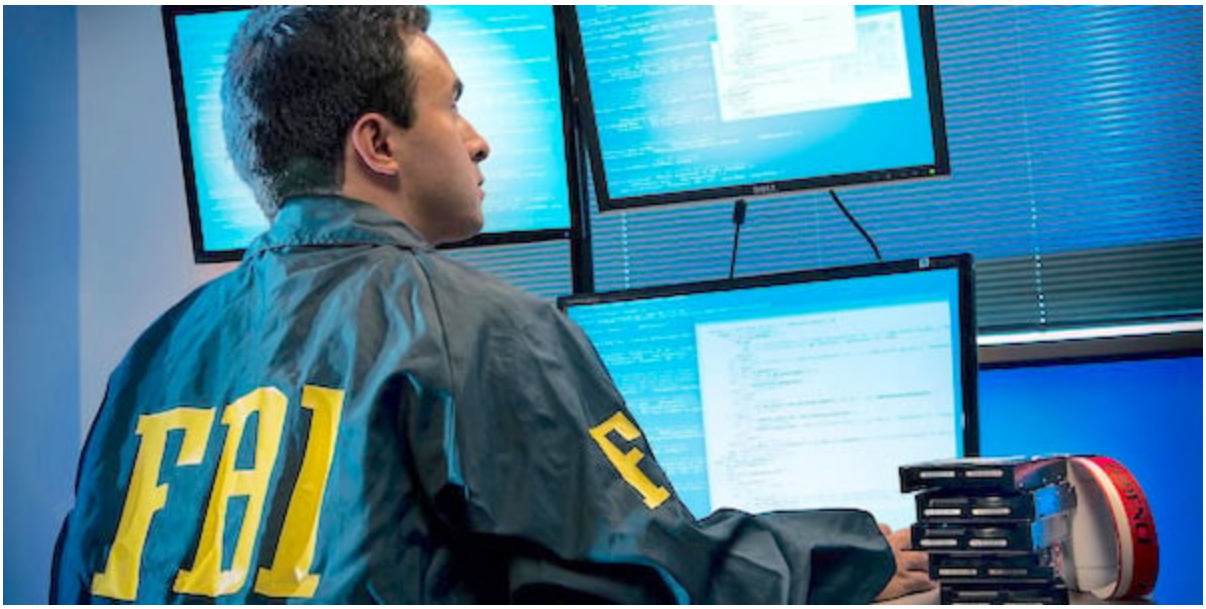
March 16, 2023

Malware

FBI shuts down 11-year-old NetWire RAT malware

Posted on March 16th, 2023 by Joshua Long 



After nearly 11 years in operation, law enforcement has shut down the distribution of the shady NetWire Remote Control software. NetWire was a commercially sold, cross-platform remote access trojan (RAT) with capabilities designed for spying on victims. Antivirus products commonly detect NetWire under names such as Netweird, NetWeirdRC, Netwire, or Wirenet.

In a press release, the U.S. Department of Justice detailed what had transpired. On Tuesday, March 7, 2023, the DOJ seized the domain `worldwiredlabs[.]com`. This site, doing business as World Wired Labs, had been selling NetWire since May 2012. Now it simply displays an FBI seizure splash screen.

The notice on the seized domain reads, in part:

> This Website Has Been Seized as part of a coordinated law enforcement action taken against the NetWire Remote Access Trojan. This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant… as part of a joint international law enforcement operation and action…

Law enforcement authorities in Croatia arrested the alleged site operator on the same day. According to reports from Brian Krebs and Croatian news (English translation), 40-year-old Mario Zanko allegedly distributed the malware. Krebs' research indicates that Zanko went by the hacker pseudonym Dugidox. Croatian authorities will reportedly prosecute the accused malware maker.

Zanko reportedly made nearly $1 million selling the software, which sold for anywhere from $60 to $140 per license over the years. This would seem to suggest that World Wired Labs likely sold at least 10,000 licenses.

In addition to the site seizure and Zanko's arrest, the DOJ reports that Swiss authorities seized the server that hosted the RAT's infrastructure. It is not clear whether this prevents existing infections from being able to phone home to command and control servers for specific NetWire deployments.

The history of NetWire Remote Control

Intego has written about this malware since the first Mac version was first discovered in 2012. Variants of the Mac version of this malware have been known under names such as **OSX/NetWeirdRC.A**, **OSX/NetWeirdRC.B**, **OSX/NetWeirdRC.C**, **OSX/Netweird**, **OSX/Netwire**, and **OSX/Wirenet**.

NetWire Remote Control's virtual box art. NetWire was commercial spyware.

NetWire Remote Control was billed as "an advanced remote control solution," but binary analyses made its actual purpose clear. As we explained in our August 2012 analysis, the first Mac version was capable of stealing passwords from Web browsers and e-mail clients, namely Firefox, Opera, SeaMonkey, and Thunderbird. Credential stealing is not behavior one would expect from legitimate computer monitoring or remote administration software. The DOJ also notes that NetWire "was advertised on hacking forums, and numerous cyber security companies and government agencies have documented instances of the NetWire RAT being used in criminal activity."

> An Analysis of the Cross-Platform Backdoor OSX/NetWeirdRC

Apple added detection for one NetWire variant to its XProtect definitions in September 2016.

> Apple Updates XProtect Malware Definitions for NetWeirdRC

In June 2019, miscreants spread NetWire malware in a broad public attack, leveraging a zero-day vulnerability in Firefox.

> Mac malware on the rise again; several new threats found: Netwire, Mokes, LoudMiner, NewTab

The end of an era; a sign of things to come?

The FBI began investigating World Wired Labs in the year 2020—around eight years after the malware surfaced, and three years before the coordinated law enforcement actions took place.

The logo of World Wired Labs, NetWire's distributor

Although it's unfortunate that it took law enforcement 11 years to stop this malware's development and proliferation, we're glad that it has finally happened. We hope that international law enforcement agencies will learn from this experience and more quickly neutralize similar malware threats in the future.

How can I learn more?

We talked about the takedown of NetWire Remote Control on episode 283 of the Intego Mac Podcast:

Each week on the **Intego Mac Podcast**, Intego's Mac security experts discuss the latest Apple news, including security and privacy stories, and offer practical advice on getting the most out of your Apple devices. Be sure to **follow the podcast** to make sure you don't miss any episodes.

You can also subscribe to our **e-mail newsletter** and keep an eye here on **The Mac Security Blog** for the latest Apple security and privacy news. And don't forget to follow Intego on your favorite social media channels:

Cyber agent photo credit: FBI, via recruitment site.

About Joshua Long

Joshua Long (@theJoshMeister), Intego's Chief Security Analyst, is a renowned security researcher, writer, and public speaker. Josh has a master's degree in IT concentrating in Internet Security and has taken doctorate-level coursework in Information Security. Apple has publicly acknowledged Josh for discovering an Apple ID authentication vulnerability. Josh has conducted cybersecurity research for more than 20 years, which has often been featured by major news outlets worldwide. Look for more of Josh's articles at security.thejoshmeister.com and follow him on Twitter. View all posts by Joshua Long →