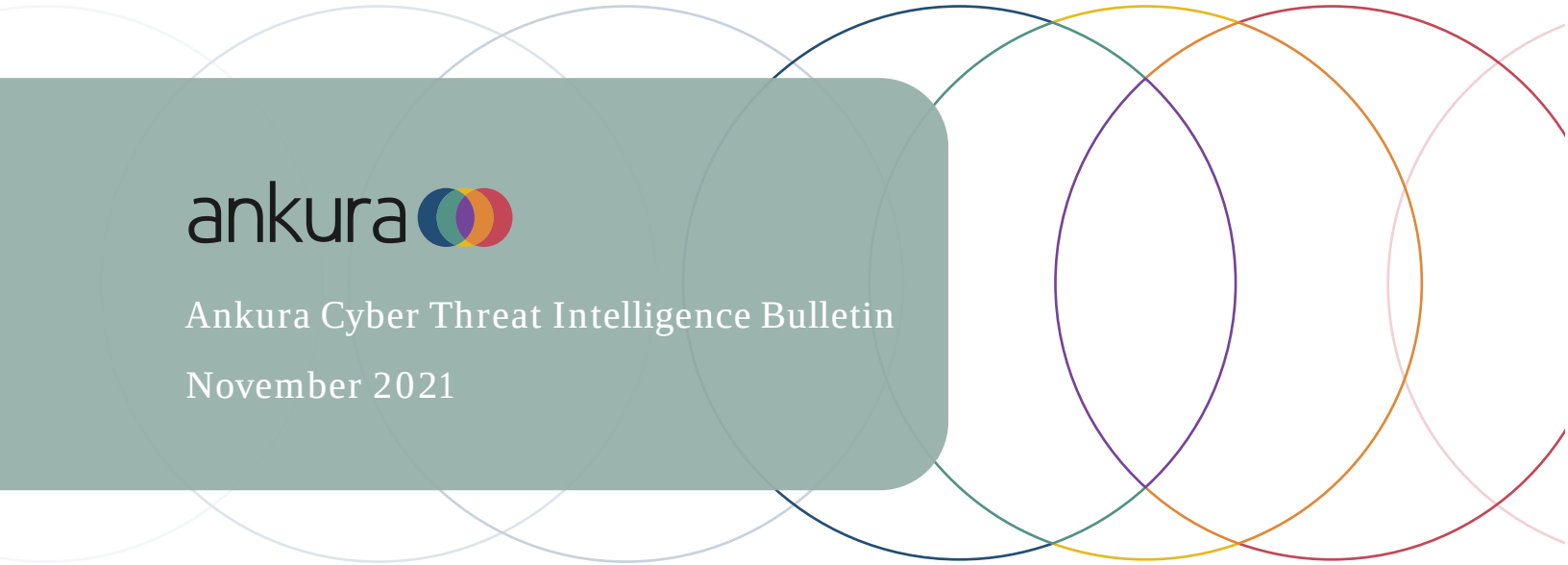


ankura

Ankura Cyber Threat Intelligence Bulletin

November 2021

Washington, DC
2000 K Street NW, 12th Floor
Washington, DC, United States 20006
+1.202.797.1111

