

RE: Advice for a spreadsheet macro that calls home?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-02/0078.html>

From: Omar Herrera (*oherrera_at_prodigy.net.mx*)

Date: 02/12/05

Date: Fri, 11 Feb 2005 20:24:04 -0600

To: pen-test@securityfocus.com

Hi Marc,

I would rather not use an active tool. At least not so fast (and this might be also a matter of forensics):

a) It might help you avoid potential legal problems (are you sure this is done with a machine property of the company you are working for and there are written policies to backup your actions?)

b) If you are not sure which machine they are extracting the information from, then you might potentially alert the suspect. He might have in place one of those personal firewalls blocking unknown process from establishing connections with other machines on the network (Excel is a good candidate to remain blocked).

c) There are a lot of worms with source code out there and it seems tempting to just grab one and change things here and there just to avoid being identified by an antivirus, but you should also know exactly what other amenities are included with the bug (keyloggers, time bombs, backdoor). Do you have the time and resources to dig into the code and assure it will perform as expected? Worst case scenario: you mess with the suspects machine, the evidence is lost and then he/she points at you for attacking his/her machine.

d) Do you have proof that the file is actually extracted from the machine and executed in another? It might be possible that the information is extracted through other means (keylogger, Trojan horses, social eng. with other information holders,...)

My recommendations are:

First make sure that the machine is not compromised and that the information leak does not take place through other means (check physical access, change passwords,...).

SecurityFocus Penetration: RE: Advice for a spreadsheet macro that calls home?

Second, make clear what your ultimate goal is: to know who did it, to prove that someone did it, or both. Sniffing and physical surveillance might be just enough, unless you really require unquestionable proof of the act.

Third, whatever is your choice, make sure that the client understands and accepts all potential risk and consequences before proceeding.

Regards,
Omar Herrera

- > -----Original Message-----
- > From: marc spamcatcher [mailto:junk@zounds.net]
- > A client wants to find out who is accessing some confidential data on his
- > machine. Looks like an inside job, the IT staff reading an .xls.
- >
- > Putting a 'call-home' macro in the file seems like a good bet, since
- > the file could be pulled in many ways, but must be opened for
- > reading. I'm thinking that when the file is opened, a network connection
- > to a server is opened, and then we know when and where it was opened from.
- >
- > Are there tools/worms that do this already I should look at? Am I
- > over-looking some problems?