proofpoint

June 23, 2015

Proofpoint Researchers Expose Underground Cybercrime Economy Triggering Surge in Malicious Macros

Leader in Advanced Threat Protection Uncovers the Cybercriminal Ecosystem Supporting the Recent Rise of Malicious Macros, Providing New Insight on Economic and Technical Drivers

SUNNYVALE, Calif., June 23, 2015 (GLOBE NEWSWIRE) -- Proofpoint, Inc., (Nasdaq:PFPT), a leading next-generation security and compliance company, announces the release of a report that exposes the economic and technical drivers behind the recent worldwide surge of malicious macros—many delivering the Dridex banking Trojan. Proofpoint's *The Cybercrime Economics of Malicious Macros* report highlights how cybercriminals have, in the last nine months, increasingly returned to cost-effective macros to reach more targets and see a greater return on their financial investment.

"Cybercrime is big business and criminals are increasingly exploiting people to circumvent automated protection systems," said Kevin Epstein, vice president of Advanced Security and Governance for Proofpoint. "Hostile actors are actively marketing malicious macros and tracking success rates—clearly they are a hot commodity. The logic is straightforward: malicious macros are effective and inexpensive, yielding better returns for attackers. Unfortunately, those economics mean malicious macros won't be going away any time soon."

Proofpoint's *The Cybercrime Economics of Malicious Macros* report combines technical analysis of malware samples from top malicious macro developers with investigation of underground cybercriminal forums. Results indicate that the high success rates and cost-effectiveness of malicious macros have rapidly and significantly altered the landscape of email-borne threats. Before the latter half of 2014, cybercriminals relied overwhelmingly on malicious URLs to deliver malware in high-volume unsolicited email phishing campaigns.

Tactics shifted significantly in September 2014 as organized cybercriminal phishing campaigns, spreading primarily the Dridex banking Trojan, adopted malicious Microsoft Word document attachments as their primary delivery vehicle. Heading into mid-2015, this trend continues to accelerate with Proofpoint researchers recording 56 different Dridex campaigns between April-May 2015 delivering, in some cases, several million email messages containing Dridex documents in a single day.

Six key findings from Proofpoint's *The Cybercrime Economics of Malicious Macros* report include:

- **Campaigns rely heavily on the human factor.** Deceptively simple and flexible malicious macros, which have replaced URL-based threats with attachment-based campaigns as the dominant threat, are rooted in their ability to use phishing techniques to exploit the human factor and trick an end user into clicking, thus avoiding many automated sandboxing checks.

- **Macros campaigns are increasingly sophisticated and evade many modern detection tactics including sandboxes.** Today's macroscampaigns are highly successful at evading not only traditional signature and reputation-based defenses, but also newer behavioral sandboxes.

- **Effectiveness is a primary driver.** The high success rates and cost-effectiveness of increasingly sophisticated malicious macros have driven the shift in malware-based email attacks.

- **Malicious macro attachment campaigns have grown in both size and frequency**. Proofpoint expects malicious macros campaigns will continue to grow until either the cost increases or effectiveness decreases to the point that significant ROI is no longer delivered.

- **Sophisticated actors lead the campaigns.** Although malicious macros offer a low barrier to entry for attackers, the predominant campaigns are still driving malware, including Dyre and Dridex. Only the most sophisticated attackers have the expertise to successfully utilize these campaigns.

- **Lower cost and high accessibility promote attacker success.** The budget for a malicious document (or "maldoc") campaign can range from zero to $1,000. Also, attachment-based unsolicited email campaigns may exceed exploit kits (EKs) in popularity. While there are a range of spamming services available, most EK services are sold in private circles and are not readily available to entry- to mid-level criminals.

The economics of email-based malicious macros underscore the fact that organizations can never underestimate the human factor—employees will almost always click. To successfully thwart today's modern attacks, organizations must deploy an advanced malware protection strategy that includes comprehensive threat intelligence and targeted attack protection that minimizes opportunities for end user interaction with phishing messages before they can click.

To download Proofpoint's *The Cybercrime Economics of Malicious Macros* report please visit www.proofpoint.com/us/id/PPWEB-Malicious-Macros. For more information on resources to manage today's evolving threat landscape, please visit: www.proofpoint.com/us/solutions/products/targeted-attack-protection

About Proofpoint, Inc.

Proofpoint Inc. (Nasdaq:PFPT) is a leading next-generation security and compliance company that provides cloud-based solutions for comprehensive threat protection, incident response, secure communications, social media security, compliance, archiving and governance. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system. Proofpoint protects against phishing, malware and spam, while safeguarding privacy, encrypting sensitive information, and archiving and governing messages and critical enterprise information. More information is available at www.proofpoint.com.

CONTACT: MEDIA CONTACT:

Patricia Hogan

Proofpoint, Inc.

408-763-3863

phogan@proofpoint.com

Source: Proofpoint, Inc.

News Provided by Acquire Media