OSM Coursework 1

ACME Vulnerability Management & Threat Intelligence Report

Student ID: 2136685

Table of Contents

1. Vulnerability Management....4
1.1. (INTERNAL) MS13-098: Vulnerability in Windows Could Allow Remote Code Execution (2893294)....4
1.1.1. MITRE ATT&CK Table....5
1.1.2. MITRE D3FEND Table....5
1.1.3. Security Protections....6
1.2. (INTERNAL) Red Hat: CVE-2021-3156: Important: sudo security update (Multiple Advisories)....6
1.2.1. MITRE ATT&CK Table....7
1.2.2. MITRE D3FEND Table....8
1.2.3. Security Protections....8
1.3. (EXTERNAL) TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)....9
1.3.1. MITRE ATT&CK Table....9
1.3.2. MITRE D3FEND Table....11
1.3.3. Security Protections....11
1.4. (EXTERNAL) Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317)..11
1.4.1. MITRE ATT&CK Table....12
1.4.2. MITRE D3FEND Table....14
1.4.3. Security Protections....15
1.5. InsightVM Vulnerability Management Tool Overview....15
1.5.1. Summary....15
1.5.2. Vulnerability Management....15
1.5.2.a. Vulnerability Scoring....15
1.5.2.b. Internal & External Vulnerabilities....16
1.5.3. Conclusion....16
2. Threat Intelligence....16
2.1. Qakbot Intelligence Summary....16
2.1.1. Executive Summary....16
2.1.2. Analyst Comments....17
2.1.3. Recommendation....17
2.2. XWorm Intelligence Report....17
2.2.1. Intelligence Summary....17
2.2.2. MITRE TTPs....17
2.2.3. Impact....18
2.2.4. Mitigations....19
2.2.5. Indicators of Compromise....19
2.3. OSINT Case Study....21
2.3.1. Threat Actor Groups....21
2.3.1.a Anonymous Sudan....21
2.3.1.b Cyber Toufan....22
2.3.1.c Killnet....22
2.3.1.d TA402....22
2.3.2. Potential Cyber Threats to Alpha Employees....23
3. References....23

List of Tables

Table 1: MITRE ATT&CK Techniques....5
Table 2: MITRE D3FEND Techniques....5
Table 3: MITRE ATT&CK Techniques....7
Table 4: MITRE D3FEND Techniques....8
Table 5: MITRE ATT&CK Techniques....9
Table 6: MITRE D3FEND Techniques....11
Table 7: MITRE ATT&CK Techniques....12
Table 8: MITRE D3FEND Techniques....14
Table 9: XWorm-associated URLs & C2s (Pachpor and Adarsh, 2023)....19
Table 10: XWorm-associated cryptocurrency wallets (Pachpor and Adarsh, 2023)....20
Table 11: XWorm-associated SHA256 hashes (Pachpor and Adarsh, 2023)....21

1. Vulnerability Management

In the following sections, the vulnerabilities outlined have been chosen using their label from their respective CVSS v2.0 scores vulnerability metrics (NIST, 2019).

1.1. (INTERNAL) MS13-098: Vulnerability in Windows Could Allow Remote Code Execution (2893294)

The MS13-089 vulnerability, CVE-2013-3900, has a CVSS score of "7.6 High" and a Rapid7 classification of "critical". CVE-2013-3900 allows a threat actor to modify an authentically signed Portable Executable (PE) file – a Windows .exe file – and insert a remote code execution payload without invalidating the signature. This tricks the Windows operating system to run the file as a trusted file. The Rapid7 scan concluded that the vulnerability is of low likelihood (severity risk "3") but very high impact (severity score "8"), as up-to-date versions of Windows have already patched this vulnerability, however the patch can be reverted by modifying registry keys. The MITRE ATT&CK table below will outline the circumstances that would lead to this vulnerability being exploited (Microsoft, 2023; NIST, 2019; NIST, 2022; Rapid7, 2023a; Rapid7, 2023c).

Moreover, the MITRE D3FEND table below will outline mitigation tactics to respond to the vulnerability being exploited and to minimise further and residual risk, and damages.

1.1.1. MITRE ATT&CK Table

Table 1: MITRE ATT&CK Techniques

Tactics	***Techniques***	***Explanation & Relevance***
Resource Development	T1587.004 – Develop Capabilities: Exploits	To exploit the vulnerability above, a threat actor must first develop a payload to insert into the legitimate, signed executable. After the payload is developed with the threat actor's intentions, it should be inserted into the PE file, without invalidating the trusted signature (MITRE, 2023).
Initial Access	T1566.001 – Phishing: Spearphishing Attachment	A threat actor may use this method to distribute the malicious executable. They may send phishing emails, with the executable as an attachment, attempting to pass it off as legitimate software, so that the victim will run the executable. The threat actor may employ a sense of urgency, or even include instructions, to ensure the malware is run (MITRE, 2023).
Execution	T1204.002 – User Execution: Malicious File	A threat actor must await for the target users to run their payload. The executable may be masqueraded to go along with the phishing email (MITRE, 2023).

1.1.2. MITRE D3FEND Table

Table 2: MITRE D3FEND Techniques

ATT&CK Technique	***D3FEND Technique(s)***	***Explanation & Relevance***
T1566.001 – Phishing: Spearphishing Attachment	D3-EF – Email Filtering	Gamma's incoming email may be filtered using specific criteria. For example, Gamma's emails may never allow the inclusion of a .exe file as an attachment (MITRE, 2024).
	D3-ER – Email Removal	Gamma's employees may delete suspicious emails, such as what they recognise as phishing attempts. This relies heavily on the employee's training and the quality of Gamma's training. Moreover, the removed emails' source must be blocked to ensure no further phishing emails being sent (MITRE, 2024).
T1204.002 – User Execution: Malicious File	D3-EDL – Executable Denylisting	Gamma may employ policies on their machines to ensure that certain file names, file paths, file hashes, or file malware scans will not run if they are mentioned in the policies (MITRE, 2024).

