FORTINET

REPORT

Threat Intelligence Report

Ransomware-as-a-Service Programs and Their Ecosystems

TABLE OF CONTENTS

About This Report and FortiRecon

This latest FortiGuard Labs Ransomware-as-a-Service (RaaS) Trend Report leverages Fortinet's FortiRecon service to provide a deep dive into what adversaries are seeing, doing, and planning, enabling organizations to better understand the threat risk posed by the growth in RaaS. The report covers global and regional threat landscape perspectives as well as protection recommendations for information technology (IT) and operational technology (OT) organizations for ransomware observed during Q2 2022.

FortiRecon is Fortinet's Digital Risk Protection (DRP) service. It is a SaaS-based service that combines three powerful technologies and services, External Attack Surface Management, Brand Protection, and Adversary Centric Intelligence, to protect critical digital assets and data from external threats. By looking into the open web, social media, mobile app stores, dark web and deep web sources, FortiRecon provides organization-specific, expert-curated and actionable external attack surface intelligence on exposed assets, threat actors' activity, their tools, and tactics. The service identifies brand infringement and monitors ransomware data leaks to proactively help remediate and execute takedowns on an organization's behalf.

"Ransomware-as-a-Service (RaaS) has expanded the threat matrix by lowering the barrier for entry to cybercriminals who no longer need to be particularly expert or cyber-savvy to launch an attack. Given the financial benefits and the increasing availability of the RaaS model, these threats are bound to increase."

– Carl Windsor, SVP Product Technology and Solutions R&D

1. Executive Summary

Ransomware is not an invention of the 21st century. It can be traced back to 1989, when Joseph Popp wrote the first known ransomware, the PC Cyborg or "AIDS" Trojan. But the number of ransomware attacks has been accelerating dramatically since 2010, reaching a point where cybercriminals today earn billions of dollars in a single year.

Cybercriminals have exploited multiple vulnerabilities, some known and others undisclosed, in software and operating systems to deliver ransomware. Other elements, such as major political, entertainment, or sporting events, are also catalysts. The COVID-19 pandemic, for example, contributed to the recent surge in ransomware. As organizations quickly transitioned to remote work, gaps were created in their cyber defenses that malicious actors were quick to exploit. Another contributing factor to the current growth in ransomware is that cybercriminals have also refined their business models. RaaS, which sells ransomware software and services for a percentage of any profits, has quickly emerged as a significant cybersecurity threat in its own right, helping attackers expedite their operations. Before the RaaS model, hackers (or threat actors) needed some proficiency in writing or accessing code before attempting a ransomware attack. But now that RaaS is available, hackers require little to no coding expertise, only needing to acquire initial network access to organizations to carry out a ransomware attack. This process has become more refined, resulting in a wave of new and often highly aggressive and malicious ransomware attacks.

1.1 RaaS Overview

Because RaaS is a low-code, Software-as-a-Service SaaS attack vector, it enables cybercriminals to purchase ransomware software on the dark web and carry out ransomware attacks without any coding knowledge. In the past, all effective hackers had to be well-versed in coding, which limited ransomware to elite criminals. However, this technical hurdle was removed when the RaaS paradigm was introduced. RaaS users don't need to be knowledgeable or even experienced to utilize the tool effectively, as with all SaaS systems. As a result, RaaS solutions enable even the most novice hackers to carry out highly complex cyberattacks.

Over the last few years, FortiGuard Labs, coupled with FortiRecon service, has observed numerous threat actors operating in underground communities. These adversaries, often affiliated with various ransomware groups, have been supplying initial access to multiple organizations worldwide to carry out ransomware attacks. The FortiGuard Labs team has engaged with some of the affiliates of these ransomware groups online, as well as multiple network access brokers, to acquire more information about their operations. This report provides that insight, coupled with our threat data and analysis, into these ransomware operations. We also provide information on the various tasks assigned to group members involved in these attacks.

2. Ransomware Groups

2.1 Structure Overview

A typical ransomware group has a corporate-like structure with multiple divisions, such as sales and HR that are responsible for recruiting top performers (e.g., communication experts, negotiators), support teams that offer continuous support to affiliates, IT teams who are responsible for software upgrades, troubleshooting, and more—all to ensure "successful" and smooth operations.

2.1.1. Development Team

These group members are tasked with developing the ransomware malware, testing the final code, fixing bugs, and releasing regular updates. Developers are often observed reusing code from other ransomware strains or reverse-engineering publicly available malware samples and including these capabilities in their own ransomware. They are also tasked with implementing various enhancements, such as updating encryption algorithms to expedite the encryption process and using obfuscation techniques to better evade security systems and antivirus software.

