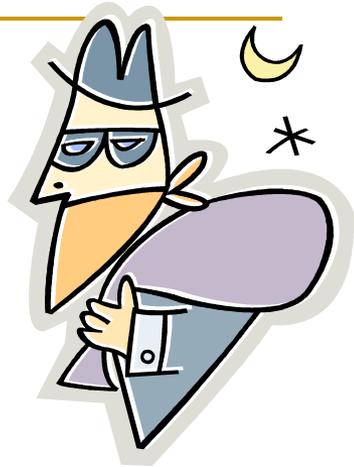

What You Don't Know About Cyber Crime Can Hurt You

Dr. Peter Stephenson, VSM, CISSP, CISM, FICAF
Director, Center for Advanced Computing and Digital Forensics
Associate Professor, Digital Forensics and Investigation
Chief Information Security Officer
Norwich University

Copyright © 2011 Peter Stephenson



One Way to Empty Your Bank * Account



- The Zeus banking Trojan
 - Steals banking credentials from the victim's computer
 - Evades anti-virus software about 55% of the time according to Trusteer (measured in the wild, not in the lab)
 - Up-to-date anti-virus only reduces the probability of a Zeus infection by about 23%
- The URLZone Trojan
 - Functions on the victim's browser
 - Rewrites the browser page to show altered bank statement
 - Harvests victim's banking credentials
 - Managed by a C&C center
 - Launders stolen money through a money mule



Does this Really Work?

Information	
Total reports in database:	6 617 397
Time of first activity:	06.09.2009 01:33:39
Total bots:	10 184
Total active bots in 24 hours:	5.86% - 597
Minimal version of bot:	1.2.4.2
Maximal version of bot:	1.2.4.2

Botnet: btn1 >>	
Actions: Reset Installs	
Time of first activity:	06.09.2009 01:33:39
Total bots:	10 184
Total active bots in 24 hours:	5.86% - 597
Minimal version of bot:	1.2.4.2
Maximal version of bot:	1.2.4.2

Installs (7 621)		Online (98)	
IN	920	HU	13
DE	757	DE	8
US	632	TR	7
BR	474	BR	6
KR	433	CO	6
TR	403	US	6
HU	291	RS	5
RO	273	AR	4
IT	267	CA	4
GB	170	GR	3
CA	159	IT	3
CO	137	CY	2
JP	136	EG	2



Does this Impact Small Businesses?

Published June 01, 2012 | FOXBusiness – “Hackers Not Attracted to Small Business? False”

- Small business owners may think the size of their company precludes them from being targets of identity theft, not realizing they are more at risk than the larger companies.
- While they think their small size means they aren't on the radar screens of hackers, the security holes is exactly what's attracting the criminals.
- If the small business's customer data is breached at the very least it can shake the confidence in the business and at the worst mean lost customers forever. If the owner is the target he or she can see the bank accounts wipe out and their cash flow disappear.
- To criminals, small businesses are the low hanging fruit.
- For many small businesses there isn't much if any separation between their information, employee information and customer data. If a hacker infiltrates the system, it could be a windfall of identifying information the criminal can sell on the black market, use to steal money or create fraudulent identities.



What to Do?

- Compliance does NOT equal security!!!
 - True security testing is a must
 - Pay for a real **penetration** test at least once per year – the cost is well worth it
- Encrypt
- Don't keep payment card (or any personal) info on your systems – for any reason
 - Use a direct payment processing service
- If you are undergoing PCI scanning, check up on your scanning vendor. A quick search with Google will reveal the vendor's true reputation.
- Report any breach immediately
- Monitor your systems, use firewalls and make sure that you network is designed for security
- Encrypt



QUESTIONS ?

