TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Opas tietomurtojen havaitsemiseen

Sisällys

1 Tiivistelmä

Tässä ohjeessa keskitytään erityisesti tietomurron havaitsemiseen lokitietojen avulla. Esimerkkeinä käytetään Windows Event Log -tapahtumalokeja tai muita Windows-käyttöjärjestelmän lokitapahtumia. Valittuja esimerkkitapahtumia on havaittu tutkituissa tietomurroista tunkeutujien jäljiltä.

2 Tietomurron torjunnasta yleisesti

Tietomurron torjunta sisältää kolme kokonaisuutta: tietomurron estäminen, tietomurron havaitseminen sekä tietomurron tutkinta. Näiden vaiheiden jälkeen alkaa tietomurrosta toipuminen, jonka tulisi sujuvasti nivoutua yhteen seuraavan tietomurron estämisen kanssa.

Tietomurron estäminen

Tietomurron täydellinen estäminen lienee lähes mahdotonta, mutta asianmukaisilla estokeinoilla tunkeutumisesta voidaan tehdä hyökkääjälle hankalaa ja puolustautujalle helpommin havaittavaa. Käytännössä tietomurron estäminen edellyttää hyvien tietoturvakäytäntöjen jalkauttamista kaikkeen toimintaan sekä hyvää kyberturvallisuushygieniaa.

Nyrkkisääntönä ainakin seuraaviin asioihin tulee kiinnittää huomiota tietomurtojen estämiseksi:

Käyttöoikeuksien hallinta
- Peruskäyttäjillä ei tule olla ylläpito-oikeuksia
- Etäkäyttöpalvelut, kuten VPN ja webmail, sekä erityissuojattavat kohteet edellyttävät vahvaa tunnistautumista
- Ylläpitotoimet tehdään erillisiltä työasemilta, jotka edellyttävät vahvaa tunnistautumista

Päätelaitteiden ja palvelinten hallinta
- Julkaistut korjauspäivitykset käyttöjärjestelmiin ja ohjelmistoihin asennetaan mahdollisimman nopeasti
- Tarpeettomat ominaisuudet ja ohjelmistot poistetaan tai niiden suorittaminen estetään peruskäyttäjiltä
- Vain sallittuja ohjelmistoja voi suorittaa vain sallituista hakemistoista tai asentaa vain sallittuihin hakemistoihin (software whitelisting)

Tietoverkon hallinta
- Verkko on jaettu eritasoisiin verkkoalueisiin, joiden välinen liikennöinti on rajoitettu vain palvelun tai sovelluksen toiminnan kannalta välttämättömään liikenteeseen

Tiedon hallinta
- Tärkeimmistä palveluista ja suojattavasta tiedosta otetaan säännölliset varmuuskopiot
- Varmuuskopioita säilytetään erillään muusta tietoverkosta

Lisäohjeita ja vinkkejä estokeinoiksi voi hakea esimerkiksi VAHTI-ohjeista [1] tai tietoturvallisuuden auditointityökalu Katakrista [3]. Myös Yhdysvaltain kyberturvallisuusviranomainen CISA [3] on sekä Australian kyberturvallisuuskeskus ACSC [4] ovat julkaisseet ohjeita tietomurron torjumiseksi.

1 https://vm.fi/julkaisut/vahti

2 https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille#5581c4b0

3 https://us-cert.cisa.gov/ncas/alerts/aa20-245a

4 https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained

Tietomurron havaitseminen

Tässä ohjeessa keskitytään tunkeutumisen havaitsemiseen Windows-ympäristössä, mutta periaatteet ovat sovellettavissa myös muihin teknisiin ympäristöihin.

Havainnointikykyä voidaan parantaa esimerkiksi seuraavilla tavoilla:

- Päätelaitteiden tietoturvaratkaisujen (Endpoint Detection and Response, EDR) käyttöönotto
- Tietoverkon tietoturvakontrollien, kuten välityspalvelimien (proxy) tai sähköpostin liitetiedostojen eristämisen (automated sandbox), käyttöönotto
- Lokitietojen kattavuuden tehostaminen
- Keskitetyn lokienhallinnan kokonaisvaltainen hyödyntäminen
- Riittävän hyvin resursoidun valvontatoiminnon (Security Operation Center, SOC) perustaminen tai hankinta palveluna

