CIRT.GY Guyana National Computer Incident Response Team

AL2024_34 Hackers Exploit AppDomain Manager Injection to Deploy CobaltStrike Beacons (02nd September 2024)

Description

A new type of cyberattack using a less common technique called AppDomain Manager Injection has been targeting government agencies in Taiwan, military entities in the Philippines, and energy organizations in Vietnam. This technique, previously used mainly for testing security, has now been weaponized by attackers.

Details

The attackers are leveraging the .NET Framework's AppDomainManager class to inject malicious code into any Microsoft .NET application running on Windows. This method is stealthier and more versatile compared to traditional DLL side-loading because it executes malicious code within the context of a legitimate, signed executable, making it harder for security software to detect.

The attack chain typically begins with the delivery of a ZIP archive containing a malicious MSC (Microsoft Script Component) file. Once the target opens this file, malicious code is executed immediately using a technique known as GrimResource. This technique exploits a cross-site scripting (XSS) vulnerability in the apds.dll library of Windows to execute arbitrary code through the Microsoft Management Console (MMC), ultimately running .NET code via the DotNetToJScript method.

The MSC file creates an exe.config file in the same directory as a legitimate Microsoft executable. This configuration file redirects the loading of certain assemblies to a malicious DLL. The DLL, which is inherited from the AppDomainManager class, is then loaded instead of the legitimate assembly, allowing the execution of malicious code within the context of the legitimate application. The final stage of the attack involves loading a CobaltStrike beacon, which the attacker can use for further malicious activities, including introducing additional payloads and facilitating lateral movement within the target's network.

Indicators of Compromise (IoCs)

Organizations should monitor for the following indicators of compromise:

- Presence of unexpected exe.config files in directories containing legitimate Microsoft executables.
- Unusual DLL files in directories where legitimate .NET applications are running.
- Suspicious network traffic indicative of CobaltStrike beacon communications.
- Execution of MSC files from unexpected or unauthorized sources.

Remediation

To mitigate the risk posed by these attacks:

1. **Update and Patch Systems**: Ensure that all systems are up to date with the latest security patches.
2. **Monitor for IoCs**: Implement monitoring to detect the creation of unexpected exe.config files, unusual DLLs, and suspicious network traffic.
3. **Harden Security Configurations**: Disable unnecessary features in the Microsoft Management Console (MMC) and .NET Framework to reduce the attack surface.
4. **User Education**: Educate users on the risks of opening files from unknown or suspicious sources, particularly ZIP archives and script components.

References

Staff, S. (2024, August 26). AppDomain Manager Injection exploited for Cobalt Strike beacon delivery. Retrieved from *SC Media*. https://www.scmagazine.com/brief/appdomain-manager-injection-exploited-for-cobalt-strike-beacon-delivery

Toulas, B. (2024, August 23). Hackers now use AppDomain Injection to drop CobaltStrike beacons. Retrieved from *BleepingComputer*. https://www.bleepingcomputer.com/news/security/hackers-now-use-appdomain-injection-to-drop-cobaltstrike-beacons/