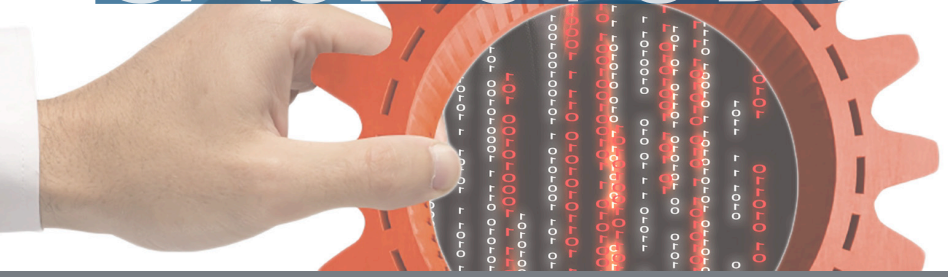
Patti Engineering Breach Mitigation

CASE STUDY



cbi
IT Risk Management

On September 30, 2015, Patti Engineering, a CSIA Certified control systems integration company offering high-caliber engineering and software development services, contacted CBI regarding potential suspicious activity on their network. They provided details of these suspicious activities which included information that pertained to a recent "virus outbreak," along with financial funds being maliciously transferred from their business banking accounts.

CBI immediately coordinated with Patti's team and arrived onsite later that morning to begin a breach investigation. The engagement included roughly three days of research and analysis conducted at the Patti Engineering in Auburn Hills, Michigan.

Upon arriving at the Patti Engineering headquarters, CBI immediately executed a custom incident response framework to triage the incident, enact proper incident response handling measures, and restore core business functionality. Once these tasks were completed, CBI worked to unweave the complex details of the attack.

The preliminary analysis indicated that this was a targeted attack with relatively sophisticated attack and social engineering vectors:

- Various spear-phishing and social engineering attacks targeted Patti Engineering that started well before any suspicious activities were identified
- Specific employees at Patti Engineering were targeted by the malicious attackers, due to the access these employees had to the online banking portal along with their roles or responsibilities within the organization
- The primary attack vector of these social engineering attacks was to compromise online banking passwords of key employees in an effort to conduct fraudulent wire transfers
- Multiple Malware variants were infecting different workstations as the social engineering attacks escalated

CBI's analysis showed that the fraudulent wire transfers were slipped into the payroll batch . Approximately $150,000 was transferred to twenty different accounts. During the time the fraudulent wire transfers were conducted, the attackers launched SPAM email floods on specific Patti Engineering email accounts in an effort by the malicious attackers to detract attention away from the fraudulent wire transfers.

The twenty account numbers in which the $150,000 was being routed to were identified as "money mules" that would be used to offload the money to another person. This is a common money laundering scheme CBI has observed in other fraudulent wire transfer breaches. Interviews with key employees working for the bank used by Patti Engineering identified that one of the money mules had come forward and contacted a bank representative.

This individual reported that he had just been hired at a new company called Platinum7 LLC.

Upon researching the Platinum7 LLC company, additional discoveries were made:

- The platinum7llc.com domain was recently registered on September 8, 2015 in Hong Kong
- The company claimed to be in existence since 2013 but this was a red flag, as the domain was just created
- The website www.platinum7llc.com contained a physical address in New York, that CBI identified as illegitimate after calling the building tenant asking for information on Platinum7 (the building was identified as an apartment complex)
- A legitimate company called Platinum7 existed from 2008-2011, and the attackers likely used this company name due to the historic data on the internet, aiding them in convincing the recruits that company was real.

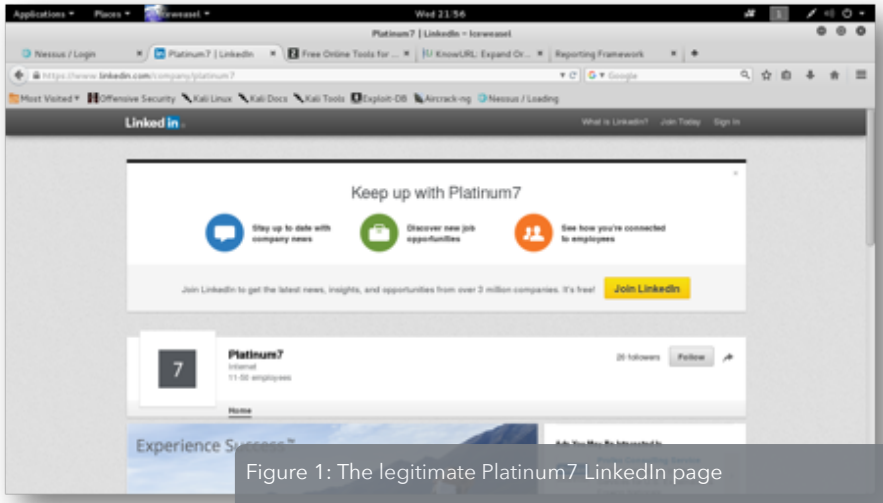


Figure 1: The legitimate Platinum7 LinkedIn page

Here we can see the old, but legitimate Platinum7 Company LinkedIn profile that the attackers used as a foundation for their attack.