Ankura Incident Response Services
Incident@ankura.com | 24/7 Assistance

CONTENTS

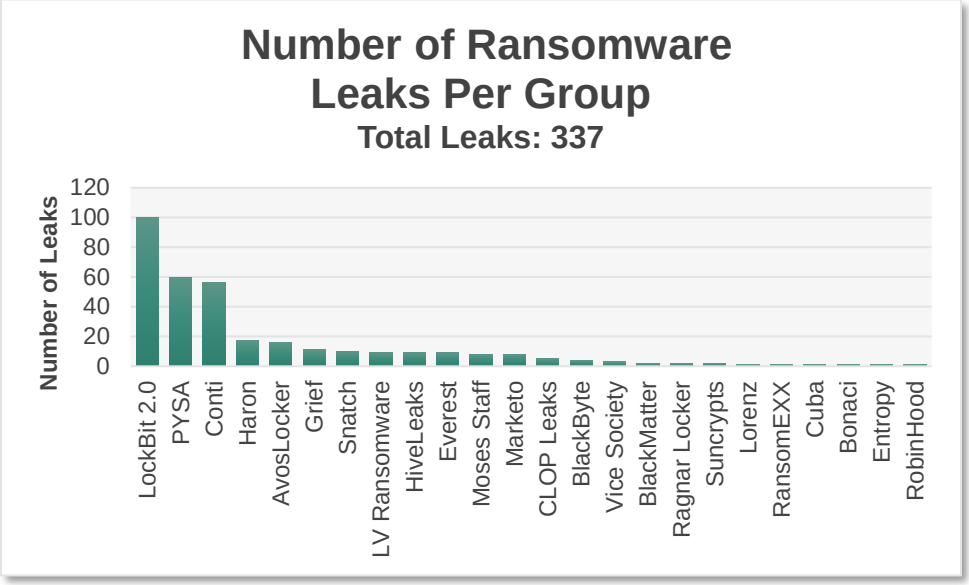
OBSERVATIONS

Over the past thirty (30) days, the Ankura Cybersecurity team has worked with clients to solve cybersecurity challenges involving recent cyber mercenary threat activity, coordinated government crackdowns on ransomware operations and affiliates, and a new open-source fuzz-testing Google tool that will allow developers, administrators, and security personnel to find vulnerable software bugs more efficiently.

For this month's report, Ankura's Cyber Threat Analysis and Pursuit Team (CTAPT) has compiled detailed metrics surrounding the tactics, techniques, and procedures (TTPs) employed by the "Void Balaur" cyber mercenary campaign. Additionally, government sanctions have been placed on ransomware groups, the organizations who accept money from them, as well as the cryptocurrency exchanges that allow their financial transactions and management.

RANSOMWARE METRICS

CTAPT analysts compile threat activity data from a variety of sources, including DarkFeed.io[1], to track ransomware and data leak trends. Below are the analytics from the past thirty (30) days compiled into a graph:



LockBit 2.0 and Conti continue to lead the pack in ransomware leaks by a wide margin. Most of the groups remain under ten (10) posts in a month. This month, analysts also observed PYSA attempt to make a PR stunt by dropping sixty (60) posts over two (2) days, though they have remained silent since. Barring any special circumstances, it is clear LockBit 2.0 and Conti intend to remain the top players in the ransomware industry to close out 2021.

VOID BALAUR: A CYBER MERCENARY CASE STUDY

This month, Trend Micro unveiled their research on a threat actor group "Void Balaur", a long-running cyber mercenary group of likely Russian origin. The term "cyber mercenary" is an apt description of Void Balaur, as while the group's activities do appear to overlap with ideologically motivated threat actors, they also carry out other types of cybercrime. The group appears to be connected to a range of social engineering and hacking attacks against numerous high-profile targets, including executives, activists, and politicians.

[1] https://darkfeed.io/

Void Balaur also has carried out numerous financially motivated attacks, targeting companies in the telecommunication, healthcare, aviation, and financial sectors.[2] Because of the wide range of tactics and target, the report provides insight into the challenges of attributing activities to a specific group.

In addition to these higher profile activities, Void Balaur appears to actively traffic sensitive information from Russian databases, which are sold on various low level Russian language forums such as Probiv and DarkMoney.[2] Popular wares include passport information, phone numbers, financial information, and other sensitive data.[3] While this can be used to facilitate other types of cybercrime, the Trend Micro report notes that Probiv data was also used by the investigative news outlet Bellingcat in their research into alleged Russian assassination attempts. While at this time it is not clear if Bellingcat bought data from Void Balaur specifically, the outlet did confirm the use of Probiv data to track flights of individuals of interest in their investigation.[4]

Indeed, while breaches due to technical vulnerabilities are often the focus of cybersecurity professionals, forums such as Probiv also offer data through compromised individuals rather than compromised technology. Bellingcat noted later that the "porous" state of Russian data protection made it relatively easy to obtain such sensitive information from compromised insiders.[5] Notably, Bellingcat's disclosure of using Probiv data appears to have resulted in a crackdown in Russia, resulting in a reduction in available data. This was reflected in Trend Micro's analysis of Void Balaur, in which at least one user expressed concern regarding their supply of sellable data.

