ACRISURE® ACRISURE®

LONDON WHOLESALE

Cyber Threat Intelligence Report

in partnership with Cybeta

ACRISURE LONDON WHOLESALE ACRISURE

Implications of the Takedown of HIVE Ransomware

ABSTRACT: The HIVE ransomware group was operating a Software-as-a-Service (SaaS) model, replete with administrators, the use of initial access brokers to collect and identify targets, and the use of affiliates to conduct the attacks. It was the model for a sophisticated multi-layer operation that included easy to use web interfaces, a commission system with affiliates that promised to them a percentage of the total ransomware paid, and a dedicated effort to smartly target only those industries who HIVE operators believed were the most likely to pay their extortion.

In July 2022, the Federal Bureau of Investigations (FBI) and global partners conducted an unprecedented investigation and enforcement campaign against elements of HIVE, culminating in arrests in late-January 2023 that effectively dismantled their disparate network worldwide. Did this unique police operation against the group and the subsequent disruption of HIVE operations change the way ransomware operators such as this and law enforcement manoeuvre moving forward? Are there lessons learned from this successful enforcement action that can be repeatable and therefore applicable against the hundreds of other ransomware groups operating globally? What lessons can the private sector learn and apply to their strategic defences moving forward?

Question 1: What was novel about the law enforcement operation against HIVE?

At least publicly, this appears to be one of the first instances of law enforcement obtaining a decryption key for a ransomware variant and actively distributing it to victims around the world. While smaller scale examples do exist, the far-reaching and comprehensive scope of the HIVE operation was unique because it involved multilateral collaboration and coordination on an unprecedented scale, purported reverse-hacking of the attacker network resulting in the global distribution of HIVE's decryption key in a manner that belied typical law enforcement and intelligence modus operandi of protecting sources and methods. Worth noting, protection of sources and methods is often a primary consideration for security services, as it is an imperative to try and protect future capabilities by not broadcasting the tools and origination of the sources of intelligence.

Question 2: Are there any notable similarities between the Colonial Pipeline incident and this operation against Hive?

When Colonial Pipeline was the victim of ransomware in 2021, approximately half of the reported $4.4M ransom payment was eventually recovered by federal authorities in the United States. The fact that cryptocurrency could, despite the wide held belief to the contrary, be both traced and captured by outside entities was one of the few instances where the technical capabilities of state security services was showcased in a public and obvious way. There was even some media speculation that the decision to utilize the recapture capability and broadcast its success was indeed purposeful and deliberate, done for no other reason than to deter future attacks against critical infrastructure.

Could it be a coincidence, then, that the scope of HIVE's takedown would be any different, particularly against this unscrupulous group of ransomware operators with a history of carrying out attacks against hospitals, educational institutions and other critical infrastructure? The answer is most certainly not. It appears the strategy of U.S. federal law enforcement and its global partners was to make a concerted effort to prosecute operations aimed at critical industries and, at the right time, make the success of those operations public to dissuade future attacks.

Question 3: Will this deterrence be effective?

Short term- yes. Long term- unlikely. Although estimates vary, leading reports have indicated that in 2022 there was a decline in the overall payment of ransoms by victims globally. Dismantling of infrastructure and disruption of operations, without accompanying punitive consequences for the ransomware o perators themselves, is unlikely to result in reduced attacks over the longer term. Whether quasi-government-sanctioned attacks or truly independent threat actors looking to get rich, the return on investment remains too great to realistically believe the HIVE takedown - or any other known law enforcement activity - will disrupt attacker capabilities for the long term. To them, it is still a lucrative numbers game and many victimized entities still decide to pay their ransoms, despite best practices and recommendations to the contrary and despite public awareness of the need for preventative risk management that can theoretically obviate the consequences of ransomware if it does occur.

In spite of this, it is undeniable that in the short-term the specific operators administering and utilizing HIVE were immediately eliminated as a threat and effectively neutered in wake of global law enforcement dismantling their infrastructure. In addition, law enforcement activity in countries such as Germany, Netherlands and other Western-aligned nations is also very likely to dissuade local ransomware operators and affiliates as well, particularly those physically located inside those countries from participating in such criminal activity.

Question 4: Why was the operation made public?

