FRACTAL INDUSTRIES

Advanced Cyber Decision Platform™ (ACDP)

Use Case: Credential Compromise Detection

Kerberos is a computer network authentication protocol employed across most enterprise networks and is the default authentication method for Microsoft Active Directory (AD) to enable authentication for enterprise services. As bad actors dig deeper into networks, Kerberos becomes a very attractive target for privilege escalation and achieving persistant, undetected access using methods such as Golden Ticket (forged Ticket Granting Ticket or TGT) or Silver Ticket (forged Ticket Granting Service or TGS) attacks.

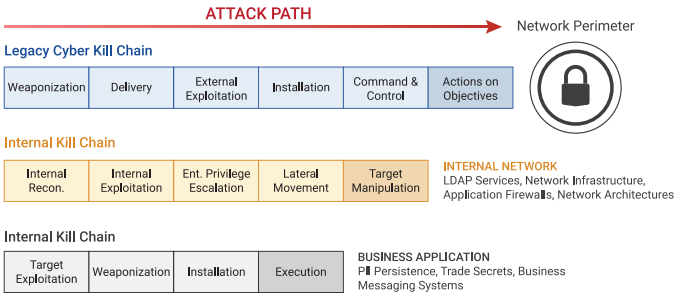


Fig.1 Attack Path: The path an attacker takes to penetrate networks is complex and spans multiple iterative phases. The attacker must penetrate your network perimeter, identify their target, and expand access to steal data from protected systems. Key to this process is a quiet method of escalating privileges to acquire access to the target.

As a stateless protocol, Kerberos transactions during the authentication process are not retained throughout or after the session, which makes it susceptible to known attacks that allow bad actors to forge Kerberos tickets or reuse stolen credentials to move laterally through the network undetected, escalating privileges until they obtain full control over files, servers, and services.

This vulnerability is widely thought to have played a critical role in some of the most publicized hacks in history, including the OPM breach of 2015[1] (during which 4 million sensitive records were exposed) and the DNC breach of 2016[2] (during which almost 20K sensitive emails were leaked). Historically such exploits have been virtually impossible to detect without the focused efforts of experienced incident responders conducting manual forensic analysis.

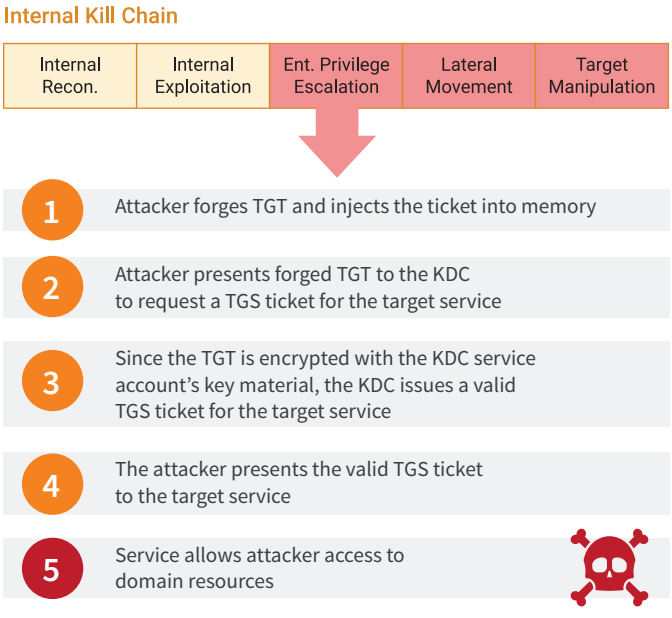
ACDP™ takes an entirely innovative approach instead. By instrumenting critical endpoints such as Domain Controllers and servers with proprietary agents that enable passive, stateful validation of Kerberos traffic, ACDP is the only application in the world to couple advanced data science methodologies with massively scalable analytics to detect ticket forgery attacks in near-real-time with no false positives—not by simply matching a signature but by maintaining a ledger of every Kerberos transaction on your network to validate every request for access to services.

By effectively transforming Kerberos from a stateless protocol to a stateful one, ACDP has demonstrated the ability to deterministically detect over 80 different variations of Golden and Silver Ticket attacks in less than a minute on average, with no false positives.

In addition to deterministic Golden and Silver Ticket attack detection, ACDP also provides heuristic detection of other forms of credential compromise in which attackers re-use credentials on Active Directory. By leveraging machine learning algorithms and AI-driven analytics to correlate additional log and telemetry data including Windows Event Log, proxy/firewall services, and other data sources, ACDP delivers a context-rich tapestry of user behavior over time for confident and timely detection of these other AD-based attacks as well:

- Pass-the-Hash
- Overpass-the-Hash
- Pass-the-Ticket
- Kerberoasting
- Skeleton Key
- DCShadow
- DCSync

Fig. 2 Golden Ticket Attack: If a bad actor gains access to the Kerberos key distribution center (KDC) they can subsequently issue a Golden Ticket—a Ticket Granting Ticket which enables another account to issue tickets to all enterprise services. If this occurs, attackers can move laterally across the network undetected, generating what appears to be legitimate traffic resulting from an apparently genuine authentication process.



[1] https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
[2] http://flashcritic.com/technical-forensics-of-opm-hack-reveal-pla-links-to-cyber-attacks-targeting-americans/