Nuclear Bot Author Arrested in Sextortion Case

krebsonsecurity.com/2019/12/nuclear-bot-author-arrested-in-sextortion-case/

Last summer, a wave of sextortion emails began flooding inboxes around the world. The spammers behind this scheme claimed they'd hacked your computer and recorded videos of you watching porn, and promised to release the embarrassing footage to all your contacts unless a bitcoin demand was paid. Now, French authorities say they've charged two men they believe are responsible for masterminding this scam. One of them is a 21-year-old hacker interviewed by KrebsOnSecurity in 2017 who openly admitted to authoring a banking trojan called "**Nuclear Bot**."

On Dec. 15, the French news daily *Le Parisien* published a report stating that French authorities had arrested and charged two men in the sextortion scheme. The story doesn't name either individual, but rather refers to one of the accused only by the pseudonym "Antoine I.," noting that his first had been changed (presumably to protect his identity because he hasn't yet been convicted of a crime).

"According to sources close to the investigation, Antoine I. surrendered to the French authorities at the beginning of the month, after being hunted down all over Europe," the story notes. "The young Frenchman, who lived between Ukraine, Poland and the Baltic countries, was indicted on 6 December for 'extortion by organized gang, fraudulent access to a data processing system and money laundering.' He was placed in pre-trial detention."

According to Le Parisien, Antoine I. admitted to being the inventor of the initial 2018 sextortion scam, which was subsequently imitated by countless other ne'er-do-wells. The story says the two men deployed malware to compromise at least 2,000 computers that were used to blast out the sextortion emails.

While that story is light on details about the identities of the accused, an earlier version of it published Dec. 14 includes more helpful clues. The Dec. 14 piece said Antoine I. had been interviewed by KrebsOnSecurity in April 2017, where he boasted about having created Nuclear Bot, a malware strain designed to steal banking credentials from victims.

My April 2017 exposé featured an interview with **Augustin Inzirillo**, a young man who came across as deeply conflicted about his chosen career path. That path became traceable after he released the computer code for Nuclear Bot on GitHub. Inzirillo outed himself by

defending the sophistication of his malware after it was ridiculed by both security researchers and denizens of the cybercrime underground, where copies of the code wound up for sale. From that story:

> “It was a big mistake, because now I know people will reuse my code to steal money from other people,” Inzirillo told KrebsOnSecurity in an online chat.
>
> Inzirillo released the code on GitHub with a short note explaining his motivations, and included a contact email address at a domain (inzirillo.com) set up long ago by his father, Daniel Inzirillo.
>
> KrebsOnSecurity also reached out to Daniel, and heard back from him roughly an hour before Augustin replied to requests for an interview. Inzirillo the elder said his son used the family domain name in his source code release as part of a misguided attempt to impress him.
>
> “He didn’t do it for money,” said Daniel Inzirillo, whose CV shows he has built an impressive career in computer programming and working for various financial institutions. “He did it to spite all the cyber shitheads. The idea was that they wouldn’t be able to sell his software anymore because it was now free for grabs.”

If Augustin Inzirillo ever did truly desire to change his ways, it wasn’t clear from his apparent actions last summer: The Le Parisien story says the sextortion scams netted the Frenchman and his co-conspirator at least a million Euros.

In August 2018, KrebsOnSecurity was contacted by a researcher working with French authorities on the investigation who said he suspected the young man was bragging on Twitter that he used a custom version of Nuclear Bot dubbed “TinyNuke” to steal funds from customers of French and Polish banks.

The source said this individual used the now-defunct Twitter account @tiny_gang1 to taunt French authorities, while showing off a fan of 100-Euro notes allegedly gained from his illicit activities (see image above). It seemed to the source that Inzirillo wanted to get caught, because at one point @tiny_gang1 even privately shared a copy of Inzirillo's French passport to prove his identity and accomplishments to the researcher.

"He modified the Tinynuke's config several times, and we saw numerous modifications in the malware code too," the source said. "We tried to compare his samples with the leaked code available on GitHub and we noticed that the guy actually was using a more advanced version with features that don't exist in the publicly available repositories. As an example, custom samples have video recording functionality, socks proxy and other features. So the guy clearly improved the source code and recompiled a new version for every new campaign."

The source said the person behind the @tiny_gang Twitter account attacked French targets with custom versions of TinyNuke in one to three campaigns per week earlier this year, harvesting French bank accounts and laundering the stolen funds via a money mule network based mostly in the United Kingdom.

“If the guy behind this campaign is the malware author, it could easily explain the modifications happening with the malware, and his French is pretty good,” the researcher told KrebsOnSecurity. “He’s really provocative and I think he wants to be arrested in France because it could be a good way to become famous and maybe prove that his malware works (to resell it after?).”

The source said the TinyNuke author threatened him with physical harm after the researcher insulted his intelligence while trying to goad him into disclosing more details about his cybercrime activities.

“The guy has a serious ego problem,” the researcher said. “He likes when we talk about him and he hates when we mock him. He got really angry as time went by and started personally threatening me. In the last [TinyNuke malware configuration file] targeting Poland we found a long message dedicated to me with clear physical threats.”

All of the above is consistent with the findings detailed in the Le Parisien report, which quoted French investigators saying Antoine I. in October 2019 used a now-deleted Twitter account to taunt the authorities into looking for him. In one such post, he included a picture of himself holding a beer, saying: “On the train to Naples. You should send me a registered letter instead of threatening guys informally.”

The Le Parisien story also said Antoine I. threatened a researcher working with French authorities on the investigation (the researcher is referred to pseudonymously as “Marc”).

“I make a lot more money than you, I am younger, more intelligent,” Antoine I. reportedly wrote in July 2018 to Marc. “If you do not stop playing with me, I will put a bullet in your head. ”

French authorities say the defendant managed his extortion operations while traveling throughout Ukraine and other parts of Eastern Europe. But at some point he decided to return home to France, despite knowing investigators there were hunting him. According to Le Parisien, he told the French authorities he wanted to cooperate in the investigation and that he no longer wished to live like a fugitive.