Anatomy of a Data Breach—How it Happens

Heather McCalley
Sr. Threat Intelligence Manager
HMccalley@Malcovery.com
– Hedda Litwin
NAGTRI Program Counsel and Cyberspace Law Chief Counsel

– Noreen Leahy
NAAG/NAGTRI Meeting Coordinator
Anatomy of a Data Breach—How it Happens

Background:

- Cybercrime is organized crime...sophisticated, highly distributed, well-funded, and widespread.
- Industry of cooperating professionals: malware writers, botmasters, spammers, carders, mules, re-shippers, etc.
Anatomy of a Data Breach—How it Happens

One reason we cannot stay ahead:

Our opponents are sharing information among themselves, such as:

– best exploits
– most-valuable target organizations
– newly-discovered vulnerabilities
– least-patched vulnerabilities
– most-efficient botnets, etc.

But most of US do not share so well.
Anatomy of a Data Breach—How it Happens

The state of the problem can be characterized by these facts:

• The **length of time between a security incident occurring and when the organization actually discovers the compromise is far too long.** Verizon’s *Data Breach Investigations Report*

• Most computers are not running **adequate anti-virus software.** Microsoft’s *Security Intelligence Report*

• Most organizations **do NOT have large operational security teams** to handle the onslaught of cyber threats. *Arbor Network’s Worldwide Infrastructure Security Report*

• Cybercriminals purchase logs from botmasters to **identify high-value targets** that they want to buy access to. *Fox-IT, Group-IB’s Anunak: APT Against Financial Institutions*

• Most breaches were caused by **malware.** *Ponemon’s 2014: A Year of Mega Breaches*
Anatomy of a Data Breach—How it Happens

Phishing Email Trends

44% of observed phishing emails were IT related, often attempting to impersonate the targeted company's IT department.

93% of phishing emails were sent on weekdays.
Anatomy of a Data Breach—How it Happens

- GOOGLE REPORT Nov. 2014
- Phishing is the main way people steal credentials
- Good phishing pages have a 45% success rate
- 20% of credentials used within 30 minutes
- Email is the primary phishing vector

Graphic from www.memeburn.com
“...sending 10 phishing e-mails approaches the point where most attackers would be able to slap a ‘guaranteed’ sticker on getting a click.”
Anatomy of a Data Breach—How it Happens

In a typical phishing attack, an attacker sends a specially crafted email message that typically appears to be from one of the many online services that a potential victim might use, but the message lures the victim to click on a link that will take them to a webpage that is used to inject malware into their device.
Anatomy of a Data Breach—How it Happens

Another type of phishing scam simply tricks the victim into entering their credentials into what appears to be a standard login screen for a particular service; when they do so, their account credentials are stolen.

If you gave up your email password (or) you re-use passwords, your other online services are then at risk of compromise.
Google Drive. Google Drive now supports multiple email providers. Keep everything. Share anything.
Select your email provider
Now, you can sign in to Dropbox with your email
Anatomy of a Data Breach—How it Happens

Fourth Quarter Malware Campaigns

- Malware Family
  - UPATRE
  - Dyre
  - Asprox
  - Cridex
  - Smokeloader
  - Neverquest
  - Andromeda
  - Keaytip
  - Cryptowall
  - Game-Over-Zeus
  - TinyBanker (Tinba)
  - Pushdo
  - Cutwall
  - Citadel
  - PonyLoader
  - KINS

- Number of Campaigns
- Chart showing campaigns by month:
  - December
  - November
  - October
Anatomy of a Data Breach—How it Happens

You have received a new fax. Date/Time: Fri, 6 Mar 2015 15:52:17 +0000 Number of pages: 59

Thank you for supporting your Better Business Bureau (BBB).

As a service to BBB Accredited businesses, we try to ensure that the information we provide to potential customers is as accurate as possible. In order for us to provide the correct information to the public, we ask that you review the information that we have on file for your company.

We encourage you to print this SBQ Form, answer the questions and respond to us. (Adobe PDF)

Please look carefully at your telephone and fax numbers on this sheet, and let us know any and all numbers used for your business (including 800, 900, rollover, and remote call forwarding). Our automated system is driven by telephone/fax numbers, so having accurate information is critical for consumers to find information about your business easily.

Thank you again for your support, and we look forward to receiving this updated information.

Sincerely,

Accreditation Services

---

Many large banks, software providers for smaller banks

NewEgg
GoDaddy
Monster
Indeed
SimplyHired
Verizon

LunarPages
Networksolutions
iWeb
AT&T
ThomsonReuters
LexisNexis Accurint
Email Attack on Vendor Set Up Breach at Target

The breach at Target Corp., that exposed credit card and personal data on more than 110 million consumers appears to have begun with a malware-laced email phishing attack sent to employees at an HVAC firm that did business with the nationwide retailer, according to sources close to the investigation.

Last week, KrebsOnSecurity reported that investigators believe the source of the Target intrusion traces back to network credentials that Target had issued to Fazio Mechanical, a heating, air conditioning and refrigeration firm in Sharpsburg, Pa. Multiple sources close to the investigation now tell this reporter that those credentials were stolen in an email malware attack at Fazio that began at least two months before thieves started stealing card data from thousands of Target cash registers.

Two of those sources said the malware in question was Citadel — a password-stealing bot program that is a derivative of the Zeus banking trojan — but that information could not be confirmed. Through a PR firm, Fazio declined to answer questions about the malware.

Spear Phishing Attacks Snag E-mail Marketers

Criminals have been conducting complex, targeted e-mail attacks against employees at more than 100 e-mail service providers (ESPs) over the past several months in a bid to hijack computers at companies that market directly to customers of some of the world's largest corporations, anti-spam experts warn.

The attacks are a textbook example of how organized thieves can abuse trust relationships between companies to access important resources that are then recycled in future attacks. According to multiple sources, the so-called "spear phishing" attacks in this fraud campaign arrived as virus-laden e-mails addressing ESP employees by name, and many cases included the name of the ESP in the body of the message.

The poisoned missives used a variety of ruses, but generally included an invitation to view images at a Web site URL included in the message — such as a link to wedding photos or an online greeting card. Recipients who clicked the links were redirected to sites that attempted to silently install software designed to steal passwords and give attackers remote control over infected systems.

Neil Schwartzman, senior director of security strategy at e-mail security provider Return Path Inc., said the spear-phishing attacks have targeted e-mail marketing companies that manage opt-in campaigns for some of the biggest corporate brands in existence.

Note to Readers: If you receive an email about this topic, be wary. If you did not request or opt-in to the e-mail list of the sender, do not click any links or attachments. You can un-subscribe by clicking the "unsubscribe" link on the e-mail. If you did receive, it is possible that someone has your e-mail address and is attempting to trick you into giving your password or credit card information.
Anatomy of a Data Breach—How it Happens