Conti and Hive ransomware operations:

Leveraging victim chats for insights

WRITTEN BY
KENDALL MCKAY
with contributions from
PAUL EUBANKS and JAIME FILSON

Updated May 2, 2022

cisco | Talos

TABLE OF CONTENTS

EXECUTIVE SUMMARY

- Through open-source research, **we obtained and analyzed over four months of chat logs – more than 40 separate conversations** – between Conti and Hive ransomware operators and their victims. The findings in this paper give an overview of the actors' communications styles, persuasion techniques, ransom negotiations, operational and targeting information, and more.
- **Conti and Hive have markedly different communication styles**, with Conti employing a range of persuasion tactics in what often seem like scripted and somewhat organized exchanges. Hive communications, by contrast, are much shorter, more direct, and void of many of the persuasion techniques that Conti employs. These differences possibly reflect varying levels of organizational oversight for affiliates or may simply exemplify the unique communication styles employed by various ransomware actors.
- **Both groups are very quick to lower ransom demands**, routinely offering substantial reductions multiple times throughout their negotiations. It is clear that the actors' initial ransom demand is rarely their bottom line.
- **Conti and Hive do research on victim organizations before determining the ransom amount**, with both groups typically asking for about one percent of the company's annual revenue. Both threat actors appear to target entities indiscriminately, likely based on what they assess to be the easiest victims to compromise for quick financial gains.
- **Hive operators displayed surprisingly poor operational security**, revealing sensitive information about their encryption process and other operational details. Other evidence suggests that Hive affiliates do not adhere to any sort of standard operating procedure and employ any and all means necessary to convince their victims to pay, including offering kickbacks to victim negotiators once the ransom payment is made.

INTRODUCTION

The ransomware space is dynamic, continually marked by new emerging ransomware variants, groups rebranding under different names or shutting down operations altogether, and new strategic partnerships between different cybercrime gangs. The focused crackdown on ransomware operations by U.S. authorities and international partners has introduced even more change into this threat space, pushing ransomware actors into the focus of law enforcement's targeted efforts to disrupt their operations. Current events on the international stage have also recently affected at least one major ransomware player, the

notorious ransomware-as-a-service (RaaS) group known as Conti. After Conti publicly supported Russia's invasion of Ukraine, a cybersecurity researcher took revenge against the ransomware gang by leaking information about the group, including the malware's source code and internal chats between affiliates.

The theme of constant change is also at play as it relates to the Hive ransomware group, as we have recently seen the threat actors update the malware after security researchers published methods for decrypting infected data. The Korea Internet and Security Agency (KISA) subsequently released a decryption utility, presumably based on this research. Hive developers updated their malware after the research was published, and it appears KISA's tool only works against earlier versions of Hive ransomware, not updated versions.

Conti and Hive are currently positioned as two of the biggest players in the ransomware scene. With Conti, while their leaks exposed interesting information from internal messages between Conti operators, such as various job roles within the organization and their process for hiring new affiliates, the chat conversations covered in this report are from entirely different sources and focus on communications between the threat actors and victims. By analyzing their chats with compromised organizations, we gained insight into how the actors determine ransom amounts, their willingness to negotiate lower prices, sales tactics and coercive means to compel victims to pay, and many other details about their operations.

Similarly, the Hive chats that we analyzed for this report between the actors and victims come as the group continues to make headlines for high-profile breaches and the security community seeks to better understand and protect against such attacks. The Hive chats we reviewed provided an interesting contrast to Conti, allowing us to compare various operational and communications methods between the two groups. The conversations also exposed important information about the Hive ransomware payload and encryption methods, highlighting at least one affiliate's poor operational security in their willingness to disclose such sensitive information. While Cisco Talos Incident Response (CTIR) engagements have included remediation of ransomware infections of all types, these chats were obtained strictly via open-source investigatory means, and not through CTIR engagements.