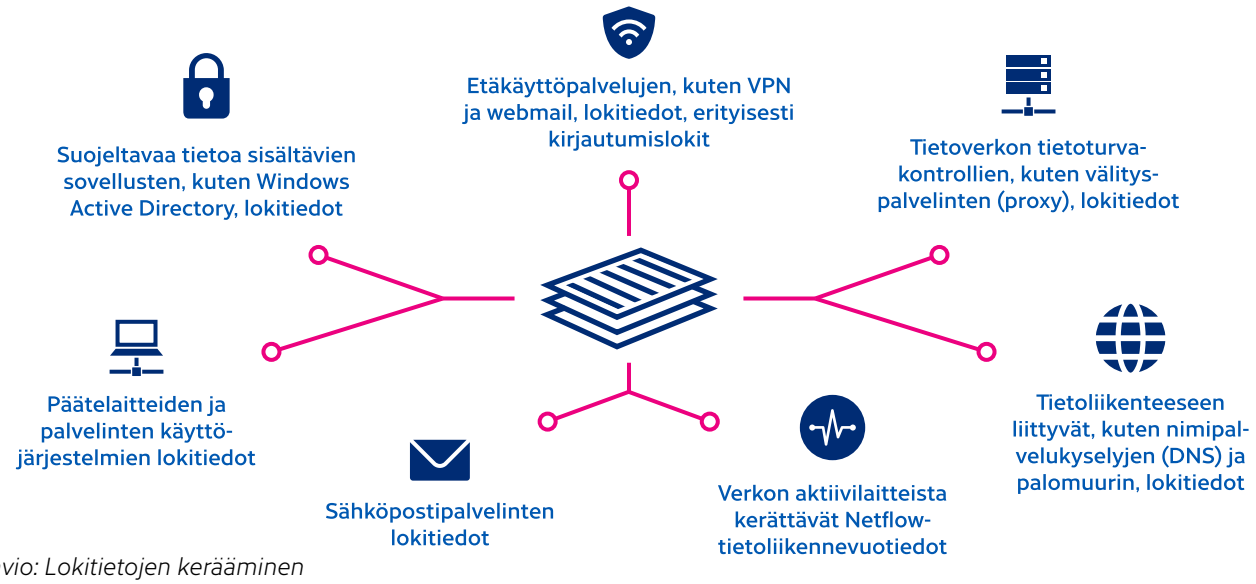
Lokitiedot kaiken ytimessä

Jotta tietomurrot voidaan tehokkaasti torjua, ne pitää pystyä havaitsemaan. Havaitsemisen ytimessä ovat asianmukaiset lokitiedot. Käytännössä tehokkaan havaitsemiskyvyn edellytyksenä on keskitetty lokienhallinta. Tähän on olemassa useita erilaisia kaupallisia ja avoimeen lähdekoodiin perustuvia tuotteita.

Kattavan lokienhallinnan avulla tietomurto on mahdollista havaita jo alkuvaiheessa. Tämä tietoturvan tukipilari edellyttää ennalta tehtyä valmistelua, mikäli sitä halutaan hyödyntää mahdollisimman tehokkaasti. Varsinaisten tietojärjestelmien lisäksi kattava lokienhallinta sisältää myös osaavan henkilöstön, joka seuraa ja säätää lokitietojen perusteella nostettavia hälytyksiä. Lisäksi tietomurtoa tutkittaessa henkilöstön tulee pystyä hyödyntämään lokitietoja tapauksen selvittämiseksi.

Kerättävien lokitietojen valintaan ja säilyttämiseen tulee panostaa. Lokilähteitä kannattaa olla useita erilaisia riittävän pitkältä ajalta kattavan näkyvyyden takaamiseksi. Vähintään seuraavista lähteistä tulee kerätä tarkoituksen mukaisia lokitietoja:

- Suojeltavaa tietoa sisältävien sovellusten, kuten Windows Active Directory, lokitiedot
- Päätelaitteiden ja palvelinten käyttöjärjestelmien lokitiedot
- Tietoverkon tietoturvakontrollien, kuten välityspalvelinten (proxy), lokitiedot
- Tietoliikenteeseen liittyvät, kuten nimipalvelukyselyjen (DNS) ja palomuurin, lokitiedot
- Verkon aktiivilaitteista kerättävät Netflow-tietoliikennevuotiedot
- Sähköpostipalvelinten lokitiedot
- Etäkäyttöpalvelujen, kuten VPN ja webmail, lokitiedot, erityisesti kirjautumislokit



Kaavio: Lokitietojen kerääminen

Tarkempia ohjeita lokienhallinnasta on saatavilla esimerkiksi Kyberturvallisuuskeskuksen lokitusohjeesta [5].

Modernit tietoturvaratkaisut (EDR) antavat monipuolisen näkymän tunkeutujan toimiin ja mahdollistavat osaltaan tunkeutumisen keskeyttämisen. Mikäli organisaatio ei käytä jotain kaupallista ratkaisua, suositellaan Microsoftin ilmaisen Sysmon-järjestelmätyökalun [6] hyödyntämistä. Se mahdollistaa normaaleja tapahtumalokeja (Event Logs) tarkemman näkymän käyttöjärjestelmän tapahtumiin. Tämä lisäksi PowerShell-komentotyökalun lokitusominaisuudet kannattaa aktivoida. Uusimmissa käyttöjärjestelmäversioissa ne ovatkin oletuksena päällä.

