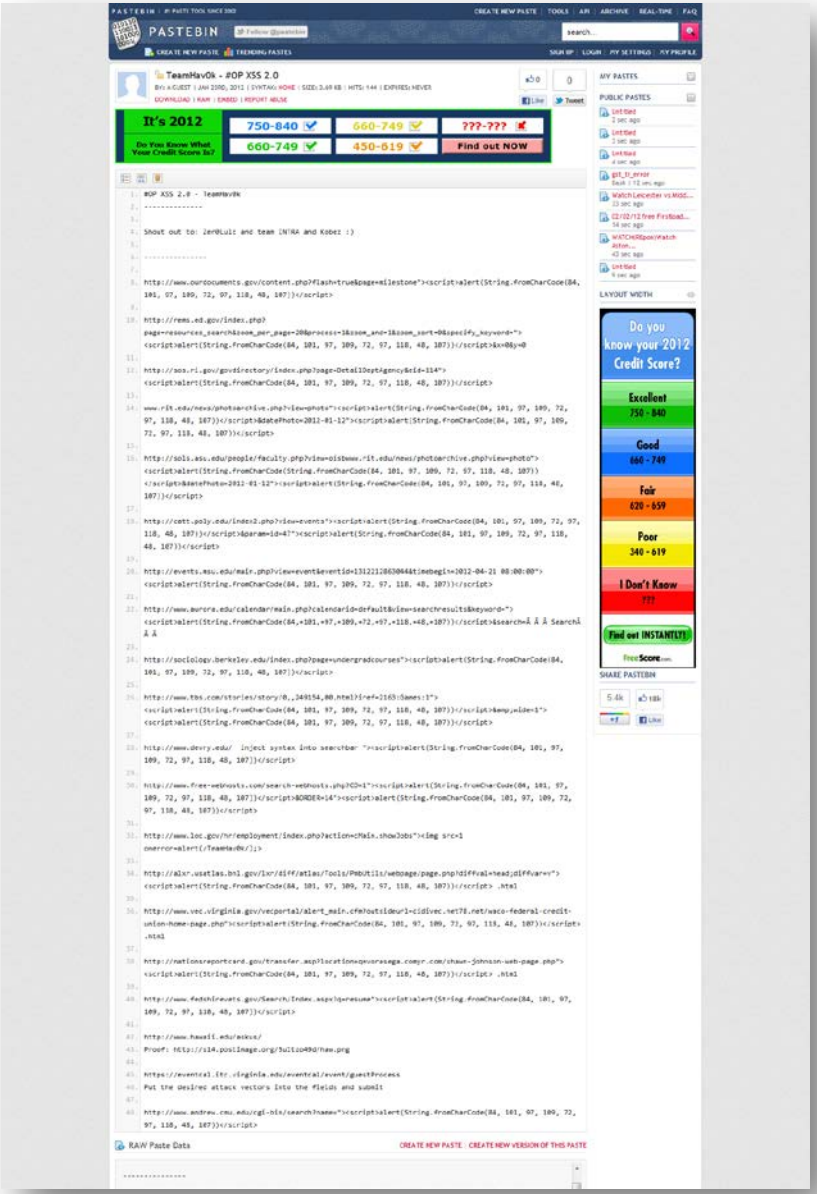
pastebin.com/KEBWLMPP

DoX of Zuffa LLC's Bitches #UgNazi.com #UFC #DanaWhite ...

1 day ago ... Frank J. Fertitta III is current CEO of Station Casinos. He is also an owner of Zuffa LLC, which is the entity that runs the Ultimate Fighting ...

