SPECTEROPS

Domain Persistence:

Detection, Triage, and Recovery

Joshua Prager & Nico Shyne

Intro Bio

Joshua Prager

- Principal Consultant - Adversary Detection
- AMU (‘18) & NYU (’24)
- Dad of Two No Limit Soldiers
- Lover of Texas Wine & Whiskey

Nico Shyne

- Consultant - Adversary Detection
- USNA ('17) & UVA MSMIT ('24)
- Former SWO/IP Officer
- Love movies and live music

“Rotate the KRBTGT Twice!!”

Purpose of the Presentation

- Started by providing remediation guidance for a client who had seen evidence of elevated domain persistence
- We began reviewing other organizations’ disaster recovery strategies

What We Found:

- Lacking in audit guidance to identify the attack paths utilized
- Too high level for operational use without additional research
- Lacking in context that demonstrated the impact against the adversary during eviction
- Lacking in context for a bare-minimum expectation for a recovery plan

Defining Domain Persistence

Domain Persistence

- These techniques can be credential theft methods, authentication functionality abuses, or endpoint management abuses

Common Denominators

- Evidence of these techniques usually represent a larger attack path
- The techniques represent the adversary obtained Tier 0 access
- Difficult to scope from an IR pers

Defining Domain Persistence

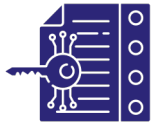
Overview

We will be discussing the following:

- Considerations surrounding the technology that enables domain persistence techniques
- High level overview of detecting these domain persistence techniques
- Triage considerations when analyzing alerts generated by each of the techniques mentioned
- Recovery operations when any of the techniques are identified as true positive
- The groundwork for developing a compromise recovery plan with detailed procedures

Domain Persistence Techniques

Credential Theft on the Domain Controller via LSASS Memory



NTDS Access

DCSync

Golden Ticket

Diamond Ticket

AD CS Certificate Theft

SCCM Site Takeover

Domain Persistence Techniques

Credential Theft on the Domain Controller via LSASS Memory

This technique can be conducted via many publicly available tools and native Windows binaries (e.g., Task Manager).

The goal of credential theft via LSASS memory is to read the virtual memory space of the LSASS.exe process and retrieve cached credential material.

The typical operational flow:

- Identify the LSASS.exe process (Usually a PID)
- *Open a handle to the LSASS.exe process*
- *Read the LSASS.exe virtual memory space*
- Parse for cached credential material

Domain Persistence Techniques

Credential Theft on the Domain Controller via LSASS Memory

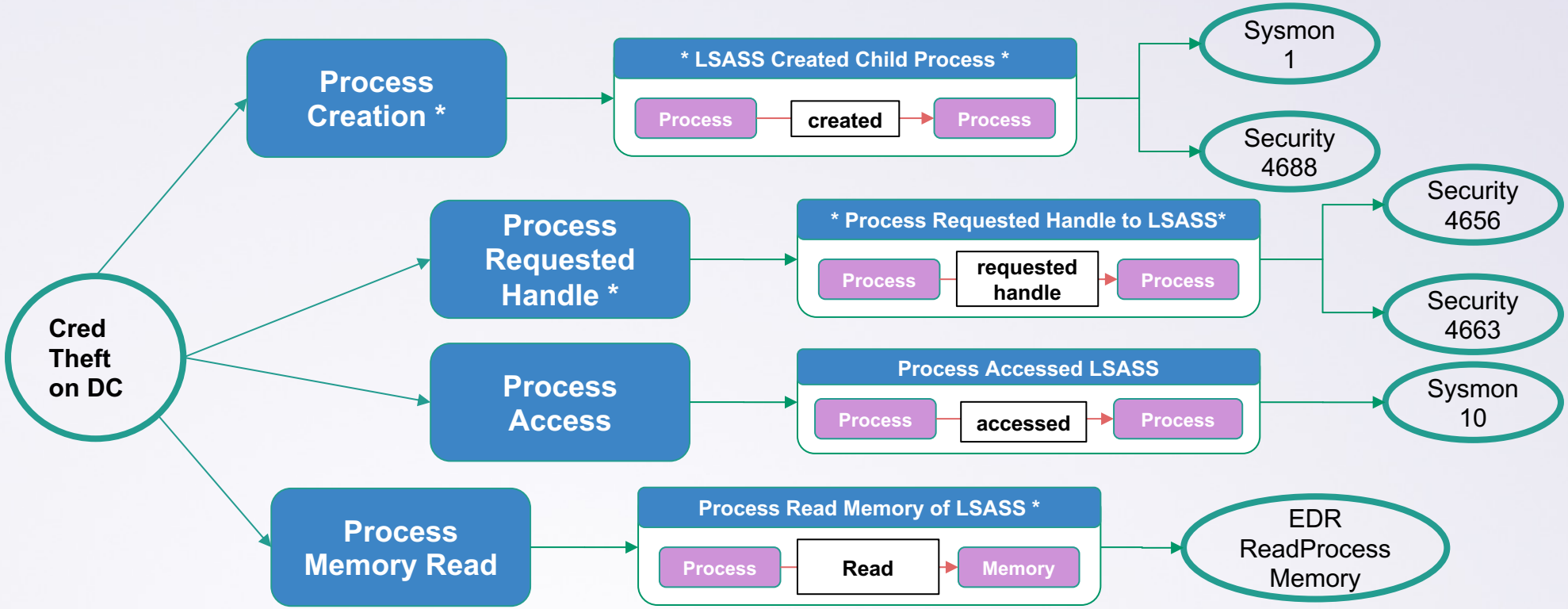
Operationally the Same

- Credential theft via LSASS memory on a domain controller is conducted operationally the same as client credential theft

Key Differences

- Lack of Preventive Controls
  - Generally, No CredGuard
- Availability to Tier 0 Accounts
  - Domain Admin interactive logins

Credential Theft on the Domain Controller via LSASS Memory



Domain Persistence Techniques

NTDS Access

Obtaining the NTDS.dit file of organizations by accessing or copying the database file enables the harvesting of credentials from the organization.

Several native Windows binaries exist for generating backups of the Active Directory database and copying the deadlocked *NTDS.dit* file.

