Lotus Blossom

Status	Done
CVE	CVE-2012-0158 / CVE-2014-6332 / CVE-2010-2883
Date	@March 6, 2025
# Number	39
Tags	APT group, Attack Technique, CVE, Cyber actors, Malware

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/unit42-operation-lotus-blossom

https://securelist.com/the-spring-dragon-apt/70726/

https://blog.talosintelligence.com/lotus-blossom-espionage-group/

Table of contents

- **Recent activities**
- **Mitre ATT&CK Mapping**
- **General mitigation possibilities**

Executive summary

- **Lotus Blossom** is a very well-known (meaning there is a lot of research papers about it) active **espionage group** operating since at least 2012 maybe even 2009 and continues to operate today, they gathering intelligence and sensitive information from regional adversaries.
- Several name can be associated to them like : DRAGONFISH, Spring Dragon, RADIUM, Raspberry Typhoon, Billbug or Thrip.
- Their origins is unclear but they may believed to be linked to Chinese state-sponsored actors, nonetheless it is clear that they are from a country with an interest in the government and military affairs of Southeast Asian nations.
- They target essentially government and military organizations in Southeast Asia but also manufacturing, telecommunications, media and education institutions such as universities.
- They used different type of Trojan or Backdoor like Elise which became Emissary, but also Sagerunex.
- Operation Lotus Blossom is a prime example of how a well-resourced adversary will deploy advanced tools, over an extended time period, sometimes years, in order to reach its goals.

Historical summary

Lotus Blossom is here from some years now, they had the time to evolve and change though the years to become whats we know today. Here is a non-exhaustive list of attacks conduct by them though the time:

Jun 2015	Operation “Lotus Blossom” Unit 42 published new research identifying a persistent cyber espionage campaign targeting government and military organizations in Southeast Asia. The adversary group responsible for the campaign, which Unit42 named “Lotus Blossom,” is well organized and likely state-sponsored, with support from a country that has interests in Southeast Asia. The campaign has been in operation for some time; they have identified over 50 different attacks taking place over the past three years.

	- https://unit42.paloaltonetworks.com/operation-lotus-blossom/
Nov 2015	Attack on French Diplomat Unit42 observed a targeted attack in November directed at an individual working for the French Ministry of Foreign Affairs. The attack involved a spear-phishing email sent to a single French diplomat based in Taipei, Taiwan and contained an invitation to a Science and Technology support group event. - https://unit42.paloaltonetworks.com/attack-on-french-diplomat-linked-to-operation-lotus-blossom/
Early 2017	In the beginning of 2017, Kaspersky Lab became aware of new activities by an APT actor they have been tracking for several years called Spring Dragon (also known as LotusBlossom). Information about the new attacks arrived from a research partner in Taiwan and they decided to review the actor's tools, techniques and activities. Using Kaspersky Lab telemetry data they detected the malware in attacks against some high-profile organizations around the South China Sea. - https://securelist.com/spring-dragon-updated-activity/79067/
Jan 2018	Attacks on Association of South East Asian Nations (ASEAN) countriesDuring the last weeks of January (2018), nation state actors from Lotus Blossom conducted a targeted malware spam campaign against the Association of South East Asian Nations (ASEAN) countries. - https://community.rsa.com/community/products/netwitness/blog/2018/02/13/lotus-blossom-continues-asean-targeting - https://www.accenture.com/t20180127T003755Z_w_/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf
Jan 2018	Back in January 2018, TAA triggered an alert at a large telecoms operator in Southeast Asia. - https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets
Jun 2018	Since Symantec first exposed the Thrip group in 2018, the stealthy China-based espionage group has continued to mount attacks in South East Asia, hitting military organizations, satellite communications operators, and a diverse range of other targets in the region.

	- https://www.symantec.com/blogs/threat-intelligence/thrip-apt-south-east-asia
Mar 2022	Billbug: State-sponsored Actor Targets Cert Authority, Government Agencies in Multiple Asian Countries - https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments-cert-authority

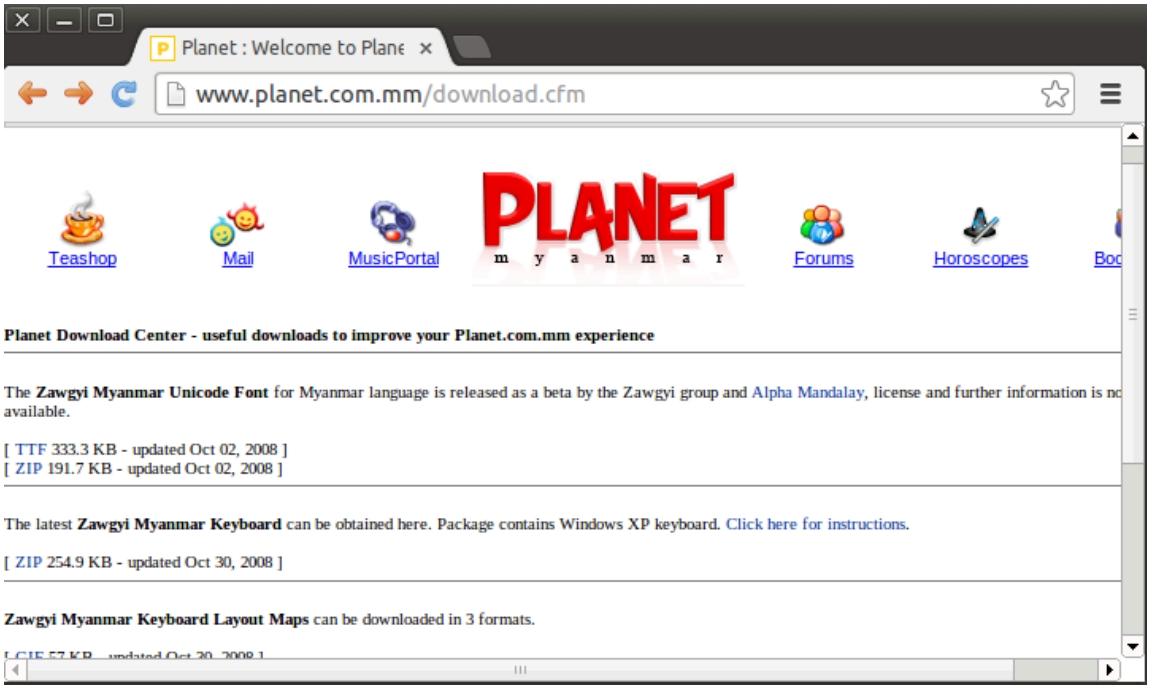
Recent activities

No real information about the recent victim's aside the fact that there is multiple campaigns targeting organizations in sectors such as government, manufacturing, telecommunications and media with the **Sagerunex backdoor**. The victims of the attacks are in the Philippines, Vietnam, Hong Kong and Taiwan.

How do they operate ?

- **Initial access**
  - Back in 2015 Lotus Blossom groups was knows (thanks to the Unit42 research paper) to use **Spearfishing** technique to conduct initial access, often using a malicious office document and decoy file containing content relevant to the target's occupation or interests. The spear phishing attachment typically included exploit code for a well-known Microsoft Office vulnerability, CVE-2012-0158 ("arguably open of the most exploited vulnerabilities of the last decade") which is used to install the Trojan on the system and then display the decoy file, tricking the user into thinking the file opened correctly. Example decoy files include:
    • A spreadsheet listing high-level officers in the Philippine Navy, along with their dates of birth and mobile phone numbers.
    • The operational humanitarian and disaster response (HADR) plan for the Armed Forces of the Philippines, stamped "Secret."
    • An invitation to the screening of a film at the Norwegian embassy.
  - According to a Kaspersky paper from 2015, Lotus Blossom as also been observed using strategic web compromises, and watering holes employing fake Flash player update re-directions. In one case, they replaced specialized font installers needed to render Myanmar font. You can see an image here of the "Planet Myanmar" website in late 2012 distributing such a package. All of the zip links were redirected to a poisoned installer zip file. The download name was "Zawgyi_Keyboard_L.zip", and it dropped a "setup.exe" that contained several backdoor components, including an Elise "wincex.dll".Operation Lotus Blossom is a prime example of how

a well-resourced adversary will deploy advanced tools, over an extended time period, sometimes years, in order to reach its goals.



Another interesting technique that Kaspersky observed in use against government targets was a campaign that lured recipients to a site redirecting users to a spoofed Flash installer site...

- Since then no real news in the evolution of Initial access techniques of Lotus Blossom. During the investigation of the 2022 Billbug campaign by Broadcom, they say to have some indications that the attackers are exploiting public-facing applications to gain initial access to the victim networks.

List of CVEs Used by Lotus Blossom and Their Purpose

CVE	Vulnerability Name	Purpose / Usage
CVE-2012-0158	**MSCOMCTL.OCX RCE Vulnerability**	Used in spearphishing campaigns to exploit Microsoft Office vulnerabilities, allowing attackers to download and execute malware like Elise. Also leveraged in the **Tran Duy Linh exploit kit** for Word-based attacks against defense contractors and government entities.
CVE-2014-6332	**Windows OLE Automation Array**	Used in a targeted attack on a **French diplomat** to install Emissary through a

	Remote Code Execution	remote code execution exploit. Also leveraged in **malicious VBS exploits** delivered via a compromised website distributing a Lurid variant payload.
CVE-2010-2883	**Adobe Reader and Acrobat CoolType.dll Buffer Overflow**	Used in **malicious PDF spearphishing campaigns** to execute arbitrary code and drop malware.
CVE-2014-xxxx *(Unspecified CVE, referenced in "half-day exploits")*	**Adobe Flash Player Exploit**	Used in **strategic web compromises and watering hole attacks**, redirecting victims to fake Flash Player updates to deliver malware.

- **Persistence :**

  ELISE

  - Elise is a custom backdoor Trojan that appears to be used exclusively by Lotus Blossom. It is part of a larger group oftools referred to as LStudio, ST Group, and APT0LSTU.
  - Elise is a relatively sophisticated tool, it gives the Lotus Blossom group their initial foothold in a network. From there, they can install additional tools, move laterally, and ex-filtrate data from the network.
  - Commands list :
    - `tasklist`
    - `ipconfig /all`
    - `net start`
    - `dir C:\progra~1`
    - `systeminf`
    - `net user`
    - `systeminfo`
  - If you want details on the 3 different variants that was used by Lotus Blossom you can read the Unit42 report or see the **Techniques Used** section describe in the MITRE ATT&CK pages of the malware.

  EMISSARY

  - Emissary is a Trojan that has been used by Lotus Blossom. It shares code with Elise, with both Trojans being part of a malware group referred to as

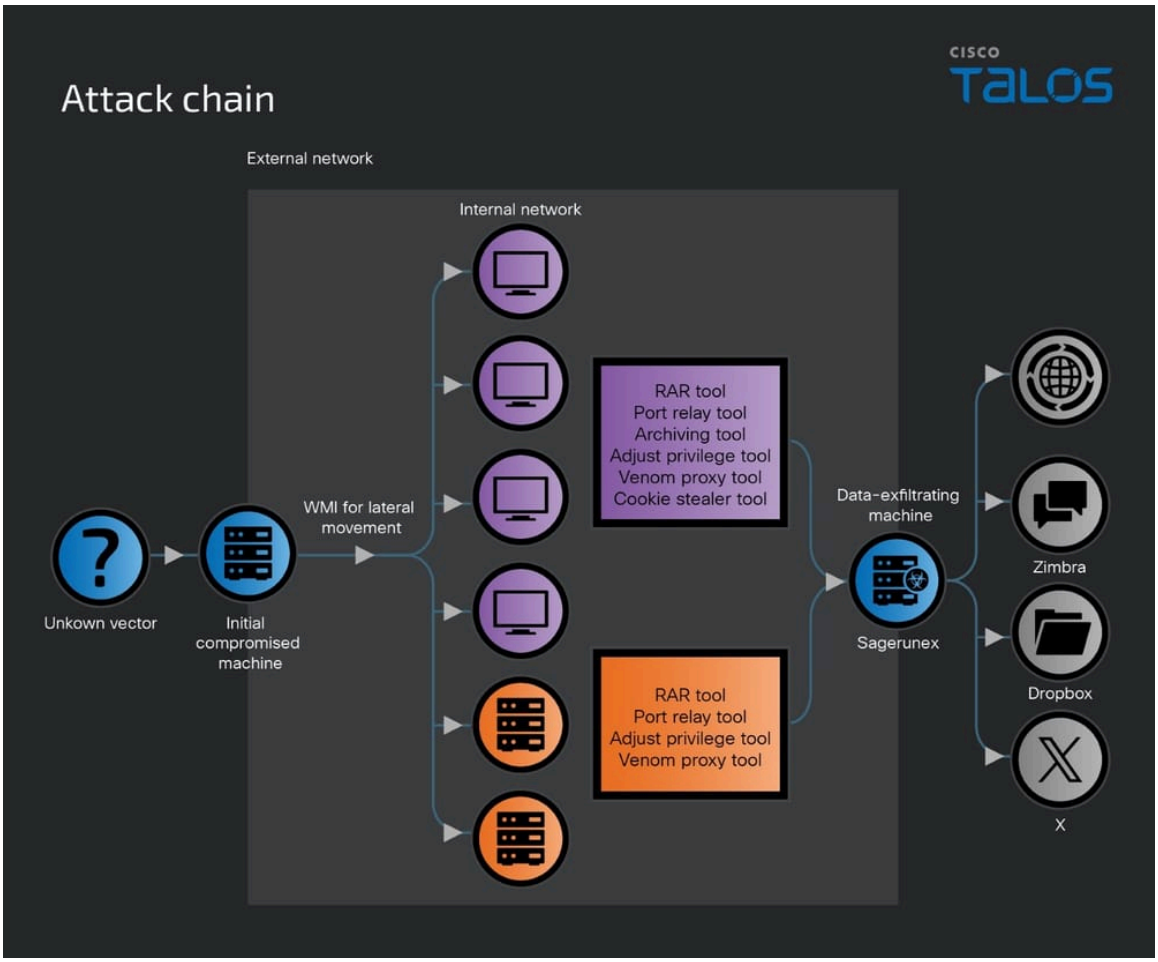
LStudio. (could be older)

- The Emissary Trojan is a capable tool to gain a foothold on a targeted system. While it lacks more advanced functionality like screen capturing, it is still able to carry out most tasks desired by threat actors: ex-filtration of files to the attacker's server, ability to download and execute additional payloads, and gain remote shell access.

- Commands list :
  - `ver`
  - `ipconfig /all`
  - `net localgroup adminstrators`
  - `net start`
  - `gpresult /z`
  - `gpresult`
  - `systeminfo`
- If you want details on the Emissary malware you can read the Unit42 report or see the **Techniques Used** section describe in the MITRE ATT&CK pages of the malware.

SAGERUNEX

- Sagerunex is a remote access tool (RAT) assessed to be an evolution of an older Billbug tool known as Evora (Elise variant A?). Sagerunex is designed to be dynamic link library (DLL) injected into an infected endpoint and executed directly in memory and then ot in the disk.
- Unlike Elise and Emissary, which are commonly used as initial access backdoors, Sagerunex is introduced later in the attack chain to establish long-term persistence and control over the compromised environment, typically deployed after some lateral movement, often using Windows Management Instrumentation (WMI) or other administrative tools.



- Often deployed before Sagerunex, Hannotog is an another Backdoor used by Lotus Blossom that act as a loader to charge Sagerunex into the memory
- It uses several communication methods to avoid detection, including:
  - HTTPS via a configured proxy
  - Dynamic proxy via WPAD (Web Proxy Auto-Discovery)
  - Internet Explorer or Firefox proxy
  - Direct connection without proxy
- And used severals tools to to **evade detection, steal credentials, and maintain persistence** in their attack campaigns.
  - **Cookie Stealer Tool**
    - PyInstaller bundle of a **Chrome cookie stealer**
    - Open-source tool from GitHub

        - Used to **harvest Chrome browser credentials**
    - **Venom Proxy Tool**
        - Developed for penetration testers using **Go language**
        - **Customized by the attackers** with a **hardcoded destination IP address**
    - **Adjust Privilege Tool**
        - Enables attackers to **retrieve another process token**
        - Used to **adjust privilege levels** for launching processes
    - **Archiving Tool**
        - Custom **compression and encryption tool**
        - **Steals files or entire folders**
        - Example: **Archives Chrome and Firefox browser cookies folders**
    - **Port Relay Tool (Mtrain V1.01)**
        - Modified version of **HTran** (proxy relay tool)
        - **Relays connections from the victim machine to the internet**
    - **RAR Tool**
        - Used to **archive or zip files** for exfiltration
- Command List Used by Lotus Blossom
    1. Reconnaissance & System Information Gathering
    - `net` → Enumerate network resources and user accounts
    - `tasklist` → List running processes
    - `quser` → Display user sessions
    - `ipconfig` → Display network configuration
    - `ipconfig /all` → Show detailed network adapter information
    - `netstat` → Display active network connections
    - `dir` → List directory contents
    2. Registry Modifications for Sagerunex Persistence
    - `reg add HKLM\SYSTEM\CurrentControlSet\Services\tapisrv\Parameters /v ServiceDll /t REG_EXPAND_SZ /d c:\windows\tapisrv.dll /f`
    - `reg add HKLM\SYSTEM\CurrentControlSet\Services\tapisrv /v Start /t REG_DWORD /d 2 /f`

        - `reg add HKLM\SYSTEM\CurrentControlSet\Services\swprv\Parameters /v ServiceDll /t REG_EXPAND_SZ /d c:\windows\swprv.dll /f`
        - `reg add HKLM\SYSTEM\CurrentControlSet\Services\swprv\Parameters /v ServiceDll /t REG_EXPAND_SZ /d c:\windows\system32\swprv.dll /f`
        - `reg add HKLM\SYSTEM\CurrentControlSet\Services\appmgmt\Parameters /v ServiceDll /t REG_EXPAND_SZ /d c:\windows\swprv.dll /f`
        - `reg add HKLM\SYSTEM\CurrentControlSet\Services\appmgmt /v Start /t REG_DWORD /d 2 /f`
        - `reg add HKLM\SYSTEM\CurrentControlSet\Services\appmgmt\Parameters /v ServiceDll /t REG_EXPAND_SZ /d c:\windows\system32\appmgmts.dll /` f
    3. Verification of Backdoor Installation
        - `reg query HKLM\SYSTEM\CurrentControlSet\Services\swprv\Parameters`
        - `reg query HKLM\SYSTEM\CurrentControlSet\Services\tapisrv\Parameters`
        - `reg query HKLM\SYSTEM\CurrentControlSet\Services\appmgmt\Parameters`
    - Several variants of Sagerunex exist, including one using Dropbox and Twitter for command and control, another leveraging Zimbra Webmail for communication and data exfiltration, and a version obfuscated with VMProtect to evade analysis and detection.
- **Ex-filtration**
    - Elise and Emissary used a series of cookie values in order to exfiltrate data though Virtual Private Server (VPS) for their C2 servers
    - The Sagerunex new variants no longer rely on the original Virtual Private Server (VPS) for their C2 servers. Instead, they use third-party cloud services such as Dropbox, Twitter, and the Zimbra open-source webmail
    - The final variant of the Sagerunex backdoor Talos discovered employs the Zimbra API to connect to a legitimate Zimbra mail service, using it as a C2 channel to exfiltrate victim information.

Mitre ATT&CK Mapping

Tactic	Technique ID	Technique Name	Context
Initial Access	T0817	Drive-by Compromise	Lotus Blossom as also been observed using strategic web compromises, and watering holes employing fake Flash player update re-directions. In one case, they replaced specialized font installers needed to render Myanma font. You can

			see an image here of the “Planet Myanmar” website in late 2012 distributing such a package.
	T0865	Spearphishing Attachment	Lotus Blossom groups was knows to use **Spearfishing** technique to conduct initial access, often using a malicious office document and decoy file containing content relevant to the target’s occupation or interests. The spear phishing attachment typically included exploit code for a well-known Microsoft Office vulnerability, CVE-2012-0158
	T1190	Exploit Public-Facing Application	Attackers may exploit public-facing applications to gain initial access.
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	Emissary can create a remote shell and execute commands. Sagerunex also uses remote shell execution for control.
	T1218.011	System Binary Proxy Execution: Rundll32	Elise and Emissary use `rundll32.exe` for execution. Sagerunex can also be executed via `rundll32.exe`.
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Elise, Emissary, and Sagerunex add Run Registry keys for persistence.
	T1543.003	Create or Modify System Process: Windows Service	Elise, Emissary, and Sagerunex configure themselves as services for persistence.
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location	Elise writes itself as `svchost.exe` in `%APPDATA%\Microsoft\Network`. Sagerunex disguises itself as legitimate system services.
	T1027.013	Obfuscated Files or Information: Encrypted/Encoded File	Elise encrypts configuration files; Emissary encrypts payloads using XOR and custom ciphers. Sagerunex encrypts its configuration and communication with AES256-CBC.
	T1027.001	Obfuscated Files or Information: Binary Padding	Emissary appends junk data to its DLL to evade detection.

	T1070.004	Indicator Removal: File Deletion	Elise can launch a remote shell to delete itself. Sagerunex also deletes its traces after execution.
	T1070.006	Indicator Removal: Timestomp	Elise timestomps CAB files it creates. Sagerunex modifies timestamps to evade forensic detection.
	T1112	Modify Registry	Sagerunex modifies registry keys to establish persistence.
Discovery	T1087.001	Account Discovery: Local Account	Elise executes `net user` after initial C2 communication. Sagerunex performs account enumeration as part of reconnaissance.
	T1082	System Information Discovery	Elise and Emissary execute `systeminfo` after initial C2 communication. Sagerunex also collects system details.
	T1016	System Network Configuration Discovery	Elise and Emissary execute `ipconfig /all`. Sagerunex uses `ipconfig /all` to collect network data.
	T1007	System Service Discovery	Elise and Emissary execute `net start`. Sagerunex executes `net start` to list active services.
	T1083	File and Directory Discovery	Elise executes `dir C:\progra~1` when initially run. Sagerunex also enumerates file structures for reconnaissance.
	T1057	Process Discovery	Elise executes `tasklist`. Sagerunex uses `tasklist` to enumerate running processes.
	T1069.001	Permission Groups Discovery: Local Groups	Emissary executes `net localgroup administrators`. Sagerunex also queries local administrator groups.
	T1615	Group Policy Discovery	Emissary executes `gpresult`. Sagerunex may also query group policy settings.
Lateral Movement	T1021.003	Remote Services: Windows Management Instrumentation (WMI)	Sagerunex is deployed through WMI for lateral movement within networks.
Credential Access	T1555	Credentials from Password Stores	Sagerunex steals credentials stored in browser cookies.
Collection	T1074.001	Data Staged: Local Data Staging	Elise stores harvested data in `AppData\Local\Microsoft\Windows\Explorer`.

			Sagerunex stages exfiltrated data in `%APPDATA%/microsoft/protect/windows/`.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	Elise and Emissary use HTTP/HTTPS for C2 communication. Sagerunex also uses HTTPS but employs proxy evasion techniques.
	T1573.001	Encrypted Channel: Symmetric Cryptography	Elise encrypts exfiltrated data with RC4. Emissary uses a GUID or XOR operations for encryption. Sagerunex encrypts C2 communication with AES256-CBC.
	T1095	Non-Application Layer Protocol	Sagerunex uses custom encrypted protocols for stealth C2 communication.
Exfiltration	T1132.001	Data Encoding: Standard Encoding	Elise exfiltrates data using Base64-encoded cookie values. Sagerunex encodes its data before exfiltration.
	T1105	Ingress Tool Transfer	Elise and Emissary download additional files from their C2 servers. Sagerunex downloads additional payloads from its C2 infrastructure.
	T1041	Exfiltration Over C2 Channel	Elise and Emissary exfiltrate data over their C2 channels. Sagerunex exfiltrates data through Dropbox, Twitter, and Zimbra Webmail.

Mitigations

- **Initial Access Mitigation**
  - Implement email security solutions
  - Train employees on phishing awareness and safe email practices.
  - Block macros in Office documents from untrusted sources.
  - Use Web Content Filtering to restrict access to potentially malicious sites.
  - Keep Adobe Flash Player disabled and ensure browsers are updated.
  - Restrict Administrative tasks like reading emails in another network
  - Apply timely patches for known vulnerabilities (e.g., CVE-2012-0158, CVE-2014-6332).
  - Regularly scan and harden public-facing servers.
- **Execution & Persistence Mitigation**

    - Implement EDR tools to detect suspicious behaviors.
    - Restrict script execution policies
    - Restrict admin privileges to prevent unauthorized service creation.
    - Monitor and log service modifications
    - Implement memory protection mechanisms
- **Privilege Escalation & Defense Evasion Mitigation**
    - Active MFA
    - Monitor Windows Event Logs
- **Lateral Movement Mitigation**
    - Network segmentation
    - Restrict WMI access to only authorized users
    - Monitor WMI execution logs
- **C2 Mitigation**
    - Implement SSL/TLS inspection
    - Monitor API calls to services like Dropbox and Twitter
- **Ex-filtration Mitigation**
    - Monitor outbound network traffic for large file transfers.
    - Restrict unapproved file-sharing services (Dropbox, Zimbra).
- **General**
    - Apply patches & Updates
    - Use SOC & SIEM monitoring
    - Implement Zero Trust Architecture