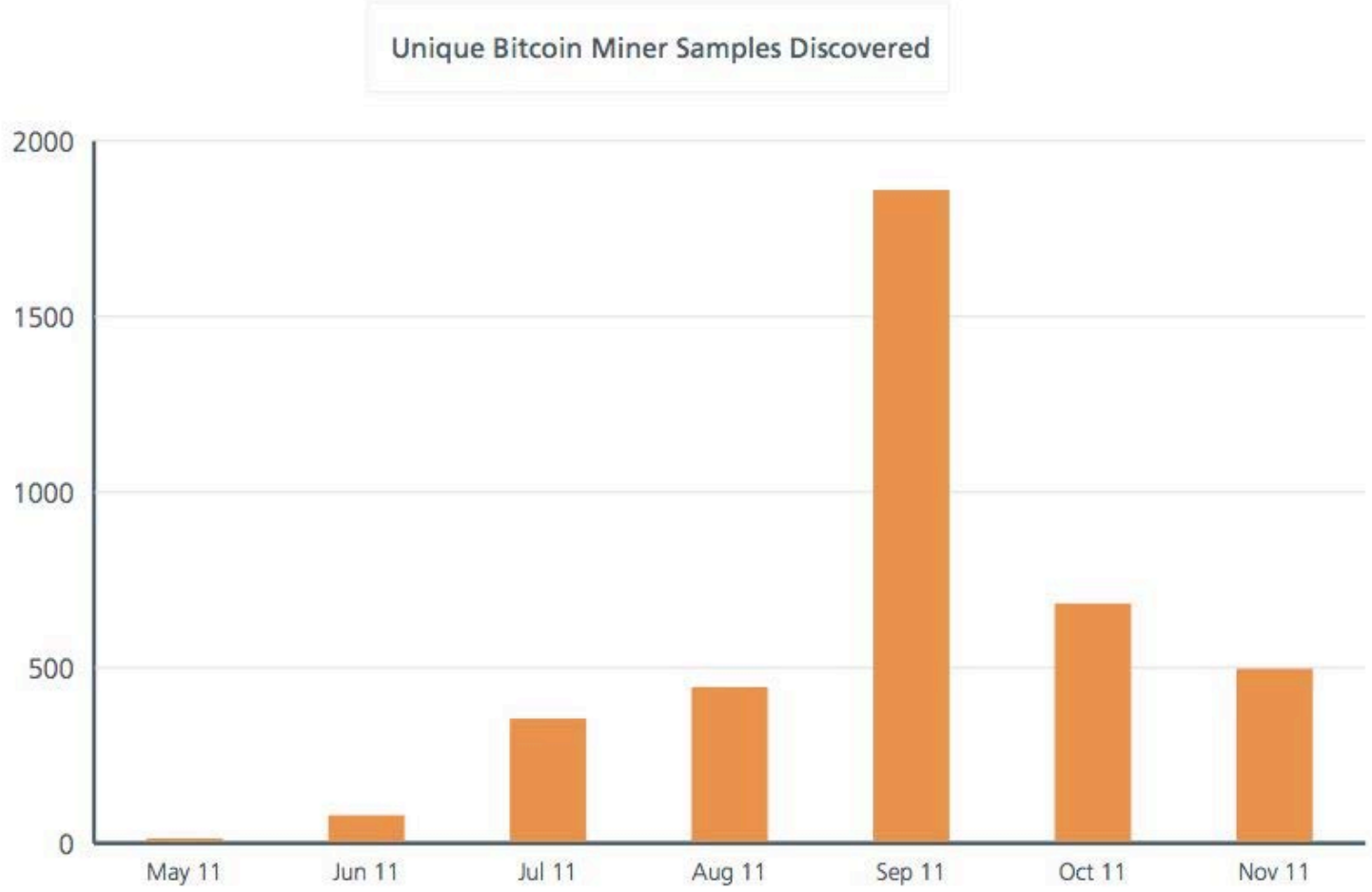
pastebin.com/ZUdQ2BAZ

Learn to love Pastebin



Virtual Currency System Attacks

Virtual currency, sometimes called cybercurrency, has become a popular way for people to exchange money online. Trojan malware easily fits into this architecture. The wallets are not encrypted and the transactions are public. Spam promoting fake Bitcoin mining tools was found in 2011. These tools actually contained malware designed to send the victims' wallet files to a remote location. We expect to see this threat evolve into a cottage industry of cybercrime next year—with spam, data theft, tools, support networks, and other associated services dedicated solely to exploiting virtual currencies.



Mobile Threats

- On PCs, rootkits and botnets deliver ads and make money off of their victims. On mobiles, we’ve seen these types of malware used in the same manner.
- Rootkits allow the installation of additional software or spyware, and botnets can cause ad clicks or send premium-rate text messages.
- Bootkits, malware that replaces or bypasses system startup, also threatens mobile devices. Although rooting one’s own phone or ebook reader opens the device to extra features or to replacing the OS, it can also allow attackers to load their own modified OS.
- Both rootkits and bootkits will proliferate in 2012, though most are currently aimed only at Android.

Rogue Certificates

- Recent threats such as Stuxnet and Duqu used rogue certificates to great effect to evade detection. Although this is not the first time we have seen this behavior (fake AV, certain Zeus variants, Conficker, and even some old Symbian malware used them), we expect to see this trend increase in 2012 and beyond.

- We are very concerned about the implications of large-scale rogue certificates on the whitelisting and application control technologies that use these certs.

- Wide-scale targeting of certificate authorities and the broader use of fraudulent, yet valid digital certificates has ramifications for public-key infrastructure, secure browsing, and transactions

Countermeasures Trends: Intelligence, Response and Red Teams

Extensive Red Teaming and SE Testing

Develop Operational Readiness

Focus on OSINT analysis and Forensics

Extensive Internal CERT Team investments

Partnerships for information sharing

McAfee®

An Intel Company

DNS Sinkhole

Active Defense with DNS

Eric Taylor, Cyber Security Architect
IT Infrastructure Partnership Team

March 2012

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Introduction to DNS

- What is DNS and How it Works

DNS in the Criminal Enterprise

- How the Bad Guys take Advantage of DNS

Active Defense with DNS

- How you can use DNS to Protect Yourself and Your users!

How to Implement a DNS Sinkhole

- Options, Architecture, Key Considerations…

References, Tool and Additional Information

DNS Sinkhole as part of the Defense in Depth Strategy

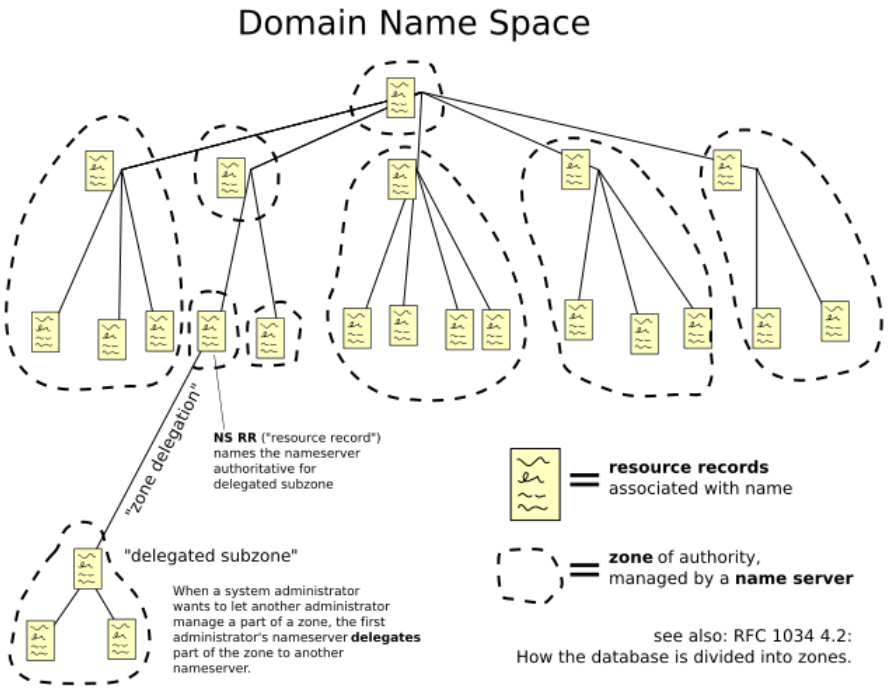
DNS PRIMER

Domain Name Service

- DNS servers resolve names, like "www.virginia.gov", to IP addresses.
- DNS is the phone book of the Internet
- Invented in 1983 by Paul Mockapetris, the Domain Name System (DNS) architecture is referenced in RFCs 882 and 883.
- Hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network
- A Domain Name Service translates queries for domain names (which are meaningful to humans) into IP addresses for the purpose of locating computer services and devices worldwide.