The typical operational flow:

- NTDS backup utility is executed targeting the NTDS.dit file
- Volume Shadow Copy (VSS) service is started
- Backup utility and VSS use the VSS API and the BackupComponents interface to create the snapshot of the NTDS.dit

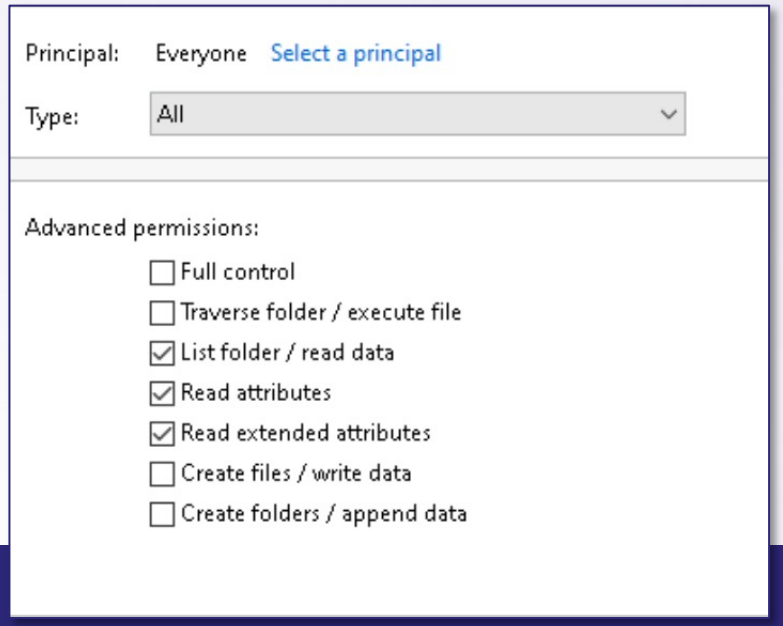
Domain Persistence Techniques

NTDS Access

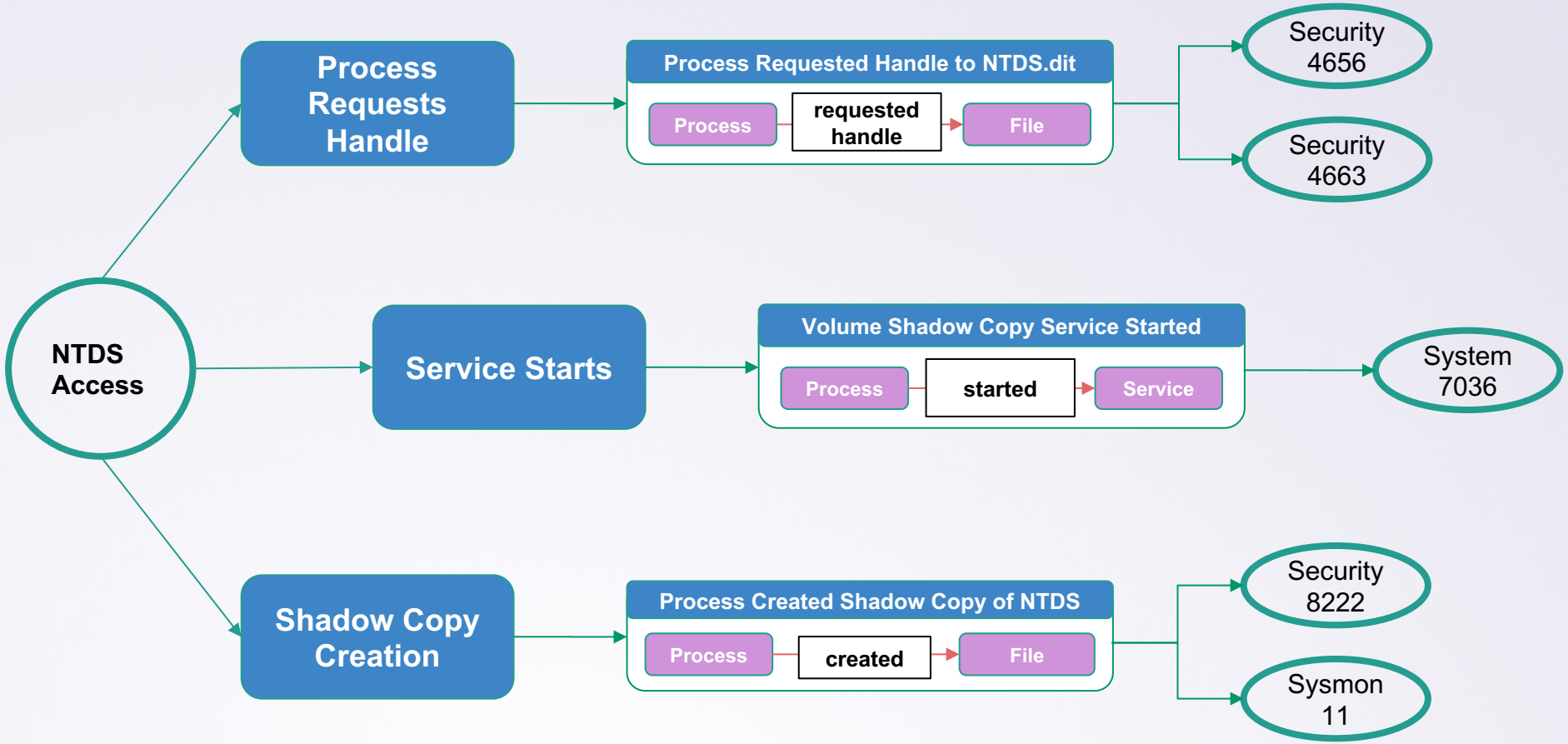
Manipulation of the NTDS.dit file generates several forms of telemetry however this telemetry is not generally enabled by default.

The System Access Control List (SACL) must be enabled to audit the access rights used to read the file.