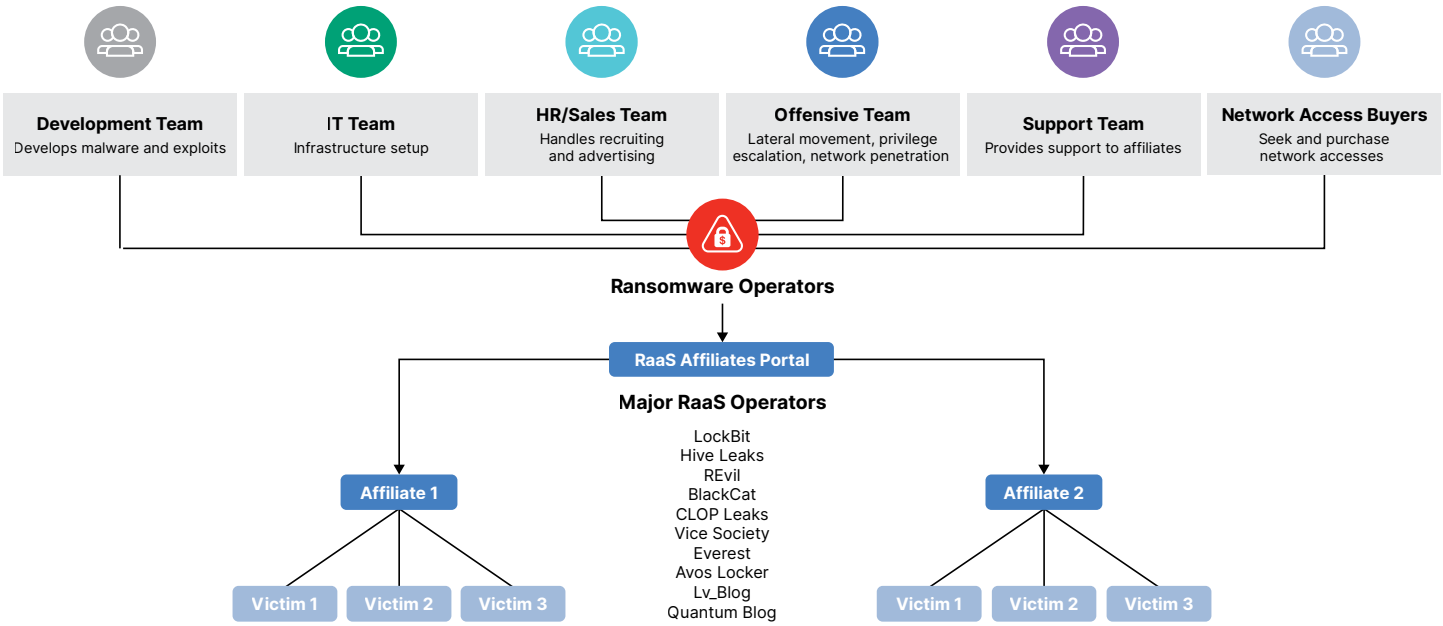

Figure 1: RaaS model

2.1.2. IT Team

The IT team members are responsible for setting up new C2 servers, maintaining backups, developing panels for affiliates, managing accounts, and similar activities to ensure a stable infrastructure that ransomware operators and their affiliates can rely on. They are also responsible for managing, troubleshooting, licensing, and updating the hardware and software assets required for operations, as well as setting up the servers used to store the data exfiltrated from the victims.

2.1.3. Recruiters, HR, Sales Teams

This team is responsible for hiring new members based on the requirements of the ransomware operators. They often use underground forums to seek out and identify such members. Based on recent online engagements with active representatives/affiliates of the infamous ransomware cartels AlphaV (aka Blackcat) and AvosLocker, we acquired interesting insights into their operations. These and similar ransomware groups are continually hiring members to join their teams to perform various tasks.

Following is a list of the most sought-after skillsets:

- Developing file-encryption programs for the development team
- Setting up and maintaining payment sites, leak sites, and communication channels for the IT infrastructure team
- Advertising the ransomware service on forums as a part of the sales team
- Communicating with journalists, posting messages on Twitter, and blogging announcements as a part of the PR/social media team. Negotiating skills are also required to effectively negotiate with their victims for their ransom payments
- Performing manual hacking and lateral movement on victims' networks to deploy the ransomware program (external contractors/affiliates)

Group Membership Fee

Groups often ask newly hired members to deposit a specific amount to the operators' accounts. For example, in one online engagement, we found that the AvosLocker ransomware group allegedly demanded ~ $4,000–5,000 from potential hires. And in a REvil RaaS program advertisement, they required a deposit of 1 BTC from new members upon hiring. This ensures that newly hired members do not scam the ransomware operators. These affiliates are given access to a panel for downloading the encryption software and listing the targeted organizations on the official site of the ransomware group to demand ransom. Affiliates also use this panel to manage their victims and communicate with them to negotiate the ransom.

2.1.4. Offensive Team

Upon successfully purchasing initial network access, information is transferred to the offensive team, which includes affiliates of various ransomware groups who have subscribed to the RaaS program. This team attempts to penetrate and move laterally within a victim organization's network and gain admin privileges over the target network. Members of this team are skilled at performing recon over a targeted organization's network, extracting user details/credentials, performing hash dumps, and discovering different types of systems in the network, such as NAS devices, backup servers, etc. Once privileged access is gained, these attackers exfiltrate sensitive data and then encrypt systems using the encryption software provided by the ransomware operators.

For example, upon gaining a persistent online engagement with a threat actor operating as "idk," who claimed to be an affiliate of the AlphV ransomware group, they infiltrated an organization's network, performed privilege escalation, exfiltrated its data, and encrypted network systems.

In other words, the members of the offensive team ensure a smooth workflow and fulfill the requirements of ransomware groups and their operations.

2.1.5. Support Team

As the name suggests, the support team is dedicated to resolving issues faced by the affiliates of the ransomware group. These could be any type of issues, such as bugs in the affiliate panel, queries regarding the network encryption process, provisioning a new build, answering questions related to the splitting of profits earned from victims, and more. This team's primary task is to ensure that affiliates can perform ransomware attacks successfully without encountering roadblocks. For more complex issues, the support team may escalate issues to the relevant team, depending on the type of problem.

2.1.6. Network Access Buyers

The primary role of these groups of individuals (or, in some cases, affiliates) is to search for access brokers on underground darknet forums and purchase access to the various organizations being advertised. They are also tasked with looking for initial access to organizations' networks using compromised VPN credentials acquired by credential stealer malware.

