From: michael.brunker@MSNBC.COM (Brunker, Michael)  
Date: Tue, May 16, 2000, 8:24am (EDT-3)

To: ulTRAX@webtv.net Subject: I'd like to talk to you

Hi. My name is Mike Brunker and I am a reporter with MNSBC.com  
(http://www.msnbc.com). I'm working on a story about Web TV security and  
stumbled across your Web pages detailing your explorations of their  
system. I'd like to talk to you about some flaws I've been hearing  
about. If you wish to remain anonymous, I can guarantee that I will not  
name you in any article I may write on this subject. If you're willing  
to talk, please reply to this email with a phone number and best time to  
call or, if you prefer, phone me at 425 703-3695. Or, we can correspond  
by email if that's your preference.   
Thanks for your consideration.

From: ulTRAX@webtv.net [mailto:ulTRAX@webtv.net]  
Sent: Tuesday, May 16, 2000 8:22 PM  
To: Brunker, Michael  
Subject: Re: I'd like to talk to you   
I don't mind discussing any topic with the press. But I have to wonder  
how well MSNBC can critique a wholly owned MS subsidiary.   
Please send me the URLs of some of your stories.   
Thanks!

From: michael.brunker@MSNBC.COM (Brunker, Michael)  
Date: Wed, May 17, 2000, 6:16am (EDT-3)

To: ulTRAX@webtv.net Subject:  
RE: I'd like to talk to you   
ulTRAX,   
Wisely, Microsoft has never made any attempt that I'm aware of to try to  
influence what MSNBC reports. Also, MSNBC is a joint venture of  
Microsoft and NBC, not a wholly owned subsidiary.   
Here are a couple stories for your perusal. I look forward to talking to  
you soon.   
http://www.msnbc.com/news/382561.asp   
http://www.msnbc.com/news/178825.asp   
http://www.msnbc.com/news/334729.asp   
http://www.msnbc.com/news/231737.asp   
http://www.msnbc.com/NEWS/287419.asp  
  
  
-----Original Message-----   
From: ulTRAX@webtv.net [mailto:ulTRAX@webtv.net]  
Sent: Wednesday, May 17, 2000 10:13 AM  
To: Brunker, Michael  
Subject: RE: I'd like to talk to you

Thanks for the links to your stories. I don't mind discussing any aspect  
of WNI security to a point. For example there are news server leaks that  
leak ANIs, user names, SSL encryption keys etc. I would not say how that  
data can be had. The Ad servers on occasion leak Accipiter (ad profiling  
software) which includes names, ANI, and what must be a person's  
profile. I would not say how this data an be obtained..... though I  
would not mind giving you some of the data so it can be verified as  
leaks. (I'm am trying again to work with WNI to close these leaks.  
Hopefully my new WNI contact will be easier to work with ;-)   
I should mention that while I tend to be the more the archivist of WTV  
hacking, I may not be up on the specific details of all the problems WNI  
has had. That being said... feel free to ask any questions. I think it  
might be better to write me at my other user darkmatter@webtv.net since  
ulTRAX's box is bulging.... and has been targeted for occasional mail  
bombing. I'd prefer no mail went undelivered.   
If you're interested in another WTV site please visit  
http://webtvexposed.tripod.com   
It needs some updating but was pretty accurate up until the Fall 99  
upgrade. I hope the owner finally finds the time to update it LOL.

Message From: michael.brunker@MSNBC.COM (Brunker, Michael)  
Date: Wed, May 17, 2000, 10:01am (EDT-3)

To: ulTRAX@webtv.net Subject:  
RE: I'd like to talk to you   
I appreciate your willingness to talk to me. I'll switch to the other  
address and send you my initial batch of questions shortly.

From: "Brunker, Michael " <[michael.brunker@MSNBC.COM](mailto:michael.brunker@MSNBC.COM)>

To: <[darkmatter@webtv.net](mailto:darkmatter@webtv.net)>

Sent: Wednesday, May 17, 2000 2:57 PM

Subject: Web TV questions  
  
ulTRAX,  
  
Let me start by explaining how I came to begin looking into Web TV security:  
  
I received a tip from a source claiming that a person or persons had  
discovered a way to access Web TV customers' account information --  
including, phone numbers, credit card information, address, etc -- and had  
posted an email address on a hacker news group (this person didn't know  
which one) that offered the data to anyone who wrote to request it.   
  
