Resumed Application on Reboot
Root Certificate Install
SAM Dumping via Reg.exe
MITRE ATT&CK™ Mapping
Query
Detonation
Contributors
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
Suspicious Process Loading Credential Vault DLL
Suspicious Script Object Execution
System Information Discovery
System Network Connections Discovery
System Owner and User Discovery
Trap Signals Usage
Unload Sysmon Filter Driver with fltmc.exe
Unusual Child Process
User Account Creation
Volume Shadow Copy Deletion via VssAdmin
Volume Shadow Copy Deletion via WMIC
Windows File Permissions Modification
Windows Network Enumeration
WMI Execution via Microsoft Office Application
WMI Execution with Command Line Redirection
Atomic Blue Detections
Enterprise ATT&CK Matrix
Schemas
Resources
License

SAM Dumping via Reg.exe

Identifies usage of `reg.exe` to export registry hives which contain the SAM and LSA secrets.

id:	aed95fc6-5e3f-49dc-8b35-06508613f979
categories:	detect
confidence:	low
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Credential Access
techniques:	T1003 Credential Dumping

Query

```
process where subtype.create and
  process_name == "reg.exe" and
  (command_line == "* save *" or command_line == "* export *") and
  (command_line == "*hklm*" or command_line == "*hkey_local_machine*" ) and
  (command_line == "*\\sam *" or command_line == "*\\security *" or command_line == "*\\sys
```

Detonation

Atomic Red Team: T1003

Contributors

- Endgame

Previous Next