Is ‘REvil’ the New GandCrab Ransomware?

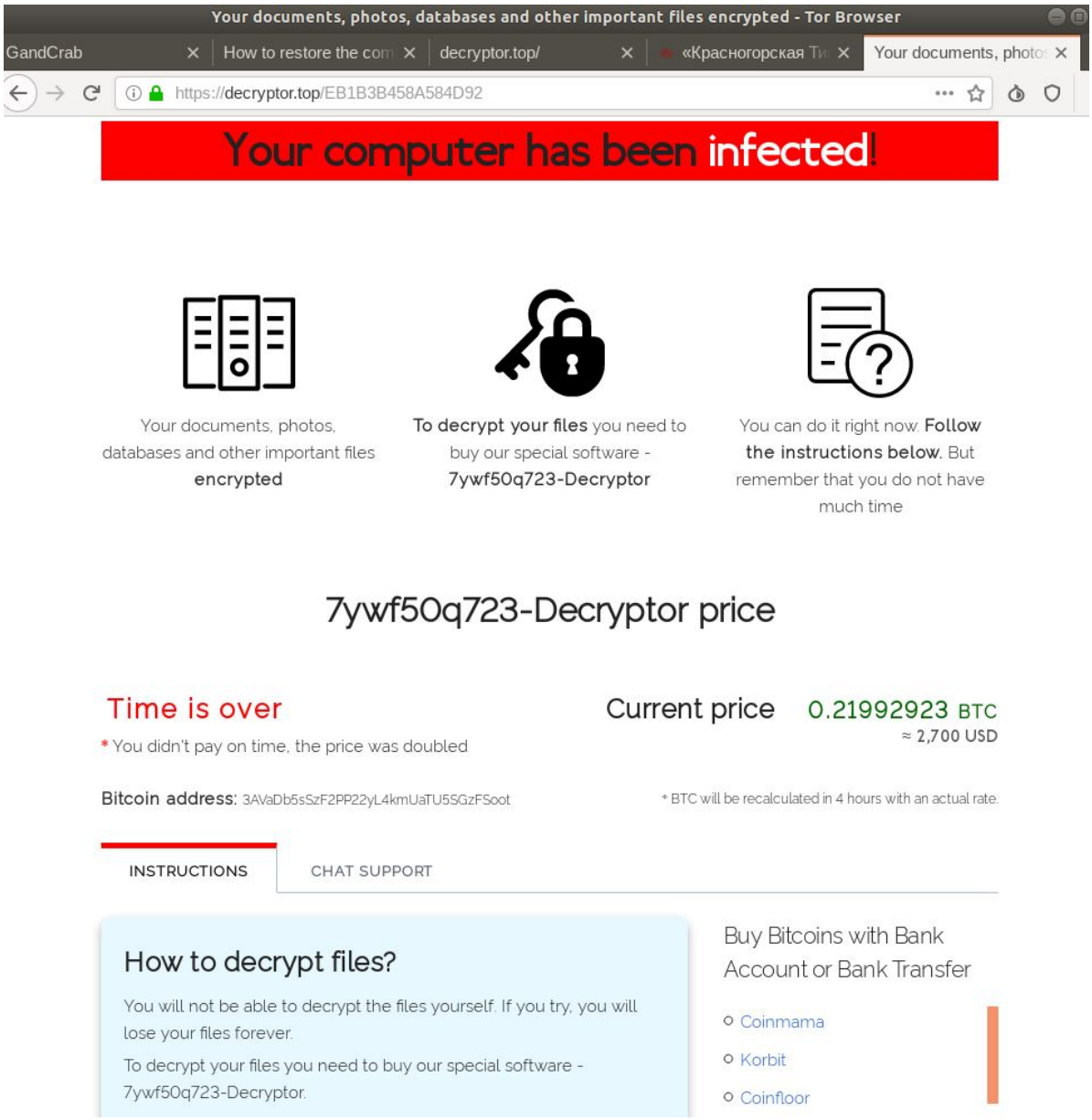
krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

The cybercriminals behind the **GandCrab** ransomware-as-a-service (RaaS) offering recently announced they were closing up shop and retiring after having allegedly earned more than $2 billion in extortion payments from victims. But a growing body of evidence suggests the GandCrab team have instead quietly regrouped behind a more exclusive and advanced ransomware program known variously as “**REvil**,” “**Sodin**,” and “**Sodinokibi**.”

