

# SECURITY CASE STUDY 2014

## CYBERARK PRIVILEGED ACCOUNT SECURITY

Valery Milman



**CYBERARK®**

# Privileged Accounts are Targeted in All Advanced Attacks

---

*“Anything that involves  
serious intellectual property  
will be contained in highly secure  
systems and privileged accounts  
are the only way hackers can  
get in.”*

Avivah Litan, Vice President and Distinguished  
Analyst at Gartner



CYBERARK®  
SCS 2014

# Privileged Accounts are Targeted in All Advanced Attacks

---

*“...100% of breaches  
involved stolen credentials.”*

*“APT intruders...prefer to  
leverage privileged accounts  
where possible, such as Domain  
Administrators, service accounts  
with Domain privileges, local  
Administrator accounts, and  
privileged user accounts.”*

Mandiant, M-Trends and APT1 Report



**CYBERARK®**  
**SCS 2014**

# CyberArk Overview



## Trusted experts in privileged account security

- Over 1,500 *privileged account security* customers – it's all we do!



## Approach privileged accounts as a security challenge

- Designed and built from the ground up for security



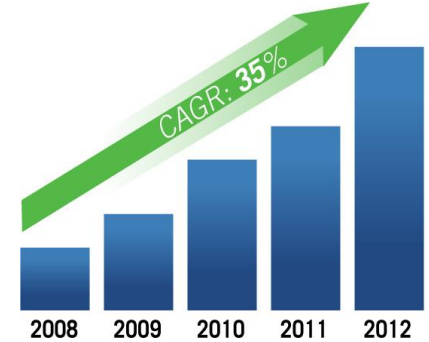
## Focus on solving business problems

- Privileged account security goes well beyond audit



## Only comprehensive privileged account security solution

- One solution, focused exclusively on privileged accounts
- Enterprise proven



Best Advanced Persistent Threat (APT) Protection

Excellence award finalist in the Best Security Company category SC 2013



# Privileged Accounts are everywhere



Shared Admin  
Accounts



Application to  
Application  
Accounts



Cloud  
Accounts

## Attack analysis – RSA SecureID attack

---

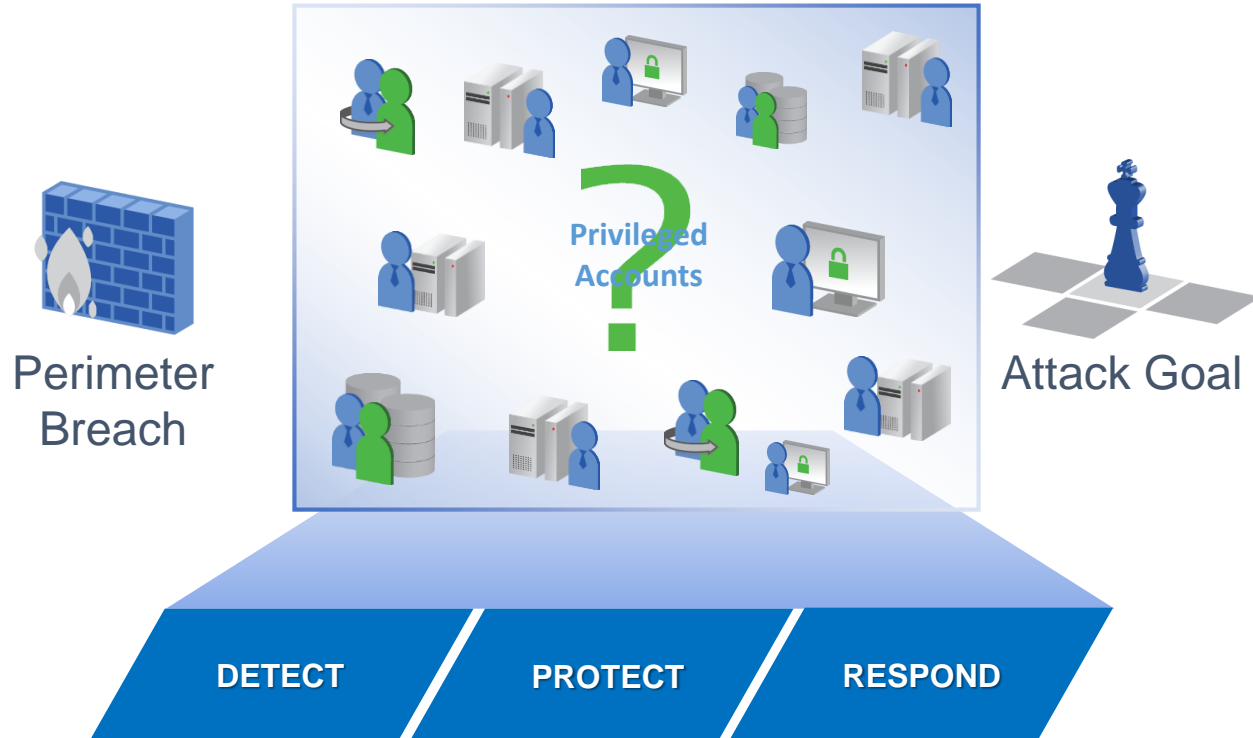
- 1) The attacker sent “phishing” e-mails with the subject line “2011 Recruitment Plan” to two small groups of employees over the course of two days.
- 2) One employee retrieved the message from his junk mail and opened the attached Excel file.
- 3) The spreadsheet contained malware that used a previously unknown, or “zero-day,” flaw in Adobe’s Flash software to install a backdoor.

