Ransomware as a Service Kit: A Novel Cybercrime Strategy to Monetize Victims' Data

Preeti S. Chauhan, IEEE

Nir Kshetri, University of North Carolina at Greensboro

The authors analyze how ransomware as a service has changed cybercriminals' business models. Some mechanisms to defend against ransomware-related threats are also discussed.

Ransomware involves using of malicious software (malware) to infect computers, encrypt various files, and hold the victim's data hostage.[1] The criminals then demand a ransom to return back the data. Traditionally, ransomware involved one group targeting a victim and launching an attack. Ransomware as a service (RaaS) is a new business model that makes it possible for criminals with little hacking experience to engage in cyberattacks by launching RaaS kits. Microsoft coined the industry term *human-operated ransomware* to represent RaaS since this is a human-driven threat where every action is driven by the humans including the target selection, varying the attack pattern based on the weaknesses they find on the targets. For example, the attackers can access the services running as a highly privileged account by running as domain admin. They can continue to steal the data, maximizing their payout by repeatedly monetizing the access until they are evicted.

Experienced hackers develop ransomware "toolkits" that have most or all the components needed to launch a malware attack. RaaS kits come with the malware and a list of potential targets. They also have a dashboard to track the success of ransomware campaigns. RaaS kit

Digital Object Identifier 10.1109/MC.2023.3298072
Date of current version: 20 September 2023

EDITORS
NORITA AHMAD American University of Sharjah;
nahmad@aus.edu
PREETI CHAUHAN IEEE Reliability Society;
preeti.chauhan@ieee.org

developers also provide support for ransom negotiations as well as customer service agents who advise affiliates to use the ransomware effectively. The customer service agents may also help victims buy cryptocurrency and transfer it to the hacker in exchange for a decryption key. In this way, RaaS providers function in the same manner as a technology business.[2]

The availability of do-it-yourself RaaS kits has reduced the barrier to entry to the cybercrime industry. Perpetrators no longer need deep technical expertise to engage in cybercrime activities.[3] Additionally, ransomware attacks have developed as means of double extortion where the hackers not only encrypt data on the target devices but also post or threaten to post the data publicly as a means to get additional ransom. The ransomware attackers also occasionally purchase access to networks from other cybercriminals as a part of their business model.

This article provides a perspective on the RaaS ecosystem and most popular business models. It also offers a detailed description of why RaaS kits users find it attractive to launch ransomware attacks and how they monetize victims' data.

RAAS ECOSYSTEM AND BUSINESS MODELS

A well-developed RaaS ecosystem exists on the dark web. According to a study conducted by cybersecurity company Carbon Black's Threat Analysis Unit (TAU) in October 2017, there were more than 6300 dark web marketplaces selling about 45,000 ransomware products.[4]

On the dark web, malware kits are advertised in the same way as a traditional retailer advertises products on their online stores. The kits have simple instructions that describe how criminals can configure the software.[5] The kits contain the graphics, web code, and the text that are needed to build fake websites that resemble the legitimate sites.[6]

Affiliates and initial access brokers (IABs) also play key roles in monetizing do-it-yourself (DIY) ransomware. Note that IABs have already gained access to networks and are offering to sell the access to the highest bidder.[7]

Some developers offer multiple RaaS products. RaaS developer RainMaker labs was reported to offer two solutions: 1) a sophisticated version Philadelphia for US$389, which provides a full unlimited license and options to personalize, and 2) Stampado RaaS kit for US$39, which is the cheaper version of Philadelphia. RainMaker labs sells Philadelphia on the Dark Web but hosts a video on YouTube that explains the basic practical details of the kit and different ways to customize the ransomware and a range of feature options available.[8]

RaaS kit developers also provide support for ransom negotiations as well as customer service agents who advise affiliates to use the ransomware effectively.

Hackers that have developed the RaaS kits follow a franchise-like business model. Some business models that are often implemented are: 1) subscription-based model in which the kits are sold, and 2) affiliate-based model in which the kits are rented to other cybercriminals under an affiliate program.[9] More details are provided next.