“We are getting a well-deserved retirement,” the GandCrab administrator(s) wrote in their farewell message on May 31. “We are a living proof that you can do evil and get off scot-free.”

However, it now appears the GandCrab team had already begun preparations to re-brand under a far more private ransomware-as-a-service offering months before their official “retirement.”

In late April, researchers at **Cisco Talos** spotted a new ransomware strain dubbed Sodinokibi that was used to deploy GandCrab, which encrypts files on infected systems unless and until the victim pays the demanded sum. A month later, GandCrab would announce its closure.



A payment page for a victim of REvil, a.k.a. Sodin and Sodinokibi.

Meanwhile, in the first half of May an individual using the nickname "**Unknown**" began making deposits totaling more than USD $130,000 worth of virtual currencies on two top cybercrime forums. The down payments were meant to demonstrate the actor meant business in his offer to hire just a handful of affiliates to drive a new, as-yet unnamed ransomware-as-a-service offering.

"We are not going to hire as many people as possible," Unknown told forum members in announcing the new RaaS program. "Five affiliates more can join the program and then we'll go under the radar. Each affiliate is guaranteed USD 10,000. Your cut is 60 percent at the beginning and 70 percent after the first three payments are made. Five affiliates are guaranteed [USD] 50,000 in total. We have been working for several years, specifically five years in this field. We are interested in professionals."

Asked by forum members to name the ransomware service, Unknown said it had been mentioned in media reports but that he wouldn't be disclosing technical details of the program or its name for the time being.

Unknown said it was forbidden to install the new ransomware strain on any computers in the Commonwealth of Independent States (CIS), which includes Armenia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine and Uzbekistan.

The prohibition against spreading malware in CIS countries has long been a staple of various pay-per-install affiliate programs that are operated by crooks residing in those nations. The idea here is not to attract attention from local law enforcement responding to victim complaints (and/or perhaps to stay off the radar of tax authorities and extortionists in their hometowns).

But **Kaspersky Lab** discovered that Sodinokobi/REvil also includes one other nation on its list of countries that affiliates should avoid infecting: Syria. Interestingly, latter versions of GandCrab took the same unusual step.

What's the significance of the Syria connection? In October 2018, a Syrian man tweeted that he had lost access to all pictures of his deceased children after his computer got infected with GandCrab.

"They want 600 dollars to give me back my children, that's what they've done, they've taken my boys away from me for a some filthy money," the victim wrote. "How can I pay them 600 dollars if I barely have enough money to put food on the table for me and my wife?"

That heartfelt appeal apparently struck a chord with the developer(s) of GandCrab, who soon after released a decryption key that let all GandCrab victims in Syria unlock their files for free.

But this rare display of mercy probably cost the GandCrab administrators and its affiliates a pretty penny. That's because a week after GandCrab released decryption keys for all victims in Syria, the No More Ransom project released a free GandCrab decryption tool developed by Romanian police in collaboration with law enforcement offices from a number of countries and security firm **Bitdefender**.

The GandCrab operators later told affiliates that the release of the decryption keys for Syrian victims allowed the entropy used by the random number generator for the ransomware's master key to be calculated. Approximately 24 hours after NoMoreRansom released its free tool, the GandCrab team shipped an update that rendered it unable to decrypt files.

There are also similarities between the ways that both GandCrab and REvil generate URLs that are used as part of the infection process, according a recent report from Dutch security firm **Tesorion**.

"Even though the code bases differ significantly, the lists of strings that are used to generate the URLs are very similar (although not identical), and there are some striking similarities in how this specific part of the code works, e.g., in the somewhat far-fetched way that the random length of the filename is repeatedly recalculated," Tesorion observed.

My guess is the GandCrab team has not retired, and has simply regrouped and re-branded due to the significant amount of attention from security researchers and law enforcement investigators. It seems highly unlikely that such a successful group of cybercriminals would just walk away from such an insanely profitable enterprise.