FortiGuard Labs, with the FortiRecon Adversary Centric Intelligence service, tracks the activities of multiple threat actors operating on cybercrime forums who advertise network access using stolen VPN credentials for Citrix, Pulse Secure, Cisco, Fortinet, and other agents. Below is an example of a representative of the AvosLocker ransomware group showing interest in purchasing network access advertised by access brokers operating on the Russian language cybercrime forum, "Exploit."

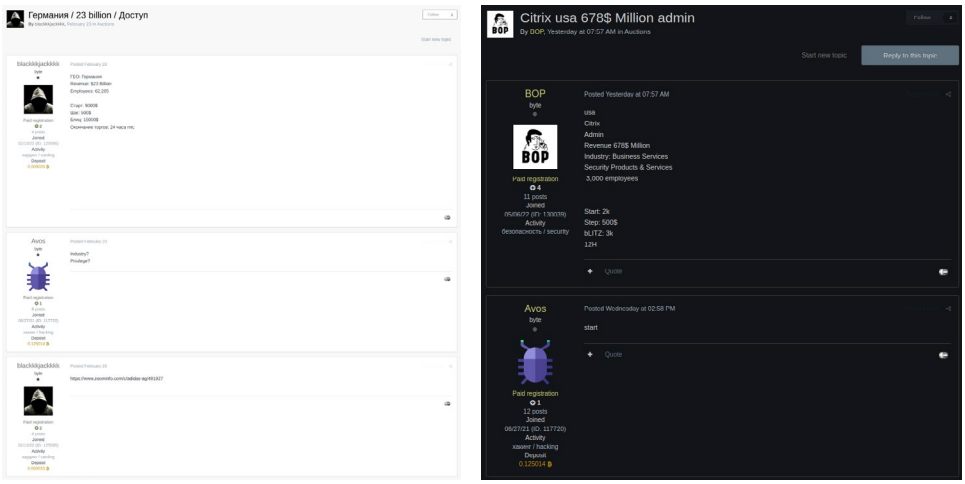

Figure 2: AvosLocker ransomware group showing interest in purchasing network access on "Exploit" forum

Initial Access Broker Lists: How Early Visibility Can Help Act—Fast

Based on FortiRecon observations, initial access via VPN is valuable data for ransomware operators as it may provide access to multiple internal infrastructures/resources of the target organizations, including their web applications, systems, servers, and confidential files/documents stored in those systems. Therefore, ransomware operators usually rely on threat actors advertising such accesses on various underground forums. We have observed multiple instances where initial access to organizations was offered on cybercrime forums by access brokers that were later impacted by ransomware attacks.

For example, on June 17, 2022, FortiGuard Labs, using the FortiRecon service, reported a threat actor—operating under the handle "I UNKNOWN I" on the Russian language cybercrime forum, "XSS"—advertising network access to Kuwait Airways. Ten days later, the organization was listed as a victim on LockBit 2.0 ransomware group's official onion site.

A similar instance was observed involving an Indian organization named ISGEC Heavy Engineering, Ltd. Access was being advertised by multiple threat actors (2022031147746, 2021111738002). In June 2022, the Head of the IT department of ISGEC Heavy Engineering registered an FIR with the Noida police, informing them about a ransomware attack (2022062773119).

Such incidents demonstrate the high probability of ransomware groups relying on network access brokers to move forward with their attacks. There is, however, an upside to this scenario. If you discover leaked credentials/RDP (Remote Desktop Protocol) access for sale on dark web marketplaces early enough, you still have time (while it's for sale on the market) to proactively take steps to block an imminent attack.

1.2 Ransomware Affiliate RaaS Panel Overview

Based on FortiGuard Labs' observations using the FortiRecon service to monitor and infiltrate cybercrime forums and online engagements with threat actors, we identified numerous incidents that provided significant insight into the RaaS panels used by the affiliates of different ransomware groups. Information on two such instances is detailed below.

2.1.7. Hive Ransomware

On May 4, 2022, an actor operating as "Sheriff_2" shared the login credentials of a RaaS panel. This actor claimed to be an affiliate working with the infamous "Hive" ransomware group on the English language cybercrime forum "Breached." We discovered that the panel offered the following capabilities:

- Chat room for negotiating with victims
- Creating unique builds for each victim that can be used to encrypt the entire network of targeted organizations. Names of victims were not disclosed on Hive's onion site.

