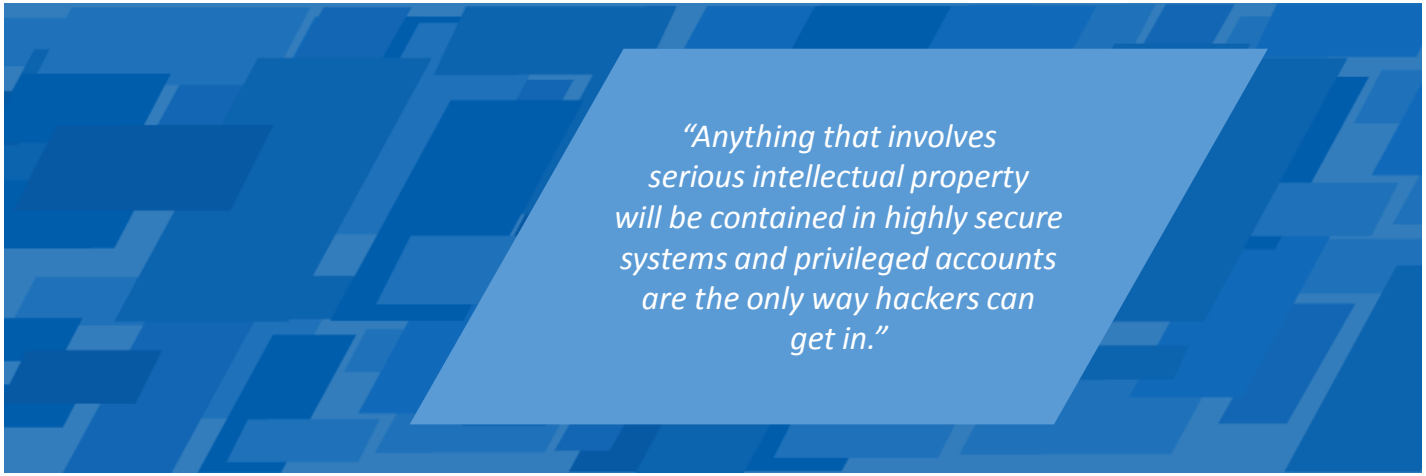
SECURITY CASE STUDY 2014

CYBERARK PRIVILEGED ACCOUNT SECURITY

Valery Milman

CYBERARK®

Privileged Accounts are Targeted in All Advanced Attacks



Avivah Litan, Vice President and Distinguished Analyst at Gartner

CYBERARK
SCS 2014

Privileged Accounts are Targeted in All Advanced Attacks

Mandiant, M-Trends and APT1 Report

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

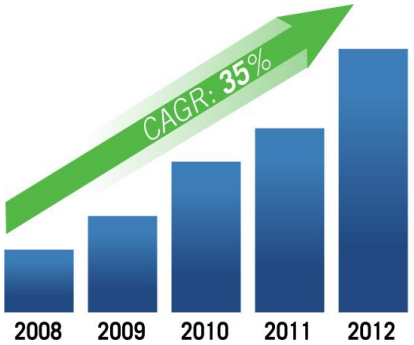
- Privileged account security goes well beyond audit

Only comprehensive privileged account security solution

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

World-class Customers

Deutsche Bank · NOVARTIS · QUALCOMM · BARCLAYS · Williams · McKESSON (Empowering Healthcare) · ING DIRECT · BT · FannieMae. · BRAUN



SC MAGAZINE AWARDS 2012 EUROPE WINNER

SC MAGAZINE AWARDS 2014 Europe WINNER

Best Advanced Persistent Threat (APT) Protection

Excellence award finalist in the Best Security Company category SC 2013

2010 Computing Security Awards — Presented By: Network computing & Computing Security

Privileged Accounts are everywhere

CYBERARK
SCS 2014

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.

