Inside REvil Extortionist “Machine”: Predictive Insights

advanced-intel.com/post/inside-revil-extortionist-machine-predictive-insights

AdvIntel July 15, 2020

- Jul 15, 2020
-
- 14 min read

Takeaways

- Cybercrime groups often operate on traditional crime group behavioral patterns.

- REvil main collective group patterns are: seeking for attention, aggression motivated by impunity, overconfidence, and rigid group identity
- REvil behavioral patterns have likely directly triggered and impacted their recent attacks against high-profile entities
- REvil operations against famous and politically engaged public entities and personalities will likely become their syndicate's main focus

Introduction

The REvil Group is one of the most prominent Russian-speaking ransomware groups in the cyber domain. In May, it made headlines for extorting numerous high-profile clients of the New York City-based entertainment and media law firm Grubman Shire Meiselas and Sacks, as well as the California-based IP law firm Vierra Magen Marcus. The threats had impactful political implications as these firms represent high profile clients, such as President Donald Trump and the United States Navy, respectively. After attempting to threaten President Donald Trump with a $42 million USD extortion, the group was even branded as a terrorist organization.

Naturally, the attacks and the subsequent political response has changed REvil's place in the cybercrime ecosystem. On one hand, the group is now more well-known than it has ever been. On the other hand, the Russian-speaking cybercrime community - a foundation is demonstrating explicit resentment to the syndicate's actions. This resentment could lead REvil to lose its foundation within the community - a foundation that is existentially important to an organized cybercrime group.

Recent events can shed light on essential aspects underlying REvil's operations - their collective identities and psychological patterns that define them as a criminal enterprise. The way that REvil communicates, operates and builds relationships is determined by the psychological and organizational motives of its members, their perception of hierarchy, self-identification, and their relationship with the community.

We have investigated REvil's discourse and behavior by applying the methodologies and concepts of criminal psychology to identify the group's unique characteristics revealed by their recent involvement in large, ethically questionable (attacks against medical institutions),

and politically impactful extortions. By applying these methodologies, we attempt to achieve a deeper understanding of the group's actions in order to successfully predict and prevent its operations.

The Breach of Trust: Extorting the Extortionist

On April 15, 2020, on the XSS forum, which serves as one of the main grounds for community relationships across the Russian speaking underground, an actor "Vivalamuerte" claimed that they have information on UNKN, the leader of the REvil group. This event, most likely preceded by a month of private negotiations, was the first major conflict between REvil and members of the Russian-specking community - a major breach of trusted relationships.

Vivalamuerte threatened to reveal information about UNKN identity unless paid $190,000 USD. "Vivalamuerte" claims this is the amount that REvil's leader owes them as this sum was invested in UNKN's original cryptolocker creation efforts in 2016. To make matters worse for UNKN and their team, prior to this extortion, UNKN has lost over 150,000 USD in a transaction operated by the Exploit forum administrators - another significant trust breach.

Two weeks later, on April 27, 2020, an Exploit forum user EXPL0 asked in broken Russian if there was room in the REvil Group ransomware program. REvil denied the request due to EXPL0's non-Russian background. However, a couple of weeks later on May 13, 2020, UNKN shared that there had been a breach and disclosure of authentication data and blamed it on EXPL0 who was integrated into the syndicate by one of UNKN's Russian speaking affiliates.