## Attack analysis – RSA SecureID attack

---

- 3) After installing a stealthy tool that allowed the hacker to control the machine from afar, he stole several account passwords belonging to the employee and used them to gain entry into other systems.
- 4) From those systems the attacker could gain access to other employees with access to sensitive data.
- 5) Then came stage three: spiriting RSA files out of the company to a hacked machine at a hosting provider, and then on to the hacker himself.

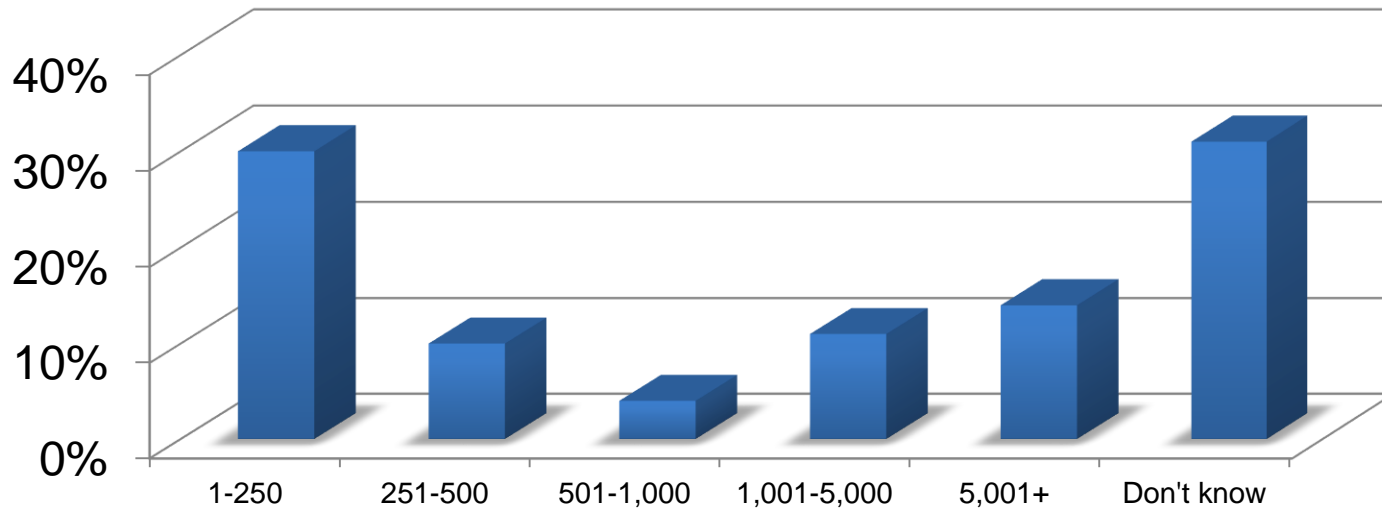
# Privileged Accounts are everywhere





## But That Fact is Not Well Understood

In Your Estimation, How Many Privileged Accounts Are There In Your Organization?



*Cyber-Privileged Account Security & Compliance Survey, May 2013 (Enterprise > 5000 Employees)*