I'm still interested in confirming that, if you have knowledge that it did  
in fact occur.   
  
But in the course of browsing through your pages and some of the others  
you've linked to I've become intrigued by the bigger picture -- i.e. how  
hackers have been able to break through WNI security and are now working  
with the company to try to get these problems fixed. Also, I'm interested in  
the extent to which Web TV tracks users' viewing habits -- which the "WebTV  
Exposed" site accurately describes as Orwellian.  
  
So in addition to the above question about the alleged credit card  
pilfering, perhaps you could start by clueing me in about your efforts to  
get the company to improve security and explain what -- if anything -- has  
come from those efforts.  
  
Thanks again for taking the time to talk about this.

From: [darkmatter@webtv.net](mailto:darkmatter@webtv.net) [mailto:darkmatter@webtv.net]  
Sent: Wednesday, May 17, 2000 3:18 PM  
To: Brunker, Michael   
Subject: Re: Web TV questions  
  
*michael.brunker  wrote:  "I received a tip from a source claiming that a  
person or persons had discovered a way to access Web TV customers'  
account information -- including, phone numbers, credit card  
information, address, etc -- and had posted an email address on a hacker  
news group (this person didn't know which one) that offered the data to  
anyone who wrote to request it."*  
  
Currently the WTV hackers are primarily working on two fronts I'm aware  
of. Some use WNI's developer WebTV simulator for PCs. Other's use the  
regular WTV boxes. This does not mean PC users can not be hacking WTV  
the old fashioned way. To date none of the contacts I know have reported  
being able to access Account Info. Two years ago hacking accounts with  
just the Plus box was possible IF a user ID was known. But I reported  
that to WNI ASAP and it was killed within days.  
  
 I had planned to send you an example of the news server data I  
mentioned in another letter, but the publisher can't find my Netherlands  
site. Hmmmmm. I'll have to track that down. My best guess of what we are  
getting is a login authentication packet sent to all the WTV servers so  
a user's requests can be validated. As part of that packet are session  
IDs, the  SSL encryption key, one's phone numbers, user ID list. It  
might contain a real name.    
  
What I referred to in another letter are RANDOM news server and ad  
server leaks that do give personal info. I have not yet received any  
explanation from my @corp contacts what exactly these leaks are so I  
have not told them how we get them.    
   
*"I'm still interested in confirming that, if you have knowledge that it  
did in fact occur."*  
  
It might be possible someone else is getting personal data via another  
route. If they are claiming credit card data or the ability the target a  
particular user, I can NOT confirm that from my sources or experience.  
  
*"But in the course of browsing through your pages and some of the others  
you've linked to I've become intrigued by the bigger picture -- i.e. how  
hackers have been able to break through WNI security and are now working  
with the company to try to get these problems fixed."*  
  
Then there's all the stories I have not put up LOL. WTV hacking seems to  
fall into two broad categories. The first is when we  are actually able  
to get data or have some capability we're not supposed to have. Hacking  
accounts two years ago qualifies. Hacking into the Previewer (alpha &  
beta tester) NG's qualifies. Connecting our boxes to other WNI networks  
such as Daily (Testdrive), Weekly, or Genpack qualifies. Being to  
remotely delete other users qualifies. Then there's category two where a  
perp uses WTV code to, say make one's box send out NG posts or letters  
without the user's knowledge. There was recently a case where a perp  
conned our boxes into sending him our box's Silicon Serial ID number  
(SSID). What can be done with SSIDs is not yet known. I recently found a  
box transfer code that uses the SSID.   
  
"Also, I'm interested in the extent to which Web TV tracks users'  
viewing habits -- which the "WebTV Exposed" site accurately describes as  
Orwellian."  
  
WNI seems to have a corporate culture intent on invading our privacy....  
and never coming clean about it. The WTV Exposed site one of my protests  
against their policies. I think everything there has been well  
documented.... as best I could given  WNI's refusal to provide  
confirmation about their specific tracking. But remember that site does  
not yet reflect more recent info. For instance with the Fall 99 Upgrades  
WNI began to finally offer users an opt-out  from the TV surveillance.  
Scant consolation given WNI had been stealing this private data from  
Plus users for a year and never formally notified us. Also needing  
updating at the Site is a review/analysis of the current TOS and Privacy  
statements.   
   