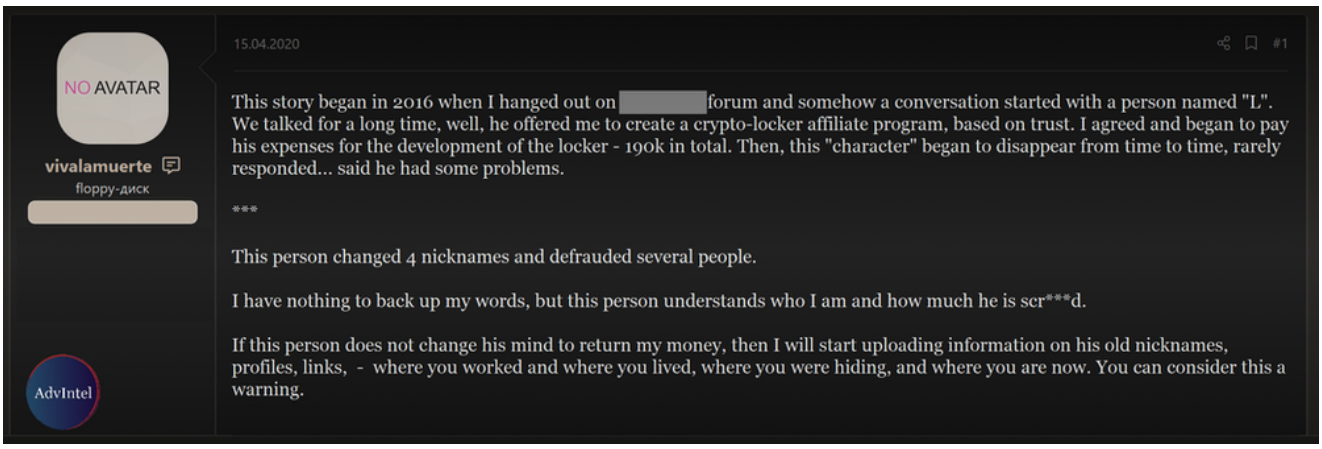


Image 1: “Vivalamuerte” has not only treated REvil leader and their family but questioned the group’s position in the hierarchy by openly challenging their reputation

This deterioration of relationships between REvil and the cyber community correlated with the group’s attack becoming more aggressive, outrageous, and unethical. For instance, on March 13, 2020, - when the private negotiations with “Vivalamuerte” extortionists were likely taking place, REvil hacked a biotechnology company, 10x Genomics, despite the COVID-19 pandemics and possible healthcare ramifications from the attack. On May 14, 2020, REvil hacked entertainment and media law firm Grubman Shire Meiselas and Sacks in order to extort high profile clients, such as Madonna, Bruce Springsteen, and Donald Trump. Then, on May 29, REvil continued the pattern of targeting high-profile law firms, hacking IP law firm Vierra Magen Marcus.

It is likely that these events are connected. The team threatened by the “Vivalamuerte” attack on their anonymity aggravated by the EXPL0 case and was taking actions defined by a threat-driven mindset. REvil may have resorted to extorting top-tier companies and individuals in order to obtain a higher payload and ensure that Vivalamuerte does not expose UNKN. The group may have been uniquely motivated to pursue highly visible targets in the hopes of obtaining higher payouts. But the connection between this extortion and REvil recent aggressive behavior is likely even deeper - defined by collective and individual psychology - specifically matters of overconfidence, feelings of impunity, and identity formation.

