Who Wrote the ALPHV/BlackCat Ransomware Strain?

krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/

In December 2021, researchers discovered a new ransomware-as-a-service named **ALPHV** (a.k.a. "**BlackCat**"), considered to be the first professional cybercrime group to create and use a ransomware strain written in the **Rust** programming language. In this post, we'll explore some of the clues left behind by a developer who was reputedly hired to code the ransomware variant.

Image: Varonis.

According to an analysis released this week by Varonis, ALPHV is actively recruiting operators from several ransomware organizations — including REvil, BlackMatter and DarkSide — and is offering affiliates up to 90 percent of any ransom paid by a victim organization.

"The group's leak site, active since early December 2021, has named over twenty victim organizations as of late January 2022, though the total number of victims, including those that have paid a ransom to avoid exposure, is likely greater," Varonis's **Jason Hill** wrote.

One concern about more malware shifting to Rust is that it is considered a much more secure programming language compared to C and C++, writes **Catalin Cimpanu** for The Record. The upshot? Security defenders are constantly looking for coding weaknesses in many ransomware strains, and if more start moving to Rust it could become more difficult to find those soft spots.

Researchers at **Recorded Future** say they believe the ALPHV/BlackCat author was previously involved with the infamous REvil ransomware cartel in some capacity. Earlier this month the Russian government announced that at the United States' request it arrested 14 individuals in Russia thought to be REvil operators.

Still, REvil rolls on despite these actions, according to **Paul Roberts** at ReversingLabs. "The recent arrests have NOT led to a noticeable change in detections of REvil malicious files," Roberts wrote. "In fact, detections of files and other software modules associated with the REvil ransomware increased modestly in the week following the arrests by Russia's FSB intelligence service."

Meanwhile, the **U.S. State Department** has a standing $10 million reward for information leading to the identification or location of any individuals holding key leadership positions in REvil.

WHO IS BINRS?

A confidential source recently had a private conversation with a support representative who fields questions and inquiries on several cybercrime forums on behalf of a large and popular ransomware affiliate program. The affiliate rep confirmed that a coder for ALPHV was known by the handle "**Binrs**" on multiple Russian-language forums.

On the cybercrime forum **RAMP**, the user Binrs says they are a Rust developer who's been coding for 6 years. "My stack is Rust, nodejs, php, golang," Binrs said in an introductory post, in which they claim to be fluent in English. Binrs then signs the post with their identification number for ToX, a peer-to-peer instant messaging service.

That same ToX ID was claimed by a user called "**smiseo**" on the Russian forum BHF, in which smiseo advertises "clipper" malware written in Rust that swaps in the attacker's bitcoin address when the victim copies a cryptocurrency address to their computer's temporary clipboard.

The nickname "**YBCat**" advertised that same ToX ID on Carder[.]uk, where this user claimed ownership over the Telegram account **@CookieDays**, and said they could be hired to do software and bot development "of any level of complexity." YBCat mostly sold "installs," offering paying customers to ability to load malware of their choice on thousands of hacked computers simultaneously.

There is also an active user named Binrs on the Russian crime forum wwh-club[.]co who says they're a Rust coder who can be reached at the @CookieDays Telegram account.

On the Russian forum Lolzteam, a member with the username "**DuckerMan**" uses the @CookieDays Telegram account in his signature. In one thread, DuckerMan promotes an affiliate program called CookieDays that lets people make money by getting others to install

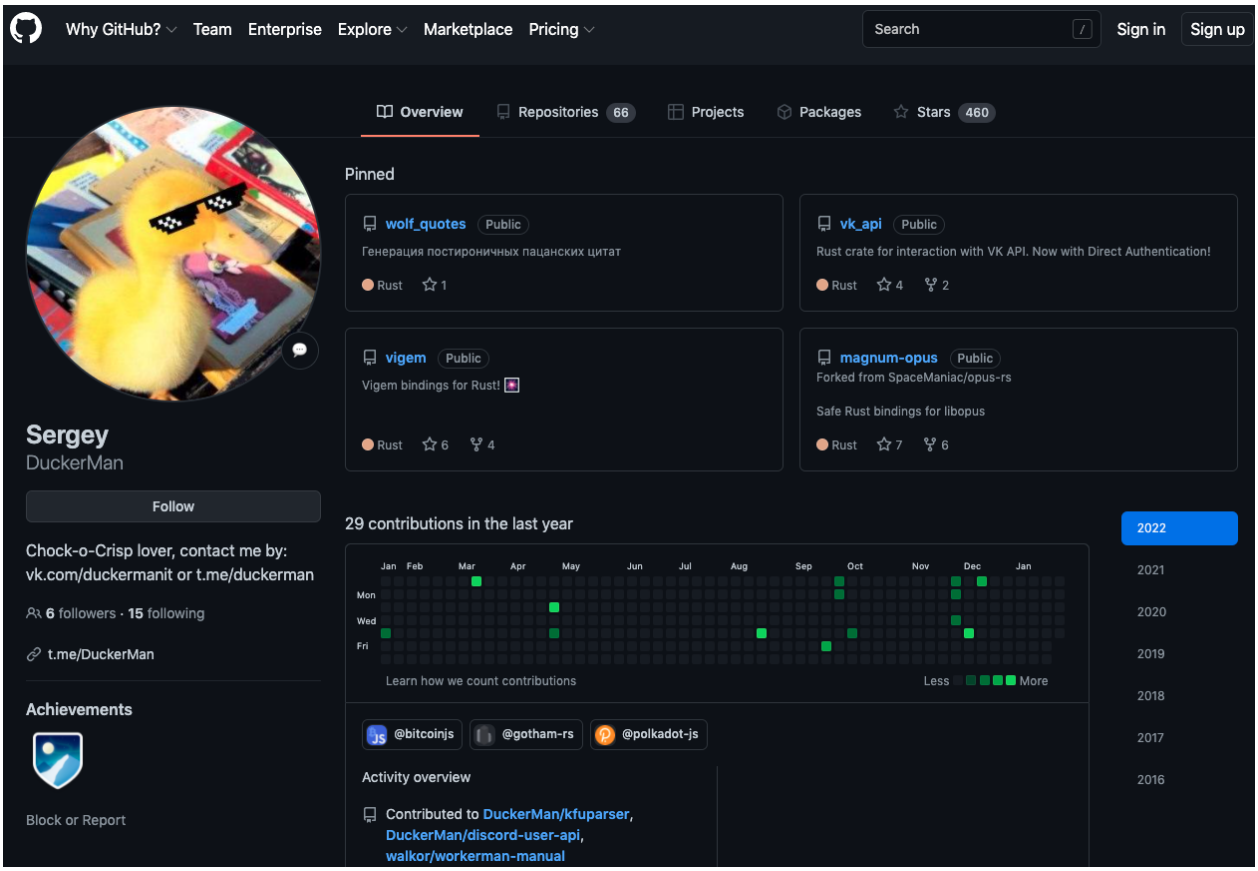
cryptomining programs that are infected with malware. In another thread, DuckerMan is selling a different clipboard hijacking program called Chloe Clipper.

