- Persistence via AppInit DLL
  - MITRE ATT&CK™ Mapping
  - Query
  - Detonation
  - Contributors
- Persistence via NetSh Key
- Persistence via Screensaver
- Persistent process via Launch Agent
- Plist Modification
- Potential Gatekeeper Bypass
- Process Discovery via Built-In Applications
- Process Discovery via Windows Tools
- Processes Running with Unusual Extensions
- Processes with Trailing Spaces
- Proxied Execution via Signed Scripts
- Reading the Clipboard with pbpaste
- Registration of a Password Filter DLL
- Registration of Winlogon Helper DLL
- Registry Persistence via Run Keys
- Registry Persistence via Shell Folders
- Registry Preparation of Event Viewer UAC Bypass
- RegSvr32 Scriptlet Execution
- Remote Desktop Protocol Hijack
- Remote Execution via WMIC
- Remote System Discovery Commands
- Remote Terminal Sessions
- Resumed Application on Reboot
- Root Certificate Install
- SAM Dumping via Reg.exe
- Scheduled Task Creation via Microsoft Office Application
- Searching for Passwords in Files
- Searching for Passwords in Files
- Service Path Modification with sc.exe
- Service Stop or Disable with sc.exe
- Startup Folder Execution via VBScript
- Startup Folder Persistence with Shortcut/VBScript Files
- Stopping Services with net.exe
- Suspicious ADS File Creation
- Suspicious Bitsadmin Job via bitsadmin.exe
- Suspicious Bitsadmin Job via PowerShell
- Suspicious File Creation via Browser Extensions
- Suspicious MS Office Registry Modifications

Persistence via AppInit DLL

Detect registry modifications of the AppInit_Dlls key, which is used by attackers to maintain persistence. AppInit DLLs are loaded into every process that users the common library `user32.dll`.

id:	822dc4c5-b355-4df8-bd37-29c458997b8f
categories:	detect
confidence:	low
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Persistence, Privilege Escalation
techniques:	T1103 AppInit DLLs

Query

```
registry where wildcard(registry_path,
    "*\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows\\AppInit_Dlls",
    "*\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Windows\\AppInit_Dlls
  )
  and not wildcard(process_path, "*\\system32\\msiexec.exe", "*\\syswow64\\msiexec.exe")
| unique registry_data
```

Detonation

Atomic Red Team: T1103

Contributors

- Endgame

Previous Next