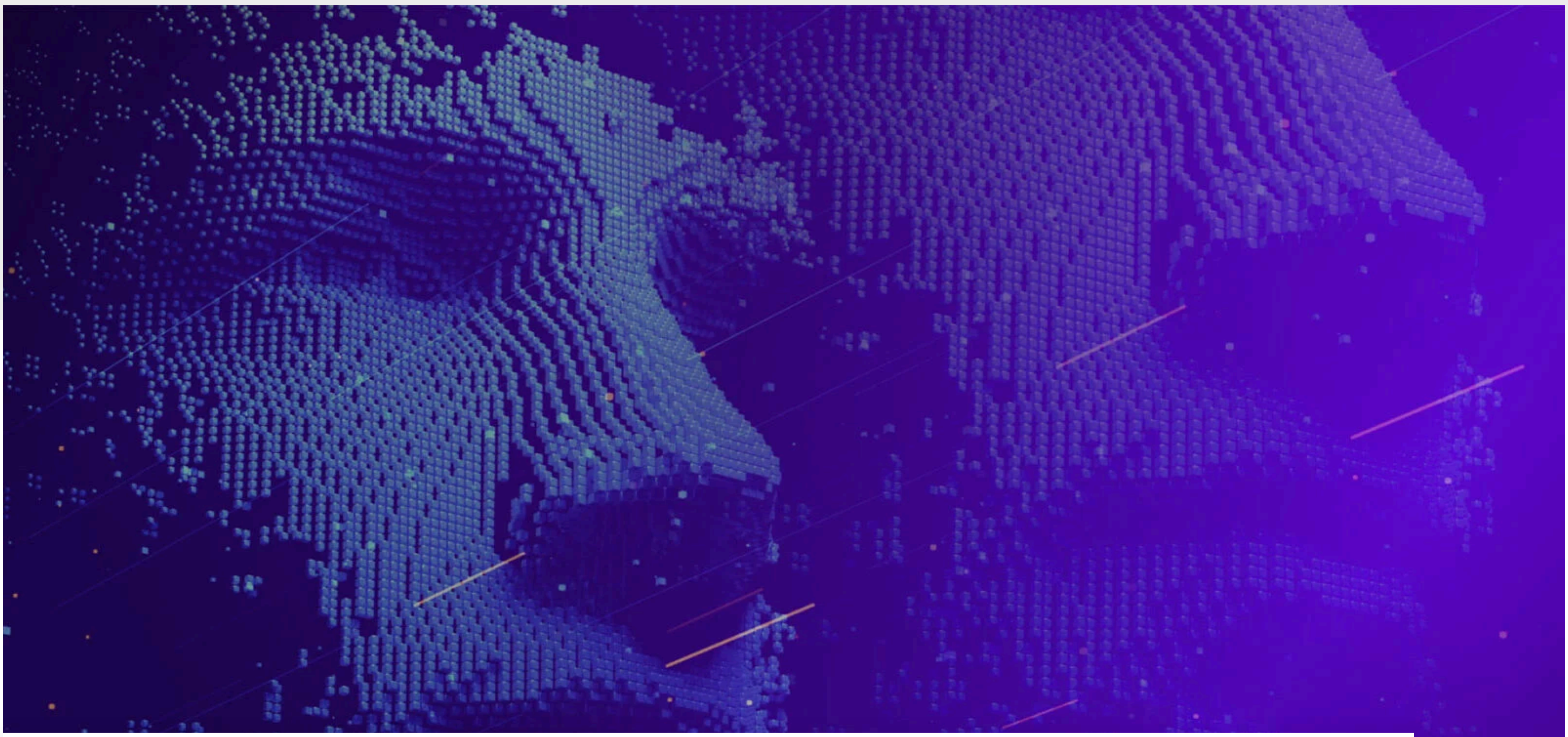


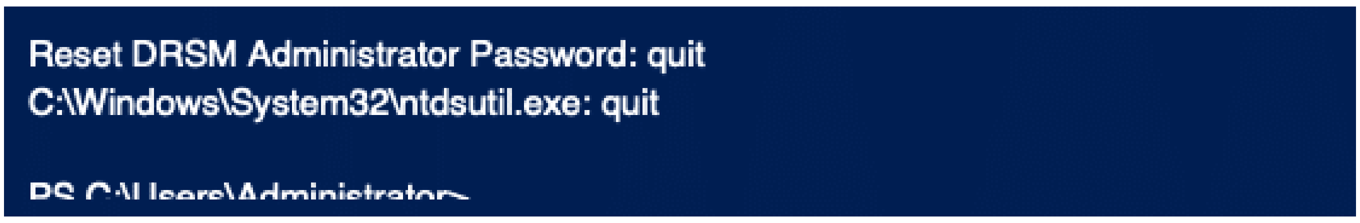
Detecting DSRM Account Misconfigurations

August 24, 2021
by Vikram Navali

PDF

During a Domain Controller (DC) promotion, administrators create a Directory Services Restore Mode (DSRM) local administrator account with a password that rarely changes. The DSRM account is an "Administrator" account that logs in with the DSRM mode when the server is booting up to restore AD backups or recover the server from a failure.

