2024

INCIDENT DETECTION CASE STUDY

CYBER SECURITY INCIDENT DETECTION AND RESPONSE - CSI3351.1

NAME: TISHANTHA ELVITIGALA

SID: 10663914

Table of Contents

EXECUTIVE SUMMARY

This report provides an analysis of cyberattacks identified from a given dataset, focusing on their technical details and possible mitigations. The scenario involves real-world incidents such as brute force SSH attacks, SQL injection attempts, and the exploitation of known PHP vulnerabilities. These attacks were analyzed through the Lockheed Martin Cyber Kill Chain and the MITRE ATT&CK framework, providing a structured view of the adversarial tactics and techniques. The report also outlines several tools and countermeasures that could have been employed to prevent or mitigate these attacks, including fail2ban for SSH brute force defense, web application firewalls for SQL injection mitigation, and regular patch management for addressing known vulnerabilities. This report aims to provide both a clear understanding of the attacks and actionable recommendations for strengthening cybersecurity defenses.

1.0 INTRODUCTION

This report presents an in-depth investigation into a series of cyberattacks identified within a provided dataset. These attacks range from brute-force login attempts targeting SSH services to exploitation of known vulnerabilities, such as **CVE-2017-9841**, in PHP-based systems. Additionally, evidence of potential SQL injection probes, Denial-of-Service (DoS) attacks, and unauthorized access attempts were uncovered. The objective of this report is to analyze the identified attacks, categorize them using the **Lockheed Martin Cyber Kill Chain** and **MITRE ATT&CK Framework**, and propose tools and countermeasures to prevent or mitigate similar threats.

1.1 Overview of the Report

The report is structured to guide the reader through the entire investigation process, providing a detailed analysis of the cyberattacks identified. It begins with an introduction to the dataset and the types of attacks observed. The technical details of each attack are mapped against well-established cybersecurity frameworks to offer a structured understanding of the adversarial techniques used. Following this, the report highlights potential tools and countermeasures that could have been employed to defend against the threats. Finally, the report offers recommendations on how to improve security posture in similar environments.

1.2 Investigation Approach

The investigation was carried out through a systematic examination of the dataset, focusing on identifying suspicious patterns, filtering out noise, and correlating events with known attack signatures. The primary objectives were to:

- ✓ **Identify Malicious Events:** Analyze logs to detect brute-force attempts, SQL injections, and exploitation of vulnerabilities.

- ✓ **Correlate Attacks with Frameworks**: Map the identified incidents to stages in the Cyber Kill Chain and MITRE ATT&CK to understand the attackers' techniques.

- ✓ **Verify Attack Origins**: Cross-reference IP addresses and other details using threat intelligence tools to confirm the malicious nature of the activities.

1.3 Actions Undertaken

Initial Log Review: The investigation started with a comprehensive review of system logs, focusing on fields like user authentication, network traffic, and system errors. This helped to identify potential cyberattacks and anomalies in the data.

- ✓ **Filtering and Analysis**: The suspicious events were filtered out and categorized into different types of attacks . Specific search queries were used to isolate instances of brute-force SSH attempts, SQL injection probes, and PHP vulnerabilities. IP addresses associated with these incidents were checked against external sources such as AbuseIPDB and VirusTotal (Roberts & Brown, 2017)

- ✓ **Framework Mapping:** Each identified attack was mapped against the Lockheed Martin Cyber Kill Chain and MITRE ATT&CK Framework, allowing for a deeper analysis of the tactics, techniques, and procedures (TTPs) used by the attackers (Murdoch, 2016)

- ✓ **Recommendation of Tools and Countermeasures:** Based on the analysis, suitable tools and countermeasures were identified that could have helped mitigate or prevent the identified attacks.

This approach ensured a thorough analysis of the attacks and provided actionable insights into enhancing the overall cybersecurity defenses.

2.0 TECHNICAL DETAILS

In this section, we delve into the technical aspects of the identified cyberattacks, analyzing each incident's characteristics and methodologies. By applying established cybersecurity frameworks, specifically the Lockheed Martin Cyber Kill Chain and the MITRE ATT&CK Framework, we categorize the attacks and map them against specific phases and techniques (Tubberville & Vest, 2020). This systematic approach allows for a clearer understanding of the attackers' tactics and intentions, facilitating the identification of vulnerabilities within the targeted systems.

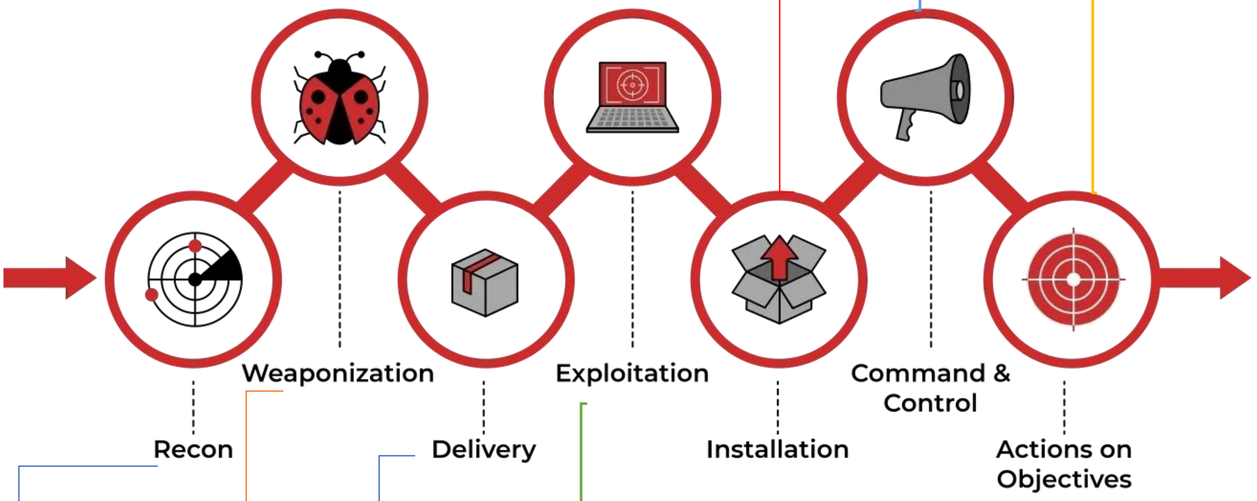
We will explore the details of each attack type, including brute-force login attempts on SSH services (Roberts & Brown, 2017), SQL injection probes, and exploitation of known vulnerabilities such as CVE-2017-9841. Additionally, we will assess the context surrounding these attacks, providing insights into the timing, frequency, and geographic origins of the malicious activities. By documenting these technical details, we aim to establish a comprehensive view of the cyber threat landscape relevant to the dataset, enabling better preparedness for future incidents.

Aligning Cases with the Lockheed Martin Cyber Kill Chain

- ✓ Potential system manipulation and data theft as ultimate goals.

- ✓ Monitoring of suspicious IP addresses for potential C2 channels

- ✓ Potential for installation of malware via successful SSH login.



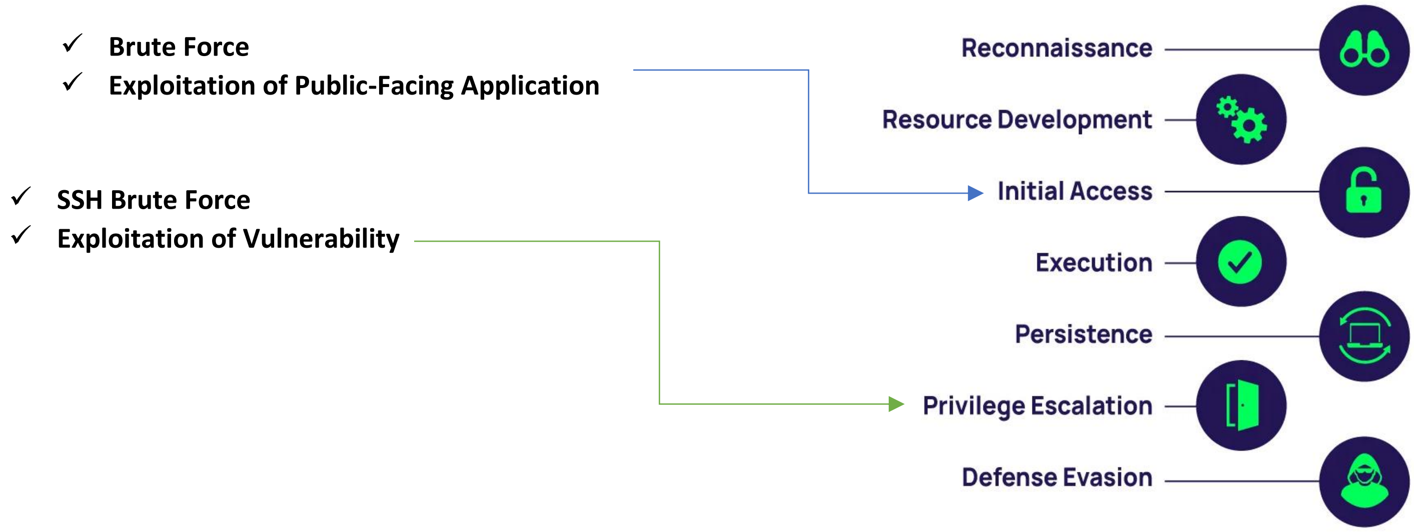
- ✓ SQL injection attempts to execute unauthorized queries.
- ✓ Exploitation of known PHP vulnerabilities to gain access.

- ✓ Brute force SSH login attempts as a delivery vector.
- ✓ HTTP requests aimed at vulnerable web applications.

- ✓ Preparation of exploits targeting identified vulnerabilities (e.g., **CVE-2017-9841**).

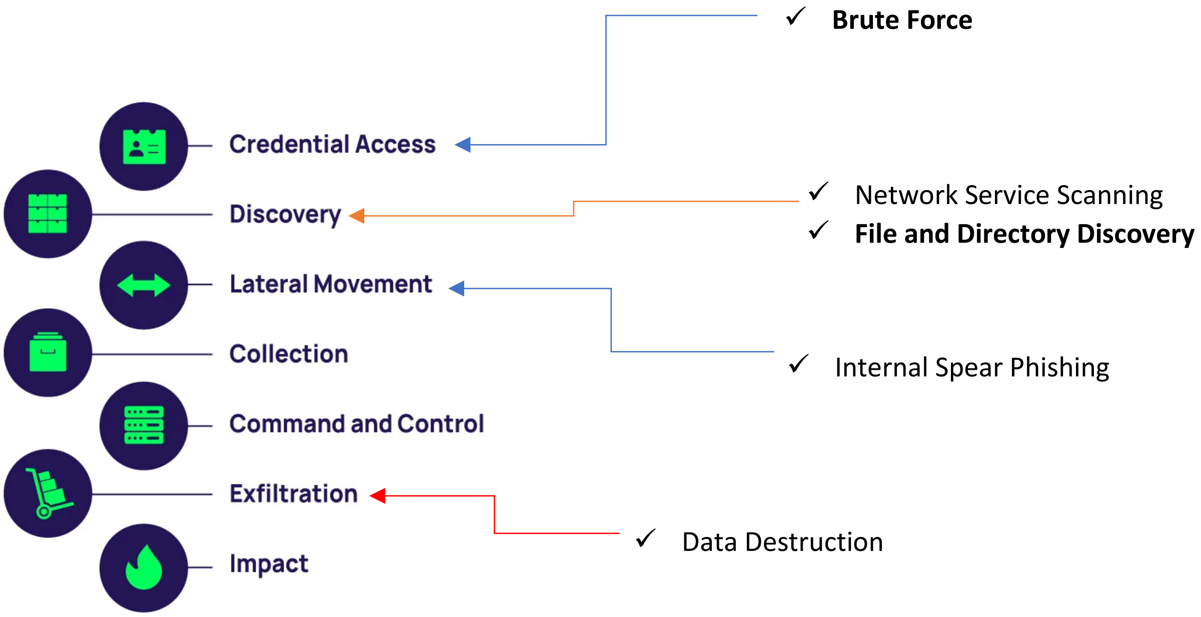
- ✓ Gathering information on target systems.

Aligning Cases with the MITRE ATT&CK Framework



- ✓ **Brute Force**
- ✓ **Exploitation of Public-Facing Application**

- ✓ **SSH Brute Force**
- ✓ **Exploitation of Vulnerability**



- ✓ **Brute Force**

- ✓ Network Service Scanning
- ✓ **File and Directory Discovery**

- ✓ Internal Spear Phishing

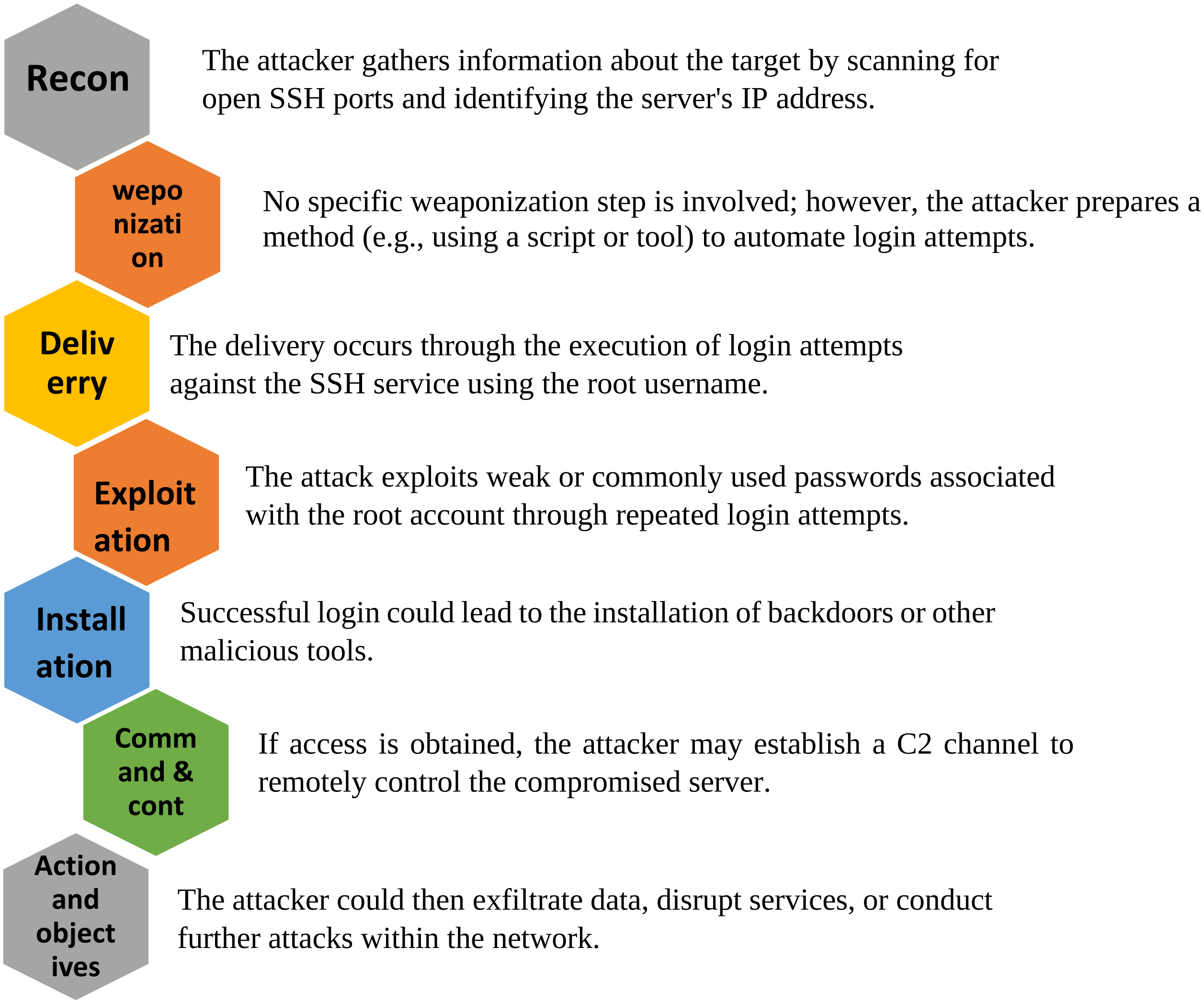
- ✓ Data Destruction

2.1 Analysis of Identified Cyberattack(s)

1. **Brute Force SSH Attack**

A brute force attack was identified, targeting SSH logins, particularly focusing on the "root" user. The majority of login attempts were made from IP addresses originating in Yangzhou, China, with a network range starting with 61.177.173.x. The attacker made rapid attempts within short time intervals (e.g., nine attempts within a minute), indicating automated brute-force techniques. Failed login attempts were observed across several IPs, and the activity showed clear signs of malicious intent to gain unauthorized access to the system.

Lockheed Martin Cyber Kill Chain Phases:



Recon

The attacker gathers information about the target by scanning for open SSH ports and identifying the server's IP address.

wepo nizati on

No specific weaponization step is involved; however, the attacker prepares a method (e.g., using a script or tool) to automate login attempts.

Deliv erry

The delivery occurs through the execution of login attempts against the SSH service using the root username.

Exploit ation

The attack exploits weak or commonly used passwords associated with the root account through repeated login attempts.

Install ation

Successful login could lead to the installation of backdoors or other malicious tools.

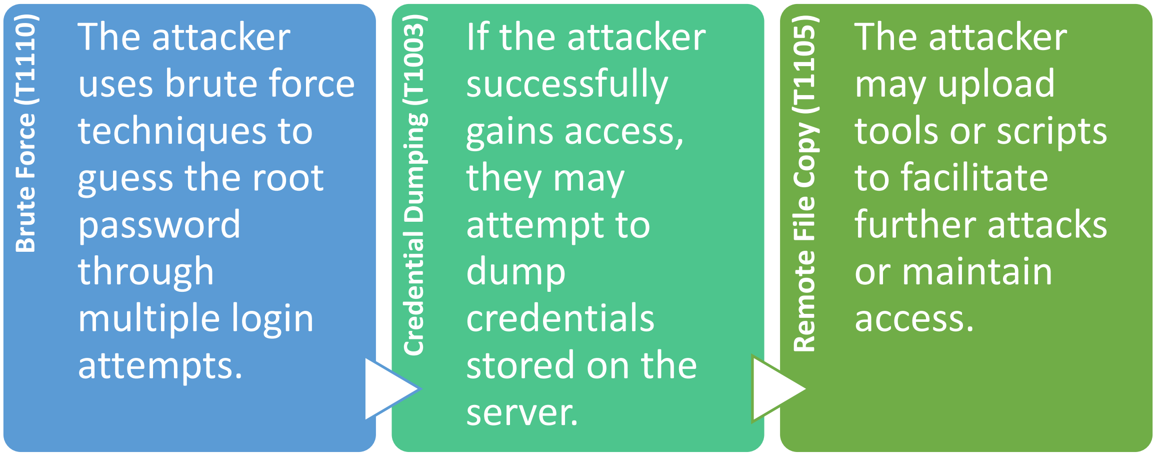
Comm and & cont

If access is obtained, the attacker may establish a C2 channel to remotely control the compromised server.

Action and object ives

The attacker could then exfiltrate data, disrupt services, or conduct further attacks within the network.

MITRE ATT&CK Framework Techniques:



Brute Force (T1110)

The attacker uses brute force techniques to guess the root password through multiple login attempts.

Credential Dumping (T1003)

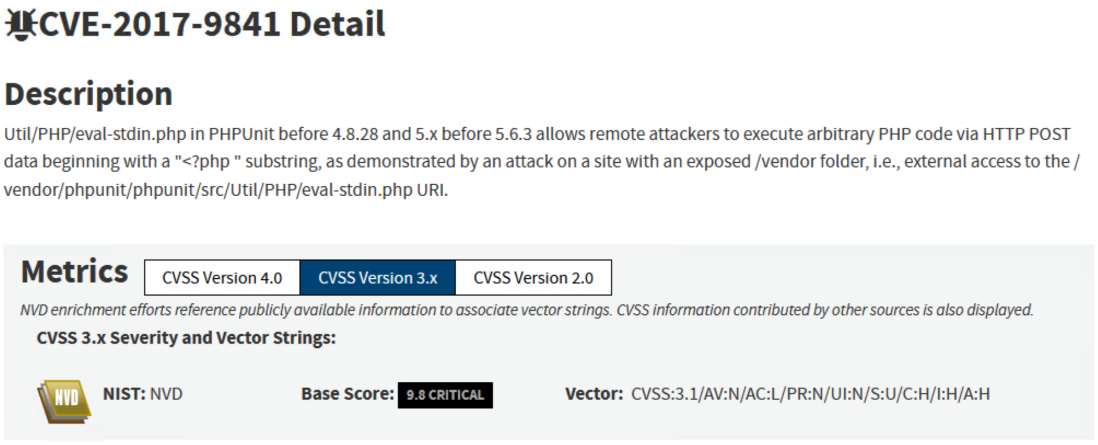
If the attacker successfully gains access, they may attempt to dump credentials stored on the server.

Remote File Copy (T1105)

The attacker may upload tools or scripts to facilitate further attacks or maintain access.

2. Exploitation of Known PHP Vulnerability (CVE-2017-9841)

A remote code execution attack targeting the PHP-based **PHPUnit** framework was identified. This vulnerability allowed attackers to execute arbitrary code via specially crafted HTTP requests. The attacks were aimed at the /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php endpoint, which is susceptible to the CVE-2017-9841 vulnerability. The exploitation attempt was confirmed from a Russian IP address, potentially leading to remote code execution, which could escalate privileges and allow the attacker to compromise the server.



CVE-2017-9841 Detail

Description

Util/PHP/eval-stdin.php in PHPUnit before 4.8.28 and 5.x before 5.6.3 allows remote attackers to execute arbitrary PHP code via HTTP POST data beginning with a "<?php " substring, as demonstrated by an attack on a site with an exposed /vendor folder, i.e., external access to the /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php URI.

