Phishing for Funds

Understanding Business Email Compromise

Keith Turpin
Chief Information Security Officer
Universal Weather and Aviation
March 2017

Introduction

Business Email Compromise (BEC):

Attacker poses as a legitimate person or business

Convinces victim to wire money to a fraudulent account or share sensitive information

Two ways to be impacted:

1. Receive fraudulent email
2. Be the impersonated sender in email sent to other organizations

The 4 Common Attack Scenarios

1. Supplier Account Change
   - A supplier requests funds be wired to a new account

2. Fraudulent Invoice
   - Company or government organization requests payment for products, services, taxes or other fees

3. Executive Transaction Request
   - An executive sends an email request for a time sensitive transaction
   - Usually requiring an immediate funds transfer
   - Often states it is a highly confidential transaction (*no telling anyone else*)

4. Executive Data Request
   - Executive requests the Human Resources, Payroll or Audit department to send them employee earnings statements, tax records or other personal information

How Bad is the Problem?

Business Email Compromise targets organizations of all sizes and in all sectors

22,000 victims have lost **3 billion dollars**

In 1½ years there was a **1,300% increase in reported losses**

Recon

Attacks are often highly targeted

Significant reconnaissance is conducted to:

- Understand an organization's business
- Identify partners and the nature of the relationship
- Collect information on organizational structure
- Discover the identities of senior executives
- Identify targets, especially new hires in key positions
- Collect logos, examples of documents and signature blocks

Information Resources

Where do attackers get the information they need?

Attackers can use tools like Maltego to automate information gathering

Corporate Websites

facebook

Malware Infections

Linked in

Dragnet Phishing

Friendly phone call

The Evil Plot Begins

Scammers need a point from which to launch their attack

1. Create an email spoofing app or use an existing service
   - Paid web services like Sharpmail
   - Downloadable tools like EMS - E-mail Spoofer
   - Use SMTP server to create your own

2. Acquire a lookalike domain
   - There are common variations and character substitutions
   - Be especially wary of long domain names

3. Compromise the user's account or device
   - Infect user's device
   - Exploit weak or reused passwords to gain access
   - Take advantage of an open mail relay

Spoof a Domain

Common techniques for domain impersonation include:

- Dropping a letter from long domain names

  john.doe@abacusproperty.com.au vs john.doe@abacuspoperty.com.au

- Substituting characters

  john.doe@singaporeair.com vs john.doe@singaporeair.com

- Using dashes or word combinations

  john.doe@kasikornbank.com vs john.doe@kasikorn-bank.com

- Using alternate top level domains

  john.doe@samsung.com vs john.doe@samsung.co

Wait... Who owns that?

Impersonated Registry

sinqaporeair.com

DOMAIN INFORMATION

Domain:
sinqaporeair.com

Registrar:
TUCOWS DOMAINS INC.

Registration Date:
2016-01-13

Expiration Date:
2018-01-13

REGISTRANT CONTACT

Name:
VistaPrint Technologies Ltd

Organization:
VistaPrint Technologies Ltd

Hosting services, like VistaPrint, are frequently exploited to launch spam and fraud attacks.

