Adversary Tactics: Red Team Operations

SPECTER OPS

Useful Resources

- SpecterOps Tools:
  - BloodHound https://github.com/BloodHoundAD/BloodHound
  - SharpHound (C# Ingestor) https://github.com/BloodHoundAD/SharpHound
  - PowerSploit https://github.com/PowerShellMafia/PowerSploit
  - PowerView https://github.com/PowerShellMafia/PowerSploit/tree/dev/Recon
  - PowerShell Empire https://github.com/EmpireProject/Empire
  - ACE https://github.com/Invoke-IR/ACE
  - Get-InjectedThread https://gist.github.com/jaredcatkinson/23905d34537ce4b5b1818c3e6405c1d2
  - Get-KerberosTicketGrantingTicket https://gist.github.com/jaredcatkinson/c95fd1e4e76a4b9b966861f64782f5a9
- Cobalt Strike https://www.cobaltstrike.com/

Useful Resources (cont'd)

- Apache mod_rewrite rules for AV vendors https://gist.github.com/curi0usJack/971385e8334e189d93a6cb4671238b10
- Scraper for ExpiredDomains.net and BlueCoat to find categorized domains https://github.com/t94j0/AIRMASTER
- SSL Certificates recon tool https://crt.sh
- Python LNK payload tool https://gist.github.com/HarmJ0y/ae04dd39cf851c862fff721fdd28f7db
- Active Directory enumeration without PowerShell https://github.com/fdiskyou/hunter
- Execute .NET assemblies through SQL Server https://github.com/sekirkity/SeeCLRly
- Investigating PowerShell Attacks https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/wp-lazanciyan-investigating-powershell-attacks.pdf

Useful Resources (cont'd)

- Mimikatz https://github.com/gentilkiwi/mimikatz
- PowerLurk https://github.com/Sw4mpf0x/PowerLurk
- RemoteRecon https://github.com/xorrior/RemoteRecon
- Invoke-Obfuscation https://github.com/danielbohannon/Invoke-Obfuscation
- dnSpy https://github.com/0xd4d/dnSpy
- Red Team Infrastructure Wiki https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
- DotNetToJScript https://github.com/tyranid/DotNetToJScript
- Ruler https://github.com/sensepost/ruler
- Koadic https://github.com/zerosum0x0/koadic
- UACMe https://github.com/hfiref0x/UACME

- Rattler https://github.com/sensepost/rattler
- sRDI https://github.com/monoxgas/sRDI
- aquatone https://github.com/michenriksen/aquatone
- Sysinternals https://live.sysinternals.com/
- PSReflect https://github.com/mattifestation/PSReflect
- OleViewDotNet https://github.com/tyranid/oleviewdotnet
- Hexacorn's EDR comparison matrix http://www.hexacorn.com/blog/2016/08/07/edr-sheet-explained/
- Hexacorn Beyond Run Key series http://www.hexacorn.com/blog/2017/01/28/beyond-good-ol-run-key-all-parts/
- Tracing WMI Activity https://msdn.microsoft.com/en-us/library/aa826686(v=vs.85).aspx

Useful Resources (cont'd)

- https://blog.harmj0y.net/ - Active Directory, red teaming
- https://enigma0x3.net/ - Lateral movement, persistence
- https://wald0.com/ - BloodHound, graph theory
- https://posts.specterops.io/ - cross post for all SpecterOps blogs
- http://www.exploit-monday.com/ - Windows internals, exploitation
- http://subt0x10.blogspot.com/ - "Trusted Things That Execute"
- http://adsecurity.org – Active Directory reference
- http://www.invoke-ir.com/ - PowerShell forensics and defense

Useful Resources (cont'd)

- BloodHound Slack https://bloodhoundhq.slack.com/
  - Invites: https://bloodhoundgang.herokuapp.com/
- PowerShell Empire Slack https://adaptiveempire.slack.com/
  - Invites: http://adaptiveempire.herokuapp.com/

- SpecterOps Whitepapers
  - https://specterops.io/resources/research-and-development