

Re: Anyone seen tgcmd.exe before?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-12/0019.html>

From: Angus (angus_md_at_yahoo.com)

Date: 12/03/03

Date: 3 Dec 2003 17:35:04 -0000

To: incidents@securityfocus.com

('binary' encoding is not supported, stored as-is) In-Reply-To:

<8614FCA8E4FB3C4A9ED38BBD9C7D38C405B118@azc-m3.ad.tgen.org>

It is spyware. Rumor has it, Comcast installs it w/ cable modems, and some laptop vendors install it as well.

<http://www.winpatrol.com/db/freesample/tgcmd.html>

>Received: (qmail 21989 invoked from network); 3 Dec 2003 16:50:32 -0000
>Received: from outgoing3.securityfocus.com (205.206.231.27)
> by mail.securityfocus.com with SMTP; 3 Dec 2003 16:50:32 -0000
>Received: from lists.securityfocus.com (lists.securityfocus.com [205.206.231.19])
> by outgoing3.securityfocus.com (Postfix) with QMQP
> id D937BA30CF; Wed, 3 Dec 2003 09:59:18 -0700 (MST)
>Mailing-List: contact incidents-help@securityfocus.com; run by ezmlm
>Precedence: bulk
>List-Id: <incidents.list-id.securityfocus.com>
>List-Post: <mailto:incidents@securityfocus.com>
>List-Help: <mailto:incidents-help@securityfocus.com>
>List-Unsubscribe: <mailto:incidents-unsubscribe@securityfocus.com>
>List-Subscribe: <mailto:incidents-subscribe@securityfocus.com>
>Delivered-To: mailing list incidents@securityfocus.com
>Delivered-To: moderator for incidents@securityfocus.com
>Received: (qmail 1131 invoked from network); 3 Dec 2003 02:16:49 -0000
>X-MimeOLE: Produced By Microsoft Exchange V6.0.6249.0
>content-class: urn:content-classes:message
>MIME-Version: 1.0
>Content-Type: text/plain;
> charset="iso-8859-1"
>Content-Transfer-Encoding: quoted-printable
>Subject: Anyone seen tgcmd.exe before?
>Date: Tue, 2 Dec 2003 19:05:06 -0700
>Message-ID: <8614FCA8E4FB3C4A9ED38BBD9C7D38C405B118@azc-m3.ad.tgen.org>
>X-MS-Has-Attach:
>X-MS-TNEF-Correlator:
>Thread-Topic: Same sequence...
>Thread-Index: AcO4g799ukgvnBVGTFysJbQnMhXWowAvBDHA

SecurityFocus Incidents: Re: Anyone seen tgcmd.exe before?

>From: "Harry Chemin" <hchemin@tgen.org>
>To: <INCIDENTS@SECURITYFOCUS.COM>
>
>I found a program on a client's laptop running Windows XP with latest =
>service pack and all hot fixes applied. The client reported that =
>someone was remotely controlling his desktop while he was on his home =
>network. The client had Zone Alarm, Symantec Anti-virus software, and =
>was using a Linksys firewall. I checked several websites for =
>information on tgcmd.exe and possibilities for the source of this =
>software appear to be either for Sony Vaio laptops or @Home support =
>software. Unfortunately, the user's laptop is an IBM Thinkpad and the =
>client had no recollection of installing the Support.com software. Here =
>is the output from fport:
>
>Pid Process Port Proto Path =20
>984 -> 3001 TCP =20
>376 -> 5000 TCP =20
>4 System -> 1056 TCP =20
>4 System -> 139 TCP =20
>0 System -> 3119 TCP =20
>0 System -> 3121 TCP =20
>4 System -> 445 TCP =20
>2936 ccApp -> 3099 TCP C:\Program Files\Common =
>Files\Symantec Shared\ccApp.exe
>2936 ccApp -> 3104 TCP C:\Program Files\Common =
>Files\Symantec Shared\ccApp.exe
>3900 msmsgs -> 9519 TCP C:\Program =
>Files\Messenger\msmsgs.exe
>1144 ccPxySvc -> 1044 TCP C:\Program Files\Norton Internet =
>Security Professional\ccPxySvc.exe
>4040 tgcmd -> 641 TCP C:\Program =
>Files\Support.com\bin\tgcmd.exe
>1756 svchost -> 1025 TCP C:\WINDOWS\System32\svchost.exe
>1756 svchost -> 3002 TCP C:\WINDOWS\System32\svchost.exe
>1756 svchost -> 3003 TCP C:\WINDOWS\System32\svchost.exe
>1452 svchost -> 135 TCP C:\WINDOWS\system32\svchost.exe
>
>984 -> 10743 UDP =20
>376 -> 3008 UDP =20
>4 System -> 1028 UDP =20
>0 System -> 123 UDP =20
>0 System -> 137 UDP =20
>0 System -> 3081 UDP =20
>4 System -> 3123 UDP =20
>4 System -> 500 UDP =20
>0 System -> 62515 UDP =20
>0 System -> 62517 UDP =20
>0 System -> 62519 UDP =20
>0 System -> 62521 UDP =20
>0 System -> 62523 UDP =20
>0 System -> 62524 UDP =20

Re: Anyone seen tgcmd.exe before?

SecurityFocus Incidents: Re: Anyone seen tgcmd.exe before?

>2936 ccApp -> 1049 UDP C:\Program Files\Common =
>Files\Symantec Shared\ccApp.exe
>2936 ccApp -> 1900 UDP C:\Program Files\Common =
>Files\Symantec Shared\ccApp.exe
>3900 msmsgs -> 138 UDP C:\Program =
>Files\Messenger\msmsgs.exe
>1144 ccPxySvc -> 1900 UDP C:\Program Files\Norton Internet =
>Security Professional\ccPxySvc.exe
>4040 tgcmd -> 1026 UDP C:\Program =
>Files\Support.com\bin\tgcmd.exe
>1756 svchost -> 1027 UDP C:\WINDOWS\System32\svchost.exe
>1756 svchost -> 123 UDP C:\WINDOWS\System32\svchost.exe
>1756 svchost -> 52070 UDP C:\WINDOWS\System32\svchost.exe
>1452 svchost -> 445 UDP C:\WINDOWS\system32\svchost.exe
>
>-----
>-----
>
>
>

