Why You Need to Get Hacked!

Penetration Testing & Network Security in the Title Industry
presented by Punctual Abstract & TrustFoundry

August 2020
Speakers

Alex Lauerman
TrustFoundry

Ted Woloszyk
CEO, Punctual Abstract

Nick Sagona
CTO, Punctual Abstract
Today’s Topics

• Cyber Security - The Threat is Real
• Why You Need to Get Hacked! (On Purpose)
• Penetration Testing - What it is, How it works
• Case Study - Punctual Abstract
• Q&A
Cyber Security - The Threat is Real

Nick Sagona, Punctual Abstract
You’ve seen the headlines ...

DC homebuyers lose $1.57 million after title company was apparently hacked

Orlando homebuyers lose $46,000 in title company impostor scheme
You’ve seen the headlines ...

Hackers impersonating mortgage and title staffers in wealthy Texas suburb to steal down payments

Police in Southlake issue warning about imposters

---

Real Estate Cyber Threats Increasing During COVID-19
According to the FBI’s Internet Crime Complaint Center

• 2019 Real Estate Cyber Crimes
  – Real Estate/Rental
  – Nearly 12K incidents

### 2019 CRIME TYPES

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Victims</th>
<th>Crime Type</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing/Vishing/Smishing/Pharming</td>
<td>114,702</td>
<td>Lottery/Sweepstakes/Inheritance</td>
<td>7,767</td>
</tr>
<tr>
<td>Non-Payment/Non-Delivery</td>
<td>61,832</td>
<td>Misrepresentation</td>
<td>5,975</td>
</tr>
<tr>
<td>Extortion</td>
<td>43,101</td>
<td>Investment</td>
<td>3,999</td>
</tr>
<tr>
<td>Personal Data Breach</td>
<td>38,218</td>
<td>IPR/Copyright and Counterfeit</td>
<td>3,892</td>
</tr>
<tr>
<td>Spoofing</td>
<td>25,789</td>
<td>Malware/Scareware/Virus</td>
<td>2,373</td>
</tr>
<tr>
<td>BEC/EAC</td>
<td>23,775</td>
<td>Ransomware</td>
<td>2,047</td>
</tr>
<tr>
<td>Confidence Fraud/Romance</td>
<td>19,473</td>
<td>Corporate Data Breach</td>
<td>1,795</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>16,053</td>
<td>Denial of Service/TDoS</td>
<td>1,353</td>
</tr>
<tr>
<td>Harassment/Threats of Violence</td>
<td>15,502</td>
<td>Crimes Against Children</td>
<td>1,312</td>
</tr>
<tr>
<td>Overpayment</td>
<td>15,395</td>
<td>Re-shipping</td>
<td>929</td>
</tr>
<tr>
<td>Advanced Fee</td>
<td>14,607</td>
<td>Civil Matter</td>
<td>908</td>
</tr>
<tr>
<td>Employment</td>
<td>14,493</td>
<td>Health Care Related</td>
<td>657</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>14,378</td>
<td>Charity</td>
<td>407</td>
</tr>
<tr>
<td>Government Impersonation</td>
<td>13,873</td>
<td>Gambling</td>
<td>262</td>
</tr>
<tr>
<td>Tech Support</td>
<td>13,633</td>
<td>Terrorism</td>
<td>61</td>
</tr>
<tr>
<td>Real Estate/Rental</td>
<td>11,677</td>
<td></td>
<td>39</td>
</tr>
<tr>
<td>Other</td>
<td>10,842</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
According to the FBI’s Internet Crime Complaint Center

- 2019 Real Estate Cyber Crime Value
  - Real Estate/Rental
  - Over $200 Million

