



Search:

in Blogs



Members login | Newsletters | Site Assistance | RSS Feeds

- Home
- News & Blogs
- Videos
- White Papers
- Downloads
- Reviews
- Popular ▾

Zero Day

Ryan Naraine and Dancho Danchev

Get Zero Day via: Mobile RSS Email Alerts Bios: Ryan's Bio Dancho's Bio

Pick a blog category

August 28th, 2009

Source code for Skype eavesdropping trojan in the wild

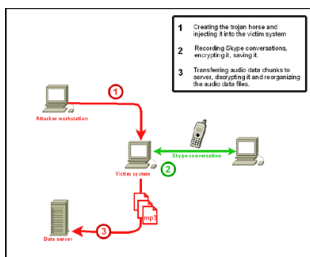
Posted by Dancho Danchev @ 4:20 am

Categories: [Anti Virus](#), [Botnets](#), [Browsers](#), [Complex Attacks](#), [Hackers](#), [Malware](#), [Pen testing](#), [Responsible disclosure](#), [Spyware and Adware](#)

Tags: [Trojan Horse](#), [Skype Technologies S.A.](#), [Spyware](#), [Spyware, Adware & Malware](#), [Government](#), [Viruses And Worms](#), [Security](#), [Dancho Danchev](#)

26 TalkBacks **+18** WORTHWHILE? 18 VOTES

ADD YOUR OPINION SHARE PRINT E-MAIL



Earlier this week, Swiss programmer Ruben Unteregger who has been reportedly working for a [Swiss company ERA IT Solutions](#) responsible for coding government sponsored spyware, has released the [source code of a trojan horse that injects code into the Skype process](#) in order to convert the incoming and outgoing voice data into an encrypted MP3 available at the disposal of the attacker.

Here's [how the trojan](#), currently [detected](#) as [Trojan.Peskyspy](#), works:

"When the Trojan is executed, it injects a thread into the Skype process and hooks a number of API calls, allowing it to intercept all PCM audio data going between the Skype process and underlying audio devices. Note: Since the Trojan listens to the data coming to and from the audio devices, it gathers the audio independently of any application-specific protocols or encryption applied by Skype when it passes voice data at the network level.

Note: The incoming and outgoing audio data are stored in separate .mp3 files. The Trojan also opens a back door on the compromised computer, allowing an attacker to perform the following actions:

- Send the .mp3 to a predetermined location
- Download an updated version
- Delete the Trojan from the compromised computer"

Skype is often dubbed a "[national security threat](#)" by governments all across the globe due to their — at least publicly acknowledged inability — to [crack the 256-bit encryption VoIP calls](#).



The HOT Spot



Smart Tech



Expert advice on innovations in healthcare and the green technologies that make it happen. [Find out more](#)

Smart Business



Discussion and advice on management issues that revolve around making your world smarter and more useful. [More Smart Advice](#)

Smart People



The best and worst moves in the management and strategy trenches. [Learn More](#)

ADVERTISEMENT ▾

Sponsored Links

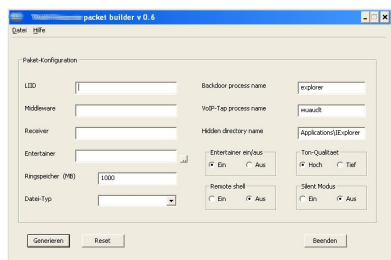
- ➔ **Recommended Download**
PC Magazine Editor's Choice Winner Best Anti-Spyware. Secure Your PC! [www.pctools.com](#)
- ➔ **Spyware Virus Remover**
Free Spyware Scan. Award-winning Spyware Remover. Download now. [www.stopzilla.com](#)

Recent Entries

- ➔ [Apache.org hit by SSH key compromise](#)
- ➔ [Snow Leopard's malware protection only scans for two Trojans](#)
- ➔ [Source code for Skype eavesdropping trojan in the wild](#)
- ➔ [The most dangerous celebrities to search for in 2009](#)
- ➔ [Hackers mailing malware-infested CDs to banks](#)

Blogs From Our Sponsors

- ➔ [Welcome to The DocuMentor](#)



And while some of these governments are reportedly spending surreal amounts of tax payer's money (Rental

of the Skype-Capture-Unit per month and instance EUR 3.500) in order to achieve their objectives, others are taking the cost-effectiveness path by attacking the weakest link in the process - the end user infected with a targeted DIY government sponsored spyware recording all ongoing and incoming Skype calls, thereby bypassing the need to attack the encryption algorithm.