	D3-DA – Dynamic Analysis	Gamma may recognise that the file is from an external source, deciding to run the suspicious executable in a "sandbox" environment, such as a virtual machine, to determine if it is malicious (MITRE, 2024).

1.1.3. Security Protections

Gamma must ensure that their Windows machines are up to date with the latest version, as the latest versions are secure. If the machines can not be upgraded, Gamma may manually edit the Windows Registry to ensure that the "EnableCertPaddingCheck" key is set to 1 (Microsoft, 2023; Roger, 2023).

Moreover, Gamma must ensure that their employees are trained to a satisfactory level against phishing, according to Gamma's information security policies.

On the other hand, Gamma must employ machine policies, such as using Microsoft's Active Directory, to introduce executable denylisting, as per the D3FEND table.

1.2. (INTERNAL) Red Hat: CVE-2021-3156: Important: sudo security update (Multiple Advisories)

The Red Hat CVE-2021-3156 vulnerability affects the sudo command in Linux systems and has the CVSS score of "7.2 High". A user with access to sudo without the need for authentication can perform a heap-based buffer overflow and escalate their priviliges due to the way sudo parses command line arguments. This gives the threat actor full control of the affected machine. According to the Rapid7 scans, this vulnerability is of low likelihood (severity risk "2") but high impact (severity score "7"), as the threat actor needs to gain access to an internal machine physically, as they are not internet-facing. Should a threat actor gain access, the MITRE ATT&CK table below will outline the circumstances that would lead to this vulnerability being exploited (Kathpal, 2021; NIST, 2019; NIST, 2023b; Rapid7, 2023c; Red Hat, 2023).

Moreover, the MITRE D3FEND table below will outline mitigation tactics to respond to the vulnerability being exploited and to minimise further and residual risk, and damages.

1.2.1. MITRE ATT&CK Table

Table 3: MITRE ATT&CK Techniques

Tactics	***Techniques***	***Explanation & Relevance***
Initial Access	T1190 – Exploit Public-Facing Application	To exploit this vulnerability, a threat actor must gain access to a computer that uses sudo, such as a Unix-like operating system. For example, the threat actor may attempt to upload a malicious Bash script with malicious code to gain elevated privileges through an unsecure upload function on Gamma's website (MITRE, 2023).
Execution	T1059.004 – Command and Scripting Interpreter: Unix Shell	As sudo is popular with Unix-like systems, a threat actor must prepare the malicious script for a Unix shell, such as the default Linux shell "bash" (MITRE, 2023).
Privilege Escalation	T1548.003 – Abuse Elevation Control Mechanism: Sudo and Sudo Caching	The vulnerability states that performing a buffer overflow on the sudo command allows a threat actor to gain elevated privileges. Gaining elevated privileges effectively gives the threat actor full control of the specific machine and the data on it. Unfortunately, as the threat actor can do anything with the computer, Gamma can face any impact (MITRE, 2023).

1.2.2. MITRE D3FEND Table

Table 4: MITRE D3FEND Techniques

ATT&CK Technique	***D3FEND Technique(s)***	***Explanation & Relevance***
T1190 – Exploit Public-Facing Application	D3-PSEP – Process Segment Execution Prevention	If a threat actor uploads a malicious payload through Gamma's services, this D3FEND technique prevents execution of anything outside the memory region specified for the service. D3-PSEP effectively stops execution of any code outside of the original code necessary for the service to run (MITRE, 2024).
T1059.004 – Command and Scripting Interpreter: Unix Shell	D3-EDL – Executable Denylisting	Gamma can enforce policies on their machines to restrict what applications can run by denying them based on file names, file paths, file hashes, file publisher (signature), file permissions, file malware scan or user-file combination (specific user accessing specific file). Gamma may deny ".sh" scripts (MITRE, 2024).
	D3-LFP – Local File Permissions	Gamma may restrict the machine's logged-in user to only access the files required for their specific actions. Moreover, Gamma may restrict a user from having access to the sudo command altogether (MITRE, 2024).
T1548.003 – Abuse Elevation Control Mechanism: Sudo and Sudo Caching	D3-LFP – Local File Permissions	Gamma may restrict the machine's logged-in user to only access the files required for their specific actions. Moreover, Gamma may restrict a user from having access to the sudo command altogether (MITRE, 2024).
	D3-FE – File Encryption	Gamma may encrypt important files stored on their machines, making them inaccessible even if they are accessed by a threat actor (MITRE, 2024).

1.2.3. Security Protections

To ensure that the sudo vulnerability is not exploited, Gamma must update the sudo version to the latest version. Moreover, Gamma must ensure that sudo access is only given to the users that must have access to it, such as system administrators.

On the other hand, Gamma should also ensure that a threat actor does not gain access to a Unix shell, for example, through reverse shell exploits. As explained above, process segment execution prevention is a good way to block those attempts.

1.3. (EXTERNAL) TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)

CVE-2013-2566 is a vulnerability in the way the RC4 cipher encrypts TLS/SSL traffic. RC4 has single-byte biases, allowing threat actors to statistically analyse the encrypted traffic and deduce the plaintext. NIST scores this vulnerability a CVSS score of "4.3 Medium" and the Rapid7 results depict that it is of low likelihood (severity rank "2") and medium impact (severity score "4"), as the RC4 encryption is not practical to break, but it is getting more feasible. Moreover, Microsoft published an RFC document prohibiting the use of RC4 in all TLS versions. Should an attacker break the RC4 cipher, the MITRE ATT&CK table below will outline the circumstances that would lead to this vulnerability being exploited (AlFardan et al., 2013; Goodin, 2015; Green, 2013; NIST, 2019; NIST, 2020; Popov, 2015, Rapid7, 2023a).

Moreover, the MITRE D3FEND table below will outline mitigation tactics to respond to the vulnerability being exploited and to minimise further and residual risk, and damages.

