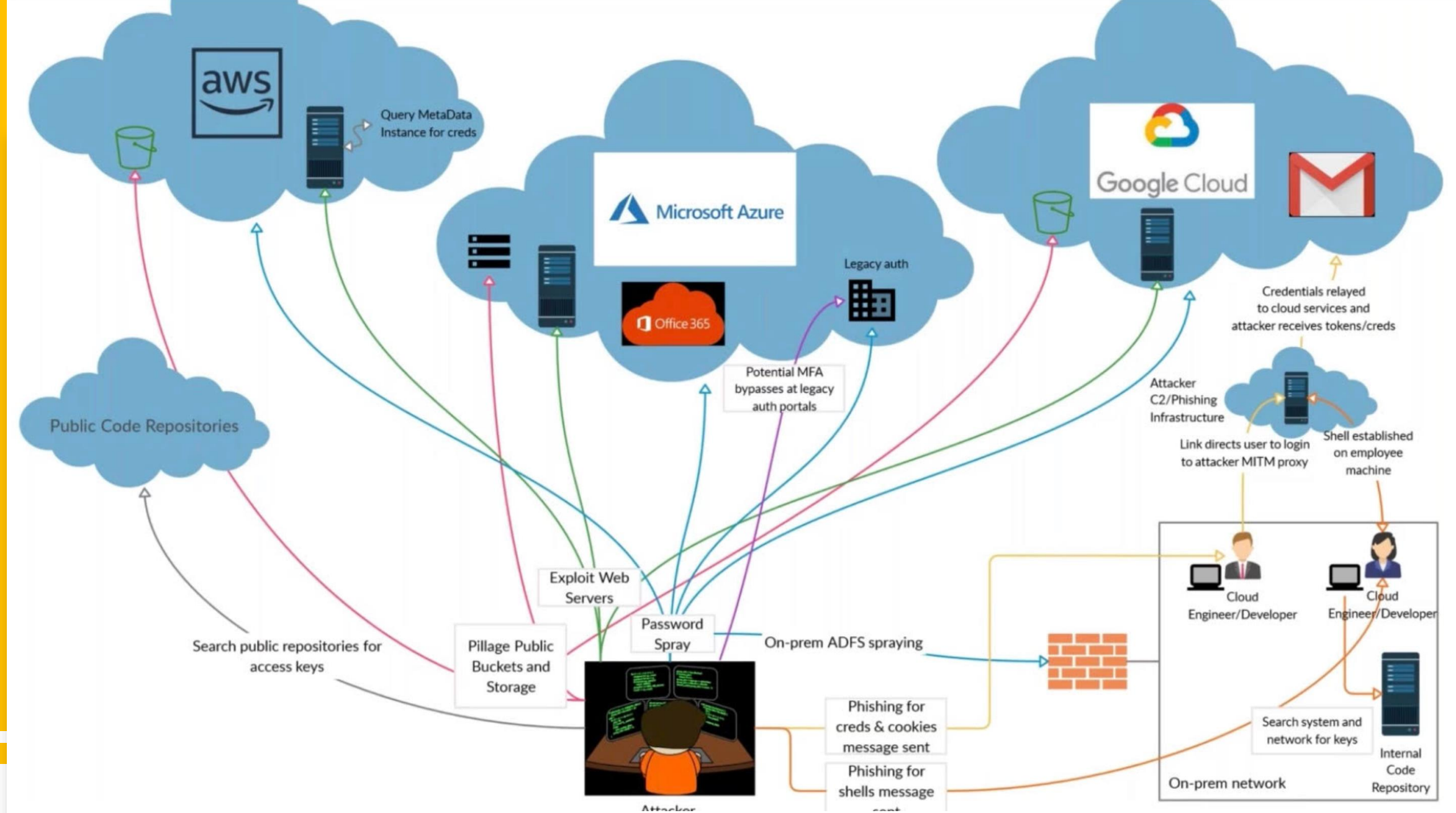
Compromising protected domain environments

Sergey Egorov

Typical attack scenario

- Reconnaissance of external facing domains, services, applications and leaked credentials with an intent to find the entry point.
- Delivery of crafted phishing emails with malicious attachments and links to the employees' mail addresses.
- Credentials reuse or execution of the payloads and establishing Command&Control (C2) communication.
- Situational analysis on the hosts with further domain enumeration.
- Lateral movement.
- ….
- Actions on the target (data exfil, DoS, ransomware).



