NCCIC
National Cybersecurity & Communications Integration Center

NCCIC ADVISORY

TARGETED PHISHING ATTACKS

April 6, 2011

SUMMARY

This advisory is intended to provide general guidance to public and private sector organizations on events potentially triggering targeted phishing attacks (often referred to as spear phishing) and to offer some suggested methods that may minimize the likelihood of a successful attack. This advisory is in response to several recent events; however the Department must maintain the anonymity of affected parties.

TRIGGER EVENTS

The following is a list, though non-exhaustive, of business activities and products that could be leveraged by an adversary to develop targeted emails addressed to individuals within an organization. These targeted emails are typically used as a catalyst to sway individuals into clicking on hyperlinks or opening attachments, thus allowing adversaries to download malicious content to the user's device and gain unauthorized entry into the organization's network.

- Media Release
- Business Mergers and Acquisitions
- Business Reports/Stock Reports/Financial Statements
- Competing for Contracts
- Awarded Contract
- Technological Breakthrough
- International Dealings
- Any other public information of interest to malicious actors
- Natural Disasters
- Referred to by other parties in their Public Release Statements
- Government/Industry Events
- Government or Industry Work Stoppages
- International or Political Events

RECOMMENDED MITIGATION STRATEGIES

The following mitigation strategies are intended to help our public and private partners proactively look for possible intrusions as part of a larger defense in depth strategy:

1. Log unsuccessful email attempts, both incoming and outgoing. Spear phishers often have to guess the mail format (i.e. firstname.lastname@xyz.com, lastname@xyz.com, FLastname@xyz.com, etc) therefore it is likely the mail server will reject mis-formatted emails. This is probably the first sign your organization may be targeted. By reviewing logs shortly after trigger events, it is possible to learn whether attempts are being made and thus new rule sets can be created to block the sender and alert the individual they are being targeted. Also, if it is determined an attack against an individual or group is possibly occurring, notify the individual or group to be more aware of the threat.
2. Log network traffic (both incoming and outgoing), especially surrounding a possible trigger event. If a successful attack occurs, network administrators will potentially see an increase in outbound traffic soon afterwards, thus indicating compromise of the network. Diligent monitoring of inbound and outbound traffic will also provide insight into new or unexplained network traffic and allow network administrators to create rule sets to block or minimize exfiltrated data.
3. Alert your IT/CIO staff prior to trigger events. By alerting network administrators prior to a press release, for example, will afford the opportunity to maintain increased network vigilance shortly afterwards. Large volumes of traffic on most networks preclude constant high alert monitoring, but by monitoring prior to and shortly after a trigger event, it narrows the bandwidth to be searched for malicious activity.
4. Notify affected parties within your organization that their contact information may be made public in some form. Prompt employees to be on the lookout for possible phishing attacks that directly relate to the trigger event.

DHS' United States Computer Emergency Readiness Team (US-CERT) encourages the public to use safe, common sense cyber practices, such as not opening emails from an unknown individual or organization, using spam filters and firewalls, running anti-virus and anti-spyware software and keeping them updated regularly. For more information, visit www.us-cert.gov or the Federal Bureau of Investigation’s (FBI) ‘Be Crime Smart’ website at:

http://www.us-cert.gov/reading_room/emailscams_0905.pdf
http://www.fbi.gov/scams-safety/

POINTS OF CONTACT

Please direct questions concurrently to the NCCIC and its appropriate component listed below:

NCCIC	US-CERT	NCS/NCC	ICS-CERT
NCCIC@HQ.dhs.gov	SWO@US-CERT.gov	NCS@HQ.dhs.gov	ICS-CERT-SOC@dhs.gov
(703) 235-8831	(703) 235-8832/8833	(703) 235-5080	(877) 776-7585