

[Chester] Welcome to Sophos Security Chet Chat episode 47 for February 7th, 2011. I'm Chester Wisniewski and I'm here with Michael Argast.

[Michael] Hi Chet.

[Chester] Welcome back, I've got quite a few topics to cover here, so I am going to try to motor right on through stuff here. Tomorrow is Patch Tuesday, so officially we don't have the exact details on which patches are available, but I have a few highlights. We do know that Microsoft will be fixing 12 vulnerabilities in Windows, Office and other products. These include what I consider quite critical ones, there's three critical, but the two that are most interesting to the public are the recursive CSS vulnerability in Internet Explorer which has been, had proof of concept out there in the wild, they are fixing that one that was a zero day last month. As well as the thumbnail rendering vulnerability that also we saw an attempted proof of concept this weekend on the ContagioBlog, although that one hasn't been exploited in the wild, clearly people are trying which is a bad sign, so both of those are high priority to get them out. Unfortunately the recently disclosed MHTML vulnerability is not going to be fixed this Tuesday, not surprising really it's only been about a week that it's been being discussed. It's hard to turn things around that quickly. There is mitigation, as we mentioned last week you should take that mitigation and disable MHTML other than in the local internet zone, follow the Microsoft Fixit advice there are GPOs and things you can deploy to solve that problem if your an Internet Explorer user. It's not exclusive to Internet Explorer so don't get confused, it's anything that uses Microsoft's rendering engine, but the primary candidate for exploitation would like be Internet Explorer. Also this is the first, kind of, joint Adobe release through MAPP as well, so the MAPP is the Microsoft Active Protection Partners and companies like Sophos participate to get advanced notification of how vulnerabilities work and to share information amongst one another to help provide advanced protection for customers before the patches are available. Adobe will be releasing a batch of updates, primarily for Windows and OS X tomorrow coinciding with Microsoft's Patch Tuesday. Linux and Unix systems will receive similar patches on February 28th, but Windows and Mac are the high priority and will get them tomorrow. It's a big patch week, block out some time in your schedule.

[Michael] Yup

[Chester] HBGary

[Michael] Yeah

[Chester] A well respected security firm was attacked by Anonymous, I guess technical the day before the Super Bowl, they announced and released and embarrassed HBGary during the beginning of the middle of the start <smile> of the Super Bowl.

[Michael] 60,000 emails up on a torrent . .

[Chester] Yeah, and they supposedly eared their backups, they dumped all of their MySQL databases and posted those as well, they got all the passwords of users of rootkit.com, which is a subsidiary of the company run by Greg Hoagland. Obviously it was a vengeance attack for trying to embarrass them because they had been investigating Anonymous on behalf of the FBI.

[Michael] It's a bit of an escalation of their methods though, you go from simple DDoS

attacks with something like LOIC to a targeted hacking attack, not particularly complex, but still definitely a change in methods and motives.

[Chester] Yeah to a degree, Anonymous is many people and it's none and all this kind of thing. The reality is that there are people that agree with the ideals that Anonymous represent that are skilled attackers and there are people who just don't know what to do and "Hey if you give me a gun, I'll shoot it". I think that is what the LOIC tool stuff was. In this case it doesn't look like it was brilliantly clever hacking, per se, but it was well executed. They combined some weaknesses with social engineering and other poor security practices on behalf of individuals, it looks like, that worked within the company. Maybe they weren't company practices, but they were...

[Michael] There were some bad password management and stuff like that occurred.

[Chester] Yeah, things that I think any company in the world, regardless of their security posture, probably has happening. You can't dictate how people run their personal lives, their own LinkedIn profiles, or how they choose their Twitter password. We can give people advice on how they should do that, but even most of us in the industry don't practice what we preach. A quick anecdote on that, I was recently working with some other security researchers and they asked me to login to the statistics for our blog. They wanted to see how many hits we get when we get Slashdotted on our stories sometimes. I went to login and of course I don't know my password to our blog, I have a password management tool I use. An encrypted vault of passwords with two factor authentication, because I actually do practice what I preach when it comes to password security. I'm like, Oh I have to go get my token, so I can login to my password vault. They were like "You blog three times a day sometimes, how could you not know your password?". I said "It's really long, and it's really secure and I can only remember so many of these darned things.". I do keep an encrypted two factor vault and then have a reasonably difficult strength password for that vault. This is the one thing I manage to drill into my brain, to have to remember. Anyhow, it's not surprising this kind of thing could happen, but it was disappointing to see a company with the degree of respect HBGary generally holds within the industry succumb to what looks like some social engineering and some stupid mistakes, honestly.

Pwn2Own, now most companies, as the summary I read before coming into the podcast...

[Michael] Don't want attention

[Chester] Exactly. Like when you say that we're going to put your device in the Pwn2Own contest, I'm sure Apple just absolutely loves that they're both the prize and the target every year at Pwn2Own here in Vancouver. Unfortunately I was disappointed to find out that I am actually on vacation during CanSecWest this year, so even though it is in Vancouver and a security conferece, I'm not going to be able to go.

[Michael] But Google is actually stepping up to the plate and saying "We want attention!"

[Chester] Yeah, shockingly right? So in addition to the \$15,000 prize at Pwn2Own Google's put up another \$20,000 on top of that if somebody can pop Chrome first.