This report builds on Talos' growing body of work that highlights the human interest component of high-profile adversaries, research that brings to light important information of intelligence value, like threat actor motivations, communications methods, operational insights, and more. A similar research endeavor from last year, for example, resulted in our paper based on chats with a self-proclaimed Lockbit ransomware operator from which we gleaned valuable, first-hand details of the operator's cybercriminal activities. Likewise, this report, which is based on an analysis of more than 40 chats over a four-month period, highlights several important takeaways for executives and the broader cybersecurity community at a time when ransomware attacks remain a major threat to organizations globally.

CONTI

COMMUNICATION STRATEGIES

Based on the chat logs we reviewed between Conti operators and victims, we observed several interesting themes and techniques the actors use to accomplish their ultimate goal of extorting organizations for large amounts of money. Conti's communication style is relatively professional, marked by seemingly scripted introductions and a matter-of-fact tone that is mostly void of emotion and hyperbole. The actors stay on message, explaining to the victim they're infected and pointing out what consequences the victim is likely to face if they fail to pay the ransom, and trying to convince the victim to pay as quickly as possible.

The actors' initial chats with compromised organizations are direct and to the point. The actors typically introduce themselves — "We are the Conti Team" — and often ask for the person communicating on the other end to identify themselves with their name, company name and position. They proceed to explain that Conti has compromised the victim's network, exfiltrated all sensitive information and encrypted the victim's files.

From there, we observed the threat actors employing a variety of different persuasion techniques. In many instances, the adversaries attempt to empathize with victims, equating themselves to business people just like the compromised entity and claiming that they want to help restore the victim's data. They appear to make the ransom payment seem like it is in exchange for their help, in one instance proclaiming, "Fortunately, Conti is here to prevent any further damage!"

The actors say they will provide "IT support" by offering a "decryption tool," even offering to give the victim a full security report upon payment to ensure that such an attack does not happen again in the future. We obtained one such security report, which is illustrated in Figure 1.

These are vague, generic recommendations with no specific implementation steps. Such guidance would be very easy to reuse across interactions with numerous victims.

The actors further mask these extortion attempts by saying they provide "damage prevention services," again purporting to be helpful assistants who can help protect the victim. In many instances, Conti operators remind victims about the consequences of having data leaked, including such information being sold on the dark web to cybercriminals who will leverage the data in their own operations, including social engineering attacks. The victim's customers, vendors, employees and investors will all be notified about the breach, Conti warns, but the threat actors claim they can resolve these problems immediately upon payment.

Conti also employed other marketing techniques to convince victims to pay, including offering Christmas and holiday discounts and other price reductions intended to make the victim feel like they are getting a good deal. Many of these deals are incentivized by quick payments, with a Conti actor offering in one instance that the victim can receive a "special discount" if "we make a deal in the next 72 hours."

The tactics outlined so far are Conti's attempts to be more empathetic and make the victim feel like Conti is helping them or cutting them a deal. However, we also observed Conti employ more aggressive techniques, including fear and coercion. The threat actors remind victims of the reputational damage and legal troubles that will result from a data leak, citing media reports about other companies who have faced multi-million and billion-dollar lawsuits for data breaches. They use scare tactics by telling the victim that the company's stock value will nosedive if Conti leaks their data and threaten to provide competitors with the stolen information. The actors remind the victim of the various governmental bodies and regulatory acts that punish organizations for data leaks and revisit the notion of employees becoming identity theft victims if the data is sold on the Dark Web. These threats seemed to intensify as Conti's frustration with the victim's slow responses or perceived lack of urgency grew.

These more aggressive tactics are consistent with recent trends reported by the U.S. government. According to CISA's 2021 global ransomware trends report, ransomware actors are diversifying their approach to extorting money, including informing the victim's partners, shareholders, or suppliers about the incident.

RANSOM NEGOTIATIONS

There were several indications that the Conti operators determine victims' ransom amounts on a case-by-case basis dependent on the organization's

Security report

We have penetrated your network using email compromise. So, first of all – provide all your employees with strict instructions regarding security measures.