# Where do your privilege accounts reside?



# Privileged Accounts are Targeted in All Advanced Attacks

alg-info@poczta.kbw.gov.pl - NULL - albert_k	735ec4b	1acac3ba6 - <bl	st-
les-dyr@poczta.kbw.gov.pl - NULL - czesław_ja	45034cc	22351edd37 - <bl	esław-
les-info@poczta.kbw.gov.pl - NULL - mikołaj_c	9d45034	1a22351edd37 - <	Mikołaj-
lom-dyr@poczta.kbw.gov.pl - NULL - jerzy_anto	449d694	a6cdcb7653c4 - <	erzy Antoni-
lub-slawomir. @poczta.kbw.gov.pl - NUI	- e02bc	5477419bc3e175df	wski - Sławomir-
lub-teresa.bi zta.kbw.gov.pl - NULL -	2247367	2193835fa39d59 -	esa-
marcin. l - NULL - damage - 098	27b4f6	lank> - <blank> -	
marcin. .pl - NULL - ml	586f426	<bl-ak> - <bl-ak>	
marcin. - NULL - illi - 21817ce	7f8 -	k> -	
mtorlow - tom - 9743a66f914cc24	lank> -		
nws-gra oczta.kbw.gov.pl - NULL	bb6a60c	1c56977e715c5b06	- Grażyna-
nws-jan oczta.kbw.gov.pl - NULL	689404b	ec61d30e00546211e	- Janusz-
ols-dyr2@poczta.kbw.gov.pl - NULL - izabela_s	0b30f42	9a06d579ca88 - <	cza - Izabela-
ols-dyr@poczta.kbw.gov.pl - NULL - walery_pis	7ed925e	4ebb08b6a - <bl	ery-
opo-dyr@poczta.kbw.gov.pl - NULL - rafal_tka	77d0c61	b3 - <blank> -	
ost-dyr@poczta.kbw.gov.pl - NULL - monika_bra	0e1be9f	d0a6f - <blank>	
pil-dyr@poczta.kbw.gov.pl - NULL - renata_ku	eebc504	f258cdd4 - <blar	a-
pio-dyr@poczta.kbw.gov.pl - NULL - grażyna_mu	bclafe4	3602f - <blank>	
pio-szym a@poczta.kbw.gov.pl - NULL - s	f2785d3	a1742eee2a21 - <	-
plo-dyr@poczta.kbw.gov.pl - NULL - joanna_gra	373cade	627b4f6 - <blan	
poz-dyr@poczta.kbw.gov.pl - NULL - marek_pud	0372cfc	cad2fe - <blank>	
poz-piot i@poczta.kbw.gov.pl - NULL - p	a2ed246	2b549bf1ac86 - <	-
prz-dyr@poczta.kbw.gov.pl - NULL - czesław_du	c60d6dc	8946 - <blank>	
rad-dyr@poczta.kbw.gov.pl - NULL - elżbieta_k	9d9fbfb	7e41d71c16 - <bl	pieta-
rad_dyr2@poczta.kbw.gov.pl - NULL - mirosław	4326646	66b4e7 - <blank> - Grzyb - Mirosław-	
rafal. @eo.pl - NULL - rkwa - e7060	52ad2	ank> - - Marcin-	
root@npc.pl - NULL - root - 8469f8e0f8c1e68e	ba7bd3d	- Super - Administrator-	
ryn-dyr@poczta.kbw.gov.pl - NULL - roman_ryn	2dacc90	94ed5c - <blank> - Ryniewicz - Roman-	
robert.k @poczta.kbw.gov.pl - NULL - robert_k	e9c630f	154a - <blank> - Bara - Robert-	



