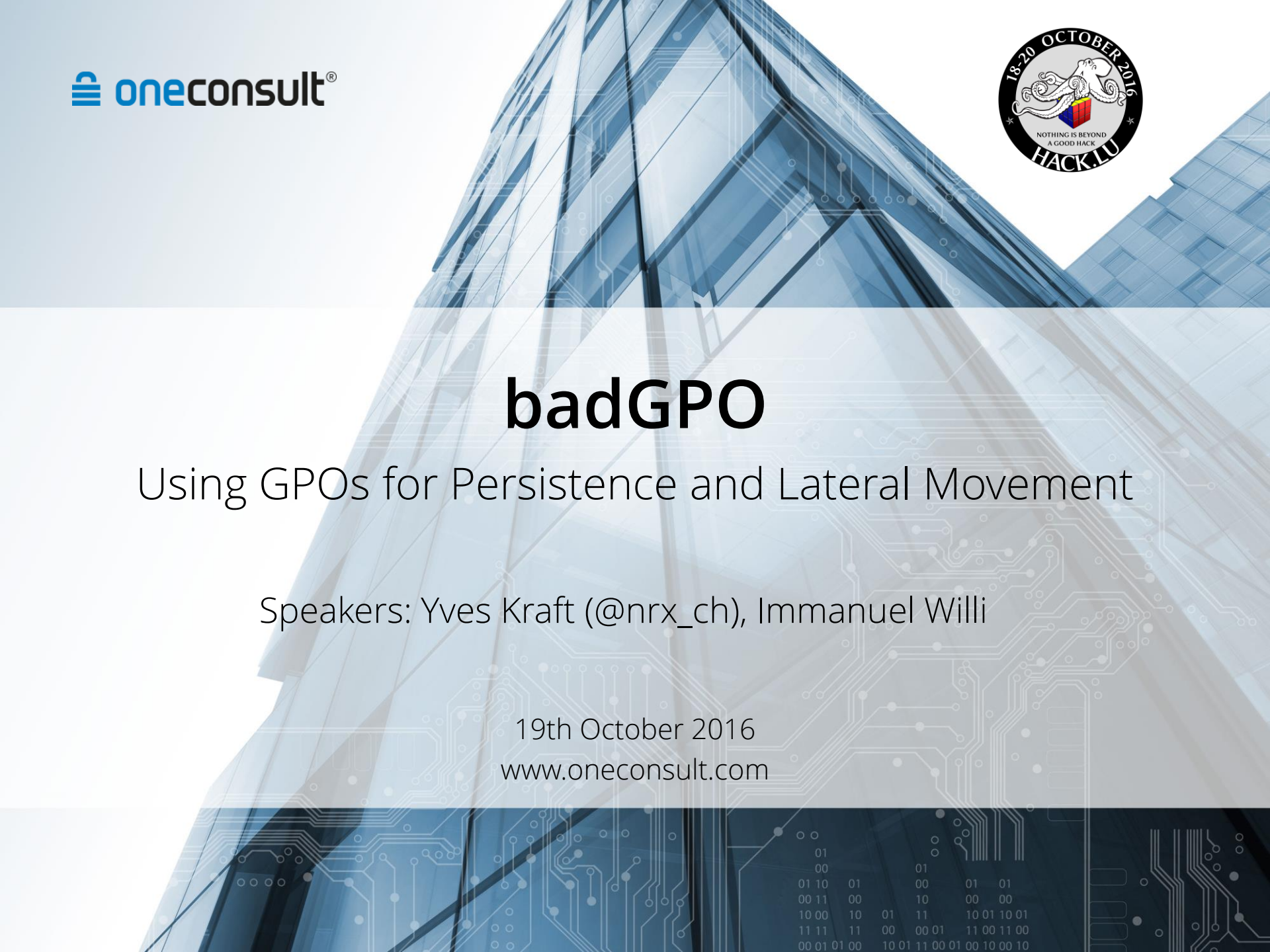


badGPO

Using GPOs for Persistence and Lateral Movement

Speakers: Yves Kraft (@nrx_ch), Immanuel Willi

19th October 2016

www.oneconsult.com

GOAL

To create awareness

or...

to give you neat ideas!

