Samen aanjagen van vernieuwing

Weerstand bieden tegen Man-in-the-Middle aanvallen

Handreiking

Auteur(s): SURF
Versie: 1.0
Datum: 3 juli 2024
Kenmerk: Weerstand bieden tegen MitM-aanvallen

Inhoudsopgave

1 Inleiding **3**

2 ARP-spoofing **4**

3 Session hijacking **5**

1 Inleiding

Een Man-in-the-Middle (MitM) is een aanval waarbij de aanvaller zich tussen twee partijen bevindt. De partijen denken direct met elkaar te communiceren, echter is de aanvaller in staat informatie af te luisteren (vertrouwelijkheid) en/of te wijzigen (integriteit) en hier misbruik van te maken. Het probleem bij dergelijke aanvallen is voornamelijk dat het voor het slachtoffer lastig of zelfs onmogelijk is om de authenticiteit van een netwerkverbinding, website, applicatie, etc. vast te stellen. In deze handreiking gaan we in op twee varianten van MitM aanvallen, namelijk ARP-spoofing en session hijacking. Beide aanvallen zijn gedemonstreerd tijdens een MBO Digitaal conferentie en op verzoek van de deelnemers is meer handelingsperspectief geboden.

2 ARP-spoofing

Het Address Resolution Protocol (ARP) is een communicatieprotocol dat IP-adressen verbindt aan fysieke adressen van machines (MAC-adressen). ARP-spoofing of -poisoning (T1557.002) is een aanval waarbij een cybercrimineel data kan onderscheppen en manipuleren. Een cybercrimineel kan bijvoorbeeld het MAC-adres van een router of gateway aannemen waardoor een gebruiker denkt met de router te verbinden, maar feitelijk communiceert met een door de cybercrimineel beheert apparaat. Zo kan bijvoorbeeld een DNS-verzoek voor surf.nl omgeleid worden naar een malafide website.

Hoe kun je het voorkomen (prevent)?

- Overweeg om het **bijwerken van de ARP-cache uit te schakelen** voor ongegronde ARP-replies;
- Overweeg **DHCP Snooping[1] en Dynamic ARP Inspection[2]** op switches in te schakelen om toewijzingen tussen IP- en MAC-adressen die zijn aangevraagd via DHCP- en ARP-tabellen te koppelen aan een poort op de switch die nepverkeer kan blokkeren;
- Overweeg **statische ARP-vermeldingen** voor netwerkapparaten (kan onhaalbaar zijn voor grote netwerken);
- **Netwerksegmentatie en subnetting** dragen bij aan het limiteren van de toegang tot het netwerk en verkleint daarmee de kans op verspreiding van ARP-poisoning aanvallen;
- **Network Access Control (NAC)** maakt het moeilijker voor aanvallers om onbekende apparaten te verbinden met het netwerk van de instelling.

Hoe kun je het detecteren (detect)?

- Overweeg een **Intrusion Prevention System** (IPS) om ARP-spoofing te detecteren en te blokkeren;
- Netwerk monitoring kan helpen om ARP-spoofing te detecteren, bijvoorbeeld wanneer aanvallers verkeer omleiden naar zichzelf en doorsturen naar het slachtoffer.

Hoe kun je erop reageren (respond)?

- Isoleer en blokkeer de bron van de aanval (verwijder van het netwerk, quarantaine);
- Beëindig ongewenste (externe) verbindingen met betrokken machines en isoleer/weiger ze tijdelijk;
- Analyseer logging (IDS/IPS/NIDS/EDR/Firewall/Proxy, etc.) om dat meer inzicht geeft in het malafide gedrag van de bron;
- Probeer het doel van de aanval / het malafide verkeer te begrijpen en identificeer de betrokken componenten (IP-adressen, poorten, protocollen, doelwitten, etc.);
- Bepaald aan de hand van de genoemde aandachtspunten passende vervolgstappen, zoals het verwijderen van malware, resetten van credentials, beëindigen van sessies, etc;
- Verzamel en deel indicators of compromise (IoC) met SURFcert;
- Meer maatregelen die je kunt treffen[3].

[1] https://owasp10.com/what-is-dhcp-snooping-what-is-man-in-the-middle-attack-how-to-configure-dhcp-snooping-security/
[2] https://owasp10.com/what-is-dai-dynamic-arp-inspection-and-how-to-configure-dynamic-arp-inspection-dai/

[3] https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-10.1/domain-enterprise/techniques/T1557/

3 Session hijacking

Het is een positieve ontwikkeling dat men steeds vaker gebruik maakt van Multifactor authenticatie (MFA). Hierdoor is het voor cybercriminelen lastiger om ongeautoriseerd toegang tot accounts te bemachtigen, bijvoorbeeld omdat (zwakke) wachtwoorden worden (her)gebruikt of ze zijn uitgelekt. Ongeacht het aantal factoren dat men toepast om zich te authentiseren is het resultaat altijd hetzelfde, namelijk een sessiecookie of token. Als cybercriminelen die kunnen bemachtigen kunnen zij zogenaamde replay aanvallen (T1557) uitvoeren en de sessie van de gebruiker overnemen. Cybercriminelen zijn dan ook in mindere mate geïnteresseerd in het kraken, raden of bemachtigen van wachtwoorden en focussen zich steeds meer op het kunnen stelen van sessiecookies en tokens. Deze trend is sterk waarneembaar aan de vele varianten infostealers en phishing panels en -kits die zich specialiseren in het verkrijgen van deze gegevens.