# Privileged Accounts are Targeted in All Advanced Attacks



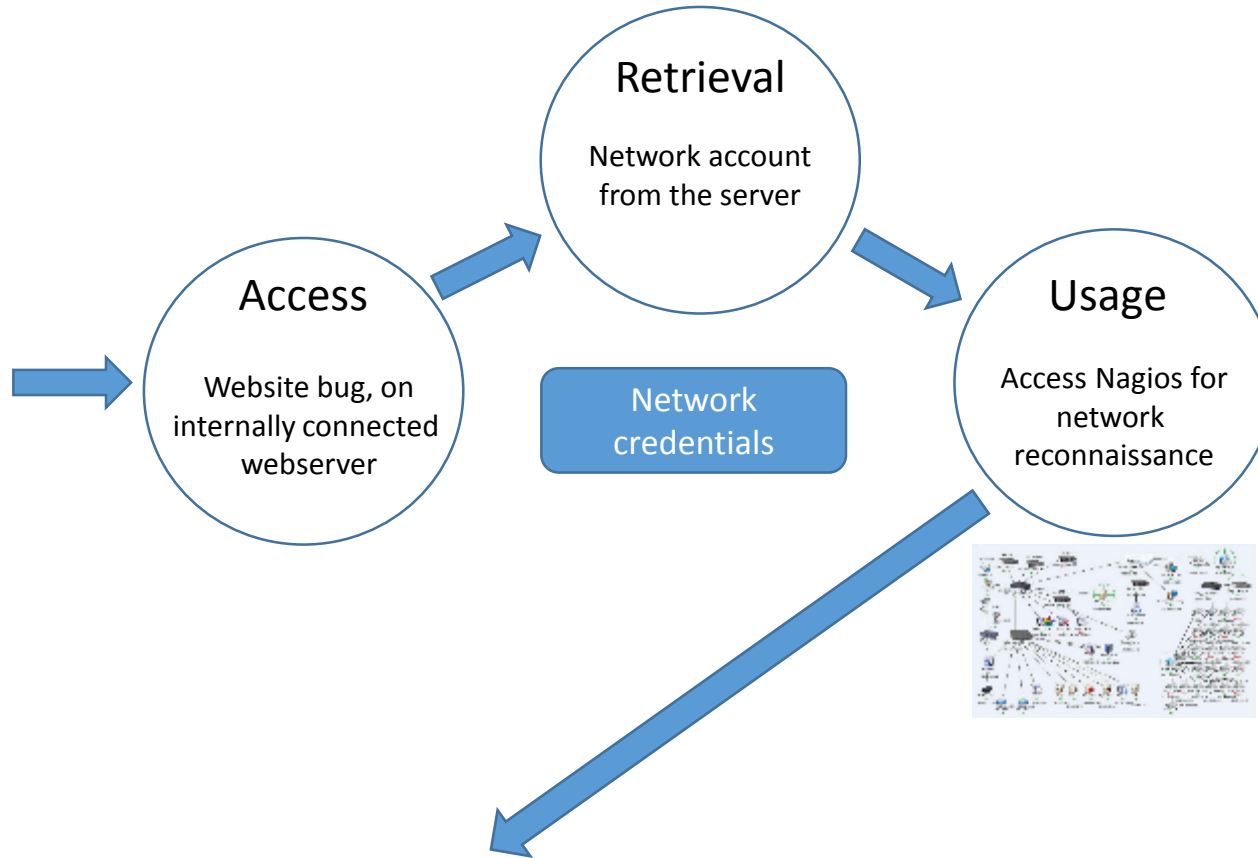
## Japan defence firm Mitsubishi Heavy Industries under Cyber Attack

Japan's top weapons maker has confirmed it was the victim of a cyber attack reportedly targeting data on missiles, submarines and nuclear power plants.

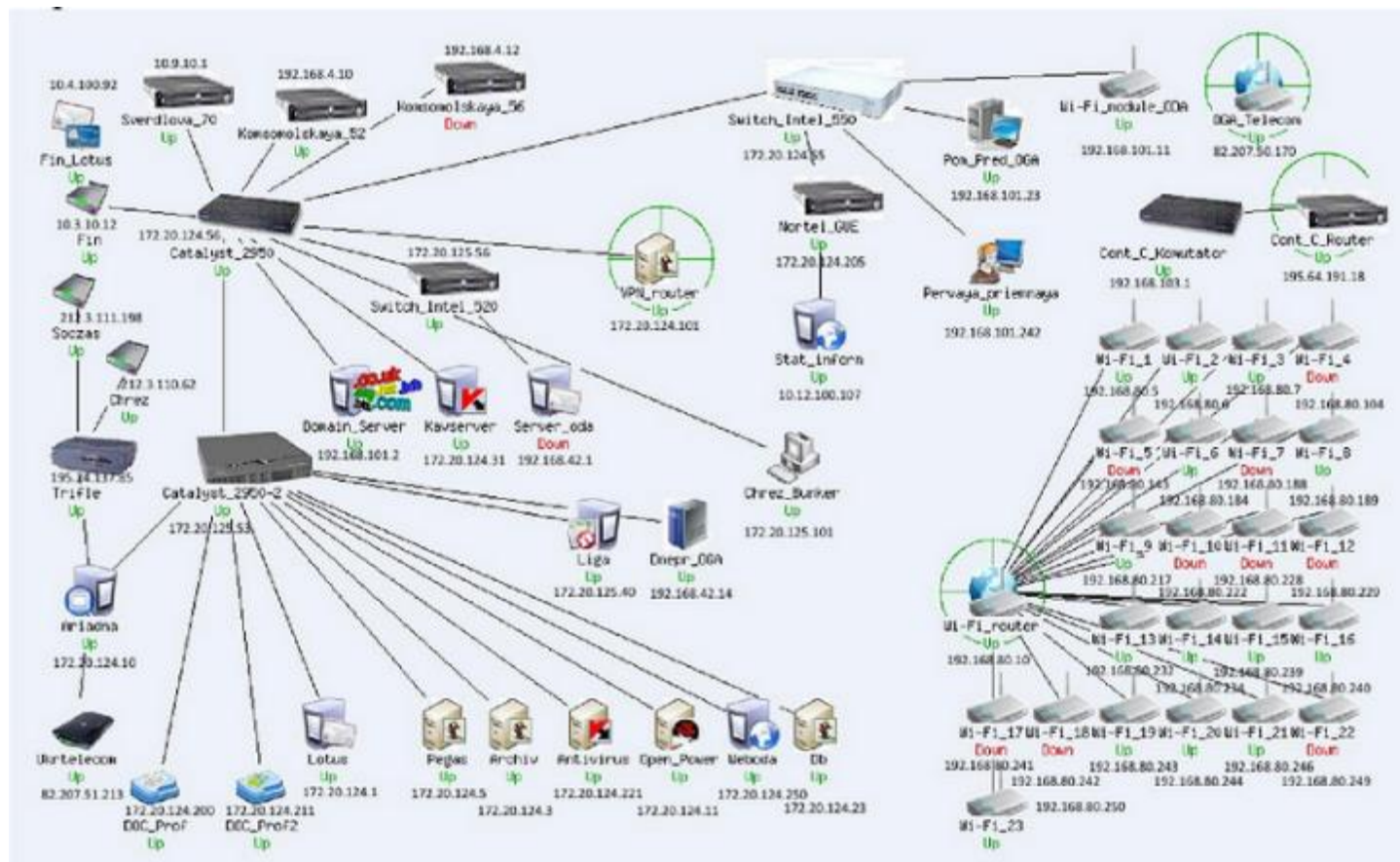
Mitsubishi Heavy Industries (MHI) said viruses were found on more than 80 of its servers and computers last month.