- Read File Attributes
- Read File Extended Attributes
- Read File Data



NTDS Access


NTDS Access
Process Requests Handle
Process Requested Handle to NTDS.dit
Process
requested handle
File
Security 4656
Security 4663
Service Starts
Volume Shadow Copy Service Started
Process
started
Service
System 7036
Shadow Copy Creation
Process Created Shadow Copy of NTDS
Process
created
File
Security 8222
Sysmon 11

Domain Persistence Techniques

DCSync

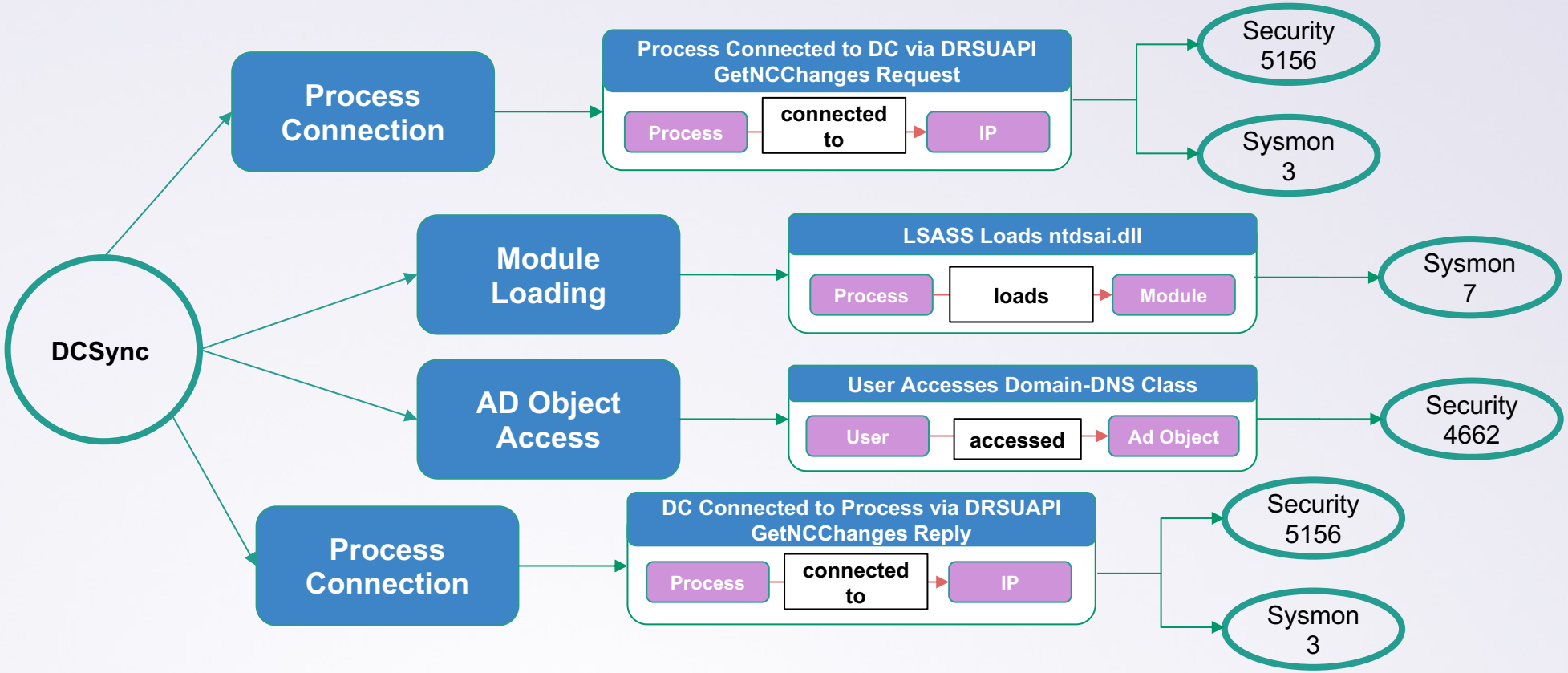
Directory Replication Service uses the MS-DRSR RPC protocol and the **GetNCChanges** RPC method to sync account and organizational container changes across multiple domain controllers.

Syncing credentials is a method by which Tier 0 accounts can be leveraged to retrieve credentials for service accounts related to authentication protocols.

The typical operational flow:

- Compromised client uses RPC method *GetNCChanges Request* to remotely request to sync account information from domain controller
- Domain controller's LSASS process loads *ntdsai/ntdsapi(.dll)* to utilize DRSUAPI RPC interface to access NTDS.dit
- Domain controller remotely syncs the credentials to compromised client via RPC method *GetNCChange Reply*

DCSync


DCSync
Process Connection
Process Connected to DC via DRSUAPI GetNCChanges Request
Process
connected to
IP
Security 5156
Sysmon 3
Module Loading
LSASS Loads ntdsai.dll
Process
loads
Module
Sysmon 7
AD Object Access
User Accesses Domain-DNS Class
User
accessed
Ad Object
Security 4662
Process Connection
DC Connected to Process via DRSUAPI GetNCChanges Reply
Process
connected to
IP
Security 5156
Sysmon 3

Domain Persistence Techniques

Golden Ticket

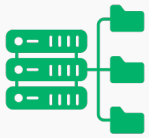
The *KRBTGT* account generates a key (a hash of its account password) and the KDC uses this key to sign and encrypt TGTs. Because Kerberos inherently trusts any TGT encrypted with that *KRBTGT* account hash, an adversary with access to that hash could generate their own TGT (a *golden* TGT) and bypass the KDC entirely.