Attention, Impunity, Confidence

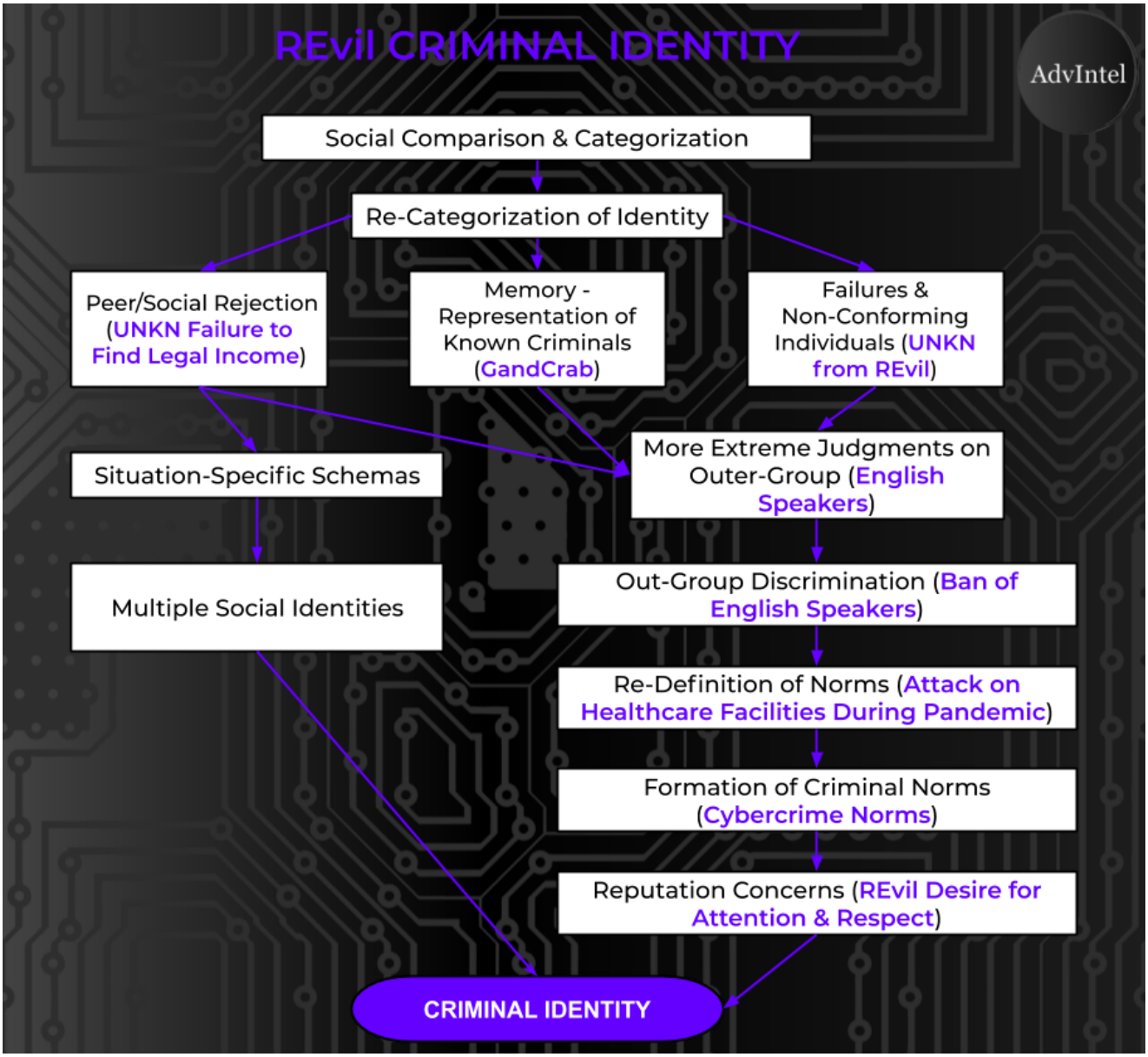


Image 2: REvil's criminal behavior patterns

REvil posts on forums are provocative, extravagant, and flamboyant. This may suggest this team is not only seeking financial profits, but also attention. This may be a style of doing business and a psychological phenomenon.

According to Vivalamuerte, UNKN has changed its nickname on the forum four times and works very hard to avoid detection. As a young man from Minsk with a troubled background, they most likely entered the cybercrime enterprise because of being financially troubled without any other financial options to turn to. If Vivalamuerte's allegations are true it is

rewarding for UNKN to be able to attract worldwide attention and be recognized in a criminal business enterprise. They most likely did not have a supportive family and can now receive recognition and notoriety for their chaotic behaviors.

This motivation is not solely egotistical and emotional. On the operational level, the fact that REvil receives a large amount of media attention from international headlines describing their renowned tools and techniques helps the group to establish a dominating place within the community. As a Ransomware-as-a-Service, group REvil uses its fame to its advantage in order to attract and recruit talented affiliates. When recruiting affiliates, they use fame as a tool of self-legitimization. The group spokesman stated: *"You can read about us in the media. An envelope with 6 zeros is an ordinary and daily business for us."*

Another essential factor shaping REvil's motivations and behavior is a feeling of impunity. While seeking profits and attention the group made the headlines, yet faced little to no punishment. The group has been caught, moreover, their predecessor, a ransomware syndicate - GandCrab, publicly bragged that they are living proof that one can steal without getting caught. Considering that UNKN may have joined cybercrime as a last resort to become rich and famous (According to Vivalamuerte) and considering the connection between the two groups REvil may be looking at GandCrab as a role model, and as an example of a successful ransomware collective *that made billions and resigned unpunished*.

The overt impunity also has an operational benefit, as just as publicity, it helps to bring talents to the group - a fundamental requirement for a successful RaaS enterprise. It is probable that REvil is aware that by receiving recognition for pulling off intelligent operations without getting caught they can recruit more capable members into their syndicate.

As such, REvil is not held accountable for its actions, receives widespread international attention for their cunning and malicious activities and feels good about their technological prowess. All of these processes feed into building up the organization's ego and convince them that due to their anonymity and skill, they will not be held accountable for their actions in the future.

The combination of attention-seeking and impunity leads to REvil's overconfidence. This can be seen in the way REvil challenged the community's ethics and principles, the arrogance and contempt with which the REvil representatives talk to other hackers and ransomware

developers, and, finally, the way the group traits their victims. This overconfidence may be the reason why the group is so hard to negotiate and so aggressive in their ways. But the same overconfidence became the group's major vulnerability.

