نمذجة التهديدات السيبرانية

MITRE | ATT&CK

الشريك الاستراتيجي لهذا العمل شركة **Cyber Cave**


بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

لماذا هذا العمل ..

التقنيات والأساليب والطرق (TTPs) التي يقوم بها المهاجمين المبتدئين (script kiddie) او المتقدمين (APT) متعددة. مما استدعت الحاجة الى وجود إطار يقوم بنمذجة تلك التهديدات الصادرة من قبل المهاجمين بطريقة سهله الفهم وفعالة عند التطبيق. ووجود هذا الإطار باللغة العربية يعزز من عملية الفهم والادراك لمستوى الهجمات والتقنيات والأساليب المتبعة لدى محللي الامن السيبراني.

شكر وتقدير

كل الشكر والتقدير للشركة السعودية (CyberCave) وكذلك الزملاء:
في الترجمة:
- مالك الدوسري
- ثامر الشمري
- محمد السحيمي
- Nowayer

مراجعة:
- صلاح الطخيس
- فهد الدريبي

عمليات الاستطلاع والمسح /Reconnaissance

إن المقصود بعمليات الاستطلاع والمسح: هي العمليات والتقنيات التي يقوم بها المهاجم سواء كانت بطريقة نشطة أو غير نشطة لجمع المعلومات والتي قد تفييده في عمليات الاستهداف المستقبلية. وقد تتضمن هذه المعلومات بعض التفصيل عن المنظمة أو الشخص المستهدف أو البنية التحتية أو الموظفين. حيث تُمكّن هذه المعلومات المهاجم من الاستفادة من تلك المعلومات المفصلة في المراحل المتقدمة من دورة حياة الهجوم كاستخدام المعلومات التي تم جمعها لتخطيط وتنفيذ الوصول الاوليّ "Initial Access" أو لتحديد الأولويات التي يجب على المهاجم القيام بها بعد عملية الاختراق الاولي، أو توجيهه بإكمال عمليات الاستطلاع حيث أن المعلومات التي تم جمعها غير كافية.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1595		المسح النشط / Active Scanning	قبل عملية الاختراق يقوم المهاجم بإجراء عمليات مسح واستطلاع وجمع للمعلومات التي قد تفييده في عمليات الاستهداف. ونقصد هنا عمليات الاستطلاع النشطة التي تأتي بتفاعل مباشر ما بين المهاجم والمستهدف. يأتي ذلك من خلال الفحص للبنية التحتية للمستهدف واكتشاف حركة مرور البيانات وهي على عكس عمليات الاستطلاع الاخرى التي تكون غير نشطة وغير مباشرة مع المستهدف.
T1595	001	المسح لمجموعة معرفات / Scanning IP Blocks	قبل عمليات الاستهداف قد يقوم المهاجم بعمليات مسح لمجموعة من المعرفات IP address لغرض جمع المعلومات الخاصة بالمستهدف حتى يتم استخدامها في المراحل المتقدمة. إن جمع المعلومات من خلال المعرفات قد يفيد المهاجم بتحديد عدد المعرفات التابعة لجهة معينة.
T1595	002	مسح الثغرات / Vulnerability Scanning	قبل عملية الاختراق يقوم المهاجم بفحص الثغرات للهدف حتى يتم استخدام نقاط الضعف في المراحل المتقدمة من العملية. إن فحص الثغرات هو عبارة عن سلسلة من عمليات الفحص للإعدادات الخاطئة للأجهزة والأنظمة والتطبيقات والشبكات (مثل اصدار التطبيق) ومحاولة المهاجم معرفة الإصدار من أجل استغلال الثغرات الخاصة به.
T1592		جمع المعلومات من النظام المستهدف / Gather Victim Host Information	قبل عملية الاختراق يقوم المهاجم بجمع المعلومات عن الاجهزة التي لدى الهدف وقد تستخدم أثناء عمليات الاختراق. ولربما تتضمن المعلومات أسماء الاجهزة وبيانات حسابات المدراء للأنظمة والمعرفات الخاصة بهم وبعض الاعدادات الخاصة بالأنظمة.
T1592	001	العتاد / Hardware	قبل عملية الاستهداف يقوم المهاجم بجمع المعلومات عن الأجهزة التي لدى الهدف والتي قد تستخدم أثناء عمليات الاختراق. وقد تحتوي المعلومات تفاصيل البنية التحتية للأجهزة والعتاد وبعض التفاصيل مثل الإصدارات الخاصة بتلك العتاد أو بعض المعلومات التي قد تكون لإضافات تم اضافتها على العتاد والتي قد تستخدم للحماية مثل (قارئ البطاقات / المؤشرات الحيوية / أجهزة التشفير المتخصصة وما الى ذلك).
T1592	002	البرمجيات / Software	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات عن البرمجيات والتطبيقات التي تفييده في عمليات الاستهداف مستقبلاً. وقد تشتمل بعض المعلومات التي تختص بالبرمجيات مثل المعلومات المرتبطة بها من إصدارات وتواريخها، أو البرمجيات التي قد تكون مضافة مع البرمجية أو التطبيقات الاصلية.
T1592	003	انظمة / Firmware	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات عن البرامج وأنظمة التشغيل الخاصة ببعض الأجهزة والتي قد تستخدم مستقبلاً، وقد تشتمل بعض المعلومات التي تختص بأنظمة التشغيل مثل المعلومات المرتبطة بها من إصدارات وتاريخها والغرض منها وآلية الاعداد، أو البرمجيات التي قد تكون مضافة مع البرمجية أو التطبيقات الاصلية.
T1592	004	اعدادات العميل / Client Configurations	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات عن اعدادات التكوين للمستهدف والتي قد تستخدم مستقبلاً في الاستهداف. قد تتضمن المعلومات طريقة الإعدادات وتفصيلاتها. بما في ذلك نوع نظام التشغيل والإصدار والأنظمة الافتراضية والبيئة المعمارية (64 bit /32 bit) او اللغة المستخدمة أو المنطقة الزمنية.
T1589		جمع المعلومات عن هوية المستهدف / Gather Victim Identity Information	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات حول هوية المستهدف والتي من الممكن استخدامها في مراحل الاستهداف المتقدمة. وقد تتضمن المعلومات الهوية الشخصية أو هويات المجموعات على سبيل المثال (أسماء الموظفين وعناوين البريد الالكتروني وما الى ذلك) بالإضافة الى بعض البيانات الحساسة مثل بيانات الأرقام السرية.

T1589	001	بيانات الاعتماد / Credentials	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات عن بيانات الاعتماد والتي قد تستخدم في مراحل الاستهداف مستقبلاً، وقد تكون بيانات الاعتماد عبارة عن حسابات يقوم المهاجم بجمعها بهدف استهداف المنظمة للشخص المستهدف في حال كان الشخص المستهدف يقوم باستخدام بيانات اعتماد موحدة.
T1589	002	البريد الالكتروني / Email Addresses	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات عن البريد الشخصي للشخص المستهدف بهدف استخدامها في المراحل المتقدمة. وذلك من خلال استهداف بعض الخدمات المتصلة بالإنترنت والتي قد تستخدم فقط للموظفين وغيرهم.
T1589	003	اسماء الموظفين / Employee Names	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات عن أسماء الموظفين التي يمكن استخدامها في مرحلة الاستهداف المتقدمة. وقد تُستخدم أسماء الموظفين لاستخراج البريد الالكتروني الخاص بهم وكذلك في مساعدة جهود المسح والاستطلاع والتصيد.
T1590		جمع معلومات الشبكة / Gather Victim Network Information	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات حول الشبكة المستهدفة والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. وقد تتضمن المعلومات المتعلقة بالشبكة مجموعة متنوعة من التفاصيل والبيانات الهامة والحساسة مثل (بيانات المعرفات وبيانات النطاق الداخلي وغيرها) وفي بعض الأحوال قد يستطيع المهاجم رسم الطوبولوجيا وطريقة عملها.
T1590	001	خصائص النطاق / Domain Properties	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات حول الشبكة المستهدفة والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة، قد تتضمن العملية بعض الخصائص عن النطاق والمالك له ووسيلة التواصل ومعلومات التسجيل. وقد تتضمن كذلك البريد الالكتروني وطريقة التعين له داخل المنظمة (مثال أول حرف من اسم الشخص واسم العائلة وهكذا).
T1590	002	اسماء النطاقات / DNS	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع معلومات أسماء النطاقات DNS الخاصة بالمستهدف والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة، قد تتضمن العملية بعض المعلومات التفصيلية عن المستهدف منها عدد الخوادم وأسماء النطاقات الفرعية والهدف منها والخدمات كذلك (مثل خدمات البريد الالكتروني وغيرها).
T1590	003	الثقة بين الشبكات وتبعياتها / Trust Network Dependencies	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات لمعرفة مستوى الثقة داخل الشبكة الخاصة بالمستهدف والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. قد تتضمن العملية بعض المعلومات التفصيلية عن المستهدف منها عدد الجهات الخارجية التي ترتبط بالمنظمة من خلال الشبكة والفروع والخدمات المدارة والمتعاقدين وما إلى ذلك.
T1590	004	طوبولوجيا الشبكات / Network Topology	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات عن هيكلة الشبكة الخاصة بالمستهدف والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة، قد تتضمن العملية بعض المعلومات التفصيلية عن هيكلة الشبكة الفيزيائية أو الافتراضية أو الخدمات المتصلة بالإنترنت. وقد تتضمن بعض المعلومات الحساسة حول الشبكات وبوابات الانترنت وبعض معلومات البنية التحتية.
T1590	005	المعرف / IP Addresses	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع معلومات المعرفات الخاصة بالمستهدف والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة، قد تتضمن العملية بعض المعلومات التفصيلية عن المعرفات الخاصة بالمنظمات وتسلسل المعرفات "IP address range". ويستطيع المهاجم من خلال المعرفات استخراج الخدمات المرتبطة بالمنظمة كالمواقع المادية الخاصة بالمنظمة ومزودي خدمات الانترنت والبنية التحتية.
T1590	006	انظمة حماية الشبكات / Network Security Appliances	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة والخاصة بأجهزة الحماية بالشبكة المستهدفة والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. قد تتضمن العملية بعض المعلومات التفصيلية عن أجهزة وجدران الحماية وخدمات الوكيل ومصفيات الانترنت والأجهزة الأخرى المتعلقة بحماية الانترنت.

T1591		جمع معلومات المنظمة المستهدفة / Gather Victim Org Information	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة حول المنظمة المستهدفة والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. قد تتضمن العملية بعض المعلومات التفصيلية عن المنظمات والتي قد تحتوي على الأقسام والإدارات وبعض الاعمال الداخلية والعمليات الخاصة بها والمهام الوظيفية وبعض الموظفين ذوي الأهمية داخل هذه المنظمة.
T1591	001	تحديد الموقع الجغرافي / Determine Physical Locations	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع معلومات المكان الجغرافي للمنظمة المستهدفة والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. قد تتضمن العملية بعض المعلومات التفصيلية عن مكان المنظمة الجغرافي والمواد الأساسية التي تعتمد عليها المنظمة بالإضافة إلى مكان البنية التحتية ومرجعتيها الإدارية والنطاق الخاص بالتحاكم القضائي حسب المنظمة والدولة والنظام القضائي.
T1591	002	علاقة الاعمال / Business Relationships	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة حول العلاقات التجارية للمنظمة المستهدفة والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. قد تتضمن العملية بعض المعلومات التفصيلية حول العلاقات التجارية للمؤسسة من الطرف الأول أو الثاني أو الثالث والخدمات المدارة والمتعاقدين أو التي لديها صلاحيات الوصول لشبكة للمنظمة. وقد يستطيع المهاجم كشف علاقات الموردين مع الشركة والقيام باستهداف البرمجيات التي تستخدمها المنظمة.
T1591	003	وتيرة العمل داخل المنظمة / Business Identify Tempo	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات عن وتيرة الاعمال داخل المنظمة المستهدفة والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. قد تتضمن العملية بعض المعلومات التفصيلية فيما يخص درجة سرعة وخطورة الاعمال وساعات العمل الرسمية وعدد أيام العمل في الأسبوع وتواريخ الشراء والبيع والشحن للموارد والأجهزة والبرامج الخاصة بالمنظمة المستهدفة.
T1591	004	تحديد الصلاحيات / Identify Roles	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة عن الأدوار والمسؤوليات والهويات للأشخاص المستهدفين داخل المنظمة المستهدفة والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. قد تتضمن العملية بعض المعلومات الحساسة عن المنظمة والكيان الهيكلي لها والأدوار للموظفين الرئيسيين بالإضافة الى البيانات والمصادر المتاحة للوصول لها.
T1598		تصيد المعلومات / Phishing for Information	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال ارسال رسائل تصيد تستهدف العاملين بداخل المنظمة المستهدفة والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. إن التصيد الاحتيالي هو الحصول على المعلومات من خلال خداع المستهدف بهدف افشاء المعلومات أو بيانات الاعتماد. حيث يختلف التصيد المقصود بجمع المعلومات عن التصيد لإيصال برمجية تنفيذية ضارة.
T1598	001	خدمات التصيد / Spearphishing Service	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال ارسال رسائل تصيد اشخاص محددين داخل المنظمة من خلال استخدام خدمات الطرف الثالث والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. إن التصيد الاحتيالي هو الحصول على المعلومات من خلال خداع المستهدف بهدف افشاء المعلومات أو بيانات الاعتماد. وغالباً ما يستخدم التصيد المستهدف الهندسة الاجتماعية كوسيلة لجمع المعلومات كإرسال وظائف أو رسائل عاجلة وهامة.
T1598	002	تصيد من خلال المرفقات / Spearphishing Attachment	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال ارسال رسائل تصيد اشخاص محددين داخل المنظمة من خلال ارفاق ملف ضار والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. إن التصيد الاحتيالي هو الحصول على المعلومات من خلال خداع المستهدف بهدف افشاء المعلومات أو بيانات الاعتماد. وغالباً ما يستخدم التصيد المستهدف الهندسة الاجتماعية كوسيلة لجمع المعلومات كإرسال وظائف أو رسائل عاجلة وهامة.
T1598	003	تصيد من خلال الروابط / Spearphishing Link	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال ارسال رسائل تصيد اشخاص محددين داخل المنظمة من خلال ارفاق رابط ضار والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. إن التصيد الاحتيالي هو

			الحصول على المعلومات من خلال خداع المستهدف بهدف افشاء المعلومات أو بيانات الاعتماد. وغالبًا ما يستخدم التصيد المستهدف الهندسة الاجتماعية كوسيلة لجمع المعلومات كإرسال وظائف أو رسائل عاجلة وهامة.
T1597		البحث في المصادر المغلقة / Sources Search Closed	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال مصادر معلومات مغلقة عن المنظمة أو الشخص المستهدف والتي يمكن استخدامها في مرحلة الاستهداف المتقدمة. وقد تكون المعلومات المتعلقة بالمستهدفين متاحة للشراء من مصادر وقواعد بيانات خاصة أو قد يقوم المهاجمين بشراء المعلومات للاستفادة منها في عمليات الاستهداف ومن أشهرها الانترنت المظلم وغيرها.
T1597	001	موفري المعلومات الاستباقية / Vendors Threat Intel	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال مصادر الخاصة بالمعلومات الاستباقية عن التهديدات التي من الممكن استخدامها في مرحلة الاستهداف المتقدمة. وقد يقدم بائِعُو المعلومات الاستباقية مصادر تغذية مجاناً أو متقدم تحتوي معلومات متقدمة وغنيّة. كما أنه في بعض الأحيان يتم تقديم معلومات حساسة مثل أسماء العملاء أو المعرفات المصابة وغيرها. وربما تحتوي بعض المعلومات تفاصيل عن الاختراقات وتسريب البيانات التي تستهدف قطاع معين أو عمليات ربط ونمذجة التهديدات المبنية على السلوك والتقنيات TTPS .
T1597	002	شراء البيانات الفنية / Purchase Technical Data	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال شراء بعض التفاصيل والمعلومات الفنية والتي من الممكن استخدامها في مرحلة الاستهداف المتقدمة. وقد يقوم بشراء تلك المعلومات من مصادر موثوقة أو من خلال الاشتراك بوسائل المدفوعة الخاصة بمصادر المسح أو الاستطلاع وغيرها.
T1596		البحث من خلال قواعد البيانات الفنية المفتوحة / Search Open Technical Databases	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال قواعد البيانات الفنية المتاحة على الانترنت عن المنظمة المستهدفة والتي من الممكن استخدامها في مرحلة الاستهداف المتقدمة. وقد تتضمن تلك المعلومات على مستودعات البيانات الخاصة بالمنظمة أو سجلات الانترنت أو عدد النطاقات والشهادات وأسماء مسجلي النطاقات أو بعض المعلومات الحساسة عن المنظمة داخل البرمجيات أو التعليقات المتوفرة عند عمليات الفحص والاستطلاع.
T1596	001	البحث من خلال اسماء النطاقات بشكل غير مباشر / DNS/Passive DNS	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال أسماء النطاقات DNS والتي من الممكن استخدامها في مرحلة الاستهداف المتقدمة. وقد تتضمن تلك المعلومات أسماء الأشخاص أو المنظمة المالكة للنطاق أو العناوين الفرعية المستهدفة ومنها على سبيل المثال خدمات البريد وغيرها.
T1596	002	مالك العنوان / whois	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال قواعد البيانات الفنية المتاحة على الانترنت عن المنظمة المستهدفة باستخدام مواقع ونطاقات WHOIS والتي من الممكن استخدامها في مرحلة الاستهداف المتقدمة. حيث يتم تخزين البيانات بواسطة WHOIS وذلك بتخزين وتسجيل البيانات من خلال سجلات الانترنت والمسؤولين عن ربط المعرفات بإصحابها حيث يمكن لأي شخص الاستعلام عن النطاق والمعرف الخاص به ومن قام بتسجيله وماهي العناوين والنطاقات الفرعية المرتبطة به.
T1596	003	الشهادات الرقمية / Digital Certificates	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال البحث في بيانات الشهادة الرقمية للحصول على معلومات حساسة والتي من الممكن استخدامها في مرحلة الاستهداف المتقدمة. حيث يتم اصدار الشهادات الرقمية من قِبل مراجع التصديق CA وذلك بهدف التحقق من أن محتوى الموقع يتم نقله والاتصال به بشكل مشفر، حيث تحتوي تلك الشهادات على بعض المعلومات الخاصة بالتسجيل مثل الاسم والشركة والموقع الجغرافي.
T1596	004	مقدم خدمات المحتوى الشبكي / CDNs	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال البحث في بيانات شبكة خدمات المحتوى الموزع CDN والتي من الممكن استخدامها في مرحلة الاستهداف المتقدمة. تسمح شبكات الخدمات الموزعة للمؤسسات باستضافة المحتوى على مجموعة متوازية من الخوادم في نطاق جغرافي حسب طلب العميل.

T1596	005	قواعد البيانات الخاصة بمنصات المسح والاستطلاع / Scan Databases	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال البحث في بيانات المسح والاستطلاع العامة والتي لا يكون لها صلة مباشرة مع المستهدف ومن الممكن استخدامها في مرحلة الاستهداف المتقدمة. تنتشر العديد من الخدمات الخاصة بالمسح والاستطلاع على الانترنت، وغالبًا تقوم هذه الأدوات بالمسح من خلال العناوين أو النطاقات أو أسماء مسجلي تلك النطاقات أو تقوم بعض الأدوات بفحص المنافذ المفتوحة وماهي شهادات التشفير المستخدمة.
T1593		Search Open Websites/Domains / البحث من خلال المواقع	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة والمتاحة على الانترنت من خلال البحث في مواقع الويب وبشكل مجاني والتي لا تكون على اتصال مباشر مع المستهدف ومن الممكن استخدامها في مرحلة الاستهداف المتقدمة، وقد تكون المعلومات المنتشرة على الانترنت مفيدة جداً للمهاجمين مثل المعلومات المتوفرة في وسائل التواصل الاجتماعي أو العقود أو طلبات التوظيف أو المكافآت وغيرها.
T1593	001	التواصل الاجتماعي / Social Media	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال البحث في وسائل التواصل الاجتماعي والتي من الممكن استخدامها في مرحلة الاستهداف المتقدمة. قد تحتوي مواقع التواصل الاجتماعي على معلومات عن المستهدفين منظمات كانوا أو اشخاص مثل مناصبهم الوظيفية أو مواقعهم الجغرافية وكذلك اهتماماتهم.
T1593	002	محركات البحث / Search Engines	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال استخدام محركات البحث حول المستهدف والتي من الممكن استخدامها في مرحلة الاستهداف المتقدمة. قد تقوم محركات البحث بالبحث وارشفة البيانات الحساسة والغير حساسة بهدف جمع المحتوى لتسهيل الوصول له من خلال فهرسته. مما قد يمكّن المهاجم من الوصول لبعض المعلومات الغير مؤمّنه وقد تقدم بعض محركات البحث فلاتر خاصة تمكنك من البحث عن امتدادات معينه أو غيرها.
T1594		البحث من خلال الموقع المستهدف / Search Victim-Owned Websites	قبل عمليات الاستهداف، قد يقوم المهاجم بجمع المعلومات الحساسة من خلال البحث في مواقع الويب الخاصة بالجهة أو الشخص المستهدف والتي من الممكن استخدامها في مرحلة الاستهداف المتقدمة. وقد تحتوي مواقع الويب تلك على معلومات متنوعة ومفصلة بما فيها أقسام الشركة وموظفيها وكذلك تركيبة البريد الالكتروني وعملائها.

Resource Development / تطوير الموارد

تطوير الموارد :قد يشتمل على قيام المهاجمين بإنشاء أو شراء أو سرقة بعض الموارد التي تفيدهم في عمليات الاستهداف وتتضمن هذه الموارد على سبيل المثال البنية التحتية للمهاجمين أو القدرات. ويمكن للمهاجم الاستفادة من هذه الموارد للمساعدة في مراحل الاستهداف المتقدمة. على سبيل المثال استخدام لوحة التحكم المتوفرة في بعض النطاقات لعمليات التحكم والسيطرة أو استخدام البنية التحتية في ارسال رسائل تصيديه أو سرقة الشهادات أو التواقيع الرقمية وذلك لتفادي الاكتشاف.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1583		امتلاك بنية تحتية Acquire / Infrastructure	قبل عمليات الاستهداف، قد يقوم المهاجم بشراء أو استئجار البنية التحتية والتي من الممكن استخدامها أثناء عملية الاستهداف. حيث توجد أنواع متعددة من الخوادم التي تتيح للمهاجم التنسيق بين العمليات الهجومية. ومن الممكن أن يقوم المهاجم باستخدام الخدمات السحابية لأعمال ضارة في أماكن مختلفة. في بعض الأحيان قد يكون المهاجم قام باستخدام برمجيات الطرف الثالث لأغراض ضارة مثل الربط بين شبكات البوت وغيرها.
T1583	.001	النطاقات Domains/	قبل عمليات الاستهداف، قد يقوم المهاجم بشراء او استئجار النطاقات والتي من الممكن استخدامها أثناء عملية الاستهداف. إن أسماء النطاقات هي مفردات يستطيع قراءتها وحفظها الانسان وهي بديل عن المعرفات IP address والجدير بالذكر أن هناك نطاقات تستطيع استخدامها بشكل مجاني.
T1583	.002	خوادم أسماء النطاقات / DNS Server	قبل عمليات الاستهداف، قد يقوم المهاجم بإعداد خوادم أسماء النطاقات DNS والتي من الممكن استخدامها أثناء عملية الاستهداف. وقد يستخدم المهاجم قنوات خوادم أسماء النطاقات لعمليات التحكم والسيطرة أو لدعم عمليات التشغيل الخاصة بالمهاجمين.
T1583	.003	الخوادم الافتراضية Virtual / Server Private	قبل عمليات الاستهداف قد يقوم المهاجم باستئجار الخوادم الافتراضية الخاصة والتي من الممكن استخدامها أثناء عملية الاستهداف. حيث توجد مجموعة متنوعة من مزودي الخدمات السحابية والتي تقوم بتوفير الخدمات السحابية والمستودعات والخوادم الافتراضية. ويقوم المهاجمون باستخدام مثل هذه التقنية لتصعب عمليات ربط عملياتهم على المحللين بشكل واضح وكذلك لسهولة اعداد تلك الخوادم وسرعة اغلاقها.
T1583	.004	الخوادم / Server	قبل عمليات الاستهداف قد يقوم المهاجم بشراء أو استئجار الخوادم والتي من الممكن استخدامها اثناء عملية الاستهداف. حيث يتم استخدام تلك الخوادم لتنفيذ العمليات الضارة ضد المنظمات المستهدفة أو يتم استخدامها كذلك في التحكم والسيطرة. والسبب خلف استخدامها هو الحفاظ على خصوصية الأدوات التي تستخدم فترة الهجوم.
T1583	.005	البوت / Botnet	قبل عمليات الاستهداف قد يقوم المهاجم بشراء أو استئجار الشبكات والتي تحتوي على عدد كبير من الأنظمة المخترقة ومن الممكن استخدامها اثناء عملية الاستهداف. حيث أن البوت عبارة عن شبكات من الأنظمة المخترقة ويتم استخدامها بتوجيهها لأداء مهام منسقة. ويمكن للمهاجمين شراء أو الاشتراك لاستخدام شبكة البوت في هجمات حجب الخدمة أو هجمات التصيد.
T1583	.006	خدمات الويب Web Services/	قبل عمليات الاستهداف قد يقوم المهاجم بشراء أو استئجار خدمات الويب والتي من الممكن استخدامها أثناء عملية الاستهداف. توجد مجموعة متنوعة من مواقع الويب الشائعة والتي يقوم المهاجمين بالتسجيل فيها والاستفادة من خدماتها (مثل خدمات التحكم والسيطرة أو خدمات نقل وتسريب وحفظ الملفات) بالإضافة إلى استخدام وسائل التواصل الاجتماعي للتحكم والسيطرة حيث يقوم المهاجمين باستخدامها لكي تساعدهم في التخفي من الرصد والاكتشاف وكذلك تسهل عليهم ربط عملياتهم.
T1586		الحسابات المخترقة / Compromise Accounts	قبل عمليات الاستهداف قد يقوم المهاجم باختراق الحسابات والتي من الممكن استخدامها اثناء عملية الاستهداف. يستخدم المهاجمون الهندسة الاجتماعية لهذا الغرض حيث يتم القيام بانتحال شخصيات معروفة لدى الشخصية المستهدفة لكي يولد الثقة لديه والتي قد تؤدي في النهاية إلى اختراق حسابه.

T1586	.001	حسابات وسائل التواصل الاجتماعي Media Social / Accounts	قبل عمليات الاستهداف قد يقوم المهاجم باختراق حسابات التواصل الاجتماعي والتي من الممكن استخدامها أثناء عملية الاستهداف. يستخدم المهاجمون الهندسة الاجتماعية لهذا الغرض. حيث يقوم المهاجمون بانتحال شخصيات معروفة لدى الشخصية المستهدفة حتى يولد الثقة لديه والتي قد تؤدي في النهاية إلى اختراق الحساب.
T1586	.002	البريد الالكتروني / Email Accounts	قبل عمليات الاستهداف قد يقوم المهاجم باختراق حسابات البريد الالكتروني والتي من الممكن استخدامها أثناء عملية الاستهداف. وقد يستخدم المهاجمون البريد الالكتروني لتعزيز العمليات التي يقومون بها. على سبيل المثال بعد عملية الاختراق للبريد الالكتروني يقوم بإرسال رسائل تصيد للمستهدفين حيث سيكون هناك إحساس بالثقة ما بين الشخص المستهدف والبريد المخترق. والتي قد يتم استخدامها لتثبيت البرمجيات الضارة أو الحصول على صلاحيات الوصول للبنية التحتية.
T1584		بنية تحتية مخترقة Compromise / Infrastructure	قبل عمليات الاستهداف قد يقوم المهاجم باختراق البنية التحتية التابعة للجهات والتي من الممكن استخدامها أثناء عملية الاستهداف. قد تشمل حلول البنية التحتية على الخوادم المادية أو السحابية أو خدمات الويب التابعة للجهات. يقوم المهاجمين بهذه الهجمات بدلًا من شراء أو استئجار البنية التحتية باستخدام تلك المنصة لمهاجمة منظمات أخرى أو من خلال استخدام تلك البنية التحتية لشبكات البوت.
T1584	.001	النطاقات / Domains	قبل عمليات الاستهداف، قد يقوم المهاجم بسرقة النطاقات الرئيسية أو الفرعية والتي من الممكن استخدامها أثناء عملية الاستهداف. إن أسماء النطاقات هي مفردات يستطيع قراءتها وحفظها الانسان وهي بديل عن المعرفات IP address والجدير بالذكر أن المهاجم يستطيع سرقة النطاقات من خلال اختراق البريد الالكتروني للمستهدف ومن ثم يقوم باستعداد كلمة المرور للنطاق المراد سرقته وفي بعض الحالات يتم استخدام الهندسة الاجتماعية أو استغلال بعض الإعدادات الخاطئة.
T1584	.002	خوادم اسماء النطاقات / DNS Server	قبل عمليات الاستهداف، قد يقوم المهاجم باختراق خوادم أسماء النطاقات التابعة لمقدمي الخدمات والتي من الممكن استخدامها أثناء عملية الاستهداف. إن أسماء النطاقات هي مفردات يستطيع قراءتها وحفظها الانسان وهي بديل عن المعرفات IP address.بعد قيام المهاجم بالاختراق يقوم بإعادة حركة المرور للاستعلامات لخوادم التحكم والسيطرة وقد يقوم باختراق خوادم أسماء النطاقات التابعة لمقدمي الخدمات لدعم العمليات التي يقوم بها.
T1584	.003	الخوادم الافتراضية Virtual / Server Private	قبل عمليات الاستهداف، قد يقوم المهاجم باختراق الخوادم الافتراضية التابعة لمقدمي الخدمات والتي من الممكن استخدامها أثناء عملية الاستهداف. توجد أنواع متعددة من مقدمي خدمات الافتراضية VMs حيث تتنوع ما بين خوادم سحابية ومستودعات وخدمات. وقد يقوم المهاجم باختراق خوادم خاصة تم شراءها أو استئجارها من قبل مقدمي الخدمات وذلك لجعل فرصة ايجادهم وربط البنية التحتية لدى المدافعين أصعب.
T1584	.004	الخوادم / Server	قبل عمليات الاستهداف، قد يقوم المهاجم باختراق الخوادم التابعة لمقدمي الخدمات والتي من الممكن استخدامها اثناء عملية الاستهداف. يسمح استخدام الخوادم من قبل المهاجمين في تنفيذ وتنظيم الهجمات. ويستخدمه المهاجمين كذلك لأغراض مختلفة بما فيها مهام التحكم والسيطرة عوضًا عن شراء أو استئجار خادم خاص.
T1584	.005	البوت / Botnet	قبل عمليات الاستهداف، قد يقوم المهاجم باختراق عدد كبير من الأنظمة والخوادم التابعة لمقدمي الخدمات والتي من الممكن استخدامها أثناء عملية الاستهداف. يقوم المهاجمين باستهداف عدد كبير من الأنظمة وذلك من أجل استخدامها كشبكة بوت والتي من الممكن توجيهها واستخدامها لعمليات هجمات حجب الخدمة وغيرها. وقد يقوم المهاجمين باختراق خوادم جاهزة لعمليات البوت أو استئجارها أو شراءها. ومن أنواع الهجمات المتوقع القيام بها هي هجمات حجب الخدمة أو التحكم والسيطرة على نطاق واسع.
T1584	.006	خدمات الويب / Web Services	قبل عمليات الاستهداف، قد يقوم المهاجم باختراق الأنظمة والخوادم التابعة لمقدمي الخدمات والتي من الممكن استخدامها أثناء عملية الاستهداف. قد يستخدم المهاجمين بعض مقدمي خدمات الويب المشهورين مثل GitHub و Twitter و Drobbox و google الخ ليقوم بالحصول على صلاحيات الحساب المستهدف من خلال استغلال الخدمات أو البنية التحتية الخاصة به وذلك لأغراض وعمليات ضارة. على سبيل المثال استخدامها لعمليات التحكم والسيطرة من خلال أدوات معدة مسبقاً وتستطيع التعامل مع الخدمات العامة مثل google و

T1587			Twitter وغيرها مما يعطي الأفضلية للمهاجم من حيث التخفي وتقليل البيانات الضارة على الشبكة حتى يصعب اكتشافه ورصدة وربطه بمجموعة أو مهاجمين معينين.
T1587		القدرات التطويرية / Develop Capabilities	قبل عمليات الاستهداف، قد يقوم المهاجم ببناء قدرات برمجية تمكنه من استخدامها أثناء عملية الاستهداف بدلًا من شرائها أو استئجارها أو حتى الحصول عليها مجاناً أو سرقتها. يمكن للمهاجمين من تطوير قدراتهم وبرمجياتهم داخليًا وهنا تأتي عملية المتطلبات الخاصة من توفر قدرات التحكم والسيطرة والتهرب من الاكتشاف والتمكن من تشفير البيانات واستخدامها لشهادات الموقعة. قد يطور المهاجمين مثل هذه الأدوات لدعم العمليات في مراحل متعددة من مراحل الهجوم.
T1587	.001	البرمجيات الضارة / Malware	قبل عمليات الاستهداف، قد يقوم المهاجم بتطوير برمجيات ضارة يمكن استخدامها أثناء عملية الاستهداف. تتضمن البرمجيات الضارة بعض الاكواد الضارة والتي تفيد في مراحل متقدمة من مراحل الهجوم. وتكون في الغالب اما تحكم وسيطرة أو أبواب خلفية أو برمجية تستطيع نسخ نفسها في الأجهزة القابلة للإزالة USB مما يفيد المهاجمين في مراحل الهجوم الأخرى. والسبب يقف خلف تطوير تلك البرمجيات هو جعل عملية اكتشافهم أصعب وكذلك التهرب من برمجيات وأنظمة الدفاع عن الشبكات والأجهزة.
T1587	.002	شهادات التواقيع البرمجية / Code Signing Certificates	قبل عمليات الاستهداف، قد يقوم المهاجم باستخدام تواقيع للأكواد ذاتيًا والتي من الممكن استخدامها أثناء عملية الاستهداف. وقد تشمل عمليات التواقيع على الأكواد والبرمجيات التنفيذية والبرامج النصية وذلك بغرض التأكيد وضمان عدم التعديل أو التغير أو الإتلاف. وقد يولد وجود التواقيع الرقمية للأكواد بعض الثقة لدى المستخدمين من أن هذه الأكواد والبرمجيات آمنة حتى وإن كان مصدرها غير معروف أو غير آمن.
T1587	.003	الشهادات الرقمية / Digital Certificates	قبل عمليات الاستهداف، قد يقوم المهاجم بإنشاء شهادات SSL/TLS موقعه ذاتياً والتي من الممكن استخدامها أثناء عملية الاستهداف. تم تصميم شهادات SSL/TLS لوضع الثقة في عملية نقل البيانات وهي تتضمن معلومات متعددة حول المفاتيح المستخدمة ومعلومات تخص التوقيع الرقمي للكيان الذي تحقق من صحة محتويات الشهادة. في حال كانت الشهادة صحيحة وكان الشخص يثق بالنطاق الذي يحمل تلك الشهادة فعندئذ يقوم بالتواصل مع النطاق المالك للشهادة. في كثير من الأحيان تفقد تلك الشهادات الموقعة ثقتها بسبب كونها موقعة ذاتيًا.
T1587	.004	الاختراق / Exploits	قبل عمليات الاستهداف، قد يقوم المهاجم بتطوير أدوات اختراق متعددة والتي من الممكن استخدامها أثناء عملية الاستهداف. حيث يتم تصميم تلك الأدوات لاستغلال ثغرات أو أخطاء برمجية وأمنيّة تستهدف الأنظمة والخوادم التي لم تقم بسد تلك الثغرات. حيث يقوم المهاجمين بتطوير أدواتهم بدل عمليات شراء أو سرقة تلك الأدوات. وقد يستخدم المهاجم قدراته من خلال المعرفة العميقة في الثغرات لبناء أدوات مطورة داخلياً. وكجزء من عمليات تطوير أدوات الاختراق يقوم المهاجم باستخدام الطرق المعتادة في عمليات البحث والهندسة العكسية للأنظمة أو الثغرات.
T1585		إنشاء حسابات أو جمعها / Establish Accounts	قبل عمليات الاستهداف، قد يقوم المهاجم بإنشاء حسابات خاصة للخدمات والتي من الممكن استخدامها أثناء عملية الاستهداف. يمكن للمهاجمين إنشاء حسابات وبناء شخصيات وهمية تحتوي على معلومات شخصية وتاريخية بهدف استخدامها في عمليات اختراق مستقبلية. وقد تكون تلك الحسابات إما في وسائل التواصل أو في المواقع الأخرى.
T1585	.001	حسابات وسائل التواصل الاجتماعي / Media Social Accounts	قبل عمليات الاستهداف، قد يقوم المهاجم بإنشاء حسابات خاصة على وسائل التواصل الاجتماعي والتي من الممكن استخدامها أثناء عملية الاستهداف. يمكن للمهاجمين إنشاء حسابات وبناء شخصيات وهمية تحتوي على معلومات شخصية وتاريخية. بهدف استخدامها في عمليات اختراق مستقبلية. وقد تكون تلك الحسابات إما في وسائل التواصل أو في المواقع الأخرى.
T1585	.002	البريد الالكتروني / Email Accounts	قبل عمليات الاستهداف، قد يقوم المهاجم بإنشاء بريد الالكتروني والذي من الممكن استخدامه اثناء عملية الاستهداف. قد يقوم المهاجمين بإنشاء حسابات بريد إلكترونية من موفري خدمات البريد المجاني لتعزيز عملياتهم الهجومية مثل عمليات التصيد وغيرها أو قد تستخدم للتسجيل في وسائل التواصل الاجتماعي وذلك لزيادة فرصة نجاح الهندسة الاجتماعية.

T1588		امتلاك القدرات / Obtain Capabilities	قبل عمليات الاستهداف، قد يقوم المهاجم بشراء أو سرقة القدرات والتي من الممكن استخدامها أثناء عملية الاستهداف بدلًا من تطويرها داخلياً أو الحصول عليها مجاناً. وقد تشتمل تلك القدرات على برمجيات ضارة أو الحصول على تراخيص لبرمجيات التحكم والسيطرة أو استغلال وسرقة الشهادات الرقمية وكذلك سرقة المعلومات الخاصة ببعض الثغرات وطرق استغلالها. من الممكن استخدام تلك القدرات في جميع عمليات الاختراق المستقبلية.
T1588	.001	البرمجيات الضارة / Malware	قبل عمليات الاستهداف، قد يقوم المهاجم بشراء أو تحميل البرمجيات الضارة والتي يمكن استخدامها أثناء عملية الاستهداف. تتضمن البرمجيات الضارة بعض الأكواد الضارة والتي تفيد في مراحل متقدمة من مراحل الهجوم. وتكون في الغالب إما تحكم وسيطرة أو أبواب خلفية أو برمجية تستطيع نسخ نفسها في الأجهزة القابلة للإزالة USB مما يفيد المهاجمين في مراحل الهجوم الأخرى. والسبب يقف خلف تطوير تلك البرمجيات هو جعل عملية اكتشافهم أصعب وكذلك التهرب من برمجيات وأنظمة الدفاع عن الشبكات والأجهزة.
T1588	.002	الأدوات / Tools	قبل عمليات الاستهداف، قد يقوم المهاجم بشراء أو تحميل أو سرقة الأدوات والتي يمكن استخدامها أثناء عملية الاستهداف وتتضمن أدوات مفتوحة المصدر او مغلقة مجانية أو مدفوعة. قد تُستخدم تلك الأدوات لعمليات ضارة على سبيل المثال استخدام PsExec .يقوم المهاجمين باستخدام أدوات معدة لعمليات تقييم الثغرات أو اختبار الاختراق وأشهرها CobaltStrike. وفيها يقوم المهاجمين إما بكسر الإصدارات المتوفرة لديهم أو سرقة التراخيص.
T1588	.003	شهادات التواقيع البرمجية / Code Signing Certificates	قبل عمليات الاستهداف، قد يقوم المهاجم بشراء أو تحميل أو سرقة تواقيع للأكواد والتي من الممكن استخدامها أثناء عملية الاستهداف. قد تشمل عمليات التواقيع على الأكواد والبرمجيات التنفيذية والبرامج النصية وذلك بغرض التأكيد وضمان عدم التعديل أو التغير أو الإتلاف. يولد وجود التواقيع الرقمية للأكواد بعض الثقة لدى المستخدمين من أن هذه الأكواد والبرمجيات آمنة حتى وإن كان مصدرها غير معروف أو غير آمن.
T1588	.004	الشهادات الرقمية / Digital Certificates	قبل عمليات الاستهداف، قد يقوم المهاجم بشراء أو سرقة أو تحميل أو الحصول على شهادات SSL/TLS موقعه ذاتياً والتي من الممكن استخدامها أثناء عملية الاستهداف. تم تصميم شهادات SSL/TLS لوضع الثقة في عملية نقل البيانات وهي تتضمن معلومات متعددة حول المفاتيح المستخدمة ومعلومات تخص التوقيع الرقمي للكيان الذي تحقق من صحة محتويات الشهادة. في حال كانت الشهادة صحيحة وكان الشخص يثق بالنطاق الذي يحمل تلك الشهادة فعندئذ يقوم بالتواصل مع النطاق المالك للشهادة. في كثير من الأحيان تفقد تلك الشهادات الموقعة ثقتها بسبب كونها موقعة ذاتيًا.
T1588	.005	الاختراق / Exploits	قبل عمليات الاستهداف، قد يقوم المهاجم بشراء أو سرقة أو تحميل أدوات اختراق متعددة والتي من الممكن استخدامها أثناء عملية الاستهداف. حيث يقوم المهاجمين باستغلال تلك الثغرات من خلال تعديل أدوات متوفرة أو شراءها جاهزة للاستخدام.
T1588	.006	الثغرات / Vulnerabilities	قبل عمليات الاستهداف، قد يكون لدى المهاجمين المعلومات الكاملة والشاملة عن الثغرات والتي من الممكن استخدامها أثناء عملية الاستهداف. نقصد بالثغرة الأمنية هي نقاط ضعف في أنظمة وبرمجيات وأجهزة الكمبيوتر. وقد يقوم المهاجمون باستغلالها بطرق مباشرة أو غير مباشرة. عادةً ما يجد المهاجمين المعلومات عن بعض الثغرات متوفرة على الإنترنت من خلال مصادر مفتوحة أو مغلقة.

