# FoggyWeb, Software S0661 | MITRE ATT&CK®



Enterprise T1071 .001 Application Layer Protocol: Web Protocols

FoggyWeb has the ability to communicate with C2 servers over HTTP GET/POST requests.[1]

Enterprise T1560 .002 Archive Collected Data: Archive via Library

FoggyWeb can invoke the `Common.Compress` method to compress data with the C# GZipStream compression class.[1]

.003 Archive Collected Data: Archive via Custom Method

FoggyWeb can use a dynamic XOR key and a custom XOR methodology to encode data before exfiltration. Also, FoggyWeb can encode C2 command output within a legitimate WebP file.[1]

Enterprise T1005 Data from Local System

FoggyWeb can retrieve configuration data from a compromised AD FS server.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

FoggyWeb can be decrypted in memory using a Lightweight Encryption Algorithm (LEA)-128 key and decoded using a XOR key.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

FoggyWeb has used a dynamic XOR key and custom XOR methodology for C2 communications.[1]

Enterprise T1041 Exfiltration Over C2 Channel

FoggyWeb can remotely exfiltrate sensitive information from a compromised AD FS server.[1]

Enterprise T1083 File and Directory Discovery

FoggyWeb's loader can check for the FoggyWeb backdoor .pri file on a compromised AD FS server.[1]

Enterprise T1574 .001 Hijack Execution Flow: DLL

FoggyWeb's loader has used DLL Search Order Hijacking to load malicious code instead of the legitimate `version.dll` during the `Microsoft.IdentityServer.ServiceHost.exe` execution process.[1]

Enterprise T1105 Ingress Tool Transfer

FoggyWeb can receive additional malicious components from an actor controlled C2 server and execute them on a compromised AD FS server.[1]

Enterprise T1036 Masquerading

FoggyWeb can masquerade the output of C2 commands as a fake, but legitimately formatted WebP file.[1]

.005 Match Legitimate Resource Name or Location

FoggyWeb can be disguised as a Visual Studio file such as `Windows.Data.TimeZones.zh-PH.pri` to evade detection. Also, FoggyWeb's loader can mimic a genuine `dll` file that carries out the same import functions as the legitimate Windows `version.dll` file.[1]

Enterprise T1106 Native API

FoggyWeb's loader can use API functions to load the FoggyWeb backdoor into the same Application Domain within which the legitimate AD FS managed code is executed.[1]

Enterprise T1040 Network Sniffing

FoggyWeb can configure custom listeners to passively monitor all incoming HTTP GET and POST requests sent to the AD FS server from the intranet/internet and intercept HTTP requests that match the custom URI patterns defined by the actor.[1]

Enterprise T1027 .004 Obfuscated Files or Information: Compile After Delivery

FoggyWeb can compile and execute source code sent to the compromised AD FS server via a specific HTTP POST.[1]

.013 Obfuscated Files or Information: Encrypted/Encoded File

FoggyWeb has been XOR-encoded.[1]

Enterprise T1057 Process Discovery

FoggyWeb's loader can enumerate all Common Language Runtimes (CLRs) and running Application Domains in the compromised AD FS server's `Microsoft.IdentityServer.ServiceHost.exe` process.[1]

Enterprise T1620 Reflective Code Loading

FoggyWeb's loader has reflectively loaded .NET-based assembly/payloads into memory.[1]

Enterprise T1129 Shared Modules

FoggyWeb's loader can call the `load()` function to load the FoggyWeb dll into an Application Domain on a compromised AD FS server.[1]

Enterprise T1552 .004 Unsecured Credentials: Private Keys

FoggyWeb can retrieve token signing certificates and token decryption certificates from a compromised AD FS server.[1]

Enterprise T1550 Use Alternate Authentication Material

FoggyWeb can allow abuse of a compromised AD FS server's SAML token.[1]

---