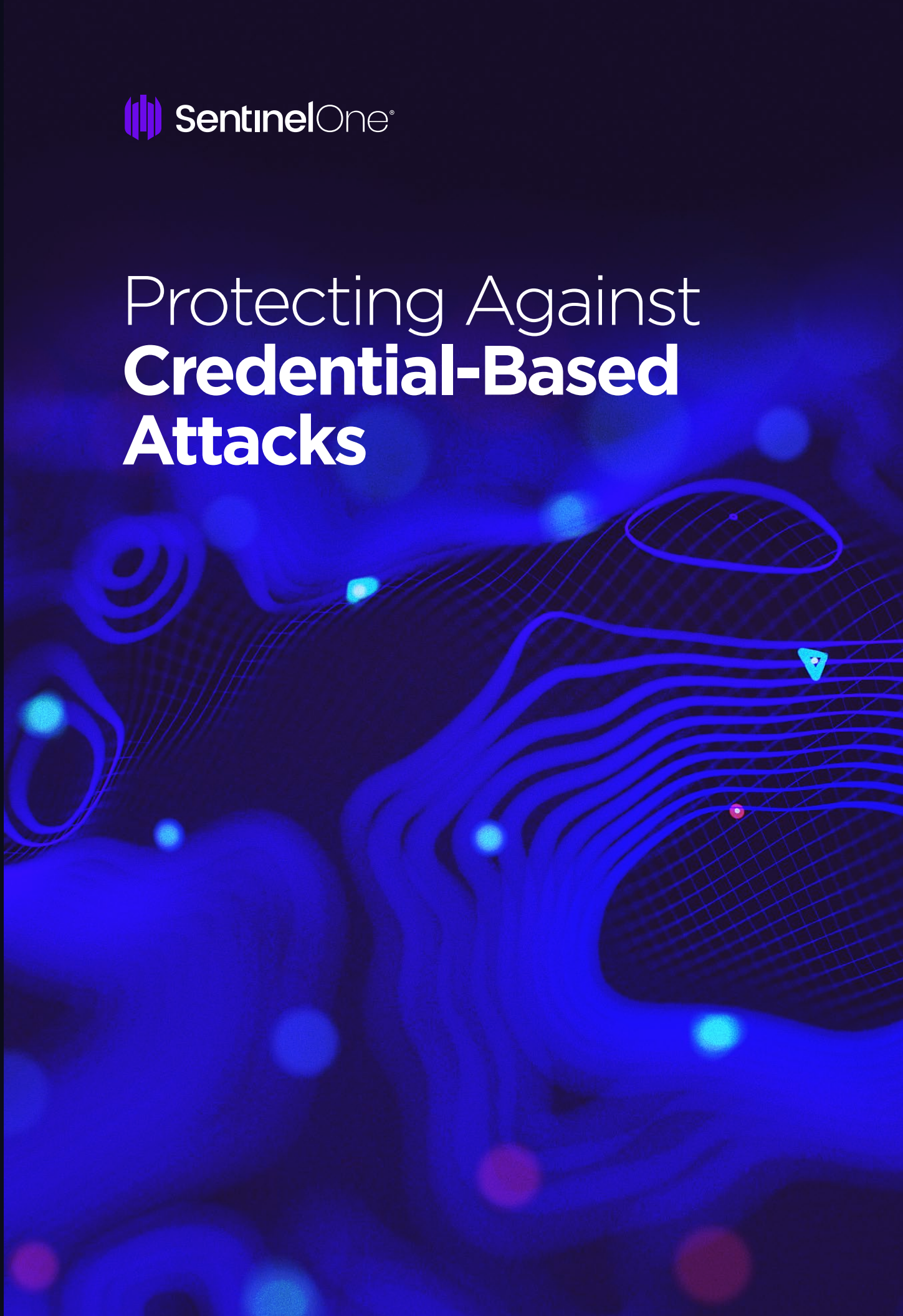
SentinelOne White Paper

SentinelOne®

Protecting Against **Credential-Based Attacks**



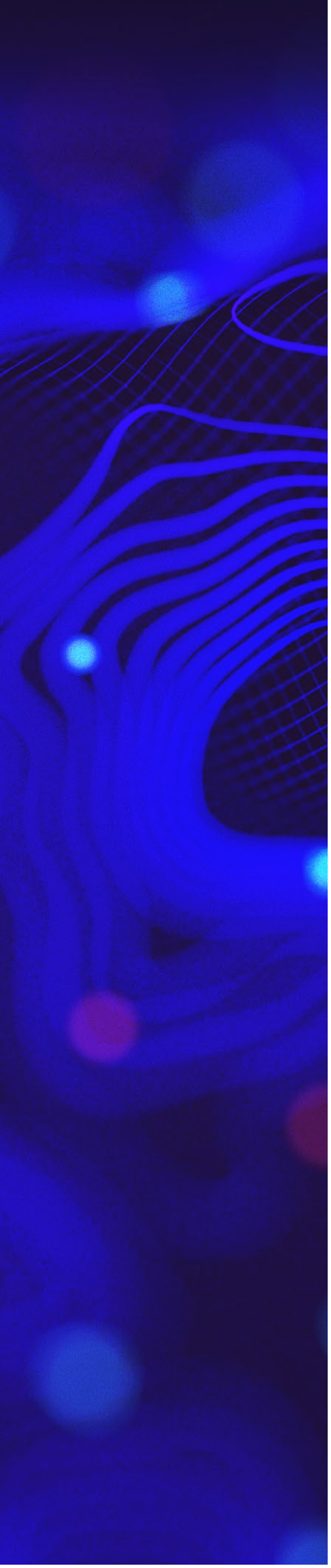


Table of Contents

01

Executive Summary

As the cybersecurity threat landscape continues to expand in both speed and scope, compromised credentials are emerging as a key element behind successful attacks. Threat actors steal credentials for multiple reasons, including selling them on the dark web, accessing enterprise infrastructure, and maintaining persistence.

According to Verizon's 2021 Data Breach Investigation Report (DBIR), 61% of all breaches involved credentials. Stolen credentials enable threat actors to create new accounts and move laterally to compromise an organization's security estate.

02

Introduction

Adversaries can leverage open-source credential dumping tools that are readily available to obtain credentials from various sources, such as databases, memory, or web browsers. These tools can help a threat actor discover credentials in the form of a hash value or a clear-text password. Once adversaries acquire credentials, they can move laterally and access restricted information.

Protecting Against Credential-Based Attacks will help readers understand how threat actors can dump credentials using advanced tools and techniques and how SentinelOne's identity security solutions can offer multiple layers of defense against credential thefts.

03

Why Do Threat Actors Target Credentials?

