Binance Helps Take Down Cybercriminal Ring Laundering $500M in Ransomware Attacks

binance.com/en/blog/421499824684902240/Binance-Helps-Take-Down-Cybercriminal-Ring-Laundering-$500M-in-Ransomware-Attacks

2021-06-24

Ransomware has become the biggest threat to online security, affecting all industries connected to the internet, from supply chains to healthcare institutions.

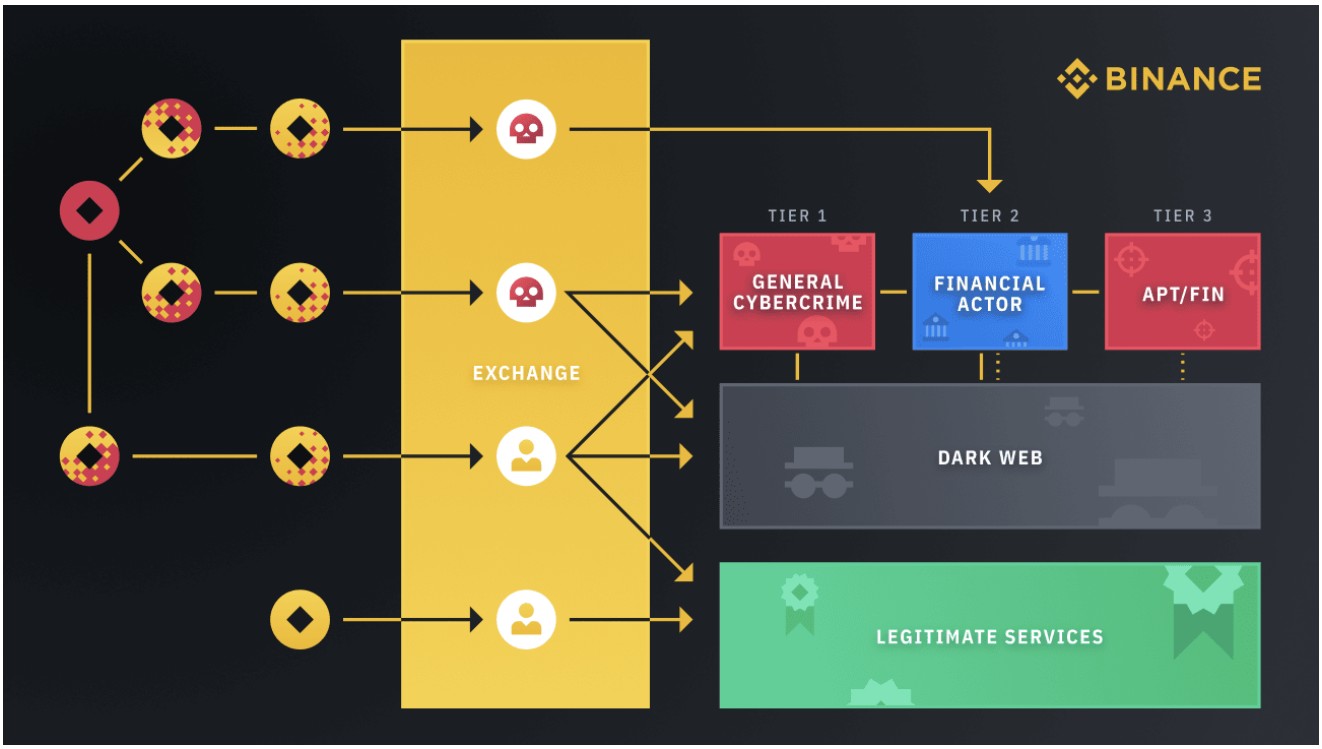
Therefore, a critical part of Binance's commitment to ensuring the secure and sustainable growth of the global crypto ecosystem involves fighting different strains of ransomware and fraud. Earlier this year we released a case study on our first Bulletproof Exchanger Project, a dedicated anti-ransomware initiative where we worked with the Ukraine Cyber Police to arrest a major cybercriminal group laundering over $42M of illicit funds.

