Kompromitēta domēna atpazīšana un atgūšanās pēc uzbrukuma

CERT.LV ir konstatējusi veiksmīgus uzbrukumus *Microsoft (MS) Exchange* serveriem Latvijā. Uzbrukumos tika izmantotas ievainojamības CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065. Pastāv risks, ka uzbrucēji ne vien iegūst darbinieku e-pastu piekļuves datus, piekļuvi e-pastu sarakstēm un adrešu grāmatiņai, bet iet soli tālāk un veic darbības, kas var kompromitēt visu uzņēmuma tīkla infrastruktūru, ļaujot piekļūt domēna kontrolierim *(Domain Controller)* un aktīvajai direktorijai *(Active Directory)*.

Apdraudētas ir visas aktuālās, lokālās (*on-premises*) *MS Exchange* versijas. CERT.LV aicina uzskatīt visus apdraudētos *MS Exchange* serverus, kam februāra beigās - aprīļa sākumā web interfeiss (owa, ecp, ews vai autodiscovery) ir bijis pieejams no interneta, par kompromitētiem, līdz brīdim, kad ir veiktas atbilstošas pārbaudes un tajās ir apstiprināts pretējais. Pārbaužu veikšanai CERT.LV iesaka izmantot sekojošus rīkus no Microsoft: https://github.com/microsoft/CSS-Exchange/tree/main/Security

Esam apkopojuši vadlīnijas rīcībai gadījumā, ja gūts apstiprinājums tam, ka domēns ir kompromitēts. Jāpiezīmē, ka katra infrastruktūra ir atšķirīga un ne visiem gadījumiem šeit aprakstītais ir piemērojams, tāpēc aicinām izvērtēt un ņemt vērā šeit aprakstīto savu iespēju robežās.

Uzbrukumos izmantotās pamatmetodes un to atpazīšana

Pass The Hash (PTH) – šī ir metode, kas ļaundariem ļauj pārvietoties pa domēnu, autentificējoties kā konkrētam sistēmas lietotājam\servisam\iekārtai (sauksim to par upuri) bez tiešas piekļuves upura parolei (*cleartext* formā), jo tiek izmantota paroles *hash* vērtība, kas tiek izgūta no aktīvās direktorijas un/vai Local Security Accounts Manager SAM datubāzēm . https://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf

PTH uzbrukumā tiek izmantotas uz iekārtas glabātās paroļu hash vērtības, kas parasti ir iegūtas no `LSASS.EXE` procesa atmiņas - atbildīgs par autentifikāciju. Incidenta konstatēšanai nepieciešams monitorēt Windows žurnālfailu EventID 4688 un skatīties, vai vecāka *(parent)* process ir, piemēram, cmd.exe vai powershell.exe, no kura ir palaists apakšprocess ar lsass.exe – šī būtu uzskatāma par anomāliju. Monitorēt visus pieslēgšanās mēģinājumus (*logon*) un piekļuves datu *(credentials*) izmantošanas novirzes no normas t.i. lietotājs pieslēdzas no darbstacijas, kuru nekad nav lietojis (EventID 4624) vai notiek vairākkārtīgi nesekmīgi pieslēgumi (EventiID 4625); neparasts darba laiks, kurā notiek pieslēgumi. Pieslēgumi, kas korelē ar citiem notikumiem, piemēram, izpildāmo datņu (.exe) palaišanu vai servisu/reģistra vērtību/plānoto uzdevumu (*scheduled tasks*) izveidošanu un palaišanu – varētu norādīt uz ļaunprātību. Windows Security žurnālfailos redzot EventID 4624 un 4625 ar LogonType 3 autentifikācijas metodi, jāpievērš uzmanība tiem notikumiem, kas nav saistīti ar domēnu un nav kā *Anonymous.* Mimikatz ir populārākais rīks, kas tiek izmanto PTH uzbrukumos – ja redzat EventID 4624 ar LogonType 3 un SecurityID: xxxx\Administrator AccountName:YYYYY (respektīvi, AccountName nav tukšs `-` un nesakrīt ar SecurityID, un noteikti uzrādās kā Administrator) tas ir uzskatāms kā artifakts, ka šis rīks ir ticis izmantots.

