Morto Worm

Justin Chang

February 26, 2012

Introduction

The Morto worm came out in August of 2011 and works by infecting machines via RDP (Remote Desktop Protocol).

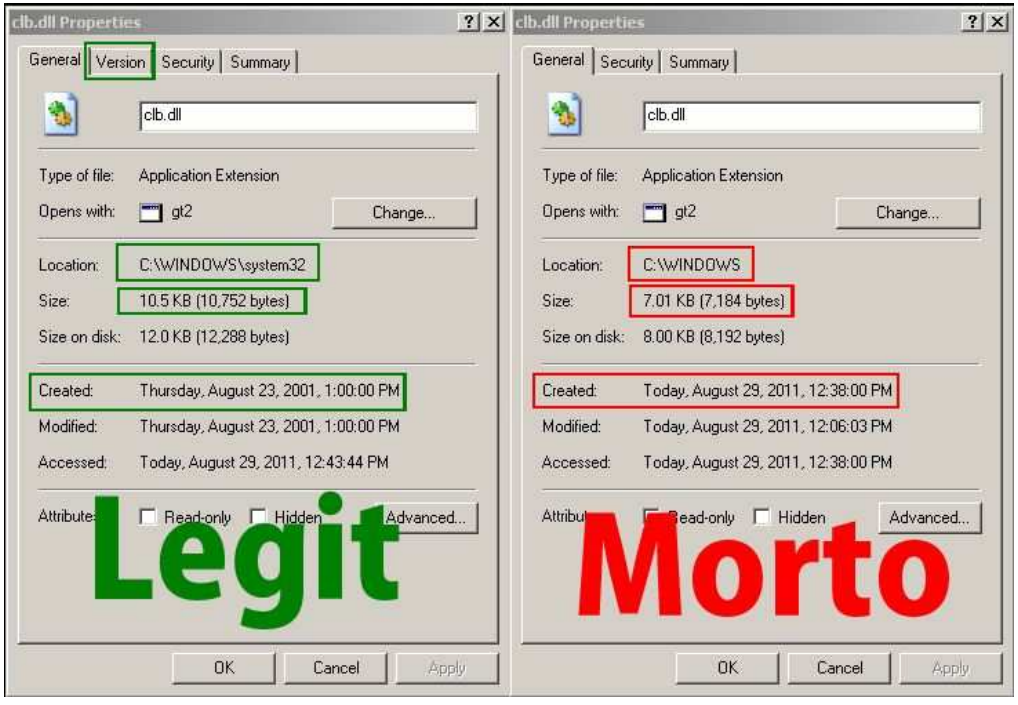
What is a Worm?

- Self-propagating, self-replicating program which uses computer networks to send copies of itself to other nodes (with or without user assistance).
- Causes harm to the network, even if only consuming bandwidth.
- Payload: code in the worm designed to do more than spread the worm.

How Does Morto Work?

- When infected, the Morto worm scans the local network for machines that have Remote Desktop Connection enabled (port 3389/TCP), which creates a lot of traffic.
- When it finds a vulnerable server, it will attempt to log in as Administrator with a series of common passwords such as admin, password, letmein, etc.
- To ensure that it remains and runs on the infected machine, Morto creates a DLL called clb.dll in the Windows directory. There is a legitimate DLL in the System directory with the same name, but when Windows searches for clb.dll, it checks the Windows directory before the System directory.
- Also terminates processes for locally running security apps.

How to Tell if Infected



A normal machine versus an infected machine

What Happens When Infected?

Morto can be controlled remotely. Once the machine is infected, the person controlling Morto has access to:

- Perform DoS attacks.
- Create a backdoor for machine to become a zombie.

Protecting Against Morto

The best way to protect against Morto? Use a secure password!!! Having a firewall and up-to-date security software helps too. And if you become infected...

http://windows.microsoft.com/en-US/windows/products/security-essentials

Questions?

http://en.wikipedia.org/wiki/Computer_worm

http://blog.webroot.com/2011/08/31/morto-worm-annoyances-outstrip-functionality/

http://www.f-secure.com/weblog/archives/00002227.html

http://www.f-secure.com/v-descs/worm_w32_morto_a.shtml

http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Worm%3AWin32%2FMorto.A