"So in addition to the above question about the alleged credit card  
pilfering, perhaps you could start by clueing me in about your efforts  
to get the company to improve security and explain what -- if anything  
-- has come from those efforts."  
  
My first efforts to warn WNI about security breaches go back to March 98  
when I noticed the mail servers were handing out User & Subscriber IDs  
in returned mail reports. It took 4 months for WNI to kill it.... then  
the numbers reappeared some 4-5 other times over years. This was  
scandalous since all I needed to hack accounts two years ago was the ID  
#.   
  
WNI was able to kill my ability to hack accounts within a few days after  
I notified them on May 7 98. I'd really have to think back to all the  
times I contacted them about one problem or another.... probably about  
15 times. Often it was about WTV codes that could be abused... say to  
poweroff another's box, or to cause one's box to mail or post.  The  
Usenet SysAdmin contacted me last December to test security at the then  
new NG voting site.  
  
Most recently I have tried to get WNI to be aware of the new server  
leaks. But this seems to be bogging down. I had to write the Usenet  
SysAdmin twice before the letter was passed on and the person who  
contacted me was not easy to work with so we broke off contact. Another  
recently contacted me about another issue... and I again let him know  
about this private tech data. He seemed to be in shock. But between the  
full mail box and the network being down Sunday, we have not discussed  
this further. I want to know what it is before telling them how we're  
getting it. Then again, that it's leaking should be enough to get them  
to find a fix.   
  
Hope this is a  good start. I'll try to get some examples of the news  
server and ad server leaks.... but why do I suspect the site has been  
deleted?

From: "Brunker, Michael " <[michael.brunker@MSNBC.COM](mailto:michael.brunker@MSNBC.COM)>

To: <[darkmatter@webtv.net](mailto:darkmatter@webtv.net)>

Sent: Wednesday, May 17, 2000 6:41 PM

Subject: RE: Web TV questions

This is a great primer and I thank you for it and for the examples you sent.  
  
I'm going out of town tomorrow for a few days, but will be back on Monday  
and will probably have another batch of questions for you then.   
  
In the meantime, please drop me a line if you hear anything further from Web  
TV types regarding the "leakage."

From: [darkmatter@webtv.net](mailto:darkmatter@webtv.net) [mailto:darkmatter@webtv.net]  
Sent: Thursday, May 18, 2000 7:57 PM  
To: Brunker, Michael   
Subject: RE: Web TV questions  
  
  
I have learned that the news and ad server leaks were plugged back a few  
months ago. The person who I had recently been writing to just was  
unaware of that fact as was I since I had not tried to get this data  
since that time.  
  
Do you have a copy of that NG post claiming someone could get credit  
card numbers of WTV users? I'd like to read it.

From: "Brunker, Michael " <[michael.brunker@MSNBC.COM](mailto:michael.brunker@MSNBC.COM)>

To: <[darkmatter@webtv.net](mailto:darkmatter@webtv.net)>

Sent: Monday, May 22, 2000 12:00 PM

Subject: RE: Web TV questions

ulTRAX,  
Sorry for the interruption in our conversation. I was out of town for a few  
days and occupied with other matters.  
  
Thanks for the update on the leaky servers. That's good news for Web TV  
users, though it's not necessarily positive for me, since it looked like a  
good peg for a story on Web TV security.  
  
I haven't been able to find any evidence of a news group posting on the  
theft of credit card info via Web TV, and my source was unclear on the  
details, having learned about it second hand and not being too knowledgeable  
about hacking. My suspicion -- if there's any merit to this -- is that the  
info was shared in a chat room rather than posted on a news group. But since  
I haven't been able to locate anyone who knows anything about it, I'm  
getting suspicious that this is nothing more than a rumor.  
  
Meanwhile, as I continue to try and get a grasp of a story line, let me ask  
you this:  
  
Based on your experience with Web TV, what do you think is the bottom line  
on the technology? Is it secure and should users feel comfortable that their  
personal information is safe?   
  
Also, has the company been responsive when you've brought security issues to  
their attention?   
  
Thanks again for taking the time to help me understand what's going on here.