Lokitietojen eheys on syytä varmistaa estämällä hyökkääjää tai haittaohjelmaa pääsemästä kiinni keskitettyihin lokitietoihin. Tämä saadaan toteutettua eriyttämällä ja suojaamalla keskitetty lokienhallintaympäristö muusta tietoteknisestä ympäristöstä.

Hyökkääjät käyttävät usein yleisesti saatavilla olevia tunkeutumistestaustyökaluja, kuten Cobalt Strike tai PowerShell Empire, jalansijansa laajentamiseen. Näiden työkalujen havaitsemien edellyttää yleensä Sysmon-työkalun tai PowerShellin lokitusominaisuuksien käyttöä.

Myös riittävän kattavasti konfiguroidulla Windows-käyttöjärjestelmän tapahtumalokilla on mahdollista saavuttaa hyvän perustason havainnointikyky. Microsoft on julkaissut kattavia ohjeita tietoturvan valvontaan (Security Auditing) [7].

Tietomurron tutkinta

Tietomurron tutkinnan (Incident Response) tarkoituksena on selvittää, mitä on tapahtunut, mahdollistaa tunkeutujan karkottaminen sekä valmistautua tietomurrosta toipumiseen. Organisaatioilla tulee olla ajantasainen poikkeamanhallintasuunnitelma, jota on päivitetty ja harjoiteltu säännöllisesti. Tutkinta edellyttää kattavaa osaamista ja kokemusta. Siksi tässä vaiheessa kannattaa olla yhteydessä viranomaisiin, kuten Traficomin Kyberturvallisuuskeskukseen, sekä hankkia apua tietoturvapalveluja tarjoavilta yrityksiltä. On myös syytä muistaa tehdä havaitusta tietomurrosta rikosilmoitus poliisille ja hoitaa tarvittaessa lakisääteinen ilmoitusvelvollisuus valvoville viranomaisille.

Tietomurron tutkinta, tunkeutujan karkottaminen ja tietomurrosta toipuminen nivoutuvat toisiinsa neljän vaiheen kautta:

- **Valmistelu**, jossa tehdään tarvittavat toimet seuraavia vaiheita varten. Tässä vaiheessa tulisi olla melko selvä käsitys siitä, mitä tunkeutuja on tehnyt ja kuinka laajalle tunkeutuminen on levinnyt.
- **Eristäminen**, jossa tunkeutujan toiminnanvapaus rajataan hallittuun kokonaisuuteen.
- **Karkotus**, jossa tunkeutujan pääsy järjestelmiin katkaistaan. Tämä vaihe edellyttää usein väliaikaista yhteyden katkaisemista julkisiin tietoverkkoihin, järjestelmien uudelleenasennuksia ja lähes aina laajamittaisia salasanojen uusimisia.
- **Varmistaminen**, jossa valvotaan, ettei tunkeutuja onnistu pääsemään takaisin järjestelmiin ja estetään vastaavan murron onnistuminen tulevaisuudessa.

Lisätietoa tietomurron tutkinnasta saa esimerkiksi VAHTI-ohjeesta [8] 8/2017 ”Tietoturvapoikkeamatilanteiden hallinta” tai Yhdysvaltain standardointielimen NIST:n poikkeamanhallinta-ohjeesta [9].

5 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

6 https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

7 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/security-auditing-overview

8 https://vm.fi/julkaisut/vahti

9 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

3 Tietomurron vaiheet

Tämä ohje on jaoteltu osioihin tietomurron eri vaiheiden mukaisesti. Vaiheiden jaottelu mukailee MITRE ATT&CK -viitekehyksen [10] mallia. Jokaisessa osioissa käsitellään siihen liittyviä keinoja tunkeutumisen havaitsemiseen ja keskeyttämiseen.

Yleiset vaiheet tietomurrossa ovat:

10 https://attack.mitre.org/

Jalansijan saavuttaminen (Initial Access)

Etäkäyttöpalvelujen hyväksikäyttö

Useiden hyökkääjien suosima tunkeutumistapa on varastettujen käyttäjätunnusten käyttäminen kohdeorganisaation etäkäyttöpalveluihin kirjautumiseen. Etäkäyttöpalvelujen, kuten VPN, webmail, Windows Remote Desktop, TeamViewer yms., lokitiedoista tulee selvittää, onko niihin kirjauduttu epätavallisista lähteistä. Epätavallisilla lähteillä tarkoitetaan erityisesti erilaisten Virtual Private Server (VPS) -palveluntarjoajien, kuten Linode, DigitalOcean, Hetzner, OVH SAS, QHoster, HostSailor, Azure, AWS tai muut vastaavat, verkkoja. Normaalisti etätyöläisten yhteydet tulevat teleoperaattoreiden kuluttaja- tai yritysliittymistä eivätkä erilaisista pilvistä.

Toisaalta myös kirjautumisiin liittyvät maantieteelliset poikkeavuudet tai mahdottomuudet voivat olla merkki tietomurron yrityksestä. Näissä tapauksissa esimerkiksi samoilla käyttäjätunnuksilla yritetään kirjautua lyhyen ajan sisällä useista eri lähteistä, jotka ovat maantieteelliseltä sijainniltaan tuhansien kilometrien etäisyydellä toisistaan.

