"HoneyMonkeys"

Description: How Microsoft's "HoneyMonkey" system works, how it finds malicious web sites before they find you, and what Microsoft is doing (and NOT doing) with this valuable security information it is now collecting.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-002.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-002-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 2 for August 25, 2005. On this episode we decided to use something a little different. Normally we have used Skype in the past for both This Week in Tech and Security Now!. But of course yesterday Google came out with its new Google Talk, and we thought we should try it. We were pretty impressed with the results. The entire interview was conducted with Google Talk. Steve and I both agreed, the best part is the incoming ringtone. Ooh. Oh, I do like that. Listen to that. Oh, I do like that. That sounds good.

Steve Gibson: I mean, that's worth it just for the ringtone.

Leo: Just for the ring. That's very pretty. Very, very pretty. Wow. So what are we going to talk about today?

Steve: Today we're going to talk about a recent emergence of some technology from Microsoft Research Branch called the Strider HoneyMonkey Exploit Detection System.

Leo: Wait a minute, wait a minute. Strider HoneyMonkey.

Steve: Yeah. Now...

Leo: Try to guess what that is, folks.

Steve: Well, honeypots, of course, are technology that's been around for a while. A honeypot is what many, for example, security systems and firms, and even just people who are interested in Internet security setup, a honeypot is a computer which is sort of stuck out on the Internet and allowed to be attacked by hackers for the purpose of finding out what sort of exploits are going on, what's out there. Basically it's a system you stick out there to be a victim of hacker attacks. And it's closely monitored, but obviously it's protected from the rest of the network so that nothing that happens to it can infect anyone else's network.

Leo: I guess it's kind of like Winnie the Pooh. You put out a honeypot and see what happens.

Steve: And it attracts the bees.

Leo: See who sticks their nose in.

Steve: Exactly.

Leo: All right. Well, that's been around for a while. There have been a lot of different...

Steve: Exactly. That's old technology, and but very effective for finding out what's out there on the Internet, you know, what types of exploits are out there. And, for example, that's the way these security firms discover new worms...

Leo: Right.

Steve: ...is that they've got honeypot or honeypot networks of computers that get infected by new worms, and that allows them to determine what's, you know, what kind of junk is out there cruising around the Internet. Well, Microsoft decided to experiment with reversing this process. Rather than wait for bad stuff to come to users, they've created a network of machines which they call "HoneyMonkeys." And if you're familiar with the old, you know, monkey see, monkey do...

Leo: Yeah.

Steve: ...the idea that monkeys mimic things that they see.

Leo: Yeah.

Steve: Well, these HoneyMonkeys mimic users who are surfing the Internet with Microsoft's Internet Explorer and getting themselves infected by malicious websites.

Leo: Oh, so they're - you mean end-users? Who are they going for here?

Steve: No, no, they're actually going for malicious websites...

Leo: Oh, the bad guys, I get it.

Steve: Yeah. But the HoneyMonkey computers pretend to be users who are, like, for example, cruising porn sites and getting themselves...

Leo: I see.

Steve: ...infected as a consequence.

Leo: So they pretend to be users in order to find malicious websites.

Steve: Exactly. It's sort of in the same way that a web search system uses spiders to spider the web and follow links.

Leo: Right, right, right.

Steve: These things go out and pull web pages from servers in order to, literally, to get themselves infected, to solicit infections of themselves.

Leo: So instead of a spider, it's a strider. But otherwise the same.

Steve: Exactly. And...

Leo: It's astride the 'Net.

Steve: Well, I'm not sure if "strider" refers to that because they've got a number of other research projects. There's something called the Strider Gatekeeper, which is a spyware detector, and a Strider GhostBuster, which is a rootkit detector.

Leo: Right.

Steve: So Strider seems to be sort of a moniker under which a number of different security-related projects are put together.

Leo: Okay

Steve: But what they do is, they use sort of like a VMware, or Microsoft's Virtual PC technology, to create a virtual PC. The reason they do this is that, once they get themselves infected, of course, they don't want to have to reformat the hard drive and reinstall Windows and everything. So a virtual PC, you're able to sort of boot from a file and just wash it away if it gets infected. So the way this starts is that Microsoft does some standard searches to, for example, find hosts files out on the Internet, which have been assembled by humans, of sites you want to stay away from. They'll also use links in spam and fishing emails. Basically, because the web is so huge - it's, you know, 10 billion pages - you just can't go out there looking at every single page because most of them are certainly not malicious. It's only sort of like the seedy sides of the web...

