AIP Conference Proceedings

RESEARCH ARTICLE | JUNE 05 2024

The challenges of cyber space with crime-as-a-service (CAAS) to amateur attackers FREE

Kothakonda Chandhar ✉; Shashikanth Kandukuri; Jangalapelli Shiva; Achi Sandeep

AIP Conf. Proc. 2971, 020072 (2024)
https://doi.org/10.1063/5.0195769

AIP Publishing

The Challenges of Cyber Space with Crime-as-a-Service (CAAS) to Amateur Attackers

Kothakonda Chandhar[1, a)], Shashikanth Kandukuri[2], Jangalapelli Shiva[3] and Achi Sandeep[4]

[1] School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India.
[2]J.S University, Shikohabad, Firozabad, UP, India .
[3] Department of Computer Science & Engineering, VITS, Karimnagar, TS, India.
[4]Computer Science & Engineering, Sri Indu College of Engineering & Technology, Sheriguda. Hyderabad, TS, India.

[a)] Corresponding author: chandu19024@gmail.com

Abstract. Phishing is a type of attack that is often used to steal user data, including personal login credentials, debit cards, or credit card numbers. For hackers, phishing is an easy way to find and track any person's information or company data. In general, an effective phishing campaign requires a well-prepared cybercriminal with technical expertise and social engineering knowledge. However, with the rise of CaaS (Crime-as a-Service), anyone can become an expert in phishing for a little charge. CaaS vendor offer everything the amateur attacker needs to make their own effective phishing attack, from point-by-point target records to marked email formats. Intruders can even pay amount for access to compromised servers to conceal their tracks all the more without any problem. By eliminating large number of barriers to entry, this type of trend has made it simple to make a compelling phishing attack. And that is a major issue for the associations being targeted.

INTRODUCTION

When a expert perpetrator or institution of offenders expand superior tools, “kits” and different packaged offerings that are provided up on the market or lease to different criminals who're typically much less experienced. Day to day, the Cyber terror has increased tremendously in acceleration and degree, with cyber criminals gaining every new activity to grow and prosper. Couple with the surprising rise in the worldwide pandemic and remote running in the third party space, and you have opened the entry to unlimited novel vulnerability [1, 2].

The possibility of that new susceptibility is fetching out much fewer skilled danger performers coming into the distance in expectation of smooth refunds, even as extra pro risk performers find a possibility for CaaS (Crime-as-a-Service). This is in which expert risk actors and offender companies expand superior equipment and packaged offerings to promote to other, commonly much less skilled, criminals to assist them perform typical cyber-attacks [3,4].

A narrow access partition being the reason:

the price of illegal activity is pooled primarily entirely on the basis of a subscription or flat-price fee per version in the way of all customers, making cybercrime offers easier and more attractive. in this scenario, provider companies need to increase their revenue, while at the same time customers profit from the actual reduction in the phrase of the rate and control the illegal trade of information [5,6].

International Conference on Research in Sciences, Engineering, and Technology
AIP Conf. Proc. 2971, 020072-1–020072-8; https://doi.org/10.1063/5.0195769
Published by AIP Publishing. 978-0-7354-4866-7/$30.00

As per the internet organized crime threat assessment(iocta) 2020[3,4] record made available by europol commodity, the malware service (malware-as-a-service (maas)) reduces the barrier to risk actors setting up cyber attacks [7,8].

Important examples of malware presented in this version are Emotet and Trickbot:

These malware programs use unit based systems that allow their key differentiators to resell and rent out portion of their suspicious code to their counterparts without conciliation. Users of malware workers need to unleash their personal strategies, techniques and tactics and use them in specially focused attacks in some cases.

Authorities and law enforcement agencies are warning internationally about the rapid professionalization of the cybercrime risk panorama that makes the CaaS[5,7] version so risky. Few unlawful groups have particularly focused on customers and agencies with their means of delivering criminal products and services to various criminal gangs without delay [9,10].