In addition to the deterrence aspect mentioned previously, the timing of enforcement action and the concomitant public awareness of these operations was most certainly tied to diminishing returns from the law enforcement operation itself. HIVE ransomware operators seeing an unusual number of victims not paying their extortions, while also observing them seemingly recover business operations quickly, certainly would have triggered both questions and counteractions by them from July 2022 through January 2023. It seems plausible, if not likely, that law enforcement consensus was the belief that the value of continuing to monitor HIVE operations and decrypt victims' data would be less than that of the massive infrastructure takedown and publicity that they generated by going public. All good intelligence operations have a natural conclusion when the ROI calculation invariably changes, and it appears the HIVE takedown was no different after its unprecedented and massively successful operation.

Question 5: Does this have anything to do with Russia's invasion of Ukraine?

Yes, very likely. There is little happening worldwide that does not have some linkage to the Russian invasion of Ukraine and the ongoing war there -- and the HIVE takedown is no different. HIVE operators are believed to be comprised of members hailing from Russia itself and former Soviet Bloc countries. All spoils from paid ransoms would essentially be a way to circumvent sanctions, generate hard cash, and personally enrich the operators and their government sponsors. In addition to the financial impact, elimination of this criminal infrastructure in third countries also has a tremendous impact on the capabilities of these groups, regardless if their intent is ransomware or not. Lastly, it is likely that the precipitous decline in ransomware attacks outside of Ukraine that coincided in late February 2022 (which was around the commencement of the Russian special operation) and continued for months later was a direct result of many Russian or Russian-sympathizing threat actors having to pivot from offensive operations and instead having to defend their own networks from outside attacks. Further degrading their capability to utilize infrastructure outside of friendly territory is likely to, at least temporarily, severely cripple these actors ability to quickly regroup.

Question 6: What are the long-term implications of HIVE for the private sector?

Just like the immediate development of countermeasures for advancements of enemy kinetic warfare capabilities, cyber can operate on a tit-for-tat basis too. It is indisputable that the entire law enforcement operation against HIVE had a pronounced and surgical impact against these groups' finances and capabilities. But it would be unprecedented and naïve to believe that these criminal elements did not immediately begin reconstituting, activating, or otherwise utilizing alternative infrastructure and capabilities as soon as they observed their victims gaining access to corporate networks and operations without having paid any extortion and especially during the HIVE global infrastructure being dismantled.

Despite the success of the HIVE strike by law enforcement, it is nonetheless important to understand that ransomware operators are not going to shrink away due to one massive and successful operation against them. Until the personal or geo-political ROI calculation undertaken everyday flips to negative, these operators have every incentive to find new and novel ways to perpetrate their attacks and collect their spoils. As law enforcement increases their capabilities to detect and respond to attackers, those same attackers will adjust tactics to avoid disruption. Companies and entities worldwide must not hope or plan on law enforcement intervention or decryption to prevent massive financial losses. Instead, they must continue to invest in the assortment of multilayer and preventative technical controls and general risk management strategies such as disaster recovery that helps firms prepare, react, and recover from the risk and damage of ransomware attacks.

About Acrisure London Wholesale and Acrisure Re

The Acrisure London Wholesale team are uniquely placed within the market to offer excellent solutions to our clients, with both scale and breadth. We focus on both one-off open market/brokerage placements as well as designing and sourcing capacity for programs. Our analytics team allows us to provide outstanding results for our many independent retail and wholesale broker partners.

Acrisure Re is a full-service (re)insurance intermediary and capital management advisor with a commitment to providing tailored risk transfer solutions for our clients. With our global team of more than 260 experienced and talented employees dedicated to providing bespoke advisory, portfolio, and reinsurance solutions, we are driving a sophisticated, tech-enabled future for the (re)insurance industry.

About Cybeta

Cybeta was founded by a specialized group of senior Intelligence Community officers with 75+ years of combined experience in the United States Central Intelligence Agency, National Security Agency, and Department of Defense. The team worked together as information operations officers targeting and extracting priority objectives from the most advanced cyber adversaries. Their skills, combined with advanced data analytics and machine learning expertise, has led to Cybeta's unparalleled productized cyber services.

Contact:

Tom Quy
Senior Vice President
tquy@AcrisureWS.com

Luke Lattner
Vice President
Luke.Lattner@cybeta.com