

Forum:[Hack Forums](#)

Thread: [Got sent a malicious dropper. Need some help de-obfuscating..](#)

motherfawker666 - July 30, 2017, 11:03 pm

I was sent some js script inside of a zip in an email and have been renaming variables and removing the dumber-than-dirt base64 variable obfuscation. I just need a bit of help understanding what exactly this script does. As of now it seems like it downloads a .DAT file from some site, renames it to some random numbers with a .jpeg extension then it runs said file after renaming to .EXE ... Can anyone get their hands on the .EXE for me so I can take a look at it? Seems as if trying to get it via web browser just times out.

[PASTEBIN LINK](#)

Vana - July 30, 2017, 11:09 pm

The domain appears to have no DNS configuration so right now it's impossible to get the .dat file.

motherfawker666 - July 30, 2017, 11:21 pm

(Jul 30, 2017 11:09 PM)Vana Wrote: [\[CITE\]](#) The domain appears to have no DNS configuration so right now it's impossible to get the .dat file.

What about from these? This is from the most recent file that was sent by the same address. They seems to be using a few redundant servers. I might have to wait until they send me a new one so I can get the fresh server info eh?

Code <http://whousexpress.bid/admin.php?f=1.doc>
<http://thalassaworks.bid/admin.php?f=1.doc>
<http://chalconcards.win/admin.php?f=1.doc>
<http://loxoconcepts.win/admin.php?f=1.doc>
<http://bocoolagodenzenz.com/admin.php?f=1.doc>

Vana - July 30, 2017, 11:32 pm

(Jul 30, 2017 11:21 PM)motherfawker666 Wrote: [\[CITE\]](#) What about from these? This is from the most recent file that was sent by the same address. They seems to be using a few redundant servers. I might have to wait until they send me a new one so I can get the fresh server info eh?

Code <http://whousexpress.bid/admin.php?f=1.doc>
<http://thalassaworks.bid/admin.php?f=1.doc>
<http://chalconcards.win/admin.php?f=1.doc>
<http://loxoconcepts.win/admin.php?f=1.doc>
<http://bocoolagodenzenz.com/admin.php?f=1.doc>

Those all give 0 byte responses for me. There might be some request verification involved, I'll keep looking into it.

motherfawker666 - July 30, 2017, 11:36 pm

(Jul 30, 2017 11:32 PM)Vana Wrote: [\[CITE\]](#) Those all give 0 byte responses for me. There might be some request verification involved, I'll keep looking into it.

I got the same result. Here is the full file for context.

<https://pastebin.com/Kcrg94Fb>

Vana - July 30, 2017, 11:54 pm

(Jul 30, 2017 11:36 PM)motherfawker666 Wrote: [\[CITE\]](#) I got the same result. Here is the full file for context.

<https://pastebin.com/Kcrg94Fb>

Might be worth it to just drop it in a VM and sniff the request.