Search Go

nGenuity
INFORMATION SERVICES

Security for the A.D.D generation

Sep 16 2009

Social Engineering: Voicemail branding for improved results

With the launch of social-engineering.org I thought I would publish one of the tactics I have used in the past to gain trust with employees while on a social engineering engagements. I found this particular pretext makes the classic tech support attack significantly more successful, even while using a non-spoofed caller ID and a phone # from out of state.

It’s commonly agreed upon that anywhere from 60-90% of communication is non-verbal. You might think that this would make a phone based attack more difficult, I’m of the opinion that it makes it easier to abuse the imagination of the victim as they have less input to observe.

Just like phishing uses visual clues to build trust with the victim, it is possible to do the same using voice mail. Many companies have standard messages that employees are to use for their voice mail, simply mirroring those makes it appear like the victim has reached another employee. Here is how the attack is outlined.

1. Attacker calls to identify voice mail of victim organization.
2. Attacker sets up their voice mail to mimic target organization.
3. Attacker calls victim either just before or just after office hours. This is the key as this triggers the employee to call the attacker back.
4. Attacker ignores callback and directs it to voice mail for the victim. Victim hears the voice of the attacker, the branding that the attacker left for the victim.
5. Attacker calls victim back and proceeds with the classic tech support attack.

Theoretical Script:

Attacker (voicemail): “Hi, you have reached the voice mail of John Doe with nGenuity. We are currently experiencing a company wide security incident. Please leave your name and number and I will contact you back as soon as I can.”

Victim (voicemail): “Hi this is Joy Doe from nGenuity accounting. You can reach me at 555-1212″

Attacker (calling vicitim): “Hi Joy this is John Doe with nGenuity technical support. I’m sorry for getting back to you so late, we have had a lot of work to do to correct this mess. Your workstation is one of the last systems that I need to clean up to be done for the day. Unfortunately this threat has locked out our administrative access so I need your username and password to take care of this.”

Now if the user doesn’t want to provide their credentials simply direct them to a website you control, branded like the company and have them install some remote access software.

The point was that voice mail can be used to improve your branding as an attacker and build credibility where there is none or very little. The victim easily forgets that they were solicited because of the number of calls. Another fun tactic to build credibility is call center background noise clips and hold music. Make it sound like your actually at work.

Tags: se, Social Engineering, voicemail

Filed in Social Engineering | Adam Baldwin

Entries RSS | Comments RSS

- **Categories**
    - Advisories (14)
    - Authentication (4)
    - Awareness (2)
    - Business Continuity (2)
    - conference (1)
    - Events (3)
    - Finance (1)
    - Healthcare (3)
    - JavaScript (1)
    - nGenuity News (3)
    - Phishing (3)
    - privacy (1)
    - Realty (2)
    - Security (5)
    - Sense of Security (2)
    - Social Engineering (3)
    - Software as a Service (1)
    - Telecommunications (2)
    - Uncategorized (3)
    - Web Application Security (24)

September 2009

M	T	W	T	F	S	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

« Aug Oct »

nGenuity Information Services is powered by WordPress

WordPress Themes