

RE: remote control program

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-06/msg00056.html>

- *From:* "Joel" <joel@xxxxxxxx>
 - *Date:* Mon, 2 Jun 2008 22:25:20 -0400
-

Adriel –

Point taken. It was late and I misunderstood/misread your comments. I didn't consider that you meant back-end security measures when I responded; I thought you were among those concerned with MITM attacks, which is obviously why I mentioned SSL. I do not know the back-end protection for logmein any more than I know the back-end protection for my bank. There is some risk that is acceptable to me. I expect a company that knows it will put itself out of business if they are vulnerable to an attack is not going to implement poor protective measures, but some would disagree with that line of thinking. I've never seen a vulnerability reported on them anywhere, although that's certainly no guarantee of security.

Regards,

Joel

-----Original Message-----

From: Adriel Desautels [<mailto:adriel@xxxxxxxxxxxx>]

Sent: Saturday, May 31, 2008 10:36 AM

To: Joel

Cc: sgp@xxxxxxxxxxxx; security-basics@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Subject: Re: remote control program

Joel,

The security of the interface has nothing to do with SSL. In fact, the security of your online banking technology also has nothing to do with SSL. SSL is only good for protecting data in transit, it does nothing at all to protect the end-points. If you can hack the end-points (client or server) then you're golden from a hackers perspective.

Likewise, your password is irrelevant especially if one of the end-points is hackable. If the technology was not properly assessed by a qualified security team then I wouldn't trust it. When I say properly assessed I mean exposed to the wrath and curiosity of a vulnerability research and exploitation project. I do not mean some crack automated scan or quickie assessment.

RE: remote control program

To get in to the application one does not need credentials, one just needs an exploitable vulnerability. SQL Injection, RFI, LFI, XSS for Phishing, etc. Those are the real keys to the kingdom, and your networks _if_ the technology is vulnerable.

Regards,
Adriel T. Desautels
Chief Technology Officer
Netragard, LLC.
Office : 617-934-0269
Mobile : 617-633-3821
<http://www.linkedin.com/pub/1/118/a45>

Join the Netragard, LLC. Linked In Group:
<http://www.linkedin.com/e/gis/48683/0B98E1705142>

Netragard, LLC – <http://www.netragard.com> – "We make IT Safe"
Penetration Testing, Vulnerability Assessments, Website Security

Netragard Whitepaper Downloads:

Choosing the right provider : <http://tinyurl.com/2ahk3j> Three Things you must know : <http://tinyurl.com/26pjsn>

Joel wrote:

How secure is any administrative interface on the web? It's only as good as the SSL, which has been broken in theory but not in practice that

I'm aware.

I bank online because I trust the interface and the encryption, but I guard my password carefully and (should) change it (more) often. I do the same with the master account password for logmein. Still, your last comment isn't true for the product... from the website it's no free lunch if some malfeasant gains the account credentials. On the website you have to know the username and password for each computer when you attempt a remote session.

More conveniently, the Ignition product has an interface that sits on my laptop and allows me to gain access in 5 to 15 seconds. And the access is usually as fast or almost as fast as being at the desktop. YMMV based upon your throughput. I have 7Mbps down and 2Mbps up at my office; that may influence the speed. However, I have a partner company that uses Ultra-VNC for remote work to the same location who complains about jitter and delay when I have no problems with at all.

Back to security, I trust that my local machine is well-secured and don't mind the Ignition program caching the credentials for all of the

RE: remote control program

users and servers. While I'm happy that the website does not cache credentials, it wouldn't be a security issue I would lose sleep over if it did as long as my channels are encrypted end-to-end. From what your company site states, testing the accuracy of the logmein encryption claims might be something you can investigate independently. If you do and find otherwise, I hope to see your findings

here or on pen-test or bugtraq.

I really do sound like a plant from the company, yes? I'm not.
<http://www.linkedin.com/pub/7/6ba/923>

Regards,

Joel
Joel at SecureNA dot com

-----Original Message-----

From: Adriel Desautels [<mailto:adriel@xxxxxxxxxxxxxx>]
Sent: Friday, May 30, 2008 7:03 PM
To: Joel
Cc: sgp@xxxxxxxxxxxx; security-basics@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Subject: Re: remote control program

So it sounds like a legit tool. What are the security implications of using this tool? How secure is the administrative interface? RAT tools always concern me when thinking about security. If a malicious kid gets control of the administrative credentials or the administration interface its very much game over. Just a thought.

Regards,
Adriel T. Desautels
Chief Technology Officer
Netragard, LLC.
Office : 617-934-0269
Mobile : 617-633-3821
<http://www.linkedin.com/pub/1/118/a45>

Join the Netragard, LLC. Linked In Group:
<http://www.linkedin.com/e/gis/48683/0B98E1705142>

Netragard, LLC – <http://www.netragard.com> – "We make IT Safe"
Penetration Testing, Vulnerability Assessments, Website Security

Netragard Whitepaper Downloads:

Choosing the right provider : <http://tinyurl.com/2ahk3j> Three Things
you must know : <http://tinyurl.com/26pjsn>

RE: remote control program

Joel wrote:

If you refer to the website and search for review, you'll find that the company is legit and has been around quite awhile. They were once called remotelyanywhere, and I don't know why the name changed, but they are very professional whenever I've called. I've had almost zero downtime over the past three years, and I said in my last post, I have 60 licenses I use every day, and I do mean 365 days a year, for remote

support all over the country.

I don't know about LAS region support. I'd call the company and ask them about any routing concerns.

Of a dozen remote tools, this is by far the most advanced tool on the market. Drag and drop to the remote screen, sound from the remote screen, print to your local printer from the remote, magnify, whiteboard,

chat, etc.

Did I mention inventory and alerts? I'm a walking ad for the company because my company is a success since this tool is so well designed. I've supported sales reps driving down the highway. Today I used my AT&T Tilt (a Windows Mobile phone) to do a remote session while I was away from my office. I've copied files for a user while playing golf on a weekend. WM6 support is a rare find. For <\$40 a year per license, I

couldn't ask for more.

Regards,
Joel

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx
[mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx] On Behalf Of sgp@xxxxxxxxxxxxx
Sent: Friday, May 30, 2008 4:10 PM
To: security-basics@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Subject: Re: remote control program

Thank you all for the answers, I need to implement remote administration several branches of my clients and was evaluating the tool (Logmein) to implement, at first I thought was spectacular, by not having to configure anything on the routers to allow access from

RE: remote control program

the

internet.

But I am very concerned about whether the tool is reliable, in other words if the company owns the tool is.

Regards.

Sergio Properzi.
San Luis Argentina.