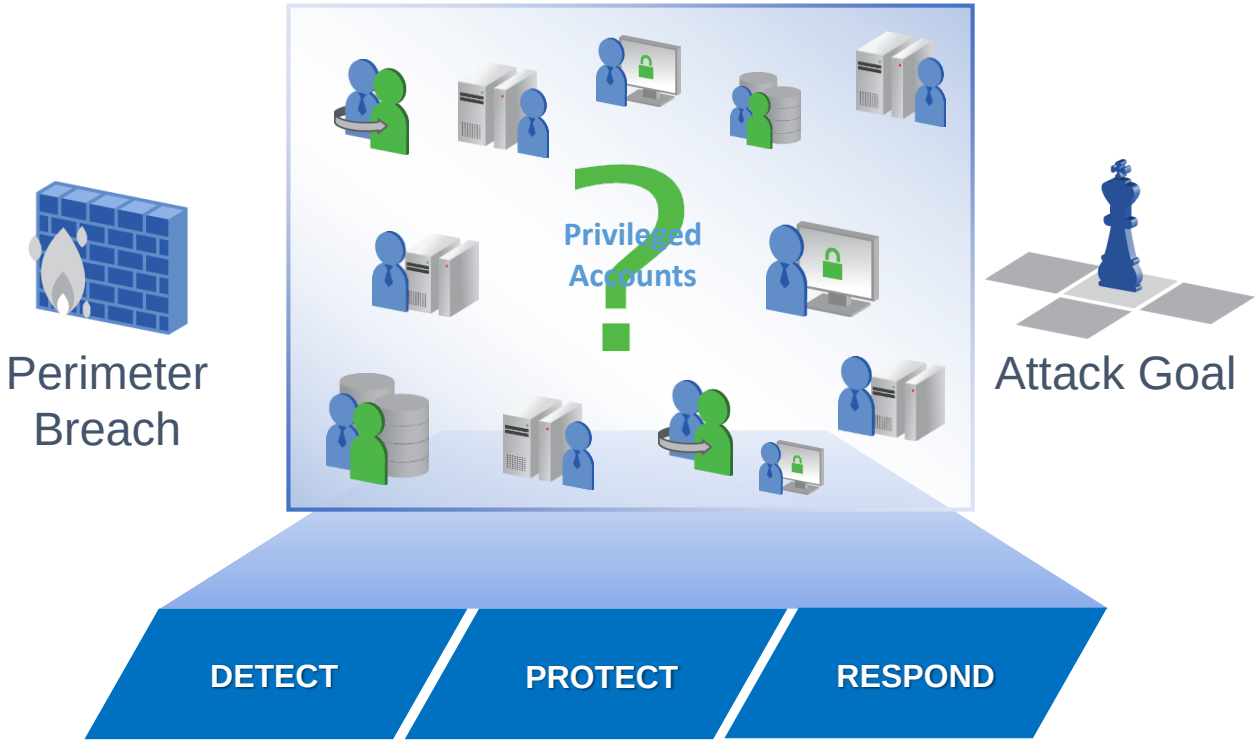
4) From those systems the attacker could gain access to other employees with access to sensitive data.

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.