From: [darkmatter@webtv.net](mailto:darkmatter@webtv.net) [mailto:darkmatter@webtv.net]  
Sent: Tuesday, May 23, 2000 8:23 PM  
To: Brunker, Michael   
Subject: RE: Web TV questions  
  
[michael.brunker@MSNBC.COM](mailto:michael.brunker@MSNBC.COM) wrote:   
  
*"That's good news for Web TV users, though it's not necessarily positive  
for me, since it looked like a good peg for a story on Web TV security."*  
  
There's always the Privacy issue ;-)  
  
*"I haven't been able to find any evidence of a news group posting on the  
theft of credit card info via Web TV, and my source was unclear on the  
details, having learned about it second hand and not being too  
knowledgeable about hacking. My suspicion -- if there's any merit to  
this -- is that the info was shared in a chat room rather than posted on  
a news group. But since I haven't been able to locate anyone who knows  
anything about it, I'm getting suspicious that this is nothing more than  
a rumor."*  
One never knows. All I know is I can't confirm the credit card angle....  
only the personal data I sent you... and the Ad Server leaks which I did  
not forward. They contained what seemed to be elements of our profile  
developed for targeting ads. I never got enough samples to figure them  
out.     
   
*"Meanwhile, as I continue to try and get a grasp of a story line, let me  
ask you this: Based on your experience with Web TV, what do you think is the bottom  
line on the technology?"*  
  
LOL I had started a thread in the <news:alt.discuss.improve.webtv> box  
called "WebTV's Fatal Flaws". It's somewhat of a rehash of the multi-box  
problem discussed in the <http://webtvexposed.tripod.com> site.  Speaking  
not as anyone with technical experience, I believe having 6 boxes to  
design upgrades for can't be the most efficient way to run a business.  
WNI has committed itself to supporting the older Classic box which was  
nice of them. But as boxes improve, there are more older boxes in the  
pipeline that WNI must support. I think this is one reason why upgrades  
are so slow in coming and bugs in the Client are so slow to fix. Server  
side bugs usually can be fixed within days. Otherwise if I wasn't  
fascinated by the technology I would still be here. I can appreciate how  
WNI  has concealed it's rather sophisticated technology  and made the  
internet as friendly and as foolproof as a toaster. It's very intuitive  
and something even a technophobic senior citizen can warm up to. For  
this WNI deserves kudos.     
  
*"Is it secure and should users feel comfortable that their personal  
information is safe?"*  
  
Is ANY system safe? I think the real question is whether an ISP is  
looking for bugs/holes, has good relations with friendly hackers... an  
early warning network of sorts,  and can fix problems ASAP.  With rare  
exceptions, WNI's problems have little to do with actually leaks in the  
network. I have been able to hack accounts and get that personal data...  
but those holes were plugged fast once WNI was notified.   
  
I think WNI's system does have some flaws that have less to do with  
holes the network, but more to do with how WNI's own codes can be used.  
  
WNI's system uses proprietary URLs such as "wtv-home:/home". Our box  
gets an IP list when we on to provide IPs and ports for each WTV service  
(the "wtv-home:/" part). This allows the network to dynamically balance  
the load on the servers.   
  
Problem with this system is as the hackers (or perps) learn more about  
these codes, they can theoretically trick someone's account into doing  
something like mailing a letter....   
  
WNI has worked hard to prevent us from using these URLs... They have  
been selectively disabled throughout the browser so some innocent victim  
won't open a letter and discover s/he sent a death threat to Bruce Leak  
or some such. Maybe it's a Chat Bomb that floods a distant Chat Room.   
  
But since it's the browser's job to access these URLs, selectively  
sabotaging them in some areas of the browser seems a losing proposition.  
As for me I want access to the URLs because that's how we explore. But I  
want WNI to know how they can be abused in letters or posts.   
  
If this doesn't make sense.. I'll try harder next time.  
  
  
*"Also, has the company been responsive when you've brought security  
issues to their attention?"*  
  
Generally yes. There was the  matter of having to resend a letter last  
December to the Usenet  SysAdmin, but to be fair when I received no  
response to the first letter and I wrote again, he apologized that it  
must have gotten lost. He did forward that second letter and it does  
seem that the problem was fixed several months ago... even without my  
ever saying how we got the private data. I personally think that WNI  
should have better cultivated it's friendly contacts in the hacker  
"community". But then, some of WNI's policies.... as outlined on  
WebTVexposed...  have made me less willing to volunteer info.

From: "Brunker, Michael " <[michael.brunker@MSNBC.COM](mailto:michael.brunker@MSNBC.COM)>

To: <[darkmatter@webtv.net](mailto:darkmatter@webtv.net)>

Sent: Wednesday, May 24, 2000 6:06 PM

Subject: RE: Web TV questions

ULtrax,  
  
I appreciate the thoughtful reply.   
  
