Pass-the-Hash: What is it & What to do about it?

Benny Lakunishok
Senior PFE
Microsoft

Story time

Defending Trends

"Symantec Corp. invented commercial antivirus software to protect computers from hackers a quarter-century ago. Now the company says such tactics are doomed to failure."

Topic: Security

Follow via:

'Antivirus is dead? If you think that's news, you've been living in a different world'

Summary: *With the continuing rise of cloud services, security execs have been proclaiming the death of antivirus software. But, according to F-Secure, the security is not so much dead as changed beyond all recognition.*

By Eeva Haaramo for Norse Code | May 14, 2014 -- 08:43 GMT (01:43 PDT)

Follow @ehaaramo

Symantec made headlines last week when a senior exec proclaimed antivirus software was "dead". It might seem a bold statement, but according to Finnish security company F-Secure, it's just a statement of fact, reflecting trends in an industry that's fast moving away from PCs.

"For years, signature-based antivirus detection has been only a fraction of what security companies have been offering," says Timo Laaksonen, VP of Content Cloud at F-Secure. "We have a huge arsenal of other tools. If someone thinks that antivirus being dead is news then we don't know in what world they have been living in for the past five to six years."

Pass-the-Hash in the News

BBC News Sport Weather Travel Future

The New York Times

January 30, 2013

Hackers in China Attacked The Times Last 4 Months

By NICOLE PERLROTH

SAN FRANCISCO — For the last four months, Chinese hackers have persistently attacked New York Times, infiltrating its computer systems and getting passwords for its reporters other employees.

After surreptitiously tracking the intruders to study their movements and help erect bette defenses to block them, The Times and computer security experts have expelled the attac and kept them from breaking back in.

THE WALL STREET JOURNAL.

MEDIA & MARKETING

Chinese Hackers Hit U.S. Media

Wall Street Journal, New York Times Are Breached in Campaign That Stretches Back Several Years

By SIOBHAN GORMAN, DEVLIN BARRETT and DANNY YADRON

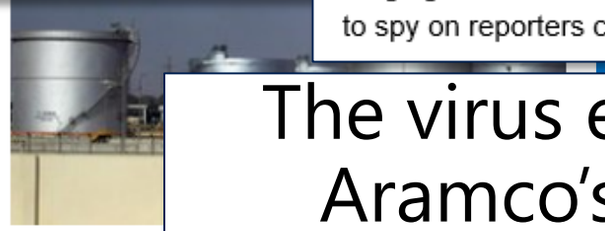
Updated Jan. 31, 2013 8:28 p.m. ET

WASHINGTON—Chinese hackers believed to have government links have been conducting wide-ranging electronic surveillance of media companies including The Wall Street Journal, apparently to spy on reporters covering China and other issues, people familiar with the incidents said.

Remote access was still restricted "as a precaution" the group said.

Oil production was not affected by the virus which struck on 15 August, Saudi Aramco added.

The company took its website offline after the attack and now carries a message on its front page apologising for any inconvenience.

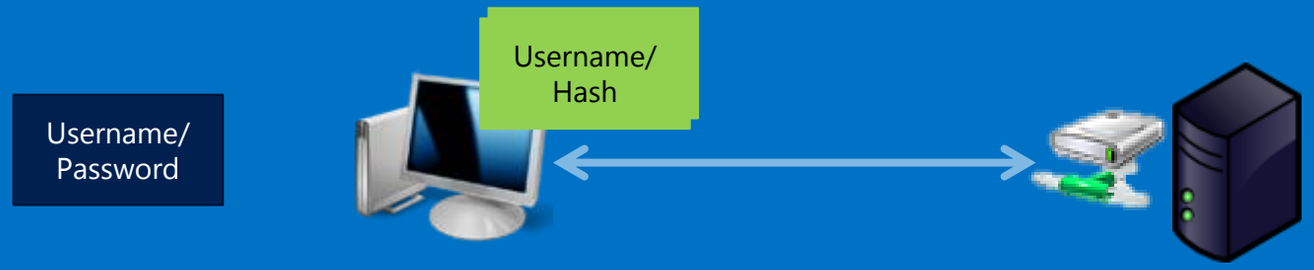


Saudi Aramco
by the virus att

The virus erased data on three-quarters of Aramco's corporate PCs — documents, spreadsheets, e-mails, files — replacing all of it with an image of a burning American flag.