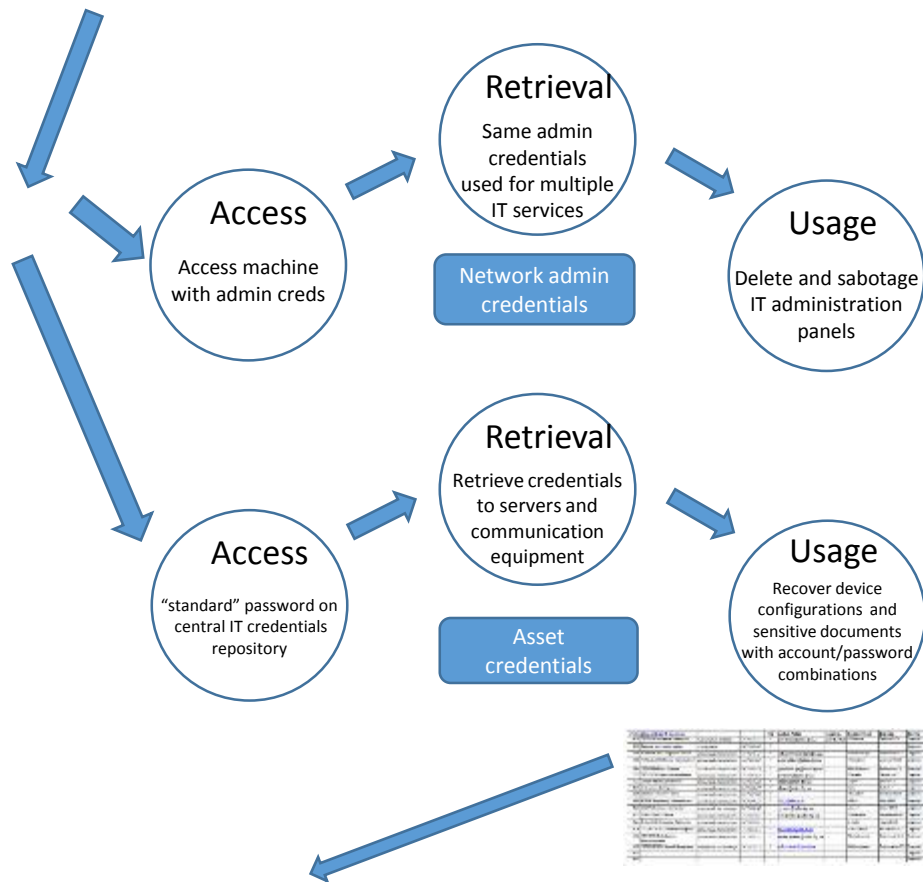


# Attack analysis – Dnepropetrovsk Governance



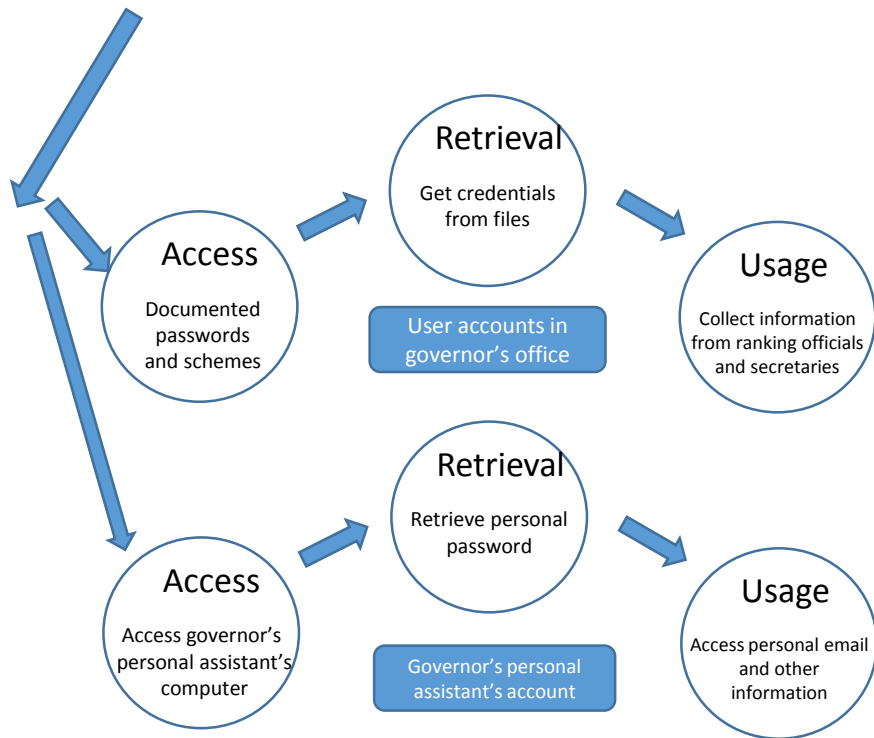
# Nagios - infrastructure monitoring map





Asset ID	Asset Name	Asset Type	Asset Location	Asset Status	Asset Owner	Asset Description	Asset Category	Asset Sub-category	Asset Value	Asset Risk	Asset Impact	Asset Mitigation
1	Server 1	Server	Room 101	Active	John Doe	Web Server	IT Infrastructure	Web Server	High	High	High	Regular updates
2	Server 2	Server	Room 102	Active	John Doe	Database Server	IT Infrastructure	Database Server	High	High	High	Regular updates
3	Server 3	Server	Room 103	Active	John Doe	File Server	IT Infrastructure	File Server	High	High	High	Regular updates
4	Server 4	Server	Room 104	Active	John Doe	Mail Server	IT Infrastructure	Mail Server	High	High	High	Regular updates
5	Server 5	Server	Room 105	Active	John Doe	Web Server	IT Infrastructure	Web Server	High	High	High	Regular updates