The typical operational flow:

- An adversary requires the FQDN of the domain, the SID of the domain, an account to impersonate, and a *KRBTGT* password hash
- The adversary passes this data to a new ticket (using a tool like mimikatz or Rubeus), and that ticket can be saved in the current session's ticket cache
- This new ticket gives access to wherever the *KRBTGT* account has access within that domain

Domain Persistence Techniques

Golden Ticket



Data Source:

- Event ID 4768 (TGT Requested)
- Event ID 4769 (Kerberos Service Ticket Requested)
- Event ID 4627 (Group Membership Information)
- Klist

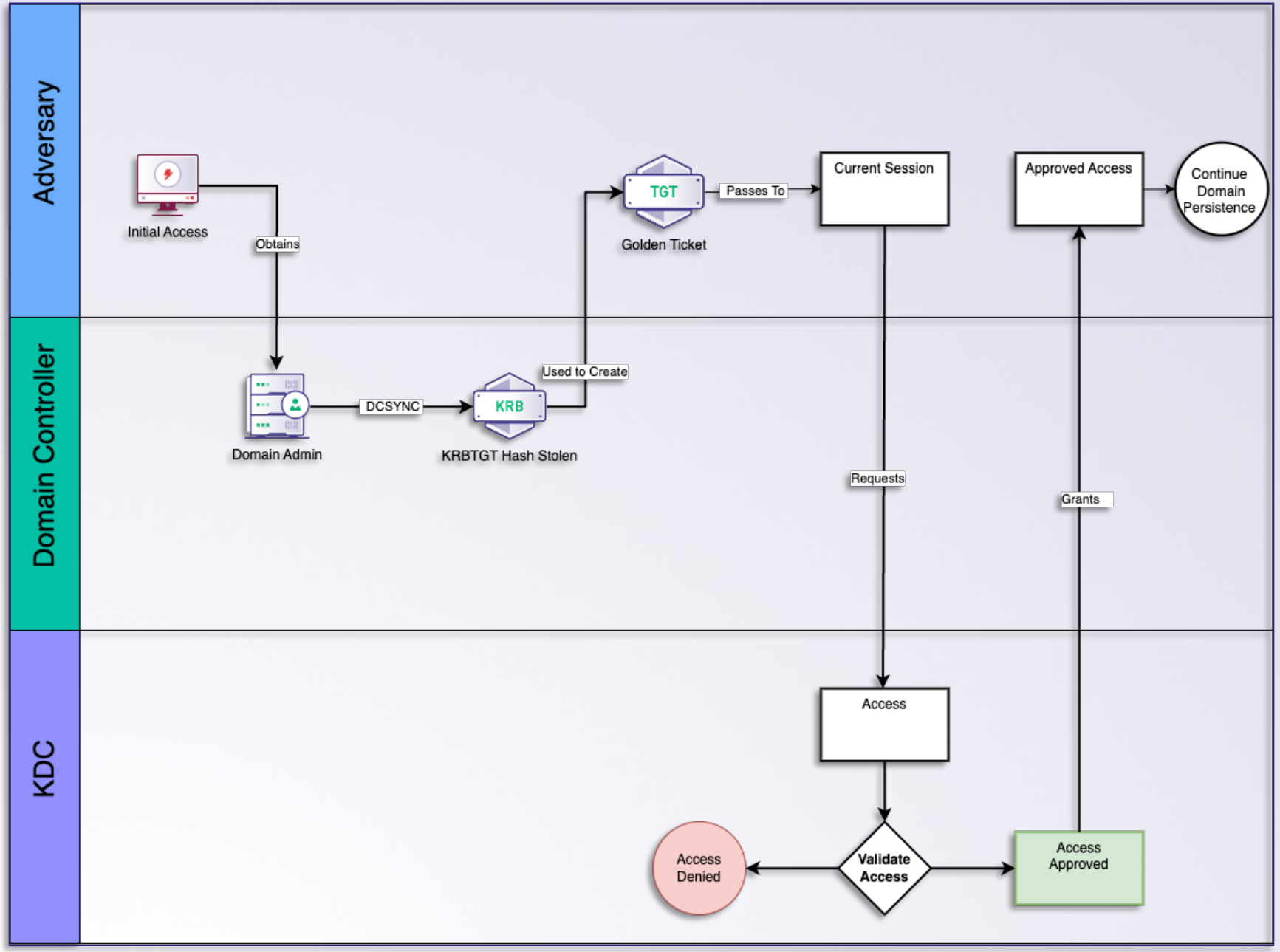
Detection Strategy

- **Focus on KRBTGT Password Hash**: Detection efforts should concentrate on identifying the theft of the KRBTGT password hash and the anomalous use of the KRBTGT account, rather than solely on the ticket requests (Event IDs 4768 and 4769), which appear identical for both legitimate and Golden Ticket attacks.
- **Monitor Group Membership Changes**: Utilize Windows Security event ID 4627 to track changes in group memberships, particularly for signs of unauthorized elevation to privileged groups like Domain Admins, which could indicate a Golden Ticket attack.
- **Track Unmatched TGS-REQs**: Look for TGS-REQs (Event ID: 4769) without a corresponding AS-REQ (Event ID: 4768) and tickets that do not display proper FQDNs, as these may suggest the use of forged tickets.
- **Use klist for Validation**: To confirm suspected Golden Ticket activities, employ the klist command to review the Kerberos ticket cache following unusual logon events (Event ID: 4624), indicating the importation of a stolen KRBTGT ticket.

Golden Ticket

Required Items:

- **Domain FQDN**
- **Domain SID**
- **Account to impersonate**
- ***KRBTGT* password hash**



Domain Persistence Techniques

Diamond Ticket

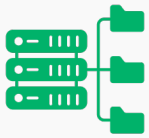
Instead of creating their own TGT (as with Golden Tickets), adversaries could instead opt to modify a legitimately issued TGT that has already been issued by the KDC.

The typical operational flow:

- Obtain *KRBTGT* password hash
- Request a legitimate TGT
- Decrypt legitimate TGT
- Modify TGT Privilege Attribute Certificate (PAC)
- Re-encrypt TGT

Domain Persistence Techniques

Diamond Ticket



Data Source:

- Event ID 4768 (Kerberos Authentication Ticket Requested)
- Event ID 4648 (A Logon Was Attempted Using Explicit Credentials)
- Event ID 4672 (Special Privileges Assigned to New Logon)
- Anomalous Access Patterns
- Kerberos Ticket Lifetimes