Basic recommendations regarding network:

1. Implement better email filtering policies
2. Implement better password policies
3. Consider blocking some particular attacks like pass-the-hash and pass-the-ticket
4. Update all of your internal systems to the latest versions
5. Review network segmentation and take care about buying hardware firewalls with filtering policies
6. Block kerberoasting attacks
7. Conduct full penetrations tests (both external and internal)
8. Implement better AV/EDR systems
9. Review group policies, remove domain and local admin rights for some users.
10. Implement better DLP software system.
11. Secure your employees email, filter incoming mail and install EDR (Sentinel, Carbon Black)
12. Monitor the update of network programs
13. Pay attention to password policies, no saving in systems
14. Backups. Must have offline backups on cassettes, and use online backups

Figure 1. *Example of security report sent to Conti victims by the threat actor.*

"The chances that Hell will freeze are higher than us misleading our customers. We are the most elite group in this market, and our reputation is the absolute foundation of our business and we will never breach our contract obligations." - Conti operator to victim

annual revenue, with the actors stating as much in several of the communications we reviewed.

Conti actors are very willing to negotiate and almost always offered or approved a lower ransom amount in the conversations we reviewed. These reductions were initiated by either Conti or the victim depending on the situation, but in instances where the victim requested a lower ransom payment, the threat actors almost always obliged quickly and with little or no hesitation. In some instances, a lower ransom payment would still cost the victim data exposure: In one case, a Conti operator agreed to lower the amount by nearly 80 percent, but with the stipulation that 80 percent of the victim's data would be published to their leak site.

The price reductions that Conti offered were generally substantial, including 10, 24, 57and 74 percent, and even higher. In one exchange, Conti dropped the ransom demand five times, with the amount dropping a net 98 percent from $50 million to $1 million. Despite Conti's willingness to negotiate, they had limits to how low they would drop the ransom amount and would eventually hold firm on a final figure. In one case, the lowest figure they were willing to accept was $100,000, although we did not have insight into the initial ransom offer or that company's annual revenue. These findings highlight the actors' willingness to negotiate and also indicate that Conti's initial ransom demand is more of a starting point for negotiations rather than a final offer.

Conti also appears similarly flexible on their payment dates, with deadlines frequently being pushed out at victims' requests. These behaviors suggest Conti operators are highly opportunistic cybercriminals who ultimately would prefer some payment as opposed to none, even if that means capitulating to repeated requests by the victim.

REPUTATION MATTERS

Like most legitimate business operations, cybercriminals depend on maintaining a "good" reputation, at least as it relates to following through on agreements with victim organizations. This is also top of mind for Conti, as the threat actors repeatedly reiterated their strong intent to uphold their end of the deal, even appearing angry at times when they perceived victims were questioning their trustworthiness. In one exchange, a Conti operator exclaimed, "THERE IS NO WAY that we will not fulfill our promises after you pay." In another conversation, a Conti actor noted the group's "vast experience" in this field, even encouraging the victim to Google the group to find evidence that they never "bluff." Conti further echoed these sentiments in the following remarks: "The chances that Hell will freeze are higher than us misleading our customers. We are the most elite group in this market, and our reputation is the absolute foundation of our business and we will never breach our contract obligations."

This level of confidence and bravado is likely an important component of Conti's ability to establish some level of trust – albeit under unique circumstances – with their "customers." The only assurance a victim organization has in believing that their stolen data won't be leaked is the threat actor's word and, by extension, the group's broader reputation. If Conti hopes to maximize payments, they have to employ a combination of coercive and persuasive tactics with firm assurances that they will uphold their end of the deal. This likely explains Conti's firm, sometimes emotional language we observed in these types of interactions.

OPERATIONAL INSIGHTS AND TTPS

These conversations also yielded insight into some of Conti's operational details and tactics, techniques and procedures

(TTPs). Conti uses ProtonMail, an encrypted email service, to communicate with victims. They also use various temporary mail and file storage sites, as revealed in their conversations with victims, including SendSpace, qaz[.]im and PrivatLab. The file hosting sites are especially useful, as Conti leverages them to share files with victims. In one case, the Conti operator directed the victim to download a deletion log from a PrivatLab site as proof that Conti destroyed all exfiltrated data after the victim paid the ransom. In another case, the same site was used to demonstrate that Conti could – and planned to – decrypt the victim's files upon payment, with the victim uploading sample encrypted files and the threat actor returning their decrypted versions via the same file share site. Conti also mentioned using Disk Wipe, a free Windows application for permanent volume data destruction, to delete the victim's files they exfiltrated after the victim paid the ransom.