“Simultaneously, European regulation enforcement has stated a increase in much less tech-savvy cyber criminals in the context of expensively exist CaaS Solutions” – reads the IOCTA releases.

“There was a visible change from what used to be a threat actor business, but now it’s a more business. It requires specialized skills (malware encryption, malware distribution, etc.) if the criminal can hire a developer or consultant to meet this need”.

Using complex attacks, criminals challenge the ability of law enforcement to investigate the cases in depth and attribute attacks to groups of criminals or a specific criminal. The CaaS service is easy to find in Cyber offence groups and markets run on the Dark Web and offering a wide variety of offers. Scammers can borrow botnet by paying in Bitcoin. Thousands of infected machines are used worldwide for all types of criminal services such as spreading malware, initiating DDoS attacks and sending spam emails. One other factor that makes Crime-as-a-Services more attractive as an alternative to crime is the availability of stolen data used for subsequent attacks [11,12].

As the popularity of crime-a-a-service grows, it is important for companies to understand what actions to do for protecting their organization information themselves. Specifically, few of the majority accepted types of CaaS have been defined, which includes:

- Phishing
- Smishing
- Vishing
- Exploit kits
- DDoS
- Ransomware-as-a-Service
- Research-as-a-Service
- Digital Currency

"Crime ware-as-a-Service (or Cybercrime as a Service) enables both technically inexperienced criminals and advanced threat actors to quickly coordinate advanced attacks.”

The term CaaS(Crimeware-a-Service or Crime-as-a-Service) refers to the implementation of a cybercrime environment to provide services and products to various cybercriminals. This version is useful for cybercriminal game and allows criminals to carry out complex attacks without the need for good technical skills.

CaaS[3] represents the most effective desire for good attackers who need to lower the barriers to entry for newer and less informed attackers and perform offensive operations. In the Crimeware-as-a-Service version, it is very complex to identify the crime of the selected character as the method and infrastructure are shared among many terrible actors [13,14].

Cyber threats are evolving at unprecedented speed and volume. Cybercriminals have taken full advantage of the latest skills to develop and prosper, which, combined with the pandemic and significant growth in remote painting and cloud access, has opened the door to new vulnerabilities. If there's one factor that drives the terrible actor's movements, it's the ability to strike [15,16].

Less-skilled danger actors are coming into the distance in hopes of clean returns; however, an excellent larger undertaking is how speedy those skilled experts interact in crime-as-a-service (CaaS)[3,7]. These expert people and crook groups are growing superior gear and packaged offerings after which promoting them to different criminals who're typically much less skilled. These hackers can then perform complicated assaults at preferred scale and on decided on victims. Monitoring for those threats is the undertaking that groups, governments, and their safety groups conflict on a day by day basis. The first step to addressing the problem is knowing the maximum not unusual place and trending CaaS offerings. The six maximum not unusual place CaaS offerings include [17].