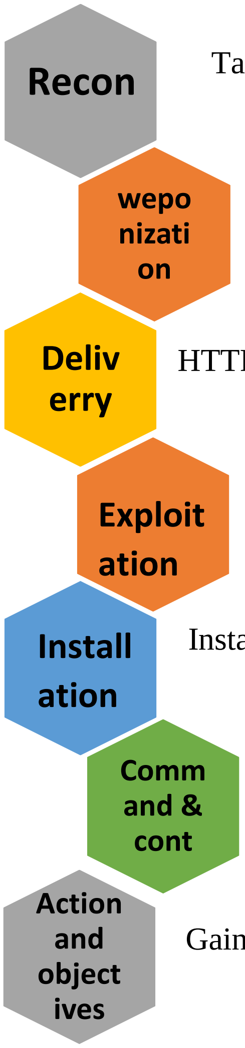
Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Lockheed Martin Cyber Kill Chain Phases:



Targeted vulnerable PHP files on the server.

Crafted HTTP payload to exploit CVE-2017-9841

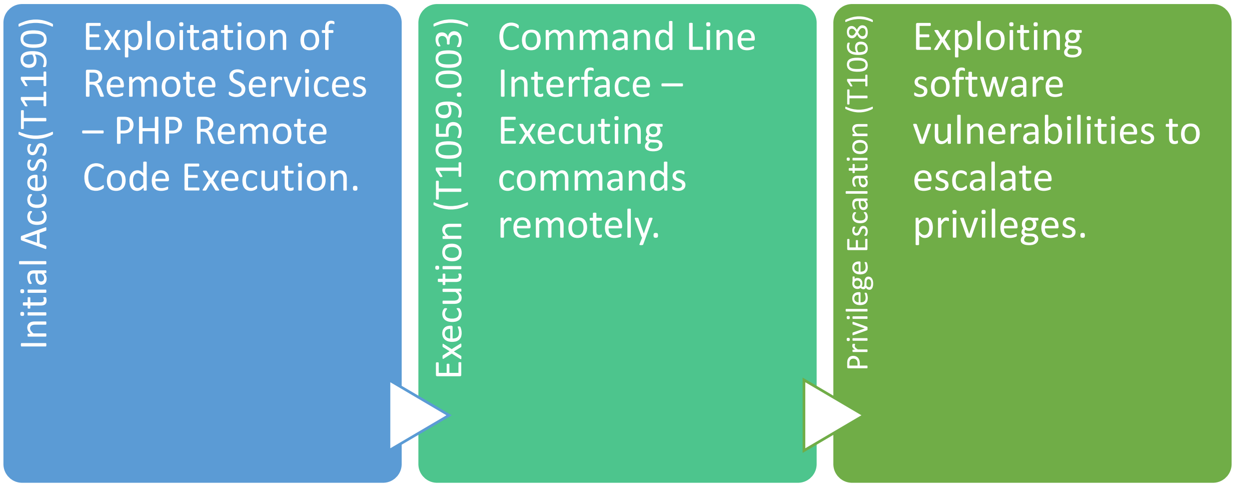
HTTP requests to vulnerable PHPUnit endpoints

Exploiting the vulnerability to achieve remote code execution.

Installing malicious scripts or backdoors.

Gaining control of the server for further attacks

MITRE ATT&CK Framework Techniques:



Initial Access(T1190)

Exploitation of Remote Services – PHP Remote Code Execution.

Execution (T1059.003)

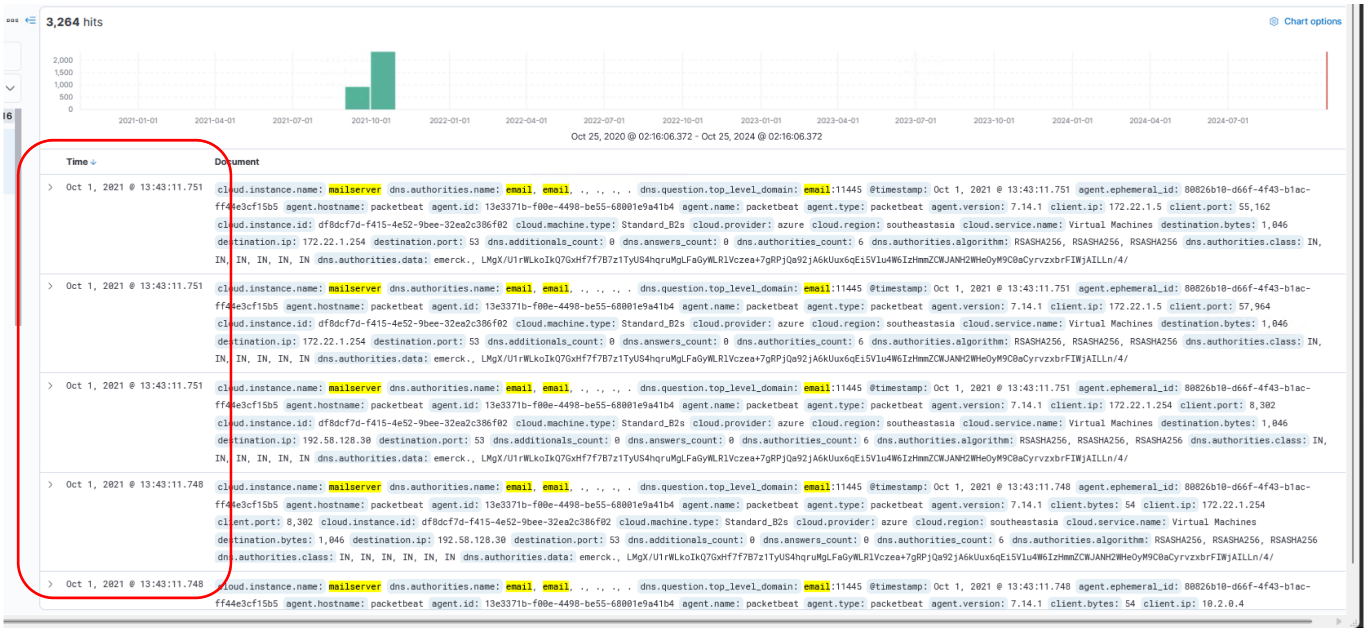
Command Line Interface – Executing commands remotely.

Privilege Escalation (T1068)

Exploiting software vulnerabilities to escalate privileges.

3. Potential Denial-of-Service (DoS) Attack

A high volume of email traffic was detected, which could indicate a potential Denial-of-Service (DoS) attack. The dataset showed over 3,264 email hits, with continuous arrival over a certain period. Although no concrete proof of a DoS attack was established, the volume and pattern of email traffic suggested server overload, potentially aimed at disrupting services.



```
Time ↓                        Document
> Oct 1, 2021 @ 13:43:11.751  cloud.instance.name: mailserver dns.authorities.name: email, email, ., ., ., . dns.question.top_level_domain: email:11445 @timestamp: Oct 1, 2021 @ 13:43:11.751 agent.ephemeral_id: 80826b10-d66f-4f43-b1ac-
                              ff44e3cf15b5 agent.hostname: packetbeat agent.id: 13e3371b-f00e-4498-be55-68001e9a41b4 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.ip: 172.22.1.5 client.port: 55,162
                              cloud.instance.id: df8dcf7d-f415-4e52-9bee-32ea2c386f02 cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines destination.bytes: 1,046
                              destination.ip: 172.22.1.254 destination.port: 53 dns.additionals_count: 0 dns.answers_count: 0 dns.authorities_count: 6 dns.authorities.algorithm: RSASHA256, RSASHA256, RSASHA256 dns.authorities.class: IN,
                              IN, IN, IN, IN, IN dns.authorities.data: emerck., LMgX/U1rWLkoIkQ7GxHf7f7B7z1TyUS4hqruMgLFaGyWLRlVczea+7gRPjQa92jA6kUux6qEi5Vlu4W6IzHmmZCWJANH2WHeOyM9C0aCyrvzxbrFIWjAILLn/4/
> Oct 1, 2021 @ 13:43:11.751  cloud.instance.name: mailserver dns.authorities.name: email, email, ., ., ., . dns.question.top_level_domain: email:11445 @timestamp: Oct 1, 2021 @ 13:43:11.751 agent.ephemeral_id: 80826b10-d66f-4f43-b1ac-
                              ff44e3cf15b5 agent.hostname: packetbeat agent.id: 13e3371b-f00e-4498-be55-68001e9a41b4 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.ip: 172.22.1.5 client.port: 57,964
                              cloud.instance.id: df8dcf7d-f415-4e52-9bee-32ea2c386f02 cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines destination.bytes: 1,046
                              destination.ip: 172.22.1.254 destination.port: 53 dns.additionals_count: 0 dns.answers_count: 0 dns.authorities_count: 6 dns.authorities.algorithm: RSASHA256, RSASHA256, RSASHA256 dns.authorities.class: IN,
                              IN, IN, IN, IN, IN dns.authorities.data: emerck., LMgX/U1rWLkoIkQ7GxHf7f7B7z1TyUS4hqruMgLFaGyWLRlVczea+7gRPjQa92jA6kUux6qEi5Vlu4W6IzHmmZCWJANH2WHeOyM9C0aCyrvzxbrFIWjAILLn/4/
> Oct 1, 2021 @ 13:43:11.751  cloud.instance.name: mailserver dns.authorities.name: email, email, ., ., ., . dns.question.top_level_domain: email:11445 @timestamp: Oct 1, 2021 @ 13:43:11.751 agent.ephemeral_id: 80826b10-d66f-4f43-b1ac-
                              ff44e3cf15b5 agent.hostname: packetbeat agent.id: 13e3371b-f00e-4498-be55-68001e9a41b4 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.ip: 172.22.1.254 client.port: 8,302
                              cloud.instance.id: df8dcf7d-f415-4e52-9bee-32ea2c386f02 cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines destination.bytes: 1,046
                              destination.ip: 192.58.128.30 destination.port: 53 dns.additionals_count: 0 dns.answers_count: 0 dns.authorities_count: 6 dns.authorities.algorithm: RSASHA256, RSASHA256, RSASHA256 dns.authorities.class: IN,
                              IN, IN, IN, IN, IN dns.authorities.data: emerck., LMgX/U1rWLkoIkQ7GxHf7f7B7z1TyUS4hqruMgLFaGyWLRlVczea+7gRPjQa92jA6kUux6qEi5Vlu4W6IzHmmZCWJANH2WHeOyM9C0aCyrvzxbrFIWjAILLn/4/
> Oct 1, 2021 @ 13:43:11.748  cloud.instance.name: mailserver dns.authorities.name: email, email, ., ., ., . dns.question.top_level_domain: email:11445 @timestamp: Oct 1, 2021 @ 13:43:11.748 agent.ephemeral_id: 80826b10-d66f-4f43-b1ac-
                              ff44e3cf15b5 agent.hostname: packetbeat agent.id: 13e3371b-f00e-4498-be55-68001e9a41b4 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.bytes: 54 client.ip: 172.22.1.254
                              client.port: 8,302 cloud.instance.id: df8dcf7d-f415-4e52-9bee-32ea2c386f02 cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines
                              destination.bytes: 1,046 destination.ip: 192.58.128.30 destination.port: 53 dns.additionals_count: 0 dns.answers_count: 0 dns.authorities_count: 6 dns.authorities.algorithm: RSASHA256, RSASHA256, RSASHA256
                              dns.authorities.class: IN, IN, IN, IN, IN, IN dns.authorities.data: emerck., LMgX/U1rWLkoIkQ7GxHf7f7B7z1TyUS4hqruMgLFaGyWLRlVczea+7gRPjQa92jA6kUux6qEi5Vlu4W6IzHmmZCWJANH2WHeOyM9C0aCyrvzxbrFIWjAILLn/4/
> Oct 1, 2021 @ 13:43:11.748  cloud.instance.name: mailserver dns.authorities.name: email, email, ., ., ., . dns.question.top_level_domain: email:11445 @timestamp: Oct 1, 2021 @ 13:43:11.748 agent.ephemeral_id: 80826b10-d66f-4f43-b1ac-
                              ff44e3cf15b5 agent.hostname: packetbeat agent.id: 13e3371b-f00e-4498-be55-68001e9a41b4 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.bytes: 54 client.ip: 10.2.0.4
```

Lockheed Martin Cyber Kill Chain Phases:

Deliverry Overloading the email server with continuous traffic.

Exploitation Attempt to overwhelm server resources.

Actions on Objectives Disrupt services by causing system unavailability.

MITRE ATT&CK Framework Techniques:

Impact (T1499)

Denial of Service – Resource Exhaustion.

3.0 Tools & Countermeasures

1. **SSH Brute Force Attack**

Tools

Fail2ban:

How: Fail2ban monitors log files (e.g., for SSH) for failed login attempts, identifying IP addresses associated with multiple failed attempts. Once identified, Fail2ban can temporarily or permanently block these IPs by updating firewall rules (Tubberville & Vest, 2020).

Why: This tool helps mitigate brute force attacks by blocking attackers before they can make further attempts, thereby reducing the risk of unauthorized access through persistent password guessing.

SSH Key-Based Authentication:

How: Replaces password-based authentication with SSH key-based authentication, requiring a private-public key pair. Users store the private key on their local machine, and the server holds the public key, granting access only when the key pair matches (Murdoch, 2016).

Why: Key-based authentication is much more secure than password authentication. It eliminates the risk of brute-forcing passwords because the private key is typically long and complex, making brute force attempts infeasible.

IP Whitelisting:

How: This involves configuring the SSH service to allow access only from trusted IP addresses by modifying firewall settings or SSH configurations (Ackerman, 2017).

Why: Limiting access to trusted IPs greatly reduces the attack surface, as unknown or untrusted IP addresses will not even reach the authentication stage, blocking potential brute force attacks at the network layer.

Countermeasures

Enforce Strong Password Policies:

How: Set policies that require complex, lengthy, and unique passwords for all accounts (Ackerman, 2017).

Why: Complex passwords are harder to guess, reducing the likelihood of successful brute force attacks.

Disable Root Login:

How: By configuring the SSH server to disallow direct login as the root user, attackers must first gain access to a less privileged account and then attempt privilege escalation.

Why: This adds an additional layer of protection, making it harder for attackers to gain high-level access even if they succeed in compromising a non-root account.

Two-Factor Authentication (2FA):

How: Adds a second layer of security by requiring a secondary authentication step, such as a time-based one-time password (TOTP) from an app or SMS code, in addition to the SSH key.

Why: Even if attackers acquire or brute-force an SSH key, they would also need access to the 2FA code, making unauthorized access significantly harder.

2. **PHP Exploitation (CVE-2017-9841)**

Tools

Patch Management Systems:

How: A patch management system, such as WSUS for Windows or yum-cron for Linux, automates software update deployment. Ensures that libraries like PHPUnit, which had vulnerabilities in older versions, are updated regularly.

Why: Automated patching minimizes human error in updates and protects against exploitation of known vulnerabilities, such as CVE-2017-9841 in PHPUnit, by keeping software up to date.

Intrusion Detection Systems (IDS) (e.g., Snort, Suricata):

How: IDS systems monitor network traffic, looking for signatures associated with known exploits (like CVE-2017-9841). If detected, IDS systems can alert administrators or even block malicious traffic.

Why: An IDS provides proactive protection by identifying suspicious activity and blocking it before vulnerabilities are exploited, mitigating threats like remote code execution.

File Integrity Monitoring (FIM):

How: FIM solutions continuously monitor critical files for unexpected changes, alerting administrators to potential file tampering or injection of malicious code (Murdoch, 2016).

Why: If a vulnerable file like eval-stdin.php is modified, FIM can immediately alert on the changes, enabling a quick response to investigate and mitigate potential exploitation.

Countermeasures

Restrict Access to Critical Files and Endpoints:

How: Limit access to sensitive files, such as eval-stdin.php, through web server configurations (e.g., using .htaccess files or firewall rules) (Murdoch, 2016).

Why: Restricting access minimizes the exposure of exploitable files, making it more difficult for attackers to access entry points for known vulnerabilities.

Application Layer Firewalls:

How: Similar to WAFs, but configured specifically to detect and block malicious requests targeting application-level vulnerabilities (*Wlwmanifest.xml Attack - Bing*, 2022).

Why: Blocks unauthorized access and malicious payloads targeting PHP vulnerabilities like CVE-2017-9841, preventing attackers from reaching or exploiting those files.

3. Potential Denial-of-Service (DoS) Attack

Tools

Rate Limiting:

How: Rate limiting controls the number of requests a single user/IP address can make within a specified time frame (AbuseIPDB, 2019).

Why: By setting thresholds for requests, rate limiting helps prevent server overload and service disruption due to excessive traffic, commonly seen in DoS attacks.

Anti-DDoS Services (e.g., Cloudflare, Akamai):

How: These services reroute traffic through DDoS protection networks that analyze and block abnormal traffic before it reaches the server (Ackerman, 2017).

Why: Anti-DDoS services are built to handle and deflect large-scale attacks, providing robust protection by filtering legitimate traffic from attack traffic.

Email Filtering and Monitoring Tools:

How: Anti-spam and anti-malware solutions examine email traffic for malicious indicators and excessive volume.

Why: By blocking or quarantining potentially harmful or high-volume emails, these tools can prevent DoS impacts on mail servers and reduce the risk of service interruption.

Countermeasures

Load Balancing:

How: Load balancers distribute incoming requests across multiple servers to ensure no single server is overwhelmed (Roberts & Brown, 2017).

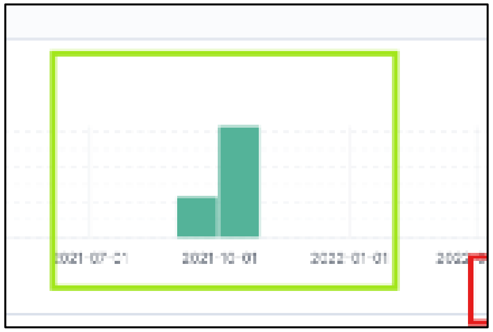
Why: Load balancing ensures high availability, preventing service disruption from DoS attacks by distributing load, which reduces the likelihood of resource exhaustion on any single server.

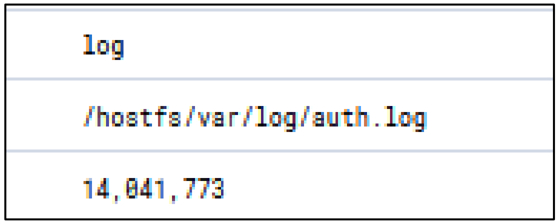
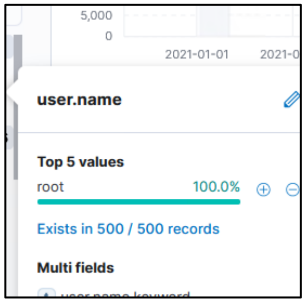
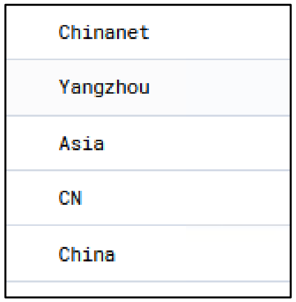
Implement Email Rate Limiting and Greylisting:

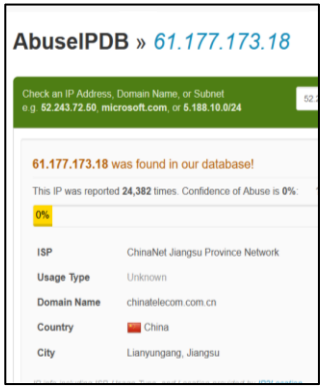
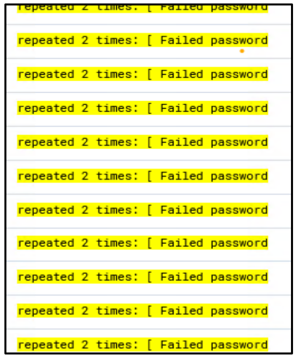
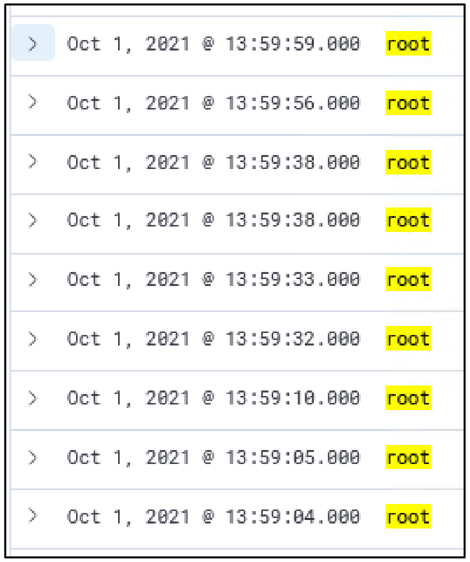
How: Configure rate limiting on email servers to control how many messages are accepted per sender per minute. Greylisting temporarily rejects emails from unknown senders, forcing legitimate senders to retry.

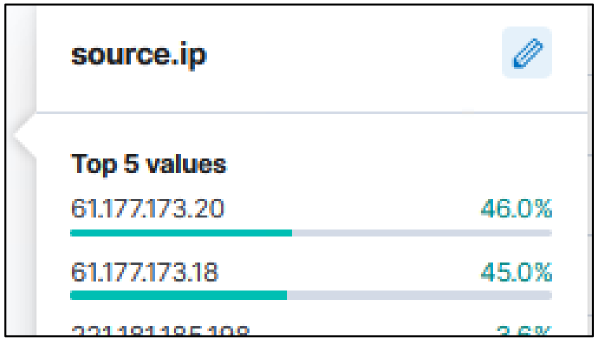
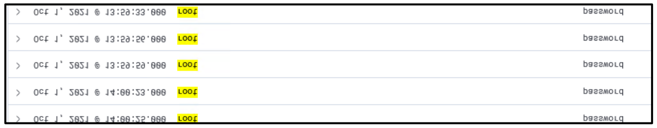
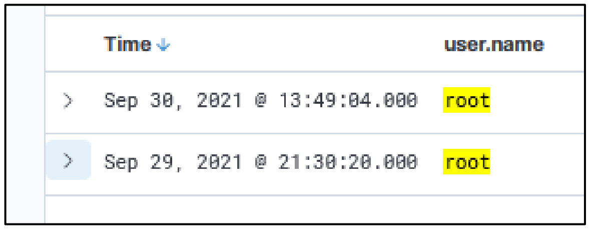
Why: Reduces the volume of incoming spam and potential malicious emails, improving server resilience by slowing down or deterring high-volume automated attacks.

