

# Cyber Security at LSA

## (& Software License Compliance)

Presented to:

All LSA Department Faculty Meetings

By: Christopher Brenner

January 10, 2011



# The Problem – Data Breaches/Identity Theft

- UM IT Security Services Office tells us that the campus network receives:
  - About 30 network ‘attacks’ per hour, in truth, we are scanned and attacked 24/7/365
- Web/DB servers with Sensitive data are subject to these attacks
- Laptop Computers, USB drives and smart phones are periodically lost or stolen
- Internal Attacks & Crimes Involving IT equipment
- Identity Theft: largest growing area in organized crime
  - Occurs every 79 seconds ([idtheft.about.com](http://idtheft.about.com))



# Internal Attacks

## ID thief draws probation, restitution (Archived From the Ann Arbor News)

By **anash** January 25, 2008, 7:12PM

An Ann Arbor man who defrauded nearly 200 people out of thousands of dollars by stealing their identities was sentenced to probation, court records show.

**Matthew Kent Li**, 38, was ordered to serve four years of probation and pay more than \$221,000 in restitution during his sentencing before Washtenaw County Circuit Judge Archie Brown.

Last month, Li, a former graduate student and research assistant at the University of Michigan, pleaded guilty to 13 counts of identity theft and additional counts of using a computer to commit a crime and illegally acquiring identification information. Police said he stole the Social Security numbers of at least 169 people from across the country by using the Internet. He used that information then to establish credit card accounts.









# Stolen Research?

- New York Times - September 2005:
- Michael Brown (Caltech) vs. Jose-Luis Ortiz (Institute of Astrophysics of Andalusia, Spain)
- Ortiz published discovery of new planet before Brown
- Only a day before the discovery was reported, computers traced to Dr. Ortiz and his student visited a **Web site** containing data on where and when the Caltech group's telescope was pointed at new planet
- Harvard-Smithsonian Center for Astrophysics, director "I request that Ortiz et al. be stripped of official discovery status and that the I.A.U. issue a statement condemning their actions."
- Brown is now credited with discovery of 'dwarf planet Eris'
- [http://www.nytimes.com/2005/09/13/science/space/13plan.html?\\_r=1](http://www.nytimes.com/2005/09/13/science/space/13plan.html?_r=1)





## Compromised Systems (leading to Data Breaches/possible IT Theft)

-  UNIVERSITY of VIRGINIA June 2007 - 6000 SSNs
-  Ohio State University Dec 2010 – 750,000 SSNs
-  UNIVERSITY OF MICHIGAN School of Ed – July 2007 – 5500 SSNs
-  Eastern Michigan University – September 2010 – no SSNs but unknown # of Passwords/PINs compromised (direct deposit)



# LSA Specific Incidents

- Feb 2009 - machine umopt1.grid.umich.edu SSHD compromise. Confirm w/JH – related to CITI compromise?
- January 2010 – USB keylogger found in LSA classroom attached to presentation Computer – DPS involved and forensics done on computer (related to hospital incident?)
- June & July, 2010 - 2 Stolen laptops – both had student grades, one has Human Subject Research Data (thankfully, anonymized) – one recovered leading to description of thief
- Fall 2010 - Compromised desktop with HSR data
- In FY 2009, there were 328 IT Security Incidents reported in LSA – 2 Serious
- In FY 2008, there were 353 IT Security Incidents reported in LSA – 3 were Serious



# UA's Audit of Research Computing in LSA

- Training and Guidance <<<<<
- Security Policy <<<<<<<<<<<<<
- Data Classification
- Data Storage
- Backups
- Disaster Recovery Plan
- Antivirus
- Physical Security



# Possible Consequences

- Damage to your Department's and/or the College's Image & Reputation
- Loss of Alumni donations to your Department or Research funding
- Lawsuits filed against the Department/University
- Potential for Identity Theft and fraud crimes (will attackers sell this information to organized crime?)
- Informing victims is now required (MI ESB #309 Law 7/07) – fines for non-compliance can reach \$750K
- Media Notification & Negative Public Relations
- Your Research is posted on a Foreign Site before you have published – Institutional Review Board (IRB)
- Costs of Forensics Investigation and Service Disruption/Restoration



# LSA.Security Resources

- Report IT Security Incidents to this email group:

- [lsa.security@umich.edu](mailto:lsa.security@umich.edu)

As per SPG 601.25

- Find IT Security Documentation here:

- [www.lsa.umich.edu/lsa-security](http://www.lsa.umich.edu/lsa-security)



# Reporting Cyber Security Incidents

- If you aren't sure it's an Incident, just send it! (as email)
- We need: **Machine name, IP Address, DNS name of the computer, what alerted you to this Incident, WHEN did the incident happen – date/time. WHERE – building and room#.**
- Include your local IT Staff – they are knowledgeable.
- What constitutes a serious incident? Any Sensitive info on a compromised system.
- Phishes are OK to report (volume)



# Software License Compliance

- 2001 – Associate Dean and LSA IT Manager received formal letter from the Business Software Alliance (BSA). LSA was very nearly audited (fines could have been expensive).
- Response was to begin forming a Software Licensing Team and deploying supporting technologies to better insure license compliance.
- K2 Keyserver (software metering system) setup – clients installed on LSA computers.
- Other non-LSA units wanted to join (UmichITAM consortium begins)
- Software Information Industry Association (SIIA) – like the BSA.