الاختراق الاولي / Initial Access

الاختراق الاولي: يتكون الوصول الاولي من مجموعة من التقنيات التي تستخدم للحصول على صلاحيات أولية للوصول للنظام او الشبكة المستهدفة. وتشتمل الأساليب المستخدمة ما بين رسائل تصيدية او استغلال نقاط الضعف على الخدمات المتصلة بالإنترنت. وقد يسمح الوصول الاولي للمهاجم باستمرارية وانتشاره داخل الشبكة بل قد يستطيع المهاجم الحصول على احد الحسابات الفعالة واستخدامه في احد الخدمات المتصلة بالإنترنت او تغير كلمات المرور الخاصة بها.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1189		الاختراق من خلال الوصول Compromise Drive-by	يمكن للمهاجمين من الوصول للنظام من خلال قيام المستخدم بزيارة موقع من خلال عمليات التصفح. وقد يقوم المهاجم باختراق الموقع وحقنه باكواد تمكن من سحب بعض المعلومات الهامة من المتصفح دون عملية اختراقه المعتادة. ان بعض تقنيات الهجوم تقوم على استهداف المتصفحات المصابة بثغرات
T1190		اختراق تطبيقات المتصلة بالأنترنت / Public- Exploit Facing Application	قد يحاول المهاجمون الاستفادة من نقاط الضعف على الانظمة والاجهزة المتصلة بالإنترنت بشكل مقصود او غير مقصود. ويمكن ان تكون نقاط الضعف اما ثغرة برمجية او خطا في الاعدادات او خطا في تصميم البرمجيات وامانها. وغالباً ما تكون هذه التطبيقات تطبيقات الويب، لكن من الممكن ان تتضمن خدمات مثل قواعد البيانات SQL وخدمات SMB,SSH. او ادارة اجهزة الشبكات SNMP. او اي تطبيق اخرى يمكن الوصول له من خلال الانترنت.
T1133		خدمات الاتصال عن بعد / External Remote Services	قد يستفيد المهاجمين من الخدمات الخارجية المتصلة بالإنترنت والتي تودي الوصول بشكل مباشر لأجهزة وانظمة الشبكة. وتتيح الخدمات الوصول عن بعد مثل VPN وCitrix. ان الاجهزة والخدمات هي تسمح للمستخدمين بالوصول عن بعد لأجهزة وموارد النظام. وكما توجد بعض خدمات الاتصال عن بعد لها بوابات تحقق ومصادقة ومن امثلتها خدمة " Windows Remote Management"
T1200		العتاد الاضافي / Hardware Additions	قد يستخدم المهاجمون بعض ملحقات الكمبيوتر والشبكات لضمان الوصول الاولي. لم يتم رصد مجموعات هجوم تقوم بمثل هذه الهجمات. وقد يتم استخدامها في بعض الاحيان من قبل مختبري الاختراق للوصول الاولي لشبكة. ومثل هذه الملحقات متوفرة بكثره ومنها ما هو متوفر بشكل مفتوح ومغلق المصدر وتجاري. مثل اجهزة تسجيل ضربات المفاتيح وهجمات اعتراض البيانات وحقن النواة واستخراج الذاكرة العشوائية او من خلال استغلال بعض ملحقات الاتصال اللاسلكي.
T1566		التصيد / Phishing	قد يستفيد المهاجمين من رسائل التصيد للوصول لأنظمة المستهدف. ويتم ارسال رسائل التصيد باستخدام الهندسة الاجتماعية. ويمكن استخدام كذلك التصيد المستهدف الموجهة. والتي قد تستهدف الافراد والشركات والقطاعات والصناعات. وقد يتم ارسال عدد ضخم من رسائل التصيد الغير مرغوبة بها محمله بالبرامج الضارة.
T1566	.001	التصيد بواسطة المرفقات / Spearphishing Attachment	قد يستفيد المهاجمين من رسائل التصيد التي تحتوي على مرفقات ضارة بهدف الوصول للأنظمة المستهدفة. ويتم ارسال رسائل التصيد باستخدام الهندسة الاجتماعية. ويمكن استخدام كذلك التصيد المستهدف الموجهة. والتي قد تستهدف الافراد والشركات والقطاعات والصناعات. ومن السيناريوهات المستخدمة ارسال بريد ضار محمل ببرمجيات ضارة وحيث يعتمدون على المستخدم او المستهدف في تفعيل برمجياتهم الضارة من خلال الهندسة الاجتماعية مثل ظهوره كمصدر موثوق.
T1566	.002	التصيد من خلال الروابط / Link Spearphishing	قد يستفيد المهاجمين من رسائل التصيد التي تحتوي على روابط ضارة بهدف الوصول للأنظمة المستهدفة. ويتم ارسال رسائل التصيد باستخدام الهندسة الاجتماعية. ويمكن استخدام كذلك التصيد المستهدف الموجهة. والتي قد تستهدف الافراد والشركات والقطاعات والصناعات. وقد يستخدم المهاجمون الاستهداف من خلال روابط ضارة بدل من المرفقات وذلك لتهرب من انظمة الكشف والرصد ومن الممكن اقناع المستهدف من خلال استخدام الهندسة الاجتماعية وظهور ان الرابط امن وموثوق.
T1566	.003	التصيد بواسطة الخدمات / Spearphishing via Service	قد يقوم المهاجمون بالاستفادة من خدمات الطرف الثالث لإرسال رسائل تصيديه مستهدفة. حيث ان التصيد المستهدف من خلال الخدمات هو أحد عمليات التصيد الاحتيالي. ويختلف عن البقية حيث يكون قائم على الاطراف الثالثة بدل من استخدام البريد الخاص بالمهاجم او انتحال صفة بريد اخر.

T1091		النسخ المطابق بواسطة الاجهزة القابلة للإزالة / Replication Through Removable Media	قد يستفيد المهاجمون من الاجهزة القابلة للإزالة لاستهداف الانظمة والشبكات الغير متصلة بالأنترنت او المعزولة. حيث يتم حقنها ببرمجية ضارة ويتم الاستفادة من الخدمة المدمجة مع انظمة ويندوز "Autoran". والتي تسمح بتشغيل البرمجية من لحظة ادخال القرص القابل للإزالة. وقد يقوم البرنامج الضار بنسخ نفسة او تعديل البرمجيات المراد استهدافها
T1195		اختراق الموردين / Supply Chain Compromise	قد يقوم المهاجمين بالتلاعب بالمنتجات او آليات او طرق تسليم المنتجات قبل وجهتها النهائية. وذلك لغرض اعتراض او التلاعب بالبيانات او اختراق النظام.
T1195	.001	اختراق المتطلبات الخاصة بالبرمجيات / Compromise Software Dependencies and Development Tools	قد يقوم المهاجمين بالتلاعب بالمتطلبات الخاصة ببعض البرمجيات او ادوات تطوير البرمجيات قبل وصولها الى المستهلك النهائي. وقد تعتمد بعض البرمجيات على الملحقات الخارجية والاضافات لكي تعمل بشكل سليم. وتختلف تلك الاضافات والمتطلبات والتي قد تكون مفتوحة المصدر او مغلقة المصدر.
T1195	.002	اختراق تطبيقات الموردين / Software Compromise Supply Chain	قد يتلاعب المهاجمين بمكونات التطبيق الخاص بالموردين قبل تسليمها للمستهلك النهائي وذلك بهدف. الاختراق للنظام او التلاعب بالبيانات وحيث يتم استهداف تطبيقات الموردين بالعديد من الطرق على سبيل المثال التلاعب بالشفرة المصدرية للتطبيق او تعديله او التغيرات التي يتم ارسالها مع التحديثات للمستهدفين.
T1195	.003	اختراق العتاد الخاص بالموردين / Hardware Compromise Supply Chain	قد يتلاعب المهاجمين بمكونات بالعتاد الخاص بالموردين قبل تسليمها للمستهلك النهائي وذلك بهدف .الاختراق للنظام او التلاعب بالبيانات وحيث يتم استهداف العتاد الخاص بالموردين بالعديد من الطرق على سبيل المثال تركيب اجهزة وبرمجيات التجسس. والتي قد يتم تركيبها اما على الخوادم او اجهزة الشبكة او النهايات الطرفية.
T1199		علاقة الثقة بين المنظمات / Relationship Trusted	قد يستفيد المهاجمون من العلاقات الثقة بين المنظمات. حيث صلاحيات الوصول المبنية على الثقة بين الاطراف قد يستفيد منها المهاجمون بسبب قلة آليات التدقيق والتحقق للوصول للشبكات
T1078		حساب فعال / Valid Accounts	قد يستفيد المهاجمون من استغلال بيانات الدخول وذلك لتحقيق الوصول الاولي والتمكن والتخفي ورفع الصلاحيات داخل الشبكة. حيث يمكن استخدام بيانات الدخول المخترقة لتجاوز بعض آليات الحماية والتحكم الموضوعة سواء على مستوى الانظمة او الشبكات. ومن الممكن استخدام بيانات الدخول للأنظمة البعيدة مثل خدمات الاتصال الظاهري VPN وخدمات البريد الالكتروني وخدمات الاتصال بسطح المكتب عن بعد. وقد يستخدم المخترقون تلك البيانات للوصول لمناطق حساسة وحرجة داخل الشبكة. وفي حال كانت الصلاحيات عالية لدى الحساب المخترق فقد يتجنب المستخدمون استخدام برمجيات اضافية لتصعيد الصلاحيات وذلك يساعدهم في التهرب من انظمة الحماية داخل الشبكة.
T1078	.001	حساب افتراضي / Default Accounts	قد يستفيد المهاجمون من الحسابات الافتراضية واستخدامها لعمليات الوصول الاولية او التمكن او التخفي او رفع وتصعيد الصلاحيات او التهرب من انظمة الحماية. ان الحسابات الافتراضية قد تأتي مضمنة مع الانظمة والتطبيقات. مثل حساب الضيف في انظمة الويندوز. وكذلك بعض الحسابات الافتراضية قد تأتي على شكل حسابات خاصة بالجهات المصنعة للمنتج او موفري تلك الخدمات. في بعض الاحيان تكون الحسابات الافتراضية بصلاحيات مدير للنظام مثل حساب مدير النظام في AWS وحساب الخدمات الافتراضي في Kubernetes
T1078	.002	حساب مدير النظام / Domain Accounts	قد يستفيد المهاجمون من الحسابات الخاصة بمدراء النظام واستخدامها لعمليات الوصول الاولية او التمكن او التخفي او رفع وتصعيد الصلاحيات او التهرب من انظمة الحماية. ان حسابات مدراء النظام والتي في العادة وجدت لإدارة الأذونات للأنظمة والخدمات في Active directory. ويمكن لحسابات مدراء النظام ادارة حسابات المستخدمين والمسؤولين والخدمات.

T1078	.003	حسابات محلية / Local Accounts	قد يستفيد المهاجمون من الحسابات المحلية للنظام واستخدامها لعمليات الوصول الاولية او التمكن او التخفي او رفع وتصعيد الصلاحيات او التهرب من انظمة الحماية. ان حسابات المحلية هي التي تم انشاءها من قبل المنظمة بهدف تقديم الدعم او الخدمات.
T1078	.004	حسابات على الخدمات السحابية / Accounts Cloud	قد يستفيد المهاجمون من الحسابات للخدمات الحسابية واستخدامها لعمليات الوصول الاولية او التمكن او التخفي او رفع وتصعيد الصلاحيات او التهرب من انظمة الحماية. ان حسابات المحلية هي التي تم انشاءها من قبل المنظمة بهدف تقديم الدعم او الخدمات او تطبيقات SaaS وفي بعض الحالات قم يتم توحيد الحسابات ما بين الانظمة السحابية وخدمات ادارة الصلاحيات والهويات التقليدية Active Directory.

التنفيذ او التشغيل /Execution

التنفيذ: يتكون التنفيذ او التفعيل الى تشغيل بعض الاكواد البرمجية الضارة على نظام محلي او عن بعد والتي تعطي المهاجم افضلية التحكم والسيطرة على المستهدف. وغالباً تقترن جميع العمليات والتقنيات والأساليب المتقدمة بعد القيام بعملية (التنفيذ او التشغيلExecution). ومن الأمثلة عمليات قيام المهاجم باستخدام أدوات عن بعد بهدف التحكم والسيطرة بالأنظمة من خلال سكربت PowerShell.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1059		سطر الاوامر التفاعلي / Command and Scripting Interpreter	قد يسئ المهاجمون استخدام واجهة سطر الاوامر لتنفيذ تعليمات وسكربتات وواجهة سطر الاوامر تستخدم عادة لتعامل مع النظام وهي متوفرة في مختلف الانظمة. وتأتي مدمجة في معظم الانظمة وتعطي بعض القدرات المتقدمة لتحكم بالنظام ومن امثلتها Unix Shell و CMD و PowerShell.
T1059	.001	سكربت PowerShell	قد يقوم المهاجمون باستخدام اوامر PowerShell لتنفيذ تعليمات ضارة. وPowerShell هي واجهة سطر اوامر تفاعلية قوية وبيئية نصية تمكنك من التحكم بالنظام وهي تستخدم لنظام ويندوز. ويمكن للمهاجمين من استخدام PowerShell لتنفيذ العديد من العمليات بما في ذلك تشغيل الملفات التنفيذية واستكشاف الملفات وغيرها. على سبيل المثال تعليمة cmdlet Start-Process والي تسمح بتشغيل الاوامر وتنفيذها وامر Invoke-Command cmdlet والتي تسمح بتفعيل وتشغيل الاوامر عن الانظمة المحلية او عن بعد. والجدير بالذكر ان للاتصال بالنظام عن بعد قد تحتاج الى صلاحيات مدير النظام.
T1059	.002	سكربت AppleScript	قد يقوم المهاجمون باستخدام AppleScript لتنفيذ تعليمات برمجية ضارة و AppleScript هي لغة برمجة نصية لأنظمة MacOS وهي مصممة للتحكم في التطبيقات وبعض اجزاء من النظام عبر استخدام الرسائل بين التطبيقات وتسمى AppleEvent. ويمكن ارسال رسائل AppleEvent هذه بشكل مستقل او كتابتها بسهولة من خلال AppleScript. ويمكن لهذه التعليمات من تحديد عدد النوافذ المفتوحة على سطح المكتب وتسجيل ضربات المفاتيح والتواصل مع معظم البرمجيات التي تعمل محلياً او عن بعد.
T1059	.003	سطر الاوامر التفاعلي الخاص بالويندوز / Windows Command Shell	قد يقوم المهاجمون باستخدام سطر الاوامر ويندوز CMD لتنفيذ تعليمات ضارة. وسطر الاوامر CMD هو سطر الاوامر الرسمي في ويندوز. وقد يتم استخدام سطر الاوامر لتحكم في معظم خصائص النظام وكذلك التحكم في بعض الصلاحيات والادوار.
T1059	.004	سطر الاوامر التفاعلي الخاص بالينكس / Shell Unix	قد يقوم المهاجمون باستخدام سطر الاوامر UNIX لتنفيذ تعليمات برمجية ضارة. وهو موجه الاوامر الاساسي لأنظمة Linux وMacOS.وعلى الرغم توجد بعض الاختلافات البسيطة في سطر الاوامر مثل (zsh ,sh, bash) واعتمادية نظام التشغيل وكذلك اصدارات النسخ. وحيث يمكنك التحكم في معظم خصائص النظام من خلال سطر الاوامر وبعض الخصائص تحتاج الى صلاحيات مدير نظام.
T1059	.005	سكربت Visual Basic	قد يقوم المهاجمون باستخدام لغة Basic VB-Visualلتنفيذ تعليمات برمجية ضارة. ولغة VB تم انشاؤها من قبل مايكروسوفت وتسمح اللغة بتفاعل مع أكثر التقنيات الخاصة بالويندوز مثل استخدام Object Model وWindows API. حيث ان لغة VB تعتبر من اللغات القديمة قليلً وحيث من المخطط للغة انه يتم دمجه مع .NET Framework وNET Core وهي اللغة التي تدعم منصات متعددة.
T1059	.006	لغة Python	قد يقوم المهاجمون باستخدام لغة بايثون لتنفيذ تعليمات برمجية ضار. ان لغة بايثون هي أحد اللغات العالية المستوى والمشهورة والتي تتمتع بقدرات قوية جداً. تستطيع لغة البايثون من تنفيذ تعليمات برمجية تفاعلية من سطر الاوامر من خلال استخدام python.exe او من خلال أحد ملفاتها .py. والتي يمكن تشغيلها على معظم الانظمة التي تدعم لغة البايثون ويمكن كذلك للغة من جمع الاكواد وتنفيذها وتشغيلها.
T1059	.007	سكربت JavaScript/JScript	قد يقوم المهاجمون باستخدام JavaScript لأغراض ضارة ان JavaScript هي لغة نصية مستقلة عن النظام الاساسي ويتم تشغيلها والتفاعل معها بشكل مباشر وهي عادة مرتبطة مع المتصفحات ومن الممكن تشغيل JavaScript على النظام بشكل مباشر دون الحاجة الى وجود متصفح.
T1059	.008	سطر الاوامر التفاعلي الخاص بالشبكات /	قد يقوم المهاجمين باستغلال السكربتات او سطر الاوامر المدمج CLI في الشبكة لتنفيذ أوامر او تعليمات برمجية ضارة. ان سطر الأوامر وسيلة لتفاعل مع النظام ويتم استخدامها من قبل مدراء الشبكة والمستخدمين لعرض معلومات النظام او تعديل بعض العمليات المرتبطة

	Network Device CLI		بالنظام والقيام ببعض الوظائف الخاصة بمدراء الشبكة. وتحتوي CLIs على مستويات مختلفة من الصلاحيات والاذونات باختلاف الاوامر المنفذة.
T1609	ادارة والتحكم بالمستودعات / Container Administration Command		قد يستخدم المهاجمون خدمة ادارة المستودعات لتنفيذ اوامر ضارة بها. والتي قد تسمح خدمة ادارة المستودعات بـ Docker deamon او خادم Kubernetes API او Kubelet بإدارة المستودعات عن بعد في البيئة المستهدفة.
T1610	تثبيت المستودعات / Deploy Container		قد يقوم المهاجمون بتثبيت المستودعات داخل المنظمة المستهدفة بهدف تنفيذ بعض الاوامر الضارة او لتفادي الاكتشاف. وفي بعض الاحيان يقوم المهاجم بتثبيت أحد المستودعات بهدف تنفيذ بعض التعليمات البرمجية المرتبطة ببعض العمليات الضارة مثل تنزيل او تفعيل البرمجية الضارة. وقد يقوم المهاجمون بتثبيت مستودع جديد من غير اعدادات او قواعد او صلاحيات وذلك لتفادي بعض اجهزة وانظمة الحماية المتوفرة في المنظمة.
T1203	الاختراق بواسطة المستهدف / for Exploitation Client Execution		قد يستغل المهاجمون نقاط الضعف في البرمجيات الخاصة بالمستخدمين من اجل تنفيذ تعليمات برمجية ضارة. حيث ان الثغرات والتي تتواجد في تطبيقات المستخدمين لمختلف الاسباب ومنها عدم كتابة الاكواد البرمجية بشكل امن والتي من الممكن استغلالها من قبل المهاجمين. وغالباً يقوم المهاجمون باستهداف برمجيات المستخدمين وذلك من اجل تنفيذ تعليمات برمجية ضارة عن بعد والتي تمكنه من الوصول والسيطرة على النظام المصاب.
T1559	Inter-Process Communication		قد يقوم المهاجمون باستخدام آليات الاتصال بين العمليات IPC من اجل تنفيذ تعليمات برمجية ضارة على النظام بشكل مباشر او عن بعد. حيث يتم عادة استخدام IPC لأغراض مشاركة المعلومات او التواصل مع بعضها البعض من خلال تنفيذ بعض اوامر المزامنة. ويتم استخدام IPC ايضاً بشكل شائع لتجنب ما يسمى (deadlocks).
T1559	Component Object Model	.001	قد يقوم المهاجمون باستخدام COM او Component Object Model Windows وذلك لتنفيذ تعليمات برمجية محلياً على النظام المصاب. وCOM هو مكون اتصال بين العمليات IPC. وكذلك يتيح التفاعل مع واجهة التطبيقات الويندوز API. او تمكين العمليات البرمجية القابلة للتنفيذ. حيث من خلال COM تستطيع الكائنات التي لدى العميل الاتصال بالكائنات الخاصة بالخوادم والتي عادة تكون عبارة عن ملفات تنفيذية او ملفات DLL.
T1559	تبادل المحتوى الديناميكي / Dynamic Data Exchange	.002	قد يقوم المهاجمون باستخدام Windows Dynamic Data Exchange (DDE) لتنفيذ تعليمات واوامر عشوائية. وDEE هو بروتوكول من العميل للخدام للاتصال للمرة واحدة او من خلال استخدام IPC.بمجرد استخدام DEE يمكن للتطبيقات من تبادل العمليات بشكل متسلسل. وتنقسم التنبيهات الى اشعارات عند تغير البيانات وعناصرها وتسمى (Warm). واشعارات عن تكرار او تغير عناصر البيانات وتسمى (Hot). او من خلال طلبات تنفيذ الأوامر
T1106	Native API		قد يقوم المهاجمون من التواصل واستخدام واجهة برمجة التطبيقات (native APIs) لتنفيذ تعليمات برمجية ضارة. حيث تسمح API من الاتصال والتحكم في بعض الخصائص بالأنظمة والخدمات والتي قد تصل الى مستوى التعديل على مستوى النواة والأجهزة والبرمجيات والتطبيقات والذاكرة العشوائية. ويتم استغلال (native APIs) عادة عند بدء الإقلاع او عند تنفيذ الاعمال المجدولة والروتينية.
T1053	جدولة المهام والاعمال Scheduled / Task/Job		قد يقوم المهاجمين من استخدام جدولة المهام لتسهيل عمليات الاختراق (الاولي او الإصرار والتخفي داخل الشبكة). حيث توجد عمليات جدولة الاعمال والمهام في أكثر أنظمة التشغيل لأغراض تسهيل الاعمال بتنفيذ بعض التعليمات البرمجية او النصية بتاريخ ووقت محددين. ويمكن كذلك جدولة الاعمال للأنظمة عن بعد بشرط استيفاء عمليات التحقق على سبيل المثال (RPC و الوصول للملفات او الطابعات في بيئة الويندوز). عادة ما تتطلب جدولة الاعمال في بعض الأنظمة التي تعمل عن بعد امتيازات او صلاحيات إدارية على النظام المستهدف.

T1053	.001	بيئة لينكس / At (Linux)	قد يستخدم المهاجمون جدولة المهام والاعمال لتنفيذ إجراءات ضارة على النظام بهدف الوصول الأولى او تنفيذ تعليمات برمجية ضارة. يتيح امر (at) لمدراء النظام من جدولة المهام.
T1053	.002	بيئة ويندوز / At (Windows)	قد يستخدم المهاجمون جدولة المهام والاعمال لتنفيذ إجراءات ضارة على النظام بهدف الوصول الأولى او تنفيذ تعليمات برمجية ضارة. يتيح امر (at.exe) بشرط إضافة المستخدم كعضو في مجموعة Administrates .
T1053	.003	Cron	قد يستخدم المهاجمون الأداة المساعدة لجدولة المهام والاعمال (Corn) لتنفيذ إجراءات ضارة على النظام بهدف الوصول الأولى او تنفيذ تعليمات برمجية ضارة. أداة Corn عبارة عن برنامج جدولة وظائف واعمال بناء على الأوقات المطلوبة من قبل المستخدم او المهاجم. يحتوي ملف (Corntab) على بيانات الاعمال التي تم جدولتها والمراد تشغيلها والاوقات المحددة لتنفيذ. يتم عادة حفظ ملف (Corntab) في مسارات النظام المعتادة.
T1053	.004	تشغيل /Launchd	قد يستخدم المهاجمون برنامج (Launchd) بشكل ضار بهدف اجراء جدولة للأعمال بهدف الوصول الاولي او الإصرار والبقاء داخل الشبكة. برمجية (Launchd) هي برمجية تأتي مع أنظمة macOS وهو مسؤول عن تحميل وصيانة الخدمات التي تعمل على أنظمة التشغيل وبشكل خفي. حيث يتم الاستفادة من البرنامج (Launchd) من تحميل التعليمات لكل برنامج عند طلبة من قائمة مخصصة تسمى (plist). وتستطيع إيجادها في المسار التالي (/System/Library/LaunchDaemons) و (/Library/LaunchDaemons) حيث تحتوي هذه القائمة على الملفات التنفيذية التي سيتم تشغيلها على النظام
T1053	.005	جدولة الاعمال / Scheduled Task	قد يستخدم المهاجمون أداة (Scheduler Windows Task) بشكل ضار بهدف اجراء جدولة للأعمال بهدف الوصول الاولي او الإصرار والبقاء داخل الشبكة. هناك عدة طرق للوصول لبرنامج جدولة المهام (Scheduler Windows Task) ويمكن تشغيل بشكل مباشر من خلال سطر الأوامر. او يمكن فتحة بشكل مباشر من لوحة التحكم كبرنامج له واجهة رسومية بشرط ان يكون لديك صلاحيات مدير لنظام. وقد يستخدم المهاجمين طرق أخرى للوصول للبرنامج من خلال استدعاه باستخدام (Windows netapi32 او تضمينه من خلال .NET) لأنشاء جدولة للأعمال والمهام.
T1053	.006	Systemd Timers	قد يستخدم المهاجمون أداة (systemd) بشكل ضار بهدف اجراء جدولة للأعمال بهدف الوصول الاولي او الإصرار والبقاء داخل الشبكة. أداة (systemd) هي ملفات تستطيع التحكم بشكل مؤقت ببعض الخدمات ويمكن من خلالها القيام بجدولة الاعمال من خلال وضع (حدث) على (التقويم) وهو مشابه لأداة (Corn) في بيئة لينكس.
T1053	.007	وظائف تنظيم المستودعات / Container Orchestration Job	قد يقوم المهاجمون باستخدام وظائف جدولة الاعمال والمهام التي توفرها أدوات التنسيق والدعم للمستودعات مثل (Kubernetes) لجدولة او نشر مستودعات مُهيئة لتنفيذ تعليمات برمجية ضارة. وتقوم هذه المهام بتشغيل المستودعات بوقت وتاريخ محددين مماثلة لما في (Corn) يمكن ايضاً أتمتة عمليات الجدولة وخلافة للمحافظة واستمرارية صلاحية الوصول.
T1129		Shared Modules	قد يقوم المهاجمون باستخدام (modules shared) لتنفيذ تعليمات برمجية ضارة. حيث يمكن لـ(Windows module loader) من تحميل ملفات DLL من مسارات عشوائية على النظام او من خلال Naming Convention (UNC). وحيث ان هذه الوظيفة من وظائف NTDLL.dll التي هي جزء من API Windows Native والتي يمكن استدعاؤها من وظائف مثل انشاء عمليات او تحميل العمليات.. وما الى ذلك الى Win32 API.
T1072		ادوات نشر وتثبيت البرمجيات / Software Deployment Tools	قد يقوم المهاجمون بالوصول والتحكم الى مجموعة من البرامج الخاصة بالطرف الثالث المثبتة على الجهة المستهدفة. مثل أنظمة الإدارة والمراقبة وتثبيت الأنظمة وذلك لأهداف ضارة ومن أشهرها التنقل داخل الشبكة. وقد تكون مثل هذه الأدوات مستخدمه لأغراض إدارة الشبكة وليست ضارة مثل (e.g., SCCM, HBSS, Altiris, etc.)

T1569		خدمات النظام / System Services	قد يقوم المهاجمون باستغلال الخدمات الخاصة بالنظام لتنفيذ تعليمات برمجية ضارة. حيث يستطيع المهاجم من تنفيذ تعليمات برمجية ضارة من خلال التفاعل مع الخدمات الخاصة بالنظام. حيث يوجد العديد من الخدمات يتم تنفيذها مع عمليات بدا التشغيل. والتي من الممكن استغلالها لتمكين المهاجم من البقاء داخل الشبكة اكثر قدر ممكن من الوقت.
T1569	.001	Launchctl	قد يقوم المهاجمون باستغلال (launchctl) الخاصة بنظام macOS لتنفيذ تعليمات برمجية ضارة. حيث يتحكم Launchctl ويتعامل مع خدمات وأدوات أخرى مثل Launch Agents و Launch Daemons. ولكن يمكنك تنفيذ تعليمات برمجية أخرى كذلك. ويدعم كذلك Launchctl تلقى الأوامر بشكل تفاعلي او إعادة إخراجها بطرق أخرى حسب المدخلات.
T1569	.002	تشغيل الخدمات / Service Execution	قد يقوم المهاجمون بالتحكم بإدارة التحكم في خدمات الويندوز (Windows service control manager) لتنفيذ تعليمات برمجية ضارة. ان (services.exe) هي واجهة تفاعلية لإدارة الخدمات ومعالجتها. ويمكن للمستخدمين من الوصول الى مدير التحكم في الخدمة من خلال واجهة المستخدم الرسومية وكذلك بعض أدوات النظام مثل .NET,.ec.exe.
T1204		التفعيل بواسطة المستخدم / User Execution	قد يقوم المهاجمون بالاعتماد على بعض ردود الأفعال الخاصة بالمستخدمين وذلك لتفعيل الأوامر والتعليمات البرمجية الضارة. قد يقع المستخدم ضحية للهندسة الاجتماعية وذلك بهدف ان يقوم بتفعيل وتنفيذ تعليمات برمجية قد تضر بالنظام الخاص به. على سبيل المثال (فتح ملف او رابط او مستند ضار) والتي قد تأتي من عمليات تصيد.
T1204	.001	رابط ضار / Malicious Link	قد يعتمد المهاجمون على قيام المستخدمين بالنقر على الرابط الضار من اجل تنفيذ او تحميل تعليمات برمجية ضارة وتنفيذها. وعادة تأتي مثل هذه الأساليب من خلال استخدام الهندسة الاجتماعية لأغراء المستخدمين على الضغط على الروابط. ويسمى بالتصيد من خلال الروابط (Link Spearphishing). وقد يؤدي الضغط على الروابط في بعض الأحيان الى استغلال ثغرات امنية في تطبيق او متصفح، وقد يقوم المهاجم بتوجيه المستخدمين لتنزيل ملفات ضارة ومن ثم تفعيلها وتنفيذها.
T1204	.002	ملف ضار / Malicious File	قد يعتمد المهاجمون على قيام المستخدمين بفتح ملفات ضارة من اجل تنفيذ تعليمات برمجية ضارة. وعادة تأتي مثل هذه الأساليب من خلال استخدام الهندسة الاجتماعية لأغراء المستخدمين على فتح الملفات والتي في العادة تودي الى تفعيل اكواد ضارة. ويسمى بالتصيد من خلال الروابط (Spearphishing). وقد يستخدم المهاجمون أنواع وصيغ متعددة من الملفات مثل .doc, . ,pdf, .xls, .rtf, .scr, .exe, .cpl ،.lnk, .pif,..
T1204	.003	نسخ صورية ضارة / Malicious File	قد يعتمد المهاجمون على المستخدمين ففي تفعيل وتنفيذ بعض النسخ الضارة او ان تكون بعض هذه المستودعات مدمج بها برمجيات ضارة. ومن امثلة النسخ الصورية التي من الممكن استغلالها Amazon Web Services (,Amazon Machine Images (AMIs) (AWS Google Cloud Platform (GCP). حيث يقوم المهاجم بعد عملية حقن احد المستودعات بخداع المستخدم وتثبيت هذه المستودعات داخل البيئة الخاصة به وبالتالي يستطيع المهاجم من تخطي وسائل الحماية. لذلك لابد من الواعي اللازم للمستخدمين بعدم تحميل النسخ الصورية الغير معروفة. ومن امثلة النسخ المشبوهة نسخ تأتي ببرمجيات تعدين.
T1047		ادارة الاجهزة الخاصة بالويندوز / Windows Management Instrumentation	قد يقوم المهاجمون باستخدام Windows Management Instrumentation (WMI) للتنفيذ تعليمات ضارة. و WMI هي احدى مميزات إدارة انظم ويندوز التي تستطيع من خلالها الإدارة والوصول للأجهزة المحلية والبعيدة. تعتمد خدمة WMI للوصول للأنظمة المتصلة بها محلياً وعن بعد بروتوكول SMB وخدمة PRCS للوصول عن بعد. حيث تعمل PRCS على منفذ 135.

البقاء قدر المستطاع داخل النظام المخترق/ Persistence

البقاء داخل الشبكة المخترقة هي تقنية او أسلوب يستخدمه المهاجمين بهدف البقاء داخل النظام حتى ولو تم إعادة تشغيل الأنظمة او تغير بيانات الاعتماد او أي من الانقطاعات التي قد تحدث وتفقد المهاجم صلاحيات الوصول للنظام المخترق. وقد تتغير الأساليب المستخدمة باستمرار. ان الأساليب المستخدمة في عملية البقاء داخل الشبكة أكثر قدر ممكن قد تكون على شكل صلاحيات وصول او بعض الإجراءات او تغير بعض الاعدادات والتي تمكن وتسمح للمهاجم من الاستمرار بصلاحياته على النظام المخترق. مثل استبدال بعض التعليمات البرمجية الغير ضارة بتعليمات برمجية ضارة او إضافة بعض التعليمات البرمجية الضارة عن بدء تشغيل النظام.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1098		التلاعب بالحسابات / Account Manipulation	قد يقوم المهاجم بالتلاعب بالحسابات للحفاظ على صلاحيات الوصول للأنظمة المستهدفة. قد يكون التلاعب بالحسابات أي اجراء يقوم به المهاجم من شانه الحفاظ على الحسابات المخترقة في النظام المستهدف. مثل تعديل بيانات كلمات المرور واذونات المستخدمين. او التلاعب بالسياسات الموضوعة في الحفاظ على الحسابات وقد يقوم المهاجم بتغير كلمات المرور بشكل متكرر لكي يقوم بتفادي (سياسة تغير كلمات المرور كل فترة من الزمن). ولكي تتم عملية تغير او التلاعب بالحسابات يجب ان تتوفر لدى المهاجم الصلاحيات المناسبة والأذونات لكي يقوم بمثل هذه العمليات.
T1098	.001	بيانات الاعتماد السحابية / Cloud Additional Credentials	قد يقوم المهاجم بإضافة بعض الحسابات الخاصة به لتحكم بالخدمات السحابية وذلك بهدف البقاء داخل المنظمة المستهدفة.
T1098	.002	تفويض الصلاحيات على مستوى البريد / Exchange Email Delegate Permissions	قد يقوم المهاجم بالحصول على مستوى محدد من الصلاحيات الإضافية مثل الحصول على صلاحيات (قراءة، صلاحيات كامله) على مستوى البريد الالكتروني وقد يقوم المهاجم بإضافة بعض الحسابات الخاصة به للبقاء داخل البريد المخترق. وقد يقوم المهاجم باستخدام بعض الإضافات والصلاحيات مثل (Add-MailboxPermission PowerShell cmdle) وهي متوفرة في خوادم البريد الالكتروني المستضافه داخلياً. او يقوم باستخدام صلاحيات واذونات التحكم في حال استخدام الخدمات السحابية للبريد الالكتروني مثل Office 365.
T1098	.003	اضافة صلاحيات مدير النظام لخدمات 356 اوفيس / Add Office 365 Global Administrator Role	قد يقوم المهاجمين باستغلال إضافة صلاحيات (Global Administrator) وذلك بهدف البقاء داخل خدمات Office 365 أطول فترة ممكنة. باستخدام الأذونات الكافية، يمكن للحساب المخترق الحصول على صلاحيات الوصول الى الاعدادات والبيانات بشكل غير محدود. بما في ذلك إمكانية تغير كلمات المرور للمسؤولين الاخرين. باستخدام دور المسؤول العام.
T1098	.004	مفاتيح التصاريح لخدمات SSH/ SSH Authorized Keys	قد يقوم المهاجمين بتعديل(authorized_keys SSH) للحفاظ علي صلاحيات الوصول للبيئة المستهدفة أطول فترة ممكنة. حيث ان أنظمة لينكس وماك اوس يستخدمونها بشكل كبير (key-based authentication) وذلك لتأمين عمليات جلسات SSH عن بعد وادارتها. يقوم ملف Author_keys في SSH بتحديد المفاتيح التي يمكن استخدامها لعملية تسجيل الدخول الى حساب المستخدم الذي تم تكوين هذه الملف من اجله، ويوجد هذه الملف عادة في الدليل الرئيسي للمستخدمين في (user-><home>/.ssh/authorized_keys). ويمكن للمستخدمين من اجراء تعديلات على ملف تكوين SSH للنظام من PubkeyAuthentication و RSAAuthentication الى (Yes) لضمان تمكين مصادقة المفتاح العام و RSA. ويوجد ملف التكوين الخاص بـ(SSH) في (/etc/ssh/sshd_config)
T1197		وظائف BITS Jobs	قد يقوم المهاجمين باستخدام وظائف (BITS) لتنفيذ تعليمات برمجية ضارة او استخدامها لمسح الاثار التي يخلفها المهاجم. ان خدمة (Windows Background Intelligent Transfer Service (BITS) هي عبارة عن آلية لنقل الملفات بشكل غير متزامنة وذات نطاق ترددي منخفض ويتم استعراضها من خلال (COM). ويتم استخدام (BITS) بشكل شائع من قبل المراسلين (messengers) او أي تطبيق يفضل العمل في الخلفية ويستخدم (idle bandwidth) من غير مقاطع أي بروتوكول أخرى يعمل بالشبكة. ويتم تنفيذ مهام نقل الملفات من خلال وظائف (BITS)، والتي تحتوي على قائمة انتظار لملف واحد او اكثر من ملف.

