



Tracing A Cracker - The Unorthodox Method

Paris2K writes: Paris2K got HACKED ;-)

My fellow boxters and other readers,

In this article I will tell you the story of how I got "hacked". I will take you on a trip through the events as they occurred and through my mind and thoughts from the moment I realised I got "hacked" until the moment I got my chance to take revenge.

Paris2K got HACKED ;-)

As some of you might, and some of you might not know, a short while back someone at Neworder posted some personal information about me on the board. Information he could have only gained by having at least to a certain extent, access to my computer. Someone got pissed off with me and decided to attack me. I came online unsuspectingly and read my memo's. One memo was from this guy who I will from now on refer to as "the attacker", saying something like:

"You moron, you should use proxies."

I didn't think much of it. You'd be surprised how much weird memos some of the regulars at Neworder get! Anyways, I proceeded with my doings until just a few minutes later when multiple people were telling me to go to the Neworder board. (btw thanks for this). It seemed Paris2K had been owned ;-)

The attacker left the following message on the Off Topic board:

*Posted by "The Attacker" (Standard user) *.18.16.121 - 2003/Feb/08 06:06*

"Poor guy

A 23 yr. old guy named Jorn aka Paris2K from Amsterdam thinks he's so smart. He started dissing me without any reason so here i go: IP :62.234.122.224 --> using Kaspersky Anti-Virus (wahaha)"

And with these nice words he posted several things that should not have been in his knowledge including the contents of my Neworder cookie and the following information:

----- system info-----

Username: P2K
Terminalsession-id: 0
Number of processors: 1
Processortype: x86 Family 15 Model 2 Stepping 4
Windows-version: 5.1
Active compiled version: 2600
Service Pack: None
type: Uniprocessor Free
registered organisation: P2K inc
registrerd owner: P2K
Running tasks:
1248 Explorer.EXE
1308 Winampa.exe
1324 avpcc.exe
1332 Mixer.exe
1368 msmsgs.exe
1408 ApacheMonitor.exe
1812 Apache.exe
1832 avpcc.exe
1872 avpm.exe
1916 nvsvc32.exe
2044 vsmon.exe
176 Apache.exe
3036 iexplore.exe
3240 aphex.exe

Anyone want his apache admin code ? C:\Program Files\Apache Group\Apache2\ ?? Anyway, ist early morning .. gotta go to sleep. hope you liked my tut. :P PS. He jij vuile lul !, volgende keer ga je maar je moeder dissen !... Nog 1 piep uit je bek en je PC is er aan, niet alleen je PC , maar je heel internet leven want ik publiceer alles wat ik heb van je ! Inc je outlook database !

The last part is in Dutch and roughly translates as:

"P.S. Hey you asshole!, next time go and diss your mama! If I hear as much as one more sound out of you, your PC will die and not only your PC, but your entire online life 'cause I will publish all I have of you! Including your outlook database!"

I say "roughly" because I did not feel like translating the huge amount of spelling errors and it's hard to literally translate so much foul language.

Well, of course I was rather surprised. First of all my pc seemed to have been hacked. I run a dekstop on which I dualboot windows XP and Red Hat Linux and on this box I keep all my personal stuff. So naturally I did not feel very happy about all this. What surprised me however, was the fact that the hacker stated he did this because I "dissed" him. Yes, once in a while I wake up on the wrong side of the bed; I have a few beers to many or my girlfriend brakes up with me. On those days, I can be quite the grumpy guy, but normally I'm actually quite friendly. I try to answer questions on the board with patience and reply in a normal fashion to even the dumbest memos I get. I actually often take the time and effort to memo people when I delete their post, to tell them why I did it, so next time they'll know the drill and their posts wont get deleted anymore. And on februari the 8th I woke up on the right side of the bed, I hadnt had too much beers, and my girlfriend... well she had left me way back ;-) So there was no reason for me to "diss" anyone. And I couldnt remember having done so the last couple of days. As it turned out, I had replied to "attacker's" post on the board in which he asked how to create a virus that shuts down anti-virus software. I replied to him that viruses might not be the best way to go, because eventually they always land you in trouble. I guess this to him is "dissing". Anyways, at least now I knew what his motivation had been.