CYBERARK

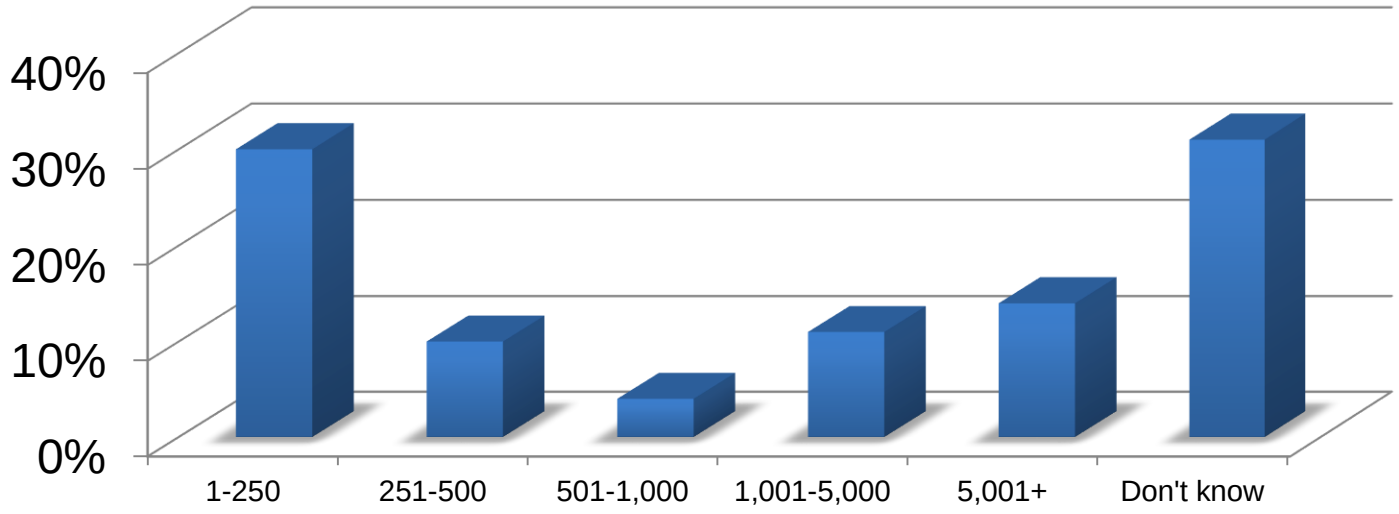
SCS 2014

Privileged Accounts are everywhere



But That Fact is Not Well Understood

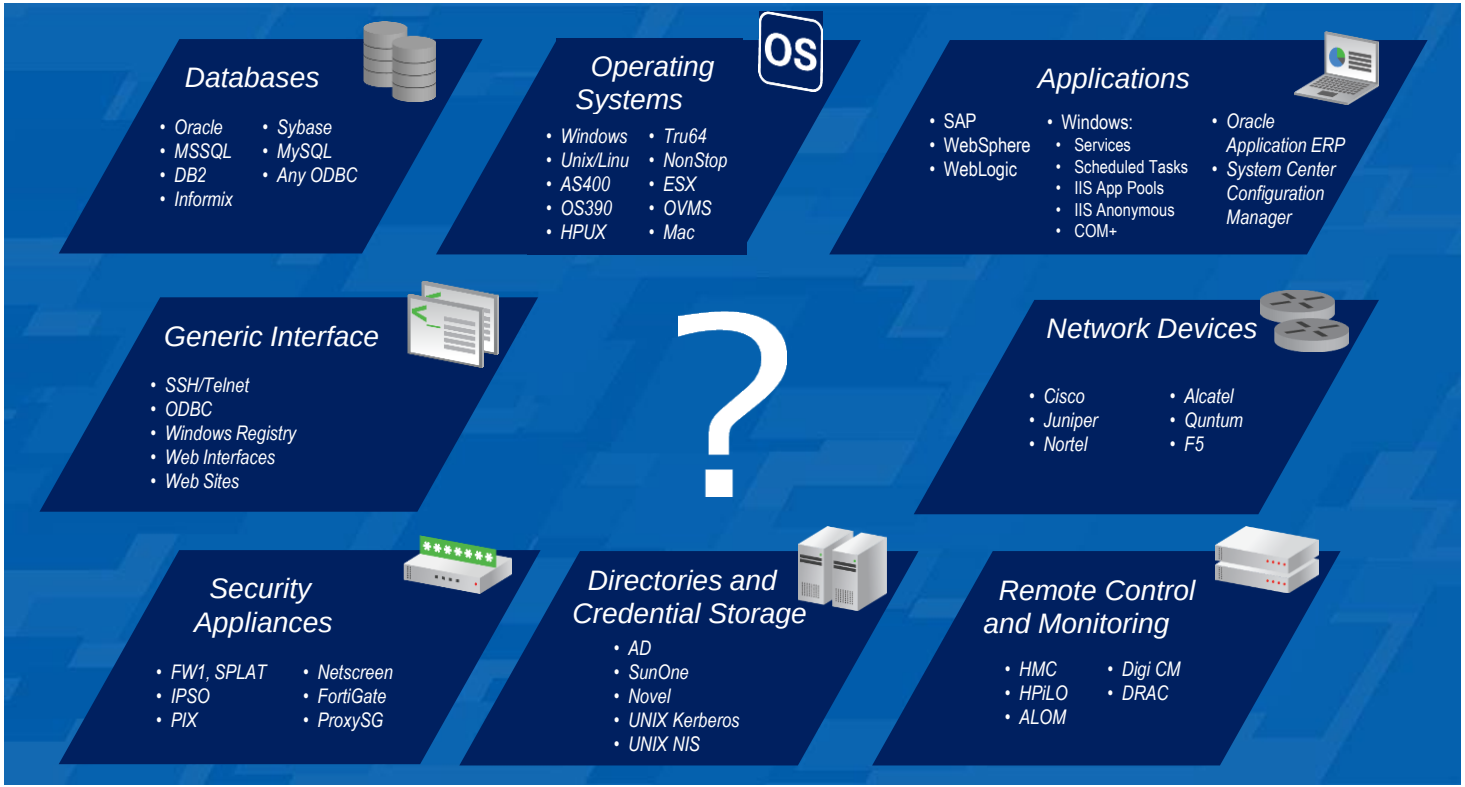
In Your Estimation, How Many Privileged Accounts Are There In Your Organization?



