Fall 2012 Spear Phishing Incident – Executive Summary

Prepared for ITCC Security Subcommittee by S&T Information Technology

Incident Overview and Impact

During fall 2012, the Missouri S&T campus, the University of Missouri system, and many other universities across the nation suffered an ongoing series of spear phishing attacks designed to damage credibility in the Universities and exploit their email systems. These attacks consisted of incoming email messages designed to look like official S&T communiqués to trick vulnerable users into providing their campus userid and password. There were resulting compromised email accounts that were then utilized to send outgoing spam, monitor official S&T communications, and launch additional spear phishing attacks.

During the active phase of the attacks, IT discovered the phishers were monitoring our outgoing official communications to replicate our style to better disguise their subsequent emails. Adopting methods from peer institutions and companies suffering similar, concurrent attacks, we immediately ceased mass (campus-wide) email communications. We directed our communiqués to identified executive representatives. After ensuring these accounts had not been compromised, we sent targeted communications and asked that the recipients accept the responsibility of delivering our message to their constituents and personally reiterate the urgency and importance of email security.

The large amount of outbound email spam from the UM-wide compromised accounts resulted in the placement of the entire UM system on spam blacklists. These lists are used by email providers to prevent spam from entering their domains. Once the university was placed on one or more of these blacklists, the subscribing domains would block all emails from the offending domain (us) with or without notice to the sender and recipient. There are a wide variety of blacklists and related restrictions most of which require manual intervention for a domain to be removed or 'unblocked.' It can take 24 hours or more to get off most email blacklists, so it is critical for email providers to prevent large amounts of spam from leaving their systems in the first place.

Emergency measures to restore reliable email services were prioritized to reduce impact to users of the preferred, secure Exchange environment. Additional efforts were established to protect the more vulnerable environments by minimizing the number of outbound messages per minute and the number of recipients per message sent by users using the SMTP protocol. SMTP is typically used by POP and IMAP email clients to send outbound email. As a result of these limits, email clients using POP and IMAP became unreliable in sending email. Users would sometimes successfully send email and other times would get errors sending email or would silently fail so the user thought the email was sent. As of Dec 10th, 2012, 1725 staff pop/imap users across all of UM were impacted, 223 of those at S&T.

Throughout the POP/IMAP restrictions, faculty and staff using Exchange clients, such as Outlook or owa.mst.edu, were not affected by the emergency measures. Efforts were made to direct POP/IMAP users to utilize the web interface (owa.mst.edu) or an Outlook client as a more stable and secure alternative.

Incident Overview and Impact (continued)

Spear phishing attacks from the web occur throughout the year, but during the month of October 2012 it is reported that they increased over 1200%. Typically, the University experiences less than a dozen compromised accounts annually. Due to the increased volume and targeted nature of the October 2012 attacks, over 50+ accounts were identified as compromised during the month of October alone. There is still suspicion that compromised 'sleeping' accounts may still exist within our environment that continue to eluded detection.

Before and since the attacks of October 2012, IT continues to diligently monitor for attack, are prepared to react as needed, and are in the process of assessing our response to aim for improvement.

Timeline of Events and Actions

Tue. Sept. 25 UM reported upcoming blacklist blocks to S&T IT Staff

Mon. Oct. 1 **S&T received spear phishing attack**

Wed. Oct. 3 **S&T received spear phishing attack**
Chronicle published "Hacker Group Breaches Thousands of University Records to Protest Higher Education"

Fri. Oct. 5 Informed S&T IT staff of mst.edu placement on limited blacklist
Began investigation of blacklist impact and remediation process, addressed issues on case-by-case basis

Sat. Oct. 6 *3:45 am* - **S&T received *widespread* spear phishing attack**
8:00 hour - Blocked link, reported to hosting company
Began work with campus communications department for notification
9:58 am - Deployed email notification to all S&T employees and students
Encouraged users to verify suspicious emails with Help Desk
1:04 pm - **S&T received spear phishing attack, emulating OWA**
Initiated technical assistance efforts on compromised accounts

Mon, Oct. 8 Exchange team report shared with S&T IT Staff
Since Oct 5 - 10+ accounts sent over 6 million messages
Since Oct 7 - 4 additional accounts sent 300,000+ messages

Tue. Oct. 9 Investigated compromised S&T accounts at request of UM Chief of Staff
Findings reported to S&T Provost
Emergency preventative measures proposed for implementation in UM-based Exchange environment to maintain integrity of mail delivery system
IT leadership evaluated circumstances and opted to withhold mass notification efforts at this time

Wed. Oct. 10 Proposed changes were successfully implemented in Exchange environment
Afternoon - Microsoft blacklist blocks lifted
2:00 hour - **S&T received spear phishing attack, targeted at web users**