Pass-the-Hash (PtH) Definition

- "Hash" = cached credential
  - Usually not "cleartext"
  - Identically powerful to "cleartext" by most systems
  - Can be stored in memory or persisted on disk
- Most operating systems cache credentials for single sign on (SSO)

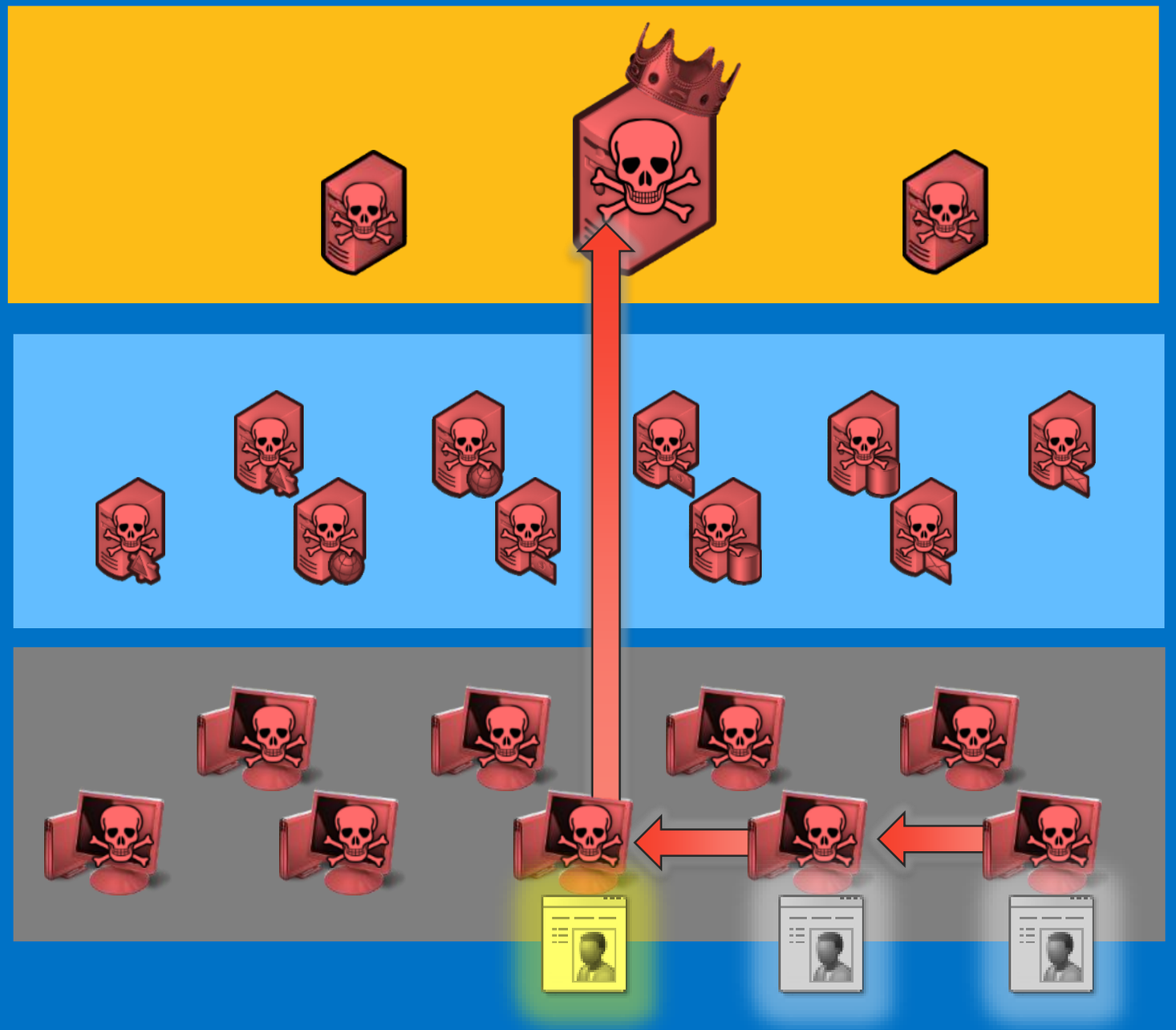


Pass-the-Hash Technique

- Attacker gains local admin access to initial system
- Uses collected hashes to move laterally through the network
- Additional hashes are collected as they go
  - New hashes give access to additional systems
  - Network/domain privileged account compromised → Game Over

Pass the Hash

1. Attacker targets workstation(s)
2. User running as local admin (or critical security vulnerability) is compromised, attacker harvests credentials
3. Attacker uses credentials for lateral movement or privilege escalation
4. Attacker acquires domain admin credentials
5. Attacker exercises full control of data and systems in the environment