Leo: Right.

Steve: ...the bad neighborhoods, where there's a useful expectation that you might have something malicious trying to use an exploit in your browser to infect your machine. So they sort of start off seeding their HoneyMonkeys with - I know, it's fun to say.

Leo: Sounds more interesting, really, than it is, actually, I hate to say.

Steve: Well, but wait till I tell you what the results have been.

Leo: So they've set up these honeypots. They've established striders, or spiders, to search the bad areas of the 'Net for bad guys. Then what?

Steve: Well, so the idea is that, after running this for one month, that is, seeding their HoneyMonkey project with a bunch of potentially bad URLs that they've collected from, you know, just doing web searches of people's hosts file, which are like URL block lists...

Leo: Right.

Steve: ...essentially, Microsoft has found 752 URLs which attempt to infect their Windows Internet Explorers by using known vulnerabilities.

Leo: Interesting.

Steve: They actually sort of release these HoneyMonkeys on a URL in stages. They call it a "pipeline." They'll first use an unpatched XP, then a Service Pack 1 with patches, then a Service Pack 2 unpatched, then a Service Pack 2 with all recent patches, in a series of stages, and even, finally, a Service Pack 2 that's got all the latest patches, to find out whether there's any pages out there that have any unknown zero-day exploits.

Leo: Something that Microsoft hasn't yet patched.

Steve: And they have found one.

Leo: They did.

Steve: Yeah.

Leo: Now, when did they find these?

Steve: They actually found one which, fortunately, they knew about, but which had never been publicly disclosed.

Leo: Wow. Now, what does that tell them?

Steve: Well, yeah, exactly. This demonstrates that there are websites out there using exploits that have been discovered but kept quiet, and are actively working to infect people's machines.

Leo: This addresses something that the security community has for a long time called "security through obscurity." The feeling in a lot of companies - I always thought Microsoft kind of had this feeling that, well, if you just don't tell anybody, nobody will know there's a problem. Well, apparently you don't have to tell anybody. Hackers find these problems anyway.

Steve: Well, what they're also doing is they're analyzing the interconnectivity of these exploit sites. What they have found is, within the top 30 exploiting sites, many of them are owned by the same people...

Leo: Oh, interesting.

Steve: ...and the site registration addresses covers more than ten countries.

Leo: Wow. So you think there's a ring?

Steve: Well, there's a great deal of interaction among the sites, with sites referring them to each other.

Leo: Ah, interesting.

Steve: One guy, for example, owns the number one, the number three, and the number ten exploit sites in terms of strength; and 61 other exploit sites redirect traffic to this guy.

Leo: So is this the Osama bin Laden of hackers?

Steve: Well, essentially what's happening is there are now, I mean, the way this is shaping up is that the notion of infecting people's machines with spyware is becoming a business model.

Leo: Right.

Steve: I mean, it's not just hackers now. It's people trying to acquire a spam box, as we know, zombie machines, basically trying to make money from maliciously infecting other machines.

Leo: Is that why spyware has gotten so much worse, and viruses have gotten so much worse, because now there's money in the equation? Before it was just to show off.

Steve: Yes. Exactly. It's not just a hacker home from high school in the afternoon, unsupervised, screwing around.

Leo: Well, it might be, but now he wants money.

Steve: Exactly. Exactly.

Leo: It might have been. It might still be this kid after school. But now he wants something - he's making some money. This is the paper route of the 21st century.

Steve: Right. Well, and a couple of other things have been found. First of all, most of the exploit URLs are pornography sites.

Leo: Okay.

Steve: So, I mean, and that's not a surprise to anyone who's been on the 'Net for a long time. You know...

Leo: It's a little self-selecting, though. These are sites that Microsoft has seeded, right? I mean, so where do they get these sites originally? I mean, maybe that's because that's what Microsoft had, is what I'm saying, right?

Steve: Well, no, what they did was they did searches for...

Leo: So they searched the entire 'Net. They didn't kind of limit their search.

Steve: Well, they did searches, for example, using MSN Search, I would imagine. They...

Leo: Well, there's your problem right there.

Steve: They did searches for people who had posted their hosts file or their list of known spyware sites. It was sort of...

