Successful ransomware is organized crime

Introduction

Over the course of the last five months, the Ransomware as a Service (RaaS) group known as *Egregor* has risen to arguably the highest level of notoriety among other RaaS competitors.[i] Based on the group's dedicated leaking site, there are at least 200 victims posted due to not paying the extortion. The Kivu Threat Intelligence Team believed Egregor's success could only come about through coordinated structure, in other words, **organized crime**. We hypothesized that if the flow of cryptocurrency is analyzed based on the distribution of payments alongside forensic evidence of their malicious activity within a victim's network – we can better understand Egregor's success.

According to the UN Convention on Transnational Organized Crime (also known as the Palermo Convention) an "organized criminal" group shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established pursuant to this Convention, in order to obtain, directly, or indirectly, a financial or other material benefit; (b) "Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or more serious penalty; and (c) "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure. **We believe our analysis holds that Egregor is a structured group that can scale according to the size of the attack**, that the affiliates employed to scale are commonly used among different variants and **that the economics of using contracted affiliates and time spent within a victim's network directly affects the size of the extortion demands sought by the group**.

Egregor A Structured Group

We tracked seven ransomware attacks where Kivu facilitated payments and held forensic evidence[ii]; we determined an understanding of the suspected number of affiliates involved. By following the extorted money disbursed from the original paid wallet, we discovered pre-determined shares of profits among each order of the disbursements, alluding to a hierarchy of members and affiliates. By mapping the payments along the blockchain of wallets receiving their pre-determined share, we believe the Egregor group is owned and operated by no more than **10-12** core members. The core members direct their attacks at the disposal of no more than **20-25** semi-exclusively vetted members who are referred to as affiliates[iii].

Extortion Disbursements

Within the first two or three disbursements, Egregor owners will deposit between **8-10%** to wallets where the crypto remains unspent. Between the fourth and fifth disbursements, we see **2%** of the extortion sent to wallets and forwarded off to mule natured wallets where it is mixed with other inherited illegal (and legal) services. The sixth disbursement sits around **.2%**, where we believe this small amount is sent to the negotiators who communicate with ransomware victims coordinating and agreeing to an extortion. We believe negotiators exhibit the lowest barrier of entry and technical knowledge needed to support the overall mission of ransomware, thus the lowest share of profits. Finally, the remainder of the crypto appears to be distributed at roughly **70%** towards one to two different clustered affiliates who we suspect carried out the attack itself.

Where Does the Money Go Once in the Hands of Affiliates?

Kivu's Forensics team has examined affiliates will exhibit a variety of risk appetites within victim networks to mitigate detection. Therefore, we can assess affiliates will exhibit ranges of risk appetite when also mixing and laundering the extorted money in their own best perceived mechanisms. Those mechanisms include high-risk exchanges generally within Russia and adjacent countries, exchanges such as *Binance* in China, and darknet marketplaces such as *Hydra, UniCC, FEshop*, and the now-closed *Joker's Stash*.[iv] The strongest share of profits within darknet marketplaces is sent to *Hydra*, Russia's most prominent marketplace for illegal goods and services delivering in nearly every Russian city and province.[v]

Additionally, the Kivu team discovered corroboration between Egregor affiliates and the ransomware groups known as *DoppelPaymer* and *NetWalker*. We believe ransomware affiliates will operate between multiple RaaS groups where economic opportunity is present.[vi]

