

Forum:[Hack Forums](#)

Thread: [PhotoLocker || HTTP Panel || Statistics](#)

Photo. - January 17, 2014, 6:46 pm

I've been wanting to code one of these for a while, now. So, I thought why not.

Name: PhotoLocker

Coded in: C# & PHP

Features: Completely locks the victim's screen

Persistence

HTTP Panel

Advanced Statistics

Password via panel

Server side

Anti-VM

Anti-Sandbox

Mutex

Kills common processes

Botkiller

That's basically just some of the features summed up, I'll continue to develop this throughout the duration of this thread.

All feedback & suggestions are greatly appreciated.

Panel:

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

I'm thinking of \$15, for lifetime inc unlimited re-builds. Sounds fair?

CSGO - January 17, 2014, 6:49 pm

Vouch for Photo! This is a very HQ product and works 100%. Thank you!

kingroot - January 17, 2014, 10:25 pm

Code Completely locks the victim's screen

Persistence
HTTP Panel
Advanced Statistics
Password via panel
Server side
Anti-VM
Anti-Sandbox
Mutex
Kills common proccesses
Botkiller

How exactly does 'anti-vm & anti-sandbox' work? SandBox works at a kernel level, i don't see you being able to bypass this in .NET
How does one exactly bypass a 'VM'?

For botkiller i'm assuming you're looking at modules that were mapped using virtualqueryex and comparing the types.

Persistence? How does this work, do you inject code into other processes that monitor your main module?

be prepared to explain this shit if you want people to believe

SpaceKase - January 18, 2014, 2:08 am

(Jan 17, 2014 11:25 PM)kingroot Wrote: [CITE](#) Code Completely locks the victim's screen

Persistence
HTTP Panel
Advanced Statistics
Password via panel
Server side
Anti-VM
Anti-Sandbox
Mutex
Kills common proccesses
Botkiller

How exactly does 'anti-vm & anti-sandbox' work? SandBox works at a kernel level, i don't see you being able to bypass this in .NET
How does one exactly bypass a 'VM'?

For botkiller i'm assuming you're looking at modules that were mapped using virtualqueryex and comparing the types.

Persistence? How does this work, do you inject code into other processes that monitor your main module?

be prepared to explain this shit if you want people to believe
Preach, fucking preachhhh
We need more people explaining HOW things work on this forum.

Product looks great, I'll definitely be a customer once I see it's got some reviews!

Caillou - January 18, 2014, 2:10 am

What must they do to remove the locker?

Moji - January 18, 2014, 3:23 am

Vouch for Fhoto, product looks great.

GLWS mate!

m4dh4ck3r - January 18, 2014, 3:27 am

(Jan 18, 2014 03:10 AM)Caillou Wrote: [\[CITE\]](#) What must they do to remove the locker?
The victims probably will be asked to complete a survey.

Tastylicious - January 18, 2014, 3:27 am

(Jan 17, 2014 11:25 PM)kingroot Wrote: [\[CITE\]](#) How exactly does 'anti-vm & anti-sandbox' work?
SandBox works at a kernel level, i don't see you being able to bypass this in .NET
How does one exactly bypass a 'VM'?
My guess: Since this is C# and he did not mention any hooking (Hue) or whatsoever, it is checking if these processes are running and tries kills them.

(Jan 17, 2014 11:25 PM)kingroot Wrote: [\[CITE\]](#) For botkiller i'm assuming you're looking at modules that were mapped using virtualqueryex and comparing the types.
My guess: Deletes every .exe-File in AppData and other common folders where malware is usually dropped.

(Jan 17, 2014 11:25 PM)kingroot Wrote: [\[CITE\]](#) Persistence? How does this work, do you inject code into other processes that monitor your main module?
My guess: VBS-File checking if file is existent and running, if not run it again.

Bat™ - January 18, 2014, 4:40 am

(Jan 18, 2014 04:27 AM)Tastylicious Wrote: [\[CITE\]](#) My guess: Since this is C# and he did not mention any hooking (Hue) or whatsoever, it is checking if these processes are running and tries kills them.

My guess: Deletes every .exe-File in AppData and other common folders where malware is usually dropped.

My guess: VBS-File checking if file is existent and running, if not run it again.
Did Fhoto 'personally' PM you to answer these ? ??

?

GI

Tastylicious - January 18, 2014, 4:47 am

(Jan 18, 2014 05:40 AM)Bat™ Wrote: [\[CITE\]](#) Did Fhoto 'personally' PM you to answer these ? ??

?

GI

No, as I said these are my guesses since that is what is common for HF-Malware.

Fhoto. - January 18, 2014, 4:49 am

(Jan 18, 2014 05:40 AM)Bat™ Wrote: [\[CITE\]](#) Did Fhoto 'personally' PM you to answer these ? ??

?

GI

Lol, what?

I don't even know him.

Stop bashing this thread.

Tastylicious - January 18, 2014, 4:50 am

(Jan 18, 2014 05:49 AM)Photo. Wrote: [\[CITE\]](#) Stop bashing this thread.

Didn't mean to bash anything ?

Expect feedback if you post a thread and don't be mad if people post their thoughts!

Photo. - January 18, 2014, 4:52 am

(Jan 18, 2014 05:50 AM)Tastylicious Wrote: [\[CITE\]](#) Didn't mean to bash anything ?

Expect feedback if you post a thread and don't be mad if people post their thoughts!

I was talking to Bat, not you, aha.

I forgot to say thank-you for your feedback.

