National Cyber Security Centre

Cyber Security Advisory

CSA-006-17

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

4 April 2017

Detecting the Misuse of Administrative Credentials

Summary

1. The NCSC's experience responding to security incidents has revealed that in almost all sophisticated cyber intrusion cases, attackers deliberately seek out and then use administrative[1] credentials to further compromise systems. In some instances, attackers have obtained credentials from a compromised third party provider who had access into the victim organisation's network.
2. The NCSC has also noted that malicious cyber actors are increasingly moving away from the use of malware, preferring instead to use legitimate means of remote access such as Virtual Private Networking (VPN) or Remote Desktop Protocol (RDP), leveraging stolen credentials.
3. These trends have increased the importance of detecting administrative credential misuse, as traditional security measures such as antivirus or edge security appliances are increasingly failing to detect intrusions.

Details

4. One of the key goals of many attackers early in an intrusion is to obtain the highest level of privileged access possible. This ensures they can establish persistent access across the network and not be hindered by any access controls when completing their operational goals. Sometimes attackers will create their own administrative accounts once they have the appropriate privileges to do so.
5. Attackers will often obtain access to these credentials through the usage of credential dumping tools and leverage stolen hashes through pass-the-hash style attacks. These tools are often open source with a few common examples being "Mimikatz" and "secretsdumper.py".

[1] For the purposes of this advisory, administrative credentials will predominantly refer to Windows accounts in either the Local or Domain Administrator groups but can also be taken to mean accounts with similar levels of access on other operating systems, such as the root account on Linux.

6. Sometimes, through outsourcing or other third party relationships, third party entities will have access into their customer's networks. This means that a compromise of one organisation will have flow on effects for others. A public demonstration of this was the breach of a major US retailer in 2013, where cyber criminals reportedly gained initial access by compromising the retailer's air conditioning contractor. Although this level of external access is sometimes required, it can expose organisations to new risks.
7. Once an attacker has administrative credentials and a legitimate means of remotely accessing systems, such as RDP or VPN access, there is no longer a requirement for the attacker to use malware to access systems. If an attacker is using these typically legitimate means for access, they will blend into typical usage patterns and be harder to detect.
8. In order to improve detection rates for these kinds of intrusions it is important for systems administrators and/or security teams to be able to properly audit and detect the misuse of privileged accounts.

Prevention Recommendations

9. *Minimise administrative privileges* - One of the most important measures organisations can take to prevent the misuse of administrative credentials is to minimise user privileges on their systems. This will both minimise the chances of an attacker initially gaining access to privileged credentials and will reduce background noise related to their use, improving the chances of detection. A simple control to help minimise administrative credential use is to give administrators two accounts: one with user privileges for normal usage and an account with administrative privilege for usage only when they specifically require it. Further information on implementing least privilege can be found under the ASD Essential Eight mitigations: https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm#mitigation4
10. *Implement further access controls around privileged accounts* – Given the powerful nature of privileged accounts, they generally warrant higher levels of access control than standard user accounts. At a minimum, the following controls should be implemented:
    a. Disallow remote logons for accounts with administrative permissions.
    b. Enforce second factor authentication or one-time passwords for accounts with administrative privileges.
11. *Fully appraise the risk from external access* – Organisations need to consider the risk whenever outsourcing or allowing external organisations to access their IT infrastructure. Organisations should ensure that these third parties maintain a level of security practice that they would consider appropriate for their own information assets. The possibly of a third party compromise and what effect that would have on their own networks must be considered.
12. *Consider specific credential management solutions* – Depending on organisational requirements, a solution designed specifically to manage privileged credentials may

be appropriate. Many vendors are offering what are known as Privileged Identity Management (PIM) or Privileged Access/Account Management (PAM) systems which can implement advanced controls and assist in the management of credentials.

Detection Recommendations

13. *Log and audit administrative privilege use* – In order to detect misuse, organisations must establish a suitable means to both audit and log the usage of administrative credentials. Logs will have to be centralised and effectively aggregated to allow for full visibility into the locations where administrative credentials are used. For a list of the types of logs that should be retained see the ASD advisory at: https://www.asd.gov.au/publications/protect/Cyber_Security_Incidents_Are_You_Ready.pdf.

    Specific logging requirements for administrative credentials will vary depending on individual organisations but at a minimum should cover:

    a. The creation of new accounts with administrative privilege.
    b. The addition of administrative privileges to existing accounts.
    c. Reactivation of disabled accounts with administrative privileges.

14. *Proactively monitor privileged accounts* – Although traditional logging and auditing will go a long way to help detect privileged account misuse, active monitoring or "threat hunting" related to administrative credentials will help detect their misuse in a more timely manner. This will involve developing a baseline of what normal administrative credential use looks like on your network and investigating any deviations from this, such as logons from unexpected locations or privileged accounts accessing systems they are not responsible for administering.

15. *Detection of pass-the-hash attacks* – The NSA logging guidelines details how to detect pass-the-hash style attacks through analysis of the Windows Event Log: https://www.iad.gov/iad/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm

    (note that this website presents a self-signed certificate from the US DoD and will cause your browser to prompt you with a warning).

16. *Vendor based detection solutions* – There are a range of security appliances and software-based solutions designed specifically to detect privileged account misuse or other related indicators of compromise. Although the NCSC does not specifically endorse any particular vendors or security products, the following are examples of these solutions[2] which may be worth further investigation for your organisation:
    a. Microsoft Advanced Threat Analytics.
    b. LogRhythm – User Threat Analytics Module.
    c. Canary honeypots.

[2] The NCSC has not evaluated any of these products for effectiveness and emphasise that organisations must thoroughly evaluate any vendor solution to ensure it meets their individual organisation's requirements.

*The NCSC can be contacted by email via **incidents@ncsc.govt.nz** or by phone on: **04 498 7654**. We encourage you to contact us at any time if you require any further assistance or advice.*