Document Title

Mitigation of Phishing Campaigns		
CATEGORY: SOCIAL	ID: 10001-INV-USER-SOCIAL	OWNER:
	DATE: MM-DD-YYYY	AUTHOR:

Objective Statement

This playbook provides instructions for handling end-user reported phishing campaigns against <company name> employees. The goal is to prevent the introduction of backdoors into the company infrastructure, which may lead to data theft and reputation loss.

Scope and Applicability

Phishing emails against <Company> employees

Methodology and Procedures

The following paragraphs elaborate the instructions to be carried out by the IRT – Incident Response Team.

Table of Contents

Handling Employee Phishing Reports1

Investigation

Step 1: Get IoCs 2

Step 2: Is it a Campaign? 3

Response:

Alerting Employees 4

Flagging "Bad" Emails 4

Removing Emails from User Inboxes 4

Blackholing DNS 4

Blocking Download URL 4

Report Malware 4

Deploy AV Signatures 4

Final Steps 1

Handling Employee Phishing Reports – Incident Response Part

1. Check the *spam@<companyname>.com* inbox at least every hour for employee reports
2. If a new report comes in, create a new ticket in <Ticket System or Excel>.
3. Obtain the original email from the end-user and attach it to the ticket
4. Validate the email whether it is a phish
    1. Check the hostname part of all links in the email within the following toolsets:
        - https://otx.alienvault.com
        - Virustotal
        - IBM Xforce Exchange
    2. Check the URL inside the link by hovering over it, is it the same? (e.g. *www.ebay.com*) ?
    3. Does the email try to evade SPAM filters?
    4. Does the sender seem to be forged?

If the email is a false positive, thank the user for the report and resolve the ticket. Otherwise, continue with the instructions below.

Investigation Step 1: Get IoCs

Collect and record the IoCs below into the <Ticket System or Excel> ticket.

1. Full download URL(s) from the email
2. Hostname from URL
3. Visit http://www.kloth.net/services/nslookup.php and get the IPs belonging to the hostname
4. Do reverse lookup and record the PTR record
5. Connect to Sandbox Environment or Fire up a Linux VM, curl the URL to retrieve the file
    1. Calculate the md5 and sha256 hashes
    2. Pack the file with "zip" on the VM and encrypt it with the password: "virus"
    3. Copy the zipped file to your desktop with scp
    4. Attach file and hashes to the JIRA ticket
6. Subject link of the email
7. Sender of the email
8. Hostname and IP address of the sender's SMTP server

Investigation Step 2: Is it a Campaign?

Search <Ticketing System or Excel> for emails with similar senders, subjects, contents or URLs

1. If this is the first phish in a new campaign, skip to the next paragraph
2. If the phish is part of a campaign
    1. Create a master ticket (if necessary) in <Ticketing System or Excel>
    2. Relate new ticket to master ticket
    3. Associate related tickets with the master ticket

Alerting Employees

If this is the <x> ticket/report related to the master ticket in <Ticket System>, we need to warn our end-users of the emerging threat.

1. Go to <\xzy – OneNote> and take the pre-approved email template and canned message
2. Fill in the appropriate details
3. Send the template to the internal PR on communications@<company name>.com
4. Give the PR team a call on #12345 and let them now we have a pre-negotiated incident situation here and the company-wide alert should go out ASAP.

Block Emails on the SMTP Server

As the phisher can easily change the subject line or sender of the emails, try to find a common pattern in the email headers of the related emails. For instance, all emails might share the *X-Mailer:* and *X-PHP-Script:* headers.

1. View the source of the original phishing emails under the master <Ticket System> ticket
2. Try to find common patterns

If you manage to find a some common attributes, contact IT Email Support and request to block all incoming emails based on the identified pattern.

Flagging "Bad" Emails

Send the original email to IT Email Support asking them to feed it to the company's Bayesian SPAM filter.

Removing Emails from User Inboxes

Check the SMTP logs whether the same email has been delivered to other users. Engage IT Email Support in removing similar emails from the affected employee mailboxes.

1. Go to <company SIEM, Email eDiscovery, or IR Tool>
2. Search for the subject line from the original phish
3. Search for the sender email address from the original phish
4. If you identify other recipients in the SMTP logs
    1. Export affected recipients into a CSV file
    2. Contact IT Email Support and ask them to remove the phishes from the affected mailboxes

Blackholing DNS

We have a pre-approved process with IT and other parties to hijack certain DNS requests on the domain controllers by resolving them to 127.0.0.1

1. Go to https://otx.alienvault.com or similar threat information services.
2. Pivot on hostname and collect related hostnames
3. Contact IT Support and send them the list of hostname IoCs to be blackholed

Blocking Download URL

This process will block the dropper to be downloaded if a user clicks on the malicious URL in the phish.

1. Try to identify a pattern in the URL. For example if the URL is: http://hackedwebsite.com/dl.php?campaign=ra&id=12731342834923919

2. Create a reasonable regex like: ^.+/dl.php?.*campaign=ra.$
3. Contact the proxy team at proxy@<company>.com to block URLs based on the pattern

Report Malware Sample to ISAC or Microsoft (or similar services)

Send the sample to ISAC to get the updated malware signature, which will block users from opening files already downloaded (unless the malware file mutates).

1. Send the malware sample from the <ticketing system> ticket to malware@malware.<isac>.com

Deploy AV Signatures or Additional IoC (your choice of AV)

If AV Vendor replies with the additional signature file, we push it out to the endpoints as the following:

1. AV Signatures
    1. Take the *dat* file received from <AV Vendor> and attach it to the ticket
    2. Send the *dat* file to IT Engineering and ask them to push it immediately
2. Hash Files
    1. Take the *dat* file received from <AV Vendor> and attach it to the ticket
    2. Send the *dat* file to IT Engineering and ask them to push it immediately

Final Steps

We use the Mitigation of Phishing Campaigns runbook to block further emails coming in

1. Open a new [Ticketing System] ticket
2. Add the IoCs to the new ticket
3. Link the old ticket together with the new ticket
4. Resolve the old JIRA ticket
5. Open the Mitigation of Phishing Campaigns (**10001-INV-USER-SOCIAL**) playbook from the playbook repository
6. Block emails part of the phishing campaign by following the instructions in the other playbook