King Arthur's Castle (Server 2019)

Altoid0

01
Background

Whoami

- 6 Years/5 seasons of Cyberpatriot experience
- Open division All american
- 2 x National Champion
- CyberAegis Windows Officer and RvB Coordinator

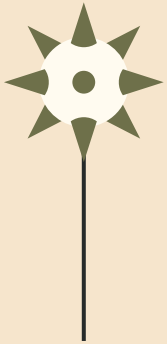
Thought Process

- CyberPatriot practice
- Realisticish vulnerabilities and misconfigurations
  - Hence why you saw no media file points
- Real world persistence mechanisms/malware
  - Cobalt Strike, Payload templates, Fileless malware, user-land drivers, DLLs
  - Lots of knowledge taken from Rasta Mouse's courses
- Asked users not to update to score hotfixes for famous vulnerabilities
  - Rewards research

Script!?1?

Pros

- Fast



Cons

- 100% gonna miss stuff
  - Causes greater confusion later on

02

Forensic Questions

Yea I hate these too

Forensic Question 1

Due to the recent breach of the kingdom's security we require you to do some investigation as to which systems the attacker was able to compromise as well as what operations they carried out on those given systems. According to the SIEM the attackers used RDP to log on to another machine within the kingdom. Due to certain artifacts windows preserves we believe you can recover information about what the attacker was doing on the other machine. Please tell us the command that ran on the machine to which they pivoted to.

Solution

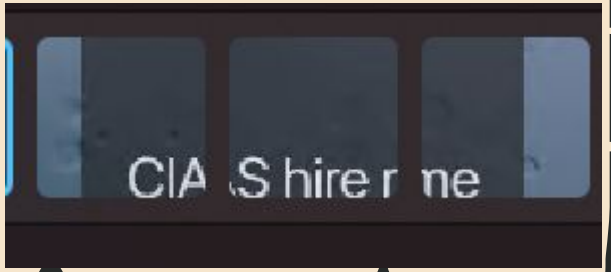
RDP Artifacts
RDP Bitmap Caching
Solution Script
- Make sure you're reading from the right Cache000X.bin

Piece images together

Answer

vaultcmd /list

Hints to another vuln on the image



Forensic Question 2

Thanks to the use of network monitoring we have identified that the previous perpetrators downloaded a copy of netcat on to the system. We know that they modified elements of defender in order for the binary to properly execute. What is the name of the setting that was modified?

Solution

Keyword here is **properly** execute
Understand that the question is referencing defender configs for a specific program
Exploit Protection

- Windows Security -> App and Browser control -> Exploit Protection Settings -> Program Settings -> twain32.exe
  - Run AV scan to identify twain32.exe as the netcat backdoor and from there look at program overrides
- Get-ProcessMitigation -RegistryConfigFilePath export.xml

Answer

Code integrity guard, SignedBinaries, BinarySignature, MicrosoftSignedOnly, AllowStoreSignedBinaries

Forensic Question 3

After the breach it is unclear which actions were carried out by the attacker and which by the previous admin. We believe some software was installed on to the system on 1/2/2023 and used for file indexing. What was product version, who is the manufacturer, and what is the full domain name this program's installer contacts during installation?

Solution Parts 1 and 2

MSI Installation Event Logs

- Get-WinEvent -FilterHashtable @{LogName='Application';ProviderName='MsiInstaller'} | FL

Answer

1.4.1.1022, voidtools

Solution Part 3

Upload installer (exe one I'm sorry) to Virustotal -> Relations tab

Answer

time.windows.com

03

Vulnerabilities

The goods

User Auditing

Active Directory Users and Computers (dsa.msc)

- Removed unauthorized user Molly McDonald
  - “Prevent object from accidental deletion”
- Removed unauthorized user t
  - “Prevent object from accidental deletion”
  - “Show only in advanced mode”
    - View -> Advanced Mode
- Ed's password is not stored using reversible encryption
  - Properties -> Account -> Store password using reversible encryption
- Binky is sensitive and cannot be delegated
  - Properties -> Account -> Account is sensitive and cannot be delegated
  - Domain admin account therefore attributing its credentials to some other task or service could be dangerous
- Punella requires kerberos preauth
  - Failure to require kerberos preauth allows for ASREProasting (bruteforce of a user’s kerberos session key)
- Removed unauthorized Schema admin Alan
- Removed unauthorized DNS admin Bitzi
  - Can lead to privilege escalation (ServerLevelPluginDLL)
- Enterprise Admins are no longer managed by Domain Users
  - Enterprise Admins -> Properties -> Managed By -> Clear
  - Changes permissions so that Domain users can update membership of the Enterprise Admin group

