SILVERFORT

# Multi-Factor Authentication:
# Not Just For Admins

# MFA Must Cover All Your Enterprise Users

It's common knowledge today that MFA is a highly effective security control. However, there is a prevalent misconception that it is enough to implement MFA for the admin/privileged accounts rather than across the entire enterprise workforce.

The logic behind this is that only compromised admin/privileged accounts introduce a critical risk to the enterprise. However, this assumption is fundamentally flawed.

The following paper includes four different use cases of identity-based attacks, including real-life examples from attacks that have recently taken place. These use cases could not be addressed properly by a limited implementation of MFA only for admin accounts, and all **of them would have been prevented had MFA been deployed across all users in the organization.**

While each use case is accompanied with a case study example, it should be noted that all of them represent **common patterns** that have been observed and documented in numerous instances.

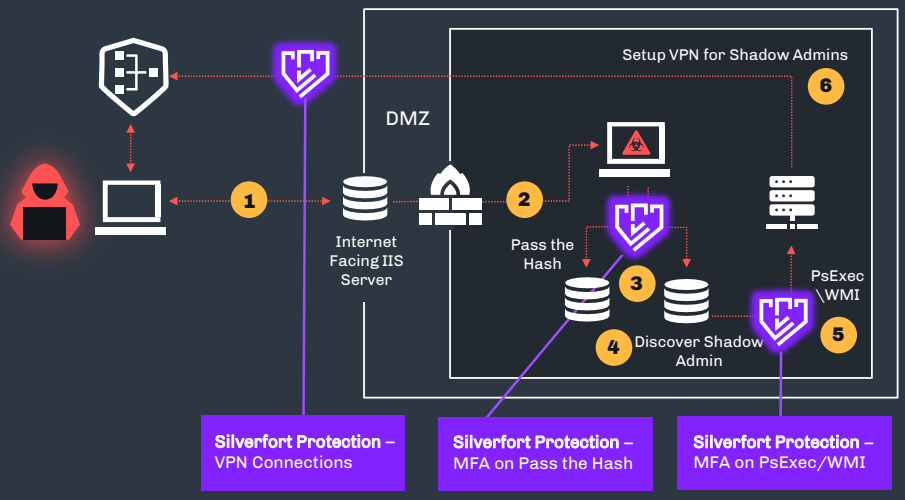
In the following diagrams you will find a breakdown of the attack stages. Silverfort's symbol indicates which stages could have been stopped with Silverfort's Unified Identity Protection platform.

## Shadow Admins

Shadow Admin accounts are user accounts that have sensitive privileges – not because they are members of a privileged Active Directory (AD) group, but because they were inadvertently assigned permissions that can allow them to take over other privileged accounts and leverage them to reach their target systems and compromise them. Because they are not part of a privileged AD group, they are typically overlooked by admins who are not aware of their existence, creating a critically exposed attack surface.

### APT10 Operation Soft Cell Shadow Admins Compromise

June 2019 | Telco Providers Network Takeover




Attack Flow

1. INITIAL ACCESS: Utilize existing webshells on the victim's application server.
2. CREDENTIAL ACCESS 1: Mimikatz memory dump.
3. LATERAL MOVEMENT 1: Pass the Hash using dumped hashes.
4. CREDENTIAL ACCESS 2: Discover shadow admins accounts.
5. LATERAL MOVEMENT 2.1: Utilize PSExec and WMI to log in to servers with the compromised shadow admins accounts.
6. PERSISTENCE: Set up VPN service for the shadow admins for remote login.

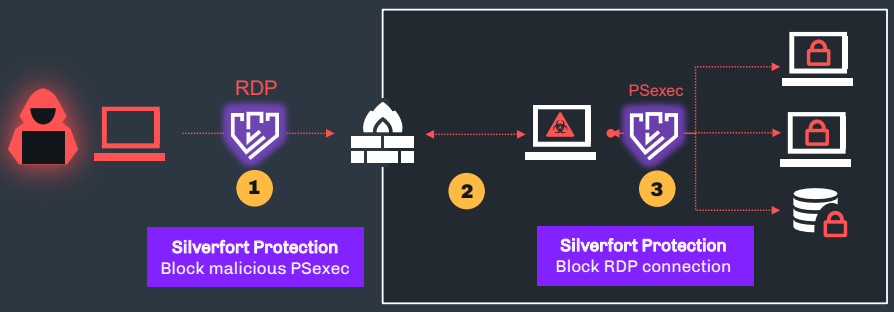
To read more about the Hidden Dangers of Shadow Admins - click here

# Automated Ransomware

Automated Ransomware propagation (WannaCry, NotPetya, Ryuk, etc.) strives to access shared folders and encrypt mission-critical data files. These shared folders are within the access privileges of the standard enterprise users, enabling attackers to inflict mass damage without ever needing to compromise an admin account.

