Open Access Library Journal
2025, Volume 12, e13973
ISSN Online: 2333-9721
ISSN Print: 2333-9705

MyCloudBills Pen Test and Network Security Assessment

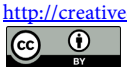
Marcello D'Angelone

National College of Ireland, Dublin, Ireland
Email: x21113777@student.ncirl.ie

How to cite this paper: D'Angelone, M. (2025) MyCloudBills Pen Test and Network Security Assessment. *Open Access Library Journal*, **12**: e13973.
https://doi.org/10.4236/oalib.1113973

Received: July 18, 2025
Accepted: August 25, 2025
Published: August 28, 2025

Copyright © 2025 by author(s) and Open Access Library Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/



Open Access

Abstract

This research paper describes two of the most common attack vectors that an attacker could use to access MyCloudBills' network, a fictitious SaaS company. The research about the Network topology and the analysis of the mitigating solution can be used as a reference for both Pen Testers and Blue Teams to develop attack and defense techniques, respectively.

Subject Areas

Computer and Network Security

Keywords

Vulnerability, Attack Vector, Log4j, Phishing, Security Controls

1. Executive Summary

Preserving the Confidentiality, Integrity and Availability of Customers' Data is the number one priority for a fictitious SaaS company like MyCloudBills. MyCloudBills provides cloud-based bills and salary management services to end-users and professionals. The Web application is hosted by the Company Data Center and Amazon Web Services (AWS). Users can access through their browser with two-factor authentication and securely pay their bills, link bank accounts, credit cards and review their financial transactions. The type of data stored in the company database includes Pernal Identifiable Information (PII), Bank Accounts, Credit Card, and other highly sensitive information. According to the 2021 Verizon's Data Breach Investigation report [1], one in every three organisations was breached due to an unpatched vulnerability. On the other hand, phishing emails represented

36% of the causes for the remaining data breaches. This paper describes two of the most recent real-world examples of attack vectors, along with some of the security controls that would dramatically improve the overall security posture and yield a better investment return for MyCloudBills. In summary, we will demonstrate how patch management, vulnerability management and Security Awareness Training would be the most effective mitigating solutions.

2. Network Setup

The Web Application, written in Java, is leveraging open-source technologies, specifically MySQL, as a Database, Apache as a Web Server, and CentOS 8.5 as the Operating System. The underlying Hypervisor technology enables hot patching and live migration of Workloads. Table 1 describes the software version and release date in detail.

Table 1. Software components.

MyCloudBills Application Framework			
Technology	Implementation details	Version	Release date
CentOS	Operating Systems	8.5-2111	2021-11-16
Apache	Web server	2.4.52	2021-12-20
Java	Programming Language	17	2021-09-14
MySQL	Stores credentials, database users, roles, financial details, and account balance	8.0.27	2021-10-19
VMWare ESXi	Type 1 Hypervisor	7.0 Update 3	2021-10-05

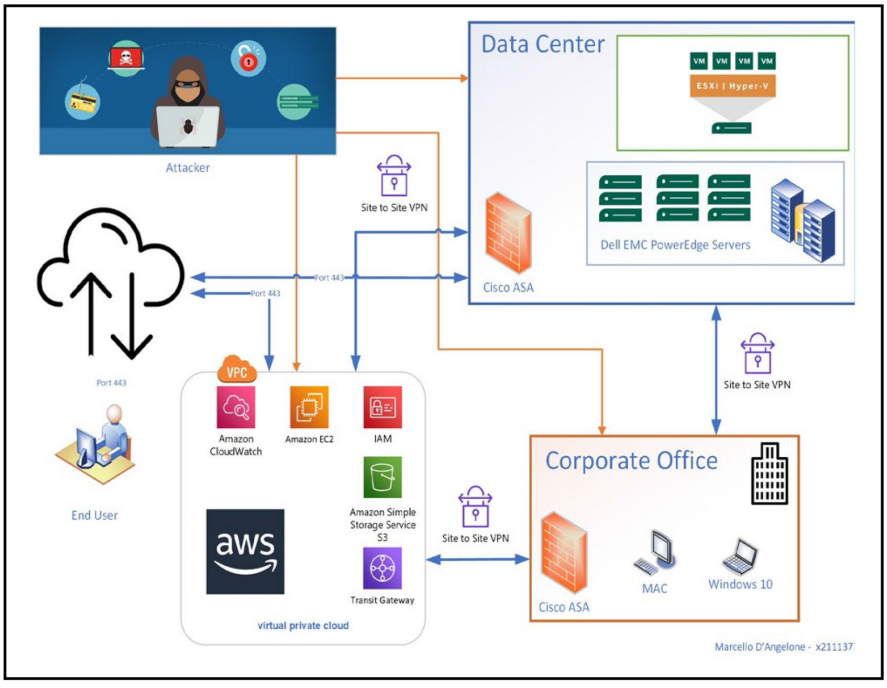


Figure 1. Network infrastructure and data flow.