After thinking about this for a while, what's most striking to me about what  
I've seen on your Web site and those of your fellow WebTV wanderers is that  
this appears to be a case where a company has benefited from the interaction  
with hackers.  
  
Is that an accurate picture, or is that too simplistic a view (I do recall  
reading somewhere that there were incidents where users were getting booted  
off the system after intrusions were discovered)?   
  
Anyway, if it is the case, how do you think this developed rather than the  
more typical adversarial relationship?   
  
Thanks for continuing to plow through this with me.

From: darkmatter@webtv.net [mailto:darkmatter@webtv.net]  
Sent: Sunday, August 06, 2000 8:21 PM  
To: Brunker, Michael   
Cc: darkmatter@webtv.net  
Subject: about that story...  
  
  
Just wondering if you ever wrote your story on WebTV? If so, what's the  
URL?   
  
On another subject, I'm not sure there's a story in this or not.   
  
Aside from all of WNI's other problems with the last upgrade, there is  
another problem that WNI has REFUSED to fix in over 29 months. Whether  
this is a technical story or a comment on WNI's negligence, is for  
someone else to determine.  
  
There is a well-known flaw in the WTV newsreader. When responding to a  
post, it references the original posts ID but also is linked to the  
Subject Line.   
  
So, say there are two threads named TEST 1 and TEST 2..... if someone  
responds to TEST 1 but changes the Subject line to TEST 2, the two  
threads become "melded".   
  
In the hands of malicious creeps, they can meld 1500 posts in a  
newsgroups bringing it to its knees.   
  
This problem has been known since March 98. WNI has neither fixed it or  
set up any expedited procedures to identify Melders, terminate them, and  
nuke out the problem posts and restore NGs..  
  
Now, 29 months later terrorists are STILL destroying newsgroups at  
will, and despite what must be 1000s of letters to their abuse  
department: the melders run free and the rest of us lose use of the  
newsgroup. It seems paying top dollar for WTV service doesn't get us  
much.  
  
WNI's inaction is also a factor in newsgroup/mail flooding. A webtv box  
can be "tricked" into mailing a letter or posting a newsgroup article  
just by opening a post/letter with these commands. WTV's abuse  
department gets a lot of these letters seemingly sent by users, but this  
technique could also be used to mail a death threat to the President.  
Since the mailto command would actually be an embed from a site, not in  
the letter itself, the perp could easily delete the evidence there.  
(BTW, these mailto bombs can also be used to steal private account  
information such as the box's unique Silicon ID Number.)  
  
Typically these "bombs" have been used to post new bombs containing more  
bomb instructions. The NG system underwent a massive attack last March.  
Over 100 NGs were affected.   
  
These bombs can also be used to flood a user's mailbox or post to a  
distant chat room. There was another "bomb" that used a WTV  
mail-forwarding command to steal user's mail. One such mail-theft post  
probably affected hundreds of users and forwarded their mail to a  
hotmail account.   
  
Maybe NONE of these problems has an easy technical fix. In which case  
it's up to WNI to QUICKLY identify these posts, nuke them, then  
terminate the user.   
  
But here is the problem. WNI's abuse department has NO way to quickly  
deal with these problems. I have identified flooder posts and have  
written abuse, the NG SysAdmin, their usenet@corp addresses, and cc:ed  
to Bruce Leak. WEEKS later, the flooder/info-theft/mail-bomb posts are  
still up. I cannot remember when WNI last nuked a bomb.  
  
Is there a story here? Maybe not. But then again, is this MS/WNI's idea  
of customer service in the face of the competition?  
  
ulTRAX

From: Brunker, Michael - michael.brunker@MSNBC.COM  
Subject: RE: about that story...   
Date: Mon, 7 Aug 2000 14:11:18 -0700

ulTRAX,  
  
No, I never did write anything based on our earlier conversations. I felt  
like I had some interesting material, but I was still searching for a "peg"  
when I was shanghaied for some other project.  
  
This mailbombing abuse and lack of action by WNI does sound interesting, but  
I'd like to find out a bit more about it before I decide to proceed. And  
first I need to finish up a project I've been working on, which will take a  
couple days.   
  
I'll message you again on Thursday or Friday and set the conversational ball  
in motion if that's OK with you.  
  
Thanks for getting back to me.  
  
Mike Brunker