The Void Balaur case study is carrying some lessons for researchers and cybersecurity experts. The first is that while technical vulnerabilities can lead to leaking personal data, nontechnical threats to privacy can create just as much opportunity for threat actors in countries where data privacy laws are lax or unenforced. Additionally, the groups overlap with other threat actors reveals the difficulty in attributing specific activity and reveals the value of long-term research to uncover patterns of illicit activity. Finally, as the Bellingcat case study shows, trafficking this data can have real world impacts beyond simple data leakage.

GOLDDUST ARRESTS INDIVIDUALS TIED TO RANSOMWARE

Over the past few months, multiple agencies around the globe have made an international joint effort to take down multiple currently active ransomware groups. United States law enforcement agencies were a part of this joint effort, with the creation of the Department of Justice (DOJ) Ransomware and Digital Extortion Taskforce, which also included departments within the Federal Bureau of Investigations (FBI) and the National Security Agency (NSA)[6]. Shortly after the Kaseya Attack, multiple law enforcement agencies from many foreign countries, such as France, Germany, Romania, and Europol (European Union Law Enforcement Agency), combined their intelligence efforts, and expanded to a joint investigation team named "GoldDust" to track down hackers belonging to the infamous group REvil.[7] Efforts were made to create a coalition of foreign intelligence agencies in order to combat ransomware and it seems to be an ideal solution to apprehending individuals involved in ransomware-based attacks. Recently, arrests were made by United States law enforcement to apprehend individuals involved with REvil and GandCrab.

GandCrab was a known Ransomware-as-a-Service (RaaS) hacking group that shut their services down in 2019 and released an updated version of their team/services, as a new method of attack, under a different alias known as "REvil." This infamous hacking group was the same threat actor that attacked JBS Foods

[2] https://documents.trendmicro.com/assets/white_papers/wp-void-balaur-tracking-a-cybermercenarys-activities.pdf
[3] https://www.bbc.com/news/world-europe-48348307
[4] https://www.newyorker.com/news/dispatch/how-bellingcat-unmasked-putins-assassins
[5] https://www.bellingcat.com/resources/2020/12/14/navalny-fsb-methodology/
[6] https://www.esecurityplanet.com/threats/kaseya-ransomware-arrest/
[7] https://urgentcomm.com/2021/11/09/u-s-charges-ukrainian-national-for-kaseya-ransomware-attack/

and was also responsible for hacking into the technology security firm Kaseya. A week following July 4th, 2021, REvil suddenly shutdown without a reason and/or an explanation. Recent news from Europol says that a total of seven (7) individuals who have been identified as working partners for a ransomware cartel have been arrested in South Korea, Romania, and Kuwait.[8] The RaaS affiliates intrude into companies, deploy ransomware, and distribute the profits made from such intrusions with coders employed by REvil and GandCrab. Europol has been assisting with other agencies and security firms to apprehend suspects involved with this type of attack. The efforts to apprehend these individuals also led to the United States charging a Ukrainian hacker responsible for the Kaseya breach.