Conti also uses a variety of other publicly available tools in their operations, based on our observations in CTIR engagements and open-source reporting. These tools and utilities enable every phase of their attack, including initial access, discovery, persistence, lateral movement, defense evasion and more. In addition to these publicly available tools, such as Cobalt Strike and ADFind, Conti also leverages utilities that are natively found on Windows operating systems, such as Windows Management Instrumentation (WMI), the Windows command-line utility Nltest, and remote desktop protocol (RDP).

In one instance, we observed the Conti operator making vague references to additional TTPs, including the infection vector. The actor informed the victim that they had infiltrated the victim's network, "researched them, and found critical vulnerabilities, which enabled [Conti] to access and exfiltrate [the victim's] documentation and encrypt [their] file servers, SQL servers, subdomains, and local networks." Based on our observations in CTIR engagements, Conti actors leverage many different vulnerabilities for initial access and lateral movement. Specifically, we have seen them exploit the widely reported vulnerabilities affecting the Apache Log4j logging utility. We have also observed Conti targeting vulnerable Microsoft Exchange servers as the point of initial infection via PowerShell execution of webshells, according to CTIR findings. This serves as a reminder of the importance of organizations applying a patch management system and keeping all software up-to-date with proper security updates.

We also gleaned some insight into Conti's dwell time, with an operator mentioning in one conversation that they had infiltrated the victim's network and "stayed there for 18 days," which, the actor noted, was enough time to "study all [of the victim's] documentation and gain access to [the victim's] files and services." Dwell time, or the amount of time an adversary has access to a victim's network, is often difficult to discern during incident response engagements. An organization may have insufficient logging and/or the initial infection vector is usually difficult to identify in most cases, adding to the challenge of pinpointing the exact timeframe an adversary may have gained access. In an April 2022 report, security researchers noted Conti activity spanned 19 days, which is highly consistent with the operator's claim.

HIVE

COMMUNICATION STRATEGIES

Hive's communication style differed significantly from Conti based on our observations. Compared to Conti's somewhat scripted, more professional tone that mostly followed the same format across many conversations, Hive operators seem far more informal and less disciplined, with the conversations' structure varying greatly and actors sometimes exhibiting poor operational security.

Hive's greeting – "Hello and welcome to Hive. How may I help you?" – is much shorter and more direct than Conti's introduction. The Hive operators do not lead with a full explanation of what happened to the victim, but instead jump right into ransom negotiations, informing the victim of how much money it will take to decrypt their files with little to no context. We saw Hive provide some generic, bulleted points on these topics, but they were much less detailed than those from Conti. Figure 2 shows an example, which was mentioned immediately after Hive greeted the victim and informed them of the ransom amount.

As seen from this excerpt, which is largely representative of the general tone of all the Hive chats we reviewed, the exchange is short, direct, and not customized for the specific victim. Separately, we observed a few instances of Hive mentioning that they would provide the victim with a security report upon payment, but we did not see such a report provided in the communications we analyzed.

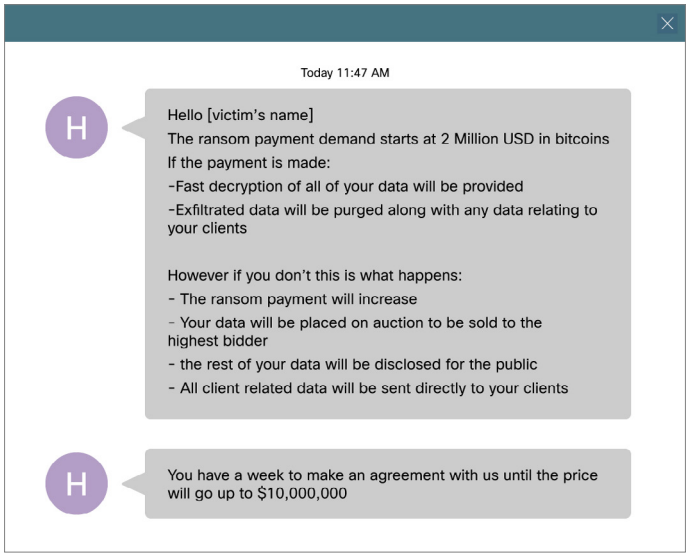

Figure 2. *Example of communications between Hive ransomware actors and a victim.*

