

IDENTITY THEFT: DIMINISHING THE RISK



AGENDA

- Who is committing these crimes?
- How are they doing it?
- Protecting your business
- Resources



WHO THE ACTORS ARE

- Old idea – “script kiddies”
- New idea – Organized freelancers
- Newer idea – State sponsored organized crime
- Newest idea - Evangelists



CHALLENGES

- Zero liability
- Organized crime
- Thieves rarely get caught
- Thieves rarely prosecuted
- Law enforcement lack of resources
- Businesses are not protecting themselves
- Constant breaches



HOW ARE THEY DOING IT?

- Malware
- Windows XP
- Account takeovers
- Common business scams
- Social engineering – ISHING



MALWARE

- Facts
- Avenues



FACTS

- Malicious + Software
- Unwanted software that compromises computer systems
 - Spyware/Adware
 - Viruses
 - Worms
 - Trojans



FACTS

- 74K new malware strains created every day in 2012 Panda Labs
- 75% of malware is engineered to steal money or information Kaspersky Labs
- Mac Malware up 30% McAfee Labs
- Mobile platforms the new target
- Anti-Malware software only catches
~25%-35% of the active threats



AVENUES

- Email with an attachment or link
- Downloaded software or media
- Web surfing to a bad web page
- Drive by downloads
- USB drives
- Social networks



WINDOWS XP SECURITY - WHAT HAPPENED?

- XP is 12 years old, that's like 100 in Internet years
- Support ended on April 8th, 2014
- Microsoft has been announcing for years
- XP is still commonly used by consumers and some businesses



ACCOUNT TAKEOVER

- Targets
- Causes
- What to watch for



TARGETS

- Online banking accounts
- Email
- Social Networking
- Administrative systems
- Retirement/investment accounts



CAUSES

- Password Leaks
- User recycling of passwords
- Malware
- Keystroke logging
- Phishing
- Users discloses passwords willingly
- Breaches / intrusions



WHAT TO WATCH FOR

- Email addresses you have seen before, but out of character
- Email addresses change during correspondence (sometimes slightly)
- Very bad English, terms, and spelling not used in the US (kindly, firstly)
- Emergencies that prevent calling or other contact (meetings, death in family, out of country)
- Time stamps on email are not right
- Requests for information that the customer should have
- Wires to foreign recipients or individuals
- Immediacy or emergencies to get things done “now”
- Changed vendor payment information



COMMON BUSINESS SCAMS

- Invoice scam
- Lonely Heart/internal
- Business partner
- Credit card advance/worthless checks
- Checks and data breach



SOCIAL ENGINEERING

- What it is
- -ishing
- Targeted attacks
- Recon/signs



WHAT IT IS

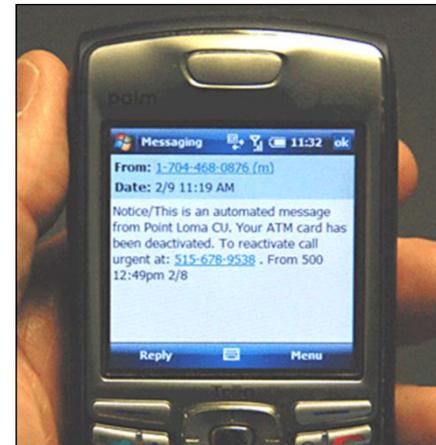
- Deception, manipulation, or persuasion to obtain information or take action
- Has always been around
- Easier than ever
- Very effective
- Unknowing Cooperation!



-ISHING

- Phishing – Email
- Vishing - Voice
- SMSishing – Text

Impersonates banks, websites (iTunes, ebay, facebook),
YOUR COMPANY...



-ISHING - EMAIL WITH MALWARE EXAMPLE

From: nacha.org [mailto:report@nacha.org]

Sent: Thursday, November 12, 2013 8:59 AM

To: bsmith@abcxyzcorp.com

Subject: Rejected ACH transaction, please review the transaction report

Dear bank account holder,

The ACH transaction, recently initiated from your bank account (by you or any other person), was rejected by the Electronic Payments Association. Please review the transaction report by clicking the link below:

[Unauthorized ACH Transaction Report](#)

Copyright ©2013 by NACHA - The Electronic Payments Association



TARGETED ATTACKS

- Phishing becomes “spear phishing” when specific people/roles are targeted
 - Executives (CEOs, CFOs, COOs)
 - Finance personnel
 - Call center
 - IT staff
- Install malware/get sensitive data/access to systems



RECON/SIGNS

- Out of office messages
- “War dialing”
- Fake shipping calls
- Impersonating management, legal, IT
- Social media surfing
- USB drives lying around
- CDs mailed to employees
- Unauthorized wireless networks
- Physical security (theft or entry)
- Email account takeovers



HOW TO PROTECT YOUR BUSINESS

- Understand the issues
- Defense in depth
- Employee education
- Policies / procedures
- Protecting your systems & accounts



DEFENSE IN DEPTH

- Employee Education
- Policies and Procedures
- Protect Your Systems & Accounts



PROTECTING YOUR SYSTEMS

- Secure your systems:
- Use, and keep updated, quality antivirus, anti-spam, and antispyware software
- Aggressively keep computer systems up to date via patching (patches)
- Use firewalls (hardware and software)
- Implement web content filtering and scanning



PROTECTING YOUR SYSTEMS & ACCOUNT

- Perform banking on a dedicated, locked down computer
- Create and enforce policies for acceptable computer use
- Protect passwords
- Limit systems administrator access
- Monitor systems for unusual activity
- Contact your Bank immediately if you suspect a compromise
- Reconcile in timely manner
- Positive Pay
- ACH Filters & Blocks



RESOURCES

- Federal Trade Commission site, <http://www.onguardonline.gov>
- US Computer Emergency Readiness Team (US-CERT) provides many security tips that can make you safer online and offline. Please visit them at <http://www.us-cert.gov/ncas/tips/>.
- <http://www.lookstoogoodtobetrue.com/>
- Associated Bank, <https://www.associatedbank.com/security>
- Social Security Administration
www.ssa.gov
Social Security Fraud Hot Line: (800) 269-0271
- U.S. Postal Inspection Service
<https://postalinspectors.uspis.gov/>
Social Security Fraud Hot Line: (800) 372-8347



RESOURCES

- If you have experienced fraud:
 - Contact the fraud units of the three agencies:
 - Trans Union Credit Services - www.transunion.com
(800-680-7289)
 - Equifax Credit Services - www.equifax.com
(800-525-6285)
 - Experian Credit Services - www.experian.com
(888-397-3742)
 - FEDERAL TRADE COMMISSION
Identity Theft Clearinghouse
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
877-438-4338