Leo: So they were going through other people saying, this is where we've had problems.

Steve: Exactly.

Leo: Because you'll post your hosts file asking for help or offering, actually, help, saying "block these sites."

Steve: Exactly. Here's a list of all the bad domains that I don't let my computer go to.

Leo: So this is what the community has been saying.

Steve: And so these are people sharing them.

Leo: Right. So, interesting. So I guess advice, piece of advice number one would be stay away from adult websites.

Steve: I think that's probably a really good idea, I mean, because...

Leo: That's a honey bucket of their own, isn't it, a honeypot of their own, really, if you think about it. Hackers are going to put their bad stuff on sites that they know people will be drawn to.

Steve: Right. Well, and we've also seen - apparently there is a shopping site which performs exploits. There are now - they have discovered some of these URLs are freeware sites...

Leo: Oh, boy.

Steve: ...that not only offer freeware where the freeware contains spyware...

Leo: Right.

Steve: ...but the site itself is using browser vulnerabilities to directly install spyware in people's machines. So just going to a freeware website, you know, one of the obviously low reputation sites, but still, you know, that's one thing we're seeing. And there are even some search sites which - they found more than 20 malicious search sites where using the site to do searches attempts to infect your machine with malware.

Leo: So to kind of explain this in a little bit of more detail, of course people understand, if you download a program, you run the risk of that program being malicious. But that's not the only way they're infecting you. These sites, just by visiting the site you're getting infected?

Steve: Well, in fact, that's what - in order to test that, that's what the HoneyMonkeys do. They take a fresh computer with some level of patching done.

Leo: Right.

Steve: They simply display the page. They go to the URL and wait a few minutes.

Leo: Right.

Steve: They don't explore links, they don't click on buttons saying yes to anything.

Leo: They just sit there.

Steve: They just go to the page. And then what they're doing is they're using this other technology that Microsoft has to detect rootkit activity, these other Strider projects, the so-called GhostBuster and the Gatekeeper, to detect any changes that are made to the machine as a result of just going to this page. And so that's what they're detecting. So basically Microsoft, for the first time, is being proactive in sending Windows out onto the Internet and monitoring whether changes are made - exploitive changes, presumably - just by going and visiting a website.

Leo: And you think this is a good technique? You think this is a good policy, a way to do it?

Steve: Actually, I'm very excited about it. Now, it means a couple things that are interesting. They also, in their research report, they check to see whether various search engines, like Google and Yahoo! and MSN, contained the links, that is, these URLs that they found. Google and Yahoo! and MSN did. Microsoft removed them from their search engine, so that MSN no longer contains these bad URLs.

Leo: There's the little ad for Microsoft in there. But I would hope that they told Google and Yahoo!, as well.

Steve: No. Microsoft's very competitive. They're, you know, you and I have talked about how...

Leo: So here's the press release. Microsoft has found bad sites. We're not going to tell anybody, but we'll block them on MSN.

Steve: And - exactly.

Leo: Oh, man.

Steve: And, notice also, Microsoft...

Leo: I was starting to like them for a minute, there.

Steve: Notice also that Microsoft is only checking for IE vulnerabilities, not for Netscape, not for Mozilla Firefox or anything else.

Leo: Interesting.

Steve: And the other thing is that Microsoft is now feeding these things to their security team...

Leo: To fix.

Steve: ...it's the ISE, the Microsoft Internet Security Enforcement Team, and getting involved with the FBI to go after these sites and begin to corral this. So suddenly...

Leo: Well, that's one thing I wanted to ask you, though. A lot of malicious sites open and close very rapidly. For instance, the fishing sites are only up for a few days. So they're really only catching a certain kind of scammer.

Steve: Well, and the other thing they're doing, it also argues for them not revealing the URLs that they're monitoring because they're now...

Leo: Yeah, they're watching.

Steve: ...monitoring these sites, and they're watching them for the emergence of new exploits.

Leo: Right. How long has Microsoft been doing this Strider MonkeyPot thing, whatever it's called?

Steve: It's been about six months.

Leo: All right.

Steve: And the news, I mean, the security community a few weeks ago really began buzzing about it because they produced a research report.

Leo: Right.

