IDENTIFIKÁCIA POSTUPU ÚTOČNÍKA V SIETI

Adam Kundracik

3Ib, 2022 - 2023

Abstrakt. Laterálny pohyb je súbor techník ktoré používajú útočníci, po tom ako získajú prvotný prístup, na pohyb v rámci siete. Budeme detegovať laterálny pohyb a hľadať postupnosť krokov, ktoré danú techniku charakterizujú, ako príručku pre ľudí ktorí danej problematike čelia alebo čeliť môžu.

Kľúčové slová: Laterálny pohyb, útočník, techniky, nástroje, EventCollector, PsExec

1 Úvod

V tejto práci budeme analyzovať techniku laterálneho pohybu, ktorou sa páchateľ dokáže pohybovať sieťou a napádať ďalšie zariadenia pomocou rôznych skriptov alebo iných prostriedkov.

Keďže v dnešnom svete je kybernetických útokov čoraz viac a viac, je potrebné zvyšovať povedomie ľudí aj o tejto problematike. Práve preto by sme vďaka tejto práci chceli dopomôcť k tomu, aby ľudia mali možnosť zistiť, aké všelijaké nástrahy na nich vo svete číhajú a ako fungujú.

Prakticky ukážeme, ako sa jednotlivé nástroje prejavujú a ako ich môžeme prostredníctvom zozbieraných logov detegovať. Výsledkom práce budú zistenia priamo použiteľné na zlepšenie porozumenia postupu útočníka, ale aj ako danú skutočnosť zistiť. Získané výsledky povedú k zvýšeniu kybernetickej bezpečnosti v praxi, ako aj prípadnej skorej detekcie, k zrýchlenému konaniu užívateľa, ktorý útokom čelí.

2 Laterálny pohyb (Lateral movement)

Laterálny pohyb je technika používaná na prevzatie kontroly nad systémom a získanie prístupu k rôznym iným systémom v rámci siete [12]. V článku ***What Is Lateral Movement? (Čo je laterálny pohyb?)*** [11], laterálny pohyb definujú ako techniku, ktorú útočníci používajú na rozširovanie sa na viacerých zariadeniach v sieti, ktorých cieľom je získať, alebo zničiť citlivé údaje na napadnutom zariadení [11].

Laterálny pohyb vieme rozdeliť do 3 fáz: **Fáza pozorovania, získania prístupových údajov a eskalácia práv a získania prístupu do zariadenia**.

V prvej fáze útočník pozoruje, skúma a mapuje sieť, jej používateľov a zariadenia v nej. Toto mapovanie mu napomáha pochopiť jej hierarchiu, identifikovať potenciálne zariadenia, ktoré sú objektmi jeho záujmu. Útočníci v sieti nasadzujú rôzne nástroje, aby zistili kde v sieti sa nachádzajú, k čomu môžu získať prístup a aké firewally sa v sieti využívajú.[1]

Vo fáze dva sa útočník snaží nadobudnúť prihlasovacie údaje, ktoré potrebuje aby sa mohol v sieti pohybovať. Jednou z možností ako získať tieto údaje je oklamanie používateľov, napríklad phishingovým útokom. Medzi ďalšie bežné techniky patria napr. **Pass the Hash, Pass the Ticket alebo nástroje ako Mimikatz.** [1]

V tretej fáze útočník vykonáva laterálny pohyb po sieti a napadá zariadenia kým nedôjde k dátam, ktoré hľadá. [1]

Techniky laterálneho pohybu

Útočníci sa snažia, aby v sieti boli čo najmenej viditeľní. Keďže využívanie externých nástrojov môže byť veľmi ľahko vystopovateľné, snažia sa využívať nástroje, ktoré sú na hostiteľskom zariadení už nainštalované. Môžu to byť napríklad nástroje ako: PowerShell, Windows Management Instrumentation (WMI) ale aj
PsExec. [11]

V nasledujúcich podkapitolách sa bližšie zaoberáme vybranými technikami, ich popisom, správaním a nástrojmi ktoré sú s nimi spojené.

2.1 Využívanie vzdialených služieb

Využívanie vzdialených služieb je technika, pomocou ktorej sa útočník snaží dostať do siete napríklad pomocou programovej chyby nezabezpečeného softvéru. Následne je útočník schopný na zariadení spustiť kód, ktorý mu dopomôže k jednoduchšiemu postupu po zariadeniach v rámci siete [13]. Túto teóriu rovnako popisuje aj MITRE ATT&CK matica, ktorá hovorí, že daná technika slúži na získanie neautorizovaného prístupu k interným systémom v rámci siete prostredníctvom programovej chyby v softvéri [7].

