

comp.security.misc: Re: Is this what it looks like?

Re: Is this what it looks like?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2001-12/0322.html>

From: sponge (mtubi@python.net)

Date: 12/24/01

From: mtubi@python.net (sponge)

Date: Mon, 24 Dec 2001 07:56:55 GMT

Yes, Gator is one of the more insidious pieces of spyware on the market. Spyware is software that meets one or more of the following criteria:

Does it install components (which are not a part of the program proper) without your knowledge or consent?

Does it connect to the Internet without your knowledge or consent?

Does it send information on you or your system without your knowledge or consent?

If one or more of the above, it's spyware. Basically, Gator --- and spyware in general --- is designed to find out about you, where you go on the Internet, how long you spend, what ads you click on, etc. Gator, aka eGuard, I believe, also has the ability to overlay their ads on top of those run by the "real" website.

Dump it unless you are willing to run it on a non-networked, non-internet-capable machine, or if you are willing to filter the IPs it contacts out. I am preparing a list of spyware-owned IP addresses for use by firewall to block them. You can also block them using DNSKong and putting Gator and eGuard on separate lines, but you also have to use a full blocklist. I posted a complete DNSKong blocklist one in alt.privacy.spyware recently.

BTW, do you happen to know the IP it's trying to contact (run netstat -an to find out.) THX.

sponge

Find out more about spyware at:

alt.privacy.spyware

<http://www.cexx.org>

Salon: "The Parasite Economy"

http://www.salon.com/tech/feature/2001/08/02/parasite_capital/index.html

Re: Is this what it looks like?

comp.security.misc: Re: Is this what it looks like?

Additional spyware info

<http://www.spywareinfo.com>

<http://66.34.160.192/spywareinfo/index.html>

www.spychecker.com

<http://grc.com>

On Sun, 23 Dec 2001 16:11:10 +0200, Lance Delacroix

<lance_delacroix@fastmail.fm> wrote:

>I hope somebody out there who knows more than I do can help me
>evaluate this situation.

>

>I recently did a software search for educational games and such for my
>three-year-old child. One of the sites that turned up was
>www.wyvern.com, which has a lot of free screen-savers and other stuff,
>and some toys at <http://www.wyvern.com/freegames.htm#123LEARN>.

>

>All of their stuff is free, ostensibly subsidized by Gator, a company
>that provides a free piece of software along with every Wyvern
>download: "As part of the install, we install a small program that
>allows Gator to introduce their software to our users." (from
><http://www.wyvern.com/freegames.htm#FreeGames>)

>

>Reading on, Wyvern says that Gator's software "is a cool piece of
>software that helps you remember passwords, and fill out forms online.
>It is free to use, has no negative side effects, and only does what
>you tell it." (also from the preceding URL).

>

>Now, I remembered the name Gator from a post in
>comp.security.firewalls (from mtubi@python.net Wed Dec 19 06:29:22
>2001) in which Gator was listed as one of a number of "known parasite
>services". Very interesting.

>

>Somewhere in the mess of blurbs I found something (I can't find it
>again now) that said that Gator's program, called "Trickle", would be
>downloaded unobtrusively, a tiny bit at a time, so as to avoid
>interfering with my surfing pleasure.

>

>I downloaded the kiddy software and installed it. Then I checked the
>new directory and found a file called called "Trickle_blahblahblah".
>Soon afterwards, I got an alert from my Tiny Personal Firewall telling
>me that Trickle was trying to connect outward. "No need for that," I
>thought, and I denied it and then deleted it from the directory where
>it had lodged. I installed a second kiddy game and it put a second
>copy of Trickle onto my computer, which I also deleted.

>

>Now I'm no genius, but it looks to me like this "cool" software was
>something whose job it was to send information about my computer to
>Gator. Whaddaya think? Am I right? You can check it out for
>yourself through the above URLs. If I'm correct about this, the full
>text on <http://www.wyvern.com/freegames.htm#FreeGames> will make some

Re: Is this what it looks like?

comp.security.misc: Re: Is this what it looks like?

>pretty hilarious reading.

>

>Thanks.

- *Next message:* [Ross Williams: "The Tao Of Backup!"](#)
- *Previous message:* [Martin Bishop: "Re: What are the disadvantages of Pgp ???"](#)
- *In reply to:* [Lance Delacroix: "Is this what it looks like?"](#)
- *Next in thread:* [Lance Delacroix: "Re: Is this what it looks like?"](#)
- *Reply:* [Lance Delacroix: "Re: Is this what it looks like?"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)