SECURITY NOW!

Transcript of Episode #91

Marc Maiffret

Description: Steve and Leo talk with Marc Maiffret, founder of eEye Digital Security of Aliso Viejo, California. eEye has perhaps done more forensic and vulnerability testing research to increase the remote security of Windows than any other group, including Microsoft. They continue to find and report an amazing number of Windows security vulnerabilities.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-091.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-091-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 91 for May 10, 2007: Marc Maiffret of eEye Digital Security.

It's time for Security Now, Episode 91, and a great episode, one of the rare interview episodes coming up in just a little bit. Let's welcome Steve Gibson of GRC.com fame. Hello, Steve.

Steve Gibson: Hey, Leo. Well, of course we're cheating a little bit. We already recorded this fantastic interview with Marc Maiffret, who is the founder, actually cofounder with a friend of his, of eEye Security, that we talk about, I mean, their name comes up over and over and over because these are the guys, for example, that are finding all kinds of problems in Windows, telling Microsoft about them, and then waiting month and month and month for Microsoft to finally patch the problem, during which - and I remember saying this. And one of the questions I asked Marc, because I wanted to make sure we were right about this, during that interval when they are aware of a vulnerability, Microsoft is aware of a vulnerability, and there's this window of potential zero-day exploitation.

Well, due to the technology that eEye has, their users are preemptively protected. And, in fact, not only are they protected - and actually it's even better than I was saying - not only are they protected because eEye knows well before Windows has been updated, but eEye's technology, as we're going to hear Marc describe it, is fundamentally preemptive because he's doing a filtering at many levels, one of which is the protocol level. So, for example, they're looking at the data coming in for sanity checking, saying does this make sense? And so even if there's a vulnerability which Windows is unaware of and which actually eEye is unaware of, their system will catch and block unknown problems.

And what we learned really - and I'm very excited about this, I want to make sure people don't miss this - is there is essentially a one-year free download for domestic users. And even after that one year Blink is very affordable. I'm very excited by what we learned during this hour-long conversation with Marc.

Leo: Well, we'll get to that, of course, in just a little bit. Before we do, anything you want to clear up, clean up, fix, or rebut from last episode?

Steve: Yes, yes, yes. I'm going to try to do a better job of reading my mail because I'm finding so much good stuff in there. So I'm expanding the definition of our top-of-the-show errata to calling it maybe "Errata and Mailbag," so that we have the opportunity of sharing just one or two good things that people have noted. And many listeners commented about RSA's SecurID. You remember that two weeks ago - or was it last week? It was last week we talked about the multifactor authentication. And SecurID was RSA's token that shows a six-digit constantly changing, well, changing once every minute, changing number which moves - it's sort of a pseudorandom sequence. It moves through a progression that is a function of the cryptographic information stored inside this thing. And whenever you connect to an RSA-based server it's able to synchronize.

Well, a huge number of people said, hey, we use SecurID, and one thing you forgot to mention is that when you set up for this system, you provide them with a password which you prepend to the front of those six digits. So that adds something you know to the something you have in order to get two-factor authentication. And it's clear that this varies. So apparently you don't have to do that. Some people use a four-digit or four-number PIN. Other people actually use their own password that they've chosen. But I did want to bring it up because many people wrote to say, hey, part of this is it's not just these six digits because that would only give you single-factor authentication, something you have, proving that you have the token in your possession which is generating this number. But you also prepend something that you know being your hopefully secret PIN or password.

Then I had one fun anecdote from someone named Scott in Washington. He wanted to keep his last name private, and I don't blame him. You'll see why in a second.

Leo: Washington state, or Washington, D.C.?

Steve: Washington, D.C.

Leo: Oh, okay.

Steve: Regarding hand scanners. You know, the idea - we were talking about the biometrics of hands. And I mentioned how, for example, I didn't feel that hand sizing would be enough, clearly would be accurate enough and distinguishing enough and essentially differentiating enough to use as your sole ID. But, for example, when I enter Level 3, I do it with a pass card coupled with my hand so that the system is able to say, oh, this is maybe Steve. Let's see whether this is his right hand. Oh, yes, we believe it, and then it unlocks the door.

So Scott says, "As for your discussion on hand geometry, most of the studies I've seen said it can be sufficient for low-risk physical access. If you are using hand geometry for access to a server room, what was the security leading to the door? Was this another layer in the physical access controls of the location where the servers were located? I ask because I am reminded of my college days, where they used hand geometry for access to the dining halls. Those of us who were non-weekend meal plans used to take the cards from friends with similar hand geometry to use at the dining hall. Even if the friend ate earlier, I could still use his card to get in and have my own free meal.

Leo: Seconds. Wow. Okay, there’s a flaw.

Steve: Isn’t that great? So I loved that because, you know, you’d go around high-fiving people to find somebody who has the same size hand and then say, hey, do you have the weekend meal plan? Could I borrow your card? Because the system wouldn’t be good enough to know.

Leo: Right. I hope they’ve gotten better than that.

Steve: And then finally we heard from a 12-year-old listener with a note that I got a kick out of.

Leo: I love that. Man, I wish my 12 year old would listen.

Steve: Well, his name, this guy is Justin Girard. And he says, "Hey, Steve. I’m a 12-year-old kid who listens to Security Now! and is quite computer savvy. A few weeks back my drive in my two-year-old XPS-600 just died. I don’t know what it was, but I just got a BSOD." And then he wrote, "The Blue Screen of Death’s brother, the Black Screen of Death."

Leo: Ooh, even worse.

Steve: He says, "I scheduled a Geek Squad visit so they could fix it. I was watching what he was doing, and he popped a CD into the system. Lo and behold it booted into SpinRite."

Leo: Well, now I have new respect for the Geek Squad.

Steve: Well, not quite, Leo. Wait till I’m done here. It says, "Needless to say, SpinRite fixed it. And I’m now a firm believer and will be getting a copy soon." Okay. The bad news is, I’ve checked with my office. The Geek Squad has no license for SpinRite.

Leo: Oh, I hope that’s not - maybe it was his personal copy.

Steve: Well, but you can’t use a personal copy...

Leo: They need a commercial license.

Steve: Yeah. We actually have three. We have the normal end-user license, a single user. And I have no problem if people use it on all the machines they own. And as we’ve heard in the past, if a buddy of yours has their machine die, I’m not going to complain if you go fix his machine. Then we have our site license, which says a company is welcome to use it on all of their machines in a single location, if they will have four copies. The cool thing about that is people can buy one to try it, and then buy three more to qualify for the site license. I mean, just - it's very nice. Obviously this is all the honor system. But I've been very impressed with how many sets of four I've been seeing sold after we made this more clear during our podcast.

Leo: Good, good.

Steve: And then we have what we call an enterprise license, which is ten copies. And you can't buy ten over the website because we limit it to four just to prevent there from being any chance for funky abuse of some sort. But if you just write to our sales email address on our website, Sue will allow you to purchase ten copies. And an enterprise license allows you to use it on multiple sites within a single enterprise and, you know, just for as long as you want to, to fix all the machines you have trouble with. The problem is, of course, the Geek Squad has been in trouble before, as you may remember, Leo, from using unlicensed software.

Leo: Oh, okay. I was going to say...

Steve: Oh, this is not our Nerds guys, the Nerds On Site guys.

Leo: No, they're good. That's something else.