Instead of building multiple Data Centers in different Geo-locations, MyCloud-Bills adopted a Hybrid cloud strategy to expand its offerings. The Hybrid cloud infrastructure is an environment that combines private on-premises with public third-party cloud services. This architecture, which enables the movement of workloads between different environments, provides better flexibility, allowing organisations to scale data and applications to meet customer demands and handle any overflow. This way, companies pay for cloud services only when needed, containing growing and complex subscription fees without being locked into a single cloud provider. According to [2], the Hybrid cloud market is expected to grow by almost 20% over the next few years. The increasing popularity of this model is due to the combination of the advantages of the traditional Data Center with the scalability of the Public Cloud Solutions. A survey carried out in 2020 [3] found that 58% of enterprises have or are expected to adopt a hybrid solution in the short term. This is also reflected in the growth of the adoption of open-source technologies such as containers and Kubernetes. **Figure 1** represents the main Network Components, the data flow between the Infrastructure, and an End User accessing the application via a Web Browser using the HTTPS protocol on port 443. The orange arrows represent the possible entry points for an attacker motivated to access the Company's network and steal data for financial gain.

This type of network's selection and design are relevant due to its popularity and increasing demand for Software as a Service (SaaS) applications. The complexity and broad range of technologies adopted to support this Infrastructure provide an interesting approach to researching weaknesses and vulnerabilities that a potential attacker could exploit with real-world examples.

2.1. Network Devices

The company network devices, described in **Table 2**, are deployed in the Corporate Office, the main Data Center and the AWS Virtual Private Cloud (VPC). Cisco Adaptive Security Appliance (ASA), series 5500-x, are the physical appliance used in the Data Center and the Corporate Office, two for each site. In contrast, AWS hosts the virtual version of the firewall: the ASAv 100. The Firewalls arrays are configured in Active/Standby failover mode, which means that only one firewall appliance passes traffic in one site at a time. If one firewall fails at one site, the second takes over and becomes the primary Active firewall. The three sites are interconnected via Virtual Private Network (VPN). Site-to-Site VPN allows encrypting data, voice and video stream creating an IPSec tunnel between two or more sites as represented in **Figure 2** [4].

Every Employees' Computer comes with the Cisco "Anyconnect" VPN client, pre-installed in "Always On", which means an encrypted tunnel connects automatically to the Corporate Office. This type of configuration secured their network connection also when they were required to work from home during the Pandemic.

As per Cisco recommendations, the Network infrastructure has been config-

ured following the "Three-tier Hierarchical Network Model" [5] represented in Figure 3. This model ensures high availability and redundancy to support mission-critical applications.

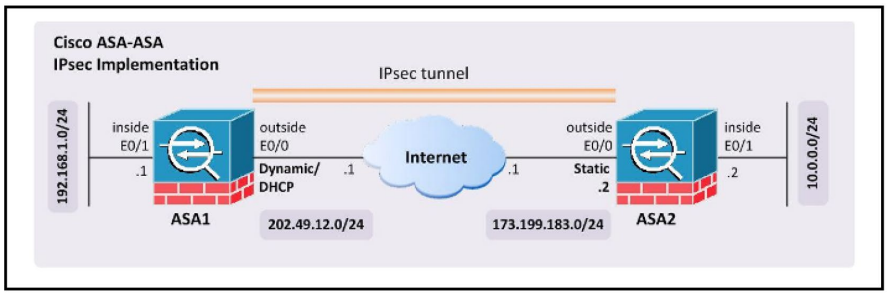


Figure 2. Site-to-Site VPN [4].

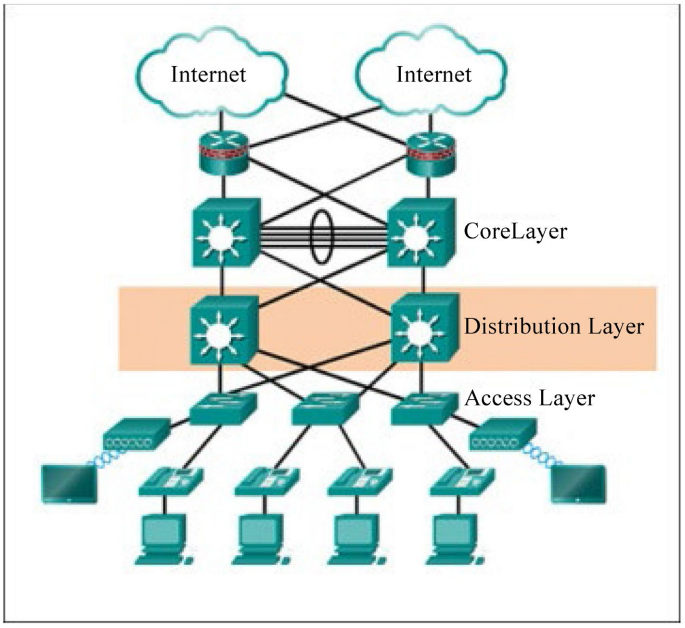


Figure 3. Cisco three-tier hierarchical network model [5].