6	Server 6	Server	Room 106	Active	John Doe	Database Server	IT Infrastructure	Database Server	High	High	High	Regular updates
7	Server 7	Server	Room 107	Active	John Doe	File Server	IT Infrastructure	File Server	High	High	High	Regular updates
8	Server 8	Server	Room 108	Active	John Doe	Mail Server	IT Infrastructure	Mail Server	High	High	High	Regular updates
9	Server 9	Server	Room 109	Active	John Doe	Web Server	IT Infrastructure	Web Server	High	High	High	Regular updates
10	Server 10	Server	Room 110	Active	John Doe	Database Server	IT Infrastructure	Database Server	High	High	High	Regular updates





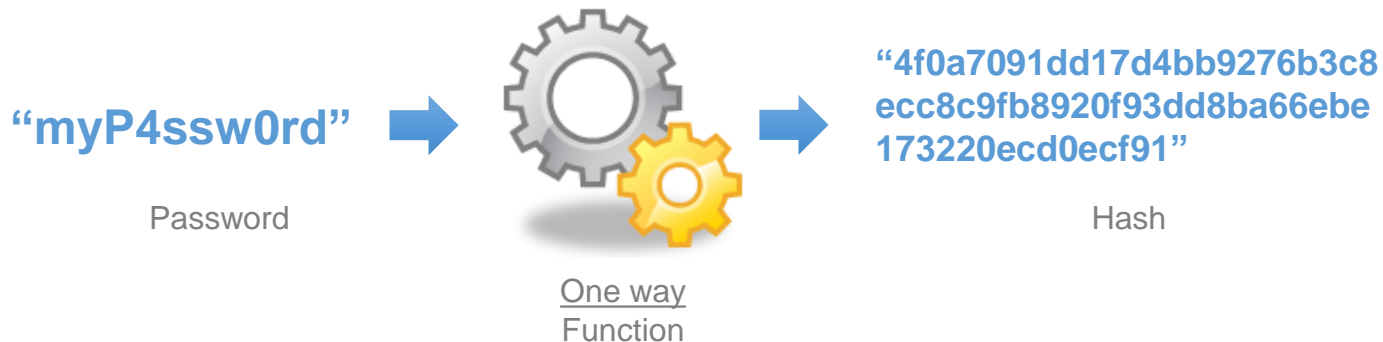




# Pass the Hash Attack On Privileged credentials

# Credentials – more than what you think...

- Forms of credentials
  - Passwords
  - Biometric identification
  - Magnetic tape on credit cards
  - ...*and more*
  - **Password hashes!**
    - Designed to protect the account password from being exposed
    - BUT...can also assist an attacker in gaining privileged access to your most sensitive assets