# LSA-Licenses

- Report Software Licensing purchases here:
- Ask Software Licensing questions here:
  - [Lsa-license@umich.edu](mailto:Lsa-license@umich.edu)
- Find Software Licensing info here:
- <http://www.lsa.umich.edu/lisait/lisa-sec-itam/license>



# Cyber Security Issues & Questions

- Google – email/collaboration applications
- NSF – Data Management Plans (1/18/11)
- Recommended Encryption level: AES-256
- Mobile Device Security (SMART phones, iPads, etc)
- DMCA: Fair Use Policy (25% of publication) – how does this apply to digital media? UM Library's Fair Use Evaluator:  
<http://librarycopyright.net/fairuse/> Bobby Glushko!
- using e-mail – when is it secure, forwarding to gmail.
- Online grading (offered thru MAIS?) – use it!
- Ctools – its been audited, it's good.
- Social networks – DL# and fullname/DoB
- FERPA and storing Grades on your computer (old UMID)
- Security measures & energy-saving initiatives at LSA?
- Wolverine Access – m-token requirement.



# Cyber Security 101

- Use Password protected screen savers (public space vs. locked Office)
- Strong Passwords – more than 9 characters, mix of UPPER/lowercase, numbers, non-alphanumerics
- Do Backups!
- Keep computers up-to-date
  - Patches, Anti-Virus, and Anti-Spyware
- Turn on Firewalls (keep them on)
- Be careful of ‘Peer-to-peer’ applications like IM, Skype Suite, Kazaa, bit-torrent applications
- Utilize Data Encryption solutions (Bitlocker, Filevault, encrypted disk image)



# Scareware – hit the power button

## Spyware alert!

### Vulnerabilities found

Your computer is infected by spyware - 25 serious threats are found while scanning your files and registry. It is strongly recommended to entirely clean your computer in order to protect the system against future intrusions.

[Why you need to be protected against spyware?](#)



Upgrade to full version of VirusResponse Lab 2009 security kit to clean your computer and prevent new security and privacy attacks. You will have daily updates and online protection against Internet attacks.

Activate VirusResponse Lab 2009

Stay unprotected

**WARNING!!!** Quick System Scan Results

 **XP antivirus Online Scanner detected dangerous spyware on your system!**

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

Name	Type	Risk level
 <b>Spyware.IEMonster.b</b>	<b>Spyware</b>	<b>CRITICAL</b>
 <b>Zlob.PornAdvertiser.Xplisit</b>	<b>Spyware</b>	<b>High</b>
 <b>Trojan.InfoStealer.Banker.s</b>	<b>Trojan</b>	<b>Medium</b>

[Remove All](#) [Ignore](#)

Protection Center (Unregistered version)

**Protection Center**

Security Status  
manage security modules

**System Scan**  
scan & fix your computer

Scan type: ☒ Quick ☐ Deep ☐ Memory Scan

[Start](#) [Stop](#) [Pause](#)

#	Vendor	Type	Location	Threat Level
1	Trojan-Cookie.Win32...	Makware	C:\Documents and Settings\Hoi_K...	Medium
2	GayCodic.JackAlert	Makware	C:\WINDOWS\System32\winatm.dll	Medium
3	webSearch.Win32	Makware	C:\WINDOWS\System32\Drivers\...	Medium
4	PORN.perversion.R30	Makware	C:\WINDOWS\System32\Drivers\...	Medium
5	Virus.Win32.Gpco...	Viruses	C:\WINDOWS\System32\Wbe...	High
6	Email-Worm.Win...	Network ...	C:\WINDOWS\System32\Wbe...	High
7	Net-Worm.Win32...	Network ...	C:\WINDOWS\Fonts\85855.fon	High
8	Net-Worm.Win32...	Network ...	C:\WINDOWS\Fonts\small.fon	High
9	Trojan-Downloader...	Trojan Prog...	C:\WINDOWS\Help\camera.hp	Medium

Scan complete.  
Objects scanned: 30329  
Threats detected: 19  
Removed: 0

[Remove Threats](#)

**Upgrade to full version now!**  
Easy one-click registration

**Your Computer is not protected**  
[click here to fix security problems](#)

Build 189-CBD29028

Windows Internet Explorer

**Warning!**

W32.Myzor.FK@yf is a virus that infects files with .exe extensions. It attempts to steal passwords and private information from the infected computer.

