Cybercrimes Investigation via Honeypots in Cloud Environments

Vitalii Susukailo[a], Sviatoslav Vasylyshyn[a], Ivan Opirskyy[a], Volodymyr Buriachok[b], and Olena Riabchun[b]

[a] *Lviv Polytechnic National University, 12 Stepana Bandery str, Lviv, 79000, Ukraine*
[b] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

This article explores the capabilities of honeypots in cloud environments. Analyses the problem of cybercrimes investigation in cloud environments. Defines and examines appropriate technologies used by cybersecurity professionals during the cybercrimes investigation. Identifies advantages of honeypots usage in cloud infrastructure.

Keywords

Honeypot, cloud environment, cloud infrastructure, cybercrime, Amazon web services, Azure cloud platform, IaaS, PaaS, SaaS.

1. Introduction

Cloud technologies are increasingly used every day. Although the cloud environment can give organizations the freedom to experiment and scale the resources, it also increases the attack surface.

Cloud security is the joint responsibility of the cloud provider and the cloud customer. Depending on the cloud service model, information security responsibilities should be adequately defined and documented. For SaaS and PaaS models provider is responsible for infrastructure layer security controls, such as patching of services and Operating systems, vulnerability management, hardening of the hypervisor, physical security of the datacenter, etc. But at the same time, it does not mean that customer is not responsible for the information security controls. Cloud customers, which use SaaS and PaaS services, must follow vendor hardening recommendations and security best practices for applications or services they are using. It is also necessary to regularly conduct a supplier security assessment to evaluate controls provided by SaaS or PaaS service providers to ensure that the application provides appropriate security controls and comply with the requirements of international laws and regulations [1].

For the Infrastructure as a Service model cloud customer is responsible for the Operating System configuration, resource scaling, software-defined networks management, and infrastructure layer maintenance, except physical security, hypervisors, network, and virtual machines management. It means that there are more controls, which should be defined for IaaS, such as security monitoring, vulnerability management, incident management, operating system hardening, etc. It's also the responsibility of cloud customers to detect and respond to cloud security threats and ensure the proper protection against cybercrimes. There are plenty of cybersecurity tools and technologies provided by cloud service providers, which can detect and prevent cyber. Still, in *t*, his article will focus on a reliable and straightforward solutions for the incident investigation process in IaaS [2].

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: vitalii.a.susukailo@lpnu.ua (A.1); sviatoslav.i.vasylyshyn@lpnu.ua (A.2); iopirsky@gmail.com (A.3); v.buriachok@kubg.edu.ua (B.4); o.riabchun.asp@kubg.edu.ua (B.5)
ORCID: 0000-0003-4431-9964 (A.1); 0000-0003-1944-2979 (A.2); 0000-0002-8461-8996 (A.3); 0000-0002-4055-1494 (B.4); 0000-0002-4400-0112 (B.5)

2. Cyber Security Threats for Cloud Environments

The threat of data breaches retains its number one for cloud environments. Breaches can cause great reputational and financial damage. They could potentially result in loss of intellectual property (IP) and significant legal liabilities. Inadequate access management, as a cloud environment, not a threat can lead to cloud system compromise. To avoid this threat, cloud customers should protect credentials, ensure automated rotation of cryptographic keys, passwords, and certificates, ensure scalability, require cloud service administrators to use multi-factor authentication, define password policy for management plane and each service deployed in the cloud [3].

One more common cloud security threats are insecure interfaces and APIs. APIs and user interfaces are often the most exposed parts of a system, and it encourages security by design approach to building them. To ensure protection against these threats, the following controls were proposed to ensure by Cloud Security Alliance:

- API security best practices such as oversight of items like inventory, testing, auditing, and abnormal activity protections must be established.
- API keys should be protected, and any key avoid reuse should be avoided.
- It is recommended to use an open API framework such as the Open Cloud Computing Interface (OCCI) or Cloud Infrastructure Management Interface (CIMI).

Lack of cloud security architecture and strategy is another critical threat, which should be taken into account while evaluating cloud services risks. The security architecture needs to align with business goals and objectives, threat modeling should be performed regularly, and continuous monitoring should be ensured for each type of cloud service model. These controls can help organizations ensure secure architecture for cloud infrastructure.