T1547		تسجيل الدخول التلقائي / Boot or Logon Autostart Execution	قد يقوم المهاجم باستخدام اعدادات النظام تنفيذ تعليمات برمجية ضارة من خلال اعدادات لجعل التنفيذ يتم بشكل تلقائي من خلال عملية الإقلاع او تسجيل الدخول وذلك بهدف الاستمرار والبقاء داخل الشبكة أطول فترة ممكنة. قد يحتوي نظام التشغيل على آليات لتشغيل البرامج تلقائياً عند الإقلاع او تسجيل الدخول الى الحساب. وقد تتضمن هذه الاليات تنفيذ البرامج تلقائياً التي يتم وضعها في قائمة مخصصة على سبيل أمثال وضع بعض (Registry Windows) وقد يقوم المهاجم بتحقيق نفس هذه العملية والاهداف عند التعديل على نوات النظام.
T1547	.001	مفاتيح التسجيل والتشغيل التلقائي/ Run Registry Keys / Startup Folder	قد يقوم المهاجم باستخدام مجلد بدء التشغيل (Startup) لإضافة البرمجيات او المفاتيح(run keys) الضارة الخاصة به. وستودي ادخال (run keys) في (Registry) او (Startup) الى جعل البرنامج يعمل عند قيام المستخدم بعملية تسجيل الدخول. سيتم تنفيذ هذه البرامج في حساب المستخدم الذي تم تفعيلها به والتي قد تحتاج الى أذونات خاصة مرتبطة بالحساب المستخدم.
T1547	.002	تصاريح الحزم / Authentication Package	قد يقوم المهاجمين باستخدام تصاريح الحزم لتنفيذ وتشغيل (DLLs) عند اقلاع النظام. حيث يتم تحميل ملفات DLL لحزم المصادقة لنظام ويندوز بواسطة (Local Security Authority (LSA)) عند بدء عملية التشغيل للنظام. حيث توفر عمليات الدعم لتسجيل الدخول المتعددة وكذلك إضافة بروتوكولات الأمان لنظام التشغيل.
T1547	.003	Time Providers	قد يقوم المهاجمين من استغلال (providers time) لتنفيذ او تشغيل (DLLs) عند اقلاع النظام. ان (W32Time) يتيح مزامنة الوقت عبر النطاقات. ويقوم (W32Time) بمسؤولية استرداد الوقت (time stamps) من العتاد والشبكة وإخراج القيام الى المستخدمين في الشبكة.
T1547	.004	Winlogon Helper DLL	قد يقوم المهاجمين باستخدام (Winlogon) للتنفيذ تعليمات ضارة من خلال تشغيل (DLLs) او برامج تنفيذية عند تسجيل الدخول. ان (Winlogon) هي احد مكونات نظام ويندوز وهي مسؤولة عن الإجراءات عند تسجيل الدخول او الخروج بالإضافة الى خدمة (SAS) والتي تكون عند الضغط على (Ctrl-Alt-Delete) ويتم تسجيل المدخلات في (\HKLM\Software[\Wow6432Node\]\Microsoft\Windows NT\CurrentVersion\Winlogon) و (\HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon) والتي تستخدم لإدارة البرامج والوظائف المساعدة الإضافية التي تدعم عملية(Winlogon)
T1547	.005	Security Support Provider	قد يقوم المهاجمين باستخدام (support providers (SSPs security)) للتنفيذ تعليمات ضارة من خلال تشغيل (DLLs) او برامج تنفيذية عند اقلاع النظام. يتم تحميل (security support providers (SSPs)) في (Local Security Authority (LSA)) كعملية عند بدء النظام. بعد عملية التحميل LSA,SSPJ كDLLs يقوم بتشفير الأرقام السرية من صيغة نصية الى صيغة مشفرة والتي تكون مخزنة في نظام ويندوز، مثل أي كلمة مرور يتم استخدامها عند عمليات تسجيل الدول او استخدام PIN كذلك.
T1547	.006	Kernel Modules and Extensions	قد يقوم المهاجمين بتعديل النواة وذلك لتنفيذ تعليمات تلقائية ضارة بالنظام عند الإقلاع. ان وحدات التحميل (LKMs) داخل النواه هي أجزاء من تعليمات برمجية يمكن الكتابة عليها او محيها في النواه عند الطلب. وهي تعمل على زيادة قدرات النواه دون الحاجة الى إعادة تشغيل النظام. على سبيل المثال(التعاريف الخاصة بالأجهزة) والتي تسمح للنواة بالوصول الى العتاد والتعاريف المتصلة بالنظام.
T1547	.007	Re-opened Applications	قد يقوم المهاجمين بتعديل ملفات (plist) للقيام بتشغيل برمجيات ضارة بشكل تلقائي عندما يقوم المستخدم بتسجيل الدخول او بدء تشغيل النظام في (Mac OS X 10.7 (Lion)). يستطيع المستخدمون تحديد برامج او تطبيقات للإعادة فتحها بشكل تلقائي عندما يقوم المستخدم بتسجيل الدخول للأجهزة الخاصة بهم بعد إعادة التشغيل. بدل ان يتم ذلك عبر فتح البرامج كل برنامج على حدة. وهناك قائمة للمفلات التي تعمل عند بدء التشغيل (plist). وتستطيع ايجادها في (Library/Preferences/com.apple.loginwindow.plist/~) و (.Library/Preferences/ByHost/com.apple.loginwindow.* .plist/~)

T1547	.008	LSASS Driver	قد يقوم المهاجمين بإضافة او تعديل (drivers LSASS) وذلك لضمان البقاء داخل الشبكة أطول فترة ممكنة في النظام المخترق. ان النظام الفرعي في الويندوز (Windows security subsystem) هو عبادة عن مجموع من المكونات تدير وتنفيذ سياسات الأمان على النظام او النطاق. ان (LSA) هو المكون الرئيسي والمسؤول عن سياسة الأمان المحلية و التحقق من صلاحيات المستخدم. ان (LSA) تحتوى على العديد من المكتبات الديناميكية (DLL) وهي كالعادة مرتبطة بوظائف امان أخرى. والتي تعمل جميعها في عملية LAS او (lsass.exe)
T1547	.009	Shortcut Modification	قد يقوم المهاجم بإضافة او تعديل الاختصارات لتشغيل او تنفيذ تعليمات برمجية ضارة عند الإقلاع او عند عملية تسجيل الدخول للنظام. ان الاختصارات أو الرموز هي طرق للإشارة إلى الملفات أو البرامج الأخرى التي سيتم فتحها أو تنفيذها عند النقر فوق الاختصار أو تنفيذه عند بدء تشغيل النظام.
T1547	.010	مراقبة الشاشات / Port Monitors	قد يقوم المهاجمين باستغلال (port monitors) لتشغيل ملفات ضارة من خلال ملفات (DLL) والتي تعمل عند اقلاع النظام وذلك للبقاء داخل الشبكة أطول فترة ممكنه. ان (port monitors) تستطيع استخدامه من خلال الاتصال بـ (AddMonitor API) والتي تسمح بتحميل ملفات DLL عند بدء التشغيل. تستطيع اجادة ملفات DLL في " C:\Windows\System32" وسيتم تحميله بواسطة خدمة التخزين الموقت للطباعة(spoolsv.exe) عند اقلاع النظام. ان (spoolsv.exe) هي عمليات تعمل كذلك تحت (SYSTEM) والتي يقصد بها صلاحيات النظام. ويمكن تحميل ملفات DLL اذا كانت هناك الاذونات المناسبة للكتابة في المسار المخصص في (HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors.)
T1547	.011	Plist Modification	قد يقوم المهاجمين باستخدام (plist) لتشغيل البرامج اثناء اقلاع النظام او عند عمليات تسجيل الدخول. وتحتوي قائمة (plist) على ملفات يتم استخدامها في نظام (macOS و OS X)وهي تحتوي على الإعدادات الخاصة بالتطبيقات والخدمات. الملف تمت كتابته بترميز (UTF-8) وتستطيع استعراضه من خلال قارئ ملفات XML. وتأتى الإعدادات ما بين (<>). وهي توضح التفاصيل متى يجب البرامج. ومسار الملفات التنفيذية. والاذونات المطلوبة لتشغيلها.. وغيرها الكثير. تتواجد (plists) في مواقع معينة اعتمادًا على العرض منها مثل (Library/Preferences/) والتي يتم استخدامها عند رفع الصلاحيات. و (~ /Library/Preferences) عند استخدام تلك الصلاحيات.
T1547	.012	طباعة العمليات / Print Processors	قد يقوم المهاجمين باستخدام (processors print) لتشغيل مكتبات DLL ضارة اثناء اقلاع النظام. وذلك لأغراض ضارة مثل البقاء داخل النظام المخترقة او تصعيد الصلاحيات. ان (print processors) هي مكتبات DLL التي يتم تحميلها بواسطة (print spooler service, spoolsv.exe) اثناء عمليات الإقلاع.
T1547	.013	XDG Autostart Entries	يمكن للمهاجمين من اجراء تعديلات على (autostart entries XDG) لتنفيذ وتشغيل البرمجيات او الأوامر اثناء اقلاع النظام. ان بيئة لينكس و المتوافقة مع (XDG) والتي تعمل مع .(XDG autostart entries) ستسمح للتطبيقات بالعمل بشكل تلقائي اثناء بدء التشغيل لبيئة سطح المكتب او عند تسجيل الدخول بشكل افتراضي. ويتم تخزين الادخالات في (XDG autostart entries) في (etc/xdg/autostart/) او (~ /.config/) او في الامتدادات التي تحمل صيغة (.desktop).
T1547	.014	Active Setup	قد يقوم المهاجمين بإضافة مفاتيح التسجيل (Registry key) الى الإعدادات النشطة (Active Setup) بهدف البقاء داخل الشبكة اطول فترة ممكنة. ان (Active Setup) هو أحد آليات نظام ويندوز التي يتم استخدامها لتنفيذ وتشغيل البرمجيات عندما يقوم المستخدم بتسجيل الدخول. حيث يتم تنفيذ القيمة المخزنة في (Registry key) بعد عملية تسجيل الدخول من المستخدم الى الكمبيوتر. سيتم تنفيذ هذه الأوامر والقيم في حساب وصلاحيات المستخدم ولها مستوى وأذونات مرتبطة بالحساب المستخدم.
T1037		الاقلاع او الدخول التلقائي / Boot or Logon Initialization Scripts	قد يقوم المهاجمين باستخدام بعض السكربتات لتنفيذ تعليمات برمجية ضارة بشكل تلقائي عن اقلاع النظام بهدف البقاء داخل النظام المخترق أطول فترة ممكنة. حيث يمكن استخدام السكربت تنفيذ بعض المهام الإدارية في الأنظمة. والتي قد ينطوي عليها

			تنفيذ وتشغيل البرمجيات او ارسال المعلومات الى خادم داخلي. يمكن ان تختلف السكربت من نظام الى اخر وطرق تطبيقها هل سيكون محلياً او عن بعد.
T1037	.001	سكربت الدخول بيئة ويندوز / Logon Script (Windows)	قد يقوم المهاجمين باستخدام سكربت تسجيل الدخول لأنظمة ويندوز والتي يتم تنفيذها بشكل تلقائي عند بداية عملية تسجيل الدخول. والهدف منها هو البقاء داخل النظام المخترق أطول فترة ممكنة. يسمح نظام ويندوز بتشغيل سكربتات تسجيل الدخول على مستوى المستخدمين او المجموعات. ويتم ذلك عن طريق إضافة المسار المطلوب الى(HKCU\Environment\UserInitMprLogonScript) في (Registry key).
T1037	.002	سكربت الدخول بيئة ماك / Logon Script (Mac)	قد يقوم المهاجمين باستخدام سكربت تسجيل الدخول لأنظمة ماك اوس والتي يتم تنفيذها بشكل تلقائي عند بداية عملية تسجيل الدخول. والهدف منها هو البقاء داخل النظام المخترق أطول فترة ممكنة. يسمح نظام ماك بتشغيل وتنفيذ سكربتات او ما يسمى (known as login hooks) تسجيل الدخول كلما قام المستخدم بالدخول للنظام. حيث يقوم (known as login hooks) بتنفيذ السكربت عند تسجيل الدخول وهو على عكس (Startup Items) يقوم (login hooks) بتنفيذ البرمجيات عند استخدام صلاحيات مدير النظام(root).
T1037	.003	سكربت الدخول لشبكات / Network Logon Script	قد يقوم المهاجمين باستخدام سكربت الشبكة والتي يتم تنفيذها بشكل تلقائي عند بداية عملية الدخول. والهدف منها هو البقاء داخل النظام المخترق أطول فترة ممكنة. يمكن استخدام سكربتات التي تعمل على مستوى بدء التشغيل في الشبكة من خلال (Active Directory او Group Policy Objects). تحتاج هذه السكربتات الى صلاحيات وأذونات محددة لكي يتم تعينها او استخدامها. بحسب اختلاف الأنظمة قد يستطيع المهاجم تنفيذ هذه السكربتات على نظام محدد او عدد من الأنظمة داخل الشبكة المستهدفة.
T1037	.004	Rc Scripts	قد يقوم المهاجمين بتعديل سكربت (RC) والذي يتم تنفيذه خلال الإقلاع لنظام (Unix). ان هذه الملف يسمح لمدراء النظام بربط وبدء الخدمات المخصصة الى قائمة بدء التشغيل النظام. وعادة تتطلب (RC) امتيازات مدير النظام لإجراء التعديلات (root).
T1037	.005	ادوات بدء التشغيل / Startup Items	قد يقوم المهاجمون باستغلال (Startup Items) لتنفيذ تعليمات برمجية ضارة عند اقلاع النظام بهدف البقاء في النظام أطول فترة ممكنة. ان (Startup Items) تعمل عادة في المرحلة الأخيرة من الإقلاع. وتحتوي على برامجه او سكربتات قابلة للتنفيذ او التشغيل بجانب الاعدادات التي يستخدمها النظام لتحديد الترتيب المتوقع لتشغيل وتنفيذ العناصر المتوفرة في (Items Startup).
T1176		اضافات المتصفح / Browser Extensions	قد يقوم المهاجمون باستغلال المتصفحات لتنفيذ تعليمات برمجية ضارة بهدف البقاء في النظام أطول فترة ممكنة. ان الإضافات المتوفرة في المتصفحات هي برمجيات صغيره تعمل مع المتصفح. وتستطيع تثبيتها مباشرة من خلال المتصفح او من خلال المتجر المخصص ولديها من الصلاحيات ما لدى المتصفح.
T1554		اختراق برمجيات المستخدم Client Compromise / Software Binary	قد يقوم المهاجمين بتعديل والتلاعب ببعض الاكواد البرمجية الخاصة بالبرمجيات الموجهة للمستخدمين بهدف البقاء في النظام أطول فترة ممكنة. ان البرمجيات الخاصة بالمستخدمين تمكنهم من الاستفادة من الخدمات. ومن اشهرها SSH للمستخدمين و FTP و برامج البريد الالكتروني و المتصفحات.
T1136		انشاء حساب / Create Account	قد يقوم المهاجمين بإنشاء حسابات بهدف البقاء في النظام أطول فترة ممكنة. حيث يقوم المهاجم بإنشاء حسابات مع صلاحيات كافية. او قد يقوم المهاجم بإنشاء حساب اخر لا يتطلب بيانات دخول او تحقق لتسهيل عمليات الدخول والوصول عن بعد وذلك لتحميل الأدوات الضارة وتثبيتها على النظام.
T1136	.001	حساب محلي / Local Account	قد يقوم المهاجمين بإنشاء حسابات محلية على النظام المستهدف بهدف البقاء في النظام أطول فترة ممكنة. ان الحسابات المحلية يتم انشاءها من قبل المنظمات لعدة أغراض وعلى سبيل المثال (الدعم، وحسابات الخدمات) وتتمتع هذه الحسابات بصلاحيات عالية وتستطيع انشاء حساب محلي على النظام من خلال الامر التالي(net user /add).

T1136	.002	حساب مدير نظام / Domain Account	قد يقوم المهاجم بإنشاء حساب مدير النظام (Domain account) بهدف البقاء في النظام أطول فترة ممكنة. وحسابات مدراء النظام عادة يتم ادارتها بواسطة (Active Directory Domain Services) حيث تم انشاءها وتحديد الصلاحيات والاذونات للحسابات على الأنظمة والخدمات. وقد تشتمل حسابات مدراء النظام على حسابات الخدمات وكذلك الحسابات الإدارية الأقل صلاحية منها. ومع توفر الصلاحيات المناسبة تستطيع انشاء حساب مدير نظام بواسطة الامر التالي (net user /add /domain).
T1136	.003	حساب الخدمات السحابية / Cloud Account	قد يقوم المهاجم بإنشاء حساب على الخدمات السحابية بهدف البقاء في النظام أطول فترة ممكنة. مع وجود صلاحية مناسبة قد يقوم المهاجم بإنشاء حساب اخر لاستخدامه في الوصول عن بعد وبشكل مباشر من دون استخدام أي أدوات أخرى على النظام.
T1543		انشاء او تعديل العمليات على الانظمة / Create or Modify System Process	قد يقوم المهاجمين بإنشاء او تعديل العمليات على مستوى النظام بغرض تنفيذ تعليمات برمجية ضارة بهدف البقاء في النظام أطول فترة ممكنة. فعندما يقوم النظام بالإقلاع ستعمل العمليات بشكل مباشر في الخلفية. سواء كان النظام ويندوز او لينكس. حيث ان هذه العمليات يتم تصنيفها كخدمات. اما في نظام ماك اوس يتم تشغيل العمليات بواسطة (Launch Daemon) و (Launch Agent) لإنهاء تهيئة عمليات النظام و البدء بتنفيذ وتحميل عمليات المستخدم.
T1543	.001	تفعيل البرمجية / Launch Agent	قد يقوم المهاجمين بإنشاء او تعديل العمليات على مستوى النظام بغرض تنفيذ تعليمات برمجية ضارة باستخدام (launch agents) وذلك بهدف البقاء في النظام أطول فترة ممكنة. وفقاً لمطوري شركة آبل، عندما يقوم المستخدم بتسجيل الدخول يتم بدء عملية تشغيل العمليات الخاصة بكل مستخدم من خلال (launch-on-demand) والموجودة في (plist) والتي تستطيع الوصول لها من خلال (/System/Library/LaunchAgents, /Library/LaunchAgents/, و $HOME/Library/LaunchAgents) ان (launch agents) لديهم قائمة من الملفات المرتبطة بملفات تنفيذيه يتم تفعيلها عند بدء التشغيل.
T1543	.002	خدمات النظام / Systemd Service	قد يقوم المهاجمين بإنشاء او تعديل العمليات الخاصة بخدمات (systemd)، وذلك بهدف البقاء في النظام أطول فترة ممكنة. ومن المتعارف على ان (systemd) يقوم بإدارة العمليات في الخلفية او الخدمات وموارد النظام الأخرى. ان (systemd) هو النظام التهيئة الافتراضي في (init) في أكثر توزيعات لينكس مثل (Debian 8, Ubuntu 15.04, CentOS 7, RHEL 7, Fedora 15). حيث تم إيجاده لاستبدال الأنظمة القديمة التي تعمل بـ(init) والتي تشتمل على (SysVinit و Upstart). وحيث ان (systemd) يتعامل كذلك مع الأنظمة السابقة والقديمة.
T1543	.003	خدمات الويندوز / Windows Service	قد يقوم المهاجمين بإنشاء او تعديل العمليات الخاصة بخدمات الخاصة بنظام (Windows)، وذلك بهدف البقاء في النظام أطول فترة ممكنة. عندما يقوم الويندوز بعمليات الإقلاع الخاصة بالنظام بعد ذلك يقوم بتشغيل البرمجيات والتطبيقات من خلال استدعاء الخدمات التي تعمل في الخلفية الخاصة بالنظام. ان نظام الخدمات والإعدادات تشتمل على مسارات الملفات للخدمات والاوامر القابلة للتنفيذ. ويتم تخزينها في (Windows Registry). ومن الممكن ان يتم تعديل اعدادات الخدمات من خلال أداة (sc.exe او Reg).
T1543	.004	Launch Daemon	قد يقوم المهاجمين بإنشاء او تعديل العمليات الخاصة بخدمات (launch daemons) وذلك بهدف البقاء في النظام أطول فترة ممكنة. وفقاً لمطوري شركة آبل، عندما يقوم المستخدم بتسجيل الدخول يتم بدء عملية تشغيل العمليات الخاصة بكل مستخدم من خلال (launch-on-demand) والموجودة في (plist) والتي تستطيع الوصول لها من خلال (/System/Library/LaunchAgents/ ,Library/LaunchAgents, و $HOME/Library/LaunchAgents) ان (launch agents) لديهم قائمة من الملفات المرتبطة بملفات تنفيذيه يتم تفعيلها عند بدء التشغيل.
T1546		تنفيذ الاحداث حسب المعطيات / Event Triggered Execution	قد يقوم المهاجم باستغلال بعض الاحداث المعينة بهدف البقاء داخل النظام المخترق أطول فترة ممكن او رفع الصلاحيات. تمتلك أنظمة التشغيل وسائل لمراقبة تلك الاحداث ومتابعتها مثل عمليات تسجيل الدخول او أنشطة أخرى مثل تشغيل تطبيقات او اكواد برمجية

T1546	.001	تعديل الملف الافتراضي / File Change Default Association	قد يقوم المهاجمون باستغلال الاقتران والارتباط بين الملفات للتنفيذ تعليمات برمجية ضارة على سبيل المثال(عند تحديد ملف يتن تحديد البرنامج الافتراضي لتشغيله) ويسمى (البرنامج الافتراضي). يتم تخزين تحديد اقتران الملفات في سجل الويندوز (Windows Registry) ويستطيع المستخدم ومدراء النظام تعديلها او أي برنامج يملك صلاحيات الوصول وتعديل على (Windows Registry) وتستطيع تعديلها من خلال أداة (assoc) بصلاحيات مدير النظام. يستطيع كما ذكرنا التطبيق تعديل التطبيق الافتراضي المرتبط من خلال استدعاء ملف معين ثم إجباره بفتح من خلال برنامج اخر.
T1546	.002	شاشة التوقف/ Screensaver	قد يقوم المهاجمون باستغلال شاشة التوقف (عدم نشاط المستخدم) لتنفيذ تعليمات برمجية ضارة بهدف البقاء داخل النظام المخترق أطول فترة ممكن. وشاشات التوقف هي برمجيات يتم تنفيذها بعد عدم نشاط المستخدم على الكمبيوتر بواسطة وقت تم تحديده مسبقاً من الاعدادات. وتأتي امتداداتها بصيغة (.scr). تستطيع إيجاد ملفات شاشات التوقف في هذا المسار(C:\Windows\System32\, او C:\Windows\sysWOW64\) وفي نظام من نوع (bit-64) يأتي مع حافظات الشاشة او شاشات التوقف المثبتة بشكل تلقائي مع الويندوز.
T1546	.003	Windows Management Instrumentation Event Subscription	قد يقوم المهاجمون بتصعيد الصلاحيات او تشغيل ملفات ضارة باستخدام (Windows Management Instrumentation subscription (WMI) event) وذلك بهدف البقاء داخل الشبكة المخترقة أطول فترة ممكنة او تصعيد الصلاحيات. ويمكن استخدام الاحداث (Event) مع (WMI) بغرض تنفيذ الاكواد عند تحديد وقت حدوث الحدث. على سبيل المثال(تفعيل الاحداث عندما يقوم المستخدم بتسجيل الدخول ..الخ)
T1546	.004	Unix Shell Configuration Modification	قد يقوم المهاجمون باستغلال الأوامر التي تتم بواسطة المستخدم لتنفيذ تعليمات برمجية ضارة بهدف البقاء داخل المنظمة أكبر قدر ممكن. يقوم نظام (Unix Shells) بتنفيذ وجدولة العديد من الاعمال والاعدادات والسكربتات والاحداث. على سبيل المثال (عندما يقوم المستخدم بالتفاعل مع واجهة سطر الأوامر او استخدام (SSH)). فمن خلال المثال السابق يتم التواصل باستخدام (Shell). ويقوم (Shell) حينها بتفعيل السكربتات الخاصة بالنظام والمتواجدة في(/etc) والمجلد الرئيسي الخاص بالمستخدم (~ /) من اجل تهيئة البيئة الخاصة به. وعادة يتم تهيئة البيئة للمستخدمين عند تسجي الدخول للنظام من خلال (/etc/profile). يتم تفعيل هذه السكربتات والاوامر من خلال مستويات من الاذونات تم اعدادها مسبقاً. ان هذه السكربتات ومع وجود الصلاحية والاذونات المناسبة كما ذكرنا يستطيع المستخدم تعديل البيئة الخاصة به
T1546	.005	Trap	قد يقوم المهاجمين بتشغيل التعليمات الضارة بواسطة (interrupt signal). يقوم الامر(Trap) بالسماح بالبرامج و(Shells) بتخصيص الأوامر التي سيتم تفعيلها عند استقبال (interrupt signal)، والاستخدام الشائع لهذه الطريقة هو سكربت يسمح للبرامج بالتفاعل عند حصول (interrupt signal) مثل عند عملية (القص/الصق) في لوحة المفاتيح.
T1546	.006	LC_LOAD_DYLIB Addition	قد يقوم المهاجمين بتشغيل التعليمات الضارة بواسطة (tainted binaries) او (Mach-O binaries) وهي تحتوي على تعليمات برمجية تستخدم لإجراء عمليات معينة عند تحميل (binary). تقوم التعليمات في (LC_LOAD_DYLIB) في (Mach-O binaries) لنظامي (MacOS, OS X) بالتواصل مع المكتبات الديناميكية او ما تسمى بـ(dylibs) التي يتم تحميلها اثناء ووقت تنفيذ تلك العمليات. وتستطيع استخدام هذه (complied binary) بشكل خاص باشتراط وجود الاعدادات والتوافقية الصحيحة. وهناك أدوات كثير تستطيع القيام بهذا العمل من التغيرات.
T1546	.007	Netsh Helper DLL	يقوم المهاجمين بتنفيذ تعليمات برمجية ضارة بهدف البقاء داخل الشبكة أطول فترة ممكنه من خلال تشغيل مكتبات والاعتماد على (Netsh Helper DLLs) لتنفيذها. برمجية (Netsh.exe) او ما تعرف بي(Netshell). هي عبارة عن سطر أوامر تقوم بالتفاعل مع اعدادات الشبكة والأنظمة. وهي تحتوي على وظائف و أدوات لإضافة (helper DLLs) وتستطيع اضافة المزيد من القدرات والوظائف لها. وتستطيع إيجاد المسار الخاص بها في الويندوز (Windows Registry) في (HKLM\SOFTWARE\Microsoft\Netsh).

T1546	.008	Accessibility Features	قد يقوم المهاجم بتنفيذ تعليمات برمجية يتم تفعيلها بواسطة مميزات وامكانيات الوصول المتاحة بواسطة مايكروسوفت او ما يسمى (accessibility features) وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات. ويحتوي نظام ويندوز على مميزان إمكانية الوصول والتي يمكن تشغيلها باستخدام مجموعة من المفاتيح قبل عملية تسجيل الدخول للمستخدم على سبيل المثال(عندما يكون المستخدم على شاشة تسجيل الدخول). قد يقوم المهاجم بتعديل هذه البرمجيات واضافة سطر الأوامر والتي تسمح له بالتحكم والسيطرة من دون الحاجة الى تسجيل الدخول للنظام بشكل فعلي.
T1546	.009	AppCert DLLs	قد يقوم المهاجم بتنفيذ تعليمات برمجية يتم تشغيله بواسطة (AppCert DLLs) والتي يتم تفعيلها من ضمن العمليات (processes). وذلك بهدف رفع الصلاحيات. ان (Dynamic-link libraries (DLLs))هي احد مكونات (AppCertDLLs) والمتواجدة في (HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session\Manager) والتي يتم استدعائها في كل وظائف واجهة برمجة التطبيقات (API) بهدف انشاء العمليات، انشاء العمليات مستخدمين و (,reateProcess CreateProcessWithLoginW, CreateProcessWithTokenW, or WinExec ,CreateProcessAsUser.)
T1546	.010	AppInit DLLs	قد يقوم المهاجمين بتنفيذ تعليمات برمجية ضارة بهدف رفع الصلاحيات وتحدث العملية إثناء تحميل العمليات الخاصة بـ(AppInit DLLs). ان (Dynamic-link libraries (DLLs))هي احد مكونات (AppInit_DLLs) والمتواجدة في (HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows) or HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows) are loaded by user32.dll) والتي يتم استدعائها في كل وظائف والعمليات التي يتم تحميلها الى (user32.dll). وعلى الاغلب ان جميع البرامج تستخدم هذه العمليات حيث ان مكتبة (user32.dll) مكتبة شائعة ومستخدمة بكثرة.
T1546	.011	Application Shimming	قد يقوم المهاجمين بتشغيل تعليمات برمجية ضارة بهدف رفع الصلاحيات وذلك من خلال الاستفادة من ما يسمى بـ(application shims) او (Microsoft Windows Application Compatibility (Application Shim Infrastructure/Framework)). وتم عمله للسماح بالتوافق مع إصدارات ويندوز القديمة وجعل البرمجيات تعمل حتى مع اصدار احدث. على سبيل المثال (ان هذه التقنية تسمح للمطورين بتطبيق الإصلاحات والتطوير دون الحاجة الى إعادة كتابة البرامج من جديد) والمثال السابق في حل تم كتابة برنامج لويندوز XP وجعلة قابل للعمل على ويندوز ١٠
T1546	.012	Image File Execution Options Injection	قد يقوم المهاجم بتنفيذ تعليمات برمجية ضارة من خلال (Image File Execution Options (IFEO) debuggers) وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات. تقوم (IFEO) بتمكين المطورين من ارفاق مصحح الأخطاء مع التطبيق او البرمجية. فعند القيام باي عملية سيكون مصحح الأخطاء موجود من ضمن (IFEO) للتطبيق. والتي تودي الى انشاء عملية جديدة من ضمن مصحح الأخطاء. على سبيل المثال (C:\dbg\ntsd.exe -g notepad.exe).
T1546	.013	PowerShell Profile	قد يقوم المهاجم بتنفيذ تعليمات برمجية ضارة من خلال استغلال التفاعل مع (PowerShell profiles) وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات. ان (profile.ps1) هو سكربت يعمل حينما يقوم (PowerShell) بالعمل. وتستطيع من خلاله تخصيص البيئة الخاصة بالمستخدم.
T1546	.014	Emond	قد يقوم المهاجم بتنفيذ تعليمات برمجية ضارة باستخدام (Event Monitor Daemon (emond)) وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات. يقوم (emond) بتنفيذ الاحداث (event) من مختلف الخدمات ويقوم بإداراتها من خلال محرك بسيط يقوم من خلاله باتخاذ الإجراءات المناسبة. ويقوم (emond binary) في مجلد (/sbin/emond) بتحميل جميع القواعد من مستودع (/etc/emond.d/rules/) ويقوم بعد ذلك باتخاذ الإجراءات حسب الاحداث المحددة له.

T1546	.015	Component Object Model Hijacking	قد يقوم المهاجم بتنفيذ تعليمات برمجية ضارة من خلال اختطاف وسرقة (Component Object Model (COM)) عند تشغيله. ان (COM) هو احد مكونات نظام الويندوز حيث يقوم بتمكين التفاعل ما بين البرمجيات ونظام التشغيل. ويتم تخزين مختلف (COM) في (Registry).
T1133		خدامات الاتصال عن بعد External Remote Services	قد يستغل المهاجمون خدمات الاتصال عن بعد لأغراض الوصول الاولي او البقاء داخل الشبكة أكثر قدر ممكن. تتيح الخدمات عن بعد مثل (Citrix وVPN) وبعض الطرق الأخرى للمستخدمين الوصول عن بعد لموارد الشبكة الداخلية. وغالباً ما توجد ما تسمى بـ(gateways) لإدارة الاتصالات والتحقق من صحة الحسابات لهذه الخدمات. وكما ان خدمة (Windows Remote Management) تستخدم للاتصال عن بعد.
T1574		انتحال مجال التنفيذ / Flow Hijack Execution	قد يقوم المهاجمين باعتراض تشغيل البرامج لتنفيذ تعليماتهم البرمجية الضارة، وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات وقد يستغل المهاجم مثل هذه الهجمات في تخطي القيود على التنفيذ او التحكم بطريقة عمل التطبيقات داخل النظام.
T1574	.001	DLL Search Order Hijacking	قد يقوم المهاجمين باعتراض طلبات البحث (search order) لتنفيذ تعليماتهم البرمجية الضارة DLLs، وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات. ان نظام ويندوز يستخدم طريقة شائعة في عملية البحث عن مكتبات DLL المطلوب تحميلها في احد البرامج او التطبيقات. وقد يستخدم المهاجمين هذه الميزة لتنفيذ اغراضهم الخبيثة.
T1574	.002	DLL Side-Loading	قد يقوم المهاجمين بتحميل مكتباتهم (DLL) الضارة للنظام. وتتشابه هذه الهجمة مع الهجمة السابقة (DLL Search Order Hijacking). ويختلف (side-loading) عنه انه يقوم بتحميل تلك DLL بدل من زرعها ضمن الترتيب الخاص بالبحث عن DLL ثم انتظار النظام او الضحية من استدعائها. وقد يقوم المهاجمون بهذه الطريقة من خلال زرعها ثم يقوم المهاجم باستدعائها من خلال برمجيات معتمدة وغير ضارة.
T1574	.004	Dylib Hijacking	قد يقوم المهاجم بتنفيذ تعليماته البرمجية الضارة من خلال وضعها داخل (dylib (dynamic library)) مع اسم متوقع من التطبيق المراد استهدفه ان يقوم بتشغيلها. ان (dylib (dynamic library)) ستقوم بالبحث ومحاولة إيجاد (dylib) بناء على الترتيب التسلسلي للمسارات/الامتدادات الخاصة بعمليات البحث. وقد تكون المسارات التي تؤدي الى(dylib) مسبوقة بـ(@rpath). و(@rpath) هي التي تسمح للمطورين بتحديد مجموعة المسارات الخاصة بالبحث وقت التنفيذ. وبالإضافة الى ذلك اذا لم يتم ربطها بالشكل المناسب مثل استخدام (LC_LOAD_WEAK_DYLIB). سيستمر البرنامج بتنفيذ التعليمات حتى في حال عدم وجود(dylib) المتوقع. مما يتيح للمطورين من تشغيل تطبيقاتهم على إصدارات متعددة من (macOS) مع إضافة واجهات برمجة تطبيقات جديدة (API).
T1574	.005	Executable Installer File Permissions Weakness	قد يقوم المهاجمين بتنفيذ تعليماتهم البرمجية الضارة من خلال اعتراض او سرقة (binaries) المستخدم في عملية التثبيت. وقد تتم هذه العملية بشكل تلقائي من خلال تنفيذ بعض (binaries) من اثناء عملية التثبيت. في حال كانت الصلاحيات /الاذونات الخاصة بمجلدات النظام التي تحتوي على (binaries) المستهدف في العملية. او الصلاحيات/الاذونات الخاصة بنفس (binaries) تم اعدادها بشكل غير صحيح. فقد يقوم (binaries) بإعادة كتابة نفسه فوق (binaries) اخر باستخدام الاذونات والصلاحيات الممنوحة له. وفي بعض الأحيان قد يعمل في اعلى صلاحيات والتي قد تتضمن صلاحيات (SYSTEM).
T1574	.006	Dynamic Linker Hijacking	قد يقوم المهاجمين بتشغيل وتنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة المتغيرات(Variables) في البيئة من خلال استخدام (dynamic linker) لإضافتها للمكتبات المشتركة او ما يسمى بـ(libaraies Shared). من خلال عمليات التحضير لتنفيذ او تشغيل البرنامج. ويقوم (linker dynamic) بتحميل مسارات الخصائص البيئية للمكتبات المشتركة من خلال المتغيرات البيئية (environment variables) والملفات مثل (LD_PRELOAD) في نظام لينكس او (DYLD_INSERT_LIBRARIES) في نظام MacOs. يتم إعطاء أولوية تحميل المكتبات التي تم تحديدها اولاً، حتى يتم أعطاها أولوية على مكتبات النظام التي لها نفس الاسم

			الوظيفي. وعادة ما يتم استخدام هذه المتغيرات من قبل المطورين لتصحيح الأخطاء دون الحاجة الى عمل (recompile). ويتم تنفيذ وظائف مخصصة دون الحاجة الى تغير أي من المكتبات الاصلية.
T1574	.007	Path Interception by PATH Environment Variable	قد يقوم المهاجمين بتشغيل او تنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة المتغيرات (variables) التي يتم تحميلها في المكتبات. قد يقوم المهاجم بوضع برنامجه من المقدمة في القائمة المخزنة في مسارات البيئة (PATH environment variable). والتي سيقوم نظام التشغيل ويندوز بتشغيله عند عملية البحث بشكل تسلسلي باستخدام قائمة (PATH) والتي يتم استدعائها من خلال سكربت او سطر الأوامر.
T1574	.008	Path Interception by Search Order Hijacking	قد يقوم المهاجمين بتشغيل او تنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف ترتيب البحث والذي من المفترض انه يستدعي برنامج اخر. ونظراً ان بعض البرامج لا تستدعي برامج أخرى باستخدام قائمة (PATH)، قد يقوم المهاجم بوضع ملفاته في القائمة التي سيتم استدعاء البرمجيات منها. والتي سيتسبب بجعل النظام بتشغيل برنامجه الضار بسبب استدعاء برنامج اخر له.
T1574	.009	Path Interception by Unquoted Path	قد يقوم المهاجمين بتشغيل او تنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف المراجع الخاصة بالملفات. قد يستغل المهاجم المسارات الغير محدده بعلامات الاقتباس ("") والتي من خلالها يقوم بوضع تعليماته البرمجية التنفيذية في اعلى القائمة في (PATH). والتي عندما يقوم نظام التشغيل الويندوز بالاختيار من القائمة سيقوم بتشغيله.
T1574	.010	Services File Permissions Weakness	قد يقوم المهاجمين بتشغيل تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة (binaries) التي يتم استخدامها من قبل الخدمات. يستغل المهاجمين سير العمل (Flaws) الخاصة بالصلاحيات لنظام الخدمات في الويندوز لاستبدال (binaries) التي يتم تنفيذها عند تنفيذ الخدمات. وبعض الخدمات قد يتم تفعيلها بشكل تلقائي بواسطة (binaries) مخصص لتنفيذ وظيفة محددة. اذا تم تحديد الصلاحيات المجلد الذي يحتوي على (binaries) المستهدف او الصلاحيات على (binaries) بذاته، فقد يقوم المهاجم بالكتابة فوقة بالصلاحيات الممنوحة له في المجلد او (binaries) بذاته والتي قد تكون صلاحيات عالية او صلاحيات النظام (SYSTEM) التي تسمح له بهذا العمل والتنفيذ.
T1574	.011	Services Registry Permissions Weakness	قد يقوم المهاجمين بتشغيل تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة مدخلات (Registry) المستخدمة من قبل الخدمات في النظام. يستغل المهاجمين سير العمل (Flaws) الخاصة بالصلاحيات لنظام لل(Registry) في الويندوز لاعادة تنفيذ التعليمات البرمجية الأصلية للبرمجيات التي يتحكم بها. والتي يستخدمها لتشغيل الاكواد الضارة من خلال الخدمات. ويقوم نظام ويندوز بحفظ الخدمات المحلية والاعدادات الخاصة بها في (HKLM\SYSTEM\CurrentControlSet\Services) والخدمات التي يتم تخزينها في (Registry keys) قد يتم التلاعب بها او تعديلها لجعلها تقوم بتنفيذ الخدمات الضارة والتي من شأنها ات تقوم بتشغيل أدوات او تنفيذ تعليمات برمجية او تشغيل PowerShell او Reg. ويتم التحكم في الوصول الى (Registry keys) من خلال قوائم التحكم في الوصول والاذونات (Access Control Lists and permissions).
T1574	.012	COR_PROFILER	قد يستغل المهاجمين المتغيرات في البيئة لـ (COR_PROFILER) والتي قد تؤدي الى اختطاف/سرقة آلية عمل البرنامج والتي تقوم بتحميلها الى .NET CLR. ان (COR_PROFILER) هي احد المميزات لاطار (.Framework NET) والتي تسمح للمطورين بتحديد ملفات التعاريف .NET. DLL/External الغير مدارة (unmanaged) ليتم تحميلها في كل عملية من عمليات .NET CLR. وتم إيجاد وتصميم ملفات التعريف لمراقبة وتصحيح الأخطاء البرمجية التي يتم تنفيذها بواسطة .NET CRL.
T1525		تفعيل نسخة صورية / Implant Container Image	قد يقوم المهاجمين بزراع نسخة صورية (Image) او مستودع (container) يحتوي على تعليمات برمجية ضارة وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات بعد عمليات الدخول الاولي. من الأمثلة المشهورة (Amazon Web Services (AWS) Amazon Machine Images (AMIs, Azure ,Google Cloud Platform (GCP) Images) وكذلك بعض النسخ المستخدمة في (Docker) والتي قد تستخدم كأبواب خلفية. بخلاف آلية رفع البرمجيات او التعليمات البرمجية الضارة

			يقوم هنا المهاجم باستخدام أسلوب زراعة النسخة الضارة في البيئة الخاصة بالمستهدف. باختلاف طريقة عمل البيئة لدى الجهة المستهدفة فقد يوفر للمهاجم آلية وصول لفترة طويلة من الوقت.
T1556		تعدي العمليات المصرح بها Modify / Authentication Process	قد يقوم المهاجمين بتعديل آلية وطريقة عمل المصادقة للمستخدمين او السماح للوصول لبعض الحسابات بطريقة غير مرغوبة. ان عملية المصادقة تتم من خلال آليات متعددة مثل (Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM)) في نظام الويندوز و (pluggable authentication modules (PAM)) في نظام لينكس و (authorization plugins) في نظام MacOs. وجميع التقنيات التي ذكرت سابقاً هي المسؤولة عن تخزين وحفظ بيانات المصادقة والتحقق منها. والتي قد تسمح في بعض الأحوال للمهاجمين من المصادقة على خدمة او نظام دون الحاجة الى استخدام حسابات فعالة وصحيحة.
T1556	.001	Domain Controller Authentication	قد يقوم المهاجم بتصحيح. عمليات المصادقة على (Domain Controller) وذلك بهدف تخطي وسائل التحقق المتبعة وتمكينه من الوصول الى الحسابات.
T1556	.002	Password Filter DLL	قد يقوم المهاجمين باستخدام (Filter DLL Password) في عمليات المصادقة لتحقق من صحة بيانات الاعتماد
T1556	.003	Pluggable Authentication Modules	قد يقوم المهاجمين بتعديل (authentication modules (PAM pluggable)) للوصول الى بيانات الاعتماد او تفعيل حسابات غير مرغوب فيها. ان (pluggable authentication modules (PAM)) هو نظام معياري للإعدادات الخاصة للملفات و المكتبات والملفات التنفيذية والتي تقوم بتوجيه آلية المصادقة للعديد من الخدمات. ومن اشهرها هي (pam_unix) والتي تقوم باسترداد المعلومات الخاصة بمصادقة الحساب وتعينها والتحقق منها في (etc/passwd/) و (etc/shadow/)
T1556	.004	Network Device Authentication	قد يقوم المهاجم بالاستفادة من التشفير الخاص بكلمات المرور في أنظمة التشغيل او ما يسمى (Patch System Image). وبالتالي يستفيد منها المهاجمين في تجاوز آليات المصادقة للحسابات المحلية على أجهزة الشبكة.
T1137		خدمات الاوفيس مع بدء التشغيل / Office Application Startup	قد يستفيد المهاجمين من التطبيقات المساندة مع (Microsoft Office) وذلك بهدف البقاء داخل الشبكة المخترقة أطول فترة ممكنة وخصوصاً عند بدء تسجيل الدخول. وكما هو معروف ان (Microsoft Office) هو برنامج تابع لشركة مايكروسوفت ويعمل على نظام ويندوز ويعمل على أكثر الشبكات الخاصة بالمنظمات. وهناك طرق متعددة لعملية البقاء داخل الشبكة في (Microsoft Office) والتي تعمل مع بدء تشغيل التطبيق. والتي تشمل مثل وحدات المايكرو (Macros) او القوالب او بعد الإضافات الإضافية.
T1137	.001	ملفات المايكرو / Office Template Macros	قد يقوم المهاجمين باستغلال القوالب الخاصة بـ(Microsoft Office) لاختراق النظام والبقاء أطول فترة ممكنة. ان (Microsoft Office) يحتوي على قوالب متعددة ويتم استخدامها لتخصيص بعض طرق العرض والانماط. ويتم تشغيل القوالب الأساسية للتطبيق في كل مره تقوم باستخدامه.
T1137	.002	Office Test	قد يقوم المهاجمين باستغلال (Office Test) وهو عبارة عن (Registry key) وذلك بهدف لاختراق النظام والبقاء أطول فترة ممكنة. ان (Office Test) يسمح للمستخدم بتحديد مكتبة (DLL) التي سيتم تنفيذها كل مره عند تشغيل النظام. يعتقد ان (Registry key) يستخدم من قبل النظام لتحميل مكتبات DLL للاختبارات وتصحيح الأخطاء اثناء تطوير تطبيقات Office. ولا يتم انشاء (Registry key) بشكل تلقائي اثناء التثبيت.
T1137	.003	Outlook Forms	قد يستغل المهاجمين القوالب الخاصة بـ(Microsoft Outlook) وذلك بهدف لاختراق النظام والبقاء أطول فترة ممكنة. والمعروف ان تطبيق (Microsoft Outlook) يستخدم لأرسال البريد الالكتروني وقد يستخدم المهاجمين بعض القوالب بشكل ضار. والتي يمكن استخدامها وتفعيلها اثناء ارسال بريد الالكتروني على سبيل المثال.
T1137	.004	الصفحة الرئيسية لبرنامج استخدام البريد / Outlook Home Page	قد يستغل المهاجمين باستغلال المميزات التي في الصفحة الرئيسية للبريد الالكتروني (Microsoft Outlook's Home Page) وذلك بهدف لاختراق النظام والبقاء أطول فترة ممكنة. وتوجد هذه الصفحة لتخصيص بعض الاعدادات وهي من المميزات القديمة المتوفرة في برنامج (outlook). ومن امثلتها تخصيص عرض المجلدات وغيرها. وتسمح هذه الميزة بتحميل وعرض عنوان (URL)

			داخلي او خارجي كلما تم فتح المجلد. ويمكن انشاء صفحة HTML ضارة من شأنها تنفيذ تعليمات برمجية عند فتحها بواسطة الصفحة الرئيسية للبريد الالكتروني.
T1137	.005	القواعد في رنامج استخدام البريد / Rules Outlook	قد يستغل المهاجمين باستغلال القواعد الخاصة بالبريد الالكتروني (Outlook rules) وذلك بهدف لاختراق النظام والبقاء أطول فترة ممكنة. ان (Outlook rules) تسمح للمستخدمين بتخصيص وأتمته عمليات التحكم بالبريد الالكتروني. ومن امثلتها نقل بعض العناوين البريدة بشكل تلقائي الى مجلد مخصص او تمريره الى بريد الالكتروني اخر وهي تستخدم في حال كان هناك بعض الكلمات المحددة في البريد او تحديد من البريد المرسل وغيرها ... ويمكن للمهاجمين من انشاء قواعد ضارة من خلالها يتم تنفيذ تعليمات برمجية ضارة عندما يقوم المهاجم بإرسال بريد الإلكتروني للمستهدف.
T1137	.006	الاضافات Add-ins	قد يقوم المهاجمين باستغلال بعض الوظائف الإضافية الخاصة بـ(Microsoft Office) وذلك بهدف لاختراق النظام والبقاء أطول فترة ممكنة. وهناك العديد من الإضافات التي من الممكن استخدامها على منتجات مايكروسوفت مثل (Word/Excel) ومكتباتها التي تسمى (WLL/XLL)، و إضافات (VBA) و إضافة (Office Component Object Model (COM) وبعض الإضافات الخاصة بالاتمته، ومحرر الخاص بـ(VBE). و (Visual Studio Tools for Office (VSTO)) واضافات البريد الالكتروني كذلك.
T1542		نظام اقلاع جاهز / Pre-OS Boot	قد يقوم المهاجمين باستغلال آليات الإقلاع الخاصة بالنظام كطريقة للبقاء أطول فترة ممكنة في النظام. وتعرف هذه الأنظمة بالأنظمة الأساسية قبل عملية اقلاع نظام التشغيل.
T1542	.001	System Firmware	قد يقوم المهاجمين بتعديل ما يسمى بـ(firmware system) وذلك بهدف لاختراق النظام والبقاء أطول فترة ممكنة. ان (BIOS (Input/Output System Basic و (Unified Extensible Firmware Interface (UEFI)) او (Extensible Firmware Interface (EFI)) جميعهم هي أنظمة تشغيله ثابته من نوع (firmware) وهي تعمل ما بين نظام التشغيل والعتاد الخاص بالجهاز.
T1542	.002	Component Firmware	قد يقوم المهاجمين بتعديل ما يسمى بـ(component firmware) وذلك بهدف لاختراق النظام والبقاء أطول فترة ممكنة. وقد يستخدم بعض المهاجمين طرق معقده ومتقدمة جداً لتنفيذ مثل هذه العمليات المتقدمة في الاختراق والتي تؤدي الى تثبيت (component firmware) ضار يقوم يتنفيذ تعليمات البرمجية الضارة على نظام التشغيل او النظام الخاص بـ(BISO). ان هذه الأساليب تتشابه مع (System Firmware) ولكن يتن تنفيذها على بعض المكونات والاجهزة التي لا تمتلك مستوى قدرات في فحص مستوى سلامتها
T1542	.003	برمجية ضارة مع اقلاع النظام / Bootkit	قد يقوم المهاجمين باستغلال ما يسمى بـ(bootkits) وذلك بهدف البقاء أطول فترة ممكنة. ويتم استخدام (bootkits) كطبقة أسفل نظام التشغيل. ومثل هذه الاستغلال صعب الاكتشاف مالم يتم التحقق منه.
T1542	.004	ROMMONkit	قد يقوم المهاجمين باستغلال ما يسمى بـ(Monitor (ROMMON ROM)) وذلك من خلال تحميل أنظمة (firmware) ضار وذلك بهدف البقاء أطول فترة ممكنة. ومثل هذه الاستغلال صعب الاكتشاف مالم يتم التحقق منه.
T1542	.005	TFTP Boot	قد يقوم المهاجمين باستغلال (netbooting) لتحميل نظام تشغيل غير مصرح به من خادم نقل الملفات بواسطة بروتوكول (TFTP). يتم استخدام (TFTP boot (netbooting)) بشكل شائع بين مدراء الشبكات لتحميل الاعدادات الخاصة بأجهزة الشبكات والنسخ الصورية (Image) من خادم مركزي او مستودع. ان (netbooting) هو واحد من الخيارات المسموح بها للإقلاع الخاص بالنظام ويمكن استخدامه لتحكم والإدارة وكذلك مركز لحفظ النسخ الصورية (Images).
T1053		Scheduled Task/Job	قد يقوم المهاجمين باستغلال وظائف الجدولة او ما يسمى بـ(Scheduled Task/Job) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. ان (Scheduled Task/Job) هي أداة متوفرة في اكثر أنظمة التشغيل وذلك بهدف جدولة تشغيل البرمجيات السكربتات عند تاريخ او وقت محدد. وتستطيع كذلك الجدولة عن بعد في حال توفرت لديك الصلاحيات المناسبة على سبيل المثال للجدولة عن بعد ((ex: RPC and file and printer sharing in

			Windows environments)). وعلى الاغلب ان جدولة الاعمال عن بعد تستلزم وجود المستخدم في مجموعة مدراء النظام او ان يكون لدى المستخدم بعض الصلاحيات العالية على النظام البعيد.
T1053	.001	بيئة لينكس / At (Linux)	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال في نظام لينكس وتسمى (at) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. ان الامر (at) يتم استخدامه فقط من قبل مدراء النظام لجدولة الاعمال كما تم ذكره.
T1053	.002	بيئة ويندوز / At (Windows)	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال في نظام ويندوز وتسمى (at.exe) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. ان الامر (at.exe) متوفر كبرمجية تنفيذية هدفها جدولة الاعمال لنظام ويندوز لكي تعمل في وقت او تاريخ محدد. ويتطلب استخدام (at.exe) تفعيل خدمة (Scheduler Task). وان يتم استخدام احد الحسابات التي في مجموعة مدراء النظام.
T1053	.003	Cron	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال وتسمى (cron) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. ان الامر (cron) تعمل حسب الوقت المحدد لها وهي موجهه لنظام (Unix). وتحتوي (crontab) على جدول الادخالات الخاصة بـ(cron) والاوقات المراد تشغيلها به والمسارات المطلوب تفعيلها او الملفات التنفيذية.
T1053	.004	Launchd	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال وتسمى (Launchd daemon) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. ان الامر (Launchd) موجهه لنظام (macOS). وهي مسؤولة عن تحميل واداة الخدمات الخاصة بنظام التشغيل. ان عملية تحميل (parameters) لكل عملية تشغيل لل(Launchd) تتم بشكل خفي ويتم قراءتها من قائمة مخصصة او ما تسمى بـ(plist) و المتواجدة في (/ System/Library/LaunchDaemons and /Library/LaunchDaemons). وتحتوي (LaunchDaemons) على قائمة يتم الإشارة لكل ملف تنفيذي والمسار الخاص به الذي سيتم تنفيذ البرمجية منه.
T1053	.005	جدولة المهام Scheduled Task	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال وتسمى (Windows Task Scheduler) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. توجد طرق متعددة للوصول الى (Windows Task Scheduler) في نظام ويندوز. تستطيع الوصول لها بشكل مباشر من سطر الاوامر او من خلال الواجهة الرسومية الخاصة بأدوات مدراء النظام من لوحة التحكم. وفي بعض الأحيان قد يقوم المهاجمين بتفعيلها من خلال (.NET wrapper) وقد يتم استخدام (netapi32) في المكتبات الخاصة بنظام ويندوز.
T1053	.006	Systemd Timers	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال وتسمى (systemd timers) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. أداة (systemd timers) هي عبارة عن ملفات بامتدادات يرمز لها بـ(.timer) والتي يتم التحكم بالخدمات من خلالها و (systemd timers) قد يتم استخدامه لتنفيذ الاحداث الخاصة بالتقويم. ويمكن استخدامها كبديل لـ(Cron) في نظام لينكس.
	.007	Container Orchestration Job	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال وتسمى (task scheduling) التي توفرها المستودعات مثل (Kubernetes) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. وتقوم تلك المستودعات بتنفيذ وجدولة الاعمال والمهام بشكل تلقائي لتنفيذه بوقت وتاريخ محدد، وهي تشبه الى حد كبير (cron) لنظام لينكس. وقد يتم استخدام هذا الأسلوب للاستيلاء على المستودعات المتصلة مع المستودع الذي تم تنفيذ التعليمات البرمجية الضارة مع مرور الوقت.