Windows and Pass-the-Hash

- Windows supports SSO through security packages, which store “hashes”:
  - MSV1_0: NTLM, NTLMv2 hash
  - WDigest: cleartext
  - Kerberos: TGTs, service tickets and cleartext
- Many connections require NTLMv2
  - Target system specified as IP address
  - Legacy applications
  - Server configuration

Windows Pass-the-Hash Attack Tools

- "Discovered" in 1997
  - SMB client accepted NTLM password hashes
- "Weaponized" in 2008 by Hernan Ochoa (Amplia Security)
  - Pass-the-Hash Toolkit injected NTLM hashes into a logon session
  - More advanced Windows Credential Editor (WCE) introduced in 2010
  - Bread-and-butter for pentesters

Pass-the-Ticket

- Kerberos is not immune
- First “discovered” in 2010:

- Weaponized by Herman Ochoa in 2011

Demo

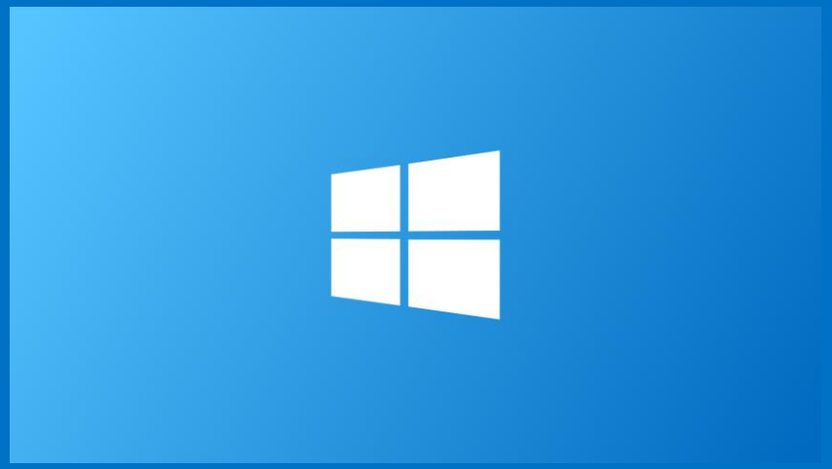
Windows Credential Editor

Current Guidance

Mitigation	Effectiveness	Effort required	Privilege escalation	Lateral movement
Mitigation 1: Restrict and protect high privileged domain accounts	Excellent	Medium	√	-
Mitigation 2: Restrict and protect local accounts with administrative privileges	Excellent	Low	-	√
Mitigation 3: Restrict inbound traffic using the Windows Firewall	Excellent	Medium	-	√

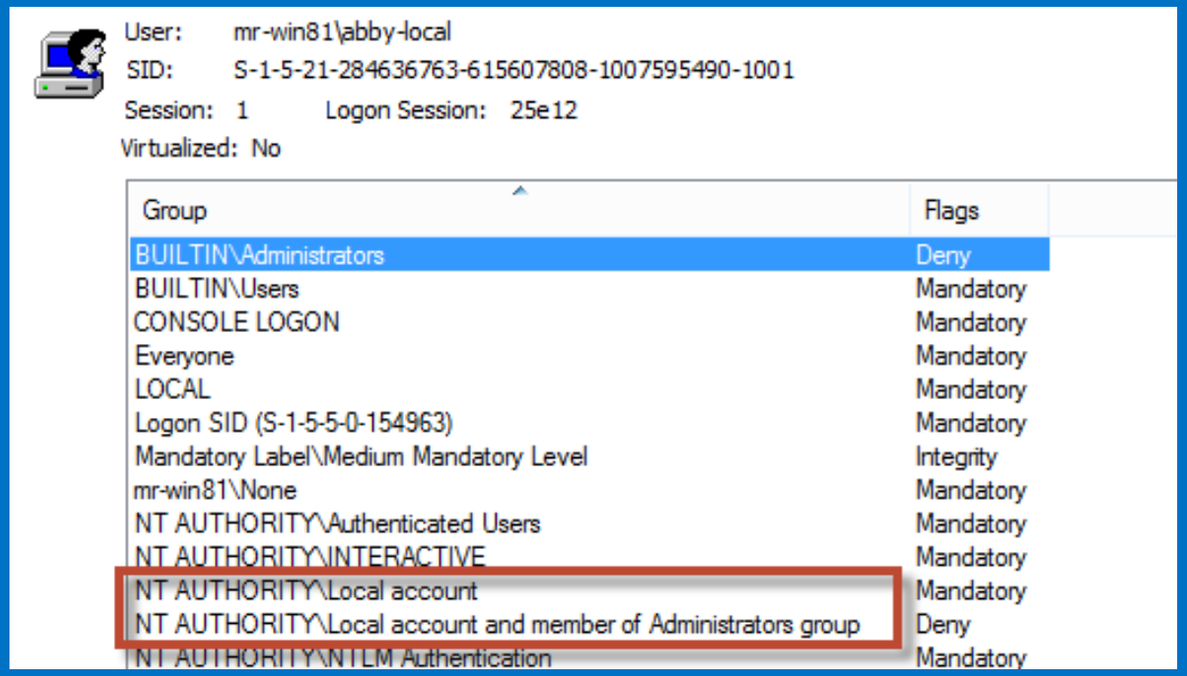
Other mitigation	Effectiveness	Effort required	Privilege escalation	Lateral movement
Disable the NTLM protocol	Minimal	High	-	-
Smart cards and multifactor authentication	Minimal	High	-	-
Jump servers	Minimal	High	√	-
Rebooting workstations and servers	Minimal	Low	-	-

