Girls Power Tech - Google Chrome Malware & Botnet

Lilly Chalupowski
Security Application Developer - Threat Intelligence
&
Xandria Richman
Cyber Security Analyst - Shift Lead

May 3, 2018

Table of Contents

Abstract

A Girls Power Tech 2018 Google Chrome Malware & Botnet presentation and demo handout.

1 Introduction

In this handout we will cover the terminology and concepts in the presentation.

2 Disclaimer

The tools and techniques covered in this handout can be dangerous and are being showing for educational purposes only It is a violation of Federal laws to attempt gaining unauthorized access to information, assets or systems belonging to others, or to exceed authorization on systems for which you have not been granted. Only use these tools with / on systems you own or have written permission from the owner. We (the speakers) do not assume any responsibility and shall not be held liable for any illegal use of these tools.

3 Github Repository

Download Working Files

chrome-crusader

```
#!/usr/bin/env bash
cd ~
sudo apt-get -qq update
sudo apt-get -qq -y install git
git clone https://github.com/lillypad/chrome-crusader.git
cd ~/chrome-crusader/
```

Project Directory Structure

The project directory structure is as follows:

```
chrome-crusader
├── bin
│   ├── handouts
│   │   └── girlspowertech
│   │       └── girlspowertech.pdf
│   └── presentation
│       └── girlspowertech
│           └── girlspowertech.pdf
├── configure.sh
├── docs
├── LICENSE
├── Makefile
├── requirements.txt
└── src
    ├── chrome-optimizer
    └── cnc-server
```

Programming Languages

- Python
- JavaScript
- JSON

4 Terminology

Malware

> Wikipedia
>
> Software that is intended to damage or disable computers and computer systems.

manifest.json

> Google Developer Documentation
>
> Every app has a JSON formated manifest.json file, that provides important information.

Command & Control Server

> Wikipedia
>
> A computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.

Hooking

> Wikipedia
>
> In computer programming, hooking covers a range of techniques used to alter or augment the behavior of an operating system, of applications, or of other software components by intercepting function calls or messages or events passed between software components. Code that handles such intercepted function calls, events or messages is called a hook.

5 Building the Project

Installing Dependancies

install-deps.sh

```
#!/usr/bin/env bash
sudo apt-get -qq update
sudo apt-get -qq -y install python \
    python-pip \
    chromium \
    texlive \
    texlive-latex-extra \
    pylint \
    npm \
    nodejs
sudo npm install -g jshint
```

Building

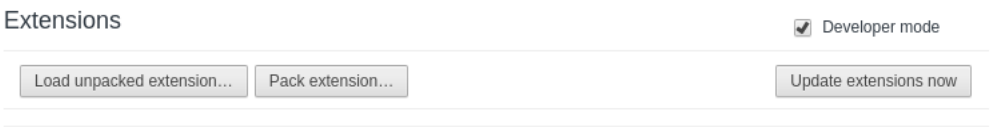
build.sh

```
#!/usr/bin/env bash
make
```

6 Install & Run

Installing the Extension

- Open Google Chrome or Chromium
- Open Extensions Menu
- Check Developer mode
- Load unpacked extension...
- Browse to the folder src/chrome-optimizer/ and click open



Running the C&C Sever

run-cnc-server.sh

```
#!/usr/bin/env bash
cd src/cnc-server/scripts/
./ccserver.py
```

You will now start to see events populate in the sever console.

7 Summary

It is important to be aware of what extensions are installed in your browser as malicious extensions can exfiltrate your credentials, cookies, conversations as well as web history.