AGENDA

- Introduction
- Malicious Group Policies
- Countermeasures
- Future Work

HOW IT STARTED

- Remote Management [Line 565]
  […]
  5) GPO
  If all those protocols are disabled or blocked by the firewall, once you're Domain Admin, you can use GPO to give users a login script, install an msi, execute a scheduled task [13], or, like we'll see with the computer of Mauro Romeo (one of Hacking Team's sysadmins), use GPO to enable WMI and open the firewall.

- Persistence [Line 726]
  To hack companies, persistence isn't needed since companies never sleep. I always use Duqu 2 style "persistence", executing in RAM on a couple high-uptime servers.

Source: https://ghostbin.com/paste/6kho7

THOUGHTS ABOUT PHINEAS FISHERS WRITE-UP

- Initial idea
  - Create a POC that uses group policies (GPOs) to distribute malware in a sneaky way to gain persistence in an automated manner.
- Initial goal
  - Infect (a subset of) domain joined systems using a backdoor in memory of high uptime servers.
- Steps to take
  - Create or inject into an existing GPO
    - Set Run/RunOnce registry key
  - Link GPO to domain/organizational unit
  - Wait for incoming connections ☺

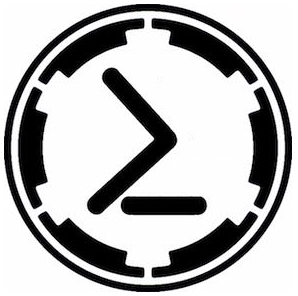
INTRODUCTION TO GROUP POLICIES

- Group Policy provides the centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment:
  - Administrative templates
  - Security settings
  - Software installation
  - Scripts
  - Remote Installation Services
  - Internet Explorer maintenance
  - Folder redirection

INTRODUCTION TO GROUP POLICIES

- GPOs tend to get messy
  - Stored all over the place
  - Naming conventions
  - Grown historically
  - Not decommissioned
- Hard to read
- Problems with privileges