Table 2. Network infrastructure.

Tot	Vendor	Model	Role
4	Cisco Adaptive Security Appliance	5500-x	Firewall
2	Cisco ASAv	100	Firewall
4	Cisco Catalyst	6800	Core Switch
10	Cisco Catalyst	2948G-L3	Layer 3 Switch
150	Cisco Catalyst	4000	Access Switch
50	Cisco WLC	8540	Wireless Lan Controller
250	Cisco Aironet	1200	Access point

The *Core Layer*, also known as the backbone layer, consists of four Cisco Catalyst 6800, the *Distribution Layer* consists of ten Layer 3 Catalyst 2948G-L3 switches, and the *Access Layer* consists of 150 Catalyst 4000. The Corporate Office also provides Wi-Fi services centrally managed with 50 Cisco Wireless Lan Controller 8540 (WLC) connected to the *Access Layer* switches. The WLC controls over 250 Cisco Aironet 1200 Series Access Points disseminated in the Corporate Office. The network is segmented into different Virtual Local Area Networks (VLANs) for data, voice, Wi-Fi and Out-Of-Band (OOB) management.

2.2. Corporate Office Infrastructure

The corporate office infrastructure described in Table 3, consists of four Active Directory Domain Controllers that provide authentication authorization and accounting to 2000 employees, two Exchange Email Servers running on six Dell PowerEdge R710. Ten Infoblox servers provide core networking services such as DNS, DHCP, and NTP. The fleet of endpoints is equally split between 1000 Lenovo Windows Machines and 1000 MacBook Pro. They are all managed with Intune Endpoint Manager, a cloud-based Mobile Device Management (MDM), Mobile Application Management (MAM) and PC Management Solution. All Software Applications, Application updates and Operating Systems updates are installed to the Endpoints through Intune. However, end-users are also local Administrators on their own Devices, which means that they can install unsupported applications or make some configuration changes. Each employee has Cisco Unified IP Phone 7942G on his desk, which is also available in each of the 50 meeting rooms for a total of 2050 devices. The meeting rooms in question are equipped with Cisco Webex Room 70 Panorama to enable conference calls with third-party organizations.

Table 3. Corporate office infrastructure.

Tot	Vendor	Model	Role
6	Dell PowerEdge	R710	Active Directory/Mail Server
10	Infoblox	2225	DNS DHCP NTP
1000	Lenovo	T480s	Windows Laptop
1000	Mac Book Pro	M1	Apple Laptop
2050	Cisco Unified IP Phone	7942G	IP Phone
50	Cisco Webex Room	70 Panorama	Audio Video

2.3. Data Center Infrastructure

The Data Center infrastructure, described in Table 4, comprises a Server farm of 2000 Dell PowerEdge EMC. This type of architecture provides modular and scalable processing power, which can be expanded depending on the workload re-

quirements [6]. The entire Server fleet is running VMWare ESXi Hypervisor. On top of this, 100,000 instances of CentOS are running along with the remaining Application Framework described in Table 1. Guards on a 24/7/365 shift rotation constantly monitor access to the facility.

Table 4. Data center infrastructure.

Tot	Vendor	Model	Roles
2000	Dell PowerEdge EMC	R6525	VMWare ESXi

2.4. AWS Infrastructure

MyCloudBills has also invested in shifting the workload to the AWS Cloud Infrastructure. The vendor selected is one of the first cloud computing providers since 2008, according to the Gartner Magic Quadrant represented in Figure 4, one of the leaders in Cloud infrastructure and Platform as a Service for over 12 years [7].

Figure 4. Gartner magic quadrant [7].

The Company decided to replicate the services deployed in the physical Data Center to offload the workload during peak hours and provide failover backup for

disaster recovery scenarios. On the Company's Virtual Private Cloud (VPC) Infrastructure, 150,000 EC2 instances are running CentOS Operating System. AWS Identity and Access Management (IAM) provides access control across all Company's AWS resources. This includes workforce users, through AWS Single Sign-On (SSO) according to the least-privilege permissions, as well as granting only the required access to workloads through IAM roles and policies [8]. The Backup is stored on 500 Simple Storage Service (S3) Buckets of 500 TB each. The AWS Transit Gateway acts as a cloud router to streamline and scale the network connection between the Data Center and the Corporate office. This simplifies connection to other VPC for future growth and secure communication by encrypting traffic [9]. The Cloud Services are constantly monitored by Amazon CloudWatch, which provides Application logging, metrics, events and alerting to ensure minimum downtime and resolve potential performance issues in a timely manner [10].