Medzi nástroje využívane pri Využívanie vzdialených služieb patria napríklad: **Bad Rabbit** [17]**, Conficker** [18], **Emotet** [19], **Empire** [20] **a Flame** [21] [7].

Skupiny ktoré využívali túto techniku, sú napríklad**: Fancy Bear (APT28)** [22], **Dragonfly** [23], **Fox Kitten [**24], **menuPass** [25] [7].

K bežným terčom útoku patrí napríklad Remote Desktop Protokol

(RDP), taktiež známy ako vzdialená plocha. Dôvod je jednoduchý. RDP je frekventovane používaný v mnohých veľkých firmách. RDP nám povoľuje vzdialený prístup k zariadeniu [13]. Medzi Ďalšie patria aj SMB protokol, služby web servera ale aj MySQL [7].

2.2 Internal Spearphishing

Internal spearphishing je technika slúžiaca na zneužitie účtov v internej sieti ako vstupný bod do nej. Bežným úkazom tohoto podvodu je využitie klamlivého linku ktorý sa používateľovi môže javiť ako skutočný. Ten ho následne presmeruje na nimi vytvorenú webovú službu do ktorej používateľ bez tušenia zadá svoje citlivé údaje ako napr. heslo. [8][16]

Medzi skupiny ktoré využívali techniku Internal spearphishing patria napríklad: **Hexane** [26], **Gamaredon Group** [27], **Kimsuky** [28], **Lazarus Group** [29] [8].

2.3 Vzdialené služby

Vo väčších sieťach zvyknú byť servery organizované do domén. Keďže na prístup do domény stačí jedna sada prihlasovacích údajov, útočníkovi stačí získať tieto údaje a následne získava prístup do všetkých zariadení pomocou rôznych protokolov ako je SSH alebo RDP.

Medzi nástroje využívane pri Využívanie vzdialených služieb patria napríklad: **Kivars** [30], **MacMa** [31], **Stuxnet** [32]. [9]

2.4 Laterálny prenos nástroja

Laterálny prenos nástroja je technika pri ktorej útočník premiestňuje súbory medzi zariadeniami v sieti v ktorej sa nachádza. Tento nástroj tak môže byť premiestňovaný zo zariadenia na zariadenie hocikde v rámci siete. Zväčša ide o nástroje, ktoré im pomáhajú v laterálnom pohybe a v rozširovaní sa na ďalšie zariadenia. [15]

Medzi nástroje využívane pri laterálnom prenose nástrojov patria napríklad: **BITSAdmin [33], príkazový riadok [34], FTP protokol [35], Netwalker [36]** atď.[15]

Skupiny ktoré využívali túto techniku, sú napríklad: **Aoqin Dragon, GALLIUM, Wizard Spider** a mnohé ďalšie[15].

2.5 Replikácia pomocou odnímateľných zariadení

Technika replikácie pomocou odnímateľných zariadení spočíva v šírení škodlivého programu na odnímateľne zariadenie ako je napríklad USB. Toto zariadenie sa následne môže na zariadeniach spúšťať automaticky po tom, čo sa pripojí k systému.

Táto technika zvyčajne zahŕňa kopírovanie súborov alebo úpravu existujúcich súborov uložených na vymeniteľnom médiu. Malvér sa zvyčajne tvári ako neškodný legitímny súbor. [37] [38]

Medzi nástroje využívane pri replikácii pomocou odnímateľných zariadení patria napríklad: **Agent.btz [33], CHOPSTICK [34], Conficker, [35], Crimson [36]** atď.[38]

Skupiny ktoré využívali túto techniku, sú napríklad: **Fancy Bear (APT28), Aoqin Dragon , Darkhotel** a mnohé ďalšie[15].

2.6 Nástroje na nasadenie softvéru

Nástroje na nasadenie softvéru je technika pri ktorej je do aplikácie tretej strany vpustený malvér ktorý útočníkom napomáha pri laterálnom pohybe v rámci siete.

Prístup môže byť použitý na laterálny presun do iných systémov, zhromažďovanie informácií alebo vymazanie pevných diskov na všetkých koncových bodoch [39]. Povolenia potrebné na vykonanie tejto akcie sa môžu líšiť v závislosti od nastavenia systému. Niekde môžu postačovať lokálne prihlasovacie údaje, inde sa môžu vyžadovať prihlasovacie údaje domény [40].

