IceApple, Software S1022 | MITRE ATT&CK®

Archived: 2026-04-05 16:42:36 UTC

Enterprise T1087 .002 Account Discovery: Domain Account

The IceApple Active Directory Querier module can perform authenticated requests against an Active Directory server.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

IceApple can use HTTP GET to request and pull information from C2.[1]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

IceApple can encrypt and compress files using Gzip prior to exfiltration.[1]

Enterprise T1005 Data from Local System

IceApple can collect files, passwords, and other data from a compromised host.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

IceApple can use a Base64-encoded AES key to decrypt tasking.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

The IceApple Result Retriever module can AES encrypt C2 responses.[1]

Enterprise T1041 Exfiltration Over C2 Channel

IceApple's Multi File Exfiltrator module can exfiltrate multiple files from a compromised host as an HTTP response over C2.[1]

Enterprise T1083 File and Directory Discovery

The IceApple Directory Lister module can list information about files and directories including creation time, last write time, name, and size.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

IceApple can delete files and directories from targeted systems.[1]

Enterprise T1056 .003 Input Capture: Web Portal Capture

The IceApple OWA credential logger can monitor for OWA authentication requests and log the credentials.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

IceApple .NET assemblies have used `App_Web_` in their file names to appear legitimate.[1]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

IceApple can use Base64 and "junk" JavaScript code to obfuscate information.[1]

Enterprise T1003 .002 OS Credential Dumping: Security Account Manager

IceApple's Credential Dumper module can dump encrypted password hashes from SAM registry keys, including `HKLM\SAM\SAM\Domains\Account\F` and `HKLM\SAM\SAM\Domains\Account\Users\*\V`.[1]

.004 OS Credential Dumping: LSA Secrets

IceApple's Credential Dumper module can dump LSA secrets from registry keys, including: `HKLM\SECURITY\Policy\PolEKList\default`, `HKLM\SECURITY\Policy\Secrets\*\CurrVal`, and `HKLM\SECURITY\Policy\Secrets\*\OldVal`.[1]

Enterprise T1620 Reflective Code Loading

IceApple can use reflective code loading to load .NET assemblies into `MSExchangeOWAAppPool` on targeted Exchange servers.[1]

Enterprise T1505 .004 Server Software Component: IIS Components

IceApple is an IIS post-exploitation framework, consisting of 18 modules that provide several functionalities.[1]

Enterprise T1082 System Information Discovery

The IceApple Server Variable Dumper module iterates over all server variables present for the current request and returns them to the adversary.[1]

Enterprise T1016 System Network Configuration Discovery

The IceApple ifconfig module can iterate over all network interfaces on the host and retrieve the name, description, MAC address, DNS suffix, DNS servers, gateways, IPv4 addresses, and subnet masks.[1]

Enterprise T1552 .002 Unsecured Credentials: Credentials in Registry

IceApple can harvest credentials from local and remote host registries.[1]
