REvil: Analysis of Competing Hypotheses

digitalshadows.com/blog-and-research/revil-analysis-of-competing-hypotheses/

July 28, 2021

Until the 13th of July, 2021, things appeared to be going as expected with the threat actors behind REvil (AKA Sodinokibi) ransomware. Then, suddenly, the fairly public group vanished. With them disappeared their notorious "Happy Blog," payment page, and other infrastructure that supported their ransomware and extortion operations. That same day, their primary representative was banned on the popular Russian-language forum XSS where they'd been a fixture since the inception of their brand of ransomware.

Today, there is still a lot of speculation on the whereabouts of REvil, and many great minds have some pretty informed hot takes.

Was it…

- Law enforcement?
- A rebrand?
- Too much notoriety?
- Take the money and run?

Since there's been no official conclusion to this story, we at Digital Shadows performed the ancient intelligence ritual known as the **Analysis of Competing Hypotheses (ACH)** to see all the perspectives around specific events and moments that may help shed light on a most likely outcome.

Spoiler alert: We're still not entirely sure. Also, this is still just, like, our opinion, man, so please take it with a grain of salt.

What is an ACH?

An analysis of Competing Hypotheses (ACH) is typically a tabletop exercise that gathers intelligence analysts in a dark, smoke-filled room or a cave for hours to days at a time for a reasoned discussion. Much of the talk is usually based on what we've seen or learned over time about this particular actor, which includes our observations, as well as outsiders'. With an ACH, it's not about the most correct hypothesis, as all hypotheses hold the same weight; it's about which one(s) you might be able to prove.

Without further ado, let's dive into our six "competing" hypotheses belo

Hypothesis 1: Law Enforcement Action

This scenario so far is one of the top contenders, mainly because there is so much convincing evidence that points to law enforcement action:

Point: Speed of site outage

For starters, the speed at which all of the sites went down. It's not uncommon for actors to run into technical problems, either because of Tor's limitations or an unforeseen application or coding issue. The fact that everything was gone so quickly and seemingly under cover of darkness seemed different.

Not to mention, REvil's sites were observed to be more stable than most, so an outage lasting longer than 24 hours was a little out of character for the group. When you consider that "Unknown," their forum representative, was banned on the same day, it also lends some credence to the theory. Typically, forum bans are not to be taken lightly. Bans are rarely done

by request and usually occur because of some arbitration issue. The user was called out for being suspicious, or there's a question of law enforcement having access to a forum persona.

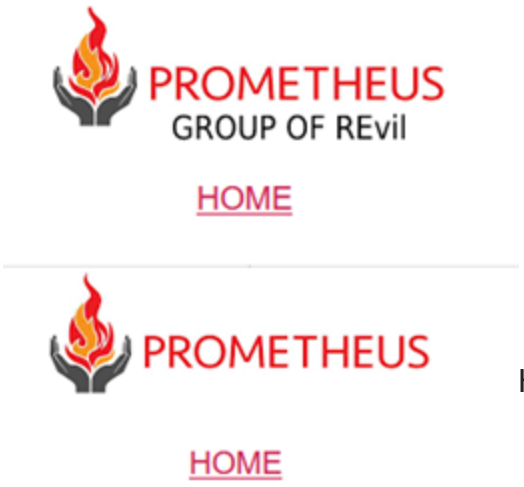
Point: Increased government rhetoric

Second, there's a combination of public factors that also contribute to this outcome. In the wake of the G7 summit, there was a PR-like Russian media release where the Russian FSB director stated he was ready to work with US law enforcement in the struggle with ransomware.

Coincidentally, the Biden administration and various government agencies stepped up rhetoric particularly against ransomware, which would be seen more as a terrorist attack if performed against critical infrastructure. There were also calls in the media to involve the intelligence community because of the aforementioned tougher stance on ransomware.

Point: Removal of REvil branding

Finally, in the underground itself, the actor behind Prometheus ransomware broadcast their affiliation with REvil until the week they went silent. The newest branding for Prometheus removed any mentions of REvil, and they have historically been one of the more staunch affiliates with REvil.



How it started (top), and how it's going (bottom) with Prometheus and REvil.

REvil themselves have never been shy in the spotlight. In the aftermath of Colonial Pipeline, they openly bragged about how good the business was getting, in terms of money to be made, as well as the number of affiliates. They also were unconcerned about the forum bans and rising US pressure and rhetoric. They also removed any restrictions on targets: Everything was fair game. Talk like that would seem to draw more attention, which does raise the possibility that maybe a law enforcement organization received their orders after someone reached the "enough" point.

Counterpoint: No claimants as of yet

What is working against these theories are a few possibilities. Namely, in the wake of every significant takedown in recent years, law enforcement also hasn't been shy to take any credit. In past operations, we've seen government banners plastered across sites when they're taken down, public indictments against operators in various courts, and press releases hitting major outlets.

