Ransomware Enforcement Operations in 2020 and 2021

March 31, 2022 • Julian Vogele

Insikt Group

Introduction

During the last 2 years, ransomware has been dominating cybersecurity headlines around the world. It is no longer only being discussed within the security community but is recognized as a systemic threat across most industries and geographies. Terms like RaaS (ransowmware-as-a-service) and REvil have even entered the mainstream news.

Historically, both technical and non-technical reporting has primarily focused on actual ransomware attacks. Gathering knowledge about victims, ransomware groups, their affiliations and extortion strategies, TTPs, and IOCs helps to protect against them through prevention and detection. However, discussed less frequently and less systematically are law enforcement actions taken against ransomware operators and their co-conspirators, which have become an important pillar to combat the threat.

This report looks at international law enforcement operations and is based on data collected over the last 2 years. We first address common difficulties faced by law enforcement, then outline trends and observations by distinguishing between different types of law enforcement activities, and finally provide a timeline of all events. Through this report, we aim to create an overview of the status quo and to better understand the effectiveness of law enforcement in the medium term.

Common Difficulties Faced by Law Enforcement

Of late, ransomware groups have become more professionally organized and technologically sophisticated. This growing sophistication, alongside persistent weaknesses in the systems of targets such as default credentials and exposed RDP access, has led to a massive increase in ransomware attacks. Where defense systems fail, law enforcement is required to respond. But those seeking to take down ransomware groups face many challenges.

Lack of Reporting

In the UK, it has been estimated that only 1.7% of all fraud and cyber crime incidents were reported between September 2019 and September 2020. While the reporting rate for ransomware attacks may be higher than that, given that it is harder to cover them up, ransomware attacks remain an underreported crime according to Europol's IOCTA report. This lack of reporting is often a result of the victim organization's primary focus on business continuity and limiting reputational and financial damage. Several law enforcement agencies across Europe say they have only heard of ransomware cases via reports in local media. Without reliable and valid data on the number and types of cyber attacks (that is, attack vectors), it is difficult for law enforcement agencies to accurately evaluate threats and react appropriately, resulting in threats not being given the resources or priority they deserve. In turn, by investigating every attack possible, law enforcement can gain a better picture of the ransomware landscape and assist in providing free tools.

Lack of Skills, Technology, and Data

Law enforcement response to ransomware attacks requires advanced skills (such as reverse engineering, threat hunting), technology (such as cryptocurrency tracing tools), and data resources (such as threat intelligence). These 3 conditions are not always available, making it difficult for less-equipped agencies. Even well-resourced agencies in countries like the US struggle to acquire all of the tools necessary to counter ransomware actors. This becomes most apparent in the public sector's historical lack of ability to recruit, train, and retain talent when competing with the private sector. However, with public funding in cybersecurity increasing as shown by UK's National Cyber Strategy, EU's Cybersecurity Strategy, or the US Infrastructure Investment and Jobs Act, the public sector will be significantly strengthened to better defy ransomware groups.

International Nature of Cybercrime

Cybercrime operates independently of national boundaries. Ransomware gangs work with affiliates from across the globe. To successfully fight ransomware, international collaboration is indispensable. While international organizations such as INTERPOL or EUROPOL have set good examples and are essential for combating ransomware, there is still room for improvement in defining intelligence-sharing processes or legal frameworks. Legal hurdles are particularly difficult when diplomatic relations between countries are strained or non-existent and there is no reciprocity or systems established to extradite and charge threat actors. For example, US requests for Russian help extraditing ransomware groups have produced no results for a long time,

even after a Russian-US summit in June 2021. After Russia's invasion of Ukraine in February 2022 and resulting geopolitical changes, it remains to be seen how Russia's role will evolve.

Law Enforcement Operations Against Ransomware

To get a better overview of law enforcement operations against ransomware and better assess their effectiveness in the medium term, we collected data on publicly known law enforcement events in 2020 and 2021. After enriching the data with other publicly available information (such as which authorities were involved in the event), we categorized them into operations against (1) ransomware operators (including arrests, but also freezing of funds), (2) malware facilitators (such as for initial access), and (3) money laundering operations using cryptocurrency exchanges. The following sections examine important trends and observations based on this data.

Volume of Law Enforcement Operations has Increased

While 2021 was globally seen as the year of ransomware attacks, it was also the year of law enforcement operations against ransomware. According to public reporting, there were 38 law enforcement operations in 2021, compared to only 4 in 2020. The vast majority of the law enforcement operations in 2021 (31 out of 38) were against ransomware operators. 4 operations were against malware facilitators and 3 operations were against cryptocurrency exchanges (SUEX, General, and Chatex) that facilitated money laundering operations.

