Cyber Crime Trends

2017 Update

CliftonLarsonAllen

CLAconnect.com

Themes

- Hackers have “monetized” their activity
  - More hacking
  - More sophistication
  - More “hands-on” effort
  - Smaller organizations targeted

Mitigation Themes

- Employees that are aware and savvy
- Networks resistant to malware
- Relationships with banks maximized

What are they doing?

- Organized Crime
  – Wholesale theft of personal financial information

- CATO– Corporate Account Takeover
  – Use of online credentials for ACH, CC and wire fraud

- Ransomware

Black Market Economy - Theft of PFI and PII

Active campaigns involving targeted phishing and hacking focused on common/known vulnerabilities.

- Target
- Goodwill
- Jimmy Johns

- University of Maryland
- University of Indiana

- *Anthem*
- *Blue Cross Primera*

- Olmsted Medical Center
- Community Health Systems

Credit Card Data For Sale

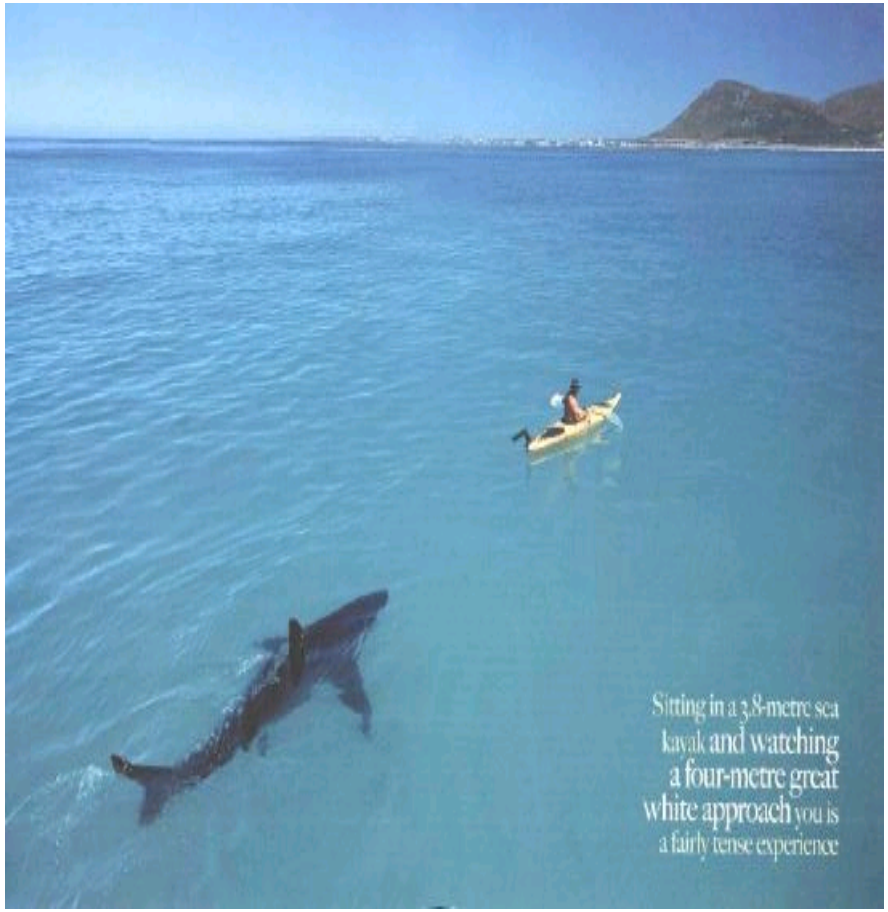
Estimate of Prices (without PIN, with PIN, PIN and good balance)

Dumps	US			EU			CA, AU	
Visa Classic	$15	$80		$40	$150		$25	$150
Master Card Standard		$90			$140			$150
Visa Gold/Premier	$25	$100	$200	$45	$160	$250	$30	$160
Visa Platinum	$30	$110		$50	$170		$35	$170
Business/Corporate	$40	$130		$60	$170		$45	$175
Purchasing/Signature	$50	$120		$70			$55	
Infinite				$130	$190		$60	$200
Master Card World		$140						
AMEX	$40			$60			$45	
AMEX Gold	$70			$90			$75	
AMEX Platinum	$50							

Corporate Account Takeover

- Catholic church parish
- Hospice
- Collection agency
- Main Street newspaper stand
- Electrical contractor
- Health care trade association
- Rural hospital
- Mining company

- On and on and on and on…….



CATO – 3 Versions

1. Deploy malware – keystroke logger

2. Deploy malware – man in the middle

3. Recon / email persuasion
    1. ***"Whaling"***
    2. ***Business email Compromise***
    3. ***CEO attack***

Multi-Factor Authentication Solutions

- MFA is critical
- Silver bullet?