T1505		Server Software Component	قد يقوم المهاجمين باستخدام المميزات القابلة للتطوير في الخوادم وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. وقد تتضمن التطبيقات من نوع (Enterprise server applications) على مميزات تمكن المطورين من كتابة وتثبيت البرمجيات او السكربتات لتحسين قدرات التطبيق الحالية. مما قد نمكن المهاجمين من تثبيت وتنفيذ التعليمات او البرمجيات الضارة من خلال استغلال التحسينات المستخدمة في تطبيقات الخوادم.
T1505	.001	SQL Stored Procedures	قد يقوم المهاجمين باستغلال إجراءات تخزين (SQL) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. ان (SQL Stored Procedures) هي تعليمة برمجية يمكن حفظها وإعادة استخدامها لكيلا يقوم المستخدمين لقاعدة البيانات من إعادة كتابة استعلامات (SQL). وحيث تم تفعيل (SQL Stored Procedures) من خلال استعلام (SQL) الى قاعدة البيانات باستخدام التعاريف الخاصة بها على سبيل المثال (تشغيل او إعادة تشغيل خادم SQL)
T1505	.002	Transport Agent	قد يقوم المهاجمين باستغلال (transport agents Microsoft) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين البقاء أطول فترة ممكنه داخل النظام المخترق. ان (Microsoft transport agents) العمل بواسطة البريد الالكتروني حيث يتم تمريره بواسطة بعض المهام مثل تصفية البريد المزعج، تصفية البريد الضارة او إضافة التواقيع الرقمية الى نهاية جميع الرسائل الخاصة بالبريد الالكتروني الصادرة. ويمكن كتابة (Microsoft transport agents) بواسطة المطورين ومن ثم عمل (complied) بواسطة (.NET). وسيتم استدعاء (transport agents Microsoft) خلال احد المراحل المحددة في عملية ارسال البريد الالكتروني والتم تم تحديدها من قبل المطورين.
T1505	.003	ابواب خلفية Web Shell	قد يقوم المهاجمين بإعداد الأبواب الخلفية (WebShells) في خوادم الويب بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين البقاء أطول فترة ممكنه داخل النظام المخترق. ان (WebShells) هي سكربتات يتم رفعها على خوادم الويب حيث تسمح للمهاجم بالوصول لخوادم الويب. وقد يتم إضافة بعض الخواص المتقدمة لل(WebShells) لتنفيذ سطر الأوامر (Command line) داخل النظام.
T1205		Traffic Signaling	قد يقوم المهاجمين باستخدام (signaling traffic) بهدف إخفاء المنافذ المفتوحة او إخفاء بعض الوظائف الضارة والتي تستخدم بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين البقاء أطول فترة ممكنه داخل النظام المخترق. وتستخدم في بعض الأحيان من خلال سطر الأوامر (line Command) والتي تستخدم ما يسمى بـ(magic value او تسلسل محدد) والذي يتم ارساله لتحفيز استجابة معينة. مثل فتح او اغلاق أحد المنافذ او تنفيذ بعض المهام الضارة. وقد يقوم المهاجم بإرسال مجموعة من الحزم قبل اجراء أي عملية من فتح او اغلاق المنافذ والتي ستمكنه من التحكم والسيطرة على النظام المصاب. وعادة ما تكون هذه السلسلة من الحرم يتم تحديدها مسبقاً مثل (Port Knocking). ولكن قم يتم تضمين بعض التعليمات الفريدة من نوعها بعد اكمال عملية ارسال الحزم مما يقوم بفتح المنفذ او أغلاقه في جدار الحماية الخاص بالمستضيف او ما يسمى بـ(host-based firewall) او من خلال تشغيل برمجية مخصصة لذلك.
T1205	.001	Port Knocking	قد يقوم المهاجمين باستخدام (port knocking) بهدف إخفاء المنافذ المفتوحة او إخفاء بعض الوظائف الضارة والتي تستخدم بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين البقاء أطول فترة ممكنه داخل النظام المخترق. ولكي يتم تفعيل/اغلاق المنافذ يقوم المهاجم بإرسال سلسلة من المحاولات التي تم تعريفها سابقاً. او يستطيع المهاجم استخدام بعض البرمجيات والتي من شأنها القيام بفتح المنافذ او اغلاقها في جدار الحماية الخاص بالمستضيف او ما يسمى بـ(host-based firewall)
T1078		حساب فعال / Valid Accounts	قد يقوم المهاجم باستغلال بيانات الاعتماد للحسابات الفعالة وذلك بهدف الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. ان بيانات الاعتماد المخترقة قد يستخدم لتخطي عناصر التحكم بالوصول (access controls) التي تم تطبيقها على الأنظمة والموارد الخاصة بالشبكة. وقد يتم استخدام هذه الحسابات للوصول للأنظمة

			عن بعد او الخدمات مثل VPN او البريد الالكتروني او سطح المكتب البعيد من خلال المتصفح. وقد يتم استخدام بيانات الاعتماد المخترقة لتصعيد الصلاحيات لأنظمة محدد او الوصول الى منطقة حساسة داخل الشبكة المستهدفة. وقد يقوم المهاجم بتنفيذ عملياته الضارة ببيانات الاعتماد المخترقة دون الحاجة الى تبيث بعض البرمجيات الضارة والتي قد تؤدي الى اكتشافه.
T1078	.001	حساب افتراضي / Default Accounts	قد يقوم المهاجم بالحصول على بيانات الاعتماد للحسابات الافتراضية في النظام والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. ان الحسابات الافتراضية هي التي يتم انشاءها بشكل افتراضي داخل الأنظمة مثل حساب (Guest او Administrator) في نظام ويندوز. الحسابات الافتراضية قد تأتي كذلك من الأنظمة الخاصة ببعض العتاد من الشركة المصنعة. والتي قد تكون حساب مدير للنظام. ان حساب مدير النظام الخاص بخدمات (AWS) وحساب الخدمات الافتراضي في (Kubernetes)
T1078	.002	حساب مدير النظام / Domain Accounts	قد يقوم المهاجمين باستغلال بيانات الاعتماد الخاصة بمدراء النطاق (domain account) والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. ان حسابات مدراء النطاق والتي يتم التحكم بها من قبل (Service Active Directory Domain) والتي من خلالها يتم إعطاء الصلاحيات و التكوين لخدمات للنظام. ومن الممكن ان تكون حسابات مدراء. النظام عبارة عن حسابات مستخدمين او خدمات.
T1078	.003	حساب محلي / Local Accounts	قد يقوم المهاجمين باستغلال بيانات الاعتماد الخاصة بالحسابات المحلية (local account) والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. الحسابات المحلية يتم اعدادها من قبل المنظمة بهدف تقديم خدمات الدعم للأنظمة عن بعد او لتفعيل بعض الخدمات الوصول للأنظمة و ادارتها.
T1078	.004	حساب الخدمات السحابية / Cloud Accounts	قد يقوم المهاجمين باستغلال بيانات الاعتماد الخاصة بالحسابات على الخدمات السحابية (cloud account) والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. حسابات الخدمات السحابية قد يتم انشاءها واعدادها من قبل المنظمة بهدف تقديم خدمات الدعم للأنظمة عن بعد او لتفعيل بعض الخدمات الوصول للأنظمة وادارتها او التطبيقات. قد يتم توحيد الحسابات الخاصة بالخدمات السحابية مع الحسابات في النطاقات (Window Active Directory)

تصعيد الصلاحيات / Privilege Escalation

تصعيد الصلاحيات: يقوم المهاجمين باستخدام أساليب متعددة للحصول على صلاحيات اعلى عند اختراق النظام او الشبكة، حيث ان المهاجم بعد عملية الوصول الأول واكتشاف الشبكة والاطلاع عليها قد يواجه صعوبة في الوصول لبعض الأنظمة او الخدمات بسبب محدودية الصلاحيات والاذونات التي قام باختراقها مما يستدعي الى رفع الصلاحيات لهذا الحساب من خلال استغلال اما ثغرات في النظام او اعدادات خاطئة او ثغرات برمجية

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1548		اساءة استخدام ميزة رفع الصلاحيات / Abuse Elevation Control Mechanism	قد يقوم المهاجم بالتلاعب واستغلال آليات التحكم في رفع الصلاحيات للحصول على صلاحيات او أذونات اعلى. وتحتوي معظم أنظمة التشغيل الحديثة على آلية لتحكم في الصلاحيات والتي تهدف الى رفع او التحكم في الصلاحيات لحساب او خدمة محددة من اجل أداء المهام المطلوب تنفيذها على النظام. والتي تكون في معظم الاحول من إعطاء صلاحيات لبعض المستخدمين للقيام بمهام حساسة وحرجة تتطلب صلاحيات عالية. وقد يقوم المهاجم بطرق مشابه للاستفادة من طرق رفع الصلاحيات المتوفرة مع النظام من اجل رفع الصلاحيات الخاصة به.
T1548	.001	Setuid and Setgid	قد يقوم المهاجمين باستخدام ما يسمى بـ(shell escapes) او استغلال الثغرات في التطبيقات مع ما يطلق عليه (setsuid) او (setgid bits) وذلك بهدف الحصول على كود ضار يعمل في حسابات مستخدمين اخرين. ان في نظام (لينكس او ماك او اس). عندما يتم تعين (setuid او setgid bits) لاحد التطبيقات، سيعمل التطبيق بامتيازات المستخدم او المجموعة المستهدفة. والحالة الطبيعية عند أي تشغيل التطبيق يتم تنفيذه بصلاحيات المستخدم الحالي. بغض النظر عن المستخدم المالك للتطبيق او المجموعة. ومع ذلك هناك حالات تحتاج بعض التطبيقات فيها الى تنفيذ بعض الوظائف التي تحتاج الى صلاحيات عالية حتى وان كان المستخدم لا يمتلك تلك الصلاحيات.
T1548	.002	تخطي صلاحيات التحكم بالحسابات / Bypass User Account Control	قد يقوم المهاجمين بتخطي آليات التحكم في حساب المستخدم وذلك بهدف رفع الصلاحيات على النظام. نظام ويندوز يمتلك ما يسمى بـ(Windows User Account Control (UAC)) وهي تسمح برفع الصلاحيات والتي تقوم بتتبع سلامة عمليات التصعيد من الصلاحيات الأقل الى الأعلى. وعادة ما يتم تنفيذ وتعديل والوصول تلك المهمة بصلاحيات مدير النظام والتي تأتي علي شكل (تبويب) للمستخدم لتأكيد على العملية، وذلك بهدف تنبيه المستخدمين ان هذه المهمة تتطلب صلاحيات عالية وقد تقوم بالتأثير على النظام وقد تتطلب في بعض الأحيان من مدراء النظام المحلي (Local او domain) ادخال كلمة المرور لإكمال الإجراءات.
T1548	.003	Sudo and Sudo Caching	قد يقوم المهاجم بتنفيذ (and/or use the suoders sudo caching) لرفع الصاحيات. قد يقوم المهاجمين بتنفيذ بعض الأوامر التي من شأنها استدعاء بعض العمليات التابعة لمستخدمين اخرين والاستفادة منها للحصول على صلاحيات اعلى.
T1548	.004	Elevated Execution with Prompt	قد يقوم المهاجمين من استخدام (AuthorizationExecuteWithPrivileges API) لرفع الصلاحيات من خلال استخدام الطلب من المستخدمين بيانات الاعتماد الخاصة بهم. ان الهدف من استخدام (API) هو إعطاء المطورين للتطبيقات طريقة سهله لاجراء العمليات بصلاحيات عالية جداً، على سبيل المثال تثبيت تطبيق او تحديث. حيث ان (API) لا تقوم بالتحقق من التطبيق الذى يطلب تلك الصلاحيات هل هو تطبيق ضار او غير ضار او تم تعديله.
T1134		التلاعب بالتوكن / Access Token Manipulation	قد يقوم المهاجمين بتعديل (tokens) للقيام بتنفيذ عمليات بحساب مستخدم اخر او حساب النظام (SYSTEM) وذلك بهدف تخطي آليات التحكم. يستخدم نظام ويندوز (tokens) لتحديد ملكية العمليات التي قيد التشغيل. ويمكن للمستخدم من التلاعب بـ(tokens) لتظهر العملية التي قيد التشغيل كما انها لو كانت تابعة لمستخدم اخر او تابعة لعملية أخرى (process child of a different). وعند القيام بذلك تأخذ هذه العملية سياق الأمان المرتبطة بـ(tokens) الجديد الذي تم ربطه به.
T1134	.001	Token Impersonation/Theft	قد يقوم المهاجمين بانتحال او بتكرار (token) الخاص بمستخدم أخرى وذلك بهدف رفع الصلاحيات او تخطي آليات التحكم. المهاجمين يستطيعون انشاء وتكرار (token) الموجود باستخدام (DuplicateToken(Ex)). ويمكن بعد ذلك استخدام(token) المكرر لعملية تسمى بـ(ImpersonateLoggedOnUser) والتي تسمح باستدعاء (thread) معين وانتحال صفة مستخدم مسجل دخوله الى النظام. او استخدام (SetThreadToken) لتعينه وربطه بـ(thread) مخصص.

T1134	.002	Create Process with Token	قد يقوم المهاجمين بإنشاء عملية جديدة او تكرار (token) بهدف رفع الصلاحيات او تخطي آليات التحكم. يمكن للمهاجمين من تكرار (token) باستخدام DuplicateToken(Ex) و يستخدمها مع CreateProcessWithTokenW بهدف انشاء عملية جديدة تحت المستخدم المنتحل. هذه الطريقة مفيدة جداً لإنشاء العمليات تحت حسابات مستخدمين اخرين.
T1134	.003	Make and Impersonate Token	قد يقوم المهاجمين بإنشاء او انتحال (tokens) بهدف رفع الصلاحيات او تخطي آليات التحكم. في حال كان لدى المهاجم اسم مستخدم وكلمة مرور ولكن المستخدم لم يقم بتسجيل الدخول للنظام، فيمكن للمهاجم من انشاء جلسة (Session) للمستخدم باستخدام وظيفة (LogonUser). هذه الوظيفة ستقوم باستعادة نسخة من رمز (tokens) الخاصة بالجلسة ويقوم المهاجم بعد ذلك باستخدام (SetThreadToken) لربط (tokens) بـ(thread) مخصص.
T1134	.004	Parent PID Spoofing	قد يقوم المهاجمين بانتحال (identifier (PPID parent process)) لعملية جديدة (New process) بهدف التخفي من عملية (مراقبة العمليات) او لرفع الصلاحيات. وعادة ما يتم انشاء العمليات الجديدة مباشره من بواسطة (parent او calling) مالم يتم تحديد مكان الاستدعاء بشكل واضح. ان أحد الطرق لتعيين (PPID) بشكل واضح لعملية جديدة هي عبر استدعاء (CreateProcess API call)، والذي يدعم (parameter) لتحديد (PPID) ومن ثم استخدامه. يتم استخدام هذه الوظيفة في نظام ويندوز بواسطة (Windows features) على سبيل المثال (UAC) والتي تقوم بتصحيح عملية (PPID) بعد عملية طلب رفع صلاحية تلك العملية واستدعائها بواسطة (SYSTEM) والتي تتم عادة من خلال (svchost.exe or consent.exe) بدلاً من استخدام صلاحيات المستخدم نفسه.
T1134	.005	SID-History Injection	قد يقوم المهاجم باستخدام (Injection SID-History) بهدف رفع الصلاحيات او تخطي آليات التحكم. ان (Windows security identifier (SID)) هو قيمة فريدة تستخدم لتعريف حسابات (المستخدم/المجموعة). ان (SID) تستخدم بواسطة تقنيات الأمان في نظام ويندوز وكذلك تقنية (Tokens). حيث يمكن للحساب الاحتفاظ بـ(SID) في (SID-History Active Directory) والتي تسمح بعملية تسمى بـ(inter-operable) والتي تسمح باستخدام/تبادل الحسابات/المعلومات بين النطاقات (Domains). على سبيل أمثال (تضمين جميع القيام الخاصة بـ(tokens access) في (SID-History).
T1547		تسجيل الدخول التلقائي / Boot or Logon Autostart Execution	قد يقوم المهاجم باستخدام اعدادات النظام تنفيذ تعليمات برمجية ضارة من خلال اعدادات لجعل التنفيذ يتم بشكل تلقائي من خلال عملية الإقلاع او تسجيل الدخول وذلك بهدف الاستمرار والبقاء داخل الشبكة أطول فترة ممكنة. قد يحتوي نظام التشغيل على آليات لتشغيل البرامج تلقائياً عند الإقلاع او تسجيل الدخول الى الحساب. وقد تتضمن هذه الاليات تنفيذ البرامج تلقائياً التي يتم وضعها في قائمة مخصصة على سبيل أمثال وضع بعض (Registry Windows) وقد يقوم المهاجم بتحقيق نفس هذه العملية والاهداف عند التعديل على نوات النظام.
T1547	.001	مفاتيح التسجيل والتشغيل التلقائي/ Run Keys / Registry Startup Folder	قد يقوم المهاجم باستخدام مجلد بدء التشغيل (Startup) لإضافة البرمجيات او المفاتيح(run keys) الضارة الخاصة به. وستودي ادخال (run keys) في (Registry) او (Startup) الى جعل البرنامج يعمل عند قيام المستخدم بعملية تسجيل الدخول. سيتم تنفيذ هذه البرامج في حساب المستخدم الذي تم تفعيلها به والتي قد تحتاج الى أذونات خاصة مرتبطة بالحساب المستخدم.
T1547	.002	تصاريح الحزم / Authentication Package	قد يقوم المهاجمين باستخدام تصاريح الحزم لتنفيذ وتشغيل (DLLs) عند اقلاع النظام. حيث يتم تحميل ملفات DLL لحزم المصادقة لنظام ويندوز بواسطة (Local Security Authority (LSA)) عند بدء عملية التشغيل للنظام. حيث توفر عمليات الدعم لتسجيل الدخول المتعددة وكذلك إضافة بروتوكولات الأمان لنظام التشغيل.
T1547	.003	Time Providers	قد يقوم المهاجمين من استغلال (providers time) لتنفيذ او تشغيل (DLLs) عند اقلاع النظام. ان (W32Time) يتيح مزامنة الوقت عبر النطاقات. ويقوم (W32Time) بمسؤولية استرداد الوقت (time stamps) من العتاد والشبكة وإخراج القيام الى المستخدمين في الشبكة.

T1547	.004	Winlogon Helper DLL	قد يقوم المهاجمين باستخدام (Winlogon) للتنفيذ تعليمات ضارة من خلال تشغيل (DLLs) او برامج تنفيذية عند تسجيل الدخول. ان (Winlogon) هي احد مكونات نظام ويندوز وهي مسؤولة عن الإجراءات عند تسجيل الدخول او الخروج بالإضافة الى خدمة (SAS) والتي تكون عند الضغط على (Ctrl-Alt-Delete) ويتم تسجيل المدخلات في (\HKLM\Software[\Wow6432Node\]\Microsoft\Windows NT\CurrentVersion\Winlogon) و (\HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon) والتي تستخدم لإدارة البرامج والوظائف المساعدة الإضافية التي تدعم عملية(Winlogon)
T1547	.005	Security Support Provider	قد يقوم المهاجمين باستخدام (support providers (SSPs security)) للتنفيذ تعليمات ضارة من خلال تشغيل (DLLs) او برامج تنفيذية عند اقلاع النظام. يتم تحميل (security support providers (SSPs)) في (Local Security Authority (LSA)) كعملية عند بدء النظام. بعد عملية التحميل LSA,SSPI كDLLs يقوم بتشفير الأرقام السرية من صيغة نصية الى صيغة مشفرة والتي تكون مخزنة في نظام ويندوز، مثل أي كلمة مرور يتم استخدامها عند عمليات تسجيل الدول او استخدام PIN كذلك.
T1547	.006	Kernel Modules and Extensions	قد يقوم المهاجمين بتعديل النواة وذلك لتنفيذ تعليمات تلقائية ضارة بالنظام عند الإقلاع. ان وحدات التحميل (LKMs) داخل النواه هي أجزاء من تعليمات برمجية يمكن الكتابة عليها او محيها في النواه عند الطلب. وهي تعمل على زيادة قدرات النواه دون الحاجة الى إعادة تشغيل النظام. على سبيل المثال(التعاريف الخاصة بالأجهزة) والتي تسمح للنواة بالوصول الى العتاد والتعاريف المتصلة بالنظام.
T1547	.007	Re-opened Applications	قد يقوم المهاجمين بتعديل ملفات (plist) للقيام بتشغيل برمجيات ضارة بشكل تلقائي عندما يقوم المستخدم بتسجيل الدخول او بدء تشغيل النظام في (Mac OS X 10.7 (Lion)). يستطيع المستخدمون تحديد برامج او تطبيقات للإعادة فتحها بشكل تلقائي عندما يقوم المستخدم بتسجيل الدخول للأجهزة الخاصة بهم بعد إعادة التشغيل.بدل ان يتم ذلك عبر فتح البرامج كل برنامج على حدة. وهناك قائمة للمفلات التي تعمل عند بدء التشغيل (plist). وتستطيع ايجادها في (~/Library/Preferences/com.apple.loginwindow.plist) و (~/Library/Preferences/ByHost/com.apple.loginwindow.* .plist).
T1547	.008	LSASS Driver	قد يقوم المهاجمين بإضافة او تعديل (drivers LSASS) وذلك لضمان البقاء داخل الشبكة أطول فترة ممكنة في النظام المخترق. ان النظام الفرعي في الويندوز (Windows security subsystem) هو عبادة عن مجموع من المكونات تدير وتنفيذ سياسات الأمان على النظام او النطاق. ان (LSA) هو المكون الرئيسي و المسؤول عن سياسة الأمان المحلية و التحقق من صلاحيات المستخدم. ان (LSA) تحتوى على العديد من المكتبات الديناميكية (DLL) وهي كالعادة مرتبطة بوظائف امان أخرى. والتي تعمل جميعها في عملية LAS او (lsass.exe)
T1547	.009	Shortcut Modification	قد يقوم المهاجم بإضافة او تعديل الاختصارات لتشغيل او تنفيذ تعليمات برمجية ضارة عند الإقلاع او عند عملية تسجيل الدخول للنظام. ان الاختصارات أو الرموز هي طرق للإشارة إلى الملفات أو البرامج الأخرى التي سيتم فتحها أو تنفيذها عند النقر فوق الاختصار أو تنفيذه عند بدء تشغيل النظام.
T1547	.010	مراقبة الشاشات / Port Monitors	قد يقوم المهاجمين باستغلال (port monitors) لتشغيل ملفات ضارة من خلال ملفات (DLL) والتي تعمل عند اقلاع النظام وذلك للبقاء داخل الشبكة أطول فترة ممكنه. ان (port monitors) تستطيع استخدامه من خلال الاتصال بـ (AddMonitor API) والتي تسمح بتحميل ملفات DLL عند بدء التشغيل. تستطيع اجادة ملفات DLL في " C:\Windows\System32" وسيتم تحميله بواسطة خدمة التخزين الموقت للطباعة(spoolsv.exe) عند اقلاع النظام. ان (spoolsv.exe) هي عمليات تعمل كذلك تحت (SYSTEM) والتي يقصد بها صلاحيات النظام. ويمكن تحميل ملفات DLL اذا كانت هناك الاذونات المناسبة للكتابة في المسار المخصص في (HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors).
T1547	.011	Plist Modification	قد يقوم المهاجمين باستخدام (plist) لتشغيل البرامج اثناء اقلاع النظام او عند عمليات تسجيل الدخول. وتحتوي قائمة (plist) على ملفات يتم استخدامها في نظام (macOS و OS X)وهي تحتوي على الإعدادات الخاصة بالتطبيقات والخدمات. الملف تمت كتابته بترميز

			(UTF-8) وتستطيع استعراضه من خلال قارئ ملفات XML. وتأتي الإعدادات ما بين (<>). وهي توضح التفاصيل متى يجب البرامج. ومسار الملفات التنفيذية. والاذونات المطلوبة لتشغيلها.. وغيرها الكثير. تتواجد (plists) في مواقع معينة اعتمادًا على العرض منها مثل (Library/Preferences/) والتي يتم استخدامها عند رفع الصلاحيات. و (~ /Library/Preferences) عند استخدام تلك الصلاحيات.
T1547	.012	طباعة العمليات / Print Processors	قد يقوم المهاجمين باستخدام (processors print) لتشغيل مكتبات DLL ضارة اثناء اقلاع النظام. وذلك لأغراض ضارة مثل البقاء داخل النظام المخترقة او تصعيد الصلاحيات. ان (print processors) هي مكتبات DLL التي يتم تحميلها بواسطة (print spooler service, spoolsv.exe) اثناء عمليات الإقلاع.
T1037		نظام اقلاع او الدخول بواسطة سكربت / Boot or Logon Initialization Scripts	قد يقوم المهاجمين باستخدام بعض السكربتات لتنفيذ تعليمات برمجية ضارة بشكل تلقائي عن اقلاع النظام بهدف البقاء داخل النظام المخترق أطول فترة ممكنة. حيث يمكن استخدام السكربت تنفيذ بعض المهام الإدارية في الأنظمة. والتي قد ينطوي عليها تنفيذ وتشغيل البرمجيات او ارسال المعلومات الى خادم داخلي. يمكن ان تختلف السكربت من نظام الى اخر وطرق تطبيقها هل سيكون محلياً او عن بعد.
T1037	.001	سكربت الدخول لنظام ويندوز / Logon Script (Windows)	قد يقوم المهاجمين باستخدام سكربت تسجيل الدخول لأنظمة ويندوز والتي يتم تنفيذها بشكل تلقائي عند بداية عملية تسجيل الدخول. والهدف منها هو البقاء داخل النظام المخترق أطول فترة ممكنة. يسمح نظام ويندوز بتشغيل سكربتات تسجيل الدخول على مستوى المستخدمين او المجموعات. ويتم ذلك عن طريق إضافة المسار المطلوب الى(HKCU\Environment\UserInitMprLogonScript) في (Registry key).
T1037	.002	سكربت الدخول لنظام ماك Logon Script (Mac)	قد يقوم المهاجمين باستخدام سكربت تسجيل الدخول لأنظمة ماك اوس والتي يتم تنفيذها بشكل تلقائي عند بداية عملية تسجيل الدخول. والهدف منها هو البقاء داخل النظام المخترق أطول فترة ممكنة. يسمح نظام ماك بتشغيل وتنفيذ سكربتات او ما يسمى (known as login hooks) تسجيل الدخول كلما قام المستخدم بالدخول للنظام. حيث يقوم (known as login hooks) بتنفيذ السكربت عند تسجيل الدخول وهو على عكس (Startup Items) يقوم (login hooks) بتنفيذ البرمجيات عند استخدام صلاحيات مدير النظام(root).
T1037	.003	سكربت تسجيل الشبكة / Network Logon Script	قد يقوم المهاجمين باستخدام سكربت الشبكة والتي يتم تنفيذها بشكل تلقائي عند بداية عملية الدخول. والهدف منها هو البقاء داخل النظام المخترق أطول فترة ممكنة. يمكن استخدام سكربتات التي تعمل على مستوى بدء التشغيل في الشبكة من خلال (Active Directory او Group Policy Objects). تحتاج هذه السكربتات الى صلاحيات وأذونات محددة لكي يتم تعينها او استخدامها. بحسب اختلاف الأنظمة قد يستطيع المهاجم تنفيذ هذه السكربتات على نظام محدد او عدد من الأنظمة داخل الشبكة المستهدفة.
T1037	.004	Rc Scripts	قد يقوم المهاجمين بتعديل سكربت (RC) والذي يتم تنفيذه خلال الإقلاع لنظام (Unix). ان هذه الملف يسمح لمدراء النظام بربط وبدء الخدمات المخصصة الى قائمة بدء التشغيل النظام. وعادة تتطلب (RC) امتيازات مدير النظام لإجراء التعديلات (root).
T1037	.005	ادوات بدء التشغيل / Startup Items	قد يقوم المهاجمون باستغلال (Startup Items) لتنفيذ تعليمات برمجية ضارة عند اقلاع النظام بهدف البقاء في النظام أطول فترة ممكنة. ان (Startup Items) تعمل عادة في المرحلة الأخيرة من الإقلاع. وتحتوي على برامجه او سكربتات قابلة للتنفيذ او التشغيل بجانب الاعدادات التي يستخدمها النظام لتحديد الترتيب المتوقع لتشغيل وتنفيذ العناصر المتوفرة في (Items Startup).
T1543		انشاء او تعديل عمليات النظام / Create or Modify System Process	قد يقوم المهاجمين بإنشاء او تعديل العمليات على مستوى النظام بغرض تنفيذ تعليمات برمجية ضارة بهدف البقاء في النظام أطول فترة ممكنة. فعندما يقوم النظام بالإقلاع ستعمل العمليات بشكل مباشر في الخلفية. سواء كان النظام ويندوز او لينكس. حيث ان هذه العمليات يتم تصنيفها كخدمات. اما في نظام ماك اوس يتم تشغيل العمليات بواسطة (Launch Daemon) و (Launch Agent) لإنهاء تهيئة عمليات النظام و البدء بتنفيذ وتحميل عمليات المستخدم.

T1543	.001	تفعيل البرمجية / Launch Agent	قد يقوم المهاجمين بإنشاء او تعديل العمليات على مستوى النظام بغرض تنفيذ تعليمات برمجية ضارة باستخدام (launch agents) وذلك بهدف البقاء في النظام أطول فترة ممكنة. وفقاً لمطوري شركة آبل، عندما يقوم المستخدم بتسجيل الدخول يتم بدء عملية تشغيل العمليات الخاصة بكل مستخدم من خلال (launch-on-demand) والموجودة في (plist) والتي تستطيع الوصول لها من خلال (/Library/LaunchAgents/, System/Library/LaunchAgents, و $HOME/Library/LaunchAgents) ان (launch agents) لديهم قائمة من الملفات المرتبطة بملفات تنفيذيه يتم تفعيلها عند بدء التشغيل.
T1543	.002	خدمات النظام / Systemd Service	قد يقوم المهاجمين بإنشاء او تعديل العمليات الخاصة بخدمات (systemd)، وذلك بهدف البقاء في النظام أطول فترة ممكنة. ومن المتعارف على ان (systemd) يقوم بإدارة العمليات في الخلفية او الخدمات وموارد النظام الأخرى. ان (systemd) هو النظام التهيئة الافتراضي في (init) في أكثر توزيعات لينكس مثل (Debian 8, Ubuntu 15.04, CentOS 7, RHEL 7, Fedora 15). حيث تم إيجاده لاستبدال الأنظمة القديمة التي تعمل بـ(init) والتي تشتمل على (SysVinit و Upstart). وحيث ان (systemd) يتعامل كذلك مع الأنظمة السابقة والقديمة.
T1543	.003	خدمات الويندوز / Windows Service	قد يقوم المهاجمين بإنشاء او تعديل العمليات الخاصة بخدمات الخاصة بنظام (Windows)، وذلك بهدف البقاء في النظام أطول فترة ممكنة. عندما يقوم الويندوز بعمليات الإقلاع الخاصة بالنظام بعد ذلك يقوم بتشغيل البرمجيات والتطبيقات من خلال استدعاء الخدمات التي تعمل في الخلفية الخاصة بالنظام. ان نظام الخدمات والإعدادات تشتمل على مسارات الملفات للخدمات والاوامر القابلة للتنفيذ. ويتم تخزينها في (Windows Registry). ومن الممكن ان يتم تعديل اعدادات الخدمات من خلال أداة (sc.exe او Reg).
T1543	.004	Launch Daemon	قد يقوم المهاجمين بإنشاء او تعديل العمليات الخاصة بخدمات (launch daemons) وذلك بهدف البقاء في النظام أطول فترة ممكنة. وفقاً لمطوري شركة آبل، عندما يقوم المستخدم بتسجيل الدخول يتم بدء عملية تشغيل العمليات الخاصة بكل مستخدم من خلال (launch-on-demand) والموجودة في (plist) والتي تستطيع الوصول لها من خلال (/System/Library/LaunchAgents, /Library/LaunchAgents, و $HOME/Library/LaunchAgents) ان (launch agents) لديهم قائمة من الملفات المرتبطة بملفات تنفيذيه يتم تفعيلها عند بدء التشغيل.
T1484		Domain Policy Modification	قد يقوم المهاجمين بتعديل الاعدادات الخاصة بتكوين النطاقات (domain) وذلك بهدف التخفي داخل الشبكة او تصعيد الصلاحيات في النطاق المستهدف. ان التقنية التي يعمل بها النطاق (domain) تسمح له بالتحكم بالأنظمة والتقنيات وكذلك المستخدمين داخل هذا النطاق وكيف تقوم هذه الأجهزة والأنظمة والمستخدمين بالتواصل، حيث يقوم بحوكمتها حسب الحاجة. والسياسة الخاصة بهذه النطاقات تحتوي على اعدادات التواصل ما بين النطاقات والنطاقات الفرعية وما في حكمها. وقد تتضمن التعديلات على السياسة الخاصة بالنطاق (GPOs) تغير على مستوى العلاقة ما بين النطاقات المرتبطة به.
T1484	.001	Group Policy Modification	قد يقوم المهاجمين بتعديل الاعدادات الخاصة بتكوين مجموعة سياسة النطاقات (GPOs) وذلك بهدف تصعيد الصلاحيات في النطاق المستهدف. تسمح سياسة النطاقات (GPOs) بتعديل و إدارة المستخدمين او الأجهزة من خلال (Active directory AD). وكما انها تعتبر مستودع للإعدادات الخاصة بسياسة النطاقات والتي تستطيع الوصول لها من خلال (\Policies\<DOMAIN>\SYSVOL\<DOMAIN>\)
T1484	.002	Domain Trust Modification	قد يقوم المهاجمين بإضافة خاصية الثقة (trusts) بين النطاقات او تعديل خصائص ثقة سابقة في النطاق المستهدف، وذلك بهدف تصعيد الصلاحيات او التخفي داخل الشبكة. تسمح تفاصيل الثقة في النطاق او (trusts) بمعرفة اذا كان هناك علاقة ما بين نطاقين مختلفين، وكذلك خصائص المصادقة والتخويل ما بين النطاقات ومعرفة الموارد المشتركة ما بينهم. وبقد تتضمن الثقة ما بين النطاقات معلومات عن الحسابات وبيانات الدخول ووسائل المصادقة المستخدمة على الخوادم والرموز(tokens).