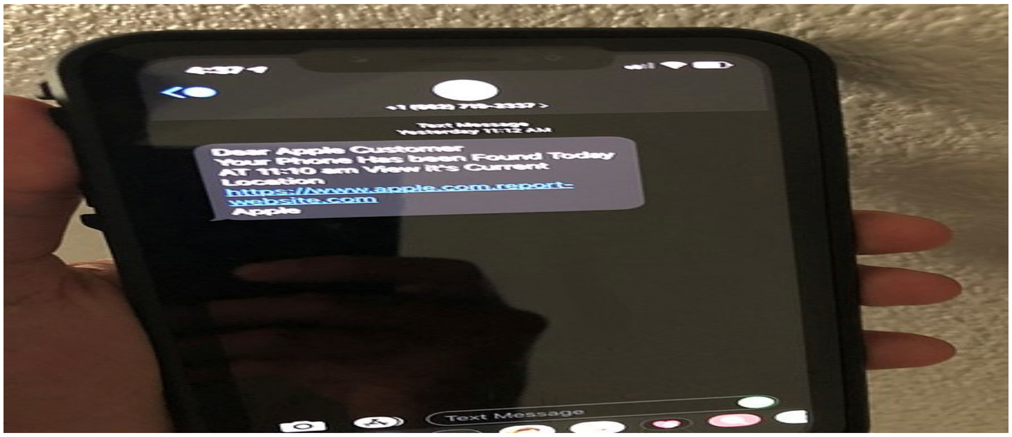
Phishing

It remains one of the top attack vectors used to compromise organizations [2], so it's no surprise that shipments of these capabilities have dramatically increased. Phishing kits and phishing platforms are available on the dark web for cheap (around $10) to facilitate attacks on companies. Furthermore, with little knowledge or skill required, these toolkits and platforms are highly customizable and have varying degrees of automation, making them very attractive to criminals

FIGURE 1. Phishing

Smishing

Smishing[6] is a phishing SMS in which an attacker tricks a user into sending a text message and impersonates a trusted source to steal the user's sensitive information. The level of trust users have in their smart devices has led attackers to launch a variety of mobile security attacks, including smishing attacks. Various reports clearly show that smishing attacks have increased significantly in recent years. This article provides a new framework for detecting smishing attacks. This model uses a naive Bayes classifier to filter text messages. Furthermore, the proposed model analyzes the content of text messages and extracts the words commonly used in the refinement of messages. Since SMS text messages are very short and are usually written in the Lingo language, we have used text normalization to convert the messages to a standard format for better functionality.



Dear Apple Customer
Your Phone Has been Found Today
AT 11:10 am View it's Current
Location
https://www.apple.com.report-website.com
Apple

FIGURE 2. Sample SMS Smishing

Vishing

Vishing in one of the electronic frauds often called as voice phishing. A Vishing[10] attack can be conducted by smart phone or voice call. In which individuals are tricked over the phone to revealing personal information or financial information to unauthorized entities. With the proliferation of smart phones, tablets, and hotspots, social engineering attacks on smart phones are now common place. Voice phishing relies on personal trust in telephone services. This is because targets tend to overlook potential scammers who perform this type of scam using techniques such as caller ID spoofing and highly automated systems[7,10]. However, as the profits of traditional phishing attacks continue to decline, scammers are looking for ways to use voice phishing to retrieve users' financial account numbers, passwords, and other personal data.

FIGURE 3. Vishing Scam

Exploit Kit

Exploitation involves developing code and tools to exploit known vulnerabilities. One of the most popular toolkits, RIG can cost up to $150 per week to spread ransomware, Trojan horses, and other types of malware. There is a vast network of dealers with complex business structures that facilitate criminals. However, marginal prevalence has declined since 2016 due to increased automatic browser updates and decreased use of Flash..

DDoS Service

Criminal groups no longer need to create botnets to launch attacks against targets. Today, they can hire these services on demand. The time required to launch an attack is minimal, and the infrastructure can be turned on and off quickly and efficiently, making monitoring and mitigation even more difficult. Decentralized denial of service (DDoS) -based services are also cheap and accessible [11], and many vendors offer subscriptions on the dark web. For example, the cheapest plan is $4 per month, with simultaneous attacks with an attack time of 310 seconds. The most expensive plan is $62 per month and simultaneous attacks are 10,900 seconds. All of this makes DDoS services particularly dangerous given the ease of deployment and benefits to criminals. Some estimates show a profit of up to 96% per attack.