## Pay2key Remote RDP + Automated Lateral Movement

November 2020 | Ransomware delivered through automated propagation infrastructure




Attack Flow :

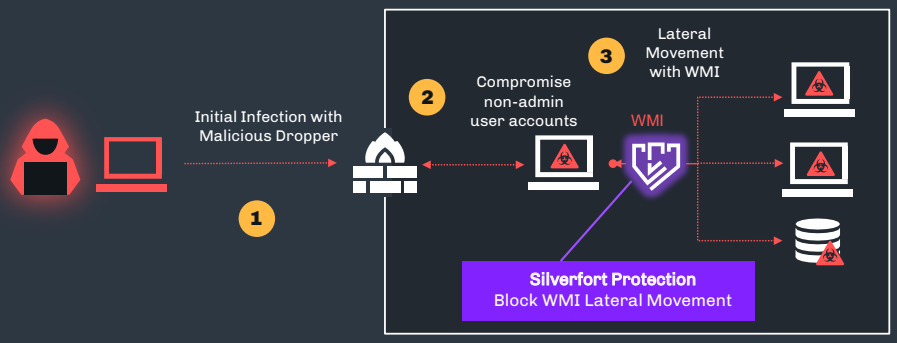
1. COMPROMISED CREDENTIALS: Initial infection of a single machine through manual RDP connection.
2. Configure this machine as a C2 proxy within the victim's network.
3. COMPROMISED CREDENTIALS: Execute Pay2Key ransomware on other machines in the network through PSexec within a single hour.

# Standard Domain Users Attack Surface

In many lateral movement attacks, threat actors avoid targeting the admin accounts since they are assumed to be closely monitored and protected. Instead, threat actors target standard domain users and either elevate their privileges or seek misconfigurations that enable these accounts to access additional resources.

## FunnyDream Lateral Movement with Domain Accounts

November 2020 | >200 systems infected within Southeast Asian governments




Attack Flow :

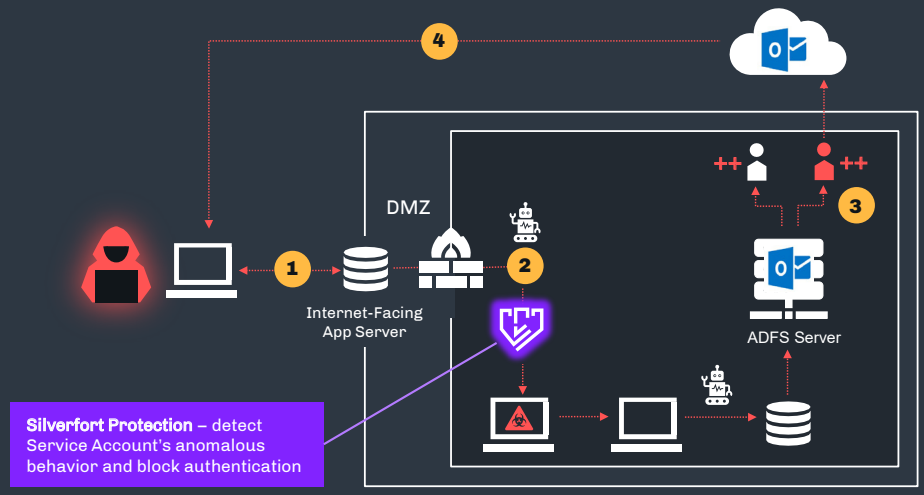
1. INITIAL INFECTION: With malicious dropper.
2. CREDENTIALS ACCESS: Dump user credentials from compromised machines.
3. LATERAL MOVEMENT: Utilize compromised credentials with WMI to access additional machines.

# Service Accounts

Service accounts are highly privileged accounts used for machine-to-machine communications. Since they are not associated with a human user, they cannot be subject to MFA protection. However, Silverfort's dedicated solution for service accounts proactively prevents attackers from utilizing them for lateral movement. Silverfort automatically discovers and monitors the behavior of all service accounts in your environment and provides an out-of-the-box access policy which prevents them from accessing resources when detecting a deviation from their standard behavior.

## SunBurst Attack Hybrid Network Lateral Movement

December 2020 | Massive global attack on numerous public and private organizations




Attack Flow

1. INITIAL ACCESS: SolarWinds Orion servers in DMZ.
2. LATERAL MOVEMENT - REMOTE SERVICES: Use Orion Service Accounts to reach ADFS server.
3. PERSISTENCE: CREATE ACCOUNT: Elevate privileges of existing users and create new admin users.
4. LATERAL MOVEMENT - ALTERNATE AUTHENTICATION: Access and exfiltrate data from Outlook accounts.

# About Silverfort

Silverfort is the provider of the first Unified Identity Protection Platform that consolidates security controls across corporate networks and cloud environments to block identity-based attacks. Using innovative agentless and proxyless technology, Silverfort seamlessly integrates with all existing IAM solutions (such as AD, ADFS, RADIUS, Azure AD, Okta, Ping, AWS IAM, etc.), extending their coverage to assets that could not be protected until today, such as homegrown/legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access and more. It continuously monitors all access of users and service accounts across both cloud and on-premise environments, analyzes risk in real time using an AI-based engine, and enforces adaptive authentication and access policies. Silverfort allows organizations to prevent data breaches, achieve compliance, reduce costs and simplify cloud migration. Silverfort is trusted by large enterprises around the world and was named a Gartner 'Cool Vendor'.

**To learn more, schedule a meeting:**
**www.silverfort.com/request-a-demo**


info@silverfort.com

www.Silverfort.com

**US**
(+1) 646 893 7857
43 Westland Avenue,
Boston, MA, USA

**Israel**
(+972) 77 202 4900
30 Haarbaa St, 26th Floor,
Tel Aviv, Israel


Gartner COOL VENDOR 2019