3. Attack Vectors

On November 24th 2021, Apache Foundation was notified about one of the most critical vulnerabilities since the disclosure of the one affecting its Struts framework, which caused the Equifax breach in 2017. Because of the criticality, the widespread usage, and the recent findings around the Log4j vulnerability, this would be one of the most likely attack vectors exploiting MyCloudBills Web Application. The second attack vector that could be used to access the Company's network is Phishing Email. This is one of the most common social engineering techniques that exploits the weakest link of an organization: the human element. The following subsections will describe each attack vector's motives, techniques, targeted devices, and exploits.

3.1. Log4j Vulnerability Description

Apache Log4j version 2 is a popular Java library used as a logging framework for debugging many web applications and services. On December 9th 2021, the first zero-day Exploit, also known as Log4Shell, was discovered in the wild [11]. This new vulnerability was introduced with the "*Java naming and Directory Interface*" (JNDI) API, which allows the library to retrieve Java Objects using protocols such as LDAP and DNS. An Attacker can easily leverage this input validation flaw to execute arbitrary code on the affected system. This is rated as a Critical-risk vulnerability as it does not require user interaction or permission, can be exploited remotely, and is widely used in this Java library.

3.2. Log4j Exploitation Motive

According to Mandiant [12], threat actors financially motivated tried to exploit this vulnerability by deploying cryptocurrency miners. Other actors, specifically targeting external-facing Web Servers, are attempting to gain access to the internal Infrastructure, leading to other monetisation activities such as data theft and ransomware deployment.

3.3. Log4j Exploitation Techniques

To exploit this vulnerability, an attacker can inject malicious JNDI lookup payloads inside of HTTP request headers or via POST requests crafting a command such as:

${jndi:ldap://attacker.com/malicious_java_class}

As represented in Figure 5, the LDAP referral server will redirect the request to

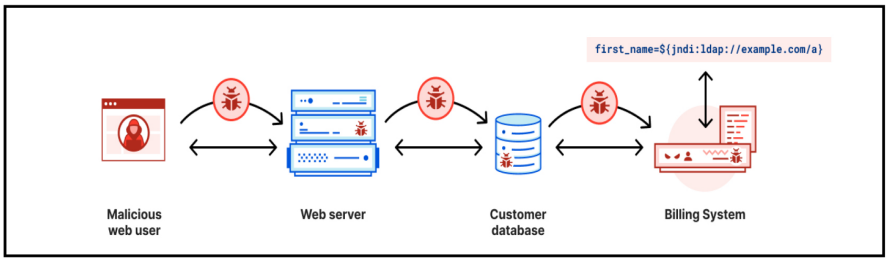


Figure 5. Log4j exploitation technique [11].

a secondary HTTP server hosts the victim's malicious Java class, leading to a Remote Code Execution (RCE) [11].

3.4. Log4j Target Versions

All Log4j versions from 2.0-beta9 to 2.14.1 are affected by this vulnerability. Version 2.15.0, the fix released by Apache to fix this vulnerability on December 6th 2021, did not completely address the flaw on certain non-standard configurations [13]. This was resolved on a new release, version 2.16.0, available since December 13th. However, another Denial-of-Service Vulnerability was found on the latest version, which was finally fixed with version 2.17.0 released on December 18th. Cisco confirmed that this vulnerability affects Webex Servers [14]; all other network equipment is not affected. The complete list of vendors impacted has been updated and published on GitHub [15]. This includes Amazon, VMware, and Webex.

3.5. Log4j Known Vulnerabilities

On December 8th 2021, the Apache Software Foundation disclosed CVE-2021-44228, with a Common Vulnerability Scoring System (CVSS) score of 10 [16]. This flaw includes Common Weakness Enumeration (CWE) CWE-20 for improper input validation, CWE-400 for Uncontrolled Resource consumption and CWE-520 for Deserialization of Untrusted data [17]. CVE-2021-45046 was disclosed one week after the release of version 2.15.0 as the patch did not address the deserialization of untrusted data on certain non-standard Log4j configurations. The CVSS score was set to 9.0 as RCE was still possible [18]. Finally, CVE-2021-45105 was disclosed on December 16th for Log4j version 2.16.0 with a CVSS score of 7.5. Although this vulnerability is less critical than the one affecting the previous versions, an attacker could still perform a Denial of Service (DoS) attack and crash

the application.