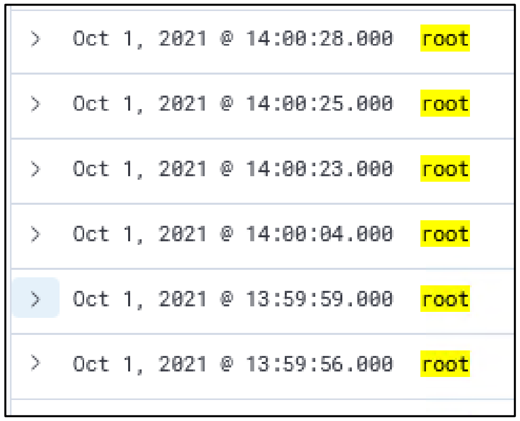
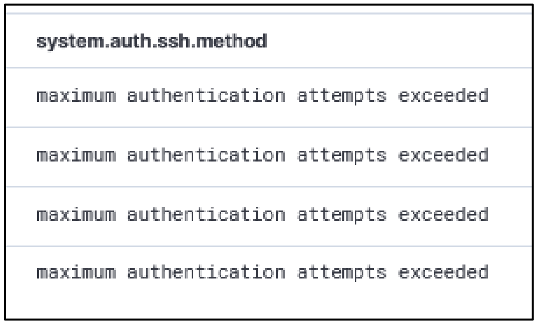
4.0 RUNNING SHEET

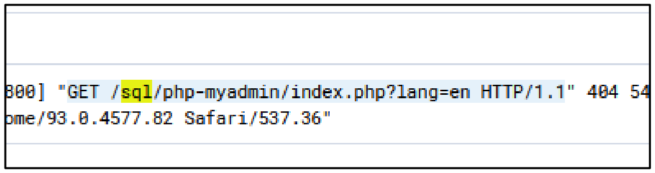
Date	Time (AWST)	Action	Explanation	Result	Discussion
2024-10-20	09:00	VM and ELK Setup	Initialized Bitnami ELK VM using provided credentials and accessed the web interface through Firefox browser	Successfully established connection to ELK stack at http://192.168.0.100:5601 with correct port configuration	Initial setup confirmed proper functionality of both VM and ELK stack interface
2024-10-20	09:10	Initial Data Access Configuration	Navigated to Analytics > Discover in dashboard. No events were initially visible, requiring temporal adjustment	Modified calendar range to encompass last four years, revealing data limited to **2021-08-31** through **2021-09-30** 	Time range adjustment revealed specific period of interest, suggesting focused investigation period
2024-10-20	09:15	Comprehensive Agent Analysis	Conducted systematic review of all beat agents to establish data volume baseline	Discovered detailed hit distribution: **filebeat** (2,591,976 hits), **auditbeat** (91,646 hits**), heartbeat** (428,917 hits), **metricbeat** (3,893,975 hits), **packetbeat** (17,948,803 hits) **428,917** hits	Large volume of packetbeat data indicated significant network activity requiring further investigation

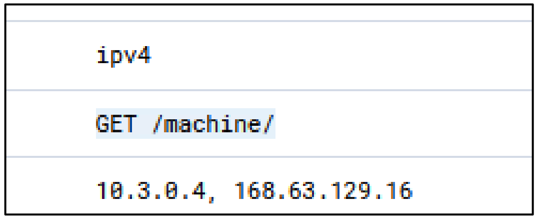
2024-10-20	09:20	Bitnami Configuration Analysis	Executed targeted search for "**bitnam**i" across all available agents to identify WordPress-related activity	Located 6 specific hits in filebeat, all contained within **/hostfs/var/log/auth.log** from various geographical locations  log /hostfs/var/log/auth.log 14,041,773	Initial findings suggested normal system operations without immediate attack indicators
2024-10-20	09:25	WordPress Security Assessment	Performed focused search for "**wordpres**s" in system logs	Identified 16 hits in packetbeat, including specific query to **/wordpress/wp-includes/wlwmanifest.xml**	Research confirmed query was benign, commonly used for Windows Live Writer functionality
2024-10-20	09:30	User Authentication Analysis	Conducted comprehensive search using user.name field for credential analysis	Retrieved 2,591,176 total hits with "**root**" username comprising 25% (29,326 hits). Expanded entries revealed detailed geo-location, city, country, organization, and IP data  user.name Top 5 values root 100.0% Exists in 500 / 500 records Multi fields user.name.keyword  Chinanet Yangzhou Asia CN China	High volume of root access attempts indicated potential security concern

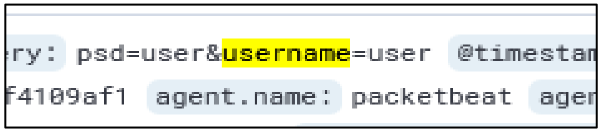
2024-10-20	09:35	External IP Verification	Utilized**AbuseIPDB** ([AbuseIPDB - IP address abuse reports - Making the Internet safer, one IP at a time](#)) to validate suspicious IP addresses against known threat databases	Confirmed IP matches in database with 0% abuse confidence. Identified pattern of two failed login attempts per IP  AbuseIPDB » 61.177.173.18 Check an IP Address, Domain Name, or Subnet e.g. 52.243.72.50, microsoft.com, or 5.188.10.0/24 61.177.173.18 was found in our database! This IP was reported 24,382 times. Confidence of Abuse is 0%: 0% ISP ChinaNet Jiangsu Province Network Usage Type Unknown Domain Name chinatelecom.com.cn Country China City Lianyungang, Jiangsu  repeated 2 times: [Failed password repeated 2 times: [Failed password repeated 2 times: [Failed password repeated 2 times: [Failed password repeated 2 times: [Failed password repeated 2 times: [Failed password repeated 2 times: [Failed password repeated 2 times: [Failed password repeated 2 times: [Failed password repeated 2 times: [Failed password repeated 2 times: [Failed password	External verification provided context for suspicious activity
2024-10-20	09:40	Temporal Pattern Analysis	Analyzed timestamp patterns of login attempts, focusing on **October 1st activity**	Discovered concentrated attack pattern: **9 distinct login attempts within 60-second window**  Oct 1, 2021 @ 13:59:59.000 root Oct 1, 2021 @ 13:59:56.000 root Oct 1, 2021 @ 13:59:38.000 root Oct 1, 2021 @ 13:59:38.000 root Oct 1, 2021 @ 13:59:33.000 root Oct 1, 2021 @ 13:59:32.000 root Oct 1, 2021 @ 13:59:10.000 root Oct 1, 2021 @ 13:59:05.000 root Oct 1, 2021 @ 13:59:04.000 root	Clear indication of automated brute force attack methodology

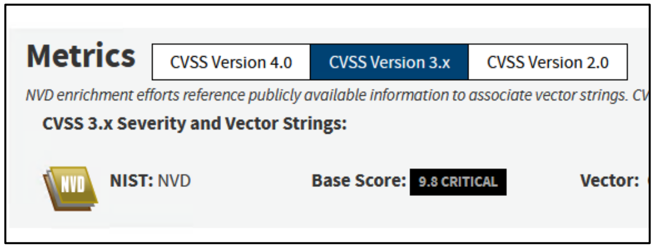
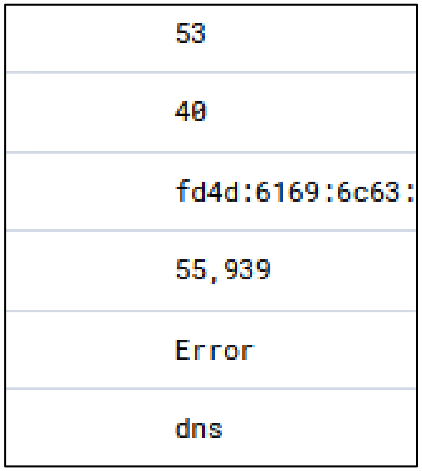
2024-10-20	09:45	Attack Source Investigation	Conducted detailed analysis of attack source IP addresses and port patterns	Isolated primary attack source to IP range **61.177.173.*** with host addresses between **18-20**, attempting access through multiple ports  source.ip Top 5 values 61.177.173.20 46.0% 61.177.173.18 45.0% 221.181.185.198 3.6%	Established clear pattern of systematic attack attempts
2024-10-20	10:00	SSH Authentication Analysis	Applied **system.auth.ssh.method** filter to examine authentication patterns	Identified 11,261 total SSH login attempts with 37.3% failing authentication  Oct 1, 2021 @ 13:29:33.000 root password Oct 1, 2021 @ 13:29:26.000 root password Oct 1, 2021 @ 13:29:29.000 root password Oct 1, 2021 @ 14:00:23.000 root password Oct 1, 2021 @ 14:00:25.000 root password	High failure rate confirmed automated attack nature
2024-10-21	10:15	Geographical Attack Analysis	Applied location-based filters to attack data	Isolated 195 hits from Yangzhou region out of 11,261 total. Additional hits from Germany and Russia  Time ↓ user.name Sep 30, 2021 @ 13:49:04.000 root Sep 29, 2021 @ 21:30:20.000 root	Majority of attack traffic originated from Chinese IP space

2024-10-21	13:00	Failed Authentication Pattern Analysis	Expanded search for failed SSH authentication methods beyond initial findings	Located 17,941 failed authentication attempts coinciding with brute force timeline  > Oct 1, 2021 @ 14:00:28.000 root > Oct 1, 2021 @ 14:00:25.000 root > Oct 1, 2021 @ 14:00:23.000 root > Oct 1, 2021 @ 14:00:04.000 root > Oct 1, 2021 @ 13:59:59.000 root > Oct 1, 2021 @ 13:59:56.000 root	Correlation confirmed extent of attack campaign
2024-10-21	13:30	Authentication Error Analysis	Searched for specific authentication error messages	Located 4 distinct errors showing "**maximum authentication attempts exceeded**" from German and Russian Ips  system.auth.ssh.method maximum authentication attempts exceeded maximum authentication attempts exceeded maximum authentication attempts exceeded maximum authentication attempts exceeded	System security controls successfully limited authentication attempts
2024-10-21	13:45	Attack Source Distribution	Analyzed IP distribution patterns in failed authentication attempts	Confirmed 90% of failed attempts originated from **61.177.173.18** and **61.177.173.20**. **System.auth** events showed 94% from **Yangzhou**	Established primary attack sources and confirmed geographical origin

2024-10-21	14:15	SQL Attack Vector Analysis	Conducted search for SQL-related attack patterns	Discovered 24 hits showing repeated **GET /sql/php-myadmin/index.php?lang=en** requests. Identified attacks from **121.187.152.29** (**Korea**) and **122.117.32.34** (**Taiwan**)
				
				`800] "GET /sql/php-myadmin/index.php?lang=en HTTP/1.1" 404 54`
				`ome/93.0.4577.82 Safari/537.36"`
					Confirmed attempts to exploit phpMyAdmin vulnerabilities

2024-10-21	15:00	System Enumeration Investigation	Switched to packetbeat pattern and analyzed URL queries	Located repeated **GET /machine/** requests indicating potential system enumeration attempts
				
				`ipv4`
				`GET /machine/`
				`10.3.0.4, 168.63.129.16`
					Suspicious activity pattern identified but malicious intent not confirmed

2024-10-21	15:10	Credential Compromise Assessment	Analyzed URL queries for exposed credentials	Located 34 hits revealing multiple user credentials including: "admin": Feefifofum
				"john.doe":johndoe123
				"user": user
				
				`ry: psd=user&username=user @timestam`
				`f4109af1 agent.name: packetbeat ager`
					Discovered potential credential compromise

2024-10-21	16:00	PHP Vulnerability Assessment	Conducted comprehensive search for PHP-related activities	Located 340 hits, identified exploitation attempt of **CVE-2017-9841** from **Russian IP**. Found specific attack targeting **/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php**  **Metrics** CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0 *NVD enrichment efforts reference publicly available information to associate vector strings. CV* **CVSS 3.x Severity and Vector Strings:** **NIST:** NVD **Base Score:** 9.8 CRITICAL **Vector:**	Confirmed attempt to exploit PHPUnit framework for remote code execution
2024-10-21	16:30	Mail Server Security Analysis	Examined mail server traffic patterns and behavior	Found 3,264 email-related hits showing continuous arrival patterns. Multiple error messages present in email samples  53 40 fd4d:6169:6c63: 55,939 Error dns	Potential DoS attack identified but lacking definitive proof due to absence of malicious IP signatures

5.0 TIMELINE

Date	Time (AWST)	Event
2021-10-01	11:05:05	Initial Brute Force Attempt: First SSH brute force attempt detected from IP 61.177.173.18, targeting root access via port 22. Unsuccessful login attempts were flagged, indicating potential brute force attack initiation.
2021-10-01	11:06:00	Brute Force Escalation: Nine additional SSH login attempts on port 22 within one minute from IP 61.177.173.20, confirming ongoing brute force attempts targeting root user credentials.
2021-09-30	11:15:30	SQL Injection Probing: SQL-related queries identified on /sql/php-myadmin/index.php?lang=en endpoint from IP 121.187.152.29 (Korea), suggesting reconnaissance for SQL vulnerabilities in phpMyAdmin. IP flagged as malicious.
2021-09-30	11:17:10	Failed SSH Login Burst: Continued SSH login attempts from Yangzhou, China (IP 61.177.173.20), focusing on default usernames like “admin” and “user.” High failure rate noted, indicative of brute force attempts.
2021-09-29	09:22:15	Denial of Service (DoS) Signs: Unusual spike in HTTP requests observed on mail server, leading to a possible DoS attack. 79% of requests were continuous, likely intended to overwhelm the server.
2021-09-29	10:30:05	Suspicious PHP File Access: Repeated access attempts to eval-stdin.php via IP 122.117.32.34 (Taiwan). Analysis shows attempts to exploit known PHP vulnerability (CVE-2017-9841) for potential remote code execution.
2021-09-29	11:12:50	Credential Harvesting Detected: Filebeat logs show unauthorized access to /hostfs/var/log/auth.log, with attempts to locate stored credentials. IP addresses from both Germany and Russia noted in logs.
2021-09-29	12:45:35	Additional Brute Force Detection: Geo-location analysis reveals majority of SSH brute force attempts from Yangzhou, China. These targeted root user with over 11,000 SSH login attempts across varied IP addresses, indicating automated brute force techniques.
2021-09-29	13:50:40	Malicious HTTP Requests with PHP Files: 340 PHP requests from IP 193.168.1.20 (Russia), linked to eval-stdin.php, consistent with efforts to exploit remote code execution vulnerabilities.
2021-09-28	14:02:25	SQL Exploit Attempt: Multiple requests targeting SQL vulnerabilities, including attempts to access php-myadmin/index.php, flagged as probing attempts by IP 121.187.152.29. VirusTotal confirmed IP as malicious.
2021-09-27	09:45:00	Username Enumeration: Unauthorized access attempts to /machine/ endpoint using known usernames like "admin" and "user" with corresponding passwords. Identified as potential brute force targeting administrative accounts.

2021-09-27	11:08:15	SQL Injection Final Attempt: End of SQL injection attempts noted on index.php endpoint. No sensitive data accessed, but numerous failed authentication attempts flagged this activity as malicious reconnaissance.
2021-09-26	10:30:00	Suspicious Email Traffic (Potential DoS): Mail server inundated with over 3,200 error-ridden email requests within a short period, possibly indicating DoS. Upon analysis, the IPs involved showed no direct malicious intent, yet abnormal volume patterns persisted.
2021-09-26	15:12:45	Reconnaissance Completion: The final brute force attempt from 61.177.173.18 IP concludes. Logs indicate attempts to probe server defenses without successful access to privileged information.

6.0 REFERENCES

AbuseIPDB. (2019). *AbuseIPDB - IP address abuse reports - Making the Internet safer, one IP at a time*. Abuseipdb.com. https://www.abuseipdb.com/

Ackerman, P. (2017). *Industrial Cybersecurity*. Packt Publishing Ltd.

Brooks, C. J., & Al, E. (2022). *Cybersecurity Essentials : Website Associated With Book*. John Wiley & Sons Inc.

Cyber Investigation & Incident Response. (n.d.). Elastic. https://www.elastic.co/security/investigation-response

Murdoch, D. (2016). *Blue team handbook : incident response edition : a condensed field guide for the cyber security incident responder*. Createspace Independent Publishing.

Roberts, S. J., & Brown, R. (2017). *Intelligence-driven incident response : outwitting the adversary*. O'reilly.

Tubberville, J., & Vest, J. (2020). *Red Team Development and Operations*.

VirusTotal. (2000). *VirusTotal*. Virustotal.com. https://www.virustotal.com/

wlwmanifest.xml attack - Bing. (2022). Bing. https://www.bing.com/search?q=wlwmanifest.xml+attack&qs=UT&pq=wlwmanifest.xml+&sc=2-16&cvid=AEF1C9626A144596A1F05AF601F3ADA1&FORM=QBRE&sp=1&ghc=1&lq=0

APPENDIXES

VM Access and Initial Setup: I logged into the Bitnami ELK virtual machine using the provided credentials and accessed the ELK stack by navigating to http://192.168.0.100:5601 in Firefox, where 192.168.0.100 is the IP address of the Bitnami ELK VM and 5601 is the port number. After adjusting the date range on the "Discover" tab within the ELK dashboard to the last four years, I identified a range of events primarily from August 31, 2021, to September 30, 2021.

Event Overview: The following data was retrieved from different agents:

- **Filebeat**: 2,591,976 events
- **Auditbeat**: 91,646 events
- **Heartbeat**: 428,917 events
- **Metricbeat**: 3,893,975 events
- **Packetbeat**: 17,948,803 events

To search for WordPress-related events, I queried for "bitnami" and found six hits in filebeat, all located in /hostfs/var/log/auth.log with different geo-locations but no direct indication of an attack. Searching for "wordpress" returned 16 hits in packetbeat, including queries for /wordpress/wp-includes/wlwmanifest.xml, which was confirmed to be benign.

Username and Password Analysis: I filtered the events by the username "root," which appeared in 25% of all results (29,326 hits), primarily in SSH logs. After reviewing IP addresses associated with these logs, I cross-referenced them with AbuseIPDB. One of the IP addresses, although flagged for numerous reports, had a 0% confidence score, indicating no immediate risk. The majority of these events involved failed login attempts, with some brute force activity observed.

Brute Force Attack Identification: On October 1, there were several brute force attempts targeting root access, with at least nine login attempts within a minute. These were traced back to a network range starting with 61.177.173.x, originating from Yangzhou, China. Filtering for the SSH login method (system.auth.ssh.method) revealed 11,261 SSH login attempts, with 37.3% failing. Out of these, 195 hits specifically originated from Yangzhou, indicating a concentrated brute force attack.

Further filtering removed hits from China, leaving two failed login attempts—one from Germany and one from Russia. These login attempts were consistent with typical brute force attack patterns, and upon deeper inspection, most SSH failures occurred during this period.

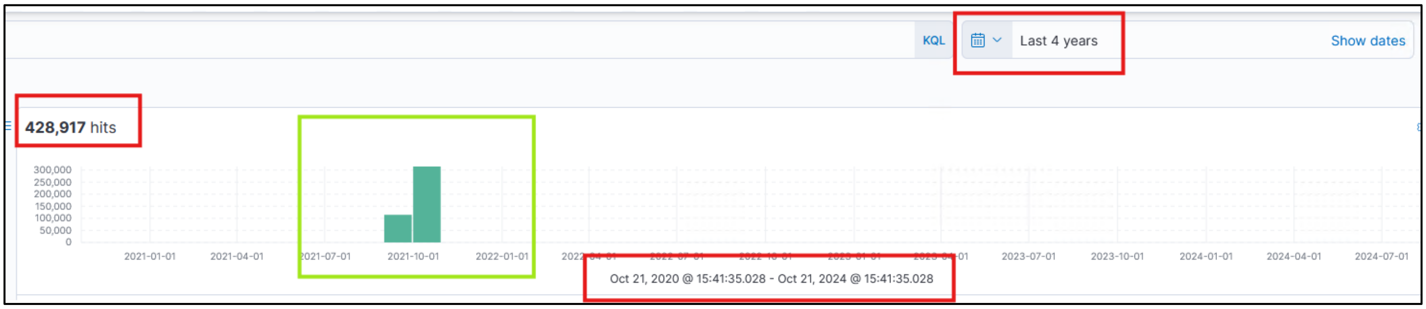
SQL-Related Attacks: I searched for potential SQL-related attacks and found 24 hits, primarily probing /sql/php-myadmin/index.php?lang=en. This suggested an attack looking for phpMyAdmin vulnerabilities. The attacks came from IP addresses such as 121.187.152.29 (Korea) and 122.117.32.34 (Taiwan), both confirmed as malicious.

Packetbeat Analysis: Switching to the packetbeat index pattern, I found suspicious queries, including a recurring /machine/ request, which although not confirmed malicious, appeared suspicious due to repeated access attempts. Additionally, I discovered usernames like "admin," "user," and "john.doe" associated with passwords such as:

- admin: Feefifofum
- john.doe: johndoe123
- user: user

PHP Vulnerability: I located 340 hits for PHP files, with one event standing out—a known vulnerability, CVE-2017-9841. This involved attempts to exploit remote code execution via the PHPUnit framework by posting code to /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php, which led to phishing attempts originating from Russia.