Attackers are using legitimate cloud services to support their activities. Hackers can use a popular service to store malware on websites like GitHub, so it's essential for cloud customers to control content used by their cloud solution.

Common on-premise threats are applicable for cloud environments, such as DDoS attacks, digital currency mining, brute-force attacks to steal credentials, exploiting vulnerabilities in outdated software, etc. Those threats should be evaluated and mitigated by cloud customers to avoid potential cloud security crimes, which will cause business damage.

3. Cloud Security Crimes Investigation Via Cloud Security Solution

Cloud security crimes can be investigated using tools provided by the cloud service provider. There are many security monitoring, detection, and response technologies that can be used to analyze cloud security crimes and prevent them as well as third-party technologies, which can be used in a cloud environment such as Splunk, ELK stack, LogRhythm, etc. But the most popular cloud service providers, such as Amazon Web Services and Azure, have built-in cybersecurity solutions. One of the solutions, which can be used to investigate cloud security crimes is Azure Log Analytics, an Azure cloud event management technology and part of the Azure Security Center.

Log Analytics is part of the overall Microsoft Azure monitoring solution. Log Analytics monitors cloud and on-premises environments to maintain both endpoints and enterprise services' availability and performance. Azure Log Analytics, as a tool for researching events in the Azure cloud environment, can perform the following functions:

- Collection of information—detailed current indicators and journals—from Azure resources and local Infrastructure.
- Visualization—built-in information panels for visualization, which will help to understand what happened quickly.
- Analysis—analysis of programs and Infrastructure.
- Response—an automatic response to incidents.
- Integration—use of 20+ partner integrations and open structure with API and SDK.

Azure Log Analytics can analyze any data loaded to it. This functionality ensures analysis of system and service events with no limitation, which is highly important to analyze data from multiple sources during a cloud security incident investigation. It is also possible to create custom searches and

alert rules to automate threat hunting and incident investigation processes. Also, all logs are stored within Azure Log Analytics platform can be used for further forensics [4].

Amazon Web Services have their security monitoring tools such as Amazon Guard Duty and AWS Cloud Trail. Amazon presents AWS CloudTrail as a technology that provides the event history of account activity, including actions taken through management plane, AWS SDKs, CLI tools, and other Amazon services. API calls history simplifies security analysis, change tracking, and troubleshooting. Besides, CloudTrail can be used to detect unusual activity in Amazon accounts. Amazon GuardDuty is a threat detection service that monitors f malicious activity and unauthorized behavior to protect cloud accounts, workloads, and data stored in Amazon S3. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty can analyze multiple events across multiple AWS data sources, such as AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs. Both of these services Amazon GuardDuty and Cloud Trail, must effectively investigate cloud security crimes in Amazon Web Services.

Build-in cloud security monitoring technologies can be effectively used with other security solutions to prevent and detect cloud security cybercrimes.

4. Honeypot Types, Behavior, and Efficiency in the Cloud Environment

Honeypot is fundamentally different from all developments in the field of security. As a rule, all products in this market are designed to solve a strictly defined function (it doesn't matter whether hardware or software is involved): the firewall solves the tasks of restricting access from one network to another at different levels, the SSH service is designed for encrypted access to operating system resources, etc. Honeypot technology is not designed to solve a specific problem but represents a whole philosophy—flexible, customizable in accordance with the goal. As you might guess, this is not a formalized product or technology, but a kind of tool, something like a microscope in the hands of a biologist. Honeypot provides security professionals with significant advantages. First of all, this is the collection of the necessary information, often containing valuable information. The deployment and operation of live bait are not particularly difficult, and Honeypot tools are, as a rule, not demanding on system resources. Special attention should be paid to the installation and operation of Honeypot. As a rule, the whole range of activities comes down to "install and wait." The most common case is with a dedicated server under the control of specialists. Today, there are many fake programs that give the impression of real, but not so, their main task is to record the entire exchange. The advantage of Honeypot is that a copy of the software can be made on a morally obsolete server that cannot handle the typical computing tasks of e-business [5].