Monthly subscription for a flat fee

Carbon Black found that the prices of the DIY kits ranged US$0.50 to US$3000 with the median price of US$10.50.[4] Criminals buying the RaaS kits under subscription-based model can also enroll in a pay-per-use scheme that would allow them access to updates, new malicious versions, and other experimental features.[10]

Affiliate programs that are the same as a monthly fee model but with a percent of the profits going to the ransomware developer/operator

The affiliate programs work based on the arrangement between an operator and the affiliate. The operator develops and maintains the tools for ransomware attacks including the ransomware payloads and payment portal for the victims. Some RaaS programs also include additional services such as leak site hosting, decryption negotiation, payment pressure and cryptocurrency transactions. The operator sells these services to the affiliate who performs the actual attack and is responsible for deployment of the ransomware attack. The affiliate gains access to networks through techniques such as spear phishing, brute force attacks on remote desktop protocol (RDP) systems, exploitation of unpatched or zero-day vulnerabilities et al. They may also purchase stolen credentials from the dark web. For instance, affiliates can work with IABs. According to cybersecurity company Tenable, IABs average fees are US$303 for control panel access and US$9874 for RDP access.[7] Per Group IB's report, Qilin RaaS group pays about 80% of the ransom (if the ransom paid is US$3 M or less) to users paying to use the company's RaaS service. For ransoms above US$3M, the affiliates can get up to 85% of the paid ransom.[11]

LAUNCHING RANSOMWARE ATTACKS AND MONETIZING VICTIMS' DATA

Attackers typically deploy ransomware to whatever network is accessible to them while some carry out targeted attacks based on the expected monetization. Sometimes the affiliates may not even know the details of how the target system was compromised and are focused primarily on the monetization aspect.

Before carrying out the actual ransomware attacks, there is reconnaissance and profiling of the target to identify the approach for attack. One of the common approaches is looking for currently running security tools, identifying the privileged users and security settings defined in the Group policy and so on Depending on the data gathered from the query, the attackers deploy the ransomware and attempt to disable the security products. Often enough, even though the target's security system can detect the threat, they may or may not be able to fully evict the attacker and the attack may continue after bypassing the security controls. The most common technique to monetize the attack involves disabling the access to critical systems and bringing the system down. Cybercriminals often utilize the techniques of double extortion wherein they ask organizations to pay for the decryption key to unlock the affected files and servers plus additional payments to destroy stolen data.[12] Several ransomware organizations also have dedicated leak sites to publish data stolen from victim organizations if they refuse to pay.[13] A newer triple extortion scheme was added in 2020, where criminals demand payments from the attacked organization's customers and third parties.[14]

RANSOMWARE ATTACKS ON THE RISE: HOW TO DEFEND?

It is argued that organizations lack incentives to secure their networks, websites, and apps due to the fact that they view the costs of doing so are higher than the cost of fixing them when they are attacked. For this reason, the chances of criminals' success with low to moderate efforts are high.[15] A motivated DIY-er can make more than US$100,000 per year, which is more than many software developers employed in the legitimate industries make, especially in developing countries.[4]

Among other factors that motivate RaaS criminals is that there is a low probability that they are arrested and convicted. For instance, Russia allegedly ignores cybercrimes unless such crimes are against their national interests.[16] This is a serious issue since Russia-linked hackers were estimated to account for 74% of all proceeds associated with ransomware attacks in 2021.[17] Russian RaaS criminals are unlikely to be extradited to the United States. Moreover, if Russian cybercriminals are arrested in other countries at the request of the U.S. government, the Russian government tries to stop their extradition to the United States using a variety of techniques.[18] In several cases, Russia has pushed for extradition of the cybercriminals to Russia rather than the United States.