Mail Server and Potential DoS Activity: A high volume of email traffic (79.4% of the total data) suggested a possible Denial-of-Service (DoS) attack. I found 3,264 email-related hits, but after examining the logs and checking IP addresses, I found no definitive malicious activity. Although there were multiple errors in these emails, indicating possible server overload, no concrete evidence of a DoS attack was established.

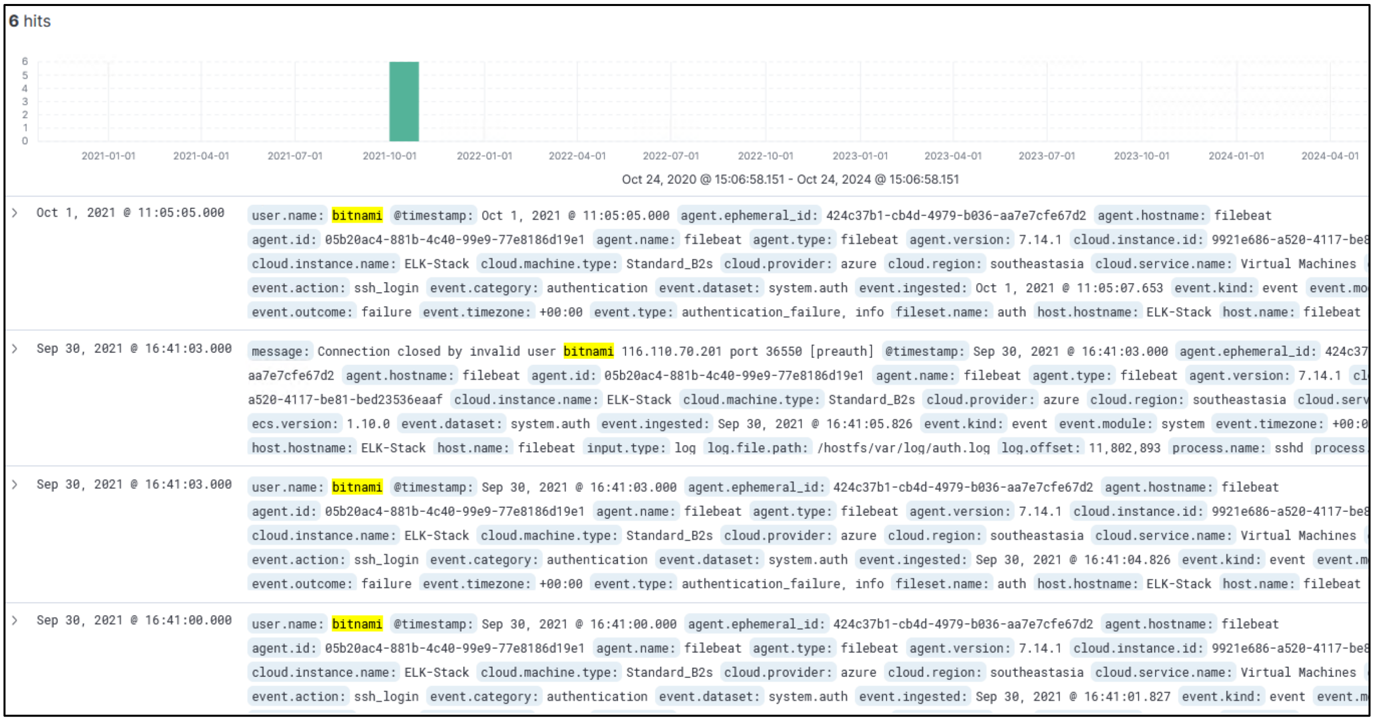


428,917 hits

Last 4 years

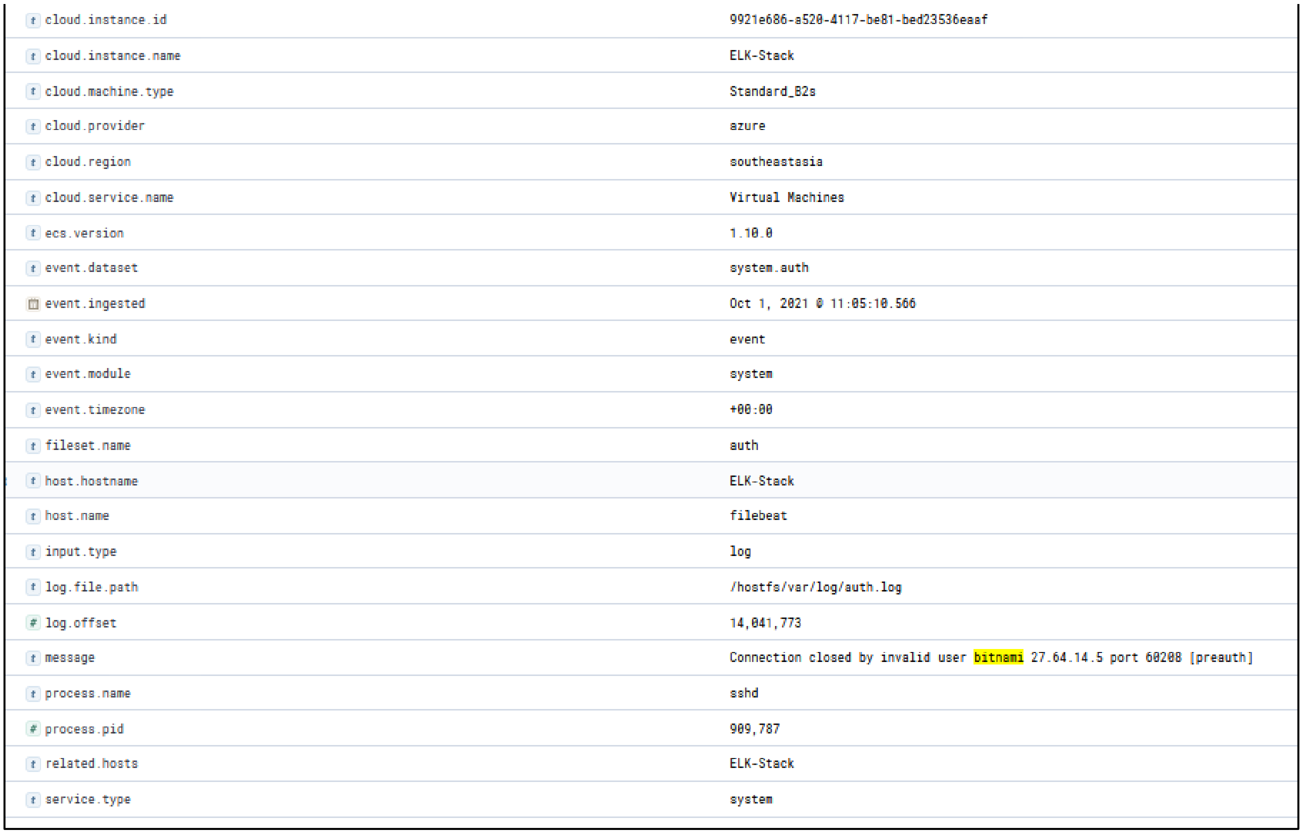
Oct 21, 2020 @ 15:41:35.028 - Oct 21, 2024 @ 15:41:35.028

Figure 1:ELk dashboard



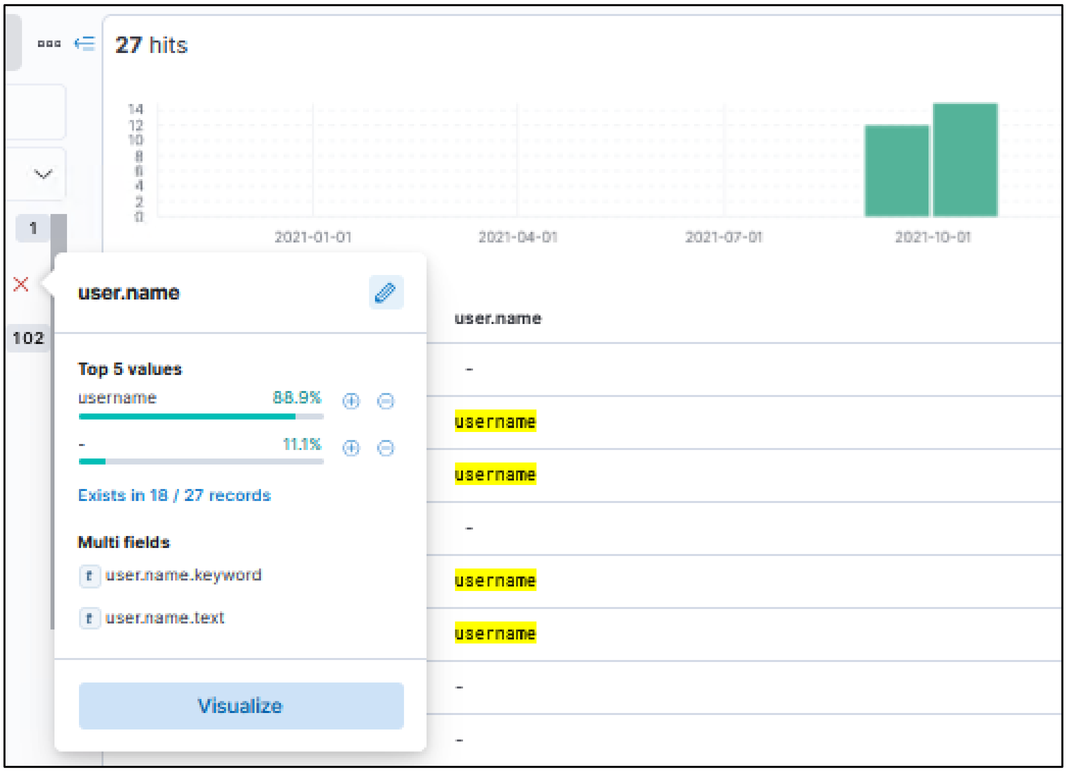
```
> Oct 1, 2021 @ 11:05:05.000    user.name: bitnami @timestamp: Oct 1, 2021 @ 11:05:05.000 agent.ephemeral_id: 424c37b1-cb4d-4979-b036-aa7e7cfe67d2 agent.hostname: filebeat
                                agent.id: 05b20ac4-881b-4c40-99e9-77e8186d19e1 agent.name: filebeat agent.type: filebeat agent.version: 7.14.1 cloud.instance.id: 9921e686-a520-4117-be8
                                cloud.instance.name: ELK-Stack cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines
                                event.action: ssh_login event.category: authentication event.dataset: system.auth event.ingested: Oct 1, 2021 @ 11:05:07.653 event.kind: event event.mo
                                event.outcome: failure event.timezone: +00:00 event.type: authentication_failure, info fileset.name: auth host.hostname: ELK-Stack host.name: filebeat

> Sep 30, 2021 @ 16:41:03.000   message: Connection closed by invalid user bitnami 116.110.70.201 port 36550 [preauth] @timestamp: Sep 30, 2021 @ 16:41:03.000 agent.ephemeral_id: 424c37
                                aa7e7cfe67d2 agent.hostname: filebeat agent.id: 05b20ac4-881b-4c40-99e9-77e8186d19e1 agent.name: filebeat agent.type: filebeat agent.version: 7.14.1 cl
                                a520-4117-be81-bed23536eaaf cloud.instance.name: ELK-Stack cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.serv
                                ecs.version: 1.10.0 event.dataset: system.auth event.ingested: Sep 30, 2021 @ 16:41:05.826 event.kind: event event.module: system event.timezone: +00:0
                                host.hostname: ELK-Stack host.name: filebeat input.type: log log.file.path: /hostfs/var/log/auth.log log.offset: 11,802,893 process.name: sshd process.

> Sep 30, 2021 @ 16:41:03.000   user.name: bitnami @timestamp: Sep 30, 2021 @ 16:41:03.000 agent.ephemeral_id: 424c37b1-cb4d-4979-b036-aa7e7cfe67d2 agent.hostname: filebeat
                                agent.id: 05b20ac4-881b-4c40-99e9-77e8186d19e1 agent.name: filebeat agent.type: filebeat agent.version: 7.14.1 cloud.instance.id: 9921e686-a520-4117-be8
                                cloud.instance.name: ELK-Stack cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines
                                event.action: ssh_login event.category: authentication event.dataset: system.auth event.ingested: Sep 30, 2021 @ 16:41:04.826 event.kind: event event.m
                                event.outcome: failure event.timezone: +00:00 event.type: authentication_failure, info fileset.name: auth host.hostname: ELK-Stack host.name: filebeat

> Sep 30, 2021 @ 16:41:00.000   user.name: bitnami @timestamp: Sep 30, 2021 @ 16:41:00.000 agent.ephemeral_id: 424c37b1-cb4d-4979-b036-aa7e7cfe67d2 agent.hostname: filebeat
                                agent.id: 05b20ac4-881b-4c40-99e9-77e8186d19e1 agent.name: filebeat agent.type: filebeat agent.version: 7.14.1 cloud.instance.id: 9921e686-a520-4117-be8
                                cloud.instance.name: ELK-Stack cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines
                                event.action: ssh_login event.category: authentication event.dataset: system.auth event.ingested: Sep 30, 2021 @ 16:41:01.827 event.kind: event event.m
```

Figure 3:results after searching "bitnami"



t cloud.instance.id	9921e686-a520-4117-be81-bed23536eaaf
t cloud.instance.name	ELK-Stack
t cloud.machine.type	Standard_B2s
t cloud.provider	azure
t cloud.region	southeastasia
t cloud.service.name	Virtual Machines
t ecs.version	1.10.0
t event.dataset	system.auth
event.ingested	Oct 1, 2021 @ 11:05:10.566
t event.kind	event
t event.module	system
t event.timezone	+00:00
t fileset.name	auth
t host.hostname	ELK-Stack
t host.name	filebeat
t input.type	log
t log.file.path	/hostfs/var/log/auth.log
# log.offset	14,041,773
t message	Connection closed by invalid user bitnami 27.64.14.5 port 60208 [preauth]
t process.name	sshd
# process.pid	909,787
t related.hosts	ELK-Stack
t service.type	system

Figure 2:expanded version of results



27 hits

user.name

Top 5 values

username	88.9%
-	11.1%

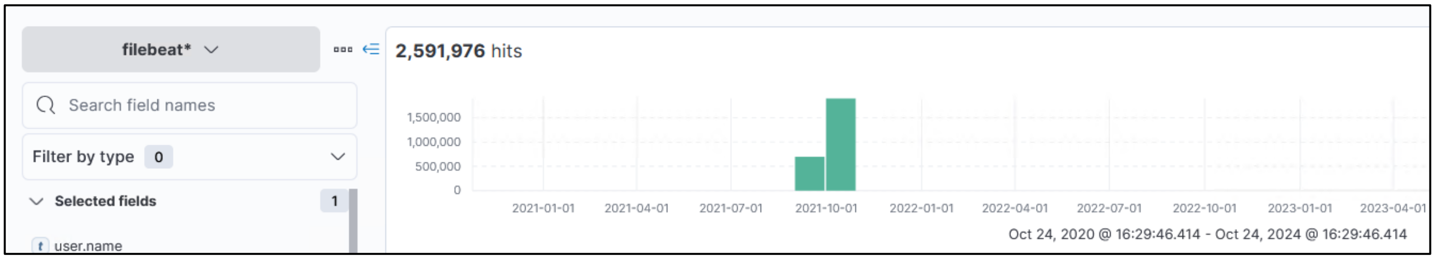
Exists in 18 / 27 records

Multi fields

- user.name.keyword
- user.name.text

user.name
-
username
username
-
username
username
-
-

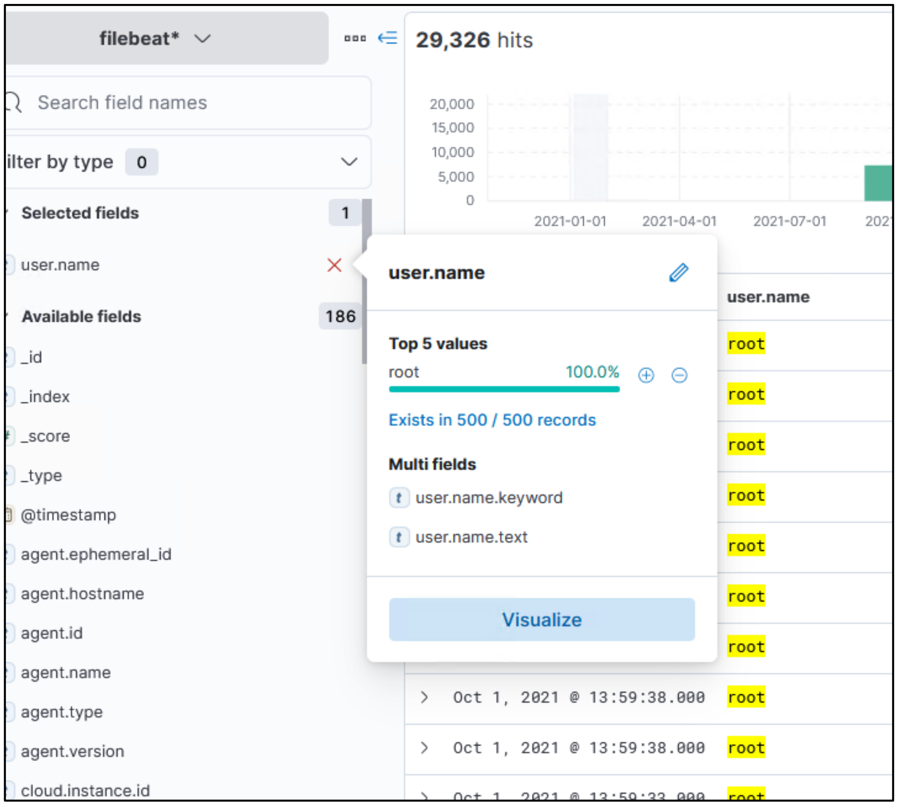
Figure 4:filter the usernames



2,591,976 hits

Oct 24, 2020 @ 16:29:46.414 - Oct 24, 2024 @ 16:29:46.414

Figure 5:filebeat score



29,326 hits

Selected fields 1

user.name

Available fields 186

_id
_index
_score
_type
@timestamp
agent.ephemeral_id
agent.hostname
agent.id
agent.name
agent.type
agent.version
cloud.instance.id

user.name

Top 5 values

root 100.0%

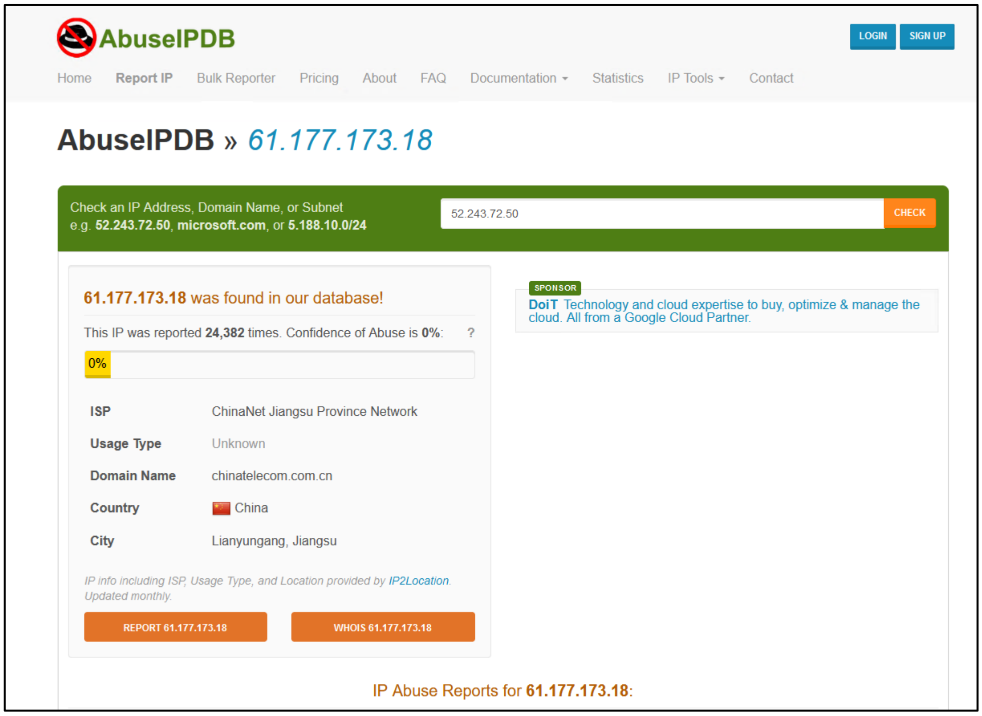
Exists in 500 / 500 records

Multi fields

user.name.keyword
user.name.text

```
                          user.name
                          root
                          root
                          root
                          root
                          root
                          root
                          root
Oct 1, 2021 @ 13:59:38.000  root
Oct 1, 2021 @ 13:59:38.000  root
Oct 1, 2021 @ 13:59:33.000  root
```

Figure 6:username :root



AbuseIPDB » 61.177.173.18

Check an IP Address, Domain Name, or Subnet
e.g. 52.243.72.50, microsoft.com, or 5.188.10.0/24

52.243.72.50

SPONSOR
DoiT Technology and cloud expertise to buy, optimize & manage the cloud. All from a Google Cloud Partner.

61.177.173.18 was found in our database!

This IP was reported 24,382 times. Confidence of Abuse is 0%: ?

