Common Vulnerabilities and Exposures in the Cloud

Aftab Hussain
University of California, Irvine
Irvine, California, USA

Anton Burtsev
University of California, Irvine
Irvine, California, USA

ABSTRACT

In this short report, we describe some vulnerabilities and exposures in the cloud, discussing some exploits between 2015 to 2018. We namely discuss two categories of attacks – social engineering attacks and cryptomiming attacks.

ACM Reference Format:
Aftab Hussain and Anton Burtsev. . Common Vulnerabilities and Exposures in the Cloud. In *University of California, Irvine (Report).* ACM, New York, NY, USA, 3 pages. https://doi.org/xx.xxxx/nnnnnnn.nnnnnnn

1 SOCIAL ENGINEERING (SE) ATTACKS

Due to the openness of a cloud computing system, in particular, its accessibility from multiple points, social engineering (SE) attacks have become very common [31]. A famous example is the attack on Ubiquiti Networks, a San Jose based American service provider of high-performance networks for businesses. In 2015, it was a victim of a SE attack [17] that resulted in a loss of 39.1 million dollars. Another famous case is the hack of Wired editor Mat Honan's Apple iCloud account in 2012 [16].

In this section, we focus on the goals of SE attacks and the technical means used to achieve them. To know about the psychological aspects of SE attacks, the reader may refer to [21]. In Subsection 1.1, we briefly describe SE attacks and discuss a particular type of attack typically delivered via SE: ransomware attacks.

1.1 SE Attack Description

SE attacks are attacks that trick people into divulging confidential information for various malicious goals, such as black-mailing, which existed even before the emergence of cloud computing (or even computing itself) [26, 30].

In the computing realm, SE attacks are achieved by baiting users into downloading an attachment or clicking a link which directs them to installing malware in their machines [14, 25]. Typically, these malware links are delivered to the users via fradulent emails or social media ([21]).

A common class of malware delivered by SE attacks is ransomware, programs that encrypt and hold victim's data for ransom. In May 2007, the WannaCry ransomware attack had infected thousands of Windows machines [19]. It exploited a vulnerability in the Windows implementation of the Server Message Block (SMB) protocol [5]. The SMB protocol helps various nodes on a network to communicate, i.e. share files, printers, serial ports, and communications abstractions such as named pipes and mail slots [27]. It is a client-server request-response protocol where servers make the resources available to clients, who connect to the servers using TCP/IP, NetBEUI or IPX/SPX protocols. The exploit allowed Microsoft's implementation to be tricked by specially crafted packets into executing arbitrary code. In 2017, ransomware attacks have been widespread, which targeted institutions like United Kingdom's National Health Service, San Francisco's light-rail network, and big companies such as FedEx [20].

The MIT Press review predicts ransomware to be among the biggest threats to cloud computing in 2018, given the increasing sizes of data that users store in the cloud [20].

Report, July 2020, Irvine, California, USA
. ACM ISBN xxx-x-xxxx-xxxx-x/YY/MM…$0
https://doi.org/xx.xxxx/nnnnnnn.nnnnnnn

2 CRYPTOMINING ATTACKS

According to security firm Malwarebytes, malicious cryptomining (or cryptojacking) has been the top cyber criminal activity detected since September 2017 [9, 35]. A Symantec report found that cryptojacking surged 8,500% in the fourth quarter of 2017 [29].

In itself, cryptomining is a legal activity: generating digitial currencies (e.g. Bitcoin, Monero, Zcash, Ethereum) in exchange for performing complex, resource-intensive, blockchain transaction verifications on a computer [34]. A blockchain is a linked list of records or blocks, where each block consists of a cryptographic hash of the previous block, a timestamp, and transaction data [22]. (For details on how blockchain transaction verification works, see [24].) Cryptomining has been widely popular recently, primarily driven by the increasing prices of some crypto currencies. However, the high profitability also led to a rise of an illegal form of the activity.

In this section, we first briefly explain malicious cryptomining and its dangers (Subsection 2.1). Then we present the vulnerabilities behind some recent cryptomining attacks that gained much attention in the cybersecurity community: the attack on Tesla's Kubernetes consoles (Subsection 2.2), the Jenkins attack (Subsection 2.3), and the Oracle WebLogic Server attack (Subsection 2.4), all of which occurred in 2018.

2.1 Malicious Cryptomining

Malicious cryptomining is the practice of stealing cloud compute resources to mine cryptocurrency [33]. Symantec reported that such activities also increasingly target IoT (Internet of Things) devices [29]. Malwarebytes's recent report [9] mentions that under the disguise of a financially motivated attack, such attacks could be the "perfect alibi for advanced threat actors".

On one hand, unmanaged cryptocurrency miners could seriously disrupt business or infrastructure-critical processes by overloading systems causing them to become unresponsive and shut down. On the other hand, performance of compromised machines can be controlled by criminals warding of any suspicion from the owners of the machines.

