1600 - An ACE Up the Sleeve: Designing Active Directory DACL Backdoors

Friday at 16:00 in Track 3
45 minutes | Demo
Andy Robbins*Red Team Lead*

Will Schroeder*Offensive Engineer*

Active Directory (AD) object discretionary access control lists (DACLs) are an untapped offensive landscape, often overlooked by attackers and defenders alike. The control relationships between AD objects align perfectly with the "attackers think in graphs" philosophy and expose an entire class of previously unseen control edges, dramatically expanding the number of paths to complete domain compromise.

While DACL misconfigurations can provide numerous paths that facilitate elevation of domain rights, they also present a unique chance to covertly deploy Active Directory persistence. It's often difficult to determine whether a specific AD DACL misconfiguration was set intentionally or implemented by accident. This makes Active Directory DACL backdoors an excellent persistence opportunity: minimal forensic footprint, and maximum plausible deniability.

This talk will cover Active Directory DACLs in depth, our "misconfiguration taxonomy", and enumeration/analysis with BloodHound's newly released feature set. We will cover the abuse of AD DACL misconfigurations for the purpose of domain rights elevation, including common misconfigurations encountered in the wild. We will then cover methods to design AD DACL backdoors, including ways to evade current detections, and will conclude with defensive mitigation/detection techniques for everything described.
Andy Robbins
As a Red Team lead, Andy Robbins has performed penetration tests and red team assessments for a number of Fortune 100 commercial clients, as well as federal and state agencies. Andy presented his research on a critical flaw in the ACH payment processing standard in 2014 at DerbyCon and the ISC2 World Congress, and has spoken at other conferences including DEF CON , BSidesLV, ekoparty, ISSA International, and Paranoia Conf in Oslo. He has a passion for offensive development and red team tradecraft, and helps to develop and teach the "Adaptive Red Team Tactics" course at BlackHat USA.

@_wald0

Will Schroeder

Will Schroeder is a offensive engineer and red teamer. He is a co-founder of Empire/Empyre, BloodHound, and the Veil-Framework, developed PowerView and PowerUp, is an active developer on the PowerSploit project, and is a Microsoft PowerShell MVP. He has presented at a number of conferences, including DEF CON , DerbyCon, Troopers, BlueHat Israel, and various Security BSides.

@harmj0y

#defcon25/by_track/track3/friday #defcon25/By_Day/_Friday