Figure 3: Breached forum post

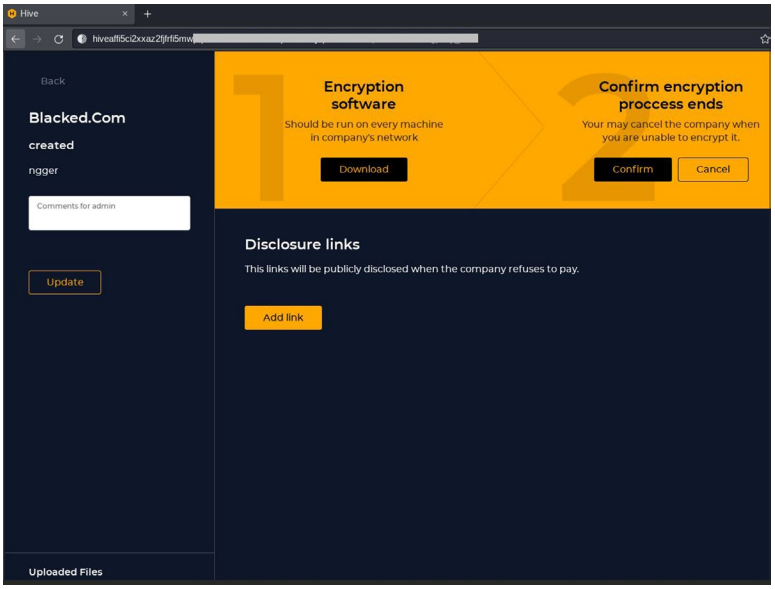

Figure 4: Hive ransomware affiliate panel

2.1.8. SolidBit Ransomware

FortiGuard Labs, with the FortiRecon Adversary Centric Intelligence service, performs an online engagement with the operators of ransomware named "SolidBit," which allegedly uses Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) public-key cryptosystem algorithms for data encryption. This ransomware group does not have any website for listing victims. However, the operators claim they will launch a new onion site in the near future. The operators also provide access to their affiliate panel over private chat, which displays the affiliate's victims. This is similar to the aforementioned "Hive" ransomware panel. However, while a Hive affiliate has the ability to generate new builds in the panel itself, the SolidBit panel does not offer this. Instead, SolidBit operators provide their affiliates with a unique build of the SolidBit ransomware executable at the time of initial application, which can be used to encrypt the target system/s. The ransomware executable and access to the following panel are only provided by the operators after an affiliate pays a registration fee of $200.

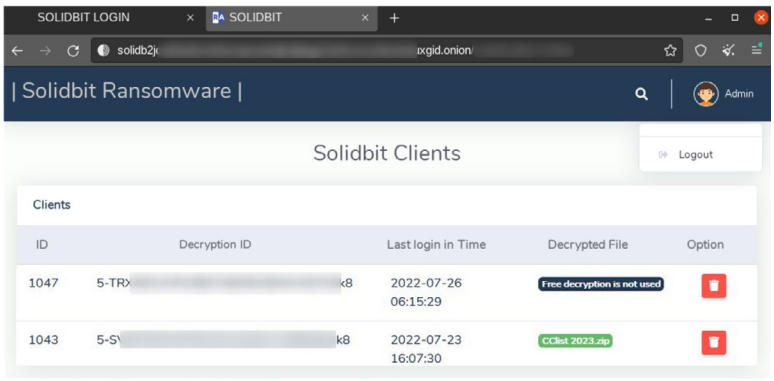

Figure 5: SolidBit ransomware affiliate panel

When this information was gathered, the SolidBit group's activities appeared to be in the development phase, because they only recently started recruiting affiliates. SolidBit ransomware victims are further asked to log in to a panel with unique decryption ID given exclusively to them. As shown below, victims can use this panel to chat with the operators to negotiate ransom and other discussions. It also allows them to decrypt a single file (up to 1 MB) for validation. We also observed a panel with a similar user interface used by the infamous LockBit ransomware group, further showing interconnections among multiple ransomware groups.

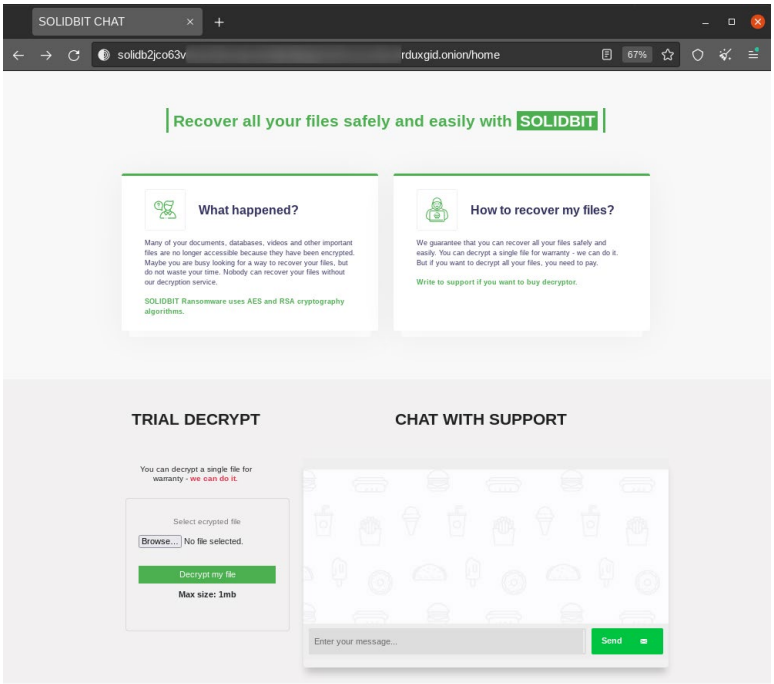

Figure 6: Ransomware members operating on cybercrime forums

1.3 Ransomware Members Operating on Cybercrime Forums

Last year, ransomware-related activities were officially banned from most top-tier forums due to the Colonial Pipeline ransomware attack. The attack served as a breaking point for ransomware due to the disruption caused by the attack on average citizens. As a result, the underground cybercrime community started to restrict ransomware gangs. Although three major hacking forums banned ransomware-related activities, they did not stop threat actors. By carefully moderating their advertisements and thereby not "officially" breaking the forum rules, many were able to evade this ban.

Members of ransomware groups have been operating on cybercrime forums for many years. We have observed the activities of several ransomware groups advertising their affiliate program and promoting their ransomware on popular cybercrime forums. The details on the operators of some of the well-known ransomware groups operating on cybercrime forums can be found below.

Note: This is not a complete list, and it has also been filtered based on the threat actor's popularity. Contact us if you are looking for more information about a specific group or groups not mentioned below.

2.1.9. LockBitSupp

Actor "LockBitSupp" joined "XSS" on March 8, 2021. They have a good number of reputation points (892+) on the forum due to actively discussing ransomware-related topics. The actor currently has 419 active posts on the forum related to malware and general discussions on ransomware.

