Cybercrime 101
Christopher Pogue
SVP, Cyber Threat Analysis
Cybercrime 101 - Agenda

- Threat Landscape
- The Attacks
- Post Breach Steps
- Conclusion
Target Missed Signs of a Data Breach

Goodwill reportedly joins list of companies affected by data breaches

Jul 22, 2014, 1:07pm CDT

Danielle Abril
Staff Writer-
Dallas Business Journal
Email | LinkedIn | Twitter | Google+

Goodwill Industries International Inc. is the latest North Texas company that could have fallen victim to cyber thieves.

Details continue to emerge about the probe into the implications of the investigation for the U.S. payment card account numbers may have been stolen, along with some expiration dates and/or cardholder names.

Affected cards were used between June 22, 2014 and July 17, 2014 at the 180 SuperValu stores and standalone liquor stores listed here.
Threat Landscape

- Dramatic increase in cyber attacks
  - Significant increase over 2013
  - Legal Challenges
    - Attribution
    - Foreign cooperation
      - Politics
      - Diverse laws
    - Positive financial impact
    - Corruption
    - MLAT process
  - Robust shadow economy
  - Lucrative and attractive lifestyle
Threat Landscape
Threat Landscape

Hacked By Hezbollah Cyber Army

WANTED BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Huang Zhenyu  Wen Xinyu  Sun Kailiang  Gu Chunhui  Wang Dong
The Attacks
The Attacks

• Marked increase in attack complexity
  – Adapting to stringent security controls & improved security technologies
    • Leverage arrogance
    • Global coordination
    • Motivation
      – Geopolitical
      – Retaliation
      – Financial
      – Opportunity
  – Custom malware
    • Family based
    • Unique to the victim location
      – Commoditization of malware packages
      – 0day equivalent
Attack Sophistication

• Creativity
  – Taking what they’re given
    • Finding ways in
    • Finding ways out
  – Indirect attacks
    • Trusted partners
    • Phishing
    • Client Side
    • BYOD
Attack Sophistication

• Trusted partners
  – Legitimate access
  – Assumption of security importance
    • Measure of equivalence
  – Difficult to test security controls
  – No mechanism for enforcement
• Phishing attacks
  – Radically improved
  – Topical and timely
    • Holidays
    • Vacations
    • Benefits enrollment
    • Consumer directed
  – It only takes one
  – Propagation can be extremely fast
• Traditional hacking vector
  – Direct server-side attack: The most common and widely used method for external attacks

• Client-Side attacks
  – Applications installed on your desktop are a potential targets (PDF readers, MS Office tools, etc...)

• Social Engineering
  – An attack that exploits human interaction
  – the goal is tricking the target into providing sensitive data or do something that should be prohibited by security policy
• Social Engineering may be used in different situations
  – In person / physical approach with target
  – Via telephone
  – E-mail (phishing)
  – Delivering potential gifts, etc. (baiting)

• There are variants that mix different approaches.

• Can be much easier for an attacker
  – Get targets to leak their credentials or to execute code on the client-side
  – Circumvents the perimeter security and creates a channel from the inside out
Post Breach Steps
Post Breach Steps

Breach Windows

- Four “Windows”
  - Initial Breach
  - Breach Identification
  - Containment of the Breach
  - Vulnerabilities are remediated
Post Breach Steps

Breach Windows

• Breach to identification
  – The most critical
  – Organizations continue to struggle here

• Identification to containment
  – Timeline
  – Impact

• Containment to eradication
  – Correct deficiencies
  – Implement additional security controls

• Business resumption
  – Back to business as usual
  – Prepare for the next attack
Post Breach Steps

Detection

• White noise or trigger event
  • Who’s watching
  • What are they watching

• Going Native
  • Legitimate credentials
  • Usage differentiation

• Intelligence Integration
  • Current threat landscape and attack vectors
  • Consider the unlikely and the improbable

• Blinding the target
  • Manipulate and/or disable security controls
  • Create analysis paralysis
Where things are going to have to go

• Intelligence correlation
  – A is OK
  – B is OK
  – A & B together are not OK

• Activity profiling
  – What is “normal”

• Defense in Depth
  – Layers
  – Understand the threat
What are you defending against

• Current attack patterns
  – **Actionable** intelligence
    • Public information
    • Investigations
    • Penetration tests
    • Malware

• Expend your time, energy, and money appropriately
  – Focus on current threat landscape

• Flexibility
  – Follow the threat
    • Tybalt cancels out Capafero
Conclusion
Conclusion

• Increased focus on data breaches
• Hacker culture, fueled by profits, nationalism, or terrorism
• Creative, bold, and relentless
• Creativity in defense
• Actionable Intelligence
• Improve detection capabilities
• Ongoing efforts
Conclusion

Closing Thought...

National Security

Report: Cybercrime and espionage costs $445 billion annually

References

- https://krypt3ia.wordpress.com/category/mil/page/6/
- http://www.auburncc.org/content.php?cid=231
- http://getbestitservices.wordpress.com/2013/05/15/it-outsourcing-decreasing-the-operational-cost-effectively/
- http://www.fortifiedsecurityservices.com/
- http://www.ucd.ie/cci/education/prospective_students/fcci_programmes.html
- http://www.experienceproject.com/stories/Love-Ice-Cream/618797
- https://twitter.com/MalSec
- http://scraping.pro/anonymous-scraping-visual-web-ripper/
- http://www.threatmetrix.com/tag/lulzsec/
Questions?