The Actual Trace

Part One

After the whole idea of my ass being owned had sunk in a little bit I had a look at the account details for mr "attacker" His account had been created on feb. 23 2003. This meant I was dealing with someone who had been with neworder for over a year. So that kinda ruled out the chance of it being anyone I know in real life. I already knew he was dutch or belgian because he left part of his rant in the dutch language. So what did I know so far? He (I assumed I didnt get owned by a girly) was probably dutch, had been a member of neworder for over a year and his nickname was "attacker". Also there was the ip-address he used to post his rant. However, this IP turned out to be useless, since it was a proxy.

But, the attacker made a few mistakes himself. For one, he obviously kept coming to the neworder board, asking questions and in doing this, he gave me the chance to find out more about him. First he showed up using the following hostname: *.speed.planet.nl Planet is one of the largest Dutch Internet Service Providers and "speed" in the hostname means that he was on a ADSL connection. So now at least I knew he wasn't using a proxy. So I thought I had him. The good thing about him using *.speed.planet.nl is the fact that this ISP gives out static IP-addresses and hostnames for this service. Nitrate2k was kind enough to get me the full hostname and IP-address from the neworder server logs and now I had a real place to start. So I got out my remote auditing tool and thought I would just start of with a scan to see what I was dealing with. To my surprise and joy I found this guy had 13 known vulnerabilities, including open netbios ports that could be connected to with a null session. You can imagine that by now I had a few plans of my own. I also surfed to the website that was hosted on this IP and what I saw there was even better. I was welcomed by a default introduction page of PHPTriad. And after some snooping around I noticed I could enter the phpmyadmin control panel. This was too easy. And so I looked through the mySQL database a bit, but couldnt find all that much interesting stuff. But then again, mySQL was running as a root process. And I had acces to it. It all seemed a bit to easy.

But then things changed. The attacker started showing up at neworder with a different hostname: *.a-chello.nl Chello is another Dutch ISP, one that provides cable modem connections. This got me a bit worried. Most of all because after running a scan on this IP/hostname (which is static too) I found out this one had no vulnerabilities what so ever and had almost no services running. This was not good news. By now I didnt know which ip/hostname combination was his. Was it the *.speed.planet.nl or the *.a-chello.nl one? Since it is not likely for someone to have both an ADSL and a Cable connection in his home, from two different ISP's, only one could be his. The other must have been at some public place like a library or a school or University, or maybe at one of his friends houses. Lateron he kept on coming to neworder with the *.a-chello.nl hostname so I focused on that one as being his. As said before, the remote box was secured quite well, or at least had none of the known vulnerabilities and had a minimum of services running.

Three Choices

I now had a couple of choices. I could forget about it, secure my box better and get on with my life. That's one. I had IP/hostname information about 2 accounts he used, I had the post he made on the board, revealing info about me and I had a whole bunch of entries in my apache server log, coming from his IP, obviously trying to hack me. So my second option would be to contact his ISP with this information. At best that would get them as far as to disable his ISP account, but even if they were to go that far, I would never know because they probably wouldn't tell me. And chances were they'd just give him a warning. I could go to the police, that was another option, but would that really be worth the trouble? For me or for them? I don't know. The Dutch police are (like in many countries) getting stricter ans stricter. Laws are being passed often and punishment is getting higher. For now, I decided not to. Then there was the option of plain old and cold revenge. I chose last. If I would succeed that would be cool. If I would not, I could always fall back on my contingency plan: contact his ISP and contact the coppers.

Part Two

I was gonna find out as much as I could about this guy. Now time was on my side. I could take as much time as I needed and while I did I got madder day by day. Who did this fucker think he was? Messing with me and my computer while all I did was try to give him some good advice. Free of charge I might add. And thus, while working on securing my box better, I started to try and find out what ever info I could. But that was harder then I thought. What did I have to go on? An IP-address/hostname combination. The knowledge that he lived in my country. That was about it. Now I

see all of you thinking: "Social Engineer his ISP, get that account information from them! You'll have everything you would ever want! His name and address!"

But when push comes to shove and you actually decide to give that a try, you'll notice that just getting someone on the phone who has access to that kind of account information is just not as easy as it is in the movies. And even if I would have, convincing them to give me the info would have been quite the mission impossible. Needless to say I'm not Kevin Mitnick and the Dutch ISP's aren't dumb. But one night, while talking to rattlesnake online I came up with an idea. Why not try social engineering the attacker? I mean, he still visits neworder. Why not? I talked about the idea to rattlesnake and resolution, and we decided I could at least give it a try. And thus I created a new account at neworder. (Which the attacker could have seen from the account details, but luckily he didn't) and this time used proxies. I used a proxy in the USA. Why? Cause for a short while, I was going to be an American. Why? Well basically, because I couldn't be Dutch. That would be too obvious. Then Mr "attacker" posted the following question on the board (something like this):

"How can I make a website so that it installs software automatically on the visitor's PC?"