Attackers could abuse DSRM account to maintain their persistence and access to the organization's Active Directory. Administrators set the DSRM password while configuring Active Directory and typically do not follow the recommendation of changing its passwords regularly. Knowing this, attackers will attempt to create a permanent backdoor to establish a connection in the future. An attacker can change the DSRM account password by running the



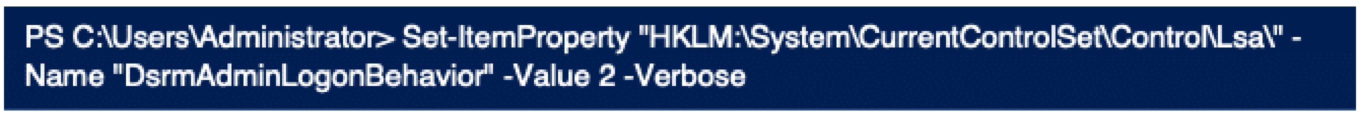
```
Reset DRSM Administrator Password: quit
C:\Windows\System32\ntdsutil.exe: quit

PS C:\Users\Administrator>
```

Once an attacker has the DSRM password, it is possible to use this account to log on to the DC over the network as a local administrator. An attacker can extract both the local administrator and AD administrator password hashes using an open-source credential dumping tool, such as running Mimikatz with the commands “*lsadump::sam*” and “*lsadump::lsa /patch*”, respectively.

With the local administrator password hash, the attacker can change the Windows registry to log into the DC using DSRM hashes without rebooting the server. The attacker can confirm the “DsrmAdminLogonBehavior” registry key value under HKLMSystemCurrentControlSetControlLsa and create possible REG_DWORD values as shown below:

- 0 – the default value. Can use the DSRM administrator account only if the DC starts in DSRM.
- 1 – Use the DSRM administrator account to log on if the local AD DS service is stopped.
- 2 – Always use the DSRM administrator account (This setting is not recommended because password policies do not apply to the DSRM administrator account).

The attacker will try to set the registry key “DsrmAdminLogonBehavior” value to 2, as shown below.



```
PS C:\Users\Administrator> Set-ItemProperty "HKLM:\System\CurrentControlSet\Control\Lsa\" -
Name "DsrmAdminLogonBehavior" -Value 2 -Verbose
```

An attacker further uses additional techniques such as Pass the Ticket (PTT) to access the DC and laterally move on the network. The following Mimikatz commands help to achieve their goals.

- “*privilege::debug*”
- “*sekurlsa::pth /domain:attivo1.local /user:Administrator /ntlm: fc063a56bf43cb54e57a2522d4d48678*”

Safely Expanding the Frontiers of AI & LLMs | S Ventures’ Investment in Galileo
October 25, 2024

The Good, the Bad and the Ugly in Cybersecurity – Week 43
October 25, 2024

Climbing The Ladder | Kubernetes Privilege Escalation (Part 1)
October 23, 2024

Blog Categories

Cloud
Company
Data Platform
Feature Spotlight
For CISO/CIO
From the Front Lines
Identity
Integrations & Partners
macOS
PinnacleOne
The Good, the Bad and the Ugly

The DSRM account activation provides a useful attack method to pull domain credentials and maintain persistence across the organization’s network. Administrators should implement appropriate password and registry key settings for these accounts and continuously monitor for misconfigurations that expose Active Directory to an attack.

Singularity™ Ranger AD is a cloud-delivered solution designed to uncover vulnerabilities in Active Directory and Azure AD. Get additional AD attack detection and conditional access capabilities to protect enterprise identity infrastructure with Singularity Ranger AD Protect.

References

https://adsecurity.org/?p=1714

https://adsecurity.org/?p=1785

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- New EMA Research Confirms Active Directory Is Under Attack
- DCSync Attack Protection Against Active Directory
- Exit Sandman | How SentinelOne Deflects APT-Level Identity Security Risks

Read More

Get a demo

Defeat every attack, at every stage of the threat lifecycle with SentinelOne

Book a demo and see the

SentinelLabs

SentinelLabs: Threat Intel & Malware Analysis

We are hunters, reversers, exploit developers, & tinkerers

Wizard Spider and Sandworm

MITRE Engenuity ATT&CK Evaluation Results

SentinelOne leads in the latest Evaluation with

Experiencing a Breach? 1-855-868-3733 Small Business Contact Cybersecurity Blog

SentinelOne blog

EN

SentinelOne
Secure Tomorrow™

Company

Our Customers
Why SentinelOne
Platform
About
Partners
Support
Careers
Legal & Compliance
Security & Compliance
Contact Us
Investor Relations

Resources

Blog
Labs
Product Tour
Press
News
FAQ
Resources
Ransomware Anthology

Sign Up For Our Newsletter

Business Email →

Language

English

Global Headquarters

444 Castro Street
Suite 400
Mountain View, CA 94041

+1-855-868-3733

sales@sentinelone.com