T1546		تنفيذ الاحداث حسب المعطيات / Event Triggered Execution	قد يقوم المهاجم باستغلال بعض الاحداث المعينة بهدف البقاء داخل النظام المخترق أطول فترة ممكن او رفع الصلاحيات. تمتلك أنظمة التشغيل وسائل لمراقبة تلك الاحداث ومتابعتها مثل عمليات تسجيل الدخول او أنشطة أخرى مثل تشغيل تطبيقات او اكواد برمجية
T1546	.001	تعديل الملف الافتراضي / File Change Default Association	قد يقوم المهاجمون باستغلال الاقتران والارتباط بين الملفات للتنفيذ تعليمات برمجية ضارة على سبيل المثال(عند تحديد ملف يتن تحديد البرنامج الافتراضي لتشغيله) ويسمى (البرنامج الافتراضي). يتم تخزين تحديد اقتران الملفات في سجل الويندوز (Windows Registry) ويستطيع المستخدم ومدراء النظام تعديلها او أي برنامج يملك صلاحيات الوصول وتعديل على (Windows Registry) وتستطيع تعديلها من خلال أداة (assoc) بصلاحيات مدير النظام. يستطيع كما ذكرنا التطبيق تعديل التطبيق الافتراضي المرتبط من خلال استدعاء ملف معين ثم إجباره بفتح من خلال برنامج اخر.
T1546	.002	شاشة التوقف/ Screensaver	قد يقوم المهاجمون باستغلال شاشة التوقف (عدم نشاط المستخدم) لتنفيذ تعليمات برمجية ضارة بهدف البقاء داخل النظام المخترق أطول فترة ممكن. وشاشات التوقف هي برمجيات يتم تنفيذها بعد عدم نشاط المستخدم على الكمبيوتر بواسطة وقت تم تحديده مسبقاً من الاعدادات. وتأتي امتداداتها بصيغة (.scr). تستطيع إيجاد ملفات شاشات التوقف في هذا المسار(C:\Windows\System32\, او C:\Windows\sysWOW64\) وفي نظام من نوع (bit-64) يأتي مع حافظات الشاشة او شاشات التوقف المثبتة بشكل تلقائي مع الويندوز.
T1546	.003	Windows Management Instrumentation Event Subscription	قد يقوم المهاجمون بتصعيد الصلاحيات او تشغيل ملفات ضارة باستخدام (Windows Management Instrumentation subscription (WMI) event) وذلك بهدف البقاء داخل الشبكة المخترقة أطول فترة ممكنة او تصعيد الصلاحيات. ويمكن استخدام الاحداث (Event) مع (WMI) بغرض تنفيذ الاكواد عند تحديد وقت حدوث الحدث. على سبيل المثال(تفعيل الاحداث عندما يقوم المستخدم بتسجيل الدخول ..الخ)
T1546	.004	Unix Shell Configuration Modification	قد يقوم المهاجمون باستغلال الأوامر التي تتم بواسطة المستخدم لتنفيذ تعليمات برمجية ضارة بهدف البقاء داخل المنظمة أكبر قدر ممكن. يقوم نظام (Unix Shells) بتنفيذ وجدولة العديد من الاعمال والاعدادات والسكربتات والاحداث. على سبيل المثال (عندما يقوم المستخدم بالتفاعل مع واجهة سطر الأوامر او استخدام (SSH)). فمن خلال المثال السابق يتم التواصل باستخدام (Shell). ويقوم (Shell) حينها بتفعيل السكربتات الخاصة بالنظام والمتواجدة في(/etc) والمجلد الرئيسي الخاص بالمستخدم (~ /) من اجل تهيئة البيئة الخاصة به. وعادة يتم تهيئة البيئة للمستخدمين عند تسجي الدخول للنظام من خلال (/etc/profile). يتم تفعيل هذه السكربتات والاوامر من خلال مستويات من الاذونات تم اعدادها مسبقاً. ان هذه السكربتات ومع وجود الصلاحية والاذونات المناسبة كما ذكرنا يستطيع المستخدم تعديل البيئة الخاصة به
T1546	.005	Trap	قد يقوم المهاجمين بتشغيل التعليمات الضارة بواسطة (interrupt signal). يقوم الامر(Trap) بالسماح بالبرامج و(Shells) بتخصيص الأوامر التي سيتم تفعيلها عند استقبال (interrupt signal)، والاستخدام الشائع لهذه الطريقة هو سكربت يسمح للبرامج بالتفاعل عند حصول (interrupt signal) مثل عند عملية (القص/الصق) في لوحة المفاتيح.
T1546	.006	LC_LOAD_DYLIB Addition	قد يقوم المهاجمين بتشغيل التعليمات الضارة بواسطة (tainted binaries) او (Mach-O binaries) وهي تحتوي على تعليمات برمجية تستخدم لإجراء عمليات معينة عند تحميل (binary). تقوم التعليمات في (LC_LOAD_DYLIB) في (Mach-O binaries) لنظامي (MacOS, OS X) بالتواصل مع المكتبات الديناميكية او ما تسمى بـ(dylibs) التي يتم تحميلها اثناء ووقت تنفيذ تلك العمليات. وتستطيع استخدام هذه (complied binary) بشكل خاص باشتراط وجود الاعدادات والتوافقية الصحيحة. وهناك أدوات كثير تستطيع القيام بهذا العمل من التغيرات.
T1546	.007	Netsh Helper DLL	يقوم المهاجمين بتنفيذ تعليمات برمجية ضارة بهدف البقاء داخل الشبكة أطول فترة ممكنه من خلال تشغيل مكتبات والاعتماد على (Netsh Helper DLLs) لتنفيذها. برمجية (Netsh.exe) او ما تعرف بي(Netshell). هي عبارة عن سطر أوامر تقوم بالتفاعل مع

			اعدادات الشبكة والأنظمة. وهي تحتوي على وظائف و أدوات لإضافة (helper DLLs) وتستطيع اضافة المزيد من القدرات والوظائف لها. وتستطيع إيجاد المسار الخاص بها في الويندوز (Windows Registry) في (HKLM\SOFTWARE\Microsoft\Netsh).
T1546	.008	Accessibility Features	قد يقوم المهاجم بتنفيذ تعليمات برمجية يتم تفعيلها بواسطة مميزات وامكانيات الوصول المتاحة بواسطة مايكروسوفت او ما يسمى (accessibility features) وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات. ويحتوي نظام ويندوز على مميزان إمكانية الوصول والتي يمكن تشغيلها باستخدام مجموعة من المفاتيح قبل عملية تسجيل الدخول للمستخدم على سبيل المثال(عندما يكون المستخدم على شاشة تسجيل الدخول). قد يقوم المهاجم بتعديل هذه البرمجيات واضافة سطر الأوامر والتي تسمح له بالتحكم والسيطرة من دون الحاجة الى تسجيل الدخول للنظام بشكل فعلي.
T1546	.009	AppCert DLLs	قد يقوم المهاجم بتنفيذ تعليمات برمجية يتم تشغيله بواسطة (AppCert DLLs) والتي يتم تفعيلها من ضمن العمليات (processes). وذلك بهدف رفع الصلاحيات. ان (Dynamic-link libraries (DLLs))هي احد مكونات (AppCertDLLs) والمتواجدة في (HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\) والتي يتم استدعائها في كل وظائف واجهة برمجة التطبيقات (API) بهدف انشاء العمليات، انشاء العمليات مستخدمين و (reateProcess, CreateProcessAsUser ,CreateProcessWithLoginW, CreateProcessWithTokenW, or WinExec.)
T1546	.010	AppInit DLLs	قد يقوم المهاجمين بتنفيذ تعليمات برمجية ضارة بهدف رفع الصلاحيات وتحدث العملية إثناء تحميل العمليات الخاصة بـ(AppInit DLLs). ان (Dynamic-link libraries (DLLs))هي احد مكونات (AppInit_DLLs) والمتواجدة في (HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows or HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows are loaded by user32.dll) والتي يتم استدعائها في كل وظائف والعمليات التي يتم تحميلها الى (user32.dll). وعلى الاغلب ان جميع البرامج تستخدم هذه العمليات حيث ان مكتبة (user32.dll) مكتبة شائعة ومستخدمة بكثرة.
T1546	.011	Application Shimming	قد يقوم المهاجمين بتشغيل تعليمات برمجية ضارة بهدف رفع الصلاحيات وذلك من خلال الاستفادة من ما يسمى بـ(application shims) او (Application Shim Microsoft Windows Application Compatibility (Infrastructure/Framework)). وتم عمله للسماح بالتوافق مع إصدارات ويندوز القديمة وجعل البرمجيات تعمل حتى مع اصدار احدث. على سبيل المثال (ان هذه التقنية تسمح للمطورين بتطبيق الإصلاحات والتطوير دون الحاجة الى إعادة كتابة البرامج من جديد) والمثال السابق في حل تم كتابة برنامج لويندوز XP وجعلة قابل للعمل على ويندوز ١٠
T1546	.012	Image File Execution Options Injection	قد يقوم المهاجم بتنفيذ تعليمات برمجية ضارة من خلال (Image File Execution Options (IFEO) debuggers) وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات. تقوم (IFEO) بتمكين المطورين من ارفاق مصحح الأخطاء مع التطبيق او البرمجية. فعند القيام باي عملية سيكون مصحح الأخطاء موجود من ضمن (IFEO) للتطبيق. والتي تودي الى انشاء عملية جديدة من ضمن مصحح الأخطاء. على سبيل المثال (C:\dbg\ntsd.exe -g notepad.exe).
T1546	.013	PowerShell Profile	قد يقوم المهاجم بتنفيذ تعليمات برمجية ضارة من خلال استغلال التفاعل مع (PowerShell profiles) وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات. ان (profile.ps1) هو سكربت يعمل حينما يقوم (PowerShell) بالعمل. وتستطيع من خلاله تخصيص البيئة الخاصة بالمستخدم.
T1546	.014	Emond	قد يقوم المهاجم بتنفيذ تعليمات برمجية ضارة باستخدام (Event Monitor Daemon (emond)) وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات. يقوم (emond) بتنفيذ الاحداث (event) من مختلف الخدمات ويقوم بإداراتها من خلال محرك بسيط يقوم من خلاله باتخاذ الإجراءات المناسبة. ويقوم (emond binary) في مجلد (sbin/emond/) بتحميل جميع القواعد من مستودع (/etc/emond.d/rules/) ويقوم بعد ذلك باتخاذ الإجراءات حسب الاحداث المحددة له.

T1546	.015	Component Object Model Hijacking	قد يقوم المهاجم بتنفيذ تعليمات برمجية ضارة من خلال اختطاف وسرقة (Component Object Model (COM)) عند تشغيله. ان (COM) هو احد مكونات نظام الويندوز حيث يقوم بتمكين التفاعل ما بين البرمجيات ونظام التشغيل. ويتم تخزين مختلف (COM) في (Registry).
T1068		Exploitation for Privilege Escalation	قد يقوم المهاجمين باستغلال نقاط الضعف في البرمجيات وذلك بهدف تصعيد الصلاحيات. ان استغلال الثغرات او نقاط الضعف في البرمجيات حدث عندما يقوم المهاجم باستغلال نقاط الضعف الناشئة عن خلل برمجي او خطا في تنفيذ الخدمات او ثغرة برمجية على مستوى النواه الخاصة بالنظام او البرامج الأساسية في نظام التشغيل. وغالباً ما تعيق المهاجمين من التقدم في اختراق المنظمة المستهدفة هي الصلاحيات والاذونات الممنوحة للوصول لنظام او تقنية معينه، لذلك من المحتمل ان يقوم المهاجمين باستغلال هذه الثغرات لرفع صلاحياتهم.
T1574		انتحال مجال التنفيذ / Hijack Execution Flow	قد يقوم المهاجمين بتنفيذ تعليمات برمجية ضارة تقوم باختطاف وسرقة الالية التي يقوم النظام بتشغيل البرمجيات بها. ان(Hijack Execution Flow) قد يتم استخدامه للبقاء داخل الشبكة بشكل مستمر للمهاجم، حيث ان (Hijack Execution Flow) يعمل بشكل مستمر. وقد يقوم المهاجمين كذلك باستخدام هذه الميزة لرفع الصلاحيات او التهرب من الاكتشاف .
T1574	.001	DLL Search Order Hijacking	قد يقوم المهاجمين باعتراض طلبات البحث (search order) لتنفيذ تعليماتهم البرمجية الضارة DLLs، وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات. ان نظام ويندوز يستخدم طريقة شائعة في عملية البحث عن مكتبات DLL المطلوب تحميلها في احد البرامج او التطبيقات. وقد يستخدم المهاجمين هذه الميزة لتنفيذ اغراضهم الخبيثة.
T1574	.002	DLL Side-Loading	قد يقوم المهاجمين بتحميل مكتباتهم (DLL) الضارة للنظام. وتتشابه هذه الهجمة مع الهجمة السابقة (DLL Search Order Hijacking). ويختلف (side-loading) عنه انه يقوم بتحميل تلك DLL بدل من زرعها ضمن الترتيب الخاص بالبحث عن DLL ثم انتظار النظام او الضحية من استدعائها. وقد يقوم المهاجمون بهذه الطريقة من خلال زرعها ثم يقوم المهاجم باستدعائها من خلال برمجيات معتمدة وغير ضارة.
T1574	.004	Dylib Hijacking	قد يقوم المهاجم بتنفيذ تعليماته البرمجية الضارة من خلال وضعها داخل (dylib) (dynamic library)) مع اسم متوقع من التطبيق المراد استهدفه ان يقوم بتشغيلها. ان (dylib) (dynamic library)) ستقوم بالبحث ومحاولة إيجاد (dylib) بناء على الترتيب التسلسلي للمسارات/الامتدادات الخاصة بعمليات البحث. وقد تكون المسارات التي تؤدي الى(dylib) مسبوقة بـ(@rpath). و(@rpath) هي التي تسمح للمطورين بتحديد مجموعة المسارات الخاصة بالبحث وقت التنفيذ. وبالإضافة الى ذلك اذا لم يتم ربطها بالشكل المناسب مثل استخدام (LC_LOAD_WEAK_DYLIB). سيستمر البرنامج بتنفيذ التعليمات حتى في حال عدم وجود(dylib) المتوقع. مما يتيح للمطورين من تشغيل تطبيقاتهم على إصدارات متعددة من (macOS) مع إضافة واجهات برمجة تطبيقات جديدة (API).
T1574	.005	Executable Installer File Permissions Weakness	قد يقوم المهاجمين بتنفيذ تعليماتهم البرمجية الضارة من خلال اعتراض او سرقة (binaries) المستخدم في عملية التثبيت. وقد تتم هذه العملية بشكل تلقائي من خلال تنفيذ بعض (binaries) من اثناء عملية التثبيت. في حال كانت الصلاحيات /الاذونات الخاصة بمجلدات النظام التي تحتوي على (binaries) المستهدف في العملية. او الصلاحيات/الاذونات الخاصة بنفس (binaries) تم اعدادها بشكل غير صحيح. فقد يقوم (binaries) بإعادة كتابة نفسه فوق (binaries) اخر باستخدام الاذونات والصلاحيات الممنوحة له. وفي بعض الأحيان قد يعمل في اعلى صلاحيات والتي قد تتضمن صلاحيات (SYSTEM).
T1574	.006	Dynamic Linker Hijacking	قد يقوم المهاجمين بتشغيل وتنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة المتغيرات(Variables) في البيئة من خلال استخدام (dynamic linker) لإضافتها للمكتبات المشتركة او ما يسمى بـ(libaraies Shared). من خلال عمليات التحضير لتنفيذ او تشغيل البرنامج. ويقوم (linker dynamic) بتحميل مسارات الخصائص البيئية للمكتبات المشتركة من خلال المتغيرات البيئية (environment variables) والملفات مثل (LD_PRELOAD) في نظام لينكس او (DYLD_INSERT_LIBRARIES) في نظام MacOs. يتم إعطاء أولوية تحميل المكتبات التي تم تحديدها اولاً، حتى يتم أعطاها أولوية على مكتبات النظام التي لها نفس الاسم

T1574	.007	Path Interception by PATH Environment Variable	قد يقوم المهاجمين بتشغيل او تنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة المتغيرات (variables) التي يتم تحميلها في المكتبات. قد يقوم المهاجم بوضع برنامجه من المقدمة في القائمة المخزنة في مسارات البيئة (PATH environment variable). والتي سيقوم نظام التشغيل ويندوز بتشغيله عند عملية البحث بشكل تسلسلي باستخدام قائمة (PATH) والتي يتم استدعائها من خلال سكربت او سطر الأوامر.
T1574	.008	Path Interception by Search Order Hijacking	قد يقوم المهاجمين بتشغيل او تنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف ترتيب البحث والذي من المفترض انه يستدعي برنامج اخر. ونظراً ان بعض البرامج لا تستدعي برامج أخرى باستخدام قائمة (PATH)، قد يقوم المهاجم بوضع ملفاته في القائمة التي سيتم استدعاء البرمجيات منها. والتي سيتسبب بجعل النظام بتشغيل برنامجه الضار بسبب استدعاء برنامج اخر له.
T1574	.009	Path Interception by Unquoted Path	قد يقوم المهاجمين بتشغيل او تنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف المراجع الخاصة بالملفات. قد يستغل المهاجم المسارات الغير محدده بعلامات الاقتباس ("") والتي من خلالها يقوم بوضع تعليماته البرمجية التنفيذية في اعلى القائمة في (PATH). والتي عندما يقوم نظام التشغيل الويندوز بالاختيار من القائمة سيقوم بتشغيله.
T1574	.010	Services File Permissions Weakness	قد يقوم المهاجمين بتشغيل تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة (binaries) التي يتم استخدامها من قبل الخدمات. يستغل المهاجمين سير العمل (Flaws) الخاصة بالصلاحيات لنظام الخدمات في الويندوز لاستبدال (binaries) التي يتم تنفيذها عند تنفيذ الخدمات. وبعض الخدمات قد يتم تفعيلها بشكل تلقائي بواسطة (binaries) مخصص لتنفيذ وظيفة محددة. اذا تم تحديد الصلاحيات المجلد الذي يحتوي على (binaries) المستهدف او الصلاحيات على (binaries) بذاته، فقد يقوم المهاجم بالكتابة فوقة بالصلاحيات الممنوحة له في المجلد او (binaries) بذاته والتي قد تكون صلاحيات عالية او صلاحيات النظام (SYSTEM) التي تسمح له بهذا العمل والتنفيذ.
T1574	.011	Services Registry Permissions Weakness	قد يقوم المهاجمين بتشغيل تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة مدخلات (Registry) المستخدمة من قبل الخدمات في النظام. يستغل المهاجمين سير العمل (Flaws) الخاصة بالصلاحيات لنظام لل(Registry) في الويندوز لاعادة تنفيذ التعليمات البرمجية الأصلية للبرمجيات التي يتحكم بها. والتي يستخدمها لتشغيل الاكواد الضارة من خلال الخدمات. ويقوم نظام ويندوز بحفظ الخدمات المحلية والاعدادات الخاصة بها في (HKLM\SYSTEM\CurrentControlSet\Services) والخدمات التي يتم تخزينها في (Registry keys) قد يتم التلاعب بها او تعديلها لجعلها تقوم بتنفيذ الخدمات الضارة والتي من شأنها ات تقوم بتشغيل أدوات او تنفيذ تعليمات برمجية او تشغيل PowerShell او Reg. ويتم التحكم في الوصول الى (Registry keys) من خلال قوائم التحكم في الوصول والاذونات (Access Control Lists and permissions).
T1574	.012	COR_PROFILER	قد يستغل المهاجمين المتغيرات في البيئة لـ (COR_PROFILER) والتي قد تؤدي الى اختطاف/سرقة آلية عمل البرنامج والتي تقوم بتحميلها الى .NET CLR. ان (COR_PROFILER) هي احد المميزات لاطار (.Framework NET) والتي تسمح للمطورين بتحديد ملفات التعاريف .NET. DLL/External الغير مدارة (unmanaged) ليتم تحميلها في كل عملية من عمليات .NET CLR. وتم إيجاد وتصميم ملفات التعريف لمراقبة وتصحيح الأخطاء البرمجية التي يتم تنفيذها بواسطة .NET CRL.
T1055		حقن العمليات / Process Injection	قد يقوم المهاجمين بحقن العمليات وذلك بهدف رفع الصلاحيات او التهرب من الاكتشاف. وقد تستخدم حقن العمليات لتنفيذ تعليمات ضارة في بعض العمليات النشطة. والتي قد تسمح بحقن والوصول الى العمليات في الذاكرة العشوائية (Memory) او النظام او الشبكة. وتعتبر عملية حقن العمليات من الأساليب المتبعة من قبل المهاجمين حيث انها تعمل وكأنها عملية طبيعية وغير ضارة.
T1055	.001	Dynamic-link Library Injection	قد يقوم المهاجمين بحقن (libraries (DLLs dynamic-link) داخل العمليات وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن DLL تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة

T1055	.002	حقن البرمجيات الجاهزة للعمل / Portable Executable Injection	قد يقوم المهاجمين بحقن (PE) داخل العمليات وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن PE تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1055	.003	Thread Execution Hijacking	قد يقوم المهاجمين بحقن بعض البرمجيات الضارة في العمليات التي يتم اختطافها وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (Thread Execution Hijacking) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة.
T1055	.004	Asynchronous Procedure Call	قد يقوم المهاجمين بحقن بعض البرمجيات الضارة في العمليات النشطة من خلال asynchronous procedure call (APC) وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (APC) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة.
T1055	.005	Thread Local Storage	قد يقوم المهاجمين بحقن بعض البرمجيات الضارة في العمليات النشطة من خلال (thread local storage (TLS)وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (TLS callback) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة.
T1055	.008	Ptrace System Calls	قد يقوم المهاجمين بحقن بعض البرمجيات الضارة في العمليات النشطة من خلال (processes via ptrace (process trace system calls) وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (Ptrace system call) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة.
T1055	.009	Proc Memory	قد يقوم المهاجمين بحقن برمجيات ضارة عبر استخدام (Proc) لملفات النظام وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (Proc memory) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1055	.011	Extra Window Memory Injection	قد يقوم المهاجمين بحقن برمجيات ضارة عبر استخدام (Extra windows memory EWM) لملفات النظام وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (EWM) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1055	.012	Process Hollowing	قد يقوم المهاجمين بحقن برمجيات ضارة عبر استخدام عمليات تم ايقافها وتسمى بـ(hollowed processes) وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (hollowed processes) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1055	.013	Process Doppelgänging	قد يقوم المهاجمين بحقن برمجيات ضارة عبر استخدام (process doppelgänging) وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (process doppelgänging) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1055	.014	VDSO Hijacking	قد يقوم المهاجمين بحقن برمجيات ضارة عبر استخدام اختطاف او انتحال (VDSO) وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (VDSO او Virtual dynamic shared object) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1053		جدولة الاعمال والمهام / Scheduled Task/Job	قد يقوم المهاجمين باستغلال وظائف الجدولة او ما يسمى بـ(Scheduled Task/Job) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. ان (Scheduled Task/Job) هي أداة متوفرة في اكثر أنظمة التشغيل وذلك بهدف جدولة تشغيل البرمجيات السكربتات عند تاريخ او وقت محدد. وتستطيع كذلك الجدولة عن بعد في حال توفرت لديك الصلاحيات المناسبة على سبيل المثال للجدولة عن بعد ((RPC: ex Windows in sharing printer and file and environments)). وعلى الاغلب ان جدولة الاعمال عن بعد تستلزم وجود المستخدم في مجموعة مدراء النظام او ان يكون لدى المستخدم بعض الصلاحيات العالية على النظام البعيد.
T1053	.001	بيئة لينكس / At (Linux)	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال في نظام لينكس وتسمى (at) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. ان الامر (at) يتم استخدامه فقط من قبل مدراء النظام لجدولة الاعمال كما تم ذكره.
T1053	.002	بيئة ويندوز / At ((Windows	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال في نظام ويندوز وتسمى (at.exe) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. ان الامر (at.exe) متوفر كبرمجية تنفيذية هدفها جدولة الاعمال

T1053			لنظام ويندوز لكي تعمل في وقت او تاريخ محدد. ويتطلب استخدام (at.exe) تفعيل خدمة (Scheduler Task). وان يتم استخدام احد الحسابات التي في مجموعة مدراء النظام.
T1053	.003	Cron	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال وتسمى (cron) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. ان الامر (cron) تعمل حسب الوقت المحدد لها وهي موجهه لنظام (Unix). وتحتوي (crontab) على جدول الادخالات الخاصة بـ(cron) والاوقات المراد تشغيلها به والمسارات المطلوب تفعيلها او الملفات التنفيذية.
T1053	.004	Launchd	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال وتسمى (Launchd daemon) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. ان الامر (Launchd) موجهه لنظام (macOS). وهي مسؤولة عن تحميل واداة الخدمات الخاصة بنظام التشغيل. ان عملية تحميل (parameters) لكل عملية تشغيل لل(Launchd) تتم بشكل خفي ويتم قراءتها من قائمة مخصصة او ما تسمى بـ(plist) و المتواجدة في (/ System/Library/LaunchDaemons and /Library/LaunchDaemons/). وتحتوي (LaunchDaemons) على قائمة يتم الإشارة لكل ملف تنفيذي والمسار الخاص به الذي سيتم تنفيذ البرمجية منه.
T1053	.005	جدولة الاعمال / Scheduled Task	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال وتسمى (Windows Task Scheduler) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. توجد طرق متعددة للوصول الى (Windows Task Scheduler) في نظام ويندوز. تستطيع الوصول لها بشكل مباشر من سطر الاوامر او من خلال الواجهة الرسومية الخاصة بأدوات مدراء النظام من لوحة التحكم. وفي بعض الأحيان قد يقوم المهاجمين بتفعيلها من خلال (.NET wrapper) وقد يتم استخدام (netapi32) في المكتبات الخاصة بنظام ويندوز.
T1053	.006	Systemd Timers	قد يقوم المهاجمين باستغلال أداة جدولة الاعمال وتسمى (systemd timers) وذلك بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق. أداة (systemd timers) هي عبارة عن ملفات بامتدادات يرمز لها بـ(.timer) والتي يتم التحكم بالخدمات من خلالها و (systemd timers) قد يتم استخدامه لتنفيذ الاحداث الخاصة بالتقويم. ويمكن استخدامها كبديل لـ(Cron) في نظام لينكس.
T1078		حساب فعال / Valid Accounts	قد يقوم المهاجم باستغلال بيانات الاعتماد للحسابات الفعالة وذلك بهدف الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. ان بيانات الاعتماد المخترقة قد يستخدم لتخطي عناصر التحكم بالوصول (access controls) التي تم تطبيقها على الأنظمة والموارد الخاصة بالشبكة. وقد يتم استخدام هذه الحسابات للوصول للأنظمة عن بعد او الخدمات مثل VPN او البريد الالكتروني او سطح المكتب البعيد من خلال المتصفح. وقد يتم استخدام بيانات الاعتماد المخترقة لتصعيد الصلاحيات لأنظمة محدد او الوصول الى منطقة حساسة داخل الشبكة المستهدفة. وقد يقوم المهاجم بتنفيذ عملياته الضارة ببيانات الاعتماد المخترقة دون الحاجة الى تبيث بعض البرمجيات الضارة والتي قد تؤدي الى اكتشافه.
T1078	.001	حساب افتراضي / Default Accounts	قد يقوم المهاجم بالحصول على بيانات الاعتماد للحسابات الافتراضية في النظام والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. ان الحسابات الافتراضية هي التي يتم انشاءها بشكل افتراضي داخل الأنظمة مثل حساب (Guest او Administrator) في نظام ويندوز. الحسابات الافتراضية قد تأتي كذلك من الأنظمة الخاصة ببعض العتاد من الشركة المصنعة. والتي قد تكون حساب مدير للنظام. ان حساب مدير النظام الخاص بخدمات (AWS) وحساب الخدمات الافتراضي في (Kubernetes)
T1078	.002	حساب مدير النظام / Domain Accounts	قد يقوم المهاجمين باستغلال بيانات الاعتماد الخاصة بمدراء النطاق (domain account) والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. ان حسابات مدراء النطاق والتي يتم التحكم بها

			من قبل (Service Active Directory Domain) والتي من خلالها يتم إعطاء الصلاحيات و التكوين لخدمات للنظام. ومن الممكن ان تكون حسابات مدراء. النظام عبارة عن حسابات مستخدمين او خدمات.
T1078	.003	حساب محلي / Local Accounts	قد يقوم المهاجمين باستغلال بيانات الاعتماد الخاصة بالحسابات المحلية (local account) والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. الحسابات المحلية يتم اعدادها من قبل المنظمة بهدف تقديم خدمات الدعم للأنظمة عن بعد او لتفعيل بعض الخدمات الوصول للأنظمة و ادارتها.
T1078	.004	حساب الخدمات السحابية / Cloud Accounts	قد يقوم المهاجمين باستغلال بيانات الاعتماد الخاصة بالحسابات على الخدمات السحابية (cloud account) والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. حسابات الخدمات السحابية قد يتم انشاءها واعدادها من قبل المنظمة بهدف تقديم خدمات الدعم للأنظمة عن بعد او لتفعيل بعض الخدمات الوصول للأنظمة وادارتها او التطبيقات. قد يتم توحيد الحسابات الخاصة بالخدمات السحابية مع الحسابات في النطاقات (Window Active Directory)

التهرب من الاكتشاف / Defense Evasion

التهرب من الاكتشاف: غالباً ما يقوم المهاجمين بالتهرب من الاكتشاف بعد عملية الاختراق باستخدام أساليب متعددة. وقد تشتمل تلك العمليات على الغاء تثبيت او تعطيل الخدمات/الأجهزة/الأنظمة/التطبيقات الأمنية. او تشفير وترميز البيانات والسكربتات. وقد يقوم المهاجم باستغلال الثقة في بعض العمليات المعروفة داخل النظام لإخفاء برمجياته الضارة. وبعض التقنيات التي قد يستخدمها المهاجم لتخريب الدفاعات.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1548		اساءة استخدام ميزة رفع الصلاحيات / Elevation Control Abuse Mechanism	قد يقوم المهاجم بالتلاعب واستغلال آليات التحكم في رفع الصلاحيات للحصول على صلاحيات او أذونات اعلى. وتحتوي معظم أنظمة التشغيل الحديثة على آلية لتحكم في الصلاحيات والتي تهدف الى رفع او التحكم في الصلاحيات لحساب او خدمة محددة من اجل أداء المهام المطلوب تنفيذها على النظام. والتي تكون في معظم الاحول من إعطاء صلاحيات لبعض المستخدمين للقيام بمهام حساسة وحرجة تتطلب صلاحيات عالية. وقد يقوم المهاجم بطرق مشابه للاستفادة من طرق رفع الصلاحيات المتوفرة مع النظام من اجل رفع الصلاحيات الخاصة به.
T1548	.001	Setuid and Setgid	قد يقوم المهاجمين باستخدام ما يسمى بـ(shell escapes) او استغلال الثغرات في التطبيقات مع ما يطلق عليه (setuid) او (setgid bits) وذلك بهدف الحصول على كود ضار يعمل في حسابات مستخدمين اخرين. ان في نظام (لينكس او ماك او اس). عندما يتم تعين (setuid او setgid bits) لاحد التطبيقات، سيعمل التطبيق بامتيازات المستخدم او المجموعة المستهدفة. والحالة الطبيعية عند أي تشغيل التطبيق يتم تنفيذه بصلاحيات المستخدم الحالي. بغض النظر عن المستخدم المالك للتطبيق او المجموعة. ومع ذلك هناك حالات تحتاج بعض التطبيقات فيها الى تنفيذ بعض الوظائف التي تحتاج الى صلاحيات عالية حتى وان كان المستخدم لا يمتلك تلك الصلاحيات.
T1548	.002	تخطي صلاحيات التحكم بالحسابات / User Account Control Bypass	قد يقوم المهاجمين بتخطي آليات التحكم في حساب المستخدم وذلك بهدف رفع الصلاحيات على النظام. نظام ويندوز يمتلك ما يسمى بـ(Windows User Account Control (UAC)) وهي تسمح برفع الصلاحيات والتي تقوم بتتبع سلامة عمليات التصعيد من الصلاحيات الأقل الى الأعلى. وعادة ما يتم تنفيذ وتعديل والوصول تلك المهمة بصلاحيات مدير النظام والتي تأتي علي شكل (تبويب) للمستخدم لتأكيد على العملية، وذلك بهدف تنبيه المستخدمين ان هذه المهمة تتطلب صلاحيات عالية وقد تقوم بالتأثير على النظام وقد تتطلب في بعض الأحيان من مدراء النظام المحلي (Local او domain) ادخال كلمة المرور لإكمال الإجراءات.
T1548	.003	Sudo and Sudo Caching	قد يقوم المهاجم بتنفيذ (and/or use the suoders sudo caching) لرفع الصاحيات. قد يقوم المهاجمين بتنفيذ بعض الأوامر التي من شأنها استدعاء بعض العمليات التابعة لمستخدمين اخرين والاستفادة منها للحصول على صلاحيات اعلى.
T1548	.004	Elevated Execution with Prompt	قد يقوم المهاجمين من استخدام (AuthorizationExecuteWithPrivileges API) لرفع الصلاحيات من خلال استخدام الطلب من المستخدمين بيانات الاعتماد الخاصة بهم. ان الهدف من استخدام (API) هو إعطاء المطورين للتطبيقات طريقة سهله لاجراء العمليات بصلاحيات عالية جداً، على سبيل المثال تثبيت تطبيق او تحديث. حيث ان (API) لا تقوم بالتحقق من التطبيق الذى يطلب تلك الصلاحيات هل هو تطبيق ضار او غير ضار او تم تعديله.
T1134		التلاعب بالتوكن / Access Token Manipulation	قد يقوم المهاجمين بتعديل (tokens) للقيام بتنفيذ عمليات بحساب مستخدم اخر او حساب النظام (SYSTEM) وذلك بهدف تخطي آليات التحكم. يستخدم نظام ويندوز (tokens) لتحديد ملكية العمليات التي قيد التشغيل. ويمكن للمستخدم من التلاعب بـ(tokens) لتظهر العملية التي قيد التشغيل كما انها لو كانت تابعة لمستخدم اخر او تابعة لعملية أخرى (child process of a different). وعند القيام بذلك تأخذ هذه العملية سياق الأمان المرتبطة بـ(tokens) الجديد الذي تم ربطه به.
T1134	.001	Token Impersonation/Theft	قد يقوم المهاجمين بانتحال او بتكرار (token) الخاص بمستخدم أخرى وذلك بهدف رفع الصلاحيات او تخطي آليات التحكم. المهاجمين يستطيعون انشاء وتكرار (token) الموجود باستخدام (DuplicateToken(Ex)). ويمكن بعد ذلك

T1134	.002	Create Process with Token	قد يقوم المهاجمين بإنشاء عملية جديدة او تكرار (token) بهدف رفع الصلاحيات او تخطي آليات التحكم. يمكن للمهاجمين من تكرار (token) باستخدام DuplicateToken(Ex) و يستخدمها مع CreateProcessWithTokenW بهدف انشاء عملية جديدة تحت المستخدم المنتحل. هذه الطريقة مفيدة جداً لإنشاء العمليات تحت حسابات مستخدمين اخرين.
T1134	.003	Make and Impersonate Token	قد يقوم المهاجمين بإنشاء او انتحال (tokens) بهدف رفع الصلاحيات او تخطي آليات التحكم. في حال كان لدى المهاجم اسم مستخدم وكلمة مرور ولكن المستخدم لم يقم بتسجيل الدخول للنظام، فيمكن للمهاجم من انشاء جلسة (Session) للمستخدم باستخدام وظيفة (LogonUser). هذه الوظيفة ستقوم باستعادة نسخة من رمز (tokens) الخاصة بالجلسة ويقوم المهاجم بعد ذلك باستخدام (SetThreadToken) لربط (tokens) بـ(thread) مخصص.
T1134	.004	Parent PID Spoofing	قد يقوم المهاجمين بانتحال (identifier (PPID parent process)) لعملية جديدة (New process) بهدف التخفي من عملية (مراقبة العمليات) او لرفع الصلاحيات. وعادة ما يتم انشاء العمليات الجديدة مباشره من بواسطة (parent او calling) مالم يتم تحديد مكان الاستدعاء بشكل واضح. ان أحد الطرق لتعيين (PPID) بشكل واضح لعملية جديدة هي عبر استدعاء (call CreateProcess API)، والذي يدعم (parameter) لتحديد (PPID) ومن ثم استخدامه. يتم استخدام هذه الوظيفة في نظام ويندوز بواسطة (Windows features) على سبيل المثال (UAC) والتي تقوم بتصحيح عملية (PPID) بعد عملية طلب رفع صلاحية تلك العملية واستدعائها بواسطة (SYSTEM) والتي تتم عادة من خلال (svchost.exe or consent.exe) بدلاً من استخدام صلاحيات المستخدم نفسه.
T1134	.005	SID-History Injection	قد يقوم المهاجم باستخدام (Injection SID-History) بهدف رفع الصلاحيات او تخطي آليات التحكم. ان (Windows identifier (SID security)) هو قيمة فريدة تستخدم لتعريف حسابات (المستخدم/المجموعة). ان (SID) تستخدم بواسطة تقنيات الأمان في نظام ويندوز وكذلك تقنية (Tokens). حيث يمكن للحساب الاحتفاظ بـ(SID) في (SID-History Active Directory) والتي تسمح بعملية تسمى بـ(inter-operable) والتي تسمح باستخدام/تبادل الحسابات/المعلومات بين النطاقات (Domains). على سبيل أمثال (تضمين جميع القيام الخاصة بـ(tokens access) في (SID-History).
T1197		وظائف BITS Jobs	قد يقوم المهاجمين باستخدام وظائف (BITS) لتنفيذ تعليمات برمجية ضارة او استخدامها لمسح الاثار التي يخلفها المهاجم. ان خدمة (Windows Background Intelligent Transfer Service (BITS) هي عبارة عن آلية لنقل الملفات بشكل غير متزامنة وذات نطاق ترددي منخفض ويتم استعراضها من خلال (COM). ويتم استخدام (BITS) بشكل شائع من قبل المراسلين (messengers) او أي تطبيق يفضل العمل في الخلفية ويستخدم (idle bandwidth) من غير مقاطع أي بروتوكول أخرى يعمل بالشبكة. ويتم تنفيذ مهام نقل الملفات من خلال وظائف (BITS)، والتي تحتوي على قائمة انتظار لملف واحد او اكثر من ملف.
T1140		فك الترميز من الملفات او المعلومات Deobfuscate/Decode Files or Information	قد يقوم المهاجم باستخدام تقنيات من شأنها ترميز وتشفير الهجمات التي يقوم بها وذلك بهدف التخفي من الاكتشاف او تصعيب عملية التحليل، والتي قد تحتاج الى برمجيات او طرق خاصة لعكس العملية وفك الترميز او التشفير. وقد يستخدم المهاجمون طرق متعددة في عملية الترميز او التشفير والتي قد تكون مدمجة مع البرمجية الضارة او قد يقوم باستخدام احد الخدمات التي تكون متاحة مع النظام المستهدف.
T1610		تثبيت المستودعات / Deploy Container	قد يقوم المهاجمون بتثبيت المستودعات داخل المنظمة المستهدفة بهدف تنفيذ بعض الاوامر الضارة او لتفادي الاكتشاف. وفي بعض الاحيان يقوم المهاجم بتثبيت أحد المستودعات بهدف تنفيذ بعض التعليمات البرمجية المرتبطة ببعض العمليات

			الضارة مثل تنزيل او تفعيل البرمجية الضارة. وقد يقوم المهاجمون بتثبيت مستودع جديد من غير اعدادات او قواعد او صلاحيات وذلك لتفادي بعض اجهزة وانظمة الحماية المتوفرة في المنظمة.
T1006		الوصول المباشر للقرص / Direct Access Volume	قد يقوم المهاجم بالوصول الى القرص الصلب بشكل مباشر وذلك لتخطي الصلاحيات والاذونات المرتبطة بالملفات او لتفادي أنظمة المراقبة. ان نظام ويندوز يسمح للبرامج بالوصول بشكل مباشر للأقراص الصلبة بشكل مباشر. يمكن للبرمجيات التي تملك صلاحيات الوصول المباشر من قراءة وكتابة من تجاوز عناصر التحكم المرتبطة بالملفات وكذلك تخطي أنظمة المراقبة الموجودة على الملفات.
T1484		Domain Policy Modification	قد يقوم المهاجمين بتعديل الاعدادات الخاصة بتكوين النطاقات (domain) وذلك بهدف التخفي داخل الشبكة او تصعيد الصلاحيات في النطاق المستهدف. ان التقنية التي يعمل بها النطاق (domain) تسمح له بالتحكم بالأنظمة والتقنيات وكذلك المستخدمين داخل هذا النطاق وكيف تقوم هذه الأجهزة والأنظمة والمستخدمين بالتواصل، حيث يقوم بحوكمتها حسب الحاجة. والسياسة الخاصة بهذه النطاقات تحتوي على اعدادات التواصل ما بين النطاقات والنطاقات الفرعية وما في حكمها. وقد تتضمن التعديلات على السياسة الخاصة بالنطاق (GPOs) تغير على مستوى العلاقة ما بين النطاقات المرتبطة به.
T1484	.001	Group Policy Modification	قد يقوم المهاجمين بتعديل الاعدادات الخاصة بتكوين مجموعة سياسة النطاقات (GPOs) وذلك بهدف تصعيد الصلاحيات في النطاق المستهدف. تسمح سياسة النطاقات (GPOs) بتعديل و إدارة المستخدمين او الأجهزة من خلال (Active directory AD). وكما انها تعتبر مستودع للإعدادات الخاصة بسياسة النطاقات والتي تستطيع الوصول لها من خلال (\Policies\<DOMAIN>\SYSVOL\<DOMAIN>\)
T1484	.002	Domain Trust Modification	قد يقوم المهاجمين بإضافة خاصية الثقة (trusts) بين النطاقات او تعديل خصائص ثقة سابقة في النطاق المستهدف، وذلك بهدف تصعيد الصلاحيات او التخفي داخل الشبكة. تسمح تفاصيل الثقة في النطاق او (trusts) بمعرفة اذا كان هناك علاقة ما بين نطاقين مختلفين، وكذلك خصائص المصادقة والتخويل ما بين النطاقات ومعرفة الموارد المشتركة ما بينهم. وبقد تتضمن الثقة ما بين النطاقات معلومات عن الحسابات وبيانات الدخول ووسائل المصادقة المستخدمة على الخوادم والرموز(tokens).
T1480		Execution Guardrails	قد يقوم المهاجمين بتنفيذ تعليمات برمجية (guardrails) والتي تختلف باختلاف طريقة كتابة الآلية من قبل المهاجم وكذلك البيئة المستهدفة والهدف منها. حيث ان (guardrails) قد تكون تستهدف نظام محدد وذلك لتقليل لفت الانتباه للبرمجية في حال تم تحميلها من قبل أنظمة أخرى غير مستهدفة. وقد يستخدم المهاجمون معايير محددة والتي قد تتضمن أسماء لشبكات او مجلدات مشاركة او عناوين لأنظمة محددة او اسم نطاق محدد (Active Directory) او عناوين داخلية او خارجية.
T1480	.001	Environmental Keying	قد يقوم المهاجم باستخدام ما يسمى بـ (environmentally key) او برمجية ضارة وذلك بهدف التخفي وتلافي الاكتشاف حينما يكون الهجوم موجهة لنظام معين داخل الجهة المستهدفة. ان آلية (key environmentally) تستخدم طرق مشفرة لتنفيذ الأوامر حسب المتغيرات التي تحدث في البيئة والتي تم برمجيتها سابقاً من قبل المهاجم بناء على معرفة مسبقة من قبل بالبيئة الخاصة بالمستهدفة.
T1211		Exploitation for Defense Evasion	قد يقوم المهاجمين باختراق الأنظمة والتطبيقات لتخطي الحماية، تخطي الحماية تحدث عندما يقوم المهاجم باستغلال الثغرات التي تحدث عن وجود خطاء في البرنامج او أنظمة التشغيل او النواة. وقد توجد بعض الثغرات الأمنية في برامج الحماية نفسها تسمح للمهاجم بتنفيذ تعليماته البرمجية.
T1222		File and Directory Permissions Modification	قد يقوم المهاجم بتعدي الصلاحيات الخاصة بملف او مجلد محدد وذلك لتفادي سياسة التحكم في الوصول (ACLs) والوصول للملفات المحمية. ان صلاحيات الوصول للمجلدات والملفات المحمية عادة تدار بواسطة ACLs ويتم اعدادها بواسطة مدير النظام او المالك للملف او المجلد. تختلف وسائل تطبيق آليات التحكم في الوصول للملفات والمجلدات

			باختلاف النظام. ولكنها يم تحديدها بشكل صريح اما لمستخدم محدد او مجموعة محدده والتي يمكن له او يمكن لهم تنفيذ الإجراءات مثل (القراءة ، الكتابة، التنفيذ، الخ..)
T1222	.001	تعديل صلاحيات الملفات والمجلدات للويندوز / Windows File and Directory Permissions Modification	قد يقوم المهاجم بتعدي الصلاحيات الخاصة بملف او مجلد محدد وذلك لتفادي سياسة التحكم في الوصول (ACLs) والوصول للملفات المحمية. ان صلاحيات الوصول للمجلدات والملفات المحمية عادة تدار بواسطة ACLs ويتم اعدادها بواسطة مدير النظام او المالك للملف او المجلد. تختلف وسائل تطبيق آليات التحكم في الوصول للملفات والمجلدات باختلاف النظام. ولكنها يم تحديدها بشكل صريح اما لمستخدم محدد او مجموعة محدده والتي يمكن له او يمكن لهم تنفيذ الإجراءات مثل (القراءة ، الكتابة، التنفيذ، الخ..)
T1222	.002	تعديل صلاحيات الملفات والمجلدات لينكس / Linux and Mac File and Directory Permissions Modification	قد يقوم المهاجم بتعدي الصلاحيات الخاصة بملف او مجلد محدد وذلك لتفادي سياسة التحكم في الوصول (ACLs) والوصول للملفات المحمية. ان صلاحيات الوصول للمجلدات والملفات المحمية عادة تدار بواسطة ACLs ويتم اعدادها بواسطة مدير النظام او المالك للملف او المجلد. تختلف وسائل تطبيق آليات التحكم في الوصول للملفات والمجلدات باختلاف النظام. ولكنها يم تحديدها بشكل صريح اما لمستخدم محدد او مجموعة محدده والتي يمكن له او يمكن لهم تنفيذ الإجراءات مثل (القراءة ، الكتابة، التنفيذ، الخ..)
T1564		اخفاء الادلة / Hide Artifacts	قد يقوم المهاجمين بإخفاء الانشطة الخاصة بهم داخل الأنظمة لكي لا يتم اكتشافهم. حيث ان بعض الأنظمة تأتي بوظائف تساعد المهاجمين على إخفاء تلك الاحداث والأنشطة، مثل إخفاء ملفات الخاصة بالنظام او بعض المهام الخاصة بمدراء النظام من اجل ان لا يقوم المستخدمين بالعبث بها. وهذه الميزة قد تمكن المهاجم من استغلالها في إخفاء الأنشطة الخاصة بهم.
T1564	.001	اخفاء الملفات او المجلدات / Hidden Files and Directories	قد يقوم المهاجمين بعملية إخفاء لبعض الملفات او المجلدات بهدف التخفي من الاكتشاف. حيث ان هذه الميزة تمكن من إخفاء الملفات من عرضها عند قيام المستخدم بزيارة ملف محدد من خلال واجهة العرض الرسومية. وقد يحتاج المستخدمون تفعيل خيار مشاهدة الملفات المخفية لكي تظهر لهم. او من خلال سطر الأوامر استخدام (dir /a لنظام ويندوز) و (ls -a لنظام لينكس وماك او اس).
T1564	.002	اخفاء المستخدمين / Hidden Users	قد يقوم المهاجم بإخفاء بعض المستخدمين الذين تم انشاءهم حديثاً لكي يتفادى عملية الاكتشاف. حيث ان لكل مستخدم في نظام ماك او اس لديه معرف فريد مرتبط به، حيث عند انشاء أي مستخدم تستطيع مشاهدة المعرف الفريد الخاص به.
T1564	.003	اخفاء النوافذ / Hidden Window	قد يقوم المهاجم بإخفاء بعض النوافذ المفتوحة عن المستخدمين والتي عادة ما تكون هذه النوافذ ضارة، ويمكن إخفاء النوافذ التي يتم عرضها عند فتح التطبيق، والهدف من اخفاءها لتجنب من ازعاج المستخدمين وتشتيت انتباههم.
T1564	.004	NTFS File Attributes	قد يستخدم المهاجمين (NTFS) لإخفاء الأنشطة الضارة الخاصة بهم، جميع عمليات (New Technology File System) تحتوي على جزء خاص بها يحتوي على Master File Table MFT والذي يحتوي على سجل لكل ملف او مجلد في هذا الجزء. حيث ان لكل مدخل له الجزء الخاص به مع تقنية MFT على سبيل المثال Extended Attributes EA و known as one Data attribute is present Alternate Data Streams ADSs when more than والتي تستخدم لتخزين البيانات.
T1564	.005	اخفاء ملفات النظام / Hidden File System	قد يقوم المهاجم بإخفاء الملفات الخاصة بالنظام وذلك بهدف إخفاء الأنشطة الضارة عن المستخدمين وأجهزة الحماية. ان أنظمة التشغيل توضح الهيكلة لتخزين البيانات والوصول لها عند تخزينها في القرص الصلب. والتي عادة ما يتعامل المستخدمين مه نظام الملفات من خلال تطبيقات تسمح له بالوصول لتلك الملفات والمجلدات، والتي تعد بمثابة وسيلة للوصول لجزء معين من القرص الصلب. ومن امثله هذه الأنظمة AT, NTFS, ext4, and APFS وبعض الأنظمة الأخرى قد تشمل على NTFS Volume Boot Record (VBR) and Master File Table (MFT) in.

