

Forum:[Hack Forums](#)

Thread: [The Detailed Guide on Formgrabbers](#)

pr0t0typ3 - June 5, 2012, 2:06 pm

What is Form Grabbing ?

Form grabbing is an advanced method of capturing web form data within various browsers. Often confused with traditional keylogging (recording individual keystrokes), this method intercepts the API in browsers that is used to transmit information and collects web form data before it is passed over to the internet. (Source: Wikipedia.org)

How does Form Grabbing work ?

A Formgrabber does replace the function that is used to send information to the internet with its own function. Every time the browser does submit information to the internet, the replacement function is called first and the intruder is able to access the web forms the browser does send to the internet before they are actually sent. The intruder is also able to modify these forms or prevent them from being sent.

View detailed diagram:

Spoiler [\(Click to View\)](#)

What are webforms ?

A webform on a web page allows a user to enter data that is sent to a server for processing. Webforms resemble paper or database forms because internet users fill out the forms using checkboxes, radio buttons, or text fields. For example, webforms can be used to enter shipping or credit card data to order a product or can be used to retrieve data (e.g., searching on a search engine or logging into a website). (Source: Wikipedia.org)

View example:

Spoiler [\(Click to View\)](#)

[img]http://scdn5.apptivo.com/wp-content/uploads/2012/04/paypal_login.png[/img]

Why are Formgrabbers superior to traditional forms of password stealing malware ?

While Password Stealers only recover credentials saved in the browser and Keyloggers do require the user to type in the credentials, Formgrabbers just require the information/credentials you want to access to be used/sent. No matter if the credentials are typed into the browser (with a physical or virtual keyboard), they are saved in the browser and used to login at a later point or they are copied into the login fields, the grabbing process of a Formgrabber is always successful, while neither a Stealer nor a Keylogger would be able to perform a successful recovery in every case mentioned above.

If Formgrabbers are that good, why can't I find any good cheap one ?

If we look back to the year 2007 when the Crimeware-Pack Zeus was released, and the first "famous" Formgrabber hit the market, you had to invest between 700 \$ and 15.000 \$ (for the full package with all features as there was no standalone formgrabber). You might ask yourself, why there are not tons of good Formgrabbers which are much cheaper if they are really superior to all traditional forms of malware (used for credential stealing) and the answer is pretty easy: They are a lot harder to do than Stealers or Keyloggers. The programmer needs knowledge about the process architecture of Windows, the art of hooking functions (which often have to be found in memory first using special algorithms), a native language like C/C++, Delphi (in exceptional cases) or ASM,

reverse engineering to find out about the behavior of the browser as well as a lot of time and money to invest into a talented web developer to create a powerful web-panel where the logs that have been "grabbed" are sent to. This means that high prices are more than justified, they are needed to preserve the right of ownership for such a powerful and dangerous tool to people who are serious about what they do.

Where can I get Formgrabbers and what do I need to pay attention to ?

In many "underground" forums you can find formgrabbers as plugins or additional modules for HTTP Bots, while standalone Formgrabbers are rare to find. You need to pay attention to a fair price , an unique functionality and a good web-panel (this is a very important point). You might ask yourself what unique means in this context. Over the last months some Formgrabber sources for various Browsers (Internet Explorer and Firefox) became public and have been heavily copied and published, while most people were unable to create proper Formgrabbing methods (Methods that are able to grab HTTP as well as HTTPS traffic) for Google Chrome, Opera and Safari. Also pay attention that the Formgrabber does support the grabbing of SSL encrypted traffic (used by HTTPS connections for many login sites).

Ebol? - June 5, 2012, 2:08 pm

Just skimmed through it, but it looks amazing. Thanks for the guide! I will read it in full when I get home. (:

Orgy2 - June 5, 2012, 2:11 pm

This should stop quite some confusion between stealers, keyloggers & formgrabbers.

Good job bruv.

MineSQL - June 5, 2012, 3:34 pm

To bad more people arnt HQ like you. :(it saddens me that no one replied.

pr0t0typ3 - June 7, 2012, 4:40 am

(Jun 5, 2012 03:34 PM)Editzzzz | Elite.Exe Wrote: [\[CITE\]](#) To bad more people arnt HQ like you. :(it saddens me that no one replied.To be honest, it also saddens me :(I spent around 45 minutes writing this and doing the diagram and people don't even care enough to reply.

Blizzard - June 7, 2012, 4:43 am

Great tutorial, I liked the diagram and it is very well explained. Thanks.

CarrotMilk - June 7, 2012, 12:25 pm

Good stuff pr0t0! Should clear up a lot for some people :).