Figure 1: Recent arrests made with the corresponding countries in which the arrests have been made.[8]

As previously mentioned, Kaseya, the information technology security firm was breached during a ransomware attack. Individuals behind this specific ransomware attack are known to be working partners of the infamous hacking group known as REvil. Ukrainian hacker, Yaroslav Vasinskyi, has been arrested in Poland by United States government authorities on October 8th, 2021 after an arrest warrant was issued by U.S. authorities. Vasinskyi has been identified as responsible for the data breach attack on Kaseya and was charged with "conspiracy to commit fraud and related activity in connection with computers, substantive counts of damage to protected computers, and conspiracy to commit money laundering."[9] The suspect is currently awaiting extradition to the United States where he faces additional charges related to ransomware attacks committed against other companies within the United States. The formation of GoldDust, originating back in 2018, resulted in the apprehension of the mentioned suspects involved in these recent ransomware attacks. Additional efforts have been made by the United States law enforcement to apprehend more individuals involved in ransomware activity.

The United States is also offering a $10 million reward for any information provided on the threat actor "Darkside." Darkside is a cyber hacking group that originated in Europe targeting victims with ransomware attacks as well as extortion. The U.S. State department is offering up to five (5) million dollars for intelligence that can aid in the arrest of individuals involved with conspiracy in any country. The reward is a method of demonstrating to the public that there is a commitment to protecting victims of ransomware attacks. Darkside ceased their services on May 17, 2021, and as a new method of attack, attempted to bounce back into the cybersecurity realm with the new alias "BlackMatter" only to disappear yet again from authorities.[10] Many suspects have been apprehended with the help of GoldDust, foreign intelligence efforts, and more, although many more individuals/hacking groups form almost every day creating unnecessary chaos/disruption to the public. Individuals like Aleksandr Zhukov continue to evolve and wreak havoc by creating bots/scripts to cause disruptions/losses.

[8] https://therecord.media/europol-seven-revil-gandcrab-ransomware-affiliates-were-arrested-in-2021/
[9] https://thehackernews.com/2021/11/us-charges-ukrainian-hacker-for-kaseya.html
[10] https://thehackernews.com/2021/11/us-offers-10-million-reward-for.html

Aleksandr Zhukov, the owner of the moniker “Methbot”, also known as “King of Fraud”, has created and operated “Methbot/3ve” which is known for posting real ads on fraudulent websites. Zhukov hired programmers to build and manage operation and kept seventy-five percent (75%) of profits. A U.S. judge sentenced Zhukov to ten (10) years in prison for running the botnet from 2014-2018. Zhukov was arrested in November 2018 while he was traveling to Bulgaria on an FBI-issued arrest warrant. Zhukov was formally charged the following week. According to the record, “Aleksandr Zhukov was found guilty in trial and convicted in May of 2021 of wire fraud conspiracy, wire fraud, money laundering conspiracy and money laundering.”[11] Many efforts have been made by the United States government as well as foreign law enforcement agencies around the globe coming together to put an end to the ransomware activity and shut down RaaS (Ransomware-as-a-Service) services. Efforts have been made by the United States coupled with other countries around the globe who are also experiencing such losses and disruptions to everyday services, and more. Joint international teams, such as GoldDust, assist in the apprehension of such experienced individuals. Continuous efforts will be made to mitigate financial losses and disruptions caused by these types of attacks.

U.S. SANCTIONS RANSOMWARE-AFFILIATED CRYPTO EXCHANGES

The United States war on ransomware reached a tipping point in 2021. Driven by the attacks on Colonial Pipeline, who paid $4.4 million to the ransomware group DarkSide,[12] and JBS Foods, paying $11 million to REvil[13], ransomware operators have seen huge profits this year. The Biden administration has started to take action by hitting these ransomware groups where it counts: their paychecks. The U.S. Treasury has started issuing sanctions, which are administered by the Office of Foreign Assets Control (OFAC). Sanctions are intended to stop businesses in the US from being able to trade or financially transact with a country or organization. These usually come in during arms deals or individuals attempting to send money to families overseas. Adding ransomware groups and organizations who accept their money has been the newest weapon in the government’s arsenal against these criminals.