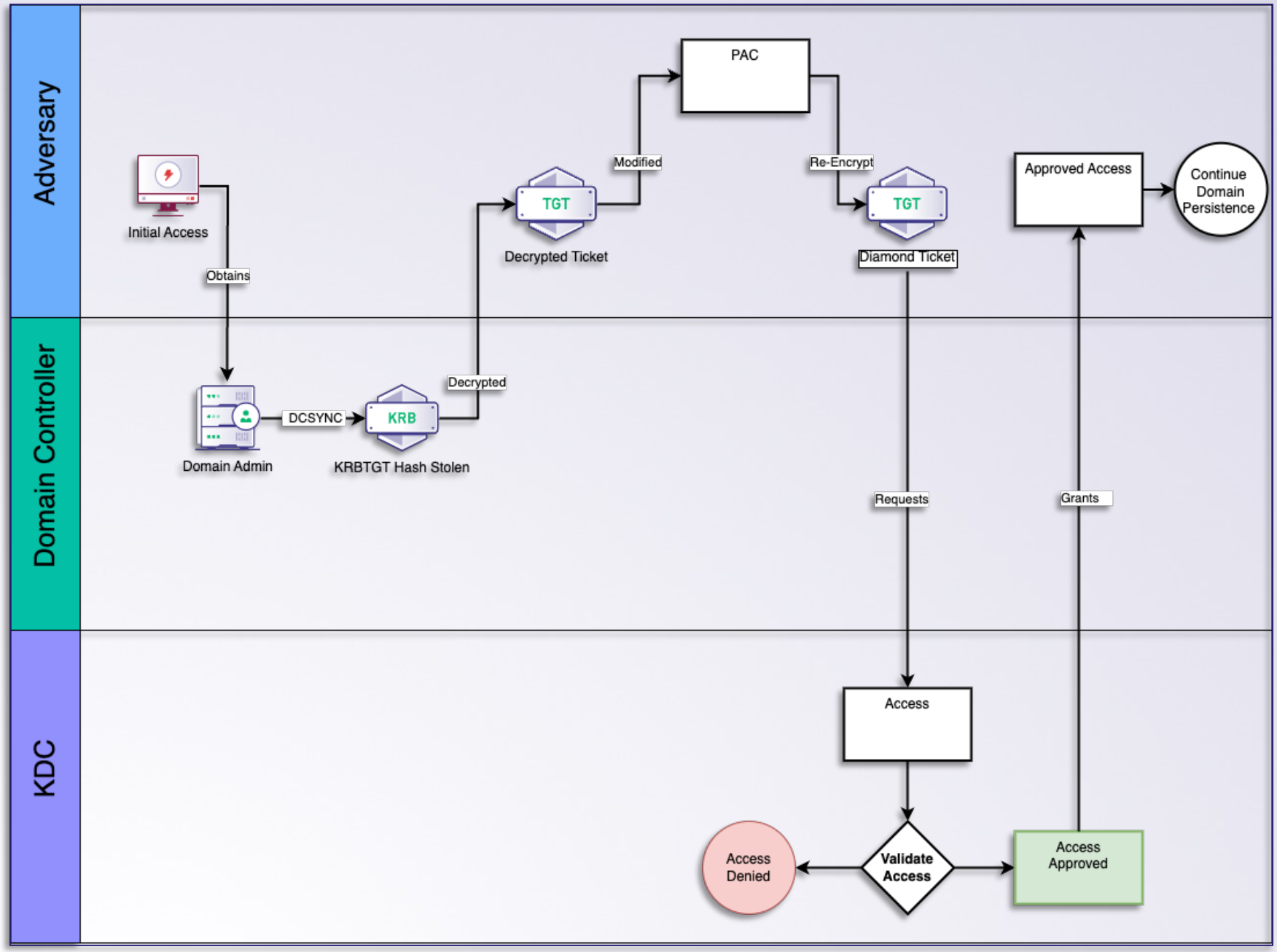
Detection Strategy

- **Monitor KRBTGT Password Hash Theft:** Use detection strategies like lsadump, NTDS.dit access, and DCSync to identify unauthorized access to the KRBTGT account's password hash.
- **Detect Anomalies in Group Membership Changes:** Watch for unexpected changes, such as low-privilege users gaining high-privilege group memberships (e.g., Domain Admins) without corresponding administrative actions.
- **Analyze Kerberos Ticket Requests (Event ID 4768) and Modifications (Event ID 4648):** Look for anomalies in ticket requests and modifications, especially where the PAC of a legitimately issued TGT is altered.
- **Track Anomalies in AS-REQs:** Identify discrepancies in AS-REQs, particularly where the PA-PAC-REQUEST is set to false, indicating potential manipulation of authentication tickets.
- **Employ Additional Validation Techniques:** Use tools like klist or ACE: Get-KerberosTicketCache for targeted investigation and validation of suspicious Kerberos ticket operations.

Diamond Ticket

Required Items:

- **Domain FQDN**
- **Domain SID**
- **Account to impersonate**
- **KRBTGT password hash**



Domain Persistence Techniques

ADCS Certificate Theft

Typically, both root and subordinate Certificate Authorities (CA) are not treated with the same sensitivity as DCs. For example, while a server admin may not be able to access the DCs, a CA may be accessible.

Obtaining local admin on a CA enables the extraction of the private key which can be used for forge certificates. Default forged cert validity is 1 year.

The typical operational flow:

- Obtain NT Authority\SYSTEM on a CA
- Enumerate the private keys on a CA
- Obtain decrypted DPAPI MasterKey
- Decrypt CA private keys and associated certificates

Domain Persistence Techniques

ADCS Certificate Theft

Forged Certificates:

Once the private cert is extracted and converted to a .pfx, a forged certificate can be created and signed by the private cert of the CA for any domain user.

The only inhibitor is that the forged cert must be used for an active user on the domain, which excludes accounts like the KRBTGT.

Domain Persistence:

With this forged cert, a machine account can be used to conduct other domain persistence techniques such as DCSync. Additionally, the forged cert can be used to request a TGT for an account and the TGT can be injected into the current user's session with Pass-the-Ticket.