T1564	.006	Run Virtual Instance	قد يقوم المهاجمين بتنفيذ تعليمات برمجية ضارة من خلال استخدام نظام افتراضي وذلك لتجنب الاكتشاف من النظام الأساسي. ان الأنظمة الافتراضية الفرعية أصبحت مشهورة وتستخدم بكثره في المؤسسات. وتختلف طريقة الاتصال بالشبكة الخاصة بالمنظمة المستهدفة حسب طريقة عمل النظام الافتراضي وهل تم استخدامها bridged adapter وغيره، ان البيانات الشبكية التي تنشأ من الأنظمة الافتراضية قد تكون صعبه الاكتشاف.
T1564	.007	VBA Stomping	قد يقوم المهاجم بإخفاء بعض الملفات الضارة مثل (Visual Basic for Applications (VBA والتي قد يتم تضمينها من ضمن ملفات مايكروسوفت اوفيس. وقد يقوم المهاجم بإخفاء VBA ما بين النصوص الغير ضارة.
T1574		انتحال مجال التنفيذ / Hijack Flow Execution	قد يقوم المهاجمين باعتراض تشغيل البرامج لتنفيذ تعليماتهم البرمجية الضارة، وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات وقد يستغل المهاجم مثل هذه الهجمات في تخطي القيود على التنفيذ او التحكم بطريقة عمل التطبيقات داخل النظام.
T1574	.001	DLL Search Order Hijacking	قد يقوم المهاجمين باعتراض طلبات البحث (search order) لتنفيذ تعليماتهم البرمجية الضارة DLLs، وذلك بهدف البقاء داخل الشبكة أطول فترة ممكنه او تصعيد الصلاحيات. ان نظام ويندوز يستخدم طريقة شائعة في عملية البحث عن مكتبات DLL المطلوب تحميلها في احد البرامج او التطبيقات. وقد يستخدم المهاجمين هذه الميزة لتنفيذ اغراضهم الخبيثة.
T1574	.002	DLL Side-Loading	قد يقوم المهاجمين بتحميل مكتباتهم (DLL) الضارة للنظام. وتتشابه هذه الهجمة مع الهجمة السابقة (DLL Search Order Hijacking). ويختلف (side-loading) عنه انه يقوم بتحميل تلك DLL بدل من زرعها ضمن الترتيب الخاص بالبحث عن DLL ثم انتظار النظام او الضحية من استدعائها. وقد يقوم المهاجمون بهذه الطريقة من خلال زرعها ثم يقوم المهاجم باستدعائها من خلال برمجيات معتمدة وغير ضارة.
T1574	.004	Dylib Hijacking	قد يقوم المهاجم بتنفيذ تعليماته البرمجية الضارة من خلال وضعها داخل (dylib (dynamic library)) مع اسم متوقع من التطبيق المراد استهدفه ان يقوم بتشغيلها. ان (dylib (dynamic library)) ستقوم بالبحث ومحاولة إيجاد (dylib) بناء على الترتيب التسلسلي للمسارات/الامتدادات الخاصة بعمليات البحث. وقد تكون المسارات التي تؤدي الى(dylib) مسبوقة بـ(@rpath). و(@rpath) هي التي تسمح للمطورين بتحديد مجموعة المسارات الخاصة بالبحث وقت التنفيذ. وبالإضافة الى ذلك اذا لم يتم ربطها بالشكل المناسب مثل استخدام (LC_LOAD_WEAK_DYLIB). سيستمر البرنامج بتنفيذ التعليمات حتى في حال عدم وجود(dylib) المتوقع. مما يتيح للمطورين من تشغيل تطبيقاتهم على إصدارات متعددة من (macOS) مع إضافة واجهات برمجة تطبيقات جديدة (API).
T1574	.005	Executable Installer File Permissions Weakness	قد يقوم المهاجمين بتنفيذ تعليماتهم البرمجية الضارة من خلال اعتراض او سرقة (binaries) المستخدم في عملية التثبيت. وقد تتم هذه العملية بشكل تلقائي من خلال تنفيذ بعض (binaries) من اثناء عملية التثبيت. في حال كانت الصلاحيات /الاذونات الخاصة بمجلدات النظام التي تحتوي على (binaries) المستهدف في العملية. او الصلاحيات/الاذونات الخاصة بنفس (binaries) تم اعدادها بشكل غير صحيح. فقد يقوم (binaries) بإعادة كتابة نفسه فوق (binaries) اخر باستخدام الاذونات والصلاحيات الممنوحة له. وفي بعض الأحيان قد يعمل في اعلى صلاحيات والتي قد تتضمن صلاحيات (SYSTEM).
T1574	.006	Dynamic Linker Hijacking	قد يقوم المهاجمين بتشغيل وتنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة المتغيرات(Variables) في البيئة من خلال استخدام (dynamic linker) لإضافتها للمكتبات المشتركة او ما يسمى بـ(libaraies Shared). من خلال عمليات التحضير لتنفيذ او تشغيل البرنامج. ويقوم (linker dynamic) بتحميل مسارات الخصائص البيئية للمكتبات المشتركة من خلال المتغيرات البيئية (environment variables) والملفات مثل (LD_PRELOAD) في نظام لينكس او (DYLD_INSERT_LIBRARIES) في نظام MacOs. يتم إعطاء أولوية تحميل المكتبات التي تم تحديدها اولاً، حتى يتم أعطاها

			أولوية على مكتبات النظام التي لها نفس الاسم الوظيفي. وعادة ما يتم استخدام هذه المتغيرات من قبل المطورين لتصحيح الأخطاء دون الحاجة الى عمل (recompile). ويتم تنفيذ وظائف مخصصة دون الحاجة الى تغير أي من المكتبات الاصلية.
T1574	.007	Path Interception by PATH Environment Variable	قد يقوم المهاجمين بتشغيل او تنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة المتغيرات (variables) التي يتم تحميلها في المكتبات. قد يقوم المهاجم بوضع برنامجه من المقدمة في القائمة المخزنة في مسارات البيئة (PATH environment variable). والتي سيقوم نظام التشغيل ويندوز بتشغيله عند عملية البحث بشكل تسلسلي باستخدام قائمة (PATH) والتي يتم استدعائها من خلال سكربت او سطر الأوامر.
T1574	.008	Path Interception by Search Order Hijacking	قد يقوم المهاجمين بتشغيل او تنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف ترتيب البحث والذي من المفترض انه يستدعي برنامج اخر. ونظراً ان بعض البرامج لا تستدعي برامج أخرى باستخدام قائمة (PATH)، قد يقوم المهاجم بوضع ملفاته في القائمة التي سيتم استدعاء البرمجيات منها. والتي سيتسبب بجعل النظام بتشغيل برنامجه الضار بسبب استدعاء برنامج اخر له.
T1574	.009	Path Interception by Unquoted Path	قد يقوم المهاجمين بتشغيل او تنفيذ تعليماتهم البرمجية الضارة من خلال اختطاف المراجع الخاصة بالملفات. قد يستغل المهاجم المسارات الغير محدده بعلامات الاقتباس ("") والتي من خلالها يقوم بوضع تعليماته البرمجية التنفيذية في اعلى القائمة في (PATH). والتي عندما يقوم نظام التشغيل الويندوز بالاختيار من القائمة سيقوم بتشغيله.
T1574	.010	Services File Permissions Weakness	قد يقوم المهاجمين بتشغيل تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة (binaries) التي يتم استخدامها من قبل الخدمات. يستغل المهاجمين سير العمل (Flaws) الخاصة بالصلاحيات لنظام الخدمات في الويندوز لاستبدال (binaries) التي يتم تنفيذها عند تنفيذ الخدمات. وبعض الخدمات قد يتم تفعيلها بشكل تلقائي بواسطة (binaries) مخصص لتنفيذ وظيفة محددة. اذا تم تحديد الصلاحيات المجلد الذي يحتوي على (binaries) المستهدف او الصلاحيات على (binaries) بذاته، فقد يقوم المهاجم بالكتابة فوقة بالصلاحيات الممنوحة له في المجلد او (binaries) بذاته والتي قد تكون صلاحيات عالية او صلاحيات النظام (SYSTEM) التي تسمح له بهذا العمل والتنفيذ.
T1574	.011	Services Registry Permissions Weakness	قد يقوم المهاجمين بتشغيل تعليماتهم البرمجية الضارة من خلال اختطاف/سرقة مدخلات (Registry) المستخدمة من قبل الخدمات في النظام. يستغل المهاجمين سير العمل (Flaws) الخاصة بالصلاحيات لنظام لل(Registry) في الويندوز لاعادة تنفيذ التعليمات البرمجية الأصلية للبرمجيات التي يتحكم بها. والتي يستخدمها لتشغيل الاكواد الضارة من خلال الخدمات. ويقوم نظام ويندوز بحفظ الخدمات المحلية والاعدادات الخاصة بها في (HKLM\SYSTEM\CurrentControlSet\Services) والخدمات التي يتم تخزينها في (Registry keys) قد يتم التلاعب بها او تعديلها لجعلها تقوم بتنفيذ الخدمات الضارة والتي من شأنها ات تقوم بتشغيل أدوات او تنفيذ تعليمات برمجية او تشغيل PowerShell او Reg. ويتم التحكم في الوصول الى (Registry keys) من خلال قوائم التحكم في الوصول والاذونات (Access Control Lists and permissions).
T1574	.012	COR_PROFILER	قد يستغل المهاجمين المتغيرات في البيئة لـ (COR_PROFILER) والتي قد تؤدي الى اختطاف/سرقة آلية عمل البرنامج والتي تقوم بتحميلها الى .NET CLR. ان (COR_PROFILER) هي احد المميزات لاطار (.Framework NET) والتي تسمح للمطورين بتحديد ملفات التعاريف .NET DLL/External الغير مدارة (unmanaged) ليتم تحميلها في كل عملية من عمليات . NET CLR. وتم إيجاد وتصميم ملفات التعريف لمراقبة وتصحيح الأخطاء البرمجية التي يتم تنفيذها بواسطة .NET CRL.
T1562		Impair Defenses	قد يقوم المهاجم بتعديل بعض الخصائص او البرمجيات للمستهدف لتنفيذ تعليمات برمجية ضارة وذلك بهدف التخفي من الاكتشاف او تعطيل وسائل الحماية، وهذه الأساليب لا تشتمل على محاولة تعطيل او التخفي من آليات الحماية من الاختراقات مثل جدران الحماية ومكافح الفايروسات، بل لديها ايضاً القدرة على الاطلاع على الوسائل الدفاعية لدى الجهة المستهدفة

			ومحاولة التخفي منها. وهذه الأساليب المستخدمة من قبل المهاجمين تستهدف البرمجيات والانظمة التي تأتي مع النظام الأساسي او التي يتم تركيبها بواسطة مدراء الشبكة.
T1562	.001	ادوات تعديل وتعطيل / Disable or Tools Modify	قد يقوم المهاجم بتعطيل أدوات الحماية وذلك بهدف التخفي من الاكتشاف، وقد يقوم المهاجم بتعطيل البرمجيات الخاصة بالحماية او تعطيل خدمات تسجيل الاحداث. او مسح السجلات او تعطيلها من خلال (registry) وذلك لضمان عدم عودتها للعمل مره أخرى، وهذا يشمل أي أدوات من أدوات الحماية والمراقبة والمسح والاستطلاع.
T1562	.002	تعطيل مسجل الاحداث في الويندوز / Windows Event Disable Logging	قد يقوم المهاجم بتعطيل مسجل الاحداث الخاص بنظام ويندوز وذلك بهدف تقليل مدى التغطية للأنظمة المستهدفة والتهرب من الاكتشاف. ان نظام تسجيل الاحداث الخاص بنظام ويندوز يقوم بتسجيل الأنشطة التي تتم على النظام مثل عمليات تسجيل الدخول، انشاء العمليات وغيرها. ويتم استخدام هذه الاحداث لتدقيق من قبل أنظمة الحماية ومحللي الامن السيبراني لرصد الأنشطة الضارة.
T1562	.003	Impair Command History Logging	قد يقوم المهاجمين بتعطيل/محي مسجل الاحداث (command history) وذلك بهدف التخفي من الاكتشاف والرصد، حيث يقوم المهاجم بإرسال أوامر ضارة ومن ثم يقوم بمحي تلك الأوامر من سجل الاحداث.
T1562	.004	تعديل او تعطيل انظمة جدران الحماية / Disable or Modify System Firewall	قد يقوم المهاجم بتعطيل جدران الحماية الخاصة بالأنظمة وذلك بهدف التخفي وتخطي ضوابط التحكم التي تم وضعها في النظام. ان حدوث تغيرات على جدران الحماية قد تؤدي الى تعطيله او تعطيل آلية العمل الخاصة به. وقد يقوم المهاجمين بتعطيل او حذف بعض القواعد الخاصة بجدران الحماية او تعديلها. وقد يقوم المهاجم بهذا العملية بطرق متعددة من خلال الأوامر او واجهة رسومية.
T1562	.006	Indicator Blocking	قد يقوم المهاجم بتعطيل او منع الاحداث من عملية التسجيل وذلك بهدف التخفي من الاكتشاف، وقد يقوم بها بطرق متعددة من خلال التعطيل او من خلال إعادة التوجيه لأنظمة لا تقوم بتسجيل الاحداث. على سبيل المثال نظام تسجيل الاحداث الخاص بـ(Event tracing for windows ETW) وذلك بواسطة تعديل الاعدادات التي تقوم بجمع هذه الاحداث. وقد يقوم المهاجم بتعديل مسجل الاحداث بطرق مختلفة اما من تعديل ملفات مرتبطة مع سجلات الاحداث او من خلال (Registry) او من خلال واجهة مدراء النظام او من خلال استخدام PowerShell في نظام ويندوز.
T1562	.007	تعديل او تعطيل جدران الحماية للخدمات السحابية / Disable or Modify Cloud Firewall	قد يقوم المهاجم بتخطي او تعديل جدران الحماية الخاصة بالخدمات السحابية وذلك بهدف تخطي صلاحيات الوصول الى الخدمات السحابية.
T1562	.008	تعطيل السجلات للخدمات الحسابية / Cloud Logs Disable	قد يقوم المهاجم بتعطيل خدمات تسجيل الاحداث الخاصة بالخدمات السحابية وذلك بهدف منع عمليات تسجيل الاحداث التي يقوم بها المهاجم وذلك بهدف التخفى من عمليات الرصد والاكتشاف.
T1070		Indicator Removal on Host	قد يقوم المهاجم بمسح او انشاء احداث وهمية على النظام المستهدف، بما في ذلك السجلات الخاصة بالأحداث او الملفات التي تم تصنيفها انها ضارة. وقد تختلف عمليات التسجيل للأحداث والأنظمة حسب النظام. مثل أنظمة ويندوز ولينكس وماك او اس. وهنا مسار الخاص لأنظمة لينكس (/var/log/*)
T1070	.001	مسح السجلات من نظام ويندوز/ Event Logs Clear Windows	قد يقوم المهاجمين بمسح الاحداق الخاصة بأنظمة ويندوز وذلك بهدف إخفاء الأنشطة المشبوهة لكي لا يتم اكتشافها. ان مسجل الاحداث في نظام ويندوز يقوم بتسجيل جميع الاحداث التي تتم على النظام وتقوم بالتنبيه والتحذير بناء على النشاط. وهناك ثلاث أنواع من أنواع مصادر تلك الاحداث وهي (الحماية، التطبيقات، النظام) على شكل ٥ أنواع من أنواع الاحداث وهي (خطا، تحذير، معلومات، تم التدقيق بشكل سليم، وفشلت عملية التدقيق)

T1070	.002	مسح السجلات من نظام لينكس وماكLinux Clear or Mac System Logs	قد يقوم المهاجمين بمسح الاحداق الخاصة بأنظمة لينكس، ماك او اس وذلك بهدف إخفاء الأنشطة المشبوهة لكي لا يتم اكتشافها. النظامين يقومان بحفظ التحركات والأنشطة الخاصة بالنظام والمستخدمين في سجل الاحداث. ومعظم سجلات الاحداث يتم حفظها في /var/log/ وهناك تقسيمه داخل هذا المجلد يعكس الوظائف الخاصة بالسجلات التي بداخله.
T1070	.003	مسح سجل الاحداث من / Clear Command History	بالإضافة للعمليات التي قد يقوم بها المهاجم من مسح سجلات الاحداث لكي لا يتم اكتشافه قد يقوم المهاجم بمسح سجل التاريخ الخاص بسطر الأوامر للنظام المخترق لكي لا يتم اكتشاف ما تمت كتابته من أوامر للنظام
T1070	.004	مسح الملفات / File Deletion	قد يقوم المهاجم بمسح الملفات الخاصة بالهجمة لكي لا يتم اكتشافها من قبل أنظمة وبرمجيات الحماية وعادة ما تكون تلك البرمجيات ضارة. وقد لا تكون جميع تلك الملفات تنفيذيه بل قد تكون ملفات يتم انشاءها من قبل المهاجم والتي قد تفيد المحللين السيبرانيين من اكتشاف ما تم عملة على الشبكة المخترقة، وقد يقوم بها كذلك المهاجم لتفادي تتبعه داخل الشبكة بعد عملية الاختراق.
T1070	.005	مسح الارتباط والاتصال بملفات المشاركة / Network Share Connection Removal	قد يقوم المهاجم بمسح الارتباط بملفات المشاركة عند الانتهاء من استخدامها وذلك لجعل عملية التتبع صعبه، ان ملفات المشاركة في نظام ويندوز SMB يتيح حذفها او إلغاءها عند عدم الحاجة لها. من خلا أداة (Net) تستطيع من خالها حذف المجلد او طريقة التواصل من خلال الشبكة مثال على الامر (net use \system\share /delete)
T1070	.006	Timestomp	قد يقوم المهاجمون بالتلاعب بالملفات من خلال تغير وقت الانشاء او التعديل لها. ان Timestomping هي تقنية تقوم بتعديل الوقت الفعلي الذي تم تعديل او حفظ او انشاء هذا الملفات. وغالباً يتم تحديد تاريخ ووقت للملف الضار مثل الملفات السليمة الأخرى في نفس المجلد وذلك بهدف التخفي عندما يقوم محلل الامن السيبراني بالتحقق من الملفات المنشأة حديثاً
T1202		Indirect Command Execution	قد يقوم المهاجمون باستغلال الأدوات الملحقة بالنظام وذلك بهدف تنفيذ أوامر (من خلال سطر الأوامر) ضارة ويتم استخدام تلك الأدوات بشكل خاص بسبب امكانيتها تجاوز بعض القيود الأمنية المحددة من قبل سطر الأوامر. يمكن استخدام العديد من الأدوات في نظام ويندوز الملحقة او المساعدة للتنفيذ أوامر، وربما يتم تنفيذ هذه الأوامر من غير حتى استدعاء سطر الأوامر CMD على سبيل المثال (Forfiles) Program Compatibility Assistant (pcalua.exe) ولنظام لينكس Windows Subsystem for Linux (WSL) وكذلك هناك أدوات متعددة تقوم بنفس الوظائف من تنفيذ أوامر بطرق مختلفة اما من خلال برمجيات او سكربتات وغيره.
T1036		Masquerading	قد يقوم المهاجمين بالتلاعب بالأدلة او الملفات او الوظائف لجعلها تبدو غير ضارة او للاستخدام الغير خبيث سواء كانت ادوات او مستخدمين او برمجيات. يحدث التلاعب عندما يتم تغير او تعديل او انشاء او استبدال وظيفة او ملف او برمجية بهدف التخفي من عملية الرصد والاكتشاف عند قيام محلل الامن السيبراني بعمل الاستجابة للحوادث. وقد تمتد تلك العمليات من التلاعب حتى يتم تعديل البيانات الوصفية.
T1036	.001	Invalid Code Signature	قد يقوم المهاجمين بالتلاعب وتقليد بعض الخصائص الإضافية لبرمجيات (توقيع الاكواد رقمياً) حقيقة لزيادة فرصة التلاعب بالمستخدمين وجعل برمجياته كأنها حقيقة وليست ضارة. ان عملية توقيع الاكواد الرقمية توفر مصادقيه من المطورين ان الاكواد البرمجية لم يتم التلاعب بها. وحيث ان عملية نسخ التواقيع الرقمية (البيانات الوصفية) قد يقوم بها المهاجم من خلال نسخها من برنامج اخر، ثم استخدامه كقالب لبرنامجه الضار. وقد تتم عملية التحقق من التواقيع الرقمية وفي حال لم يتم التحقق سيتم افشال عملية تشغيل البرمجية. ولكن قد تنطلي الحيلة على المستخدمين او المحللين.
T1036	.002	Right-to-Left Override	قد يقوم المهاجمين بالتلاعب باتجاه الاحرف من اليسار لليمين والعكس (U+202E) (RTLO or RLO) وذلك بهدف خداع المستخدم ان هذا الملف غير ضار. ان RTLO هو مجموعة حروف (غير قابلة للطباعة) يتم عرضها على الشاشة بشكل عكسي. على سبيل المثال عندما يتم عرض شاشة التوقف الخاصة بالويندوز بهذا الشكل \u202Excod.scr March 25 ويتم

			استخدام March 25 rcs.docx وهنا ملف جافا سكربت photo_high_re\u202Egnp.js ويتم عرضه كصورة photo_high_resj.png
T1036	.003	Rename System Utilities	قد يقوم المهاجمين بإعادة تسمية بعض الأدوات المساعدة في النظام بهدف التهرب من الاكتشاف وذلك بسبب ان أنظمة الحماية تقوم بمراقبة تلك الأدوات المساعدة. بعد عملية التغير لها يستطيع المهاجم استخدامها دون ان يتم اكتشافه على سبيل المثال إعادة تسمية rundll32.exe وتحدث العملية بإشكال متعددة وطرق مختلفة سواء كانت نسخ او تغير المجلد الخاص بها او إعادة تسميتها بنفسها.
T1036	.004	Masquerade Task or Service	قد يقوم المهاجمين بالتلاعب باسم مهمة او خدمة لجعلها تبدو غير ضارة وأنها حقيقية. يتم تنفيذ هذا الخدمات من خلال جدولة الاعمال او من خلال systemd والتي يتم بالعادة أعطاها اسم محدد ووصف لها. وفي نظام ويندوز يتم أعطى اسم للخدمة وكذلك اسم للعرض الخاص بهذه الخدمة. وبالعادة ان اكثر الخدمات الغير ضارة قد تتشابه في اسم العرض الخاص بها بشكل كبير، مما يجعل المهاجمين يفكرون بنفس الطريقة وإعطاء ملفاتهم الضارة نفس الأسماء.
T1036	.005	Match Legitimate Name or Location	قد يقوم المهاجمين بالتلاعب بالأسماء او المجلدات وجعلها مقاربة للمجلدات او الملفات او المواقع الخاصة بها الحقيقية وذلك بهدف التهرب من أنظمة المراقبة. ويمكن للمهاجم من القيام بذلك من خلال ملف تنفيذي في مجلد system32 واعطاه اسم كأنه ملف غير ضار. او إعطاء اسم مألوف لخدمات في النظام مثل svchost.exe او انشاء ملف اخر يحم نفس الاسم مع زيادة مسافه ما بين الاحرف لكي يوهم المحلل انه نفس الملف
T1036	.006	Space after Filename	قد يقوم المهاجم بإخفاء الامتداد الخاص بالملفات الضارة. وذلك من خلال إضافة مسافة في نهاية الملف وهذا ما يجع النظام يتعامل مع الملف بطريقة متغيرة. ولا يعمل هذا الأسلوب مع الملفات التي تأتي بامتدادات (.app)
T1556		تعديل طريقة وعملية التحقق / Modify Authentication Process	قد يقوم المهاجمين بتعديل آلية وطريقة عمل المصادقة للمستخدمين او السماح للوصول لبعض الحسابات بطريقة غير مرغوبة. ان عملية المصادقة تتم من خلال آليات متعددة مثل (Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM)) في نظام الويندوز و (pluggable authentication modules (PAM)) في نظام لينكس و (authorization plugins) في نظام MacOs. وجميع التقنيات التي ذكرت سابقاً هي المسؤولة عن تخزين وحفظ بيانات المصادقة والتحقق منها. والتي قد تسمح في بعض الأحوال للمهاجمين من المصادقة على خدمة او نظام دون الحاجة الى استخدام حسابات فعالة وصحيحة.
T1556	.001	Domain Controller Authentication	قد يقوم المهاجم بتصحيح. عمليات المصادقة على (Domain Controller) وذلك بهدف تخطي وسائل التحقق المتبعة وتمكينه من الوصول الى الحسابات.
T1556	.002	Password Filter DLL	قد يقوم المهاجمين باستخدام (Filter DLL Password) في عمليات المصادقة لتحقق من صحة بيانات الاعتماد
T1556	.003	Pluggable Authentication Modules	قد يقوم المهاجمين بتعديل (authentication modules (PAM pluggable)) للوصول الى بيانات الاعتماد او تفعيل حسابات غير مرغوب فيها. ان (pluggable authentication modules (PAM)) هو نظام معياري للإعدادات الخاصة للملفات و المكتبات والملفات التنفيذية والتي تقوم بتوجيه آلية المصادقة للعديد من الخدمات. ومن اشهرها هي (pam_unix) والتي تقوم باسترداد المعلومات الخاصة بمصادقة الحساب وتعينها والتحقق منها في (/etc/passwd) و (/etc/shadow)
T1556	.004	التحقق بواسطة اجهزة الشبكة / Device Network Authentication	قد يقوم المهاجم بالاستفادة من التشفير الخاص بكلمات المرور في أنظمة التشغيل او ما يسمى (Patch System Image). وبالتالي يستفيد منها المهاجمين في تجاوز آليات المصادقة للحسابات المحلية على أجهزة الشبكة.

T1578		Modify Cloud Compute Infrastructure	قد يقوم المهاجم بتعديل الحسابات الخاصة بالخدمات السحابية وذلك لتفادي الاكتشاف والتعديلات قد تشتمل انشاء وتعديل ومسح على أي جزء من أجزاء الخدمات السحابية اوأنظمة الافتراضية او النسخ الصورية.
T1578	.001	انشاء نسخة / Create Snapshot	قد يقوم المهاجم بإنشاء نسخة صورية للبيانات او النسخ الاحتياطية على الخدمات السحابية وذلك لتخفي من الاكتشاف. ان عملية النسخ الصورية هي أحد مكونات الاساسية للخدمات السحابية يتم اخذها بوقت محدد والتي بدورها تقوم بجعل النظام الافتراضي VM قابل للاستعادة. ويتم تخزينها على مساحة افتراضية من القرص الصلب او على جزء محدد من قرص صلب. وقد يقوم المهاجمين باستغلال الصلاحيات لأنشاء مثل هذه النسخ الصورية والاطلاع عليها بسبب انهم لا يملكون الأذونات المناسبة للوصول للبنية التحتية الحقيقة للمنظمة. وقد يقوم المهاجمين بإنشاء نسخة صورية قبل تنزيل أي ملفات ضارة وبعد عملية الاختراق والانتهاء منها يقومون باسترجاع النسخة قبل عملية الاختراق لتفادي الاكتشاف.
T1578	.002	انشاء نسخة للخدمات السحابية / Instance Create Cloud	قد يقوم المهاجمين بإنشاء نسخ افتراضية VM داخل الخدمات السحابية او الحساب وذلك بهدف التهرب من عمليات الاكتشاف. قد تسمح الصلاحيات للمهاجم بإنشاء النسخ الافتراضية او الأنظمة الافتراضية وذلك بهدف تجاوز جدران الحماية والتحكم الكامل للمهاجم بخلاف النسخة الأخرى التي لا يملك عليها الصلاحيات المناسبة وقد يقوم المهاجم بإنشاء نسخة صورية واحده من النظام الذي لا يملك صلاحيات وتطبيق اقل الصلاحيات.
T1578	.003	مسح الخدمات السحابية / Delete Instance Cloud	قد يقوم المهاجم بمحي النسخة الافتراضية على الخدمات السحابية وذلك لتفادي الاكتشاف وكذلك محي برمجياته عن النظام لكي لا يتم الحصول عليها من قبل المحللين السيبرانيين. وتفيد تلك العملية المهاجمين جداً حيث ان التتبع لهم يصبح اصعب.
T1578	.004	استعادة الخدمات السحابية / Instance Revert Cloud	قد يقوم المهاجمين باستعادة النسخ الاحتياطية من النظام المستهدف قبل تنزيل أي ملفات او عمل أي أنشطة خبيثة وذلك لتفادي الاكتشاف. وتحتوي بعض الخدمات السحابية على مميزات متعددة في عملية الاستعادة بشكل كامل او من خلال نسخة صورية يقوم المهاجم بأخذها او نسخة صورية موجودة سابقاً. وتتم تلك العملية اما من خلال لوحة تحكم خاصة او من خلال الاتصال بإAPI محدد.
T1112		تعديل الريجستري / Modify Registry	قد يقوم المهاجم بإخفاء بعض الإعدادات الضارة داخل windows registry وذلك بهدف إخفاء بعض الأنشطة الضارة. وقد تساعد بعض تلك الإعدادات في عملية مسح الأدلة او البقاء داخل الشبكة قدر الإمكان.
T1601		تعديل نسخة النظام / Modify System Image	قد يقوم المهاجمين بتعديل النسخ الخاصة بالنظام لأجهزة الشبكات وذلك بهدف التخفي قدر الإمكان من الاكتشاف. وعادة ما تكون تحتوي تلك الأجهزة على نظام وملفات وقدرات في ملف موحد.
T1601	.001	سد الثغرات لنسخة النظام / Patch Image System	قد يقوم المهاجم بتعديل نظام التشغيل الخاص بأجهزة الشبكة لإدخال قدرات جديدة من شانها تقليل عمليات المراقبة والرصد لأنشطته الضارة. وقد يقوم المهاجمين بتعديل الملف الخاص بالنظام لإدخال التعليمات البرمجية الضارة.
T1601	.002	Downgrade System Image	قد يقوم المهاجم بإعادة تثبيت نسخ اقدم من الأنظمة الخاصة بأجهزة الشبكات وذلك بسبب وجود ثغرات تتيح لله التخفي من الاكتشاف او وجود تشفير ضعيف على عملية نقل البيانات.
T1599		حدود البوابة الشبكية / Network Bridging Boundary	قد يقوم المهاجمين بتغير طريقة التعامل مع الشبكات الأخرى (الغير موثوقة) او تغير طريقة حركة مرور و توجيه البيانات وذلك بهدف تخطي وسائل الحماية المفروضة ويأتي ذللك بعد عملية اختراق الموجهة وتمرير البيانات لشبكات غير موثوقة.
T1599	.001	Network Address Translation Traversal	قد يقوم المهاجم بتعديل البيانات الخاصة بالعناوين الشبكية NAT لأجهزة الشبكة وجعلها تتواصل مع أنظمة أخرى مشبوهة والتعديل على عناوين NAT تمكن المهاجمين من تخطي بعض القيود المفروضة على توجيه حركة البيانات داخل او خارج الشبكة.
T1027		تشفير الملفات و المعلومات / Files or Obfuscated Information	قد يقوم المهاجم بعملية تشفير او ترميز لملفاته وجعلها غير قابلة للاكتشاف من قبل أنظمة الحماية والتحليل. وهذا الأسلوب مستخدم بكثره وذلك لتفادي عملية التحليل للبيانات الشبكية.

T1027	.001	Binary Padding	قد يقوم المهاجم بإضافة بيانات غير مفيدة على برمجياته وذلك بهدف جعلها غير مفهومة او لتصعيب عملية التحليل. وتحدث تلك الطريقة دون التأثير على آلية عمل برمجياتهم الضارة. ولكن قد يزيد من حجم الملف مما يجعل أنظمة الحماية غير قادرة على تحليله بسبب حجمة الكبير.
T1027	.002	Software Packing	قد يقوم المهاجمين بضغط الملفات والبرمجيات الخاصة بهم وتشفيرها وذلك بهدف إخفاء الأدوات والبرمجيات الضارة بهم. ضغط البرمجيات وتشفيرها قد تتفادى من عملية الاكتشاف من خلال استخدام آليات الاكتشاف باستخدام التواقيع الرقمية. ومعظم عمليات فك الضغط تحدث في الذاكرة العشوائية. تقوم Virtual machine software protection translates بحماية الملف التنفيذي من التعديل عند التشغيل وتقوم في نفس الوقت باستدعاء الدالة الخاصة به لتشغيلة.
T1027	.003	Steganography	قد يقوم المهاجمين باستخدام تقنيات إخفاء البيانات والمعلومات لمنع الاكتشاف (Steganographic) ويمكن إخفاء البيانات ونقلها من خلال صور او ملفات فيديو او مقاطع صوتية او ملفات نصية.
T1027	.004	Compile After Delivery	قد يقوم المهاجمين بنقل ملفاتهم قبل عملية جعلها قابله للتنفيذ (uncompiled code) وذلك بهدف تصعيب عملية الرصد والاكتشاف. ان الملفات النصية التي تحتوي على اكواد برمجية ضارة غير مجمعة لكي تكون قابلة لتنفيذ قد تكون صعبة في عمليات الرصد والاكتشاف. ويقوم المهاجمين بنقلها الى الجهاز المستهدف ومن ثم جمع تلك الملفات وجعلها قابلة للتنفيذ عبر أدوات متوفرة في النظام المستهدف مثل csc.exe او GCC/MinGW
T1027	.005	Indicator Removal from Tools	قد يقوم المهاجمين بمحي مؤشرات الاختراق الخاصة بهم بعد عملية اكتشاف برمجياتهم الخبيثة وذلك بهدف التخفي قدر المستطاع.
T1542		نظام اقلاع جاهز / Pre-OS Boot	قد يقوم المهاجمين باستغلال آليات الإقلاع الخاصة بالنظام كطريقة للبقاء أطول فترة ممكنة في النظام. وتعرف هذه الأنظمة بالأنظمة الأساسية قبل عملية اقلاع نظام التشغيل.
T1542	.001	النظام الثابت / System Firmware	قد يقوم المهاجمين بتعديل ما يسمى بـ(firmware system) وذلك بهدف لاختراق النظام والبقاء أطول فترة ممكنة. ان (Input/Output System BIOS Basic) و (Unified Extensible Firmware Interface (UEFI)) او (Extensible Firmware Interface (EFI)) جميعهم هي أنظمة تشغيله ثابته من نوع (firmware) وهي تعمل ما بين نظام التشغيل والعتاد الخاص بالجهاز.
T1542	.002	Component Firmware	قد يقوم المهاجمين بتعديل ما يسمى بـ(component firmware) وذلك بهدف لاختراق النظام والبقاء أطول فترة ممكنة. وقد يستخدم بعض المهاجمين طرق معقده ومتقدمة جداً لتنفيذ مثل هذه العمليات المتقدمة في الاختراق والتي تؤدي الى تثبيت (component firmware) ضار يقوم يتنفيذ تعليمات البرمجية الضارة على نظام التشغيل او النظام الخاص بـ(BISO). ان هذه الأساليب تتشابه مع (System Firmware) ولكن يتن تنفيذها على بعض المكونات والاجهزة التي لا تمتلك مستوى قدرات في فحص مستوى سلامتها
T1542	.003	برمجية ضارة مع اقلاع النظام / Bootkit	قد يقوم المهاجمين باستغلال ما يسمى بـ(bootkits) وذلك بهدف البقاء أطول فترة ممكنة. ويتم استخدام (bootkits) كطبقة أسفل نظام التشغيل. ومثل هذه الاستغلال صعب الاكتشاف مالم يتم التحقق منه.
T1542	.004	ROMMONkit	قد يقوم المهاجمين باستغلال ما يسمى بـ(Monitor (ROMMON ROM)) وذلك من خلال تحميل أنظمة (firmware) ضار وذلك بهدف البقاء أطول فترة ممكنة. ومثل هذه الاستغلال صعب الاكتشاف مالم يتم التحقق منه.
T1542	.005	TFTP Boot	قد يقوم المهاجمين باستغلال (netbooting) لتحميل نظام تشغيل غير مصرح به من خادم نقل الملفات بواسطة بروتوكول (TFTP). يتم استخدام (TFTP boot (netbooting)) بشكل شائع بين مدراء الشبكات لتحميل الاعدادات الخاصة بأجهزة الشبكات والنسخ الصورية (Image) من خادم مركزي او مستودع. ان (netbooting) هو واحد من الخيارات المسموح بها للإقلاع الخاص بالنظام ويمكن استخدامه لتحكم والإدارة وكذلك مركز لحفظ النسخ الصورية (Images).