The actions began in September 2021, when the U.S. Treasury OFAC Department sanctioned the Czech-registered and Russian-based cryptocurrency exchange “SUEX OTC, S.R.O.”[14] This exchange was one of the biggest avenues for ransomware groups, such as Ryuk, Conti, and Maze, to launder their stolen funds into legitimate currency. Since its launch in 2018, it has been estimated to have taken payments totaling $160 million, with $12 million from ransomware groups, $24 million from cryptocurrency scams, $24 million from mixers, $20 million from darknet marketplaces, and $82 million from high-risk exchanges.[15] This was the first major attack against ransomware operator’s and successfully disrupted a major link in their supply chain.

[11] https://therecord.media/king-of-fraud-sentenced-to-10-years-in-prison-for-role-in-methbot-3ve-botnet/
[12] https://www.cnn.com/2021/05/19/politics/colonial-pipeline-ransom/index.html
[13] https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/
[14] https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921
[15] https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021

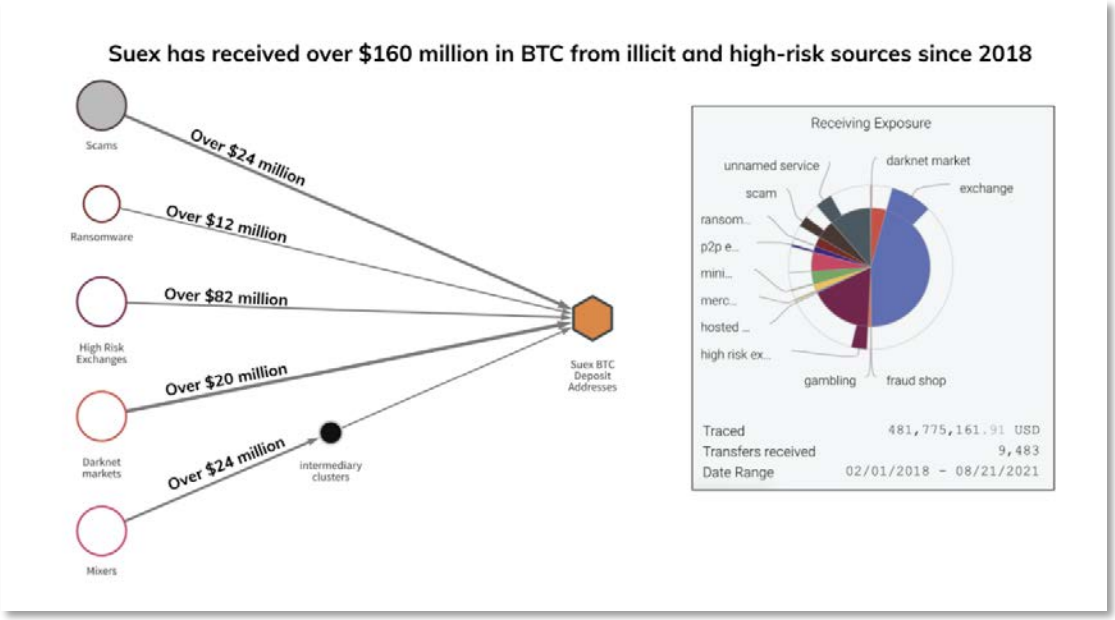


Figure 1: Suex payments from illicit and high-risk sources, from Chainalysis[15]

The next strike came in November 2021, when the US Treasury OFAC Department targeted a second cryptocurrency exchange, "Chatex". The treasury states that "analysis of Chatex's known transactions indicate that over half are directly traced to illicit or high-risk activities such as darknet markets, high-risk exchanges, and ransomware". Chatex has also been shown to have direct ties to Suex by "providing material support". As an extra measure, OFAC also added sanctions against three (3) other organizations that assisted Chatex, IZIBITS OU, Chatextech SIA, and Hightrade Finance Ltd.[16] In addition to these sanctions, OFAC have included several "specifically designated nationals" (SDNs) who are blocked from trade with US people. These designated individuals are threat actors linked to Sodinokibi/REvil, with one directly responsible for the attack against Kaseya.