Hive almost never employs any of the persuasion strategies we observed with Conti, such as marketing ploys, fear, or coercion. In the few times we did observe a Hive operator attempt to use persuasive language, it was short, matter-of-fact, and usually prompted by a question from the victim rather than Hive leading with a forceful appeal. We also observed Hive quickly become more aggressive if the victim failed to respond to the ransomware operator's initial greeting. In one case, after a victim failed to respond 14 days after Hive's initial communication, the Hive operator declared that their patience was gone and threatened to send a copy of the victim's data to the Securities and Futures Commission (SFC), a Hong Kong regulatory agency. The operator even provided individual email addresses of SFC members he planned to send the data to. Hive operators also quickly and dramatically increased the ransom demand if the victim did not respond, as seen in the excerpt above, where the ransom payment eventually jumped from $2 million to $10 million after seven days without communication from the victim.

RANSOM NEGOTIATIONS

Hive's ransom demands are typically valued at 1 percent of the victim company's annual revenue, according to Hive operators. Based on our analysis, we largely found this to be the case, but in some instances, the ransom was slightly higher at around 1.5 percent. Much like Conti, Hive appears very willing to lower their ransom demand, indicating their initial figure is rarely their bottom offer. The deduction percentage varied widely across victims and did not appear to follow any particular rule or structure. Observed deductions included 10, 15 and 25 percent and even upwards of 30 and 66 percent in other cases. These changes to the ransom demand were usually made rather easily, with little to no hesitation. However, Hive was quick to drastically increase ransom demands as punishment for lagging victim responses, as previously highlighted. In terms of victims, Hive confirmed that they target all industry verticals rather than focusing on certain sectors like healthcare.

Just like most other ransomware groups, Hive communicates with its victims via a chat portal hosted on The Onion Router (TOR). In their ransom notes, Hive provides the same TOR URL but delivers custom login credentials for each victim, which they use to log in to the chat portal to communicate with the ransomware operators.

Upon logging in, the victim's custom page is displayed (Figure 3), with the chat dialogue displayed in the center. The company's profile is featured on the left, which includes the organization's name, a brief summary of the entity, the company's website, and figures representing its revenue and number of employees. The right side of the page features a countdown to the payment deadline, a link to download the decryption software, and Hive's ransom demand and corresponding Bitcoin address to submit payment.

We observed one instance in which a Hive operator appeared to reward the victim communicant for helping negotiate the deal with the victim. In that exchange, the negotiator asked the Hive operator to keep 70 percent of the ransom amount upon payment and give the remaining 30 percent to themselves. The Hive actor ultimately agreed to give the negotiator 10 percent once the payment was made. In several cases, we observed negotiators operating on the victim's behalf, but this was the only instance where we saw Hive collaborate with them and share profits.

While this may have been an anomaly, it could represent ransomware actors' willingness to receive payment by any means. This payoff to the victim negotiator, combined with both Hive and Conti's propensity to lower ransom demands, reinforces the notion that these operators are highly opportunistic and will make compromises during their operations to compel victims to pay. This theme is also reinforced by Hive's admission that they do not focus on targeting any particular industry, suggesting instead that they