- Microsoft published Pass-the-Hash guidance in December 2012.
- Highlighted best practices and dispelled urban legends



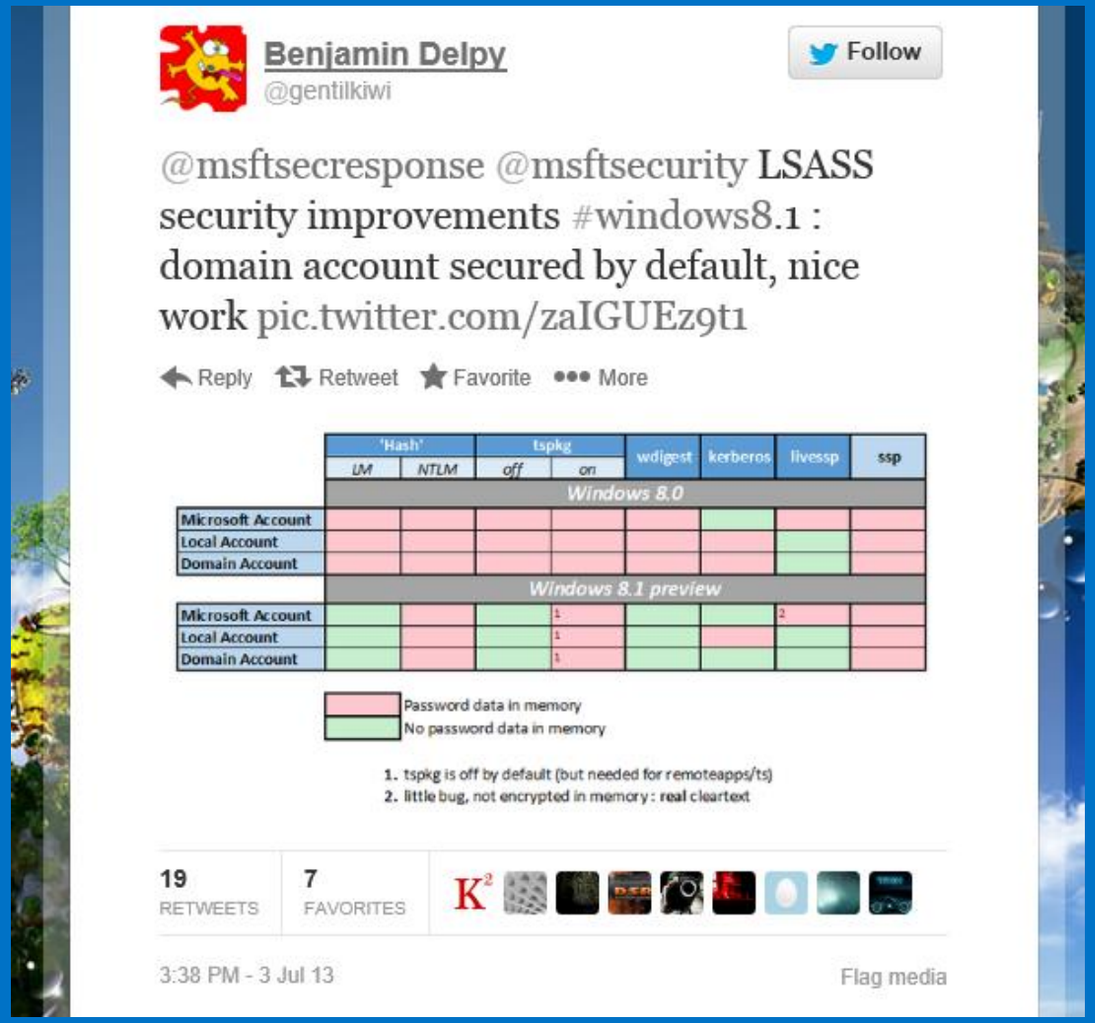
8.1 / 2012R2

Local Account Mitigations



- Two new well-known groups:
  - "Local account"
  - "Local account and member of Administrators group"
- Useful for restricting access