Talos, a CISCO security group, reported that when installing mining software, some criminals limit CPU usage and the number of cores being used to ensure users don't notice any obvious performance hit as result of mining software running on their systems [23]. The report claims victims could indefinitely remain part

of the adversary botnet, a network of automated scripts or malware-compromised machines (bots) that run over the Internet [32].

2.2 Tesla Attack [4, 11]

Vulnerability. In 2017, RedLock Cloud Security Intelligence (CSI) team found hundreds of Kubernetes administration consoles accessible over the internet without any password protection. Kubernetes [10] is an open source system for managing containerized applications across multiple hosts that provide basic mechanisms for deployment, maintenance, and scaling of applications. Containerized applications are becoming widely popular, particularly due to the cost benefits they provide by allowing multiple applications to be distributed across a single host operating system, obviating the need to set up virtual machines for each individual application [18].

We believe the above mentioned vulnerability in Kubernetes to be the following entry in the MITRE database [7], where it is described as follows:
"Default access permissions for Persistent Volumes (PVs) created by the Kubernetes Azure cloud provider in versions 1.6.0 to 1.6.5 are set to "container" which exposes a URI that can be accessed without authentication on the public internet. Access to the URI string requires privileged access to the Kubernetes cluster or authenticated access to the Azure portal."

In February 2018, one of Tesla's Kubernetes consoles was compromised by hackers [11]. Access credentials were exposed to Tesla's Amazon Web Services (AWS) environment which contained an Amazon S3 (Amazon Simple Storage Service) bucket that had sensitive data.

Attack Method. The hackers used mining pool software that configured a malicious script to connect to an "unlisted" or semi-public endpoint. The true IP address of the mining pool server was hid behind CloudFlare a free content delivery network (CDN) service. By registering for free CDN services, the hackers were able to use new IP addresses on-demand. The hackers deployed a Stratum bitcoin mining protocol based cryptojacking operation on Tesla's AWS server. The issue has since been rectified after it was reported to Tesla by the RedLock CSI team.

2.3 Jenkins Attack [4]

Vulnerability. Only a few days prior to the news of the Tesla attack, JenkinsMiner, a hybrid remote access trojan and XMRig miner reportedly started targeting vulnerable Jenkins servers. Jenkins [1] is a popular open source automation server that provides hundreds of plugins to support building, deploying and automating any project. JenkinsMiner exploited an unauthenticated remote code execution vulnerability [6]. The vulnerability was known at the time and has already been disclosed and patched in April 2017 by Jenkins. It allowed attackers to transfer a serialized Java "SignedObject" object to the Jenkins CLI (Command Line Interface), that would be deserialized using a new "ObjectInputStream", bypassing an existing blacklist-based protection mechanism. Serialization of an object entails the conversion of its state into a byte stream, from which we can reconstruct the object (deserialization).

Attack Method. The attack makes use of code injection to deploy miners in the Jenkins servers. Two requests are sent to a Jenkins server's CLI by the attacker. The first sends an initial session request, and the subsequent second request, matched by the session header corresponding to that of the first request, sends two serialized objects. One of these objects contains a Monero, an open source cryptocurrency [2], miner payload - JenkinsMiner. In addition, the second request consists of code written in PowerShell (a task-based command-line shell and scripting language built on Microsoft .NET) that executes the miner. If the miner is successfully deployed, it drastically slows down performance and thereby leads to a denial-of-service attack. For further details on the injected code and the attack, see [12].

2.4 Oracle WebLogic Server Attack [28]

Vulnerability. In early 2018, FireEye researchers observed threat actors abusing a known input validation vulnerability [8] in the WebLogic Server Security Service (WLS Security) in Oracle WebLogic Server versions 12.2.1.2.0 and earlier in order to deliver various cryptocurrency miners. Oracle WebLogic Server is an industry-grade application server for building and deploying enterprise Java EE applications supporting the Oracle Applications portfolio [15]. The vulnerability allowed attackers to exploit the server to remotely execute arbitrary code. The flaw was exploited to mine using servers of university and research institutions [3]. Oracle released a patch to fix it [13].

Attack Method. Attackers use PowerShell to download the cryptocurrency miner directly onto the victim's system, and execute it using the "ShellExecute()" method. Alternatively, the PowerShell script can also be delivered (injected), which in turn downloads miners from remote servers and can delete scheduled tasks of other known cryptominers, thereby fighting over other attackers for resources. More details on these attack methods and two additional attack methods that exploit this vulunerability are discussed here [28].

3 CONCLUSION

In this work, we described two kinds of attacks in the cloud, social engineering attacks and cryptomiming attacks, revisiting some actual attacks between 2017 to 2018.