Tunnistettujen epäilyksen alaisten käyttäjätunnusten käyttö tulee selvittää ja ne tulee sulkea hallitun suunnitelman mukaisesti. Anastettujen tunnusten tapauksessa salasanat tulee vaihtaa ja siirtyä käyttämään vahvaa tunnistautumista (multifactor authentication).

Käyttäjätunnusten hyväksikäyttö

Anastettujen pääkäyttäjätunnusten (admin-tason tunnusten) hyväksikäyttö jakaantuu yleensä kahteen päälinjaan: anastettujen tunnusten käyttäminen kirjautumisessa ja uusien admin-tason tunnusten luonti.

Kun joku admin-tason ryhmiin kuuluva käyttäjätunnus kirjautuu koneelle, syntyy lokimerkintä:

> **Event ID 4672: Special privileges assigned to new logon tai**
>
> **Event ID 4964: Special groups have been assigned to a new logon**

Hieman tätä ennen on tapahtunut lokimerkintä:

> **Event ID 4624: An account was successfully logged on**

Kirjautumismerkinnöistä 4624 kannattaa monitoroida kahdenlaisia kirjautumistyyppejä; Logon Type 3 eli verkon yli tapahtuva kirjautuminen käyttäen esim. net use -komentoa sekä Logon Type 10 eli Remote Desktop -yhteyden avulla tehty kirjautuminen. Lokimerkinnät 4672, 4964 ja 4624 voidaan kytkeä toisiinsa niissä esiintyvän yhteisen Logon ID -tunnisteen avulla.

Lokimerkinnästä 4624 selviää myös, mistä lähdeosoitteesta kirjautuminen on tehty. Näin voidaan selvittää, onko admin-tason tunnuksilla kirjauduttu järjestelmiin muilta, kuin sallituilta hallintatyöasemilta.

Microsoftin on julkaissut kuvaukset lokimerkinnöistä 4672 [11], 4924 [12] ja 4624 [13] sekä suosituksia niiden monitoroinnista.

---

11 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4672

12 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4964

13 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

Onnistuneen tunkeutumisen jälkeen hyökkääjä yrittää usein luoda itselleen uusia pääkäyttäjän tunnuksia. Windows-toimialan (domain) Active Directory -palvelimen lokitiedoista tulee selvittää, onko tunnistetun tunkeutumisen jälkeen luotu uusia admin-tason käyttäjätunnuksia. Mikäli näitä löytyy, tulee selvittää, onko ne luotu organisaation it-ylläpidon vai jonkun tuntematttoman tahon toimesta. Jälkimmäisessä tapauksessa tulee selvittää kirjautumislokeista missä, milloin ja mihin kyseisiä uusia admin-tunnuksia on käytetty. Jotta kaikki tämä olisi mahdollista, tulee Windows-toimialassa olla päällä kattavat auditointisäännöt

(Basic Audit Policies ja Advanced Audit Policies). Microsoftin on julkaissut kattavat ohjeet [14] siitä, kuinka Security Auditing pistetään päälle.

Windowsin lokitiedoissa (Windows Event Logs) uuden tunnuksen lisääminen admin-tason ryhmiin aiheuttaa jonkun seuraavista lokimerkinnöistä riippuen siitä, onko kyseessä Local Admins -ryhmä (SID S-1-5-32-544), Domain Admins -ryhmä (SID S-1-5-domaininyksilövänumero-512) vai Enterprise Admins -ryhmä (SID S-1-5-domaininyksilövänumero-519):

Event ID 4732: A member was added to a security-enabled local group
Event ID 4728: A member was added to a security-enabled global group
Event ID 4756: A member was added to a security-enabled universal group

Microsoftin on julkaissut kuvauksen lokimerkinnästä 4732 [15] ja suositukset sen monitoroinnista. Kuvaukset ja suositukset lokimerkinnöillä 4728 ja 4756 ovat samankaltaiset.

Haitallisen ohjelmakoodin suorittaminen (Execution)

Komentorivityökalujen hyväksikäyttö

Ylivoimaisesti suosituin tunkeutujien toimintatapa on hyväksikäyttää kohdejärjestelmässä jo olemassa olevia työkaluja omiin tarkoituksiinsa. Näihin kuuluvat lukuisten ylläpitotyökalujen lisäksi käyttöjärjestelmien omat komentorivityökalut eli komentotulkit. Moderneissa Windows-käyttöjärjestelmien versioissa PowerShell-komentojen lokitietojen keruu on oletuksena päällä, joten sitä kannattaa hyödyntää tunkeutumisen havaitsemiseksi.

