Proofpoint Identifies New Class of 'Industrial Phishing' Attack

'Longlining' Attacks Employ Mass Customization to Penetrate Traditional Enterprise Security Defenses and Effectively Trick End-Users at an Alarming Rate

SAN FRANCISCO, CA -- (Marketwire) -- 02/26/13 -- RSA Conference Booth #739 - Proofpoint, Inc., (NASDAQ: PFPT), a leading security-as-a-service provider, today released the results of a wide-ranging study that identified a new class of sophisticated and effective, large-scale phishing attack dubbed "longlining." Longlining, which is named after the industrial fishing practice of deploying miles-long fishing lines with thousands of individual hooks, combines successful spear phishing tactics with mass customization. Using these techniques, attackers are now able to rapidly deploy thousands of unique, malware laden messages that are largely undetectable to traditional signature and reputation-based security systems.

Worse, despite their scale, these mass customized phish were effective enough to trick more than 10 percent of recipients into clicking on malicious content capable of taking complete control of PCs and compromising corporate networks.

Proofpoint was able to trace and defeat these attacks for enterprises using Proofpoint Targeted Attack Protection™, the company's recently introduced, big data protection solution.

Phishing Meets Mass Customization

Unlike conventional mass phishing exploits, the 'hooks' (email messages) used in longlining are highly variable rather than identical, making them largely undetectable to traditional signature and reputation-based security gateways. The messages are typically varied by IP address of origination, subject line and body content. The body content also includes multiple mutations of an embedded destination URL, which typically leads to a site with a positive reputation that's been successfully compromised prior to the attack. The compromised Web destinations are loaded with hidden malware either before, during or sometimes after the attack wave has begun.

Through the use of a distributed cloud of previously compromised machines and process automation to create high variance, attackers have been able to combine the stealth techniques and malicious payloads of spear phishing messages, all capable of bypassing traditional security. Attackers' ability to distribute thousands of email-borne malicious URL 'hooks' in a matter of hours greatly improves their odds of success and their ability to exploit zero-day defects before corporate IT has time to patch vulnerable systems.

"With longlining, cyber-criminals are combining the stealth and effectiveness of spear phishing with the speed and scale of traditional phishing and virus attacks," said David Knight, executive vice president of product management for Proofpoint. "Legacy security systems and techniques simply can't cope with this combination of speed and sophistication, leaving large enterprises increasingly vulnerable to a wide-range of criminal activity and data loss."

Typical Attacks

As part of the new, six month study, which involved over one billion email messages, Proofpoint observed, documented and countered dozens of longlining attacks globally. For example, on October 3, 2012, Proofpoint observed a Russia-based attack with 135,000 emails sent to more than 80 companies in a three-hour period. To avoid detection, the attacker employed approximately 28,000 different IP addresses as sending agents, 35,000 different 'sender' aliases, and more than twenty legitimate websites compromised to host drive-by downloads of zero-day malware. Because of the different agents, sender aliases, URLs and text, no single targeted organization saw more than three emails with the same characteristic. Overall, this attack represented less than 0.06 percent of the targeted companies' mail flow (compared to 19 percent for spam and 11 percent for virus-laden email). The combination of mass customization and proportionally low volume made this longlining attack effectively invisible to traditional anti-spam products, enabling widespread access to corporate networks.

Similar attacks were documented throughout the fourth quarter of 2012 and early 2013. In another representative attack, approximately 28,800 messages were sent in multiple one-hour bursts to over 200 enterprises. The campaign consisted of 813 unique compromised URLs sent from 2,181 different sending IPs. Again, each organization saw no more than three messages with identical content.
Despite their relatively large scale, longline attacks were alarmingly effective.

- Ten percent of the email messages containing embedded malicious URLs that escaped perimeter detection were clicked on by the receiving employees.
- All the longline attacks employed so call "drive-by downloads" installed on compromised web-sites. These attacks leverage browser, PDF and Java vulnerabilities to install "rootkits" invisibly with no user action required beyond clicking on the emailed URL and visiting the infected web-site.
- Almost one out of every five clicks (19%) on malicious URLs embedded in email occurred 'off network' when employees accessed their email from home, on the road, or via mobile devices where they were outside corporate perimeter protection.


About Proofpoint, Inc.

Proofpoint Inc. (NASDAQ: PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information. More information is available at www.proofpoint.com.

Proofpoint Targeted Attack Protection is a registered trademark of Proofpoint, Inc. in the U.S. and other countries. All other trademarks contained herein are the property of their respective owners.

Add to Digg Bookmark with del.icio.us Add to Newsvine

Media Contact:

Orlando DeBruce

Proofpoint, Inc.

408-338-6829

odebruce@proofpoint.com

Sarmishta Ramesh

Ogilvy Public Relations

303-527-4615

sarmishta.ramesh@ogilvy.com

Source: Proofpoint

News Provided by Acquire Media