Prices falling for Cybercriminal Supplies

Fred Williams | November 27, 2013 | Protecting Yourself

$4
18 Sources: Target Investigating Data Breach

DEC 13

Risk Responses

- Quantify existing risk and accept it
- Mitigate existing risk to an acceptable level
- Transfer risk to a 3rd party
How can you make yourself difficult to attack?
Competitive Advantage #1

Understand your Opponent
# Summary of Actors

## Nation States
- **Agenda driven.** Sophisticated and well-funded. Least likely to perform untargeted attacks. Highly likelihood for advanced persistent threats. Risks include IP theft, compromised systems. Likely possesses zero-day vulnerabilities.

## Organized Crime
- **Financially driven.** Moderate-to-high sophistication. May possess zero-day exploits, likely botnets. Tactics include phishing (including spear phishing), ransomware.

## Hacktivists
- **Agenda driven.** Low-to-moderate sophistication. Reliance on botnets, known vulnerabilities exploited in unpatched systems. Tactics include business disruption, leaking data.

## Employees
- **Motives and capacities vary widely.** May be intentional or unintentional. Appropriate policies and controls will limit damages. Responses can be rapid and comprehensive.

## Individual Hackers
- **Ego driven.** Threat profile comparable to low/moderate-capacity Hacktivist/Organized Crime categories. Diminishing demographic.
Competitive Advantage #2

Understand Cybercriminal Behavior
Breach Methodology:

- Phishing
- Hopping
- Scraping
- Aggregating
- Exfiltrating
Cyber Kill-Chain

stop any step = stop the breach
PHISHING
HOPPING
SCRAPING
AGGREGATING
EXFILTRATING
Cyber Kill-Chain

stop any step = stop the breach
Competitive Advantage #3

Understand your Opponent’s Motivation
RANSOMWARE

- SF Muni – $73k ransom
- City of Atlanta – $52k ransom
- Anchorage, AK (Mat-Su) – $400k ransom
- Valdez, AK – Paid $27k ransom
- Jackson County, Georgia – Paid $400k ransom
Ransomware Penetration:

- Phishing – need MFA on your O365 accounts
- Port 3389 – CLOSE IT!
- Pass the Hash – TOXIC Domain Admin accts
- MFA on your VPN – is it not optional
- Identical local admin accts on all PCs – LAPS
- Unpatched PC’s / users as local admins – TOXIC
Ransomware Defenses:

- OFFLINE backups. TESTED, MONITORED backups
- Tested restore procedures
  - Offline restore methodology
  - Workstation reimages
  - Server full rebuilds
- Pre-negotiated incident response team contract
- Geofiltering of all Internet traffic
- 35% free drive space on all network drives
Regarding Cybersecurity Insurance...

Zurich Refuses to Pay Out for NotPetya ‘Act of War’

Shifting gears...

Competitive Advantage #4

Catch them in the Act
Proactive detection beats a great response, every time
Bryce Austin
CEO, TCE Strategy

Twitter: @bryceas
LinkedIn: linkedin.com/in/bryceas