PowerShell Empiren agenttisovelluksen asentaminen ja komentokanavan avaaminen tehdään usein vakioparametrien avulla. Näitä voidaan seurata PowerShellin, Sysmonin tai Windowsin tapahtumalokin merkinnöillä:

PowerShell Event ID 800

HostApplication: '*\powershell.exe ' # ja jompikumpi seuraavista
HostApplication: '* -noP -sta -w 1 -enc *' # agent startup
HostApplication: '* -NonI -W hidden -c *' # persistent command&control

PowerShell Event ID 4103

HostApplication: '*\powershell.exe ' # ja jompikumpi seuraavista
HostApplication: '* -noP -sta -w 1 -enc *' # agent startup
HostApplication: '* -NonI -W hidden -c *' # persistent command&control

Sysmon Event ID 1: Process creation

CommandLine: '*\powershell.exe ' # ja jompikumpi seuraavista
CommandLine: '* -noP -sta -w 1 -enc *' # agent startup
CommandLine: '* -NonI -W hidden -c *' # persistent command&control

14 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/security-auditing-overview

15 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4732

Event ID 4688: A new process has been created

CommandLine: '*\powershell.exe ' # ja jompikumpi seuraavista
CommandLine: '* -noP -sta -w 1 -enc *' # agent startup
CommandLine: '* -NonI -W hidden -c *' # persistent command&control

Event ID 4688 tapauksessa Group Policy "Administrative Templates\System\Audit Process Creation\Include command line in process creation events" pitää olla päällä, jotta komentoriviparametrit tallentuvat lokimerkintään

Ajastettujen toimintojen hyväksikäyttö (Scheduled tasks)

Hyvin yleinen tapa, jolla tunkeutuja pyrkii suorittamaan omaa ohjelmakoodiaan ja säilyttämään jalansijansa, on ajastettujen toimintojen (Scheduled Tasks) luominen. Uusien ajastettujen toimintojen luominen pitäisi olla tarkasti kontrolloitu ylläpidon tekemä toimi, joten tiedossa olevien ylläpitotehtävien ulkopuolella luodut uudet ajastetut toiminnot on aina syytä tarkistaa. Kun uusi ajastettu toiminto luodaan, syntyy lokimerkintä:

Event ID 4698 [16]: A scheduled task was created

Jalansijan säilyttäminen (Persistence)

Kirjautumisen yhteydessä ajettavat ohjelmat

Usein tunkeutuja pyrkii säilyttämään jalansijansa murretussa kohteessa asentamalla omaa ohjelmakoodiaan rekisteriavaimiin, jotka suoritetaan aina, kun käyttäjä kirjautuu tietokoneelle. Niin sanottuja "Run Key" -rekisterihaarojen vaihtoehtoja on useita, esimerkiksi oletuksena seuraavat:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunO nce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Once

Toisaalta kaikki rekisteriavainten muutokset tulisi tapahtua hallitusti ylläpitotoimien tai ohjelmistojen asennusten yhteydessä. Näin ollen rekisteriavainten muutoksia, erityisesti "Run Key" -rekisterihaaroissa, kannattaa monitoroida ja korreloida muiden lokitapahtumien kanssa. Kun rekisterin arvoa muutetaan, syntyy lokimerkintä:

Event ID 4657 [17]: A registry value was modified

Käyttöoikeuksien laajentaminen (Privilege Escalation)

Olemassa olevien prosessien hyväksikäyttö

Eräs tapa käyttöoikeuksien laajentamiseen on tunkeutujan koodin syöttäminen jo olemassa olevan prosessin muistialueeseen, jolloin koodin suoritetaan tuon prosessin oikeuksin. Kun Cobalt Strike yrittää syöttää itsensä toiseen prosessiin PowerShellin avulla, kohteena oleva prosessiosoite päättyy usein tavuihin 0x0B80. Tätä voidaan seurata Sysmonin tapahtumalokiin tekemällä merkinnällä:

Sysmon EventID 8: CreateRemoteThread

SourceImage: '*\powershell.exe'
StartAddress: '*0B80'

16 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4698

17 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4657

Varastoitujen käyttöoikeuksien anastaminen

Nykyisin hyökkääjän käyttöoikeuksien nosto tehdään useimmiten manipuloimalla Local Security Authority Subsystem Service (lsass.exe) -prosessin muistiavaruutta esimerkiksi Mimikatz-ohjelmiston avulla. Tästä jää Sysmonin tai Windowsin tapahtumalokiin merkintöjä kuten:

Event ID 4656: A handle to an object was requested
Event ID 4663: An attempt was made to access an object
ObjectName: 'C:\windows\system32\lsass.exe'
ProcessName: mikä tahansa muu kuin 'C:\windows\system32\wininit.exe' on epäilyttävää, esimerkiksi '*\mimikatz*'

Sysmon Event ID 10: ProcessAccess
TargetImage: 'C:\windows\system32\lsass.exe'
SourceImage: mikä tahansa muu kuin 'C:\windows\system32\wininit.exe' on epäilyttävää, esimerkiksi '*\mimikatz*'

Suojauksien väistäminen (Defense Evasion)

Suojauksien väistämiseksi ja jälkiensä peittelemiseksi tunkeutujat monesti pyrkivät hyödyntämään kohdejärjestelmässä olemassa olevia työkaluja ja välttämään omien haittaohjelmatiedostojensa tallettamista kohdejärjestelmään. Mikäli haittaohjelmia ylipäätään asennetaan, ne pyritään syöttämään suoritettavaksi suoraan muistiin.