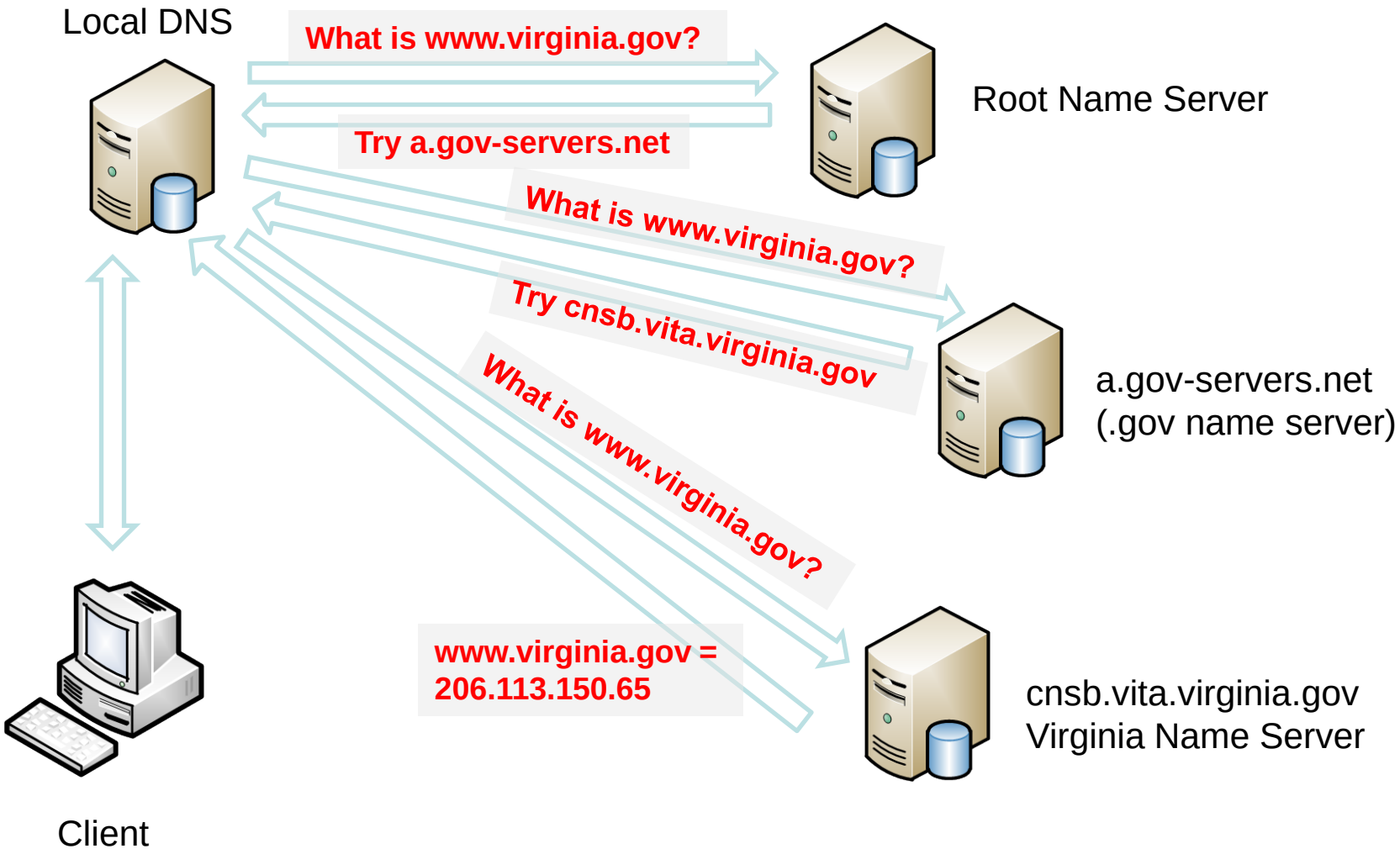
DNS Concepts

- Domain Name Space Consists of a Tree Like Architecture
- A Leaf is a Sub-Domain in which Authority is said to be Delegated
- An **Authoritative Name Server** is a Name Server That Gives Answers That Have Been Configured By an Original Source
- DNS Resolvers, is the Client-side of DNS
  - Responsible for Initiating Queries that should result in Full Resolution