1.3.1. MITRE ATT&CK Table

Table 5: MITRE ATT&CK Techniques

Tactics	***Techniques***	***Explanation & Relevance***
Reconnaissance	T1590.005 – Gather Victim Network Information: IP Addresses	A threat actor must gather IP addresses in order to be able to capture TLS/SSL traffic encrypted with the RC4 Cipher. As Gamma is a public company, they own public-facing servers with publicly available IP addresses, making their detection unavoidable. Further detection may be done through active scanning and/or phishing (MITRE, 2023).
	T1590.004 – Gather Victim Network Information: Network Topology	A threat actor must understand Gamma's network topology to know which IP address is assigned to the most valuable server to gather network data from. Moreover, the threat actor must also know the IP address of the DNS server that Gamma's traffic uses to successfully carry out the Adversary-in-the-Middle attack (MITRE, 2023).
Resource Development	T1584.002 – Compromise Infrastructure: DNS Server	Compromising a DNS server allows a threat actor to alter DNS records and redirect previously secure connections to malicious connections. This connects one of Gamma's computers to the malicious DNS record and allows the threat actor to redirect traffic to the believed "secure" connection, while intercepting and capturing traffic (MITRE, 2023).

Discovery	T1040 – Network Sniffing	A threat actor must gather network traffic information using the Adversary-in-the-Middle attack, if outside the network. If a threat actor is inside the network, they would set their network interface to promiscuous mode, capturing all traffic over Gamma's internal network. The traffic captured must be TLS/SSL traffic encrypted with the RC4 cipher (MITRE, 2023).
Collection	T1557 – Adversary-in-the-Middle	A threat actor may position themselves in the middle of a connection, perhaps using the method described above in the "DNS Server" ATT&CK technique. This allows the threat actor to capture specific RC4 cipher traffic (MITRE, 2023).
Exfiltration	T1048.001 – Exfiltration Over Alternative Protocol: Exfiltration Over Symmetric Encrypted Non-C2 Protocol	After the network traffic has been captured, a threat actor may begin to save the RC4 cipher-encrypted data and begin to break the encryption using the vulnerability discussed above (MITRE, 2023).
Impact	T1657 – Financial Theft	The threat actor may attempt to sell the data recovered from the network traffic, or hold it for ransom (MITRE, 2023).

1.3.2. MITRE D3FEND Table

Table 6: MITRE D3FEND Techniques

ATT&CK Technique	***D3FEND Technique(s)***	***Explanation & Relevance***
T1040 – Network Sniffing	D3-DNSTA – DNS Traffic Analysis	Gamma can analyse their network traffic to check whether the DNS traffic resolves to a malicious host, indicating a breach (MITRE, 2024).
T1557 – Adversary-in-the-Middle	D3-NTF – Network Traffic Filtering	Gamma can detect the malicious IP address (or network) and filter the traffic incoming or outgoing to the attacker's network (MITRE, 2024).
T1048.001 – Exfiltration Over Alternative Protocol: Exfiltration Over Symmetric Encrypted Non-C2 Protocol	D3-NTF – Network Traffic Filtering	Gamma can detect the malicious IP address (or network) and filter the traffic incoming or outgoing to the attacker's network (MITRE, 2024).
	D3-OTF – Outbound Traffic Filtering	Gamma can detect the malicious IP address (or network) and filter the traffic ongoing to the attacker's network, effectively stopping the gathering of TLS/SSL traffic encrypted with the RC4 cipher (MITRE, 2024).

1.3.3. Security Protections

To secure Gamma's systems, one must ensure that whenever TLS/SSL is used, the traffic is not encrypted by the RC4 cipher. RFC 7465 already suggested the prohibition of using RC4 as a trusted encryption method for TLS/SSL traffic. Moreover, modern browsers, such as Firefox, have already disabled RC4 by default (King, 2015; Popov, 2015).

As suggested by the MITRE D3FEND Matrix, strong firewalls will assist Gamma in acting as another layer of defense against any vulnerability that may be exploited through the network.

1.4. (EXTERNAL) Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317)

CVE-2011-4317 is a vulnerability affecting old versions of the Apache HTTP server where, if configured incorrectly, an attacker can gain access to internal servers from an external connection via a malformed URI using the "@" and ":" signs in invalid positions. NIST gives this vulnerability a CVSS score of "4.3 Medium" and the Rapid7 results show that it is of low likelihood (severity rank "2") and medium-high impact (severity score "5"). An exploit from Qualys mentions that it can bypass "security", however it does not elaborate, but it can be assumed that firewalls might not work (NIST, 2019; NIST, 2023a; Parikh, 2011; Rapid7, 2023c).

The MITRE ATT&CK table below will outline the circumstances that would lead to this vulnerability being exploited.

Moreover, the MITRE D3FEND table below will outline mitigation tactics to respond to the vulnerability being exploited and to minimise further and residual risk, and damages.

1.4.1. MITRE ATT&CK Table

Table 7: MITRE ATT&CK Techniques

Tactics	***Techniques***	***Explanation & Relevance***
Reconnaissance	T1592.002 – Gather Victim Host Information: Software	A threat actor may attempt to get the version of Apache that is running on the external server by intentionally creating an error, i.e. 403 forbidden, where the page will display the version of Apache. If the Apache version is vulnerable, the threat actor may exploit it (MITRE, 2023).
	T1590.005 – Gather Victim Network Information: IP Addresses	The threat actor may attempt to gather the IP address of the target external server using reverse DNS search (MITRE, 2023).
	T1595.001 – Active Scanning: Scanning IP Blocks	The threat actor may scan the IP address found during reconnaissance and may use the nmap tool with the "-sV" tag to scan for the service version on the external server's IP address. If the Apache version is vulnerable, the threat actor may exploit it (MITRE, 2023; nmap.org, 2023).
Initial Access	T1190 – Exploit Public-Facing Application	The threat actor may exploit the CVE-2011-4317 vulnerability found on the Apache version they discovered during the reconnaissance phase (MITRE, 2023).
Execution	T1059.004 – Command and Scripting Interpreter: Unix Shell	The threat actor may use a Unix shell that has access to the netcat tool and connect to the external server. They must create a HTTP query to "@localhost" and the port number of a service, for example 8880, using two colons, "::", as the vulnerability explained. For example, "GET @localhost::8880 HTTP/1.0\r\n\r\n", will return the HTML page of the internal service running on port 8880 (MITRE, 2023; Parikh, 2011).