Taken from BHIS talk

Agenda

- Payload delivery and execution.
- On-disk and In-memory detection evasion.
- Active Directory and Kerberos.
- Lateral movement techniques and traces.
- Constrained and Unconstrained delegation.
- GPO abuse.
- Kerberos on Linux.

Attackers’ mind-list

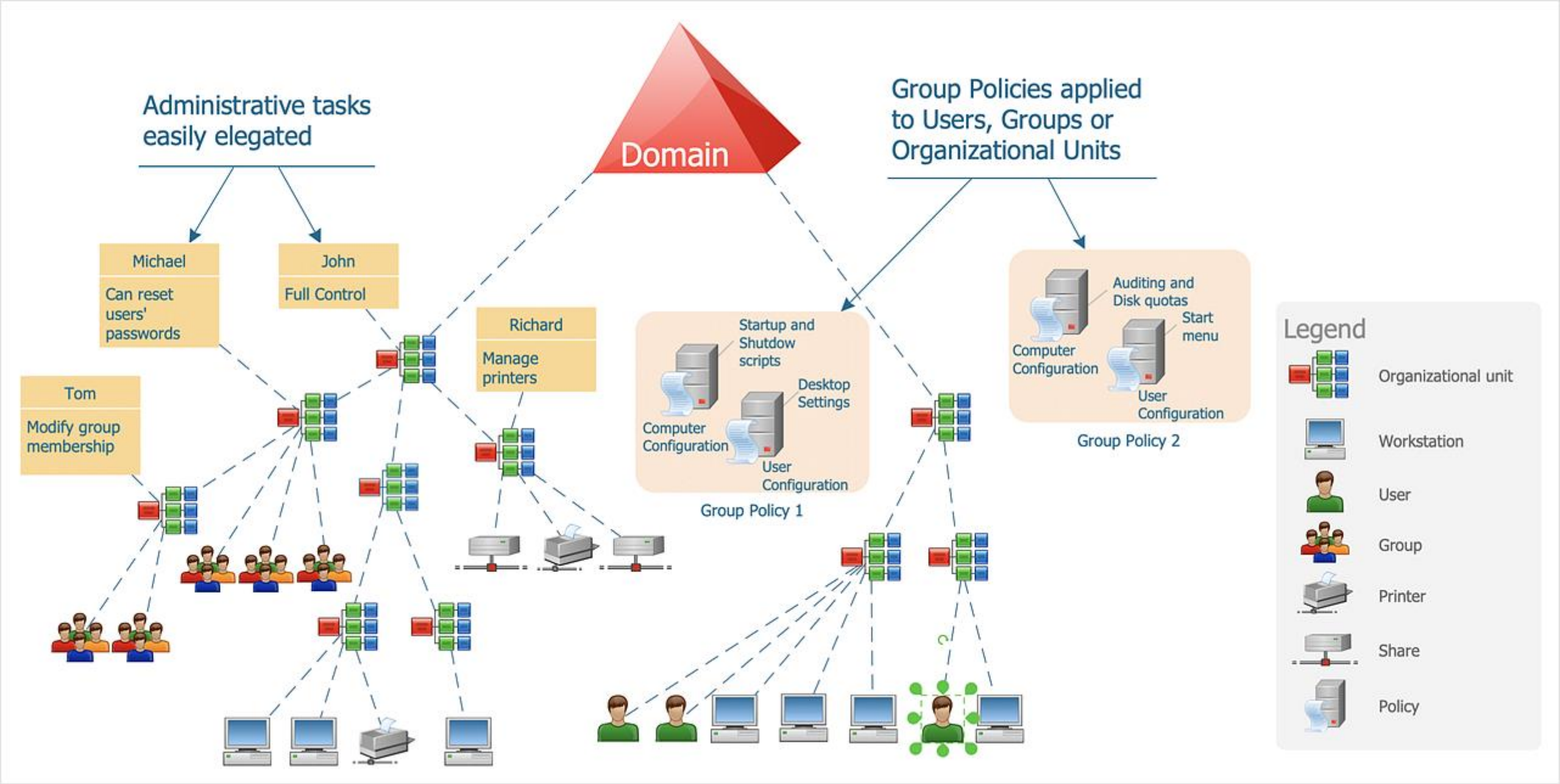
- Mail server config, filtering, malware detection, blacklists
- Host based protection and detection: FW, AV/ AMSI/EDR, App/ Device Whitelisting, Group Policies
- Network protection, segregation and anomaly detection.
- Threat detection and response: SIEM / SOAR.
- IAM, security ~~mis~~configurations, patching and more.

