An ALPHV (BlackCat) representative discusses the group’s plans for a ransomware ‘meta-universe’

By Dmitry Smilyanets

Published: 2023-01-17 · Archived: 2026-04-05 23:21:26 UTC

Editor’s Note: Late last year, cybersecurity researchers began to notice a ransomware strain called ALPHV that stood out for being particularly sophisticated and coded in the Rust programming language—a first for ransomware used in real-world attacks.

The group has since garnered a reputation for aggressively posting details about its victims publicly—roughly two dozen have been posted on the group's extortion site over the last two months. Earlier this week, reports emerged that German cybersecurity officials believe the group is responsible for the recent attack on two German logistics companies, which led to oil supply disruptions across hundreds of gas stations.

A representative from the group, which has also been called BlackCat in some reports, agreed to talk to Recorded Future analyst Dmitry Smilyanets about the group's background, intentions, and plans for the future. The interview was conducted in Russian via TOX messaging, and was translated to English with the help of a linguist from Recorded Future's Insikt Group. It has been lightly edited for clarity.

Dmitry Smilyanets: How should I address you: ALPHV, Alfa, or BlackCat?

ALPHV Support: As much as we would like to avoid it, the brand must exist to simplify interaction with insurance and recovery companies. Our only name is ALPHV. BlackCat was invented by The Record and BC.a Noberus by Symantec [Editor’s note: The name ‘BlackCat’ was mentioned first by MalwareHunterTeam].

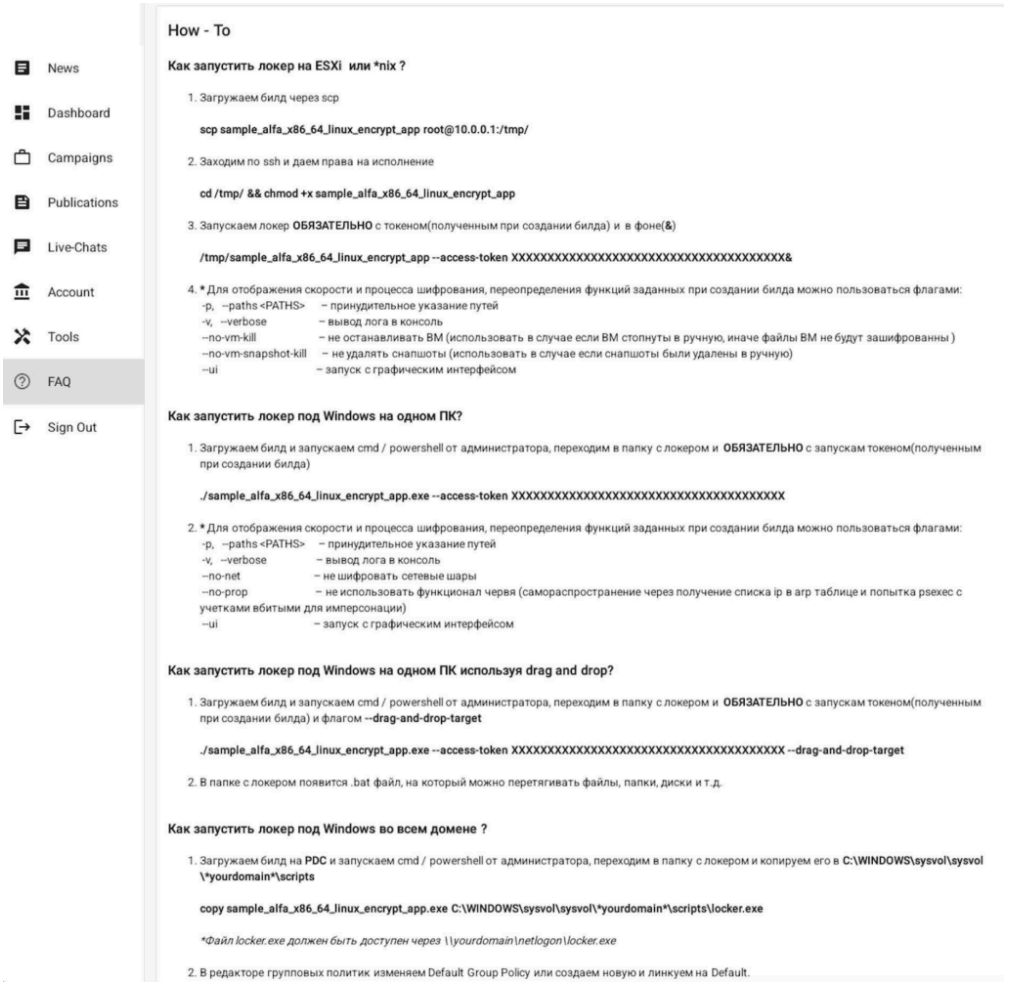
DS: You came to the ransomware scene with knowledge and experience. The code, the procedures, and the timings indicate that you have ties to REvil and possibly DarkSide. Is it a rebrand or a mix of talent under a new banner?

ALPHV: In part, we are all connected to gandrevil [GandCrab / REvil], blackside [BlackMatter / DarkSide], mazegreggor [Maze / Egregor], lockbit, etc., because we are adverts [Editor’s note: advertisers or affiliates]. Adverts write software, adverts pick a brand name, a partnership program is nothing without adverts. There is no rebranding or a mix of talents because we have no direct relation to these partnership programs. Let's just say: "We borrowed their advantages and eliminated their disadvantages."