Collective Identities

However, before we review how psychological patterns of UNKN and other leaders determined their recent behavior, one other aspect would be investigated - the group identity.

REvil is first and foremost an organized crime collective and its group identity presents a unique case across the organized crime. A recent solid trend in cybercrime psychology is for previously ethnically homogenous crime groups that did not accept others have to begin to accept individuals from different backgrounds, so they may contribute highly desirable scarce resources and skills.

In 2019, groups started to operate across domains and cultural lines as long as the payload could be ensured to be secured. The trend is especially visible with cybercrime. In contrast to traditional organized crime that requires deep trust with strong ties and familiar connections, cybercrime necessitates the formation of flexible networks and partnerships, forming a thin trust.

For instance, across Eastern European cybercrime, Russian-speakers may prefer to work with other Russian-speakers due to increased feelings of belongingness, preferences for ethnic behaviors and practices, shared cultural traditions, history, and values. But they will still establish multicultural and multiracial syndicates. An illustrative example was the FXMSP group which bragged about having American and Chinese team members.

However, REvil is an exception. The group clearly says that it will never work with non-Russian speakers. REvil's perceptions of, and attitudes toward, English-speakers members ultimately develop from their need to identify with and belong to their own group that they perceive to be superior, as a means of enhancing their level of self-esteem. REvil perceives its group members and other trustworthy Russian-speaking actors to be similar to themselves and shows preference in their attitudes and behaviors toward them.

Image 3: REvil decided to reshape their RaaS policies based on tightening identity-based selection

However, English-speakers are perceived to be dissimilar and possess less favorable qualities, and therefore they can justifiably be discriminated against. Though English-speakers are lauded on the forums for making deals more secure by asking for as many proofs as possible during deals, some stigmatize them for being difficult to make deals with.

This ethnic-based mentality and ethnic foundation for boundary formation had also misled the group leaders. Just as overconfidence and impunity, this extreme psychological pattern created new vulnerabilities for the group. As it often happens with collectives driven by distrust to the “Collective Other”, REvil had hindered their critical thinking and began blaming systemic vulnerabilities of their model on precedes against non-Russian speakers.