AV / EDR Evasion

- On-Disk:
  - Payloads tweaking, packing, obfuscation or encryption
  - Injection into legit files (PE infection)
  - Shellcode invokers
- In-Memory:
  - Process injection
  - Reflective loading
  - Process hollowing
  - Inline hooking
  - AtomBombing
  - Process Doppelgänging
  - Parent-Process Relationships (PPID-PID)
  - Injection method
  - Thread start address (associated with file)
  - Memory permissions (no RWX)
  - Memory content (avoid known strings and patterns)
- Disable AV or exempt path to the payload.

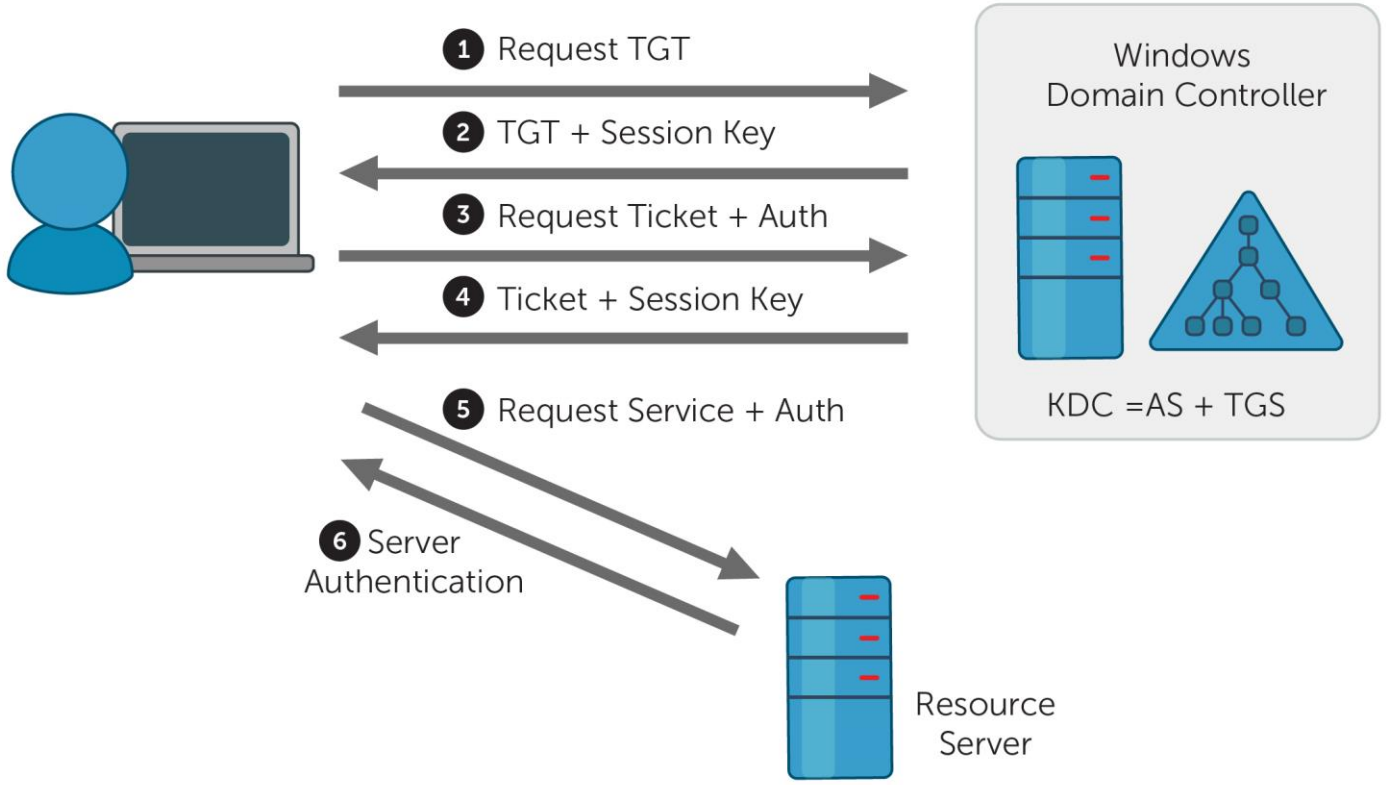
Demo. AV bypass.

