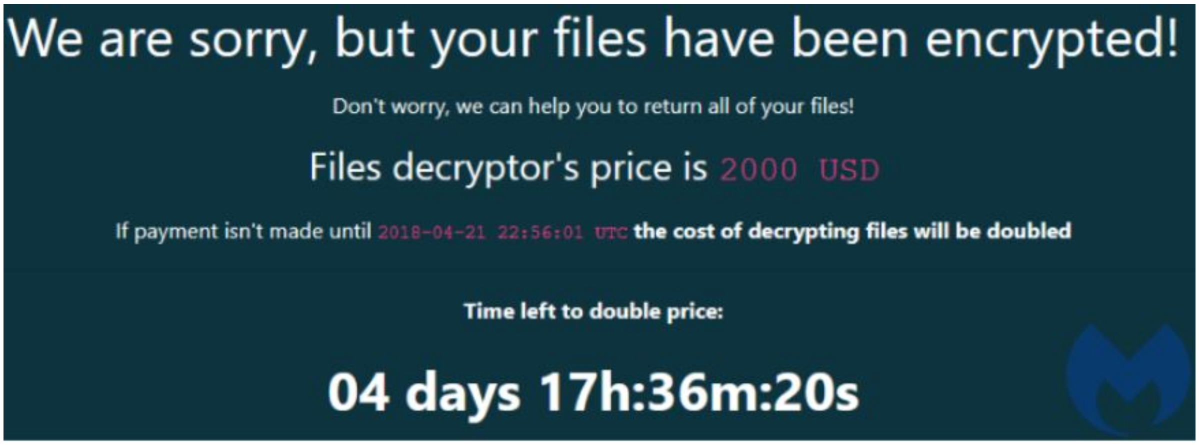
Who’s Behind the GandCrab Ransomware?

krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/

The crooks behind an affiliate program that paid cybercriminals to install the destructive and wildly successful **GandCrab** ransomware strain announced on May 31, 2019 they were terminating the program after allegedly having earned more than $2 billion in extortion payouts from victims. What follows is a deep dive into who may be responsible for recruiting new members to help spread the contagion.



We are sorry, but your files have been encrypted!

Don't worry, we can help you to return all of your files!

Files decryptor's price is 2000 USD

If payment isn't made until 2018-04-21 22:56:01 UTC **the cost of decrypting files will be doubled**

Time left to double price:

04 days 17h:36m:20s

Image: Malwarebytes.

Like most ransomware strains, the GandCrab ransomware-as-a-service offering held files on infected systems hostage unless and until victims agreed to pay the demanded sum. But GandCrab far eclipsed the success of competing ransomware affiliate programs largely because its authors worked assiduously to update the malware so that it could evade antivirus and other security defenses.

In the 15-month span of the GandCrab affiliate enterprise beginning in January 2018, its curators shipped five major revisions to the code, each corresponding with sneaky new features and bug fixes aimed at thwarting the efforts of computer security firms to stymie the spread of the malware.

“In one year, people who worked with us have earned over US $2 billion,” read the farewell post by the eponymous GandCrab identity on the cybercrime forum **Exploit[.]in**, where the group recruited many of its distributors. “Our name became a generic term for ransomware in the underground. The average weekly income of the project was equal to US $2.5 million.”

The message continued:

> “We ourselves have earned over US $150 million in one year. This money has been successfully cashed out and invested in various legal projects, both online and offline ones. It has been a pleasure to work with you. But, like we said, all things come to an end. We are getting a well-deserved retirement. We are a living proof that you can do evil and get off scot-free. We have proved that one can make a lifetime of money in one year. We have proved that you can become number one by general admission, not in your own conceit.”

Evil indeed, when one considers the damage inflicted on so many individuals and businesses hit by GandCrab — easily the most rapacious and predatory malware of 2018 and well into 2019.

The GandCrab identity on Exploit[.]in periodically posted updates about victim counts and ransom payouts. For example, in late July 2018, GandCrab crowed that a single affiliate of the ransomware rental service had infected 27,031 victims in the previous month alone, receiving about $125,000 in commissions.

The following month, GandCrab bragged that the program in July 2018 netted almost 425,000 victims and extorted more than one million dollars worth of cryptocurrencies, much of which went to affiliates who helped to spread the infections.

Russian security firm **Kaspersky Lab** estimated that by the time the program ceased operations, GandCrab accounted for up to half of the global ransomware market.

ONEIILK2

It remains unclear how many individuals were active in the core GandCrab malware development team. But KrebsOnSecurity located a number of clues that point to the real-life identity of a Russian man who appears to have been put in charge of recruiting new affiliates for the program.

In November 2018, a GandCrab affiliate posted a screenshot on the Exploit[.]in cybercrime forum of a private message between himself and a forum member known variously as “**oneiilk2**” and “**oneillk2**” that showed the latter was in charge of recruiting new members to the ransomware earnings program.

Oneiilk2 also was a successful GandCrab affiliate in his own right. In May 2018, he could be seen in multiple Exploit[.]in threads asking for urgent help obtaining access to hacked businesses in South Korea. These solicitations go on for several weeks that month — with Oneiilk2 saying he’s willing to pay top dollar for the requested resources. At the same time, Oneiilk2 can be seen on Exploit asking for help figuring out how to craft a convincing malware lure using the Korean alphabet.

Later in the month, Oneiilk2 says he no longer needs assistance on that request. Just a few weeks later, security firms began warning that attackers were staging a spam campaign to target South Korean businesses with version 4.3 of GandCrab.