Vairāk par Windows žurnālfailu EventID, kurus monitorēt PTH un PTT (Pass The Ticket) uzbrukumos, skatīt dokumenta beigās (PIELIKUMS). Par to, kā ieslēgt visus svarīgākos EventID (jo pēc noklusējuma lielākā daļa no nepieciešamajiem EventID netiek monitorēti) varat lasīt CERT.LV sagatavotajā rakstā par MS Windows domēnu auditēšanu:
https://cert.lv/uploads/iestadem/Rekomendacijas_audit_Win_2020.pdf

Papildus informāciju par Windows žurnālierakstu EventID vērtībām un to, kam pievērst uzmanību, lai pamanītu gan Mimikatz, gan citu populāru paroļu ‘zadzēju’ rīku, piemēram, Windows Credential Editor (WCE) mēģinājumus izgūt no iekārtas atmiņas lietotāju paroles un/vai hash vērtības, lasīt šeit: https://jpcertcc.github.io/ToolAnalysisResultSheet/ pie sadaļas `Password and Hash Dump`.

Pass The Ticket (PTT) – šī ir metode, kas uzbrucējam ļauj autentificēties domēnā kā sistēmas lietotājam, izmantojot Kerberos biļetenus *(Kerberos tickets)* bez piekļuves upura (šajā gadījumā tie ir servisu un darbstaciju/serveru konti) *cleartext* paroles formātam.

- Silver Ticket – tiek izmantota servisu konta paroles hash vērtība, lai piekļūtu servisiem, kas izmanto Kerberos kā autentifikācijas protokolu gan konkrētam resursam, gan sistēmai, kas uztur šo resursu (piemēram, MSSQL, Sharepoint u.c.).
- Golden Ticket – uzbrucējs, kuram ir piekļuve Key Distribution Service konta (KRBTGT) paroles hash vērtībai, var pats ģenerēt TicketGrantingTickets (TGT) t.i. uzbrucējs var veikt autentifikācijas domēnā kā jebkurš cits konts (piemēram, lietotājs, serviss, darbstacija/serveris), kas eksistē domēna aktīvajā direktorijā.

Arī pie šīs uzbrukuma metodes vispopulārākais rīks ir Mimikatz. Papildus informāciju par Windows EventID, kurus monitorēt, lai identificētu PTH un PTT uzbrukumus, meklējiet https://jpcertcc.github.io/ToolAnalysisResultSheet/ pie sadaļām `Pass-the-hash`; `Pass-theTicket`; `Capturing Domain Administrator Rights Account`.

Paroļu hash vērtību izgūšana no domēna kontroliera – ir vairāki paņēmieni, kā uzbrucējam iegūt visu domēna lietotāju hash vērtību kopiju. Visbiežāk mēģina izmantot jau iebūvētos sistēmas rīkus, lai nepievērstu sev lieku uzmanību.

- Var izmantot, piemēram, iebūvēto **`ntdsutil`** *(Active Directory domain services management utility)*, kas tiek izmantota arī leģitīmu AD rezerves kopiju izveidei, bet šajā gadījumā ļaundarim ir nepieciešamas jau Domēna Administratora tiesības. Papildus informāciju par Windows EventID, kurus monitorēt, lai pamanītu neparastas šīs rīka darbības, meklējiet https://jpcertcc.github.io/ToolAnalysisResultSheet/ pie sadaļas ` Information Collection`.
- Vēl viena populāra metode ir **DCSync**, ar kuru var izgūt lietotāju paroles no aktīvās direktorijas (tai skaitā KRBGT;Administrators utt.), izliekoties par vēl vienu kontrolieri domēnā. DCSync funkcionalitāte ir iekļauta arī plaši

lietotajā Mimikatzs rīkā (nav obligāti jābūt domēna administratora tiesībām- var būt Enterpise Admin vai Administrators grupā, kā arī var izmantot DC darbstaciju/serveru kontus). Šeit aizdomīgus notikumus var pamanīt, ja tiek monitorēti DC žurnālieraksti, kas attencināmi uz 'replication requests' (it īpaši, ja šādi pieprasījumi nāk no IP adresēm, kas nepieder domēnu kontrolieriem).

Diemžēl, ir daudz un dažādi paņēmieni, kā izgūt šo informāciju arī neizmantojot ntdsutil vai DCSync metodi, un visus gadījumus nav iespējams aprakstīt, tāpēc šeit var lasīt apkopojumu arī par citām metodēm un rīkiem - https://pentestlab.blog/tag/ntds-dit/

Vairāk par Microsoft Windows rekomendēto žurnālfailu EventID, kurus ieteicams monitorēt PTH un PTT uzbrukumos, skatīt dokumenta beigās (PIELIKUMS).