Depending on the level of complexity and its capabilities, they can be classified into three groups: weak, medium, and strong levels of interaction:

1. Low-level: easy to use, and very reliable. They imitate only a portion of the services, and the attacker will be restricted in their interaction with them. For example, they can simulate a UNIX system running telnet. Such systems are designed for the novice crackers themselves. The risk of using low-level honeypots is minimal, but it is. This is due to the fact that the software itself is also a program; therefore, it can be vulnerable. If it can be bypassed, the attacker will gain access to the rest of the network nodes. The power of these simplest honeypots is that they are simple in themselves. It is known that the simpler, the more reliable, so these programs minimize the risk associated with possible breakage of the Honeypot itself and subsequent system breakage.
2. Mid-level Honeypots provide more opportunities to reconstruct a cracker, more complex, and therefore more vulnerable. For example, such a system can model more complex web servers that can respond to non-standard commands and have a more sophisticated logging system. In UNIX, you can use the chroot command capabilities, and in Windows, VMWare virtual machines. Thus, to expand the environment of the attacker (i.e., he will be able to interact not only with "fake" services, but also with "fake" OS), and this will give more opportunities for logging. But this approach will also create more problems.
3. High-level: provide maximum information about the attacker and are as complex and dangerous as possible. They give the attacker access to a real system that does nothing and is not

connected to other systems. The structure of such a honeypot is most often the following: a bait node, a network sensor, and an information store. Such a node can be located on the network behind the firewall, and then the actual control lies on the firewall. If the bait node is incorrectly configured or some other unforeseen things occur, the attacker will be able to access the network. One of the disadvantages of such a solution may be the complexity of its implementation and the relative cost of support. According to recent research in general Honeypot and Honeynet systems are highly rated and widely used in different organizations.

The idea of Honeypot is presented in a broader sense—at the level of the whole network—Honeynet. This is a certain kind of Honeypot; however, such a system does not consist of one computer or an active network device, but of a whole network [6].

5. A honeypot is an Investigation Tool

The most valuable reason for investigating cybercrimes via Honeypot on the network is because of the information it provides; something that no intrusion detection or prevention system can provide. Armed with the information and alerts they log, network administrators learn about the types of attacks they target and have prior knowledge to figure out what they need to do to strengthen their defenses. HoneyPots comparison chart shows the differences between providers in Table 1.

There are two types of baits:

1. An enterprise honeypot is a honeypot that is deployed in a production environment and serves as a tool to investigate attacks in order to use knowledge to strengthen the security of the network further.
2. A research honeypot is a honeypot that is used by researchers and with the hope of studying attack methodologies and other characteristics such as attack motives. Then, for example, using the knowledge to create defense solutions (antivirus, anti-malware, etc.) that can prevent similar attacks in the future.

The types of data that honeypots collect (or so) from attackers may include but are not limited to:

1. Usernames, roles, and privileges that attackers use.
2. IP addresses of the network or host used for the attack.
3. What data is currently Reached, Modified, or Excluded.
4. The actual keystrokes hitters are typing, allowing administrators to see exactly what they are doing [7].

Honeypots also help with keeping hackers' attention diverted from the main net, preventing full attack power until administrators are ready to put in proper countermeasures.

Finally, we need to mention the pros and cons of using a honeypot on your network:

Plus: This is an inexpensive security measure that can provide valuable information about your attackers.

Minus: It is not easy to set up and configure, and it would be crazy to try it without an expert on hand; this can backfire and expose the network to the worst attacks. However, it goes without saying that decoys are probably the best way to catch a hacker or attack as it happens. This allows administrators to walk through the entire process step by step, following everything in real-time with each alert [8].

