Global Information Assurance Certification Paper

Threats – They come from with-in sometimes
Bruce Calvert
2 April 2001

Overview
It has been a belief that attacks to a corporate network would come from an outside source. Such is not always the case. A commonly held thought is that a larger percentage of threats come from with-in the organization that you work for. The common consensus is there is an 80% chance of an attack/threat by an employee. What is detailed here bears that out.

The incident
When the e-mail arrived the COO didn't quite know what to do. He decided to forward the e-mail to someone he thought could handle this incident with the comments "This doesn't look good".

What the e-mail stated was:
" Dear Mr.x,
We represent H.O.P.E (Hackers on Planet Earth). We have decided to hack your Website (for the better. Watch for it)." It was accompanied by an attached GIF for hackers.com.

H.O.P.E. is actually a Hacker convention where Hackers/Phreakers come to show their prowess. One of the ways hackers gain notoriety is to warn their targets of their intentions. The target then will react by hardening their site (hopefully) making it more difficult to get in. This gives the hacker a "Badge of Honor" if they do accomplish what they set out to do.

Batten down the hatches
Do you have an incident handling policy/procedure in place? RFC 1244 is a good guide for establishing and practicing Incident Handling. The crux of the matter is that you must have these mechanisms in place to properly react.
These procedures must also be exercised on a periodic basis to discover whether or not they are still workable in your ever-changing environment.

Any type of threat/hack is going to have a chilling effect on your organization. It will have one of two results. Your organization will react quickly and effectively or it will be apathetic to the threat. It all depends on the level of paranoia or "pucker factor" that your organization holds.

You must also have a user base that is trained/informed in Information Security policies and procedures that are in place. This is a continuing process and should not be ignored after their first exposure to IS policies.

Here is how we reacted. Our organization did have certain procedures in place but had not been exercised to this point.
Once the e-mail threat had been received it was not forwarded to the proper department until three days after it had been received. This illustrates the need for user education and training/familiarization with existing policies.
Once the proper department had been notified, the procedures that existed were exercised.

Once the procedures were exercised and the proper personnel were notified, things that had been on the docket for accomplishment happened rather rapidly.

Internally all remote access services were turned off temporarily. This had the effect of slowing the business processes down since file transfer was now not an option. Our organization is worldwide and servers still had to be tended to. SSH was used for remote access to certain key servers. FTP was turned off and other batch processing was delayed. Banners for services were turned off and Intrusion Detection was heightened at our hosting sites. Other tools were employed that normally would have not been used.

Port scans looking for Trojans and other exploits were used to identify whether or not servers/hosts had been compromised and listening for remote use. Anti-virus scans were escalated.

Mixed into the fray was a failed switch that took down a segment of our network. Thankfully, not the result of any hack attempts.

We then hunkered down for the weekend. Armed with an outside dial-up account on AOL to monitor the website our Control Center would monitor for any defacement of the site, plus the internal monitoring processes were heightened to alarm if anything out of the ordinary would happen. It didn't. All was quiet.

What can you get from e-mail headers?

Fortunately, a lot. In our case the message had been forwarded down to our director. This being the case the header information had changed and had no resemblance to the original. It would be up to our e-mail administrators to obtain a copy of the original e-mail so we could examine it.

The mail admins copied the e-mail from our COO's mailbox into their mailbox. By this method the original headers were preserved and we could glean some data from the message headers.

By RFC 822 standards, there is certain information that must be included in the headers of a message that transverses different systems. Added to this is the allowable way that different mail clients treat messages.

RFC 822 states:
"In this context, messages are viewed as having an envelope and contents. The envelope contains whatever information is needed to accomplish transmission and delivery. The contents compose the object to be delivered to the recipient. This standard applies only to the format and some of the semantics of message contents. It contains no specification of the information in the envelope."

Different mail clients treat this information differently. Lotus Notes utilizes a single envelope concept for message delivery. This means that message headers and body text are contained in one "envelope".

While Outlook/Exchange clients treat this differently by using the "File attach" method for the mail headers and another for the body text or message itself when traversing systems.
These methods are allowed by RFC 822 and are a commonly accepted method of message delivery.

According to the standard, utilizing the "Extended" portions of the protocol for SMTP message transmission specific information is transmitted to the recipient. These include:
IP Address of the sender not just the host it is relayed from.
Whether the message is encrypted or not etc…

It was these extended portions that we extracted to ascertain the Identity of the individual that sent the e-mail.