And this is where my new identity called "JBA" stepped in. I logged in with my new account and memod Mr "attacker" the following:

*"Hey 'attacker',
I read your post on the board. You might wanna have a look at the following links, hope it's what you're looking for. "*

And with this text I memod him a few links. One to a website that checks your browser for known vulnerabilities and explains how to protect yourself against it. And another, a Microsoft security bulletin describing a vulnerability in Microsoft Internet Explorer, allowing a malicious website to execute code on a victim's machine. It seemed Mr "attacker" did not catch on to what was happening, because a day later or so, JBA (me) received the following memo from him:

*"Thanx, this IS what I am looking for. Do you perhaps know a site with instructions on how to exploit these vulnerabilities?
Thanx"*

Note that I'm literally copying this from my memo's, so the spelling errors are his, not mine ;-) Things were going well. He fell for the social engineering and didn't seem to be suspecting anything. It was going to take some time, but in the end I would get him to trust me enough for him to tell me things about himself. His e-mail maybe, or his name. But I got impatient. And his replies showed so obviously that he didn't know what was going on, that I took a chance. I memod him the following in reply:

*Hey 'attacker' Man,
I'm glad you liked the link I send you ;-) I got some more good stuff for you. A few months ago I was working free lance for a small security company and I did some small research into known internet explorer vulns. Nothing big, but still you might like it.
Anyways, have a look at this:*

*http://www.sinred.com/modules.php?name=Downloads&d_op=viewdownload&cid=5
<http://www.sinred.com/modules.php?name=News&file=article&sid=159>*

*It's a kiddie site but they coded some usefull tools that allow you to use the internet explorer (execute) vulnerabilities very easily! And here's some extra info on one of them:
http://vil.nai.com/vil/content/v_99242.htm*

I think the first two links are probably the most useful to you. btw, I'm not much at neworder cause I work fulltime....but do you use an instant messenger (MSN/ICQ?) or something? Let me know so I can add you. Let me know if you need more help...

I'm sittin' here at a boring job anyways... ;-)

JBA

And that's when JBA, or eh.. me, got lucky. I took a chance by asking for his e-mail addy so fast, mainly because it would be only normal for him to expect at least something, after posting that info about me. But this is what he memod me in reply:

*Feb 18 2003, 20:15 (UTC+0) memo ID 60035
"Hey thanx those are some rely nice links !!
U can ad me on MSN : attacker@hotmail.com
Later"*

When he gave me his e-mail addy I had a real place to start. The idea was to continue my social engineering scheme and get more information from him. Obviously, posing as a friendly and helpfull person had earnt JBA (me) some trust. The next thing I did was visit old and trustworthy google. I entered his e-mail address and hit the search button. It returned exactly one single hit. Damn, that's not much! But this single link would prove to be pure and solid gold. Google directed me to an online magazine. An online magazine in the Papiementu language I might add. And well, I dont know about you guys but my Papiementu is kinda rusty :-). After translating some Papiementu sentences to english I found out this magazine was for people in The Netherlands, who come from one of the ABC-Islands and live in The Netherlands. Or something like that. The ABC-Islands (Aruba, Bonaire and Curacao) are part of the Dutch Kingdom. They were Dutch colonies once, but now have earned their independece. A lot of people from these Islands live in The Netherlands. In this magazine there was a small post, that was signed with the e-mail address , thats why google found this one link. But with that e-mail address, there was also a name; . I now not only had the e-mail address but also the first and the last name of the attacker. I was getting somewhere! The next thing I did was search google for his full name. I found 2 hits this time. One gave me a 404-error (page not found) and one led to an advertisement, where the guy was asking people if they had a particulair motorbike for sale. And the good thing is, he left his cellphone number with the add, so that people could call him, if they would have this motorcycle for sale. His cellphonenumber! The last thing I did was go to the Dutch online phonebook. I searched a few of the major dutch cities for his last name and shortly after I got a full hit. The phonenumber I got of the internet, was there, together with the name and full home address of the attacker. I had him ;-). A week or two had passed since the break-in and in the end it took me just a few memo's at neworder as my new split-personality JBA and maybe a few hours of info gathering on the web to trace the attacker back to his home address.