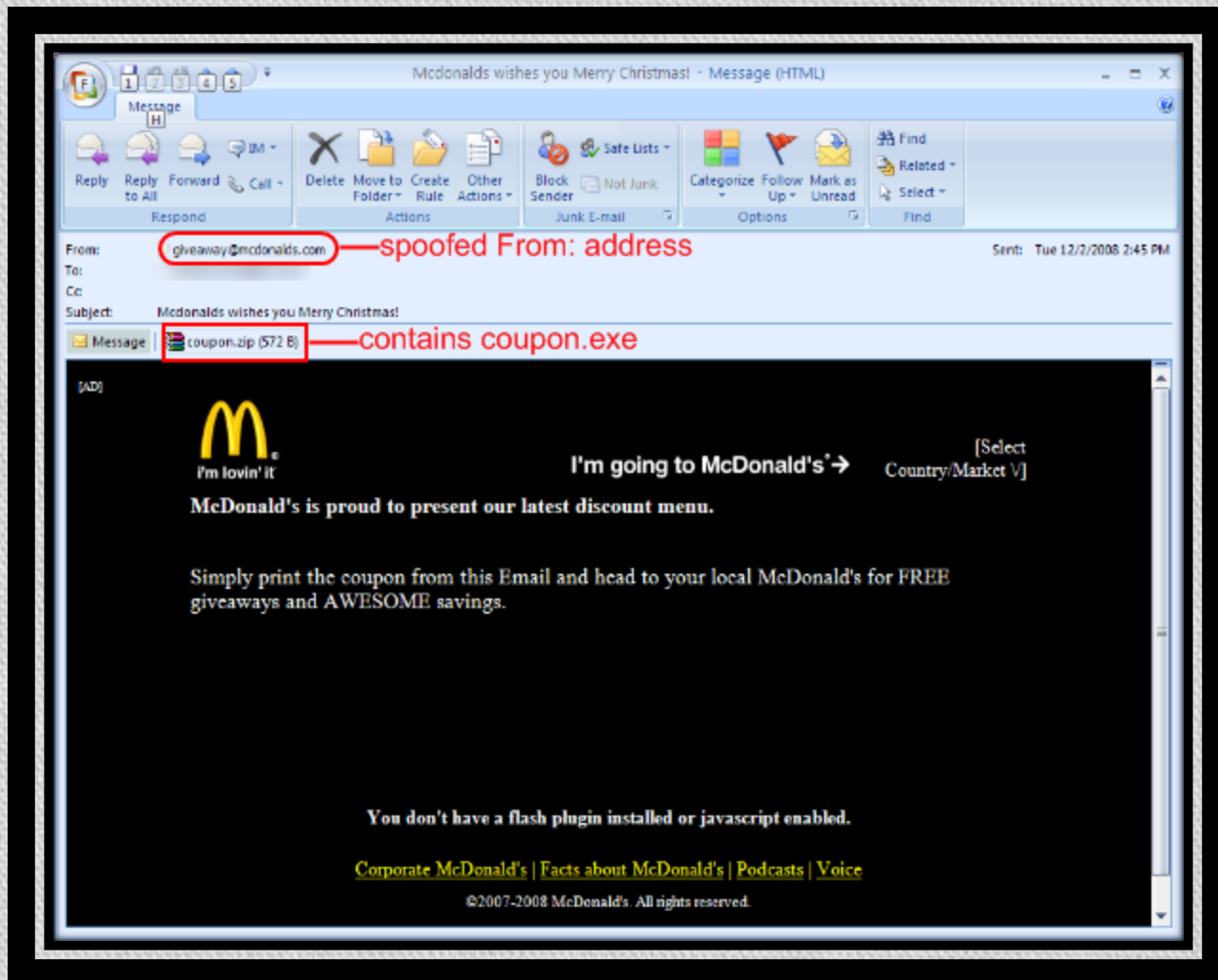
Type: Virus  
Infection Length: 138,293 bytes  
Systems Affected: Windows 95, 98, ME, NT (all versions), 2003, Windows XP (all service packs)  
Systems Not Affected: DOS, EPOC, Linux, Macintosh, Novell Network, OS/2, UNIX  
Technical details:  
1. Creates files in %Windir%\ directory. By default, this is C:\Windows.  
2. Adds values to registry keys:  
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
3. Scans the hard drive for .exe files and infects any executable files.  
Searches for passwords/information, which it may send to a remote attacker.  
Click "OK" to download officially approved security software.  
Always keep your patch levels up-to-date.

Recommendations:

[OK](#) [Cancel](#)



# There is no free lunch





# Phish Attempts

- Date: Thu, 7 Oct 2010 23:25:29 +0200 (CEST)  
From: University of Michigan <webmasterr@umich.edu>  
Reply-To: webmasterr@umich.edu  
Subject: Service Notice

Dear Web mail User,

Due to congestion in all University of Michigan,!webmail users accounts,University of Michigan would be shutting down some unused webmail account.In order to avoid the deactivation of your webmail account,you will have to confirm that is a present use account by clicking the Secure Link Below.The personal information requested is for the safety of your account. Please leave all information requested.

click here to [Secure login](#)

click here to [activate](#) OR [deactivate your email](#)

Webmaster

Copyright 2010 University of Michigan.All rights reserved.

Send as email attachment to [LSA.Security@umich.edu](mailto:LSA.Security@umich.edu) (or 'phishing-report@us-cert.gov' )



# NSF – Data Management Plans

- Effective on Grant applications after 1/18/11
- IRB
- OVPR
- Privacy and Confidentiality of respondents