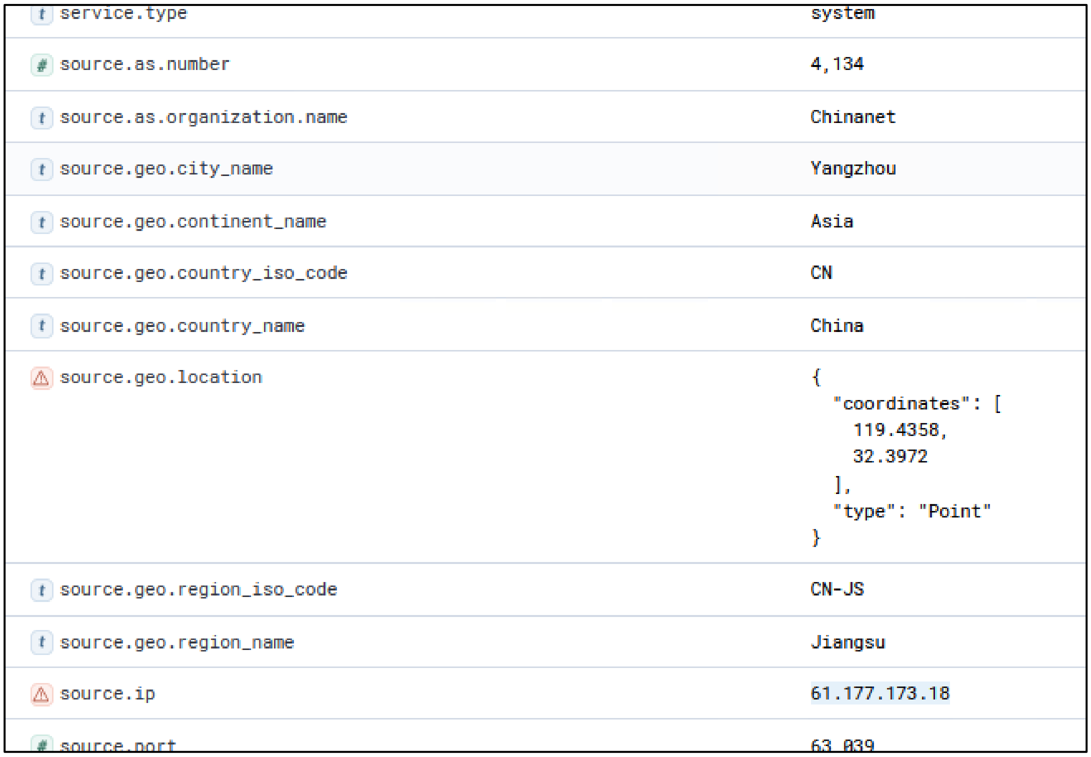
0%

ISP	ChinaNet Jiangsu Province Network
Usage Type	Unknown
Domain Name	chinatelecom.com.cn
Country	China
City	Lianyungang, Jiangsu

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

IP Abuse Reports for 61.177.173.18:

Figure 7:checking ip addresses reputation

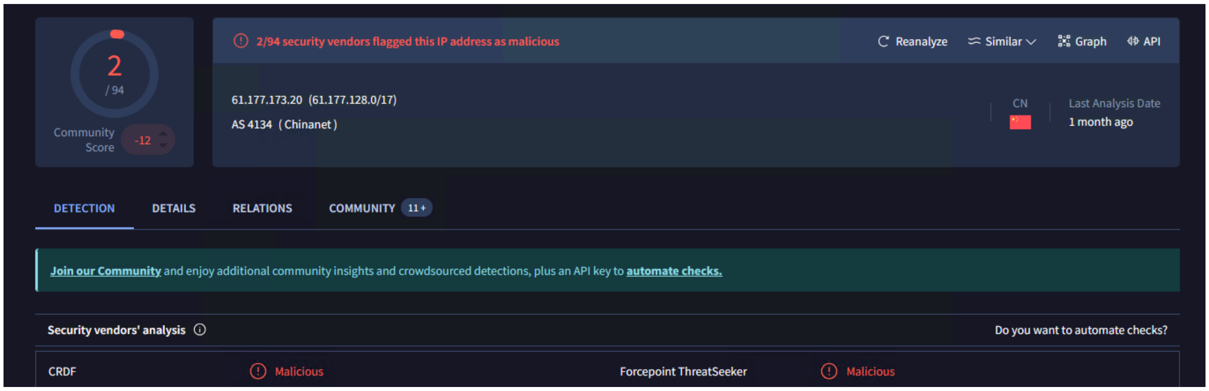


t service.type	system
# source.as.number	4,134
t source.as.organization.name	Chinanet
t source.geo.city_name	Yangzhou
t source.geo.continent_name	Asia
t source.geo.country_iso_code	CN
t source.geo.country_name	China

⚠ source.geo.location	{
	"coordinates": [
	119.4358,
	32.3972
	],
	"type": "Point"
	}

t source.geo.region_iso_code	CN-JS
t source.geo.region_name	Jiangsu
⚠ source.ip	61.177.173.18
# source.port	63,039

Figure 8:random expanded result of root



2 / 94

Community Score -12

2/94 security vendors flagged this IP address as malicious

61.177.173.20 (61.177.128.0/17)

AS 4134 (Chinanet)

CN

Last Analysis Date 1 month ago

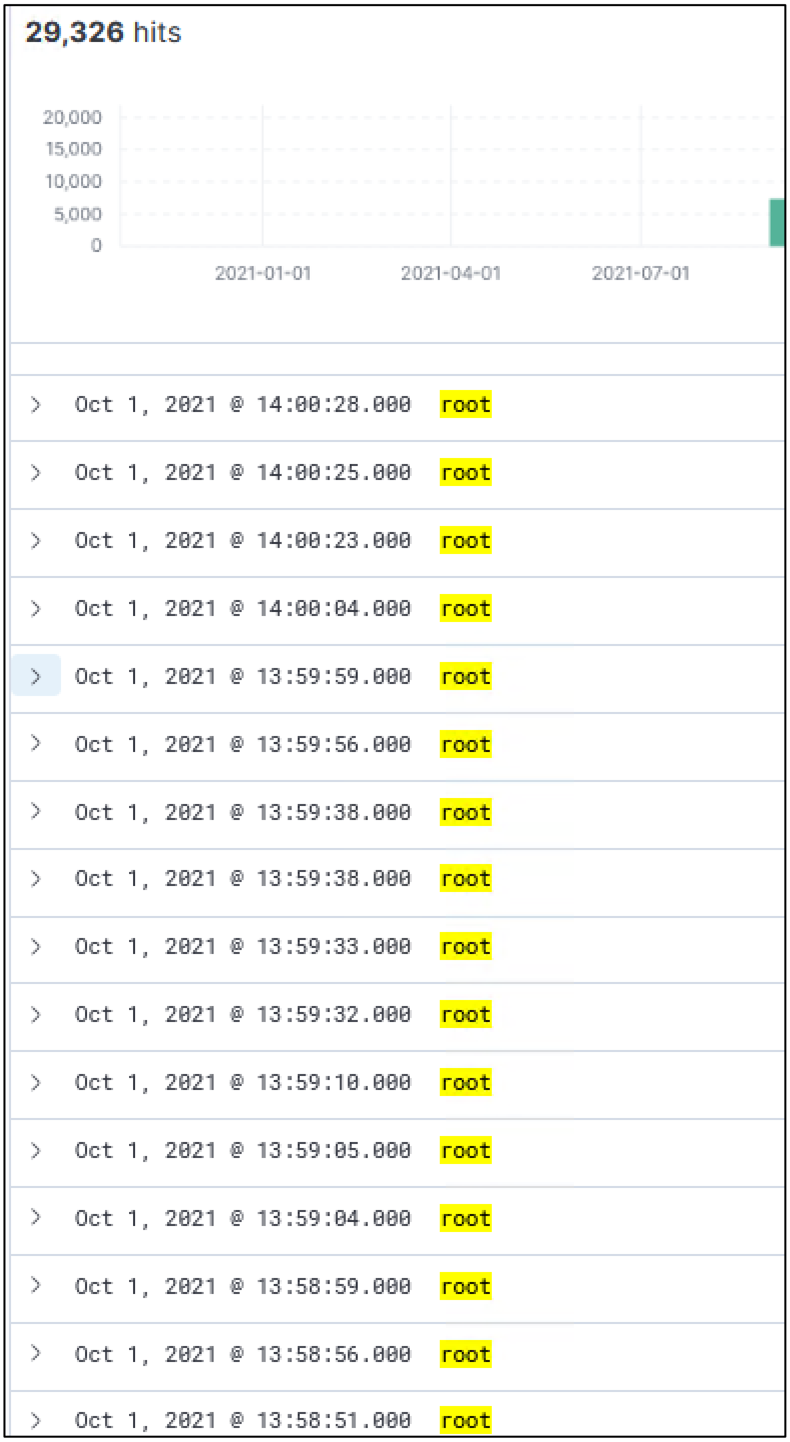
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

CRDF	Malicious	Forcepoint ThreatSeeker	Malicious

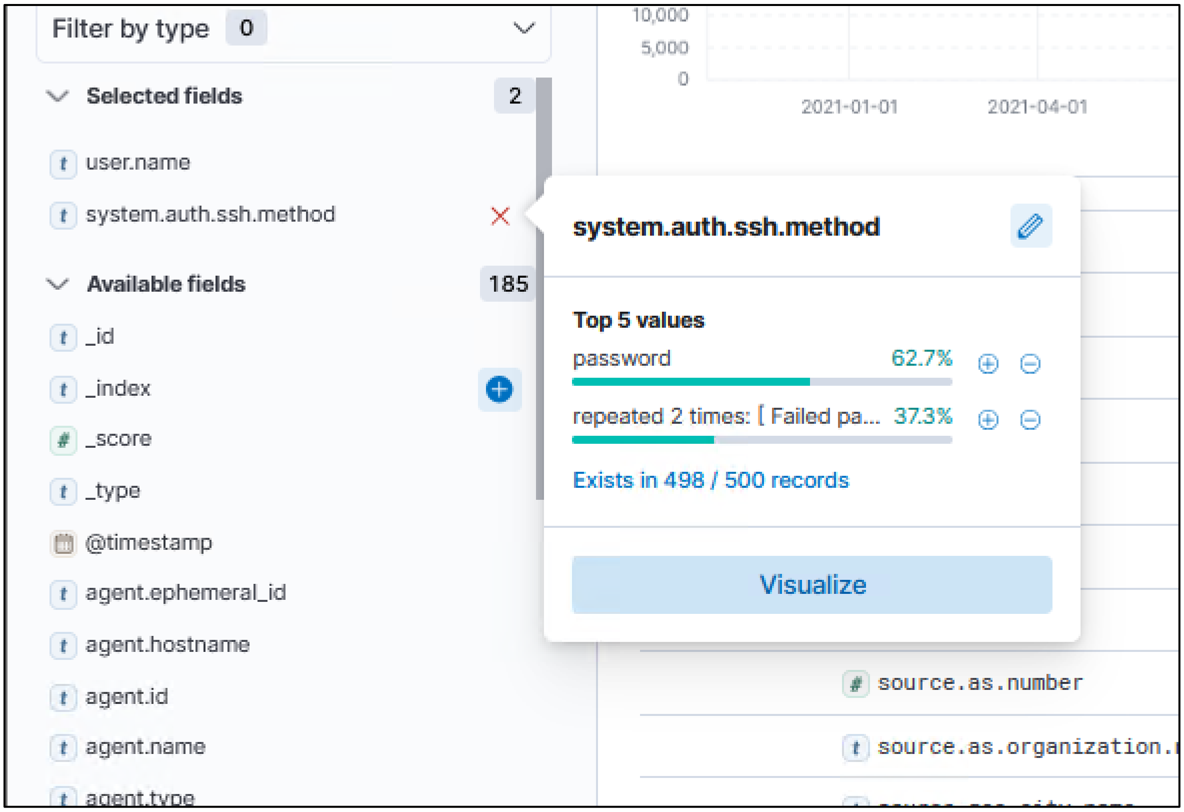
Figure 9:virustotal score of suspicious ip address from china



29,326 hits

```
>  Oct 1, 2021 @ 14:00:28.000  root
>  Oct 1, 2021 @ 14:00:25.000  root
>  Oct 1, 2021 @ 14:00:23.000  root
>  Oct 1, 2021 @ 14:00:04.000  root
>  Oct 1, 2021 @ 13:59:59.000  root
>  Oct 1, 2021 @ 13:59:56.000  root
>  Oct 1, 2021 @ 13:59:38.000  root
>  Oct 1, 2021 @ 13:59:38.000  root
>  Oct 1, 2021 @ 13:59:33.000  root
>  Oct 1, 2021 @ 13:59:32.000  root
>  Oct 1, 2021 @ 13:59:10.000  root
>  Oct 1, 2021 @ 13:59:05.000  root
>  Oct 1, 2021 @ 13:59:04.000  root
>  Oct 1, 2021 @ 13:58:59.000  root
>  Oct 1, 2021 @ 13:58:56.000  root
>  Oct 1, 2021 @ 13:58:51.000  root
```

Figure 10:root user logging attempts



system.auth.ssh.method

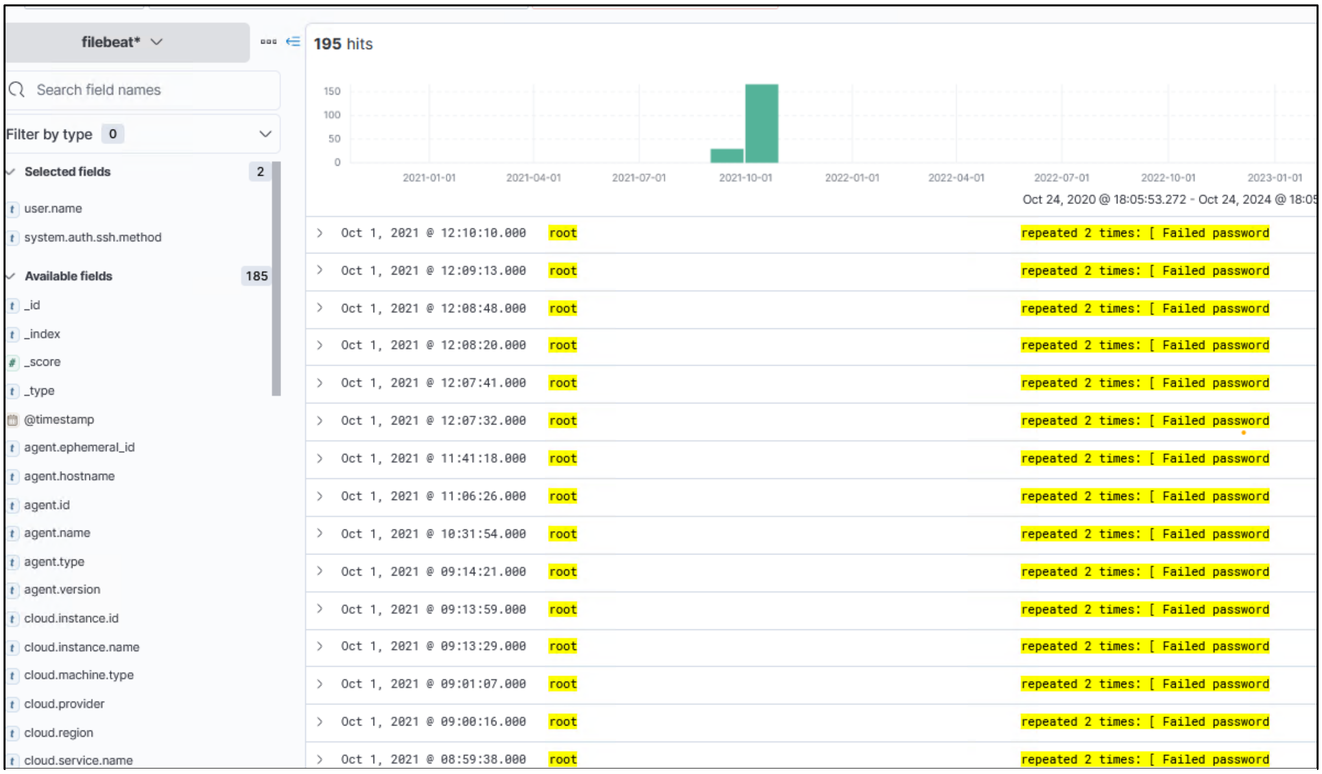
Top 5 values

password 62.7%

repeated 2 times: [Failed pa... 37.3%

Exists in 498 / 500 records

Figure 12:loking for field that repeated 2-time failed attempts

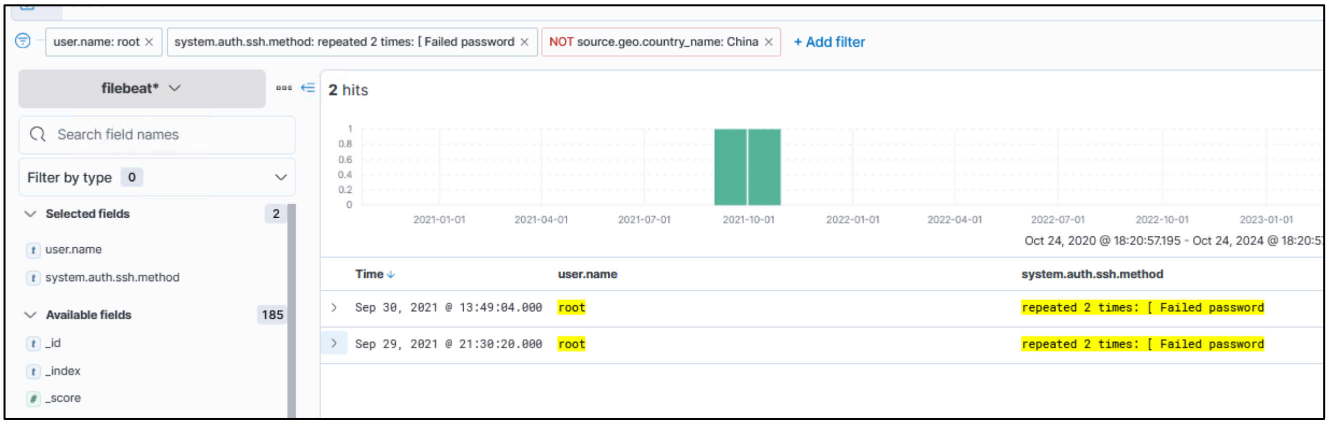


195 hits

Oct 24, 2020 @ 18:05:53.272 - Oct 24, 2024 @ 18:05

```
Oct 1, 2021 @ 12:10:10.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 12:09:13.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 12:08:48.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 12:08:20.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 12:07:41.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 12:07:32.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 11:41:18.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 11:06:26.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 10:31:54.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 09:14:21.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 09:13:59.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 09:13:29.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 09:01:07.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 09:00:16.000  root   repeated 2 times: [ Failed password
Oct 1, 2021 @ 08:59:38.000  root   repeated 2 times: [ Failed password
```

Figure 11:overview of continuous 2 repeated logging attempts



user.name: root × | system.auth.ssh.method: repeated 2 times: [Failed password × | NOT source.geo.country_name: China × | + Add filter

filebeat*

Search field names

Filter by type 0

Selected fields 2
- user.name
- system.auth.ssh.method

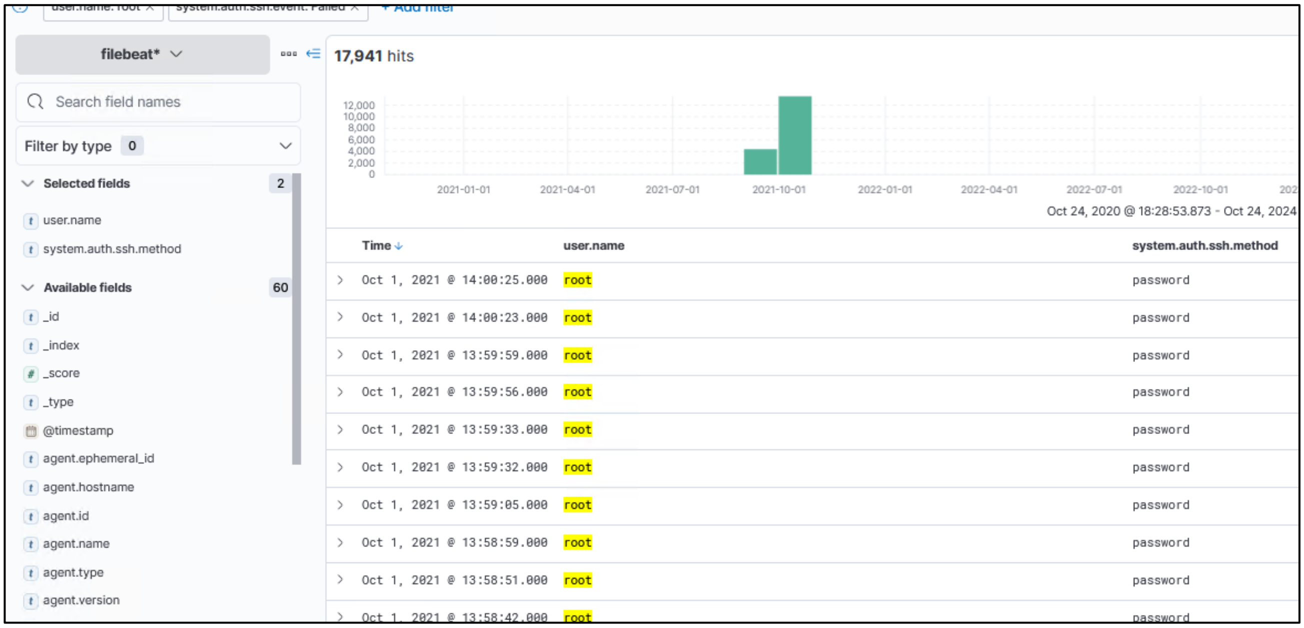
Available fields 185
- _id
- _index
- _score

2 hits

Oct 24, 2020 @ 18:20:57.195 - Oct 24, 2024 @ 18:20:5

Time ↓	user.name	system.auth.ssh.method
Sep 30, 2021 @ 13:49:04.000	root	repeated 2 times: [Failed password
Sep 29, 2021 @ 21:30:20.000	root	repeated 2 times: [Failed password