Steve: But, for example, in the case of this one zero-day exploit that had not ever been publicly disclosed, the HoneyMonkey discovered a page, a site that was doing it, identified what it was, and these guys thought, oh, my goodness, you know, here's something we've never told anybody about.

Leo: Right.

Steve: We know about it. We're going to fix it when we get around to it. But a site is already exploiting it. Well, within two weeks, 40 other sites were running the same unknown exploit.

Leo: Wow. Now, does Microsoft offer any theory as to how those sites - the guy in the first place discovered this vulnerability?

Steve: Yeah, it's the interconnectivity. I mean, there's a community, you know, a real dark underbelly here, that are communicating with each other and sharing this information. And, for example, many sites will redirect you to a different site that uses different exploits to see if some other location is able to infect you.

Leo: How about the original hacker? How did he uncover this hole?

Steve: That's a really good question.

Leo: Does he have an inside source at Microsoft maybe? Or maybe he just banged on Internet Explorer to...

Steve: Really good question. Now, and again, one of the really interesting aspects of this is that Microsoft is actively working now to clean things up, but only for them.

Leo: Right.

Steve: You know, only for their tools, only for their web search. So...

Leo: What's the reaction of the security community to that aspect of it?

Steve: Well, it's, you know, it's been sort of a mixed blessing. It's going to be interesting to see what Microsoft's going to do. The security community has suggested, well, maybe Microsoft's going to go into the URL blocking business that other companies are offering to commercial companies.

Leo: Right.

Steve: And get in there. Also, it's certainly the case that this factors into Microsoft's anti-spyware and forthcoming antivirus initiatives.

Leo: This is the subscription program they plan to offer.

Steve: Right.

Leo: And maybe that would be part of the subscription program is, oh, we know something that no one else knows, which is there's a problem that we can prevent that no one else can prevent.

Steve: Yeah.

Leo: And you'd better pay $29.95 a year to subscribe to our...

Steve: Now, the flipside of this is that, because you're not able to spoof the IP of the HoneyMonkey, and Microsoft...

Leo: By the way, ladies and gentlemen, this may be the only podcast where you ever hear the phrase, "spoof the IP of the HoneyMonkey."

Steve: So right now this HoneyMonkey network has been operating from a certain zone of IPs. And you can imagine that one of the things that the malicious websites...

Leo: Yeah. They want those numbers.

Steve: Exactly. The malicious website webmasters will block Microsoft's HoneyMonkeys from visiting their sites in order to...

Leo: Well, if they could figure out who they...

Steve: ...continue to black this out.

Leo: If they could figure out who the HoneyMonkeys are.

Steve: Exactly.

Leo: I mean, they have to find those IP addresses. I presume that's a highly guarded secret at Microsoft, right? I mean, they're not going to tell anybody.

Steve: Well, you would think that, if the HoneyMonkeys are routinely visiting these sites...

Leo: Maybe people will start noticing.

Steve: If, now that the webmasters of these malicious sites know to be, you know, on guard...

Leo: Right.

Steve: ...that they might say, wait a minute, this same, you know, here's an IP range, a block of IP addresses that seems to be coming back a lot. On the other...

Leo: That argues for Microsoft not telling anybody about this. Maybe it would have been better if Microsoft had kept this a secret.

Steve: Well, it also means that Microsoft's going to have to set up, and they have talked about setting up, networks around the world...

Leo: Right.

Steve: ...to essentially distribute their HoneyMonkeys around the globe so that they're much harder to track and verify.

Leo: And not such a bad thing, if bad guys start blocking IP addresses out of paranoia. Maybe they'll protect some innocent people, as well, right?

Steve: Well, I was going to say that...

Leo: If they blocked everybody from Redmond, Washington, that'd be great. Everybody would move to Redmond saying, I'm safe. I'm in Redmond, Washington. They might think I'm Microsoft. They might think I'm a HoneyBucket Monkey, whatever it is.

Steve: You might also argue that somebody who is using a porn site, himself or herself constantly, might have their IP blocked because they're being...

Leo: Yeah.

Steve: ...they're incorrectly being identified as a HoneyMonkey.

Leo: So, in fact, your advice would be to use more porn?

Steve: No. I think...

Leo: No.

Steve: ...you'd probably want to stay away from those sites.

Leo: The risk is there. So, now, how do we know these - now, obviously Google's not one of the search sites. But how would we know if it's a malicious search site? I mean, that's kind of scary.