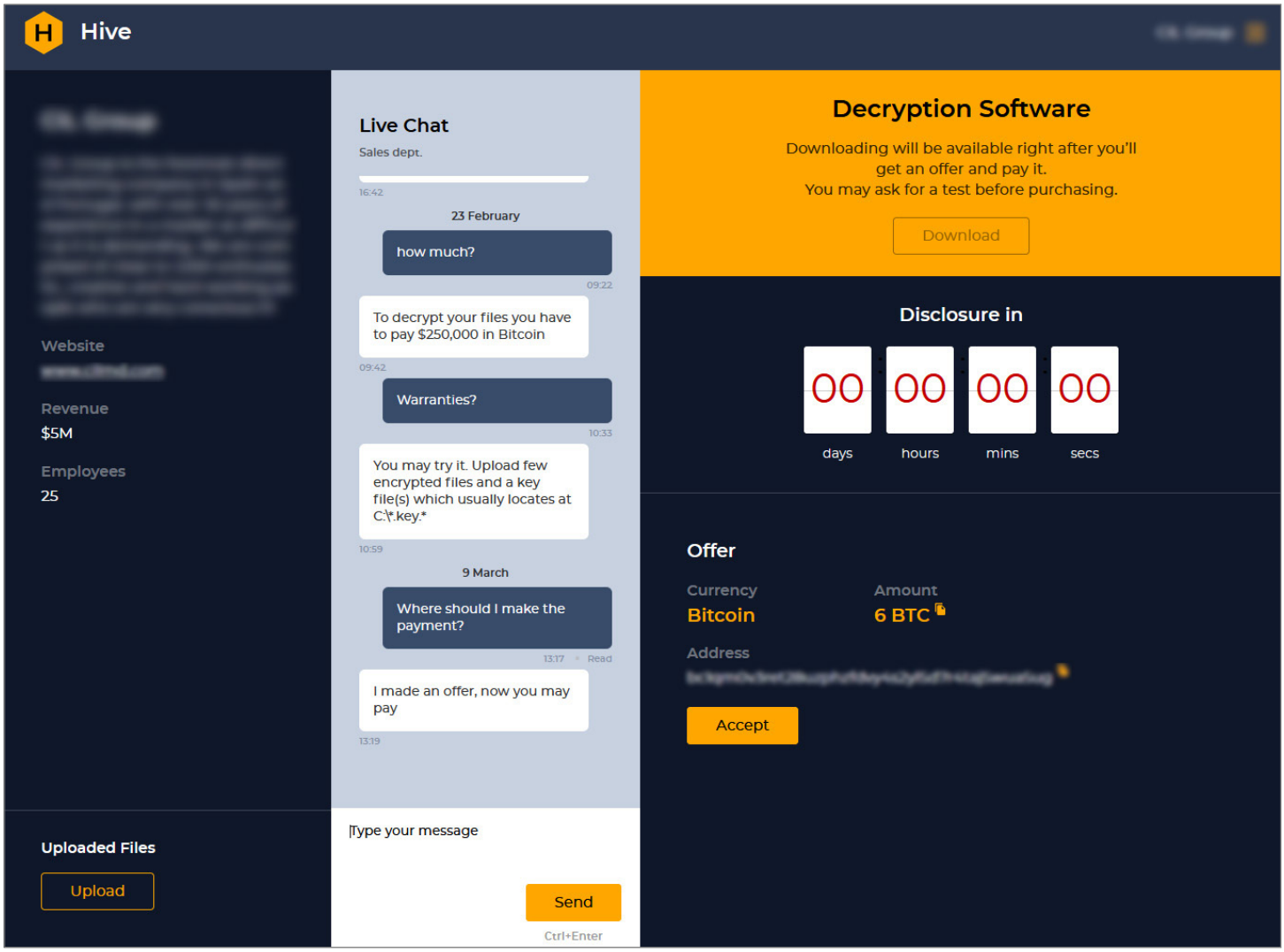

Figure 3. *Customized victim page.*

indiscriminately target organizations they may perceive are the easiest to compromise or extort.

This exchange between Hive and the negotiator may also represent the lack of standard operating procedures within the Hive group. Relatedly, it possibly represents the potential for individual affiliates to be either less disciplined – or more innovative, depending on one's interpretation – during their operations to do anything necessary to convince their victims to pay. The notion of being undisciplined is strengthened by another observation we made, mentioned in the next section, where we saw when a Hive affiliate displayed poor operational security.

OPERATIONAL INSIGHTS AND TTPS

The Hive operators revealed a surprising amount of information about various components of their operation, including details pertaining to the ransomware payload, the encryption process, and various tools and communication platforms they use. They mentioned that the ransomware payload is unique or custom for each individual victim, noting that for this reason, the file hash will not be useful for security personnel and network defenders. The operators were also forthcoming about sharing the ransomware hash with the victim when asked, even going so far as to provide the VirusTotal URL linking directly to the file sample in one case.