POWERSHELL EMPIRE

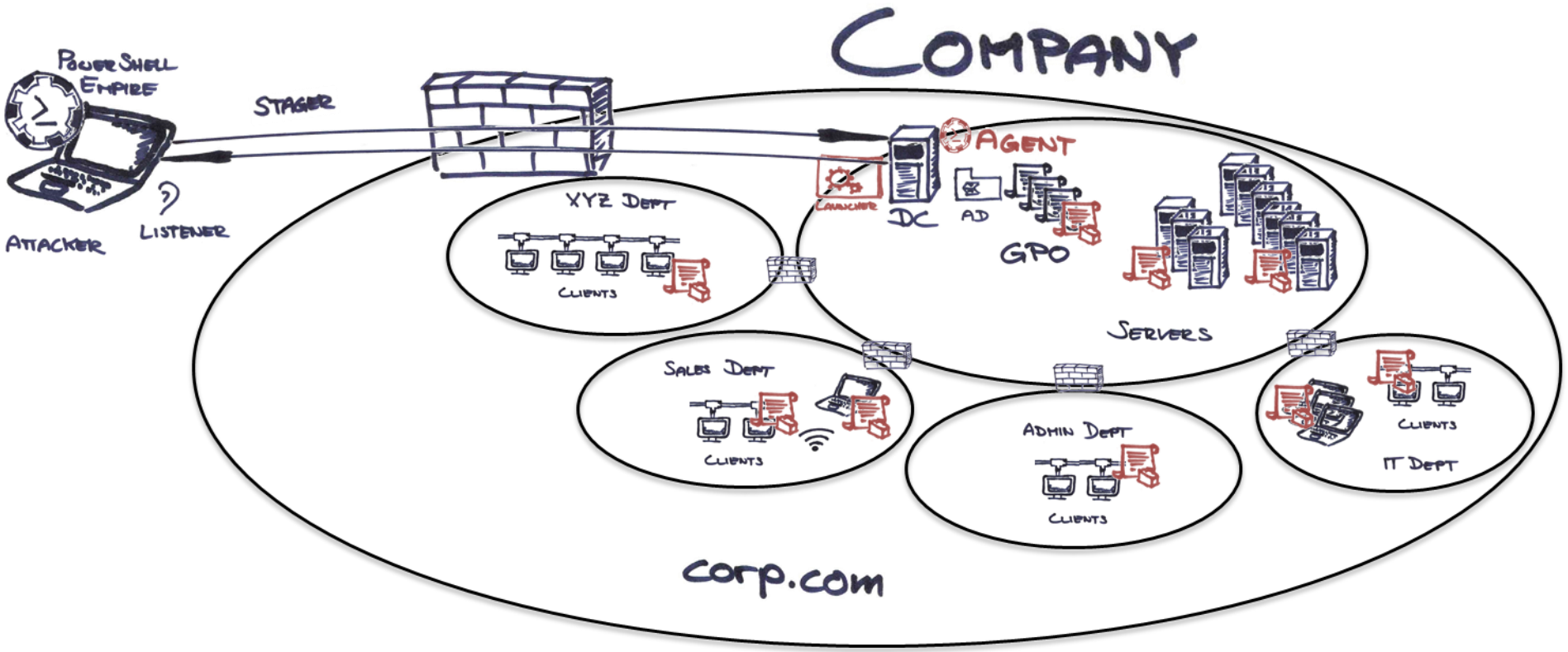


- Framework
  - Pure PowerShell post-exploitation framework
  - Cryptologically-secure communications
  - Module based post-exploitation

- Small forensic footprint
  - Runs in memory
  - Runs on PowerShell (Windows standard application)

- Web:
  - http://www.powershellempire.com
  - https://github.com/adaptivethreat/Empire

MALICIOUS GROUP POLICY ATTACK SCENARIO

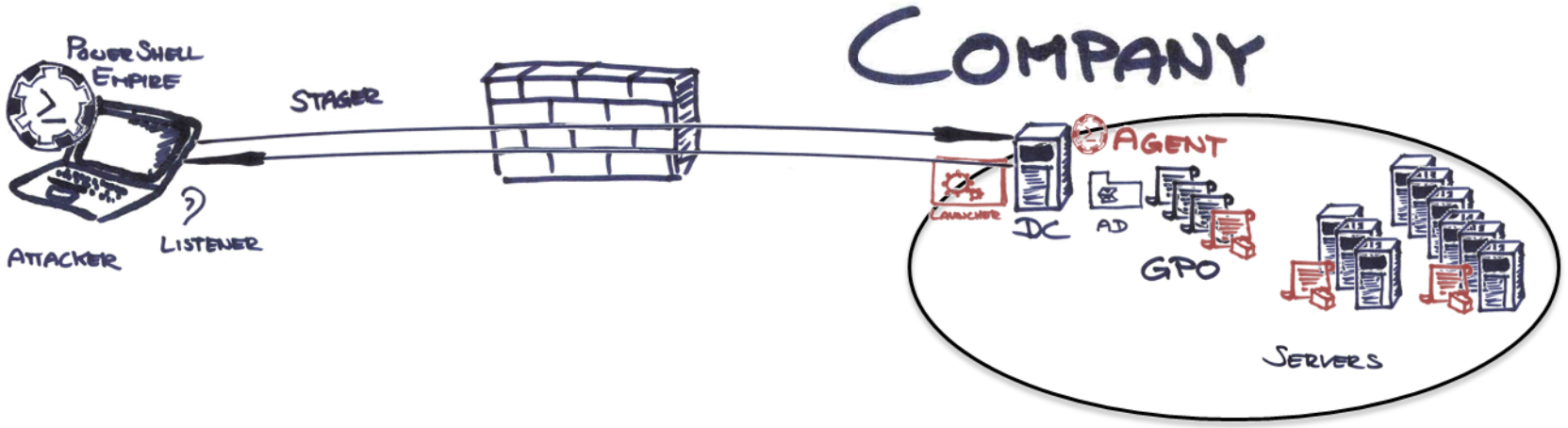


MALICIOUS GROUP POLICY ATTACK SCENARIO - DEMO TIME

- Goal
  - **Get persistence**

- Approach
  - Create a new GPO (Module: `set_GpRegistryValue`)
    - Set a “run once” registry key
  - Link GPO to domain corp.com
  - Enjoy backdoor

MALICIOUS GROUP POLICY ATTACK SCENARIO



“Get the file called proof.txt on one of the servers. Good luck!”

