IBM Global Technology Services
May 2007

The vishing guide.

Gunter Ollmann

Contents

2 Executice summary
3 What is vishing?
5 Attack vectors
6 Initiating the attack
15 Conclusions

Executive summary

Many of today's widespread threats rely heavily on social engineering—techniques used to manipulate people into performing actions or divulging confidential information—to leverage and exploit technology weaknesses. For example, "phishing" is perhaps the most commonly exploited threat currently plaguing the Internet and its users. At one point, phishing referred exclusively to the use of e-mail to deliver messages whose purpose was to persuade recipients to visit a fake Web site designed to steal authentication details. Phishing has increasingly developed into a broader category of threats that rely on social engineering to cause a message recipient to perform auxiliary activities that enable the phisher to conduct the second phase of the attack. Phishers rely on numerous Internet messaging systems to propagate their attacks. As such, many similar-sounding threats have been named based on the messaging system being used—each with its own nuances and target audiences. The following threats are all subcategories of the phishing threat:

- *"Pharming" is the manipulation of Domain Name Server (DNS) records to redirect victims.*
- *"Spear phishing" consists of highly targeted attacks.*
- *"Smishing" uses Short Message Service (SMS) on mobile phones.*
- *"Vishing" leverages Internet Protocol (IP)–based voice calling.*

This white paper specifically examines vishing and provides an analysis of current and future vectors for this particular attack.

What is vishing?

Vishing is the practice of leveraging IP-based voice messaging technologies (primarily Voice over Internet Protocol, or VoIP) to socially engineer the intended victim into providing personal, financial or other confidential information for the purpose of financial reward. The term "vishing" is derived from a combination of "voice" and "phishing."

The use of landline telephony systems to persuade someone to perform unintended actions has existed since the birth of the telephone. Who didn't make prank phone calls as a child? However, landline telephony services have traditionally terminated at a physical location known to the telephone company and could therefore be tracked back to a specific bill payer. The recent massive increase in IP telephony has meant that many telephone services can now start or terminate at a computer anywhere in the world. In addition, the cost of making a telephone call has dropped to a negligible amount.

This combination of factors has made it financially practical for phishers to leverage VoIP in their attacks. Vishing is expected to have a much higher success rate than other phishing vectors because:

- *Telephone systems have a much longer record of trust than newer, Internet-based messaging*
- *A greater percentage of the population can be reached via a phone call than through e-mail*
- *There is widespread adoption and general acceptance of automated phone validation systems*

- *The telephone makes certain population groups, such as the elderly, more reachable*
- *Timing of message delivery can be leveraged to increase odds of success*
- *The telephone allows greater personalization of the social engineering message*
- *Increased use of call centers means that the population is more accepting of strangers who may have accents asking for confidential information.*

Valuable data

Although there are multiple vectors for the phisher to conduct a vishing attack, it is important to understand the types of data that are most easily gained by the attacker leveraging IP telephony services. Typically, numeric information is more easily submitted by the victim when responding to a vishing attack using a mobile handset.

The most valuable information to the phisher is likely to be:

- *Credit card details (including expiration data and card security codes)*
- *Account numbers and their corresponding personal identification numbers (PINs)*
- *Birthdays*
- *Social Security numbers*
- *Customer loyalty card numbers*
- *Passport numbers.*

The most profitable uses of the information gained through a vishing attack include:

- *Controlling the victims' financial accounts*
- *Purchasing luxury goods and services*
- *Identity theft*
- *Making applications for loans and credit cards*
- *Transferring funds, stocks and securities*
- *Hiding criminal activities, such as money laundering*
- *Obtaining personal travel documents*
- *Receiving government benefits.*

Attack vectors

IP telephony opens a number of unique doors to any malicious attacker but lends itself strongly toward phishing attacks because of its social and technological reach. In particular, the characteristics that make IP telephony appealing to a phisher include:

- *The ability to reach any phone number from any location in the world*
- *The minimal cost to make or receive calls*
- *The ability to mask or impersonate caller ID information*
- *The ease of automating calling tasks (e.g., war dialing)*
- *The complexity of parsing voice messages for banned words and phrases*
- *The capability to use proxies to route traffic internationally, thereby obfuscating the true source of the attacks*
- *Access to malware such as bot agents to propagate and scale message delivery.*

Automated data harvesting

Vishing scams will often use automated systems to harvest victim data. The types of automated technologies available to phishers include the following:

- *Automatic recognition of tonal key presses—As vishing victims enter their confidential data through their phones' numeric keypads, the key tones are automatically converted and stored as digital numbers.*
- *Automatic voice recognition—Voice recognition technologies have reached an advanced level and can be acquired for very little money. Therefore, a phisher is not restricted to numeric data and may acquire other details, such as name and address.*

Initiating the attack

The phisher can initiate a vishing attack using a variety of methods, each of which lends itself to a particular audience and exploit vector. The primary methods for delivering the initial socially engineered message include:

- *Internet e-mail*
- *Mobile text messaging*
- *Voicemail*
- *Live phone call.*

Note that fax services are not currently available in a VoIP environment. In the near future, emerging protocols that support the sending and receiving of fax messages over VoIP will be ratified and will undoubtedly serve as another vishing delivery platform.

Internet e-mail

In some attack scenarios, victims receive an e-mail that invites, solicits or provides an incentive to call a phone number owned by the phisher. The e-mails are almost identical to the classic phishing attacks that instruct the message recipient to click on an embedded URL that takes the victim to a fake Web site to steal authentication credentials. However, in this case, the victim dials the number, and an automated voice prompts the caller to provide authentication information.

For example, the potential victim receives an e-mail such as the following:

> Dear customer,
> We've noticed that there have been three unsuccessful attempts to access your account at [name of local bank].
>
> To secure your accounts and protect your private information, [name of local bank] has locked your account. We are committed to making sure that your online transactions are secure.
>
> Please call us at [phone number with local area code] to verify your account and your identity.
>
> Sincerely,
> [Name of local bank]
> Online customer service

The socially engineered victim then dials the number. He may hear something such as this: "Thank you for calling [name of local bank]. Your business is important to us. To help you reach the correct representative and answer your query fully, please press the appropriate number on your handset." The victim is then presented with the following options:

- *Press 1 if you need to check your banking details and live balance.*
- *Press 2 if you wish to transfer funds.*
- *Press 3 to unlock your online profile.*
- *Press 0 for any other query.*

Regardless of what the caller presses, the automated system prompts him to authenticate himself. He may hear something like, "The security of each customer is important to us. To proceed further, we require that you authenticate your identity before proceeding. Please type your bank account number, followed by the pound key." The caller enters his bank account number and hears the next prompt: "Thank you. Now please type your Social Security number, followed by the pound key." The caller enters his Social Security number and again receives a prompt from the automated system: "Thank you. Now please type your PIN, followed by the pound key." The caller enters his PIN and hears one last prompt from the system: "Thank you. We will now transfer you to the appropriate representative."

At this stage, the phone call is dropped, and the victim thinks there was something wrong with the service. Alternatively, the vishing attack may redirect the victim to the real customer service line, and the victim is never aware that his authentication was appropriated by the phisher.

Mobile text messaging

Related closely to the Internet e-mail initiation vector, the phisher may also use small messages over mobile protocols such as SMS and Multimedia Messaging Service (MMS) to invite, solicit or provide an incentive to the potential victim to either phone a number or respond to the text message using SMS or MMS.

For example, the potential victim receives an SMS message such as the following, which instructs her to dial the phisher's number:

> Automatic credit watch alert! A new line of credit has been established for you at [well-known retailer]. If this is an unauthorized application, please call [phone number].

Alternatively, potential victims may receive an SMS message that seems to come from their mobile phone provider and instructs them to reply to the message with personal data. See the example below.

> You have exceeded your monthly [name of victim's cellular provider] text messaging allotment. Text messages will now be charged at 50 cents per message. Reply to this text message with your online authorization code to send an additional 500 messages for only $2.

Using the MMS message format, the phisher can send a graphical or animated message, with appropriate business logos, to further entice the potential victim.

Voicemail

Whether by making use of classical war-dialing techniques or newer Session Initiation Protocol (SIP) queries, the phisher can quickly cycle through possible phone numbers or telephony end points to enumerate live numbers. Once enumerated, the phisher can easily send a prerecorded message to each phone, typically targeting a user's voicemail inbox. Voicemail systems are targeted because message delivery scales more easily and requires less technical effort by the phisher.

The recorded nature of the voicemail lends itself toward messages that require immediate actions on behalf of the recipient. For example, the potential victim receives the following voicemail message:

> Hello, this is Sharon at The Power Company. I am urgently trying to contact you to discuss your move to Los Angeles and confirm the closing of your account and your scheduled end of service. At the present time, all power to your address will be terminated at 9:00 p.m. tomorrow. Please call customer support at [phone number] to arrange for final bill payment.