Real Singapore Air Registry

singaporeair.com

DOMAIN INFORMATION

Domain:
singaporeair.com

Registrar:
ASCIO TECHNOLOGIES, INC. DANMARK

Registration Date:
1995-03-16

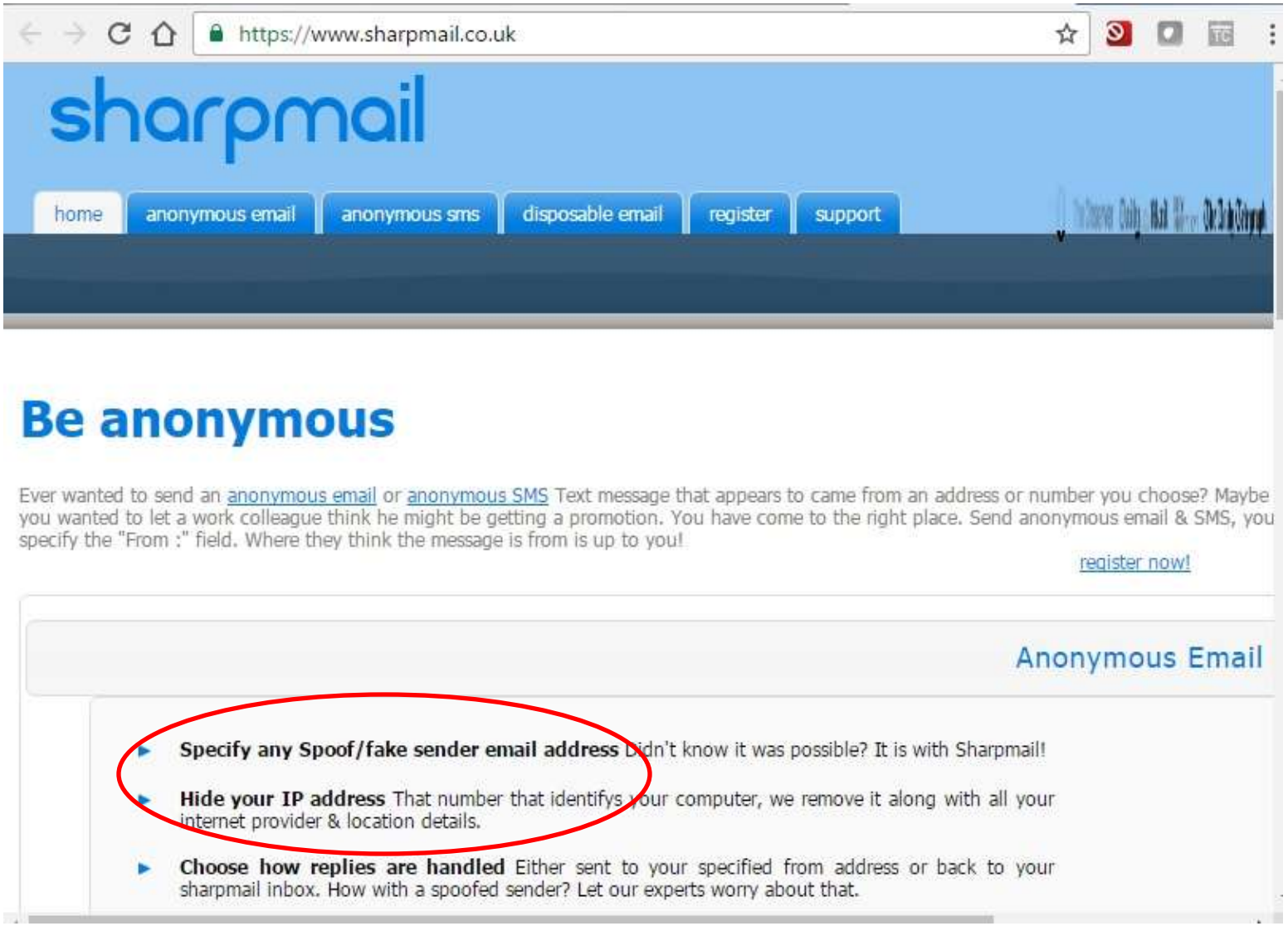
Expiration Date:
2019-03-17

REGISTRANT CONTACT

Name:
Domain Administrator

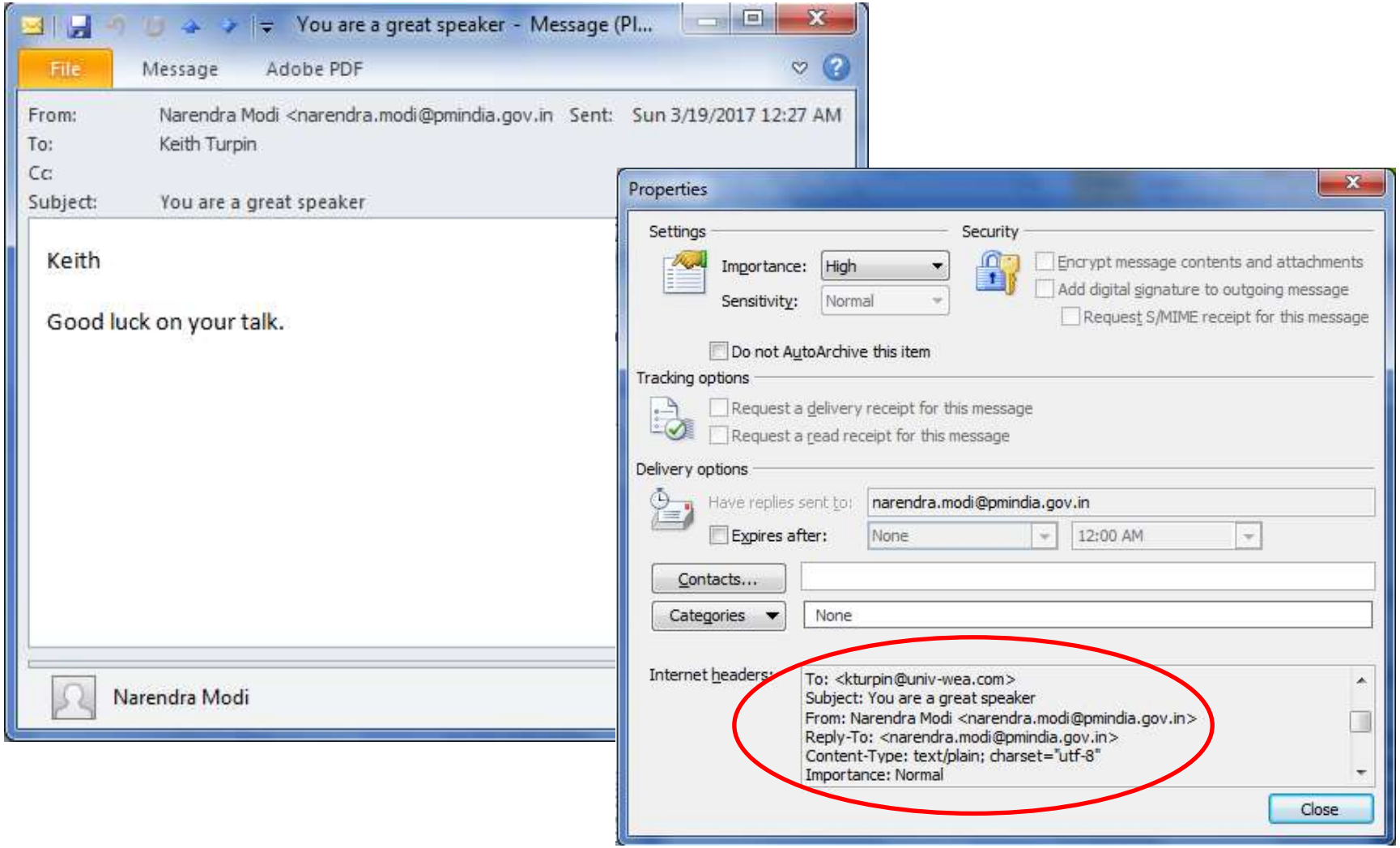
Organization:
SINGAPORE AIRLINES LIMITED

Email Spoofing as a Service



Spoofing Example

Even India's Prime Minister likes this talk...



Changing the Reply

Customizing Email Headers:

- The initial "From" field can show an expected email address
- The "Reply-To" field may be different, to enable conversations with the attacker

Below is an example of an altered Reply-To that is similar enough to fool users

- *NOTE: The attacker uses the domain name in both the "From" and "Reply-To" fields, but moves it*
  (Company name changed from actual incident)

Extract from the message header

Received: from localhost ([72.167.218.4])
User-Agent: Workspace Webmail 6.4.6
Message-ID: <.....wbe@email01.**godaddy.com**>

From: Brett Peter <brett@**cogswellcogs**.com>

Reply-To: Brett Peter brett.**cogswellcogs@mail.com**

This is what the user sees when they receive the email

This is the address that gets loaded when they reply

Hiding the Source

Open Mail Relays:

An SMTP server misconfigured to allow anonymous Internet use

- The "Received From" message header field will point back to the open relay server
- An attacker can use your own systems against you to spoof internal staff
- They can also target your business partners and the email will look like it came from you

Trusted Senders:

Attackers can host a domain with a shared hosting provider and have the same sending email servers and IP range as other companies on that provider

- Hosting provider IP ranges are generally considered trusted by email filtering services
- If both the attacker and legitimate business partners are hosted by a service provider, like GoDaddy, it makes IP blocking the sender impossible

Real Examples from a Financial Scam

Spoofing the President of the Company - 1st Email

I am informing you that we are in the process of acquiring a foreign company in order to expand our international business.