Dancho Danchev is an independent security consultant and cyber threats analyst, with extensive experience in open source intelligence gathering, malware and cybercrime incident response. He's been an active security blogger since 2007, and maintains a popular [security blog](#). See his [full profile](#) and [disclosure](#) of his industry affiliations.

[Email Dancho Danchev](#)

Subscribe to Zero Day via [Email alerts](#) or [RSS](#).

[« Previous post](#)

[Next post »](#)

Talkback

Most Recent of **26** Talkback(s)

Thread View Flat View

“ RE: Source code for Skype eavesdropping trojan in the wild

It appears that this Trojan horse doesn't currently affect the Mac environment. However, this code can easily be converted to Mac so we Mac people need to watch out also.... [\(Read the rest\)](#)

Posted by: phatkat Posted on: 08/28/09

You are currently: a Guest | [Log in](#) | [Terms of Use](#)

Social Engineering? *NEW*

Albee_Freeoneday | 08/28/09

Just one of the many reasons . . . *NEW*

wgrau | 08/28/09

" Just one of the many reasons..." *NEW*

Kaptah | 08/28/09

dogma *NEW*

Louis Ross Focke | 08/28/09

" dogma " *NEW*

Kaptah | 08/28/09

whoa, *NEW*

Louis Ross Focke | 08/28/09

NO, I do not agree with you,... *NEW*

theguru1995@... | 08/28/09

Wow... *NEW*

jasonp@... | 08/28/09

→ [Tips for Successful Document Capture](#)

→ [Yes We Can -- improve records management](#)

→ [T to the C to the O: Know your costs](#)

RICOH

Top Rated

[Researchers find insecure BIOS 'rootkit' pre-loaded in laptops](#) +66 votes

[55,000 Web sites hacked to serve up malware cocktail](#) +65 votes

[Browser flaws expose users to man-in-the-middle attacks](#) +44 votes

[Apple warns of Mac attack risk via image files](#) +30 votes

[IE8 outperforms competing browsers in malware protection -- again](#) +28 votes

[Microsoft's Bing invaded by pharmaceutical scammers](#) +20 votes

[Source code for Skype eavesdropping trojan in the wild](#) +18 votes

[Apple adds malware blocker in Snow Leopard](#) +17 votes

Follow ZDNet on [twitter](#)

ZDNet **POWER**Center

Useful content from our premier sponsors

[News, Insights, Guidance](#)

[Visit CBSMoneyWatch.com Today](#)

[Learn more >>](#)

[Top-ranked Novell support for Red Hat at 50% less](#)

[Learn more >>](#)

[Move to SUSE Linux Enterprise. Get 3 years of Red Hat support](#)

[Learn more >>](#)

[Get top-ranked Novell support for Red Hat when you switch](#)

[Learn more >>](#)

[More interoperability, plus 3 years. Red Hat support, only from Novell](#)



RE: Source code for Skype eavesdropping trojan in the wild *NEW*
andreas.tanzer@... | 08/28/09

a few bits of information *NEW*

Louis Ross Focke | 08/28/09

Good for him? *NEW*

spstanley | 08/28/09

RE: Source code for Skype eavesdropping trojan in the wild *NEW*

danm50 | 08/28/09

RE: Source code for Skype eavesdropping trojan in the wild *NEW*

wgraue | 08/28/09

Talk about the wrong way... *NEW*

jasonp@... | 08/28/09

Not Skype's only problem *NEW*

Dorkyman | 08/28/09

Skype Software and the Skype Services at Your own risk. *NEW*

Stan57 | 08/28/09

A Deal with the Devil *NEW*

rod.boggess@... | 08/28/09

Darned if you do, darned if you don't *NEW*

slylabs13 | 08/28/09

Darned if *NEW*

Louis Ross Focke | 08/28/09

I agree with you LRF.... *NEW*

theguru1995@... | 08/28/09

However, in the final analysis.. LRF *NEW*

Kaptah | 08/28/09

RE: Source code for Skype eavesdropping trojan in the wild *NEW*

intlfam | 08/28/09

RE: Source code for Skype eavesdropping trojan in the wild *NEW*

rebecca01@... | 08/28/09

RE: Source code for Skype eavesdropping trojan in the wild *NEW*

x3dre@... | 08/28/09

Bypass the bypass... *NEW*

redking44 | 08/28/09

RE: Source code for Skype eavesdropping trojan in the wild *NEW*

phatkat | 08/28/09

[Learn more >>](#)



Novell.