Domain Account Mitigations



Benjamin Delpy
@gentilkiwi

Follow

@msftsecresponse @msftsecurity LSASS security improvements #windows8.1 : domain account secured by default, nice work pic.twitter.com/zaIGUEz9t1

Reply Retweet Favorite More

	'Hash'		tspkg		wdigest	kerberos	livessp	ssp
	LM	NTLM	off	on				
	Windows 8.0							
Microsoft Account								
Local Account								
Domain Account								
	Windows 8.1 preview							
Microsoft Account				1			2	
Local Account				1				
Domain Account				1				

Password data in memory
No password data in memory

1. tspkg is off by default (but needed for remoteapps/ts)
2. little bug, not encrypted in memory : real cleartext

19 RETWEETS 7 FAVORITES

3:38 PM - 3 Jul 13 Flag media

- Reduced plaintext footprint
  - TSPKG
  - Wdigest
  - Kerberos
- LSASS Protected Mode

Additional Domain Account Mitigations

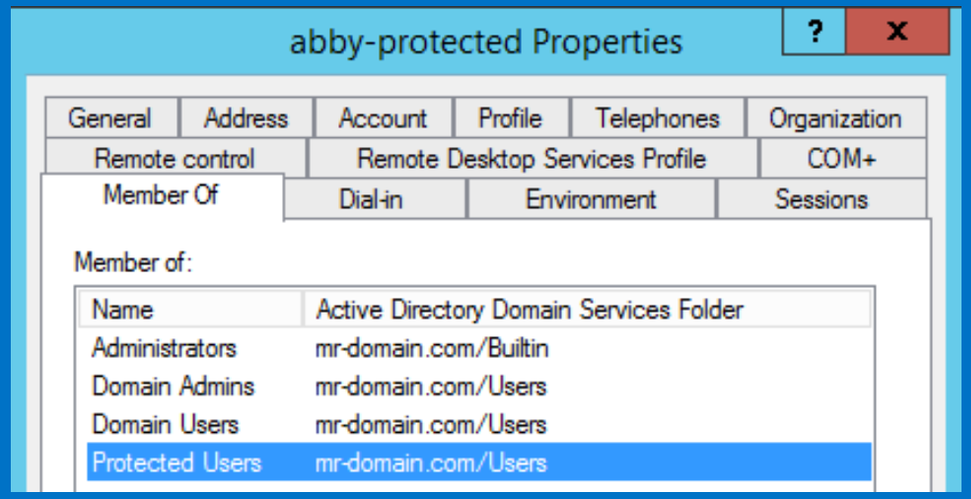
A secretary with no access to anything is phished. The attacker easily determines this but installs a kit to introduce malware that degrades performance. The secretary calls the help desk. Using smart card MFA, the help desk remotely connects to the secretary's machine. The malware captures the help desk hash. The attacker can then replay that hash on other machines, gradually gaining information on those machines. They can further capture the hashes on those systems and keep exploiting.

- US General Services Administration (GSA)

- Remote administration can expand exploits
  - RDP sends plaintext password to target
- New "restricted administration" mode sends no delegable credential

/restrictedAdmin -- Connects you to the remote PC or server in Restricted Administration mode. In this mode, credentials won't be sent to the remote PC or server, which can protect you if you connect to a PC that has been compromised. However, connections made from the remote PC might not be authenticated by other PCs and servers, which might impact app functionality and compatibility. Implies /admin.

Domain Protected Accounts



- Client hardening
  - Policy restrictions
  - NTLM hash discarded
- Domain hardening
  - NTLM authentication fails
  - Kerberos rejects weak ciphers
  - Kerberos limits ticket lifetime

Authentication Policies and Silos

- *Authentication Policies* constrain Kerberos ticket issuance
- Can configure conditions on users, computers or resources and ticket lifetime
- *Authentication Silos* enable isolation of accounts and resources that have constrained network scope
  - *Authentication Policies* are configured for users, computers and managed service accounts belonging to Silo
  - Silo member tokens include Silo claim

Conclusion

- Network security is the key to address the PtH

- Windows 8.1/2012R introduces some tools for limiting PtH
  - Local account protections
  - Domain account protections
  - Protected domain accounts
  - Authentication policies and Silos