Confidence, Community, Consequences

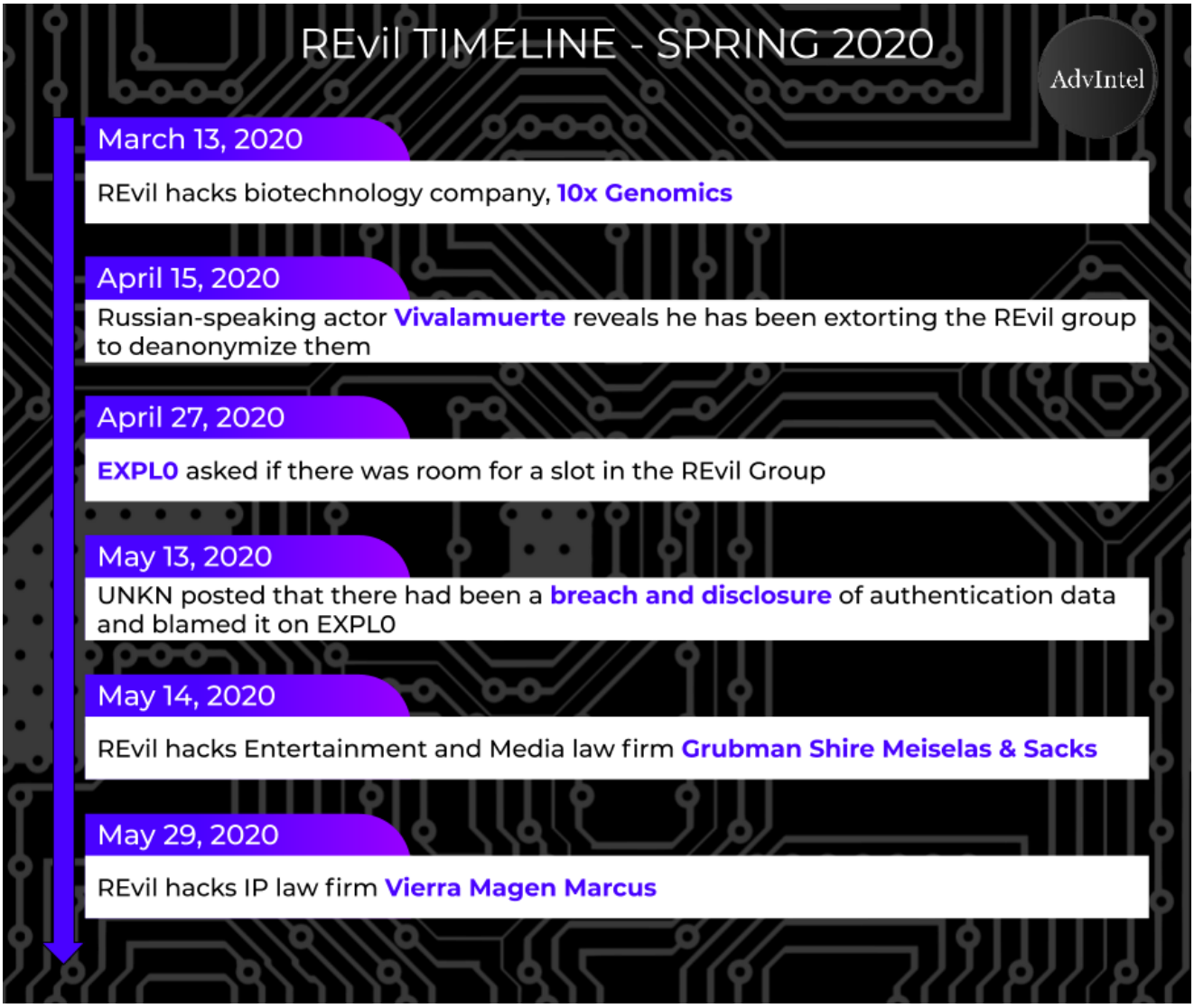


Image 4: REvil's latest activities were preceded by several important conflicts between the group and the members of the cybercrime community

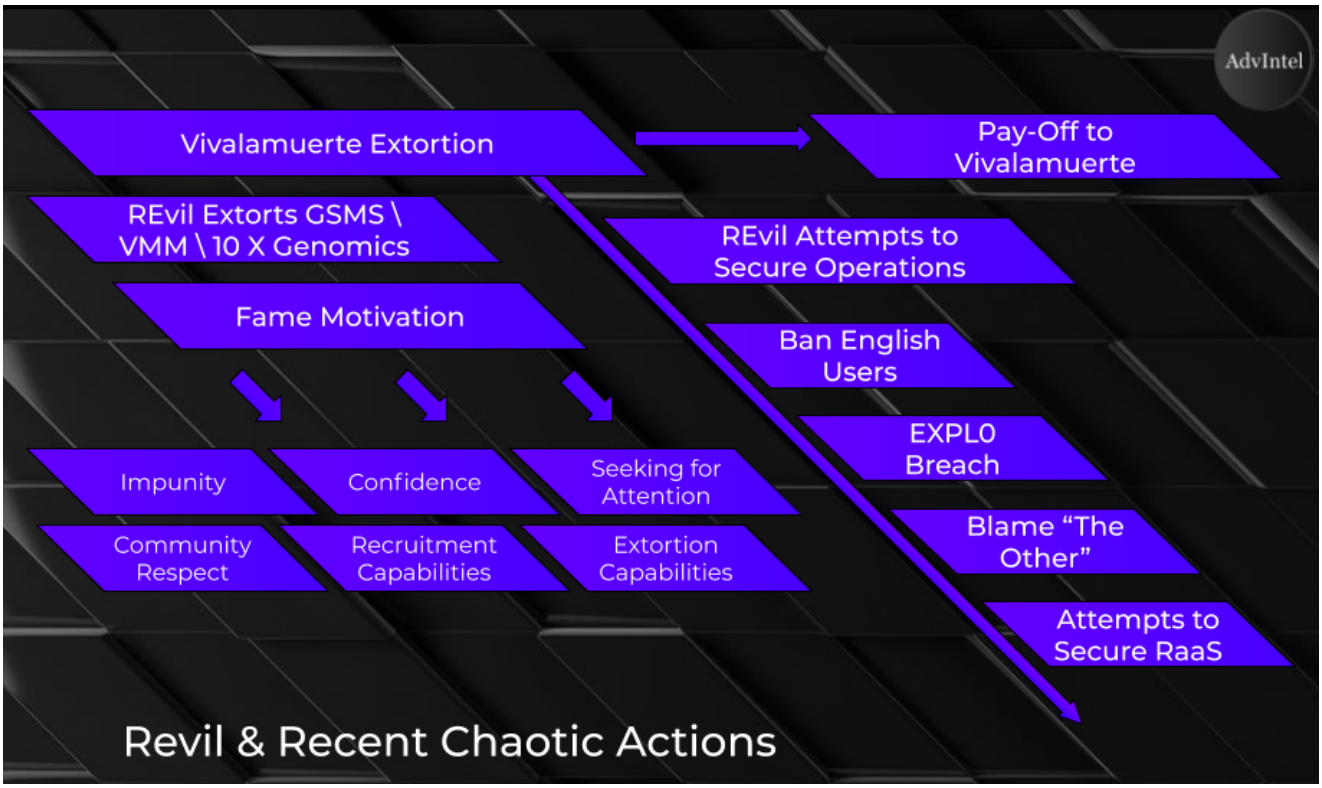
An Eastern European ransomware collective is first and foremost a community body. As a decentralized structure, RaaS relies heavily on its talent recruitment. RaaS presumes the necessity to keep a good relationship with the community. Recruitment of new affiliates, cooperation with individual experts on intrusion, the infrastructure of publishing websites for blackmailing - all this requires a solid foundation in the cybercrime community. Maintaining a consistent reputational profile is, therefore, a necessity. When REvil members that bragged about their success and power got themselves attacked, their entire foundation became vulnerable.