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

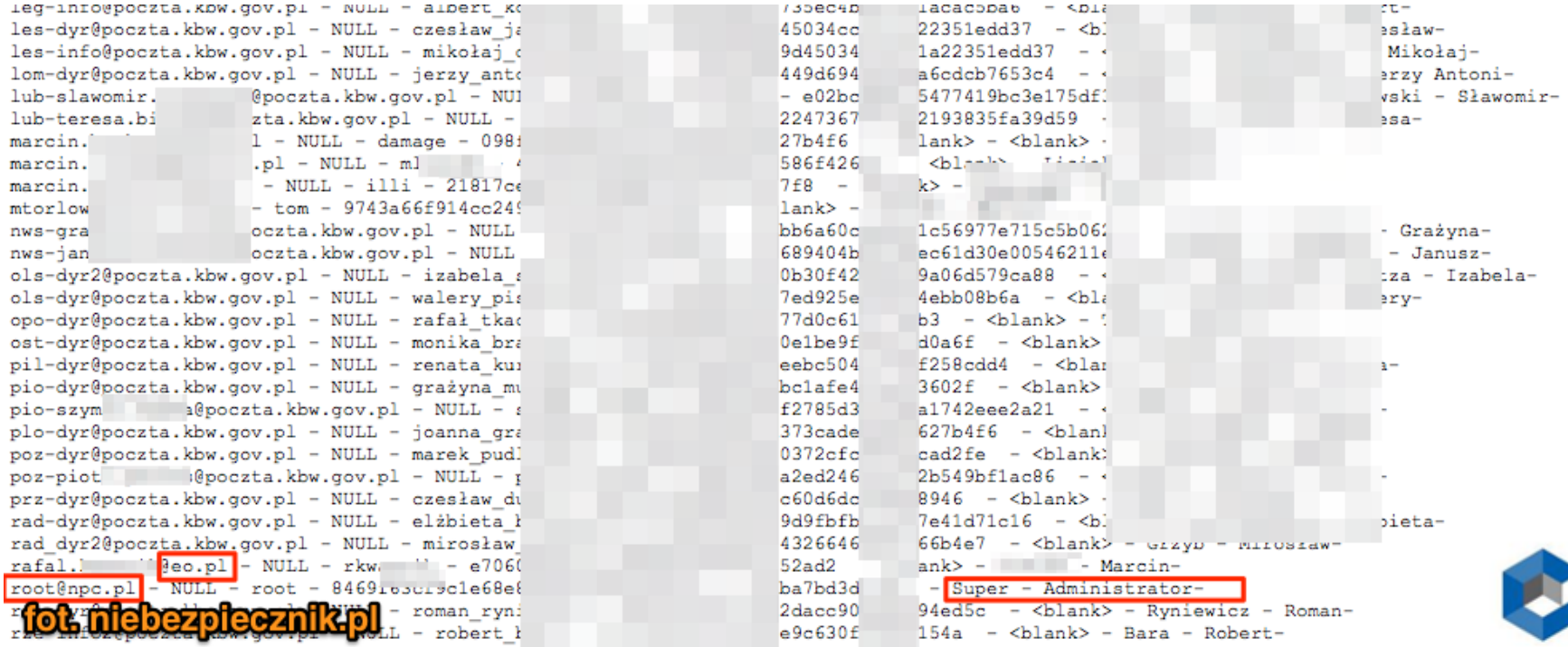
CYBERARK
SCS 2014

Where do your privilege accounts reside?



CYBERARK
SCS 2014

Privileged Accounts are Targeted in All Advanced Attacks



CYBERARK
SCS 2014

Privileged Accounts are Targeted in All Advanced Attacks

BBC News Sport Weather Earth Future Shop TV Radio More... Search

NEWS ASIA-PACIFIC

Home | UK | Africa | Asia | Australia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Environment | Tech | Entertainment | Video

Share

Japan defence firm Mitsubishi Heavy Industries under Cyber Attack

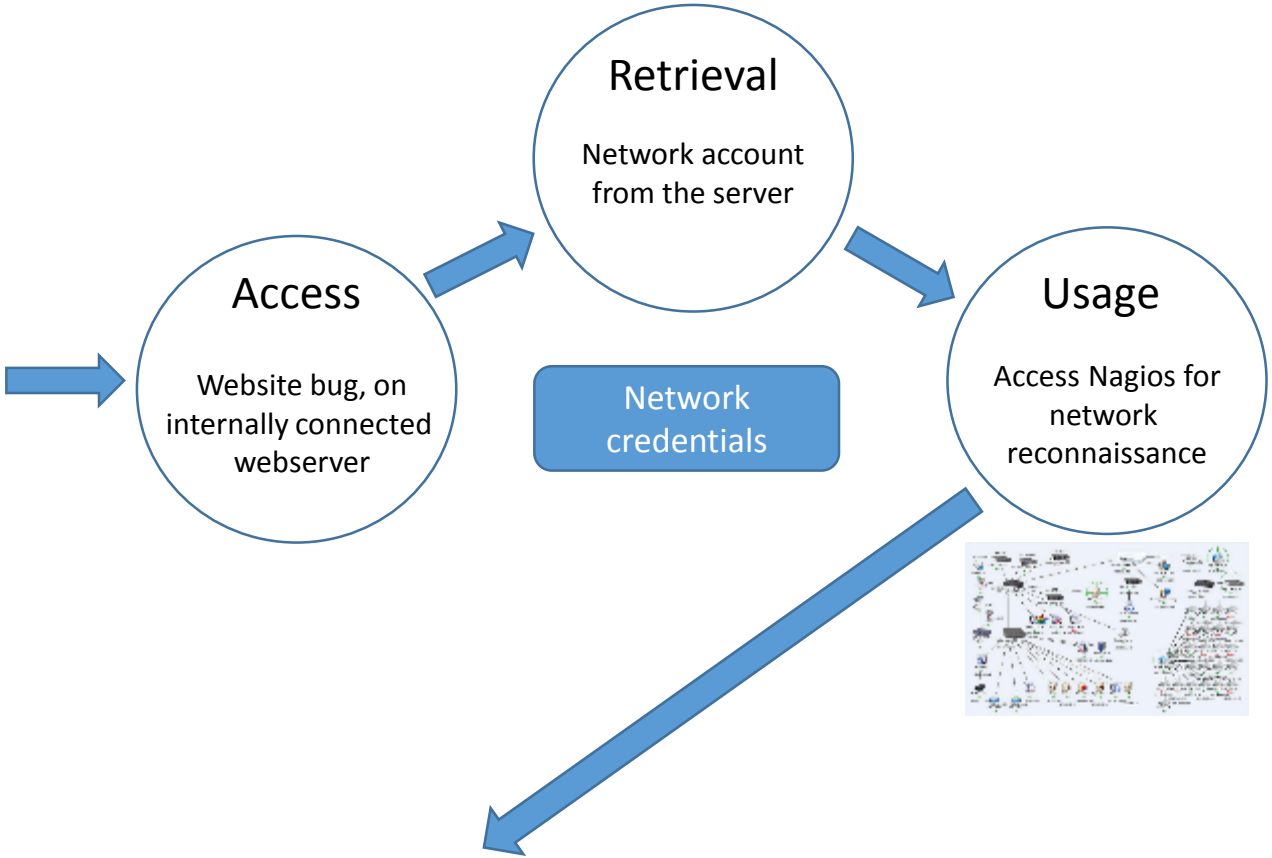
Japan's top weapons maker has confirmed it was the victim of a cyber attack reportedly targeting data on missiles, submarines and nuclear power plants.