Figure 13:other 2 repeated failed attempts that not from China



user.name: root × | system.auth.ssh.event: Failed × | + Add filter

filebeat*

Search field names

Filter by type 0

Selected fields 2
- user.name
- system.auth.ssh.method

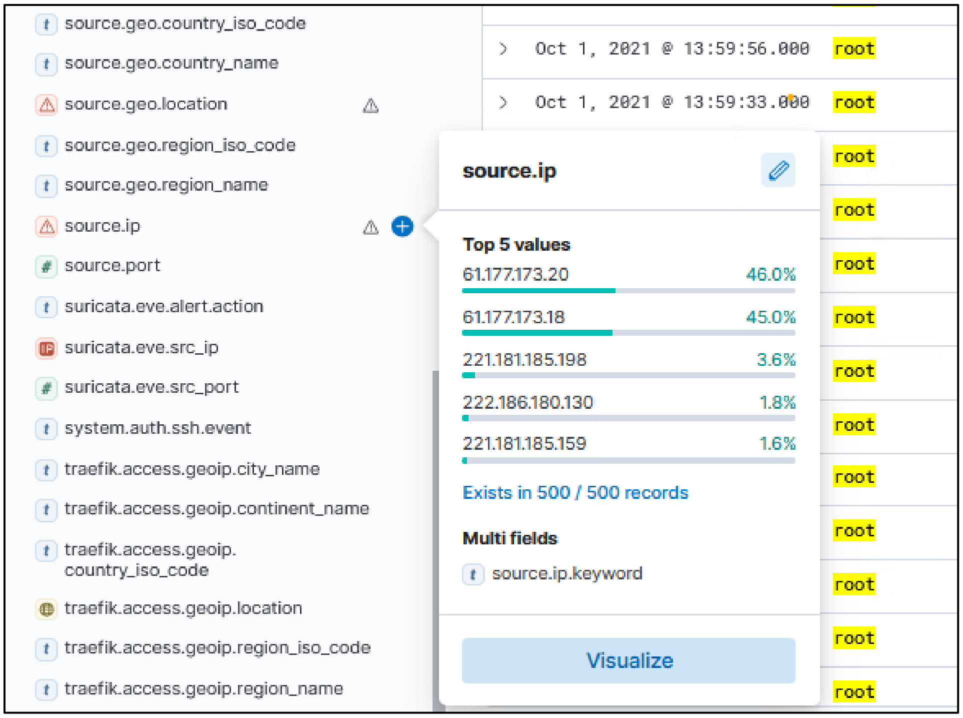
Available fields 60
- _id
- _index
- _score
- _type
- @timestamp
- agent.ephemeral_id
- agent.hostname
- agent.id
- agent.name
- agent.type
- agent.version

17,941 hits

Oct 24, 2020 @ 18:28:53.873 - Oct 24, 2024

Time ↓	user.name	system.auth.ssh.method
Oct 1, 2021 @ 14:00:25.000	root	password
Oct 1, 2021 @ 14:00:23.000	root	password
Oct 1, 2021 @ 13:59:59.000	root	password
Oct 1, 2021 @ 13:59:56.000	root	password
Oct 1, 2021 @ 13:59:33.000	root	password
Oct 1, 2021 @ 13:59:32.000	root	password
Oct 1, 2021 @ 13:59:05.000	root	password
Oct 1, 2021 @ 13:58:59.000	root	password
Oct 1, 2021 @ 13:58:51.000	root	password
Oct 1, 2021 @ 13:58:42.000	root	password

Figure 14:root password attempts


source.geo.country_iso_code
source.geo.country_name
source.geo.location
source.geo.region_iso_code
source.geo.region_name
source.ip
source.port
suricata.eve.alert.action
suricata.eve.src_ip
suricata.eve.src_port
system.auth.ssh.event
traefik.access.geoip.city_name
traefik.access.geoip.continent_name
traefik.access.geoip.country_iso_code
traefik.access.geoip.location
traefik.access.geoip.region_iso_code
traefik.access.geoip.region_name
Visualize

```
Oct 1, 2021 @ 13:59:56.000  root
Oct 1, 2021 @ 13:59:33.000  root
```

source.ip

Top 5 values

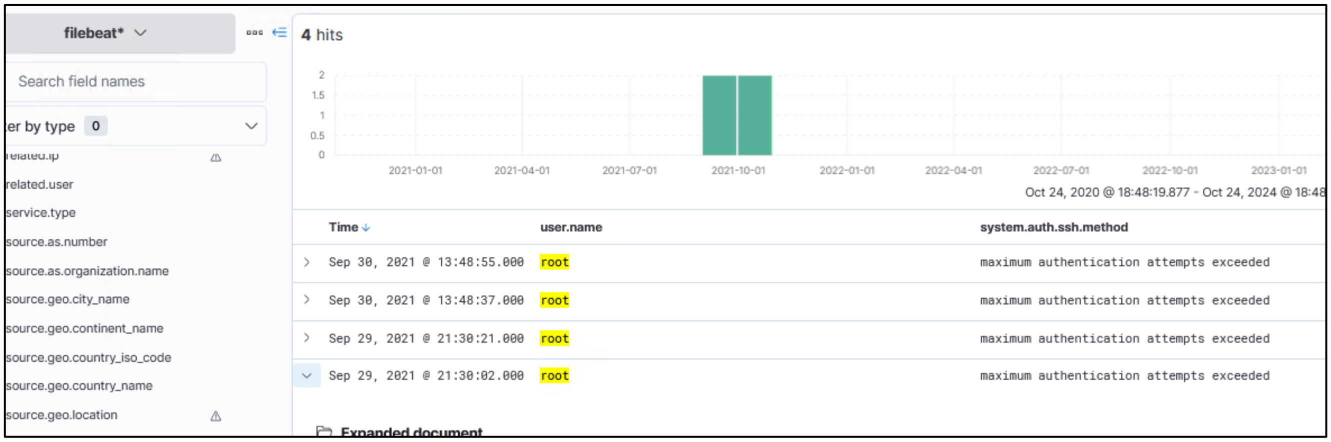
61.177.173.20	46.0%
61.177.173.18	45.0%
221.181.185.198	3.6%
222.186.180.130	1.8%
221.181.185.159	1.6%

Exists in 500 / 500 records

Multi fields

source.ip.keyword

Figure 15:source ips that interact with the logging attempts

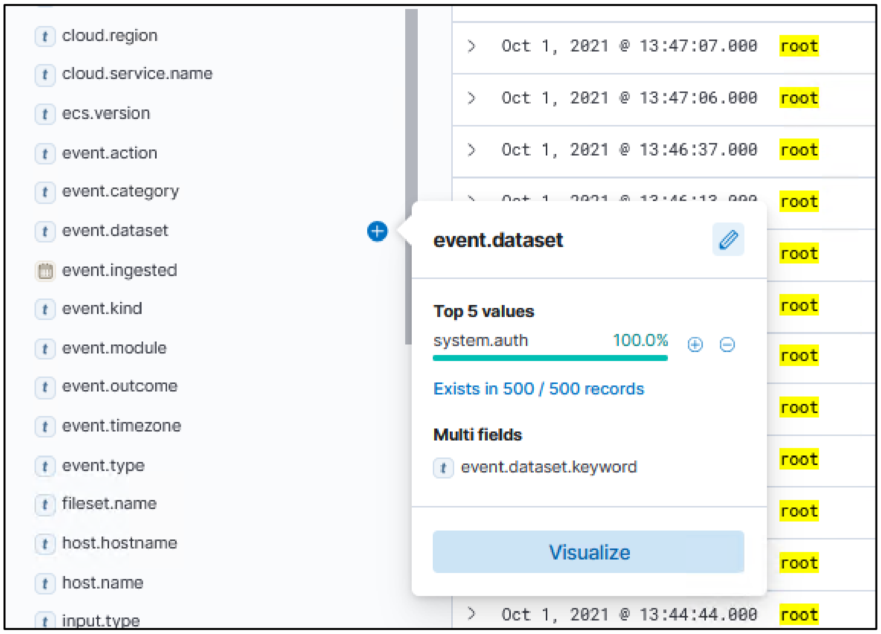


4 hits

Oct 24, 2020 @ 18:48:19.877 - Oct 24, 2024 @ 18:48

```
Time                          user.name      system.auth.ssh.method
Sep 30, 2021 @ 13:48:55.000   root           maximum authentication attempts exceeded
Sep 30, 2021 @ 13:48:37.000   root           maximum authentication attempts exceeded
Sep 29, 2021 @ 21:30:21.000   root           maximum authentication attempts exceeded
Sep 29, 2021 @ 21:30:02.000   root           maximum authentication attempts exceeded
```

Figure 16:logging attempts that came errors



- cloud.region
- cloud.service.name
- ecs.version
- event.action
- event.category
- event.dataset
- event.ingested
- event.kind
- event.module
- event.outcome
- event.timezone
- event.type
- fileset.name
- host.hostname
- host.name
- input.type

```
> Oct 1, 2021 @ 13:47:07.000 root
> Oct 1, 2021 @ 13:47:06.000 root
> Oct 1, 2021 @ 13:46:37.000 root
> Oct 1, 2021 @ 13:46:13.000 root
                             root
                             root
                             root
                             root
                             root
                             root
                             root
> Oct 1, 2021 @ 13:44:44.000 root
```

event.dataset

Top 5 values

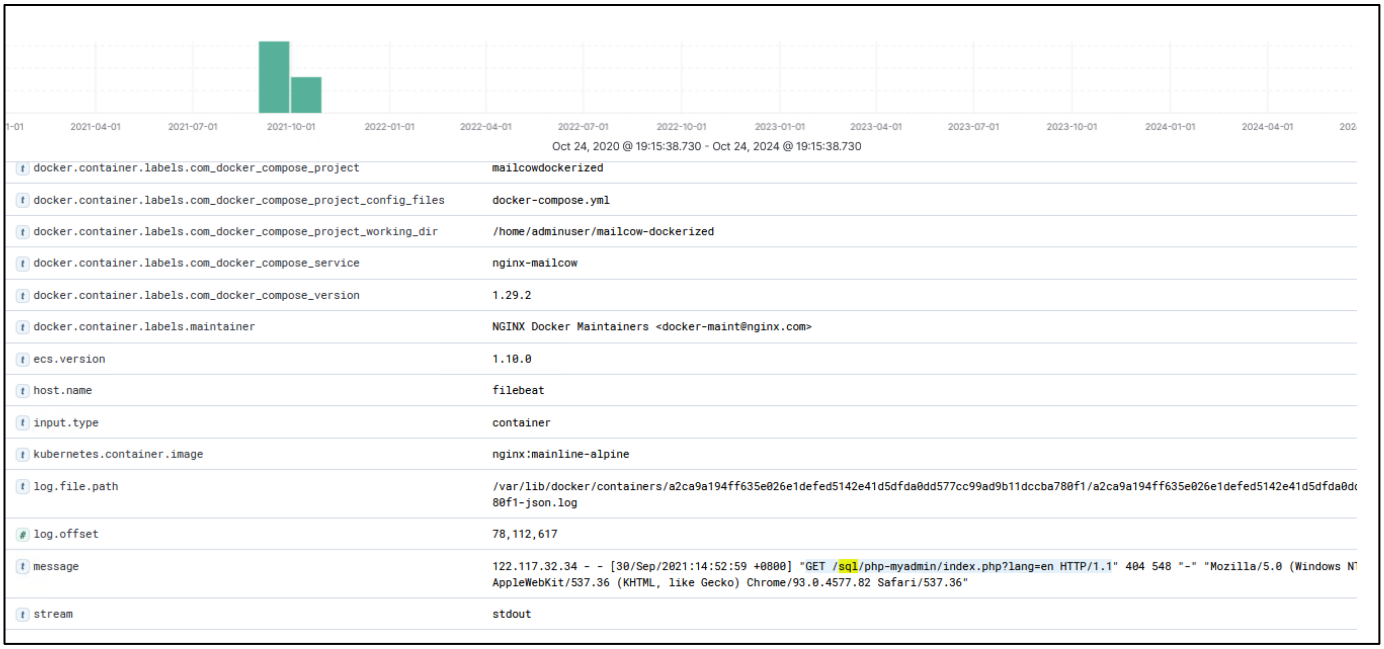
system.auth 100.0%

Exists in 500 / 500 records

Multi fields

event.dataset.keyword

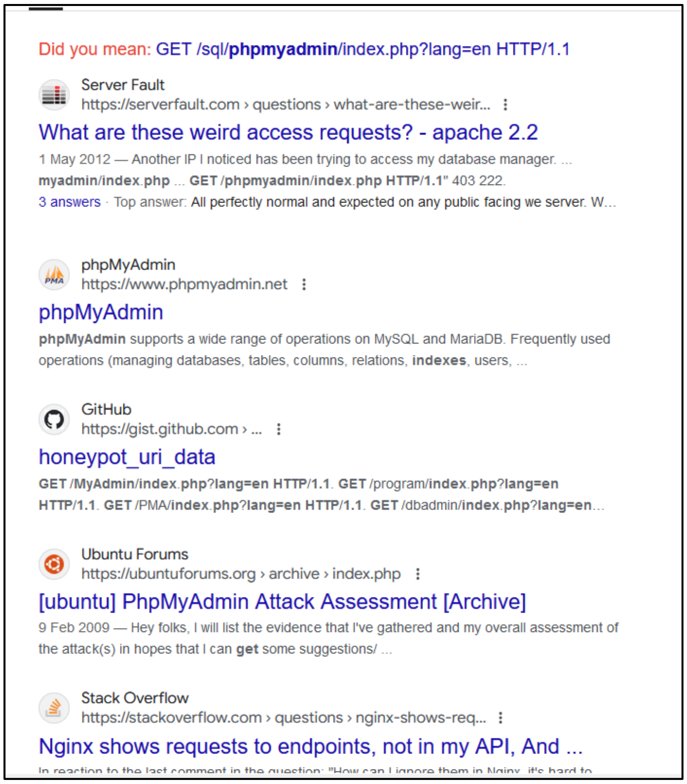
Figure 17:field data of event dataset



Oct 24, 2020 @ 19:15:38.730 - Oct 24, 2024 @ 19:15:38.730

docker.container.labels.com_docker_compose_project	mailcowdockerized
docker.container.labels.com_docker_compose_project_config_files	docker-compose.yml
docker.container.labels.com_docker_compose_project_working_dir	/home/adminuser/mailcow-dockerized
docker.container.labels.com_docker_compose_service	nginx-mailcow
docker.container.labels.com_docker_compose_version	1.29.2
docker.container.labels.maintainer	NGINX Docker Maintainers <docker-maint@nginx.com>
ecs.version	1.10.0
host.name	filebeat
input.type	container
kubernetes.container.image	nginx:mainline-alpine
log.file.path	/var/lib/docker/containers/a2ca9a194ff635e026e1defed5142e41d5dfda0dd577cc99ad9b11dccba780f1/a2ca9a194ff635e026e1defed5142e41d5dfda0d 80f1-json.log
log.offset	78,112,617
message	122.117.32.34 - - [30/Sep/2021:14:52:59 +0800] "GET /sql/php-myadmin/index.php?lang=en HTTP/1.1" 404 548 "-" "Mozilla/5.0 (Windows N AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36"
stream	stdout

Figure 18:php get request from myadmin



Did you mean: GET /sql/**phpmyadmin**/index.php?lang=en HTTP/1.1

Server Fault
https://serverfault.com › questions › what-are-these-weir...

What are these weird access requests? - apache 2.2

1 May 2012 — Another IP I noticed has been trying to access my database manager. ... **myadmin/index.php** ... **GET /phpmyadmin/index.php HTTP/1.1"** 403 222.
3 answers · Top answer: All perfectly normal and expected on any public facing we server. W...

phpMyAdmin
https://www.phpmyadmin.net

phpMyAdmin

phpMyAdmin supports a wide range of operations on MySQL and MariaDB. Frequently used operations (managing databases, tables, columns, relations, **indexes**, users, ...

GitHub
https://gist.github.com › ...

honeypot_uri_data

GET /**MyAdmin/index.php?lang=en HTTP/1.1**. **GET** /program/**index.php?lang=en HTTP/1.1**. **GET** /PMA/**index.php?lang=en HTTP/1.1**. **GET** /dbadmin/**index.php?lang=en**...

Ubuntu Forums
https://ubuntuforums.org › archive › index.php

[ubuntu] PhpMyAdmin Attack Assessment [Archive]

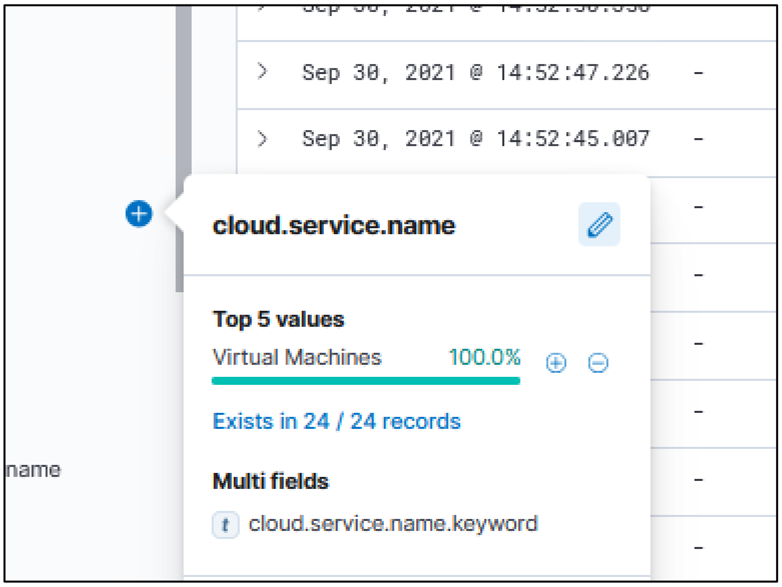
9 Feb 2009 — Hey folks, I will list the evidence that I've gathered and my overall assessment of the attack(s) in hopes that I can **get** some suggestions/ ...

Stack Overflow
https://stackoverflow.com › questions › nginx-shows-req...

Nginx shows requests to endpoints, not in my API, And ...

In reaction to the last comment in the question: "How can I ignore them in Nginx, it's hard to

Figure 19:check weather that php file is malicious or not



```
>  Sep 30, 2021 @ 14:52:47.226  -
>  Sep 30, 2021 @ 14:52:45.007  -
```

cloud.service.name

Top 5 values

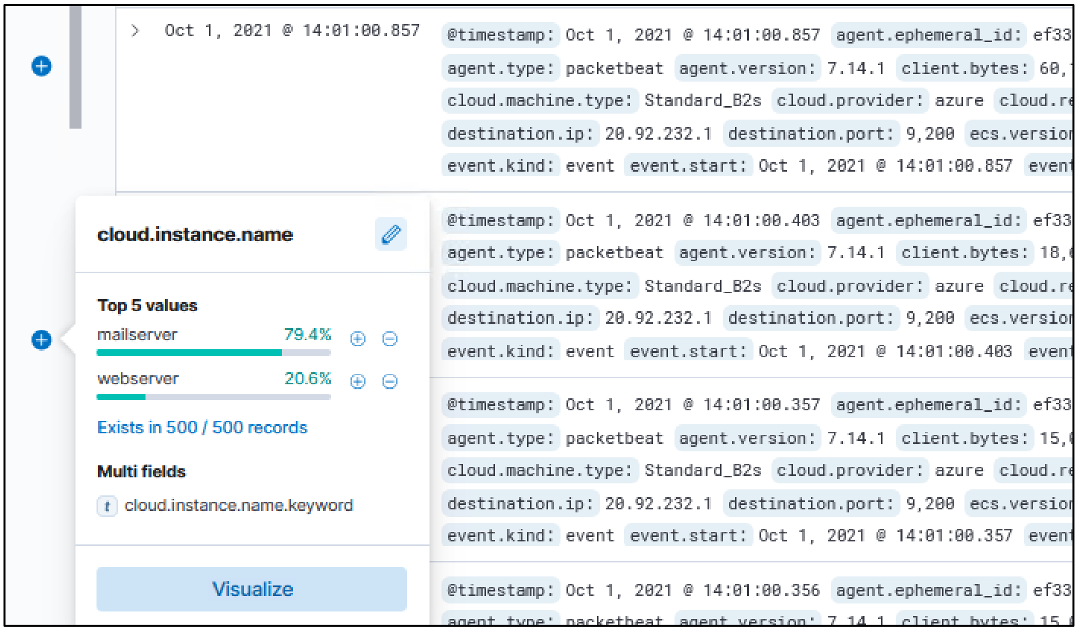
Virtual Machines 100.0%

Exists in 24 / 24 records

Multi fields

t cloud.service.name.keyword

Figure 20:searcxhing for cloud service names that access



```
> Oct 1, 2021 @ 14:01:00.857  @timestamp: Oct 1, 2021 @ 14:01:00.857 agent.ephemeral_id: ef33
                              agent.type: packetbeat agent.version: 7.14.1 client.bytes: 60,
                              cloud.machine.type: Standard_B2s cloud.provider: azure cloud.re
                              destination.ip: 20.92.232.1 destination.port: 9,200 ecs.versior
                              event.kind: event event.start: Oct 1, 2021 @ 14:01:00.857 event

                              @timestamp: Oct 1, 2021 @ 14:01:00.403 agent.ephemeral_id: ef33
                              agent.type: packetbeat agent.version: 7.14.1 client.bytes: 18,
                              cloud.machine.type: Standard_B2s cloud.provider: azure cloud.re
                              destination.ip: 20.92.232.1 destination.port: 9,200 ecs.versior
                              event.kind: event event.start: Oct 1, 2021 @ 14:01:00.403 event

                              @timestamp: Oct 1, 2021 @ 14:01:00.357 agent.ephemeral_id: ef33
                              agent.type: packetbeat agent.version: 7.14.1 client.bytes: 15,
                              cloud.machine.type: Standard_B2s cloud.provider: azure cloud.re
                              destination.ip: 20.92.232.1 destination.port: 9,200 ecs.versior
                              event.kind: event event.start: Oct 1, 2021 @ 14:01:00.357 event

                              @timestamp: Oct 1, 2021 @ 14:01:00.356 agent.ephemeral_id: ef33
                              agent.type: packetbeat agent.version: 7.14.1 client.bytes: 15,
```

