Item forwarded by D.WHITESIDE2 to M.LASKY2

Item 0622126 91/05/25 12:26

From: MITCH.WAGNER Mitch Wagner

To: D.WHITESIDE2 Donald A. Whiteside

Sub: New Uploads

BY MITCH WAGNER

It's hardly the Cuckoo's Egg or the Internet Worm, but it's still an intriguing little unsolved mystery.

Maybe you can figure out whodunit, and why. I can't. Here are the clues:

On the night of Sunday, April 14, physics students at Purdue University engaged in that time-honored collegiate tradition known as ``pulling an all-nighter'' were in for a rude surprise.

It came in the form of a piece of E-mail, purporting to come from their systems administrator, stating that ``because of security faults,'' users were required to change their passwords to ``systest001.''

The E-mail gave helpful instructions on how users could change their passwords, and concluded, politely but firmly: ``This change should be done IMMEDIATELY. We will infrm you when to change your password back to normal, which should not be longer than ten minutes.''

The official-sounding memo was a scam, said Kevin Miller, Unix system manager for the Purdue University Physics Department. Two of his users fell for it, he said.

Once they did, some unidentified cracker logged in using the systest001 password, and began to search the system for security holes. The cracker also set into motion a program that would have started another, even more ambitious break-in of the Purdue network, had it not been spotted by a suspicious user.

That script flashed a message on the screen of every logged-in user, asking to please play-test a version of Tetris_a popular video game_on the local system.

But the so-called Tetris game ws actually a script that prompted users for their log-in passwords, and_if the log-in password was given_mailed that password to an off-campus mail drop.

The systest001 and Tetris scams at Purdue University are examples of several similar break-ins that ave been happening nationwide.

Gene Spafford, an assistant professor of computer science at Purdue who specializes in security and computer ethics, called the cracking attempts ``the most amusing attempts at a break-in recent memory.''

Tetris' initia point of origin, he noted, could not be better calculated to create panic in the military mindset.

``Tetris was developed in the Soviet Union; it's one of the products of the Soviet software industry,'' he said.

He said, however, that he believes the ironies are coincidental, because he believes the hackers are too unsophisticated to have thought of the ironies themselves.

Elsewhere in the country, the systest001 memo and Tetris scam were apparently found independently. Purdue was the only site we could locate where the two scams were linked and running on the same machine.

The Computer Emergency Response Team at Carnegie-Mellon University has put out an advisory on both scams, urging users to alert their systems administrators if anyone asks for their password, or asks them to change their password.

The cracker doing this bit of social engineering is taking advantage of the fact that it's really easy to create UUCP mail that appears to come from just about anywhere_a trick that's called ``spoofng'' by the cognoscenti. Indeed, it's a traditional April Fool's Day prank to flood USENET with all sorts of messages that appear to come from well-known net personalities_including a warning against April Fool's Day spoofs signed by Spafford that Spafford himself never wrote.

CERT technical coordinator Ed DeHart said that he believes that the systest001 and Tetris scams were fairly small.

``I don't think it's widespread. It's a gut-level feeling, talking to people and based on the number of reports we've had so far,'' he said.

DeHart said he has no idea who the author of the scam is.

Neither do I_but I have one more clue.

I sent some mail to the mail drop used in the Tetris scam, stating in veiled terms my desire to do an article ``about Turboetris'' and asking for information about ``why you did what you did.'' The next morning, I got a response that expressed interest in the offer. Whoever it was that sent the mail refused to give out a real name, only an alias he or she uses on bulletin-board systems.

The correspondent promised to get back to me by phone if I agreed to his or her terms, and left a time to call. I did so.

And heard nothing until last week. At that time, I talked to people purporting to be the Tetris hackers_there were two of them_at some length, but our conversation covered so much ground that it would be better to save it for next issue's column.

So we'll do so.

(Mitch Wagner is a senior editor at UNIX Today!)

BY MITCH WAGNER

``Beta Raider'' says he and a friend started to break into computer systems about a year and a half ago, when they were about 14.

That was when his Dad got him a PC, an IBM AT clone with a 286 processor.

``I just started using it for hmework and all that jazz,'' said the 16-year-old Beta Raider. ``Then my dad got a modem, and then I called local public-domain BBSes, and then I got into pirate boards, where I started talking about things like hacking and the concept of hacking security.''

Last month, a scam which Beta Raider authored was the subject of an advisory from the Computer Emergency Response Team (CERT) at Carnegie-Mellon University. He sent mail to users urging them to try out a new version of the popular computer game Tetris. The game was nonexistent, and the mail was part of a confidence job that resulted in users having their login IDs and passwords mailed to a mail drop on a different system, for pickup by Beta Raider and his friend.

I got in touch with Beta Raider by thesimple expedient of sending mail to that mail drop. We chatted two or three times on the phone. I don't know his real name, and the only really significant personal details I know about him are his age, the fact hat he lives in a suburb near Washington, D.C., and that he attends a public high school.

(Actually, that's not entirely true. I do know one more significant thing about him: that he's not paranoid enough. He let drop a couple of other things that could be used to track him down really easily, thigs which I'm withholding in the interest of protecting sources.)

Beta Raider, like most of his brethren in the computer underground, says that when he breaks into a system, he's not in it for personal gain. Breaking in is an end in itself, a means of lerning about computers, and a means of gaining entree into other systems.

``It's a puzzle. I like to crack security,'' he said.

He likes to work from accounts that have no files in them except for system login files. That's an indication that he won't be disturbed at his work; that the legitimate owner of that account has been away for a while.

From that base, he looks around the system.

``Usually I'm looking either for technical notes, source code, or more access,'' he said. Occasionally, if he finds an interesting piece of unpublished software documentation or tips, he'll post it to the bulletin boards_but nothing, he said, that the company woudln't want out anyway.

He's also looking for .netrc files, which tell him how to log onto other systems remotely. ``If the system that I'm currently on is large enough, usually one person would have access to any other system,'' he said.

Beta Raider is aware that there's currently stiff penalties against computer crimes, but he says he doesn't worry, becase he's careful and because what he does is not that serious.

``I've talk to most of the major hacks across the country, but what they've done, you can really take notice of it,'' he said.

Beta Raider says he doesn't know what he wants to do when he rows up.

``My Mom wants me to become a lawyer, my Dad wants me to do bioengeineering or something or other,'' he said. ``I want to do something with computers.

For what it's worth, I left the interviews finding it difficult to imagine Beta Raider as he villains some computer security advocates would have us believe populate the computer underground. I also couldn't picture him as a heroic desperado of the electronic frontier, which is the picture that hip publications like MONDO 2000, Rolling Stone or The Village Voice like to paint.

He just seemes to be a bright, friendly kid_a good kid fundamentally. And he's out there doing what a lot of bright, friendly good kids have always done: getting into mischief.

(Mitch Wagner is a senior editor at UNIX Today!)

Downloaded From P-80 International Information Systems 304-744-2253