Steve: They're 100 percent legitimate and great guys.

Leo: The Geek Squad is the Best Buy people; right?

Steve: Yes. So anyway, if there's anyone listening within range of the Geek Squad...

Leo: Busted again.

Steve: ...I would invite you to upgrade yourself to an enterprise license. And then I'd be more than happy to have you guys running around popping your SpinRite boot CDs into your customers' machines and fixing their hard drives for them.

Leo: Spies everywhere. Shall we say hello to Marc Maiffret?

Steve: Absolutely. We have such a great hour ahead of us, Leo.

Leo: I'm really excited. First thing we asked him, of course, is how he got started in the security business.

MARC MAIFFRET: eEye started roughly about eight or nine years ago. And it was started by myself and my cofounder, Firas Bushnaq. And at the time I was basically your typical 17-year-old teenager, hacking and doing all the things I shouldn't have been doing. And long story...

Leo: You were kind of a black hat hacker at the time.

MARC: Yeah, at the time, yeah, definitely. And I had, long story short, the kind of wakeup call one day when I was 17 that I was, you know, raided by the FBI. And that was really the point where I knew that all this stuff I had been kind of doing that was really more of, you know, for fun and typical teenager stuff but on a much larger scale, realized that, you know, I need to actually kind of grow up and do something with my life.

Leo: You're kind of lucky you had that call to Jesus. Although I have to say, I'm thinking of Kevin Paulsen and Kevin Mitnick both got caught as minors...

MARC: Yeah.

Leo: ...and weren't sufficiently scared, I guess, to stop. So you avoided jail time.

MARC: Yeah, I never went to jail or, you know, I've never been arrested or any of that sort of stuff in my life. So I think I have some parking tickets...

Leo: And just out of curiosity, what were you doing when you got caught by the FBI?

MARC: You name it. At the time I'd been in a couple of different hacking groups, and I was a part of pretty much one that - everybody's familiar with hacking groups like The L0pht, for example. And I was part of one of the hacking groups at the time which was called Rhino9. And we were pretty much one of the first hacking groups that was focused around security and exploits around Microsoft Windows, and really like a Microsoft-centric focus around the research and the hacking. At the same time I had also been doing a lot of stuff, everything from compromising systems to, you name it, pretty much major companies or governments and...

Steve: Oh, goodness. I'm curious. At age 17 did you have a different direction sort of marked out for yourself? Did you have some interests, or were you just sort of like, I mean, I'm wondering if eEye and this switching over to doing good replaced some other plans you had, or had you nothing at that point really cast in stone?

MARC: Yeah, there wasn't really plans at the time. I mean, the whole hacking to me was really just kind of an escape from an, let's say, interesting home life, if you will. So it really just kind of was this train, you know, that I jumped on. Everything was happening fast as far as everything related to hacking and stuff. And I really didn't have a thought of where it was all going. I mean, I didn't really have a kind of perception of how big some of the stuff was that I was doing at the time.

Steve: And of course being part of Rhino9 gave you a group identity. You were now a member of something, and you were connected to a whole bunch of guys that were, you know, similar thinking.

MARC: Exactly, exactly. And, I mean, and so that I just kind of got lost in it all, really. You know, there wasn't really any kind of grand scheme or plan or anything else, and really got lost in it. And that's why, you know, I really used the sort of wakeup call, you know, as pretty much the best way because I was lost in the whole hacking and everything I was doing at the time.

And, you know, being raided was a wakeup call. And I was lucky enough that, after that happened - I had also previously, again, kind of long story short, before I was raided I actually had run away from home for about a year and was living all throughout the United States doing hacking and different stuff. Like I said, I got back, everything caught up to me, and I was raided, and pretty much made the decision at that point that high school wasn't for me. I really wasn't happy going there, not because I thought I was smarter than everybody or anything like that, but it just wasn't kind of what I wanted to be doing at the time.

So I worked out a thing with my mom and everybody else that, you know, I wanted to start working. And looked around, and being a 17 year old and whatnot it wasn't like you just go jump into a security job. So I actually got a job at a website design hosting company which Firas Bushnaq had started, and started showing him about the different tools that I had been using, which were kind of more exploit tools, or like kind of penetration testing tools. And, you know, he comes from a software development background. If you guys are familiar with the company Berkeley Systems and the After Dark screensavers and everything, he was...

Leo: Oh, that's neat. That's great.

MARC: Yeah. Remember when guys actually used to buy screensavers?

Leo: Yeah, and Berkeley Systems was the best, man. Flying Toasters and, oh, yeah.

MARC: Exactly.

Leo: Lawnmower Man.

MARC: Yeah, he kind of came from that background, you know, much more structured, standardized, but nothing security specific. And we really just got together and talked about what we'd want to do product-wise, and that's where we came up with our first product and still our most prominent product, which is Retina, which is a vulnerability assessment product. And the simplest way is that you target - here's all the different computers that exist on your network. And Retina will give you the output as far as here's all the ways that people could break into the computers, and then how to actually solve all of those problems, you know, and kind of looking at your network like a hacker, thinking like a hacker, as we would say.

And as we started having a lot of success with Retina, everywhere from - we have I think roughly about 9,000 customers using Retina, and you could name some of the biggest. The entire Department of Defense - which is funny considering I was raided when I was a kid - but the entire, though, right, entire Department of Defense is actually standardized on using Retina as their vulnerability assessment solution.

Leo: So compare Retina to something like Nmap. How is Retina different? What does it do?

MARC: Nmap is really something more of, you know, obviously as you guys know it's going to map out all your ports, and it's really going to stop at the point of here's the attack surface, as far as here's all the services and ports that exist that you could potentially use to exploit. Retina takes it many steps further, where it will actually determine what are all the vulnerabilities that exist within those services.

Leo: So it needs to know what exploits are current.

MARC: Exactly, exactly. So Retina's kept up to date with, you know, what are all the current vulnerabilities. For example, yesterday being Microsoft Patch Tuesday, two of the most critical vulnerabilities, one revolved around Microsoft Exchange and the other with the Microsoft DNS services. And Retina will be able to remotely, rather than just telling you you have Exchange running, like what an Nmap would do, Retina will tell you that Exchange is there, and here's the five different vulnerabilities or misconfigurations that you need to resolve, otherwise your system can be compromised. And that eventually built out into more of an enterprise solution with a product that we have called REM. And REM is what would be used at a Department of Defense or a large bank or something where you have 60 different Retina scanners all throughout the world that are all tunneling back to a central server to give you a consolidated view.

Steve: So essentially REM is like a centralizing management console for distributed Retina installs?

MARC: Exactly. It'd be for distributed Retina scanning. And really the kind of one of the main differences is if you look at most vulnerability assessment, the standalone solutions like Retina or like what a Nessus would be or something, those are really just saying, here's your computers, here's some vulnerabilities and that sort of stuff. When you look at like an enterprise or any sort of business level, people really want to be able to look at their vulnerabilities and attack information, and they want to be able to report and think about it the same way that they think about their business. You know, so you might want to overlay some sort of a manufacturing business process and then know what are the potential vulnerabilities and security weaknesses that are part of that process. And so REM really brings it to that kind of level, not just centralizing all of your vulnerability and attack information, but also giving you all the different kind of analytics and stuff that you would need to make sense of this mountain of data.

Steve: I'm grinning over here as I'm listening to you because you've gone totally corporate, Marc. It's paying the bills, so that's great.

