

Mariposa Botnet Author, Darkcode Crime Forum Admin Arrested in Germany

krebsonsecurity.com/2019/10/mariposa-botnet-author-darkcode-crime-forum-admin-arrested-in-germany/

A Slovenian man convicted of authoring the destructive and once-prolific Mariposa botnet and running the infamous Darkcode cybercrime forum has been arrested in Germany on request from prosecutors in the United States, who've recently re-indicted him on related charges.



NiceHash CTO Matjaž “Iserdo” Škorjanc, as pictured on the front page of a recent edition of the Slovenian daily Delo.si, is being held by German authorities on a US arrest warrant for operating the destructive “Mariposa” botnet and founding the infamous Darkcode cybercrime forum.

The Slovenian Press Agency reported today that German police arrested **Matjaž “Iserdo” Škorjanc** last week, in response to a U.S.-issued international arrest warrant for his extradition.

In December 2013, a Slovenian court sentenced Škorjanc to four years and ten months in prison for creating the malware that powered the ‘**Mariposa**’ botnet. Spanish for “Butterfly,” Mariposa was a potent crime machine first spotted in 2008. Very soon after its inception,

Mariposa was estimated to have infected more than 1 million hacked computers — making it one of the largest botnets ever created.

ButterFly Network Solutions
Offering quality networking systems for various purposes

About Products Contact us

ButterFly Network Solutions

ButterFly Network Solutions (BFNS) is providing quality, reliable, stable, fast and feature-full software, based on own developed networking protocols. We are offering advanced command&control remote systems for masses, advanced reverse proxy solutions for personal or business use and custom network-related projects on demand

Home / ButterFly Flooder

ButterFly Flooder

ButterFly Flooder (BFF) is an advanced command&control system for remote PCs that allows you to fully stress performance and stability of network applications. Besides flooding capabilities it also provides extended commanding options that no other solutions have. The third big feature is modular design, allowing you to pick&load modules on your own. All this built on top of newest ButterFly protocol gives you the best experience and reliability such software can offer!

ButterFly Flooder
Features
Changelog
Screenshots
Buy
FAQ

An advertisement for the ButterFly Bot.

Škorjanc and his hacker handle Iserdo were initially named in a Justice Department indictment from 2011 (PDF) along with two other men who allegedly wrote and sold the Mariposa botnet code. But in June 2019, the DOJ unsealed an updated indictment (PDF) naming Škorjanc, the original two other defendants, and a fourth man (from the United States) in a conspiracy to make and market Mariposa and to run the Darkode crime forum.

More recently, Škorjanc served as chief technology officer at **NiceHash**, a Slovenian company that lets users sell their computing power to help others mine virtual currencies like bitcoin. In December 2017, approximately USD \$52 million worth of bitcoin mysteriously disappeared from the coffers of NiceHash. Slovenian police are reportedly still investigating that incident.

WELCOME TO DARKODE
 "International marketplace for sewing machines and other legal stuff"

Invite a friend (No invites left) • Profile • Private Messages • Search • FAQ • Memberlist • Usergroups • PUSSY () • Log out [hidden]

Sell (TM)
 Moderators: None
 Users browsing this forum: None

[darkode.com Forum Index](#) » [Sell \(TM\)](#) [Mark all topics read](#)

Topics	Replies	Author	Views	Last Post
<input type="radio"/> Discount coupons @ e6l	5	Sana	103	Sun Jul 21, 2013 11:13 am Sana
<input type="radio"/> Access to all Voxility/LimeHost Semi-BP DC in Romania	0	off-sho.re	24	Sun Jul 14, 2013 3:18 pm off-sho.re
<input type="radio"/> [Sell] SKYPE accounts	2	wesTThug	32	Fri Mar 22, 2013 12:34 am wesTThug
<input type="radio"/> [Sell] 1.2k ftp accounts	1	wesTThug	25	Sun Mar 17, 2013 9:10 pm sp3cial1st
<input type="radio"/> eBay Shipping Service	2	MrGold	94	Wed Jan 23, 2013 6:32 am sp3cial1st
<input type="radio"/> offering High Volume High risk processing TO ONLY TM	3	TheMayor	92	Wed Oct 10, 2012 2:33 pm godname1
<input type="radio"/> WHMCS 0day	14	Doksh	600	Tue Oct 09, 2012 1:14 pm Paradox
<input type="radio"/> DB with with full info (ssn&dob)	0	Jumbie	19	Mon Sep 24, 2012 1:22 am Jumbie
<input type="radio"/> Offline POS	0	MrGold	52	Sat Jun 02, 2012 2:06 pm MrGold
<input checked="" type="radio"/> razerzone.com shop database	5	fubar	95	Wed May 30, 2012 1:33 am fubar

Display topics from previous:

[darkode.com Forum Index](#) » [Sell \(TM\)](#) All times are GMT

Page 1 of 1

Jump to:

New posts
 No new posts
 Announcement
 New posts [Locked]
 No new posts [Locked]
 Sticky

You can post new topics in this forum
 You can reply to topics in this forum
 You can edit your posts in this forum
 You cannot delete your posts in this forum
 You can vote in polls in this forum

The “sellers” page on the Darkode cybercrime forum, circa 2013.

It will be interesting to see what happens with the fourth and sole U.S.-based defendant added in the latest DOJ charges — **Thomas K. McCormick**, a.k.a “**fubar**” — allegedly one of the last administrators of Darkode. Prosecutors say McCormick also was a reseller of the Mariposa botnet, the [Zeus banking trojan](#), and a bot malware he allegedly helped create called “Ngrbot.”

Between 2010 and 2013, Fubar would randomly chat me up on instant messenger apropos of nothing to trade information about the latest goings-on in the malware and cybercrime forum scene.

Fubar frequently knew before anyone else about upcoming improvements to or new features of ZeuS, and discussed at length his interactions with Iserdo/Škorjanc. Every so often, I would reach out to Fubar to see if he could convince one of his forum members to call off an

attack against KrebsOnSecurity.com, an activity that had become something of a rite of passage for new Darkode members.

On Dec. 5, 2013, federal investigators visited McCormick at his University of Massachusetts dorm room. According to a memo filed by FBI agents investigating the case, in that interview McCormick acknowledged using the “fubar” identity on Darkode, but said he’d quit the whole forum scene years ago, *and that he’d even interned at Microsoft for several summers and at Cisco for one summer.*

A subsequent search warrant executed on his dorm room revealed multiple removable drives that held tens of thousands of stolen credit card records. For whatever reason, however, McCormick wasn’t arrested or charged until December 2018.

According to the FBI, back in that December 2013 interview McCormick voluntarily told them a great deal about his various businesses and online personas. He also apparently told investigators he talked with KrebsOnSecurity quite a bit, and that he’d tipped me off to some important developments in the malware scene. For example:

“TM had found the email address of the Spyeye author in an old fake antivirus affiliate program database and that TM was able to find the true name of the Spyeye author from searching online for an individual that used the email address,” the memo states. “TM passed this information on to Brian Krebs.”

Read more of the FBI’s interview with McCormick [here](#) (PDF).

News of Škorjanc’s arrest comes amid other cybercrime takedowns in Germany this past week. On Friday, German authorities announced they’d arrested seven people and were investigating six more in connection with the raid of a Dark Web hosting operation that allegedly supported multiple child porn, cybercrime and drug markets with hundreds of servers [buried inside a heavily fortified military bunker.](#)