Identity Assurance for Active Directory Tech Spec

Protect your most critical control—authentication

Authentication is the most important technology control because identity is fundamental to your organization's activities. Enterprises authenticate their employees, customers, and partners before authorizing them to access systems, processes, and data.

QOMPLX's Identity Assurance (IA) solution safeguards the integrity of authentication processes so you can focus on running your business. Identity Assurance's detection and Active Directory monitoring capabilities are essential to keep your company's data secure.

QOMPLX's Identity Assurance solution takes an innovative, patented approach to safeguarding authentication. IA instruments critical control infrastructure endpoints such as Domain Controllers and servers with proprietary agents that passively and statefully validate Kerberos traffic. QOMPLX's Identity Assurance solution is the only application in the market that combines advanced data science techniques with massively scalable analytics to detect ticket forgery attacks in near-real-time with no false positives[1]—not by simply matching a heuristic rule or signature, but by maintaining a ledger of every Kerberos transaction on your network to validate every request for access to services.

Approach and Methodology

Kerberos is a computer network authentication protocol used across most enterprise networks. It is also the default authentication method for Microsoft Active Directory (AD) to enable authentication for enterprise services. As Figure 1 demonstrates, as bad actors dig deeper into networks, Kerberos becomes a very attractive target for privilege escalation and achieving persistent, undetected access using methods such as Golden Ticket or Silver Ticket attacks.

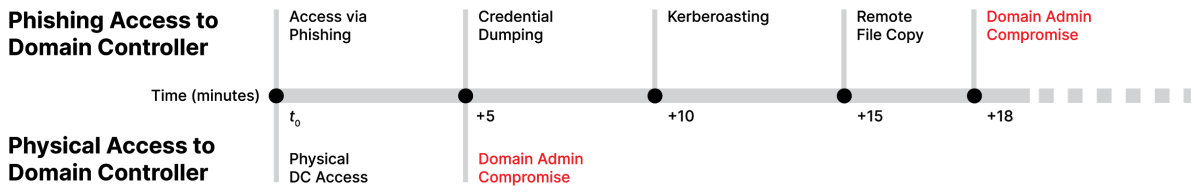

Figure 1: Attack Path Scenarios

[1] Deterministic detections, when properly configured.

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 played a critical role in some of the most publicized hacks in history.

Company	Year	Impact
MAERSK	2017	The NotPetya ransomware campaign hit the Netherlands-based global shipping company and destroyed every Windows asset connected to the network, costing Maersk over $300-million.
FedEx	2017	A subsidiary of FedEx was hit by the NotPetya ransomware campaign. It cost FedEx $300 million first-quarter revenue loss.
Marriott	2018, 2020	In 2018, Marriott was breached, resulting in the information of 500 million people being compromised. In 2020, Marriott was hit again and the attack put 5.2 million guests' information at risk.

In fact, credential forgery and privilege escalation techniques have become common factors in every large-scale ransomware attack and cyber breach of the past five years. Before now, such techniques have been virtually impossible to detect without the focused efforts of experienced incident responders conducting manual forensic analysis.

By effectively transforming Kerberos from a stateless protocol to a stateful one, QOMPLX's Identity Assurance solution can detect more than 80 variations of Golden and Silver Ticket attacks in less than 5 minutes on average, without any false positives.[2]

Identity Assurance works regardless of the tool used for the attack—Mimikatz, Cobalt Strike, Metasploit or any polymorphic or disguised variants—because it focuses on validating the protocol, and not by matching on specific tools.

In addition to deterministic Golden and Silver Ticket attack detection, QOMPLX's Identity Assurance solution also provides heuristic detection of other forms of Active Directory credential compromise.

[2] Deterministic detections, when properly configured.

Q:CYBER

Using machine learning algorithms and advanced analytics to correlate additional log and telemetry data—including Windows Event Logs, proxy/firewall services, and other data sources—QOMPLX's Identity Assurance solution delivers a context-rich picture of user behavior over time for confident and timely detection of these other AD-based attacks:

1. Golden Ticket Detection
2. Silver Ticket Detection
3. DCSync Detection
4. DCShadow Detection
5. Cloud Identity Forgery Detection (i.e., Golden SAML)
6. Skeleton Key Detection
7. Pass-the-Hash Attack Detection
8. Overpass-the-Hash Attack Detection
9. Kerberoasting Detection
10. ASRepRoasting
11. Member Added to Sensitive Group
12. Excessive Failed Login Attempts (Password Spraying)
13. Account Name Enumeration (Kerberos)
14. AdminSDHolder Modified
15. Service Installed on a Sensitive System
16. Successful Zone Transfer from Unknown Source
17. PowerShell Encoded Command Execution
18. PowerShell executed in the background
19. Discovery using built-in Windows utilities
20. Suspicious use of regsvr32
21. Honey Account Login
22. Honey Account Ticket Request

Ready to learn more about *Identity Assurance for Active Directory*? Contact us today.

+1 (703) 995-4199 | info@QOMPLX.com | www.QOMPLX.com

Why QOMPLX®

QOMPLX is the cloud-native leader in risk analytics. We help organizations make intelligent business decisions and better manage risk through our advanced, proprietary analytics platform. We are the leaders at rapidly ingesting, transforming, and contextualizing large, complex, and disparate data sources through our data factory, in order to help organizations better quantify, model, and predict risk in areas like cyber security, insurance, and finance. QOMPLX is headquartered in Tysons, VA with offices in New York, Denver, London, Cambridge, Oxford, and Montevideo. More information about QOMPLX can be found at https://www.qomplx.com/.