Risku mazināšana un atgūšanās pēc uzbrukuma (Mitigation/Hardening)

- Uzstādīt drošības atjauninājumu **KB2871997** (Windows 7, Windows 8, Windows Server 2008R2, Windows Server 2012), lai *clear-text* formātā netiktu glabāti lietotāju dati Local Security Authority Subsystem Service (LSASS) atmiņā. Kā arī sniedz citus drošības uzlabojumus - https://msrc-blog.microsoft.com/2014/06/05/an-overview-of-kb2871997/
- Nodrošināt, ka lietotāju (tai skaitā darbstaciju un servisu kontiem) piekļuves dati ir unikāli (tātad arī to paroļu hash vērtības būs unikālas), lai uzbrucēja iespējas pārvietoties pa domēnu būtu maksimāli samazinātas. Limitēt domēna administratorus – atļauja pieslēgties tikai DC un, ja nepieciešams, atsevišķiem serveriem. Nepieļaut viena un tā paša domēna lietotāja esamību lokālā administratora grupā uz vairākām iekārtām. Lokālo administratoru paroļu pārvaldībai iesakām izmantot Microsoft izveidoto rīku *Local Administrator Password Solution (LAPS):* https://www.microsoft.com/en-us/download/details.aspx?id=46899
- Iesakām veikt domēna lietotāju, izmantoto paroļu un/vai hash analīzi, lai gūtu priekšstatu, pēc kādiem kritērijiem lietotāji izvēlas paroles, un identificētu

potenciāli vājās vietas (konkrēts departaments) jeb sistemātikas modeli, kuru nepieciešams mainīt ar stingrāku paroļu politiku. Šim mērķim var izmanto Domain Password Audit Tool (DPAT) rīku (šādu darbību veikšana noteikti jāsaskaņo vadības līmenī): https://github.com/clr2of8/DPAT

- Uz Windows 10 un Windows Server 2016 uzstādīt Windows Defender Credential Guard, kas izmanto uz sistēmas pieejamās virtualizācijas iespējas (ja iekārta to nodrošina) un spēj izolēt piekļuves datus *(credentials*) no pašas operētājsistēmas: https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard
- *User Account Control* ieslēgšana uz lokālo lietotāju kontiem (ja iekārta nav domēnā), veidojot iekšējos tīkla pieslēgumus. To dara ar sekojošu reģistra atslēgu (iestatām vērtību 0 un pārliecināmies, ka RID 500 konts – Administrator (vai jebkas cits, uz ko tas ir pārsaukts) ir atslēgts):