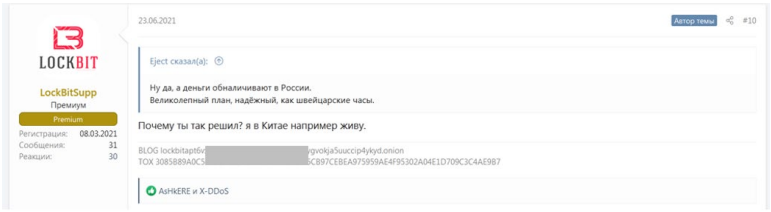

Figure 7: LockBitSupp forum

2.1.10. GandCrab

Actor "GandCrab" joined "Exploit" on December 18, 2017, by paying registration fees, and since then, has amassed an extremely high number of reputation points (68+) on the forum. They also earned a favorable reputation from forum members for unknown reasons. The actor currently has 442 active posts on the forum related to selling access, malware cryptos, and more. GandCrab ceased operations in 2019, and was the most prolific RaaS of its time ($2 billion net claimed).

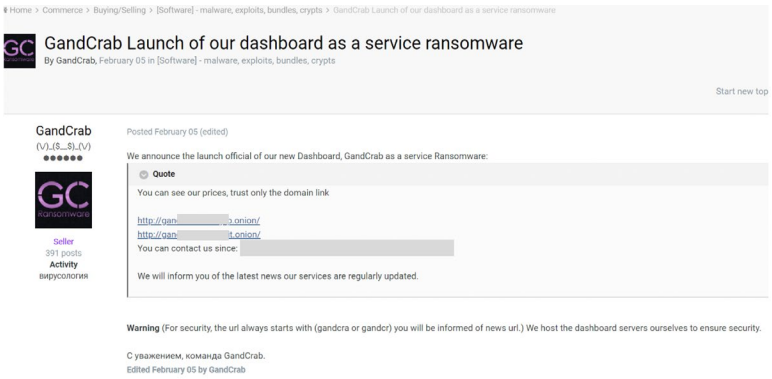

Figure 8: GandCrab forum

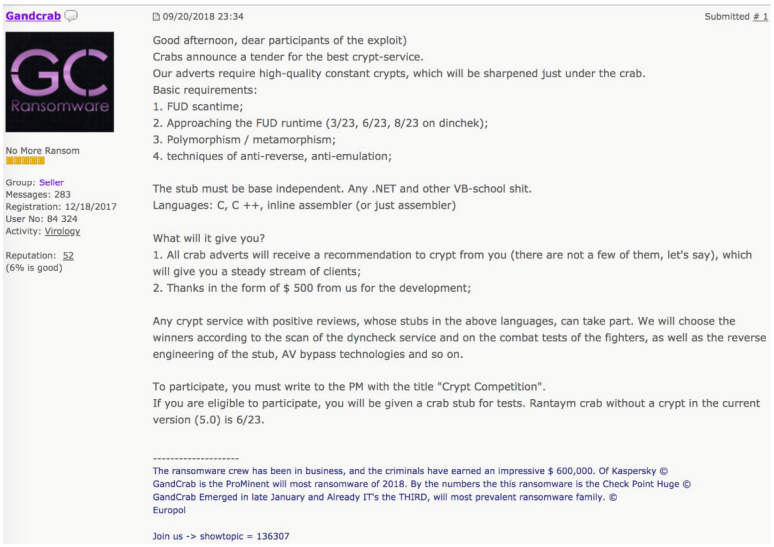

Figure 9: GandCrab forum

2.1.11. JordanConti

Actor “JordanConti” has been a member of “RAMP” since November 4, 2021. The actor has made 10 posts on the forum, including the advertisement of the RaaS program for the Conti ransomware, along with various ransomware-related discussions. The actor holds a 44+ reaction score on the forum.

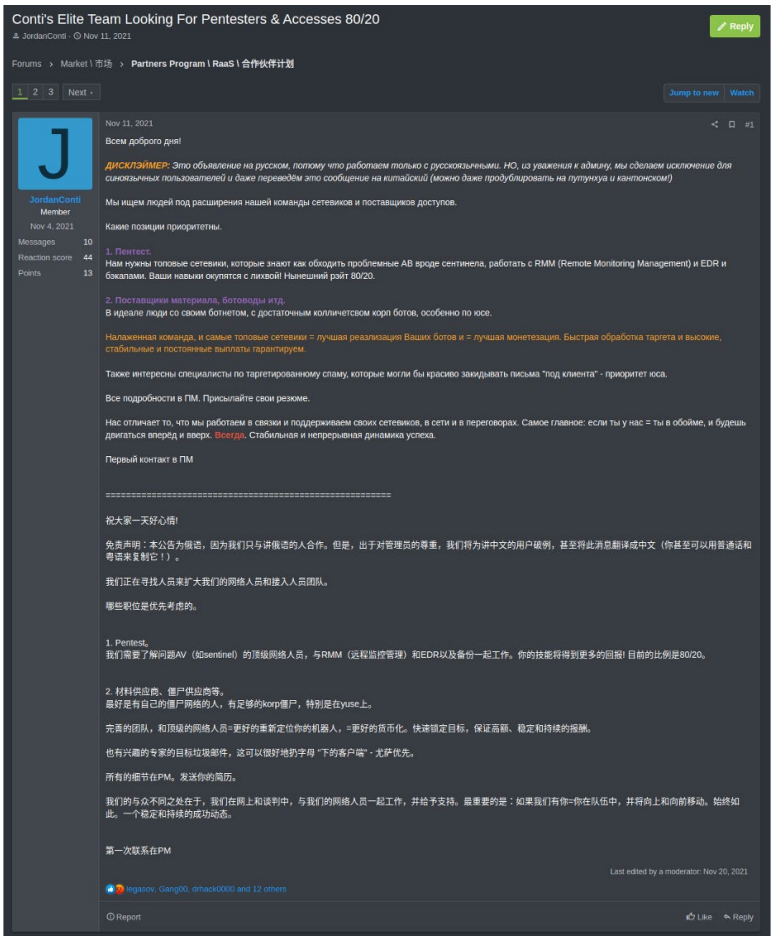

Figure 10: JordanConti forum

2.1.12. UNKN

Actor “UNKN” has been a member of the Russian cybercrime forum “Exploit” since July 4, 2019, even before paid registration began. They have an impressive number of positive reputation points (30+) on the forum. These reputation points were provided to the actor by the forum’s high, fair, and low members, including a seller and moderator, for unknown reasons. The actor has made 11 posts on the forum, mostly related to crypters, selling domains, cash-out services, and cryptocurrency. The actor is currently banned from the forum for scamming another member.