Source: wikipedia

DNS In Action



DNS IN THE CRIMINAL ENTERPRISE

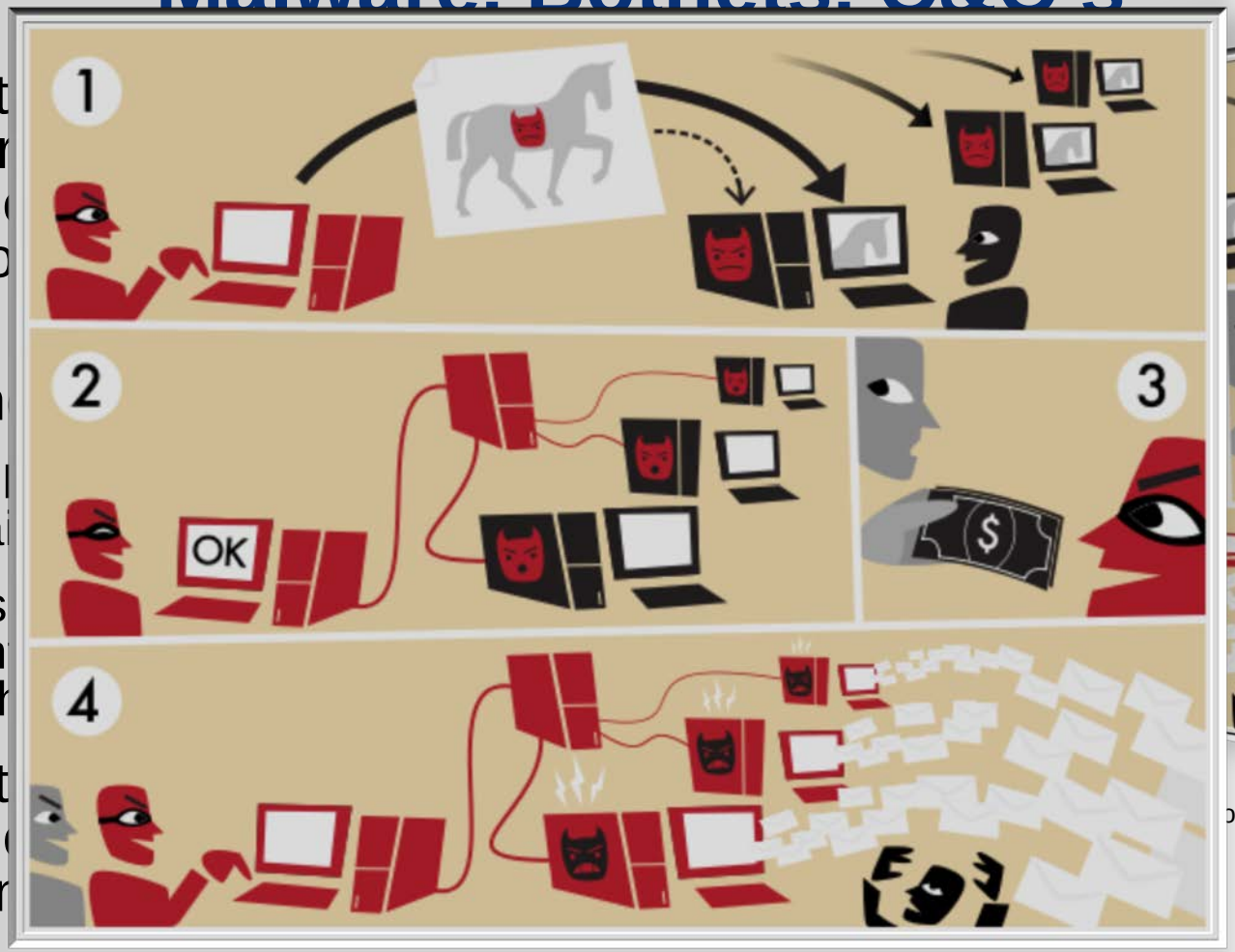
Malware, Botnets, C&C's

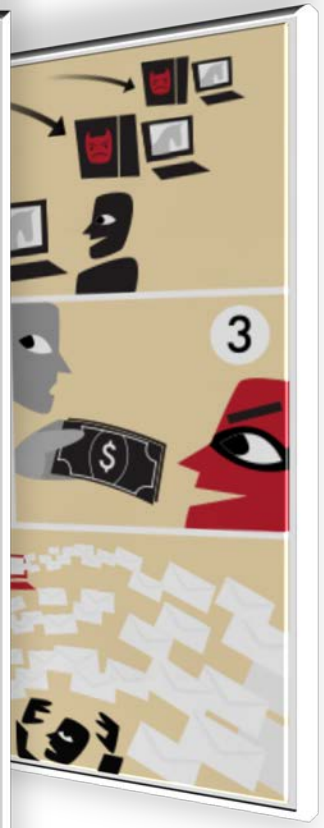
- Malicious Software – designed to exploit the computer system to install software for the purpose of malicious activity.
  - Key Logger – steals key strokes, such as passwords or bank information
  - Trojan software – backdoor access
  - Rootkits – software that allows the software to essential that it *stays* concealed
- Botnet's, SPAM Bots, FastFlux Networks
- Infection via Drive By Download or Social Engineering

```
GET /?777 HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shock
Referer: http://www.google.com/imgres?imgurl=http://daytoncreate.org/wp-cont
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
Host: dwedwedwed.co.cc
```

Malware, Botnets, C&C's

- Botnet
  Compr
  with C
  Contro
- Some
  Hostin
  - Dynl
    Afrai
  - This
    poin
    will h
- Botnet
  Downl
  User ir

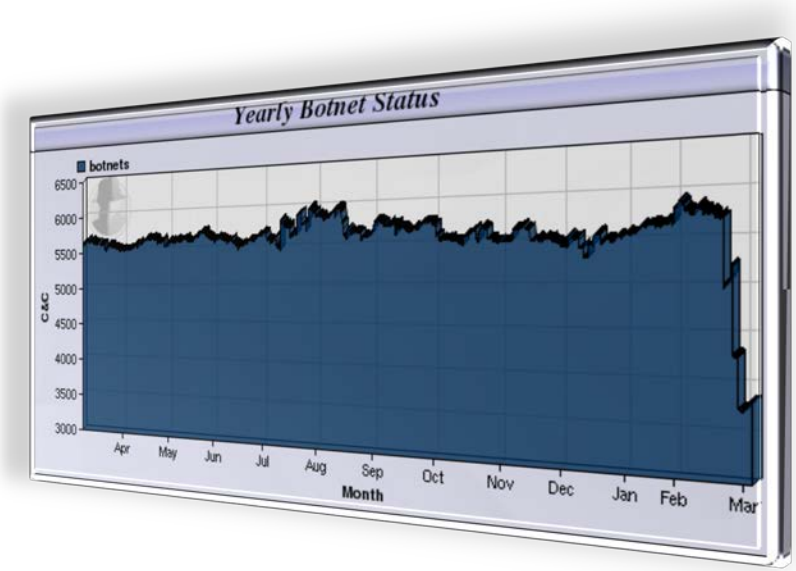




om-b

Malware, Botnets, C&C's

- Fast Flux DNS
  - Technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies
  - Peer-to-Peer Networking
  - Distributed Command and Control
  - Web-based load balancing and proxy redirection used to make malware networks more resistant to discovery and counter-measures.
- The Storm Worm is One of the Recent Malware Variants to Make Use of This Technique.



Source: ShadowServer.org

DNS SINKHOLE

Key Advantages

Simple Architecture

- Effective at detecting and blocking malicious and unwanted traffic from reaching the Internet
- Capable of mitigating many different types of threats that use DNS
- Advance Deployments could be complex, DNS is simpler then other solutions

Administration

- Automation using Scripts
- Plugs into existing network topology
- Does require a good understanding of the DNS Architecture

Cost

- Open Source Software
- Minimal Hardware Requirements or Virtual Systems

Malware Prevention through DNS Redirection (DNS Sinkhole) - DYI

Authoritative Zone

- Your DNS Server becomes Authoritative for Specified Zone
- Will Respond with an IP Address You Specify
- DNS Server will list each Zone Published

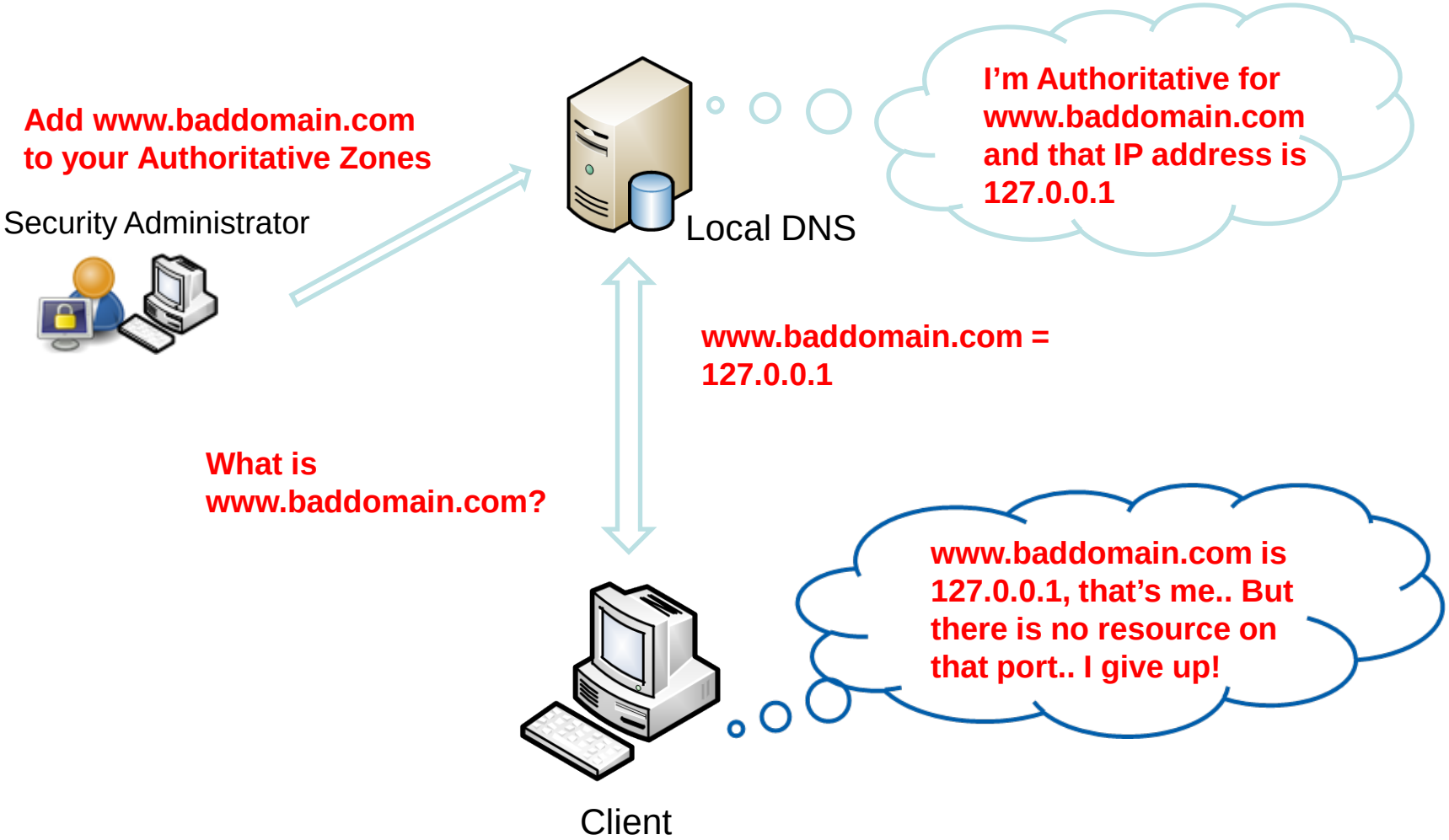
Reverse Policy Zone (RPZ)