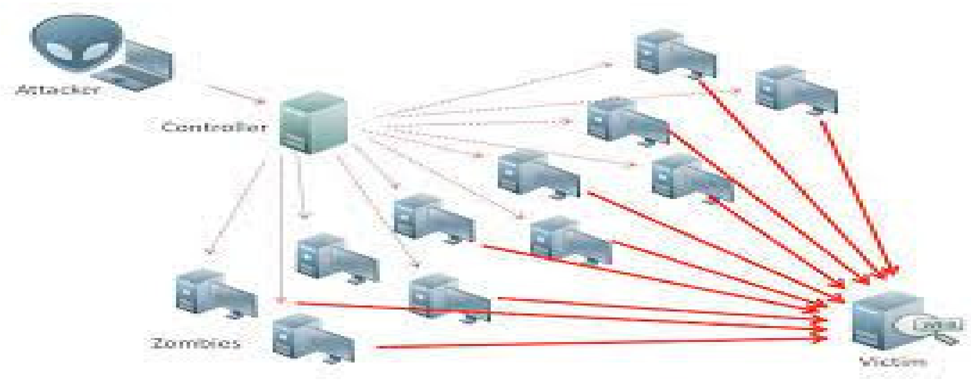


Figure 4. DDoS as Service

3.6. Ransomware-as-a-Service (RaaS)

Like DDoS, cybercriminals can use specialized ransomware [11,12] offerings to goal victims, lowering the want for a whole lot of technical understanding. those services no longer handiest provide technical know-how and information, however additionally all of the facts had to launch an attack. RaaS is available in a selection of pricing and price models, inclusive of subscription, fixed price, or earnings sharing. amounts variety from $zero to thousands of dollars for big lenses.

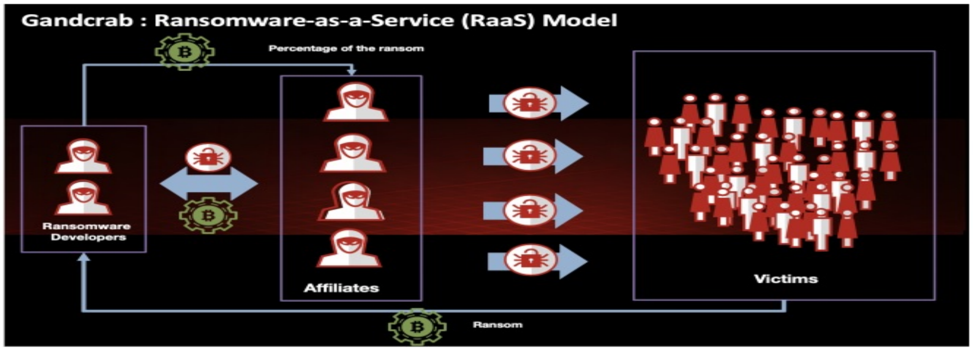


FIGURE 5. Ransomware-as-a-Service (RaaS) Model

Research-as-a-Service

This includes legal or illegal information collected about targeted victims and resale of stolen personal or organization data as compromised logins. It may also include the sale of information related to the operation of software or systems.

07 June 2024 09:05:21

FIGURE 6. Research–as–a-Service Model

Digital Currency

Crypto currencies are a widely used method of sending and collecting money by cyber criminals anonymously, ease of use, lack of borders and preventing criminals from using traditional banks. Hard to do. Crypto currency accounts generally do not require users to provide personal information and location, but allow the use of multiple accounts at once.

FIGURE 7. Digital Currency

"The most common products and services offered by Crime ware-as-a-Service chain are malware, ransom ware, phishing toolkits, and command and control infrastructure."

Lessons from the Banking Industry

The subsequent step is to consciousness on what is regularly said as opposed to honestly on collaboration. we've got visible desirable examples of cybersecurity teams operating greater closely with other insiders, in particular in banking. some of essential united kingdom and ecu banks operate inside an industry structure wherein financial and cybercrime groups were part of the equal business unit for over a decade, way to strong natural synergies among those capabilities. this is it. this is a big step forward. With the aggregate of cybercrime and financial crime corporations, integrated hubs are rising within the enterprise, which can be visible as an more suitable model of the security operation center [5,7] (SOC) control model, bringing together unique crook organizations together with fraud. industry.. Putting these units together makes it possible for organizations to raise awareness of the situation, share intelligence and threat analysis more easily, improve the ability to attract talent and have a standardized procedural framework.

Cybercrime Establish an end-to-end operating model and facilitate collaboration and integration of threat-related actions, which can more effectively disrupt illegal economies by fighting and increasing governance transparency. Another benefit of the integration center is the elimination of resources that overlap with undetected workforce. This improves efficiency and reduces costs.

