

☐ Modification of Boot Configuration

MITRE ATT&CK™ Mapping

Query

Detonation

Contributors

Modification of Id.so.preload

Modification of Logon Scripts from Registry

Modification of rc.common Script

Modifications of .bash_profile and .bashrc

Mounting Hidden Shares

Mounting Windows Hidden Shares with net.exe

MS Office Template Injection

Mshta Descendant of Microsoft Office

Mshta Network Connections

Network Service Scanning via Port

Non-browser processes making DNS requests to Dynamic DNS Providers

Office Application Startup via Template File Modification

Office Application Startup via Template Registry Modification

Password Policy Enumeration

Persistence via Applnit DLL

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

Docs » Analytics » Modification of Boot Configuration

[Edit on GitHub](#)

Modification of Boot Configuration

Identifies use of the bcdedit command to delete boot configuration data. This tactic is sometimes used as by malware or an attacker as a destructive technique.

id:	c4732632-9c1d-4980-9fa8-1d98c93f918e
categories:	detect
confidence:	low
os:	windows
created:	11/30/2018
updated:	05/17/2019

MITRE ATT&CK™ Mapping

tactics:	Impact
techniques:	T1490 Inhibit System Recovery

Query

```
process where subtype.create and
  process_name == "bcdedit.exe" and command_line == "*set *" and
  (command_line == "* bootstatuspolicy *ignoreallfailures*" or command_line == "* recoverye
```

Detonation

[Atomic Red Team: T1490](#)

Contributors

- [Endgame](#)

⬅ Previous

Next ➡

© Copyright 2019, Endgame Revision 30243396.

Built with [Sphinx](#) using a [theme](#) provided by [Read the Docs](#).