In time, other unsuspecting money mules came forward. Interviews indicated that they were promised a weekly salary in exchange for graphic design and website development work. In reality, the attackers were funneling fraudulent wire transfers to the money mules, then requesting the money mules wire the funds to another individual. One innocent money mule identified his request to transfer the funds out of his account to a user named "Egor" in the Czech Republic. Interviews with other money mules identified that they were also recruited by various Platinum7 employees. Multiple victims identified they received their job offer through Craigslist, CareerBuilder, or other online job postings.

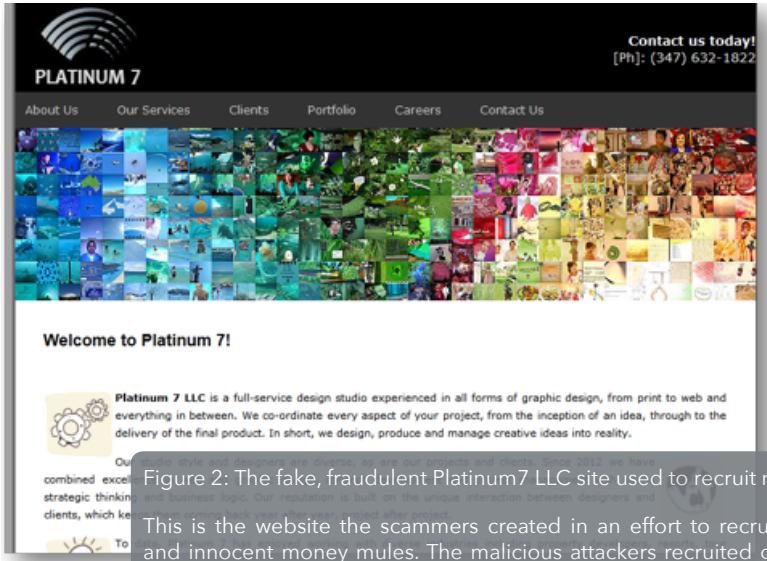


Figure 2: The fake, fraudulent Platinum7 LLC site used to recruit money mules

This is the website the scammers created in an effort to recruit both willing and innocent money mules. The malicious attackers recruited graphic design "employees" with incentives such as working from home, $2,500 in pay per week, and the ability to work with Fortune 100 companies.

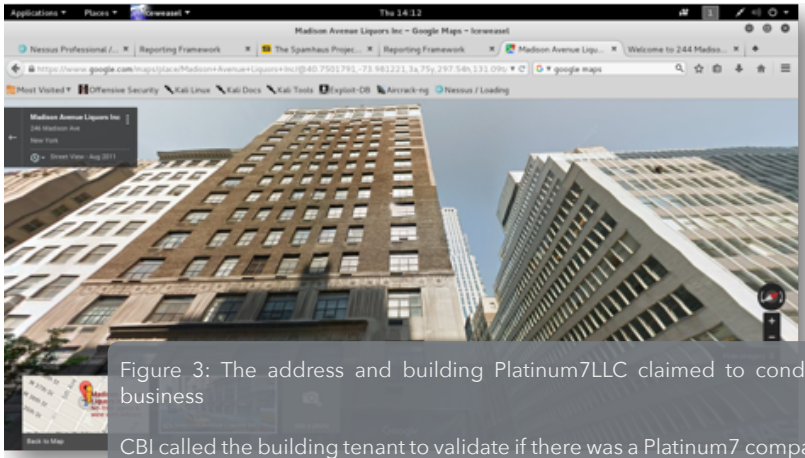


Figure 3: The address and building Platinum7LLC claimed to conduct business

CBI called the building tenant to validate if there was a Platinum7 company residing at the address. The building tenant notified CBI that there wasn't a commercial business at this building, as it was strictly zoned as a residential apartment complex.