With legitimate credentials, an attacker can access an organization's valuable data and internal systems. According to Verizon's 2021 DBIR report, financially motivated attacks continue to be the most common in breaches, from compromising an dextorting organizations themselves or selling the credentials to underground cybercrime markets.

Here are five common reasons why adversaries go after credentials:

1. To sell credentials to other cyber criminals

There are specific underground markets and forums hidden on the dark web where someone can sell or buy credentials. According to Forbes research, more than 15 billion stolen account logins (including credentials, usernames, and password pairs) are circulating on the dark web and other black marketplaces.

2. For identity theft

Through an account takeover, cyber criminals can gain unauthorized access to the victim's online accounts, including their bank and email accounts, and social media profiles.

3. To blackmail victims

Threatening victim with compromised credentials and demands for ransom.

4. To launch nation-state attacks

Adversaries increasingly target a large customer base via the cloud and managed service providers. Most start with credential theft, stealing credentials or access keys via phishing attacks and deploying malware that picks up usernames and passwords.

5. To damage a brand's reputation

When cyber criminals with financial motivations launch double extortion attacks, they do so in order to harm their target's reputation by threatening to expose that they fell victim to a ransomware attack. Infamous attacks like the major Equifax breach still impact its image, and could cause damage to stock values if an enterprise is breached and exposed.