Exfiltration	T1048.003 – Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	The threat actor can steal data over an unencrypted, non-C2 protocol, such as HTTP. Using HTTP queries, the threat actor can gain access to the internal server, for example, an email server, and exfiltrate important internal emails; or an LDAP server, exfiltrating credentials databases (MITRE, 2023; Parikh, 2011).
Impact	T1657 – Financial Theft	The threat actor may hold the data exfiltrated for ransom, or sell it for their own financial gain, while impacting the organisation's revenue and reputation (MITRE, 2023).
	T1489 – Service Stop	Depending on the service running on the internal server, the threat actor may impact the availability of services essential to business or services that can inhibit a security incident, to achieve an overall goal, for example a HTTP server or an XDR, respectively (MITRE, 2023).

1.4.2. MITRE D3FEND Table

Table 8: MITRE D3FEND Techniques

ATT&CK Technique	***D3FEND Technique(s)***	***Explanation & Relevance***
T1190 – Exploit Public-Facing Application	D3-NTF – Network Traffic Filtering	Blocking the traffic originating from the attacker will ensure that they no longer have access to the vulnerable system, or perhaps the network. For example, dropping all packets from the suspected IP address's network (MITRE, 2024).
	D3-ITF – Inbound Traffic Filtering	Restricting access from untrusted networks towards a private or internal network will ensure that only networks that have been granted access will be able to access the internal hosts. This will mitigate the risk of a threat actor being able to access Gamma's internal networks through the Apache reverse-proxy vulnerability (MITRE, 2024).
T1059.004 – Command and Scripting Interpreter: Unix Shell	D3-LFP – Local File Permissions	Setting the proper local file permissions to only the users (or groups) that must access them will ensure that a threat actor will not be able to exfiltrate them due to the computer not allowing them (MITRE, 2024).
	D3-FE – File Encryption	Encrypting files will ensure that even if a threat actor may be able to exfiltrate data, it will be ineligible to them, unless they decrypt the files (MITRE, 2024).
T1048.003 – Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	D3-NTF – Network Traffic Filtering	As explained above, blocking network traffic from a suspected network (or IP address) will ensure that the computers will not exchange data (MITRE, 2024).
	D3-OTF – Outbound Traffic Filtering	Restricting outbound traffic ensures that data will not be able to travel outwards to a threat actor. Adding the suspicious network, or rather, allowing only approved networks to get responses from the internal systems will ensure that no threat actor can exfiltrate data over HTTP (MITRE, 2024).

1.4.3. Security Protections

To secure against the Apache proxy vulnerability, the simplest solution would be to update the version of Apache. However, if this is not possible, a correct reconfiguration of the proxy is required. One must ensure that the configuration does not resemble the one below (Parikh, 2011).

```
RewriteRule ^(.*) http://10.40.2.159/$1
ProxyPassMatch ^(.*) http://10.40.2.159/$1
```

On the other hand, strong and granular firewall rules would ensure that, even with the vulnerability present, a threat actor would not be able to connect to Gamma's intranet.

1.5. InsightVM Vulnerability Management Tool Overview

1.5.1. Summary

Rapid7's InsightVM is a lightweight vulnerability management tool that can be deployed on all of an organisation's endpoints, including remote workers' machines. It employs a live dashboard where one can monitor vulnerabilities in real-time. The live dashboard can be custom-made to whoever is viewing it, be it an executive or a system administrator, making the tool accessible for all levels of understanding. InsightVM also employs attack surface monitoring with Project Sonar, making it easy to understand the organisation's vulnerable spots regardless of how complex it becomes due to its growing size. Moreover, an organisation can use InsightVM's Policy Assessment to ensure the organisation is compliant with a standard or a policy before an audit, crucial to Gamma's credibility and business continuation (Rapid7, 2023b; Rapid7, 2024).

1.5.2. Vulnerability Management

InsightVM ranks the vulnerabilities found using its "Active Risk Score". The tool uses the CVSS scores used by NIST along with proprietary Rapid7 research to give vulnerabilities a more granular and accurate score, making ranking them easier (Rapid7, 2024).

1.5.2.a. Vulnerability Scoring

InsightVM's Active Risk scores its vulnerabilities on a scale from 1 to 1000, better indicating the severety of the vulnerability. The vulnerabilities are scored using CVSS scores, along with AttackerKB and Project Heisenberg proprietary vulnerability data, providing more detailed information about the threats to InsightVM users. Active Risk shows which vulnerabilities are being currently "exploited in the wild" or which are most likely to be exploited. Apart from the Active Risk scoring from 1 to 1000, it also employs two other ranking systems, Risk Score Severity and Risk Score Severity & Publish Age, making the risk scoring more granular (Rapid7, 2024).

1.5.2.b. Internal & External Vulnerabilities

InsightVM treats found internal and external vulnerabilities in a similar fashion. A user can configure a manual scan to differentiate between external-facing assets and internal-facing assets. A user can manually run a scan on an external-facing service and analyse its vulnerabilities and vice-versa. However, this would only need to occur if InsightVM's distributed scan engine (the live scanning on each of the organisation's nodes) has failed (Rapid7, 2023b; Rapid7, 2024).

1.5.3. Conclusion

InsightVM is more than a vulnerability management tool. InsightVM allows an organisation to not only view their vulnerabilities, but make it understandable for everyone, including those not extremely technical. InsightVM would ease Gamma's vulnerability analysis by giving a live feed of the crucial vulnerabilities on all of Gamma's endpoints, overall increasing the effectiveness and swiftness of dealing with the vulnerabilities, therefore making Gamma's systems more secure. Moreover, InsightVM can help Gamma with standard and policy audits, making standardisation more easy to manage and assuring compliance with international standards such as ISO 27001 (Rapid, 2023b; Rapid, 2024).