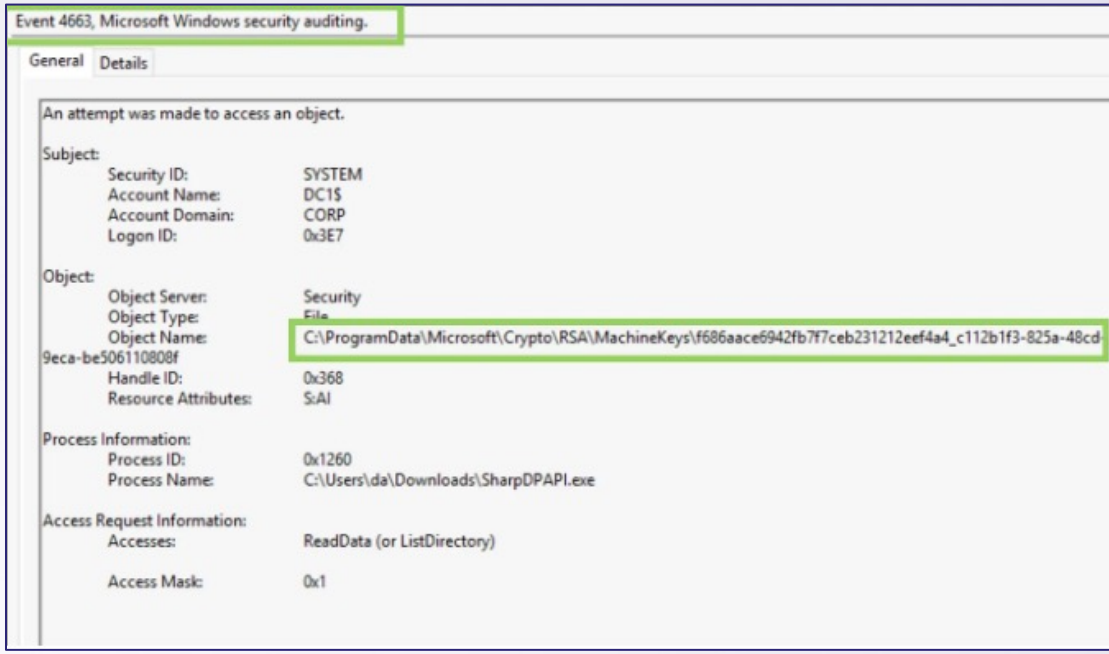
Domain Persistence Techniques

ADCS Certificate Theft

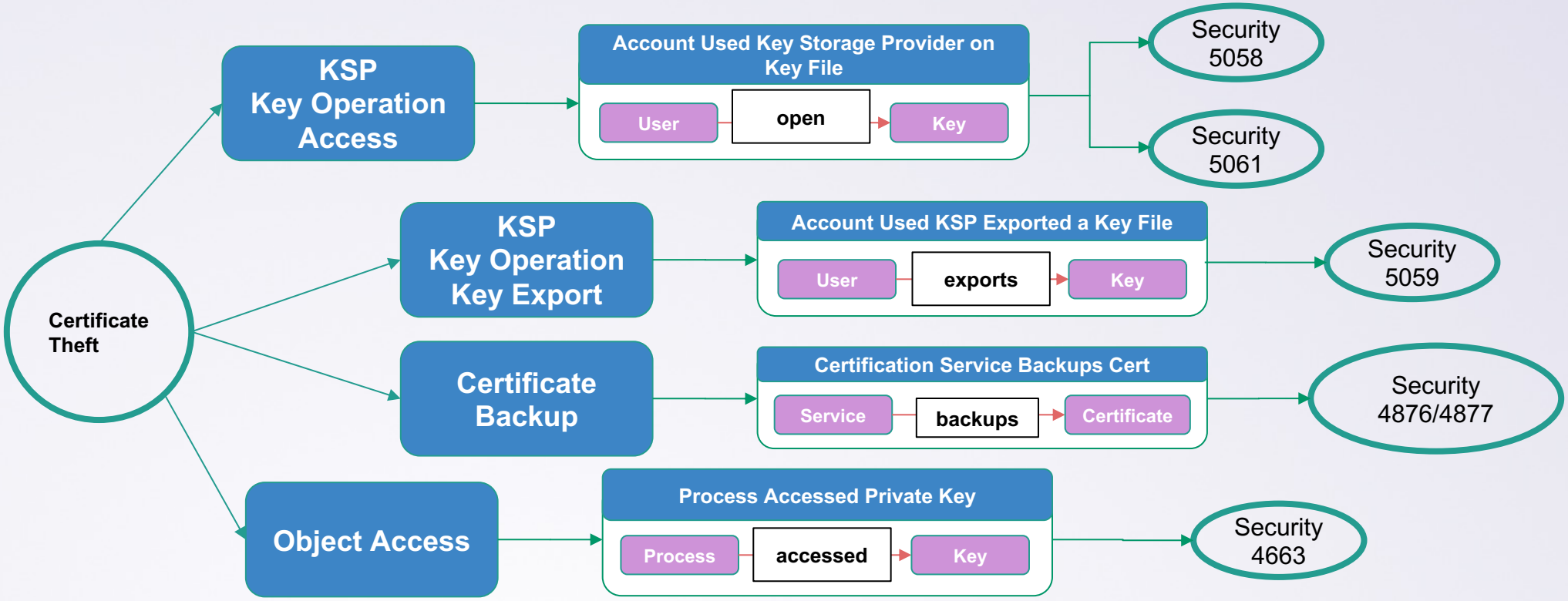
Will Schroder and Lee Christensen provide detection methods within their AD CS focused white-paper, Certified-Preowned.

These detection methods surround the private key extraction methods utilized. The Microsoft Software Key Storage Provider (KSP) records cryptographic operations like opening and exporting KSP key files.

Additionally, a SACL can be set on the private key within a CA.



ADCS Certificate Theft



Domain Persistence Techniques

SCCM Site Takeover

Endpoint Configuration Manager (formally SCCM) manages endpoint software and policies via a hierarchy scheme sometimes spanning multiple sites.

Though, SCCM employs a RBAC model, the single point of failure is the use of the site server's machine account local admin client push installation of software in the SCCM site. With the coercion of NTLM authentication from the primary site server and relayed to another system, actions can be executed in the context of local admin.