MARC: It is, it is.

Leo: And it's better than eating tuna fish in jail for three years, too.

MARC: This is true.

Steve: So at one point a while ago, when we were talking about you, I was assuming that, if you found a vulnerability that you reported under sort of so-called "responsible reporting guidelines," meaning that you secretly tell Microsoft you found something, and you'll say something about it on your site, but certainly not divulge any useful information that the bad guys could take advantage of, then are you preemptively protecting through some mechanism your customers against that so-called "zero-day," if somebody else took advantage of it?

MARC: Yeah, exactly. I mean, that was one of the things that for the longest time we've been doing is the identification of vulnerabilities through products like Retina. And we really, in doing that, part of it was the research aspect of eEye discovering vulnerabilities, you know, which I could definitely expand on. But on the point of, you know, on the protection side, I mean, that really led us to create our Blink product, which I think you guys mentioned recently.

Leo: That's very exciting, actually.

MARC: Exactly. So we really focus on the kind of vulnerabilities in security from the two perspectives of tell you everything, you know, where do we stand from a security perspective, and then actively protecting you. And that's where Blink comes in. And part of it, if you name kind of any run-of-the-mill different critical Microsoft flaws, we had been discovering so many of them, and we had a lot of customers that were telling us, why don't you guys have a solution that just protects us so that, if it takes us three months to patch or something of that nature, that's really where Blink came about in being able to shield, you know, whether it's desktops or servers from attacks, regardless if you have patches installed or not. And everything from, you know, the consumer user who maybe just isn't good about patching, there's a lot of problems that haven't been uncovered in consumer security.

But at the same time, on a business level, there's a lot of time that it takes just to roll out patches. And when you have exploits that are either zero-day, so there is no patch, or in the case of a lot of times when a patch does come out there'll be an exploit within a few hours, whereas most people it takes them typically at least a couple of weeks or more to actually roll out patches within their business. And even when they're doing that, you end up where you're rolling out patches in a rush, which means you don't really get to do all the testing to look at compatibility and that sort of thing.

So Blink being there is, you can take Windows 2000, put Blink on the system, have no patches on that system, put it live on the Internet, and it won't get compromised. And it's really taking all the research and everything that eEye's been learning in the last, you know, eight or nine years about vulnerabilities in research and putting it into a product to protect people. And I think probably the most exciting thing for me is, you know, we've been doing that on the business side as far as selling Blink to corporations and a lot of the same Retina customers.

But even more exciting is the stuff that we're doing on the consumer side because if you look at, you know, still to this day my mom and everybody else's mom that are worrying about, you know, protecting their individual consumer desktop, they're still heavily dependent on stuff like antivirus, which just isn't cut out for the types of attacks that people are facing today.

Steve: So your mom is no longer worrying about you. She's now worrying about what you used to do.

Leo: Is Blink - is it a firewall? Is it a patch program? How is it protecting me?

MARC: Blink is actually a handful of layers of protection. It doesn't really...

Steve: Is it a protocol proxy, Marc?

MARC: Yeah, actually it does a few things. So we do have that, your standard application firewalling, you know, what programs should and shouldn't communicate to the Internet. But we all know the problem with that is that my mom is going to say yes to every program or no to every program, and she's going to break things or open herself up to attack. So the application firewalling, which was really the first extension in security beyond antivirus, we have that within Blink. At the same time you can have Blink, you can turn off the application firewall, and we're still going to protect you from every attack.

And the way that we do that is through a few levels. We do do the network-based protocol analysis. So in the case of remote exploits over RPC or something of that nature we'll be analyzing a protocol and looking generically for buffer overflows, integer overflows, any sorts of malformed requests and that sort of stuff. Beyond just the network layer itself, we also have hooks into the application layer, with application-specific plug-ins for stuff like Internet Explorer and Outlook, looking for more application vulnerabilities. And then we also do protection within the actual kernel itself, hooking various APIs and looking for kind of common types of bad behavior. And then the kind of last part rounding it out is what we call kind of application protection, which is our kind of generic buffer overflow and related type of technology.

And the important part is that with Blink, you know, some people might say it truly is everything and the kitchen sink. Be hard-pressed to find another host-based security software that does everything that Blink can do. But I think one of the kind of feats of what we're able to do is that we're able to do all that with still using less memory than the McAfees and Symantecs and everybody else, and having a better performance because it's always the balance of you can really, truly protect a system; but if it means that now my mom is having a delay on her Yahoo! games coming up, she's not going to be a happy person, and she's going to start disabling things. And that's the real world that a lot of security people kind of forget is the usability aspects and stuff.

Leo: Do you still recommend using antivirus or antispyware along with Blink, or do you not...

MARC: No, one of the last layers, or one of the last couple of layers of Blink, beyond preventing attacks that come from vulnerabilities, is Blink actually has a full-blown antimalware which is antivirus and antispyware, a solution...

Leo: So you really don't need any other security software.

MARC: No, you truly don't. Even on the antivirus side itself is that, not only are we doing your classical keeping signatures up to date, looking for signatures of virus, but there's also a sandbox technology which will take an executable, emulate it in a virtual environment so we can see what's the behavior of the executable. And if we see the executable is going to connect to an IRC server in Russia and take botnet commands, we know without having a signature or not that that's a malicious piece of code.

Leo: Yeah, that's pretty obvious.

MARC: So there's a lot of stuff like that, you know. Because it's the same thing on the viruses is you're always only as good as the signature update. And we all worry about zero-day attacks today because there's no patches. But we should really think of malware as the same way, is that there is malware every day, and hundreds of them, where it is a week delay or longer...

Leo: So you're not looking at signatures at all. It's all heuristic.

MARC: Yeah. We do have a signature capability. And the reason that we added that is a lot of security companies, they love to tout the fact that they're very generic and all this other sort of stuff. It's pretty much kind of that sliding scale of the more generic you become, the higher chance that you could break valid applications or, you know...

Steve: Yes, you start having a problem with false positives.

MARC: Exactly. So we try to keep the balance of we want to be as generic as possible; but I would never come out and say, you know, you never need to update Blink again or something like that because I think that's kind of crazy talk. The other reason, you know, being able to react in a case where we didn't generically protect, being able to react to the signatures is an important thing to have there. I can safely say, if you look at Microsoft attacks in 2006, I think we had to do an after-the-fact kind of signature maybe two, three times, which is a pretty good track record. And the other important thing really on a corporate side of needing to do signatures is because, if you're doing everything generically, you can't differentiate on a threat level. So you might have a hundred events that say there was a generic RPC attack. But it's important to know was the RPC attack due to a worm, a script kiddy, a targeted attacker. You need to be able to make sense of when you have thousands of attacks that are coming into our console, what's the needle in the haystack that you should care about that you should be responding to? Which again, that's where REM on the management side comes in, to making sense of that data.

Steve: I really like the architecture you have because this protocol level filtering means that, if something did happen to get through, you can look at how it was that it got past your filters and strengthen them in a way that closes not only that particular instance, but all kinds of other latent instances that you haven't actually encountered yet.

