PIRT

RIPE53

Security Professionals

CASTLECOPS

Because Security is Everything

Agenda

1. Introduction
2. CastleCops® Brief
3. PIRT's Approach
4. Value

Introduction

- Presenter: Paul Laudanski
  - CastleCops Founder
    - paul@castlecops.com – 609.510.3894 (C)
  - Microsoft MVP Windows-Security
- CastleCops
  - www.castlecops.com
  - wiki.castlecops.com
  - de.castlecops.com

What is Phishing?

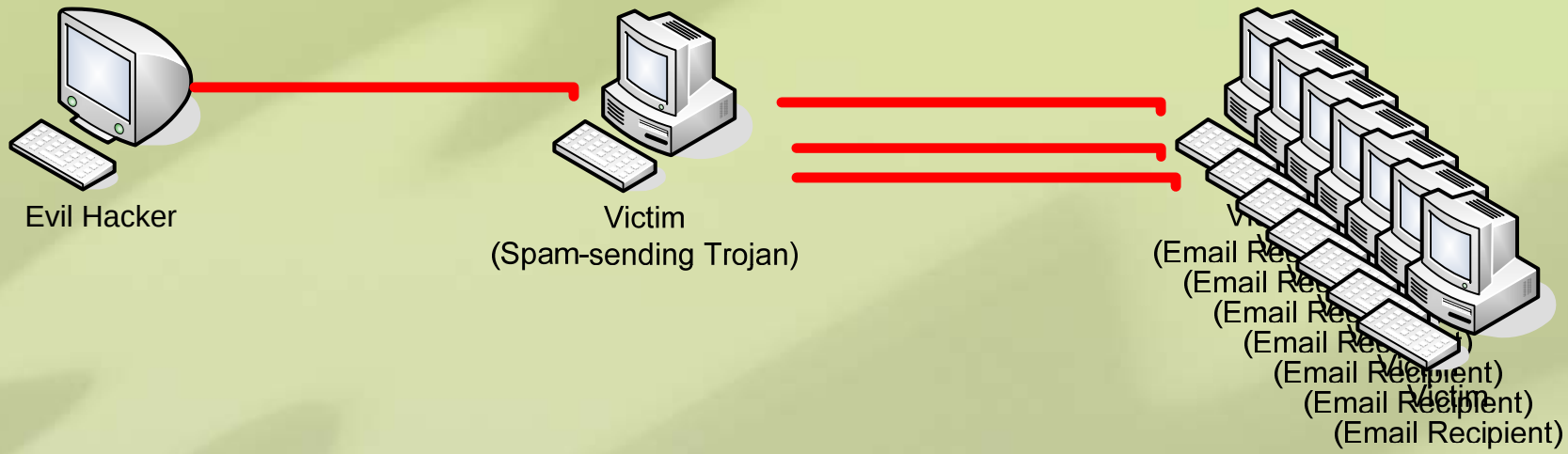
To trick people into providing their personal and financial information by pretending to be from a legitimate company, agency or organization.

-phishinginfo.org

The big question

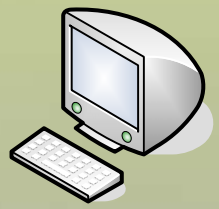
- How many of you have received phishing emails this week?

One Spam-sending Trojan



Each of the infected computers is “listening” on a pre-designated port for commands from the Phisher.

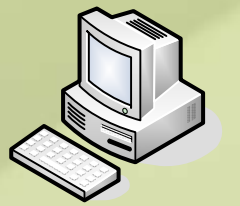
The Phisher then uses a program which automatically distributes email by sending mail THROUGH the computers which are infected.



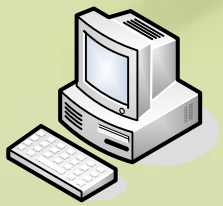
Evil Hacker

Botnet

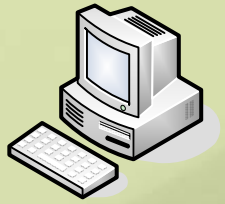
But there's not ONE SpamSender being controlled by the Evil Hacker. There are HUNDREDS. THOUSANDS. TENS of THOUSANDS!