This project is supervised by the SEC (Securities and Exchange Commission) and any leak of information regarding that project will cause the cancellation of it by the markets authorities.

For the moment, only a couple of our finance directors are involved in this operation.

Can I count on your cooperation in this operation and so we will be able to lock this acquisition today?

Spoofing the President of the Company - 2nd Email

I appointed Mr. Gordon from Deloitte law firm to take care of this matter.

Mr. Gordon will supervise the correspondence between us and the targeted company.

In order to lock this acquisition today, we must proceed to a first deposit of 325,000.00 USD.

He will get in touch with you shortly to explain you all the procedure and to provide you with the necessary bank details to proceed to the payment today.

I will be in some meetings all day regarding our matter, please update me via email.

- *NOTE: These two emails were followed by a call to the intended victim from "Mr. Gordon", but the finance person involved, quickly realized that Mr. Gordon did not have a good grasp of the organization or business. They disconnected from the call and reported the incident to management and security.*

PII Fraud Scams

Payroll and HR offices are targeted by cybercriminals posing as company executives in order to get payroll data and tax forms

Messages can be short and simple, like the following:

> Kindly send me the individual 2015 W2s and earning summaries for all of our company staff for a quick review.

Seagate finds itself in the News:

Bloomberg BNA

Seagate Technology, learned March 1, 2016 that an employee who thought a phishing e-mail was a legitimate internal company request sent information on 2015 Forms W-2 for current and former domestic employees to an unauthorized third party.

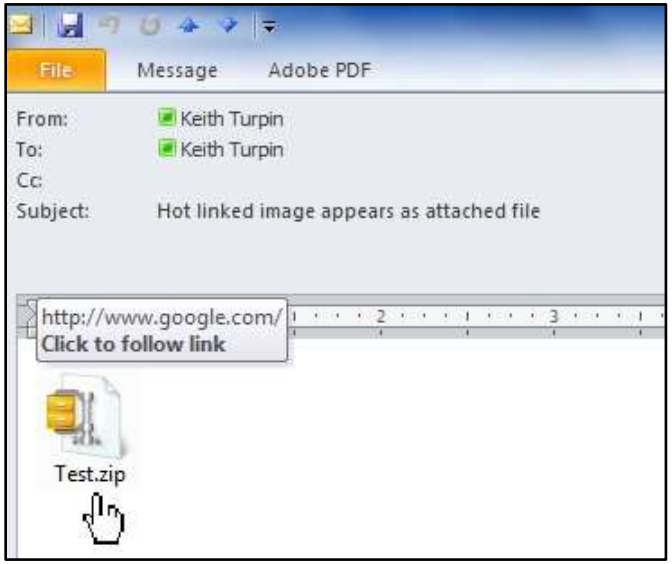
Sneaking Past Filters

How did that .Zip get through the filter?

We have seen an uptick in attackers attempting malware infections through links embedded in files or images

- *These often get past traditional email security filters*

The look-a-like attached document is really an image with an embedded link



Files are attached to email with misleading links to malicious sites

Mounting a Defense

Business Email Fraud is a like a three legged stool that relies on multiple exploit paths to succeed:

1. People
2. Business Process and Policy
3. Technology

Break any one leg, and you can stop the scam

People - Ignorance Is Not a Defense

Topics for new employee and annual training

1. If it doesn't feel right, report it
2. Carefully review the "From" in original emails and "To" when replying
3. Be wary of messages that:
   - ✓ Involve fund transfers
   - ✓ Ask for sensitive information
   - ✓ Press for urgent action
4. Never enable macros in documents that are received via email
5. Always validate unusual fund transfers and information requests using a separate, previously established contact
6. Hover over links to validate path of destination

NOTE: This may not apply if your email security gateway does URL re-writing

Process & Policy - Provide Guidance

Establish formal policies for:

- Managing wire transfers
- Changes in banking accounts
- Sharing sensitive information through non-standard requests