Käyttöoikeuksien kaappaaminen (Credential Access)

Salasanojen murtaminen

Tunkeutujat suosivat oikeiden käyttäjätunnusten käyttöä tietomurroissa. Mikäli käyttäjätunnuksia ei ole saatu ennalta haltuun esimerkiksi tietojenkalastelun avulla, tunnusten salasanoja voidaan yrittää murtaa. Erilaisia murtomenetelmiä useita, mutta yhteisenä piirteenä niissä kaikissa on lukuisat epäonnistuneet kirjautumisyritykset ennen onnistunutta murtoa. Tämän takia erityisesti etäkäyttöpalveluissa, kuten VPN, webmail, SSH, RDP yms., sekä onnistuneista että epäonnistuneista kirjautumisista tulee kerätä lokimerkinnät.

Erityisesti lukuisat lyhyehkön aikaikkunan sisällä tapahtuneet verkon yli tehdyt epäonnistuneet kirjautumisyritykset tulee tarkistaa. Tällä tarkoitetaan tapauksia, joissa esimerkiksi muutaman minuutin aikana yhteen palveluun on kertynyt useita kymmeniä tai satoja epäonnistuneita kirjautumisia käyttäen useita eri käyttäjätunnuksia, joista osaa ei ole edes olemassa. Windows-käyttöjärjestelmässä lokimerkintä on:

Event ID 4625: An account failed to log on
LogonType 3 (Kirjautuminen verkon yli)
Status ja FailureReason kertovat kirjautumisen epäonnistumisen syyn
WorkstationName ja IpAddress kertovat kirjautumista yrittäneen tietokoneen nimen ja IP-osoitteen

Sisäinen kartoitus (Discovery)

Tunkeutuja pyrkii kartoittamaan tietoverkossa olevia järjestelmiä, mikä usein aiheuttaa paljon sisäistä verkkoliikennettä ja epäonnistuneita yhteyden muodostamisyrityksiä. Mitä paremmin verkko on segmentoitu erillisiin toimintalohkoihin, sitä helpommin sisäinen kartoitus voidaan paljastaa esimerkiksi Netflow-tietojen tai palomuurilokien perusteella.

Tunkeutumisen laajentaminen (Lateral Movement)

Remote Desktop -palvelun hyväksikäyttö

Murtautuminen RDP-yhteyden kautta (RDP Brute Force Attack) aiheuttaa yleensä useita epäonnistuneita kirjautumisyrityksiä ja myös lokimerkinnän:

Event ID 4625: An account failed to log on
LogonType 10 (Kirjautuminen RDP-yhteyden yli)
Status ja FailureReason kertovat kirjautumisen epäonnistumisen syyn
WorkstationName ja IpAddress kertovat kirjautumista yrittäneen tietokoneen nimen ja IP-osoitteen

Vaihtoehtoisen autentikointi-materiaalin hyväksikäyttö

Eräs yleisesti käytetty menetelmä on niin sanottu Pass-the-Hash, jossa pyritään kirjautumaan hyödyntämällä muistista kaapattuja tunnuksia. Tämä menetelmä aiheuttaa hyökkäyksen lähteenä olevassa tietokoneessa lokimerkinnän

Event ID 4624: An account was succesfully logged on
LogonType 9 (NewCredentials)

Tässä lokimerkinnässä oleva Logon Process -arvo ”seclogo” viittaa erityisesti Pass-the-Hash -hyökkäykseen.

Vastaavasti samalla hetkellä hyökkäyksen kohteessa, joka voi olla myös sama tietokone, syntyy lokimerkintä

Event ID 4624: An account was succesfully logged on
Logon Type 3 (Kirjautuminen verkon yli)
Authentication Package: NTLM

Kirjautumistyyppi (Logon Type) 9 on hiukan epätavallinen ja syntyy esimerkiksi RunAs -komennon johdosta. Sen monitorointi ei kuitenkaan aiheuta paljoa vääriä hälytyksiä, mikäli ne saadaan korreloitua kohdassa 3.4.2 kuvatun lokimerkinnän Sysmon ID 10 sekä edellä mainitun kohteena olevan tietokoneen Event ID 4624 kanssa.

Tiedon keruu (Collection)

Ennen kuin tietoa voidaan varastaa, se täytyy kerätä. Kerätty tieto usein käsitellään, esimerkiksi pakkaamalla tai salaamalla, sopivampaan muotoon varsinaista varastamista silmällä pitäen.