Victim
(Spam-sending Trojan)

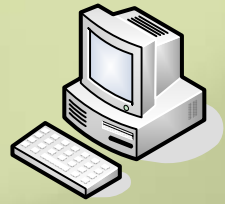


Victim
(Spam-sending Trojan)

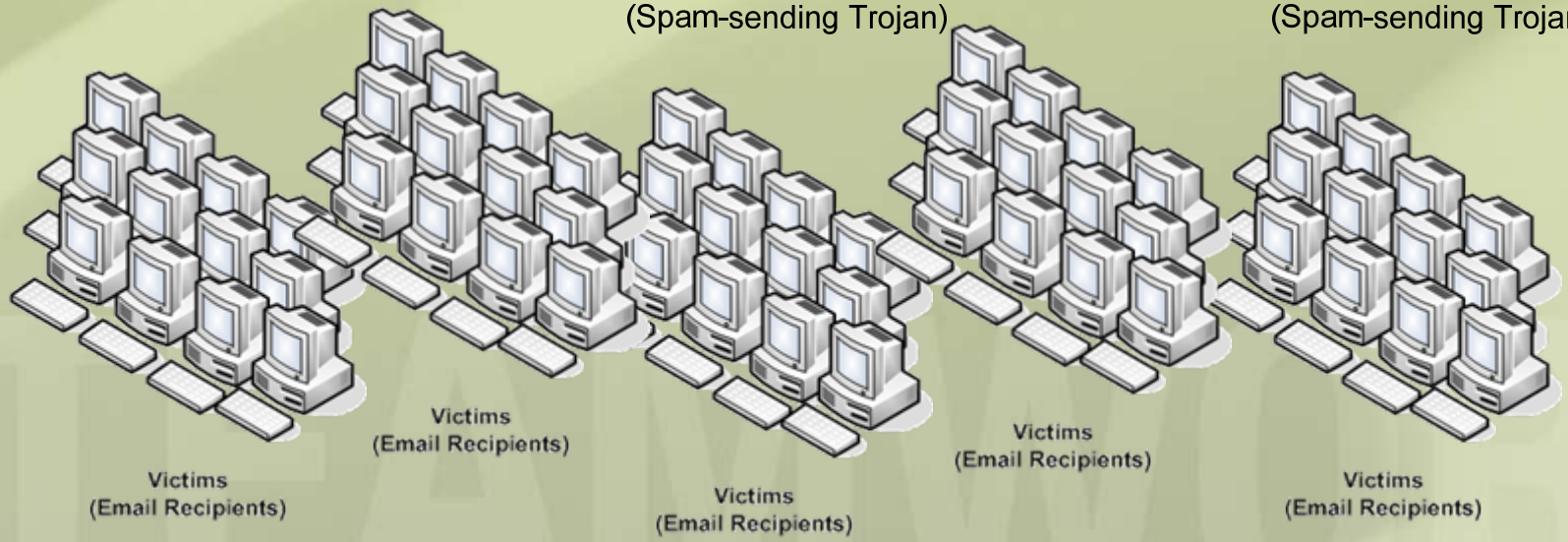


Victim
(Spam-sending Trojan)

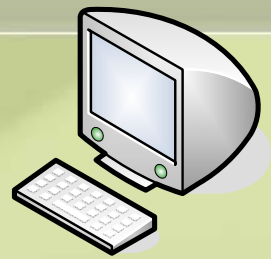
Victim
(Spam-sending Trojan)



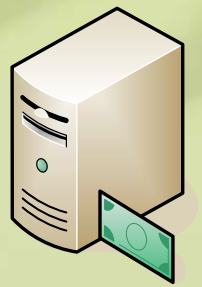
Victim
(Spam-sending Trojan)



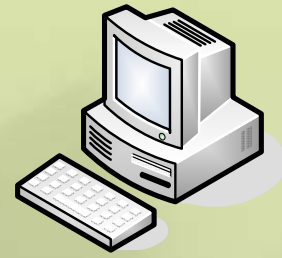
The Phishing Circle



Evil Hacker

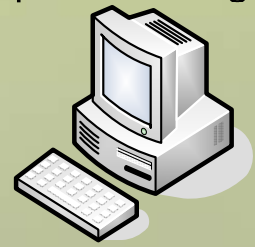


Information Exploit
Bank Mainframe



Victim
(Spam-sending Trojan)

Account Receipt
Email server



Victim
(Email Recipient)

Possible Victim
(Phishing Web Server)

When ISPs are Victims

HostGator says hackers compromised its servers using a previously unknown security hole in cPanel, the control panel software that is widely used by hosting providers. "I can tell you with all accuracy that this is definitely due to a cPanel exploit that provides root access and all cPanel servers are affected," said HostGator system administrator Tim Greer. "This issue affects all versions of cPanel, from what I can tell, from years ago to the current releases, including Stable, Release, Current and Edge."