Local Policies

- Policies were set in 3 locations
  - Local Security Policy (secpol.msc)
  - Group Policy Management Console (gpmc.msc)
    - Default Domain Controller Policy
    - Default Domain Policy
- GPMC will override secpol when GPOs are synced
  - Hence why you see these 2 icons next to settings in secpol
    - Bottom indicates it is controlled at the GPMC level

- How fix?
  - Either set all your settings into GPMC
    - Import GPO export from LGPO
  - Or just prevent domain policy from being applied
    - Gpmc.msc -> Right click desired policy -> GPO Status -> All Settings disabled
  - Run **gpupdate /force** to sync or update

Local Policy

- A secure minimum password length is set
  - 14-20
- Audit Directory Service access [Success/Failure]
  - AD object access visibility (Could help detect intrusion based on odd enumeration)
- Audit System events [Success/Failure]
- Authenticated users cannot add workstations to the domain
  - Rouge machines (noPac CVE-2021-42287/CVE-2021-42278)
- Domain users cannot enable computer and user accounts to be trusted for delegation
- Everyone no longer has control over vulnerable Netlogon secure channel connections
  - Prevents misconfiguration of a 0day patch (Zerologon CVE-2020-1472)
- LDAP server signing requirements [Require Signing]
  - Prevents ldap communication from being tampered with
- Domain logons are not cached to disk
  - Creds can be exported and cracked offline, if the DC is working as intended no need to cache
- Use FIPS compliant algorithms for encryption, hashing, and signing [Enabled]
  - Enforce the use of mostly strong/government approved algorithms

Local Policy Cont.

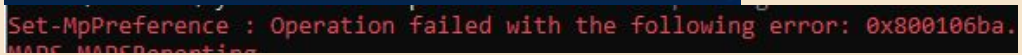
- Virtualize file and registry write failures to per-user locations [Enabled]
  - Forces non-UAC compliant apps to write to user locations preventing unintended sensitive output from being read by other users
- Users can no longer install print drivers (CVE-2021-34527 PrintNightmare)
  - Devices: Prevent users from installing printer drivers [Enabled]
  - Scenario wise this is a DC, no reason to be printing from it
- Runas different user context menu removed from start window
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoStartBanner = 1

Defensive Countermeasures

Fixing Defender

Messed with permissions on the folder in file explorer and maybe a little in registry

- Can’t edit settings?
  - 

  - 

- GUI/Commands for defender set registry keys in the same location
  - HKLM\SOFTWARE\Microsoft\Windows Defender\
- However you can also set things through GPOs which will get configured elsewhere and override
  - HKLM\SOFTWARE**Policies**\Microsoft\

Defensive Countermeasures

- Defender no longer runs in passive mode
  - HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection\ForceDefenderPassiveMode
  - Conventionally set by 3rd party AVs to ensure defender doesn't interfere with their operations
- Defender network protection enabled
  - Prevents users from accessing known malicious sites
- Defender Severe threat default action is not set to ignore
  - Threat level 5 (Severe) set to 6 (Ignore)
  - Stops defender from taking action against critical threats
- Defender ASR blocks executables in accordance with cloud based protection
  - Attack Surface Reduction rules add capabilities for defender to counter common/known exploitation techniques
  - "Block executable files from running unless they meet a prevalence, age, or trusted list criterion"
    - GUID: 01443614-cd74-433a-b99e-2ecdc07bfc25
- Defender Cloud protection is enabled
  - Needed for the above ASR rule to actually work
- Defender Attack Surface Reduction exclusions removed
  - Get-MpPreference, look for AttackSurfaceReductionOnlyExclusions
  - Since commands don't really work delete the value from registry
- Google Chrome cannot override DEP
  - Exploit protection program override
  - Windows Security -> App and Browser control -> Exploit Protection Settings -> Program Settings -> chrome.exe
    - Make sure DEP is enabled

Uncategorized Operating System Settings

- Everyone is no longer allowed full control on the SYSVOL share
  - Computer Management -> Shares -> SYSVOL -> Share Permissions -> Everyone can read
- Domain users can no longer read ntds.dit
  - C:\Windows\NTDS\ntds.dit -> Properties -> Security -> Delete domain users
- Default powershell script double click behavior not set to execute
  - HKEY_CLASSES_ROOT\Microsoft.PowerShellScript.1\Shell\(Default) not set to 0
  - Other valid options are Open and Edit which will spawn a notepad or ISE window with the given script
- Deprecated Triple DES algorithm for windows SCHANNEL disabled
  - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168\Enabled = 0
  - Triple DES has a theoretical flaw that could allow for large bits of data to produce duplicate ciphertext blocks
- NetBIOS over TCP disabled
  - HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces\Tcpip_{9e1b6253-7665-4558-8ac5-5108d39a0d59}\NetbiosOptions = 2
  - Old and unnecessary, used by red team for enumeration and spoofing
- System failures do not cause automatic memory dumps
  - HKLM\SYSTEM\CurrentControlSet\control\CrashControl\CrashDumpEnabled = 0
  - Prevents potentially sensitive information from being dumped into .dmp files if the system crashes/shuts down
  - Poorly coded apps could dump things like creds