The extravagant public profile turned REvil into a lucrative goal for other criminals. “Vivalamuerte” clearly understood that reputation is as important for UNKN as their technical skills. The extortion of REvil had a direct and traumatic impact on the group’s self-identification. REvil relies on the acquisition of loyal, talented affiliates. They must keep a reputable name in the forums in order to attract the right types of partners.

A threat of deanonymization simultaneously hit the three aspects of REvil’s collective psychology mentioned above - attention-seeking, impunity, and overconfidence. With their identity exposed, UNKN would find the attention they brought to themselves in a recent year working against them. There would be no impunity without anonymity, and, of course, the image of an overconfident gang leader would be destroyed if the information of their personality is available for everyone.

UNKN and their team had to rapidly find a response to this triple threat aimed at the very center of their collective psyche. As a result, they initiated a range of operations all aimed to bring back their reputational standing but resulting in even further complications of their case.

A Spiral of Chaos



By Spring 2020, one of the largest and most formidable ransomware syndicates was in a very pecunious condition. First, they face a deanonymization threat. Their attempt to call for even more media attention now backfired and compromised the group's impunity. Then, a Russian-Speaking member of the syndicate accepts EXPL0 who ends up compromising the group's domains. Apparently - the identity-based model of partnerships proves itself inefficient.

From a criminal psychology standpoint, REvil may have been willing to take overly confident actions if they were really being extorted by Vivalamuerte and desired to protect their anonymity at all costs. In order to extract a large payout, they were willing to act in more chaotic ways, bluffing to have information on the U.S. President in order to extort a large financial sum for information regarding Trump.

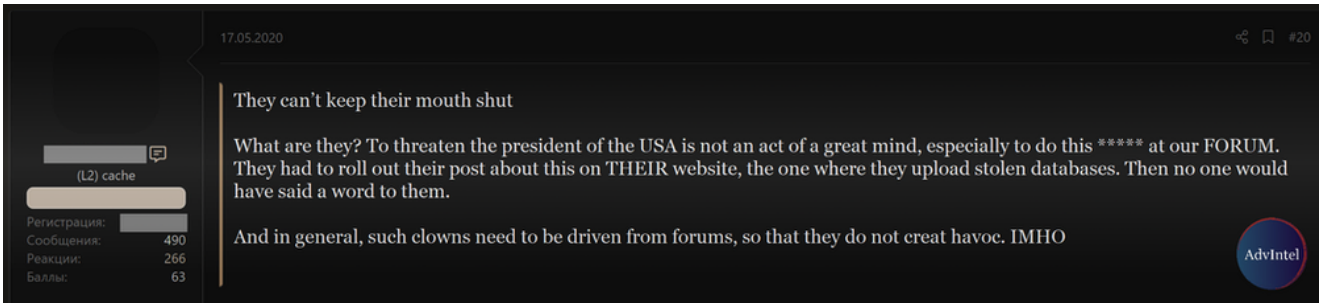


Image 5: An emphasis on publicity practiced by the group created an opposite reaction in the cyber underground itself

A high-profile attack reaching headlines beyond regional media and social networks is a perfect solution. REvil goes high and attempts to blackmail the U.S. President. Even though this sounds like a movie plot, the plan works, but the consequences are imminent.