T1055		حقن العمليات / Process Injection	قد يقوم المهاجمين بحقن العمليات وذلك بهدف رفع الصلاحيات او التهرب من الاكتشاف. وقد تستخدم حقن العمليات لتنفيذ تعليمات ضارة في بعض العمليات النشطة. والتي قد تسمح بحقن والوصول الى العمليات في الذاكرة العشوائية (Memory) او النظام او الشبكة. وتعتبر عملية حقن العمليات من الأساليب المتبعة من قبل المهاجمين حيث انها تعمل وكأنها عملية طبيعية وغير ضارة.
T1055	.001	Dynamic-link Library Injection	قد يقوم المهاجمين بحقن (libraries (DLLs dynamic-link داخل العمليات وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن DLL تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1055	.002	حقن البرمجيات الجاهزة للعمل / Executable Injection Portable	قد يقوم المهاجمين بحقن (PE) داخل العمليات وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن PE تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1055	.003	Thread Execution Hijacking	قد يقوم المهاجمين بحقن بعض البرمجيات الضارة في العمليات التي يتم اختطافها وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (Thread Execution Hijacking) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة.
T1055	.004	Asynchronous Procedure Call	قد يقوم المهاجمين بحقن بعض البرمجيات الضارة في العمليات النشطة من خلال (asynchronous procedure call APC) وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (APC) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة.
T1055	.005	Thread Local Storage	قد يقوم المهاجمين بحقن بعض البرمجيات الضارة في العمليات النشطة من خلال (thread local storage (TLS)وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (TLS callback) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة.
T1055	.008	Ptrace System Calls	قد يقوم المهاجمين بحقن بعض البرمجيات الضارة في العمليات النشطة من خلال (processes via ptrace (process system calls (trace) وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (Ptrace system call) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة.
T1055	.009	Proc Memory	قد يقوم المهاجمين بحقن برمجيات ضارة عبر استخدام (Proc) لملفات النظام وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (Proc memory) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1055	.011	Extra Window Memory Injection	قد يقوم المهاجمين بحقن برمجيات ضارة عبر استخدام (Extra windows memory EWM) لملفات النظام وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (EWM) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1055	.012	Process Hollowing	قد يقوم المهاجمين بحقن برمجيات ضارة عبر استخدام عمليات تم ايقافها وتسمى بـ(hollowed processes) وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (hollowed processes) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1055	.013	Process Doppelgänging	قد يقوم المهاجمين بحقن برمجيات ضارة عبر استخدام (process doppelgänging) وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (process doppelgänging) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1055	.014	VDSO Hijacking	قد يقوم المهاجمين بحقن برمجيات ضارة عبر استخدام اختطاف او انتحال (VDSO) وذلك من اجل رفع الصلاحيات او التهرب من الاكتشاف. ان عملية حقن (VDSO او Virtual dynamic shared object) تتم لتنفيذ تعليمات ضارة في بعض العمليات النشطة
T1207		Rogue Domain Controller	قد يقوم المهاجمين بتسجيل (Controller Domain) احتيالي وذلك بهدف التلاعب بالـ (Domain Controller (DC)). يقوم (DCShadow) بإنشاء نسخة احتيالية لتلاعب بالبيانات الخاصة بـ AD. والتي تشتمل على (objects and schemas)

			من خلال محاكات نشاط وسلوك DC. مجرد ان تتم عملية التسجيل لل DC الاحتيالي يستطيع ان يقوم بالتلاعب بكامل البنية التحتية الخاصة بالدليل النشط AD وقد يصل الى تغير كلمات المرور وبيانات الاعتماد وبعض الوظائف.
T1014		Rootkit	قد يقوم المهاجم باستخدام برمجيات rootkits وذلك لإخفاء ملفاته وبرمجياته وأنظمة وشبكاته وغيرها من عمليات الاكتشاف. ان rootkits هو برمجية تستخدم لإخفاء التعليمات البرمجية الضارة داخل النظام الأساسي وتستطيع التواصل برمجية rootkits مع باقي البرمجيات من خلال استخدام استدعاءات بواسطة API وغيرها.
T1218		Signed Binary Proxy Execution	قد يقوم المهاجم بتخطي العمليات التي تعتمد على اكتشافها بالتواقيع الرقمية وذلك من خلال استخدام أجزاء تم توقيعها رقمياً. ان بعض الاجزاء التي تم توقيعها رقمياً قد يتم تنفيذها على أنظمة ويندوز. ويمكن استخدام العديد من الأجزاء من البرمجيات الموقعة رقمياً في نظام ويندوز افتراضياً في مثل هذه الهجمات.
T1218	.001	تكوين مف HTML / Compiled HTML File	قد يقوم المهاجم باستغلال عملية جمع الملفات المتوفرة في HTML بامتداد (.chm) لإخفاء تعليمات برمجية ضارة. ويتم التعامل مع ملفات CHM كجزء من ما يسمي (Microsoft HTML Help system). ويحتوي ملفCHM على ملفات مضغوطة مثل ملفات HTML وصور وسكربتات وملفات VBA وجافا سكربت وActiveX. يتم استخدام وعرض محتويات ملف CHM من خلال متصفح الانترنت اكسبلورر عند تحميل صفحة بامتداد .HTML والتي قد تحتوي على ملفات تنفيذيه.
T1218	.002	لوحة التحكم / Control Panel	قد يقوم المهاجم باستخدام control.exe لتنفيذ تعليمات برمجية ضارة. وتقوم لوحة التحكم في نظام ويندوز بمعالجة وتنفيذ عناصر التحكم في النظام وهي أدوات مساعدة يتم من خلالها تعديل اعدادات الكمبيوتر وضبطه.
T1218	.003	CMSTP	قد يقوم المهاجم باستخدامMCSTP لتنفيذ تعليمات برمجية ضارة. ويعد Microsoft Connection Manager Profile Installer (CMSTP.exe) سطر أوامر يستخدم لإدارة الخدمات الخاصة بملفات التعريف. يقوم CMSTP.exe بقبول (installation information file INF) والتي تسمح للخدمات بالاتصال عن بعد من خلال خدمة ملف التعريف.
T1218	.004	InstallUtil	قد يقوم المهاجم باستخدام InstallUtil لتنفيذ تعليمات برمجية ضارة من خلال هذه الأداة وهي أحد الأدوات المساعدة في نظام ويندوز. وطبيعة InstallUtil تقوم على انها أداة مساعدة لسطر الأوامر وتسمح بتثبيت المصادر من خال تنفيذ تعليمات محددة عند القيام بعملية التثبيت باستخدام .NET binaries، ان أداة InstallUtil هي أداة موقع رقمياً بواسطة مايكروسوفت وتقع من ضمن نطاق .NET في أنظمة ويندوز في المسارات التالية (system: C:\Windows\Microsoft.NET\Framework\v\InstallUtil.exe and (.C:\Windows\Microsoft.NET\Framework64\v\InstallUtil.exe
T1218	.005	Mshta	قد يقوم المهاجمين باستغلال أداة mshta.exe لتنفيذ تعليمات برمجية ضارة. بامتداد ملف .hta او جافا سكربت او VBScript. وهناك امثله متعددة لطريقة استخدام mshta في عملية الوصول الاولي للمستهدف او استخدامها في عملية تثبيت البرمجيات الضارة.
T1218	.007	Msiexec	قد يقوم المهاجمين باستغلال msiexec.exe لتنفيذ تعليمات برمجية ضارة. ان أداة msiexec.exe هي عبارة عن أداة مساعدة لسطر الأوامر لبرنامج Windows Installer والتي يتم استخدامها بشك شائع في عملية تثبيت الحزم بامتداد .msi كما قامت مايكروسوفت بتوقيع msiexec رقمياً.
T1218	.008	Odbcconf	قد يقوم المهاجمين باستغلال Odbcconf.exe لتنفيذ تعليمات برمجية ضارة. ان أداة Odbcconf.exe هي عبارة عن أداة مساعدة للإعدادات الاتصال بقواعد البيانات المفتوحة (ODBC) والتي تحتوي على التعاريف و بعض مصادر البيانات Windows كما قامت مايكروسوفت بتوقيع msiexec رقمياً.

T1218	.009	Regsvcs/Regasm	قد يقوم المهاجمين باستغلال Regasm Regsvcs and لتنفيذ تعليمات برمجية ضارة. ان أداة Regsvcs and Regasm هي عبارة عن سطر أوامر تستخدم لتسجيل .NET. Component Object Model COM كل الاداتين تم توقيعها رقمياً بواسطة مايكروسوفت
T1218	.010	Regsvr32	قد يقوم المهاجمين باستغلال Regsvr32.exe لتنفيذ تعليمات برمجية ضارة. ان أداة Regsvr32.exe هي عبارة عن سطر أوامر تستخدم لتسجيل (object linking و embedding controls) وقد تشتمل على DLLs. في بيئة الويندوز. أداة Regsvr32 موقعه رقمياً بواسطة مايكروسوفت.
T1218	.011	Rundll32	قد يقوم المهاجمين باستغلال rundll32.exe لتنفيذ تعليمات برمجية ضارة. ان أداة rundll32.exe قد تستخدم بشكل ثانوي أي من خلال (Shared Modules) والتي قد يتم استغلالها للتفادي عمليات الاكتشاف من قبل أنظمة الحماية التي لا تراقب العمليات التي يتم تنفيذها بواسطة rundll32 بسبب القوائم المسموح بها او الإنذارات الخاطئة اثناء عملية التشغيل العادية. وترتبط rundll32 بشكل شائع اثناء تنفيذ ملفات DLL.
T1218	.012	Verclsid	قد يقوم المهاجمين باستغلال verclsid.exe لتنفيذ تعليمات برمجية ضارة. ان أداة verclsid.exe والمتعارف عليها كامتداد CLSID وهي الإضافة المسؤولة عن التحقق من كل الامتدادات الخاص بالمتصفح او Windows Shell.
T1216		Signed Script Proxy Execution	قد يقوم المهاجمين باستخدام سكربتات موقعه رقمياً وموثوقة للتنفيذ تعليمات برمجية ضارة. حيث يمكن استخدام العديد من السكرتبات النصية الموقعة من مايكروسوفت والتي تكون مثبته افتراضياً في نظام ويندوز. مما يمكن المهاجمين من تنفيذ تعليمات برمجية ضارة من خلال استخدامها.
T1216	.001	PubPrn	قد يقوم المهاجمين باستغلال PubPrn لتنفيذ تعليمات برمجية ضارة، ويقوم المهاجمين باستخدام PubPrn وطلك لتفادي الاكتشاف المبني على التواقيع الرقمية لاكتشاف التهديدات السيبرانية. وكذلك تخطي وسائل الحماية المبنية على التحكم في التطبيقات والتي لا تتأخذ السكربتات كتطبيقات لمنعها.
T1553		Subvert Trust Controls	قد يقوم المهاجمين بإضعاف إمكانيات التقنيات الأمنية التي من شانها اما تحذير المستخدمين من نشاط ضار او عمليات غير موثوق بها او برمجيات مشبوهة يتم تنفيذها. وقد تحتوي أنظمة التشغيل على برمجيات ومنتجات الأمان التي تسمح لها بتحديد البرمجيات او المواقع الضارة وتحديد مستوى الموثوقية بها. ومن الأمثلة عليها السماح لبرنامج بالعمل بسبب انه موقع رقمياً من قبل طرف موثوق، او تحذير المستخدم ان المحتوى المراد تثبيته تم تحميله من الأنترنت، او الحصول على تنبيه انك على وشك الاتصال بموقع غير موثوق.
T1553	.001	Gatekeeper Bypass	قد يقوم المهاجمين بتعديل خصائص الملفات التي تسمح للنظام بمعرفة إذا كانت هذه الملفات من مصادر غير موثوقة وذلك بهدف الاحتيال على عناصر التحكم مثل Gatekeeper المتوفرة في نظامي macOS and OS X. حيث تعمل عند تحميل برنامج او ملف من خلال الانترنت بتفعيل ميزة com.apple.quarantine والتي تسمح لبرنامج الحماية Gatekeeper بتنبيه المستخدم اما بالسماح او الرفض لهذا الملف او البرمجية.
T1553	.002	Code Signing	قد يقوم المهاجمين بالاستحواذ او سرقة او انشاء طرق او آليات توقيع برمجياتهم الضارة. ويوفر التوقيع الرقمي للاكواد مستوى مصادقيه لدى المطورين ان البرمجيات موثوقة. ومن الشائع لدى المهاجمين ان الشهادات الخاصة بالتواقيع يتم انشاءها او سرقتها.
T1553	.003	SIP and Trust Provider Hijacking	قد يقوم المهاجمين بالتلاعب باستخدام SIP والثقة التي يتمتع بها مع نظام التشغيل وأدوات التحكم في التطبيقات عند اجراء عمليات التحقق من صحة التواقيع الرقمية. وفي حال المستخدم العادي يقوم نظام ويندوز بالتحقق نشأت التوقيع الرقمي وكذلك سلامته. وقد تقوم بعض المتغيرات المستخدمة لتوليد الثقة في الاكواد المستخدم مثل التعاريف في نظام ويندوز والذي يقوم بالتعامل مع التواقيع الرقمية الخاصة بها على انها تواقيع رقمية امنة. وتتم مرحلة التحقق من صحة التواقيع الرقمية

			بواسطة تطبيق WinVerifyTrust باستخدام وظيفة application programming interface API والتي تقبل الاستعلامات وتحدد المستوى المناسب من الثقة المطلوبة.
T1553	.004	Install Root Certificate	قد يقوم المهاجمين بتثبيت (certificate root) على النظام المخترق وذلك لتفادي التنبيه عندما تتم عملية التحكم والسيطرة والتواصل مع النطاقات الضارة الخاصة بالمهاجم. تستخدم (certificate root) في تشفيرها المفتاح العام الذي تم انشاءه بواسطة (authority CA root certificate)، وعند تثبيت الشهادة من قبل المهاجم يقوم البرنامج او النظام بالثقة بهذه الشهادة وهي بالعادة تقوم باستخدام برتوكول TLS/SSL للاتصالات من خلال متصفحات الويب. وفي حال لم يتم تثبيت هذه الشهادة واراد المستخدم تصفح هذا الموقع ستظهر رسالة تنبيه ان علية الحذر ان الشهادة الخاصة بالموقع لم توقع رقمياً وتحتاج الى الصلاحية لتثبيتها.
T1553	.005	Mark-of-the-Web Bypass	قد يقوم المهاجمين باستغلال التنسيق الخاص بالصفحات والتحكم بها او ما يعرف بي (Mark-of-the-Web MOTW). في نظام ويندوز وعند تحميل الملفات من الانترنت لكي يضلل المستخدمين ان الملفات امنة. ان السيناريو عند تحميل الملفات يتم من خلال تصنيفها بطريقة خفية باستخدام (NTFS) و (Alternate Data Stream ADS). وربطها باسم يعرف بـ Zone.Identifier مع قيمة محددة تسمى بي MOTW. يعني ذلك أي ملف محدد بالقيمة الخاصة بـ MOTW هو ملف محمي ولا يستطيع تنفيذ الا بعض الوظائف فقط. على سبيل المثال عند تشغيل MS Office 10 وكان الملف المراد فتحة مربوط بقيمة من MOTW لا يمكن فتحة بشكل مباشر بل من خلال طريقة العرض المحمية (Protected View) واي ملف يتم ربطة بقيمة من MOTW يتم معالجته من قبل (Windows Defender SmartScreen) والتي تقوم بالمقارنة بالملفات التنفيذية المسموح بها او الغير موثوقة وتقوم بتحذير المستخدم من تفعيله او تشغيله.
T1553	.006	Code Signing Policy Modification	قد يقوم المهاجمين بتعديل سياسة توقيع الاكواد البرمجية بهدف تفعيل خاصية تنفيذ الاكواد البرمجية الغير موقعه. ان توقيع الاكواد البرمجية تعطي مستوى من الثقة لدى مطورين التطبيقات وان التطبيق موثوق ولم يتم التلاعب به. وتستطيع تضمين عنصر من عناصر التحكم بمنع تنفيذ أي برنامج لم يتم توقيعه رقمياً من العمل على النظام الخاص بك.
T1221		Template Injection	قد يقوم المهاجمين بتعديل او انشاء قوالب ونماذج جاهزة للاستخدام لملفات (Office) وذلك بهدف إخفاء تعليمات برمجية ضارة او محاولة التلاعب في عملية المصادقة. ان (Microsoft's Office Open XML OOXML) او ما يعرف بتنسيق المستندات (XML) والذي يتم استخدامه لتنسيق المحتويات في الملفات (.pptx, .xlsx, .docx) وكذلك يقوم باستبدال الامتدادات القديمة (.ppt ,.doc, .xls) الى الامتدادات التي تم ذكرها سابقاً. يقوم بتجميع وضغط ملفات OOXML داخل ملف ZIP بامتدادات XML والتي في النهاية تساعد في تحديد الشكل والمظهر النهائي الخاص بالمستند.
T1205		Traffic Signaling	قد يقوم المهاجمين باستخدام (signaling traffic) بهدف إخفاء المنافذ المفتوحة او إخفاء بعض الوظائف الضارة والتي تستخدم بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين البقاء أطول فترة ممكنه داخل النظام المخترق. وتستخدم في بعض الأحيان من خلال سطر الأوامر (line Command) والتي تستخدم ما يسمى بـ(magic value او تسلسل محدد) والذي يتم ارساله لتحفيز استجابة معينة. مثل فتح او اغلاق أحد المنافذ او تنفيذ بعض المهام الضارة. وقد يقوم المهاجم بإرسال مجموعة من الحزم قبل اجراء أي عملية من فتح او اغلاق المنافذ والتي ستمكنه من التحكم والسيطرة على النظام المصاب. وعادة ما تكون هذه السلسلة من الحرم يتم تحديدها مسبقاً مثل (Port Knocking). ولكن قم يتم تضمين بعض التعليمات الفريدة من نوعها بعد اكمال عملية ارسال الحزم مما يقوم بفتح المنفذ او أغلاقه في جدار الحماية الخاص بالمستضيف او ما يسمى بـ(host-based firewall) او من خلال تشغيل برمجية مخصصة لذلك.
T1205	.001	Port Knocking	قد يقوم المهاجمين باستخدام (port knocking) بهدف إخفاء المنافذ المفتوحة او إخفاء بعض الوظائف الضارة والتي تستخدم بهدف تنفيذ تعليمات برمجية ضارة من شأنها تأمين البقاء أطول فترة ممكنه داخل النظام المخترق. ولكي يتم

			تفعيل/اغلاق المنافذ يقوم المهاجم بإرسال سلسلة من المحاولات التي تم تعريفها سابقاً. او يستطيع المهاجم استخدام بعض البرمجيات والتي من شأنها القيام بفتح المنافذ او اغلاقها في جدار الحماية الخاص بالمستضيف او ما يسمى بـ(host-based firewall)
T1127		Trusted Developer Utilities Proxy Execution	قد يقوم المهاجمين بالاستفادة من أدوات المطورين الموثوق بها واستخدامها لتنفيذ وايصال البرمجيات الضارة الخاصة بهم. وهناك العديد من الأدوات المساعدة في عملية تطوير البرمجيات والتي يمكن استخدامها من قبل المهاجمين. والتي قد تكون أدوات مستخدمة لتصحيح الأخطاء او للهندسة العكسية وغيرها. هذه الأدوات قد تكون أدوات موقعه رقمياً مما يريد من مستوى الثقة بها. والتي قد تودي الى تخطى عناصر ووسائل الحماية الموضوعة.
T1127	.001	MSBuild	قد يقوم المهاجمين باستخدام MSBuild لتنفيذ تعليمات برمجية ضارة. ان أداة MSBuild هي أداة موثوقة في أنظمة ويندوز وهي اختصار لي (Microsoft Build Engine) وهي نظام أساسي لإنشاء وتكوين البرمجيات الخاصة بـ Visual Studio والتي يتم التعامل معها من خلال امتدادات XML والتي تقوم هي بدورها بتحديد المتطلبات والاعدادات للأنظمة المراد انشاءها.
T1535		Unused/Unsupported Cloud Regions	قد يقوم المهاجمين بإنشاء نسخ من الخدمات السحابية في مناطق جغرافية غير معروفة وذلك بهدف التخفي من الاكتشاف. ان عملية الوصول لهذه الخدمات عادة ما يتم من خلال حسابات مخترقة سابقاً بهدف إدارة البنية التحتية.
T1550		Use Alternate Authentication Material	يستخدم المهاجمين ادوات مصادقة بديلة، مثل كلمة المرور المختزلة (password hashes) ، وتذاكر Kerberos ، ورموز الوصول إلى التطبيق، من أجل التنقل داخل الشبكة وتجاوز تقنيات التحكم في الوصول إلى الأنظمة.
T1550	.001	Application Access Token	يستخدم المهاجم رموز مسروقة للوصول إلى التطبيقات لتجاوز عملية المصادقة النموذجية والوصول إلى الحسابات أو المعلومات أو الخدمات المقيدة على الأنظمة الأخرى. عادةً ما تتم سرقة هذه الرموز المميزة من المستخدمين واستخدامها بدلاً من بيانات اعتماد تسجيل الدخول.
T1550	.002	Pass the Hash	يقوم المهاجمين باستخدام تقنية Hash Pass The مع كلمات المرور التي تم سرقتها للتحرك داخل الشبكة، متخطين تقنيات التحكم في الوصول إلى الأنظمة. Pass the hash PtH هي طريقة للمصادقة كمستخدم دون الوصول إلى كلمة مرور الغير مشفرة التابعة للمستخدم. تتجاوز هذه الطريقة خطوات المصادقة القياسية التي تتطلب كلمة مرور غير مشفرة ، والانتقال مباشرة إلى جزء المصادقة الذي يستخدم كلمة مرور مختزلة.
T1550	.003	Pass the Ticket	قد يقوم المهاجمين باستخدام تقنية Ticket Pass the مع كلمات المرور التي تم سرقتها للتحرك داخل الشبكة، متخطين تقنيات التحكم في الوصول إلى الأنظمة. Pass the ticket (PtT) هي طريقة للمصادقة على نظام يستخدم تذاكر Kerberos دون الوصول إلى كلمة مرور الحساب. يمكن استخدام مصادقة Kerberos كخطوة أولى للحركة داخل أنظمة أخرى .
T1550	.004	Web Session Cookie	قد يقوم المهاجم بسرقة معلومات الجلسة (session cookies) للحصول على صلاحيات مصادقة لخدمات الويب. تتجاوز هذه التقنية بعض البرتوكولات لان الجلسة تمت مصادقتها من المستخدم الفعلي بشكل سليم.
T1078		حساب فعال / Valid Accounts	قد يقوم المهاجم باستغلال بيانات الاعتماد للحسابات الفعالة وذلك بهدف الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. ان بيانات الاعتماد المخترقة قد يستخدم لتخطي عناصر التحكم بالوصول (access controls) التي تم تطبيقها على الأنظمة والموارد الخاصة بالشبكة. وقد يتم استخدام هذه الحسابات للوصول للأنظمة عن بعد او الخدمات مثل VPN او البريد الالكتروني او سطح المكتب البعيد من خلال المتصفح. وقد يتم استخدام بيانات الاعتماد المخترقة لتصعيد الصلاحيات لأنظمة محدد او الوصول الى منطقة حساسة داخل الشبكة المستهدفة. وقد يقوم المهاجم بتنفيذ عملياته الضارة ببيانات الاعتماد المخترقة دون الحاجة الى تبيث بعض البرمجيات الضارة والتي قد تؤدي الى اكتشافه.

T1078	.001	حساب افتراضي / Default Accounts	قد يقوم المهاجم بالحصول على بيانات الاعتماد للحسابات الافتراضية في النظام والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. ان الحسابات الافتراضية هي التي يتم انشاءها بشكل افتراضي داخل الأنظمة مثل حساب (Guest او Administrator) في نظام ويندوز. الحسابات الافتراضية قد تأتي كذلك من الأنظمة الخاصة ببعض العتاد من الشركة المصنعة. والتي قد تكون حساب مدير للنظام. ان حساب مدير النظام الخاص بخدمات (AWS) وحساب الخدمات الافتراضي في (Kubernetes)
T1078	.002	حساب مدير النظام / Domain Accounts	قد يقوم المهاجمين باستغلال بيانات الاعتماد الخاصة بمدراء النطاق (domain account) والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. ان حسابات مدراء النطاق والتي يتم التحكم بها من قبل (Service Active Directory Domain) والتي من خلالها يتم إعطاء الصلاحيات و التكوين لخدمات للنظام. ومن الممكن ان تكون حسابات مدراء. النظام عبارة عن حسابات مستخدمين او خدمات.
T1078	.003	حساب محلي / Local Accounts	قد يقوم المهاجمين باستغلال بيانات الاعتماد الخاصة بالحسابات المحلية (local account) والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. الحسابات المحلية يتم اعدادها من قبل المنظمة بهدف تقديم خدمات الدعم للأنظمة عن بعد او لتفعيل بعض الخدمات الوصول للأنظمة و ادارتها.
T1078	.004	حساب الخدمات الحسابية / Cloud Accounts	قد يقوم المهاجمين باستغلال بيانات الاعتماد الخاصة بالحسابات على الخدمات السحابية (cloud account) والتي تمكنه من الوصول الاولي او البقاء أطول فترة ممكنه داخل النظام المخترق او تصعيد الصلاحيات او التهرب من الاكتشاف. حسابات الخدمات السحابية قد يتم انشاءها واعدادها من قبل المنظمة بهدف تقديم خدمات الدعم للأنظمة عن بعد او لتفعيل بعض الخدمات الوصول للأنظمة وادارتها او التطبيقات. قد يتم توحيد الحسابات الخاصة بالخدمات السحابية مع الحسابات في النطاقات (Window Active Directory)
T1497		Virtualization/Sandbox Evasion	قد يقوم المهاجمين بإنشاء وسائل مختلفة لتهرب من الاكتشاف والتي تشتمل عمليات التحليل في البيئة الافتراضية. وقد يقوم المهاجم بتغير سلوك البرمجية الضارة بناء على المعطيات التي يقوم بقراءتها عند تشغيل البرمجية الضارة فعند وجود دلالة على ان هذه البيئة هي افتراضية يقوم بحماية نفسه او إخفاء الوظائف الرئيسية التي يقوم بها البرنامج. وعادة ما يستخدم المهاجمين في برمجياتهم ما يسمى بـ(Virtualization/Sandbox Evasion) بشكل تلقائي عند عملية التشغيل وذلك لاكتشاف ماهي البيئة المراد تشغيل البرمجية الضارة بها.
T1497	.001	فحص النظام / System Checks	قد يقوم المهاجمين بإنشاء وسائل مختلفة لتهرب من الاكتشاف والتي تشتمل عمليات فحص النظام وحال وجد انه في البيئة الافتراضية. وقد يقوم المهاجم بتغير سلوك البرمجية الضارة بناء على المعطيات التي يقوم بقراءتها عند تشغيل البرمجية الضارة فعند وجود دلالة على ان هذه البيئة هي افتراضية يقوم بحماية نفسه او إخفاء الوظائف الرئيسية التي يقوم بها البرنامج. وعادة ما يستخدم المهاجمين في برمجياتهم ما يسمى بـ(Virtualization/Sandbox Evasion) بشكل تلقائي عند عملية التشغيل وذلك لاكتشاف ماهي البيئة المراد تشغيل البرمجية الضارة بها.
T1497	.002	User Activity Based Checks	قد يقوم المهاجمين بإنشاء وسائل مختلفة لتهرب من الاكتشاف والتي تشتمل عمليات فحص سلوك المستخدم وحال وجد انه في البيئة الافتراضية. وقد يقوم المهاجم بتغير سلوك البرمجية الضارة بناء على المعطيات التي يقوم بقراءتها عند تشغيل البرمجية الضارة فعند وجود دلالة على ان هذه البيئة هي افتراضية يقوم بحماية نفسه او إخفاء الوظائف الرئيسية التي يقوم بها البرنامج. وعادة ما يستخدم المهاجمين في برمجياتهم ما يسمى بـ(Virtualization/Sandbox Evasion) بشكل تلقائي عند عملية التشغيل وذلك لاكتشاف ماهي البيئة المراد تشغيل البرمجية الضارة بها.
T1497	.003	Time Based Evasion	قد يقوم المهاجم بتنفيذ بعض الطرق التي من شانها اكتشاف انه داخل بيئة افتراضية مثل التلاعب بالوقت. وفي بعض الاحيان يقوم المهاجم بتحليل البنية الخاصة بالنظام ومعرفة اوقت وساعة النظام وذلك بهدف معرفة في حال كان في بيئة افتراضية او

			(SandBox) وحمايته نفسه من تنفيذ تعليمات برمجية قد تفضح الأساليب المستخدمة. وقد تكون تلك العمليات محدده بوقت او تعمل في بداية التشغيل.
T1600		التشفير الضعيف / Weaken Encryption	قد يقوم المهاجم باختراق أجهزة التشفير على مستوى الشبكة بهدف تخطي التشفير وقراءة البيانات المارة.
T1600	.001	Reduce Key Space	قد يقوم المهاجم بتقليل حجم الجهد المطلوب لكسر التشفير وذلك من خلال تقليل قوة التشفير قبل نقلها على الشبكة.
T1600	.002	Disable Crypto Hardware	قد يقوم المهاجم بتعطيل أجهزة تشفير البيانات على مستوى الشبكة وذلك بهدف الاستفادة وتقليل وقت كسر التشفير والقدرة على جمع البيانات المارة ومعالجتها واستخراج المفيد منها.
T1220		XSL Script Processing	قد يقوم المهاجمين بحجب بعض عناصر التحكم بالأمان من التحقق من البرمجيات او اعتراضها من خلال تضمين سكربتات داخل ملفات XSL. ان (Extensible Stylesheet Language XSL) ملفات تستخدم بشكل شائع في وصف العمليات وعرض البيانات في ملفات XML. يتضمن معيار XSL دعماً لقراءة السكربتات التي يتم تضمينها بمختلف اللغات البرمجية.

الحصول على بيانات الاعتماد / Credential Access

الحصول على بيانات الاعتماد: تتم من خلال اتباع أساليب وتقنيات يقوم بها المهاجم بهدف سرقة أسماء المستخدمين وكلمات المرور، وتشتمل الأساليب والتقنيات للحصول على بيانات الاعتماد بطرق مختلفة منها مسجل ضربات المفاتيح او سحب كلمات المرور. ومن خلال استخدام بيانات اعتماد صحيحة وفعالة قد تمكن المهاجم من اختراق الأنظمة والتي تعطي المهاجم ميزة وهي صعوبة اكتشافه وتعطيه الصلاحية كذلك في انشاء حسابات أخرى.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1110		كسر كلمات المرور / Brute Force	قد يستخدم المهاجمين تقنيات القوة الغاشمة للوصول إلى بيانات الاعتماد عندما تكون كلمات المرور غير معروفة أو عند الحصول على هاش لكلمات المرور. بدون معرفة كلمة المرور لحساب أو مجموعة من بيانات الاعتماد، قد يخمن المهاجم كلمة المرور بشكل منهجي باستخدام آلية برمجية لتجربة عدة محاولات. كسر كلمات المرور تعمل من خلال التفاعل مع الخدمة التي سوف تتحقق من صحة بيانات الاعتماد لبيانات الاعتماد.
T1110	.001	تخمين كلمة المرور / Password Guessing	المهاجمين الذين ليس لديهم معرفة مسبقة ببيانات الاعتماد الحساب المشروعة داخل النظام أو البيئة قد يخمنون كلمات المرور لمحاولة الوصول إلى الحسابات. بدون معرفة كلمة المرور للحساب، قد يختار المهاجم تخمين كلمة المرور بشكل منهجي باستخدام آلية برمجية لتجربة عدة محاولات. قد يخمن المهاجم بيانات اعتماد الحساب لتسجيل الدخول دون معرفة مسبقة بكلمات مرور النظام أو البيئة أثناء العملية باستخدام قائمة من كلمات المرور الشائعة. قد يبحث المهاجم عند تخمين كلمة المرور بعين الاعتبار سياسات الهدف بشأن استخدام تقنية تعقيد كلمة المرور أو استخدام السياسات التي قد تغلق الحسابات بعد عدد من المحاولات الفاشلة.
T1110	.002	كسر كلمات المرور / Password Cracking	قد يقوم المهاجمين باستخدام هجمات كسر لمحاولة استعادة كلمات المرور المحفوظة من غير تشفير، وقد يقوم المهاجم باستخدام كلمات المرور المشفرة كذلك في هجمات أخرى مثل (Pass The Hash). وقد يتم استخدام هجمات أخرى للحصول على كلمات المرور مثل Rainbow table. وعادة ما يتم استخدام مثل هذه الهجمة في كسر كلمات المرور على أنظمة يقوم المهاجم بالتحكم بها خارج الشبكة المستهدفة. وقد ينتج عنها كسر كلمات المرور والتي قد تستخدم لتسجيل الوصول للأنظمة والخدمات المستهدفة.
T1110	.003	كسر كلمات المرور Password Spraying	قد يستخدم المهاجمين قائمة واحدة أو صغيرة من كلمات المرور شائعة الاستخدام ضد العديد من الحسابات المختلفة لمحاولة الحصول على بيانات حساب المستخدم الصالحة. يستخدم كسر كلمة المرور كلمة مرور واحدة (مثل "Password01") ، أو قائمة صغيرة من كلمات المرور شائعة الاستخدام، والتي قد تتطابق مع سياسة الامنية الخاصة بالضحية. تتم محاولة تسجيل الدخول باستخدام كلمة المرور هذه ضد العديد من الحسابات المختلفة على الشبكة لتجنب عمليات إغلاق الحساب التي تحدث عادةً عند فرض حساب واحد باستخدام العديد من كلمات المرور.
T1110	.004	Credential Stuffing	قد يستخدم المهاجمين بيانات الحسابات التي تم الحصول عليها من عمليات Dumping للحسابات غير ذات الصلة للوصول إلى الحسابات المستهدفة من خلال تداخل بيانات الحسابات. من حين لآخر، يتم تسريب عدد كبير من اسماء المستخدمين وكلمات المرور عبر الإنترنت عند اختراق موقع ويب أو خدمة والوصول إلى بيانات حسابات المستخدم. قد تكون المعلومات مفيدة للمهاجم لمحاولة اختراق الحسابات من خلال الاستفادة من عادة المستخدمين إلى استخدام نفس كلمات المرور في الحسابات الشخصية والتجارية.
T1555	.004	Credentials from Password Stores	قد يبحث المهاجمين عن مواقع يتم فيها تخزين كلمات المرور الشائعة للحصول على بيانات حسابات المستخدمين. يتم تخزين كلمات المرور في عدة أماكن على النظام، اعتمادًا على نظام التشغيل أو التطبيق الذي يحمل بيانات حسابات المستخدم. هناك أيضًا تطبيقات محددة تخزن كلمات المرور لتسهيل إدارتها وصيانتها على المستخدمين. بمجرد الحصول على بيانات الحسابات ، يمكن استخدامها لأداء التنقل داخل الشبكة والوصول إلى المعلومات المحمية.
T1555	.001	Keychain	قد يقوم المهاجمين بجمع بيانات تخزين سلسلة المفاتيح من النظام للحصول على بيانات حسابات المستخدمين. سلاسل المفاتيح هي الطريقة المضمنة لنظام macOS لتتبع كلمات مرور المستخدمين وبيانات حساباتهم للعديد من الخدمات والميزات مثل كلمات مرور WiFi ومواقع الويب والملاحظات الآمنة والشهادات و Kerberos. توجد ملفات Keychain في ~ / Library / Keychains / و / Library / Keychains / و / Network / Library / Keychains /. توفر أداة سطر أوامر الأمان، المضمنة في macOS افتراضيًا، طريقة مفيدة لإدارة بيانات حسابات المستخدمين هذه.

T1555	.002	Securityd Memory	قد يحصل المهاجم على حق الوصول إلى صلاحية المسؤول (مما يسمح له بقراءة ذاكرة securityd) ، ثم يمكنه المسح عبر الذاكرة للعثور على التسلسل الصحيح للمفاتيح في عدد قليل نسبيًا من المحاولات لفك تشفير سلسلة مفاتيح تسجيل دخول المستخدم. هذا يوفر للمهاجم جميع كلمات مرور الغير مشفرة للمستخدمين، WiFi ، البريد، المتصفحات، الشهادات، الملاحظات المحمية، إلخ.
T1555	.003	كلمات المرور من المتصفحات / Credentials from Web Browsers	قد يحصل المهاجمين على بيانات الاعتماد من متصفحات الويب من خلال قراءة الملفات الخاصة بالمستعرض الخاص بالهدف. عادةً ما تحفظ مستعرضات الويب بيانات اعتماد مثل أسماء مستخدمي مواقع الويب وكلمات المرور بحيث لا تحتاج إلى إدخالها يدويًا في المستقبل. عادة ما تقوم متصفحات الويب بتخزين بيانات الاعتماد بتنسيق مشفر داخل متجر بيانات الحسابات؛ ومع ذلك، توجد هناك طرق لاستخراج بيانات الاعتماد الغير مشفرة من متصفحات الويب.
T1555	.004	Windows Credential Manager	قد يحصل المهاجمين على بيانات الحسابات من مدير بيانات الحسابات لنظام التشغيل ويندوز. يخزن مدير حسابات بيانات الاعتماد لتسجيل الدخول إلى مواقع الويب والتطبيقات و أو الأجهزة التي تطلب المصادقة من خلال NTLM أو Kerberos في خزائن بيانات الحسابات (المعروفة سابقًا باسم Vaults Windows).
T1555	.005	Password Managers	قد يحصل المهاجمين على بيانات حساب المستخدم من مديري كلمات المرور التابعين لجهات خارجية. تعد إدارة كلمات المرور تطبيقات مصممة لتخزين بيانات اعتماد المستخدم، عادةً في قاعدة بيانات مشفرة. يمكن الوصول إلى بيانات الاعتماد عادةً بعد أن يوفر المستخدم كلمة مرور رئيسية تفتح قاعدة البيانات. بعد إلغاء تأمين قاعدة البيانات، قد يتم نسخ بيانات الاعتماد هذه إلى الذاكرة. يمكن تخزين قواعد البيانات هذه كملفات على القرص الصلب.
T1212	.003	Exploitation for Credential Access	قد يستغل المهاجمين نقاط ضعف البرامج في محاولة لجمع بيانات الاعتماد للحسابات. يحدث استغلال ثغرة في البرنامج عندما يستغل المهاجم خطأ برمجي في برنامج أو خدمة أو داخل برنامج نظام التشغيل أو النواة نفسها لتنفيذ تعليمات برمجية يتحكم فيها المهاجم. قد يتم استهداف آليات الاعتماد والمصادقة للاستغلال من قبل المهاجمين كوسيلة للوصول إلى بيانات اعتماد الحسابات المفيدة أو التحايل على عملية الوصول إلى الأنظمة. أحد الأمثلة على ذلك هو MS14-068 ، والذي يستهدف Kerberos ويمكن استخدامه لتزوير تذاكر Kerberos باستخدام أذونات مستخدم في الشبكة. قد يؤدي استغلال الوصول إلى بيانات الاعتماد أيضًا إلى تصعيد الامتياز بناءً على العملية المستهدفة أو بيانات الاعتماد التي تم الحصول عليها.
T1187	.003	Forced Authentication	قد يقوم المهاجمين بجمع مواد الاعتماد عن طريق استدعاء أو إجبار المستخدم على تقديم معلومات المصادقة تلقائيًا من خلال آلية يمكنهم من خلالها الاعتراض.
T1606	.003	Forge Web Credentials	قد يقوم المهاجمين بتزوير مواد اعتماد يمكن استخدامها للوصول إلى تطبيقات الويب أو خدمات الإنترنت. غالبًا ما تستخدم تطبيقات وخدمات الويب (المستضافة في بيئات SaaS السحابية أو الخوادم المحلية) ملفات تعريف الارتباط للجلسة أو الرموز المميزة أو المواد الأخرى لمصادقة وصول المستخدم وتفويضه.
T1606	.001	كوكيز من الويب / Web Cookies	قد يقوم المهاجمين بتزوير ملفات تعريف ارتباط الويب التي يمكن استخدامها للوصول إلى تطبيقات الويب أو خدمات الإنترنت. غالبًا ما تستخدم تطبيقات وخدمات الويب (المستضافة في بيئات SaaS السحابية أو الخوادم المحلية) ملفات تعريف الارتباط للجلسة لمصادقة وصول المستخدم وتفويضه.
T1606	.002	SAML Tokens	قد يقوم المهاجمين بتزوير رموز SAML المميزة مع أي مطالبات أذونات لمدى الحياة إذا كان يمتلك شهادة توقيع رمز SAML صالحة. العمر الافتراضي لرمز SAML المميز هو ساعة واحدة، ولكن يمكن تحديد فترة الصلاحية في قيمة NotOnOrAfter للشروط ... عنصر في الرمز المميز. يمكن تغيير هذه القيمة باستخدام AccessTokenLifetime في LifetimeTokenPolicy. تمكّن رموز SAML المزورة للمهاجمين من المصادقة عبر الخدمات التي تستخدم SAML 2.0 كآلية SSO (تسجيل دخول فردي).
T1056		Input Capture	قد يستخدم المهاجمين طرقًا لالتقاط مدخلات المستخدم للحصول على بيانات الاعتماد أو جمع المعلومات. أثناء الاستخدام العادي للنظام، غالبًا ما يوفر المستخدمون بيانات اعتماد لمواقع مختلفة ، مثل صفحات/بوابات تسجيل الدخول أو في النظام. قد تكون آليات التقاط

			المدخلات شفافة للمستخدم (مثل ربط واجهة برمجة تطبيقات بيانات الاعتماد) أو تعتمد على خداع المستخدم لتقديم مدخلات فيما يعتقدون أنه خدمة أصلية (مثل Web Portal Capture).
T1056	.001	تسجيل كلمات المرور / Keylogging	قد يقوم المهاجمين بتسجيل ضغطات مفاتيح المستخدم لاعتراض بيانات الاعتماد أثناء قيام المستخدم بكتابتها. من المحتمل استخدام Keylogging للحصول على بيانات اعتماد لفرص وصول جديدة عندما لا تكون جهود سحب بيانات اعتماد نظام التشغيل فعالة، وقد تتطلب من المهاجم اعتراض ضغطات المفاتيح على النظام لفترة طويلة من الوقت قبل التمكن من التقاط بيانات الاعتماد بنجاح.
T1056	.002	GUI Input Capture	قد يحاكي المهاجمين مكونات واجهة المستخدم الرسومية لنظام التشغيل الشائعة لمطالبة المستخدمين ببيانات الاعتماد مع مطالبة تبدو مشروعة. عندما يتم تنفيذ البرامج التي تحتاج إلى امتيازات إضافية غير الموجودة في سياق المستخدم الحالي، فمن الشائع لنظام التشغيل مطالبة المستخدم ببيانات الاعتماد المناسبة لتفويض الامتيازات المرتفعة للمهمة (على سبيل المثال: تجاوز تحكم حساب المستخدم)
T1056	.003	Web Portal Capture	قد يقوم المهاجمين بتثبيت برمجية على بوابات خارجية، مثل صفحة تسجيل الدخول إلى VPN، لالتقاط ونقل بيانات اعتماد المستخدمين الذين يحاولون تسجيل الدخول إلى الخدمة. على سبيل المثال ، قد تسجل صفحة تسجيل الدخول المخترقة بيانات اعتماد المستخدم المقدمة قبل تسجيل دخول المستخدم إلى الخدمة.
T1056	.004	Credential API Hooking	قد يرتبط المهاجمين بوظائف واجهة برمجة تطبيقات (API Windows) لجمع بيانات اعتماد المستخدم. قد تلتقط آليات الربط الضارة استدعاءات واجهة برمجة التطبيقات التي تتضمن معلمات تكشف عن بيانات اعتماد مصادقة المستخدم. على عكس Keylogging ، تركز هذه التقنية بشكل خاص على وظائف API التي تتضمن المعلمات التي تكشف عن بيانات اعتماد المستخدم.
T1557		Man-in-the-Middle	قد يحاول المهاجمين وضع أنفسهم بين جهازين أو أكثر من الأجهزة المتصلة بالشبكة باستخدام تقنية (man-in-the-middle MiTM) لدعم سلوكيات المتابعة مثل التجسس في الشبكة أو التعديل على البيانات المنقولة. من خلال إساءة استخدام ميزات بروتوكولات الشبكات الشائعة التي يمكنها تحديد تدفق حركة مرور الشبكة (مثل ARP و DNS و LLMNR وما إلى ذلك) ، قد يجبر المهاجمين جهازًا على الاتصال من خلال نظام يتم التحكم فيه من قِبل المهاجم حتى يتمكنوا من جمع المعلومات أو تنفيذ اهداف إضافية.
T1557	.001	LLMNR/NBT-NS Poisoning and SMB Relay	من خلال الاستجابة لحركة مرور شبكة LLMNR/NBT-NS ، قد ينتحل المهاجمين مصدرًا موثوقًا لتحليل الاسم لفرض الاتصال بنظام يتم التحكم فيه من قبل الخصم. يمكن استخدام هذا النشاط لجمع أو نقل مواد المصادقة.
T1557	.002	ARP Cache Poisoning	قد يسمم المهاجمين بروتوكول تحليل العنوان (ARP) لوضع أنفسهم بين اتصال جهازين أو أكثر من الأجهزة المتصلة بالشبكة. يمكن استخدام هذا النشاط لتمكين سلوكيات المتابعة مثل التجسس في الشبكة أو التعديل على البيانات المنقولة.
T1556		Modify Authentication Process	قد يقوم المهاجمين بتعديل آليات وعمليات المصادقة للوصول إلى بيانات اعتماد المستخدم أو تمكين الوصول غير المبرر إلى الحسابات. تتم معالجة عملية المصادقة من خلال آليات، مثل عملية خادم مصادقة الأمان المحلي (LSASS) ومدير حسابات الأمان (SAM) على Windows، ووحدات المصادقة القابلة للتوصيل (PAM) على الأنظمة المستندة إلى Unix ، ومكونات الترخيص الإضافية على أنظمة MacOS، المسؤولة لجمع بيانات الاعتماد وتخزينها والتحقق منها. من خلال تعديل عملية المصادقة، قد يكون المهاجم قادرًا على المصادقة على خدمة أو نظام دون استخدام حسابات صالحة.
T1556	.001	Domain Controller Authentication	قد يقوم المهاجمين بتصحيح عملية المصادقة على Domain Controller لتجاوز آليات المصادقة النموذجية وتمكين الوصول إلى الحسابات.
T1556	.002	Password Filter DLL	قد يسجل المهاجمين مكتبات الارتباط الديناميكي (DLL) لتصفية كلمات المرور الضارة في عملية المصادقة للحصول على بيانات اعتماد المستخدم بمجرد التحقق من صحتها.