The threatening e-mail had been sent from a web based mail system. The wannabe hacker did not take into account that this web based system would enter his host IP address into the message header and also would place his "Display Name" from his host in there.

What this did was to show his actual name right on the e-mail, not just the way the mail was signed (which was globalhack@Exxxxe.com). This would not become a crucial piece until later on in our investigation nor did we notice it at the outset.

We continued to trace the IP address of the originator. The mail administrators did a complete trace of every hop this mail took from mail relay to mail relay. The IP address turned out to be an AOL account. Our team now turned to a security service that we employ for further help. It was the analysts at this firm that asked if we had checked the employee directory of our company for the

name that appeared on the e-mail. Obviously we hadn't. We were in denial that this would be "one of our own". With a check of the company directory we found that this was the case. It was an employee whose name appeared on the e-mail. Now what?

Gathering Information for Legal Action

It was imperative that we move quickly to gather all of the evidence that we could. Typically, an ISP or E-mail provider does not keep activity logs for long periods of time if they keep them at all. This was case for the Web based e-mail provider; they kept no logs of any of these activities.

Fortunately for us, AOL keeps this information up to eight days. So, armed with a subpoena we asked for information directly linking this DHCP leased IP with the individual who it was assigned to. The information returned was a direct match with our employee. Now you might ask at this juncture "Couldn't this AOL account have been compromised and the employee simply didn't do this?" Yes the account could have been compromised but it was simply not the case in this matter.

The employee had several AOL "screen names" that indicated that he was conducting online sessions that were fringing on the boundaries of hacker communities (i.e. chat rooms etc…). The employee had also registered with ICQ under the same e-mail address that was on the hack threat.

Up to this point the employee had denied any involvement with any of this. Our company placed him on Administrative leave with pay until our investigation was over.

Our company has in place, an Information Protection Policy that every employee must read and sign at the start of employment. This policy states that there "is no assumption" that any information system the employee uses is "Private". This simply means that the company can look into any account you may have with them and gather data about your activities concerning the business. We used this to gather more data about this individual.

Some of the e-mail in this individuals' mailbox contained some correspondence that was written in script-kiddy "Elite" fashion. Although this in itself is not enough to condemn someone it does add credence that this employee was involved somehow within the hacking community at large or at least wanted to be.

The employee had also attended a local community college where he had attempted to take a software engineering course but had given it up in about a month.

Where to go from here – The deposition
Since our company had gone to such lengths to gather information about this incident that they (the company) decided that they must get a legal deposition from the employee. Fortunately the lawyer that was retained had recent experience in this type of case and had a pretty good idea of what was needed to depose the employee. We went over the deposition script the night before to make sure he was going to ask the right questions and it went in the right direction.

The deposition was held the next day with the employee (sans personal lawyer) in attendance. Basically the questions ranged from personal history and activities to his business activities.

He denied all activity associated with the hack threat e-mail. He did admit to knowledge of how "Fake Mail" was crafted albeit this knowledge was very limited in scope. Also he admitted to hacking into the Community College network although, given the state of a good majority of college networks, this would not be a big feat.

The "coup de gras"
We were aware of the employee's nocturnal activities and habits. We also had the time/date stamp on the e-mail, which indicated that it was sent in the wee hours of the morning and that the employee stayed up to these hours if he knew he wasn't going to be at work the next day(which he wasn't in this case). Up until this point he denied sending the mail. The lawyer then presented him with the information from AOL that associated the IP address with his account on that time and date.
At this juncture the employee capitulated and admitted to sending the threat to our COO.

Conclusion
This incident and the actions our organization took illustrate the fact that good policies and procedures need to be in place and exercised periodically. The fact that we were able to find traces of this individual prove that we were lucky in this incident. The trace information doesn't always remain. Now the company is riding the double edge sword of public relations with this case. That is another issue by itself.

References
J. Paul Holbrook, RFC 1244 Incident Handling Handbook
http://www.net.ohio-state.edu/rfc1244/incident.html

David H. Crocker, RFC 822 STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES

http://www.faqs.org/rfcs/rfc822.html

Various, Spam and Fakemail FAQ
http://www.faqs.org/faqs/net-abuse-faq/spam-faq/

Anonymous, Maximum Security 2nd Ed., Pg 423

Various,How to interpret e-mail headers
http://help.mindspring.com/docs/006/emailheaders/

Last Updated: May 30th, 2017

Upcoming Training

SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event