The CookieDays moneymaking program.

According to threat intelligence firm Flashpoint, the Telegram user DuckerMan employed another alias — **Sergey Duck**. These accounts were most active in the Telegram channels "Bank Accounts Selling," "Malware developers community," and "Raidforums," a popular English-language cybercrime forum.

I AM DUCKERMAN

The **GitHub** account for a Sergey DuckerMan lists dozens of code repositories this user has posted online over the years. The majority of these projects were written in Rust, and the rest in PHP, Golang and Nodejs — the same coding languages specified by Binrs on RAMP. The Sergey DuckerMan GitHub account also says it is associated with the "DuckerMan" account on Telegram.



Sergey DuckerMan's GitHub profile.

Sergey DuckerMan has left many accolades for other programmers on GitHub — 460 to be exact. In June 2020, for example, DuckerMan gave a star to a proof-of-concept ransomware strain written in Rust.

Sergey DuckerMan's Github profile says their social media account at **Vkontakte** (Russian version of Facebook/Meta) is **vk.com/duckermanit**. That profile is restricted to friends-only, but states that it belongs to a **Sergey Pechnikov** from Shuya, Russia.

A look at the Duckermanit VKontakte profile in Archive.org shows that until recently it bore a different name: **Sergey Kryakov**. The current profile image on the Pechnikov account shows a young man standing closely next to a young woman.

KrebsOnSecurity reached out to Pechnikov in transliterated Russian via the instant message feature built into VKontakte.

“I’ve heard about ALPHV,” Pechnikov replied in English. “It sounds really cool and I’m glad that Rust becomes more and more popular, even in malware sphere. But I don’t have any connections with ransomware at all.”

I began explaining the clues that led to his VK account, and how a key cybercriminal actor in the ransomware space had confirmed that Binrs was a core developer for the ALPHV ransomware.

“Binrs isn’t even a programmer,” Pechnikov interjected. “He/she can’t be a DuckerMan. I am DuckerMan.”

BK: Right. Well, according to Flashpoint, the Telegram user DuckerMan also used the alias Sergey Duck.

Sergey: Yep, that’s me.

BK: So you can see already how I arrived at your profile?

Sergey: Yep, you’re a really good investigator.

BK: I noticed this profile used to have a different name attached to it. A ‘Sergey Kryakov.’

Sergey: It was my old surname. But I hated it so much I changed it.

BK: What did you mean Binrs isn’t even a programmer?

Sergey: I haven’t found any [of] his accounts on sites like GitHub/stack overflow. I’m not sure, does binrs sell Rust Clipper?

BK: So you know his work! I take it that despite all of this, you maintain you are not involved in coding malware?

Sergey: Well, no, but I have some “connections” with these guys. Speaking about Binrs, I’ve been researching his personality since October too.

BK: Interesting. What made you want to research his personality? Also, please help me understand what you mean by “connections.”

Sergey: I think he is actually a group of some people. I’ve written him on telegram from different accounts, and his way of speaking is different. Maybe some of them somehow tied with ALPHV. But on forums (I’ve checked only XSS and Exploit) his ways of speaking are the same.

BK: …..

Sergey: I don’t know how to explain this. By the way, binrs now is really silent, I think he’s lying low. Well, this is all I know.

No doubt he is. I enjoyed speaking with Sergey, but I also had difficulty believing most of what he said. Also, I was bothered that Sergey hadn't exactly disputed the logic behind the clues that led to his VK account. In fact, he'd stated several times that he was impressed with the investigation.

In many previous Breadcrumbs stories, it is common at this point for the interviewee to claim they were being set up or framed. But Sergey never even floated the idea.

I asked Sergey what might explain all these connections if he wasn't somehow involved in coding malicious software. His answer, our final exchange, was again equivocal.

"Well, all I have is code on my github," he replied. "So it can be used [by] anyone, but I don't think my projects suit for malwares."

Update, Jan 29, 4:26 p.m. ET: Sergey Duckerman has deleted their GitHub account. Meanwhile, the user Binrs has been (preemptively?) banning their profile from multiple cybercrime forums where they were previously active.