HOTTABYCH

When Oneiilk2 registered on Exploit in January 2015, he used the email address **hottabych_k2@mail.ru**. That email address and nickname had been used since 2009 to register multiple identities on more than a half dozen cybercrime forums.

In 2010, the hottabych_k2 address was used to register the domain name **dedserver[.]ru**, a site which marketed dedicated Web servers to individuals involved in various cybercrime projects. That domain registration record included the Russian phone number **+7-951-7805896**, which mail.ru's password recovery function says is indeed the phone number used to register the hottabych_k2 email account.

At least four posts made in 2010 to the hosting review service makeserver.ru advertise Dedserver and include images watermarked with the nickname "oneillk2."

Dedserver also heavily promoted a virtual private networking (VPN) service called **vpn-service[.]us** to help users obfuscate their true online locations. It's unclear how closely connected these businesses were, although a cached copy of the Dedserver homepage at Archive.org from 2010 suggests the site's owners claimed it as their own.

Vpn-service[.]us was registered to the email address **sec-service@mail.ru** by an individual who used the nickname (and sometimes password) — "**Metall2**" — across multiple cybercrime forums.

Around the same time the GandCrab affiliate program was kicking into high gear, Oneiilk2 had emerged as one of the most trusted members of Exploit and several other forums. This was evident by measuring the total "reputation points" assigned to him, which are positive or negative feedback awarded by other members with whom the member has previously transacted.

In late 2018, Oneiilk2 was one of the top 20 highest-rated members among thousands of denizens on the Exploit forum, thanks in no small part to his association with the GandCrab enterprise.

Searching on Oneiilk2's registration email address hottabych_k2@mail.ru via sites that track hacked or leaked databases turned up some curious results. Those records show this individual routinely re-used the same password across multiple accounts: 16061991.

For instance, that email address and password shows up in hacked password databases for an account "oneillk2" at **zismo[.]biz**, a Russian-language forum dedicated to news about various online money-making affiliate programs.

In a post made on Zismo in 2017, Oneiilk2 states that he lives in a small town with a population of around 400,000, and is engaged in the manufacture of furniture.

HEAVY METALL

Further digging revealed that the hottabych_k2@mail.ru address had also been used to register at least two accounts on the social networking site **Vkontakte**, the Russian-language equivalent of Facebook.

One of those accounts was registered to a "Igor Kashkov" from Magnitogorsk, Russia, a metal-rich industrial town in southern Russia of around 410,000 residents which is home to the largest iron and steel works in the country.

The Kashkov account used the password "hottabychk2," the phone number **890808981338**, and at one point provided the alternative email address "**prokopenko_k2@bk.ru**." However, this appears to have been simply an abandoned account, or at least there are only a couple of sparse updates to the profile.

The more interesting Vkontakte account tied to the hottabych_k2@mail.ru address belongs to a profile under the name "**Igor Prokopenko**," who says he also lives in Magnitogorsk. The Igor Prokopenko profile says he has studied and is interested in various types of metallurgy.

There is also a Skype voice-over-IP account tied to an "Igor" from Magnitogorsk whose listed birthday is June 16, 1991. In addition, there is a fairly active Youtube account dating back to 2015 — youtube.com/user/Oneillk2 — that belongs to an Igor Prokopenko from Magnitogorsk.

That Youtube account includes mostly short videos of Mr. Prokopenko angling for fish in a local river and diagnosing problems with his Lada Kalina — a Russian-made automobile line that is quite common across Russia. An account created in January 2018 using the Oneillk2 nickname on a forum for Lada enthusiasts says its owner is 28 years old and lives in Magnitogorsk.

Sources with the ability to check Russian citizenship records identified an **Igor Vladimirovich Prokopenko** from Magnitogorsk who was born on June 16, 1991. Recall that "16061991" was the password used by countless online accounts tied to both hottabych_k2@mail.ru and the Oneiilk2/Oneillk2 identities.

To bring all of the above research full circle, Vkontakte's password reset page shows that the Igor Prokopenko profile is tied to the mobile phone number **+7-951-7805896**, which is the same number used to set up the email account **hottabych_k2@mail.ru** almost 10 years ago.

Mr. Prokopenko did not respond to multiple requests for comment.

It is entirely possible that whoever is responsible for operating the GandCrab affiliate program developed an elaborate, years-long disinformation campaign to lead future would-be researchers to an innocent party.

At the same time, it is not uncommon for many Russian malefactors to do little to hide their true identities — at least early on in their careers — perhaps in part because they perceive that there is little likelihood that someone will bother connecting the dots later on, or because maybe they don't fear arrest and/or prosecution while they reside in Russia. Anyone doubtful about this dynamic would do well to consult the Breadcrumbs series on this blog, which used similar methods as described above to unmask dozens of other major malware purveyors.

It should be noted that the GandCrab affiliate program took measures to prevent the installation of its ransomware on computers residing in Russia or in any of the countries that were previously part of the Soviet Union — referred to as the Commonwealth of Independent States and including Armenia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine and Uzbekistan. This is a typical precaution taken by cybercriminals running malware operations from one of those countries, as they try to avoid making trouble in their own backyards that might attract attention from local law enforcement.

KrebsOnSecurity would like to thank domaintools.com (an advertiser on this site), as well as cyber intelligence firms Intel471, Hold Security and 4IQ for their assistance in researching this post.

Update, July 9, 2:53 p.m. ET: Mr. Prokopenko responded to my requests for comment, although he declined to answer any of the questions I put to him about the above findings. His response was simply, "Hey. You're wrong. I'm not doing this." Silly me.