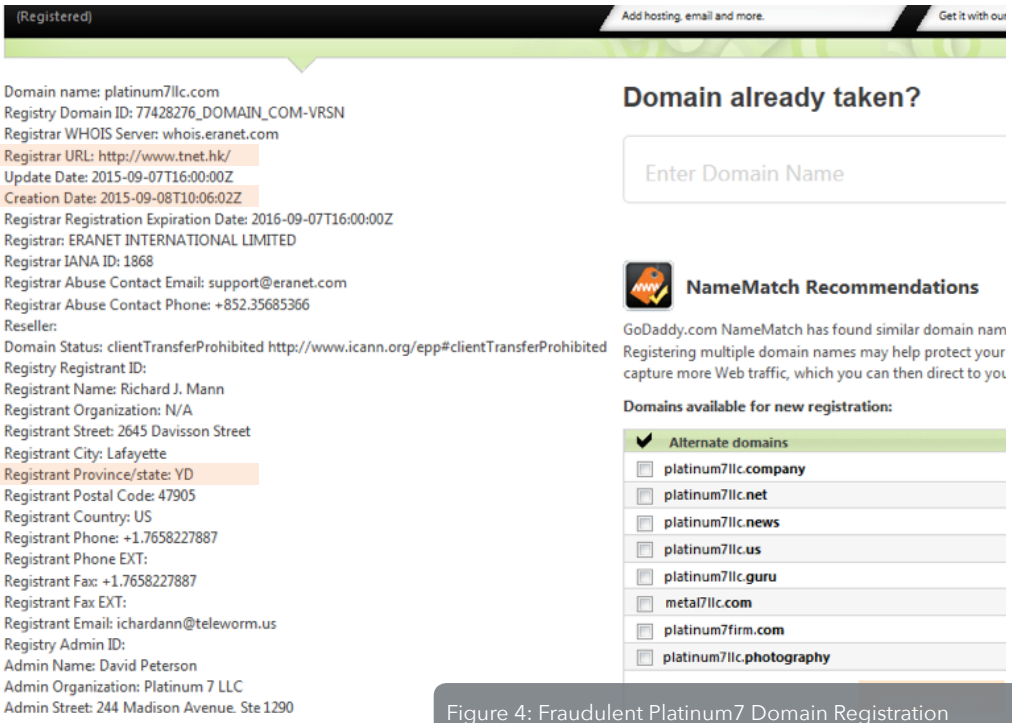


Figure 4: Fraudulent Platinum7 Domain Registration (Note creation date, Registrar URL, State, etc.)

Summary

This is a very popular attack method and demonstrates the sophistication of the crime syndicate involved. The security team at CBI was able to identify the majority of the threat chain and provided Patti Engineering with strategic recommendations to enhance their security posture and awareness. CBI then assisted Patti Engineering with implementing remediation solutions in a prioritized fashion, reducing the impact of the identified attack campaign and building a more resilient security posture that covers both people and technology.

It's also important to recognize the positive attributes associated with this incident. The engineers and information technology resources working for Patti Engineering are not traditionally trained IT professionals. Many of them have coding and electrical engineering backgrounds which contributed to the incident response effectiveness and ability to remediate the situation in days, not weeks.

Contact

www.cbihome.com

800.747.8585

cbi_info@cbihome.com

CBI HQ
1260 Woodward Heights
Ferndale, MI 48220

CBI | Detroit
1260 Library St
Detroit, MI 48226

About Patti Engineering

Patti Engineering, Inc. is a CSIA Certified control systems integration company offering high-caliber engineering and software development services. Patti Engineering's technical expertise in electrical control and information systems provides turnkey control systems integration for design/build, upgrade/retrofit and asset/energy management projects. Industrial automation, production intelligence and shop floor IT solutions services include: project management, electrical engineering, hardware design, hardware procurement, software development, installation, calibration, start-up testing, verification, documentation, training and warranty support. Customer satisfaction and project success earned the company placement in the Control Engineering Magazine's Hall of Fame.

www.pattiengineering.com

Patti Engineering

About CBI

CBI manages IT security risk and helps ensure your data is secure, compliant and available. No matter your industry our Subject Matter Experts, tailored assessments and custom solutions help safeguard your organization's information. Our proven process allows you to prepare, manage and navigate issues that can damage your business and reputation. For more than 20 years our customers have come to rely on CBI as their trusted advisor to meet their unique needs with solutions from the best professionals in the industry. Our broad subject matter expertise ensures we deliver on our promise to help defend and secure your network and endpoints; test and monitor areas of operational risk; and protect your data.

www.cbihome.com

cbi