MARC: Exactly. And that, I mean, specifically what you said is actually how we went through the design process of Blink where we sat down before figuring out do we want to do network-based or protocol or anything - a lot of security products, they tend to pick a philosophy without analyzing the data set. And we sat down, and we looked at about 5 or 6,000 different Windows-related vulnerabilities, not just Microsoft, but it could be a patch running on Windows. And looking at the 5 or 6,000 vulnerabilities, we tried to boil down what were all the common characteristics that existed that allowed the system to be compromised through this flaw? Not just the classes of attacks like buffer overflows, but how were protocols used, maybe RPC or HCP, how were they manipulated in a way.

And we really found that looking at this 5 or 6,000 vulnerability is that there truly was maybe a few hundred different commonalities between them. And that was really the first effort of making sure that Blink is looking for these things generically. And it's an ongoing process of when there's new attacks and analyzing was there other layers. You know, one of the good things about Blink is not just that we're doing the network and applications and everything, but typically, if you take something that was very popular and bad like a Sasser worm, Blink actually stopped that with three different layers of protection. So it wasn't just that we lucked out that one of our rules caught it. But a lot of times there's multiple rules within Blink that'll catch most of the attacks that exist today.

Leo: Let's use a recent example, the animated cursor flaw. And you knew about this long before Microsoft admitted to it or patched it. You knew about it in October, I think.

MARC: Yeah.

Leo: And I want to talk a little bit later on about this whole issue of when do you tell the public, how long do you hold off. And I know this is a hot one for you and a lot of security researchers. But let's ask specifically about Blink and the ANI cursor flaw. Did you put a patch in Blink? Because I know you had a patch before Microsoft did. Or do you not worry about that?

MARC: Yeah, with that flaw specifically, Blink was already protecting without an update or anything. There was a couple layers that were protecting.

Leo: That is so nice.

MARC: We do some stuff on the - kind of like what we do with the network side of analyzing protocols and how they're behaving, we do similar stuff on the file system side. But we caught it with one layer there. And then also we have a system that's generically looking for buffer overflows. So if we see you're trying to run code from some crazy place in the heap or off the stack or whatever it might be, we'll generically flag and prevent those things. So Blink itself...

Leo: That's different from DEP; right? And I presume more robust than DEP since you obviously - DEP breaks so many things.

MARC: Exactly. DEP's implemented different than how, you know, than what we're actually doing because we do, rather than something like DEP, where they're just super generically looking, hey, is there code executing off a place that it shouldn't be, we actually do a little bit of intelligence on looking at what types of code and this and that. Because you have stuff like Java, for example, that does actually do things that will make it look like you're executing code off the stack or whatever it might be, you know? And in those cases you can have false positives. So we do a lot more intelligence around when some of these cases trigger, doing a second step of, okay, is this really a bad thing or just an application that is acting a bit funny, if you will. And that's the same in the case of the ANI flaw in the sense that, you know, the two different layers, we were protecting without updating.

So for a consumer it's great because your antivirus doesn't really stop ANI. And you don't have a patch at that point. Whereas Blink, without a signature update or anything, is already preventing the attack. That's definitely a benefit for a consumer. And on the corporate level, especially if you're talking, you know, you have 2,000 systems or something, at that point again there is no patch, so you're protected without an update. But even when the patch comes out, it might take you a few weeks to roll it out or test it. If you're in the financial world, you have to do all the change control documentation, which also creates delays.

So what we ended up doing, which you were asking earlier on, we did release a third-party patch for the ANI bug. And what that was, was we actually wrote a specific code fix specific to that flaw. So this is a completely separate thing than Blink. The reason we did that is that Blink is something that, at the time, we do have the free version now, basically, and at that time it was kind of really what could we get most people's attention on to download and protect themselves. And at that it was really more, I mean, that's kind of on a business decision at the time of we could try to tell the reporters, hey, we've got this Blink thing. But reporters are all hit with, you know, ten companies that are saying my product protects and my product, you know, and that kind of thing. So the third-party patch thing is a lot easier way. And we kind of use the third-party patch, you know, the first screen that you got was you can do this one-off patch which will protect you from this single ANI flaw, or you can go download Blink, which will protect you from ANI and every single other Microsoft flaw and zero-day that has existed, basically.

Leo: Boy, if I were in the security software business I would not like you very much right now.

Steve: In fact, I was just going to say that I want to make sure our listeners heard that, and that we make sure that we heard it. So you guys have a free version of Blink that does a lot of this.

MARC: Yeah, literally we have - the marketing guys will probably shoot me for saying this. But we have Blink, which is the exact same thing that we sell to companies all throughout the world...

Steve: For like a lot of money; right?

MARC: For a lot of money, yeah. Competitive, obviously, but a lot of money, all throughout the world. And we literally took that exact same technology, and we made a personal consumer version. So we changed some of the defaults, the installation process, to make it a little bit more friendly. But the exact same kind of under-the-hood technology, and it's basically free for a year is the catch for consumer use, and anybody can go get it and download it. And everything I've been describing with the zero-day protection, the whole antivirus system, I mean, we have so many people right now that are, you know, their renewals are coming up for Symantec and McAfee, and they're all downloading Blink. And we still have work to do because, again, Blink was really first meant for companies to be using, and so it's got great protection. And the current interface we're looking to kind of simplify a little bit more and that sort of thing, make it flow and be a little bit easier for consumers. But our first and ultimate goal is to really just make the out of the box where the compatibility is good and as far as what it works with and those sort of things.

And one of the ways that we do that, and the kind of catch, as the American way goes, there's nothing really free, so our catch on free is basically that any of the attacks or vulnerabilities that are being discovered on your computer is sent back to eEye anonymously. And the two uses of that for us is, number one, to improve any bugs, so if there's a spike in Yahoo! Messenger or something, we know there's definitely a bug, something going wrong there, maybe a false positive. And then number two is to figure out what are the - maybe something that we're generically protecting with our buffer overflow system that we should have a network intrusion prevention rule for and that sort of thing. And basically all that goes back into the product for the consumers also.

Steve: Very nice. And so is Blink somehow updating itself during this first year free period also?

MARC: Yeah. So Blink, you can set it to - because the last component of Blink which I didn't even mention is there's actually our Retina products, which I was describing earlier, the 9,000 whatever customers where you can identify all your vulnerabilities, we actually threw that into Blink. So there's a full-blown vulnerability assessment solution within Blink. The engine's been slimmed down as far as interface and that sort of thing. But there's about 3,000-plus vulnerability audits that Blink will also do. And so it'll tell you what patches are missing, where to go get the patches, anything that's potentially misconfigured. One of the eye-opening statistics that we saw, all the anonymous Blink data comes back to actually one of our REM systems. And one of the interesting statistics we saw is that most home users, they're getting better at making sure they stay up to date with Microsoft patches as far as the timeline of when their Windows Update is patching their system and whatnot.

But one of the things that we saw is that the greatest number of vulnerabilities are actually the non-Microsoft vulnerabilities, the vulnerabilities within iTunes or Adobe or QuickTime or Flash. And the list goes on and on. And one of the things in 2006 that I was kind of preaching at as many conferences as I could is this idea that - a very simple idea, but it's more than a Microsoft world. And really the simplest way to compromise most consumers and most companies these days are actually through non-Microsoft vulnerabilities. It's in the corporate world your Veritas backup software having vulnerabilities, or your IBM laptops that have an ActiveX flaw, the list goes on and on.