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

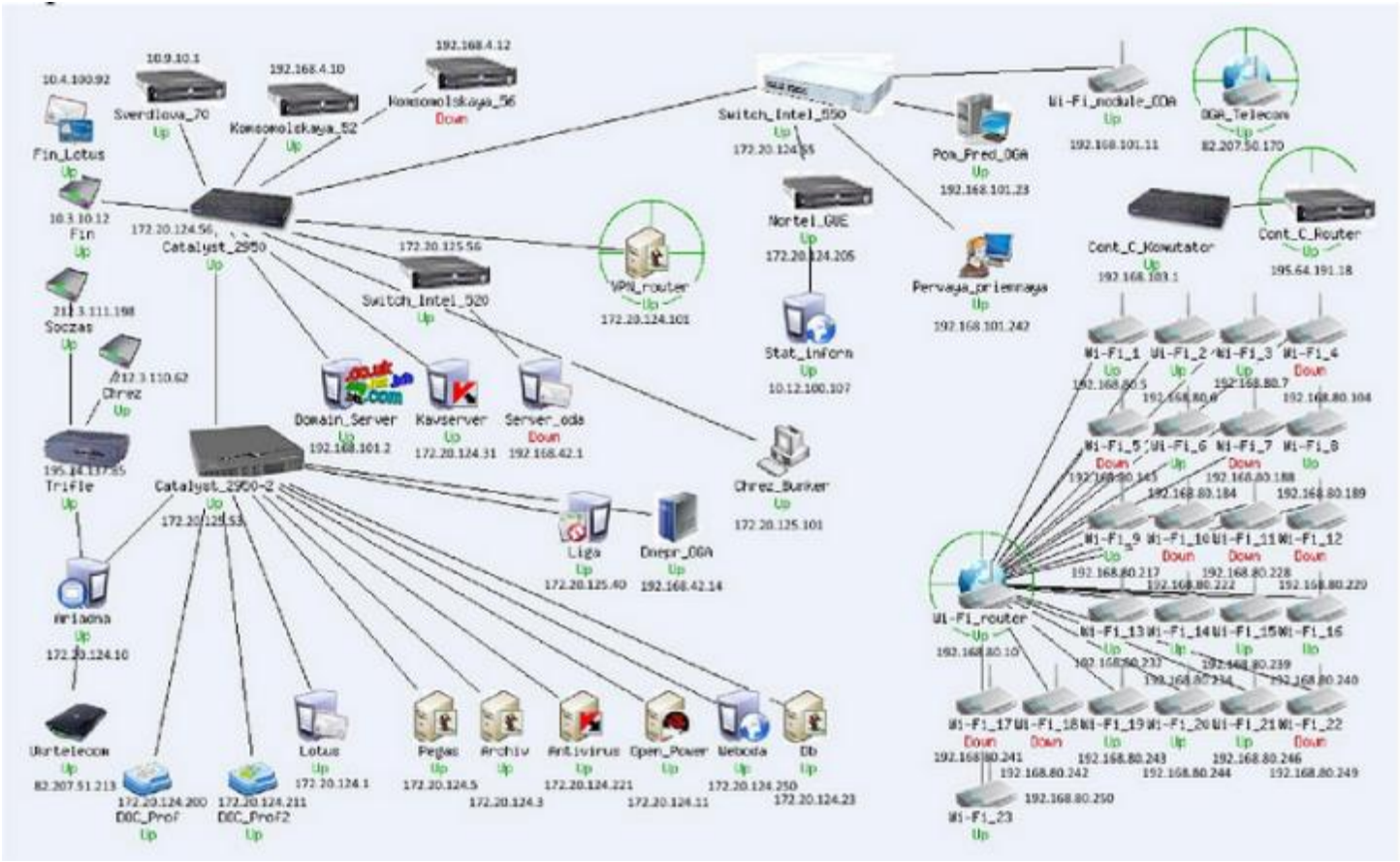
CYBERARK

SCS 2014

Attack analysis – Dnepropetrovsk Governance

