Axon Investigation: Internal Attacker Activity Detected

OPENED BY: Team Axon

Target: Enterprise Network

Severity: HIGH

THREAT SUMMARY

Within indications of potential compromise in LAB environment, it was determined that malicious activity was taking place which included lateral movement attempts, credential theft and compromise attempt into a corporate DC server.
The actions originated from the IP `10.0.0.2`, a windows machine (possibly running a Linux VM), while using Impacket tools such as `wmiexec.py` and `secretsdump.py` to operate the activity.

Compromise of multiple local and domain users was observed including an attempt for stealing `krbtgt` NT hash. It is assumed that the `krbtgt` NT hash was compromised which lets the attacker operate a Golden Ticket attack within the environment.

No additional malicious activity was observed from the device `10.0.0.2` since the end of September 29th. However, additional log sources are required in order to ascertain the credential theft was initiated successfully, how did the initial access effort occurred and wether the attack was contained.

During the investigation, an external intelligence IOC feed alert was raised and informed that LAB were targeted and a remote access information to 3 of their endpoints is offered for sale online in RussianMarket.
After investigating the leads the mentioned endpoints couldn't be found within the environment logs.

OVERVIEW

Report Time:	21 Oct 2021, 11:24 UTC
Incident Time:	21 Oct 2021, 11:24 UTC
Attack Surface:	Enterprise Network

Entities involved:

<Actors IP>:	10.0.0.2
LAB_DC:	933fa0a00c0249b674f7e8b59b2a0c99
VICTIM01:	1cb0fe01382f4b37655fec92cde1c356
VICTIM02:	2abf809599b5438f488406f10bb4d478

WHAT'S THE RISK

- Compromised passwords of highly privileged users are create high risk of full compromise of a corporate's environment.
- Theft of the `krbtgt` NT hash is extremely dangerous since with this user it is possible to generate highly privileged TGT's in the network which grants the attacker access to every resource in the Active Directory.

IMMEDIATE ACTION ITEMS

- Reset `krbtgt` and svc users passwords, since they have been exposed to a successful logon attempt.
- Restrict logon of local accounts from a remote machine (i.e. Do not allow for a local account such as `Administrator` to log in from a remote machine), since local accounts should only be used locally.
- It is strongly advised to ensure that the password of the local administrator account on machines is unique, in order to mitigate potential PtH (Pass the Hash) attacks. LAPS solution is highly recommended.
- Quarantine the machine behind the IP `10.0.0.2` as it considered compromised.
- It is advised to block C2 suspected IPs in the firewall.

EVENTS TIMELINE

VICTIM01

2021-09-29 16:54:54

- Ping from attacker to this machine
- Succesful logon with local `Administrator`
- used `wmiexec.py` to execute several discovery commands:

```
cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$\__1632935152.1 2>&1
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$\__1632935152.1 2>&1
cmd.exe /Q /c quser 1> \\127.0.0.1\ADMIN$\__1632935152.1 2>&1
cmd.exe /Q /c klist 1> \\127.0.0.1\ADMIN$\__1632935152.1 2>&1
```

#CrowdStrike logs

The attacker performed several Discovery commands to view active users and stored Kerberos tickets

VICTIM02

2021-09-29 17:08:29

Failed logon with local `administrator`

LAB_DC

2021-09-29 18:13:59

- Successful logon with svc user
- used `wmiexec.py` to execute several discovery commands:

```
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$\__1632939229.6971009 2>&1
cmd.exe /Q /c whoami /all 1> \\127.0.0.1\ADMIN$\__1632939229.6971009 2>&1
cmd.exe /Q /c whoami 1> \\127.0.0.1\ADMIN$\__1632939229.6971009 2>&1
cmd.exe /Q /c hostname 1> \\127.0.0.1\ADMIN$\__1632939229.6971009 2>&1


cmd.exe /Q /c secretsdump.py -just-dc-user 'krbtgt' lab.com/svc:passwd@LAB_DC.lab.com
1> \\127.0.0.1\ADMIN$\__1632939229.6971009 2>&1
```

#CrowdStrike logs

The attacker performed several Discovery commands and then attempted to steal `krbtgt` NT hash by operating DCSync attack.
It is assumed that the last command was DCSync execution which was accidentally executed on the DC itself within the `wmiexec` shell instead of on the attacker's device.

CYBER KILL CHAIN DISSECTION

Initial Access
10.0.0.2 - Attacking Machine
Windows machine, possibly running a Linux virtual machine. At the moment, the initial access of the actor is unknown.

Persistence
Not known at the moment.

Privilege Escalation
As it is believed that `secretsdump.py` ran, it is believed that the actor gained `krbtgt` account NT hash which allows him to operate Golden Ticket attack (T1558.001).

Defense Evasion
The actor have not being seen performing any defense evasion technique.

Credential Access
10.0.0.3 - DC
2021-09-29 04:23:45
The actor seemed to run, probably by mistake, `secretsdump.py` script aimed to extract the `krbtgt` user NT hash by operating DCSync attack. The command failed to run.
It's believed that the actor later on ran the command from its attacking machine and successfully obtained the `krbtgt` user NT hash though no evidence were found in currently ingested logs to approve it. This can be ensured by inspecting event ID 4662 on the attacked domain controller.

Discovery
The Actor executed Discovery commands on both machines:

- VICTIM02
- LAB_DC

Lateral Movement
A successful logons were observed in 2 machines originated from `10.0.0.2` with logon type 3 and authentication package of NTLM:
The VICTIM01 at 10.0.0.4 with a local `Administrator` user.
The LAB_DC at `10.0.0.3` with a service account user svc.

Collection
The actor have not being seen performing any collection actions.

Command & Control
Several IPs are suspected as C2 IPs as they were contacted only by the attacking machine and they were seen for the first time close to the time of the attack:

- `111.111.111.111`
- `222.222.222.222`
- `33.33.33.33`

Exfiltration

No exfiltration actions were seen.

HUNT RELEVANT DATA SOURCES

- CrowdStrike Logs
- PAN Logs