REFERENCES

[1] Jenkins. https://jenkins.io/.
[2] Monero. https://getmonero.org/.
[3] Oracle WebLogic Vulnerability Being Exploited by Bitcoin Miners. https://www.ren-isac.net/public-resources/alerts/REN-ISAC_ADVISORY_Oracle_WebLogic_Vulnerability_Bitcoin_Miner_Attacks_20180105v1.pdf.
[4] Tesla and Jenkins Servers Fall Victim to Cryptominers. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/tesla-and-jenkins-servers-fall-victim-to-cryptominers.
[5] Vulnerability CVE-2017-0144 in SMB exploited by WannaCryptor ransomware to spread over LAN. https://support.eset.com/ca6443/?locale=en_US&viewlocale=en_US.
[6] CVE-2017-1000353. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000353, January 29 2017.
[7] CVE-2017-1002100. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1002100, September 14 2017.
[8] CVE-2017-10271. https://www.cvedetails.com/cve/CVE-2017-10271/, October 19 2017.
[9] Cybercrime tactics and techniques: Q1 2018. https://www.malwarebytes.com/pdf/white-papers/CTNT-Q1-2018.pdf, 2018.

[10] Kubernetes. https://github.com/kubernetes/kubernetes/, 2018.

[11] Tesla Cryptojacking Attack. https://blog.redlock.io/cryptojacking-tesla, 2018.

[12] Jenkins Miner: One of the Biggest Mining Operations Ever Discovered. https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/, February 2018.

[13] Oracle Critical Patch Update Advisory. http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html, October 2017.

[14] Aaron Zimba and Luckson Simukonda and Mumbi Chishimba. Demystifying Ransomware Attacks: Reverse Engineering and Dynamic Malware Analysis of WannaCry for Network and Information Security. *Zambia ICT Journal*, 1(1):35–40, 2017. URL: http://ictjournal.icict.org.zm/index.php/zictjournal/article/view/19.

[15] REN-ISAC Security Advisory. Oracle WebLogic Server. http://www.oracle.com/technetwork/middleware/weblogic/overview/index.html.

[16] Asher Moses. Apple cloud burst: how hacker wiped Mat's 'life'. https://www.smh.com.au/technology/apple-cloud-burst-how-hacker-wiped-mats-life-20120806-23orv.html, August 2012.

[17] Brian Honan. Ubiquiti Networks victim of $39 million social engineering attack. https://www.csoonline.com/article/2961066/supply-chain-management/ubiquiti-networks-victim-of-39-million-social-engineering-attack.html, August 2015.

[18] Chris Parlette. Application Containerization: Pros and Cons. https://www.parkmycloud.com/blog/application-containerization/, 2018.

[19] Josh Fruhlinger. What is WannaCry ransomware, how does it infect, and who was responsible? https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.

[20] Martin Giles. Six Cyber Threats to Really Worry About in 2018. https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/.

[21] Mitch Tullock. Social Engineering Attacks: How to defend against them and fight back. http://techgenix.com/social-engineering-attacks/, May 2018.

[22] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, Princeton, NJ, USA, 2016.

[23] Nick Biasini, Edmund Brumaghin, Warren Mercer, Josh Reynolds, Azim Khodjbaev, and David Liebenberg. Ransom Where? Malicious Cryptocurrency Miners Takeover, Generating Millions. https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html, January 2018.

[24] Nikhil Ravindran. Understanding the blockchain technology (ELI5): What it is and how it is working - An advanced guide! https://www.epixelmlmsoftware.com/blog/how-blockchain-works-advanced-guide, November 2018.

[25] Peter Wood. Attacking the Cloud with Social Engineering. https://www.slideshare.net/PeterWoodx/attacking-the-cloud-with-social-engineering.

[26] Phishing.org. History of Phishing. http://www.phishing.org/history-of-phishing.

[27] R. Sharpe. Just What is SMB? http://samba.anu.edu.au/cifs/docs/what-is-smb.html, October 2002.

[28] Rakesh Sharma, Akhil Reddy, and Kimberly Goody. CryptoMiners: An Overview of Techniques Used Post-Exploitation and Pre-Mining. https://www.fireeye.com/blog/threat-research/2018/02/cve-2017-10271-used-to-deliver-cryptominers.html, February 15, 2018.

[29] Duncan Riley. Symantec report finds cryptojacking surged 8,500% in the fourth quarter. https://siliconangle.com/blog/2018/03/22/symantec-report-finds-cryptojacking-surged-8500-last-quarter/, March 2018.

[30] Sara Peters. The 7 Best Social Engineering Attacks Ever. https://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411, March 2015.

[31] Shirien Elamawy. 6 Most Common Cloud Computing Security Issues. http://www.oracle.com/technetwork/middleware/weblogic/overview/index.html.

[32] SéRgio S. C. Silva, Rodrigo M. P. Silva, Raquel C. G. Pinto, and Ronaldo M. Salles. Botnets: A survey. *Comput. Netw.*, 57(2):378–403, February 2013.

[33] The Redlock Security Team. Cloud Security Trends, May 2018.

[34] Jai Vijayan. Crypto-Mining Attacks Emerge as the New Big Threat to Enterprises. https://www.darkreading.com/attacks-breaches/crypto-mining-attacks-emerge-as-the-new-big-threat-to-enterprises/d/d-id/1330965.

[35] Warwick Ashford. Cryptomining is top attack type, says Malwarebytes. https://www.computerweekly.com/news/252435715/Cryptomining-is-top-attack-type-says-Malwarebytes, February 2018.