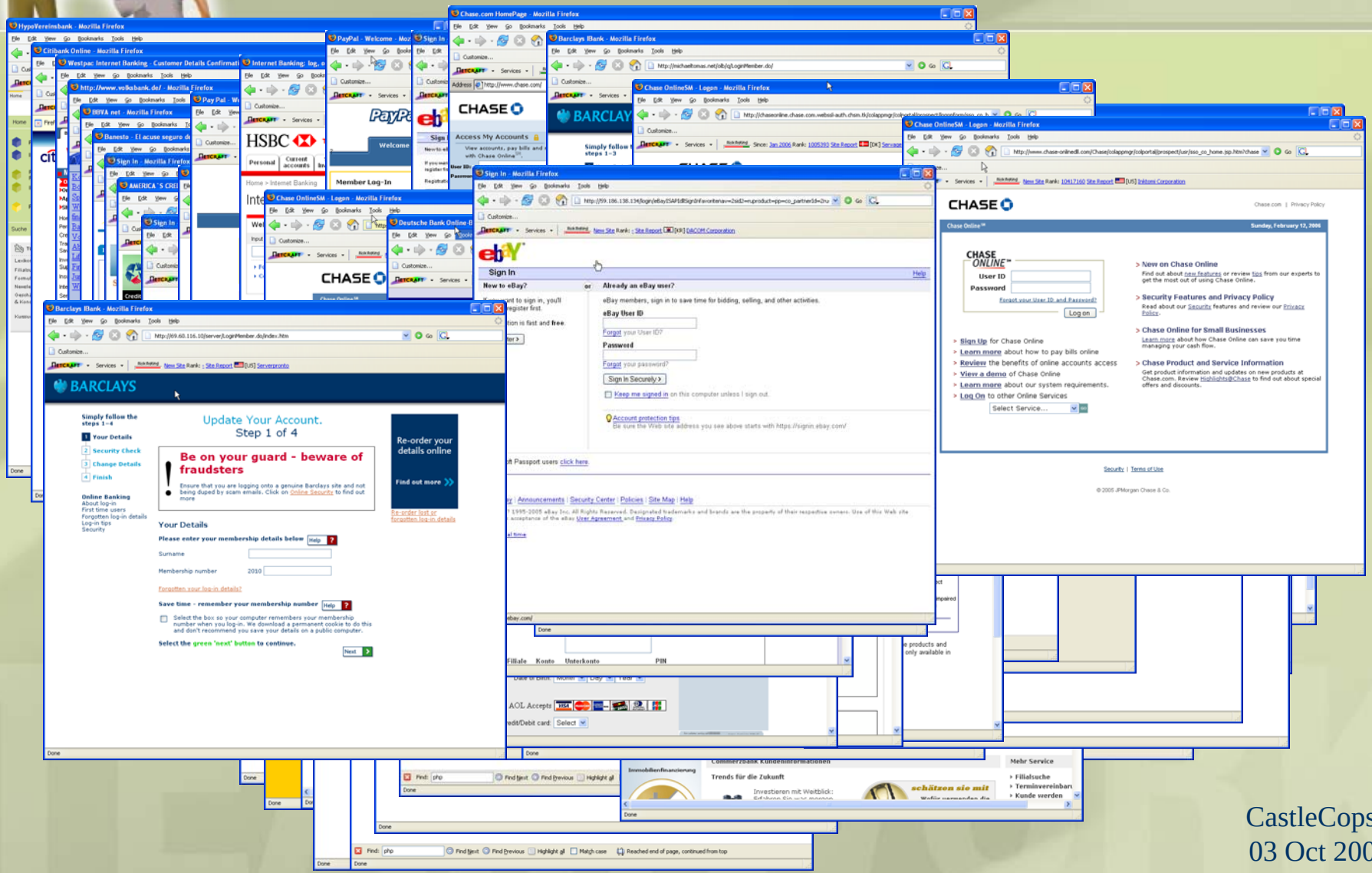
-Source: Netcraft

Victimized ISPs create Victims

- HostGator's compromised servers redirected to sites exploiting unpatched Vector Markup Language (VML*)
- Susceptible Internet Explorer web surfers became infected with – Trojans!
- More bots added to the herd