CONCLUSION

Unfortunately, there is no definitive solution to reduce the risks associated with implementing the CaaS model. This model work requires a holistic approach and constant sharing of information by security agencies and law enforcement agencies. Security professionals monitor hacking and cybercrime forums, especially those hosted on the Darknet, which need to quickly identify new threats, share information quickly to identify them, and limit the risk of cyber-attacks. Early detection of threats allows experts to share evidence of intrusion in order to detect and mitigate attacks, while law enforcement agencies identify the potential infrastructure for scammers to identify products and services that you may be trying to shut down.

REFERENCES

1. Shashikanth K, Gangadhara Srikanth, Chandhar Kothakonda, “Cybersecurity Trends in information Technology and Emerging Future Threats”, Sambodhi, 43(03), (2020).
2. Rana Alabdan Department of Information Systems, College of Computer and Information Sciences, Majmaah University, Majmaah 11952, (2020).
3. Bens Book of the Month Review of Social Engineering the Science of Human Hacking” RSA Conference Retrieved, (2020).
4. Larson, Selena, “Hacker creates organization to unmask child predators” CNN retrieved 14, (2019).
5. Shashikanth Kandukuri, Srikanth Gangadhara, “A Research Paper on Social Engineering and Growing Challenges in Cyber Security”, Think India Journal, 22(41), (2019).
6. Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark; Stavroulakis, Peter (eds.). Handbook of Information and Communication Security. Springer, (2010).
7. Dunn, John E. "Ransom Trojans spreading beyond Russian heartland". TechWorld. Archived from the originalon, (2012).
8. M Sheshikala, Sallauddin Mohmmad, D Kothandaraman, Dadi Ramesh, Ranganath Kanakam, Emotion Recognition Based on Streaming Real-Time Video with Deep Learning Approach, Computer Communication, Networking and IoT, Springer, Singapore, 2023, pp. 393-401
9. D Kothandaraman, C Chellappan, Node Rank Based Energy Efficient Routing Algorithm for Mobile Ad-hoc Network, International Journal of Computer Networks & Communications (IJCNC), 11, 45-61, (2019)
10. D Kothandaraman, C Chellappan, Human Activity Detection System using Internet of Things, International Journal on Computer Science and Engineering, 9(11), 657-665, (2017).
11. Balasundaram, A., Ashokkumar, S. and Kothandaraman, D,. SeenaNaikkora. In E Sudarshan and A Harshaverdhan, “Computer vision based fatigue detection using facial parameters, IOP Conference Series: Materials Science and Engineering”, 981(2), 2020, pp. 022005.
12. S Magesh Kumar, V Auxilia Osvin Nancy, A Balasundaram, D Kothandaraman, E Sudarshan, Innovative Task Scheduling Algorithm in Cloud Computing, IOP Conference Series: Materials Science and Engineering, 981(2), pp. 022023.
13. Yerrolla Chanti, Seena Naik Korra, Bura Vijay Kumar, A Harshavardhan, D Kothandaraman, New Technique using an IoT Robot to Oversight the Smart Domestic Surroundings, Studia Rosenthaliana (Journal for the Study of Research), issue. 0039-3347, 2019.
14. Ravi Kumar, R., Mohmmad, S., Shabana, Kothandaraman, D., Ramesh, D, “Static Hand Gesture Recognition for ASL Using MATLAB Platform, Computer Communication”, Networking and IoT. Lecture Notes in Networks and Systems, Springer, Singapore, 459, (2023).
15. Griffin, Slade E.; Rackley, Casey C. "Vishing". Proceedings of the 5th Annual Conference on Information Security Curriculum Development – InfoSecCD, (2008).

16. Taghavi Zargar, Saman ″A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks″, (2013).
17. Ben-Porat, U. Bremler-Barr, A., Levy, H. "Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks", IEEE Transactions on Computers. **62** (5), 1031–1043, (2013).