- Internet Systems Consortium (ISC) BIND 9.8 Extension
- Enables DNS Administrators to selectively Block DNS Resolution of Sites.
- Allows for Redirection to a Internal Webpage (walled garden) for End User
- Or NXDOMAIN – unable to respond
- DNS Server will list one Zone, mappings are in the Zone File

DNS Sinkhole Options

Type	Authoritative	Reverse Policy Zone	Commercial DNS Forwarder
Benefits	Inexpensive, scalable, effective	Inexpensive, scalable, effective Allows for Dynamic updates (timeliness)	Quick implementation for Small / Medium Size sites
Updates Process	Add a New Zone, Update DNS Server (may require restart)	Incremental Zone Transfers Dynamic DNS Updates	Provided by Vendor
Required software	BIND, Windows DNS, or any DNS software; Or DNS Server ISO	BIND 9.8	Setup provided by Vendor.
Disadvantages	Ongoing maintenance of Zone files	Requires a more complex setup with an Active Directory environment.	Cost $$$

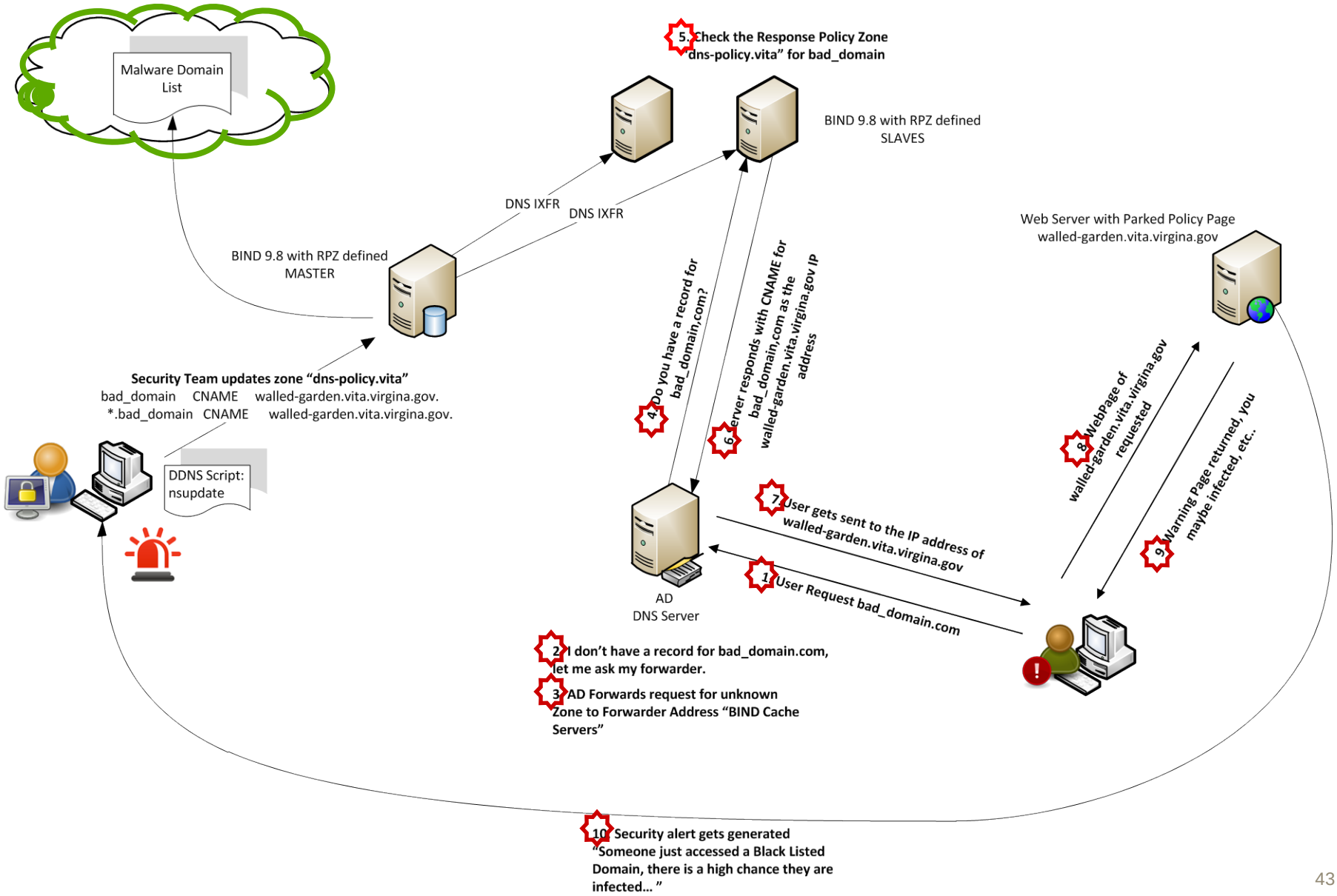
DNS Sinkhole – Simple Architecture



DNS Sinkhole – Enterprise Architecture

Enterprise Grade DNS Sinkhole using BIND Reverse Policy Zone with Split Horizon DNS

- Active Directory for Client DNS Resolver
  - Typical Enterprising using Microsoft Active Directories have DNS Built in
- BIND 9.8 for Cache DNS Server
  - If Using a Split Horizon DNS Architecture – This could be used as the forwarders for AD DNS servers
- RPZ Zone Forwards Request to Internal Webpage
  - Response to Query would Result in CNAME pointing to Walled Garden
- User Gets Webpage message
  - You could be “infected”
- Computer Security Team gets alert of possible infect client or re-direct activity.