CATO Defensive Measures

- Multi-layer authentication
- Multi-factor authentication
- Out of band authentication
- Positive pay
- ACH block and filter
- IP address filtering
- Dual control
- Activity monitoring

Ransomware

- Malware encrypts everything it can interact with
  - V1: Everything where it lands
  - V2: Everything where it lands plus everything user has rights to on the network
  - V3: Everything where it lands plus everything on the network

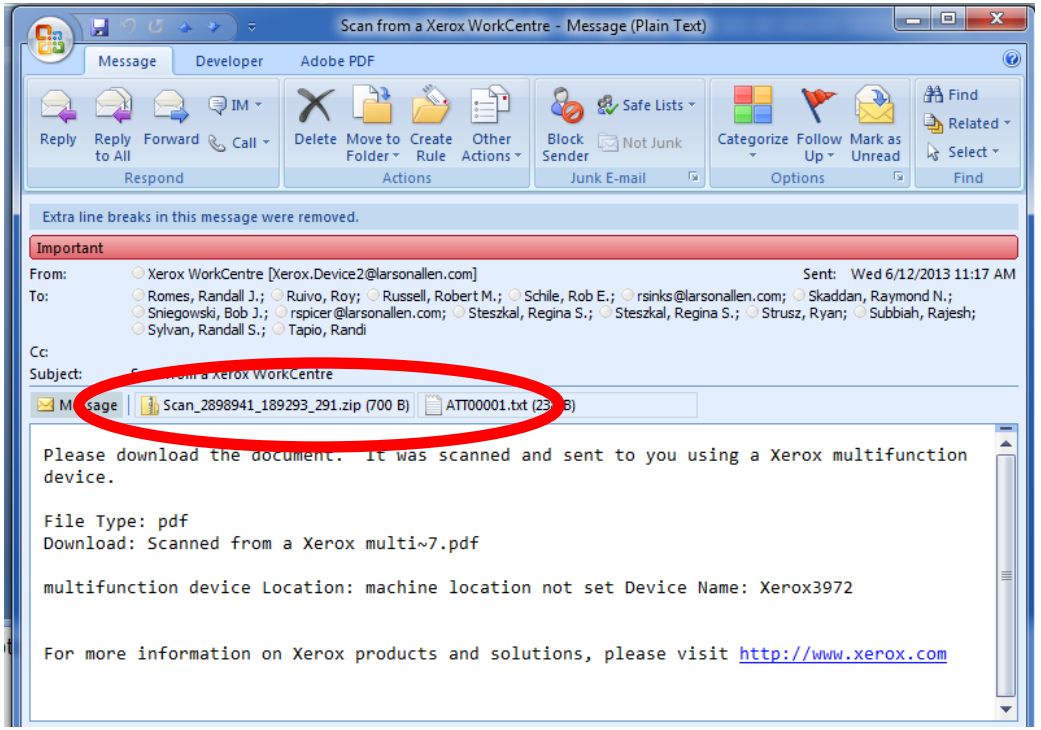
- CryptoLocker / Cryptowall

FBI Warning – Ransomware is Surging

- Single global campaign - $325Million
- US 2015 - $24Million
- Attackers are “investing” these proceeds to improve the code
  - New variants infect back ups as well

Ransomware

- Zip file is preferred delivery method
  - Helps evade virus protection
- Working (tested) backups are key



The Cost?

Norton/Symantec Corp:

- Cost of global cybercrime: $388 billion

- Global black market in marijuana, cocaine and heroin combined: $288 billion

Questions?

Hang on, it's going to be a wild ride!!

Mark Eich, Principal

Information Security Services Group

mark.eich@claconnect.com

***

(612)397-3128

Appendix:

10 Key Defensive Measures

CliftonLarsonAllen

CLAconnect.com

96% of Attacks are Preventable!

- Intrusion Analysis: TrustWave
- Intrusion Analysis: Verizon Business Services
- Intrusion Analysis: CERT Coordination Center
- Intrusion Analysis: CLA Incident Handling Team

Strategies

Our information security strategy should have the following objectives:

- Users who are more aware and savvy
- Networks that are resistant to malware
- Relationship with our FI is maximized

Ten Keys to Mitigate Risk

1. Strong Policies -

- Email use
- Website links
- Removable media
- **Users vs Admin**
- **Insurance**

Ten Keys to Mitigate Risk

2. Defined user access roles and permissions

- Principal of minimum access and least privilege
- **Users should NOT have system administrator rights**
  - **"Local Admin" in Windows should be removed (if practical)**

Ten Keys to Mitigate Risk

3. **Hardened internal systems (end points)**
   - Hardening checklists
   - Turn off unneeded services
   - **Change default password**
   - **Use Strong Passwords**
   - **Consider application white-listing**
4. **Encryption strategy – data centered**
   - Email
   - Laptops and desktops
   - Thumb drives
   - **Email enabled cell phones**
   - Mobile media

Ten Keys to Mitigate Risk

5. Vulnerability management process

- Operating system patches
- **Application patches**
- Testing to validate effectiveness –
  - "belt and suspenders"

Ten Keys to Mitigate Risk

6. **Well defined perimeter security layers:**
   - **Network segments**
   - Email gateway/filter
   - Firewall – “Proxy” integration for traffic in AND out
   - Intrusion Detection/Prevention for network traffic, Internet facing hosts, AND workstations (end points)
7. **Centralized audit logging, analysis, and automated alerting capabilities**
   - Routing infrastructure
   - Network authentication
   - Servers
   - Applications

Ten Keys to Mitigate Risk

8. Defined incident response plan and procedures

- **Be prepared**
- Including data leakage prevention and monitoring
- Forensic preparedness

Ten Keys to Mitigate Risk

9. Know / use Online Banking Tools

- Multi-factor authentication
- Dual control / verification
- Out of band verification / call back thresholds
- ACH positive pay
- ACH blocks and filters
- Review contracts relative to all these
- Monitor account activity ***daily***
- **Isolate the PC used for wires/ACH**

Ten Keys to Mitigate Risk

10. Test, Test, Test
    - "Belt and suspenders" approach
    - Penetration testing
        - ◊ Internal and external
    - Social engineering testing
        - ◊ Simulate spear phishing
    - Application testing
        - ◊ Test the tools with your bank
        - ◊ Test internal processes

"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."