January 2004 to September 2015

f-secure.com/weblog/archives/00002227.html

F-SECURE LABS

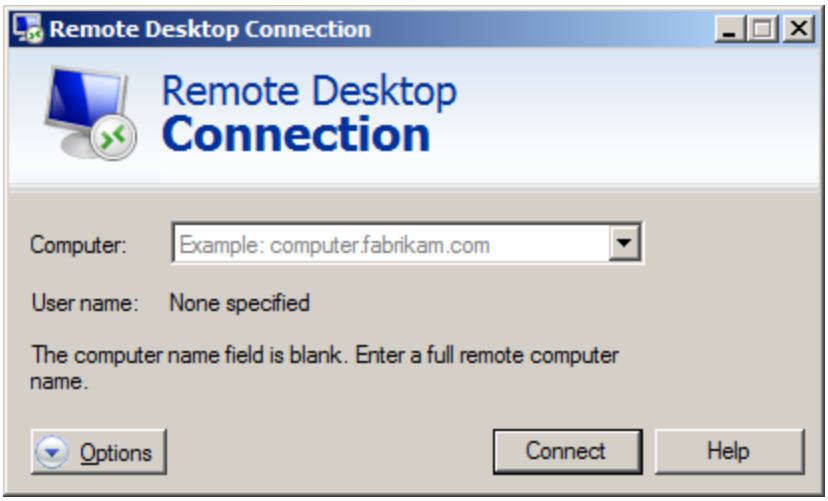
<<< NEWS FROM THE LAB - Sunday, August 28, 2011 >>>

ARCHIVES | **SEARCH**

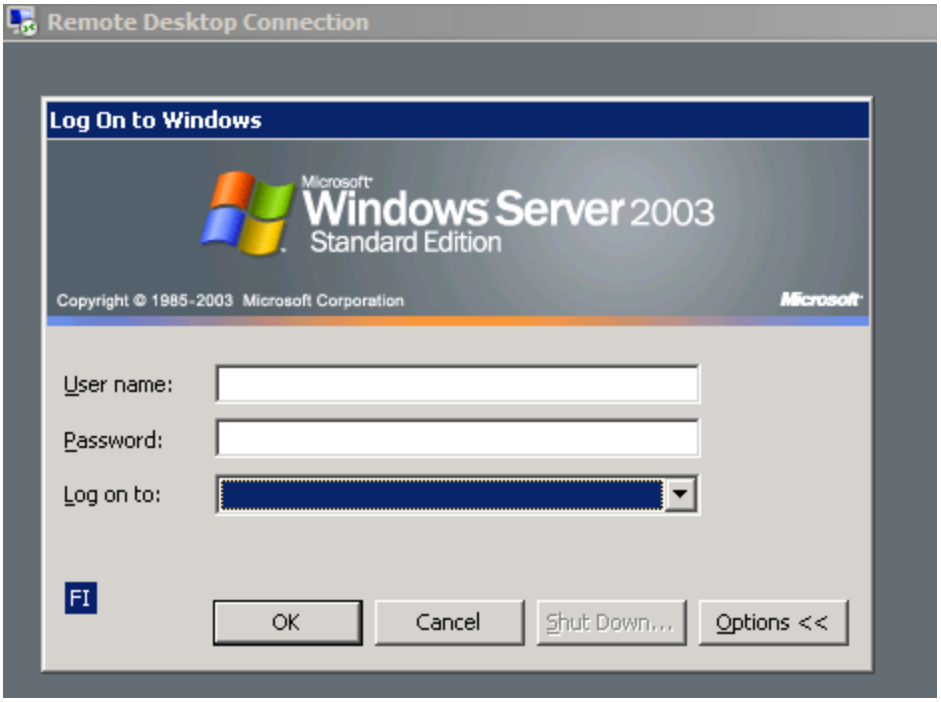
Windows Remote Desktop Worm "Morto" Spreading	Posted by Mikko @ 13:23 GMT

We don't see that many Internet worms these days. It's mostly just bots and trojans. But we just found a new Internet worm, and it's spreading in the wild. The worm is called **Morto** and it infects Windows workstations and servers. It uses a new spreading vector that we haven't seen before: **RDP**.

RDP stands for **Remote Desktop Protocol**. Windows has built-in support for this protocol via **Windows Remote Desktop Connection**. Once you enable a computer for remote use, you can use any other computer to access it.



When you connect to another computer with this tool, you can remotely use the computer, just like you'd use a local computer.



Once a machine gets infected, the Morto worm starts scanning the local network for machines that have Remote Desktop Connection enabled. This creates **a lot of traffic for port 3389/TCP**, which is the RDP port.

When Morto finds a Remote Desktop server, it tries logging in as Administrator and tries a series of passwords:

admin
password
server
test
user
pass
letmein

1234qwer
1q2w3e
1qaz2wsx
aaa
abc123
abcd1234
admin123
111
123
369
1111
12345
111111
123123
123321
123456
654321
666666
888888
1234567
12345678
123456789
1234567890

Once you are connected to a remote system, you can access the drives of that server via Windows shares such as **\\tsclient\c** and **\\tsclient\d** for drives **C:** and **D:**, respectively. Morto uses this feature to copy itself to the target machine. It does this by creating a temporary drive under letter A: and copying a file called **a.dll** to it.

The infection will create several new files on the system including **\windows\system32\sens32.dll** and **\windows\offline web pages\cache.txt**.

Morto can be controlled remotely. This is done via several alternative servers, including **jaifr.com** and **qfsl.net**.

We've seen several different samples. Some MD5 hashes include:

0c5728b3c22276719561049653c71b84
14284844b9a5aaa680f6be466d71d95b
58fcbc7c8a5fc89f21393eb4c771131d

More discussion on the topic at Technet forums.

We detect Morto components as **Backdoor:W32/Morto.A** and **Worm:W32/Morto.B**.

Updated to add: here's a link to our description.