  ✓ *Business processes must match policy requirements*

Train staff on the policy and procedures

Test your staff's compliance through phishing services:

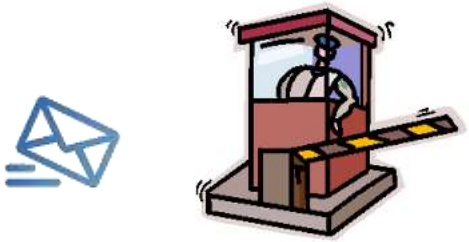
- phishme.com.....service
- phishlabs.com .....service
- ironscales.com .....service

Free Phishing tool:

- MSI Simple Phish.....microsolved.com/free-tools.html

Technology - Email Security Gateways

Email security gateways monitor email traffic



Defend against email attacks using a combination of techniques:

- Check message source for known bad IP or Domain
- Inspect the SMTP headers for inconsistencies
- Correlate the SMTP headers with SPF, DKIM, and DMARC
- Check attachments for known malware

Some providers offer additional services for zero day protection

- *Examples: ProofPoint Targeted Attack Protection & Microsoft Advanced Exchange Online Protection*

- Sandbox behavior analysis to detect new malicious files
- Link analysis and malicious site blocking

Technology - SPF, DKIM and DMARC

(SPF) Sender Policy Framework:

Looks up the domain in the "Return-Path" (the SMTP envelop sender) and verifies that the corresponding IP is authorized to send email for that domain

- Does not prevent attackers from spoofing the message "From" address
- Often spoofed when scammer has a domain in shared hosting environment (*Trusted Sender*)

(DKIM) DomainKeys Identified Mail:

Digitally signs emails and the receiver runs a DNS query to get the public key from the sender domain

- Does not prevent attackers from spoofing the message "From" address
- Limited by low adoption rate due to implementation complexity

(DMARC) Domain-based Message Authentication, Reporting and Conformance:

Builds upon both the DKIM and SPF specifications

- Verifies the "From" domain matches the "Return-Path" domain checked by SPF
- Verifies the "From" domain matches the “d= domain name” in the DKIM signature

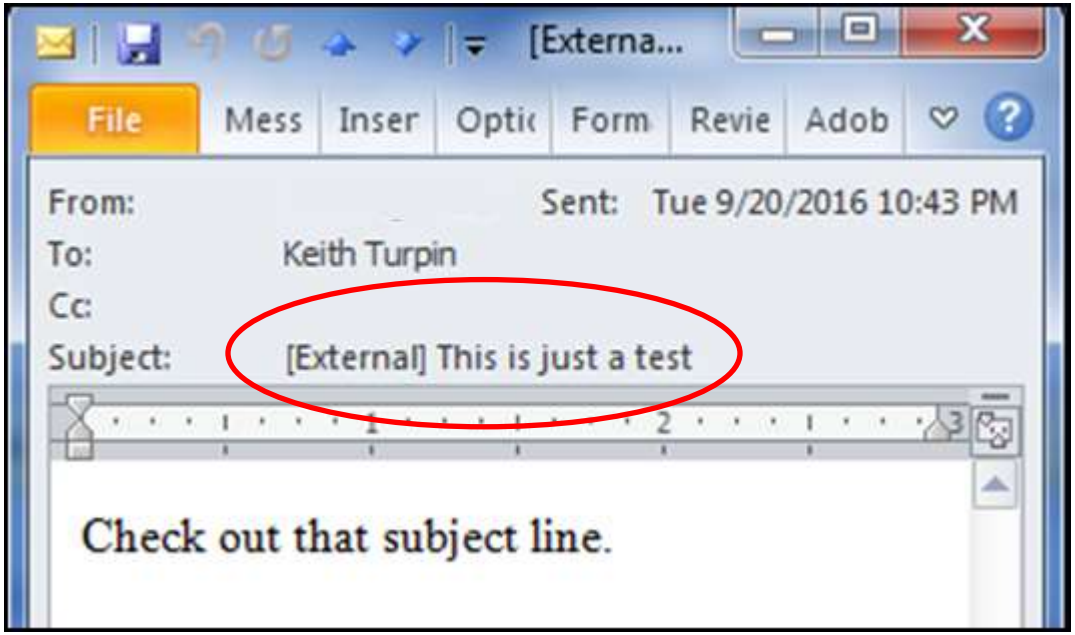
Technology - Marking External Email

Using Exchange Transport Rules to Mark Incoming Email

Add **[External]** to the beginning of the subject line for all messages sent from outside of organization

