



Trend Micro, NCA Partnership Leads to Arrests and Shutdown of Refud.me and Cryptex Reborn

- Posted on:November 23, 2015 at 4:09 am
- Posted in:Bad Sites
- Author:
  Trend Micro Senior Threat Researchers

16

A male and a female, both aged 22 and hailing from Colchester, Essex in the United Kingdom, were arrested on suspicion of operating two services featured in many malware business models – the popular counter antivirus (CAV) service Refud.me and the crypting service Cryptex Reborn. Both services have been taken down thanks to the partnership of Trend Micro's Forward-Looking Threat Research team and the National Crime Agency of the UK (NCA).

These latest takedowns are milestones in anti-cybercrime efforts. Refud.me and Cryptex Reborn were both key components of a much larger underground business model. Rendering them inoperable throws a wrench at ongoing cybercriminal operations in and beyond the UK as this can force cybercriminals to spread malware that are more prone to detection.

"This investigation is the result of Trend Micro's collaboration with the National Crime Agency of the UK (NCA) and other partners to tackle some of the core components that enable cybercriminal business models to exist," said Martin Rösler, senior director of The Forward-Looking Threat Research team for Trend Micro. Back in July 2015 Trend Micro and the NCA signed a Memorandum of Understanding (MOU), marking a significant step to understand and fight cybercrime. The agreement also formed a cross-organization virtual team to identify innovative ways of tackling specific cybercrime threats. The arrest made as a result of this partnership was announced earlier today in a joint press release.

Refud.me and Cryptex Reborn

Refud.me and Cryptex Reborn have been heavily advertised and used on cybercriminal underground forums. One particular forum, Hackforums.net, is known for hosting discussions on hacking, technology and gaming.

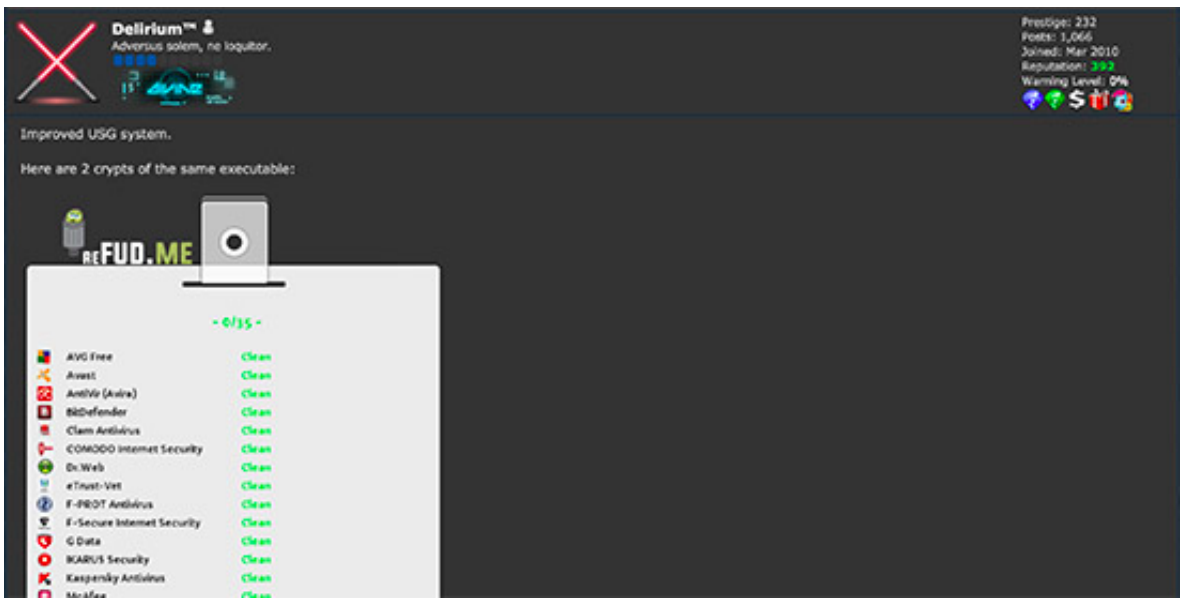

Figure 1. Example post of Refud.me scan results on Hackforums.net

Refud.me has been advertised on Hackforums.net since the end of February 2015, with several new features added during that time. A "scanwatch" feature which allows for the constant scanning and alerting of the detection status of an uploaded file was added at the end of June 2015.

