Malicious Firefox Extensions

Philippe Beaucamps, Daniel Reynaud

Loria - Carte
http://lhs.loria.fr

SSTIC'08 - June 5th, 2008

Introduction

IE : ActiveX controls, Browser Helper Objects (BHO), ...
Firefox : extensions, language packs, themes, plugins...

Firefox extensions are as powerful, or even more powerful, than ActiveX controls:

- Can be programmed in **Javascript**, **C/C++**, Python, etc.
- Can contain **native code** and run it;
- Usually **cross-platform**.

Stealth

- Hiding from the extensions list;
- Polymorphism, packing, etc.;
- Infecting other extensions (even when signed);
- Can be silently installed by native code;
- All malicious activity (code and network communication) is part of Firefox's innocuous activity.

XPCOM

XPCOM: cross-platform API exposed by Firefox to extensions.

- r/w access to the **DOM** (Document Object Model) of accessed pages, before and after being displayed ⇒ keylogging, personal info stealing, tampering Internet voting, etc.
- Clear access to **passwords** stored by Firefox;
- r/w access to the **filesystem**, the **network** (opening client and server sockets, sending mails, etc.) ;
- ... (more to explore, but it's large !)

Demo

Anatomy of a Security Disaster?

Javascript simplicity
+ Browsers ubiquity
+ Browsers' use for sensitive applications
+ Platform independence
+ No security policy

=

?