At this point REvil's goals are simple - to restore the image of overconfident top-dog, trusted and respected by the community - the main source of power that a RaaS syndicate has.

Indeed, REvil reached the global headlines, but the attack backfired. The group was being branded as a terrorist organization by the Trump Administration which, among other things, made ransom payment impossible. Previously fame and notoriety helped REvil to gain

profits. Their desire for attention and enrichment was working for hand by hand. But now, the two motives were contradicting one another.

The blunder was easy to avoid as the consequences of an attack against President Trump were quite predictable. The United States has branded smaller, less threatening (from a standpoint of the US national security) groups, with much less of an impact as terrorists. A couple of weeks before REvil's extortion attempt, the Russian Imperialist Movement, a minor white supremacy group already collapsing from the crackdown from Russian security forces, was branded as a foreign terrorist organization by the US. The Russian-speaking media extensively covered the event, accusing the US of overreaching. However, REvil ignored these signs and targeted one of the most influential people in the world attempting to extort the United States President for $42 million USD without proof of actually possessing information about him.

While not being paid, UNKN and its team attempted to utilize at least one aspect of the notorious extortion - popularity, and attention. They posted information regarding the Grubman Shire Meiselas & Sacks on the underground forums.

However, again, the attempt led to the opposite effect. Instead of getting more respect and support, REvil faced a backlash. Due to the nature of forum users' activities, many wish to keep a low profile and are uncomfortable with the amount of negative attention that REvil draws to the forums by targeting Trump. In this sense, REvil's overall desire for attention worked against them, since the community prefers silence.

An already damaged image of an omnipotent cyber syndicate, which was suddenly itself blackmailed, received a second blow, as the community started to mock REvil and openly ironize about their audacious threats. Moreover, REvil was called out for bluffing to have information about Trump. As a result, the posts were quickly deleted from forums, but the attempts to restore reputation continued as the group quickly shifted to announcing they would be auctioning off celebrity client data obtained from GSMS, beginning with Madonna.

Exaggerating is not wise for building trust and legitimacy in this enterprise because those buying the information will only purchase it if REvil's track record is legitimate. Moreover, REvil could have predicted the reaction of the community. By the way, the community

reacted to REvils bragging about attacks against medical corporations in the midst of the COVID-19 Pandemic.

On March 13, 2020, REvil stole one terabyte of data from 10x Genomics, a California-based biotechnological company, researching drugs to treat COVID-19. Following this ransomware attack, the REvil group published 10X Genomics company documents containing sensitive information about more than 1,200 employees. Some users on XSS did not agree with REvil's actions, declaring that biotechnology companies should be permitted to focus on cure research so that everyone may be in good health. One user said "this act was like spitting in the well from which one drinks. The faster humanity overcomes this infection, the faster the economy will recover which will lead to bigger earnings for us."

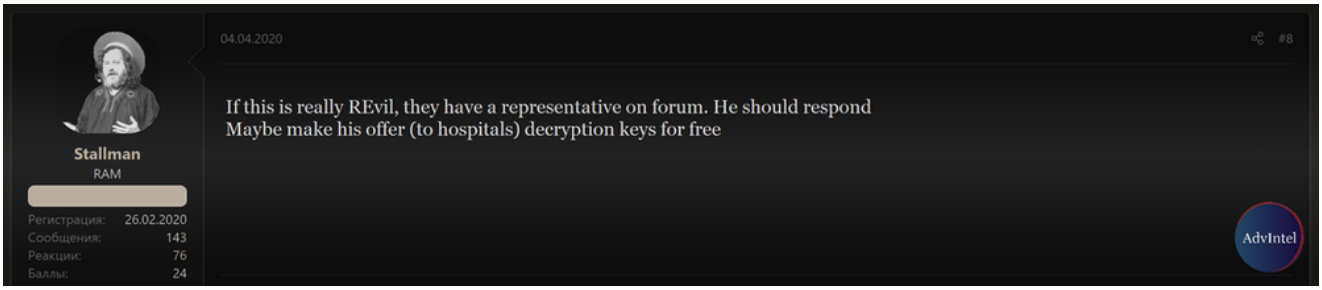


Image 6: For some older members of the Russian speaking underground, the hacker ethics is an important rule affecting their code of conduct

At the same time, REvil in response to the EXPL0 case were reshifting its business model, by reducing the number of affiliates and calling to ban English language users. Following the EXPL0 breach in May, REvil removed all English adverts dealing with English speakers and required a guaranteed advert for admission into their program. However, the EXPLO0 case occurred not because of EXPL0's identity, but because the RaaS model is itself vulnerable to such breaches. REvil does not highlight that the RaaS system itself is at fault and opts to scapegoat English-speaking users for the downfalls instead - another sign of irrational and chaotic behavior.