Services

- Dimension4 service no longer vulnerable to unquoted image path privilege escalation
  - Because of the way windows reads file paths, an attacker could trick windows into loading a binary other than the intended one and executing it as a high privileged user
  - Funny enough this is windows “intended behavior”
  - To fix just add quotes around the ImagePath value in registry
- Hidden malicious cobalt strike service payload deleted
  - Display name: Windows Push Notifications User Service_b51282d
    - Hidden with SDDL permissions (won’t see service in powershell nor in the GUI)
    - Delete service binary UnistackSvcGroup.exe
      - Made with barebones service template and custom Cobalt Strike payload
    - Delete service from registry HKLM\SYSTEM\CurrentControlSet\Services\WpnUserService_b51282d
- Windows Defender Firewall service started and enabled
  - Screwed with user running service and removed some user rights
  - Easiest fix was to export the mpssvc service reg key from a clean image and import it onto this image

Application Updates

- Google Chrome has been updated
  - Renamed the binary that does the actual updates so you had to reinstall or fix the updater binary to get points
- Notepad++ has been updated
  - Forgot to mention in ReadMe, sorry

Features

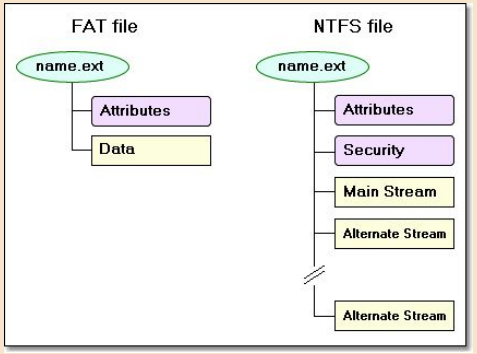
- Powershell 2.0 has been uninstalled
  - Old hence no compatibility with modern logging features like script block logging and no **AMSI**

Malware/Forbidden Files

- Malicious AMSI provider has been removed
  - Anti-Malware Scan Interface, essentially AV for powershell in-process stuff
  - Defender has its own which it uses to scan all commands
  - But you can also make your own, Microsoft literally tells you how
  - Loads DLL into powershell process every time it's executed, cool form of persistence
  - C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2211.5-0\MpAup.dll
  - Regsvr32.exe /u MpAup.dll
- WinDivert user-mode driver has been removed
  - Used to divert traffic from one port to another. Since NTLM happens over port 445 and port 445 can't be unbound from SMB you have to use a driver to intercept the traffic.
  - Diagram of attack
  - C:\Windows\System32\drivers\WinDivert64.sys
    - Signed by some random entity
      - Sigverify, driverquery.exe, sigcheck
- WMI persistence removed
  - Can be found in Autoruns
    - Autoruns only removes 1 of the 3 components.
      - Get-WMIObject -Namespace root\Subscription -Class __EventFilter -Filter "Name='Twitter'" | Remove-WmiObject -Verbose
      - Get-WMIObject -Namespace root\Subscription -Class CommandLineEventConsumer -Filter "Name='Twitter'" | Remove-WmiObject -Verbose
      - Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding -Filter "__Path LIKE '%Twitter%'" | Remove-WmiObject -Verbose

Malware/Forbidden Files

- Netsh helper dll persistence removed
  - Mitre ATT&CK explanation
  - HKLM\Software\Microsoft\NetSh\flshpnt
  - C:\Windows\System32\flshpnt.dll
- Alternate data stream with PII removed
  - Explanation
    - Normally data just gets stored into the default $DATA stream
    - But you can create another one and “link” it to a file
  - Lots of utilities to check for ADS
    - dir /r C:\Windows
  - Remove using streams.exe -d C:\Windows
- Credentials stored in Credential Manager DPAPI deleted
  - Answer to FQ1 hinted at this, run vaultcmd /list to show creds saved in DPAPI
  - C:\Users\Arthur\AppData\Roaming\Microsoft\Credentials\9E31F631DE47CF11A203910DD767293F
  - Vulnerable because by obtaining a master key from the system the creds can be cracked offline
- RDP Bitmap cache leaking plaintext credentials deleted
  - Related to FQ1, now that you know RDP bitmaps can build pictures of the target computers you should also realize that it can expose credentials
- Volume shadow copy with insecure SAM permissions deleted
  - Back up of the C drive, preserves permissions of files, and in this case the backup allowed users to read SAM aka get password hashes
  - vssadmin list shadows
  - vssadmin delete shadows /for=c:



Application Security

- LDAP SSL certificate created and configured
  - Install AD Certificate Services through server manager and configure it when prompted after install
  - Default options were fine
- LDAP anonymous access above rootDSE has been disabled
  - Allows anonymous access to parts of LDAP which could be used to enumerate information
  - LDAP://CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=lakewood,DC=local dSHeuristics
  - ADSI Edit -> Change Default Naming Context to Configuration -> Browse to path above -> Right click and locate dSHeuristics -> Clear or set it to 7 0's
- ElwoodPreschool is no longer allowed to delegate to the Domain Controller DNS server
  - Dsa.msc -> Right click computer -> Properties -> Delegation -> Delete delegation and/or Do not trust computer for delegation
- Pre-Windows 2000 computer account OnceUponARestaurant deleted
  - If there is an actual computer joined to the domain it will say its OS when you look at the computer in dsa.msc
  - If it is just a machine account with no actual computer as it is on this image you have to red team yourself a little
    - Using Impacket to test

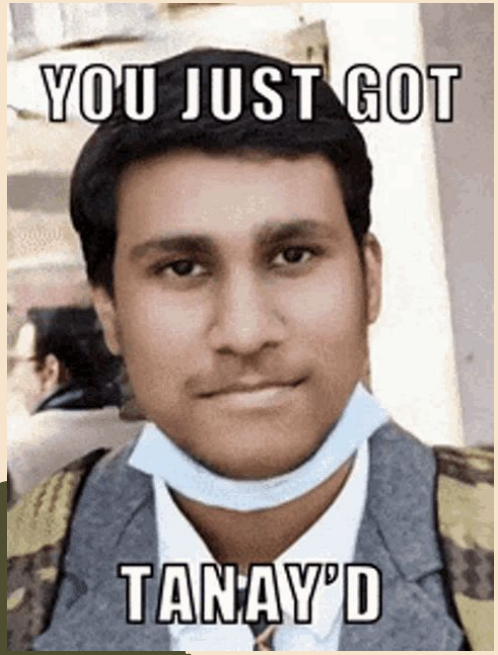
Application Security

- DNS zone lakewood.com is Active Directory integrated
  - Makes it so data is stored in AD, better for managing permissions and replicating data if needed
  - Must do this before you sign the zone or implement DNSSEC
  - Dnsmgmt.msc -> Lakewood.local -> Properties -> General -> Change zone type -> Check bottom box
- DNS zone lakewood.com is signed
  - Verifies the validity of the data DNS is returning
  - Dnsmgmt.msc -> Lakewood.local -> Right click -> DNSSEC -> Use default options
  - Now you have to configure DNS to actually validate stuff
    - dnscmd /config /enablednssec 1
    - dnscmd /config /retrieveroottrustanchors
- DNS global query block list disables IPv6 to IPv4 tunneling
  - Explanation
  - HKLM:\SYSTEM\CurrentControlSet\Services\DNS\Parameters\GlobalQueryBlockList
    - Includes isatap
  - dnscmd /config /enableglobalqueryblocklist 1
- DNS diagnostic logging for ServerLevelPluginDLLEvent enabled
  - Known privilege escalation vulnerability allowing people to go from Dnsadmin to SYSTEM by adding a DLL plugin to the server
  - Must enable logging to detect attacks like this
    - Set-DnsServerDiagnostics -EnableLoggingForPluginDllEvent $true

Application Security

- DNS rate limiting enabled and configured
  - Can help prevent against DoS vulerabilities, as it stands on the image there were some configurations set that could cause overloading problems
  - Set-DnsServerRRL -Mode Enable -Force
  - Set-DnsServerResponseRateLimiting -ResetToDefault -Force
- DNS protects against cache poisoning from fragmentation attacks (CVE-2020-25705)
  - Explanation
  - Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\DNS\Parameters" -Name MaximumUdpPacketSize -Type DWord -Value 0x4C5 -Force
- Google Chrome browser syncing disabled
  - HKLM\SOFTWARE\Policies\Google\Chrome\SyncDisabled = 1
  - Syncing in modern day browsers does a lot like syncing settings, bookmarks, history, extensions
    - All things that an org would want to control and could present security issues

Thanks for Playing



Altoid0#9779
https://twitter.com/Altoid0day