More recently Binance Security has been taking part in an international investigation with Ukraine Cyber Police, Cyber Bureau of Korean National Police Agency, US Law Enforcement, Spanish Civil Guard, and Swiss Federal Office of Police, among others, in apprehending a prolific cybercriminal ring. The group -- also known as FANCYCAT -- has been running multiple criminal activities: distributing cyber attacks; operating a high-risk exchanger; and laundering money from dark web operations and high-profile cyber attacks such as Cl0p and Petya ransomware. In all, FANCYCAT is responsible for over $500M worth of damages in connection with ransomware and millions more from other cybercrimes.

Operation FANCYCAT

Over the past year we have expanded our in-house AML detection and analytics capabilities. Based on our research and analysis, as well as our understanding of cybercriminals' history and cashout tactics, we arrived at the conclusion that the biggest security problem in the industry today is money connected to cyber attacks being laundered through nested services and parasite exchanger accounts that live inside macro VASPs, including exchanges like Binance.com. These criminals enjoy taking advantage of reputable exchanges' liquidity, diverse digital asset offerings and well-developed APIs.

In a majority of the cases associated with illicit blockchain flows coming onto exchanges, the exchange is not harboring the actual criminal group themselves, but rather being used as a middleman to launder stolen profits. Figure 1 shows an example of the money laundering process on an exchange in relation to cyber attacks:



Blockchain analysis shows a network of money launderers living inside macro exchanges which deposit and withdraw to each other to wash the money. Understanding this diagnosis, we are taking the necessary steps to prevent illicit activity. We are applying a two-pronged approach: 1) implementing our own detection mechanisms to identify and offboard suspicious accounts 2) collaborating with law enforcement to build cases and take down criminal groups.

We applied the two-pronged approach to the FANCYCAT investigation: our AML detection and analytics program detected suspicious activity on Binance.com and expanded the suspect cluster. Once we mapped out the complete suspect network, we worked with private sector chain analytics companies TRM Labs and Crystal (BitFury) to analyze on-chain activity and gain a better understanding of this group and its attribution. Based on our analysis we found that this specific group was not only associated with laundering Cl0p attack funds, but also with Petya and other illegally-sourced funds. This led to the identification and eventual arrest of FANCYCAT.

We are continuing to investigate the FANCYCAT criminal syndicate across multiple jurisdictions and the connections associated with other cyber attacks.

Making the International Crypto Ecosystem a Safer Place

At Binance, we believe that strong controls across exchanges, smart legislation and ongoing education will help immensely with weeding out bad actors. Projects such as our “Bulletproof Exchanger” and our ongoing partnerships with law enforcement, as well as security and blockchain analytics firms, will be a driving force in improving the cybersecurity measures across the wider crypto industry.

About Binance

Binance is the world's leading blockchain and cryptocurrency infrastructure provider with a financial product suite that includes the largest digital asset exchange by volume. Trusted by millions worldwide, the Binance platform is dedicated to increasing the freedom of money for users, and features an unmatched portfolio of crypto products and offerings, including: trading and finance, education, data and research, social good, investment and incubation, decentralization and infrastructure solutions, and more. For more information, visit: https://www.binance.com

About Cyber Police Department of the National Police of Ukraine

The Cyber Police Department of the National Police of Ukraine has been established as part of the Ministry of Internal Affairs of Ukraine. The department has up to 400 law enforcement officers and senior specialists, including officers employed in every region of Ukraine at local cybercrime units. Investigators of the Cyber Police Department lead criminal proceedings on such cases:

- Crimes against information security;
- Crimes in the areas of IT, telecom and copyright;
- Crimes in the areas of payment systems and commercial activities;
- Computer intelligence activities.
- Cyber crime and illegal actions with cryptocurrency.

About Cyber Bureau of Korean National Police Agency

The Cyber Bureau of Korean National Police Agency investigates cybercrimes including cyber terrorism such as ransomware and provides digital forensics services.