Steve: It is scary that, among these malicious sites, there were 20 that were found. I mean, it really argues for sticking with the top search engines...

Leo: Go to the big guys, yeah.

Steve: ...Google, Yahoo!, and MSN.

Leo: Yeah. Well, sticking with well-known sites in general, I guess.

Steve: Yes, yes.

Leo: Wow. Or patching your Windows as often as possible, not using Internet Explorer, that kind of thing, too.

Steve: Well, yeah. One of the things that many of the pages that were talking about this were referring to was the fact that this demonstrates the effectiveness of patching. Well, who ever doubted the effectiveness of patching?

Leo: No, right. That's not a question.

Steve: I mean, you absolutely want to keep...

Leo: Patch.

Steve: It's like, oh, look how many pages infected us when we just went with a brand new Windows XP. But, yeah, no kidding.

Leo: Yeah, right. Well, in fact, you just go online with an unprotected Windows XP Service Pack 1, you'll get Sasser within a minute.

Steve: Oh, it's game over. You stick it on the 'Net without a firewall up, and you're in trouble.

Leo: Yeah, yeah. So is there anything that the average user can learn from this? I mean, I guess we've said a few things. Stay away from adult sites. Be careful where you go. Stick to the kind of major, well-known sites. Any other things that we know now because of this?

Steve: No, except that I think that it does sort of flip the whole security, you know, Microsoft security disadvantage sort of upside down, to the degree that Microsoft figures out how to protect people from this.

Leo: Yeah. Well, I would like to see Firefox do this. I would like to see other companies do this. I'd like to see Apple do this, right?

Steve: That's exactly the point, is that we know that there are Firefox vulnerabilities. Apple just released a...

Leo: Big one.

Steve: ...major security update.

Leo: 40 updates, yeah.

Steve: Yeah, 44 different security patches. So I guess the point is that Microsoft used to argue that the reason we seem to look more insecure is that we're being attacked more often, and we're beginning to see, you know, non-IE attacks on other browsers and non-Windows attacks on - I mean, and Linux, for example, non-Windows attacks on other OSes.

Leo: Yeah, but none of them have been as severe yet.

Steve: None of them have been severe, although there are, you know, remote code exploit attacks all over. So you can almost argue that, because Microsoft has had such a problem for so long, they're finally getting truly proactive; and that, as a consequence, you could foresee the day where Windows is more secure than the others.

Leo: Is something like a Strider HoneyMonkey project - I can't believe I just said that - difficult to do? Is it something that other companies couldn't do, as well?

Steve: No. And there is really nothing hard about it. And in fact, in Microsoft's research report, they do talk about other companies doing this kind of thing as a proactive means of finding flaws.

Leo: I have mixed feelings about it. On the one hand, I'm glad they're being proactive. On the other hand, it kind of makes me mad that they're keeping it to themselves.

Steve: Yeah. I mean, I certainly understand that.

Leo: Yeah.

Steve: And, for example, that they're cleansing their own search engine of those dangerous URLs...

Leo: They're using it to their economic advantage, which kind of makes me a little ticked off, to be honest with you. Isn't it the tradition of the security community that you share the results of this kind of research as widely as possible? If you care about security, you don't take advantage of these flaws to boost your numbers.

Steve: It gives Microsoft a competitive advantage.

Leo: Yeah, I don't like that.

Steve: And clearly, I mean, the fact that they're now in the spyware business, or the anti-spyware business, and they're now - some people might argue that they are in the spyware business - but the anti-spyware business and the antivirus business, it's clear that security is becoming a profit center. And so Microsoft has come up with, you know, a substantially useful technology. The good news is they've published it. Everyone understands how it works. So other people can certainly set up their own HoneyMonkey systems, should they choose to.

Leo: Everybody. Make yourself a HoneyMonkey. Well, we've learned a lot. I appreciate it. More information, of course, as always, at GRC.com. That's where you'll find ShieldsUP!, SpinRite, and the many great pro bono projects that Steve Gibson always embarks on to save our bacon, or our HoneyMonkeys, as the case may be. Steve, great to talk to you.

Steve: Always a pleasure, Leo.

Leo: We'll talk again next week.

Steve: See you next week.

Leo: That's it for this edition of Security Now! with Steve Gibson. I'm Leo Laporte. Thanks for joining us. We'll see you next week.