### 2019 Crime Types Continued

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Loss</th>
<th>Crime Type</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEC/EAC</td>
<td>$1,776,549,688</td>
<td>Employment</td>
<td>$42,618,705</td>
</tr>
<tr>
<td>Confidence Fraud/Romance</td>
<td>$475,014,032</td>
<td>Civil Matter</td>
<td>$20,242,867</td>
</tr>
<tr>
<td>Spoofing</td>
<td>$300,478,433</td>
<td>Harassment/Threats of Violence</td>
<td>$19,866,654</td>
</tr>
<tr>
<td>Investment</td>
<td>$222,186,195</td>
<td>Misrepresentation</td>
<td>$12,371,573</td>
</tr>
<tr>
<td>Real Estate/Rental</td>
<td>$221,365,911</td>
<td>Theft and Embezzlement</td>
<td>$10,293,307</td>
</tr>
<tr>
<td>Non-Payment/Non-Delivery</td>
<td>$196,563,497</td>
<td>Counterfeit</td>
<td>$8,965,847</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>$160,305,789</td>
<td>Ransomware</td>
<td></td>
</tr>
<tr>
<td>Government Impersonation</td>
<td>$124,292,606</td>
<td>Denial of Service/TDoS</td>
<td>$7,598,198</td>
</tr>
<tr>
<td>Personal Data Breach</td>
<td>$120,102,501</td>
<td>Charity</td>
<td>$2,214,383</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>$111,491,163</td>
<td>Malware/Scareware/Virus</td>
<td>$2,009,119</td>
</tr>
<tr>
<td>Extortion</td>
<td>$107,498,956</td>
<td>Re-shipping</td>
<td>$1,772,692</td>
</tr>
<tr>
<td>Advanced Fee</td>
<td>$100,602,297</td>
<td>Gambling</td>
<td>$1,458,118</td>
</tr>
<tr>
<td>Other</td>
<td>$66,223,160</td>
<td>Health Care Related</td>
<td>$1,128,838</td>
</tr>
<tr>
<td>Phishing/Vishing/Smishing/Pharming</td>
<td>$57,836,379</td>
<td>Crimes Against Children</td>
<td>$975,311</td>
</tr>
<tr>
<td>Overpayment</td>
<td>$55,820,212</td>
<td>Hacktivist</td>
<td>$129,000</td>
</tr>
<tr>
<td>Tech Support</td>
<td>$54,041,053</td>
<td>Terrorism</td>
<td>$49,589</td>
</tr>
<tr>
<td>Corporate Data Breach</td>
<td>$53,398,278</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lottery/Sweepstakes/Inheritance</td>
<td>$48,642,332</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
U.S. Secret Service Creates Cyber Fraud Task Force

In recognition of the growing convergence of cyber and traditional financial crimes, the U.S. Secret Service has merged two electronic and financial crimes units into a single unified network.

The newly formed Cyber Fraud Task Force (CFTF) will focus on investigating cyber-enabled financial crimes, such as business email compromise schemes and ransomware attacks. The mission of the CFTF is to prevent, detect, and mitigate complex cyber-enabled financial crimes, with the goal of arresting and convicting the most harmful perpetrators.

“The creation of the new Cyber Fraud Task Force (CFTF), will offer a specialized cadre of agents and analysts, trained in the latest analytical techniques and equipped with the most cutting-edge technologies,” said Michael D’Ambrosio, assistant director of the U.S. Secret Service. Together with our partners, the CFTFs stand ready to combat the full range of cyber-enabled financial crimes. As the Nation continues to grapple with the wave of cybercrime associated with the COVID-19 pandemic, the CFTFs will lead the effort to hold accountable all those who seek to exploit this perilous moment for their own illicit gain.”
Real estate transaction crimes are NOT the only Cyber Crimes that threaten your title agency

• Your operation could be at risk for:
  
  - **Corporate Data Breach**: A leak or spill of business data that is released from a secure location to an untrusted environment. It may also refer to a data breach within a corporation or business where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

  - **Malware/Scareware/Virus**: Software or code intended to damage or disable computers and computer systems. Sometimes scare tactics are used by the perpetrators to solicit funds.

  - **Ransomware**: A type of malicious software designed to block access to a computer system until money is paid.
  
  - And more...
Cyber Security at your title agency is CRITICAL to protect YOUR CUSTOMERS & YOUR OPERATION
You Need to Get Hacked (on purpose) by Conducting a Penetration Test
A Penetration Test Will

• Test your system’s vulnerabilities
• Find your security flaws
• Alert you to fix them before Hackers find them
Penetration Testing – The Nitty Gritty

Alex Lauerman, TrustFoundry
What is Penetration Testing?