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy
```

GPO: Computer Configuration > [Policies] > Administrative Templates > SCM: Pass the Hash Mitigations: Apply UAC restrictions to local accounts on network logons

- Pārliecināties, ka darbstaciju konti nav pievienoti administratoru grupām, un mainīt šo kontu paroles vismaz reizi 30 dienās.
- Visiem administratoru un servisu kontiem atzīmēt parametru “Sensitive and cannot be delegated” - https://docs.microsoft.com/lv-lv/archive/blogs/poshchap/security-focus-analysing-account-is-sensitive-and-cannot-be-delegated-for-privileged-accounts
- Pārbaudīt eksistējošos servisu kontus – daudzi no ‘vecajiem’ servisiem mēdz saturēt beztermiņa paroli *(Password never expires*). Šādas vērtības nepieciešams likvidēt un uzstādīt paroli ar vismaz 30 simboliem. Vēl labāk, ja var ieviest *Group Managed Service Accounts* (gMSAs) vai *Standalone Managed Service Accounts* (sMSAs), jo tad servisu parole būs 240 simbolus gara un automātiski rotēs ik pēc 30 dienām - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/service-accounts-group-managed

- Atslēgt NTML autentifikācijas protokolu, un tā vietā izmantot Kerberos - https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain
- Atteikties no *LAN Manager* (LANMAN jeb LM) paroļu hash vērtību uzglabāšanas sistēmās, pievienojot reģistram papildus atslēgu `NoLMHash` ar vērtību 1 (LM hash vērtība pazudīs no sistēmas tikai, kad lietotājs nākamreiz nomainīs paroli) - https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/prevent-windows-store-lm-hash-password
- Administratoru kontiem izmantot *Protected Users* grupu, kas novērsīs šo lietotāju paroļu hash vērtības izgūšanu no sistēmas, piemēram, ar Mimikatz - https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group
- Administratoriem ieteicams izmantot nodalītas darbstacijas vai dažādus kontus – attiecīgi, administrēšanas pienākumiem uz DC vai serveriem viens konts un ikdienas darbiem cits. Strādājot ar Remote Desktop, aktivizēt '*Restricted Admin mode*' - https://social.technet.microsoft.com/wiki/contents/articles/32905.remote-desktop-services-enable-restricted-admin-mode.aspx
- Uzlik*t Local Security Authority (LSA)* paplašinātos drošības uzstādījumus. Tie ietver lsass.exe procesa aizsardzību, kuram uzbrucēji mēģina piekļūt, lai izgūtu sistēmā uzglabātās paroles un to hash vērtības - https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
- Izmantot darbstacijās/serveros esošo ugunsmūri, lai bloķētu client-to-client konekcijas. Atļaut ienākošos SMB pieprasījumus uz klientu sistēmām tikai no administratoru, piemēram, Helpdesk vai skenēšanas/monitoringa iekārtām.
- Atteikties no *Server Message Block* version *1* (SMBv1). Par tā atslēgšanu vairāk šeit - https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3#how-to-remove-smb-v1
- Noņemt lietotāju kontiem SIDHistory atribūtu (it īpaši svarīgi atcerēties šo pārbaudīt pēc lietotāju migrācijas uz citu domēnu un pēc tam, kad lietotājs ir

pievienots nepieciešamajām grupām): https://docs.microsoft.com/en-us/defender-for-identity/cas-isp-unsecure-sid-history-attribute

Parasti pie Pass-The-Hash uzbrukumu identifikācijas nav konkrētu indikatoru, uz kuriem var balstīties, jo tiek izpildīta tradicionālā SMB protokola autentifikācija (bet ar zagtām hash vērtībām), tāpēc nepieciešams meklēt neparastas administratoru/lietotāju darbības t.i. pētīt lietotāju uzvedību *(User and Entity Behavioral Anlytics* – piemēram, šis ir atvērtā koda rīks, kas var palīdzēt ar UEBA analīzi https://github.com/JPCERTCC/LogonTracer *)*; Izmaiņas sistēmu konfigurācijā (piemēram, veido jaunus lietotājus un/vai pievieno tos Administrator grupai `(net user /add xyz` un `net localgroup administrators xyz /add`)); Viens lietotāja konts vienlaicīgi pieslēdzies vairākām sistēmām; Lietotāju aktivitāte brīvdienās/naktīs; No vienas iekārta tiek ģenerēti vairākkārtīgi neveiksmīgi piekļuves mēģinājumi uz dažādiem kontiem (EventID 4625); Neparastas machine-to-machine konekcijas (piemēram, darbinieki mēģina piemontēt tīkla diskus (*share)*, kas iepriekš nav lietoti vai nav pat tiesību, un mēģina administrēt citas sistēmas (izveidotās sesijas uz gala iekārtas var pārbaudīt ar `net sessions` komandu); Server-to-server konekcijas.

Ja ir pamats uzskatīt, ka paroļu hash vērtības ir noplūdušas un ir iespējams identificēt konkrētus kontus, tad nepieciešams tos atslēgt (Disable) un noņemt visas grupu tiesības. Nepieciešams nomainīt visas (gan lietotājiem, gan servisu kontiem, gan darbstaciju/serveru kontiem) paroles pēc iespējas ātrāk uz visām ietekmētajām sistēmām, un tikai tad atjaunot uzlauztos kontus, protams, vēl labāk, ja tos var izveidot no jauna ar citu lietotājvārdu. Savukārt, ja kompromitēts ir DC, jāatceras nomainīt **KRBTGT** konta paroli **divas reizes** pēc kārtas (jāpiezīmē, ka šī darbība var izraisīt sistēmas nepieejamību (*down time*), piemēram, Sharepoint, Skype for Business un citai ar domēna AD autentifikāciju saistītai programmatūrai). Šeit pieejams Microsoft radītais skripts Krbtgt konta atiestatīšanai (*reset*). https://www.microsoft.com/security/blog/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/