Kill?Muvz - June 8, 2012, 8:24 am

Now this is good stuff. The concept itself is very easy to understand now the implementation and making it work only good coders manage to do it. Congratulations.

Support™ - June 10, 2012, 4:24 am

I read the whole post carefully and I must agree that this is a very well formed and truly a "detailed" guide.

Thank you pr0t0.

Dynasty@HF - June 10, 2012, 6:34 am

learnt alot from reading this thanks for the guide. ?

Oxy - June 10, 2012, 7:24 am

Good thread and nice work on the grabber.

well might do some work on that in the future but i'm not that advanced at coding yet.

First finish all the projects i'm doing right now ^^.

very interesting what it does with the forms. might get some more tools added to malware like that :)

LulzAge - June 10, 2012, 8:15 am

Thank you for such a detailed and HQ guide pr0t0. :)

I liked how you explained formgrabbing with that diagram. <3

pr0t0typ3 - June 10, 2012, 2:42 pm

Thank you for the good Feedback :) I hope it helped you

The Unknown - July 3, 2012, 2:39 pm

Thanks for sharing this pr0t0, appreciated.

Eeluminati - July 23, 2012, 2:42 am

(Jun 7, 2012 04:40 AM)pr0t0typ3 Wrote: [\[CITE\]](#) To be honest, it also saddens me :(

I spent around 45 minutes writing this and doing the diagram and people don't even care enough to reply.

I read that and it urged me to reply. It's a nice read, I just want to know where to find these 'underground' forums/websites. c:

Omarion - July 23, 2012, 3:04 am

Just skimmed through it, but it looks amazing.

CatWare - July 23, 2012, 3:12 am

thank you!

I really wondered what formgrabbing was, thank you very much for the explanation

Grunt? - July 31, 2012, 1:33 pm

This was a great read and goldmine of information. Thanks for spending your time writing this. Please keep up the good work.

leo101010101 - July 31, 2012, 6:09 pm

nice explanation and well written. good job

Dr. Michio Kaku™ - July 31, 2012, 11:40 pm

Thanx a lot for this bro.

Pity that there is low response.

Helpful guide anyways.

30xic - August 16, 2012, 8:13 pm

Thanks for sharing this proto

very detailed and made me understand how formgrabbers works!

Good Job!

.?cb. - September 12, 2012, 1:08 pm

Good tutorial, thanks for this info.

Chelsea Monday - September 12, 2012, 6:35 pm

This is great. Thanks for posting ... helped clarify quite a few things for me.

Sekret - September 13, 2012, 10:18 am

Nice informative TUT ... see plenty of people asking what basic questions related to formgrabbers

pr0t0typ3 - September 14, 2012, 4:04 am

Thanks for the positive feedback :)

cilofrapez - October 22, 2012, 2:04 pm

Thanks, it was a good explanation!!

sissy-b - December 12, 2012, 12:50 am

detailed and HQ TUT.

Big vouch for you bro, great Job!

micdonand - December 23, 2012, 2:05 pm

Grete job! I have been wanting to know about this thanks, it's appreciated keep it up

d4rk41g0r1thm - December 23, 2012, 2:12 pm

Thank you for this amazing Tutorial :)

majikz10 - January 26, 2013, 5:05 am

nice read thankyou.Keep up the good work

juragan bokep - January 26, 2013, 6:50 am

great article... someone can recommended me good bot with formgrabber?

jerrymoris - November 16, 2013, 11:37 am

@ prototyp3... i appreciate your tut. am much more clear now,, i cant pm you but i need help with setting up the formgrabber...again which is better a botnet with formgrabber or standalone formgrabber?

praetorian70 - November 16, 2013, 12:56 pm

thank you for this tutorial. This is very useful information.

N0 Us3rN4m3 - November 16, 2013, 1:49 pm

Great tutorial. I was looking at it today morning. Keep it up mate c;

MURKER - November 16, 2013, 7:08 pm

(Jun 5, 2012 02:06 PM)pr0t0typ3 Wrote: [CITE](#) Where can I get Formgrabbers and what do I need to pay attention to ?

In many "underground" forums you can find formgrabbers as plugins or additional modules for HTTP Bots, while standalone Formgrabbers are rare to find.

You don't even answer the question you yourself put forward? Where do you get these illusive FormGrabbers? You state that they are found in many underground forums wow cheers that's specific...

Why include this part if you can't even offer a valuable response?

AlkatrazZ - November 17, 2013, 6:03 am

Good job thanks you for the guide ;)