Several countries outside of the usual US and Five-Eyes axis have had several significant arrests in recent years, often announcing them as they happen or while the flash-bang grenades are still cooling off on the ground. That still hasn't happened. Though the FBI is notoriously quiet about current operations, they do announce when something big happens. We knew when the FBI was able to seize funds from the Colonial Incident with DarkSide. However, REvil's wallets are still just sitting there. While this could point to a still ongoing operation or even a more extensive involvement from an intelligence agency,the thought is *something* would've leaked somewhere by now in 2021.

Verdict: Likely, but some evidence contributes to arguments for other outcomes.

Hypothesis 2: Technical Difficulties

Point: Technical difficulties are commonplace

This theory presents some problems, namely, not having complete insight into the skills and abilities of the actual REvil operators. Also, not knowing what the entire infrastructure even looks like may be problematic. It's realistically possible that even ransomware operators have shadow IT, or otherwise offsite content and hardware that is separate from the known sites such as "Happy Blog," and we may not know all of the forum personas.

Counterpoint: No historical technical issues regarding REvil

We know that, as a general observation, their infrastructure hasn't had much downtime compared to others. Any site downtime lasting more than a day just has not been seen often, much less on all of their known public sites at the same time. Again, this lends weight to the law enforcement theory, but it could also mean a step back to rebrand or retool.

While there is a possibility that some internal strife or maybe just better job offers elsewhere for key support personnel caused everything to go down at once, the analyst in me is saying that there would've been a reflection of that somewhere on the forums. People are generally terrible with secrets, so someone would've talked about it by now.

Verdict: Probable but difficult to prove without further insights.

Hypothesis 3: Strife

Point: Business disagreements increase with more members and affiliates

Have you ever had coworkers or management you couldn't stand? Or maybe just got tired of the job or the company? There's a good chance that ransomware operators go through the same thing. One of the arguments we'd discussed on the technical difficulties aspect was the possibility of certain group members leaving to seek their fortunes elsewhere, which would leave the sites, infrastructure, or any development adrift. Some thoughts about this led to more of the specific emotions for members and affiliates of the group. Maybe there was a so-called "old guard" who didn't care for current business practices, or perhaps suspicions of law enforcement involvement or pressure on other members. Maybe trying to manage the affiliates on top of all the day-to-day work became too much.

Counterpoint: Respect and arbitration on forums

There is evidence of strife between actors on forums, and REvil was no stranger to this. Digital Shadows had previously observed some public disagreements with affiliates, as well as accusations around mismanagement of funds. There were also some open arbitration cases over time, which in itself is not uncommon on forums. However, these were resolved around the time of REvil going dark. However, the group has had a decently long tenure and generally acted quickly to quash instability. There was also a sense of respect on the forums since they did participate in forum life, which usually involves discussions about other topics and business outside of ransomware.

Counterpoint: The money is good

Also, in June, there was the aforementioned interview with lots of boasts about business doing well with plenty of affiliates. While there is an ethos among forum members, again, this feels like something that would've had some reflection in forum chatter or other media two weeks later. People talk, and gossip is a byproduct of that communication, but nothing's been seen yet. So either there's an excellent NDA (nondisclosure agreement) in place, or nothing's happened in this particular vein.

Counterpoint: It takes a warrant

The problem with proving any of this requires greater insight into the inner workings of the group itself. Going that deep requires relationship-building, whether at a business or personal level, and understanding the personalities of the group itself. Short of that, those insights may be seen piecemeal by analyzing public statements over time; otherwise, only someone with a wiretap would be able to see what's behind the scenes and not on the forums.

Verdict: Probable, but need a better understanding of the human elements at work.

Hypothesis 4: Rebrand

Point: Rebrands are in fashion

Actors typically would need to establish some credibility and reputation for a rebrand or retooling of sorts, so something to watch out for would be some kind of public announcement stating a new ransomware variant is available, and it's from the team that brought you REvil. There may be calls for new affiliates or investment into the business. Since we haven't seen that yet, this remains just a theory.

Given some of the recent talk from governments and media about REvil, there's a possibility that the newest REvil product is hiding right under our noses. Or, the heat may be too great, so this is also driving the need for a bit of silence on the part of REvil. Prometheus's recent rebrand might indicate this was happening, but we have yet to see anything mentioned on RAMP, the newest forum, or any chatter from other actors. This new forum seems to welcome ransomware, as we've already observed LockBit advertising there, so maybe this is where REvil resurfaces or behind a new variant.