But the problem is that, if you look at what exploits are being created, for example the open source platforms like Metasploit, they do cover non-Microsoft, and they come out with exploits just as fast for non-Microsoft flaws as they do for Microsoft. But if you ask the average person in the IT world, you know, what did you do when the Veritas flaw came out, did you have a Patch Tuesday, you know, there is no Patch Tuesdays or quick responses or anything else. So in the consumer world it's even worse because, again, the average consumer, they don't understand when iTunes pops up and says, you know, hey, there's a new 42-meg installer that you need to do. They're like, well, why would I do that? Because my music's playing fine, and I don't want to wait for that, you know, thing to download and whatever else. And there's a real problem with most non-Microsoft applications, you know, like some of the ones I listed where they're not good at separating features versus security updates, and also the way that they inform their users and keep that software up to date.

So I think that's probably one of the more eye-opening components of Blink is the vulnerability assessment piece on really showing you that, even if you're running Windows Update every night, you're not actually secure. There truly is other things that people can leverage to compromise you. And that's another thing that's a part of Blink that's there. And, I mean, you can't find another host-based product that does that. And that part's free, part of the free version also.

Leo: I don't suppose we could convince you to write a Blink for Mac by any chance, or Linux.

MARC: We toy with the idea. I mean, obviously that all comes down to the business side on the...

Leo: And you guys are Windows experts. I mean, that's your...

MARC: Yeah.

Steve: So what this is also saying is that, in terms of this application vulnerability issue, Windows itself is really no longer the lowest hanging fruit. There are now, because Microsoft has been effective with Windows Update, with Patch Tuesday, with over the course of the last five years slowly and painfully educating users, that message really has gotten through. But no one has really yet woken up to the fact that there's all these other things which are trying to enhance themselves by being network aware, like backup software that now wants to be on the 'Net, which is like the next round of vulnerabilities for everyone to deal with.

MARC: It is. And, I mean, it's an interesting thing. You know, one of the things I tell people is I look at the start of Microsoft security as really happening, you know, back in about 1999 or so. And that was where I personally found some of the first remotely exploitable Microsoft flaws. And then years later we saw stuff like Code Red and whatnot. And really in the last eight or nine years - eEye kind of started at the beginning of Microsoft's thing, really. But in the last eight or nine years Microsoft has progressed greatly. And they do have one of the best security response, or not just response, but really security processes in general of how they build their software, how they try to educate users and that sort of thing. And in that last eight or nine years, as Microsoft has pushed the bar to make their software more secure, researchers and also just bad guys that are trying to exploit systems, they've also improved and added a lot of skills and basically things to the toolbox, if you will.

And if you were to kind of put that on a graph, if you will, you'd see Microsoft and the average researcher just climbing and doing better. But you can label almost any other software company out there, and they're pretty much a flat line because most other software companies have never had an incentive or a reason to focus on security. I mean, Microsoft themselves, you know, as much as it might be out of the kindness of their heart or something, we all know that businesses revolve around the bottom line of money and everything else. And if you're not losing money based on having insecure software, you're not going to spend the money to make it more secure software versus adding new features to stay competitive. And I really think that there is a time coming, I mean, we saw one of the first non-Microsoft worms targeting Symantec's antivirus, and I think we're going to see a lot more of that in the future.

Steve: Yes. And frankly, while I completely agree with you that Microsoft has finally got it, look how long it took.

MARC: Yeah.

Steve: I mean, look at the incredible inertia they had.

MARC: Exactly.

Steve: Not to get it for so long. So, I mean...

MARC: And the interesting part, you know, more than the Microsoft world, usually the way that I end up, you know, because everybody usually is surprised, they're like, wow, Marc Maiffret's saying all these nice things about Microsoft, and I do mean it all. They do truly have the best practice around security than any other software company. I'll say that time and time again. The thing that worries me is not just that the attack surface is shifting and will shift to non-Microsoft flaws.

But it also worries me with all the marketing now that Microsoft does around things like Vista and Office 2007 and related, it really worries me about people becoming complacent and just kind of a little bit idle as far as making sure that we keep Microsoft on the path of writing secure software. And the way that I usually like to end that kind of presentation is I'll do a demonstration of you can basically take Windows Vista, which is the most secure thing ever for Microsoft, and Office 2007, which also went through the full, you know, security development life cycle and everything. And I'll actually do a remote exploit, remote hacking demonstration on showing a malformed Office file that then leads to code execution and uses a local Vista kernel privilege escalation so that you go from the local unprivileged user to running code in the kernel. And that pretty much shatters all layers of Vista and Office 2007 security.

And the reason that that's important is because there definitely isn't an end, and I don't think you'll see a big tapering off of Microsoft vulnerabilities. And really I think the thing that we'll come to a point on is that, when it comes to Microsoft and security, I think we'll see that, even if you're doing everything possible that you can as a software company to make your software secure, there's still going to be flaws. And there really doesn't need to be that many flaws a year to kind of cause the same negative aspect on Microsoft or really negative aspects on people's computers and networks.

So if you think about it, most businesses, if they were to have, you know, even once a month or every couple of months, a major critical vulnerability that they're worrying about, that's going to keep them busy. And when you put it in that terms you're really talking about maybe 12 vulnerabilities a year. And when you look at the entire Microsoft attack surface between the operating system and all the common applications, to say that there's not going to be 12 mistakes a year is kind of - I don't think we'll ever kind of get to that point. So there's always going to be those problems every couple of months where you do need to rush out, you do need to patch. But again, I can't say enough on that Microsoft has come a long way.

And the last point on the Vista, since I was talking about it, is Vista has a lot of security improvements. But they're really towards improvements around Microsoft code itself. If you look at something, for example, like they added the address-based randomization, which is a good way to help prevent some buffer overflows. They added that to Vista. And one of the things that’s interesting, though, is most of that is focused on Microsoft applications. So one of the flaws we found recently affects Java, which I think a couple people still use. And in the case of the Java flaw, you can be running Vista with all the latest patches, everything enabled. And if you go to the wrong website we can compromise you through a Java flaw. Which is, again, another example of the kind of non-Microsoft world.

And one last point, before we get off Microsoft, but one last point is that the two vulnerabilities that we found, the vulnerability within Vista itself, the kernel, and the vulnerability within Office 2007, the most eye-opening aspect was that the vulnerable code only exists in Office 2007 and only exists in Vista. Which means these aren’t two legacy bugs that got missed.

Leo: Brand new.

MARC: Yeah, exactly. It was new code that was added. And that to me was even more eye-opening than, hey, we found a Vista flaw, but that it was actually new code and that kind of thing.

Leo: Let’s not get off Microsoft quite yet because there is an issue that comes up with security researchers all the time, and it’s an important philosophical issue, to reveal or not to reveal when you find a security flaw.

MARC: Yeah, I mean, there’s definitely levels. And, I mean, for me there’s a lot of terms that should just be killed off like "full disclosure" and "responsible disclosure." Because everybody means things different. So to me, you know, kind of how you should handle vulnerabilities and what you should do to it, you know, what we do at eEye is, when we discover a vulnerability, we need to take it to the point of understanding everything we can about the vulnerability, knowing that a vendor isn’t always going to get it right and isn’t always going to want to tell you the truth. So we’ll research it. And it could take us, you know, could take us a month that we’re researching this thing and figuring out all the aspects. But at that point that you feel comfortable that you have as much of an understanding as you can, at that point you should be reporting it to the vendor, and you should be giving them the time that it takes to fix the flaw. In some cases...

Leo: In other words, reveal it to the vendor but not to the public right away.

