Malware Project Final Topic

Team 2

Anna Melkumyan Canosa
Andrea Victoria Piñón Rattia
Cecília Maria Rodrigues Correia
Oriol Ramos Puig

November 4th, 2025

Malware
Master's degree in Cybersecurity

Mix of **VeilVault** and **WikiWorm**

1. STORY

Alice, a fired developer from a legal-tech firm, turns intimate knowledge of the company's workflows into revenge and profit. The firm relies on Microsoft Excel 365 for contracts and budgets (shared on network drives) and an internal XWiki for documenting code and triggering CI/CD pipelines to GitLab.

Act I - Phishing:

She crafts an urgent Excel attachment and sends it to the finance mailbox. A busy, trusting employee opens the file. That single click triggers a vulnerability in Excel **(CVE-2025-47957)** and gives Alice a covert foothold inside the company network.

Act II - Initial point of access:

From that foothold she moves quietly. She probes permissions and reads the documentation platform developers trust: an internal XWiki used to document code and trigger CI/CD pipelines to GitLab. Using a vulnerability in the wiki **(CVE-2025-24893)**, Alice inserts small, harmless changes: code-like fragments and automated links disguised as legitimate templates. No one notices them, as they appear to be ordinary reference pages used by developers. However, these subtle modifications become the hidden mechanism that allows the attack to spread throughout the company's systems.

Act III - Worm:

Over the days, the modified wiki acts as a propagation engine. Webhooks and automated integrations treat the altered pages as normal inputs and carry slightly mutated versions of Alice's payload into repositories and CI pipelines. Normal developer workflows unknowingly multiply the infection.

Act IV - Encryption:

With privileges extended by the spreading payload, Alice reaches the shared legal drives that hold contracts, case files and budgets. She deploys an encryptor that locks those documents with a strong cipher, so that filenames change and access to those documents becomes impossible. Also, she takes out the documents into her own server.

Act V - Rescue:

At this point, Alice demands payment in Monero, a crypto currency. If the company does not pay for the rescue, Alice threatens to publish the confidential files on Twitter. To demonstrate her seriousness, she provides a limited but verifiable proof: a single non-critical document restored to show she controls decryption, along with a metadata only someone with internal access could obtain.

2. POSSIBLE APPROACH

Phase 1: Initial Access via Excel
- Alice emails: “Q4_Legal_Budget.xlsm – URGENT APPROVAL NEEDED” to the finance team of the company.
- File contains VBA macro that runs when opened
- Exploit: CVE-2025-47957 (Microsoft Excel use-after-free RCE)
- Exploit-DB: 52337
- Action: Downloads PowerShell dropper from attacker server

Phase 2: Pivot to Internal XWiki
- PowerShell scans network using Get-NetTCPConnection and finds XWiki at 192.168.10.50
- Exploits CVE-2025-24893 (XWiki 15.10.10 unauthenticated RCE via Solr)
- Exploit-DB: 52136
- Action: Alice exploits the vulnerability to upload a Groovy-based webshell disguised as a legitimate extension: DocumentTemplateHelper.groovy, gaining control

Phase 3: Worm Propagation via Webhooks
- Modifies wiki pages (API references templates, CI/CD doc, etc) to include malicious Groovy macros
- Wiki is linked to GitLab via webhooks. Each webhook execution carries a slightly mutated payload to evade signature-based detection (polymorphic)
- Every time a developer views a page, webhook triggers, the malicious commit is pushed to the repo, CI pipeline executes compromised code

Phase 4: Lateral Movement & Encryption
- From the compromised XWiki instance, SMB access is used to reach *fileserver**legal*\
- Deploy of a Go binary named *shadowvault.exe*, designed to operate quickly and quietly
- Encrypts *.docx, .pdf and .xlsx* and renames them with a *.locked* extension using ChaCha20-Poly1305. Filenames are obfuscated, and access becomes impossible without the decryption key.
- In the affected directory, *shadowvault.exe* leaves behind a file named *#RANSOM.txt* which contains explicit instructions: a Monero wallet address and an QR code for payment, along with a warning about the consequences of non-compliance.

Phase 5: Command & Control + Ransom
- Exfiltrates the list of encrypted files via DNS TXT records queries (a technique that bypasses most firewall rules and blends into normal network traffic) into her own server.
- So, when an employer tries to access to *fileserver**legal*\, the .txt is found with the following text:
“YOUR FILES ARE LOCKED. Send 30 XMR (like 9.1k€) to: [QR CODE]. Proof of access: [metadata snippet]”
- Payment confirmation is automated through a Telegram bot. Once the ransom is received and verified on the Monero blockchain, the bot sends the decryption key along with instructions.

3. EXPLOITS

- CVE-2025-47957 (Microsoft Excel LTSC 2024 use-after-free RCE). Executes shellcode via crafted formulas and works on unpatched Office 365. Exploit-DB: 52337.
- CVE-2025-24893 (XWiki Platform 15.10.10 unauthenticated RCE via Solr endpoint). Executes Groovy scripts as guest. Exploit-DB: 52136.