*http://www.microsoft.com/technet/security/bulletin/ms06-055.mspx

Phishing Examples



CastleCops®
03 Oct 2006

PIRT: What, Why, Who

- What
  - To quickly takedown phish
  - Shut down email escapes
- Why
  - Prevent further financial loss
  - Provide investigative reports to Law Enforcement
- Who
  - Volunteers
  - Relationships

The PIRT Solution

- Why is PIRT different than anyone else working in this space?
  - We believe in SHARING DATA
  - We believe in AVOIDING DUPLICATION
  - We believe in VOLUNTEERING to protect our fellow Netizens

Sharing Data

- PIRT reports are sent, FREE of charge, to any anti-phishing company, tool, or organization that asks for them.
- 50 organizations receive our feed.
- Our reports are public. No other anti-phishing organization lets the public review its status files.
- Most Anti-phishing organizations require either membership, or a subscription to get this information. PIRT believes Phishing can only be defeated by FREE COLLABORATION.

Avoid Duplication

- Entries are checked against our database ensuring duplicates are not re-processed by PIRT.

pirt@castlecops.com

www.castlecops.com/pirt

- By CENTRALIZING and SHARING, we avoid duplication of labor.

Volunteering

- If you are the sort of person that asks the question:

  "How can I help protect our Critical Infrastructures?"

  Or

  "How can I help stop Identity Theft?"

  Then PIRT is the place for you! Why should we pay someone else to protect OUR INTERNET?

PIRT Flow

New Report

- Submission
  - Email
  - WWW
- Pre-Fetch

Confirmation

- Verify
- Investigate
- Report
  - Everyone

Termination

- Follow-up
  - Terminate
  - Acquire Kit
    - Notify

PIRT Handler Checklist

- Get a ticket from the queue
- Is it really a phish?
- If so, what Brand?
- Document the proof.
- Find the relevant parties.
- File the report.
- Wait.
- Confirm termination.
- Escalate if necessary.

Technical

- Extract BGP Origins*
- Extract BGP Possible Peers*
- Obtain ASN to Abuse Email^
- MD5 & SHA-1 Phish Files
- dig, host, WHOIS

*www.cymru.com

^www.mynetwatchman.com

Fried Phish: Queue

Fried Phish(TM)

Phishing Incident Reporting and Termination (PIRT) Squad

A global phishing termination operation launched by CastleCops and Sunbelt Software, the volunteer PIRT Squad is comprised of folks who report phish, investigate phish, and actively work on phish takedown and termination (original concept by Robin Laudanski). PIRT is funded by CastleCops. Become a PIRT Squad terminator by reporting phish today!

[How-To / FAQ]

[My Stuff (214)] [Queue (1812)] [Checked Out (390)] [Confirmed Phish (1036)] [Terminated Phish (6911)] [Fried Phish] [Obfuscate] [Next New Report]

Select Report Range

X	ID	SIZE (B)	BEST GUESS	TITLE	ENTRY	REPORTER	TIMESTAMP	TOPIC
☐	70534	26768	37262		http://phx.corporate-ir.net/phoenix.zhtml?c=110723&	Email|Web	13 Sep, 2006 @ 10:06:59	
☐	70535	9217	15408		http://hwaiistatexz.com	159348	13 Sep, 2006 @ 10:23:10	
☐	70536	9218	15408		http://hwaiistatexz.com/	159348	13 Sep, 2006 @ 10:23:10	
☐	70537	12324	20082		http://202.67.4.50:84/ws/eBayISAPI%3bdllSignIn&co_p	Email|Web	13 Sep, 2006 @ 10:32:20	
☐	70538	0	56		http://1072128589:60006/aol/bill_form.html	Email|Web	13 Sep, 2006 @ 10:36:03	

Fried Phish: Handler

HTTP Response 14 Sep, 2006 09:30:31	HTTP/1.1 302 Object Moved HTTP/1.1 403 Access Forbidden
Initial Fetch Size	416 bytes (fetched size of "Entry" submission)
ID	66426
Title	or Select Known Title Go!
Entry	http://www.nationwide.co.uk/signon?LOB=CONS&screenid=Confirm_Ac _____ ASCII DECODED: http://www.nationwide.co.uk/signon?LOB=CONS&screenid=Confirm_Ac _____ URL DECODED: http://www.nationwide.co.uk/signon?LOB%CONS&screenid%Confirm_Ac