Hoe kun je het voorkomen (prevent)?

- Download en installeer nooit **software uit een onbekende bron** (o.a. usenet, torrents, P2P);
- Installeer in alle webbrowsers de browser-extensie **CookieAutodelete**[4] en schakel 'automatisch opruimen' in. Deze extensie zorgt ervoor dat alle cookies verwijderd worden bij het afsluiten van tabbladen of bij het herstarten van de browser (tenzij een domein op de whitelist of greylist is opgenomen). Mocht een endpoint geïnfecteerd raken met een infostealer dan is de kans dat er nog geldige cookies aanwezig zijn kleiner en kan ongeautoriseerde toegang mogelijk voorkomen worden. Bijvoorbeeld wanneer men is vergeten om zelf uit te loggen;
- **Verkort de geldigheidsduur** van sessiecookies maar houdt wel rekening met de werkbaarheid voor studenten en medewerkers. Een sessieduur van bijvoorbeeld 8 uur zorgt ervoor dat tokens slechts één werkdag geldig zijn, maar dat men niet meermaals per dag opnieuw hoeft te authentiseren;
- Zorg ervoor dat de **Secure cookie vlag** ingesteld is voor sessiecookies. Eerder is dit bijvoorbeeld wij voor de hoofdwebsites van mbo-instellingen onderzocht[5] en kun je zelf ook doen bijvoorbeeld via 'inspecteren' in de browser of een proxy (bijvoorbeeld ZAP of Foxyproxy);
- Zorg ervoor dat **sessie ID's** opnieuw gegenereerd worden na het inloggen om sessie fixatie te voorkomen[6];
- Overweeg het implementeren van **conditionele toegang** waarbij succesvol inloggen alleen kan wanneer men voldoet aan bepaalde condities, zoals bijvoorbeeld geografische beperkingen (IP-adressen, ASN, proxy), patchlevels van endpoints of tijdstippen (zoals 's nachts);
- Implementeer just-in-time toegang en hanteer het least privilege principe voor geprivilegieerde gebruikers[7];
- Installeer in alle webbrowsers de browser-extensie **uBlock Origin**[8]. Deze extensie zorgt ervoor dat advertenties en pop-ups geblokkeerd worden. Veel endpoints raken geïnfecteerd via malvertising, waarbij kwaadaardige code in advertenties geïnjecteerd

[4] https://github.com/Cookie-AutoDelete/Cookie-AutoDelete
[5] Mick Deben: Privacy & cookies (*alleen toegankelijk voor leden Netwerk IBP)
[6] https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html
[7] https://sec.surf.nl/controls/sb-13-003-privileged-access/
[8] https://ublockorigin.com/

wordt. Alleen door het bezoeken van een pagina kan een endpoint al geïnfecteerd raken. Deze extensie draagt daarom bij aan het beperken van de mogelijkheden daartoe en draagt bij aan het waarborgen van de privacy van medewerkers en studenten;
- Zorg ervoor dat alle endpoints voorzien van een (extended) **endpoint detection & response** (XDR/EDR) oplossing. EDR's dragen bij aan het detecteren en isoleren/verwijderen van malware, zoals infostealers. Monitor dit actief bijvoorbeeld aan de hand van passief en actief asset discovery;
- Implementeer webfiltering om het bezoeken van bekende schadelijke websites door gebruikers te voorkomen, bijvoorbeeld met behulp van de **DNS-firewall** van SURF[9]. Let op dat dit alleen effect heeft op gebruikers die verbonden zijn met het netwerk van de instelling;
- Gebruik een goede **VPN-oplossing** zoals EduVPN[10]. Met een VPN creëer je een beveiligde tunnel waardoor derden het verkeer niet kunnen meelezen of manipuleren.

Hoe kun je het detecteren (detect)?
- Meldingen van **SURFcert**, bijvoorbeeld wanneer instellingen opduiken op bekende fora, darkweb, Telegram groepen of ShadowServer meldingen, kunnen een indicatie zijn van infostealer infecties;
- Het kunnen **detecteren van data exfiltratie** op apparaten is cruciaal om infostealers te detecteren. Oplossingen zoals GlassWire[11] (Windows), Portmaster[12] (Windows/Linux) of Netiquette[13] (Mac) stellen een eindgebruiker in staat om uitgaande netwerkverbindingen te detecteren en te blokkeren;
- **XDR/EDR** oplossingen.

Hoe kun je erop reageren (respond)?
- Beëindig direct alle sessies van gecompromitteerde accounts en reset de credentials;
- Identificeer de bron van de infectie (machine, malware(familie), IP-adres, student, medewerker, etc.) en ondersteun de student of medewerker bij het verhelpen van de infectie;
- Verzamel en deel indicators of compromise (IoC) met SURFcert.

[9] https://www.surf.nl/diensten/surfdomeinen
[10] https://www.surf.nl/diensten/eduvpn
[11] https://www.glasswire.com/
[12] https://safing.io/
[13] https://objective-see.org/products/netiquette.html