Figure 2. The refud.me service

Refud.me provided CAV scanners, allowing users to upload a sample they want scanned, and this will then be tested for detection against typically 30-40 of the best known AV companies' products. The goal here is to ensure for a malware author or user that their malware is detected by as few companies as possible, before releasing it against their targets. It should be noted that similar legitimate multi-scanner services also exist – however a key difference with a CAV is that all sharing of samples or feedback data with the various AV companies are disabled, and this is actively advertised in advertisements.

On the other hand, Cryptex Reborn provides crypting services, which means taking a particular program, almost always malware, and modifying it to attempt to bypass the detection engines of the major antivirus companies. A piece of malware modified in such a way, that is no longer detected by an AV company at the time of release is known as FUD (Fully UnDetectable). This does not normally take into account the more advanced heuristic features of modern AV engines.

The Cryptex Reborn toolkit has undergone several major updates over time. The original tool, simply called "Cryptex" was advertised from at least October 2011. Later in 2011 this tool forked to become two crypting tools – "Cryptex Lite" and "Cryptex Advanced", each with different levels of capabilities. These tools saw frequent version updates to counteract new improvements in antivirus engines. The current major iteration of the Cryptex toolkit is entitled "Cryptex Reborn" which was first advertised in September 2014.

Figure 3. Advertisement for the tool

"Helping to take down operations such as this is part of our ongoing effort to keep the world safe for exchanging digital information, for both our customers and the Internet at large," Martin Rösler said.

Trend Micro has long believed that public-private collaboration is key to a lasting solution against cybercrime. In October, we partnered with the Federal Bureau of Investigation (FBI) and several security vendors to take down the DRIDEX botnet known for targeting banks. We have also collaborated with the International Criminal Police Organization (INTERPOL) and other vendors to take down the SIMDA botnet early this year.

Related Posts:

- Trend Micro Discovers MalumPoS; Malware Targeting Hotels and other US Industries
- CVE-2014-8439 Vulnerability: Trend Micro Solutions Ahead of the Game
- Pawn Storm Update: Trend Micro Discovers New Java Zero-Day Exploit
- Trend Micro Discovers Vulnerability That Renders Android Devices Silent

Tags: counter antiviruscryptexlaw enforcementNCArefud

Featured Stories

- 2016 Predictions: The Fine Line Between Business and Personal
- Pawn Storm Targets MH17 Investigation Team
- FBI, Security Vendors Partner for DRIDEX Takedown
- Japanese Cybercriminals New Addition To Underground Arena
- Follow the Data: Dissecting Data Breaches and Debunking the Myths

Recent Posts

- DRIDEX Spam Runs Resurface Against US Targets
- Prototype Nation: Emerging Innovations in Cybercriminal China
- Trend Micro, NCA Partnership Leads to Arrests and Shutdown of Refud.me and Cryptex Reborn
- Siri's Flaw: Apple's Personal Assistant Leaks Personal Data
- 3Q 2015 Security Roundup: Current Threats Forecast Impending Attack Scenarios

2016 Security Predictions

- From new extortion schemes and IoT threats to improved cybercrime legislation, Trend Micro predicts how the security landscape is going to look like in 2016. Read more

Popular Posts

Setting the Record Straight on Moplus SDK and the Wormhole Vulnerability
Hacking Team Flash Zero-Day Integrated Into Exploit Kits
Cybercriminals Improve Android Malware Stealth Routines with OBAD
Siri's Flaw: Apple's Personal Assistant Leaks Personal Data
Trend Micro, NCA Partnership Leads to Arrests and Shutdown of Refud.me and Cryptex Reborn

Latest Tweets

Error: Rate limit exceeded

Stay Updated

Email Subscription

Your email here

Subscribe