cloud.instance.name

Top 5 values

mailserver	79.4%
webserver	20.6%

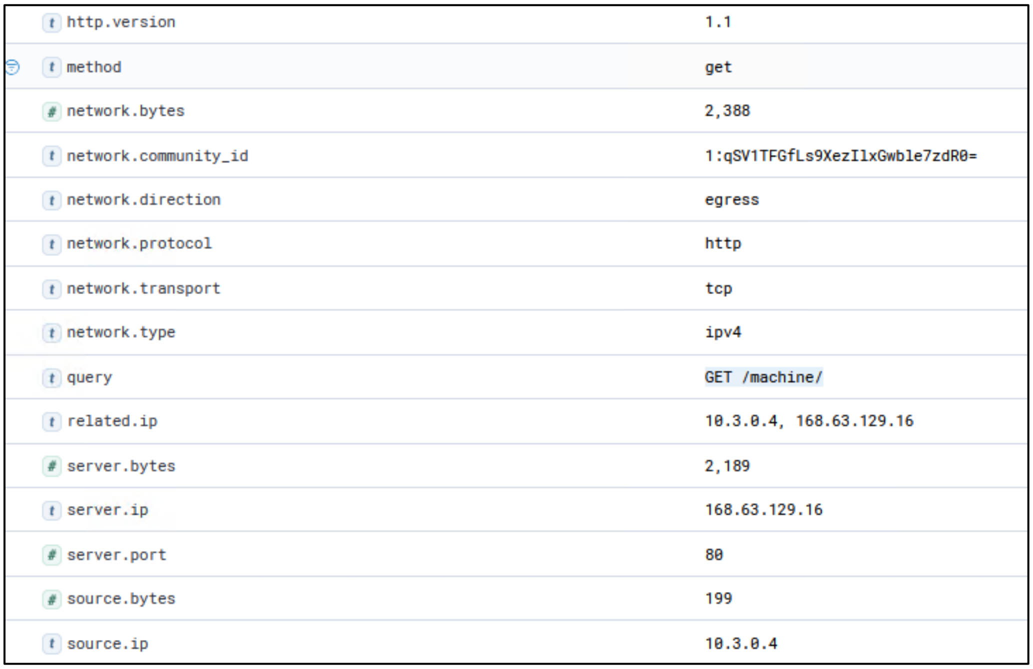
Exists in 500 / 500 records

Multi fields

cloud.instance.name.keyword

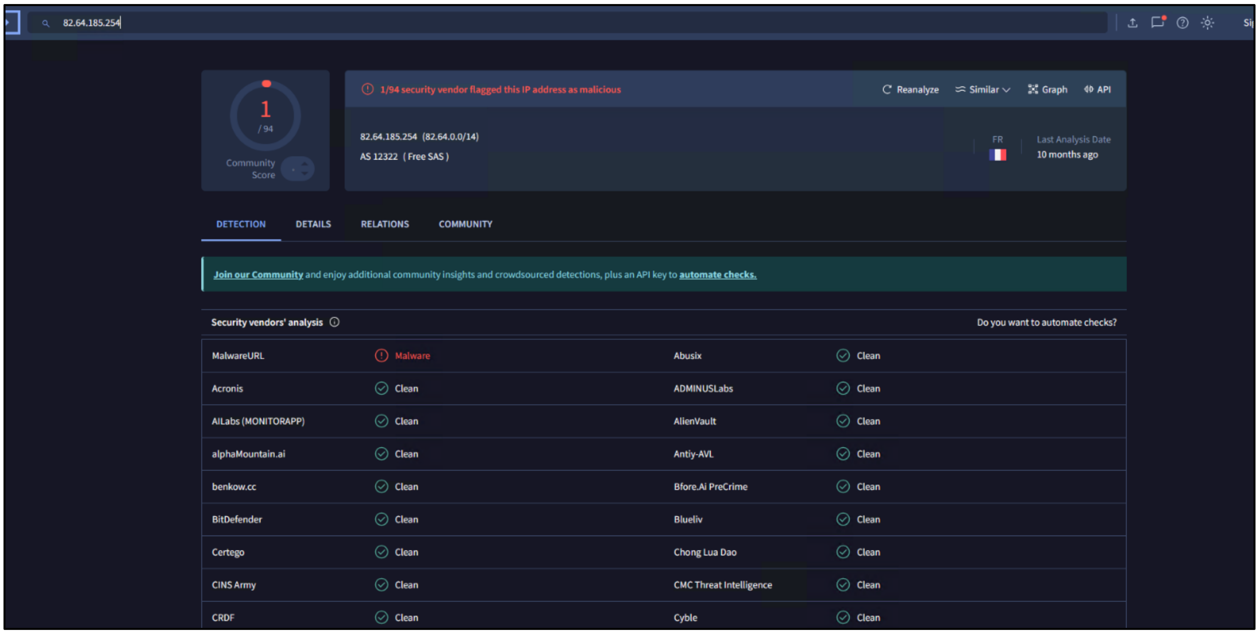
Visualize

Figure 21:filed contain data about cloud instance names



http.version	1.1
method	get
network.bytes	2,388
network.community_id	1:qSV1TFGfLs9XezIlxGwble7zdR0=
network.direction	egress
network.protocol	http
network.transport	tcp
network.type	ipv4
query	GET /machine/
related.ip	10.3.0.4, 168.63.129.16
server.bytes	2,189
server.ip	168.63.129.16
server.port	80
source.bytes	199
source.ip	10.3.0.4

Figure 22:get machine request from sql



1/94 security vendor flagged this IP address as malicious

82.64.185.254 (82.64.0.0/14)
AS 12322 (Free SAS)

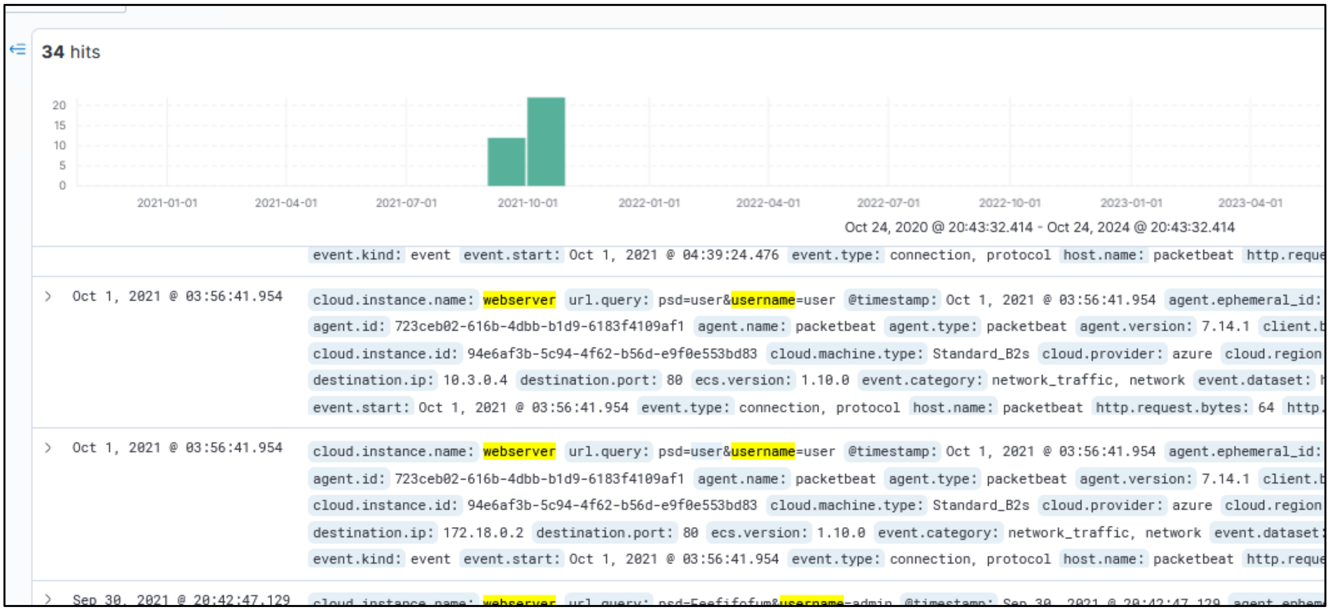
FR
Last Analysis Date
10 months ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

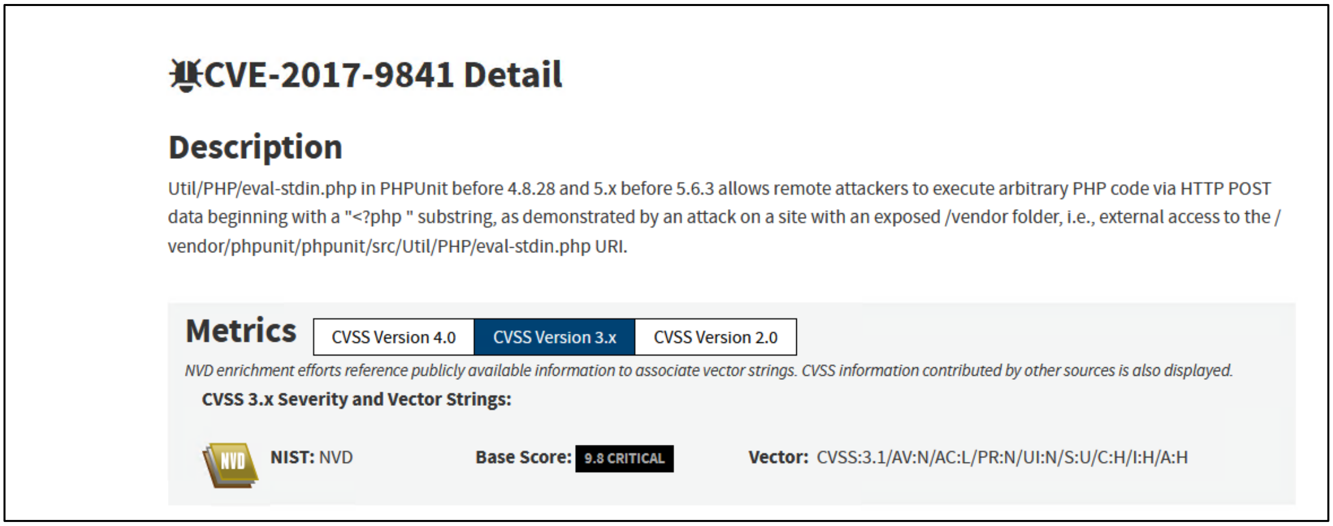
MalwareURL	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
benkow.cc	Clean	Bfore.Ai PreCrime	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Cyble	Clean

Figure 23: searching that ip is malicious or not



```
                               event.kind: event event.start: Oct 1, 2021 @ 04:39:24.476 event.type: connection, protocol host.name: packetbeat http.reque

> Oct 1, 2021 @ 03:56:41.954   cloud.instance.name: webserver url.query: psd=user&username=user @timestamp: Oct 1, 2021 @ 03:56:41.954 agent.ephemeral_id:
                               agent.id: 723ceb02-616b-4dbb-b1d9-6183f4109af1 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.b
                               cloud.instance.id: 94e6af3b-5c94-4f62-b56d-e9f0e553bd83 cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region
                               destination.ip: 10.3.0.4 destination.port: 80 ecs.version: 1.10.0 event.category: network_traffic, network event.dataset: h
                               event.start: Oct 1, 2021 @ 03:56:41.954 event.type: connection, protocol host.name: packetbeat http.request.bytes: 64 http.

> Oct 1, 2021 @ 03:56:41.954   cloud.instance.name: webserver url.query: psd=user&username=user @timestamp: Oct 1, 2021 @ 03:56:41.954 agent.ephemeral_id:
                               agent.id: 723ceb02-616b-4dbb-b1d9-6183f4109af1 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.b
                               cloud.instance.id: 94e6af3b-5c94-4f62-b56d-e9f0e553bd83 cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region
                               destination.ip: 172.18.0.2 destination.port: 80 ecs.version: 1.10.0 event.category: network_traffic, network event.dataset:
                               event.kind: event event.start: Oct 1, 2021 @ 03:56:41.954 event.type: connection, protocol host.name: packetbeat http.reque

> Sep 30, 2021 @ 20:42:47.129  cloud.instance.name: webserver url.query: psd=Feefifofum&username=admin @timestamp: Sep 30, 2021 @ 20:42:47.129 agent.ephem
```

Figure 24:serched the cloud instance webserver



CVE-2017-9841 Detail

Description

Util/PHP/eval-stdin.php in PHPUnit before 4.8.28 and 5.x before 5.6.3 allows remote attackers to execute arbitrary PHP code via HTTP POST data beginning with a "<?php " substring, as demonstrated by an attack on a site with an exposed /vendor folder, i.e., external access to the /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php URI.

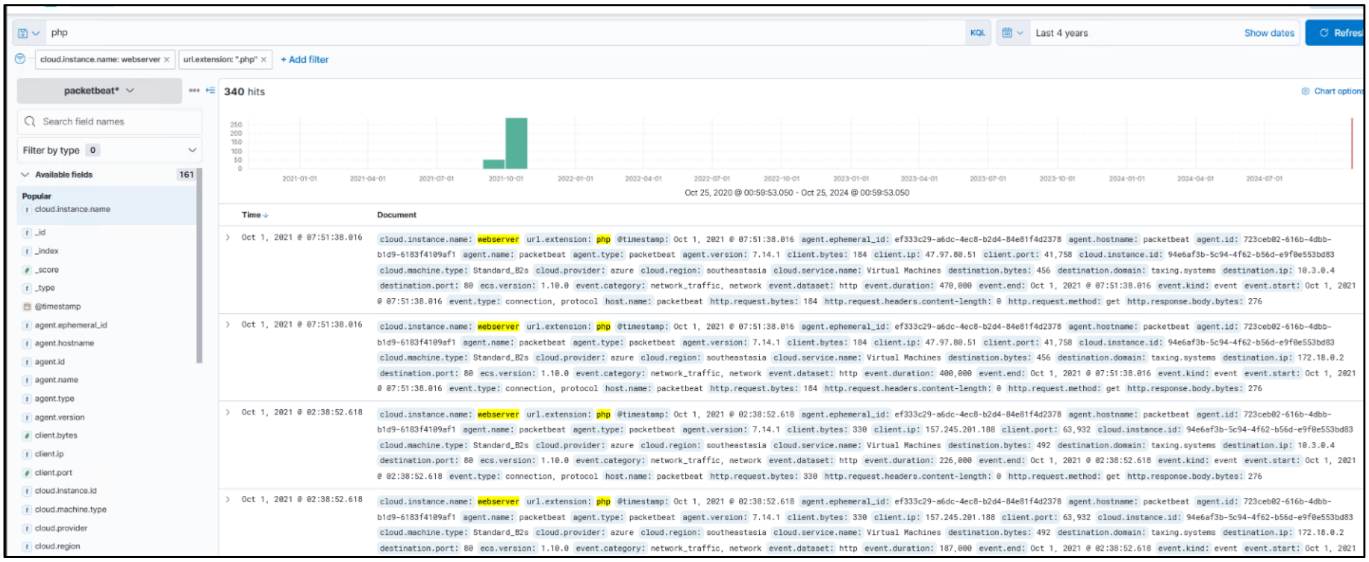
Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

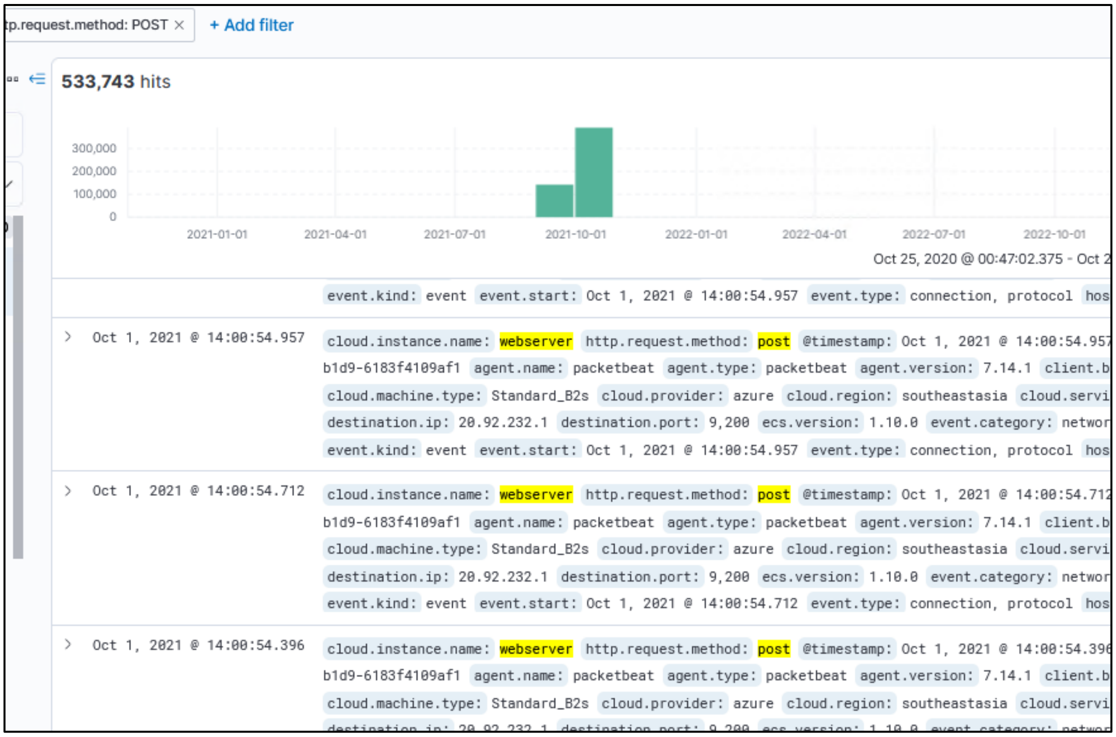
NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Figure 25:found out that ip source that who had access to the php files is malicious



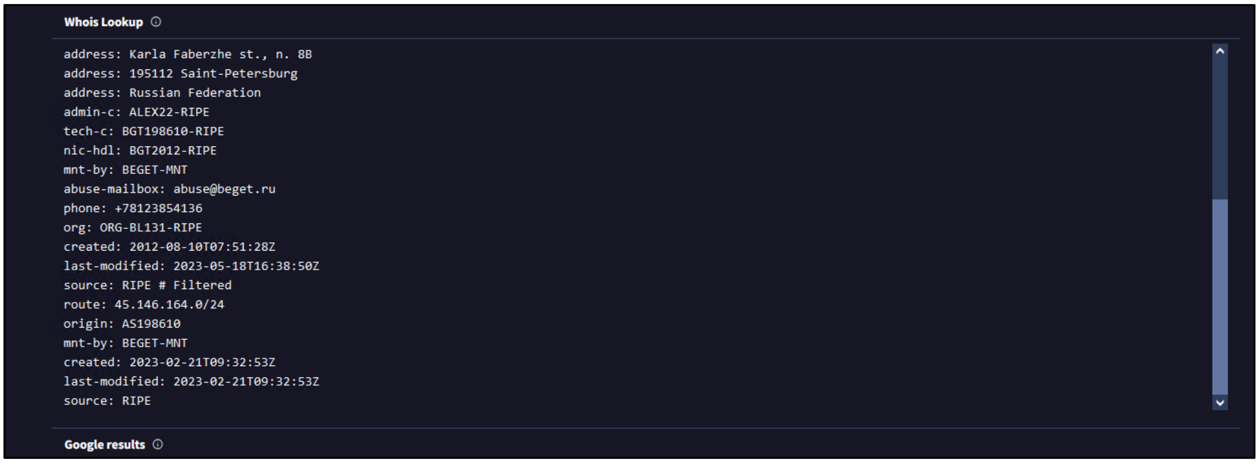
```
Oct 1, 2021 @ 07:51:38.016   cloud.instance.name: webserver url.extension: php @timestamp: Oct 1, 2021 @ 07:51:38.016 agent.ephemeral_id: ef333c29-a6dc-4ec8-b2d4-84e81f4d2378 agent.hostname: packetbeat agent.id: 723ceb02-616b-4dbb-
                             b1d9-6183f4109af1 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.bytes: 184 client.ip: 47.97.80.51 client.port: 41,758 cloud.instance.id: 94e6af3b-5c94-4f62-b56d-e9f0e553bd83
                             cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines destination.bytes: 456 destination.domain: taxing.systems destination.ip: 10.3.0.4
                             destination.port: 80 ecs.version: 1.10.0 event.category: network_traffic, network event.dataset: http event.duration: 470,000 event.end: Oct 1, 2021 @ 07:51:38.016 event.kind: event event.start: Oct 1, 2021
                             @ 07:51:38.016 event.type: connection, protocol host.name: packetbeat http.request.bytes: 184 http.request.headers.content-length: 0 http.request.method: get http.response.body.bytes: 276

Oct 1, 2021 @ 07:51:38.016   cloud.instance.name: webserver url.extension: php @timestamp: Oct 1, 2021 @ 07:51:38.016 agent.ephemeral_id: ef333c29-a6dc-4ec8-b2d4-84e81f4d2378 agent.hostname: packetbeat agent.id: 723ceb02-616b-4dbb-
                             b1d9-6183f4109af1 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.bytes: 184 client.ip: 47.97.80.51 client.port: 41,758 cloud.instance.id: 94e6af3b-5c94-4f62-b56d-e9f0e553bd83
                             cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines destination.bytes: 456 destination.domain: taxing.systems destination.ip: 172.18.0.2
                             destination.port: 80 ecs.version: 1.10.0 event.category: network_traffic, network event.dataset: http event.duration: 400,000 event.end: Oct 1, 2021 @ 07:51:38.016 event.kind: event event.start: Oct 1, 2021
                             @ 07:51:38.016 event.type: connection, protocol host.name: packetbeat http.request.bytes: 184 http.request.headers.content-length: 0 http.request.method: get http.response.body.bytes: 276

Oct 1, 2021 @ 02:38:52.618   cloud.instance.name: webserver url.extension: php @timestamp: Oct 1, 2021 @ 02:38:52.618 agent.ephemeral_id: ef333c29-a6dc-4ec8-b2d4-84e81f4d2378 agent.hostname: packetbeat agent.id: 723ceb02-616b-4dbb-
                             b1d9-6183f4109af1 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.bytes: 330 client.ip: 157.245.201.188 client.port: 63,932 cloud.instance.id: 94e6af3b-5c94-4f62-b56d-e9f0e553bd83
                             cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines destination.bytes: 492 destination.domain: taxing.systems destination.ip: 10.3.0.4
                             destination.port: 80 ecs.version: 1.10.0 event.category: network_traffic, network event.dataset: http event.duration: 226,000 event.end: Oct 1, 2021 @ 02:38:52.618 event.kind: event event.start: Oct 1, 2021
                             @ 02:38:52.618 event.type: connection, protocol host.name: packetbeat http.request.bytes: 330 http.request.headers.content-length: 0 http.request.method: get http.response.body.bytes: 276

Oct 1, 2021 @ 02:38:52.618   cloud.instance.name: webserver url.extension: php @timestamp: Oct 1, 2021 @ 02:38:52.618 agent.ephemeral_id: ef333c29-a6dc-4ec8-b2d4-84e81f4d2378 agent.hostname: packetbeat agent.id: 723ceb02-616b-4dbb-
                             b1d9-6183f4109af1 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.bytes: 330 client.ip: 157.245.201.188 client.port: 63,932 cloud.instance.id: 94e6af3b-5c94-4f62-b56d-e9f0e553bd83
                             cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines destination.bytes: 492 destination.domain: taxing.systems destination.ip: 172.18.0.2
                             destination.port: 80 ecs.version: 1.10.0 event.category: network_traffic, network event.dataset: http event.duration: 187,000 event.end: Oct 1, 2021 @ 02:38:52.618 event.kind: event event.start: Oct 1, 2021
```