Medzi nástroje využívane pri replikácii pomocou odnímateľných zariadení patrí napríklad **Wiper** [41].

Skupiny ktoré využívali túto techniku, sú napríklad: **OceanLostus (APT32)** [42], **Threat Group-1314** [43], **Silence** [44] a mnohé ďalšie. [40]

2.7 Znehodnotenie zdieľaného obsahu

Táto technika spočíva v infikovaní zdieľaného úložiska alebo iného zdieľaného miesta škodlivými súbormi. Tieto súbory po následnom spustení infikujú zariadenie nič netušiaceho užívateľa ktorý tieto súbory spúšťa. Tento proces napomáha útočníkom v laterálnom pohybe. [39]

Súbory používajú kamuflovanie pôvodných súborov pomocou .LNK, a tieto nové súbory vyzerajú ako tie pôvodné, legitímne. .LNK súbory obsahujú zabudovaný príkaz, ktorý spustí skrytý súbor . Škodlivé súbory sa tvária ako neškodné a legitímne. Využívajú sa na to .LNK súbory, ktoré tak vyzerajú, no obsahujú v sebe príkaz ktorý spustí skrytý súbor v adresári, no stále vykonáva príkaz zadaný užívateľom, aby to vyzeralo, že všetko je v poriadku. [45]

Medzi nástroje využívane pri replikácii pomocou odnímateľných zariadení patria napríklad: **Conti [46], H1N1 [47], Stuxnet, [48], Ramsay [49]** atď.[45]

Skupiny ktoré využívali túto techniku, sú napríklad: **BRONZE BUTLER, Gamaredon Group , Darkhotel** a mnohé ďalšie.

2.8 Alternatívne spôsoby autentifikácie

V systéme sa na pri autentifikácii do medzipamäte alebo na disk ukladajú autentifikačné tokeny, ktoré majú za úlohu overiť, či sa používateľ úspešne autentifikoval, bez toho, aby sa od neho vyžadovalo opätovné prihlásenie. Ich získaním môžu útočníci získať prístup do systému bez potreby poznať prihlasovacie údaje jeho vlastníka. Medzi najčastejšie techniky patria: **pass the hash** alebo **pass the ticket** spoločne s využívaním **webových cookies**. [52]

Pass the hash (obídenie hash-u)

Na vykonanie techniky pass the hash je potrebné najskôr aplikovať techniku **Credential Access** (prístup k povereniu) [53], čo je súbor techník určených na krádež prihlasovacích mien a ich hesiel. Najčastejšie ide o **keylogging [50]** alebo **credential dumping [51].** [54]

Útočníci môžu získané hash-e hesiel využívať na prihlásenie do vzdialeného zariadenia bez toho aby vedeli aké heslo mu prislúcha. Po získaní hash-u útočníci tento hash posúvajú serveru, ktorý ich autentifikuje. Po tomto kroku útočník získava prístup do systému a môže vykonávať laterálny pohyb na ďalšie zariadenia v sieti. [53]

Pass the ticket (obídenie lístku)

Ide o techniku autentifikovania sa do systému pomocou kerberos lístkov bez hlbšieho poznania hesiel. Kerberos tikety sú získavané technikou s názvom credential dumping [51].

V závislosti od úrovne prístupu možno získať servisný lístok alebo lístok na udelenie lístku. Servisný lístok nám udeľuje prístup k určitému zdroju, medzitým čo lístok udeľujúci lístky nám poskytuje prístup k akémukoľvek zdroju ku ktorému má používateľ oprávnenia. [54]

Strieborný lístok umožňuje útočníkovi falšovať iba lístky TGS (ticket-granting service) pre konkrétne služby. Vstupenky TGS sú zašifrované hash-om hesla pre službu. Ak teda útočník ukradne hash pre určitú službu, môže pre túto službu falšovať vstupenky TGS. [57]

Zlatý lístok poskytuje držiteľovi neobmedzený prístup. Ak protivník získa hash hesla KRBTGT, vlastní zlatý lístok, ktorý mu dáva právomoc pristupovať k akémukoľvek ľubovoľnému zdroju v systéme. Tento útok je ťažko odhaliteľný. [58]