Cheers.

Tastylicious - January 18, 2014, 4:53 am

(Jan 18, 2014 05:52 AM)Photo. Wrote: [\[CITE\]](#) I was talking to Bat, not you, aha.

I forgot to say thank-you for your feedback.

Cheers.

Oh ? Well, alright then I wish you GLWS ?

Bat™ - January 18, 2014, 5:00 am

(Jan 18, 2014 05:49 AM)Photo. Wrote: [\[CITE\]](#) Lol, what?

I don't even know him.

Stop bashing this thread.

Lol, I'm not.

Guess I was wrong. :P

Ill just quote this line from Tasty's post ?

"Expect feedback if you post a thread and don't be mad if people post their thoughts!"

Anyways GLWS :P

Photo. - January 18, 2014, 5:03 am

(Jan 18, 2014 06:00 AM)Bat™ Wrote: [\[CITE\]](#) Lol, I'm not.

Guess I was wrong. :P

Ill just quote this line from Tasty's post ?

"Expect feedback if you post a thread and don't be mad if people post their thoughts!"

Anyways GLWS :P

Thanks you for yours feedback, Bat!

Can't wait to release this ?

velox - January 18, 2014, 6:03 am

Nice idea but the name kinda sucks imo.

tux1 - January 18, 2014, 6:12 am

So Photo I didn't notice you answer the questions, so is what this guy says correct then?

(Jan 18, 2014 04:27 AM)Tastylicous Wrote: [\[CITE\]](#) My guess: Since this is C# and he did not mention any hooking (Hue) or whatsoever, it is checking if these processes are running and tries kills them.

My guess: Deletes every .exe-File in AppData and other common folders where malware is usually dropped.

My guess: VBS-File checking if file is existent and running, if not run it again.

Photo. - January 18, 2014, 7:52 am

(Jan 18, 2014 07:03 AM)velox Wrote: [\[CITE\]](#) Nice idea but the name kinda sucks imo.

Yeah, I know. I'll probably change it, aha.

(Jan 18, 2014 07:12 AM)tux1 Wrote: [\[CITE\]](#) So Photo I didn't notice you answer the questions, so is what this guy says correct then?

Yes

Yes

Nope

That's it ?

Prince of Persia - January 18, 2014, 10:14 am

(Jan 17, 2014 07:49 PM)Scarface. Wrote: [\[CITE\]](#) Vouch for Photo! This is a very HQ product and works 100%. Thank you!

Why are you vouching on a product that isn't out and is placed in the market place discussions..?

Bat™ - January 18, 2014, 10:17 am

Just a doubt, why does it have botkiller?

To kill the bot from which it is exec from?

What you can do is verify md5, of the bot, if it matches leave it else kill it.

The md5 can be supplied from the panel. If needed.

GI

Photo. - January 18, 2014, 3:13 pm

(Jan 18, 2014 11:17 AM)Bat™ Wrote: [\[CITE\]](#) Just a doubt, why does it have botkiller?

To kill the bot from which it is exec from?

What you can do is verify md5, of the bot, if it matches leave it else kill it.

The md5 can be supplied from the panel. If needed.

GI

In-case it gets killed by another piece of active malware, it kills basic malware only. Yes, I'll do that.

Still looking for ideas/suggestions.

This should be out today, I'm adding more options to the panel.

This will be only \$5.

hansbald - January 19, 2014, 7:16 am

I talked to him over skype, his explorer kill function is funny and all features work. Is it the first Locker with Panel on HF?

Auxil - January 19, 2014, 7:23 am

PhotoLocker is most likely the first Web-Panel Survey Locker on HF. Great job Photo. You always bring, new and original ideas to HF. I have seen his site personally, and it already looks very nice.

Miki - January 19, 2014, 7:40 am

Is this survey based locker? and how would one go about removing it?

Photo. - January 19, 2014, 8:07 am

(Jan 19, 2014 08:40 AM)Miki Wrote: [\[CITE\]](#) Is this survey based locker? and how would one go about removing it?

Yes, it is.

You enter the code, that the user is given.

User does the survey -> Gets code from survey -> Uses code to unlock.

Bat™ - January 19, 2014, 8:16 am

(Jan 19, 2014 08:23 AM)Ad?be Wrote: [\[CITE\]](#) PhotoLocker is most likely the first Web-Panel Survey Locker on HF. Great job Photo. You always bring, new and original ideas to HF. I have seen his site personally, and it already looks very nice.

Actually, if you see it was my idea.

Photo. - January 19, 2014, 8:20 am

(Jan 19, 2014 09:16 AM)Bat™ Wrote: [\[CITE\]](#) Actually, if you see it was my idea.

Nah, it wasn't.

It was mine, but I saw one with it before. Not being sold on HF.

iDuL - March 4, 2014, 11:53 pm

Relevant post: <https://hackforums.net/showthread.php?tid=4090710>

You can get the source to this for free now because OP is perm banned.

FearYO - March 6, 2014, 1:09 pm

(Mar 5, 2014 12:53 AM)iDuL Wrote: [\[CITE\]](#) Relevant post:

<https://hackforums.net/showthread.php?tid=4090710>

You can get the source to this for free now because OP is perm banned.

That's mean.

Thread does not exist.

xhflhkeuhwguu34 - *March 6, 2014, 1:33 pm*

(Mar 6, 2014 02:09 PM)FearYO Wrote: [\[CITE\]](#) That's mean.

Thread does not exist.

You have to be upgraded to see it.

Don't gravedig.