KERBEROS ATTACKS: WHAT YOU NEED TO KNOW

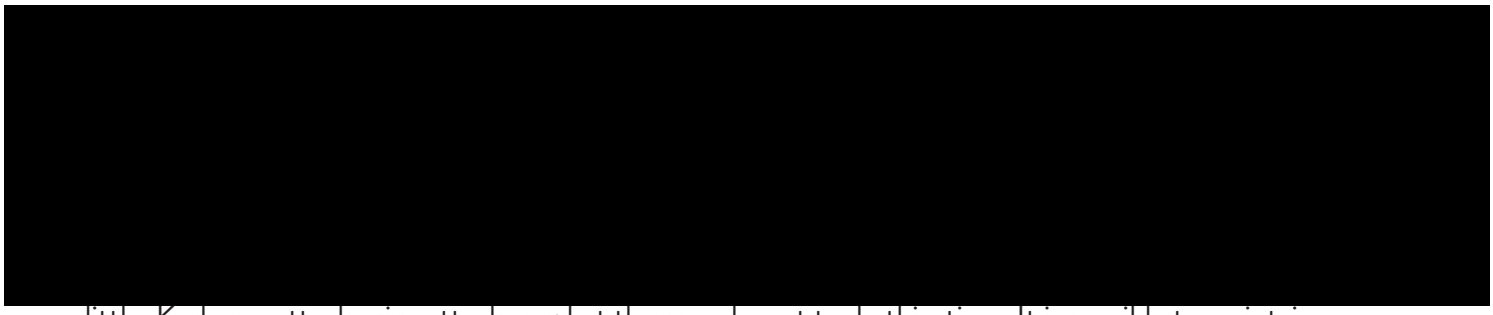
October 9, 2015 | CyberArk Labs, Security and Risk | Matan Hart

Privileged account exploitation is at the center of targeted cyber attacks, and post-mortems of today's most high-profile breaches – from Sony Pictures to Office of Personnel Management (OPM) – reveal an increasingly predictable pattern. Attackers crash through the network perimeter, hijack credentials and use them to move laterally throughout the network, taking additional credentials and escalating privileges along the way to accomplish their goals.

Combining privileged accounts with attacks on the Kerberos authentication in Windows domains raises the stakes of the cyber threat. During such attacks, threat actors target domain administrator privileges, which provide unrestricted access and control of the IT landscape. Armed with these privileges, attackers can stealthily manipulate Domain Controllers (and Active Directory) and generate Kerberos tickets to obtain unauthorized access.

Identified as one of the most dangerous attack techniques at this year's RSA Conference, Kerberos attacks are troublesome for three primary reasons:

- **Access:** Once an attacker has Local Admin privileges, it is possible to dump additional credentials, which if



little. Kerberos attacks give attackers what they need most to do this: time. It is possible to maintain persistence with Kerberos tickets, even when credentials have been changed.

While there are several types of attacks on authentication protocols – including Pass-the-Hash, Overpass-the-Hash and Pass-the-Ticket – the most destructive of all is the Golden Ticket. This technique can mean "game over" for an organization and complete loss of trust in the IT infrastructure.

InfoWorld's Robert Grimes well described this devastating attack in his article, *Fear the Golden Ticket Attack*, when he wrote, "If you have domain admin/local admin access on an Active Directory forest/domain, you can manipulate Kerberos tickets to get unauthorized access. A golden ticket attack is one in which you create a Kerberos-generating ticket that is good for 10 years or however long you choose. You can be anyone (assuming you have their hash), add any account to any group (including highly privileged groups), and for that matter, do anything you want within Kerberos authentication capabilities. You can even create usable Kerberos tickets for user/computer/service accounts that don't even exist in Active Directory. A golden ticket isn't merely a forged Kerberos ticket – it's a forged Kerberos key distribution center."

Executing this level of attack requires domain administrator credentials, putting these credentials directly in the crosshairs of any advanced attacker or malicious insider. To maintain control of your IT infrastructure, it is absolutely critical to prevent attackers from ever compromising a domain administrator credential.

CyberArk's latest Global Advanced Threat Landscape Survey revealed that far too many organizations remain focused on defending against perimeter attacks, including phishing, while discounting attacks launched from deep inside an organization, such as Kerberos attacks, that can be the most devastating. To help organizations fully understand the severity of Kerberos attacks and take actionable steps to reduce risk, we've developed a white paper – Maintain Control of Your Business: Protect Your Domain Controller from Kerberos Attacks – which is available for download. Learn about:

- Several increasingly prevalent Kerberos attack methods, which can enable control over a target's network by commandeering the domain controller;
- Key strategies for reducing risk and blocking an attacker's progress at two critical phases of the attack lifecycle: credential theft and lateral movement;
- The integral role of analytics and machine learning for early detection of anomalous activity and rapid

CATEGORIES

- Awards
- CyberArk Labs
- DevOps
- Endpoint
- Events
- Guest Blogs
- Regulations, Audit & Compliance
- Reports
- Security and Risk
- Surveys
- Technology Partners
- Uncategorized
- Videos

RECENT POSTS

- Security is a Team Game—Join the Big Leagues in CyberArk Marketplace

- When Breaches Hit Home

SCAN YOUR NETWORK

Webinar Series: On The Front Lines

Upcoming Archived