[Michael] Yeah, so either they're really confident that Chrome won't get popped, or they want some security attention that will help them uncover the vulnerabilities in their browser and get them security. Right? It's hard to know which of them is their motivation, but either way I think bully on them. It's a good step.

[Chester] Yeah, and I think to reinforce that you can look at this from two other perspectives. \$20,000 to Google is not much money, one. Two, how much does it cost to hire a security researcher who may not be able to even find that that vulnerability?

[Michael] It's a good return on investment, right?

[Chester] Aw, it's awesome. And then three, what is the cost of being owned, as the Pwn2Own contest says, let's ask HBGary if this incident cost them \$20,000 or not. Preventative approaches are always an ounce of prevention a pound of cure kind of situation kind of thing. Then if you hire somebody for \$50,000 or \$100,000 to do pen testing, or security audit or you hire somebody that's a good professional that knows what their doing. What they're finding will prevent the types of incidents of things that happen often to companies like HBGary. I hate to keep picking on them, but they're the story this week, unfortunately for them. It's hard to justify these budgets when you are going to your management and you're like "I really need \$10,000 before we can post this new website, because I need somebody to test it, I need somebody from the outside to test our vendor who's providing the services to make sure that they're living up to their parts of the contract that we negotiated on how our site is going to be secured." That investment up front pays off in spades. There is no way to prove it unfortunately, its hard, you never know if you would have been the victim, so it's impossible to know. I think Google's demonstrating by this action that they know it.

[Michael] Yep, it's a good step on their part.

[Chester] Nasdaq got attacked as well and they had a rather large compromise.

[Michael] Yeah, I don't think it's surprising that Nasdaq and the other financial organizations are under attack. The fact is they came out publicly and said that they had been compromised. They said it didn't involve trades and stuff like that, they claim that the financial system is still secure. There's still some serious concerns about what happened here.

[Chester] If trades were involved, do you think they would have said so?

[Michael] No, no that would cause a lot of concern in the market.

[Chester] So, I think it would be safe to say we don't no.

[Michael] Yeah, we don't know.

[Chester] They apparently did with withhold, or hold back for some period of time while investigations were occurring from disclosing and some people have criticized that and other people say they shouldn't have ever said anything about it. I guess the issue is that when these situations occur we're not learning from them when we don't discover kind of to some degree

[Michael] What happened

[Chester] At a high level what happened and I really wish there were a way to encourage these organizations, in their moment of embarrassment, when they're having to have the PR team on high alert out there in the press with the camera bulbs flashing.

[Michael] Give us the details!

[Chester] Well yeah, you don't have to tell us specifics, but in the HBGary case it looks like we are going to learn a lot of the details of how this went down. That's excellent news for everybody to be able to step back and go Hmmmmm.

[Michael] How does that apply to me?

[Chester] Would this have happened to my company and if it would, what could I do to prevent it? Most of the time instead it's us going "eh" 300,000 records were lost, what happened? "Hackers broke into our server".

[Michael] How did they do that?

[Chester] What does that mean? Did you just leave it wide open without a firewall? and your MySQL database password was 'database'? What happened here right? I think we really need to learn from these incidents. Last story, RBS WorldPay which has been a topic that I've covered a lot in my Anatomy of an Attack series.

[Michael] On again, off again, yep.

[Chester] Hacker #3 as I referred to him in my presentations, does have a name, his name is Yevgeny. He was arrested about six months ago by the Russian authorities, he's been under house arrest.

[Michael] He's now plead guilty.

[Chester] Yeah, apparently \$10 million he claims was his take on it.

[Michael] Which was quite a lot of money and it's going to be interesting to see.. the Russians have a notoriously poor record for serious sentencing around this kind of attack. The FBI's threatening people with 10 years in jail for participating in a DDoS, it will be interesting to see what the Russians give this guy for masterminding or being part of the plot behind stealing \$10 million.

[Chester] I think we will all rest better at night if we focus on the fact that they arrested him and that they are going to punish him, as opposed to what the sentence might be. It's a step forward at all

[Michael] Yep

[Chester] to get international cooperation to actually detain these guys and make it clear that the FBI can work with the Ukrainians, the Estonians, the Russians. That we're not going to tolerate this international stuff just and just sweep it under the carpet and go "it's a bunch of foreign criminals, let's lock ourselves down and throw the internet kill switch". Which we don't really have time to talk about this week. There is a lot of American society that can be a bit xenophobic and we're always blaming the Russians and the Chinese and although they may be at fault sometimes, I think this is a good example of cooperation even if the sentence is probably going to be less than what most of us would like to see for such a serious financial crime.

[Michael] Yup.

[Chester] I was going to wrap up, but I have one last comment. RSA is next week in San Francisco, CA. Please come visit us, we are going to be in the South exhibition hall right inside the front door. When you walk in and you look up you should see myself, Paul Ducklin and the rest of the Sophos crew. With our brand new logo and booth, so please come by and say hi. If you would like to have a chat, we'll be more than happy to chat.

We'll be doing live malware demonstrations and things at the booth throughout the day every 15 or 20 minutes. We'd love to see you there, we also have three main conference sessions. Our speakers James Lyne and Arabella Hallowell will be speaking at the main conference, so if your a full conference attendee please stop by our sessions.

On that note that wraps up Sophos Security Chet Chat 47. As always you can get our podcasts at podcasts.sophos.com or on iTunes. For the latest news go to nakedsecurity.sophos.com. Until next time, stay secure.