

Assignment Guidance and Front Sheet

This front sheet for assignments is designed to contain the brief, the submission instructions, and the actual student submission for any WMG assignment. As a result the sheet is completed by several people over time, and is therefore split up into sections explaining who completes what information and when. Yellow highlighted text indicates examples or further explanation of what is requested, and the highlight and instructions should be removed as you populate 'your' section.

This sheet is only to be used for components of assessment worth more than 3 CATS (e.g. for a 15 credit module, weighted more than 20%; or for a 10 credit module, weighted more than 30%).

To be completed by the student(s) prior to final submission:

Your actual submission should be written at the end of this cover sheet file, or attached with the cover sheet at the front if drafted in a separate file, program or application.

Student ID or IDs for group work	U2136249
----------------------------------	----------

To be completed (highlighted parts only) by the programme administration after approval and prior to issuing of the assessment; to be consulted by the student(s) so that you know how and when to submit:

Date set	Tuesday 10th October 2023
Submission date (excluding extensions)	Friday 12th January 2024 by 16:00pm.
Submission guidance	To be submitted electronically via Tabula.
Late submission policy	If work is submitted late, penalties will be applied at the rate of 5 marks per University working day after the due date, up to a maximum of 10 working days late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means after the submission deadline time as well as the date – work submitted after the given time even on the same day is counted as 1 day late.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

To be completed by the module owner/tutor prior to approval and issuing of the assessment; to be consulted by the student(s) so that you understand the assignment brief, its context within the module, and any specific criteria and advice from the tutor:

Module title & code	Operational Security Management (WM3B4)
Module owner	Dr. Christo Panchev

Module tutor	Hassan Raza
Assessment type	Course Work 1
Weighting of mark	40

Word count	3000 words You will not be penalised for producing under length work, provided quality is not sacrificed to brevity. Learning to write to a limit is one of the skills the degree is designed to encourage you to cultivate.		
Does the word count allow +10%? Select ONE	Does the word count include tables? Select ONE	Does the word count include references? Select ONE	Does the word count include appendices? Select ONE
Yes	No	No	No
If appendices are included, will they be marked? No			

Submission format	PDF
-------------------	-----

Module learning outcomes (numbered)	<ul style="list-style-type: none"> • Anticipate cyber behaviors, both deliberately adversarial and unintentionally inept, that would undermine an organization's viability. • Critically evaluate the vulnerabilities of an organization through active probing of its systems. • Manage cyber resources to maintain an organization's viability in the face of adversarial or unintentional threats.
Learning outcomes assessed in this assessment (numbered)	As above
Marking guidelines	Generally indicated within specification
Academic resources guidance	<p>You will have an opportunity to ask questions and get support on the assessment after it has been handed to you. You will be supported in this assessment through:</p> <ol style="list-style-type: none"> 1. A special Moodle forum. 2. Through emails directed to the module tutor. <p>Notes to students:</p> <p>If support is provided on a Teams Channel or a Moodle forum, please ensure you check previous questions posted on the channel. The Teams/Moodle channel will typically be closed one week before the submission date and no new questions will be addressed, please organise your time accordingly. Please be patient with module tutors. Please turn on your Teams Channel/Moodle notifications. If a tutor has not responded to a query within 5 working days, please email the module tutor.</p>

Special instructions	<p>Do not include the PMA specification in the submission.</p> <p>Spelling/grammar. Ensure that you spell check the submission, use a grammar checker and ensure that you proofread your work prior to submission. Spell/grammar checkers must be set to UK English, do not use 'Americanised' spellings.</p> <p>References. References are to be included at the end of the report using the Harvard referencing system. You should not include a bibliography. Each reference must be connected to a citation within the main body of the report.</p> <p>Do not attempt to hide text within JPEGs, this will be construed as an attempt to mislead the assessor.</p> <p>Coherence. A poorly worded report will hide excellent content. The narrative should be easy to read, and arguments should be presented coherently and convincingly.</p> <p>Presentation. At this stage in your studies, there is no excuse for poor presentation. You will not receive marks for presentation; however, your submission will be penalised for poor presentation.</p> <p>Formatting. All figures and tables must be properly labelled and captioned. All pages must be numbered. Formatting must be consistently applied throughout the submission. Submissions that stray from this guidance may be penalised.</p>
----------------------	--

Contents

Part 1.1 - MITRE ATT&CK and MITRE D3FEND Analysis.....	5
Internal: Critical- CVE-2021-44228 (Log4j2).....	5
MITRE DEF3ND Analysis:.....	6
Internal: Medium - CVE-2022-26925 – LSA Spoofing	6
MITRE ATT&CK Analysis:.....	7
MITRE DEF3ND Analysis:.....	8
CVE-2022-23943 – External: Critical	9
MITRE DEF3ND Analysis:.....	10
External: Medium - CVE-2021-23841	10
MITRE DEF3ND Analysis:.....	11
Part 1.2 – Vulnerability Management Tool Recommendation	12
Part 2.1: Threat Intelligence Summary	14
Threat Intelligence Report – QakBot Malware.....	15
Part 2.2 - OSNIT Analysis: Alpha	18
HEXANE:	18
Moses Staff:	19
CopyKittens:	21
POLONIUM:	22
Appendix A.....	23
Appendix B	27
Appendix C	28
References:.....	29
Figure 1 - Qualys Launch Vulnerability Scan	23
Figure 2 - Qualys Schedule Vulnerability Scan	23
Figure 3 - Qualys VMDR Portal.....	24
Figure 4 - Qualys Feed.....	24
Figure 5 Qualys Report.....	25
Figure 6 - Qualys Could Agent	25
Figure 7 - Qualys Policy Compliance	26
Figure 8 - XWorm hosted for Sale.....	27
Figure 9 - Telegram group to provide updates on Worm tools.....	27
Figure 10 - Sampel Qakbot campaign.....	28

Part 1.1 - MITRE ATT&CK and MITRE D3FEND Analysis

Internal: Critical- CVE-2021-44228 (Log4j2)

CVE-2021-44228 in Log4j 2 poses a high risk to Gamma's online banking platform due to its widespread presence, ease of exploitation, and potentially devastating impact. Attackers can gain initial access through user-controlled inputs, escalate privileges, move laterally within the network, and steal sensitive data or disrupt operations. However, proactive vulnerability management, network segmentation, IDS/IPS deployment, threat intelligence monitoring, and code analysis practices can significantly mitigate this risk. Implementing these controls is crucial for protecting Gamma's critical infrastructure and minimising potential damages from Log4j 2 exploitation. (INCIBE, 2022)

MITRE ATT&CK Analysis:

Stage - Tactic(s) ID	Technique(s)	Procedurals
Initial Access (TA0001)	Exploit Public-Facing Application (IT1190)	Threat actor crafts a malicious web request containing an arbitrary string with JNDI syntax and injects it into a vulnerable application's log data (e.g. user input, URLs, HTTP headers, or logging messages). This triggers the Log4j2 vulnerability to parse the malicious string and remotely load and execute arbitrary code.
	Spearfishing Attachment (T1193)	Threat actor sends a spear phishing email with malicious JNDI injection payload embedded in a crafted JAR file (e.g. via attachment), containing the vulnerable Log4j2 code that exploits the vulnerability.
	Supply Chain Compromise (T1195)	Threat actor exploits third-party libraries or dependencies containing Log4j2 vulnerability or to gain
Execution (TA0002)	Scheduled Task (T1053)	Once Malicious data is injected and parsed by log4j2, it can be interpreted as a JNDI lookup, leading to an RCE, allowing the threat actor to download and execute arbitrary code on the target system.
Persistence (TA0003)	Modify Registry (T1112)	Threat actor establishes persistence by modifying the system registry keys, or startup folder through Remote Code Execution RCE by exploiting log4j2 vulnerability.
Privilege Escalation (TA0004)	Valid Accounts (T1078)	Threat actor leverages RCE gained through Log4j2 vulnerability to escalate privileges by exploiting vulnerable system accounts or misconfigured permissions.
	Exploitation for Privilege Escalation (T1068)	Threat actor leverages RCE gained through Log4j2 vulnerability to exploit local vulnerabilities to escalate privileges within the compromised system, gaining access to more sensitive resources.
Impact (TA0040)	Network Denial of Service (T1498)	Threat actor could disrupt system operations by deleting critical files, corrupting data, or deploying denial-of-service attacks. This could

		cause widespread disruption, making it difficult for legitimate users to access critical resources, leading to financial loss, reputational damage, or even compliance violations.
	Data Exfiltration	Threat actor embeds data exfiltration techniques within the injected code Logs containing sensitive information (e.g. AMCE credentials, PII data) are sent to attacker-controlled servers. Or to deploy ransomware, causing encryption or deletion of critical data, resulting in significant disruption and potential financial losses for AMCE.