The Biden administration has stated they will take stronger actions against the ransomware threat. The sanctions against ransomware groups and operators are a much-needed step in the right direction to keeping that promise. Breaking the money flow of a criminal organization is one of the most effective ways to dismantle it and these sanctions do exactly that. With additional measures such as monetary bounties for information on these groups, as the Department of State has recently released, potential ransomware operators may think twice before joining these criminal groups.

GOOGLE UNVEILS NEW FUZZ-TESTING TOOL

Fuzzing is the automated or manual process of finding vulnerable software bugs by randomly feeding data into a target program until a potentially exploitable bug or vulnerability in the infrastructure is found. Similar to how brute-forcing works, fuzzing is an essential tool in the toolkit of threat actors in the digital age where anyone can build a machine with enough resources to flood a victim application with junk data in order to find an exploitable bug. What began as a cheap technique has since grown into an important step in an actor's tactics, techniques, and procedures (TTPs), with fuzz testing usually being the first step in cracking a system. Due to services like Amazon giving threat actors the capability to easily spin up entire networks of computers that are dedicated to running fuzz-tests in parallel, fuzzing has not only grown in popularity but is now also easier for many actors to setup and collect data autonomously. To counter this, Google has

[16] https://home.treasury.gov/news/press-releases/jy0471

announced the release of “ClusterFuzzLite”, with the goal to integrate fuzz-testing into the software development workflow.

Fuzz-testing is not only essential for threat actors, but also software developers. By fuzzing software before the release, developers can more quickly and efficiently catch bugs that would slip through most manual checks and review. Fuzzing has also been added to the minimum standard requirements for code verification in the National Institute of Standards and Technology’s (NIST’s) guidelines for software verification since the White House Executive Order on Improving the Nations’ Cybersecurity (EO 14028)[17]. ClusterFuzzLite was announced by Google on November 11, 2021, as a continuous fuzz-test solution that runs as a part of development workflows (specifically the Continuous Integration workflows) to find vulnerabilities. ClusterFuzzlite is an easily integrated tool that can be integrated with a few short lines of code to catch bugs before they are committed to a code repository and enhancing the security of a software supply chain. The tool works with OSS-Fuzz program, another fuzzing tool by Google, that has caught over 6,500 vulnerabilities and 21,000 functional bugs since its release in 2016. By building ClusterFuzzLite with this tool, any project can easily integrate the new fuzzing standard into their workflow. The tool is easy to setup, works with closed source repositories, and offers useful features such as: continuous fuzzing, sanitizer support, corpus management, and coverage report generation. This would give software develops the chance to find bugs while in the development of the software and provide an immediate patch before the software is released into the public code base.[18]

[17] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or
[18] https://security.googleblog.com/2021/11/clusterfuzzlite-continuous-fuzzing-for.html

TRENDING IOCS

The following technical indicators of compromise (IOCs) are associated with monitored threat groups and/or campaigns of interest within the past thirty (30) days. IOCs can be utilized by organizations to detect security incidents more quickly and easily, as indicators may not have otherwise been flagged as suspicious or malicious.

Indicator	Type	Attribution
contact@contipauper[.]com	Email	Conti
sales@arrakisconsulting[.]com	Email	Conti
it_work_support@xmpp[.]jp	Email	Conti
185.141.63.120	IP	Conti
82.118.21.1	IP	Conti
162.244.80.235	IP	Conti
85.93.88.165	IP	Conti
5.149.252.179	IP	Conti
82.117.252.211	IP	Conti
296-docxonecloud[.]me	Email	Void Balaur
307-oneexeldocpdf[.]me	Email	Void Balaur
0310-peoplesound[.]club	Email	Void Balaur
801l4rg3bvvt22kcckt5[.]ru	Email	Void Balaur
877dwi3f1end9z4w3c81t[.]ru	Email	Void Balaur
033-mothernear[.]icu	Email	Void Balaur