Figure 26:webserver php data



```
                            event.kind: event event.start: Oct 1, 2021 @ 14:00:54.957 event.type: connection, protocol hos

> Oct 1, 2021 @ 14:00:54.957  cloud.instance.name: webserver http.request.method: post @timestamp: Oct 1, 2021 @ 14:00:54.957
                            b1d9-6183f4109af1 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.b
                            cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.servi
                            destination.ip: 20.92.232.1 destination.port: 9,200 ecs.version: 1.10.0 event.category: networ
                            event.kind: event event.start: Oct 1, 2021 @ 14:00:54.957 event.type: connection, protocol hos

> Oct 1, 2021 @ 14:00:54.712  cloud.instance.name: webserver http.request.method: post @timestamp: Oct 1, 2021 @ 14:00:54.712
                            b1d9-6183f4109af1 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.b
                            cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.servi
                            destination.ip: 20.92.232.1 destination.port: 9,200 ecs.version: 1.10.0 event.category: networ
                            event.kind: event event.start: Oct 1, 2021 @ 14:00:54.712 event.type: connection, protocol hos

> Oct 1, 2021 @ 14:00:54.396  cloud.instance.name: webserver http.request.method: post @timestamp: Oct 1, 2021 @ 14:00:54.396
                            b1d9-6183f4109af1 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.b
                            cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.servi
                            destination.ip: 20.92.232.1 destination.port: 9,200 ecs.version: 1.10.0 event.category: networ
```

Figure 27:http request methods of webserver

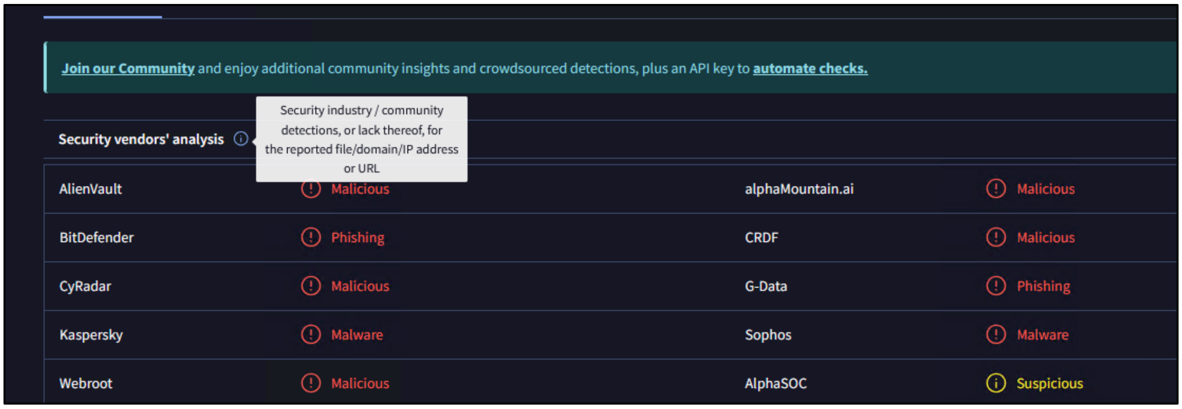


Whois Lookup ⓘ

```
address: Karla Faberzhe st., n. 8B
address: 195112 Saint-Petersburg
address: Russian Federation
admin-c: ALEX22-RIPE
tech-c: BGT198610-RIPE
nic-hdl: BGT2012-RIPE
mnt-by: BEGET-MNT
abuse-mailbox: abuse@beget.ru
phone: +78123854136
org: ORG-BL131-RIPE
created: 2012-08-10T07:51:28Z
last-modified: 2023-05-18T16:38:50Z
source: RIPE # Filtered
route: 45.146.164.0/24
origin: AS198610
mnt-by: BEGET-MNT
created: 2023-02-21T09:32:53Z
last-modified: 2023-02-21T09:32:53Z
source: RIPE
```

Google results ⓘ

Figure 28:detailed view of phishing ip address



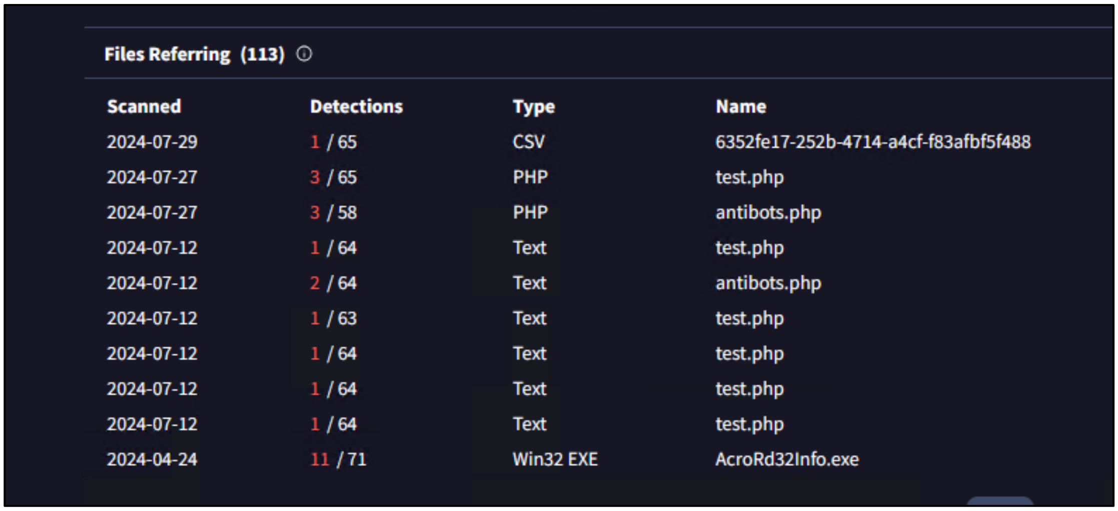
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Security industry / community detections, or lack thereof, for the reported file/domain/IP address or URL

AlienVault	Malicious	alphaMountain.ai	Malicious
BitDefender	Phishing	CRDF	Malicious
CyRadar	Malicious	G-Data	Phishing
Kaspersky	Malware	Sophos	Malware
Webroot	Malicious	AlphaSOC	Suspicious

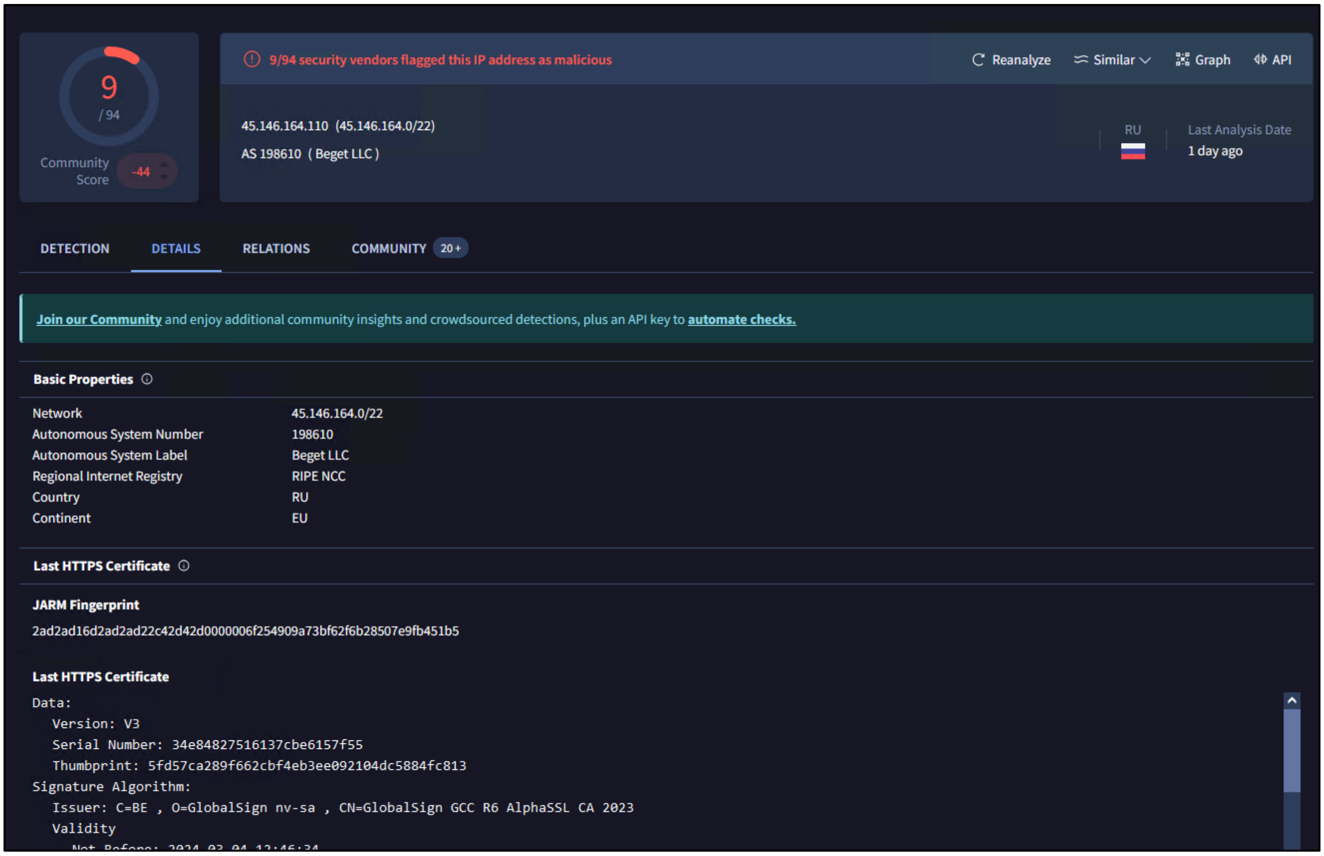
Figure 29:malwer defenders who identified that ip is malicious



Files Referring (113)

Scanned	Detections	Type	Name
2024-07-29	1 / 65	CSV	6352fe17-252b-4714-a4cf-f83afbf5f488
2024-07-27	3 / 65	PHP	test.php
2024-07-27	3 / 58	PHP	antibots.php
2024-07-12	1 / 64	Text	test.php
2024-07-12	2 / 64	Text	antibots.php
2024-07-12	1 / 63	Text	test.php
2024-07-12	1 / 64	Text	test.php
2024-07-12	1 / 64	Text	test.php
2024-07-12	1 / 64	Text	test.php
2024-04-24	11 / 71	Win32 EXE	AcroRd32Info.exe

Figure 30:file referring of that phishing ip



9/94 security vendors flagged this IP address as malicious

45.146.164.110 (45.146.164.0/22)
AS 198610 (Beget LLC)

Last Analysis Date
1 day ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic Properties

Network	45.146.164.0/22
Autonomous System Number	198610
Autonomous System Label	Beget LLC
Regional Internet Registry	RIPE NCC
Country	RU
Continent	EU

Last HTTPS Certificate

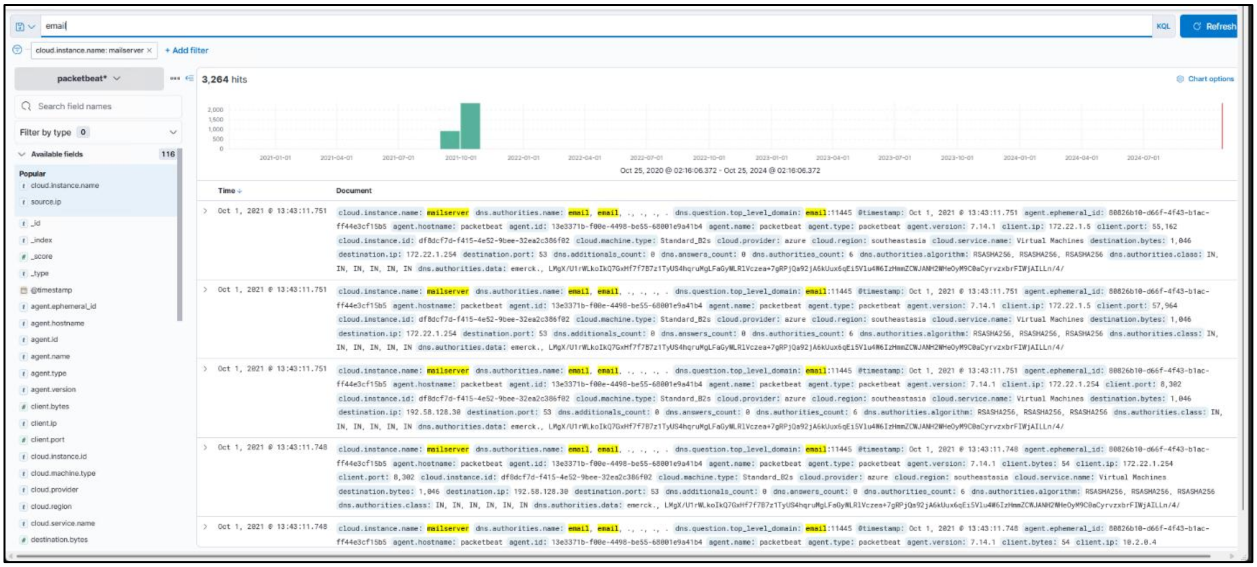
JARM Fingerprint

2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5

Last HTTPS Certificate

```
Data:
  Version: V3
  Serial Number: 34e84827516137cbe6157f55
  Thumbprint: 5fd57ca289f662cbf4eb3ee092104dc5884fc813
Signature Algorithm:
  Issuer: C=BE , O=GlobalSign nv-sa , CN=GlobalSign GCC R6 AlphaSSL CA 2023
  Validity
    Not Before: 2024 03 04 12:46:34
```

Figure 32:properties and other details of phishing ip



```
> Oct 1, 2021 @ 13:43:11.751  cloud.instance.name: mailserver dns.authorities.name: email, email, ., ., ., . dns.question.top_level_domain: email:11445 @timestamp: Oct 1, 2021 @ 13:43:11.751 agent.ephemeral_id: 80826b10-d66f-4f43-b1ac-
                              ff44e3cf15b5 agent.hostname: packetbeat agent.id: 13e3371b-f00e-4498-be55-68001e9a41b4 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.ip: 172.22.1.5 client.port: 55,162
                              cloud.instance.id: df8dcf7d-f415-4e52-9bee-32ea2c386f02 cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines destination.bytes: 1,046
                              destination.ip: 172.22.1.254 destination.port: 53 dns.additionals_count: 0 dns.answers_count: 0 dns.authorities_count: 6 dns.authorities.algorithm: RSASHA256, RSASHA256, RSASHA256 dns.authorities.class: IN,
                              IN, IN, IN, IN, IN dns.authorities.data: emerck., LMgX/U1rWLkoIkQ7GxHf7f7B7z1TyUS4hqruMgLFaGyWLR1Vczea+7gRPjQa92jA6kUux6qEi5V1u4W6IzHmmZCWJANH2WHeOyM9C0aCyrvzxbrFIWjAILLn/4/
> Oct 1, 2021 @ 13:43:11.751  cloud.instance.name: mailserver dns.authorities.name: email, email, ., ., ., . dns.question.top_level_domain: email:11445 @timestamp: Oct 1, 2021 @ 13:43:11.751 agent.ephemeral_id: 80826b10-d66f-4f43-b1ac-
                              ff44e3cf15b5 agent.hostname: packetbeat agent.id: 13e3371b-f00e-4498-be55-68001e9a41b4 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.ip: 172.22.1.5 client.port: 57,964
                              cloud.instance.id: df8dcf7d-f415-4e52-9bee-32ea2c386f02 cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines destination.bytes: 1,046
                              destination.ip: 172.22.1.254 destination.port: 53 dns.additionals_count: 0 dns.answers_count: 0 dns.authorities_count: 6 dns.authorities.algorithm: RSASHA256, RSASHA256, RSASHA256 dns.authorities.class: IN,
                              IN, IN, IN, IN, IN dns.authorities.data: emerck., LMgX/U1rWLkoIkQ7GxHf7f7B7z1TyUS4hqruMgLFaGyWLR1Vczea+7gRPjQa92jA6kUux6qEi5V1u4W6IzHmmZCWJANH2WHeOyM9C0aCyrvzxbrFIWjAILLn/4/
> Oct 1, 2021 @ 13:43:11.751  cloud.instance.name: mailserver dns.authorities.name: email, email, ., ., ., . dns.question.top_level_domain: email:11445 @timestamp: Oct 1, 2021 @ 13:43:11.751 agent.ephemeral_id: 80826b10-d66f-4f43-b1ac-
                              ff44e3cf15b5 agent.hostname: packetbeat agent.id: 13e3371b-f00e-4498-be55-68001e9a41b4 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.ip: 172.22.1.254 client.port: 8,302
                              cloud.instance.id: df8dcf7d-f415-4e52-9bee-32ea2c386f02 cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines destination.bytes: 1,046
                              destination.ip: 192.58.128.30 destination.port: 53 dns.additionals_count: 0 dns.answers_count: 0 dns.authorities_count: 6 dns.authorities.algorithm: RSASHA256, RSASHA256, RSASHA256 dns.authorities.class: IN,
                              IN, IN, IN, IN, IN dns.authorities.data: emerck., LMgX/U1rWLkoIkQ7GxHf7f7B7z1TyUS4hqruMgLFaGyWLR1Vczea+7gRPjQa92jA6kUux6qEi5V1u4W6IzHmmZCWJANH2WHeOyM9C0aCyrvzxbrFIWjAILLn/4/
> Oct 1, 2021 @ 13:43:11.748  cloud.instance.name: mailserver dns.authorities.name: email, email, ., ., ., . dns.question.top_level_domain: email:11445 @timestamp: Oct 1, 2021 @ 13:43:11.748 agent.ephemeral_id: 80826b10-d66f-4f43-b1ac-
                              ff44e3cf15b5 agent.hostname: packetbeat agent.id: 13e3371b-f00e-4498-be55-68001e9a41b4 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.bytes: 54 client.ip: 172.22.1.254
                              client.port: 8,302 cloud.instance.id: df8dcf7d-f415-4e52-9bee-32ea2c386f02 cloud.machine.type: Standard_B2s cloud.provider: azure cloud.region: southeastasia cloud.service.name: Virtual Machines
                              destination.bytes: 1,046 destination.ip: 192.58.128.30 destination.port: 53 dns.additionals_count: 0 dns.answers_count: 0 dns.authorities_count: 6 dns.authorities.algorithm: RSASHA256, RSASHA256, RSASHA256
                              dns.authorities.class: IN, IN, IN, IN, IN, IN dns.authorities.data: emerck., LMgX/U1rWLkoIkQ7GxHf7f7B7z1TyUS4hqruMgLFaGyWLR1Vczea+7gRPjQa92jA6kUux6qEi5V1u4W6IzHmmZCWJANH2WHeOyM9C0aCyrvzxbrFIWjAILLn/4/
> Oct 1, 2021 @ 13:43:11.748  cloud.instance.name: mailserver dns.authorities.name: email, email, ., ., ., . dns.question.top_level_domain: email:11445 @timestamp: Oct 1, 2021 @ 13:43:11.748 agent.ephemeral_id: 80826b10-d66f-4f43-b1ac-
                              ff44e3cf15b5 agent.hostname: packetbeat agent.id: 13e3371b-f00e-4498-be55-68001e9a41b4 agent.name: packetbeat agent.type: packetbeat agent.version: 7.14.1 client.bytes: 54 client.ip: 10.2.0.4
```

Figure 31:derch email in email server whether if there is an any attack