Payback Time

I now had all the information I could have hoped for and all the information I needed for a full, sweet revenge. I'll leave to you the thoughts about what I could have done and will tell you what I actually did. The following might sound incomprehensible to some of you and I hope wise to other, but I decided to do nothing. Nothing??? Well, yes, nothing in terms of revenge. Why you may ask.. First of all, having succeeded in tracing this guy all the way to his home address was a huge achievement itself. I was looking at his full name and a picture of him. I could walk by his house, I could even follow him if I had wanted to. It felt damn good. I now had the power to take big revenge, but merely being able to do so, was reward enough for me. Second of all, as time went by I got more and more anxious to trace the attacker, but even though it was great feeling to succeed and actually trace him, I basically lost interest to retaliate along the way.

Anatomy of The Hack

To be honest, there isn't really an anatomy of the hack. Or rather, I don't know the hack was done. It's been difficult for me to find out just what happend during this hack and how he got in, how far he got in and whether he actually got in. As for the information he posted about me; my name and age were on my website. He obviously just copied that. No elite-ness there. The neworder cookie, well that could have been done by taking advantage of known vulnerabilities in the version of internet explorer I was using. Or thats what I believe, mainly also because he memod me saying I was a dumbass for not using proxies. That could mean he never actually really hacked my computer, but only tricked me into visiting a malicious website. This could be possible. However, that leaves a few questions. There's the path for my apache server, but it was version 2.* and that gets installed as a default in C:\Program Files\Apache Group\Apache2 and this is information he could have also obtained by using a known vulnerability for apache on windows that allows an attacker to view this path. But that leaves the

system info, the running tasks and the fact that he knew I ran Kaspersky Antivirus Software. And that's what troubles me. The "outlook database"-comment also makes me wonder. I don't use outlook, so there's no data there. People have suggested that he may have used a trojan, but I have my doubts about that theory. My computer is in a Local Area Network, behind a hardware firewall/router. There were no ports forwarded from the router to my computer, with the exception of port 80 for my webserver. And although a trojan is capable of opening a port on a pc to transfer data from the server to the client, I doubt it's capable of accessing my router, which is of course password protected and then setting it to forward a trojan port to my pc. Somehow I don't see this happening, but feel free to correct me if I'm wrong on this. Most of what I'm doing here is guessing anyways. This brings me to my apache server logs. My logs were horribly full of signatures that showed many people had been trying to hack my website ever since it was up. None succeeded, luckily. The attacker in this case left more log entries than the rotten sandwich in my room has green spots. It's hard to determine from the logfiles what kind of remote auditing tool / scanner he used. And having no experience with analyzing server logfiles for hacking attempts, I couldn't make much up from it. In the end my guess is he made use of a vulnerability in my browser, tricking me to visit a certain link and maybe some sort of file disclosure vulnerability in the version of the apache webserver I was running. Any suggestions or guesses are of course welcome ;-)

Note

I am not a vengeful person and therefore I have changed the name of the hacker used in this article and I have disclosed virtually none of his personal information. Why you might ask? For one I have neither the time nor the lust for a full scale cyberwar with anyone. I like to consider myself an intelligent being; I enjoy computers and computer security and do and have at times (like I'm sure most of you) pushed the boundaries of what is legal and what is ethically and morally acceptable, but I see no usefulness in trying to destroy someone's computer or perform any other purely malicious act. However, having that said I would like to promise that if in any way he does or tries something similar again I will not hesitate to take all collected data, including apache server logs with his IP to the nearest police station or directly to our National Cybercrime Squad. And believe me when I say that these people are anxiously waiting for easy cases.

Afterword

At the end of this little article I would like to take the opportunity to thank a number of people who helped me out with all this. Thanks go to marek and nitrate2k who offered their help and provided me with the full hostname and ip-address of the hacker from neworder's server logs. Disclosing this kind of information about neworder members of course is not normal procedure but I'm glad that in this case they decided to make an exception. Also my thanks go out to both rattlesnake and resolution who helped me out during my search. Your friendship in cyberspace is very much appreciated!

Paris2K