In one of the communications we reviewed, the Hive operator stated that it is impossible to recover the decryption keys from memory and decrypt files. The ransomware overwrites the decryption key in memory to prevent its recovery.

In terms of the encryption process, the threat actor revealed that the ransomware only encrypts about 100KB of each file, including the first 4KB, the last 4KB, and several blocks in the middle of the file. The Hive operator noted that the ransomware acts fast, which is probably enabled by this partial encryption. The Hive ransomware is not aware ahead of time how big or small the files are that it will need to encrypt, so it has to make a tradeoff decision between speed and accuracy. That tradeoff is seen in the ransomware encrypting files quickly, but not thoroughly. Mistakes the Hive developers made in their encryption schema make key recovery trivial. The malware only partially encrypts files, and reuses a small key for every file it encrypts. The Hive malware authors likely thought they were being clever by overwriting the key in memory after the encryption process was complete to prevent investigators from recovering the key directly from device memory, but they were not clever enough to realize that they made the classic cryptography blunder of one-time-pad reuse, which allows the user to recover the key simply by comparing the encrypted contents together bitwise. This type of error suggests the malware developers are not well-versed in crucial cryptography mechanisms. We assess that many other ransomware groups likely have similarly glaring problems, especially the ones that advertise speed as a performance metric.

The encryption process is started by a random field value, according to the Hive operator, and after the encryption is completed, the program overwrites the area of memory where the key was stored to prevent key recovery. They note that private and public RSA keys are only used to encrypt/decrypt the random field value, and it is only possible to decrypt the files if you know that random field value. While the actor specified the “random field” is not generated by a pseudo-random number generator (PRNG), this detail appeared to be a sarcastic comment made in jest, based on the context of the chat. A PRNG is an algorithm used to create a value which appears random, and is often used as a seed to generate entropy in cryptography systems for tasks related to key security and modes of operation.
They also noted that encryption is done using public RSA keys, decryption is done using private RSA keys. It's important to note this is only the case for encrypting the symmetric key used, not the victims’ files. In other words, Hive only uses asymmetric RSA public key encryption for securing the symmetric key used to encrypt all the files, an important distinction.

The Hive operator confirms the generated key is re-used to encrypt all the files. They then state it is “exported,” possibly meaning “written,” to "disk using a few RSA public keys applied." This possibly means RSA public key encryption is used to encrypt the key on disk. After the file content encryption routine is done, the key is re-written to prevent recovery from memory. This suggests the key used for file content encryption is a symmetric key, which is obscured by a public key routine. The affiliate further states the decryption software has RSA private keys used to decrypt the exported (presumably symmetric) key, which is then used to decrypt file contents. It appears that the actors mean the symmetric key is stored in memory, but the key itself is encrypted using RSA public key encryption. If this is the case, it would be difficult to recover the key even if it was not over-written later in the execution. However, it does not matter what the actors do to try and hide the key during the encryption process; the problem resides with symmetric key reuse in the first place, which allows a person who only has access to the encrypted file contents to then shake out the symmetric key by comparing the encrypted files to each other bitwise. Separately, the Hive operator also noted that the key file usually has the extension “*.key.*” – such as “.key.frg.15” –and is typically located at the root directory of shared folders, according to the Hive actor.

In this same conversation, the Hive actor said that they use “some kind of Vernam’s cipher,” not an AES cipher, for encryption. This speaks to the key length constraints mentioned above: Notably, Vernam’s cipher – a simple substitution cipher – requires the key length to be the same as the message text length, which is possibly why only 100KB of each file is encrypted.

This detailed account of Hive’s ransomware and encryption process underscores the actor’s poor operational security.

During these conversations, the Hive operator noted that they had never disclosed this encryption information to anyone before, raising questions about why they elected to share such details in that particular instance. It is possible that they were boasting about that component of their operation and they simply did not understand, or care about, the significance of sharing this type of information. Regardless, these disclosures again suggest a lack of

"Almost all antiviruses are useless against real hackers."
- Hive operator to victim

discipline or standard operating procedure, as well as a strong disregard for safeguarding sensitive information.