Overall, InsightVM would vastly improve Gamma's communication between departments, security of Gamma's systems and, as a result, Gamma's reputation as an online bank.

2. Threat Intelligence

2.1. Qakbot Intelligence Summary

2.1.1. Executive Summary

Qakbot is a Remote-Access Trojan (RAT) known to be a banking trojan, stealing financial data from infected bank systems. This makes Gamma a prime target for threat actors with access to Qakbot (Malpedia, 2023).

Qakbot attempts to infect victims with "malspam". The term "malspam" refers to spam emails that contain malicious attachments. Qakbot may use compromised email credentials or attempt to hijack an email thread to appear more credible (CISA, 2020).

2.1.2. Analyst Comments

Qakbot attempts to first spread using a malicious Microsoft Office macro, therefore the malicious email attachment may appear as an important Excel document related to Gamma's activities, i.e. a quarterly report. A threat actor's first attack Qakbot uses phishing, a form of social engineering, to target poorly trained employees (CISA, 2020).

Should Qakbot infiltrate Gamma's network, it would begin to impede Gamma's activities, and at worst halt them, as the employees would get their business accounts hijacked. This would cause Gamma's reputation to plummet, causing a loss in customers and therefore profits. Moreover, Gamma may be subject to a GDPR fine, if personally identifiable information (PII) is stolen along with the financial data.

2.1.3. Recommendation

It is recommended to employ mandatory social engineering training for Gamma's employees, as 83% of UK businesses that suffered a cyber attack reported it as phishing, making it a common attack vector (CISA, 2020; Griffiths, 2024).

To ensure these spam emails never reach employees, Gamma must keep its spam email filter up to date and email policies must be granular, for example marking external emails (CISA, 2020).

2.2. XWorm Intelligence Report

2.2.1. Intelligence Summary

XWorm is a multi-phase remote-access trojan (RAT) that first spreads itself through phishing emails. It is designed to steal cryptocurrency and sensitive data by hijacking crypto-wallets, i.e. MetaMask, and Telegram accounts (ANY.RUN, 2023a; Pachpor and Adarsh, 2023).

XWorm has multiple versions and it is sold as malware-as-a-service. Once it established persistence, a command-and-control server can make XWorm do anything it wants, even launch ransomware on the affected computers (ANY.RUN, 2023a).

2.2.2. MITRE TTPs

1. A threat actor may begin with a Word document attached to a phishing email, luring a victim by showing itself as an invoice (Initial Access – T1566.001) (MITRE, 2023; Pachpor and Adarsh, 2023).

2. The Word document would hold a VBA script which executes upon opening the Word document (Execution – T1204.002) (MITRE, 2023).

3. The script would access a blogspot URL which would redirect to a download link of a Powershell script, then automatically launching it. Upon launching, XWorm is downloaded off a Mediafire server and installed into the Public directory (Command and Control – T1102; Execution – T1059.001; Collection – T1074.001) (ANY.RUN, 2023b; MITRE, 2023; Pachpor and Adarsh, 2023).

4. Upon being launched, XWorm establishes persistance by inserting a shortcut of itself into Windows' Startup directory, using the Task Scheduler afterwards to restart itself with elevated privileges. (Persistence – T1547.001; Privilege Escalation – T1053.005) (ANY.RUN, 2023b; MITRE, 2023).

5. XWorm attempts connection with a control server at port 13394 (Command and Control - T1571) (ANY.RUN, 2023b; MITRE, 2023).

6. XWorm attempts to verify if it is running in a sandboxed environment by querying an online IP discovery service that can also detect virtual environments (Reconnaissance – T1590.005). If XWorm detects it is running in a sandboxed environment, it crashes (ANY.RUN, 2023b; MITRE, 2023).

7. If XWorm continues running, it attempts to transmit data collected about the host (username, OS version and a victim identifier hash) and its own version to Telegram (Discovery – T1082 ; Command and Control – T1102.002) (ANY.RUN, 2023b; MITRE, 2023).

8. According to ANY.RUN's (2023b) initial analysis of XWorm, the malware is obfuscated (Defense Evasion – T1027). In a later stage of analysis, ANY.RUN (2023b) reverse engineered the malware and established that XWorm uses the Windows Management Instrumentation to check whether it is running in a sandboxed environment (Execution – T1047) (MITRE, 2023).

2.2.3. Impact

Gamma is an online bank that, perhaps, just as other online banks such as Revolut and Monzo, hold cryptocurrency. XWorm will attempt to overwrite Gamma's cryptocurrency addresses to its own to deceive customers and steal their crypto coins (Pachpor and Adarsh, 2023).

Moreover, XWorm is able to carry out ransomware attacks, encrypting Gamma's sensitive and financial data. If this occurs, Gamma will be required to halt activities while backups are restored, losing customer data, i.e. transactions, gathered between the last backup and the current time, affecting integrity and availability. Gamma's customers are likely to lose trust in the bank, due to their crypto coins being lost, causing Gamma to lose the customers and having to pay for damages (Pachpor and Adarsh, 2023).

On the other hand, GDPR laws state that if any personally identifiable information is disclosed, affecting confidentiality, fines will be imposed on Gamma (Pachpor and Adarsh, 2023).

2.2.4. Mitigations

Firstly, Gamma must ensure that their employees are thoroughly trained in detecting phishing emails and other social engineering techniques. As stated in Griffiths (2024), phishing is a common attack vector, therefore it is in Gamma's best interest to ensure that the employees are properly trained.

D3-EF – Email Filtering – Gamma must ensure that their organisation's email server filters emails coming from outside the organisation. This can be done by marking the outside emails to let Gamma's employees know to be extra careful when interacting with the email (MITRE, 2024).