MARC: Exactly. I mean, you should never really reveal it to - reveal details like actual specific details you should never reveal to the public until a patch has been created. The problem comes into play is that, in the case of companies like Microsoft, they can end up taking sometimes close to a year to actually create a patch. And they have all these crazy reasons of why that is. To me there’s really no excuse to take a year. And the problem that comes into play with that is that, for a company like eEye, I mean, we’re a business, and the last thing in the world from all sorts of perspectives that we want to do is release a zero-day or something. It doesn’t help anybody. I can definitely see why a lot of independent researchers do come to the point of frustration, where it has taken so long for Microsoft that they do just want to tell people about it because especially in the current climate, where one of the things we’re almost worried about is zero-day attacks, the longer Microsoft takes to patch a certain flaw, the more chances that the flaw is already known within the underground as being used to exploit systems.

And the ANI vulnerability is one of the perfect examples of that, where it was actually found by a security company, or the second ANI flaw, not the eEye one, was actually found by a security company and then was actually - took months for Microsoft. And we saw it come out in the wild and in a zero-day fashion. And that really, again, goes back to these isn’t a lot of time, you know, you’ve got to make a good patch. You know, it needs to go through QA and stuff. But I think we could all safely say that, you know, a year is probably too long.

You know, and again it comes down that, you know, there’s independent researchers who - there really is no - there’s nothing illegal. You can go release as many zero-day as you want tomorrow, and that’s a whole ‘nother debate about laws. But there’s nothing illegal about releasing a new flaw tomorrow without telling a vendor. And, you know, for a lot of independent researchers there really is no motivation to work with the vendor because it’s a very painful process. The vendor wants to minimize everything they can about the flaw, whether that’s saying what’s right or wrong or what’s real or not. It still is a marketing problem for them, and they want to minimize everything. So there’s kind of a lot of B.S. that a lot of the researchers have to go through. And I can’t blame a lot of independent researchers for not wanting to have to go through that for six months with Microsoft or some companies out there that are even worse, like the Oracles of the world.

Steve: And ultimately you guys, security researchers, never get anything back really for the trouble except maybe a little mention in some postscript note somewhere at the bottom of an announcement of, you know, thanks to so-and-so for reporting this.

MARC: Exactly. I mean, for independent researchers, you get some recognition. You post your advisory on a mailing list or something. So maybe if you’re looking for a job or you want to get noticed by an eEye or somebody like that. But yeah, otherwise it’s a lot of time without really any value. And that’s why you see a lot of independent researchers that, not only are they actually just not simply telling Microsoft, but they’re not actually telling anybody. They’re actually selling the exploits to third parties, you know. And in some cases it could be legitimate third parties, you know, companies like iDefense or, you know, the TippingPoint initiative and stuff like that. But in a lot of cases these things are being sold, in some cases to the bad guys, if you will, that are using zero-day to couple it with, you know, whatever scam of the month that they’re doing as far as phishing attack or something of that nature.

We saw with the ANI zero-day that within about a week of it becoming kind of a public thing, that there was actually already websites that were hosting it, and it had malware attached to it, too. Where if you went to that website it would actually scan looking for credit card information on your system to be sent back. And that was all in a very short period of time. And that kind of gets back to what I was saying on Blink is that the attacks now are very different, that the bad guys aren’t hoping you accidentally run an EXE from an attachment. They’re hoping that you go to the wrong web page or that you’re using Microsoft Office, and you open a Word document or whatever, because they’re taking advantage of vulnerabilities within software flaws much more these days than the kind of human, for lack of a better word, stupidity or whatnot.

Steve: One of the things, as I’m sure you know, that early on I was really waving my arms around about was that Microsoft for years kept shipping Windows systems with open services. You know, with exposed services. So I was early on the bandwagon, trying to get people to run personal firewalls. And more recently, you know, being behind a router, which is inherently giving you stateful connection protection.

MARC: Exactly.

Steve: So it really is the case, first of all, finally with Service Pack 2 having its own firewall running by default, thank god, and everything since then. And even more so with so many residential users now being behind routers, the nature of attacks has really changed...

MARC: Exactly.

Steve: ...to one where you're counting on users to go out and do something to get themselves infected, rather than having just a system sitting there doing nothing that is going to automatically pick up a Blaster worm over its Internet connection.

MARC: Exactly. Yeah, I mean, you're totally right. I mean, the attacks have shifted from being the kind of network-based, the Sassers, the Blasters, and those kinds of things, to really targeting a lot more of the kind of client applications. Which to me is a kind of scarier proposition because, if you're targeting the Outlook vulnerability, the Office vulnerabilities or something of that nature, a Skype vulnerability, which we'll get to in a minute - no, I'm just kidding. But if you're targeting those kinds of application vulnerabilities, especially in the business world, most average companies, they're very dependent on perimeter security, you know, they put up their firewall, and they kind of have the same thing that we used to say back in the '90s of you got your castle and the moat and everything like that. And most businesses are still that way. You know, maybe they have antivirus on the desktop is about it.

But when it comes to these client application vulnerabilities, the easiest way to really do some damage and get some data out of a company is to send the Microsoft Word zero-day to the HR department at a large company, and the lady in HR opens it, Word disappears, she's none the wiser, now I have that computer compromised. Now that I'm on the inside of your network, I take a remote attack like the DNS zero-day to target your active directory server. And now I've compromised that, and I can do anything I want to your company. And this all happens within a few hours. And the big problem there, again, is because we're not really protecting the insides of our network. You know, we've put all these walls around it. And as one would expect, the attacks shift. Well, if there's walls everywhere, I'm going to go ahead and find different ways, either kind of under or over or whatnot. And that's what we're seeing with all the kind of client application attacks and file format attacks.

Steve: I generally, it seems, if I look back, go sort of from one crusade to another. And I'm sure you are aware of my raw sockets crusade before the launch of XP, trying not to let Microsoft send XP out with raw sockets. And of course it took a couple of years and two service packs before they finally, reluctantly, pulled that out. Now the thing that I drive Security Now! listeners, and especially Leo, crazy with is I'm so against browser scripting because it's just such a problem. I mean, if you're scripting in your browser, you've enabled your client, your browser client, to run code from any site you visit.

MARC: Yes, exactly, I mean...

Steve: And how is that ever going to be safe?

MARC: Yeah, and it honestly is really headed for the worst. I mean, you guys know as much as anybody that the browser is becoming - might as well be becoming the operating system almost itself, you know, if Google and everybody else has their way. And as that happens more it means that you're going to have so much more of this kind of web-enabled content and stuff. And really all that ends up doing, whether it's active scripting or Flash or what's the new Microsoft Silverlight, I believe it's called.

Leo: That's right.

MARC: As all these things are added to the browser to make the browser kind of this more rich experience and really to make it like a Win32 app and everything else, the more that they do that, the more that you increase the attack surface, or really the number of areas where an attacker can supply malformed code and potentially compromise the system and whatnot. So, I mean, that is almost, from a browser perspective, there's kind of no end in sight as far as the "browser vulnerabilities." But I really think a lot of that is you could almost say there's also no end in sight on operating system vulnerabilities. And it's really a byproduct of the browser itself becoming much more of this platform, you know what I mean, that everything's starting to live in and exist in.

Steve: Right. And again, it's not so much that things on the outside are any longer able to come in because, as you said, there is good border security. Now it's things, you know, on the inside, things people do that invite the bad guys in across your border.