The typical operational flow:

- Coerce NTLM authentication of the Primary SCCM Site server machine account
- Relay NTLM authentication of the machine account to another host

Domain Persistence Techniques

SCCM Site Takeover

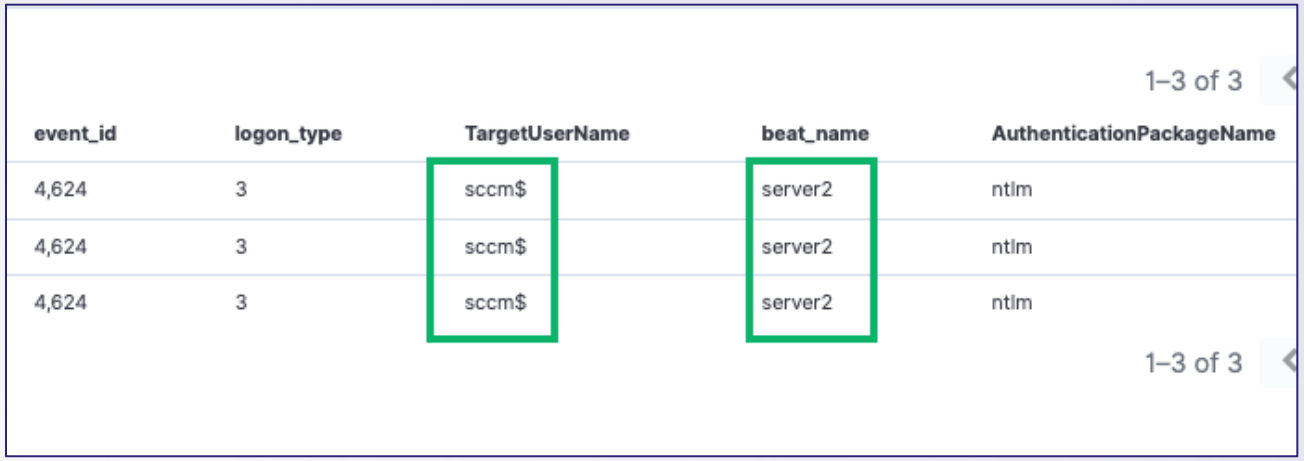
Once authentication is relayed to a site database server, SQL queries can be crafted to insert a user account into the *RBAC_Admins* role which allows full administrative privileges over the SCCM service.

By authenticating to the SCCM Administration Service API, local administrative access to the site server can be established. At this point, the entire SCCM site and all correlated site clients are exposed to elevated execution.

Domain Persistence Techniques

SCCM Site Takeover

Relaying machine accounts to from one machine to another host will display a mismatch in logon telemetry. For example, the SCCM Primary Site server machine account will appear to login to a machine that is **not** the primary site server.



1–3 of 3

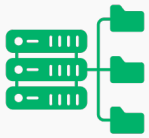
event_id	logon_type	TargetUserName	beat_name	AuthenticationPackageName
4,624	3	sccm$	server2	ntlm
4,624	3	sccm$	server2	ntlm
4,624	3	sccm$	server2	ntlm

1–3 of 3

Typically, machine accounts only log into themselves or the DC for domain authentication.

Domain Persistence Techniques

SCCM Site Takeover



Data Source:

- SACLs
  - A read access SACL set on the System Management container
- Successful Logon Events
  - Enables the monitoring of both user, service and machine accounts.

Detection Strategy

- A SACL set on the System Management container within Active Directory will identify enumeration techniques of the site servers
- Monitoring for the logon of the Primary Site Server machine account ($SCCM) where the host that is being logged onto is **not** a DC or the Primary Site Server itself

Recovering From Domain Compromise

Post Compromise Guidance

Post Compromise Guidance

Recovery Strategy Requirements

- Most organizations have domain recovery strategies as a requirement dictated by compliance
- However, they often lack quality and valid testing

Ensuring Quality Strategies

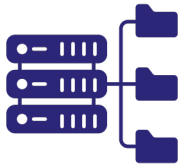
- Domain recovery strategy per environment category
- Ensure each strategy has a successful exit scenario
- Consider worst case scenarios
  - e.g., How will you recover with Veeam if the DC that manages RDP authentication is compromised?

Post Compromise Guidance

Determine the Scope

Rotate Certificates

Replace or Reprovision Domain Controllers



Enable Additional Auditing

Rotate Accounts and Object Secrets

Determine the Scope

Identify the Population of Affected Systems/Users

Scope of Investigation and Containment

- Typically, this is focused on systems and users flagged in an alert

Impact of Privileged Access & Domain Persistence

- Severity escalates due to the privileged access required of domain persistence
- Evidence of domain persistence indicates a larger attack path

Determine the Scope

Identify the Population of Affected Systems/Users

Known Affected Systems:

- Known affected tier 0 systems are the initial focus
  - Domain controllers
  - KRBTGT service account
  - CA(s)
  - Config Mgr Primary Site Server

Potentially Affected Systems:

- Consider the capabilities of the privileged access achieved
- Determine the principals and tier 0 systems that could be impacted by access achieved by attacker
- Ex: AZ-Hybrid – Highly Privileged Entra accounts that are both on prem and in EntraID

Replace or Reprovision Domain Controllers

Some things can’t be rotated…

Limitations in Security Rotation:

- The Domain DPAPI Backup Key on a domain controller is non-rotatable (as per Microsoft guidelines).

