Whaling

Anatomy of an Attack

Protecting Your Organization

from CEO Email Scams

mimecast® | making email safer for business

It's no secret that social engineering attacks, including phishing, spear-phishing and whaling, have grown from a nuisance to a colossal problem. A growing list of companies have been hit by these methods — sometimes to the tune of millions of dollars in data or financial losses.

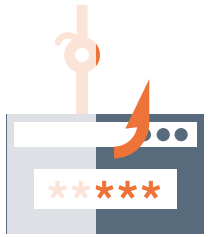
Whaling — derived from an analogy with a big "phish" — is particularly threatening because it's both highly deceptive and damaging. A cyber-criminal, disguised as the CEO, CFO or other senior executive, typically sends an email message to a recipient and convinces this person to initiate a wire or data transfer. These attacks are also referred to as impersonation attacks or business email compromise attacks.

Whaling schemes led to more than $2.3 billion in losses over the last three years, according to the Federal Bureau of Investigation (FBI).[1]

THE 5 PHASES OF A WHALING ASSAULT

1 In the crosshairs

Cyber thieves frequently rely on social media sites, such as LinkedIn™, to gather details about a high-level executive to impersonate along with a lower-level target. The target is typically a controller or human resources executive with the authority to request a financial transaction or send data without additional approvals. A key part of the scam is to make the target react to the perceived power of the spoofed executive.



55%
of organizations witnessed an increase in the volume of whaling attacks at the end of 2015.[2]

2 The domain game

Crooks register a domain that appears similar to the actual domain for a company. For instance, *testcompany* becomes "*testconpany*" or "*testcornpany*." This creates potential confusion. The busy target may not notice the fake domain.

70%
of whaling attacks involve domain spoofing.[3]

3 Gone phishing

The recipient receives an email message with his or her name on it, as well as other details that make it look authentic. This includes relevant details about the impersonated executive and likely mentions a specific business initiative.

72%

of whaling attackers pretended to be the CEO, while 36% were attributed to the CFO.[4]

4 Victim's assistance

To the target, the email looks authentic — and prompts for the specific action or transaction leading to a loss. The request usually has a sense of urgency and it may request that the individual bypass normal procedures.

43%

of organizations witnessed an increase in attempted sensitive data transfers involving whaling or CEO impersonation fraud over the last three months.[5]

5 On the money

In most cases, cyber thieves impersonating a high-level executive request a wire transfer or for the recipient to send tax data containing personal employee information, such as W-2 forms in the U.S. or P60 forms in the U.K.

41 companies fell for W-2 fraud in the first quarter of 2016.[6]

HOW BIG IS THE PROBLEM?

64% of IT security professionals regard email as a major cybersecurity threat to their business.[7]

65% don't feel fully equipped or up-to-date to reasonably defend against email-based attacks.[8]

WHY WHALING WORKS

Messages appear highly credible. They are well researched using social engineering techniques that exploit the natural human tendency to trust and be helpful. Messages use the right names, correct titles and have very similar-looking domain names. They are custom-written to avoid spam filters.

They appear to originate from the CEO, CFO or another senior executive and often request immediate action. They're almost always under the amount or threshold required for a second signature. In some cases, impersonation messages are sent by thieves when a key executive is on vacation — making an external or unknown domain name seem legitimate.

WHY WHALING WORKS

Only 15% of IT security professionals say their C-suite is "extremely engaged" in email security, while nearly half say their C-suite is only "somewhat engaged," "not very engaged" or "not engaged at all." [9]

The targeted company lacks essential authentication and controls, such as a second signature or sign-off on key transfers or transactions. Or, the recipient ignores key procedures for fear of raising the ire of the CEO or CFO. In many instances, employees are duped into thinking that checking on a transaction might slow things down and derail a key deal.

Organizations may lack essential security safeguards, including endpoint security, data encryption and email gateway technology to identify suspicious email.

ATTACKS IN MOTION

The list of companies that have fallen victim to whaling attacks continues to grow:

FACC: The Austrian aircraft industry supplier lost 50 million euros ($57.6 million), reportedly due to a whaling attack. Its stock fell 17% after the breach became public. [10]

Seagate: A successful whaling attack landed thieves up to 10,000 W-2 tax documents for all current and past employees. [11]

Snapchat: An employee fell for an email impersonating a request from CEO Evan Spiegel and compromised payroll data for 700 employees. [12]

Ubiquiti Networks: The high-performance networking tech company suffered a $39.1 million loss as a result of a whaling attack. The San Jose-based firm has recovered only a portion of the sum. [13]

Weight Watchers International: A whaling email allowed thieves to obtain tax data for nearly 450 current and former employees. [14]

SUCCESS STORY

Specialty recruitment firm Athona Ltd., based in the U.K., used Mimecast's Impersonation Protect cloud-based anti-whaling service to identify and block whaling emails — without generating false-positives. This helped protect the firm's reputation and reduced the risk of disruption and data theft.