- PowerShell tweaks
- Payload encryption
- Shellcode runner
- Process injections


Administrative tasks easily elegated
Domain
Group Policies applied to Users, Groups or Organizational Units
Michael
Can reset users' passwords
John
Full Control
Richard
Manage printers
Tom
Modify group membership
Startup and Shutdow scripts
Desktop Settings
Computer Configuration
User Configuration
Group Policy 1
Auditing and Disk quotas
Start menu
Computer Configuration
User Configuration
Group Policy 2
Legend
Organizational unit
Workstation
User
Group
Printer
Share
Policy

[Source]

Kerberos from an attacker's perspective.



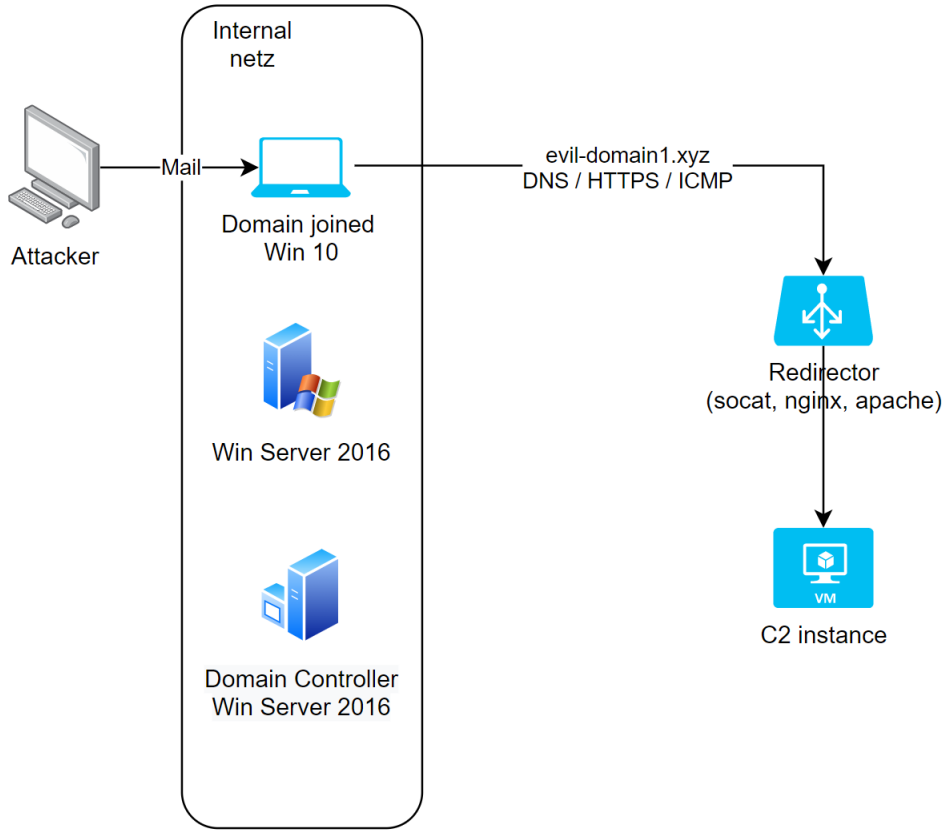
1 - Overpass the hash, AS-REP roasting
2 - Golden ticket
3 - Kerberoasting
4 - Silver Ticket
5 - Pass the ticket

Lateral Movement

Techniques	Protocol / Default Ports
PsExec, Service Control	SMB / 445
WMI, Scheduled Tasks	RPC / 135
Remote Desktop	RDP / 3389
Windows Remote Management	WinRM / 5985, 5986
DCOM	RPC / 135, 1024++
Admin / Dev tools, code repos Configuration / Orchestration tools WSUS, SCCM, AV, GPO Vulnerable Apps and Infras DB links …	