Využívanie webových cookies

Autentifikačné súbory cookie sa bežne používajú vo webových aplikáciách vrátane cloudových služieb po tom, ako sa používateľ autentifikoval do služby. Slúži k tomu, aby sa užívateľ nemusel mnohokrát autentifikovať po každej návšteve danej služby. Útočník je schopný dané súbory cookies získať a následne ich importovať do prehliadača. Po importovaní získava prístup k aplikácii ako používateľ, až dokiaľ súbor cookie nestratí svoju platnosť. Po prihlásení na web môže útočník získať prístup k citlivým informáciám, čítať e-maily alebo vykonávať akcie, na ktoré má konto obete oprávnenie. [56]

Literatúra

[1] https://www.crowdstrike.com/cybersecurity-101/lateral-movement/
[2] https://attack.mitre.org/software/S0029/
[3] https://www.pcwdld.com/what-is-winrm
[4] https://www.varonis.com/blog/what-is-mimikatz
[5] https://blog.netwrix.com/2022/12/16/crackmapexec_tutorial/
[6] https://jpcertcc.github.io/ToolAnalysisResultSheet-
[7] https://attack.mitre.org/techniques/T1210/
[8] https://attack.mitre.org/techniques/T1534/ [9]
https://attack.mitre.org/techniques/T1021/
[10] https://www.windows-security.org/windows-service/windows-event-collector
[11] What Is Lateral Movement?,
https://www.paloaltonetworks.com/cyberpedia/what-is-lateral-movement
[12] Lateral movement, (Somashekarappa, 2021)
[13] https://www.extrahop.com/resources/attacks/remote-services-exploitation/
[14] https://attack.mitre.org/techniques/T1021/
[15] https://attack.mitre.org/techniques/T1570/
[16] https://dmcxblue.gitbook.io/red-team-notes/lateral-movement/internal-spearphishing
[17] https://www.proofpoint.com/us/threat-reference/bad-rabbit

[18] https://sk.wikipedia.org/wiki/Conficker
[19] https://en.wikipedia.org/wiki/Emotet
[20] https://www.alpinesecurity.com/blog/empire-a-powershell-post-exploitation-tool/
[21] https://en.wikipedia.org/wiki/Flame_(malware)
[22] https://attack.mitre.org/groups/G0007/
[23] https://attack.mitre.org/groups/G0035/
[24] https://attack.mitre.org/groups/G0117/
[25] https://attack.mitre.org/groups/G0045/
[26] https://attack.mitre.org/groups/G1001/
[27] https://attack.mitre.org/groups/G0047/
[28] https://attack.mitre.org/groups/G0094/
[29] https://attack.mitre.org/groups/G0032/
[30] https://attack.mitre.org/software/S0437/
[31] https://attack.mitre.org/software/S1016/
[32] https://attack.mitre.org/software/S0603/
[33] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/bitsadmin
[34] https://en.wikipedia.org/wiki/Command-line_interface
[35] https://sk.wikipedia.org/wiki/Protokol_prenosu_súborov
[36] https://heimdalsecurity.com/blog/netwalker-ransomware-explained/
[37] https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/40ceb597-1319-4eca-8d29-fbff1793f35e.xhtml
[38] https://attack.mitre.org/techniques/T1091/
[39] https://www.senseon.io/resource/mitre-attck-lateral-movement-techniques-how-threat-actors-move-within-a-network/
[40] https://attack.mitre.org/techniques/T1072/
[41] https://attack.mitre.org/software/S0041/
[42] https://attack.mitre.org/groups/G0050/
[43] https://attack.mitre.org/groups/G0028/
[44] https://attack.mitre.org/groups/G0091/
[45] https://attack.mitre.org/techniques/T1080/
[46] https://flashpoint.io/blog/history-of-conti-ransomware/
[47] https://blogs.cisco.com/security/h1n1-technical-analysis-reveals-new-capabilities
[48] https://en.wikipedia.org/wiki/Stuxnet
[49] https://en.wikipedia.org/wiki/Ramsay_Malware
[50] https://attack.mitre.org/techniques/T1056/001/
[51] https://attack.mitre.org/techniques/T1003/
[52] https://attack.mitre.org/techniques/T1550/

[53] Jain, U. (Máj 2018). *University of Houston.* Dostupné na Internete: University of Houston: https://uh-ir.tdl.org/bitstream/handle/10657/3109/JAIN-THESIS-2018.pdf?sequence=1&isAllowed=y
[54] https://attack.mitre.org/techniques/T1550/003/
[55] https://attack.mitre.org/techniques/T1550/002/

[56] https://attack.mitre.org/techniques/T1550/004/
[57] https://www.netwrix.com/silver_ticket_attack_forged_service_tickets.html
[58] https://www.netwrix.com/how_golden_ticket_attack_works.html