

BSides Charm (2017) Talk Slides Posted – Detecting the Elusive: Active Directory Threat Hunting

Event IDs that Matter: Domain Controllers

EventID	Description	Impact
4768	Kerberos <u>auth</u> ticket (TGT) was requested	Track user <u>Kerb auth</u> , with client/workstation name.
4769	User requests a Kerberos service ticket	Track user resource access requests & <u>Kerberoasting</u>
4964	Custom Special Group logon tracking	Track admin & “users of interest” logons
4625/4771	Logon failure	Interesting logon failures. 4771 with 0x18 = bad pw
4765/4766	SID History added to an account/attempt failed	If you aren’t actively migrating accounts between domains, this could be malicious
4794	DSRM account password change attempt	If this isn’t expected, could be malicious
4780	ACLs set on admin accounts	If this isn’t expected, could be malicious
4739/643	Domain Policy was changed	If this isn’t expected, could be malicious
4713/617	Kerberos policy was changed	If this isn’t expected, could be malicious
4724/628	Attempt to reset an account's password	Monitor for admin & sensitive account pw reset
4735/639	Security-enabled local group changed	Monitor admin/sensitive group membership changes
4737/641	Security-enabled global group changed	Monitor admin/sensitive group membership changes
4755/659	Security-enabled universal group changed	Monitor admin & sensitive group membership changes
5136	A directory service object was modified <small>Sean Metcalf [@Pyrotek3 sean@TrimarcSecurity.com]</small>	Monitor for GPO changes, admin account modification, specific user attribute modification, etc.

I recently presented my talk “Detecting the Elusive: Active Directory Threat Hunting” at BSides Charm in Baltimore, MD.

Slides are now posted in the [Presentations section](#).

I cover some of the information I’ve posted here before:

- [PowerShell Security](#)
- Detecting Kerberoasting: [Part 1](#) and [Part 2](#)

On Sunday, April 30th, 2017, I spoke at BSides Charm in Track 2 at 2pm.

Here’s the talk description from the [BSides Charm website](#):

Detecting the Elusive: Active Directory Threat Hunting

Attacks are rarely detected even after months of activity. What are defenders missing and how could an attack be detected?

This talk covers effective methods to detect attacker activity using the features built into Windows and how to optimize a detection strategy. The primary focus is on what knobs can be turned and what buttons can be pushed to better detect attacks.

One of the latest tools in the offensive toolkit is “Kerberoast” which involves cracking service account passwords offline without admin rights. This attack technique is covered at length including the latest methods to extract and crack the passwords. Furthermore, this talk describes a new detection method the presenter developed.

The attacker’s playbook evolves quickly, defenders need to stay up to speed on the latest attack methods and ways to detect them. This presentation will help you better understand what events really matter and how to better leverage Windows features to track, limit, and detect attacks

This presentation covers the type of log data required to properly

For the curious, here’s an outline of the talk:

- The current issues with monitoring
- Logging
 - Command logging
 - Sysinternals SysMon
 - Interesting Microsoft binaries to monitor (thanks Casey Smith! @subtee)
 - Microsoft Windows Event Forwarding (WEF)
- PowerShell Logging
 - PowerShell without PowerShell.exe (PS>Attack)
 - PowerShell obfuscation with Invoke-Obfuscation & detection
- Auditing attack activity
 - Standard auditing vs Advanced auditing
 - Recommended DC auditing
 - Special Logon auditing
 - Event IDs that matter: Domain Controllers & all Windows systems
 - Logon types (4624)
 - Password Spraying & detection
 - Kerberoasting & detection

Slides are now posted in the [Presentations section](#).

(Visited 8,017 times, 1 visits today)