Subject: OT: iPhone now hacking platform
Posted by AA on Tue, 09 Oct 2007 16:22:16 GMT
View Forum Message <> Reply to Message

Let's NOT turn this into a bashfest, ok guys?
intention here is too warn you about this very popluar device, nothing more.

http://www.eweek.com/article2/0,1895,2191471,00.asp

iPhone Turned into Pocket-Sized Hacking Platform
By Lisa Vaas
October 2, 2007

All iPhone applications run with full root privileges and any application vulnerability means winner takes all.

said H.D. Moore, thanks to the well-known security researcher having published shell code for the smart phone and instructions on how to use it as a portable hacking platform.

Because of his work, Moore's highly popular Metasploit Framework penetration-testing tool can now be used to easily write point-and-click exploits targeting iPhone

control of the device, given that all of the phone's applications run with root access.
Moore on Sept. 25 published details of his recent work on the iPhone.
Besides publishing shell code, Moore revealed multiple security chasms on Apple's device: The first and most shocking is that each and every process

What that means: A security vulnerability in any iPhone application can lead to complete system takeover.
"A rootkit takes on a whole new meaning when the attacker has access to the camera, microphone, contact list and phone hardware. Couple this with 'always-on' Internet access over EDGE and you have a perfect spying device," Moore said.

Others agree. "The shellcode combined with the number of bugs present in the iPhone finally make mobile attacks a real threat," wrote Errata Chief Technology Officer David Maynor in a blog posting.

and one of a trio who were first to unveil security issues with the iPhone

interview that he wishes he'd been able to use Metasploit when he was writing exploits for the gadget back in July.
"It will certainly make life easier" for others who write exploit code for

the iPhone, he said. "Metasploit is the go-to point-and-click [pen-testing] interface. It's really designed to help you write exploits and deploy [them] in ways anyone can use. Jailbreak [another development tool] was available [at the time Miller was writing exploits]. But now [Moore] has Metasploit where you can right away build payloads that run as executables on the iPhone."

As it is, within three days of the smartphone's July launch hackers cracked the iPhone's firmware, finding not only that the phone runs on a Unix-like operating system but going so far as to extract the master root and other system passwords.
Click here to read more about security issues with the iPhone.
Moore waited until the iPhone price dropped and until the toolchain tool for iPhone application development was released before he bought an iPhone to pick apart.
He first installed AppTapp, an iPhone package manager that downloads applications

a VT-100 Terminal to the phone, and voila (after a "few headaches," he said), he had shell access.
Moore says he can now generate working iPhone shellcode with a version of Metasploit 3.
Once he had shell access, he found not only that all applications run with root access, but an assortment of other things potentially interesting to malware writers or to any of the many people who love to hack iPhones.

One such observation: The iPhone has a potential security pitfall in that its MobileMail application supports Microsoft Office document formats by using the OfficeImporter framework when converting files into viewable form. "This looks like a great target for file-format fuzzing and some late-night reverse engineering," Moore said.

Another potential way for attackers to get into the phone is through the mDNSResponder service, which runs by default, Moore said. The mDNSResponder, used by iTunes for music sharing, is part of the Bonjour application suite, which provides automatic and transparent configuration of network devices.

When the iPhone first syncs with iTunes, its host name is changed, Moore said. The default hostname becomes "User's iPhone," with the Mac OS X user account name filling in for "User." If the iPhone is connected to a Wi-Fi network, the mDNS service exposes the iPhone owner's user name.
That particular security exposure hasn't yet responded to Moore's probes, he said, making active discovery "less likely."
Moore has also been playing with the "vibrate" shellcode released by Miller at Black Hat 2007. By the time the security show rolled around, Independent Security Evaluators had already revealed, shortly after the smart phone's release, that Apple's popular multifunctional device could be exploited for data theft or snooping purposes.
At the time, Miller, Jake Honoroff and Joshua Mason created an exploit for

the iPhone's Safari Web browser wherein they used an unmodified device to surf to a maliciously crafted drive-by download site. The site downloaded exploit code that forced the iPhone to make an outbound connection to a server controlled by the security firm.

The researchers showed that a compromised device then could be forced to send out personal data, including SMS text messages, contact information, call history, voice mail information, passwords, e-mail messages and browsing history.

Miller told eWEEK that with Moore's Metasploit work, the time needed to write iPhone exploits has substantially shrunk. "One thing interesting about the work H.D.'s done, if you look at the time frame, is it took us two days to find a vulnerability and write something to where we knew it was legitimate. [It took] seven or eight days after that to having a working exploit. If we had what H.D. has done, it would have taken maybe a day or less. Having this available now will cut what we did from two weeks to two days.

Now that the iPhone has been out for months, is the desire to hack it still at a fever pitch? Miller said that given how much personal information an attacker can shake out of the device, "It probably is something people should worry about."

"[Like H.D. said in his blog,] It's always on, it's always on the Internet, and you can get a lot of personal information. It's a viable target," Miller said.

So now it's time for real fun.

"It's going to be such good times," one blogger wrote after Moore published

saturation (some predict 14M sold by end of 2008,) a mesh networking application (or something to cross-connect the myriad of networking options) and an attractive application to encourage the owners to share amongst each other (say, some funky music sharing application or social networking tie-in, or instant messaging.) That'll lay the ground work for some very effective malware."

For his part, Moore said in his posting that he's added support for iPhone executables to the msfpayload command, allowing users to generate stand-alone bind/reverse shell executables using a syntax supplied in his posting. Next up is an XOR encoder, and then all hell should break loose.

"Once the XOR encoder is done, the only step left is to find the bugs and write the exploits :-)," Moore wrote.

By the time this article posted, Apple had not responded to a request for comment.

---