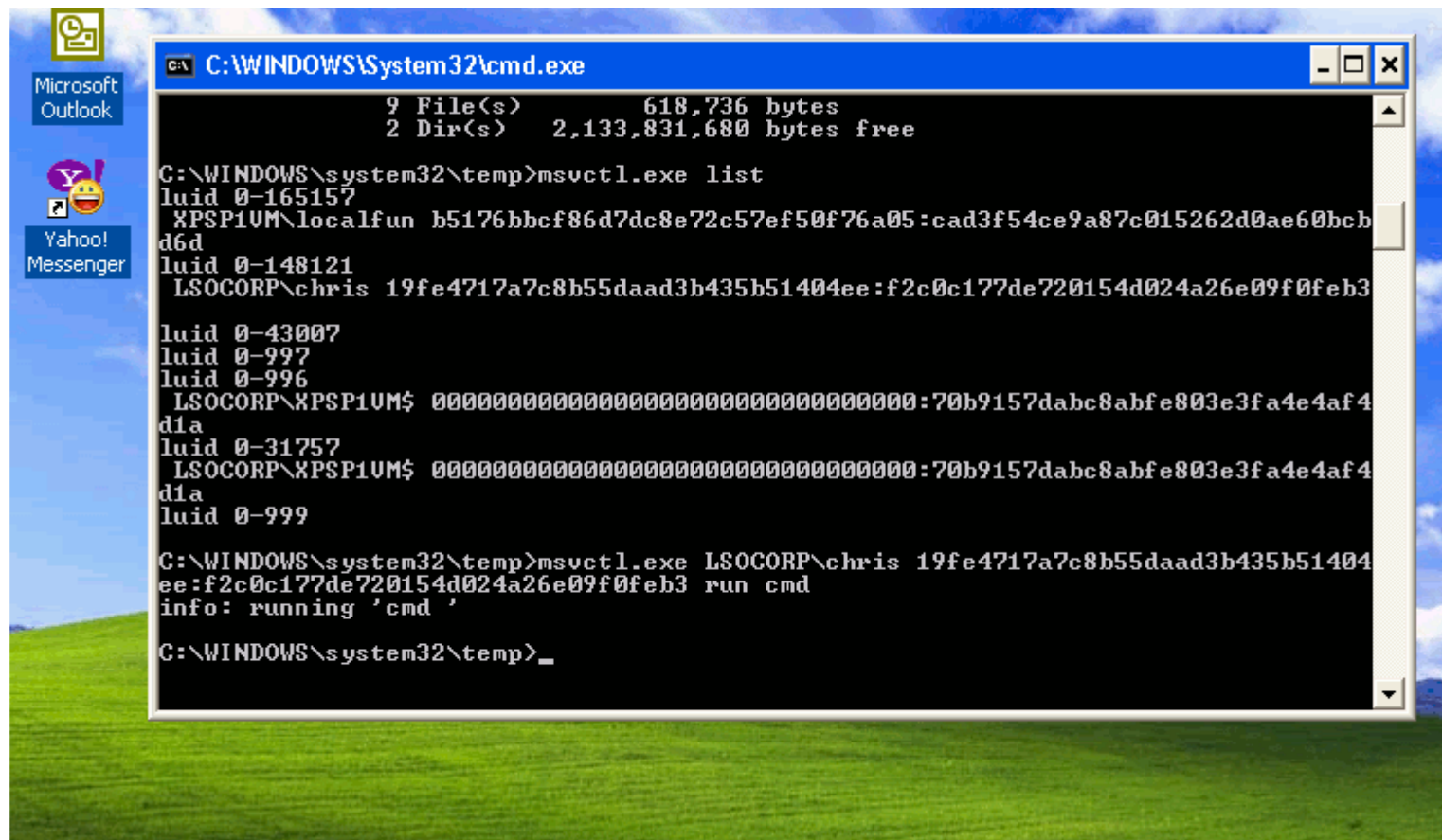


# Pass-the-Hash (PtH) – a form of Credential Theft

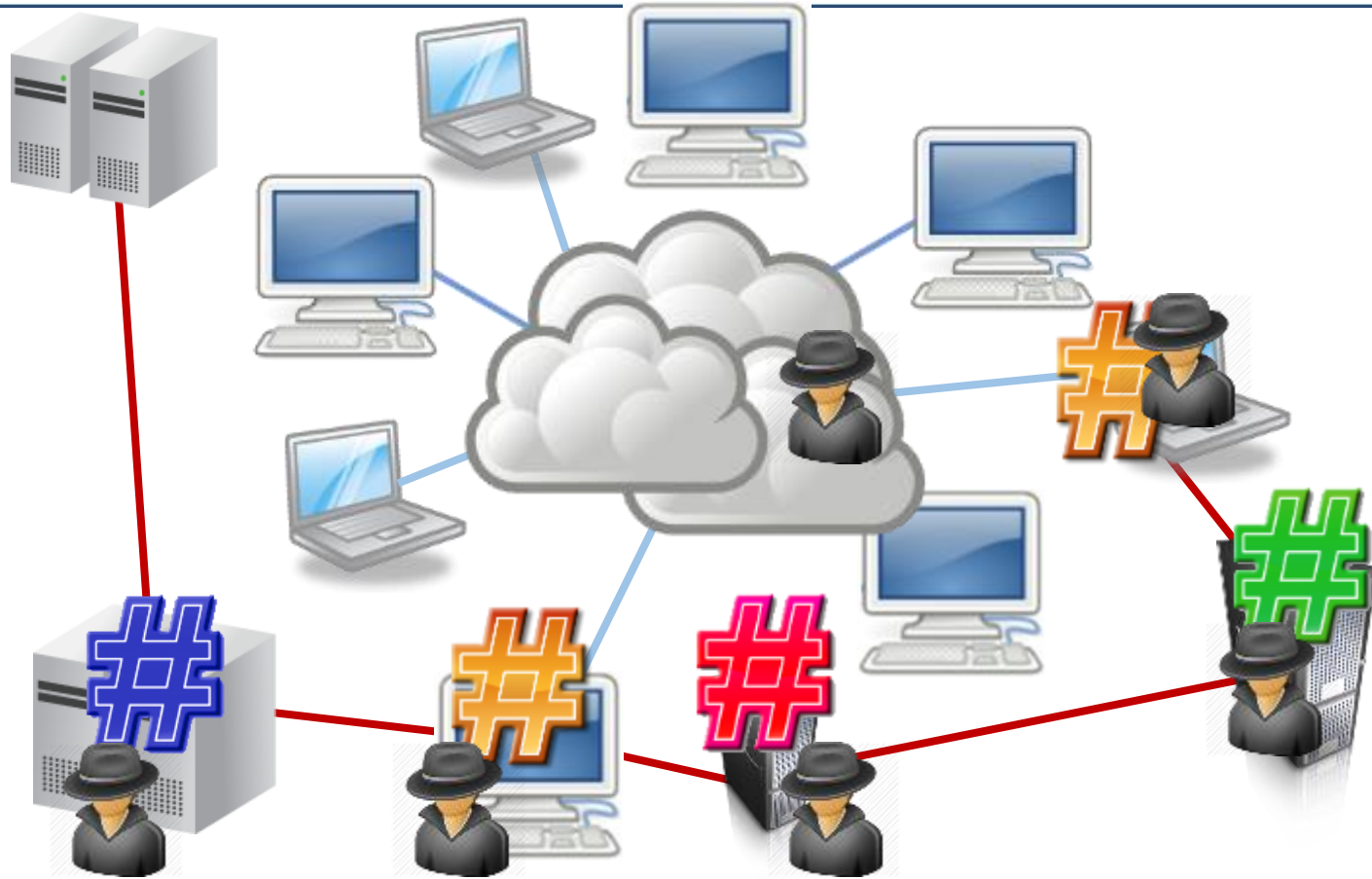
---

- First published in 1997. Has been a beloved toy by attackers since 2008. Widely covered during 2013.
- **A by-design flaw** in Windows.  
Microsoft: “We can’t mitigate”.
- How simple is it to leverage an attack?

# Pass-the-Hash (PtH) – a form of Credential Theft



# Pass-the-Hash – how does it really work?



# CyberArk - Solving The Privileged Account Security Problem

## Threats

- Advanced Threat
- Insider Threats
- Securing the Hybrid Cloud
- Securing Application Credentials
- Securing Shared Admin Accounts
- Sharing Sensitive Information

## Audit and Compliance

- Control & Accountability for Privileged Users
- Monitor & Record Privileged Activity
- Compliance Reporting
- Remote User Access Control
- Auditing Secure File Transfer

## Industrial Controls/SCADA

- Securing and Monitoring Shared Admin Accounts for ICS Systems
- Controlling and Monitoring Remote Vendors
- Smart Grid Security



Contact us for more information:  
<http://www.cyberark.com/contact/>