MARC: Exactly. And we see that, I mean, if the attacks like we've seen that have come across stuff like MySpace, for example, you know, embedding things within that, and then using that to do different browser attacks and, you know, that sort of stuff kind of goes on and on. And I think one of the interesting aspects that people haven't really talked much or done too much forward thinking on is one of the scary aspects of security as we move into kind of this everything's hosted online, everything's, you know, managed services and software as a service and whatnot. As everything becomes more hosted on the web, it becomes actually harder for third-party independent researchers to actually audit products at that point for vulnerabilities.

Steve: Good point.

MARC: If you take, for example, what Google is doing with a lot of kind of, you know, basically trying to bring something like Microsoft Office in a web browser experience, you can't really sit there and test that experience for vulnerabilities because when you're doing the testing you're actually doing it with a third-party server, which at that point becomes illegal for you to actually do that. A lot of the software companies are excited by that idea. I know some of the security guys at Microsoft love what Microsoft is doing with Microsoft Live because they're like, if the software's on the web server, you can't really mess with it as much in the legal manner, so we shouldn't see as many flaws.

The bad thing is that the white hat, the good researchers, the guys at places like eEye, yeah, it does make it harder for us to look for flaws because we're not going to illegally interact with a Microsoft web server or a Google. But the real bad guys who don't care about laws, they're still going to be looking for flaws, and they're still going to be finding them. So in those cases it kind of cripples some of the good researchers. And the thing that becomes kind of compounded by it all is that, when you have all these kind of web-enabled, you know, and online services and stuff, it makes it where I don't need to find, you know, if I find that vulnerability within Outlook, for example, I can target a user here, a user there. If I find the vulnerability within, you know, Outlook Live or whatnot, some web-based version, that means now I have the potential to compromise a system that now houses every user of Outlook. And so the kind of value of an attack becomes much greater as everything turns into hosted web servers and everything else. So that's going to be interesting.

Steve: You know, one thing that you're touching on brings up an issue that I was going to ask you about, and that is the work you've been doing and its potential collision with the DMCA.

MARC: Yeah. One good thing about the DMCA, it does actually have a provision that, if you're doing reverse engineering because of doing security research and looking for vulnerabilities, that is actually legal and protected. A lot of people blur the lines on and get up in arms on DMCA as really more around people that are defeating, you know, the copyright restrictions and stuff like that, which is what it was meant for. But you can go and take Internet Explorer and reverse engineer and print out all the Assembly code and do whatever you want as far as looking for flaws. And there's nothing illegal about doing that. But like I said, if it's hosted on a web server, you can't really sit there and throw different attacks at it all day because that does become illegal, you know, depending how it's done. So I think that'll be kind of an interesting shift and change in, you know, how we're doing vulnerability research, how companies are protecting from those sort of things.

And some benefits is that, if there is a flaw within a web service, unlike something like Outlook, where you have to now push a patch out through Windows Update and hope everybody out there gets it, with the web-enabled stuff you change it on one server, you know, your cluster of servers, and now everybody's protected. So it does make some things on security actually a lot easier and a lot better.

Steve: But you're right, by centralizing all of that - and notice in an instance like, for example, Google Mail, where you also have everybody's data in addition, so you've got centralized repository of data, and if you're able to get into that server and farm the data, you know, we're talking about spectacular, you know, the potential for spectacular disasters.

MARC: Oh, definitely. And I think we haven't even begun to see how that goes. I mean, if you look at the data theft that we all worry about today, you know, when TJX or somebody like that loses customer data, I mean, those things are obviously bad. And if somebody does SQL injection and gets customer data, it's a bad thing. But when you talk about now we're going to have most all home users that all their data is sitting online at a third party, number one, there's a lot of weird privacy things. I always joke with friends that I'm pretty sure the NSA started Google because that's the best way to spy on everybody. But not only is the privacy stuff there, but if those servers are compromised, now you're talking about instant access to everybody's data.

And it's similar to, you know, when we make analogies about, you know, the kind of real world, if you will, to cyberspace about, you know, in the real world I could go door to door, trying to break into a house. In cyberspace it's easier because I can sit from one computer in the middle of China and attack thousands of systems. And then when you start talking about it moving to this kind of web, you know, service-type stuff, now it's - I don't even need to attack a thousand systems. Now I'm the one guy sitting in China that's attacking one server somewhere, and now I get those thousands of systems, virtual systems, if you will.

Steve: When they come over and hook up to that central location.

MARC: Exactly.

Steve: I mean, you don't think of it this way, of course. But in the same way that IRC servers are used to collect zombies, you have the same sort of networking model where a whole bunch of browser clients are all connected to a central server. And, you know, you just send them all a vulnerable ActiveX control, which they'll happily instantiate...

MARC: Exactly.

Steve: ...and off you go.

MARC: Exactly. So like I said, I think that'll be interesting to see how that all kind of progresses and plays out.

Steve: What do you think about Windows versus Mac security?

MARC: Yeah, I mean, a lot of - some of the stuff in Vista, like address space randomization and the whole UAC annoying stuff and everything, I mean, some of it's just real bad knockoffs of what has existed in the UNIX world forever. You know, especially on the kind of user experience side of security. The main thing that it still comes down to is, you know, personally I think the Mac is great. I use it for all my music recording and all that. But from a security perspective, Windows still is the 90-whatever percent of what the world is running on. So you're always going to have more Microsoft vulnerabilities.

The thing that I think is very sad about Apple is that Apple doesn't write any more secure, or necessarily worse, but any more secure software than Microsoft's or anybody. Apple's code is just as bad as anybody else's. But there is kind of the thought for most people that Apples and

Macs are more secure. Mostly again it’s because people in the research community, if I’m going to spend three weeks looking for a bug, I’m not going to do it in Apple because there’s not as much value compared to Windows.

Steve: Well, and you guys are also big in the enterprise space. And, you know, enterprise is PCs running Windows.

MARC: Yeah, exactly. So, I mean, the point I was getting to on it being sad about Apple is that they really are at a point right now that, if they truly started to focus on security, they could actually get security right before people realize that they’re actually not as secure as all the ads and all the kind of the culture around it, the blogs and everything else would lead people to believe. They do pretty much the same mistakes that, you know, Microsoft was doing eight, nine years ago, where security is more of a marketing problem. You know, the way that they do updates and the way that they do the notifications is very flawed. We’ve found a handful of Apple, like QuickTime and whatnot, flaws in the past. And again, it was very much the kind of culture of Microsoft, you know, eight or nine years ago and stuff.

Steve: And of course it’s no surprise that people think that the Mac is more secure than Windows because we see those two guys on our TV sets now talking about how...

Leo: It must be, yeah, the ads say so.

Steve: One guy is able to get sick, and the other one can’t get sick. And it’s like, okay.

Leo: Yeah, I thought that was kind of asking for it, yeah.

MARC: Exactly. Oh, yeah. I mean, I kind of equated that ad to, you know, when Oracle came out and did their whole "unbreakable" campaign, and Oracle went from not really a target to everybody went after Oracle for that. Again, there’s a different value thing because Oracle is actually, you know, right there with SQL, number one database stuff. So there’s value in finding Oracle flaws as far as the impact and what you can do and number of people affected.