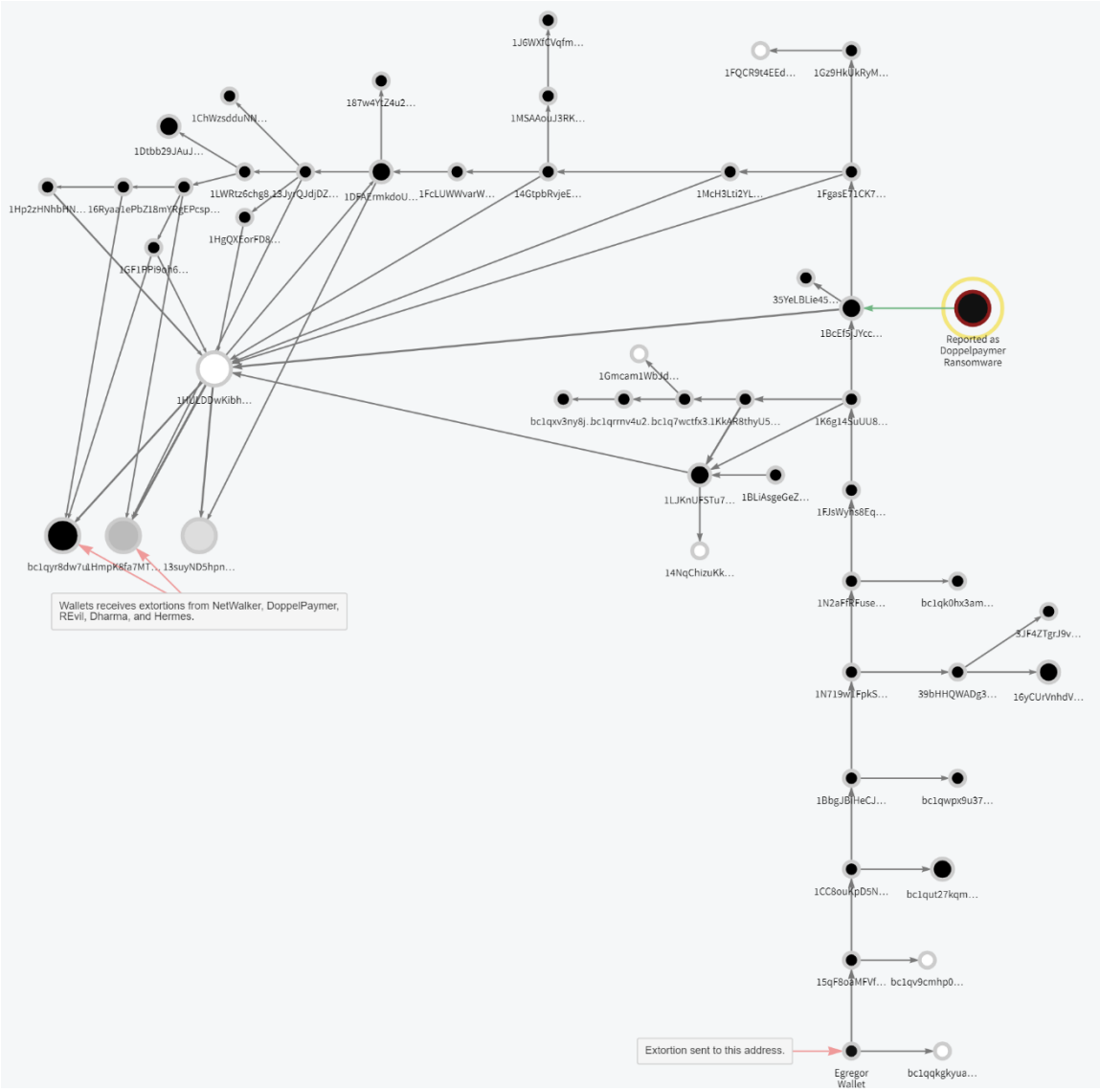
Kivu's Examined Ransomware Attacks:

The following are the seven ransomware attacks where an extortion payment was facilitated, alongside forensic evidence where available. Upon closer inspection, we can see the ransom demands increase based on *the number of suspected affiliates* and or *the time cyber criminals spend within the victim's network.*

Attack #	*Ransom Demand (USD)*	*Ransom Paid (USD)*	*Suspected # of Affiliates*	*Time Spent in Network (Days)*
1	*$15M*	*$2M*	*25-35*	*No forensic evidence.*
2	*$14M*	*$7M*	*25-35*	*No forensic evidence.*
3	*$10M*	*$2.4M*	*12-15*	*13.5*
4	*$7M*	*$3.5M*	*25-30*	*6.5*
5	*$1M*	*$500K*	*20-25*	*No forensic evidence.*
6	*$1M*	*$425K*	*20-30*	*1*
7	*$100K*	*$100K*	*10-13*	*3*

Examining Attack #2:

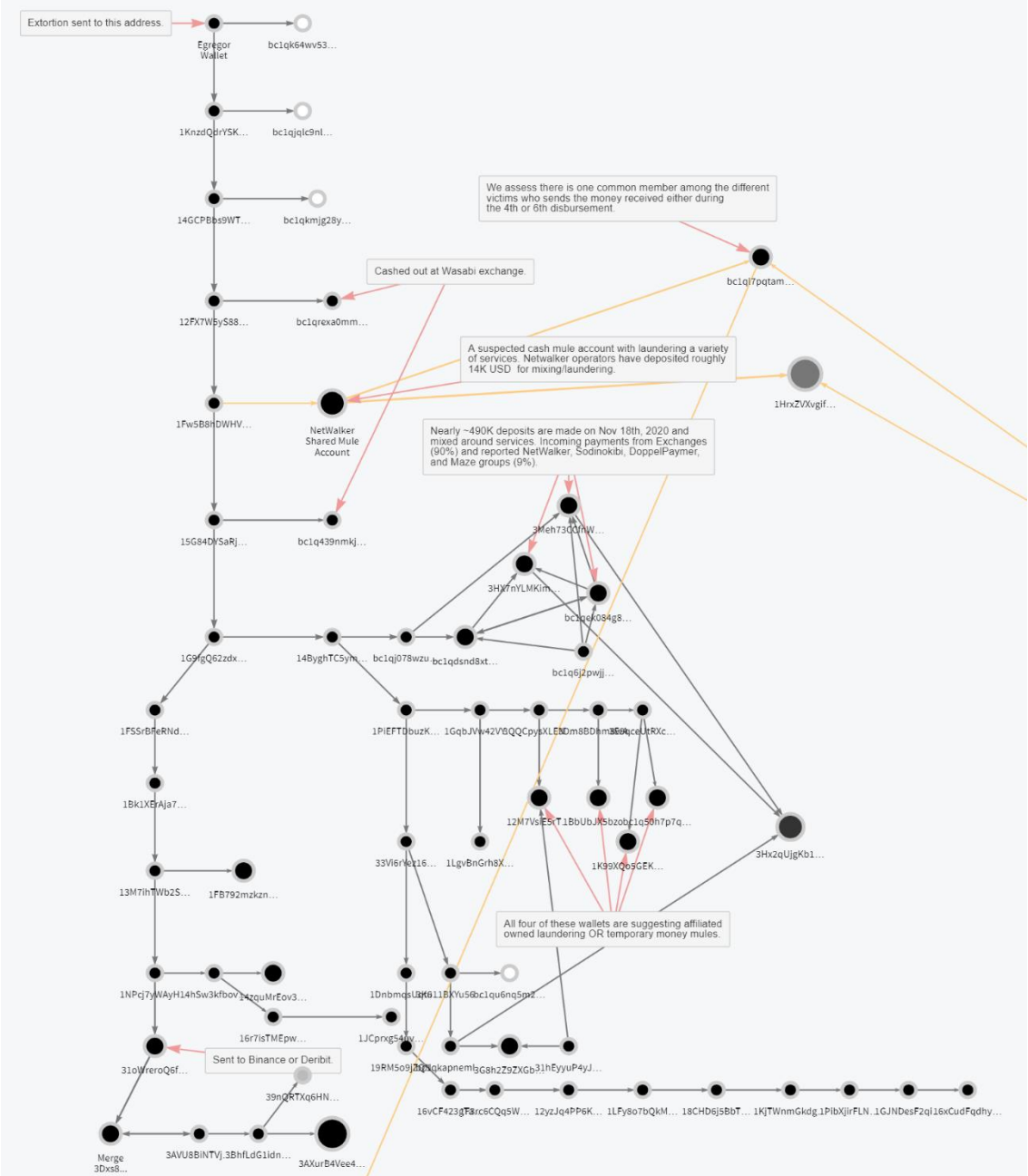
This victim's ransom price was set at a hefty **$14M** USD and settled for **$7M** USD as the victim had to quickly restore operations. Notably, roughly **220BTC** were deposited from a DoppelPaymer reported wallet within disbursements below. Towards the final stretch of disbursements, we notice majority of the affiliates send their money to wallets flagged for receiving extortions from *NetWalker* and *DoppelPaymer*, as well smaller amounts from the ransomware groups known as *Sodinokibi* (*REvil*), *Dharma*, and *Hermes*. Based on the number of wallets used for disbursements, we believe somewhere between **25-35** affiliates were involved throughout the timeline of this attack. Due the time-sensitive nature of the victim's need to restore and sanitize their critical devices for business continuity, our forensic evidence is limited and therefore assess this attribution within **low-medium** levels of confidence.