04

Where Are Credentials Stored?

Endpoints store different types of credentials in use, including login details, passwords, secret tokens, session cookies, private keys, and digital certificates, among others, in different locations. Specific applications also store passwords to make it easier for users to manage and maintain.

Once threat actors acquire these credentials, they can use them to access critical data, elevate privileges, and perform lateral movement across the victim's network. Adversaries frequently look in common password storage locations (such as Windows Credential Manager, Credentials from Web Browser, etc.) to get the information they need to launch an attack.

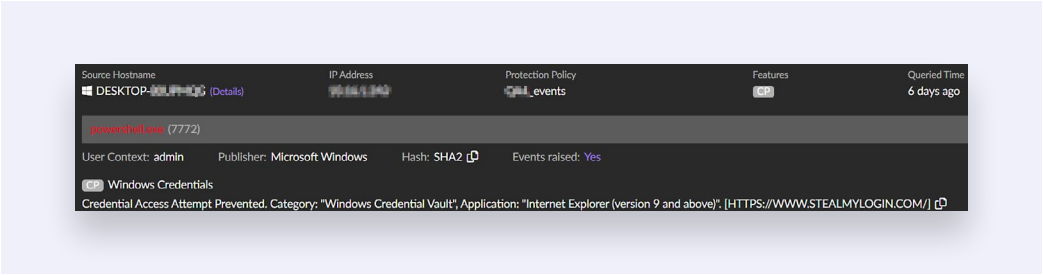


FIG: Singularity Identity Successfully Prevents an Attempt to Access Windows Credential Vault

Common Credential Stores:

File System on disk. These will persist across reboots.

- Can be clear text or encrypted
- Some applications are located in databases and stored as files.

Windows Registry

- OS and Applications save user and system specific data in Registry.
- Applications save credentials in Windows Registry.

Vaults

- Operating Systems or third-party applications provide vaults.
- Examples: Windows Credential Manager Vault, KeePass.

Memory

- Credentials get loaded into memory as clear-text passwords or hashes.
- Generated Tokens (Kerberos) after authentication also are saved in memory.
- These are not persisted in the File System and will be lost after reboot. Some expire after a period.

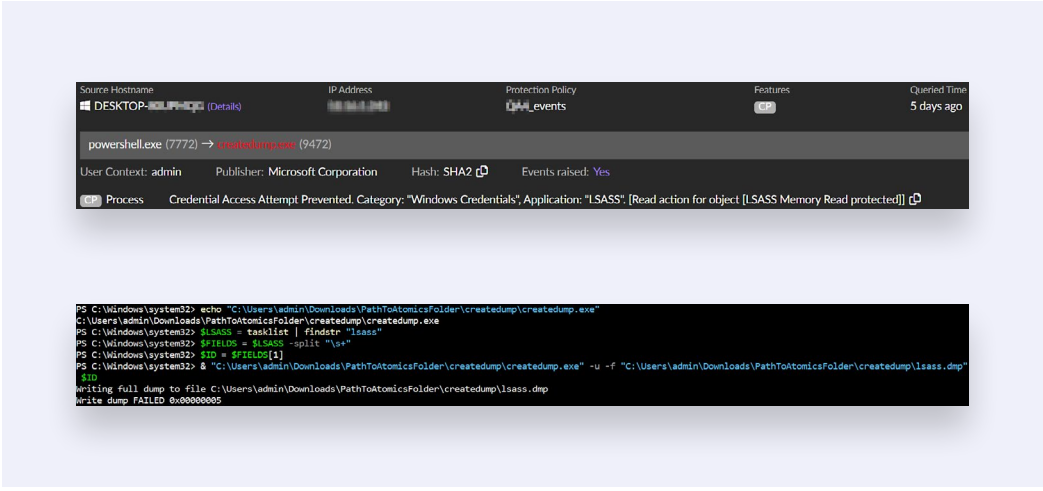
05

How Do Adversaries Steal Credentials?