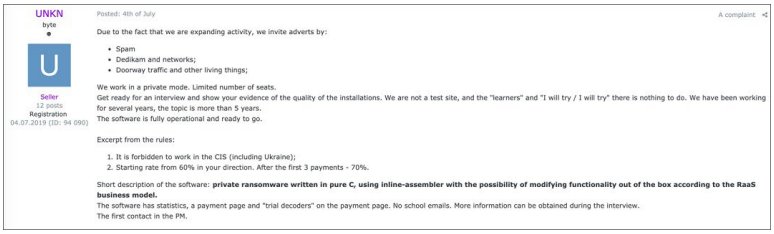

Figure 11: UNKN forum

2.1.13. Avos

Actor “Avos” is a member of “RAMP.” They joined on November 4, 2021, and have a 12+ reaction score on the forum. The actor currently has 15 active posts related to selling accesses, hiring pen-testers, and advertising the RaaS program. The actor also had a presence on the Russian language cybercrime forum “Exploit.”

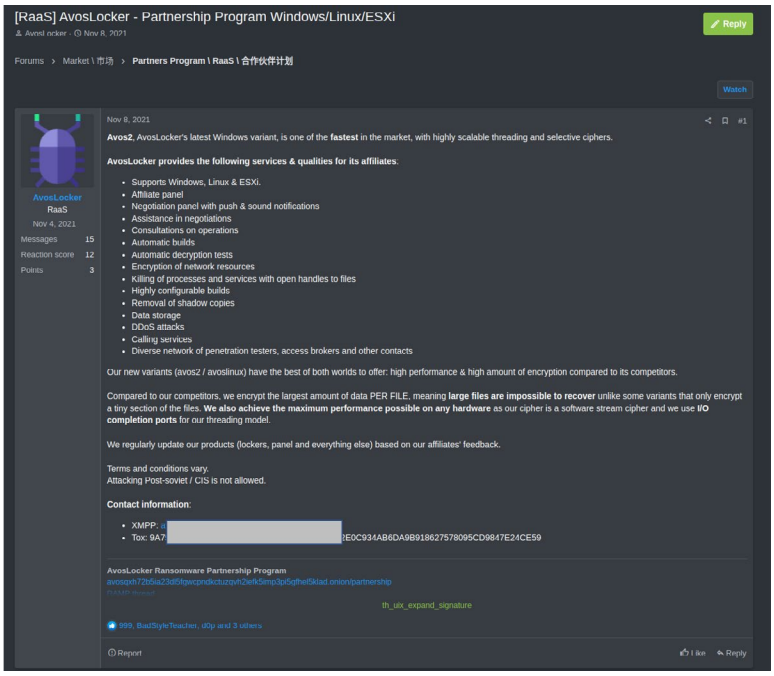

Figure 12: Avos forum

2.1.14. UNC1756

Actor “UNC1756” is a new member of “Exploit,” having only joined on March 9, 2022, without paying any registration fees. They hold a good count of reputation points (10+) provided to the actor by other forum members for being resourceful. The actor has made 47 posts on the forum related to topics such as seeking network access, hash cracking, dumping databases, vulnerabilities, exploitation, and more.

2.1.15. idk

In recent online engagements with an actor operating as “idk” on “Exploit,” the actor claimed to be an affiliate of the “Hive” ransomware group, later joining the AlphV ransomware group (2022052614925, 2022053125966, 2022060239387). Actor “idk” has been a paid member of “Exploit” since October 2021, and holds a low count of positive reputation points (2+) on the forum that were provided for being a reliable seller. The actor was recently banned from the forum for installing backdoors in the networks of organizations whose access is sold to various buyers on the forum. Based on activities observed on the forum, the actor usually uploads posts related to selling and purchasing access, malware, and subscribing to bulletproof hosting services.

2.1.16. jsworm

Actor “jsworm” is a member of “Exploit,” joining on April 30, 2019, by paying registration fees. They have a low number of reputation points (1+) on the forum. One positive reputation point was provided to the actor by a member of the forum who is a seller for being a good customer. The actor currently has 184 active posts on the forum related to RATs, stealers, malware cashing-out services, discussions on ransomware, and more.

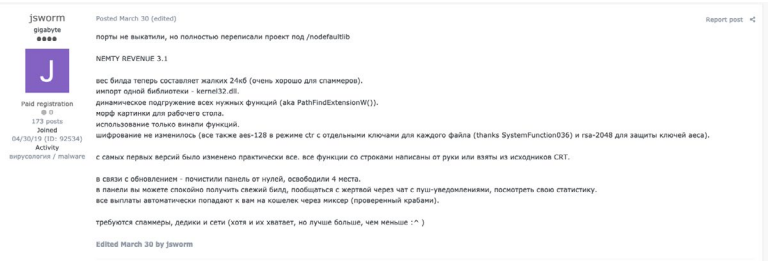

Figure 13: jsworm forum

2.1.17. Bugatti

Actor “Bugatti” became a paid member of “Exploit” in February 2019, and holds 0 reputation points on the forum. The actor made 10 posts on the forum, but they are currently inactive and have deactivated their account.