- *You could alternately add text to the top or bottom of the message body*

This provides a clear visual cue for users



NOTE:
Use an addition outbound transport rule that strips [External] from replies

or

Add an exception to the incoming rule that looks for [External] and does not re-add it during a conversation

Technology - Block Spoofing IPs

Exchange and many email security gateways support rules for blocking external email impersonating your domain

- These rules typically use a blacklist
- Create exceptions for external organizations authorized to impersonate your domain
  - ✓ *Be sure to allow sufficient time to monitor and identify external senders*
- Rather than delete these emails, you may want to redirect them to a security team mailbox for review

See Supplemental Material

Technology - If It Gets Through, Delete It

Deleting with Exchange Management Shell

Exchange Management Shell can be used to conduct searches across an entire organization and delete email before users are exposed

- Wide scale removal of malicious email is a valuable incident response technique when email defenses have failed
- Use caution doing mail cleanups or you may find legitimate email disappearing
- The key to successfully finding and deleting the emails is using multiple searches and always running reports to validate what email will be deleted

See Supplemental Material

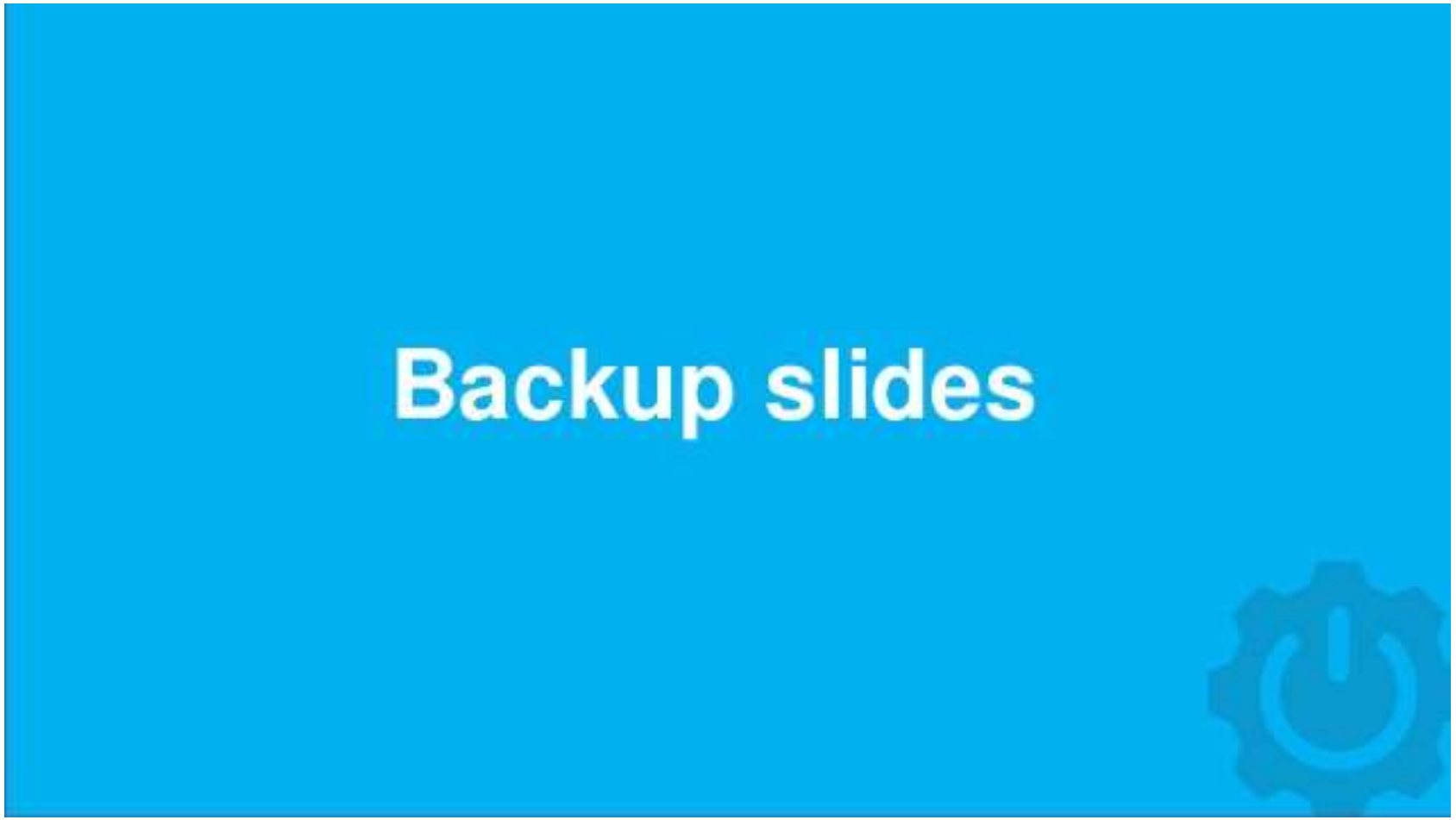
Report IT

It is important to act quickly if you suffer a financial loss:

- Contact your financial institution immediately
- Request that your financial institution contact the corresponding financial institution where the fraudulent transfer was sent
- Contact your local government agency assigned to address cyber crime
  - *They might be able to help return or freeze the funds*
  - *Actions taken in the first 72 hours are critical*

Questions

More Useful Information



Process - Keep Everyone Informed

When malicious email gets through, let people know

Establish a standard notification template to send to affected users

Sample Notification

Please Read - Important security message!

A malicious email was sent to you, from "**<<Insert sender>>**".

The subject line was "**<<Insert Subject Line>>**"

The email contained a **<<malicious attachment / link to a malicious website>>**.

If you **<<opened the file / clicked the link please>>**, please contact IT Security immediately so that we can insure the PC is not infected.

Our email system administrators will be removing this email from all accounts affected by this incident. By the time you see this email, the malicious email may already be removed from your inbox.