MALICIOUS GROUP POLICY ATTACK SCENARIO - DEMO TIME

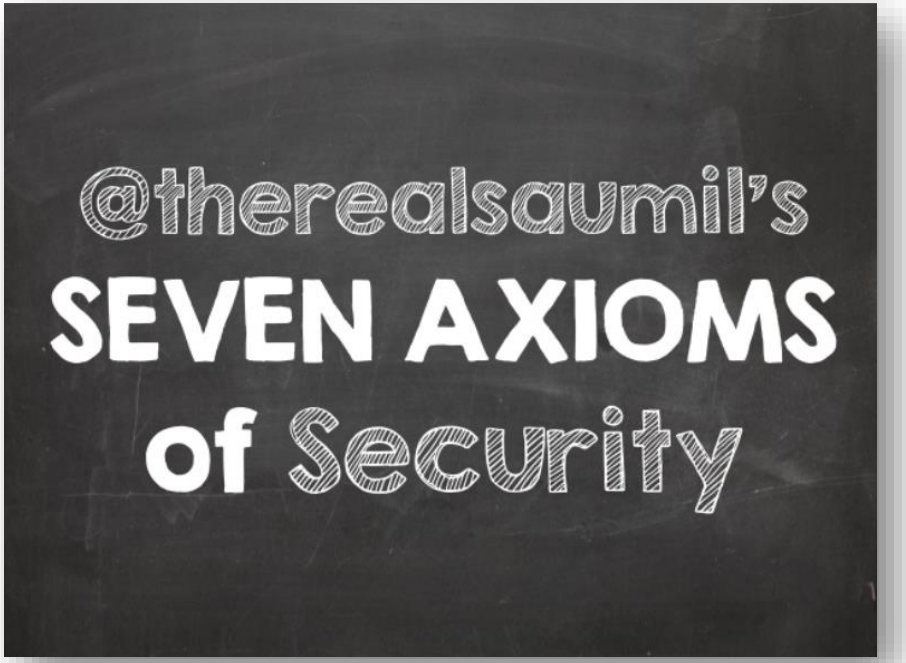
- Goal
  - **“Get the file called proof.txt on one of the servers. Good luck!”**

- Approach
  - Read existing Group Policies (Module: `get_gpo`)
  - Create/inject malicious Group Policy
    - Open FW port for WMI (Module: `set_gpo_fw`)
    - Start WMI service (Module: `set_gpo_servicestatus`)
  - Remotely apply Group Policy (Module: `invoke_gpo_update`)
  - Search for proof.txt

MALICIOUS GROUP POLICY ATTACK SCENARIO - SUMMARY

- Advantages
  - Using non intrusive Microsoft standard procedures
  - Flying under the radar of monitoring (SIEM)
  - Defeating physical and logical barriers
  - Reaching out to every domain joined system
  - Comfortable way to gain persistence and move laterally

COUNTERMEASURES



Hack.lu 2016: Infosec Crossroads (Saumil Shah)

COUNTERMEASURES

egg-laying, wool and milk yielding pig

- There is no all-in-one solution!

- But… Things you can do:
  - Review your GPOs
  - Limit admin privileges (least privilege principle)
  - Restrict application usage
  - Monitoring & IDS (intrusion detection)
  - Healthy information security ecosystem
  - …

FUTURE WORK

- Cover more attack vectors and implement more GPO related PowerShell Empire modules
  - Registry Settings (Run/RunOnce, Autostart) ✓
  - Firewall manipulations ✓
  - Start/stop services ✓
  - Invoke GPO update remotely ✓
  - Login script
  - Task scheduler
  - Install MSI package
  - File search
  - Bridging an airgap
  - ...?
- Preserve timestamp of manipulated GPOs

THANKYOU.PS1


```
Enter-PSSession –Session $currentTalk
Write-Host “Thank you for your attention!”
Write-Host “If there are any questions, we would be happy to answer them”

$questions = Get-Questions

foreach ($question in $questions) {
    Get-Item $question | Write-Host $answer
}

# Note: Now it’s time to clap!
# Either if you want us to leave or it was an inspiring talk

{ Get-Feedback } until (audienceClaps –eq False)
Exit-PSSession

Get-Beer | Invoke-PraiseDemoGods
```

CONTACT US

oneconsult®

Yves Kraft (@nrx_ch)
yves.kraft@oneconsult.com

Immanuel Willi
immanuel.willi@oneconsult.com

Switzerland

Oneconsult AG
Schützenstrasse 1
8800 Thalwil

Tel +41 43 377 22 22
info@oneconsult.com

Oneconsult AG
Bärenplatz 7
3011 Bern

Tel +41 31 327 15 15
info@oneconsult.com

Germany

Subsidiary of Oneconsult AG
Karlstrasse 35
80333 Munich

Tel +49 89 452 35 25 25
info@oneconsult.de