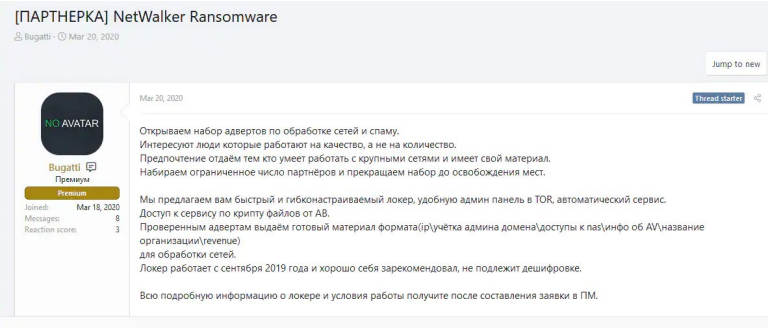

Figure 14: Bugatti forum

2.1.18. ransom

Actor “ransom” has been a member of “RAMP” since December 2021. The actor has advertised the RaaS program for the AlphV ransomware group, which was reported by FortiGuard Labs.

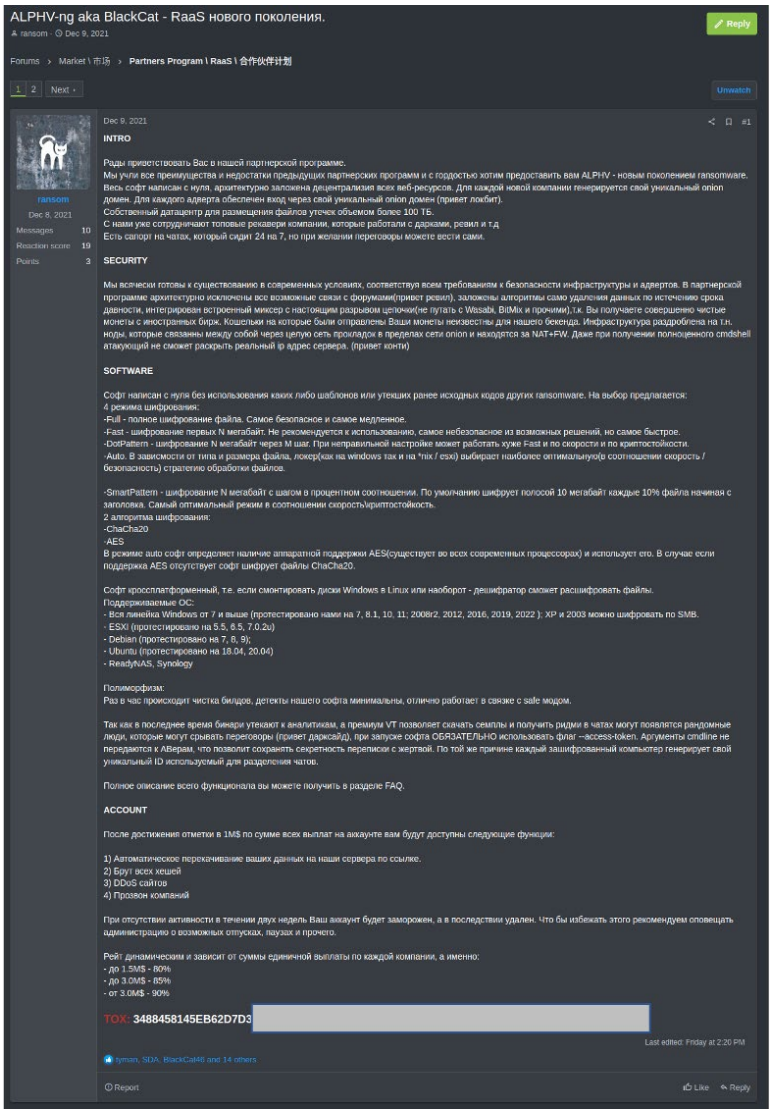

Figure 15: ransom forum

3. Key Findings and Lessons Learned

3.1. Ransomware Group Structure

In February 2022, a Ukrainian security researcher leaked over 60,000 internal chats from the "Conti" ransomware group and published them on Twitter. From those leaked chats, FortiGuard Labs found several noteworthy features that indicate that ransomware groups function in a highly systematic manner and have a structure to their operations:

- Affiliates purchase access to the networks of various organizations through network access brokers who are active in underground forums. We found a conversation between two representatives of the "Conti" ransomware group discussing the network access advertised by an actor operating as "Orangecake" on "Exploit."
- These chat logs also revealed multiple instances of words like "boss" and "chief," indicating they have a leader within their group. Approximately 10% of the users whose chats were leaked accounted for 80% of the messages sent, indicating that a handful of users play a major role in running operations. This also suggests that important decisions and strategies are concentrated within a small group.
- Based on the timestamps of the messages found in the chat logs, we observed that several "Conti" affiliates focus their efforts on a limited number of hours per day, with activity slowing between 5:00 p.m. and 12:00 p.m. and peaking between noon and 6:00 p.m. For more information, see The Affiliate's Cookbook — A Firsthand Peek into the Operations and Tradecraft of Conti.