If the file is still in your in box, **do not open it; please delete it right away**.

Thank you for helping keep the company safe.

- *Use periodic informational bulletins to raise awareness of specific scams that users may be exposed to*

Process - Sample Security Bulletin

Attached is an example of the types of bulletins I send out about once a month

Topics range from issues affecting business to security issues that help people be more secure in their personal lives

IT Security Bulletin
Aviation Industry Email Scams

Date: September 13, 2010
Audience: All Employees and Contractors

Beginning about a year ago, the business aviation industry became increasingly attacked by cyber criminals attempting to commit fraud and infect PCs with malware via multiple e-mail phishing scams. We've recently seen a further ramp up of this activity, including several attempts targeting our clients.

The National Business Aviation Association recently published an article warning its members of these threats.

The most common threats are what are referred to as phishing schemes. In phishing scams, someone poses as a legitimate person or business in order to obtain information such as login credentials, or banking information, or to otherwise compromise your computer. A phishing target may receive an email message that appears to have been sent by a known associate or well-known organization like NBAA, which we have seen happen. Links or attachments in the message may appear harmless, but when they are clicked on or opened, they may trick the recipient into providing personal or financial information, or infect their computer with a virus.

What you need to do
Contact IT Security immediately if you:

- Receive an e-mail you believe to be suspicious and a possible phishing scheme
- Speak to a client who is concerned they may be receiving e-mails impersonating you or someone else at the Company
- Read the tips below on how to help identify malicious cyber threats and prevent them from infecting your computer or gaining access to sensitive information

How you can spot a scammer

- Be wary of unusual messages that ask for sensitive information, or ask you to provide information urgently.
- Confirm an email is legitimate before opening any attachments.
- Never enable macros in documents that are received via email.
- If an email requests sensitive information or requests were transfers to a new account, be sure to follow company process to validate these requests are legitimate and authorized.

Again, if you believe you have been compromised or have any further questions, please alert the IT Security immediately. You may need to change your passwords, or turn off your computer until you can get assistance.