Ja ir pieejama aktīvās direktorijas rezerves kopija, tad nepieciešams atjaunoties uz versiju, par kuru esat droši, ka tajā laikā nebija kompromitācijas pazīmju, jo pēc uzbrukuma var būt pievienoti jauni lietotāju/servisu/iekārtu konti. Pēc

kopijas uzstādīšanas noteikti nomainīt visas paroles lietotāju/servisu/iekārtu kontiem un ar uzsvaru uz KRBTGT kontu, kuram paroli mainām 2x.

P.S. Aicinām pievērst uzmanību Wndows **EventID 4769**(pēc tam, kad KRBTGT konta parole ir 2x atiestatīta), kas tiek ģenerēts uz domēna kontroliera. Ja šis notikums tiek ģenerēts ar statusa kodu 0x1F "Integrity check on decrypted field failed" - šis ir potenciāls indikators, ka iepriekš ģenerētu *Golden ticke*t mēģina izmantot arī pēc konta Krbtgt atiestatīšanas.

Papildus informācijas avoti par Pass-the-Hash/Pass-the-Ticket un ar tiem saistītiem uzbrukumiem – aizsardzību, auditēšanu un atkopšanos:

Pass the Hash/Pass the Ticket:

https://www.microsoft.com/en-us/download/details.aspx?id=36036

https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf

https://adsecurity.org/?p=1515

DCSync uzbrukums: https://adsecurity.org/?p=1729

SidHistory https://adsecurity.org/?p=1772

Vairāk par Protected Users Group: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts

Reset Computer Account: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753596(v=ws.11)?redirectedfrom=MSDN

Par to, kāpēc nepieciešams atslēgt SMBv1: https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858

Rekomendācijas auditēšanas iestatījumiem Windows domēna infrastruktūrā: https://cert.lv/uploads/iestadem/Rekomendacijas_audit_Win_2020.pdf

Rīki

LogonTracer:
https://github.com/JPCERTCC/LogonTracer

DPAT (Domain Password Audit Tool):
https://github.com/clr2of8/DPAT

CISA Hunt and Incident Response Program (CHIRP):
https://github.com/cisagov/CHIRP

PIELIKUMS – Windows EventID, kas potenciāli varētu būt saistīti ar PTH/PTT uzbrukumiem

[Šī informācija apkopota no Microsoft izstrādātā materiāla par PTH - https://www.microsoft.com/en-us/download/confirmation.aspx?id=36036]

Application

Event ID 4688 - A new process has been created.

Authentication

Event ID 4648 - A logon was attempted using explicit credentials.

Event ID 4624 - An account was successfully logged on.

Kerberos events - domain controllers

Event ID 4769 - A Kerberos service ticket was requested.

Event ID 4768 - A Kerberos authentication ticket (TGT) was requested.

Event ID 4776 - The domain controller attempted to validate the credentials for an account.

Authentication - domain controllers

In Applications and Services logs at Microsoft\Windows\Authentication.

Under ProtectedUserFailures-DomainController

Events generated when an account that is a member of the Protected Users security group tries to use blocked authentication options.

Event ID 100 – NLTM usage attempted.

Event ID 104 – DES or RC4 attempted for Kerberos Authentication.

Trustworthy Computing 23

Under AuthenticationPolicyFailures-DomainController

Events that are generated when an account is used outside of the allowed authentication policy silos.

Event ID 101 – NTLM usage attempted.

Event ID 105 – Kerberos authentication from a particular device was not permitted.

Event ID 106 – The user or device was not allowed to authenticate to the server.

Event ID 305 – Kerberos TGT request did not meet access control restrictions.

Event ID 306 – User, device or both do not meet the access control restrictions.

Detect LSA plug-ins and drivers that fail to run as a protected process

If audit mode is enabled for the Local Security Authority Subsystem (LSASS), an event will be generated when Lsass.exe attempts to load an unauthorized driver.

Applications and Services Logs\Microsoft\Windows\CodeIntegrity

Event ID 3065: Code integrity check determined that a process attempted to load a particular driver that did not meet the security requirements for Shared Sections. However, due to the system policy that is set, the image was allowed to load.

Event ID 3066: This event records a code integrity check that determined that a process (usually lsass.exe) attempted to load a particular driver that did not meet the Microsoft signing level requirements. However, due to the system policy that is set, the image was allowed to load.