Mikäli tunkeutuja on onnistunut murtautumaan sähköpostiohjelmistoihin, hän on saattanut tehdä piilotettuja viestien välittämissääntöjä, jotka välittävät viestinnän tunkeutujan hallussa olevaan kohteeseen.

Komentokanava (Command and Control)

Käytännössä kaikki tietomurrot edellyttävät jonkinlaista komentokanavaa. Tätä tarvitaan niin jalansijan saavuttamiseen, tunkeutumisen laajentamiseen kuin tiedon varastamiseenkin.

Verkkoyhteyden luominen

Mikäli hyökkääjä yrittää luoda komentokanavia tai ladata lisää haittaohjelmien verkosta käyttäen komentorivityökaluja, niistä tulee Sysmon-työkalun lokimerkintä

Sysmon Event ID 3: Network connection
Image: esimerkiksi '*\powershell.exe' tai '*\cmd.exe'
DestinationIp: kertoo liikenteen kohteena olevan osoitteen. Tästä kannattanee suodattaa pois sisäiset osoitteet

Tunkeutuja voi käyttää hyväkseen myös lukuisia muita kohdejärjestelmässä olevia ohjelmistoja, varsinkin haittaohjelmien ja lisätyökalujen lataamiseen. Esimerkiksi seuraavia ohjelmistoja on käytetty tunkeutumisen apuna [18]:

- powershell.exe
- bitsadmin.exe
- certutil.exe
- psexec.exe
- wmic.exe
- mshta.exe
- mofcomp.exe
- cmstp.exe
- windbg.exe
- cdb.exe
- msbuild.exe
- csc.exe
- regsvr32.exe

Windows-ympäristössä olevia tunkeutujan hyväksikäyttämiä ohjelmistoja on kerätty LOLBAS-projektin sivulle [19].

Tietoliikenneanalyysi

Cobalt Striken agenttisovellus (Beacon) luo oletusasetuksilla kolmen sekunnin välein uuden TCP-yhteyden käyttäen uutta lähdeporttia. Mahdollisuuksien mukaan tätä normaalista ihmisten toiminnasta poikkeavaa liikennettä kannattaa pyrkiä seuraamaan eri tietoliikennelokeista. Yleisestikin komentokanaville on ominaista se, että pakettien koot ja yhteyksien muodostamisen frekvenssi ovat selvästi säännöllisempiä kuin normaalissa ihmisten aiheuttamassa liikenteessä.

Tietoliikenneprotokollien väärinkäyttö liittyy pääsääntöisesti haitalliseen toimintaan ja niitä kannattaa pyrkiä monitoroimaan. Yleisesti käytössä olevista menetelmistä mainittakoon DNS-sivukanava ja räätälöidyt protokollat.

DNS-sivukanavassa DNS-nimipalvelukyselyjä käytetään komentokanavana. Tällöin komennot ja vastaukset välitetään normaalin DNS-liikenteen seassa. Kanava erottuu normaalien kyselyjen suurena määränä ja poikkeavana sisältönä.

Räätälöidystä protokollista yleisin esimerkki on se, että HTTPS-liikenteelle varatun TCP-portin 443 kautta liikennöidään muuta, kuin HTTPS-liikennettä.

Tiedon varastaminen (Exfiltration)

Tiedon varastamisen havaitsemiseksi kannattaa seurata poikkeamia liikennemäärissä. Ne voivat olla esimerkiksi epätavallisen suuria tiedonsiirtoja poikkeuksellisiin kohteisiin tai liikenne saattaa näyttää menevän väärään suuntaan. Tyypillisesti www-sivustoilta ladataan (download) enemmän dataa, kuin sinne talletetaan (upload). Toisaalta tiedon varastamiseen käytettävät sessiot voivat kestoltaan olla epätavallisen pitkiä tai niitä voi olla epätavallisen paljon. Myös normaaleja internetin tiedostojen jakopalveluita, kuten Dropbox tai Google Drive, käytetään usein tiedon varastamisen apuna.

Tiedon tai järjestelmien muokkaus tai tuhoaminen (Impact)

Ennen tätä vaihetta tietoon tai järjestelmiin ei ole tehty muutoksia ja ne ovat olleet käytettävissä, joskin myös tunkeutujalle. Tähän vaiheeseen kuuluvat niin tiedon kuin järjestelmien käyttökelvottomaksi saattaminen. Tyypillisiä esimerkkejä ovat lukuisat kohdennetut kiristyshaittaohjelmahyökkäykset [20] tai valtiollisten toimijoiden sabotaasiohjelmat kuten NotPetya [21].

18 https://blog.talosintelligence.com/2019/11/hunting-for-lolbins.html

19 https://lolbas-project.github.io/

20 https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html

21 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

4 Yhteenveto

Pääsääntöisesti tietomurrot noudattelevat motiivista riippumatta suurin piirtein samankaltaista etenemisprosessia kohteen tiedustelusta tunkeutumisen ja leviämisen kautta varsinaisen lopullisen päämäärän toteuttamiseen. Mikäli lokitietojen kerääminen on tehty oikein, tietomurron eri vaiheista jää jälkiä, jotka on mahdollista havaita hyvillä lokienhallinnan menetelmillä.