ADVERTISEMENT ▼

Archives

→ [August 2009](#)

→ [July 2009](#)

→ [June 2009](#)

→ [May 2009](#)

→ [April 2009](#)

→ [March 2009](#)

[All "Zero Day" talkbacks](#)

ZDNet Blogs

- [All About Microsoft](#)
- [The Apple Core](#)
- [Between the Lines](#)
- [BriefingsDirect](#)
- [Collaboration 2.0](#)
- [Community, Incorporated](#)
- [Dev Connection](#)
- [Digital Cameras & Camcorders](#)
- [Ed Bott's Microsoft Report](#)
- [Emerging Tech](#)
- [Enterprise Web 2.0](#)
- [Forrester Research](#)
- [Googling Google](#)
- [GreenTech Pastures](#)
- [Hardware 2.0](#)
- [Home Theater](#)
- [iGeneration](#)
- [Managing L'unix](#)
- [The Mobile Gadgeteer](#)
- [On Sustainability](#)
- [Rational Rants](#)
- [The Semantic Web](#)
- [Service Oriented](#)
- [Smartphones and Cell Phones](#)
- [Social Business](#)
- [Social CRM: The Conversation](#)
- [Software & Services Safari](#)
- [Software as Services](#)
- [Storage Bits](#)
- [Team Think](#)
- [Tech Broiler](#)
- [Technology and the Global Supply Chain](#)

What do you think?

Subject (max length: 75):

Reply:

Add your opinion




Sponsored

White Papers, Webcasts, and Downloads

-  [Why Isn't Server Virtualization Saving Us More? A Few Small Changes May Dramatically Increase Your Efficiency](#)
VMware
Companies have rapidly adopted server virtualization over the past few ...
[Download Now](#)
-  [Open Standards Technologies Provide the Ingredients for Delivering Security Across the Papa Gino's Enterprise](#)
Dell
Papa Gino's Holdings Corporation founded by the entrepreneur operates one ...
[Download Now](#)
-  [Three Steps You Need to Know to Stop Data Loss](#)
Varonis
Sensitive data exposed to misuse or loss... it is the stuff of nightmares ...
[Download Now](#)

- Irregular Enterprise
- IT Facts
- IT Project Failures
- Laptops & Desktops
- Lawgarithms
- Linux and Open Source
- Tom Foremski: IMHO
- The ToyBox
- Virtually Speaking
- The Web Life
- ZDNet Education
- ZDNet Government
- ZDNet Healthcare
- Zero Day

White Papers, Webcasts, and Downloads

-  [Open Standards Technologies Provide the Ingredients for Delivering Security Across the Papa Gino's Enterprise](#)
Dell
Papa Gino's Holdings Corporation founded by the entrepreneur operates one ...
[Download Now](#)
-  [The Impact of Virtualization Software on Operating Environments](#)
VMware
Today's use of virtualization technology allows IT professionals to ... [Download Now](#)
-  [Server Consolidation and Containment With Virtual Infrastructure](#)
VMware
To meet the constant demand to deploy, maintain and grow a broad array of ...
[Download Now](#)



ZDNet News & Blogs

Hardware, IT Management, Networking, Operating Systems, Photo Galleries, Security, Software, Web Technology, All News, Dev Connection, Emerging Technology, Enterprise Alley, Googling Google, GreenTech Pastures, IT Project Failures, Linux and Open Source, Managing Linux, The Social Web, Storage Bits, Virtually Speaking, The Web Life, Podcasts

Product Reviews

A/V Receivers, Cell Phones & Accessories, Desktop Monitors, Desktops, Digital Cameras, Digital Camcorders, Flat-panel TVs, Laptops, Portable Video Players (PVPs), PDAs, Smartphones, Software, Storage

Product Blogs

The Toybox, Digital Cameras, Laptops and Desktops, Mobile Gadgeteer, SOHO Networking, Smartphones and Cell Phones, Home Theater

White Papers & Webcasts

Cost Control / Risk Management, Customer Support Services, IT HR / Staffing / Training, Resources Management, Strategic Planning, Webcasts

Downloads

Antivirus Software, File and Disk Management Utilities, Image Editing, Privacy Software, Shell and Desktop Management Enhancements

Site Help & Feedback | Site Map

Popular on CBS sites: [Fantasy Football](#) | [Madden NFL10](#) | [PGA Championship](#) | [iPhone](#) | [Video Game Reviews](#) | [US Open](#) | [Antivirus Software](#)

[About CBS Interactive](#) | [Jobs](#) | [Advertise](#)

[Visit other CBS Interactive Sites](#) [Select Site](#)

© 2009 CBS Interactive Inc. All rights reserved. | [Privacy Policy](#) | [Terms of Use](#)