3.2. Most Common Attack Vectors for Ransomware

Our research team found several attack vectors that ransomware actors commonly use. They include:

- Unsecured Remote Desktop Protocol (TCP/UDP port 3389) connections
- Email phishing exploit kits
- The exploitation of known software vulnerabilities
- Unsecured database services (MongoDB, Elasticsearch, MYSQL, etc.)
- Stolen credentials (third-party breaches, stealer infection)
- Weak/default passwords (brute-force attacks)

Finally, ransomware operations are becoming more sophisticated, and our research illustrates how organized they are. And as ransomware has become increasingly lucrative, the cybercrime community has continued to evolve. As a result, we can expect new and more insidious methods for extortion, data exfiltration, and disruption as attacks grow in frequency, sophistication, and profitability. RaaS has expanded the threat matrix by lowering the barrier for entry to cybercriminals, who no longer need to be particularly expert or cyber-savvy to launch an attack. Given the financial benefits and the increasing availability of the RaaS model, these threats are bound to increase. Nevertheless, organizations can still shore up their defenses against the growing risks of ransomware attacks.

4. Recommendations

4.1. Defending Against Ransomware Attacks

While ransomware targets small businesses, mid-sized companies, and large enterprises across every industry, some industries are more vulnerable than others. To help protect networks against ransomware and other cyberattacks, FortiGuard Labs recommends that organizations:

- **Continuously monitor their external attack surface to detect vulnerable, exposed assets and leaked credentials.** The discovery of externally facing assets that may be vulnerable to an attack poses a critical risk for your organization. We typically see attackers selling RDP access and databases obtained by abusing misconfigurations on web servers. Solutions such as FortiRecon service continuously monitor the external attack surfaces of organizations, enabling security admins to discover unknown/known externally exposed and vulnerable assets. In addition, the service monitors the dark web, underground and invite-only adversary forums, open-source intelligence (OSINT) sources, and more. It also detects and alerts on data/credential leaks, allowing you to respond proactively, thereby preventing or minimizing the impact of an attack. What's more, you can take advantage of FortiGuard Labs' in-depth knowledge and expertise, coupled with FortiRecon advanced technology, in acquiring leaked credentials/data on behalf of your organization, helping you take action earlier and faster against imminent cyber threats.
- **Monitor your organization's digital footprint and conduct takedowns to maintain brand integrity and protect customer trust.** We often see attackers leveraging an organization's brand reputation to deceive employees and customers into providing sensitive data/credentials via fake websites, mobile apps, or even social media accounts, which attackers then use to penetrate the organization. The FortiRecon Digital Risk Protection Service closely monitors and looks for brand-infringing domains, mobile apps, and social media accounts, and once found, can take them down at your command.
- **Implement multi-factor authentication (MFA) and strong password policy.** We continuously monitor the darknet for leaked credentials of corporate portals used by employees and regularly find them for sale on forums. You can reduce your risk from such exposure by enforcing MFA combined with a strong password policy across all user accounts.
- **Limit access rights.** Implement least privileges for all users and admins and only grant the rights they need to complete their daily tasks.
- **Make regular data backups.** Backups should be tested for malware and maintained off-site and offline, where attackers cannot access them. Demanding a ransom only works because a business has no other way to access its data.
- **Patch early and patch often.** Ransomware such as WannaCry and NotPetya relied on unpatched vulnerabilities to spread worldwide. Organizations should also lock down RDP and even turn it off if it's not required.
- **Ensure tamper protection is enabled.** Ryuk and other ransomware strains attempt to disable endpoint protection.
- **Protect your endpoints.** Even the best-trained employees occasionally make mistakes. Installing antivirus and antimalware software on computers adds an extra layer of protection, especially against phishing attacks and credential stealers. However, the best antivirus and antimalware programs are only as good as their latest version. Regularly installing patches and updates will prevent hackers from exploiting system weaknesses.
- **Replace end-of-life software.** Organizations unable to perform rapid scanning and patching of internet-facing systems should consider moving these services to mature, reputable cloud service providers (CSPs) or other managed service providers (MSPs). Reputable MSPs can patch applications such as webmail, file storage, file sharing, chats, and other employee collaboration tools for their customers.
- **Develop (and test) an incident response plan.** A robust incident response plan helps in assessing a threat and minimizing damage. Organizations should always have a fully equipped incident response team, whether staffed internally or contracted through an MSSP, and regularly run tabletop exercises to ensure readiness and refine processes and protocols.
- **Threat Intelligence.** Cyber Threat Intelligence (CTI) helps enterprises collect data about current and potential cyber risks. It also helps organizations determine whether a cyberattack can threaten their particular security environment. A Darknet Threat intelligence solution, such as FortiRecon, can also help organizations monitor darknet chatter related to the organization or data leaks that can result in financial losses before they are even made public. Such crucial and time-sensitive data can help organizations handle incidents appropriately and take all necessary legal steps.

4.2. Stolen Credentials

To protect their systems and stored data and decrease the risk of falling victim to credential stealers, such as RedLine and Vidar Stealer, organizations need to deploy an advanced antivirus solution such as FortiClient. Following is a list of Fortinet's recommendations for protecting your systems from stealer attacks:

- **Security awareness training.** End-user training is critical in helping your employees recognize and be wary of unsolicited emails and phishing campaigns, as well as suspicious social media, including messages with embedded links or file attachments that might lead to the distribution of further malicious payloads.
- **Multi-factor authentication.** MFA should always be used to reduce the effectiveness of any stolen credentials. Your organization should also mandate strong password policies for all employees.
- **Email security.** Precautions must be taken to prevent end-users from receiving potentially malicious email attachments or links, as well as configuring protocols and security controls, such as DKIM, DMARC, and SPF. Ensure your secure mail gateway can detect, label, disarm, and even remove malicious emails and attachments.
- **Abnormal endpoint behavior.** Continuously monitoring the network for abnormal endpoint behavior, such as requests to domains with a low reputation score, helps organizations detect intrusions early and take appropriate, preemptive action.

November 17, 2022 5:57 PM
1712716-A-0-EN