Given the absence of any public law enforcement moves and a lack of any general statements one way or another about any outcomes, this starts to become a very likely scenario. We've seen this repeatedly happen as significant players stepped away to change their business model, even just this year. In 2019 the group behind GandCrab went silent for a bit, and then suddenly, Sodinokibi and REvil became the new thing in 2020.

One thing to note: an almost throwaway quote buried in the last couple of paragraphs from a BBC story on Kaseya from 23 July 2021 deserves some attention here. The journalist's contact who claimed to have some insider knowledge of REvil stated that all of this is "part of a new beginning." Whether this is just a wild claim from someone to gain street credibility or this is a vetted source speaking the truth, it keeps the door open to the possibility of a later reemergence of REvil in a different form especially considering other indicators.

Verdict: Likely, but need to observe for other indicators.

Hypothesis 5: Vacation or Retirement

Point: Vacation is all I ever wanted

This one's tough to prove because without knowing group personas outside of the dark web, it's hard to look for beach selfies on Instagram that could serve as the smoking gun here. We've touched on this a few times, but Dmitri Alperovich of Crowdstrike fame floated the idea that new Russian safe havens in Crimea, along with the summer heat of Moscow, could've driven operators to take some time off. There's also a saying that "a Russian resort is preferable to an American prison."

Point: Riding off into the sunset with bags of money

Retirement is definitely a route that's been done before, especially when GandCrab (the yet unconfirmed variant connected to REvil) decided to close up shop back in 2019. Most recently, we've seen this to some extent with groups like Avaddon and Babuk Locker, who exited in various forms this year. Babuk, however, came back fairly quickly under a new moniker.

Looking at attacks over time, REvil was stepping up each attack in terms of ransom amounts, to the point that the ransom for the Kaseya attack was to be a record $70 million payout. Based on information from ransomwhe.re, we do know there's at least four wallets with just over $12 million in Bitcoin sitting there. Either way, not a bad pile of money to retire on, potentially.

Counterpoint:

What does work against this theory was the lack of any public announcements either way. Also it would likely take some time to move funds around in wallets, and in the instance of law enforcement involvement, time would likely be another factor to consider.

Counterpoint: Travel may be difficult

If the operators are indeed operating from Russia or any of the former Soviet republics, between COVID restrictions on travel in various countries as well as the potential for landing in an extradition country, travel could be problematic.

Verdict: Realistically possible, but difficult to prove either way, without more information and insight.

Hypothesis 6: The Wildcard

This area served as a drop-off point for any ideas that hadn't been mentioned. Ideas like alien abduction were not off the table but were found to be too improbable and reasonably difficult to prove.

The always useful "Aliens" meme, courtesy of knowyourmeme.com.

What is a more likely scenario for the wildcard is a combination of factors from the other hypotheses. There were not quite enough convincing arguments to make a hypothesis the best one. Some are stronger than others, primarily because of what we can prove or at least consider.

For example, law enforcement might've infiltrated critical infrastructure or compromised specific members, which means a forced reorganization of the business. Or pressure was on among affiliates or group members who didn't like all of the attention, which forced a retirement or job search for some, while others stayed on to figure out the next course of action. There may have even been dreaded customer churn among affiliates, and the public bravado in June 2021 about the aftermath of JBS was just smoke and mirrors.

We may just be seeing a cooling-off period, a rebrand, and maybe even a reorganization, which throws law enforcement off the scent. They may even still be around but using different, less public means to communicate, recruit, and advertise. It may end up being all of these factors, a combination of them, or none at all. Either way, we haven't necessarily closed the book on this group yet. Given some pretty significant successes over the last couple of years for REvil, it might be too soon to retire, but on this third iteration, maybe it's only time to change some logos for this Oceans 13 crew.

Verdict: There are several motivating factors brought up in different areas, but law enforcement action and/or rebrand are the most likely.

Changes in the Threat Landscape

This has been a pretty remarkable year in terms of major events impacting the threat landscape. We've seen record-breaking attacks, lots of groups entering and exiting the scene, and finally some attention from the very top: even heads of government are talking about it; not to mention the news cycle has caught on. The fact that no one has come to a

decent conclusion yet speaks to a number of factors. If it is a rebrand, the group has amazing operational security, and if there is some outsider knowledge about it, this is showing that sometimes, there is truly honor among thieves. If it was law enforcement, the silence continues to be a little unnerving.

At Digital Shadows, we continue to scour the world for information about this and other campaigns to keep our clients informed. As we spoke about in our recent Q2 2021 Ransomware research, this is a problem that's not going away, and despite one group's probable exit, there are more gaining in prominence. If you're curious about our intelligence, you can take Searchlight for a free test drive for seven days or get a customized demo to understand ransomware threats in your organization's industry and geography.

Tags: ACH / Kaseya / Ransomware / REvil / Threat Intelligence