3.6. Log4j Exploits

The first Exploit Proof of Concept (POC) appears to have been released on December 9th 2021. On December 10th, a user of Exploit.in shared a link to another POC exploit on the same day that other users are sharing tips on how to scan vulnerable servers on XSS.is. December 14th, a Phyton snippet based on the Exploit POC is published on Exploit-db.com with EDB-ID: 50590 [19]. On the 16th SAINT penetration testing software was the first to include the Exploit for this vulnerability. On the 19th, Dridex and Meterpreter payloads were detected attacking external web servers [12].

3.7. Log4j Impact

An unauthenticated, remote actor that successfully exploits this vulnerability will be able to steal MyCloudBills data, deploy ransomware or perform a DoS attack, compromising the confidentiality, integrity and availability of MyCloudBills Application. This may result in reputational damage and regulatory fines.

3.8. Log4j Exploitation Attempts

According to the Palo Alto telemetry system [13], represented in **Figure 6**, a total of 60,476,284 hits have triggered the signature related to Log4j exploits from the 10th to the 20th of December.

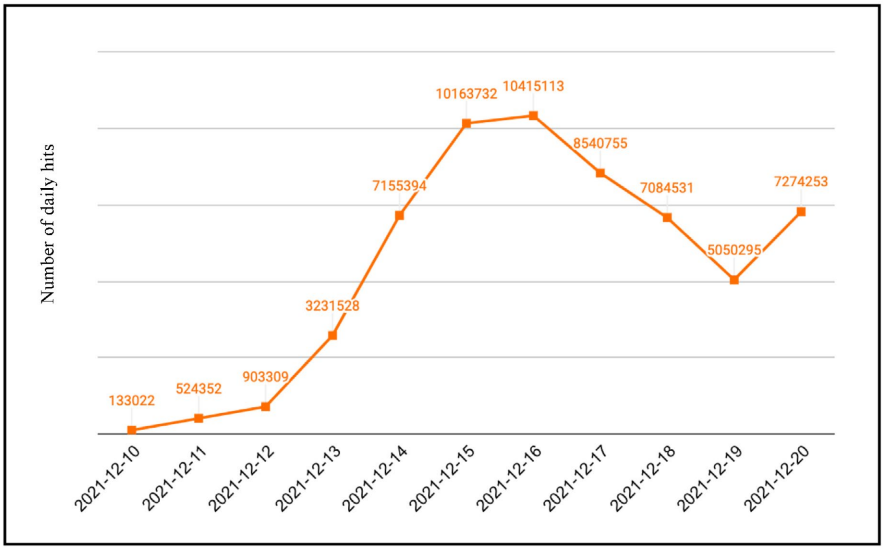


Figure 6. Daily hits of Apache Log4j Palo Alto signature [13].

This clearly indicates a massive scanning activity in opportunistic attempts to identify vulnerable Web Applications. GreyNoise observed that most of the attacks originated from 150 IP addresses belonging to The Onion Ruter (TOR) exit points [20]. **Table 5** summarizes Log4j main characteristics.

Table 5. Log4j summary.

Log4j Technical Details	
First reported	November 24th 2021
Attacking Difficulty	Easy
Exploitation Vectors	Network Connectivity
Exploitation Consequence	Remote Code Execution Denial of Service Local Code Execution
Exploitation Rating	Wide
Vulnerability type	Input Validation
CVE Numbers	CVE-2021-44228/ (CVSS score 10) CVE-2021-45046/ (CVSS score 9.0) CVE-2021-45105/ (CVSS score 7.5)
Mitigation Details:	Patch: Users with Java 8 or later should upgrade to release 2.17.1 Users with Java 7 should upgrade to release 2.12.2 Users with Java 6 should upgrade to release 2.3.1 Workaround: If patching is not possible, remove the JndiLookup class from the classpath: zip -q -d log4j-core-*.jar org/ap

3.9. Phishing Definition

Phishing is one of the most common types of cyberattacks. [21] defines this cybercrime as a combination of both *social engineering* and *technical subterfuge* perpetrated to steal personal identity, data and financial account credentials by fooling the victim into believing they are dealing with a trustworthy, legitimate party. The unwary employee receives a malicious email containing a link or an attachment that allows an attacker to compromise a system and access a network.

3.10. Phishing Motive

Most of the time, Phishing campaigns are used to gather user credentials for financial services or gain access and perform a lateral movement in the corporate network. They have also been used to deploy malware or ransomware on the end-user system more recently. The outcome is always to obtain illicit financial gains.

3.11. Phishing Techniques

Phishing techniques may vary from a generic malicious email sent to a broad audience to targeting employees in a particular department (Finance or IT) or the company's Execs. This type of phishing, classified as spear phishing and whaling, respectively, is far more dangerous as the attacker is crafting dedicated and more convincing emails to entice the victim to open their malicious content. As reported in [22], attackers are now leveraging Open-Source Intelligence (OSINT) tools such as Maltego to gather information about the victims on social media or

other internet resources.