Table 1.
HoneyPots comparison chart

Provider/Specifications	Illusive Networks Deception Platform	TrapX Deception Grid Platform	Xello Deception Platform
Fake OS platforms		Windows Linux	Windows Linux
Phased attack detection	Active intelligence Lateral movement	Active intelligence Lateral movement Exfiltration	Active intelligence Lateral movement
C&C Detection	–	+	–
MITM Detection	–	+	–
Emulated Traps	+	+	+
Industry Lures	+	+	–
NAC Integration	+	+	–
Full OS Traps	+	+	+
SIEM Integration	+	+	+
Endpoint Integration	+	+	+
EDR	+	+	+
Active Directory	+	+	+
Inline Correlation	+	+	+
Sandbox Integration	–	+	–
Database	–	+	+
POS	–	+	–
ATM	–	+	–
SCADA	+	+	+
IoT [9]	+	+	+
Clouds	unknown	AWS/Azure/ OpenStack	–
Using Client Images	+	+	+
Open API for Integration	+	+	+
Botnet Detection	–	+	Roadmap
Automatic Code Analysis	–	+	–
Trap Constructor	–	+	+
API State Passing	–	+	+
Forensics Collection	+	–	+
Distribution of Lures to Real Hosts	+	–	+
Mechanism for Creating Lures in AD	–	–	+
Integration with Container Orchestration Systems	–	unknown	+
No Need for Deep Intervention in the Enterprise Network Infrastructure	+	–	+
Possibility of Full Administrative Access in the OS	+	–	+

6. Conclusions

The main task solved by information security specialists at the facilities of the information and telecommunications infrastructure is the collection of information to prevent attacks on protected information objects. Previously, the collection of information was carried out after the occurrence of an information security incident, then on the basis of the data obtained, “patches” and “patching holes” in the security system were released. The only information the information security specialists had at their disposal was information left in the compromised system. As a rule, this information is very scarce, and it sorely lacks to prevent further the emergence of threats to the security of protected information resources. The use of network honeypots to detect attacks on protected information resources will allow you to collect as much information as possible about the attack itself and about the goals of the attackers, as well as prevent unauthorized access to protected information resources. The network decoy should work in a stealth mode so that the attacker will not be aware of its presence. Currently, there is a steady trend of transferring computing power to the cloud infrastructure. Cloud computing technology is the next-generation technology and business. Cloud service providers must ensure the security of the services they provide. Businesses are looking to move their information infrastructure to cloud services, but most cannot afford the resulting information security threats. For the most part, existing cloud services offer a standard set of information security tools, such as various firewalls, the use of different authentication methods, attack detection systems based on signature analysis, etc. Cloud services, in comparison with classical information systems, are more vulnerable from the point of view of the damage. In a cloud environment, all information resources are interconnected and controlled by centralized controllers. If you gain access to one information resource in the cloud, all the others are at risk. Instead of piling up various security systems over a cloud service, it is more efficient to implement fake information resources. It is proposed to solve this problem by using the technology of network “bait.” It is advisable to use the network “decoy” in the cloud service Honeypot as a Service (HaaS). This allows you to reduce the initial and operational costs of maintaining the Infrastructure, increase the efficiency of system deployment, and provide the possibility of remote management.

7. References

[1] V. Susukailo, I. Opirskyy, S. Vasylyshyn, Analysis of the use of software baits as a means of ensuring information security, in: IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), 2020, pp. 242–245.

[2] J. Wiley, Threat Hunting For Dummies, Carbon Black Special Edition, 2017.

[3] A. Bessalov, et al., Analysis of 2-Isogeny Properties of Generalized form Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, July 7, 2020, vol. 2746, pp. 1–13.

[4] J. Petters, Endpoint Detection and Response (EDR): Everything You Need to Know, 2017.

[5] O. Milov, A. Voitko, I. Husarova, O. Domaskin, I. Opirskyy, O. Fraze-Frazenko, Development of methodology for modelling the interaction of antagonistic agents in cybersecurity systems, Eastern-European Journal of Enterprise Technologies 2 (2019). 56–66. doi: 10.15587/1729-4061.2019.164730.

[6] Z. A. Khan, U. Abbasi, Reputation Management Using Honeypots for Intrusion Detection in the Internet of Things, Electronics 9 (2020) 4–15. doi:10.3390/electronics9030415.

[7] M. Akiyama, T. Yagi, T. Hariu, Y. Kadobayashi, HoneyCirculator: distributing credential honeytoken for introspection of web-based attack cycle, International Journal of Information Security 17 (2017) 135–151. doi: 10.1007/s10207-017-0361-5.

[8] R. Mogull, J. Arlen, F. Gilbert, A. Lane, D. Mortman, G.Peterson, M. Rothman, The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0? Cloud Security Alliance, 2017.

[9] I. Kuzminykh, et al., Investigation of the IoT device lifetime with secure data transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems 11660 (2019) 16–27. doi: 10.1007/978-3-030-30859-9_2.