With the Mac that statement still isn’t true. But if they become more successful as a business, in the sense of gaining more market share and everything else, they will become more of a target. And my real hope for them right now is that they pretty much are untainted. Mac has a great perception of being secure and being better and all this stuff. And if they really started now focusing on security, by the time that they get to the point where they have the market share that’ll cause them to be a target, they could be secure. And the whole perception that exists now could actually be a reality, and it could be a great thing for them. The part that is just on a random personal crusade level frustrating for me is most of the people at Apple still don’t seem to get that from a security perspective. They’re actually kind of drinking their own Kool-Aid without actually doing some fact-checking.

Leo: Well, I hope they’re listening right now. Hey, one last question. Yeah, please listen, guys, wake up. Wake up. Blink is not available right now for Vista. Do you have plans to make it available for Vista?

MARC: Yeah. We’re shooting right now towards the end of the year, basically.

Leo: Okay.

Steve: And Leo, you know no security-conscious user is going to be using Vista now anyway. So...

Leo: Well, I don't know if that's true. Is that really true? Would you say that's true? Don't use Vista if you're worried about security?

MARC: No, I wouldn't say don't use it. If you have Windows XP today, from a security perspective there's not that much compelling stuff that I would say upgrade because of security. If there's some features that you think are interesting, I don't know what those would be; but if there's some features you think are interesting in Vista, then maybe you want to upgrade because of that, or just go get a Mac.

Leo: But you're saying an important - get a Mac, right. You said an important thing, which is don't upgrade to Vista for security.

MARC: Yeah. I think that one of the interesting things with Vista in general is that there really isn't a lot of compelling features to upgrade to Vista versus XP. I mean, most of the stuff is the same or, again, very much a catch-up to the Mac.

Leo: Things like UAC doesn't make a difference.

MARC: No, things like UAC don't, I mean, things like UAC is - there's even a lot of internal stuff at Microsoft where there's...

Leo: Mark Russinovich has been saying that.

MARC: Oh, yeah. It's an annoyance thing. It has no real value. And so I don't think, you know, you should run out and purchase Vista because you want to be more secure. That's not the reason. If you're buying a new computer, and it comes with Vista, you know, by all means go for it. It's definitely not less secure. But the hundred whatever dollars it is to get Vista, to do it based on security, I mean, there's not enough.

Leo: Sounds like your most secure situation is to run XP or Windows 2000 and Blink.

MARC: XP and Blink.

Steve: And tell us what happens after the first free year as a Blink user, as a Blink personal user. Is it then something that is affordable from then on?

MARC: Yeah, so after that it's - and you can even buy it now if you don't want to send, you know, anonymous stuff to eEye, and you want support. I believe the specific price is about $26 or so.

Steve: Oh, my God.

Leo: That's a good deal, yeah.

Steve: Leo, I think we're going to sell a lot of copies of Blink.

Leo: Yeah. I think that it's very compelling. You can't, I should just say, we have a lot of listeners outside the U.S. and Canada. I presume this is for legal reasons, you can't get it outside the U.S. and Canada for free.

MARC: For the free version, exactly. We do have a restriction on that for a number of boring legal reasons.

Steve: And it's lighter weight than the Symantec or the McAfee security suites. I mean...

Leo: Sounds like it's much lighter weight, yeah.

Steve: That immediately - that really perked my ears up immediately.

MARC: Exactly. I mean, we use, you know, when I was talking about all the layers that we have, we're smart where, depending on what application and what attack, the layers don't overlap themselves as far as effort on the computer. So it'll use less, not only RAM, you know, memory and whatnot, but also - so as far as the CPU performance and that sort of thing. And I gave you an - actually Blink Personal after the year, or if you want support now, it's $24.95 for one computer, or three computers is $29. So.

Leo: It's a very good deal. Thank you for making that so affordable. That's great.

MARC: No, definitely, definitely. So I'm hoping my mom stops calling me about - it's funny, when we're building stuff, when we're adding stuff in engineering for stuff like Blink, I mean, there's just as much features as we want to get done and complete just for our own network and protecting ourselves, and then also all of our, you know, family members. We're like, no, no, we've got this great thing, you know, on a personal level. So...

Steve: Well, Marc, this has been absolutely fantastic. And I am so glad that we followed up on once a few weeks ago saying, hey, you know, we ought to have Marc on.

Leo: Yeah, it's been really great.

Steve: This has really been good.

MARC: No, definitely, I mean, thanks for the invitation. I always listen to you guys. And when we got the offer I was ecstatic. So, I mean, I've known you guys both before, and you guys are doing a great job, man. Keep it up.

Steve: Thank you so much.

Leo: That's Marc Maiffret, and the company is eEye.com. You can get Blink if you go to the eEye.com site, and you click the Products button and drop it down, Blink Personal is the free one for folks in the U.S. and Canada. And then you can also buy a license if you're outside. And I think 20 - what'd he say, 22 bucks? That's not bad.

Steve: 20-something 95, you know, the marketing guys have been into it, of course. I've got to say, you know, I am going to start recommending this. What he talked about, the architecture of Blink, is so correct compared to always following behind and doing pattern-based, you know, download the latest security update and you're not safe until then, this thing preemptively protects people. And what I love most, you know me, coding everything in Assembly language, is that apparently, from what Marc said, this is dramatically lighter weight than any of the contemporary monster security suites. So I think this gives you, I mean, certainly you want to be behind - I guess you want to be behind a personal firewall. We didn't really ask him if it's also doing firewall technology because he did mention that at the enterprise level it has that, too. But, you know, anybody with XP and Vista already has one. I don't know if it does outbound protection. I'm going to have to study it a little bit. But, boy, Leo, I think this is terrific.

Leo: Steve, any other items? Next week we've got our Q&A; right?

Steve: Yes, we're going to launch into our Q&A. And then the week after that we're going to continue with a never-ending stream of hopefully fun and entertaining and interesting security discussion.

Leo: Well, more people are listening all the time. I was just taking a look at the numbers, and great growth, and we're really glad that you listen to the show, and we hope you will keep listening.

A reminder, of course, that GRC.com is Steve's home on the Internet. That's where you can go to find 16KB versions of the show for the bandwidth-impaired. You can get transcripts. I think this would be a great show to get the transcript of. We'll make sure Elaine gets to work on that right away. We also have notes there, and previous shows, and Steve's great free security utilities, things like SecurAble, that's the new one, Shoot The Messenger, Unplug n' Pray, DCOMbobulator, and then the world-famous ShieldsUP, rapidly approaching 50 million uses. You going to have a party for that or anything?

Steve: Oh, we'll say hi.

Leo: Woohoo! You should give something to the 50 millionth user. We can work out something if you want. You want to have a prize package for the 50 millionth user? Would your logs be able to tell you who that was?

Steve: No. We're at 49.816 million.

Leo: At the rate that you go, how soon is that? A week? Two? Three? You've got a couple hundred thousand?

Steve: No, we do about 25,000 a day. So it looks like it'd be about, oh, yeah, about ten days.

Leo: Holy cow. Holy cow, that's really neat. A horn should go off, anyway. GRC.com. That's also where you'll find SpinRite, which is the ultimate disk recovery and maintenance utility, a must-have. And guys on the Geek Squad, don't worry, you can get a license. Just go there. It's very affordable.

Steve: We're big on forgiveness here, Leo.

Leo: Amnesty program. Anybody who's got SpinRite and doesn't have a license just...