

Vishing

Slade E. Griffin
Sword and Shield Enterprise Security, Inc.

1431 Centerpoint Boulevard
Suite 150
Knoxville, TN 37932
865.244.3500
slade@sses.net

Casey C. Rackley

Fountainhead College of Technology
Center for Information Assurance & Cybersecurity
Training (IACT)
3203 Tazewell Pike
Knoxville, TN 37918
865.688.9422
casey.rackley@fountainheadcollege.edu

ABSTRACT

This paper is intended to discuss an emerging threat vector which combines social engineering and technology. Utilizing Voice over Internet Protocol (VoIP) convenience combined with electronic mail phishing techniques, “Vishing” has the potential to be a highly successful threat vector. Vishing victims face identity theft and/or financial fraud. The goal of this paper is to illustrate how the attack can be carried out in order to increase information security awareness. The discussion will contain documentation from actual events (to display the threat as current), proof-of-concept (to demonstrate ease of execution), and theoretical arguments (to discuss the possible future impact).

Categories and Subject Descriptors

K.6.5 [Security and Protection] Unauthorized access – *hacking, phreaking*

C.2.2 [Network Protocols] Applications – *VoIP, SMTP, FTP, etc*

D.4.6 [Security and Protection] Access Controls, Invasive Software – *viruses, worms, Trojan horses*

H.1.2 [User/Machine Systems] Human factors

H.4.3 [Information Systems Applications] Communications Applications – *Electronic mail*

K.3.2 [Computing Milieux] Computer and Information Science Education - *Information systems education*

History of Computing – *Hardware, People, Software, Systems*

General Terms

Documentation, Design, Security, Human Factors, Legal Aspects

Keywords

VoIP, phishing, vishing, threat, telephony, information assurance, education, training, digital BPX, PSTN

1. INTRODUCTION

Users of information technology, specifically e-mail, have become attuned to standard phishing techniques. Publicity

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

InfoSecCD Conference '08, September 26-27, 2008, Kennesaw, GA, USA. Copyright 2008 ACM 978-1-60558-333-4/00/0006...\$5.00.

regarding this method of financial fraud and identification theft have left this threat vector in a much weaker position, though it is likely still somewhat successful. Users are now trained to not click the obfuscated link, which requires the hacker to retool his technique as the landscape of user intelligence evolves. As technology increases and becomes more prevalent, the human factor remains the most viable target for would-be attackers. The attack has moved seamlessly back and forth between e-mail to one of our most trusted utilities, the telephone system, now combining the two. For example, in 2006, a dentist's office contracted a network engineer to ascertain the cause of a network slowdown. Further investigation by the contract engineer turned up vague references to this new type of attack. The contractor decided to call the author of this paper in as a trained incident handler/forensic analyst to discuss the possible legal aspects and variables surrounding the cost/time trade-off of a full investigation. Further research by this author indicated that there was little public awareness of this threat vector, and that users were not being well educated on the multiple attack vectors it contains.

2. ATTACK DESCRIPTION

2.1 Access

The first item needed by the attacker is an Internet-facing victim. The attacker must gain unauthorized access and of a computer with Internet access. The method of compromise – gaining physical access, or “hacking” -- is inconsequential, as long as the attacker is able to install and run software. If the compromise does not result in Administrator, Root or System level access, privilege escalation would also be needed.

2.2 Digital PBX

Once the attacker has control of this host, a digital private branch exchange (PBX) needs to be installed. Both commercial and open-source programs exist. Examples include Asterisk¹ and Skype⁴. Asterisk is an open-source hybrid TDM and packet voice PBX and IVR platform with ACD functionality. Moreover, Asterisk is quite possibly the most powerful, flexible and extensible of the available programs. Its name comes from the asterisk symbol (*), which in UNIX (including Linux) and DOS environments represents a wildcard, matching any filename. Similarly, Asterisk the PBX is designed to interface any piece of telephony hardware or software with any telephony application, seamlessly and consistently.²

Trixbox³ is a packaged operating system for Asterisk. This implementation greatly diminishes the need for any type of advanced knowledge of telephony and VoIP. Trixbox is a Knoppix like distribution that can be run from a CD if an attacker has local access to a victim machine. This makes it easier for attackers who are not comfortable with the command line interface for Asterisk.

Skypei⁴ can also be used as the VoIP PBX for this attack, although it should be noted that the free version has limited functionality. The flexibility of the digital PBX is one of the major factors contributing to the potentially high success rate of this threat. Skypei has the ability to configure their outbound phone number. This allows an attacker to spoof any number he chooses.

Lastly, an attacker needs the ability to record the phone conversation. This functionality is built into the most digital PBX software. Asterisk has the ability to both record calls (voicemail function) and later e-mail the recorded file to any destination. This flexibility gives the attacker the ability to either consolidate his efforts to one server, which serves both the voice and spam/e-mail functions, or to more widely disperse the attack in order to make tracking the attacker more difficult.

2.3 Caller ID Spoofing

It should be noted that an attacker cannot utilize an existing phone number but can configure its own number to reflect the entity of its choosing. For example, an attacker could not use the phone number 202-456-1111, as this number is currently in use by the White House as a comments line. But an attacker could use any number not in use (for example, 123-456-7890), and make it appear to be the White House calling from that number. This simple configuration within the PBX software could be very convincing to potential victims.

2.4 Spoofed e-Mail

Once the software is installed and configured, the attacker must distribute the fake phone number to potential victims. This can be done via e-mail as displayed in figure 1 below.