The malicious email content, like the one represented in Figure 7, usually redirects the user to a compromised URL. Attackers abuse a functionality that allows organizations to use their primary domains while redirecting users to third-party service providers' domains [23]. Users who click the link are redirected to the attacker's infrastructure, containing PHP code to tailor the content and prompt the user to enter their credentials.

The effectiveness of this technique is supported by other studies [24] that confirm that almost 20% of employees clicked a phishing link in a simulation exercise, and 13.4% submitted their credentials.

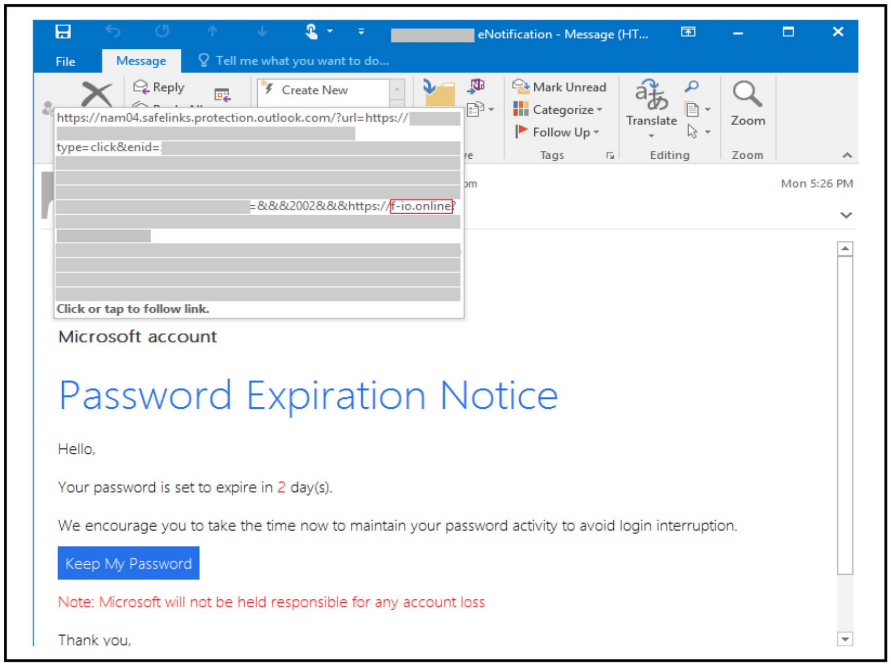


Figure 7. Phishing email redirecting to a malicious URL [23].

3.12. Targeted Industries

According to the Anti-Phishing Working Group (APWG) report [21], financial institutions are the most targeted by phishing emails with 29.2%, followed by Social Media 14.8% and the Payment Industry with 12.2%.

3.13. Impact of Phishing

According to the 2021 State of the Phish report [25], loss of data is the most common impact of successful phishing attacks, with 60%, followed by Credential compromise and Ransomware infection, 52% and 47%, respectively. Figure 8 shows the top 5 consequences of successful phishing attacks.

It takes a single user who falls victim to this attack vector to compromise a vast amount of confidential data. A study from the Ponemon Institute estimates that the financial impact quadrupled in the past six years, increasing from $3.8 million

in 2015 to $14.8 million in 2021 [26]. This includes the cost of the loss of employee productivity, the cost of ransomware, and business disruption due to phishing.

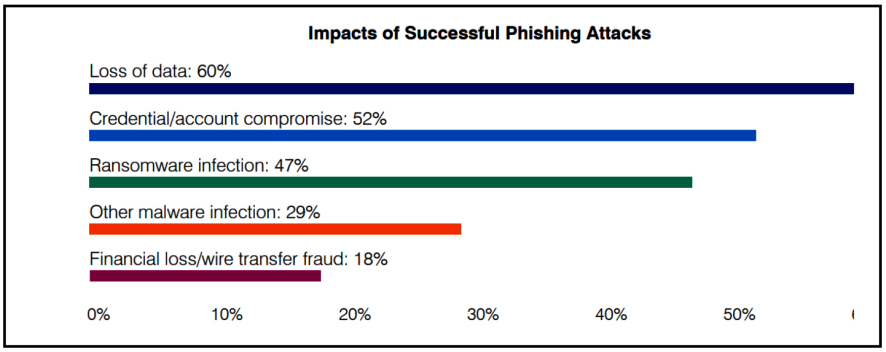


Figure 8. Impacts of successful phishing attacks [25].

3.14. Microsoft 365 Phishing Attack

In August 2021, Microsoft reported a widespread credential Phishing attack using an open redirector link [23]. The common theme of such emails was the recipient domain in the subject and a large button in the body that leads to a page where the victim is prompted to enter their credentials to reset their password.

