THREATS & DEFENSES

DCEPT: An Open-Source Honeytoken Tripwire

WEDNESDAY, MARCH 2, 2016
BY: JOE STEWART

SecureWorks researchers have created a solution known as DCEPT (Domain Controller Enticing Password Tripwire) to detect network intrusions.

High-profile network breaches are occurring with increasing frequency, and when details of the attack are revealed, our network security consulting team noticed an all-too-familiar pattern is repeated: the attacker gains a foothold on a single computer on the network, then uses network-administrator credentials stolen from that system's memory cache to compromise the rest of the computers in the domain.

In Microsoft Windows networking, a domain is a group of computers that have registered with a central database known as the domain controller. Using a Windows component known as Active Directory (AD), network administrators can manage all user accounts, processes, and permissions on devices that have joined the domain. A special administrative account known as the domain administrator can authenticate to and control any computer in the domain. This all-powerful account can simplify and streamline network administration tasks, but can also provide unfettered network access to attackers. Many network administrators are unaware that using this account to log in casually to network workstations for routine maintenance carries great risk.

The best option for attackers with a foothold on a Windows network to move laterally is to obtain the domain administrator account password. By default, Windows caches login credentials in memory, and privileged local users can extract them. When a domain administrator logs in to a compromised workstation interactively (via keyboard, remote desktop, or command-line tools such as the PsExec utility), their password is stored in the credential cache. Using popular credential-theft tools such as Mimikatz, an attacker with local administrator privileges can dump the cache and read the password and/or its hash (which is as effective as the password, given how Windows authentication works). With this information, the attacker gains total control of the network.

restore an entire enterprise network is daunting. Due to the increasing prevalence and magnitude of such attacks, administrators should be selective and careful when using domain administrator credentials.

DCEPT Detections Facilitate Incident Response

Mitigation is only one part of a successful defense strategy. Another is instrumentation — being able to detect when an attack is taking place. It can be difficult to detect credential-scraping attacks using traditional intrusion detection techniques, because the only network indications are network logins that appear typical at the packet level. Solutions that look for suspicious patterns of login activity are often costly and require training to identify "normal" activity.

SecureWorks researchers have devised a simple tripwire-style intrusion detection system for Active Directory (AD) based on honeytokens. In information security, honeytokens are pieces of information, seeded on a network, that reveal that an attack is taking place when they are accessed or used. Honeytokens can be elements such as a user account, a database entry, an email address, or a document. The concept is not new; the term was first coined in 2003 by Augusto Paes de Barros, and the technique has been in use since before then.

SecureWorks is releasing the DCEPT proof-of-concept honeytoken-based Active Directory intrusion detection system as open-source code to benefit network administrators. SecureWorks researchers expanded a basic idea suggested by SANS handler Mark Baggett in a February 2015 blog entry titled "Detecting Mimikatz Use On Your Network." In addition to detecting that a domain privilege escalation is being attempted, DCEPT identifies which computer the honeytoken credential was stolen from and when. This information can be very useful to the victim organization's incident response team. The DCEPT tool consists of three parts: an agent that puts a honeytoken domain administrator password into memory on endpoints, a network service that generates unique honeytokens at the request of an agent, and a sniffer service that looks at network traffic for signs that the honeytoken password is being sent in an authentication request.

DCEPT Agent

The agent puts honeytoken credentials into memory by calling the CreateProcessWithLogonW Windows API to launch a suspended subprocess with the LOGON_NETCREDENTIALS_ONLY flag. It refreshes this process with a default time period of one day, obtaining new honeytoken credentials from the DCEPT generation server each time.

The sniffer process runs alongside the generation server and looks for Kerberos pre-authentication packets destined for the AD domain controller that match the honeytoken username. Upon receiving one of these packets, DCEPT attempts to brute-force decrypt the contents using all of the honeytoken credentials stored in the database. If a packet is successfully decrypted, then a generated alert reveals the name of the compromised computer the honeytoken password was stolen from and the time period when it happened.

Deploying DCEPT

DCEPT can be downloaded from GitHub. A Docker container build for the server component simplifies deployment. The agent is provided as C# source code only so network administrators can audit and compile it before deploying to endpoints. Instructions for installation are provided in the repository.

Tags: OPEN SOURCE INTRUSION DETECTION SYSTEM

RELATED CONTENT