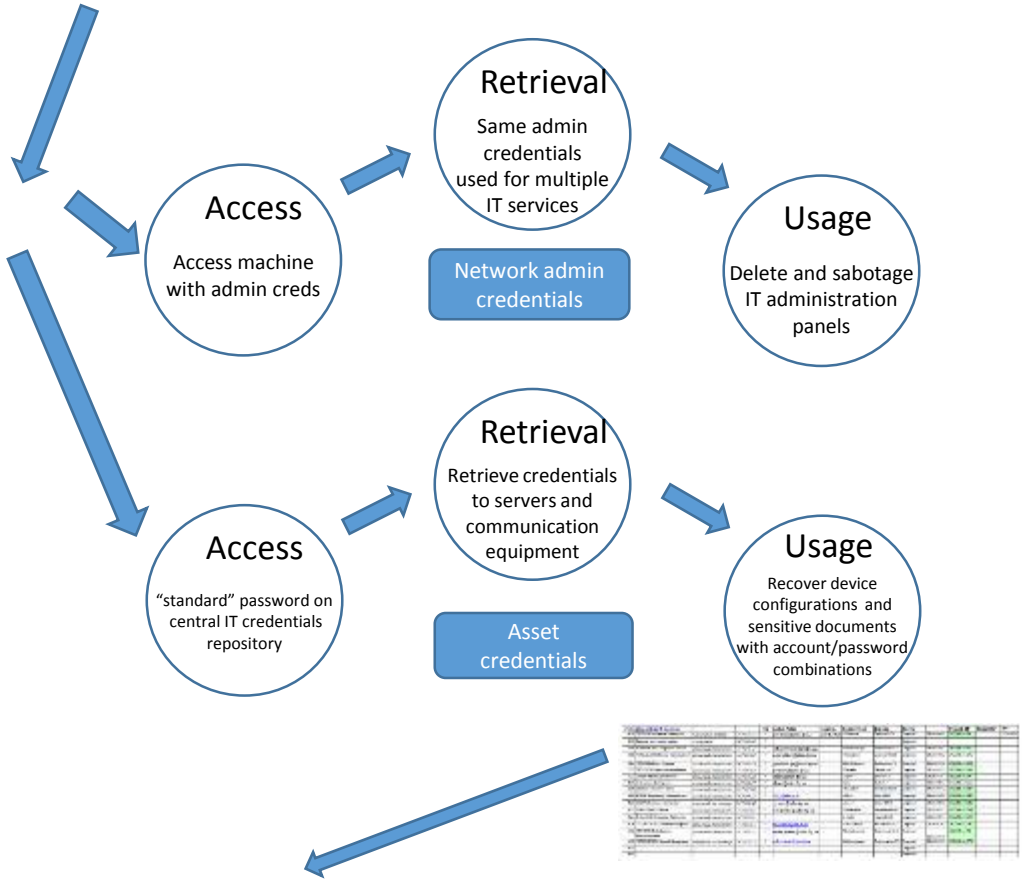


Nagios - infrastructure monitoring map



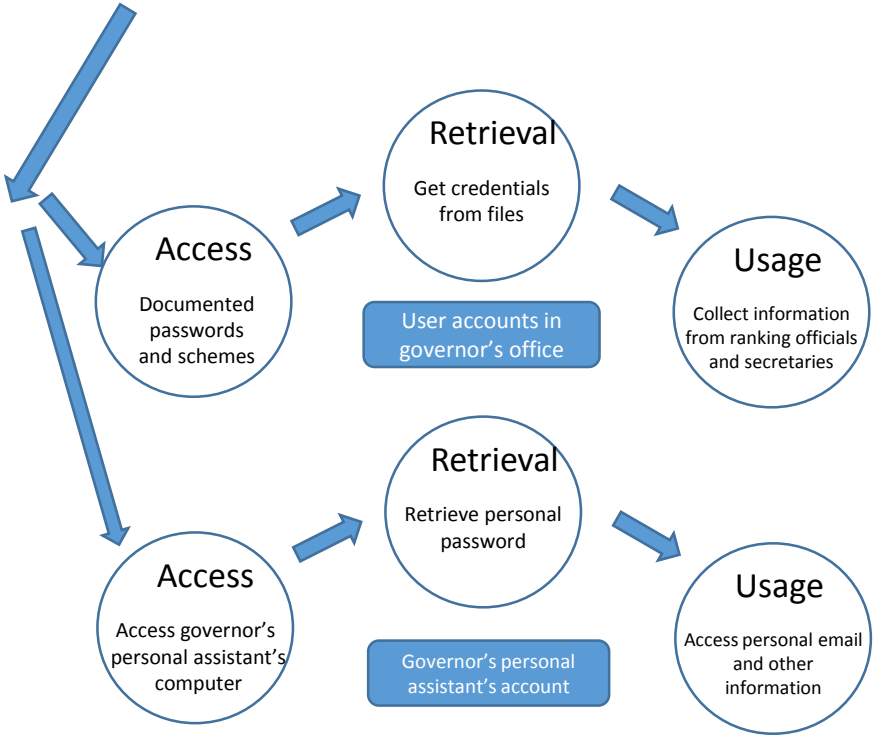
CYBERARK
SCS 2014

Cont.