However, these braggings and exaggerations, chaotic behavior can be explained if we take the psychological and social components. It is critical for the crime syndicates to be respected and supported, as they are consistently forming new partnerships on the forums. Moreover, REvil leveraged fear through publicity by targeting A-listers. Standard personal information is valuable but sensitive celebrity information is even more valuable. These deeply impactful crimes get into the minds of their victims because celebrities and

companies alike know that if they do not pay that someone else will in an auction. REvil worked its way to the top of the hierarchy by weaponizing their superior tactics, techniques, and technology on the most public of figures.

This breach of trust by the community - the threat of losing anonymity triggered REvil to think with more of a threat mindset which is essentially different from strategic management in which the group operated previously. REvil was more motivated to commit a high-profile attack to restore the group's reputation after the Vivalamuerte extortion, to keep recruiting talented members, and to increase the likelihood of a payout because other celebrities and companies will be scared of the group since they are so popular and never caught. However - high-profile attacks exacerbated the relationships with the community. As was the case with the EXPL0 case breach, the clash between organizational and identity approaches leads to poor mitigation.

By making each new attempt to improve their case, REvil only exacerbated the conflicts and contradictions which led to their troubles in the first place.

What Can We Learn?

Socio-cultural forces play an important role in the genesis and sustainability of organized cybercrime groups. Identity comprises motivators that direct criminal activities such as emotions, beliefs, and attitudes. REvil achieves a sense of self-consistency by manifesting their identity with their criminal behaviors, such as victimizing high-level targets, accumulating technological prowess, and not allowing English speakers to work with them. Collaborative ties require trust and mitigation of uncertainties as trust is a mechanism for people to cope with risk and uncertainty in interactions with others.

In cybercriminal computer-mediated communications trust is more than just a mental aspect. When REvil cooperates with someone on a forum, there is always a possibility that person is either a fellow cybercriminal, a dishonest trader, a researcher, or a law enforcement associate. Uncertainty is treated as a cost to the enterprise as a breach of trust can severely impair their sophisticated business model. Bonding capital in crime is usually manifested through strong interpersonal relationships with close friends or family. The next best thing to develop trust is to possess the same ethnicity and values. In cybercrime, lacking non-verbal and social context cues, trust becomes a valuable and scarce resource. This is why REvil

relies on having a shared ethnic background as well as two reputation-based systems that mitigate uncertainty: reviewed vendors and escrow services - this group depends on a collective community trust to operate.

A breach of trust, on the other hand, reverts the entire environment upside down. REvil are unique in their approach as they are loud, extravagant, ethnically explicit, and invest in decentralization practices. They use this extravagance to extort ransom and obtain respect. Yet, when their relationships with they can not trust the community and the community do not trust them, the same psychological and behavioral patterns that enable them to be creative and unique make them more prone to being caught, more vulnerable psychologically, and more chaotic in mitigating crisis.

REvil is most certainly far from collapsing, but the recent complications with the public and with the criminal community have revealed some important trends. REvil's operations just as their predecessor GandCrab were heavily based on the exploitation of fears, pride, and vanity. These groups need attention to prosper. But if such syndicates receive too much negative attention from targeting authoritative figures such as the U.S. President, or making too much noise in the community, they may have to effortfully retire or rebrand again. Apparently, this was what happened with GandCrab, and this is the paradox of attention, embedded in the fabric of these gang's operations.

Seeing as how UNKN has changed his name 4 times in the past and GandCrab changed their practices after receiving too much fame, it is likely that REvil will only succeed with this name for so long before having to make significant changes to their name, identity, and code. REvil can only work for so long attacking such well-known targets. Trust, professionalism, and technological proficiency are more important to REvil now than ever. This organization is running on limited time if they have already rebranded once with some of the same people and some of the same code. The same story can repeat.