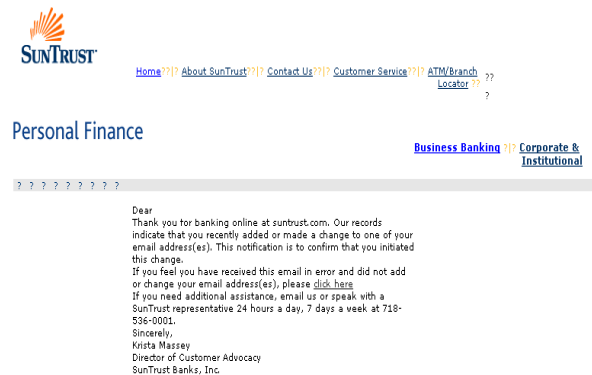


Figure 1. Vishing e-mail

The e-mail pictured above uses both the traditional obfuscated link attack vector as well as a fake phone number for the victim to

call if he is not comfortable clicking a link in an e-mail. E-mail is currently the most popular attack vector for this threat.

2.5 Analog Targeting

Prior to executing the attack, the potential attacker must have a “real” phone number or acquire access through “phreaking” (stealing telephone system access). At some point the attacker can expand criminal activities by crossing over to the analog phone world. This can be accomplished by purchasing a hardware device that converts the digital session initiation protocol (SIP) to the public switched telephone network (PSTN). The Sipura SPA-1000⁵ is a highly functional and inexpensive example of a converter at less than \$100. Alternatively, the attacker can use an Internet telephony service provider (ITSP) to perform this service for them. ITSPs are numerous and can be found easily on the Web.

2.6 Attack Vectors

The attack can be executed in multiple ways. After the attacker has gained control of a system with Internet access, installed digital PBX, and found a way to bridge SIP to PSTN, he is ready to choose the attack vector. As mentioned previously, a fabricated e-mail is currently the most popular attack vector. Additional attack vectors include automatically dialing a pre-determined set of numbers, war dialing, and using a digitized phone tree or menu for the victim to listen to. Additionally, attackers may choose to manually execute the calls in order to bring their social engineering skills into play. Hybrid attacks using the above three vectors could also be used. Figure 2 displays one possible framework for this attack.

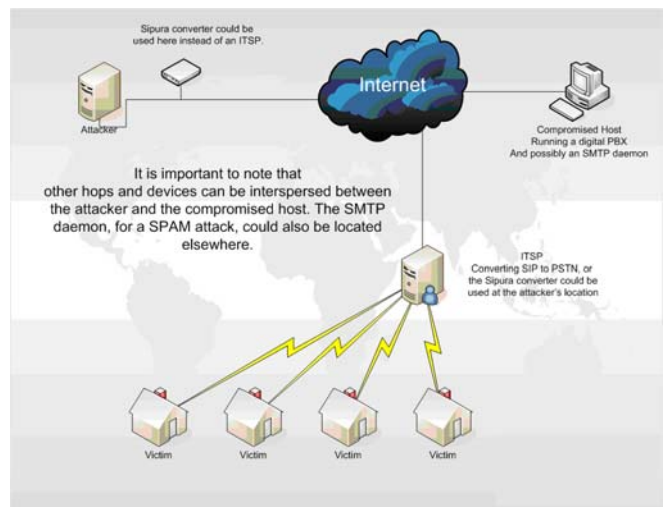


Figure 1. Attack Framework.

3. DEFENSE

Prevention of this type of attack requires multiple layers of protection. System administrators, network engineers, application developers and other people working in IT must practice due diligence. Supervisors must take care to ensure that employees are using secure computing practices, to prevent the exploitation of IT resources. Even with IT professionals doing their best to protect an infrastructure’s assets, new vulnerabilities and threats

will continue to emerge. Information Assurance education and training must also be a part of the secure computing process. Educating users about the different types of threats that are present, and training them on how best to respond to these attacks, can greatly reduce the success rate attackers currently enjoy.

4. CONCLUSION

With little knowledge of telephony, it took this author less than one hour to set up a Trixbox server configured to automatically forward recorded VoIP calls. An ITSP to bridge to PSTN would have cost less than \$10 per month, enabling the attack to actually be carried out. The economic risk-to-reward ratio appears high if the attack is configured correctly. The success rate of these attacks may also escalate rapidly if the attackers choose to collaborate and/or put more effort into the preparation of the attack.

Future attacks involving Vishing could be highly successful with only moderate changes to the existing attack vectors. Basing the attack on locality (vs. using the larger name banks or Internet outlets) could greatly increase the success rate. Users will not respond to a solicitation if they do not use the bank or retailer the attacker is spoofing. Coordinating the attack by researching the banks for a given geographical area, and correlating that area's phone numbers, may have a higher success rate. To further

increase the success rate, attackers could call the local financial intuitions and digitally record the phone menu, increasing the success rate even more.

Attackers may also begin to share information in order to have data that is more accurate. This is akin to the sharing of open proxy or mail relay servers that people routinely post online. Manually calling individuals, instead of using recorded menus, is also likely to increase the trust level between the attacker and the victim. Users who are uncomfortable with technology or who dislike automated phone menus may be especially susceptible to this method of attack.

5. REFERENCES

- [1] <http://astersik.com>
- [2] Unknown, 2008
- [3] <http://www.trixbox.org/>
- [4] <http://www.skype.com/>
- [5] <http://www.sipura.com/products/spa1000.htm>
- [6] <http://www.voip-info.org/wiki/>