Regards,

Technology - Exchange Spoofing Protection

Add your own domain to the list of blocked senders in Exchange 2013, Exchange 2016, or Office 365

1. Go into the Admin Center >> Exchange
2. Click on the mail flow section, then click the **+** sign
3. In the right-hand area and select “Create a new rule…"
4. Name your new rule
5. Click on "more options"
6. Choose “Apply this rule if…” and select "The sender is internal/external"
   - Select the location of "outside the organization"
7. Add a condition and then choose “The sender's domain is” and input your company’s email domain(s)
8. Choose what happens under "Do the following..."
9. Add IPs of authorized senders in the "Except if..."

Technology – Deleting with Exchange Management Shell

One common mistake is deleting too many emails as malware often has subject lines that will match many other legitimate emails. There will also be cases where malware is sent from a user that has been compromised, but also sent legitimate emails. So it is not always best to delete all emails sent form a particular address.

The key to successfully finding and deleting the emails is to run a report on the data that will be deleted before doing the deletion and ensuring that you have narrowed your target deletions to only the targeted threat. Sometimes it is much faster to do several searches and deletes instead of trying to catch everything at one time because complicated searches on Terabytes of data can be excruciatingly slow. It is often better to keep the search very simple.

The following are examples of searches we might perform to find, report, and delete emails:

Get-Mailbox -ResultSize Unlimited | Search-Mailbox -SearchQuery {Subject:"Your online order was successfully submitted. Thank you!"} -Logonly -LogLevel Full -SearchDumpster -TargetMailbox administrator -TargetFolder Inbox

ResultSize Unlimited – Exchange limits searches by default to 1000 mailboxes. If your organization has more than 1000 mailboxes, this command expands the search to all mailboxes:

{} – on the inside of these characters, is the term you will be searching for. The most common searches will be done by Subject, To, From, or Date
Logonly – this tells the search to take no action except to log the results
LogLeve Full – This is the extent of the log you want to create
SearchDumpster – This operator expands the search to not only deleted items, but to deleted, deleted items. This is a good practice so malware is not accidentally recovered by a restore
TargetMailbox – This is the mailbox you would like the report mailed to
TargetFolder – this is the folder inside the mailbox you would like the report placed in

Technology - Using Exchange Management Shell-2

The following is an example of a compound search using the AND operator:

Get-Mailbox -ResultSize Unlimited | Search-Mailbox -SearchQuery {Subject:"Your online order was successfully submitted. Thank you!" AND To:"rvasami@univ-wea.com"} -Logonly -LogLevel Full -SearchDumpster -TargetMailbox administrator -TargetFolder Inbox

Both of these searches will email a csv that can be opened in excel and examined to ensure the search captured the data you would like to remove. The following is the command to use after you have assured you want to delete the data:

Get-Mailbox -ResultSize Unlimited | Search-Mailbox -SearchQuery {Subject:"Your online order was successfully submitted. Thank you!"} –DeleteContent

Or

Get-Mailbox -ResultSize Unlimited | Search-Mailbox -SearchQuery {Subject:"Your online order was successfully submitted. Thank you!" AND To:"rvasami@univ-wea.com"} -DeleteContent

Useful Resources

Checking Risky Attachments

- Virus Total (file and website scanning): https://www.virustotal.com
- Malwr: https://malwr.com/
- Sucuri SiteCheck (website checker): https://sucuri.net/scanner/

Email Blacklist Checking Sites:

- Barracuda Reputation Block List (BRBL): http://barracudacentral.org/rbl
- SORBS SPAM Blacklist: http://www.sorbs.net/lookup.shtml

Open email Relay testing tools:

- Mail Radar: http://www.mailradar.com/openrelay/
- MX Toolbox: http://mxtoolbox.com/diagnostic.aspx
- DNS Goodies (lots of site analysis tools): http://dnsgoodies.com/

Domain Lookup Tools:

http://www.whois.com
https://whois.icann.org

Anti-Phishing Working Group (APWG)

- APWG's membership includes more than 1800 institutions worldwide: http://www.antiphishing.org/

Best resource for information on SPF, DKIM and DMARC:

https://blog.returnpath.com/how-to-explain-spf-in-plain-english
https://blog.returnpath.com/how-to-explain-dkim-in-plain-english-2
https://blog.returnpath.com/how-to-explain-dmarc-in-plain-english