Figure 1: The number of law enforcement operations against malware facilitators, cryptocurrency exchanges related to ransomware operations, and ransomware operators, January 2020 to December 2021 (Source: Recorded Future)

This massive increase shows how the systemic risk ransomware poses to economies and societies has finally made it onto the agenda of law enforcement. The lower level of law enforcement operations in 2020 is at least partially explained by less reporting of ransomware attacks. Additionally, the real and potential harms of ransomware are probably yet to be felt, with devastating events such as the Colonial Pipeline ransomware attack increasing the pressure for governments to act.

In parallel to the significant increase in volume of law enforcement operations, the operations have also become more diverse in terms of targets and means used. Targets range from ransomware groups themselves over malware facilitators to other supporting infrastructure such as specific cryptocurrency exchanges used for money laundering or facilitating transactions involving illicit proceeds. Other future targets might include insiders or initial access brokers. Means include "hack backs", arrests, or account or seizure of illicit proceeds, among others.

Many Ransomware Groups Are Targeted

Law enforcement has been targeting many ransomware groups and co-conspirators over the last 2 years, with some of them being targeted significantly more often than others (see Figure 2). Whether ransomware groups and their facilitators are targeted by law enforcement likely depends on factors such as the availability of relevant intelligence, reachability of operators, security operations of operators, total expected benefit through successful law enforcement operations, and the priority given to a group.

Figure 2: Number of law enforcement operations against specific ransomware groups, malware facilitator, or cryptocurrency exchange, January 2020 to December 2021 (Source: Recorded Future)

For example, REvil, responsible for 288 attacks in 2020 and 2021 based on our data, was targeted at least 5 times by law enforcement. Law enforcement operations against REvil began mid-2021, after the group attacked JBS, and later Kaseya VSA. Both attacks were considered to be particularly severe and posed a risk to the US national stability, moving the group up on law enforcement's priority list. Such operations included arrests of suspects in the US, Poland, and Romania as well as a "hack back" orchestrated by multiple countries pushing REvil offline.

Similar things can be said about NetWalker, which was specifically targeting the healthcare sector during the COVID-19 pandemic, taking advantage of the global crisis to extort victims. In total, NetWalker is responsible for at least 144 attacks in 2020 and 2021 based on data. Publicly known law enforcement operations against NetWalker took place in January 2021 and resulted in the arrest of a Canadian citizen as well as the seizure of dark web sites associated with NetWalker and cryptocurrency from ransom payments.

International Collaboration Is Key

Given the international nature of the ransomware ecosystem, international collaboration has been key. Based on our data, almost 50% of all law enforcement operations in 2020 and 2021 were the result of international law enforcement collaboration. The most prominent collaborations are FVEY, Europol JCAT, and Europol EC3. For the remaining operations, it was not possible to determine whether they were based on international collaboration or not.

Collaboration has not only been important between public sector agencies across countries (public-public), but also between public sector agencies and private sector companies. One example is the No More Ransom website, which is an initiative by the Dutch police, Europol, Kaspersky and McAfee with the goal of helping victims of ransomware retrieve their encrypted data without having to pay the criminals.

Dominant Role of the US

Recorded Future has found that US organizations have been the most targeted by ransomware attacks, accounting for roughly 50% of all tracked attacks. US organizations also suffer the most economic damage from ransomware attacks. As a result, US authorities are also the most active in law enforcement operations countering ransomware threat actors. In at least 65% of all law enforcement operations against ransomware groups or co-conspirators included in our data, US authorities such as the Federal Bureau of Investigation (FBI) or the US Cyber Command were involved. The active role of the US is also reflected outside of law enforcement such as the Stop Ransomware initiative, a one-stop hub for ransomware resources started by the US Department of Justice (DOJ) and the US Department of Homeland Security (DHS), together with federal partners.

Outlook

While prevention through appropriate security measures is the best cure against ransomware attacks, a system is only as strong as its weakest point. The recent Log4Shell vulnerability has just shown how quickly software can turn into a severe risk. Therefore, despite improvements in security systems, it is more than likely that ransomware attacks will continue to succeed in the years ahead, requiring law enforcement to respond.

While it is too early to provide a definitive answer as to whether law enforcement operations against ransomware groups have been effective so far, there is some indication that the combination of different types of law enforcement operations carried out by international alliances may effectively reduce the number of attacks. For this reason, it is likely that international law enforcement collaboration will strengthen further (for example, between the US and Japan) and diversify (for example, the FBI shifting focus to alternative means such as seizures, formation of the Virtual Asset Exploitation Team (VAXU) as announced during Munich Cyber Security Conference 2022).

Future analyses will provide more definitive evidence, and a better, more systematic analysis of law enforcement is needed. This report provides one such example in discussing the increase in volume of law enforcement operations and distinguishing between different types of law enforcement activities based on data from the last two years. It also shows how law enforcement operations have become more diverse in terms of targets and means. In addition, we highlight the importance of international collaboration and the dominant role of US law enforcement. Regarding the latter, with ransomware groups attacking more and more organizations outside of the US, more law enforcement operations and initiatives by other countries are likely to occur.