CYBERARK
SCS 2014

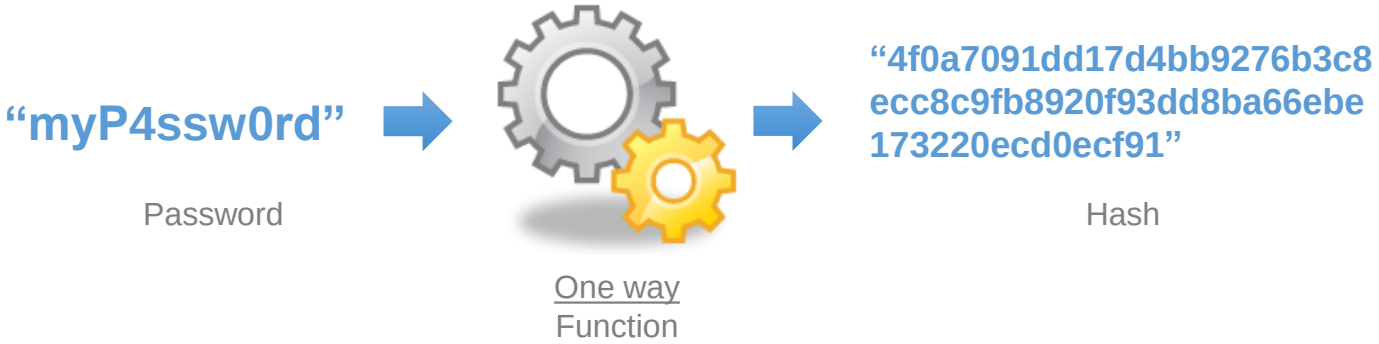
Cont.



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



CYBERARK
SCS 2014

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.

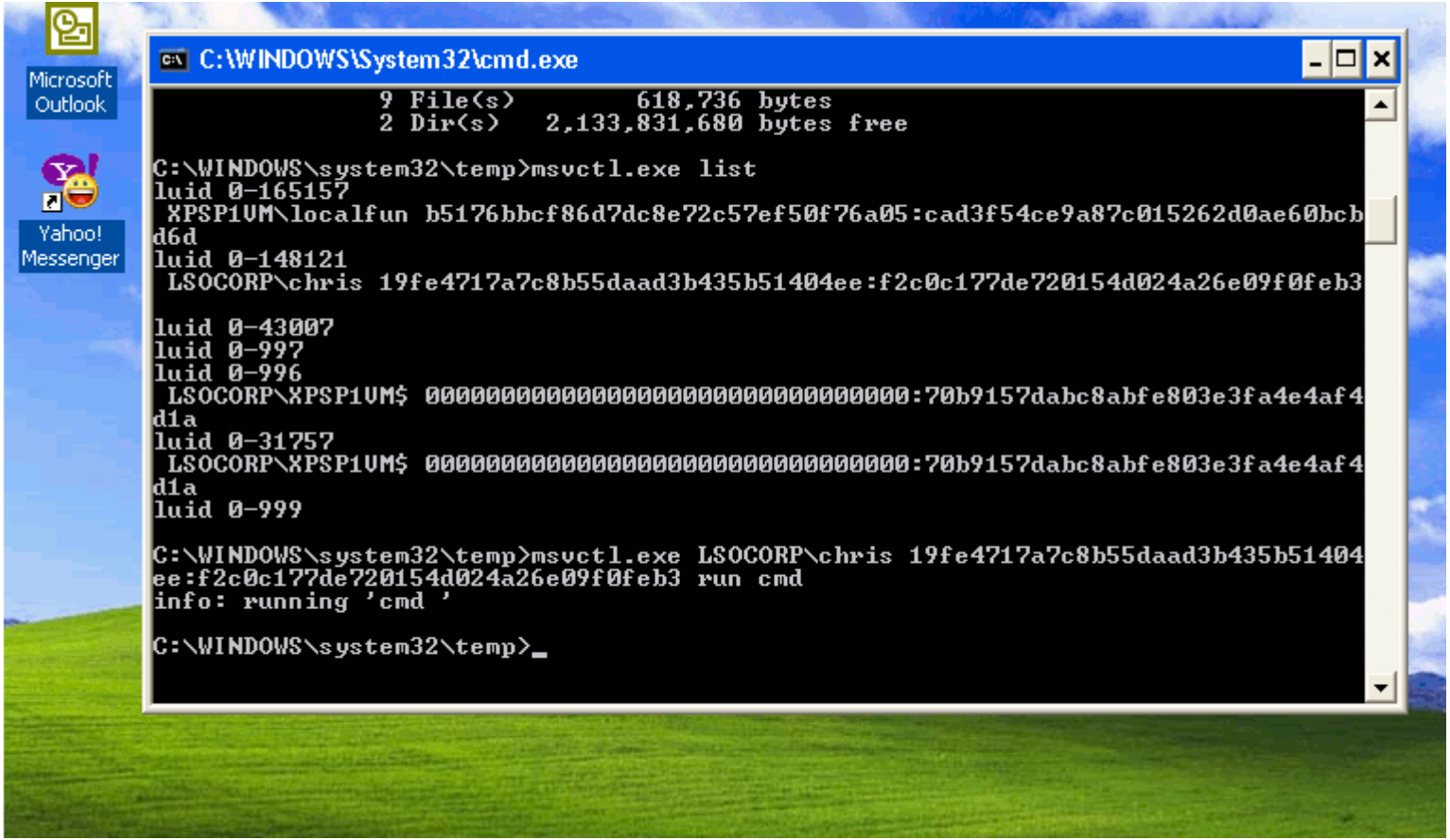
- **A by-design flaw** in Windows.
  Microsoft: “We can’t mitigate”.