MITRE DEF3ND Analysis:

Security Protections	ATT&CK Mitigations	Explanation & Relevance
Application Hardening	Exploit Protection (M1050)	Deploying IDS/IPS systems configured to detect and block exploit attempts targeting Log4j vulnerabilities can provide real-time protection against attacks.
Network Security	Restrict Web-Based Content (M1021)	Monitoring network traffic for anomalous activity, such as suspicious LDAP lookups or spikes in traffic originating from unfamiliar sources, can help detect exploitation attempts.
Log Monitoring	Behaviour Prevention on Endpoint (M1040)	Implementing code analysis tools and sandboxing environments can help detect malicious JNDI payloads and prevent their execution within Gamma's systems.
Security Operations	User Training (M1017)	Implement a security operations centre (SOC) to monitor and analyse logs for suspicious activity. Have a well-defined incident response (IR) plan in place to respond to security incidents effectively. Conduct regular security awareness training for employees.

Internal: Medium - CVE-2022-26925 – LSA Spoofing

Threat actors could exploit CVE-2022-26925 to compromise Gamma's domain controllers, potentially leading to significant financial and reputational damage. By sending crafted NTLM authentication requests, attackers could gain initial access, establish persistence, move laterally, steal sensitive data, and disrupt operations. To mitigate these risks, Gamma should prioritise network segmentation, endpoint protection, multi-factor authentication, prompt patching, and a robust SOC. While the likelihood of exploitation is deemed "high" due to the vulnerability's publicly available exploit code (Tenable, 2022), the potential impact score is "critical" given the sensitive nature of Gamma's financial data and operations.

MITRE ATT&CK Analysis:

Tactic	ATT&CK Technique	Explanation & Relevance
Initial Access	Exploit Public Services (T1190)	<p>Threat actor exploits this vulnerability by sending custom crafted NTLM authentication request to the vulnerable LSARPC interface on a domain controller.</p> <p>This could trick the domain controller into authenticating the attacker, granting them initial access to Gamma's network.</p>
Persistence	Remote Services (T1333)	<p>Threat actor leverages the compromised domain controller to establish persistence by creating malicious services or modifying existing ones.</p> <p>These services could be used for further exploitation, process injection, lateral movement to escalate the attacker's privileges, enabling access to Gamma's sensitive information.</p>
Execution	Remote Services: Remote Desktop Protocol (RDP) (T1021.001)	<p>Threat actor uses compromised local accounts to gain access to other systems on the network, including user workstations and services.</p> <p>RDP is a common target for lateral movement with the goal to access unauthorised systems and potentially establish a foothold in Gamma's network.</p>
Credential Access	Use Alternate Authentication Material: Pass the Hash (T1550.002)	<p>Threat actor obtains NTLM hashes of user's passwords, using them to authenticate to other systems on the network without rising suspicious by monitoring logs.</p> <p>This could be obtained by compromising the domain controller's access to user credentials, potentially exposing current PII information about Gamma's employees.</p>
Defence Evasion	Indirect Command Execution (T1202)	<p>Threat actor uses compromised services and scripts to indirectly execute commands on other systems, making it harder to detect malicious activity.</p> <p>This could be achieved through scheduled tasks, modification of registers or PowerShell remoting techniques.</p>
Command and Control	Modify Authentication Process: Domain Controller Communication (T1556.001)	<p>Threat actor uses compromised domain controller as a C2 server to communicate with malware to control and monitor the attack.</p> <p>Once this is accomplished, it more difficult to track and disrupt the attacker's activities, potentially enabling attackers to find more critical information about Gamma's operations to sell, encrypt or expose.</p>
Impact	Data Manipulation (T1565)	<p>Threat actor steals, modifies and disrupt business operations and availability by compromising admin accounts.</p> <p>This could have a significant impact on Gamma's financial and reputational consequences such as</p>

regulatory fines, ransomware payment, exposure of customer PII information.

MITRE DEF3ND Analysis:

Security Protections	ATT&CK Mitigation	Explanation & Relevance
Network Security	Network Segmentation (M1030), Filter Network Traffic (M1037), Limit Access to Resource Over Network (M1036)	<p>Segment and restrict network access to domain controllers.</p> <p>This can be done by monitoring and filtering network traffic for suspicious activity, such as unexpected NTLM authentication request.</p> <p>Implement Network Access Control (NAC) to restrict access to sensitive digital resources</p>
Endpoint Security	Behaviour Prevention on Endpoint (M1040), Antivirus / Anti-Malware (M1049), Disable or Remove Feature or Program (M1042)	<p>Implement endpoint detection and response (EDR) solutions to detect and respond to malicious activity on user devices.</p> <p>Use antivirus and anti-malware software with up to date signatures</p> <p>Harden endpoints by disabling unnecessary services and applications</p>
Identity and Access Management	Multi-factor Authentication (M1032), Privilege Account Management (M1026), User Prevention on Endpoint (M1040)	<p>Implement Strick password policies and enforce multi-factor authentication (MFA) for all user accounts.</p> <p>Implement Privilege access management (PAM) to control access to sensitive accounts and resources.</p> <p>Monitor user activity for suspicious behaviour</p>
Vulnerability Management	Vulnerability Scanning (M1016)	<p>Apply security patches promptly. Regular scan systems for vulnerabilities and prioritise remediation using the vulnerability management lifecycle.</p> <p>Use a vulnerability management program to tract and manage vulnerabilities</p>
Security Operations	User Training (M1017)	<p>Implement a security operations centre (SOC) to monitor and analyse logs for suspicious activity.</p> <p>Have a well-defined incident response (IR) plan in place to respond to security incidents effectively.</p> <p>Conduct regular security awareness training for employees.</p>

CVE-2022-23943 – External: Critical

While CVE-2022-23943 in Apache's mod_sed module presents a potentially worrisome RCE vulnerability, its exploitation path is intricate and requires crafting specific malicious HTTP requests. This increases the attacker's skill threshold and reduces the likelihood of immediate widespread exploitation. However, the potential impact in Gamma's online banking environment is severe, considering possible data exfiltration of customer finances and other sensitive information. Therefore, proactive defense measures are crucial. Gamma should prioritise patching vulnerable servers, implementing WAFs with appropriate rules, and maintaining robust endpoint security to detect and block malicious activity. Continuous vulnerability management and SOC monitoring will further strengthen their defenses against this and other potential threats. By layering these controls and actively monitoring their efficacy, Gamma can significantly mitigate the risk of successful exploitation and minimise potential losses. (MITRE, 2022a)

ATT&CK Tactics	ATT&CK Techniques	Explanation & Relevance
Initial Access	External Remote Services (T1133)	Threat actor exploits vulnerability in “mod_sed” Apache module by crafting HTTP requests that trigger out-of-bounds write errors. In turn, crashing the Apache server process and allow the attacker to overwrite server-side memory with arbitrary code.
Execution	Command and Scripting Interpreter (T1059)	Once RCE is achieved, threat actor compromises the internal server to run arbitrary commands or scripts on the system. Potentially downloading and executing malware to modify system files or establish connections to other systems on the network
Privilege Escalation	Local Privilege Escalation (T1068)	Threat actor is able to escalate their privileges to root or admin user role in the system by altering the permissions assigned to the Apache process. Granting the attacker wider access to system resources and controls for further attack actions
Lateral Movement	Exploitation of Remote Services (T1210)	Attacker moves laterally within the network by exploiting vulnerabilities in other systems, leveraging compromised accounts, or using legitimate tools such as remote desktop and network protocols, enabling the attacker to expand their foothold and access Gamma’s sensitive digital assets.
Impact	Data Exfiltration (T1565)	Threat actor exfiltrates valuable data from network systems and servers. Potentially including customer data, financial information or other sensitive assets stored on the vulnerable systems.

MITRE DEF3ND Analysis:

Security Protection	ATT&CK Mitigation	Explanation & Relevance
Network Security	Restrict Web-based Content (M1021)	<p>Implement web application firewalls (WAFs) with appropriate rules to detect and block suspicious HTTP requests targeting the mod_sed module.</p> <p>Monitor network traffic for anomalies and suspicious activity around web servers, such as unexpected connections or data exfiltration attempts.</p>
Web Application Security	SSL/TLS Inspection (M1021)	<p>Update Apache HTTP Server to the latest version that addresses.</p> <p>Implement least privilege principle for web application accounts and services.</p> <p>Regularly scan web applications for vulnerabilities and prioritise remediation efforts.</p>
Endpoint Security	Behaviour Prevention on Endpoint (M1040)	<p>Deploy endpoint detection and response (EDR) solutions to monitor endpoints for suspicious activities like unauthorised execution of binaries or attempts to establish outbound connections to malicious domains.</p> <p>Utilise anti-malware software with up-to-date signatures to detect and block malicious code execution.</p>
Security Operations	User Training (M1017)	<p>Implement a security operations centre (SOC) to monitor and analyse logs for suspicious activity.</p> <p>Have a well-defined incident response (IR) plan in place to respond to security incidents effectively.</p> <p>Conduct regular security awareness training for employees.</p>

External: Medium - CVE-2021-23841

While CVE-2021-23841's potential exploitability requires malicious X.509 certificates and vulnerable applications, its ability to trigger application crashes and potentially lead to privilege escalation poses a significant threat to Gamma's online bank. Attackers could leverage this vulnerability to gain initial access, escalate privileges, move laterally within the network, and ultimately steal sensitive customer data or disrupt financial operations. Gamma should prioritise patching vulnerable applications, implementing rigorous vulnerability management practices, and deploying EDR solutions to detect and respond to potential attacks. The likelihood of exploitation is moderate due to the need for specific conditions, but the potential impact score is high due to the sensitive nature of Gamma's data and operations (NIST, 2022).

MITRE ATT&CK Analysis:

AT&CK Tactics	ATT&CK Technique	Explanation & Relevance
---------------	------------------	-------------------------

Discovery	Discovery of Unidentified Assets	Threat actor crafts custom X.509 certifications with malicious issuer strings to trigger the NULL pointer dereference in X509_issuer_and_serial_hash() function. This could reveal hidden assets or network components due to unexpected crashes from processing the certificates.
Resource Development	Remote Services	Threat actor hosts malicious servers containing custom certificates that trigger the vulnerability.
Lateral Movement	Internal Service Discovery	The malfunctioning application due to the vulnerability might expose internal network information during error logs or crash analysis, aiding the threat actor in identifying systems for lateral movement.
Impact	Execution	Threat actor successfully exploits network systems to execute arbitrary code within the vulnerable application, enabling the attacker to install malware, steal data or disrupt Gamma's operations.

MITRE DEF3ND Analysis:

Security Protections	ATT&CK Mitigations	Explanation & Relevance
System Security	Code Signing (M1045)	Verifying code signing on applications and libraries used can ensure legitimacy and prevent loading malicious code triggered by the vulnerability.
Network Security	Network Segmentation (M1030), Limit Access to resource over network (M1035)	Limiting access to internal network resources and segmenting critical systems can restrict the attacker's reach and prevent lateral movement even if initial exploitation occurs.
Memory Safety Protections	Privileged Process Integrity (M1025), Limit Software Installation (M1033)	Utilising tools like address space layout randomisation (ASLR) and data execution prevention (DEP) can hinder exploitability by making it harder for attackers to gain control of the application's execution flow.
Vulnerability Management	Vulnerability Scanning (M1016)	Apply security patches promptly. Regular scan systems for vulnerabilities and prioritise remediation using the vulnerability management lifecycle. Use a vulnerability management program to track and manage vulnerabilities

Part 1.2 – Vulnerability Management Tool Recommendation

This section outlines how Gamma can leverage Qualys Vulnerability Management Detection & Response (VMDR) tool to effectively to efficiently classify, prioritise, manage, and remediate vulnerabilities across their internal and external-facing digital assets (Qualys, 2023). By implementing the vulnerability management lifecycle within Qualys, Gamma can strengthen their security posture and minimise exposure to cyberattacks (Kosinski, 2023).

Vulnerability Management Lifecycle with Qualys:

1. **Discover:**
 - Utilise Qualys Cloud Agents for automatic asset discovery and inventory on all endpoints, servers, and network devices (Qualys, 2021).
 - Schedule regular scans with Qualys Vulnerability Scanner to identify vulnerabilities in operating systems, applications, and network infrastructure (appendix A).
 - Integrate with existing Configuration Management Database (CMDB) tools such as Device42 to enrich asset data and ensure accuracy.
2. **Prioritise:**
 - Leverage Qualys TruRisk™ engine to assess vulnerabilities based on exploitability, CVSSv3 score, business criticality, and asset context (Qualys, 2022)
 - Utilise custom tags and filters to segment and prioritise vulnerabilities based on specific criteria (e.g., regulatory compliance, attack vectors, affected platforms) (appendix A).
 - Set automated notifications for high-risk vulnerabilities requiring immediate attention (Appendix A).
3. **Assess:**
 - Qualys Patch Management provides detailed information on available patches for identified vulnerabilities (Qualys, 2023a).
 - Utilise Qualys Threat Feed and integrated threat intelligence to understand exploitability risk based on real-time attack data (Appendix A).
 - Conduct additional manual vulnerability assessments for complex or critical vulnerabilities.
4. **Report:**
 - Generate pre-configured or custom reports to track vulnerability trends, remediation process, and overall security posture (Appendix A).
 - Schedule automated reports for key stakeholders with actionable insights and remediation recommendations
 - Integrate reporting with SIEM for broader security incident context.
5. **Remediate:**
 - Deploy patches directly from Qualys Patch Management to vulnerable systems using Qualys Cloud Agents (Qualys, 2021).
 - Leverage remediation workflows to automate patch prioritisation, approval, and deployment based on pre-defined policies (Appendix A).
 - Implement rollback capabilities to mitigate potential issues arising from patch deployment.
6. **Verify:**
 - Monitor patch deployment success through Qualys Vulnerability Scanner follow-up scans (Appendix A).

- Utilise Qualys Compliance Engine to demonstrate patching compliance with internal and external regulations (Qualys, 2019).
- Implement continuous monitoring with Qualys Continuous Monitoring to detect newly discovered vulnerabilities or system changes that may introduce new risks.

By Implementing Qualys VMDR and adhering to the vulnerability management Lifecycle, Gamma can leverage a robust, automated and risk-based approach to vulnerability management to proactively address incoming threats, strengthen the online bank's security posture, and build ultimately building trust with Gamma's customers.

Part 2.1: Threat Intelligence Summary

Title:	XWorm Malware Threat Intelligence
Intelligence Summary	XWorm is a modular and customisable Remote Access Trojan (RAT) (Pachpor and S., 2023), used to steal sensitive data, deploy ransomware and launch DDoS attacks. First emerging in 2022, it has been actively sold as a malware-as-a-service (MaaS) on underground forums (appendix B), making it readily available to less skilled attackers. This makes it a significant threat to financial institutions like Gamma Online Bank. (Electron, kinoshi and glebyao, 2023)
MITRE ATT&CK: Tactics Techniques and Procedurals (TTPs)	<ol style="list-style-type: none"> 1. Initial Access: Phishing (T1556): (.001), Content Injection (T1659) 2. Execution: User Execution: Malicious File (T1204.002), Windows Management Instrumentation (T1047) 3. Persistence: AutoStart Execution: Registry Run Keys - Start-up Folder (T1547.001), Logon Script – Windows (T1037.001), Create or Modify System Process: Windows Service (T1543.003) 4. Command and Control: Bidirectional Communication (T1082) 5. Defence Evasion: Obfuscated Files (T1027), Subvert Trust Controls: Code Signing (T1553.002) 6. Privilege Escalation: Bypass User Account Control (T1548.002), Modify System Process: Windows (T1543.003) 7. Credential Access: Keylogging (T1056.001), OS Credential Dumping (T1003) 8. Discovery: Remote System Discovery (T1018), Network Service Discovery (T1046) 9. Lateral Movement: Remote Desktop Protocol (T1021.001), Remote Service Session Hijacking (T1563) 10. Impact: Data Manipulation (T1565), Data Encrypted for Impact (T1486)
Impact	<p>The XWorm poses a potential threat to Gamma due to its:</p> <ul style="list-style-type: none"> - Targeted data exfiltration: Capabilities to steal login credentials, bank account details, customer PII information and financial data. - Ransomware deployment: Potential to encrypt critical bank systems and demand ransom payments. - DDoS attacks: Ability to disrupt online banking services and cause financial losses.
Mitigations	
Indicators of Compromise (IOCs)	<p>File Hashes:</p> <ul style="list-style-type: none"> - F6BB396FD836F66CD9F33CA4B0262DD7 (trojan.xworm) - 754EA134EE015C95CCFEA4915E4F6B5C (msbuilds.exe) - 250c1b9f4f4b2fe05977ed2dc0bd85ec (Recovery.dll) - 090f6384ef4463a23a331d03e796af6c (Options.dll) <p>IP addresses:</p> <ul style="list-style-type: none"> - 185.15.242.183 - 104.250.125.197 <p>DNS Names:</p> <ul style="list-style-type: none"> - xworm-update[.]xyz - xworm-down[.]xyz
References	Refer to reference section

Threat Intelligence Report – QakBot Malware



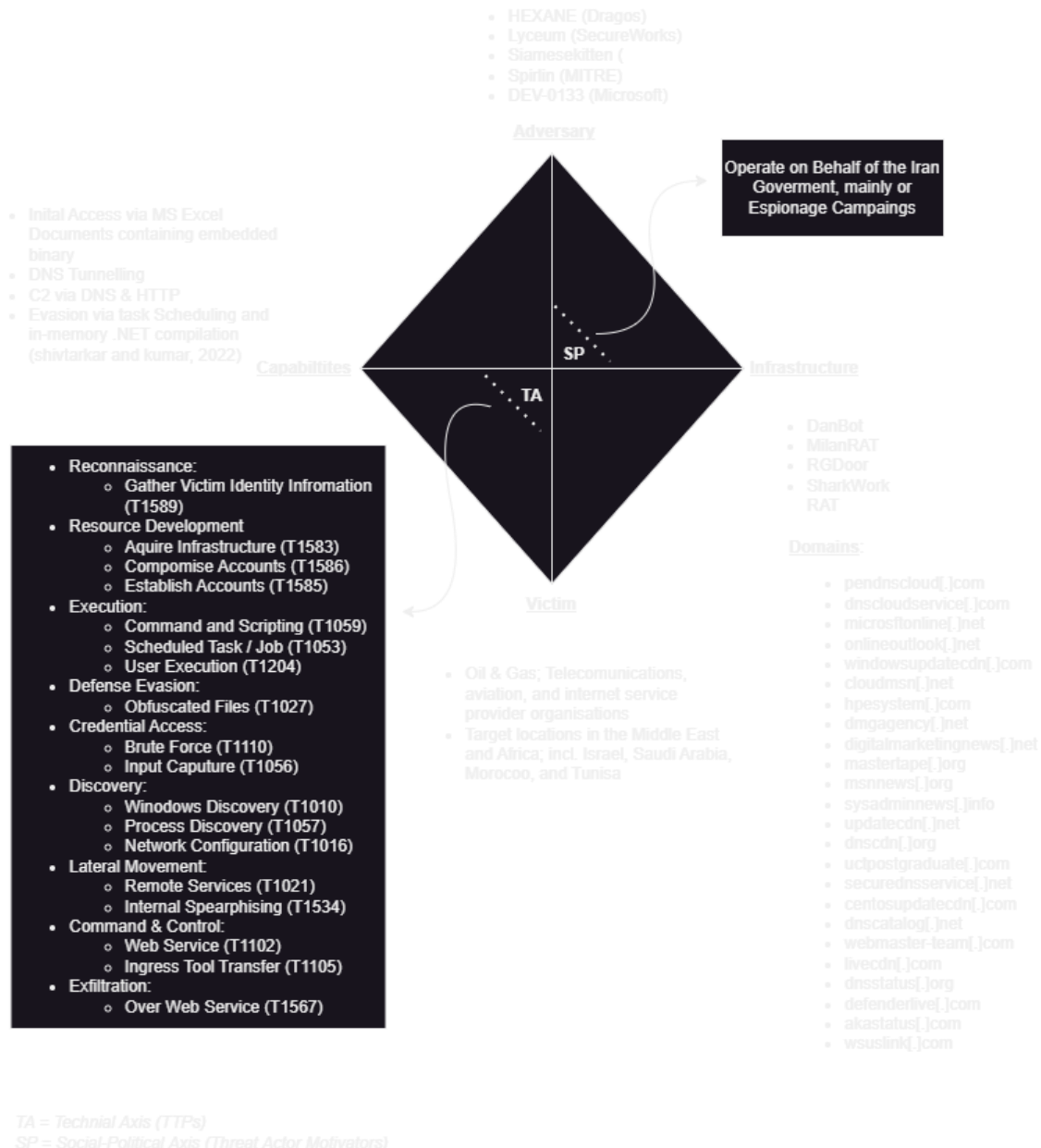
Executive Summary	<p>The QakBot malware, also known as QBot or Pinksliptbot, was first detected in 2007, in association to the GOLD LAGOON threat attack group (Secureworks, 2023). Since its first appearance the QakBot family has evolved from a banking trojan to steal banking credentials into a multi-purpose botnet, contributing to major malware infections worldwide such as; ProLock, Black Basta, REvil (Guibernau, 2023). These cyberattacks are distributed through spam campaigns, using spam or hidden emails (appendix C).</p> <p>Qakbot continues to persist in the current threat landscape as a major threat (MSTI, 2021), enabling cybercriminals to pick and choose the “building blocks” they need for each attack chain (MSTI, 2021). Access to victim devices via compromised credentials (TT121) used by QakBot malware are often sold in underground forums (appendix C), posing a significant risk to Gamma, as if compromised it could expose customer identifiable information, disrupt financial systems and business operations, damage the reputation of the organisation and impose regulatory fines.</p> <p>QakBot poses a significant threat to financial institutions like Gamma, due to the modularity nature of the malware family, it provides threat actors with a range of capabilities including performing reconnaissance, lateral movement, gathering and exfiltrating data to delivering payloads such as ransomware MSTI (2022).</p>
Analyst Comments	<p>Impact Statement: Due to the malware’s modularity nature, a successful Qakbot attack on Gamma could lead to:</p> <ul style="list-style-type: none"> • financial losses: stolen customer PII sensitive information, ransom payments, fraudulent access to funds, potential regulatory fines • Reputational damage: loss in customer trust and confidence, negative media coverage • Operational Disruption: DDoS attacks, data breaches affecting business operations. <p>The QakBot is delivered via one of three email methods: malicious links, malicious attachments, or embedded images (CISA, 2023). These campaigns have in common the use of malicious macros in Excel office documents, once the victim downloads and opens the malicious Excel file, the text in the document attempts to lure them into enabling the macro (appendix C). Once macros are enabled, the attack phase begins. First, it connects to a predefined set of IP addresses to download additional payloads, which is then injected into a legitimate process. The injected process then creates a .dll file to create a scheduled task as a means of persistence. Then QakBot attempts to steal credentials by loading the Vault Credential Library file to enumerate credentials. Finally, it tries to exfiltrate data from affected devices such as emails, files and other sensitive information through C2 server. (Lytzki, 2023)</p> <p>Indicators of Compromise: the FBI has observed the following threat actor tactics, techniques and procedurals (TTPs) in association with QakBot injections:</p> <ul style="list-style-type: none"> • Sets up persistence via the Registry Run Key. It will delete this key when running and recover before the system restarts: “HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<random_string>” • Writes its malicious executable to disk to maintain persistence in the following directory: “C:\Users\<user>\AppData\Roaming\Microsoft\<random_string>\”

	<ul style="list-style-type: none"> • Encrypts registry configuration detailing information about the bot to the following registry key: “HKEY_CURRENT_USER\Software\Microsoft\<random_string>” • See Appendix X for all the affiliated IP addresses associated with QakBot.
Recommendations	<ol style="list-style-type: none"> 1. Deploy a recovery plan: maintain copies of Gamma’s sensitive information in a physically separate, segmented and secure location. (i.e., external servers, the cloud) 2. Strengthen authentication controls: Comply with NIST’s standard when managing password policies. 3. Implement Phishing-resistant Multi-Factor Authentication (MFA): 4. Network Segmentation: prevent spread of ransomware by controlling traffic flows and restrict adversary lateral movement. 5. Implement time-based access for all accounts set at admin level and higher: enforcement of the Zero Trust model and Principle of least privilege. (Process where a network wide policy is set to automatically disable admin accounts when they are not needed using Active Directory)
References	Refer to Reference Section

Part 2.2 - OSNIT Analysis: Alpha

Threat Intelligence Diamond Model was used to analyse and investigate potential attack groups which could disrupt Alpha's operations by identifying the; Adversary, Victim, Infrastructure, and Capabilities, these are listed below:

HEXANE:



References Used:

<https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign>

<https://www.clearskysec.com/siamesekitten/>

<https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/>

<https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor>

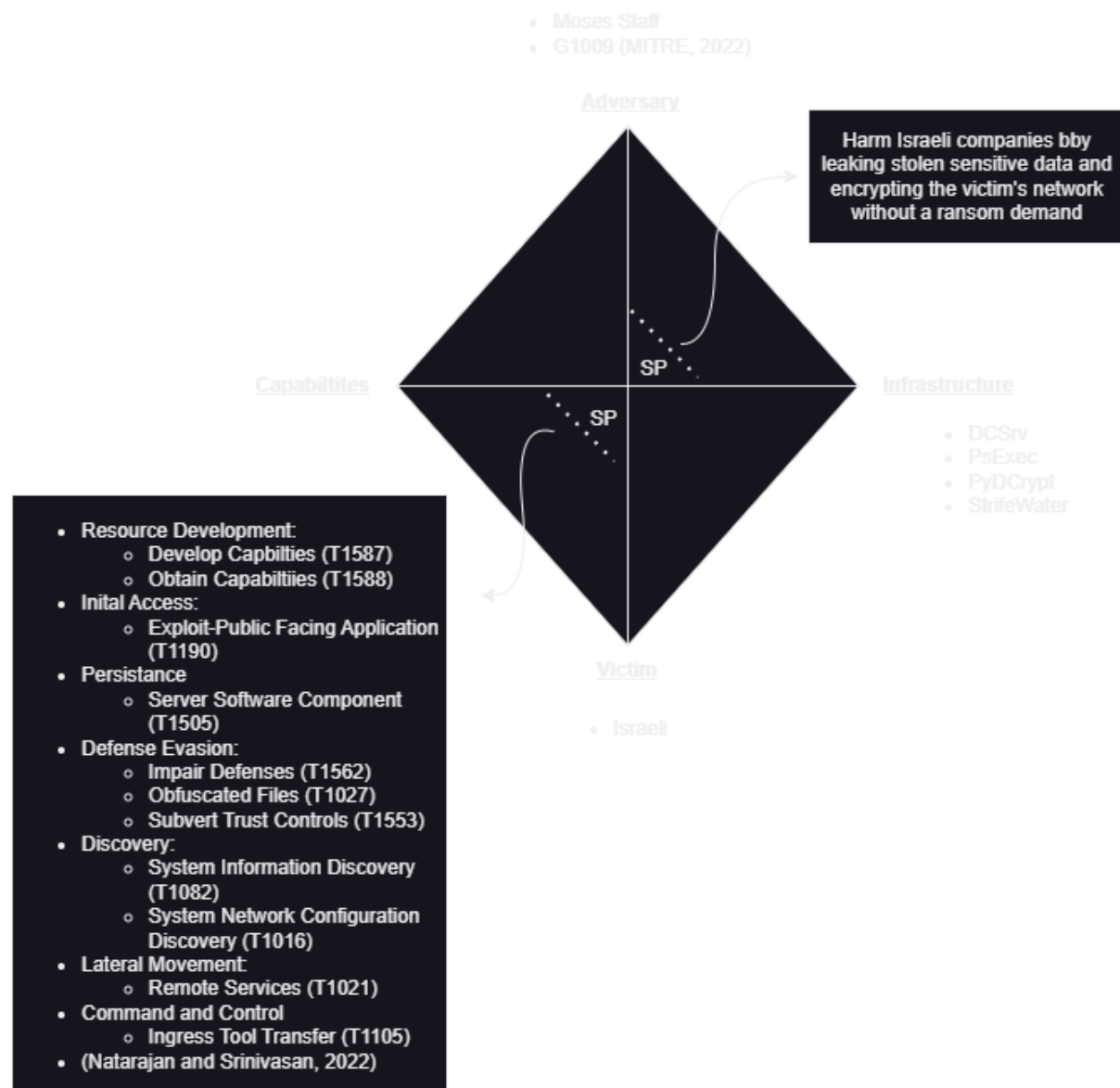
<https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign>

<https://attack.mitre.org/groups/G1001/>

<https://www.clearskysec.com/siamesekitten/>

<https://vblocalhost.com/uploads/VB2021-Kayal-et-al.pdf>

Moses Staff:



TA = Technical Axis (TTPs)

SP = Social-Political Axis (Threat Actor Motivators)

References Used:

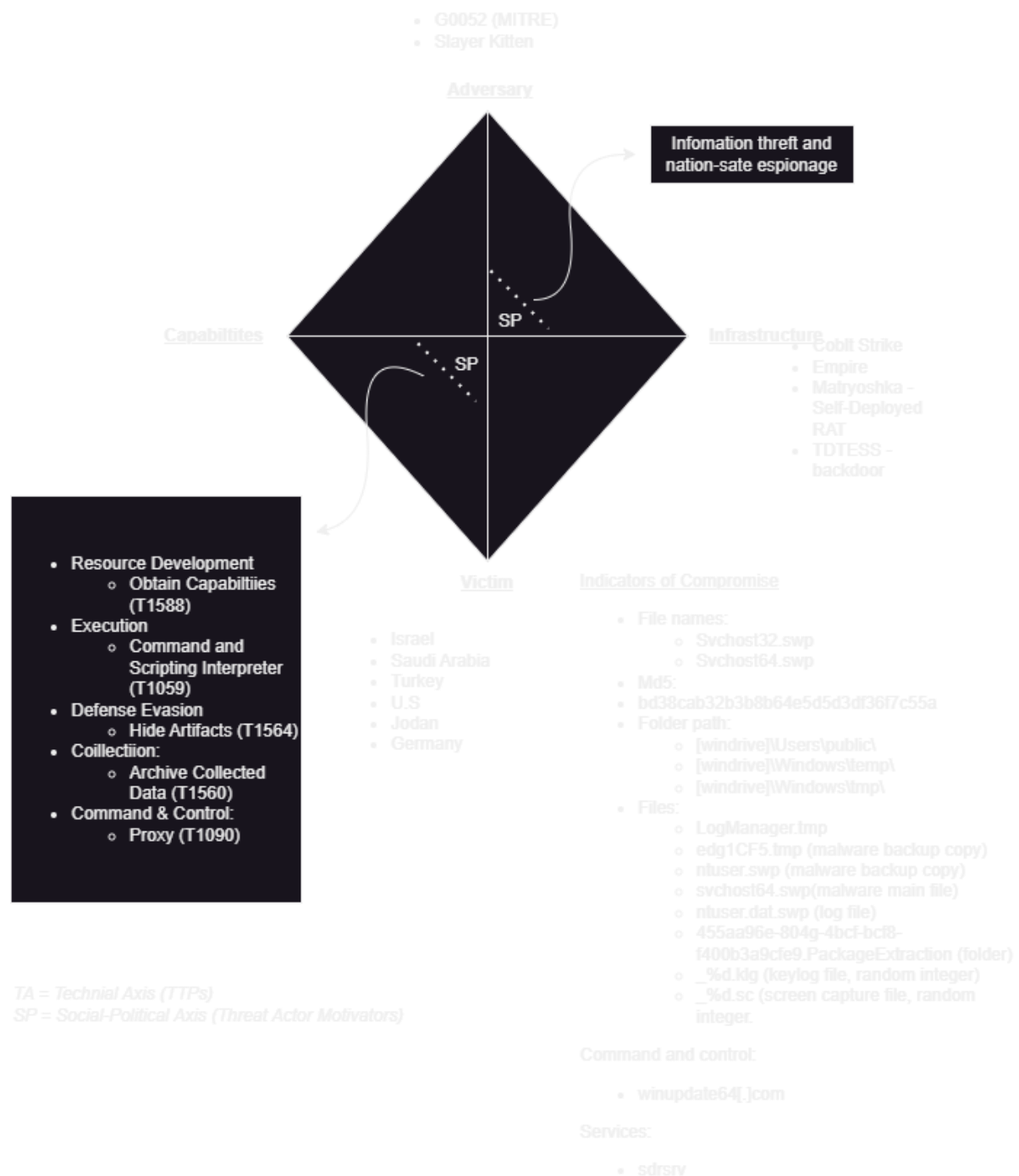
<https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/>

<https://www.cybereason.com/blog/research/striefwater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations>

<https://securelist.com/a-hack-in-hand-is-worth-two-in-the-bush/110794/>

<https://attack.mitre.org/groups/G1009/>

CopyKittens:



References Used:

<https://attack.mitre.org/groups/G0052/>

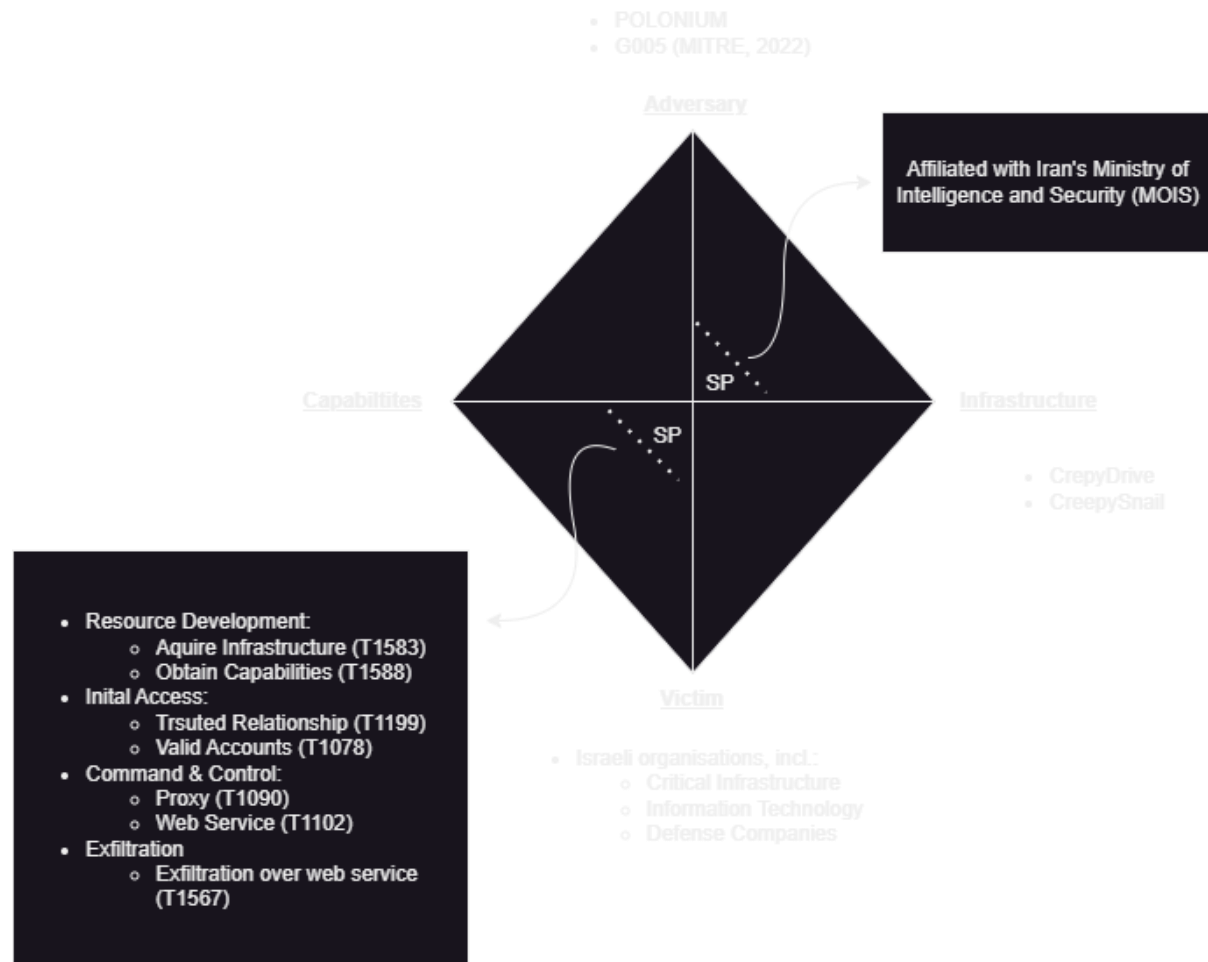
https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf

<https://www.darkreading.com/vulnerabilities-threats/iranian-cyber-espionage-group-copykittens-successful-but-not-skilled>

<https://www.microsoft.com/en-us/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/>

<https://www.clearskysec.com/copykitten-jpost/>

POLONIUM:



TA = Technical Axis (TTPs)

SP = Social-Political Axis (Threat Actor Motivators)

References Used:

<https://attack.mitre.org/groups/G1005/>

<https://www.microsoft.com/en-us/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/>

<https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/>

Appendix A

The figure consists of two screenshots from the Qualys web interface. The left screenshot, titled "Launch Vulnerability Scan", shows the "General Information" section where a scan is named "Scan on FQDNs", the option profile is "Initial Options (default)", and the processing priority is "0 - No Priority". The "Choose Target Hosts from" section shows "Assets" selected, with "FQDN(s)" entered as "www.abc.com, www.xyz.com". The right screenshot, titled "New Scheduled Vulnerability Scan", shows the "Target Hosts" section with the same "FQDN(s)" entered. Both screenshots have red circles highlighting the "FQDN(s)" input fields.

Figure 1 - Qualys Launch Vulnerability Scan

The screenshot shows the "Schedule Vulnerability Scan Creation" interface, specifically "Step 3 of 6: Configure scan settings". A progress bar on the left indicates that "Task details", "Target", and "Settings" are completed, while "Scheduling", "Notification", and "Review And Confirm" are pending. The "Settings" section includes "Scanner Appliance" (set to "External"), "DNS Override" (set to "None"), and "Email notification" (checked). A red circle with the number "1" and a dotted arrow points to the "From Address" dropdown menu, which is currently set to "Qualys Inc <qualys@qualys.com>". Other options in the dropdown include "jdoe@example.com" and "Qualys Inc".

Figure 2 - Qualys Schedule Vulnerability Scan

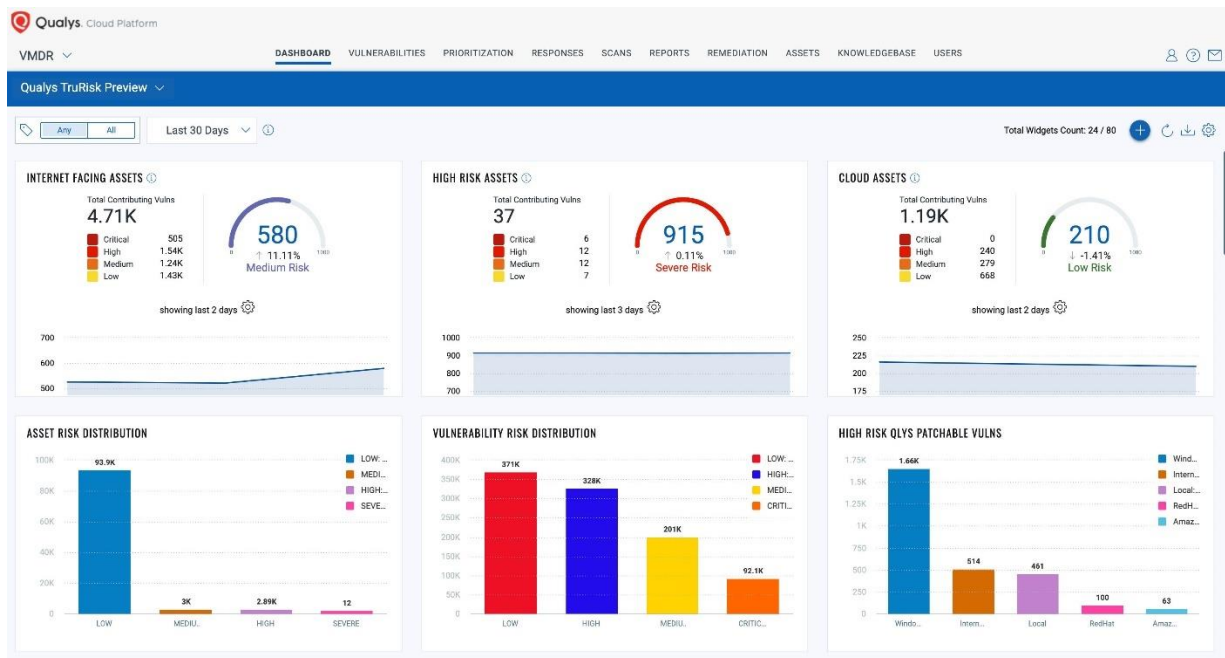


Figure 3 - Qualys VMDR Portal

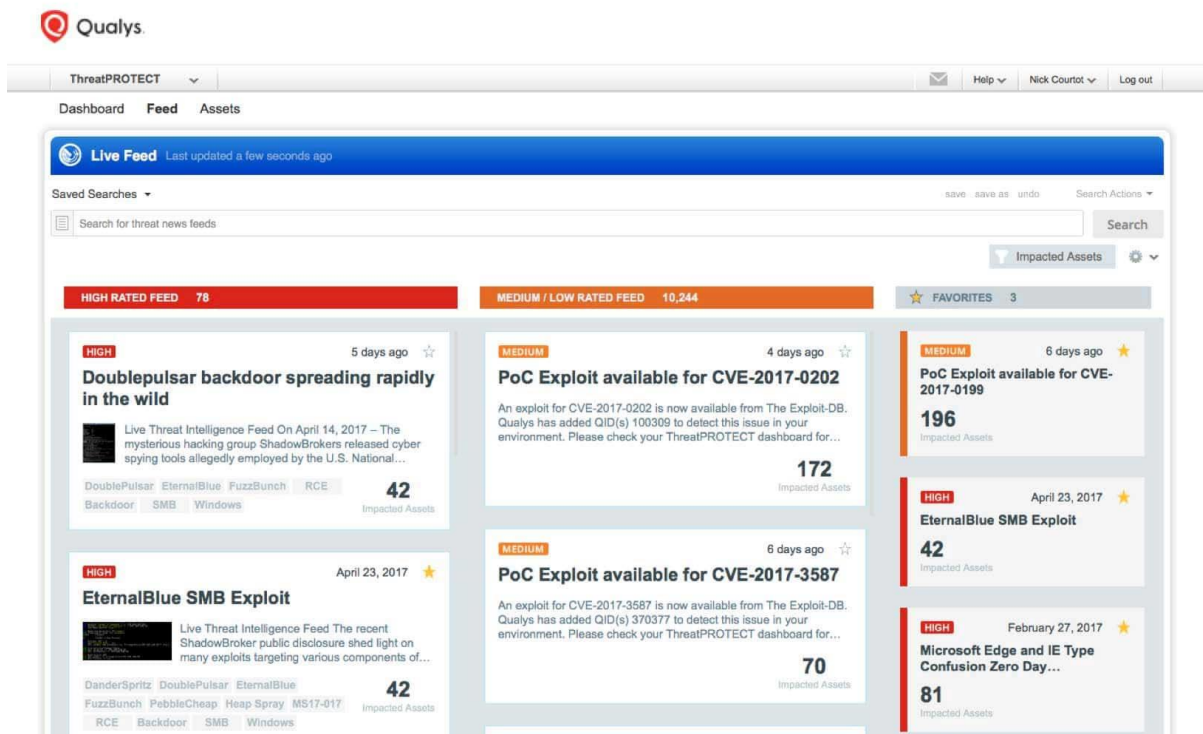


Figure 4 - Qualys Feed

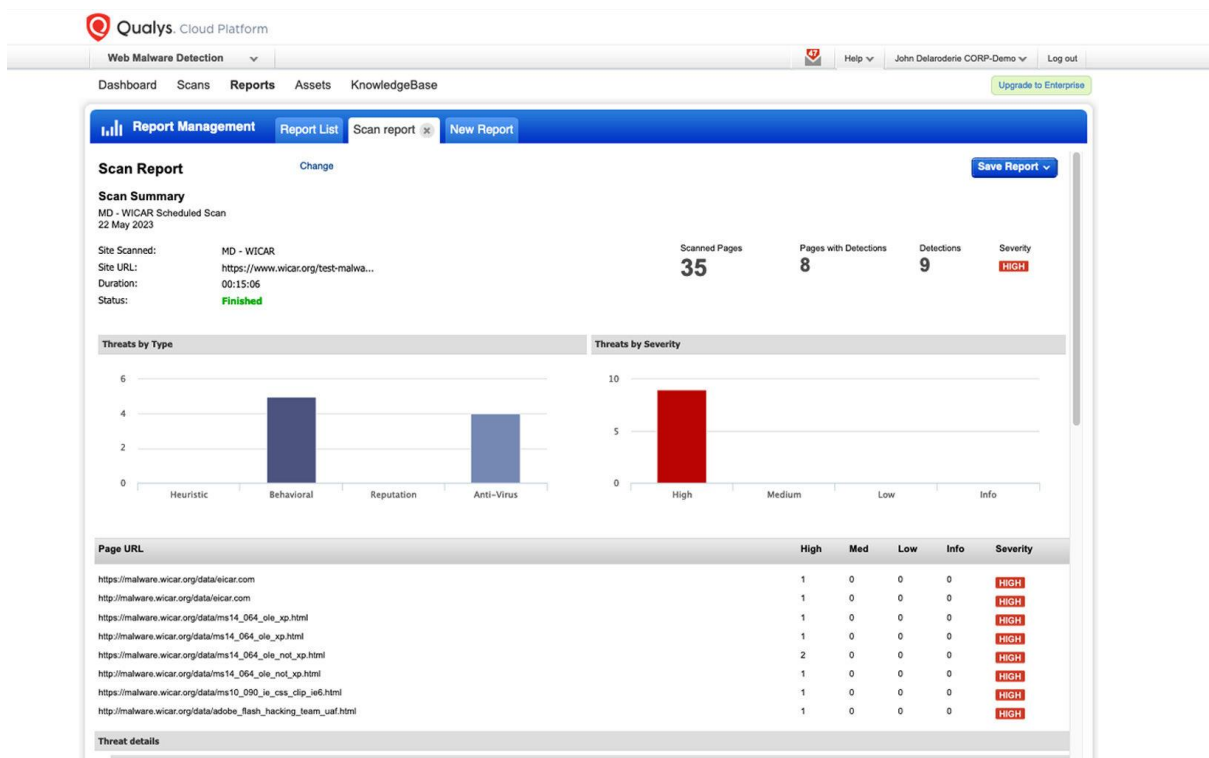


Figure 5 Qualys Report

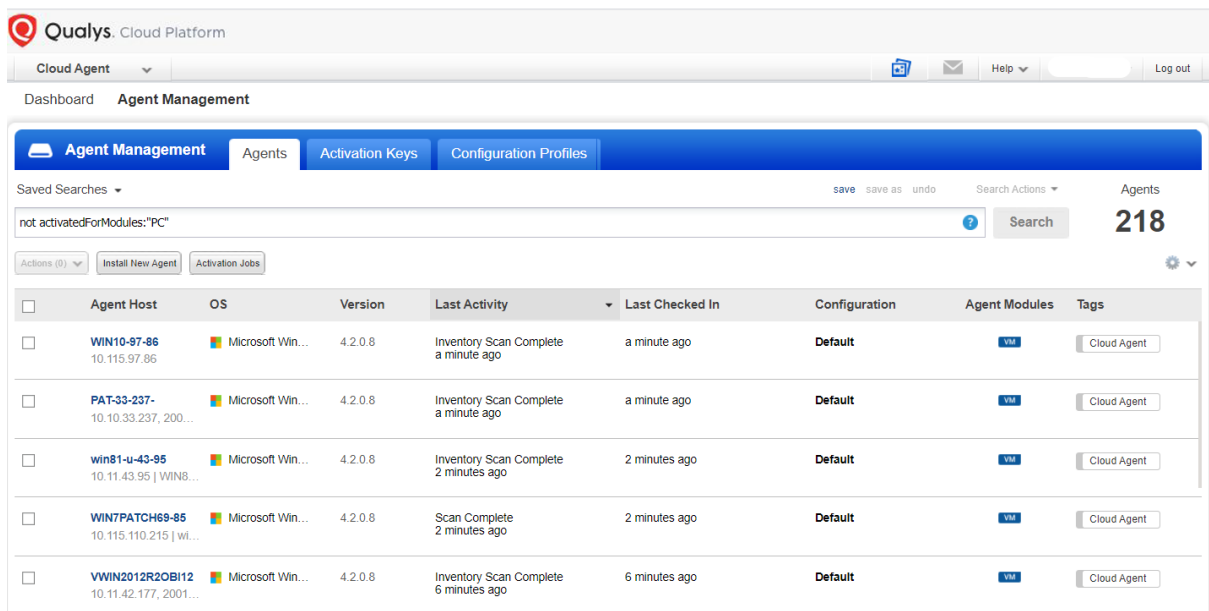


Figure 6 - Qualys Cloud Agent

Policy Editor

Turn help tips: On | OffLaunch Help

Overview

Search this policy

CIS Benchmark for Amazon Linux 2016, v2.0.0 [Scored, Level 1 and Level 2]

Policy Information

Sections23

Technologies1

Controls345

Status:ActiveDeactivate

Locking:Block other usersOFF

Last Evaluated:08/21/2017 at 04:49:16 (GMT-0700)

Created By:Lavish Jhamb (quays_lh8)

Assigned Technologies (1)Edit

Amazon Linux AMIassigned to 345 controls

Asset Groups (0)Tags (0)Edit | Hide

You have no assets assigned to this policy yet.

Cover page

This CIS certified policy for 'Amazon Linux 2016' is based on the 'CIS Amazon Linux Benchmark, v2.0.0'. The policy contains '...

Read all

Sections

Add SectionReorder

Section	Title	Controls
1	Filesystem Configuration Add Controls Copy Controls Remove Edit	34
2	Configure Software Updates Add Controls Copy Controls Remove Edit	2
3	Filesystem Integrity Checking Add Controls Copy Controls Remove Edit	3
4	Secure Boot Settings Add Controls Copy Controls Remove Edit	4
5	Additional Process Hardening Add Controls Copy Controls Remove Edit	6


Cancel

☐ Evaluate now

Save As...Save

Figure 7 - Qualys Policy Compliance

Appendix B




Entrepreneur
 Providing customer services since August 2020


Products Sold
 105

Product Quality
 5 (22 reviews)


[Products](#)
[Contact](#)
[Feedback](#)
[Terms](#)
[Trusted Advisor](#)




Hidden Malware Builder v2.0
\$45.00
Stock




Hidden CPLApplet Builder V2.0
\$80.00
Stock



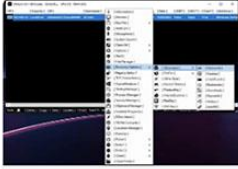
UAC Bypass Builder V2.0
\$50.00
Stock




XBinder V2.0
\$80.00
Stock



H-Malware Builder V5 Lifetime
\$50.00
Stock




XWorm V3.1 Lifetime
\$300.00
Stock




XWorm V4.0 Lifetime
\$400.00
Stock

Figure 8 - XWorm hosted for Sale

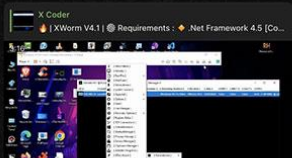

XCodeGroup
 8 945 members

Pinned Message
 XWorm V4.1 | Requirements...


[JOIN GROUP](#)



XWorm V4.1 Ransomware
 8 5 1
 10:52 AM



XWorm V4.1 HVNC
 10 2
 10:57 PM



XWorm V4.1 HRDP
 18 1
 10:58 PM

Figure 9 - Telegram group to provide updates on Worm tools

Appendix C

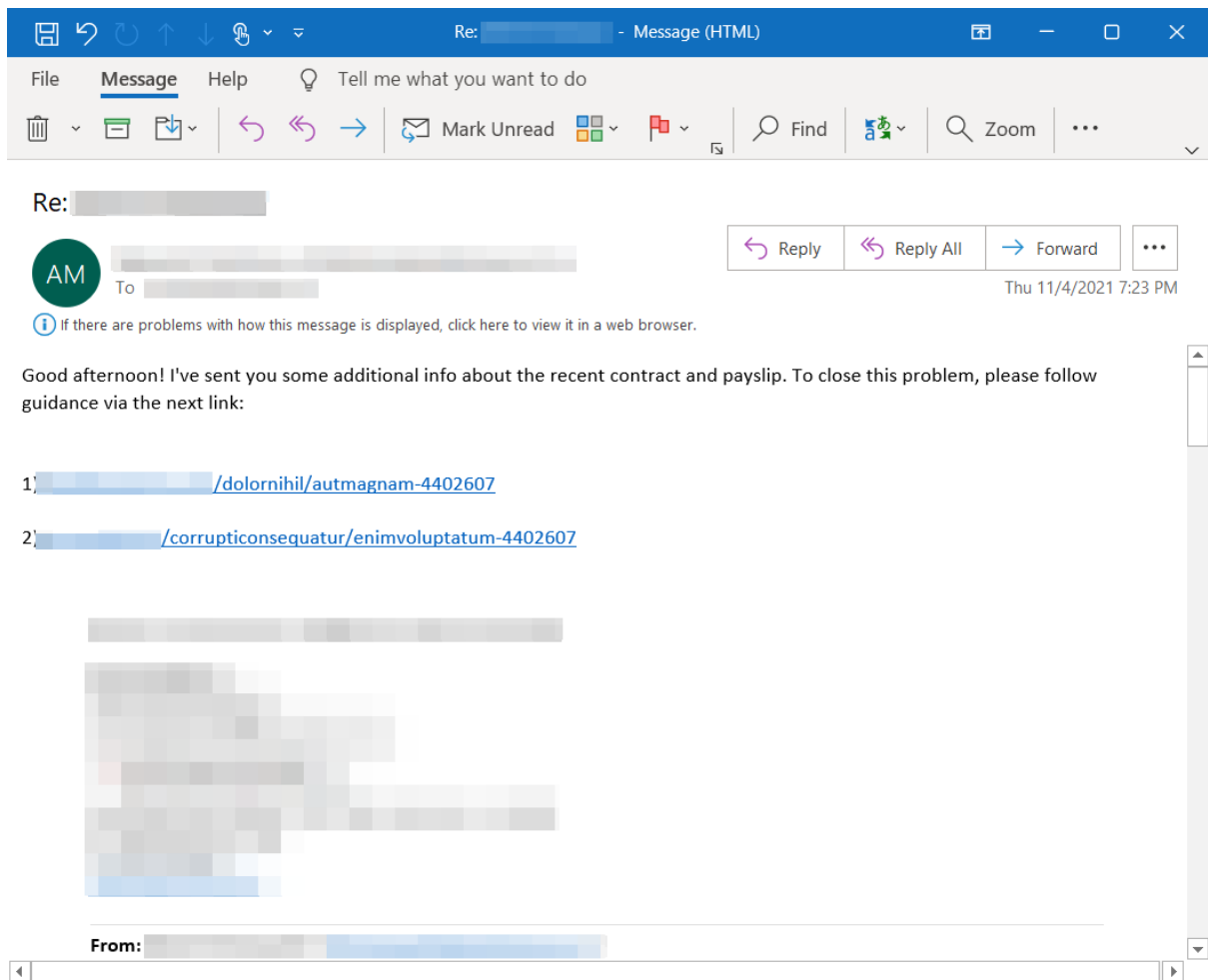


Figure 10 - Sampel Qakbot campaign

References:

- Caltagirone, S., Pendergast, A. and Betz, C. (2013). *The Diamond Model of Intrusion Analysis*. [online] Available at: <https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>.
- CISA (2023). *Identification and Disruption of QakBot Infrastructure / CISA*. [online] www.cisa.gov. Available at: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-242a>.
- Electron, kinoshi and glebyao (2023). *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/>.
- Gi7w0rm (2023). *Uncovering DDGroup — A long-time threat actor*. [online] Medium. Available at: <https://gi7w0rm.medium.com/uncovering-ddgroup-a-long-time-threat-actor-d3b3020625a4> [Accessed 17 Jan. 2024].
- Gudzis, M. (2018). *HEXANE, Lyceum, Siamesekitten, Spirlin, Group G1001 / MITRE ATT&CK®*. [online] attack.mitre.org. Available at: <https://attack.mitre.org/groups/G1001/>.
- Guibernau, F. (2023). *Emulating the Evolving Cybercrime Malware QakBot*. [online] AttackIQ. Available at: <https://www.attackiq.com/2023/01/25/emulating-qakbot/> [Accessed 18 Jan. 2024].
- INCIBE (2022). *Log4Shell: analysis of vulnerabilities in Log4j / INCIBE-CERT / INCIBE*. [online] www.incibe.es. Available at: <https://www.incibe.es/en/incibe-cert/blog/log4shell-analysis-vulnerabilities-log4j> [Accessed 18 Dec. 2023].
- Kayal, A., Lechtik, M. and Rascagneres, P. (2021). *Lyceum Reborn: Counterintelligence in the Middle East*. [online] Available at: <https://vblocalhost.com/uploads/VB2021-Kayal-et al.pdf>.
- Kosinski, M. (2023). *What Is the Vulnerability Management lifecycle?* [online] IBM Blog. Available at: <https://www.ibm.com/blog/vulnerability-management-lifecycle/>.

Lytzki, I. (2023). *XWorm Malware: Exploring C&C Communication*. [online] ANY.RUN's Cybersecurity Blog. Available at: <https://any.run/cybersecurity-blog/xworm-malware-communication-analysis/> [Accessed 19 Jan. 2024].

Millington, E. and Danilevich, I. (2021). *QakBot, Software S0650 / MITRE ATT&CK®*. [online] attack.mitre.org. Available at: <https://attack.mitre.org/versions/v13/software/S0650/> [Accessed 18 Jan. 2024].

MITRE (2022a). *CVE - CVE-2022-23943*. [online] cve.mitre.org. Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23943> [Accessed 19 Jan. 2024].

MITRE (2022b). *POLONIUM, Group G1005 / MITRE ATT&CK®*. [online] attack.mitre.org. Available at: <https://attack.mitre.org/groups/G1005/>.

MSTI (2021). *A Closer Look at Qakbot's Latest Building Blocks (and How to Knock Them down)*. [online] Microsoft Security Blog. Available at: <https://www.microsoft.com/en-us/security/blog/2021/12/09/a-closer-look-at-qakbots-latest-building-blocks-and-how-to-knock-them-down/>.

MSTI (2022). *Ransomware as a service: Understanding the Cybercrime Gig Economy and How to Protect Yourself*. [online] Microsoft Security Blog. Available at: <https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>.

Natarajan, P. and Srinivasan, M. (2022). *Moses Staff, Group G1009 / MITRE ATT&CK®*. [online] attack.mitre.org. Available at: <https://attack.mitre.org/groups/G1009/>.

NIST (2019). *NIST Special Publication 800-63B*. [online] Nist.gov. Available at: <https://pages.nist.gov/800-63-3/sp800-63b.html>.

NIST (2022). *NVD - CVE-2021-23841*. [online] nvd.nist.gov. Available at: <https://nvd.nist.gov/vuln/detail/CVE-2021-23841> [Accessed 19 Jan. 2024].

Pachpor, P. and S., A. (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/>.

Qualys (2019). *Qualys Policy Compliance: IT Policy Compliance App* / Qualys. [online] [www.qualys.com](https://www.qualys.com/apps/policy-compliance/). Available at: <https://www.qualys.com/apps/policy-compliance/>.

Qualys (2021). *Why You Need Cloud Agent*. [online] Available at: <https://www.qualys.com/docs/qualys-cloud-agent-datasheet.pdf> [Accessed 19 Jan. 2024].

Qualys (2022). *Qualys VMDR TruRisk, VMDR TruRisk FixIT, and VMDR TruRisk ProtectIT* / Qualys. [online] www.qualys.com. Available at: <https://www.qualys.com/apps/vulnerability-management-detection-response/trurisk/>.

Qualys (2023a). *Qualys Patch Management: Automated Patch Solution* / Qualys, Inc. [online] www.qualys.com. Available at: <https://www.qualys.com/apps/patch-management/>.

Qualys (2023b). *Qualys VMDR - Vulnerability Management Tool* / Qualys. [online] www.qualys.com. Available at: <https://www.qualys.com/apps/vulnerability-management-detection-response/#:~:text=A%20single%20solution%20for%20cybersecurity>.

Secureworks (2023). *Qakbot Campaign Delivered Black Basta Ransomware*. [online] www.secureworks.com. Available at: <https://www.secureworks.com/blog/qakbot-campaign-delivered-black-basta-ransomware>.

shivtarkar, N. and kumar, A. (2022). *Lyceum .NET DNS Backdoor*. [online] www.zscaler.com. Available at: <https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor> [Accessed 19 Jan. 2024].

Stuart H. (2019). *Zero Trust Architecture Design Principles*. [online] www.ncsc.gov.uk. Available at: <https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles>.

Tenable (2022). *Microsoft's May 2022 Patch Tuesday Addresses 73 CVEs (CVE-2022-26925)*. [online] Tenable®. Available at: <https://www.tenable.com/blog/microsofts-may-2022-patch-tuesday-addresses-73-cves-cve-2022-26925>.