Phishing

Why an attack created in 1987 still works today

TJ OConnor

GIAC (GSE, GSEC, GCFW, GCIA, GCIH, GCFA, GREM, GPEN, GWAPT, GCFE)

Phishing

- "*Phishing emails typically contain misspellings, are addressed to a generic audience, ask for personal information or include the need to act immediately*." – West Point IT105 Curriculum

- The above statement is no longer true. In fact, the following more accurately describes today's phishing:
  - Spear phishing and whaling towards targeted individuals
  - Combined with information from social networking sites
  - Contain highly-personalized information
  - Appears to come from a legit authority
  - Phishing drop sites look identical to legit sites
  - Combined with zero-days to avoid IDS & Virus Scans

- The majority of people fail to understand how phishing can be combined to pivot towards the internal network

How phishing leads to a much greater threat…

- *"One skilled phishing attack can lead to total devastation in a company." – Social-Engineer.org*

- RSA Breach
  - A targeted email with an exploit embedded in an Excel spreadsheet
  - Combined with information found on social networking sites
  - Exploit installed remote access toolkit (RAT)
  - RAT used to steal source code for RSA Secure IDs
  - May 2011, stolen IDs used to attack three defense contractors

- Operation Aurora
  - Attacked over 34 high-tech and defense companies
  - A targeted email that included an IE-6 Zero Day
  - Attack pivoted towards Source Code Repositories
  - July 2011, we see several successful attacks against Gmail

Phishing's role in the overall attack anatomy…

- Individuals are targeted based on information found in company directory on web or on social networking sites
- Targeted individuals are emailed either a link or an Adobe pdf, or MS Office document
- Link or embedded document exploits vulnerability that makes a reverse callback to remote attacker
- Attacker installs remote access toolkit; uses toolkit to search machine, its privileges and pivot towards internal network
- PR department dubs it an advanced persistent threat (APT) in order due to concern about financial liability to customers

Why it is only getting worse…

- Continued false education
  - Phishing seen as an attempt to solicit users
  - Thought of as only malformed URLs
  - Client-side attacks not discussed routinely
- Integration with social networking
  - Our lives today are routinely divulged on the internet
  - Information can be harvested to create personal phishing emails
- Social Engineering Toolkit
  - GUI to create spear-phishing campaigns
  - Can deliver client-side-exploits, install a remote access kit
- Lack of accountability and understanding
  - *Does the average end user understand that three separate defense contractors were compromised because one RSA employee opened an Excel Spreadsheet from an email?*

References

Banks, David. "Spear Phishing Tests Educate People About Online Scams." The Wall Street Journal, August 17th, 2005.

Binde, Beth et al. "Assessing Outbound Traffic to Uncover Advanced Persistent Threat." Retrieved from the Sans Institute Web Site: http://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf. Last accessed 08 June 2011.

EECS. "IT105 Intro to Information Technology." Retrieved from Internal US Military Academy D/EECS Web Site: http://www-internal.eecs.usma.edu/courses/it105/. Last accessed 08 June 2011.

Kang, Cecilla. "Hundreds of Gmail accounts hacked, including some senior US government officials." Retrieved from Washing Post Web Site: http://www.washingtonpost.com/blogs/post-tech/post/google-hundreds-of-gmail-accounts-hacked-including-some-senior-us-government-officials/2011/06/01/AGgASgGH_blog.html. Last accessed 08 June 2011.

Kennedy, David, "The Social Engineering Toolkit." Retrieved from SecManiac Web Site: www.**secmaniac.com**. Last accessed 08 June 2011.

Ragan, Steve. "Three Military Contractors Linked to Post RSA Attacks" Retrieved from the Tech Herald Web Site: http://www.thetechherald.com/article.php/201122/7225/Three-military-contractors-linked-to-post-RSA-attacks. Last accessed 08 June 2011.

Social Engineer.Org, www.social-engineer.org. Last Accessed 08 June 2011.

Zeltser, Lenny "Phishing Messages May Include High Personalized Information." Retrieved from the Internet Storm Center Web Site: http://isc.sans.org/diary.html?storyid=1194. Last accessed 08 June 2011.