Adversaries often rely on various techniques to crack user credentials easily and break into a system.

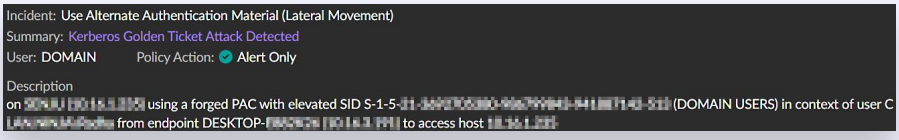
Phishing is the most efficient technique where adversaries create illegitimate emails and websites. They embedded these malicious website links in emails and sent them to the targeted users to provide their usernames and passwords. In many cases, phishing leads to a ransomware attack when the user mistakenly downloads an attachment or clicks on a malicious link that downloads and executes malware onto the system.

Brute Force is a trial-and-error technique that adversaries use to discover valid user credentials by guessing every possible combination of characters until they find the correct combination.



In the images above, SentinelOne successfully detects and prevents attempts for cyber criminals to access and exfiltrate credentials.

Once an adversary compromises an endpoint through phishing, they can obtain a username and password using credential dumping or brute-force techniques. They then use these credentials to access restricted information, move laterally, and install other malware. The following section discusses how adversaries can leverage tools to accomplish their desired results.



06

How SentinelOne Protects You From Credential Theft

SentinelOne offers comprehensive credential protection to stop credential theft early in the attack cycle and conceal credentials from untrusted applications.

Singularity Identity enables organizations to:

Cloak credentials and hide real credentials from adversaries and their tools.

Bind credentials to applications and prevent unauthorized access by binding credentials to critical applications across the network. Singularity Identity supports over 80+ applications and allows only the legitimate application(s) to access its saved credentials.

Deploy Deceptive Artifacts including deceptive credentials, accounts, and files, among others. Trick threat actors into stealing these decoy artifacts from an endpoint, and trick them into engaging and revealing themselves.

Ready for a Demo?

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

sentinelone.com

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2022 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

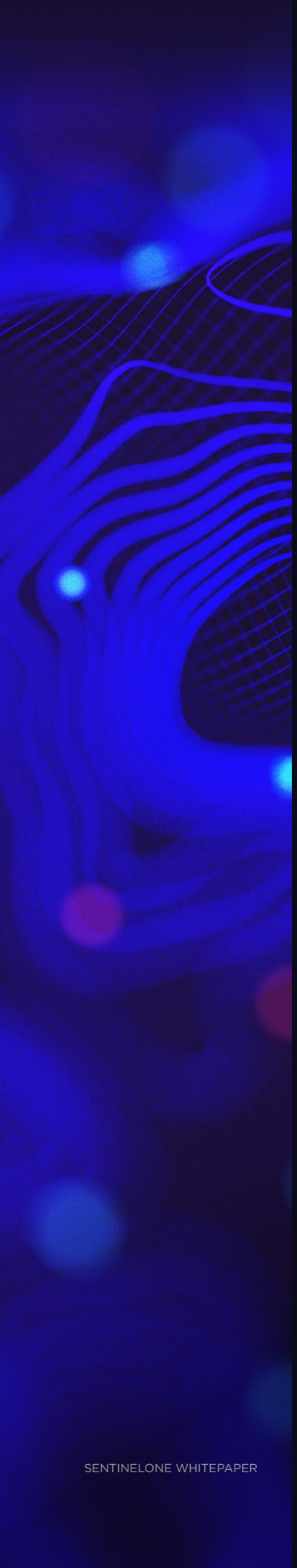
Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection
- Top Analytic Coverage, 3 Years Running
- 100% Real-time with Zero Delays

Gartner Peer Insights

96% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · 100 VIRUS · SE Labs BEST Innovator WINNER 2021 · AAA · Trusted Cloud Provider CSA



SentinelOne

Contact us

sales@sentinelone.com

+1-855-868-3733

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

sentinelone.com

23_WP_004_PROTECTING_AGAINST_CBA_05012023