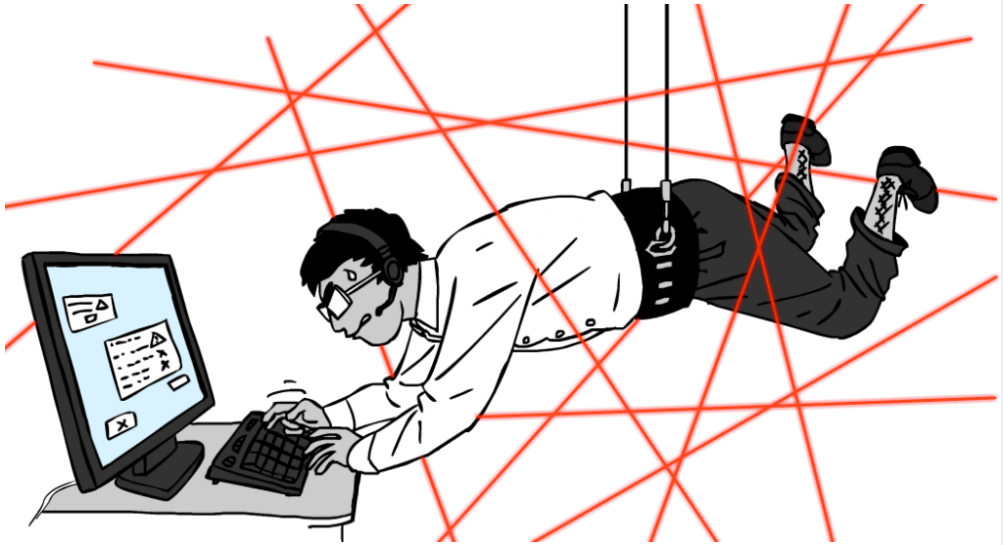
Demo. Lateral Movement.

- Service creation and hiding
- WMI + regsvr32
- MsBuild
- UAC bypass
- Unconstrained delegation + Printer Bug = DA
- Constrained delegation
- GPO Abuse

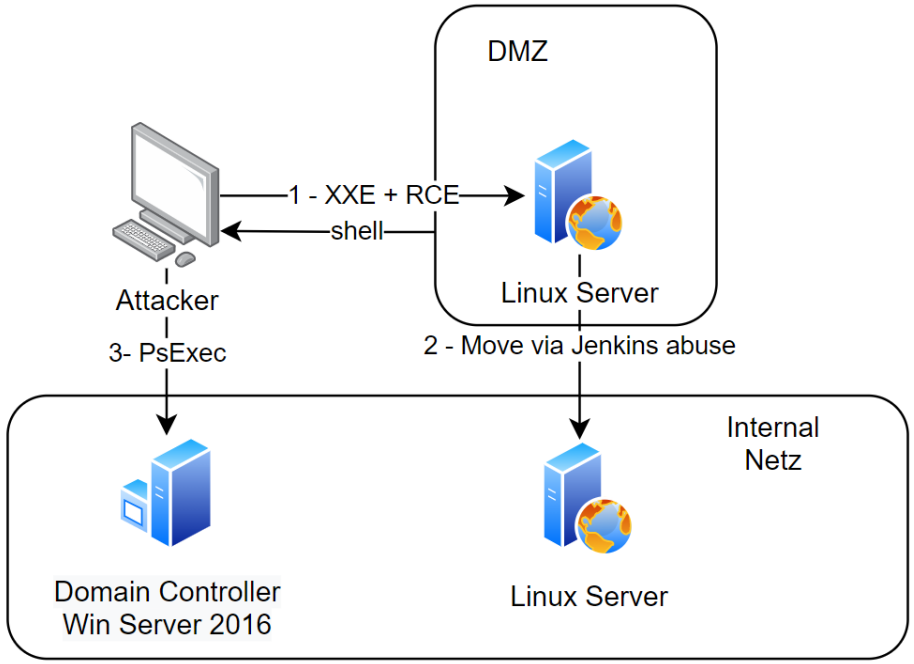


Detection Bypass During Post Exploitation

- Use of custom tools and techniques.
- Avoid using powershell.exe
- Avoid querying endpoints
- Blend into normal traffic and behavior.
- LoL bins and scripts.
- Use of less monitored systems (Unix, IoT).
- Speed (Not Petya, Infection Monkey).
- Disable agent / logging.



Demo. From Linux to Domain Admin.



- XXE
- LFI + Command Execution
- Linux Privilege Escalation
- Port Forwarding techniques
- Jenkins exploitation
- Abuse Kerberos on Linux
- Pass the ticket with PSExec

Summary.

- Most of known malicious activity can be detected for the price of events to review.
- Most of known detection techniques can be avoided.
- Domains are complex and full of abuse possibilities if not analyzed regularly for security issues.
- Clouds make the attackers' life more interesting.