DS: You mentioned multiple advantages over Conti and Lockbit ransomware variants, do you recognize other ransomware groups as competitors or business partners?

ALPHV: Without exaggeration, we believe that at the moment, there is no competitive software on the market. In addition to high-quality software, for advanced partners, we provide the full range of services related to ransom — metaverse or premium concierge — call it whatever you want. We are in a different weight category, so we don’t

recognize anyone, and we won't do TikTok ransomware houses. Separately, we want to thank the media for a detailed and honest review of the malware. The results speak for themselves.



DS: Are you going to add support for the Chinese language following the RAMP and Lockbit strategic expansion to the east?

ALPHV: We are absolutely not interested in any cooperation, expansion, or interaction with other affiliates and work only with Russian-speaking partners. Recently there was the first purge, the second one will come soon and we will close our doors. We do not plan to expand geographically (before the implementation of plans to take over the whole world), but we will definitely add Chinese after Arabic :)

DS: Why RUST? Are you trying to obfuscate previously used code? Cross-compiling?

ALPHV: RUST is chosen as a modern cross-platform low-level programming language. In the console command, the project name is alphv-N(ext)G(eneration). We have made a truly new product, with a new look and approach that meets modern requirements for both a RaaS solution and high-class commercial software.

DS: Why did you add Access tokens and unique domains for every victim?

ALPHV: As adverts of darkmatter [DarkSide / BlackMatter], we suffered from the interception of victims for subsequent decryption by Emsisoft.

[Editors note: Smilyanets contacted Emsisoft malware analyst Brett Callow for clarification, which we are including below for additional context.]

> Intel from various sources indicates that the actors behind BlackMatter may have replaced their dev team after we discovered and exploited a weakness in their ransomware, and the new team created ALPHV. Their comments about the chats perhaps support that.— ***Brett Callow, Emsisoft***

DS: You mentioned business contacts with the recovery companies who “previously worked with REvil and DarkSide.” Do negotiators help you to get what you want, or do they usually just get in the way?

ALPHV: Recovery companies we work with only simplify the process. They have their own personal discounts that can vary between 20-40% and the entire recovery process takes no more than 24 hours from the moment of the first contact.

An interesting fact: the real names of the companies were obtained as a result of the analysis of the correspondence of the victims after the network was encrypted, i.e. at the moment of negotiations, we understood with whom we were talking.

DS: How do you place yourself in the geopolitical fight between Russia and the USA?

ALPHV: Absolutely apolitical.

DS: You don’t recommend your affiliates target government, healthcare, and educational institutions, as well as prohibit attacks on Commonwealth of Independent States (CIS). How do you control your affiliates and enforce the rules?

ALPHV: We control preventively — at registration. As you can see, we do not run an active advertising campaign and easily cut ties with non-compliant partners, but no matter how hard we try to filter people when creating an account — shit happens. There was already one episode with (I quote) "not the neighboring countries." Decryption keys were issued automatically with the affiliate getting banned.

DS: One of the published victims is from the healthcare industry, how did this happen?

ALPHV: We do not attack state medical institutions, ambulances, hospitals. This rule does not apply to pharmaceutical companies, private clinics.

DS: Please explain how these special features work: Calls, DDoS, Brute, Mixer, Mega.

ALPHV: The entire list of options described below is available exclusively for adverts who have reached the mark of $1.5 million in the number of payments.

Calls. Outsourced solutions for calls. If communication with the victim is lost, you can try to establish contact by phone, in extreme cases, inform competitors about the leak. Not yet integrated into the panel, works in manual mode.DDoS. Own botnet for performing the most powerful DDoS attacks. Everything is clear here. Not yet integrated into the panel, works in manual mode.Brute. Own GPU data center + outsourcing rented facilities, own dictionaries, and rules. Currently is not available. In the future, it will allow adverts to break hashes in the panel.Mixer. This is not our mixer at all :) There is no process of mixing coins in our platform. When performing

an operation, our coins just go into the classic mixer for subsequent manipulations, and we get absolutely clean and verified coins, which even the most diligent exchange market will be happy with.Mega. Own distributed onion storage that simplifies the negotiation process for both our adverts and victims. Most dialogues begin with a request for a list/content of stolen files. We try to teach adverts to upload files to our data center immediately or even before the encryption process itself. In the future, this will allow sharing data on the volume/number of files, a file tree, and/or even a file shredder log to confirm the safe deletion of all existing files to the victim automatically; and today the storage allows you to avoid blocking from file hosting and simplifies the process of managing files between advert and victim. Already integrated into the panel, works automatically.

DS: Are you building a dream team ransomware partnership?

ALPHV: This was done at the planning stage. Our main goal is to create our own RaaS meta-universe that includes the full range of services related to our business.

DS: How will the ransomware scene change in the future?

ALPHV: Follow our updates :)

DS: Can you tell me a secret — who is “super admin”?

ALPHV: A very humble person, our spiritual and technical leader.

An ALPHV (BlackCat) ransomware representative posting on a popular hacking forum. IMAGE: RECORDED FUTURE.

DS: Can you comment on the investigation by Brian Krebs, in which he pointed out the connection between “binrs,” a developer, and ALPHV?

ALPHV: The investigations of couch analysts will always amuse the natives of the darknet. We are far beyond what Mr. Krebs can imagine.

No previous article

No new articles

Dmitry Smilyanets

Mission-driven and Russian-speaking intelligence analyst with type A personality. Dmitry has twenty years of experience and expertise in cybercrime activity that includes being a former member of an elite Russian-based hacking organization.