- How simple is it to leverage an attack?

CYBERARK

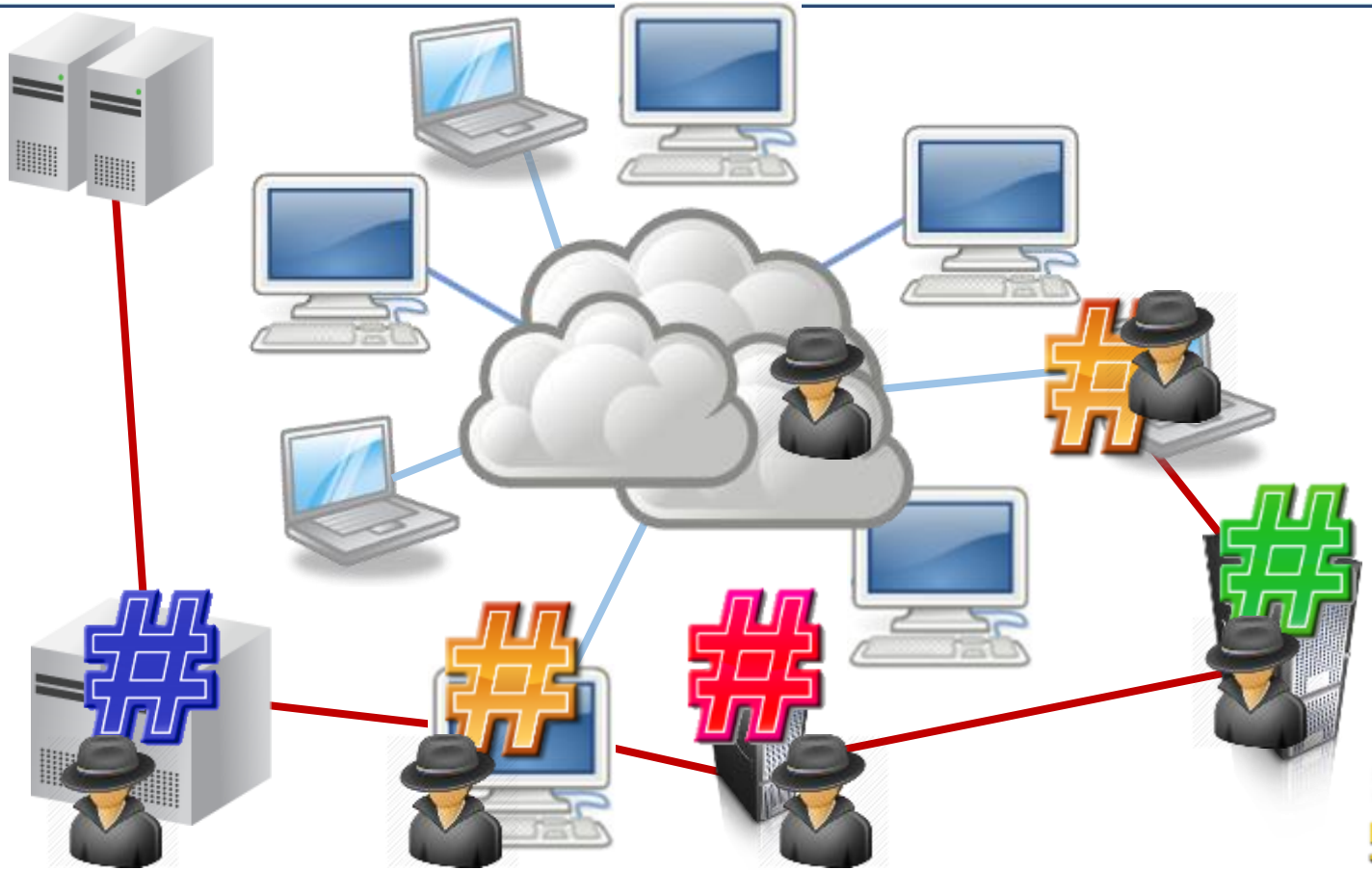
SCS 2014

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



CYBERARK
SCS 2014

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



CYBERARK
SCS 2014

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

CYBERARK
SCS 2014

Contact us for more information:

http://www.cyberark.com/contact/

Valery Milman

Valery.Milman@Cyberark.com