Fried Phish: Handler

HTTP Response 14 Sep, 2006 07:05:18	500 Can't connect to www.bankofscotland.co.uk.systemupgrade.telinand.biz:80 (Bad hostname 'www.bankofscotland.co.uk.systemupgrade.telinand.biz')
Initial Fetch Size	8482 bytes (fetched size of "Entry" submission)
ID	67664
Title	**Bank of Scotland, Fifth Third Bank, Suntrust, VolksBank** or Select Known Title Go!
Entry	http://www.bankofscotland.co.uk.systemupgrade.telinand.biz/customers.ibc

Handler Tools

Handler Tools

Search Duplicates by domain or phish URL

Change Report Status

confirmed phish

Process All Input

dig/host/WHOIS

Use this field for running WHOIS and dig commands on just a domain name or IP address. Examples: "example.com", "www.example.com", "192.168.1.1".

fetch page

Use this field to fetch a web page. Example: "http://example.com/index.htm".

ASN/BGP Prefix Tools (Step 1: origin + peer)

Enter IP Address (example 192.168.1.1).

ASN/BGP Prefix Tools (Step 2: ASN)

Enter ASN Number (example: 14779).

Handler Tools

Add Handler Note (This is public)
Enter any notations here. On thread alert, entries will be placed into topic.

Add LAW ENFORCEMENT Sensitive Data (This is private)
Entries here will only be displayed in fp=handler.

Add "Destination Emails"

Email address (one at a time):

Finalize your report first, and then send out the email alert.

Handler Notes

Handler Note: 05 Aug, 2006 12:40:15	Fetching page source: Suceeded. The phishing site was active at the time of investigation. Phish URL #3: (Wells Fargo) http://www.eclipsedguild.net/dkp/templates/cache/online.wellsfargo.com/ Browser access directs to an Wells Fargo phishing site. Fetching page source: Suceeded. The phishing site was active at the time of investigation. Phish URL #4: (Banl of America) http://www.eclipsedguild.net/dkp/templates/cache/e-online-banking/ Browser access directs to an Bank of America phishing site. Fetching page source: Suceeded. The phishing site was active at the time of investigation. Phish URL #5: (AOL) http://www.eclipsedguild.net/dkp/templates/cache/AOL%20new/ URL #5 Redirects to URL #6: http://www.eclipsedguild.net/dkp/templates/cache/AOL%20new/bill_form.html Browser access directs to an AOL phishing site. Fetching page source: Suceeded. The phishing site was active at the time of investigation.
Handler Note: 05 Aug, 2006 13:01:36	daveai: www.eclipsedguild.net has address 67.18.11.31
Handler Note: 05 Aug, 2006 13:28:29	daveai: NOTE: Kits discoverd for all of the above

Fried Phish: Fetch

Report for [ ] **at 05 Sep, 2006 @ 23:10:49**

View Report Go!

whois | dig | host | fetch | asn

fetched page

[rm] http://www.bankofscotland.co.uk.systemupgrade.telinar at 05 Sep, 2006 @ 23:10:56
MD5 Fingerprint: 994bf4c034d9a4bc8b07a4f25be87633
SHA1 Fingerprint: afd3f2e5e13369668d2fcaef53bba8f9262f4147

```
HTTP/1.1 301 Moved Permanently
Date: Wed, 06 Sep 2006 03:14:27 GMT
Server: Apache/1.3.36 (Unix) mod_ssl/2.8.27 OpenSSL/0.9.7f PHP/4.4.2 mod_perl/1.29 FrontPage/5.0.2.2510
Location: http://www.bankofscotland.co.uk.systemupgrade.telinand.biz/customers.ibc/
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1

HTTP/1.1 200 OK
Date: Wed, 06 Sep 2006 03:14:29 GMT
Server: Apache/1.3.36 (Unix) mod_ssl/2.8.27 OpenSSL/0.9.7f PHP/4.4.2 mod_perl/1.29 FrontPage/5.0.2.2510
Last-Modified: Wed, 23 Aug 2006 15:15:41 GMT
ETag: "288102-2122-44ec711d"
Accept-Ranges: bytes
Content-Length: 8482
Content-Type: text/html
```

Frequent Single Phish

- Wachovia
- ~130 Distinct PIRT Reports
  - aka distinct locations

Real Wachovia - Today

WACHOVIA

Locations

ONLINE SERVICES LOGIN

Enter the appropriate login information below, and select your service.

Retirement Plan Participants: Login

User ID

Remember my User ID Learn More

Password

Case Sensitive

Service Selection: Choose a service...

Login

Customer Service

User ID & Password Help
Forgot your User ID?
Reset your Password

Customer Access Number: Login

Easier Access.

Logging in to Online Services is now easier on wachovia.com.

Take a look

Customer Agreement | Privacy | Security | Legal

© 2006 Wachovia Corporation. All rights reserved.

The Wachovia Phish

WACHOVIA

ONLINE SERVICES LOGIN

Enter the appropriate login information below, and select your service.

Retirement Plan Participants: Login

User ID

Remember my User ID Learn More

Password

Case Sensitive

Service Selection Choose a service...

Login

Customer Service

User ID & Password Help
Forgot your User ID?
Reset your Password

Customer Access Number: Login

Easier Access.

Logging in to Online Services is now easier on wachovia.com.

Take a look

Customer Agreement Privacy Security Legal

© 2006 Wachovia Corporation. All rights reserved.

How it renders today

Wachovia Logo

Online Services Login

Enter the appropriate login information below, and select your service.

- Retirement Plan Participants: Login

User ID

Remember my User ID Learn More

Password

Case Sensitive

Service Selection Choose a service...

Login

Wachovia Attack Vector

Excerpt:

accountwachovia-update.com
asm78.com
bierweek.zhtc.nl
bipolarsupport.org
bnbhomeslanka.com
boa100.com
boa2.org

Domains Used

Fried Phish: ASNs

Corresponding BGP Origin ASN

62.75.244.88 at 29 May, 2006 @ 11:56:06

AS | BGP Prefix | CC | Registry | Allocated

"8972 | 62.75.128.0/17 | DE | ripencc | 2001-07-27"

Possible BGP peer ASNs one AS hop away from BGP Origin ASN

62.75.244.88 at 29 May, 2006 @ 11:56:06

AS Peers | BGP Prefix | CC | Registry | Allocated

"13237 25074 34088 | 62.75.128.0/17 | DE | ripencc | 2001-07-27"

Wachovia Attack - ASNs (part)

| "15456 | DE | ripencc | 2000-07-04 | DENOC-15456 DENOC Network“
| "16245 | DK | ripencc | 2001-02-07 | NGDC NetGroup DataCenter A/S - ngdc.net“
| "1902 | EU | ripencc | 1993-09-01 | CONTACTEL CTT Backbone“
| "20746 | IT | ripencc | 2001-05-16 | ASN-IDC IT Telecom S.p.A."
| "29402 | FR | ripencc | 2003-08-29 | CTN1 CTN1 European Network“
| "34788 | DE | ripencc | 2005-04-05 | NMM-AS Neue Medien Muennich GmbH“
| "39561 | RU | ripencc | 2006-03-20 | AGAVA Agava JSC AS number“
| "5413 | GB | ripencc | 1995-09-12 | AS5413 PIPEX Communications“
| "8732 | RU | ripencc | 1998-03-26 | COMCOR-AS AS for Moscow Telecommunication Corporation (COMCOR)"

Top 5 Phish Originating ASNs

- 270
  - 14779 & 14780 | US | arin | 2000-02-07 | INKTOMI-LAWSON - Inktomi Corporation
- 135
  - 4134 | CN | apnic | 2002-08-01 | CHINANET-BACKBONE No.31,Jin-rong Street
- 112
  - 4766 | KR | apnic | 1996-04-22 | KIXS-AS-KR Korea Telecom
- 93
  - 3216 | RU | ripencc | 1994-04-15 | SOVAM-AS Golden Telecom, Moscow, Russia
- 71
  - 7132 | US | arin | 1996-09-13 | SBIS-AS - SBC Internet Services

Top 5 RIPE Originating ASNs

- 93
  - 3216 | RU | ripencc | 1994-04-15 | SOVAM-AS Golden Telecom, Moscow, Russia
- 64
  - 3269 | EU | ripencc | 1994-11-14 | ASN-IBSNAZ TELECOM ITALIA
- 57
  - 8560 | DE | ripencc | 1997-11-26 | SCHLUND-AS Schlund _ Partner AG
- 49
  - 12322 | FR | ripencc | 1999-03-11 | PROXAD AS for Proxad ISP
- 34
  - 5413 | GB | ripencc | 1995-09-12 | AS5413 PIPEX Communications

Phish Originating Assignments

- ARIN: 2,501
- RIPENCC: 1,621
- APNIC: 1,360
- LACNIC: 252
- AfriNIC: 18

Email Alerts

[PIRT#55620] AOL, BOA, PayPal, Wachovia, Wells Fargo P...

