

---

# Vulnerability Summary

## January 2005

Paul Asadoorian  
Andrew Veitch  
Brown University



# Vulnerabilities

---

- Web Browser Security Update
- BackupExec Buffer Overflow
- WINS Buffer Overflow
- Phishing Update
- Vulnerabilities of Interest

# Web Browser Security Update

---

- Latest in Internet Explorer vulnerabilities
- Two largest threats are:
  - MS05-1: HTML Helper ActiveX
  - MS05-2: ANI Cursor File

# Web Browser Security Update

---

- HTML Helper ActiveX
  - Masks as “Helper Link”
  - Uses Java call to exec local code
  - All Versions of Windows effected 98-XP SP2
- Install available patch **KB890175**

# Web Browser Security Update

---

- Buffer Overflow in Malformed ANI
  - Exploits IE and Explorer's Handling of ANI
  - Effects {IE, Office, Outlook, Explorer}
  - Win XP SP2 is not effected
- Proof of Concept Available:
  - Example

# Web Browser Security Update

---

- Defense:
  - Use alternate browser
  - Apply patches
  - Turn off drag and drop functionality

# BackupExec Buffer Overflow

---

- Older Versions of BackupExec vulnerable
  - 8.6 – 9.x effected
  - Exploits handling of incoming requests
  - Effects Server side
  - Proof of Concept available

# BackupExec Buffer Overflow

---

- Vendor Recommends
  - Patch or upgrade newest version 10.0
  - Block TCP port 6101
    - We will looking into blocking this at the border

# WINS Buffer Overflow

---

- Affected products include Windows NT/2000/2003/XP
- WINS – Translates NetBIOS names to IP addresses
- Remote exploitation possible and common

# WINS Buffer Overflow

---

- Defense:
  - Patch your systems
  - Block TCP port 42
  - Disable the WINS service
- We now block TCP port 42 from the Internet

# Phishing Update

---

*“Phishing is a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, data suggests that phishers are able to convince recipients to respond to them. As a result of these scams, an increasing number of consumers are suffering credit card fraud, identity theft, and financial loss.”*

<http://www.antiphishing.org>

# Phishing Update

---

- Phishing Scams are on the rise
  - Average monthly growth rate in phishing sites July through December 2004: **24%**
- Most phishing attacks focus on financial information (banks, credit cards, paypal)
- Phishing takes advantage of browser vulnerabilities

# Phishing Update - Example



wamu.com A Washington Mutual, Inc. Web site

← Links to legitimate site

## Security Center Advisory!

Washington Mutual is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, Washington Mutual employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the Washington Mutual system for unusual activity.

We recently have determined that different computers have logged onto your Washington Mutual Online Banking account, and multiple password failures were present before the logons. We now need you to re-confirm your account information to us. If this is not completed by **Jan 31, 2005**, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner.

In order to confirm your Online Bank records, we may require some specific information from you.

[Click here to verify your account](#) ← Links to 128.123.167.157

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

We apologize for any inconvenience.

If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

Thank you for using Washington Mutual!

# Phishing Update - Example

---

- 128.123.167.157 belongs to New Mexico University
- The banner link goes to the legitimate Washington Mutual web site
- The web site at 128.123.167.157 looks just like Washington Mutual's and asks user for credit card and/or bank information

# Phishing Update - Example

---

- Likely scenario:
  1. Attacker breaks into 128.123.167.157
  2. Attacker uploads web site and malicious code
  3. SPAM gets sent to millions of people telling them to update their account
  4. A few hundred people fall for it and give up their personal information
  5. Attacker goes on shopping spree for new skateboard, roller blades, the works 😊

# Phishing Update

---

- Defense
  - Filter SPAM and don't open it
  - Always go to the web site directly, never click on links inside email
  - Patch your OS regularly, and keep browser up to date
  - Use an alternate web browser
  - View email in plain text, not HTML
  - Be smart, don't be afraid to call your bank or credit card company
    - They will not ask for your card number, they have it already!

# Vulnerabilities of Interest

---

- Bind Versions 8 & 9 vulnerable to DoS
  - <http://www.isc.org/sw/bind/bind-security.php>
- PHP/ASP/CGI web applications security flaws (phpBB)
  - <http://www.security.nnov.ru/search/news.asp?binid=4344>
- Multiple implementations of LDAP Directory Server vulnerable to buffer overflow
  - <http://www.kb.cert.org/vuls/id/258905>

**/\* The End \*/**

---

Questions? Comments? Flame Mail? Donations?

[Paul\\_Asadoorian@brown.edu](mailto:Paul_Asadoorian@brown.edu)

This presentation:

<http://www.brown.edu/Research/SysAdmins/vuln-jan-2005.pdf>

## **Paul's Essential Security Links**

<http://packetstormsecurity.nl/>

<http://www.incidents.org>

<http://www.security.nnov.ru/>

<http://www.astalavista.com/>

<http://www.cert.org>

<http://www.l0t3k.org/>

<http://www.whitehats.com>

<http://www.securiteam.com/>

<http://rr.sans.org>

<http://www.k-otik.com>