D3-ER – Email Removal – Gamma must employ software that can detect suspicious emails on their email server. Suspicious emails may be ones that have an executable as an attachment, while Gamma's policy is to not send executables as attachments. When these suspicious emails are detected, follow-up actions such as blocking the sender, must be done (MITRE, 2024).

D3-NTF – Network Traffic Filtering – Gamma must ensure that they employ a strong incoming and outgoing firewall, with granular rules that are kept up to date with the new IOCs, such as the ones listed below. Gamma must take publicly-available IOCs and integrate them into their firewalls to ensure that the traffic to and from these domains get blocked. Gamma can consider the possibility of introducing software that automates this with the newest malware definitions (MITRE, 2024).

2.2.5. Indicators of Compromise

Table 9: XWorm-associated URLs & C2s (Pachpor and Adarsh, 2023)

XWorm-associated URLs & C2s
updateccdata[.]duckdns[.]org
hxxps://adobeupdate2023[.]blogspot[.]com/atom[.]xml
hxxps://download2431[.]mediafire[.]com/o7khka7z7uxgxXFo9SrPO7wP0cQwlUtJopql7sPYu3y5km5nQCrqO0tfHsvP8gHpJy7pFWUtQVWCag6RRTAapOY9w/zfilcaiw6chd9hu/invoice-1588307354[.]pdf[.]js
hxxps://updatepower2023[.]blogspot[.]com/atom[.]xml
hxxps://529f38d0-3744-4286-b484be860d475d25[.]usrfiles[.]com/ugd/529f38_6521c5ccbd8d46acb81ce3eb5cc3cc56[.]txt

stanthely2023[.]duckdns[.]org
port3000newspm[.]duckdns[.]org
zenova[.]duckdns[.]org
hxxps://urlintimacygoombguch[.]blogspot[.]com/atom[.]xml
hxxps://powpowpowff[.]blogspot[.]com/atom[.]xml
hxxps://adobeacrobateupdate2023[.]blogspot[.]com/atom[.]xml
hxxps://abodeupdatenew[.]blogspot[.]com/atom[.]xml
hxxps://updatingmsoffice[.]blogspot[.]com/atom[.]xml
hxxps://huskidkifklaoksikfkfijsju[.]blogspot[.]com/atom[.]xml
hxxps://a[.]pomf[.]cat/kfbahy[.]hta
hxxps://73cceb63-7ecd-45e2-9eab-f8d98aab177f[.]usrfiles[.]com/ugd/73cceb_b5b6005e2aa74cf48cd55dca1a2ff093[.]docx
hxxps://73cceb63-7ecd-45e2-9eab-f8d98aab177f[.]usrfiles[.]com/ugd/73cceb_e5a698286daf43ac87b4544a35b1a482[.]txt
6[.]tcp[.]eu[.]ngrok[.]io (ANY.RUN, 2023b)

Table 10: XWorm-associated cryptocurrency wallets (Pachpor and Adarsh, 2023)

XWorm-associated cryptocurrency wallets
BTC: 3CghDNiD2J5xsS9i1wzwbvwdTJxokqGCmC
ETH: 0x8af86e2c7126d08387e71ec6699bc69f957cdee6
TRC20: TeoYgXKbx5nKq3i6jB2KsHby93bWQuKi1C

Table 11: XWorm-associated SHA256 hashes (Pachpor and Adarsh, 2023)

XWorm-associated SHA256 hashes
d7e4ac9db513592230624aab493aceb6acbbd3503b286ce64e6d808850fbaab7
0d90fde0cc738db8dbc06852a68e13820e7227ab10679ac1dceac13840e571f5
a5822895ccbd489703c94c24f6b4b41ce78cb9a39992e9df130932b07193f7d5
f515bb9186cc9e8b8aff3a4c65284493c7a3f703c9ff70c2c656bb5e0b95003d
dca74423e6e7b7ee5e696099549dacb4e1ffb9dccccd81e0ac1f7ce2b6be2003
f3e6621928875a322ee7230ccf186bdaa5609118c4a6d1c2f4026adfb8e88744
93e72f97f81af71808283cd10ab5b7ddf0038d232fb89956e8b5329c0c8797ba
9f255b6109a66d6db5b525dab165b6e5a59da6a26bcee6221bbc2bfa36829690
bf5ea8d5fd573abb86de0f27e64df194e7f9efbaadd5063dee8ff9c5c3baeaa2
3c45a698e45b8dbb1df206dec08c8792087619e54c0c9fc0f064bd9a47a84f16

2.3. OSINT Case Study

2.3.1. Threat Actor Groups

2.3.1.a Anonymous Sudan

Anonymous Sudan is a Russian-affiliated hacktivist group targeting entities that engage in what they deem to be anti-Muslim activity. In April 2023, Anonymous Sudan attacked critical targets in Israel's infrastructure, such as the Mossad and Industrial Control Systems, with pro-Palestine motivations (Braithwaite, 2023; Cloudflare, 2023; Schappert, 2023).

Anonymous Sudan's capabilities are threats through public announcements and distributed denial of service (DDoS) attacks using HTTP traffic to flood targets and render them useless or sluggish. They do not use botnets, but rather they use rented servers, which can output more traffic than personal devices, making attacks more effective but also more expensive. They are believed to work with other Russian-affiliated groups, such as Killnet, to conduct such expensive flood attacks (Braithwaite, 2023; Cloudflare, 2023; Petkauskas, 2023; Schappert, 2023).

2.3.1.b Cyber Toufan

Cyber Toufan Al-aqsa is an Iranian-backed hacktivist group conducting aggressive cyber attacks and psychological warfare (political statements, propaganda). They target Israeli organisations, conducting data breaches and sensitive data extraction, and even collaborate with other threat actor groups. For example, Cyber Toufan attacked Signature-IT in Israel, an e-commerce and website hosting service, managing to extract websites belonging to businesses and national entities. They publish databases collected from the websites which contain gigabytes of personal information. In November 2023, they stopped releasing data leaks, for the duration of the Israel-Palestine ceasfire. They can possibly target Alpha with these aggressive methods and extract sensitive research data and even employees' personal information, leading to GDPR fines (Kaur, 2023; SOCRadar, 2023).