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

This message is High Priority.

From: CastleCops PIRT Squad

Date: Saturday, August 05, 2006 7:08 PM

To: abuse@theplanet.com; spoof@paypal.com; abuse@wachovia.com; reportphish@wellsfargo.com; abuse@bankofamerica.com; abuse@aol.net; security@google.com; cory@google.com; phishing@cc.yahoo-inc.com

Cc: daveai; Paul; Gary; reportphishing@antiphishing.org; phishing-report@us-cert.gov; rwilliams@ic3.gov

Subject: [PIRT#55620] AOL, BOA, PayPal, Wachovia, Wells Fargo Phish on your network (AS21844)

Email Alerts

CastleCops has discovered a AOL, BOA, PayPal, Wachovia, Wells Fargo phish operating at the link(s) below. We are sending this email to request your assistance in removing this fraudulent webpage(s). In addition, CastleCops works on a daily basis with law enforcement and brand owners to try to identify phishers. You may be in possession of critical clues that would help that process.

- http://www.eclipsedguild.net/dkp/templates/cache/paypal-online/customers/Secured/Service/mysql/ssl/connection/ /login/
- http://www.eclipsedguild.net/dkp/templates/cache/wachoviabank/
- http://www.eclipsedguild.net/dkp/templates/cache/online.wellsfargo.com/
- http://www.eclipsedguild.net/dkp/templates/cache/e-online-banking/

Email Alerts

Reference this ticket for a detailed analysis including phish HTML source code:

http://castlecops.com/modules.php?name=Fried_Phish&fp=phish&id=55620&in=1

If it is within your power, we are requesting that you identify any files placed on the server by the phisher, and share a copy with an appropriate law enforcement agency. If you do not have a relationship with a law enforcement agency, CastleCops PIRT Team would be happy to forward these files to our chosen law enforcement partner, the FBI. If you would prefer to send these files directly, they may be sent to the National Cyber Forensics Training Alliance, care of FBI Special Agent Mike Eubanks at phish@ncfta.net. Please reference [PIRT#55620].

Web server log files may reveal the IP address used by this hacker. Even if it is not his "true" IP address, it may help us to link this phisher to other crimes. Phishing "kit" files may reveal the email address used by this hacker to harvest stolen data. Again, this may help us to link this phisher to other crimes, and to provide assistance to victim brands or individuals.

Thank you for your cooperation!

CastleCops PIRT Squad
(Phishing Incident Reporting & Termination)

Email Alerts

The following organizations have all been notified:

Alice's Registry, Anti-Phishing Working Group, Australian Computer Emergency Response Team (AusCERT), Authentium, Blue Coat, Brand Dimensions, Compete, Co-Logic, ContentKeeper Technologies, CyberDefender, EveryDNS, Federal Bureau of Investigation (FBI), Firetrust, For Critical Software Ltd, Fortinet, Forum of Incident Response and Security Teams (FIRST), FraudWatch International, Infotex, Internet Crime Complaint Center (IC3), Internet Identity, Intellectual Property Services, Korea Information Security Agency (KISA), Korea Internet Security Center (KrCERT/CC), Laboratoire d'EXpertise en Securite Informatique (LEXSI), Malware Block List, National Cyber-Forensics and Training Alliance (NCFTA), Netcraft, NYSERNet, Okie Island Trading Company, OpenDNS, Rede Nacional de Ensino e Pesquisa (RNP), SonicWALL, Sunbelt-Software, Support Intelligence, SURBL, Symantec, Team Cymru, Thomas Jefferson National Accelerator Facility (JLab), TrustDefender, United Online, United States Computer Emergency Readiness Team (DHS US-CERT), Websense, Webwasher, XBlock

Public response thread: http://castlecops.com/t163754-.html
Reference: CastleCops PIRT Squad Report #55620
PIRT FAQ: http://wiki.castlecops.com/PIRT
Submit Phish: pirt@castlecops.com
Live XML Feed: http://www.castlecops.com/article6619.html