Tähän oppaaseen on kerätty esimerkkejä yleisesti havaituista jäljistä, joita on tavattu tutkittaessa tietomurtoja. Näiden vinkkien avulla on mahdollista muodostaa omalle organisaatiolle räätälöity tehokas toimintamalli tietomurtojen havaitsemiseksi.

5 Kooste tapahtumalokien esimerkeistä

Käyttäjätunnusten hyväksikäyttö (Initial Access)

Event ID 4624: An account was succesfully logged on
Logon Type 3 (Kirjautuminen verkon yli)
Logon Type 10 (Remote Desktop)

Event ID 4672: Special privileges assigned to new logon
Event ID 4964: Special groups have been assigned to a new logon
Event ID 4732: A member was added to a security-enabled local group
Event ID 4728: A member was added to a security-enabled global group
Event ID 4756: A member was added to a security-enabled universal group

Komentorivityökalujen hyväksikäyttö (Execution)

PowerShell Event ID 800
HostApplication: '*\powershell.exe ' # ja jompikumpi seuraavista
HostApplication: '* -noP -sta -w 1 -enc *' # agent startup
HostApplication: '* -NonI -W hidden -c *' # persistent command&control

PowerShell Event ID 4103
HostApplication: '*\powershell.exe ' # ja jompikumpi seuraavista
HostApplication: '* -noP -sta -w 1 -enc *' # agent startup
HostApplication: '* -NonI -W hidden -c *' # persistent command&control

Sysmon Event ID 1: Process creation
CommandLine: '*\powershell.exe ' # ja jompikumpi seuraavista
CommandLine: '* -noP -sta -w 1 -enc *' # agent startup
CommandLine: '* -NonI -W hidden -c *' # persistent command&control

Event ID 4688: A new process has been created
CommandLine: '*\powershell.exe ' # ja jompikumpi seuraavista
CommandLine: '* -noP -sta -w 1 -enc *' # agent startup
CommandLine: '* -NonI -W hidden -c *' # persistent command&control

Ajastettujen toimintojen hyväksikäyttö (Initial Access)

Event ID 4698: A scheduled task was created

Kirjautumisen yhteydessä ajettavat ohjelmat (Persistence)

Event ID 4657: A registry value was modified

Olemassa olevien prosessien hyväksikäyttö (Privilege Escalation)

Sysmon EventID 8: CreateRemoteThread
SourceImage: '*\powershell.exe'
StartAddress: '*0B80'

Varastoitujen käyttöoikeuksien anastaminen (Privilege Escalation)

Event ID 4656: A handle to an object was requested
Event ID 4663: An attempt was made to access an object
ObjectName: 'C:\windows\system32\lsass.exe'
ProcessName: mikä tahansa muu kuin 'C:\windows\system32\wininit.exe' on epäilyttävää, esimerkiksi '*\mimikatz*'

Sysmon Event ID 10: ProcessAccess
TargetImage: 'C:\windows\system32\lsass.exe'
SourceImage: mikä tahansa muu kuin 'C:\windows\system32\wininit.exe' on epäilyttävää, esimerkiksi '*\mimikatz*'

Salasanojen murtaminen (Credential Access)

Event ID 4625: An account failed to log on
LogonType 3 (Kirjautuminen verkon yli)
Status ja FailureReason kertovat kirjautumisen epäonnistumisen syyn
WorkstationName ja IpAddress kertovat kirjautumista yrittäneen tietokoneen nimen ja IP-osoitteen

Remote Desktop -palvelun hyväksikäyttö (Lateral Movement)

Event ID 4625: An account failed to log on
LogonType 10 (Kirjautuminen RDP-yhteyden yli)
Status ja FailureReason kertovat kirjautumisen epäonnistumisen syyn
WorkstationName ja IpAddress kertovat kirjautumista yrittäneen tietokoneen nimen ja IP-osoitteen

Vaihtoehtoisen autentikointimateriaalin hyväksikäyttö (Lateral Movement)

Event ID 4624: An account was succesfully logged on
Logon Type 3 (Kirjautuminen verkon yli)
Authentication Package: NTLM

Event ID 4624: An account was succesfully logged on
LogonType 9 (NewCredentials)

Verkkoyhteyden luominen (Command and Control)

Sysmon Event ID 3: Network connection
Image: esimerkiksi '*\powershell.exe' tai
'*\cmd.exe'
DestinationIp: kertoo liikenteen kohteena olevan osoitteen.
Tästä kannattanee suodattaa pois sisäiset osoitteet

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus

PL 320, 00059 TRAFICOM

p. 029 534 5000

kyberturvallisuuskeskus.fi

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus