January 07, 2025

EAGERBEE Backdoor Targets Middle Eastern ISPs and Governments

Overview: Kaspersky Labs has identified a sophisticated cyberespionage campaign utilizing the EAGERBEE backdoor to compromise internet service providers (ISPs) and governmental organizations in the Middle East. This campaign, potentially linked to the CoughingDown, demonstrates advanced malware capabilities through novel techniques, including DLL hijacking, service injection, and a range of specialized plugins. EAGERBEE's arsenal of tools enables extensive malicious activities, such as process exploration, file manipulation, remote access, and stealthy persistence mechanisms. Kaspersky's analysis highlights overlap between EAGERBEE and the CoughingDown malware framework, though attribution remains inconclusive.

CTI Analysis: EAGERBEE employs DLL hijacking as its primary infection method, using legitimate Windows services such as SessionEnv to deploy malicious components. The service injector targets system processes and allocates memory to introduce the backdoor bytes while executing stub code for further exploitation. Once deployed, the backdoor gathers detailed system information, including network addresses, OS details, and process identifiers, which it transmits to a command-and-control (C2) server. Encrypted protocols such as SSL and TLS ensure secure communication between the malware and its operators. The backdoor's Plugin Orchestrator (ssss.dll) coordinates various plugins that support file management, remote access, and network reconnaissance while evading detection.
Kaspersky's investigation revealed EAGERBEE's integration of previously undocumented components, such as plugins for file system manipulation and network connection listing. The malware operates stealthily, using encryption and memory-resident modules to avoid triggering alarms. The use of hardcoded C2 IP addresses and sophisticated plugin orchestration underscores the campaign's strategic intent and technical prowess.

Commands and task descriptions for each of the plugins:

File Manager Plugin: This plugin is responsible for managing file system tasks such as file manipulation, permissions, and payload injection

- 0x02: Check and enable system privileges for the process

- 0x06: List files, folders, and get information about USB devices from specific locations.
- 0x07: Get information about drives
- 0x08: Delete multiple directories/files
- 0x09: Create a new directory
- 0x0A(10): Rename a directory/file
- 0x0B(11): Move or copy a directory/file
- 0x0C(12): Move or copy multiple directories/files
- 0x0D(13): Inject an executable or DLL into memory
- 0x0F(15): List files/folders recursively, read, and write files
- 0x14(20): Launch a command via CreateProcessW
- 0x22(34): Adjust file/folder permissions (DACL) for specific groups
- 0x23(35): Load a DLL via LoadLibraryW
- 0x24(36): Set a label of a file system volume
- 0x26(38): Copy an existing file and set timestamps to match user32.dll

Process Manager Plugin: This plugin manages running processes such as listing, terminating, and launching processes.

- 0x10(16): Terminate a process with specified process ID
- 0x11(17): Run a command line or launch a module via CreateProcessW
- 0x1E(30): List running processes and associated user accounts
- 0x26(38): Set file attributes

Remote Access Manager Plugin: This plugin facilitates remote access, allowing RDP connections and command shell access.

- 0x0B(11): Enable and configure RDP settings for persistence
- 0x0D(13): Download a file and initiate an RDP session
- 0x1D(29): Start a command shell (cmd.exe) and send commands to the C2 server
- 0x1E(30): Start the command shell (if not running) and execute received commands
- 0x21(33): Terminate the command shell process and stop reading its output

Service Manager Plugin: This plugin manages system services, allowing creation, modification, and enumeration of services.

- 0x11(7): Create a new service (shared or own process)
- 0x12(18): Stop and delete a service
- 0x13(19): Start a service
- 0x14(20): Stop a service
- 0x1E(30): Enumerate all services and collect information

Network Manager Plugin: This plugin lists and manages network connections, both IPv4 and IPv6.

- 0x1E(30): Get details of TCP and UDP connections, including state, addresses, ports, and owning PID.

Impact Analysis: The EAGERBEE backdoor poses significant threats to the affected ISPs and governmental entities. By leveraging advanced plugins, attackers can exfiltrate sensitive data, compromise network integrity, and maintain persistent access to critical systems. The malware's capabilities to inject additional payloads and manipulate system files heighten the risk of further exploitation, while its ability to evade detection complicates mitigation efforts. The potential overlap with CoughingDown signals the involvement of a highly resourced and strategic adversary, likely targeting geopolitical and strategic information in the Middle East.

Mitigation

To counter the EAGERBEE threat, organizations are advised to:

- Implement strict access controls and restrict privileges for critical processes to prevent unauthorized injections.
- Regularly update antivirus and endpoint protection solutions to detect emerging threats like EAGERBEE.
- Monitor system logs and network traffic for unusual activity, particularly related to DLL loading and service modifications.
- Employ application whitelisting to block unauthorized executables and DLL files.

- Conduct frequent security audits and vulnerability assessments to identify and mitigate potential entry points for attackers.

Conclusion: The discovery of EAGERBEE underscores the growing sophistication of cyberespionage campaigns targeting critical institutions. The advanced techniques employed by malware, coupled with its novel components, highlight the importance of proactive and layered defense mechanisms. While the exact attribution remains uncertain, EAGERBEE's association with the CoughingDown framework points to a well-funded and capable adversary. By implementing robust security measures and maintaining vigilance, organizations can reduce the risk of compromise and protect sensitive assets from such advanced threats.

Source:

https://securelist.com/eagerbee-backdoor/115175/

https://securityonline.info/eagerbee-advanced-backdoor-targets-middle-eastern-isps-and-government-entities/

https://www.bleepingcomputer.com/news/security/eagerbee-backdoor-deployed-against-middle-eastern-govt-orgs-isps/

https://www.hendryadrian.com/web/?url=https://www.hendryadrian.com/eagerbee-with-updated-and-novel-components-targets-the-middle-east/