Attack #2: Ransom Demand: $14M. Ransom Paid: $7M. Number of members and affiliates involved: 25-35.

Examining Attack #4:

In this attack, we counted the highest number of affiliates involved.[vii] The victim organization faced a **$7M** extortion demand and settled for a payment of **$3.5M**. Our forensic evidence in this attack indicated the ransomware group took turns maintaining persistence over the course of **6.5 days**. We again see a shared wallet between NetWalker and Egregor at the fourth disbursement. Once the affiliates begin receiving their share of profits, the money is distributed 90% among exchanges and 9% within *NetWalker*, *DoppelPaymer*,

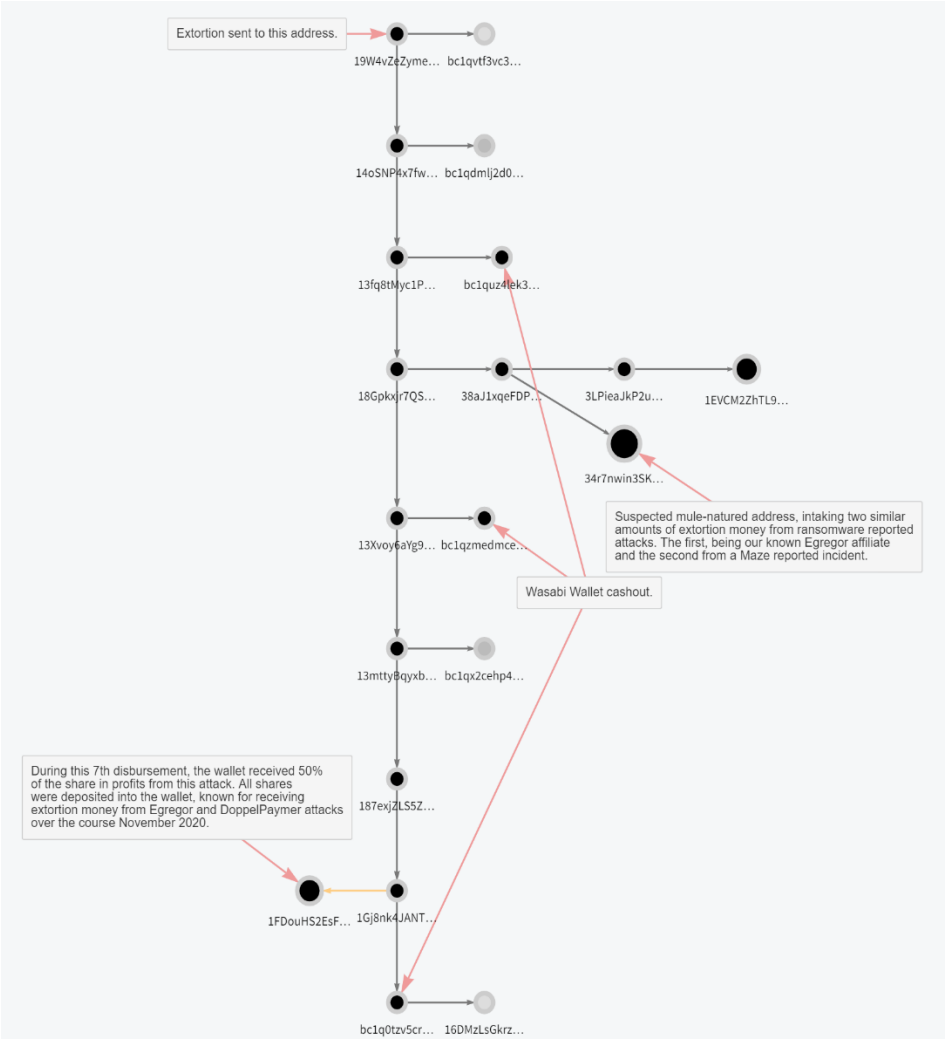


Attack #4: Ransom demand: $7M. Ransom Paid: $3.5M. Number of members and affiliates involved: 25-35.