• Simulated attack
  – Goal based to simulate a real attack
  – Not an audit
Different Types of Penetration Testing?

• Network
  • External Network
  • Internal Network

• Application
  • Web Application (including APIs)
  • Mobile Application

• Social Engineering
  • Email
  • Phone

• Red Team
  • Can encompass all of the above
How is Penetration Testing Performed

• Planning
  • Kickoff call to discuss approach and agree upon rules
    • Testing restrictions
    • Whitelist testing IPs
  • Discuss or convey information
    • Evasive vs non-evasive testing
  • The approach to how much information is conveyed is sometimes referred to as “blackbox/greybox/whitebox”

• Automated tools perform basic analysis
  • Finds low hanging fruit quickly
  • Only performing this step is called a Vulnerability Assessment, which is not a penetration test
How is Penetration Testing Performed

- **Manual testing**
  - Analyze each listening service for vulnerabilities

- **Reporting**
  - Most companies deliver results as a PDF
What does Penetration Testing Identify?

• Anything that would be of value to an attacker
  • Misconfigurations
    • Sensitive information accidentally exposed
  • Weak credentials
  • Technical vulnerabilities
How do I Find a Penetration Testing Provider

• **Speak with multiple vendors**
  • Get referrals, especially from someone who understands penetration testing
  • Evaluate the skill level of the company and consultants
  • Review company information (blog, LinkedIn profiles, etc.)
Part of an Overall Security Program

• Security is not a one-step process
Case Study: Punctual Abstract

Ted Woloszyk, Punctual Abstract
Security & Working with Vendors

• I know from personal experience...
• Security matters at every touchpoint in title production chain
  – Even though title evidence is public record, it’s pulled together all in one place that makes it attractive to criminals
  – Minimize your liability & risk
  – Professional business practices in security indicates professionalism across the board
Punctual Abstract: Who We Are

• A national leader in title evidence research
  – Millions of title abstracts performed since 1993
  – Based in New Orleans metro
  – Searches performed nationwide
  – Boots-on-the-ground & online
  – Fully examined product
Punctual Abstract: What We Do

• Residential Searches
  – Current Owner (refinance, home equity, loan modification, credit risk and tax sales)
  – Two owner (pre-foreclosure)
  – Full Abstract (buy/sell & REO)
  – Custom Searches

• Commercial Search Examples
  – Cell phone tower, shopping mall, hotel, levee, DOT
Punctual Abstract: Security Steps We’ve Taken

- SOC 1 Type 1 Certified
- Working on SOC 2 Certification
- Technologically advance, IT staff of 8
- Integrates with most closing software platforms
- Performs periodic penetration tests
- Trains our staff to identify & delete suspicious emails
- System flags fraudulent emails made to appear internally generated but comes from outside sources
Penetration Test - How to Prepare

• External Network Penetration Test
  • Provide your IP Address(es) to the Penetration Tester
    – IP is a set of numbers that are your internet connection’s address
    – Other than that, there’s no other prep
    – Additional information will need to be provided for
      – Internal Testing
      – Social Engineering
      – Phishing
Penetration Test Results

• Address the issues found, you may need IT help to do this
  • Close up gaps
  • Repair any vulnerabilities
    – Run the test again
    – Fix issues
    – Keep doing it until you get a test back with no real vulnerabilities
Penetration Test

• What to expect:
  • That’s how we knew they had started the simulated hack!
  • We asked them to stop
  • We addressed the issue
  • Started again
What the Penetration Test Might Find

• Hardware & Software Concerns
  – Outdated:
    • equipment
    • firmware
    • software
  – Open Ports or other access
How Often to Perform a Penetration Test

- Ideally: Every Quarter
  - If Possible: Every Quarter
  - At least: Yearly
CONTACT INFO

Ted Woloszyk | twoloszyk@punctualabstract.com
Nick Sagona | nsagona@punctualabstract.com
Alex Lauerman | alex.lauerman@trustfoundry.net