6 WAYS TO HARPOON THE THIEVES

1 Educate and inform employees

Coach key employees to recognize an impersonation email and what steps to take to avoid falling victim to thieves. Train them to pick up the phone and verify a large transaction.

2 Use simulations

An effective method for detecting weaknesses and raising awareness is the use of tests and simulations. This takes the form of a staged whaling message that is intentionally sent to key individuals in the organization.

3 Make faking messages difficult

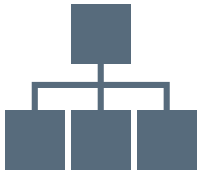
Customized stationery and unique identifiers contained in messages — as well as changes in design periodically — make it more difficult for cyber thieves to create convincing-looking emails.

4 Tap technology

A highly-effective method for thwarting thieves is advanced email gateway technology that identifies and, if desired, quarantines suspicious messages through the use of names, domains and keywords.

5 Stay alert

Monitoring and alert services that notify organizations when a new or different threat exists are also valuable. In today's fast-moving cybersecurity environment, hours and even minutes matter.



6 Rethink procedures

It may be necessary to change authentication and approval methods by adding a second signature or lowering the monetary amount required to trigger secondary approval. Multilevel authentication and approvals can greatly reduce risk.

67% of firms have witnessed **an increase in attacks designed to extort money** in the last three months.[15]

PLAYING IT SAFE

Social engineering attacks, including whaling, are increasing rapidly. Through a combination of awareness, simulations, technology, and better internal systems and processes, it's possible to dramatically reduce risks and build a cybersecurity foundation that better protects your organization from financial and data loss.

Over 90% of cyberattacks begin with email, and social engineering-led email attacks are growing rapidly.[16]

Mimecast Impersonation Protect is an essential layer of email security. Visit **Mimecast.com** to learn more about the **Targeted Threat Protection** service to protect your organization against catastrophic data and financial losses.

Sources

1 FBI, "FBI Warns of Dramatic Increase in Business E-Mail Scams," April, 4, 2016

2 Mimecast, "A Whale of a Tale: How to Stop the Rising Tide of Impersonation Attacks," 2016

3, 4, 5 Ibid

6 CSO Online, "Phishing attacks targeting W-2 data hit 41 organizations in Q1 2016," May 24, 2016

7 Mimecast, "65 Percent of Global Businesses Ill-Equipped to Defend Against Email-Based CyberAttacks," Feb. 17, 2016

8, 9 Ibid

10 ComputerWeekly.com, "$54m cyber fraud hits aircraft supplier share price," Jan. 22, 2016

11 KrebsonSecurity, "Seagate Phish Exposes All Employee W-2's," March 16, 2016

12 CNN.com, "Snapchat employee fell for phishing scam," Feb. 29, 2016

13 CSO, "Ubiquiti Networks victim of $39 million social engineering attack," Aug. 6, 2015

14 MSN.com, "Tax Forms: Cybertheft Schemes on the Upswing," April 4, 2016

15 Mimecast, "Industry-First Impersonation Protect from Mimecast Combats New Spike in Multi-Billion Dollar Whaling Threat," April 5, 2016

16 Ibid

ABOUT Mimecast

Mimecast makes business email and data safer for thousands of customers and millions of employees worldwide. Founded in 2003, the Company's next-generation cloud-based security, archiving and continuity services protect email, and deliver comprehensive email risk management in a single, fully integrated subscription service. Mimecast reduces email risk and the complexity and cost of managing the array of point solutions traditionally used to protect email and its data. For customers that have migrated to cloud services like Microsoft Office 365™, Mimecast mitigates single vendor exposure by strengthening security coverage, combating downtime and improving archiving.

Mimecast Email Security protects against malware, spam, advanced phishing and other emerging attacks, while preventing data leaks. Mimecast Mailbox Continuity enables employees to continue using email during planned and unplanned outages. Mimecast Enterprise Information Archiving unifies email, file and instant messaging data to support e-discovery and give employees fast access to their personal archive via PC, Mac and mobile apps.

To learn more, visit www.mimecast.com.