Malware Domain List
5. Check the Response Policy Zone "dns-policy.vita" for bad_domain
BIND 9.8 with RPZ defined SLAVES
DNS IXFR
DNS IXFR
BIND 9.8 with RPZ defined MASTER
Web Server with Parked Policy Page walled-garden.vita.virgina.gov
Security Team updates zone "dns-policy.vita"
bad_domain CNAME walled-garden.vita.virgina.gov.
*.bad_domain CNAME walled-garden.vita.virgina.gov.
DDNS Script: nsupdate
4. Do you have a record for bad_domain.com?
6. Server responds with CNAME for bad_domain.com as the walled-garden.vita.virgina.gov IP address
8. WebPage of walled-garden.vita.virgina.gov requested
9. Warning Page returned, you maybe infected, etc..
7. User gets sent to the IP address of walled-garden.vita.virgina.gov
1. User Request bad_domain.com
AD DNS Server
2. I don't have a record for bad_domain.com, let me ask my forwarder.
3. AD Forwards request for unknown Zone to Forwarder Address "BIND Cache Servers"
10. Security alert gets generated "Someone just accessed a Black Listed Domain, there is a high chance they are infected... "

Malware Domain Blocklist

- Several List Providers available
- Commercially available
  - Near Zero False Positive
  - Quickly updated
  - Normally includes freely available list also
  - Typically support RPZ, Authoritative Zones, or bulk data feeds
- Free for Noncommercial Use
  - Collected via various sensors and community participation

- 170+ Domains added March 2nd 2012

Scalability and Performance

- DNS is a Highly Scalable System
- Multiple Redundant Servers can be Provisioned
- A Single DNS BIND with 1GB or RAM could Support a Load Well over 20,000 Clients
- Can be Located in Different Geographic Locations

Limitations, Caveats & Warnings

- Using DNS server does not prevent malware or spyware which uses an IP address from connecting.
- Blocking by IP address is a better job for firewalls and routers, which usually do not block by domain name.
- Using Windows DNS for a DNS Sinkhole is a little more complicated
- Don’t forget to remove cleaned or stale domains

Limitations, Caveats & Warnings

- Does Not Detect Malware or Eradicate Malware
- Must Take Proper Care When Implementing New Zones or RPZ Updates, You Could Block Legitimate Sites!
- TTL or Ghost Cache Records Could Cause Records to Still Respond
  - This could allow DNS clients to cache records for a extended period of time
- Does not Extend to the Road Warrior or Home User

Caveats & Warnings

- Why user your DNS server, when I can use my own…
- Malware with Build-in DNS will never use the Sinkhole
- Unless; Transparent redirection of DNS queries using WCCPv2 or NextGen Firewalls
- Strict Control of DNS traffic required..

DNSChanger

Source: FBI.gov

Sinkhole Alternatives

- Intrusion Prevention Systems – provide some control over DNS, looking for anomalous DNS packets, short DNS time-to-live, Integration with Vendors DNS Blocklist, etc..
- Darknets – is a portion of routed network that has not active services but can be used to collect data about anomalous network traffic
  - This can be used as monitoring network to collect malware looking for new victims
- Routing Sinkholes – using routing protocols to forward IP addresses or subnets to a null interface (bit bucket) or a security monitoring device.

REFERENCES, TOOLS & LIST PROVIDERS

References

- Windows DNS Server Blackhole Domains Tool - http://www.sans.org/windows-security/2010/08/31/windows-dns-server-blackhole-blacklist
- Taking Back DNS - http://www.isc.org/community/blog/201007/taking-back-dns-0
- The canonical reference to DNS RPZ - https://deepthought.isc.org/article/AA-00525/0/Building-DNS-Firewalls-with-Response-Policy-Zones-RPZ.html
- EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis - http://iseclab.org/papers/bilge-ndss11.pdf
- BlackHole DNS for Malware and Spyware - http://www.malwaredomains.com/wordpress/?page_id=6

DNS Tools

- DNS Sinkhole ISO - http://isc.sans.edu/diary.html?storyid=9037
- Passive DNS - A network sniffer that logs all DNS server replies for use in a passive DNS setup - https://github.com/gamelinux/passivedns
- Snort Rules for DNS spyware - http://www.autoshun.org/downloads/bhdns.rules
- DNS lookup tool using Passive DNS replication to collect public DNS data - http://www.bfk.de/bfk_dnslogger.html?query=sans.org#result
- PortSentry – Used to collect possible infected host by listening on several or all port. - http://sourceforge.net/projects/sentrytools/

DNS Malware List Providers

- **SURBL Data Feeds - http://www.surbl.org/**
- **Spamhaus - spamhaus.org**
- **securityZONES - http://www.securityzones.net/**
- **Malware Domains – www.malwaredomains.com**
- **Ad Banners - http://pgl.yoyo.org**
- **Hosts files - http://hosts-file.net – (Check EULA)**
- **ZeuS Tracker - https://zeustracker.abuse.ch**
- **Malware Database (AMaDa) Blocklist (sandbox signatures) - http://amada.abuse.ch**
- **SANS suspicious domains - http://isc.sans.edu/feeds/suspiciousdomains_High.txt**
- **Malware Patrol - http://www.malwarepatrol.net/cgi/submit?action=list_bind**
- **Exposure (A service that identifies domain names by performing large-scale passive DNS analysis) - http://exposure.iseclab.org/about.html**
- **Malware Threat Center - http://www.mtc.sri.com/ & http://www.blade-defender.org/**

Questions?

Virginia Information Technologies Agency

Overview of Important Information Security Laws

Bob Baskette

Senior Manager, Security Operations and Architect

Title 18 USC Section 1029

Access Device Statue

- Fraud and related activity in connection with the illegal use of access devices

- Intended to prevent unauthorized access to accounts, theft of money, products, or services using illegally generated or obtaining access credentials

Title 18 USC Section 1029

- Criminalizes the possession, use, or trafficking of unauthorized access devices or device making equipment to engage in unauthorized access to money, goods, and services

- Defines penalties for fraud and illegal activity that can take place through the use of such counterfeit access devices

Title 18 USC Section 1029

- Access Devices can include
  - Password dictionaries
  - Stolen credentials, credit card numbers, Bank Pin

- The Secret Service is normally charged with investigating Access Device Statue violations

Title 18 USC Section 1029

- One additional example of Access Device Statute crime is the creation of a website or use of emails to offer false or fictitious products in an effort to capture credit card information

- The activity is considered criminal whether or not a computer is involved

Title 18 USC Section 1030

Computer Fraud and Abuse Act

- Amended by the Patriot Act to extend the definition to include any computer located outside the United States so long as the system could affect the United States.