The key to defending against ransomware attacks lies in robust detection and mitigation technologies. The alerts could be categorized and combined to enable security hardening capabilities to address them collectively. Some techniques to address the RaaS attacks include the following:

1. Best practices in detection and defense against the ransomware attacks:
   a) discovery and identification
   b) containment and remediation
   c) recovery and communication
   d) security audits to identify potential blind spots
   e) implementation of the lessons learnt by addressing the security blind spots.
2. Data backups:
   a) maintain regular and frequent backups
   b) making multiple backups and storing them on separate devices in different locations
   c) testing backups regularly to ensure they can be retrieved.
3. Attack prevention:
   a) credential hygiene and auditing the credential exposure
   b) cloud hardening to secure system against vulnerabilities for attack by removing all nonessential components such as programs, account functions, applications, permissions, and access to reduce the routes for attacks
   c) implementation of reliable and modern endpoint protection that can work on advanced algorithms and works automatically in the background around the clock
   d) implementation of advanced anti-phishing protection.
4. In case of an attack:
   a) taking measures to reduce the attack surface

> Attackers typically deploy ransomware to whatever network is accessible to them while some carry out targeted attacks based on the expected monetization.

    b) segmenting the network to hinder proliferation across the environment.
5. Invest in user training and build a culture of security.

HOW WILL THE FUTURE OF RAAS LOOK LIKE?

RaaS owners continue to evolve their methods (business models) due to the enhanced focus on preventing these attacks. As the governments, law enforcement agencies, and security researchers continue to collaborate on identifying and apprehending the ransomware groups, the bad actors are being forced to up their game. Below are some of the potential paths of evolution of RaaS.[19]

ATTACKS ON CLOUD ENVIRONMENTS

With the continued movement to cloud services, the attackers may shift their focus to target cloud infrastructure and platforms to expand their ransomware business. The attackers may develop the RaaS models for cloud environments and create new forms of attack tailored to the cloud application.

STOCK MARKET MANIPULATION

The ransomware groups can do something like "short and distort" which is illegal manipulation of the stock market. The attackers can get access to a company's sensitive information in the data scanning phase. They short sell the company's securities in this timeframe, launch an attack to disrupt the company's operations, and delay the announcements related to the attack, causing the company stock price to go down. They then buy the stock option causing losses of millions of dollars to the company's shareholders even for very short-lived attacks and breaches.

SUPPLY CHAIN COMPROMISE

Supply chain is another area where RaaS can create disruptions by blocking out services; the impact here could be much wider due to the connected nature of supply chain where the same services are accessed by multiple customers. Companies often outsource the software needs to the supplier companies. By blocking these suppliers and disrupting the supply chain, ransomware criminals can maximize the extortion depending upon the blast radius of the software user base.