4. Mitigation Solutions

The attack vectors described in this paper exploit two different types of vulnerability. One is technical, whereas the other is merely human. As such, the relevant mitigating solutions will be discussed separately.

4.1. Log4j Mitigations

The first step for effective mitigation is to gather details from the inventory to determine which Log4j version is running on various systems. Inventories of hardware and software assets are the top two *critical security controls* developed by the Center for Internet Security (CIS) in collaboration with SANS Institute to protect organizations from the most common attack vectors [27]. Vulnerability scanners such as Qualys or stand-alone tools such as log4shell scanners [28] must be used to identify this security flaw and validate the remediation. Tools such as log4-finder [29] can also be used locally to scan systems. As of December 28th, patching systems to 2.17.1 is the most effective solution. Internet-facing assets, including cloud-based ones, should be the top priority. If patching is not an option, the JndiLookup class could be removed from the class path org/apache/logging/log4j/core/lookup/JndiLookup.class [30].

Configure Cisco Snort rules 300055-300058 for Firewall Threat Defence [31], the Intrusion Prevention System (IPS) module for its ASA firewall.

Another mitigation step would be to block outbound LDAP connections or create an alert that triggers any 389/TCP connections initiated from DMZ hosts to anywhere.

Implement a cloud-based Web Application Firewall solution such as Cloudflare [30], which protects from both Log4jShell and DoS attacks by simply redirecting the traffic to Cloudflare's global edge network. This seems the least effective mitigation as some examples of WAF bypass have been detected in the wild [32].

4.2. Phishing Email Mitigations

In regard to the email security framework, MycloudBills was inspired by the recommendations outlined in the NIST SP 800-45 version 2 [33].

One of the most effective steps to mitigate Phishing emails is to provide Security Awareness and Training to the MyCloudBills employees. This should go hand in hand with phishing simulation exercises, whereby the employees are tested to identify and report suspicious emails. Proofpoint [25] reported that employees are 90% less likely to be susceptible to phishing emails after following security education modules. This data is confirmed by [26], which calculates a reduction of the financial impact of phishing by more than 50% if training and awareness programs are conducted for the employees.

Deploy a Privilege and Access Management solution to all Windows and Apple Endpoints so that employees are no longer local administrators on their devices. This could be an effective solution to prevent the installation of malware or other malicious attachments.

An additional technical, operational control that may reduce the risk of phishing attacks by 85% [1] is an investment in an email Filtering security solution. For instance, Microsoft Defender for Office 365 prevents suspicious emails from being delivered to the end-user and notifies them before clicking on malicious links. According to [23], 13 billion such emails were blocked only in 2020. Another feature called "Safe Links Defender for Office 365" performs a real-time scan of URLs when end-users click them and blocks them before they can cause harm.

Finally, two-factor authentication should also be implemented on every application to mitigate the impact if an attacker has stolen credentials.

5. Conclusions

This research paper presented two examples of the most common attack vectors we have seen in the past years. It is not the first time that a zero-day exploit, such as Log4jShell, is actively targeting assets in the wild, or Employees have fallen victim to Phishing emails. Although such attacks are becoming increasingly sophisticated, some standard security controls and frameworks such as NIST and CIS are essential to prioritize remediation and mitigate the risk.

First, to respond quickly to any vulnerability, it is essential to have up-to-date and comprehensive software and asset inventory. This would significantly improve the remediation time to identify vulnerable assets and the time it usually takes to patch them. Scanning tools are fundamental to reporting vulnerabilities and validating remediation. However, some types of software, such as Java libraries, may be more challenging to detect promptly.

Regarding Phishing, Security Awareness Training remains one of the primary and most cost-effective solutions to reduce the likelihood of successful phishing scams. However, other security measures such as Email Filtering and Privilege and Access Management solutions will dramatically reduce the attack surface.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Verizon (2021) 2021 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

[2] Mordor Intelligence (2021) Hybrid Cloud Market, Industry Share, Size, Growth Mordor Intelligence.

[3] Casey, K. (2020) Hybrid Cloud by the Numbers, 2020: 10 Stats to See. https://enterprisersproject.com/article/2020/7/hybrid-cloud-10-statistics

[4] Firewall, C.X. (2021) Configuring Site to Site IPSec VPN Tunnel between Cisco Routers. https://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/867-cisco-router-site-to-site-ipsec-vpn.html

[5] Cisco Networking Academy (2014) Hierarchical Network Design Overview (1.1)>Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

[6] Dell Technologies (2021) PowerEdge FX Series—Enterprise Servers. https://www.delltechnologies.com/en-us/servers/modular-infrastructure/poweredge-fx/index.htm

[7] Dignan, L. (2021) Top Cloud Providers in 2021: AWS, Microsoft Azure, and Google Cloud, Hybrid, SaaS Players. https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas/