- Federal law that addresses acts that compromise computer network security

Title 18 USC Section 1030

- Prohibits
  - Unauthorized access to computers and network systems
  - Extortion through threats of such attacks
  - Transmission of code or programs that cause damage to computers

- Addresses the unauthorized access to government, financial institutions, and other computer and network systems

Title 18 USC Section 1030

- Defines the jurisdiction of the FBI and Secret Service

- To violate Section 1030 the act must be committed with full knowledge that the access of the computer system is without authorization or exceeds authorized access

Title 18 USC Section 1030

- A “Protected Computer” is defined by CFAA as any computer used by the U.S. Government, financial institution, or any system used in interstate or foreign commerce or communications

- CFAA is the most widely utilized Federal statute used to prosecute computer crimes due to the "interstate or foreign commerce" clause

Title 18 USC Section 1030

- The FBI is responsible for cases dealing with national security, financial institutions, and organized crime

- The Secret Service is responsible for any crimes pertaining to the Treasury Department and any other computer crime that does not fall under the FBI including protecting critical infrastructure

Title 18 USC Section 1030

- CFAA criminalizes the act of knowingly causing the transmission of a program, information, code, or command without authorized access to the protected computer that results in intentional damage

- The use of malicious software is prosecuted under CFAA

Title 18 USC Section 2510/2701

Electronic Communications Privacy Act

- Intended to protect communications from unauthorized access

- Provides one exception
  - If one of the parties in the communication authorizes the interception no law has been broken

Title 18 USC Section 2510/2701

- Comprised of two components:
  - One amended the Wiretap Act
  - One amended the Stored Communications Act

Title 18 USC Section 2510/2701

- Amended the Wiretap Act
  - Extended coverage to electronic communications
  - Protects communications including wire, oral, and data during transmission from unauthorized access and disclosure
  - Prohibits any intentional interception of wire, oral, or electronic communication in an illegal manner

Title 18 USC Section 2510/2701

- Amended the Stored Communications Act
  - Protects communications before and/or after the communications are transmitted and stored electronically at another location
  - Protects data while at rest

Digital Millennium Copyright Act (DMCA)

- Implemented in 1998 to support the World Intellectual Property Organization Copyright Treaty (WIPO)
- Requires adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors and must restrict acts in respect to their works that are not authorized

Digital Millennium Copyright Act (DMCA)

- Prohibits someone from tempering with and breaking an access control mechanism that is put into place to protect an item that is protected under the copyright law

- Only protects works that fall under the copyright act

Digital Millennium Copyright Act (DMCA)

- Prohibits the sale and use of tools that can break protection schemes including encryption

- Provides an encryption research exemption to allow for identifying the flaws and vulnerabilities of encryption technologies

Digital Millennium Copyright Act (DMCA)

- Provides an exemption for engaging in the act of security testing
- A violation can occur even if the copyright material is not accessed

Cyber Security Enhancement Act of 2002

- Stipulates that attackers who carry out certain computer crimes may now get a life sentence

- If the attack could result in bodily harm or possible death or pose a threat to public health and safety the attack could face life in prison

Cyber Security Enhancement Act of 2002

- Allows the Service Provider to report suspicious behavior without risking customer litigation

- All reports are exempt from the Freedom of Information Act

Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!

Virginia Information Technologies Agency

The Shell Game: Finding the correct shell for your code

Bob Baskette

Senior Manager, Security Operations and Architect

Shell Code Basics

- It is the executable component of a payload designed to exploit a vulnerable application to execute arbitrary code

- A malicious individual can cause a vulnerable application to execute instructions provided by the malicious individual instead of the application

Shell Code Basics

- The malicious code provides either shell access to a remote computer or access to an existing shell with higher privileges

- Modern shell code can also provide encrypted network communications and in-memory process manipulation

System Calls

- Used to request a specific action be performed by the the operating system

- Programs that run in user space must follow a specific procedure for interacting with the operating system

System Calls

- Intel-based X86 systems can issue system calls by invoking the int 0x86 interrupt instruction
- Can also used the dedicated sysenter system call

System Calls

- Microsoft Windows operating systems generally require a user space program to make standard function calls into core Windows library functions

- Virtually all capabilities required by shell code are controlled by the operating system

Microsoft Windows System Calls

- Need to located the required library in memory since the library may be load to a different location or may not be loaded

- DLLs do not necessary appear at the same location in memory on all versions of windows

Unix / Linux System Calls

- Unix / Linux shell code system calls require little more than using the int 0x80 interrupt call after placing the proper values in specific registers

Basic Shell code

- Requires writing assembly code that will spawn a new shell process on the target computer
- The spawned shell process will accept input from the attacker

Basic Shell code

- To launch the new shell process
  - Use the execve system call on the Unix System
  - Use the Create Process function call on Microsoft Windows

Basic Shell code

- To control the input / output of the new shell the attacker must understand
  - The relationship between each child process and how each process inherits system properties
  - The input / output file descriptors from the parent

Basic Shell code

- Regardless of operating system, processes are provided three open files
  - stdin = standard input
  - stdout = standard output
  - stderr = standard error

- Will need to create the shell process such that the shell input / output file descriptors become stdin, stdout, stderr

Port Binding Shell code

- Also called a “Bind Shell”
- The attacker is required to reconnect to the victim once the exploit is successful in order to get attached to the command shell
- Can use a tool such as Netcat to pass the keystrokes to the remote shell

Port Binding Shell code

- Steps needed to create a bind shell
  - Create a TCP socket
  - Bind the socket to an attacker-supplied port
  - Make the socket a listening socket
  - Accept a new connection
  - Duplicate the newly accepted socket onto stdin, stdout, and stderr
  - Spawn a new command shell process to use the new socket

Port Binding Shell code

- The conditions needed to allow port binding shell code
  - The network environment of the target must allow the initial attack to reach the vulnerable service of the target
  - The network environment must allow the attacker to establish a new inbound connection to the port that the shell code is bound to

Port Binding Shell code

- Can be effective in environments where the firewall is not blocking / filtering inbound ports to the target

- Port Binding Shell code cannot distinguish the inbound caller and could allow other individuals to connect to the bind port

Reverse Shell code

- Used when a firewall may block access to the listening socket
- Requires a process that can generate an outbound connection
- Many firewalls are not configured to filter or inspect connections

Reverse Shell code

- Designed to reverse the direction in which the second connection is made and will initiate a new connection to a specific port on the attacking computer
- Does not bind to a specific port on the target system
- Also called a “Call-back” shell

Reverse Shell code

- Steps to establish a reverse connection
  - Create a TCP socket
  - Configure the socket to connect to an attacker-specific port and IP address
  - Connect to the specific port and IP address
  - Duplicate the newly connected socket onto stdin, stdout, and stderr
  - Spawn a new command shell process and use the new socket

Reverse Shell code

- Most reverse shells use TCP-port 80 or TCP-port 443 to hide the outbound connection.