Copyright CastleCops 2006, All Rights Reserved. http://www.castlecops.com

XML Feed

- Free upon request
- Formatted by PIRT report ID
  - Lists all originating ASNs
  - Displays all phish URLs
  - References a public PIRT report
  - Displays ‘up’, ‘down’, or ‘n/a’ status
  - Reveals originating IP addresses
  - Shows ‘confirmed/terminated’ switch
- Private [CC PIRT] ListServ
- We ask for public recognition

Top 20 Targets - Jun 2006

PayPal	279	CUNA	13
eBay	142	Barclays	10
BOA	50	1st Natl Bank Alaska	8
Nationwide	31	IRS	8
Wachovia	30	Citi	8
e-gold	21	Sparkasse	7
Wells Fargo	18	Volksbank	7
Banca Intesa	18	Halifax	6
HSBC	16	Alaska FCU	6
Chase	15	National Credit Union	6

Top 20 Targets - Jul 2006

PayPal	202	HSBC	12
eBay	188	Lloyds TSB	9
BOA	34	Banamex	8
Wachovia	33	SBB&T	7
Chase	22	Fith Third Bank	7
e-gold	21	Netbank	6
Wells Fargo	17	Citizens NB of Tex	6
Nationwide	15	AOL	6
Volksbank	15	Halifax	6
BancaIntesa	12	NAFCU	6

Top 20 Targets - Aug 2006

PayPal	147	Halifax	10
eBay	118	Wells Fargo	8
BOA	37	CitiBank	8
Fifth Third	25	NCUA	8
Wachovia	24	NAFCU	7
Nationwide	22	Netbank	6
Bank Scotland	15	MSGCU	6
Volksbank	14	Chase	6
e-gold	13	Texas Dow ECU	5
Barclays	10	Nat'l Australia Bank	5

Preliminary - Sep 2006

- PayPal 168
- eBay 112
- Wachovia 32
- Nationwide 16
- BOA 13

Value

- Freely share phish information
- Source codes saved for law enforcement
- Kits obtained
- All brands are processed
- Botnets revealed
- Obfuscated code translated
- Phish takedown and consumer protection

Value

- PIRT is active in the trenches searching for phish
- Keep the LE up-to-date on new trends as they happen
  - As opposed to waiting for financial losses, calls from victims
- Our data helps build better criminal profiles
- Drop emails reported
  - Immediately frozen (further financial loss stopped)

Value

- Helped identify crime groups and individuals
- Helps identify victim companies and which relationships need to be developed
- Certain reports led to LE opening up cases

Future

- Output
  - Map/trend susceptible platforms (OS & application)
  - Ratio of hacked sites to fraud domains
  - Trend ‘phishiest’ locales
  - Enrichment of XML Feed
- Interface
  - LE Search
  - API Toolkit

How can you help?

- Establish relationships
  - EuroJust, etc...
  - European, Asian, Middle Eastern
    - LEAs
    - CERTs
    - ISPs
    - Registrars
- Send PIRT your phish
- Send Volunteers to handle reports

Relationships

8e6 Technologies, Alice's Registry, Anti-Phishing Working Group, Australian Computer Emergency Response Team (AusCERT), Authentium, Blue Coat, Brand Dimensions, CERT / Software Engineering Institute / Carnegie Mellon University (CERT/CC), Compete, Co-Logic, ContentKeeper Technologies, CyberDefender, Cyveillance, EveryDNS, Federal Bureau of Investigation (FBI), Firetrust, For Critical Software Ltd, Fortinet, Forum of Incident Response and Security Teams (FIRST), FraudWatch International, IronPort, Infotex, Internet Crime Complaint Center (IC3), Internet Identity, Intellectual Property Services, Korea Information Security Agency (KISA), Korea Internet Security Center (KrCERT/CC), Laboratoire d'EXpertise en Securite Informatique (LEXSI), Malware Block List, National Cyber- Forensics and Training Alliance (NCFTA), Netcraft, NYSERNet, Okie Island Trading Company, OpenDNS, Rede Nacional de Ensino e Pesquisa (RNP), SonicWALL, Sunbelt-Software, Support Intelligence, SURBL, Symantec, Team Cymru, Thomas Jefferson National Accelerator Facility (JLab), TrustDefender, United Online, United States Computer Emergency Readiness Team (DHS US-CERT), Websense, Webwasher, XBlock

Summary

- PIRT is a policy based organization
  - We work with agencies to terminate phish legally and quickly
- PIRT is not in the business of hacking
- PIRT is a vetted volunteer agency
- PIRT shares its data
- PIRT reports all phish on a server without bias

paul@castlecops.com