Journal of Digital Forensic Practice ›
Volume 1, 2006 - Issue 3: Phishing and Online Fraud, Part II

Report

The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond

Aaron Emigh

Pages 245-260 | Published online: 24 Feb 2007

Cite this article https://doi.org/10.1080/15567280601049985

Full Article | Figures & data | References | Citations | Metrics

Reprints & Permissions | Read this article | Share

ABSTRACT

“Crimeware” is software that performs illegal actions, unanticipated by a victim running the software, that are intended to yield financial or other benefits to the attacker. Crimeware is a ubiquitous fact of life in modern online interactions. It is distributed via a wide variety of mechanisms, and attacks are proliferating rapidly. For example, in the month of May 2006, at least 215 unique keyloggers—just one type of crimeware—were observed in the wild. Once installed, crimeware benefits the attacker in many ways, including theft of stored confidential data, denial-of-service extortion, spamming, click fraud, and aggregation of compromised information for further criminal activity. The installation and operation of crimeware and the varieties of countermeasures deployed suggest similarities of information flow and potential chokepoints.

KEYWORDS:

botnet | click fraud | crimeware | DNS poisoning | online fraud | hijacking | identity theft | keylogger | malware | pharming | phishing | piggybacking | ransomware | rootkit | screenlogger | transaction generator | Trojan | virus

Notes

*Aaron Emigh is Managing Director of Radix Labs, a security consultancy, and Executive VP of Technology at Six Apart, the world leader in blogging software and services. He serves on the US Department of Homeland Security-SRI International Identity Theft Technology council, the US Secret Service San Francisco Electronic Crimes Task Force, the Board of Directors of the Sierra Nevada Infragard Chapter, and the Board of Directors of Ravenwhite, Inc.

Disclaimer: This article is a Joint Report of the U.S. Department of Homeland Security—SRI International Identity Theft Technology Council, the Anti-Phishing Working Group, and IronKey, Inc. Points of view expressed in this document are those of the author and do not necessarily represent the official position of the DHS S&T Directorate or IronKey, Inc.

Adida, Ben, David Chau, Susan Hohenberger, and Ronald L. Rivest. Lightweight Signatures for Email. Draft of June 18, 2005; to appear.

Anti-Phishing Working Group. “Phishing Activity Trends Report: December 2005.” The Anti-Phishing Working Group, December 2005.

Close, Tyler. Waterken YURL: Trust Management for Humans. Waterken Technical Report, July 2004.

Emigh, Aaron. Online Identity Theft: Technology, Chokepoints and Countermeasures. Report of the Department of Homeland Security—SRI International Identity Theft Technology Council, October 3, 2005.

Financial Services Technology Consortium. “Understanding and Countering the Phishing Threat.” FSTC Counter-Phishing Project Whitepaper, January 31, 2005.

Heasman, John. “Implementing and Detecting an ACPI BIOS Rootkit.” NGS Consulting technical report, January 2006.

Herzberg, Amir, and Ahmad Gbara. TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks. Draft of November 11, 2004; forthcoming.

The Honeynet Project & Research Alliance. “Know Your Enemy: Tracking Botnets.” Report of the Honeynet Project, March 13, 2005.

The Honeynet Project & Research Alliance. “Know Your Enemy: Phishing.” Report of the Honeynet Project, May 16, 2005.

IEEE P1363 Working Group. “IEEE P1363.2: Standard for Password-Based Public Key Cryptographic Techniques.” IEEE Draft D20, March 28, 2005; forthcoming.

Jagatic, T., N. Johnson, M. Jakobsson, and F. Manczer. “Social Phishing.” To appear in Communications of the ACM, 2006.

Jakobsson, Markus. “Modeling and Preventing Phishing Attacks.” Phishing Panel in Financial Cryptography '05.

Jakobsson, Markus, Adam Young, and Aaron Emigh. Distributed Phishing Attacks. To appear.

Litan, Avivah. “Phishing Attack Victims Likely Targets for Identity Theft.” Gartner FirstTake FT-22-8873, May 4, 2004.

Morris, Robert T. “A Weakness in the 4.2BSD UNIX TCP/IP Software.” Computing Science Technical Report 117, AT&T Bell Laboratories, February 1985.

Rager, Anton. “Advanced Cross-Site-Scripting with Real-time Remote Attacker.” Avaya Labs Technical Report, February 9, 2005.

Rasmussen, Rod. “Phishing Prevention: Making Yourself a Hard Target.” Internet Identity/APWG, April 5, 2004.

Rescorla, Eric. “Optimal Time to Patch Revisited.” RTFM.com working paper.

RSA Security. “3rd Annual Opinion Research Corporation Security Survey.” RSA Security Report, February 14, 2005.

Stasiukonis, Steve. Social Engineering, the USB Way. Dark Reading, June 7, 2006.

Stewart, Joseph. “Win32.Grams E-Gold Account Siphoner Analysis.” LURHQ Threat Analysis Report, November 4, 2004.

United States District Court for the Central District of California. USA v. Jeanson James Ancheta. Grand Jury Indictment CR OS-1060 (February 2005).

Young, Adam, and Moti Yung. “Cryptovirology: Extortion-Based Security Threats and Countermeasures.” IEEE Symposium on Security and Privacy 1996.