Pass-the-Hash

and other credential theft and reuse techniques

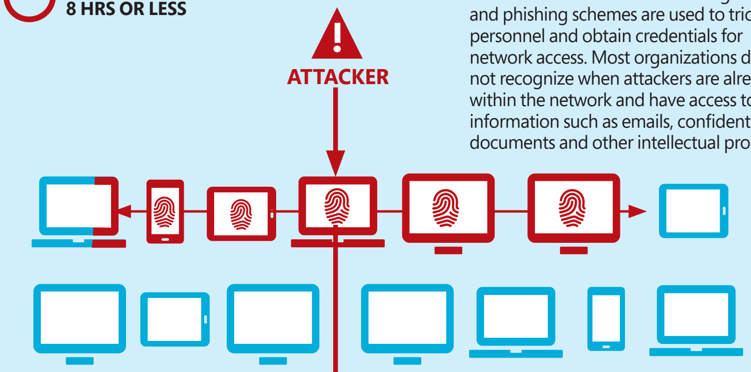
Microsoft

The most effective defense against PtH and other credential theft attacks requires organizations to deploy a comprehensive set of strategies and the available technical features and capabilities.
Learn more at www.microsoft.com/pth

ELAPSED TIME: 8 HRS OR LESS

GET CREDENTIALS

Malicious tactics such as social engineering and phishing schemes are used to trick personnel and obtain credentials for network access. Most organizations do not recognize when attackers are already within the network and have access to information such as emails, confidential documents and other intellectual property.



ELAPSED TIME: 24 HRS OR LESS

GET DATA

The attack doesn't stop there. Attackers look for the next set of credentials with elevated permissions to access servers. Once elevated credentials are obtained and servers are compromised, organizations risk losing revenue, brand reputation, and business continuity.

ELAPSED TIME: 48 HRS OR LESS

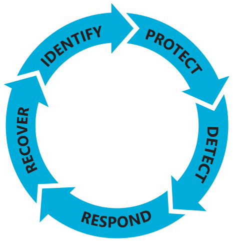
GET CONTROL

The ultimate goal of the attackers may be to gain access to the domain controllers, the central clearing hub for all credentials and identities. Once compromised, an attacker has complete control over an entire organization. All assets, intellectual property, physical property, and personal information are in jeopardy.

Create a planned approach using these strategies and features

STRATEGIES

- Identify all high value assets
- Protect against known and unknown threats
- Detect PtH and related attacks
- Respond to suspicious activity
- Recover from a breach



FEATURES	DESCRIPTION	AVAILABLE ON			REQUIRES DOMAIN UPGRADE
		Windows 7/Server 2008 R2	Windows 8/Server 2012	Windows 8.1/Server 2012 R2	Windows Server 2012 R2 Domain Functional Level
Logon restrictions with new well-known security identifiers (SIDs)	Use the new SIDs to block network logon for local users and groups by account type, regardless of what the local accounts are named	✓	✓	✓	
Enforce credential removal after logoff	New mechanisms have been implemented to eliminate session leaks in LSASS, thereby preventing credentials from remaining in memory	✓	✓	✓	
Remove LAN Manager (LM) hashes from LSASS	LAN Manager legacy hashes are no longer stored in LSASS	✓	✓	✓	
Remove plaintext credentials from LSASS for domain accounts	Plaintext credentials are removed from LSASS after logon in some versions of Windows	✓	✓	✓	
Restricted Admin mode for Remote Desktop Connection*	The Remote Desktop application and service have been updated to support authentication without providing credentials to the remote host	✓	✓	✓	
Protected Users security group client side protections	The types of credentials available are reduced for Members of the Protected Users group	✓	✓	✓	
Protected Users security group	The new Protected Users security group enables administrators to restrict authentication to the Kerberos protocol only for group members within a domain	✓	✓	✓	✓
Authentication Policy and Authentication Policy Silos	New Authentication policies provide the ability to restrict account authentication to specific hosts and resources			✓	✓
LSA protection	Allows the LSASS process to be turned into a Protected Process preventing other processes (including processes running as SYSTEM\Administrator) that are not signed by Microsoft from tampering with the LSASS process			✓	

*Remote Desktop service (RDP Session Host) support for this feature is only available on Windows 8.1 and Windows Server 2012 R2.