2.3.1.c Killnet

Killnet is a Russia-aligned group, believed to be working with another Russian-aligned group, Anonymous Sudan. Killnet targets Israeli websites, government and otherwise, with DDoS attacks, taking them offline. Unlike Anonymous Sudan, Killnet uses a large botnet capable of generating 2.4 Tbps of traffic, utilising different DDoS available scripts, and their own proprietary tools to carry out attacks. Killnet has claimed responsibility for attacking logistics facilities and healthcare facilities, therefore Alpha's systems can be at risk of being targeted (Flashpoint, 2024; Gallagher and Robertson, 2023; Quorum Cyber, 2023).

2.3.1.d TA402

TA402 is a Palestinian-aligned threat actor, conducting phishing campaigns against Middle Eastern governments. They use cloud services such as Dropbox and Google Drive to host multifunctional malware, such as XLL files and RAR files, however TA402 frequently changes their infection chain to avoid detection. TA402 also own infrastructure that they utilise for command and control communications (Malpedia, 2023b; Miller, 2023).

2.3.2. Potential Cyber Threats to Alpha Employees

Threat actors that attack industrial control systems (ICS), such as Anonymous Sudan and ThreatSec, are sure to attack Alpha's facilities in Israel and Palestine, regardless of Alpha's political positioning. Attacking the SCADA architecture of Alpha's ICS systems will halt the employees' activities by halting the R&D facilities' internal communication and data collection between different media control systems (Lapienytė, 2023; Thomasnet, 2024).

Cyber Toufan targets organisations that operate in Israel, making Alpha a target. They consistently attempt to collect sensitive personal information, such as employee details, leaking them online (SOCRadar, 2023).

3. References

AlFardan, N.J., Bernstein, D.J., Paterson, K.G., Poettering, B. and Schuldt, J.C.N. (2013). *Wayback Machine*. [online] web.archive.org. Available at: https://web.archive.org/web/20130922170155/http://www.isg.rhul.ac.uk/tls/RC4biases.pdf [Accessed 16 Dec. 2023].

ANY.RUN (2023a). *XWorm | Malware Trends Tracker*. [online] XWorm | Malware Trends Tracker. Available at: https://any.run/malware-trends/xworm [Accessed 10 Jan. 2024].

ANY.RUN (2023b). *XWorm: Technical Analysis of a New Malware Version*. [online] ANY.RUN's Cybersecurity Blog. Available at: https://any.run/cybersecurity-blog/xworm-technical-analysis-of-a-new-malware-version/.

Braithwaite, S. (2023). *Anonymous Sudan Targets Israel's Critical Infrastructure – Westoahu Cybersecurity*. [online] University of Hawai'i - West O'ahu. Available at: https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/anonymous-sudan-targets-israels-critical-infrastructure/ [Accessed 11 Jan. 2024].

CISA (2020). *Qbot/QakBot Malware*. [online] Available at: https://www.cisa.gov/sites/default/files/2023-02/202010221030_qakbot_tlpwhite.pdf [Accessed 10 Jan. 2024].

Cloudflare (2023). *What is Anonymous Sudan?* [online] cloudflare.com. Available at: https://www.cloudflare.com/learning/ddos/glossary/anonymous-sudan/ [Accessed 11 Jan. 2024].

Flashpoint (2024). *Killnet*. [online] Flashpoint. Available at: https://flashpoint.io/intelligence-101/killnet/ [Accessed 11 Jan. 2024].

Gallagher, R. and Robertson, J. (2023). *Cyberattacks Targeting Israel Are Rising After Hamas Assault*. [online] TIME. Available at: https://time.com/6322175/israel-hamas-cyberattacks-hackers/ [Accessed 11 Jan. 2024].

Goodin, D. (2015). *Once-theoretical crypto attack against HTTPS now verges on practicality*. [online] Ars Technica. Available at: https://arstechnica.com/information-technology/2015/07/once-theoretical-crypto-attack-against-https-now-verges-on-practicality/ [Accessed 16 Dec. 2023].

Green, M. (2013). *Attack of the week: RC4 is kind of broken in TLS*. [online] A Few Thoughts on Cryptographic Engineering. Available at: https://blog.cryptographyengineering.com/2013/03/12/attack-of-week-rc4-is-kind-of-broken-in/ [Accessed 16 Dec. 2023].

Griffiths, C. (2024). *The Latest Phishing Statistics (updated January 2024) | AAG IT Support*. [online] aag-it.com. Available at: https://aag-it.com/the-latest-phishing-statistics/ [Accessed 10 Jan. 2024].

Kathpal, H. (2021). *CVE-2021-3156: Heap-Based Buffer Overflow in Sudo (Baron Samedit)*. [online] Qualys Security Blog. Available at: https://blog.qualys.com/vulnerabilities-threat-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit [Accessed 15 Dec. 2023].

Kaur, G. (2023). *Cyberattacks on Israel intensify as the war against Hamas rages: Check Point*. [online] CSO Online. Available at: https://www.csoonline.com/article/1249135/cyberattacks-on-israel-intensify-as-the-war-against-hamas-rages-check-point.html [Accessed 11 Jan. 2024].

King, A. (2015). *Deprecating the RC4 Cipher*. [online] Mozilla Security Blog. Available at: https://blog.mozilla.org/security/2015/09/11/deprecating-the-rc4-cipher/ [Accessed 9 Jan. 2024].

Lapienytė, J. (2023). *Hacktivists in Palestine and Israel after SCADA and other industrial control systems*. [online] cybernews.com. Available at: https://cybernews.com/cyber-war/palestine-israel-scada-under-attack/ [Accessed 11 Jan. 2024].