REFERENCES

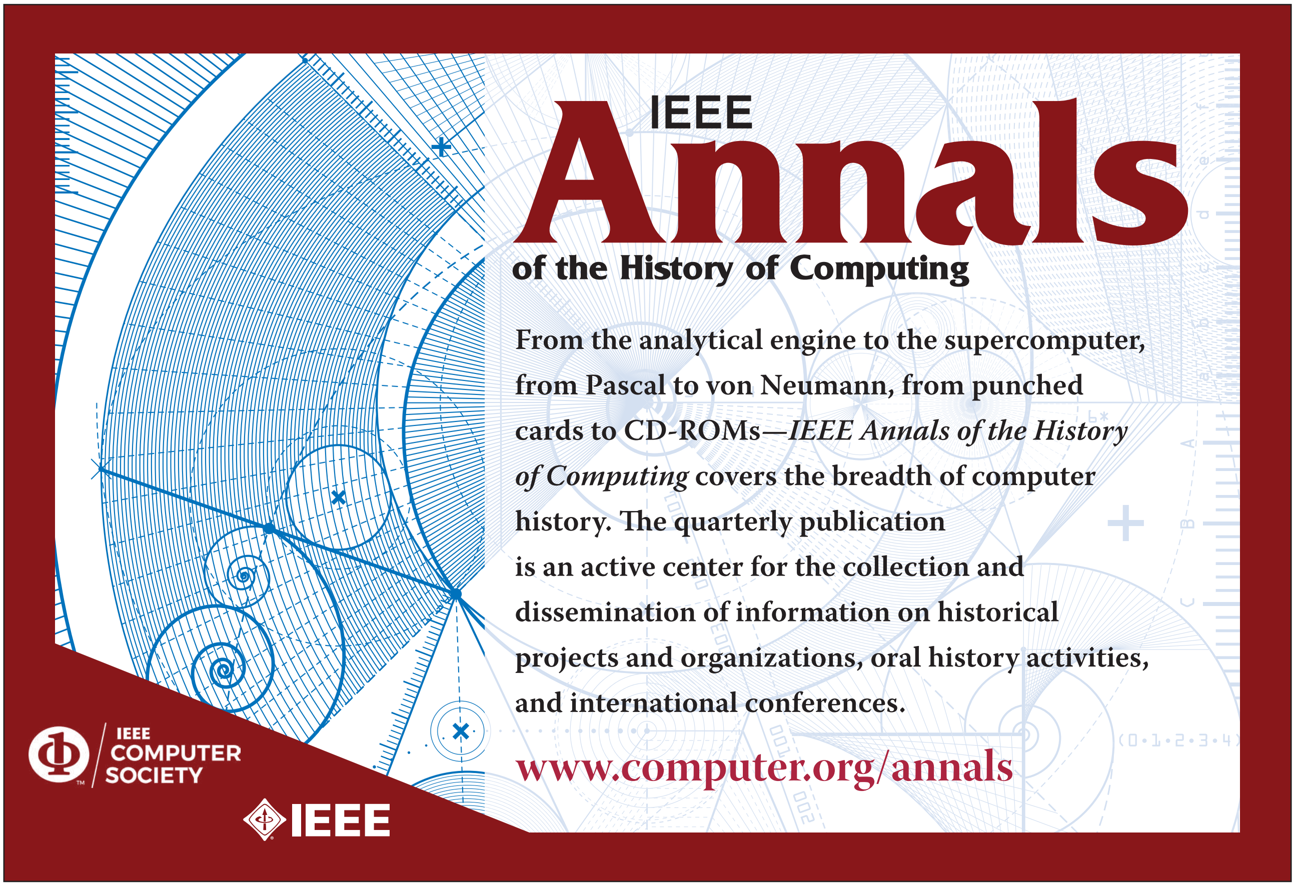
1. K. Baker, "Ransomware as a service (RaaS) explained how it works & examples," *CrowdStrike*, Jan. 2023. Accessed: Jul. 14, 2023. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
2. K. D. Schwartz, "Ransomware, at your service," *ITPRO Today*, Dec. 2022. Accessed: Jul. 14, 2023. [Online]. Available: https://www.itprotoday.com/vulnerabilities-and-threats/ransomware-your-service
3. "Ransomware attacks fracture between enterprise and ransomware-as-a-service in Q2 as demands increase." Coveware. Accessed: Jul. 14, 2023. [Online]. Available: https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report
4. S. Sjouwerman. "Carbon black says ransomware kit sales on the dark web shoot up 2,502%." KnowBe4. Accessed: Jul. 14, 2023. [Online]. Available: https://blog.knowbe4.com/carbon-black-says-ransomware-kit-sales-on-the-dark-web-shoot-up-2502
5. *DIY Kits for Sale on Dark Web Spark Rise of Ransomware-as-a-Service*. (Mar. 2017). Naked Security. [Online]. Available: https://nakedsecurity.sophos.com/2017/03/20/diy-kits-for-sale-on-dark-web-spark-rise-of-ransomware-as-a-service/
6. "Script Kiddie Bonanza – Do-it-yourself phishing kits!" Bill Mullins' Weblog. Accessed: Jul. 14, 2023. [Online]. Available: https://billmullins.wordpress.com/2008/06/23/script-kiddie-bonanza-do-it-yourself-phishing-kits/
7. "Tenable research reveals 'do-it-yourself' ransomware kits have created thriving cottage industry of cybercrime." Tenable. Accessed: Jul. 14, 2023. [Online]. Available: https://www.tenable.com/press-releases/tenable-research-reveals-do-it-yourself-ransomware-kits-have-created-thriving
8. *5 Ransomware as a Service (RaaS) Kits – SophosLabs Investigates*. (Dec. 2017). Naked Security. [Online]. Available: https://nakedsecurity.sophos.com/2017/12/13/5-ransomware-as-a-service-raas-kits-sophoslabs-investigates/
9. "Ransomware-as-a-service (RaaS): How it works." Fortra. Accessed: Jul. 14, 2023. [Online]. Available: https://www.tripwire.com/state-of-security/ransomware-service-raas-works
10. V. Unterfingher. "Ransomware-as-a-service (RaaS) – The rising threat to cybersecurity." Heimdal. Accessed: Jul. 14, 2023. [Online]. Available: https://heimdalsecurity.com/blog/ransomware-as-a-service-raas/
11. J. Burt, "Ransomware-as-a-service groups rain money on their affiliates," *The Register*, May 2023. Accessed: Jul. 14, 2023. [Online]. Available: https://www.theregister.com/2023/05/17/ransomware_affiliates_money/
12. D. Carmack, "What we know about darkside, the Russian hacker group that just wreaked havoc on the east coast," Heritage Found., Washington, DC, USA, 2019. [Online]. Available: https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hacker-group-just-wreaked-havoc
13. D. Palmer, "Have we reached peak ransomware? How the internet's biggest security problem has grown and what happens next," *ZDNet*, Jun. 2021. Accessed: Jul. 14, 2023. [Online]. Available: https://www.zdnet.com/article/have-we-reached-peak-ransomware-how-the-internets-biggest-security-problem-has-grown-and-what-happens-next/
14. N. Kshetri and J. Voas, "Ransomware as a business (RaaB)," *IT Prof.*, vol. 24,