Thur. Oct. 11 **S&T received spear phishing attack**
S&T technicians collaborated with UM technicians to further modify the shared Exchange environment to circumvent additional attacks
All constituents agreed to immediate throttling measures

Timeline of Events and Actions (continued)

Fri. Oct. 12 **S&T received *multiple* spear phishing attacks**
S&T distribution and netgroup lists identified as vulnerable risk
UM system CIOs conducted emergency call to discuss mitigation plans
S&T IT leadership explored non-mass email communication options
3:30 pm - Deployed email to select campus leaders for distribution to constituents
IT Communications manager called each campus leader to verify authenticity and urgency of message

Sat. Oct. 13 Status report indicates improvement after mitigative efforts

Tue. Oct. 16 **S&T received spear phishing attacks, exploiting netgroups**

Wed. Oct. 17 **S&T received *continued* spear phishing attacks, exploiting netgroups**
ITCC discussed and noted concern regarding the impact of email environment changes on alternative, non-supported mail clients and the lack of direct communication from IT to faculty

Thur. Oct. 18 S&T IT Security officials responded to ITCC concern

Fri. Oct. 19 **S&T received spear phishing attacks, targeting students**
Thunderbird users continue to report dissatisfaction with restrictive measures

Mon. Oct. 22 UM Division of Information Technology (DoIT) reviewed progress and announced next steps in SPAM remediation efforts

Tue. Oct. 23 S&T IT staff and leadership discussed local implications of UM-proposed actions and evaluated solutions in terms of impact to S&T users

Fri. Nov. 2 IT Security addressed mail delivery concerns, importance of Postini use, and relevant information about recent attacks with the Provost, ITCC Chair, and S&T Chair of Chairs.

Mon. Nov. 5 Information from Nov. 2nd shared with the Provost Cabinet at the request of the Provost. October 12th notice provided as handout.
IT Leadership focused efforts on internal discussions to evaluate priority and resources available for IT security efforts.

Wed. Nov. 14 ITCC Meeting – General discussion regarding email security.
ITCC motion: The ITCC insists filtering of outbound spam begin asap.

Thur. Nov. 15 DoIT offered to meet with ITCC regarding UM-level measures taken

Sun. Dec. 9 IT provided spreadsheet of proposed solutions, mitigation steps, and prevention measures to the ITCC security group and requested assistance in considering, prioritizing, and identifying appropriate resources for a timely implementation

Dec 10 IT attended Faculty Council Rules, Procedures & Agenda (RP&A) meeting

December IT staff continued discussion within and externally with the UM-wide Exchange group regarding long-term solutions, no conclusion reached. ITCC security subcommittee invited to participate.

Jan 14 IT attended Faculty Council Rules, Procedures & Agenda (RP&A) meeting

Lessons Learned

Upon reflection, several lessons and action items were identified. They relate to the incident itself, the process used to respond to the incident, and the emergency measures implemented:

- IT was prohibited from using the campus Emergency Mass notification system for the incident (needs review)
- There is no UM-wide critical incident response process to guide coordination and communication
- The S&T IT Critical Incident Response manual intended to guide internal coordination, escalation, and communication is outdated and unavailable for implementation
- Need to separate campus outbound streams to reduce impact of future incidents. (completed)
- ITCC and RP&A subgroups of the Faculty Senate expressed concerns about the lack of communication to the faculty regarding the incident and the emergency actions
- S&T faculty and staff were vulnerable to phishing attack. More awareness needed to raise skepticism and educate users on proper reporting and response in case of attack
- S&T IT lacks sufficient definition of email client support
- S&T netgroup-based AD distribution lists are not secure and are easy targets for spam
- IT lacks a defined crisis communication matrix upon which to base decision regarding when to notify all of campus or its subgroups; extra concern is given to avoid "spamming" our own users with information they consider irrelevant

Solution, Mitigation and Prevention Steps/Measures

IT is currently researching, analyzing, assessing for impact, and determining the internal resourcing requirements for the following measures. The ITCC Security group has been invited to assist by considering, prioritizing, and finding the appropriate resources for implementing the measures in a timely and appropriate manner.

- Raise customer awareness on information security, email
- Decide what S&T wants to do to improve security re: SMTP/IMAP/POP
- Decide how to manage distribution lists more securely (netgroup management)
- Password reset cycle and rules (FIM impacts)
- Digital signing implementation
- Outbound spam/email filtering and per user email throttling
- Improve IT incident response plans
- Intrusion Detection Systems (i.e. Snort)
- Radius Server migrations
- Firewall improvements
- Audits (Past, Present and Future)