- Must use another port if the victim uses a proxy server to connect to outside hosts

Find Socket Shell code

- Technique designed to reuse the same network connection as the original attack
- Will use the existing connection since the port must be open for the initial attack to be successful
- Has the benefit that no new network connectors will be visible on the victim

Find Socket Shell code

- The challenge to implementing the shell code is to find the open socket since the value of the file descriptor may not be known in advance

- Once found, the shell code must duplicate the socket descriptor to cause the spawned shell to communicate over the open socket

Find Socket Shell code

- A popular technique for locating the proper socket descriptor is to enumerate all possible file descriptors (0 to 255) in the vulnerable application and then query each descriptor to see if it is remotely connected to the attacker

Command Execution Code

- Used when it is not desirable to establish a new network connection or carry out shell operations over an unencrypted session

- The payload uses a single command to establish a more secure connection
  - Copy an SSH public key to the target
  - Invoke system command to add a new user
  - Modify a configuration file to allow a backdoor shell

Command Execution Code

- The payload must perform the following:
  - Stipulate the name of the command that is to be executed
  - Stipulate any command-line arguments for the command to be executed
  - Invoke the execve system call to executed the command

File Transfer Code

- Payload that provides a simple file upload facility
- Can be used to upload a binary to the target and then execute the binary

File Transfer Code

- File Transfer process
  - Open a new file
  - Read data from a network connection
  - Write the data to a new file (connection would be part of a shell)
  - Repeat the read/write process until all data is sent
  - Close the file

Multistage Shell code

- The exploit used to invoke the target vulnerability may not provide enough usable storage space to inject the desired shell code

- Can use a multistage process to upload shell code that is too large for the available storage space

Multistage Shell code

- Multistage payloads consist of two or more stages of shell code
- Sole purpose of the first stage is to load additional shell code and then pass execution control to the newly loaded segment of shell code

Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!

Upcoming Events

Virginia Information Technologies Agency

Information Security System Association

ISSA

DATE: Wednesday, Mar 14, 2012

LOCATION: Maggiano's Little Italy
11800 West Broad Street, #2204, Richmond, VA 23233
TIME: 11:30 - 1:00pm. Presentation starts at 11:45.
Lunch served at 12.
COST: ISSA Members: $20 & Non-Members: $25

SPEAKER: Deneen DeFiore, GE, Site Leader for ISTC

TOPIC: GE's Information Security Technology Center (ISTC) in Glen Allen

Virginia Information Technologies Agency

CISSP Boot Camp

Offered at Thomas Nelson Community College

Certified Information Systems Security Professional (CISSP) is the leading industry security certification for information security professionals. The CISSP Boot Camp is a vigorous week-long training program designed to prepare practicing security professionals to sit for the CISSP Exam.

Class Dates: Monday, March 12 – Friday, March 16 *(8:00 a.m. – 5:00 p.m.)*

At Peninsula Workforce Development Center, 600 Butler Farm Road, adjacent to the TNCC Hampton campus.

Registration: Price $1000.

Call (757) 825-2937 or (757) 258-6591 to register.

http://tncc.edu/business-community/workforce-development/continuing-education/certified-information-systems-security-professional-cissp/

Virginia Information Technologies Agency

DOA Offering Training

Understanding the Yellow Book

Government Auditing Standards

- Understand key Yellow Book principles and standards of revised 2011 Yellow Book
- Understand the content of key chapters:
  - Chapter 1: ethical principles which underlie all audit work
  - Chapter 3: the general standards that apply to all audits: independence, professional judgment, competence, and quality control and assurance—note: independence will be emphasized since it is the focus of the 2011 changes
  - Chapters 6 and 7: fieldwork and reporting standards for performance audits
- Understand additional changes incorporated in the 2011 revised Yellow Book

Instructor: Carole Buncher (Carole Buncher and Associates)
Date: 03/28/2012
Time: 8:15-4:45
Location: James Monroe Building DOE Conf. Rm. 22nd FL
Cost: $ 160.00 (earn 8 CPE's for this course!)
Register: **https://hrtraining.doa.virginia.gov/Training_Schedule.cfm?New=0925**

ISACA Offering Training

CISA Review Class

Location: EdgeComm, 4913 Fitzhugh Ave, Ste: 201, Richmond, VA 23230
Time: 6 – 9 pm
Dates: May 7, 9, 14, 16, 21, 23
Instructor: Jerry Jarvis, CISA, CRISC, CIA, CFSA
Registration: Online at www.isaca-va.org/

Discount for early registration before April 15. Registration closes May 4.

Course will cover all (5) job practice domains of the CISA body of knowledge.

- ***The process of Auditing Information Systems***
- ***Governance and Management of IT***
- ***Information Systems Acquisition, Development & Implementation***
- ***Information Systems Operations, Maintenance & Support***
- ***Protection of Information Assets***

Sample tests will be administered and discussed.

Virginia Information Technologies Agency

ISACA Offering Training

CISM Review Class

Location: EdgeComm, 4913 Fitzhugh Ave, Ste: 201, Richmond, VA 23230
Time: 6 – 9 pm
Dates: May 8, 10, 15, 1,. 22, 24
Instructor: John Karabaic, CIPP/IT, CISM, CISSP &
Chandra Barnes, CISM,CRISC
Registration: Online at www.isaca-va.org/

Discount for early registration before April 15. Registration closes May 4.

Course will cover all (5) domains of the CISM body of knowledge.

- ***Information Security (IS) Governance***
- ***Information Risk Management***
- ***IS Program Development***
- ***IS Program Management***
- ***Incident Response & Management***

Sample tests will be administered and discussed.

Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - April 4, 2012

Speaker: Laurie Jarrett (VCU) on Grant Writing basics

Wednesday - May 2, 2012

Speaker: Alana Foster with RSA

ISOAG will be held the 1st Wednesday of each month in 2012

IS Orientation Sessions

Tuesday - May 8, 2012 9:00 – 11:30a (CESC)

Email CommonwealthSecurity@VITA.virginia.gov if you are interested in attending.

IS Orientation is now available via webinar!

COV IS Council

Do you know someone who is passionate about and could make a difference in strengthening the information security posture of the Commonwealth?

Nominate them to be a member of IS COUNCIL!

Send your nomination to:
CommonwealthSecurity@VITA.Virginia.Gov

ISOAG-Partnership Update

IT Infrastructure Partnership Team
Bob Baskette

March 7, 2012

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

ADJOURN