no. 2, pp. 83–87, Mar./Apr. 2022, doi: 10.1109/MITP.2022.3157208.

15. P. Gillin, “The grim state of cybersecurity: It’s awful, and it’s only going to get worse,” *SiliconANGLE*, Apr. 2018. Accessed: Jul. 14, 2023. [Online]. Available: https://siliconangle.com/2018/04/14/grim-state-cybersecurity-awful-going-get-worse/
16. N. Kshetri, *Cybersecurity Management: An Organizational and Strategic Approach*. Toronto, ON, Canada: Univ. of Toronto Press, 2021.
17. “74% of ransomware revenue goes to Russia-linked hackers,” *BBC*, Feb. 2022. Accessed: Jul. 14, 2023. [Online]. Available: https://www.bbc.com/news/technology-60378009
18. D. Volz and F. Schwartz, “Russia steps up efforts to shield its hackers from extradition to U.S.,” *Wall Street J.*, Nov. 2019. Accessed: Jul. 14, 2023. [Online]. Available: https://www.wsj.com/articles/russia-steps-up-efforts-to-shield-its-hackers-from-extradition-to-u-s-11572949802
19. F. Hacquebord, S. Hilt, and D. Sancho, “The future of ransomware,” *Trend Micro*, Dec. 2022. Accessed: Jul. 14, 2023. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-future-of-ransomware

PREETI S. CHAUHAN is a technical program manager at Google, Sunnyvale, CA 94089 USA. She is a coeditor of the “Data” column for *Computer*. Contact her at preeti.chauhan@ieee.org.

NIR KSHETRI is a professor at the Bryan School of Business and Economics, University of North Carolina at Greensboro, Greensboro, NC 27412 USA. He is the “Computing’s Economics” column editor of *Computer*. Contact him at nbkshetr@uncg.edu.



Digital Object Identifier 10.1109/MC.2023.3306190