[8] AWS (2017) AWS Identity & Access Management. Amazon Web Services, Inc. https://aws.amazon.com/iam/

[9] AWS (2017) AWS Transit Gateway—Amazon Web Services. Amazon Web Services, Inc. https://aws.amazon.com/transit-gateway/

[10] AWS (2018) Amazon CloudWatch—Application and Infrastructure Monitoring. Amazon Web Services, Inc. https://aws.amazon.com/cloudwatch/

[11] Robinson, T. (2021) Apache Log4j Threatens, Well, Everything. Security Boulevard. https://securityboulevard.com/2021/12/apache-log4j-threatens-well-everything/

[12] Mcwhirt, M. and Hultquist, J. (2021) Log4Shell Initial Exploitation and Mitigation Recommendations. Mandiant. https://www.mandiant.com/resources/log4shell-recommendations

[13] Yan, T., *et al.* (2021) Apache Log4j Vulnerability CVE-2021-44228: Analysis and Mitigations. Unit42, 10-Dec-2021. https://unit42.paloaltonetworks.com/apache-log4j-vulnerability-cve-2021-44228/

[14] Cisco Systems (2021) Cisco Security Advisory: Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021. Cisco, 10-Dec-2021.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEb

[15] YfryTchsGD (2022) Log4jAttackSurface. https://github.com/YfryTchsGD/Log4jAttackSurface

[16] MITRE (2021) CVE-CVE-2021-44228. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

[17] NIST (2021) NVD-CVE-2021-44228. https://nvd.nist.gov/vuln/detail/CVE-2021-44228

[18] NIST (2021) NVD-CVE-2021-45046. https://nvd.nist.gov/vuln/detail/CVE-2021-45046

[19] Leonjza (2021) Apache Log4j2 2.14.1—Information Disclosure. Exploit Database, 14-Dec-2021. https://www.exploit-db.com/exploits/50590

[20] Mandiant (2021) Report—Mandiant Advantage. https://advantage.mandiant.com/reports/21-00026146

[21] APWG (2021) Phishing Activity Trend Report APWG ORG 2021. https://docs.apwg.org/reports/apwg_trends_report_q2_2021.pdf

[22] Uehara, K., Mukaiyama, K., Fujita, M., Nishikawa, H., Yamamoto, T., Kawauchi, K., *et al.* (2020) Basic Study on Targeted E-Mail Attack Method Using OSINT. In: *Advances in Intelligent Systems and Computing*, Springer, 1329-1341. https://doi.org/10.1007/978-3-030-15032-7_111

[23] Microsoft (2021) Widespread Credential Phishing Campaign Abuses Open Redirector Links. Microsoft Security Blog, 26-Aug-2021. https://www.microsoft.com/security/blog/2021/08/26/widespread-credential-phishing-campaign-abuses-open-redirector-links/

[24] Terranova Security (2021) 2020 Phishing Benchmark Global Report. https://terranovasecurity.com/wp-content/uploads/2021/01/GPT-2020-Report-EN-1.pdf

[25] Proofpoint (2021) 2021 State of the Phish, an In-Depth Look at User Awareness, Vulnerability and Resilience.

[26] Ponemon Institute (2021) The 2021 Cost of Phishing Study. https://www.proofpoint.com/sites/default/files/analyst-reports/pfpt-us-ar-ponemon-2021-cost-of-phishing-study.pdf

[27] Center for Internet Security (2021) CIS Critical Security Controls® v8 CIS Critical Security Controls. CIS, May 2021.

[28] Wortley, F., Thompson, C. and Allison, F. (2021) Guide: How to Detect and Mitigate the Log4Shell Vulnerability (CVE-2021-44228 & CVE-2021-45046). https://www.lunasec.io/docs/blog/log4j-zero-day-mitigation-guide/

[29] Fox-It (2021) Log4j-Finder. GitHub. https://github.com/fox-it/log4j-finder

[30] Gabor, G. and Bluehs, A. (2021) CVE-2021-44228—Log4j RCE 0-Day Mitigation. The Cloudflare Blog. http://blog.cloudflare.com/cve-2021-44228-log4j-rce-0-day-mitigation/

[31] Market Screener (2021) Cisco: Protecting against Log4j with Secure Firewall & Secure IPS. Market Screener. https://www.marketscreener.com/quote/stock/CISCO-SYSTEMS-INC-4862/news/Cisco-Protecting-against-Log4j-with-Secure-Firewall-Secure-IPS-37309859/

[32] Manraj, B. (2021) Exploiting Log4j. Apache Solr, Cyber Secure.

https://www.manrajbansal.com/post/exploiting-log4j-apache-solr

[33] Tracy, M., Jansen, W., Scarfone, K. and Butterfield, J. (2007) Guidelines on Electronic Mail Security. Information Technology Laboratory Computer Security Resource Center.