Maze, and *Sodinokibi* (*REvil*) grouped wallets. Other affiliates instead choose to send their money among the usual Russian based high-risk exchanges. Between the first two instances and others not shown, we noticed one common member who disburses their own share of profits directly to the wallets of other known attacks we tracked. In other words, we believe at least 3 of our attacks we responded to involved one common affiliate with a distinct ranking. We assess their risk appetite may not be low, thus directly connecting multiple attacks with each other.

Examining Attack #7:

In Attack #7, we see the smallest number of affiliates involved and consequently, the smallest ransom demand as well. The victim organization faced a **$100K** extortion demand and settled for the original ask. Our forensic evidence here indicates the threat actors held persistence for roughly **3 days**. Here we believe the number of involved affiliates and members ranges between **10-13**. In this chain of disbursements, we were able to catch on to an affiliate sending money to a wallet previously flagged for receiving Maze extortions. For context, Egregor affiliates are widely believed to have joined following the cease of Maze's RaaS operations.[viii] During the second to last disbursement, we noticed one affiliate taking in half the share of profits and sending the money to a wallet hosting Egregor and DoppelPaymer money from incidents reported over the course of November 2020.



Attack #7: Ransom demand: $100K USD. Ransom Paid: $100K USD. Number of members and affiliates involved: 10-13.

Assessment:

Kivu's Threat Intelligence team assesses **Egregor's Ransomware as a Service group alludes to international violations of organized crime by scaling at a contractual level based on the size of the attack. The economics of using contracted affiliates and time spent within a victim's network directly affects the size of the extortion demands sought by the group**. While these variables are two driving vectors of rising extortion demands, an attackers' perception of the victim's ability to pay continues to exhibit significance.

Brief Recommendations:

The strength of an adversary to scale the resources to their malicious operations enables persistence at the disadvantage of the targeted organization. Therefore, Kivu strongly believes Ransomware as a Service' success is contingent on the targeted organization's overall level of security through **proactive defense** and **hunting** measures. When we understand our adversaries' economic models, we can disrupt their malicious activity by driving up their cost.

Threat Intel Reports

Kivu produces regular Threat Intel Reports using proprietary intelligence and publicly available information. Our aim is to provide easily digestible insight into cyber threat trends and threat actors' methods so that organizations can take actions to protect their networks and data.

About Kivu

Kivu is a leading global cyber security firm that offers a full suite of pre- and post-breach services, specializing in the forensic response to cyber-attacks and ransomware incidents. By combining analyst expertise, patented proprietary technology and exclusive threat intelligence, we deliver cutting edge cyber security solutions to organizations in need across the globe. Headquartered in the U.S. with offices worldwide, Kivu is a trusted cyber incident partner to insurance carriers and law firms.

kivuconsulting.com

[i] **FBI: Egregor Ransomware PIN, January 2021**

[ii] While Kivu responded to other cases involving the Egregor group, these seven incidents involved necessary payment facilitation to map the member and affiliate network.

[iii] **Carnegie Mellon University: Ransomware as a Service Threats, Definition**

[iv] **BleepingComputer: Stolen Credit Card Shop Joker's Stash Closes After Making a Fortune**

[v] **Bloomberg: Darknet Market Had a Record 2020, Led by Russian Bazaar Hydra**

[vi] **Chainalysis: Ransomware Connections Maze, Egregor, SunCrypt, DoppelPaymer**

[vii] Due to the seemingly more complicated nature of disbursements, Kivu's Threat Intelligence team does not rule out the possibility there may be attempts at obfuscating the disbursement of payments.

[viii] **MalwareBytes: Threat Profile Egregor Ransomware is Making a Name for Itself**

Contact Us

For more information on how Kivu can help protect organizations from cyber attacks and help manage cyber incidents, email us at **info@kivuconsulting.com**