Malpedia (2023a). *QakBot (Malware Family)*. [online] malpedia.caad.fkie.fraunhofer.de. Available at: https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot [Accessed 10 Jan. 2024].

Malpedia (2023b). *TA402 (Threat Actor)*. [online] malpedia.caad.fkie.fraunhofer.de. Available at: https://malpedia.caad.fkie.fraunhofer.de/actor/ta402 [Accessed 11 Jan. 2024].

Microsoft (2023). *CVE-2013-3900 - Security Update Guide - Microsoft Security Response Center*. [online] msrc.microsoft.com. Available at: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900 [Accessed 15 Dec. 2023].

Miller, J. (2023). *TA402 Uses Complex IronWind Infection Chains to Target Middle East-Based Government Entities | Proofpoint US*. [online] Proofpoint. Available at: https://www.proofpoint.com/us/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-middle-east-based-government [Accessed 11 Jan. 2024].

MITRE (2023). *Techniques - Enterprise | MITRE ATT&CK®*. [online] attack.mitre.org. Available at: https://attack.mitre.org/techniques/enterprise/ [Accessed 26 Dec. 2023].

MITRE (2024). *D3FEND Matrix | MITRE D3FEND™*. [online] d3fend.mitre.org. Available at: https://d3fend.mitre.org/ [Accessed 9 Jan. 2024].

NIST (2019). *NVD - Vulnerability Metrics*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln-metrics/cvss [Accessed 15 Dec. 2023].

NIST (2020). *NVD - CVE-2013-2566*. [online] nvd.nist.gov. Available at: https://nvd.nist.gov/vuln/detail/CVE-2013-2566 [Accessed 16 Dec. 2023].

NIST (2022). *NVD - CVE-2013-3900*. [online] nvd.nist.gov. Available at: https://nvd.nist.gov/vuln/detail/CVE-2013-3900 [Accessed 15 Dec. 2023].

NIST (2023a). *NVD - CVE-2011-4317*. [online] nvd.nist.gov. Available at: https://nvd.nist.gov/vuln/detail/CVE-2011-4317 [Accessed 16 Dec. 2023].

NIST (2023b). *NVD - CVE-2021-3156*. [online] nvd.nist.gov. Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-3156 [Accessed 15 Dec. 2023].

nmap.org (2023). *Service and Version Detection | Nmap Network Scanning*. [online] nmap.org. Available at: https://nmap.org/book/man-version-detection.html [Accessed 18 Dec. 2023].

Pachpor, P. and Adarsh, S. (2023). *Uncovering the XWorm Malware Campaign*. [online] www.trellix.com. Available at: https://www.trellix.com/about/newsroom/stories/research/old-loader-new-threat-exploring-xworm/ [Accessed 10 Jan. 2024].

Parikh, P. (2011). *Apache HTTP Server Reverse Proxy/Rewrite URL Validation Issue*. [online] Qualys Security Blog. Available at: https://blog.qualys.com/vulnerabilities-threat-research/2011/11/23/apache-reverse-proxy-bypass-issue [Accessed 16 Dec. 2023].

Petkauskas, V. (2023). *Anonymous Sudan: neither anonymous nor Sudanese*. [online] cybernews.com. Available at: https://cybernews.com/editorial/anonymous-sudan-explained/ [Accessed 11 Jan. 2024].

Popov, A. (2015). *RFC7465 - Prohibiting RC4 Cipher Suites*. [online] datatracker.ietf.org. Available at: https://datatracker.ietf.org/doc/html/rfc7465 [Accessed 16 Dec. 2023].

Quorum Cyber (2023). *Killnet Threat Actor Profile*. [online] Quorum Cyber. Available at: https://www.quorumcyber.com/threat-actors/killnet-threat-actor-profile/ [Accessed 11 Jan. 2024].

Rapid7 (2023a). *Executive Summary Report | InsightVM Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/executive-report/ [Accessed 15 Dec. 2023].

Rapid7 (2023b). *Welcome to InsightVM | InsightVM Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm [Accessed 9 Jan. 2024].

Rapid7 (2023c). *Working with vulnerabilities | InsightVM Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/insightvm/working-with-vulnerabilities/ [Accessed 15 Dec. 2023].

Rapid7 (2024). *Vulnerability Management Tool, Top Rated Scanner: InsightVM*. [online] Rapid7. Available at: https://www.rapid7.com/products/insightvm/.

Red Hat (2023). *CVE-2021-3156 - Red Hat Customer Portal*. [online] access.redhat.com. Available at: https://access.redhat.com/security/cve/cve-2021-3156 [Accessed 15 Dec. 2023].

Roger, R. (2023). *CVE-2013-3900 WinVerifyTrust Signature Validation Vulnerability - Microsoft Q&A*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/answers/questions/1182542/cve-2013-3900-winverifytrust-signature-validation [Accessed 9 Jan. 2024].

Schappert, S. (2023). *Anonymous Sudan targets Israel premier and Mossad*. [online] cybernews.com. Available at: https://cybernews.com/news/anonymous-sudan-targets-israel-mossad-netanyahu/ [Accessed 11 Jan. 2024].

SOCRadar (2023). *Dark Web Profile: Cyber Toufan Al-aqsa*. [online] SOCRadar® Cyber Intelligence Inc. Available at: https://socradar.io/dark-web-profile-cyber-toufan-al-aqsa/[Accessed 11 Jan. 2024].

The Hacker News (2023). *Inside XWorm: Malware Analysts Decode the Stealthy Tactics of the Latest Variant*. [online] The Hacker News. Available at: https://thehackernews.com/2023/09/inside-code-of-new-xworm-variant.html [Accessed 10 Jan. 2024].

Thomasnet (2024). *Types of Industrial Control Systems - A Thomas Buying Guide*. [online] www.thomasnet.com. Available at: https://www.thomasnet.com/articles/instruments-controls/types-of-industrial-control-systems/ [Accessed 11 Jan. 2024].