

Re: Need some help

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-05/0049.html>

From: Drew B. [Security Expertise/Freelance Security research]. (*d4rkstorm_at_gmail.com*)

Date: 05/15/05

Date: Sun, 15 May 2005 11:21:25 +1000

To: "M. Boelen" <michael@rootkit.nl>

Thankyou,

I will send you the mailer 'kit' and the optional information regarding the extern dependancies, and a referrer incase you need to know more info.

The files are complete and intact (the kit was found before the people had a chance to rm a thing).

Notes for others (security minded) while this kit is examined more :: It was not well installed, a better trained Unix user would have made this thing extremely well hidden (the installation was the main reason the machine was even seen,i suspect this would be running nice and safe on many other mail apps, and even now i have started to see a qmail.* ebay-spoof,so perhaps they hve even patched)

This was a 'good' coder/s, but they obviously have some trouble with facets of running/maintaining a fBsd machine using Qmail.

The webdownload info (3 sites it somehow uses),and 5 irc servers on Undernet.org seem to be the actual source of the controlling.

As mentioned,its unfound and the closest I could get to examining it was after many many hours and alot of help and use of rKhunter.

The only reason i have not forwarded this to an A/V company is my lack of faith in them,and simply no time, my apooogies.

For the A/v who are keen to improve theyre apps;

The FreeBSD Port of F-Prot was running nice and happily alongside it:(. (The app that actually spotted the malfunction after running tests seem to be rKhunter,but that only displays some 'possibles' , as mentioned,it will run happily with F-prot,hence i assume it has been encrypted well). Also, strangely, It shows up as an 'infected' file using a heuristics test with AVG (www.grisoft.com) on Windows,using theyre "free" version.

Regards,

Drew B.

PS: Excellent job with rKhunter,I look forward to any help i can give and get from rKhunter :-), regarding 'spare time' i would help gladly.

Expect the complete kit in 20mins max Michael,again thankyou.

On 5/15/05, M. Boelen <michael@rootkit.nl> wrote:

> *Hi,*

FreeBSD-Security: Re: Need some help

>
> *I'm the author of Rootkit Hunter, and ofcourse interested. Unfortunately*
> *I can't promise you to investigate it (within a small amount of time-->*
> *due to my spare time..). If you want, you can also send me the file(s)*
> *later.*
>
> *If you decide to give me a copy, please password-protect the files*
> *(rar/zip archive).*
>
> *Michael*
> *Rootkit.nl*
>
>> *Hello,*
>> *I would like to ask for some specialist assistance in dissecting a*
>> *'rootkit' (seems to be massmailing specific,crafted somehow from*
>> *another kit perhaps)*
>>
>> *It was found running on 5.x machines belonging (sofar) to my*
>> *knowledge, 2 companies,one of wich was an isp and another a webhosting*
>> *service running bsd.*
>> *I will provide the kit and further details as soon as i am sure the*
>> *thing will be dealt with by someone official.*
>> *Being properly examined so all exploits within it can be marked*
>> *out,whether new and/or old-modified is important and I cannot*
>> *successfully complete dissection with my current equipment.*
>> *The attacks are still happening, the familiar 'ebay' login page or*
>> *paypal, however, the bug itself is Linux-platform speciic, extremely*
>> *stable, and extremely hard to remove.*
>> *Anyone interested who has the abality,especially an A/V tech/worker*
>> *with a certificate from the company or atleast email header,or anyone*
>> *associated that can link this to freebsd security offically.*
>> *I can confirm that it is stable and running on v5.x FreeBSD now, and*
>> *have no idea how long i has been around.*
>> *Regards,*
>> *(&&assist)*
>>

>> *Drew B.*
>> *Independant Security analysis,for Aussies.*
>> *Security researcher/expert,threat-focus,Freelance.*
>>
>> freebsd-security@freebsd.org *mailing list*
>> <http://lists.freebsd.org/mailman/listinfo/freebsd-security>
>> *To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"*
>>
>
>

--

Drew B.
Independant Security analysis,for Aussies.

Re: Need some help

FreeBSD-Security: Re: Need some help

Security researcher/expert,threat-focus,Freelance.

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"