We note that these chats predate the recent research published by researchers from South Korea's Kookmin University detailing a method for decrypting files infected with Hive ransomware. The Korean Internet and Security Agency (KISA) released a recovery tool about a month later. Based on more recent Hive-victim conversations from March that we obtained, the ransomware operators appear to be using their updated encryptor and imply that any other decryption tool would be useless. For example, in their initial greetings with victims, they now state, "Please note that it is updated encryptor, there is no way to decrypt files other than to pay." Hive updated their ransomware in early March to address the encryption flaws revealed by the researchers, according to open-source reports. In late March, the actors made additional updates, converting their VMware ESXi Linux encryptor to the Rust programming language and adding new features to make it harder for security researchers to monitor their negotiations with victims. This indicates that the Hive developers are still very active and intent on continuing their operations despite repeated setbacks by security researchers and government efforts to thwart their activities.

In addition to these specific revelations about encryption methods, Hive also provided some more general insight into their operations, mentioning in one exchange that they did not put much effort into trying to evade detection. This confidence in their operations was echoed in other communications, where they flaunted their reputation, the ransomware's encryption speed, and skills at evading detection, noting in one exchange that, "Almost all antiviruses are useless against real hackers." Despite the actor's claim, we have observed Hive using some defense evasion tactics based on CTIR data, including abusing msiexec.exe to proxy execution of malicious payloads, deleting shadow copies, clearing Windows event logs, and modifying and/or disabling security tools, such as antivirus software, to avoid detection of their malware, tools and activities.

Similar to Conti, Hive uses a combination of tools and utilities found natively on the victim's operating system, such as RDP, PsExec, and msiexec, PowerShell, along with publicly available tools like Cobalt Strike, AnyDesk and others, according to CTIR findings. They also use various file sharing sites, such as PrivatLab and ProtonMail to communicate with victims, based on the communications we reviewed.

GENERAL GUIDANCE AND MITIGATION STRATEGIES

These conversations revealed that, like many cybercriminals, Conti and Hive are opportunistic actors who likely seek to compromise victims through the easiest and fastest means possible, which often include exploiting known vulnerabilities. This is a reminder to all organizations to implement a strong patch management system and keep all systems up-to-date. Another way to mitigate the threat of adversaries exploiting vulnerabilities is to monitor for suspicious network traffic, such as large quantities or anomalous activity that could be indicative of scanning. Threat actors may conduct vulnerability scanning to collect host information that can be used to identify exploitable or unpatched software and applications. Vulnerability scans typically harvest running software and version numbers, listening ports or other network artifacts to identify any weaknesses.

Organizations should also perform general system hardening that includes removing services or protocols running on endpoints where they are unnecessary. Ensure that unnecessary ports and services are closed to prevent the risk of discovery and potential exploitation. Additionally, organizations should consider hardening devices, including systems, networks, and security devices, to minimize and limit the success of any attacks. This includes actively adding applications to the allowlist and blocklist in order to control which programs are operating on your system.

It is also essential for organizations to implement policies to prevent adversaries from using credentials that are either sold on dark web cybercriminal forums or that have been leaked in other data breaches. Organizations should require employees to use multi-factor authentication (MFA) to

provide a higher level of security and ensure that leaked or stolen credentials cannot be used to access systems and resources. Creating long, complex passwords and enabling MFA will help prevent threat actors from using stolen or default and valid credentials. If feasible, require MFA for all users with administrative privileges, as well as external login and remote access methods for applications used within the environment. MFA is the most effective method for preventing remote-based compromises and can stop access to compromised accounts by requiring all users to provide a second form of authentication.

If valid accounts are compromised or leveraged, conduct a full password reset, especially for all privileged accounts in the domain. The lack of MFA remains one of the biggest impediments to enterprise security. Many ransomware and phishing incidents could have been prevented if MFA had been properly enabled on critical services, such as a virtual private network (VPN) or endpoint detection response (EDR) solutions.

