FARSIGHT SECURITY

Solution Paper

# Spear Phishing: The '#1 Threat…'

## Introduction

A survey of 300 U.S. and U.K. companies (conducted by leading British technology research company Vanson Bourne on behalf of Cloudmark) revealed that in 2016:[1]

> *[…] almost two thirds of IT decision makers interviewed say spear phishing ranks as either their organization's top security concern (20 percent) or among their organization's top three (42 percent) security concerns.*

It's not hard to see why given other findings in that report, including:

- **The average cost of a spear phishing attack was $1.6 million dollars** -- obviously, criminal phishing gangs really like those big spear phishing "paydays."
- **84% of respondent had at least one phishing attack that penetrated their organization's security.** This demonstrates that criminal phishing gangs know how to tackle most traditional defensive measures you may be counting on for phishing protection.

### Traditional Defensive Measures -- Things Like A/V, User Training & Two Factor Authentication -- Just Aren't Good Enough Anymore

Phishing has been a problem for two decades,[2] but lately things have been getting worse, not better. Phishing volume is way up,[3] and the nature of phishing campaigns has evolved, too.

In the old days, identical poorly-written generic phish would get sent indiscriminately to anyone the phishers could find to spam. That was then. Today, phishing gangs tend to be much more sophisticated, often preferring to focus their efforts on a small number of high-value targets (such as senior executives, wire-transfer specialists at banks, privileged network administrators and so forth). Those targets then get sent carefully-crafted never-before-seen "spear phishing" messages tailored just for them, indistinguishable from a legitimate message from the company's CEO, a major customer, a crucial supplier, etc.

Spear phishing may not always work, but when a high-value target does mistakenly trust a message s/he shouldn't, the damage to the victim and the payoff to the phisher can be huge.

**That's why you need to take the fight against phishing to the next level with Farsight Security's new NOD product line.**

### Most New Domains Are Junk (Or Worse)

A couple of new effective-2nd-level-domains[4] get created on average, every second, all day long. While it would be wonderful if those domains represented the best the Internet could help to produce, all-too-often those newly created domains are of little value -- or out-and-out dangerous (like spear phishing domains).

Criminals count on being more agile than cyber defenders, creating new domains and immediately using them for attacks before domain reputation companies can notice and block them. So what's a site to do?

### Blocking ALL Newly Seen Domains For Minutes or Hours

Legitimate sites don't need their domain names to be accessible immediately after they're created. Criminals, on the other hand, have only hours -- sometimes just minutes -- to do their evil deeds before their domains get noticed and blocked.

That's a crucial difference. It allows sites like yours to safely block ALL newly observed domain names for minutes or hours, just long enough to give your existing domain reputation service provider time to assess those new domains, green lighting or permanently blocking them as appropriate.

See how Farsight Security's worldwide network of hundreds of sensors can help protect you during that brief but absolutely critical window of vulnerability. We can protect:

- Your email servers with our easy-to-integrate Newly Observed Domains (NOD) email blocklist, or
- All applications that rely on your company's DNS, using our NOD RPZ (Response Policy Zones).[5]

**Don't be one of those companies that makes a $1.6 million dollar mistake!**

[1] https://blog.cloudmark.com/2016/01/13/survey-spear-phishing-a-top-security-concern-to-enterprises/

[2] http://www.phishing.org/history-of-phishing/

[3] "The number of phishing websites observed by APWG increased 250% from the last quarter of 2015 through the first quarter of 2016," http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

[4] https://publicsuffix.org/

[5] https://dnsrpz.info/