Cortana
Rise of the Automated Red Team

Raphael Mudge
@armitagehacker
Overview

- Background
- Cortana
- Distributed Bots
- Post-exploitation
- Behavior Modification
- User Interface

This work was made possible through DARPA’s Cyber Fast Track program.
What this talk is not

- Not a Cortana tutorial
- Some features are skipped entirely
- An exploration of the software agent programming paradigm
  - This is sad
  - Because it is fun
  - 😞
Today’s Goals

- Demonstrate what Cortana can do
- Cover major functionality
- Encourage you to try it.
Introduction: Raphael Mudge

- Formerly, IRC LaMeR
- Developer, jIRCii IRC Client
- Developer, Sleep Scripting Language
- Developer, Armitage
- Founder, Strategic Cyber LLC
Introduction: jIRCii
Introduction: Sleep

- Perl inspired syntax
- Built on Java
- Extensible
- Small! (~250KB)
- Embedded in jIRCii
Introduction: Armitage
Armitage Collaboration
Cortana: What is it?

- A Scripting Language to:
  - Automate Metasploit Framework
  - Extend Armitage
Cortana: What is it?
The Software Agent Lense...

- Cortana is a domain-specific language to develop “Agents” that conduct cyber operations...
  - Team server provides distributed communication
  - Metasploit offers capabilities and data model
  - Cortana offers means to create long running agents that perceive context and respond to it.
  - Cortana also provides tools to debug, understand, and assure positive control of agents
Cortana: What it does

- Metasploit Control
- Data Management
- Post-Exploitation
- Team Server Participation
- Modify Armitage Behavior
- Extend Armitage User Interface
Cortana: Alternatives

- Extend Metasploit Framework
  - Modules
  - Plugins
  - RC files
- Metasploit RPC Server
- msfcli
Distributed Bots
Problem...

- **Jolly:** It’d be nice if there was a way to know when new hosts/services pop up
- **Chris:** I’m constantly running scans, I’ll put the data where ever you like...
- **Me:** I think I can help...
- **Chris:** I don’t want to import my scans every minute. Can we automate this?
on event_name {
    # do this stuff
    # $1 = first argument
    # $2 = second argument
    # $n = nth argument
}
Data Events

Hosts Request N

Fire host_remove event

Do nothing

Fire host_add event

Hosts Request N + 1
Data Events

- Credentials
- Hosts
- Loots
- Routes
- Services
- Sessions
Host/Service Notify Bot
Host Import Bot

DEMO
15:52:29 *** ChrisImportBot-pHEAR joined
15:53:59 *** ChrisImportBot-pHEAR joined
16:01:04 *** *illis joined
16:06:17 <raffi-cortana> I see 10.235.94.140:21 () tcp
16:06:17 <raffi-cortana> I see 10.235.94.190:143 () tcp
16:08:18 <raffi-cortana> I see 10.235.29.12:443 (nginx 0.8.54 ) tcp
display>
Post-exploitation
Problem

- I want to control sessions
  - With multiple actors using them
  - With assurance that the script won’t lose control
Background

- Interacting with a Meterpreter session:

```c
on meterpreter_command { 
    # $1 = session id
    # $2 = command and arguments
    # $3 = output
}
```

```c
m_cmd(session id, "command");
```
Background

- Interacting with a process through a meterpreter session:

```c
on exec_command {
    # $1 = session id
    # $2 = command and arguments
    # $3 = output
}

m_exec(session id, "command");
```
Background

- Interacting with a Shell session:

```c
on shell_command {
  # $1 = session id
  # $2 = command and arguments
  # $3 = output
}
```

```c
s_cmd(session id, "command");
```
A cool demo
Behavior Modification
Problem

- I want to alter how Armitage does X
  - Use a different payload for certain attacks
  - Integrate a different executable with psexec
  - Modify Armitage icon display
Background

- Filters, hook an action and change the parameters

```perl
filter some_filter_name {
    # inspect $1, $2, $3, etc.
    return @_; 
}
```
Another cool demo
User Interface
Problem

- I want to extend Armitage with new features
  - Integrate third-party tools
  - Expose Metasploit Framework features
  - Control Cortana capabilities
Background

- Cortana scripts may:
  - Define keyboard shortcuts
  - Define popup menus
  - Create console tab interfaces
  - Create table interfaces
The last cool demo
Cortana: What is it?

- A Scripting Language to:
  - Automate Metasploit Framework
  - Extend Armitage
Summary

- Background
- Cortana
- Distributed Bots
- Post-exploitation
- Behavior Modification
- User Interface

This work was made possible through DARPA’s Cyber Fast Track program.
Where to go from here...

- Twitter: @armitagehacker
- Email: rsmudge@gmail.com

Cortana is posted at:

- WWW: http://www.fastandeasyhacking.com