Because the potential victim has no intention of moving and certainly does not wish to have his power turned off, he will call the number, at which time he will be asked to authenticate himself—perhaps using a credit card and PIN.

Left message – primary rate callback

With the "left message" vector, the phisher purposefully aims to reach the voicemail repository of the intended victim to leave a message. The message urges the recipient to phone the number left by the phisher. The number is configured to be a primary rate (or similar) service that, when dialed by the victim, generates charges that are billed to the victim and earn the phisher money.

Left message – exploit payload

Here the phisher purposefully aims to reach the voicemail repository of the intended victim to leave a specially constructed message. Because the technology used to receive and store voicemail messages is likely to be very different from the device an intended victim will use to play back the message, it is probable that specially constructed messages may be left that would exploit weaknesses in the play-back technology without adversely affecting the voicemail storage device. Consequently, when the intended victim connects to her voicemail storage system and retrieves the message for playback, a vulnerability is exploited to allow the phisher to either take control of the device or cause it to perform actions not normally authorized by the victim.

Live

The ability to mask or impersonate various caller IDs is particularly important to phishers. By changing caller ID data, they can help reinforce their social engineering story as well as make it more difficult to track the source of an attack. IP telephony services that allow Internet phones to use local dialing code "point of presence" (POP) exit points (i.e., a phone number within the same regional calling code) can similarly increase the success of an attack.

By merely leveraging this ability—as well as the ability to place an Internet call from anywhere in the world—the phisher can also conduct what could best be called "live" attacks. In a live attack, the phisher initiates the call to

the potential victim, who then encounters an automated voice system that encourages him to supply personal information. To be successful, the phisher will either impersonate a well-known national entity (a major bank or retail chain) or a local business (a local radio station or government office) and use an appropriate caller ID.

As the cost of Internet calling falls even further, it will be financially viable for organized criminals to essentially build their own call centers to manually walk potential victims through the vishing scam. In other words, they will not be required to use a recorded message. Such a manual attack vector would likely have the highest success rates of all vishing scams.

Fraudulent live attacks can similarly use the social engineering aspects described in the previous sections of this paper but may be more successful by using more local, timely and interactive messages, such as the following:

- *Paid survey—After answering the electronic questions, the victim is asked to enter bank card details so that money can be immediately credited to the account.*
- *Tax alert—The victim is warned that, as a resident of a certain county, he may be able to benefit from a recent tax change. All he has to do is say his name, address and Social Security number.*

Future attacks

Vishing will inevitably advance beyond the current range of attack vectors to constitute one component of a sophisticated and targeted attack. Consider the following:

- *Dumpster diving—The attacker regularly trawls through the trash of local retailers and will often find receipt rolls and voided transaction notes. These receipts already hold a wealth of information, for example, cardholders' names, full or partial credit card numbers, transaction dates, items purchased, costs, etc., all of which can be easily leveraged in a highly personalized phishing attack.*
- *Card-owner validation—Consumers are frequently asked to validate their presence during a high-value purchase at the checkout. Usually the cash register operator is told to dial a bank number to get a transaction authorization number, but first the bank must speak with the cardholder and verify that he is, in fact, the account owner. It would be a relatively easy task for organized attackers to insert or impersonate this validation process, especially in collusion with the register operator. This would enable them to obtain additional personal information about their victims, for example, birth dates, Social Security numbers, etc.*

- *Handset blackmail—The phisher may persuade victims to receive or install a software update to their phones. The phone is then locked and only able to receive or call numbers owned by the phisher. To unlock the phone, the victim must call a specific primary rate number.*
- *Exploit payloads—The phisher causes the phone to automatically prefix all calls with a primary rate routing number, either transparently generating revenue for the phisher with each call by the victim, or automatically intercepting, recording and transcribing the victim's phone calls to automatically identify confidential information.*

Conclusions

Phishing has proven to be an extremely profitable business for criminals. As IP telephony services mature and market penetration expands, we can expect criminal organizations to more frequently adopt phishing techniques, and we can expect to see further evolution of the vishing threat.

Vishing will become an increasingly popular attack vector for phishers because of its ability to reach beyond the computer screen and target a broader range of potential victims and because it is a more effective platform for launching social engineering attacks. The historical trust that consumers have placed in telephony services—the assumption that the phone number calling the consumer can be traced back to a (local) billable address—will be fully leveraged by phishers for maximum profit gain.

For more information

For additional information, contact your IBM sales representative or your IBM Business Partner or visit:

ibm.com/us/iss

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
05-07

GTW01255-USEN-00