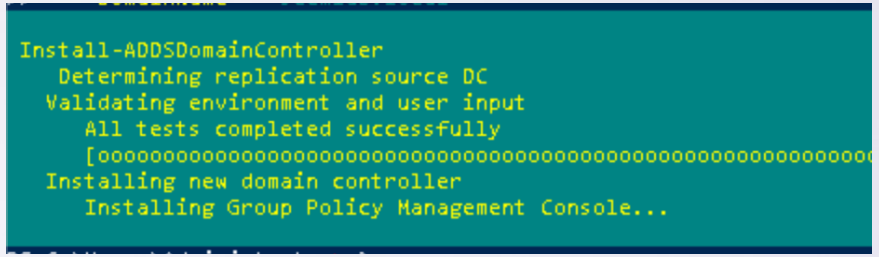
Risks of Privileged Domain Persistence:

- Compromises the integrity of the domain controller's DPAPI Backup Key.
- The compromised key can decrypt any domain user's data across all machines in the domain *even if the passwords of either account is changed*

Replace Domain Controllers

Replace or Reprovision

1. Using an existing server (e.g., not a current DC) or adding a new server to the domain
    1. Apply latest patches to new or existing server
2. Add AD DS roles
    1. Install-WindowsFeature AD-Domain-Services
3. Promote server to Domain Controller + DNS
    1. Install-ADDSDomainController
4. Validate and Transfer FSMO Roles
    1. netdom query fsmo
    2. $Server = Get-ADDomainController -Identity ”dc2.corp.local”
       Move-ADDirectoryServerOperationMasterRole -Identity $Server -OperationMasterRole
       SchemaMaster,DomainNamingMaster,PDCEmulator,RIDMaster,InfrastructureMaster



Replace Domain Controllers

Replace or Reprovision

5. Validate that health of new Domain Controller
    1. Dcdiag /v
    2. repadmin /replsummary
    3. repadmin /queue
    4. repadmin /showrepl * /errorsonly
6. Remotely Uninstall AD DS from In-Scope DC
    1. Invoke-Command -ComputerName DC1 -ScriptBlock { Uninstall-ADDSDomainController -LocalAdministratorPassword (ConvertTo-SecureString -AsPlainText "NewLocalAdminPassword" -Force) -ForceRemoval -Force } -Credential (Get-Credential)
7. Remove In-Scope DC from the Network
8. Begin Account/Object Rotation

Account Rotation

User Accounts

Domain Persistence Pattern:

- Domain compromise incidents typically involve one or two compromised domain admin accounts.
- These accounts play a central role in the execution of the larger attack path.

Immediate Response:

- Disable compromised Tier 0 (domain admin) accounts immediately.
- These accounts act as critical choke points in the security infrastructure.

Proactive Account Triaging:

- Identify and disable accounts that had interactive or remote sessions on the same hosts as the compromised domain admins.
- This step is crucial as these accounts are vulnerable to credential theft by privileged accounts.
- Begin domain-wide account credential rotation

Account Rotation

Service Accounts

Domain Persistence Techniques:

- Overprivileged service accounts are often exploited to gain access to Tier 0 systems.

Challenges in Password Rotation:

- Rotating service account passwords can be complex, particularly in organizations dependent on legacy applications.

Immediate Response:

- Temporarily disable service accounts listed as affected until password rotation is complete.

Account Rotation

Service Accounts

Collaboration for Minimal Disruption:

- Incident Response teams should collaborate with Security Engineering.
- Aim for a careful balance between security measures and operational continuity, especially for service accounts tied to customer-facing products.

Proactive Security Resilience:

- Rotate service account passwords, ensuring a minimum length of 30 characters for increased security.

Account Rotation

Service Accounts - KRBTGT

Initial KRBTGT Password Change

- Change the KRBTGT account password once and ensure this change is replicated across all domain controllers.

Second Password Rotation

- Perform a second password change for the KRBTGT account after confirming replication success. This step ensures the previously compromised password hash is completely removed from the environment.

Comprehensive Coverage:

- Execute this two-step password rotation process for the KRBTGT account in every domain affected by the compromise to eliminate lingering risks.

Account Rotation

Machine Accounts

Machine Account Considerations

- Machine account passwords as such do not expire in Active Directory. They are exempted from the domain's password policy.
- Machine account password changes are driven by the CLIENT. The client's netlogon service handles machine password updates, not Active Directory
- Resetting the client's machine account password locally will disconnect the client from the domain until the domain trust is re-established.

Rotating the Machine Account:

- The *Reset-ComputerMachinePassword* cmdlet can reset the client machine account password
- The client will need to be rejoined to the domain
- **This will not remediate coercion and relay attacks**
  - Install hotfix KB15599094 and disable NTLM for client push installation (prevents coercion via client push)

Trust Realm Object Rotation

Forest Trust

Tier 0 Domain to Forest

- Depending on the direction of domain trust within a forest, Tier 0 privileged accounts can access other domains with elevated access
- This may modify the scope of the investigation drastically
- E.g., Parent Domain -> Child Domains

Inter-Realm Trust Key

- Manually initiate the trust password update with netdom.exe
- Start with compromised domain first
- Continue with other side of directional trust
- Allow replication to all domains within the forest trust

Certificate Authority Rotation

Private PKI Cert Theft Recovery

Root CA

- Begin revocation of all subordinate CA certificates
- Update revocation labels of certificates in Revoked Certificates folder from "Certificate Hold" to "CA Compromise" to prevent un-revoking
- Manually publish the updated CRL

Clients

- Force CRL update on clients
  - certutil -setreg chain\ChainCacheResyncFiletime @now
- Decommission old Root CA
- Generate new key pair on new Root CA
- Distribute certificates and offline new Root CA

Additional Auditing

How Do We Know Which New Logs to Ingest?

How to Identify New Log Sources to Ensure Domain Persistence is Detected Earlier:

1. Start with threat modeling:
    1. Determine the largest attack surfaces
    2. Define the thresholds of materialistic impact
2. Identify use cases surrounding the techniques related to the attack paths hypothesized in the threat modeling
3. Of those use cases, validate detective and preventive controls already in place
4. Identify gaps in telemetry and protective controls
5. Ingest/Apply additional auditing surrounding those controls

Conclusion

Domain Persistence: Detection

Many organizations do not have custom detections designed to identify domain persistence behavior. These detections are important because they represent a larger attack path.

Domain Persistence: Recovery

Reducing adversary dwell time after identifying these techniques is critical. Organizations that have pre-planned/documented restore playbooks can confidently recover from these scenarios quickly.

Questions & Resources

Research and Validate

The below link includes many of the books, blogs, and references that we dove into while researching these topics:

- GitHub Link

Special Thanks:

- Alex Sou
- Jared Atkinson
- Chris Thompson
- Garrett Foster
- Will Schroder
- Lee Chagolla-Christensen

SPECTEROPS

Thanks!

Josh Prager | jprager@specterops.com

Nico Shyne | nshyne@specterops.io