T1556	.003	Pluggable Authentication Modules	قد يقوم المهاجمين بتعديل وحدات المصادقة (PAM) للوصول إلى بيانات اعتماد المستخدم أو تمكين الوصول غير المبرر إلى الحسابات. PAM هو نظام معياري لملفات التكوين والمكتبات والملفات القابلة للتنفيذ والتي توجه المصادقة للعديد من الخدمات. وحدة المصادقة الأكثر شيوعًا هي pam_unix.so ، والتي تقوم باسترداد معلومات مصادقة الحساب وتعيينها والتحقق منها في / etc/passwd و / etc/shadow.
T1556	.004	Network Device Authentication	قد يستخدم المهاجمين Patch System Image لتشفير كلمة مرور في نظام التشغيل، وبالتالي تجاوز آليات المصادقة الأصلية للحسابات المحلية على أجهزة الشبكة.
T1040		التجسس على الشبكة / Network Sniffing	قد يتجسس المهاجمين على حركة مرور الشبكة لالتقاط معلومات حول بيئة الضحية، بما في ذلك مواد المصادقة التي يتم تمريرها عبر الشبكة. يشير تجسس الشبكة إلى استخدام وضعية الشبكة على نظام لمراقبة أو التقاط المعلومات المرسلة عبر اتصال سلكي أو لاسلكي. قد يضع المهاجم وضعية الشبكة في الوضع promiscuous للوصول بشكل غير تفاعلي إلى البيانات أثناء النقل عبر الشبكة، أو استخدام منافذ span لالتقاط كمية أكبر من البيانات.
T1003		سحب كلمات المرور / OS Credential Dumping	قد يحاول المهاجمين سحب بيانات الاعتماد للحصول على تسجيل الدخول إلى الحساب ومواد بيانات الاعتماد، عادةً في شكل كلمات مرور مختزلة أو كلمة مرور غير مشفرة، من نظام التشغيل والبرامج. يمكن بعد ذلك استخدام بيانات الاعتماد لإجراء للتنقل داخل الشبكة والوصول إلى المعلومات المقيد الوصول لها.
T1003	.001	LSASS Memory	قد يحاول المهاجمين الوصول إلى مواد الاعتماد المخزنة في ذاكرة العملية الخاصة بخدمة (LSASS). بعد أن يقوم المستخدم بتسجيل الدخول، يقوم النظام بإنشاء وتخزين مجموعة متنوعة من مواد الاعتماد في ذاكرة عملية LSASS. يمكن جمع مواد الاعتماد هذه بواسطة مستخدم يحمل صلاحية مدير مسؤول أو حساب نظام واستخدامها لإجراء تنقلات داخل الشبكة باستخدام استخدام مواد المصادقة البديلة.
T1003	.002	Security Account Manager	قد يحاول المهاجمين استخراج مواد الاعتماد من قاعدة بيانات إدارة حساب الأمان (SAM) إما من خلال تقنيات الذاكرة أو من خلال سجل Windows حيث يتم تخزين قاعدة بيانات SAM. SAM هو ملف قاعدة بيانات يحتوي على حسابات محلية للنظام، عادةً تلك التي يتم العثور عليها باستخدام الأمر net user. يتطلب جميع قاعدة بيانات SAM الوصول إلى مستوى النظام.
T1003	.003	NTDS	قد يحاول المهاجمين الوصول إلى أو إنشاء نسخة من قاعدة بيانات مجال Active Directory لسرقة معلومات الاعتماد، وكذلك الحصول على معلومات أخرى حول الحسابات في الشبكة مثل الأجهزة والمستخدمين وحقوق الوصول. بشكل افتراضي، يوجد ملف NTDS (NTDS.dit) في %SystemRoot%\NTDS\Ntds.dit لوحدة Domain Controller.
T1003	.004	LSA Secrets	قد يحاول المهاجمين الذين لديهم وصول SYSTEM في شبكة الضحية الوصول إلى (LSA)، والتي يمكن أن تحتوي على مجموعة متنوعة من مواد الاعتماد المختلفة، مثل بيانات اعتماد حسابات الخدمة. يتم تخزين أسرار LSA في التسجيل في HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets. يمكن أيضًا التخلص من أسرار LSA من الذاكرة.
T1003	.005	Cached Domain Credentials	قد يحاول المهاجمين الوصول إلى بيانات اعتماد المجال المخزنة مؤقتًا المستخدمة للسماح بحدوث المصادقة في حالة عدم توفر Domain Controller.
T1003	.006	DCSync	قد يحاول المهاجمين الوصول إلى بيانات الاعتماد والمعلومات الحساسة الأخرى عن طريق إساءة استخدام واجهة برمجة تطبيقات (API Windows Domain Controller) لمحاكاة عملية النسخ المتماثل من شبكة تحكم خارجية باستخدام تقنية تسمى DCSync.
T1003	.007	Proc Filesystem	قد يقوم المهاجمين بجمع بيانات الاعتماد من المعلومات المخزنة في نظام ملفات Proc أو /proc. يحتوي نظام ملفات Proc على Linux على قدر كبير من المعلومات المتعلقة بحالة نظام التشغيل التي قيد التشغيل. يمكن للعمليات التي تعمل بامتيازات مدير المسؤول استخدام هذه الميزة لكشف الذاكرة الحية للبرامج التي قيد التشغيل. إذا قامت أي من هذه البرامج بتخزين كلمات المرور بكلمة مرور غير مشفرة أو كلمات مرور مختزلة في الذاكرة، فيمكن عندئذٍ جمع هذه كلمات المرور للاستخدام أو لعمل هجوم القوة الغاشمة.

T1003	.008	/etc/passwd and /etc/shadow	قد يحاول المهاجمين تفريغ محتويات / etc/passwd و / etc/ shadow لتمكين اختراق كلمات المرور دون اتصال بالإنترنت. تستخدم معظم أنظمة تشغيل Linux الحديثة مجموعة من / passwd / etc و / etc / shadow لتخزين معلومات حساب المستخدم بما في ذلك كلمة مرور مختزلة في / etc/shadow. افتراضيًا، لا يمكن قراءة / etc/shadow إلا بواسطة مستخدم مدير المسؤول.
T1528		Steal Application Access Token	يمكن للمهاجمين سرقة رموز الوصول إلى تطبيق المستخدم كوسيلة للحصول على بيانات اعتماد للوصول إلى الأنظمة والموارد البعيدة. يمكن أن يحدث هذا من خلال الهندسة الاجتماعية وعادة ما يتطلب إجراء المستخدم لمنح حق الوصول.
T1558		Steal or Forge Kerberos Tickets	قد يحاول المهاجمين تخريب مصادقة Kerberos عن طريق سرقة أو تزوير تذاكر Kerberos لتمكين تمرير التذكرة.
T1558	.001	Golden Ticket	قد يقوم المهاجمين الذين لديهم كلمة مرور مختزلة لحساب KRBTGT بتزوير تذاكر منح تذكرة Kerberos (TGT)، والمعروفة أيضًا باسم التذكرة الذهبية. تمكن التذاكر الذهبية المهاجمين من إنشاء مواد توثيق لأي حساب في Active Directory.
T1558	.002	Silver Ticket	المهاجمين الذين لديهم كلمة مرور مختزلة لحساب خدمة خاص بالضحية (مثل SharePoint، MSSQL) قد يزورون تذاكر خدمة منح تذاكر Kerberos (TGS) ، والمعروفة أيضًا باسم التذاكر الفضية. تُعرف أيضًا تذاكر Kerberos TGS بتذاكر الخدمة.
T1558	.003	Kerberoasting	قد يسيء المهاجمين استخدام بطاقة منح تذكرة Kerberos صالحة (TGT) أو التنصت في حركة مرور الشبكة للحصول على تذكرة خدمة منح التذاكر (TGS) التي قد تكون عرضة لـ Brute Force.
T1558	.004	AS-REP Roasting	قد يكشف المهاجمين عن بيانات اعتماد الحسابات التي عطلت مصادقة Kerberos عن طريق مهاجمة كلمة المرور لرسائل Kerberos.
T1539		Steal Web Session Cookie	قد يسرق المهاجم ملفات تعريف ارتباط تطبيقات الويب أو جلسة الخدمة ويستخدمها للوصول إلى تطبيقات الويب أو خدمات الإنترنت كمستخدم مصادق عليه دون الحاجة إلى بيانات اعتماد. غالبًا ما تستخدم تطبيقات وخدمات الويب ملفات تعريف الارتباط للجلسة كرمز مميز للمصادقة بعد مصادقة المستخدم على موقع ويب.
T1111		Two-Factor Authentication Interception	قد يستهدف المهاجمين آليات المصادقة ذات العاملين FA2، مثل البطاقات الذكية، للوصول إلى بيانات الاعتماد التي يمكن استخدامها للوصول إلى الأنظمة والخدمات وموارد الشبكة. يوصى باستخدام مصادقة ثنائية أو متعددة العوامل (FA2 أو MFA) وتوفر مستوى أعلى من الأمان من أسماء المستخدمين وكلمات المرور وحدها، ولكن يجب أن تكون المؤسسات على دراية بالتقنيات التي يمكن استخدامها لاعتراض آليات الأمان هذه وعمل آلية دفاعية لمنعها.
T1552		Unsecured Credentials	قد يبحث المهاجمين عن الأنظمة المخترقة للعثور على بيانات اعتماد مخزنة بشكل غير آمن والحصول عليها. يمكن تخزين بيانات الاعتماد هذه أو وضعها في غير مكانها في العديد من المواقع على النظام، بما في ذلك ملفات الغير مشفرة (مثل Bash History) ، أو نظام التشغيل أو المستودعات الخاصة بالتطبيق (مثل بيانات الاعتماد في التسجيل)، أو الملفات/العناصر المتخصصة الأخرى (مثل المفاتيح الخاصة).
T1552	.001	بيانات الاعتماد داخل الملف / Credentials In Files	قد يقوم المهاجمين بالبحث في أنظمة الملفات المحلية ومشاركات الملفات البعيدة عن الملفات التي تحتوي على بيانات اعتماد مخزنة بشكل غير آمن. يمكن أن تكون هذه الملفات التي أنشأها المستخدمون لتخزين بيانات الاعتماد الخاصة بهم، أو مخازن بيانات الاعتماد المشتركة لمجموعة من الأفراد، أو ملفات التكوين التي تحتوي على كلمات مرور لنظام أو خدمة ، أو شفرة المصدر أو الملفات الثنائية التي تحتوي على كلمات مرور مضمنة.
T1552	.002	Credentials in Registry	قد يقوم المهاجمين بالبحث في السجل على الأنظمة المخترقة بحثًا عن بيانات اعتماد مخزنة بشكل غير آمن. يخزن سجل Windows معلومات التكوين التي يمكن أن يستخدمها النظام أو البرامج الأخرى. قد يستفسر المهاجمين من السجل بحثًا عن بيانات الاعتماد وكلمات المرور التي تم تخزينها للاستخدام من قبل برامج أو خدمات أخرى. في بعض الأحيان يتم استخدام بيانات الاعتماد هذه لعمليات تسجيل الدخول التلقائية.
T1552	.003	Bash History	قد يبحث المهاجمين في محفوظات أوامر bash على الأنظمة المخترقة بحثًا عن بيانات اعتماد مخزنة بشكل غير آمن. يتتبع Bash الأوامر التي يكتبها المستخدمون في سطر الأوامر باستخدام الأداة المساعدة "history". بمجرد تسجيل خروج المستخدم، يتم مسح السجل إلى

T1552	.004	Private Keys	قد يبحث المهاجمين عن ملفات شهادة المفتاح الخاص على الأنظمة المخترقة للحصول على بيانات اعتماد مخزنة بشكل غير آمن. تُستخدم مفاتيح وشهادات التشفير الخاصة للمصادقة والتشفير أو فك التشفير والتوقيعات الرقمية. تتضمن امتدادات ملفات الشهادة والمفتاح الشائعة: .key ، .pgp ، .gpg ، .ppk ، .p12 ، .pem ، .pfx ، .cer ، .p7b ، .asc..
T1552	.005	Cloud Instance Metadata API	قد يحاول المهاجمين الوصول إلى Instance Metadata API Cloud لجمع بيانات الاعتماد والبيانات الحساسة الأخرى.
T1552	.006	Group Policy Preferences	قد يحاول المهاجمين العثور على بيانات اعتماد غير آمنة في أعدادات (Group Policy Preferences). GPP هي أدوات تسمح للمسؤولين بإنشاء سياسات داخل المنظومة باستخدام بيانات الاعتماد المضمنة. تسمح هذه السياسات للمسؤولين بتعيين حسابات محلية.
T1552	.007	Container API	قد يجمع المهاجمين بيانات الاعتماد عبر واجهات برمجة التطبيقات API داخل بيئة حاويات. تسمح واجهات برمجة التطبيقات في هذه البيئات ، مثل Docker API و Kubernetes APIs ، للمستخدم بإدارة موارد الحاوية ومكونات المجموعة عن بُعد.
			ملف .bash_history الخاص بالمستخدم. لكل مستخدم، يوجد هذا الملف في نفس الموقع: ~ / .bash_history. عادةً ما يتتبع هذا الملف آخر 500 أمر للمستخدم. غالبًا ما يكتب المستخدمون أسماء المستخدمين وكلمات المرور في سطر الأوامر كمعلمات للبرامج، والتي يتم حفظها بعد ذلك في هذا الملف عند تسجيل الخروج. يمكن للمهاجمين إساءة استخدام هذا من خلال البحث في الملف عن بيانات الاعتماد المحتملة.

الاستطلاع والاكتشاف / Discovery

الاستطلاع: قد يقوم المهاجمين باستخدام الأساليب والتقنيات التي تمكنهم من الاستطلاع والاكتشاف داخل النظام او الشبكة المخترقة. ان هذه الأساليب تدعم المهاجمين في استطلاع الأنظمة للبيئة المستهدفة وتعطيهم الأفضلية في اتخاذ القرارات قبل القيام او تثبيت البرمجيات او التنقل داخل الشبكة. وتسمح كذلك هذه الأساليب للمهاجمين من الاطلاع على ما يمكنهم الوصول الية او التحكم به، وقد يقوم المهاجم باستخدام أدوات تأتي مع الأنظمة او برمجيات غير ضارة للاستفادة منها في عمليات الاستطلاع والاكتشاف.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1087		الاستطلاع بحث عن الحسابات / Account Discovery	قد يحاول المهاجمين الحصول على قائمة بالحسابات على نظام أو داخل البيئة المستهدفة. يمكن أن تساعد هذه المعلومات المهاجمين في تحديد الحسابات الموجودة للمساعدة في متابعة سلوكها.
T1087	.001	حساب محلي / Local Account	قد يحاول المهاجمين الحصول على قائمة بحسابات النظام الداخلية. يمكن أن تساعد هذه المعلومات المهاجمين في تحديد الحسابات الداخلية الموجودة على النظام للمساعدة في متابعة سلوكها.
T1087	.002	حساب مدير النظام / Domain Account	قد يحاول المهاجمين الحصول على قائمة بكل الحسابات التي داخل الشبكة المخترقة. يمكن أن تساعد هذه المعلومات المهاجمين في تحديد الحسابات الموجودة داخل الشبكة للمساعدة في متابعة سلوكها.
T1087	.003	حساب البريد / Email Account	قد يحاول المهاجمين الحصول على قائمة بعناوين البريد الإلكتروني والحسابات. قد يحاول المهاجمين سحب قوائم عناوين Exchange مثل قوائم العناوين العمومية (GALs).
T1087	.004	حساب الخدمات السحابية / Cloud Account	قد يحاول المهاجمين الحصول على قائمة بالحسابات السحابية. الحسابات السحابية هي تلك الحسابات التي تم إنشاؤها وتكوينها بواسطة شركة لاستخدامها من قبل المستخدمين أو الدعم عن بُعد أو الخدمات أو لإدارة الموارد داخل مزود خدمة سحابية أو تطبيق SaaS.
T1010		برمجيات اكتشاف الويندوز / Window Application Discovery	قد يحاول المهاجمين الحصول على قائمة برمجيات الويندوز المفتوحة. يمكن أن تنقل قوائم الويندوز معلومات حول كيفية استخدام النظام أو تعطي سياقًا للمعلومات التي تم جمعها بواسطة keylogger.
T1217		استطلاع المفضلة في المتصفح / Bookmark Browser Discovery	قد يقوم المهاجمين بجمع الإشارات المرجعية للمتصفح لمعرفة المزيد حول الضحية. قد تكشف إشارات المتصفح المرجعية عن معلومات شخصية عن المستخدمين (مثل: المواقع المصرفية ، والاهتمامات ، ووسائل التواصل الاجتماعي ، وما إلى ذلك) بالإضافة إلى تفاصيل حول موارد الشبكة الداخلية مثل الخوادم أو الأدوات أو لوحات المعلومات أو البنية التحتية الأخرى ذات الصلة.
T1580		اكتشاف واستطلاع البنية التحتية للخدمات السحابية / Cloud Infrastructure Discovery	قد يحاول المهاجم اكتشاف الموارد المتاحة داخل بيئة البنية التحتية للمنظمة مثلا كخدمة (IaaS). يتضمن ذلك موارد خدمة الحوسبة مثل الطابعات والأنظمة الافتراضية والنسخ الاحتياطية بالإضافة إلى موارد الخدمات الأخرى بما في ذلك خدمات التخزين وقواعد البيانات.
T1538		لوحة المراقبة للخدمات السحابية / Service Cloud Dashboard	قد يستخدم المهاجم واجهة المستخدم الرسومية GUI للوحة المراقبة للخدمة السحابية مع بيانات اعتماد مسروقة للحصول على معلومات مفيدة من بيئة سحابية تشغيلية، مثل خدمات وموارد وميزات محددة. على سبيل المثال، يمكن استخدام GCP Command Center لعرض جميع الأصول، وماهي نتائج المخاطر الأمنية المحتملة، ولإجراء استعلامات إضافية، مثل البحث عن عناوين IP العامة والمنافذ المفتوحة.
T1526		استطلاع الخدمات السحابية / Discovery Cloud Service	قد يحاول المهاجم جمع الخدمات السحابية التي تعمل على أي نظام بعد الدخول عليه. يمكن أن تختلف هذه الأساليب من النظام الأساسي كخدمة (PaaS)، إلى البنية التحتية كخدمة (IaaS)، أو البرامج كخدمة (SaaS). توجد العديد من الخدمات عبر مختلف موفري السحابة ويمكن أن تشمل التكامل المستمر والتسليم المستمر (CI / CD) ووظائف Lambda و Azure AD وما إلى ذلك.
T1613		Container and Resource Discovery	قد يحاول المهاجمين اكتشاف المستودعات والموارد الأخرى المتوفرة داخل بيئة المستودعات. قد تتضمن الموارد الأخرى الصور وعمليات النشر والبودات والعُقد ومعلومات أخرى مثل حالة Cluster.

T1482	استطلاع الثقة بين النطاقات / Discovery Domain Trust		قد يحاول المهاجمين جمع معلومات حول علاقات ثقة النطاق التي يمكن استخدامها لتحديد فرص التنقل داخل الشبكة في بيئات Windows متعددة النطاقات. توفر علاقات الثقة بالنطاق آلية للنطاق للسماح بالوصول إلى الموارد بناءً على إجراءات المصادقة الخاصة في نطاق آخر. تسمح علاقات الثقة بالنطاق لمستخدمي النطاق الموثوق به بالوصول إلى الموارد في نطاق الثقة. قد تساعد المعلومات المكتشفة للمهاجم في إجراء SID-History Injection، وتمرير التذكرة، و Kerberoasting. يمكن تعداد علاقات الثقة بالنطاق باستخدام استدعاء Win32 API () DSEnumerateDomainTrusts وأساليب .NET و LDAP. من المعروف أن الأداة المساعدة لـ Windows Nltest يتم استخدامها من قبل المهاجمين بجمع النطاقات الموثوقة.
T1083	الاستطلاع للملفات والمجلدات / File and Directory Discovery		قد يقوم المهاجمين بجمع الملفات والأدلة أو البحث في مواقع محددة في نظام ضحية أو مجلدات المشاركة في الشبكة عن معلومات معينة داخل نظام ملفات. قد يستخدم المهاجمين المعلومات من استطلاع الملفات والدليل أثناء الاكتشاف الآلي لمعرفة سلوكيات المتابعة، بما في ذلك ما إذا كان المهاجم يصيب الهدف بالكامل أم لا أو يحاول اتخاذ اهداف محددة.
T1046	استطلاع خدمات الشبكة / Network Service Scanning		قد يحاول المهاجمين الحصول على قائمة بالخدمات التي تعمل في الأنظمة عن بعد، بما في ذلك تلك التي قد تكون عرضة لاستغلال البرامج عن بُعد. تتضمن طرق الحصول على هذه المعلومات عمليات فحص المنافذ ومسح الثغرات الأمنية باستخدام الأدوات التي يتم تنزيلها في النظام.
T1135	استطلاع ملفات المشاركة / Network Share Discovery		قد يبحث المهاجمين عن المجلدات ومحركات الأقراص الصلبة المشتركة على الأنظمة التي تعمل عن بعد كوسيلة لتحديد مصادر المعلومات لتجميعها كمقدمة للتجميع ولتحديد الأنظمة المحتملة ذات الأهمية للتنقل داخل الشبكة. غالبًا ما تحتوي الشبكات على محركات أقراص صلبة ومجلدات مشتركة في الشبكة تمكّن المستخدمين من الوصول إلى مجلدات التي تحتوي على ملفات على أنظمة مختلفة عبر الشبكة.
T1040	التجسس على الشبكة / Network Sniffing		قد يتجسس المهاجمين على حركة مرور الشبكة لجمع معلومات حول بيئة ما، بما في ذلك مواد المصادقة التي يتم تمريرها عبر الشبكة. يشير تجسس الشبكة إلى استخدام واجهة الشبكة على نظام لمراقبة أو التقاط المعلومات المرسلة عبر اتصال سلكي أو لاسلكي. قد يضع المهاجم واجهة الشبكة في الوضع promiscuous للوصول بشكل غير تفاعلي إلى البيانات أثناء تنقلها عبر الشبكة، أو استخدام منافذ span لالتقاط كمية أكبر من البيانات.
T1201	الاطلاع على سياسة كلمات المرور / Password Policy Discovery		قد يحاول المهاجمين الوصول إلى معلومات مفصلة حول سياسة كلمة المرور المستخدمة داخل شبكة الضحية. سياسات كلمات المرور للشبكات هي طريقة لفرض كلمات مرور معقدة يصعب تخمينها أو اختراقها من خلال القوة العائمة. سيساعد هذا المهاجم على إنشاء قائمة بكلمات المرور الشائعة وإطلاق القاموس أو هجمات القوة العائمة التي تلتزم بالسياسة (على سبيل المثال ، إذا كان الحد الأدنى لطول كلمة المرور هو 8، فلا تحاول استخدام كلمات مرور مثل 'pass123' ؛ عدم التحقق من أكثر من 3-4 كلمات مرور لكل حساب إذا تم تعيين القفل على 6 لعدم قفل الحسابات).
T1120	Peripheral Device Discovery		قد يحاول المهاجمين جمع معلومات حول الأجهزة الطرفية والمكونات المتصلة بنظام الكمبيوتر. يمكن أن تتضمن الأجهزة الطرفية موارد إضافية تدعم مجموعة متنوعة من الوظائف مثل لوحات المفاتيح أو الطابعات أو الكاميرات أو قارئات البطاقات الذكية أو وحدات التخزين القابلة للإزالة. يمكن استخدام المعلومات لتعزيز وعيهم بالنظام وبيئة الشبكة أو يمكن استخدامها لمزيد من الإجراءات
T1069	استطلاع الصلاحيات للمجموعات / Permission Groups Discovery		قد يحاول المهاجمين العثور على إعدادات المجموعات والصلاحيات في نطاق الشبكة. يمكن أن تساعد هذه المعلومات المهاجمين في تحديد حسابات المستخدمين والمجموعات المتاحة، وعضوية المستخدمين في مجموعات معينة، والمستخدمين والمجموعات التي لديها صلاحيات عالية.

T1069	.001	المجموعات المحلية / Local Groups	قد يحاول المهاجمين العثور على مجموعات النظام المحلية وإعدادات الصلاحيات. يمكن أن تساعد معرفة صلاحية مجموعات في النظام المحلي المهاجمين في تحديد المجموعات الموجودة وأي المستخدمين ينتمون إلى مجموعة معينة. قد يستخدم المهاجمين هذه المعلومات لتحديد المستخدمين الذين لديهم صلاحيات عالية، مثل المستخدمين الموجودين ضمن مجموعة مدراء النظام المحليين.
T1069	.002	مجموعة مدراء النظام / Domain Groups	قد يحاول المهاجمين العثور على مجموعات على مستوى النطاق وإعدادات الصلاحيات. يمكن أن تساعد معرفة مجموعات مع الصلاحية الممنوحة على مستوى النطاق المهاجمين في تحديد المجموعات الموجودة وأي المستخدمين ينتمون إلى مجموعة معينة. قد يستخدم المهاجمين هذه المعلومات لتحديد المستخدمين الذين لديهم صلاحيات عالية، مثل مدراء أنظمة النطاق.
T1069	.003	مجموعة الخدمات السحابية / Cloud Groups	قد يحاول المهاجمين العثور على مجموعات الخدمات السحابية وإعدادات الصلاحيات. يمكن أن تساعد معرفة صلاحيات مجموعات السحابية المهاجمين في تحديد الأدوار المحددة للمستخدمين والمجموعات داخل بيئة ما، بالإضافة إلى المستخدمين المرتبطين بمجموعة معينة.
T1057		Process Discovery	قد يحاول المهاجمين الحصول على معلومات حول العمليات الجارية على النظام. يمكن استخدام المعلومات التي تم الحصول عليها لفهم البرامج أو التطبيقات الشائعة التي تعمل على الأنظمة داخل الشبكة. قد يستخدم المهاجمين المعلومات من عملية الاكتشاف أثناء الاكتشاف الآلي لتشكيل سلوكيات المتابعة، بما في ذلك ما إذا كان المهاجم ينوي أصابة الهدف بالكامل أم لا أو يحاول تنفيذ أهداف محددة.
T1012		Query Registry	قد يتفاعل المهاجمين مع سجل Windows لجمع معلومات حول النظام والتكوين والبرامج المثبتة.
T1018		اكتشاف والاستطلاع للخدمات عن بعد / Remote System Discovery	قد يحاول المهاجمين الحصول على قائمة بالأنظمة الأخرى حسب عنوان IP أو اسم الجهاز أو أي معرف آخر على شبكة يمكن استخدامها للتنقل داخل الشبكة من النظام الحالي. يمكن أن توجد الوظائف داخل أدوات الوصول عن بُعد لتمكين ذلك، ولكن يمكن أيضًا استخدام الأدوات المساعدة المتاحة على نظام التشغيل مثل Ping أو net view باستخدام Net. قد يستخدم المهاجمين أيضًا ملفات المضيف المحلية (على سبيل المثال: C:\Windows\System32\Drivers\etc\ hosts أو / etc/hosts) من أجل اكتشاف اسم المضيف لتعيينات عناوين IP للأنظمة البعيدة.
T1518		استطلاع البرمجيات / Software Discovery	قد يحاول المهاجمين الحصول على قائمة بإصدارات البرامج والبرامج المثبتة على نظام أو في بيئة سحابية. قد يستخدم المهاجمين المعلومات من Software Discovery أثناء الاكتشاف الآلي لتشكيل سلوكيات المتابعة، بما في ذلك ما إذا كان المهاجم ينوي أصابة الهدف بالكامل أم لا أو يسعى الى عمل أهداف محددة.
T1518	.001	استطلاع برمجيات الحماية / Software Security Discovery	قد يحاول المهاجمين الحصول على قائمة ببرامج الأمان والتكوينات والأدوات الدفاعية وأجهزة الاستشعار المثبتة على نظام أو في بيئة سحابية. قد يشمل ذلك أشياء مثل قواعد جدار الحماية ومكافحة الفيروسات. قد يستخدم المهاجمين المعلومات من Security Software Discovery أثناء الاكتشاف الآلي لتشكيل سلوكيات المتابعة، بما في ذلك ما إذا كان المهاجم ينوي أصابة الهدف بالكامل أم لا أو يسعى الى عمل أهداف محددة.
T1082		الاطلاع على معلومات النظام / Information System Discovery	قد يحاول المهاجم الحصول على معلومات مفصلة حول نظام التشغيل والأجهزة، بما في ذلك الإصدار والتصحيحات والإصلاحات وحزم الخدمة والبنية. قد يستخدم المهاجمين المعلومات من System Information Discovery أثناء الاكتشاف الآلي لتشكيل سلوكيات المتابعة، بما في ذلك ما إذا كان المهاجم ينوي أصابة الهدف بالكامل أم لا أو يسعى الى عمل أهداف محددة.
T1614		System Location Discovery	قد يقوم المهاجمين بجمع المعلومات في محاولة لحساب الموقع الجغرافي لجهاز الضحية. قد يستخدم المهاجمين المعلومات من System Location Discovery أثناء الاكتشاف الآلي لتشكيل سلوكيات المتابعة، بما في ذلك ما إذا كان المهاجم ينوي أصابة الهدف بالكامل أم لا أو يسعى الى عمل أهداف محددة.

T1016		الاطلاع على اعدادات الشبكة / System Network Configuration Discovery	قد يبحث المهاجمين عن تفاصيل حول تكوين الشبكة وإعدادات الأنظمة التي يصلون إليها أو من خلال اكتشاف معلومات الأنظمة البعيدة. توجد العديد من أدوات إدارة نظام التشغيل التي يمكن استخدامها لجمع هذه المعلومات. تتضمن الأمثلة Arp و / ipconfig و ifconfig و nbtstat و route.
T1016	.001	Internet Connection Discovery	قد يتحقق المهاجمين من وصول الأنظمة المخترقة الى الإنترنت. يمكن إجراء ذلك أثناء الاكتشاف الآلي ويمكن تحقيقه بعدة طرق مثل استخدام طلبات Ping و tracert و GET إلى مواقع الويب.
T1049		الاطلاع على الاتصالات الخاصة بنظام الشبكات / System Network Connections Discovery	قد يحاول المهاجمين الحصول على قائمة باتصالات الشبكة من أو إلى النظام المخترق الذي يصلون إليه حاليًا أو من الأنظمة البعيدة عن طريق الاستعلام عن المعلومات عبر الشبكة.
T1033		الاطلاع على بيانات مالك العنوان / System Owner/User Discovery	قد يحاول المهاجمين تحديد المستخدم الأساسي، أو المستخدم المسجل حاليًا، أو مجموعة المستخدمين التي تستخدم نظامًا بشكل شائع، أو ما إذا كان المستخدم يستخدم النظام بشكل نشط. يمكنهم القيام بذلك، على سبيل المثال، عن طريق استرداد أسماء مستخدمي الحساب أو باستخدام جمع بيانات الأعتماد نظام التشغيل. يمكن جمع المعلومات بعدة طرق مختلفة باستخدام تقنيات الاكتشاف الأخرى ، لأن تفاصيل المستخدم واسم المستخدم منتشرة في جميع أنحاء النظام وتشمل ملكية عمليات النظام الجارية، وملكية الملف/الدليل، ومعلومات الجلسة، وسجلات النظام. قد يستخدم المهاجم المعلومات من مالك النظام واكتشاف المستخدم أثناء الاكتشاف الآلي لتشكيل سلوكيات المتابعة، بما في ذلك ما إذا كان المهاجم ينوي أصابة الهدف بالكامل أم لا أو يسعى الى عمل أهداف محددة.
T1007		الاطلاع على خدمات النظام / System Service Discovery	قد يحاول المهاجمين الحصول على معلومات حول الخدمات المسجلة. الأوامر التي قد تحصل على معلومات حول الخدمات التي تستخدم أدوات نظام التشغيل هي "sc" و "Tasklist / svc" باستخدام Tasklist و "net start" باستخدام Net، ولكن قد يستخدم المهاجمين أيضًا أدوات أخرى. قد يستخدم المهاجمين المعلومات من System Service Discovery أثناء الاكتشاف الآلي لتشكيل سلوكيات المتابعة، بما في ذلك ما إذا كان المهاجم ينوي أصابة الهدف بالكامل أم لا أو يسعى الى عمل أهداف محددة.
T1124		الاطلاع على وقت النظام / System Time Discovery	قد يجمع المهاجم معلومات مثل وقت النظام أو المنطقة الزمنية من نظام محلي أو عن بعد. يتم تعيين وقت النظام وتخزينه بواسطة Windows Time Service داخل نطاق للحفاظ على مزامنة الوقت بين الأنظمة والخدمات في الشبكة.
T1497		Virtualization/Sandbox Evasion	قد يستخدم المهاجمين وسائل مختلفة لاكتشاف وتجنب بيئات المحاكاة الافتراضية والتحليل. قد يشمل ذلك تغيير سلوك المهاجم بناءً على نتائج عمليات التحقق من وجود الأدلة التي تشير وجوده على بيئة الآلة الافتراضية (VME) أو Sandbox. إذا اكتشف المهاجم وجود VME، قد يقوم بتغيير برمجياته الخبيثة لقطع الاتصال بالضحية أو إخفاء الوظائف الأساسية للبرمجية الخبيثة. يمكنهم أيضًا البحث عن أدوات VME قبل تنزيل برمجيات خبيثة ثانوية أو إضافية. قد يستخدم الأعداء المعلومات المستفادة من Evasion Virtualization/Sandbox أثناء الاكتشاف الآلي لمعرفة سلوكيات المتابعة.
T1497	.001	System Checks	قد يستخدم المهاجمين فحوصات مختلفة للنظام لاكتشاف وتجنب بيئات المحاكاة الافتراضية والتحليل. قد يشمل ذلك تغيير سلوك المهاجم بناءً على نتائج عمليات التحقق من وجود الأدلة التي تشير بأنه على بيئة الآلة الافتراضية (VME) أو Sandbox. إذا اكتشف المهاجم وجود VME، قد يقوم بتغيير برمجياته الخبيثة لقطع الاتصال بالضحية أو إخفاء الوظائف الأساسية للبرمجية الخبيثة. يمكنهم أيضًا البحث عن أدوات VME قبل تنزيل برمجيات خبيثة ثانوية أو إضافية. قد يستخدم الأعداء المعلومات المستفادة من Evasion Virtualization/Sandbox أثناء الاكتشاف الآلي لمعرفة سلوكيات المتابعة.
T1497	.002	User Activity Based Checks	قد يستخدم المهاجمين فحوصات مختلفة لنشاط المستخدم لاكتشاف وتجنب بيئات المحاكاة الافتراضية والتحليل. قد يشمل ذلك تغيير السلوك بناءً على نتائج عمليات التحقق من وجود دلائل التي تدل على بيئة الآلة الافتراضية (VME) أو sanbox. إذا اكتشف

			المهاجم وجود VME، قد يقوم بتغيير برمجياته الخبيثة لقطع الاتصال عن الضحية أو إخفاء الوظائف الأساسية للبرمجية الخبيثة التي تم زراعتها. يمكنهم أيضًا البحث عن أدوات VME قبل تنزيل برمجيات ثانوية أو إضافية. قد يستخدم المهاجمين المعلومات المستفادة من Sandbox Evasion / Virtualization أثناء الاكتشاف الآلي لتشكيل سلوكيات المتابعة.
T1497	.003	Time Based Evasion	قد يستخدم المهاجمين طرقًا مختلفة تستند إلى الوقت لاكتشاف وتجنب بيئات المحاكاة الافتراضية والتحليل. قد يشمل ذلك جمع الخصائص المستندة إلى الوقت، مثل مدة تشغيل النظام أو ساعة النظام، بالإضافة إلى استخدام أجهزة ضبط الوقت أو المشغلات الأخرى لتجنب بيئة الجهاز الظاهري (VME) أو Sandbox، وتحديدًا تلك التي تعمل تلقائيًا أو تعمل فقط لفترة محدودة من الوقت.

التنقل داخل الشبكة / Lateral Movement

التنقل داخل الشبكة: يقوم المهاجمين بالتنقل داخل الشبكة باستخدام أساليب وتقنيات مختلفة تمكنه من التحكم والتنقل في الأنظمة المخترقة عن بعد. وغالباً يقوم المهاجمين بمحاولة الاستطلاع والاكتشاف داخل الشبكة ومن ثم التنقل بين الأنظمة. ومن النتائج المرجوة من عمليات الاستطلاع والاكتشاف هو المقدرة على التنقل للنظام او الحسابات المكتشفة. وقد يلجأ المهاجم الى تثبيت برمجيات/أدوات تمكنه من التحكم والسيطرة على الأنظمة عن بعد وتتيح له فرصة التنقل ما بين الأنظمة. وقد يستخدم المهاجمين حسابات فعالة وحقيقة لعمليات التنقل داخل الشبكة والأنظمة والتي قد تصعب عمليات الاكتشاف.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1210		اختراق الخدمات عن بعد / Exploitation of Remote Services	يستغل المهاجم خدمات الوصول عن بُعد للحصول على وصول غير شرعي إلى الأنظمة الداخلية بمجرد دخوله الشبكة. يتم استغلال الثغرة في البرنامج عندما يكون هناك خطأ برمجي في بالبرنامج أو خدمة أو في برمجيات نظام التشغيل أو نواة التشغيل نفسها لتنفيذ برمجيات خبيثة يتحكم فيها من خلال المهاجم. الهدف الشائع لاستغلال الخدمات التي تتيح الوصول عن بُعد بعد الاختراق هو التنقل داخل الشبكة لتمكين الوصول إلى أنظمة أخرى.
T1534		التصيد الداخلي / Internal Spearphishing	يستخدم المهاجم التصيد الداخلي للوصول إلى معلومات إضافية أو استغلال مستخدمين آخرين داخل شبكة الضحية بعد أن يكون لديهم حق الوصول إلى الحسابات أو الأنظمة داخل الشبكة. التصيد الداخلي هو هجوم متعدد المراحل حيث ممكن أن يكون حساب البريد الإلكتروني مفعل في جهاز المستخدم والتحكم فيه يتم عن طريق برامج خبيثة مثبته مسبقًا أو عن طريق اختراق بيانات اعتماد حساب المستخدم. يحاول المهاجمين الاستفادة من حساب داخلي موثوق به لزيادة احتمالية خداع الضحية للوقوع في محاولة التصيد الاحتيالي.
T1570		Lateral Tool Transfer	يقوم المهاجمين بنقل أدوات أو ملفات مختلفة بين الأنظمة المخترقة في الشبكة. يقوم المهاجم بنسخ الملفات من نظام إلى آخر حتى يضمن بقاء الملفات والادوات طوال بقائة في الشبكة . يقوم المهاجم بنسخ الملفات بين الأنظمة المصابة الداخلية لدعم التنقل داخل الشبكة باستخدام بروتوكولات مشاركة الملفات الموجودة مثل مشاركة الملفات عبر SMB لمشاركة الشبكة المتصلة أو مع الاتصالات المصادق عليها مع SMB / Windows Admin Shares أو Protocol Remote Desktop. ويمكن أيضًا نسخ الملفات على نظامي Mac و Linux باستخدام أدوات مثل scp و rsync و sftp.
T1563		اختطاف الخدمات عن بعد Remote Service / Session Hijacking	من الشائع ان يتحكم المهاجم في الجلسات الموجودة مسبقًا مع خدمات الوصول عن بُعد للتنقل داخل الشبكة. يسمح للمستخدمين استخدام بيانات وثوق صالحة لتسجيل الدخول إلى خدمة مصممة خصيصًا لقبول الاتصالات عن بُعد ، مثل telnet و SSH و RDP. عندما يقوم المستخدم بتسجيل الدخول إلى إحدى الخدمات، سيتم إنشاء جلسة تسمح له بالحفاظ على جلسة تفاعلية مع تلك الخدمة.
T1563	.001	SSH Hijacking	يقوم المهاجم بالدخول الغير مشروع لجلسة SSH للمستخدم الفعلي للتنقل داخل الشبكة. يعد SSH (Secure Shell) وسيلة للوصول عن بُعد على أنظمة Linux و macOS. يسمح للمستخدم بالاتصال بنظام آخر عبر ممر مشفر، وعادة ما يتم المصادقة عليه من خلال كلمة مرور أو شهادة أو استخدام انواع مفاتيح تشفير غير متماثل.
T1563	.002	RDP Hijacking	يقوم المهاجم باختطاف جلسة سطح المكتب تفاعلية للمستخدم الشرعي للتنقل داخل الشبكة. يعد جلسة سطح المكتب ميزة شائعة في أنظمة التشغيل. يسمح للمستخدم بتسجيل الدخول إلى جلسة تفاعلية باستخدام واجهة مستخدم رسومية لسطح مكتب على نظام عن بعد. تشير Microsoft إلى تنفيذها لبروتوكول سطح المكتب البعيد RDP على أنه خدمات سطح المكتب البعيد (RDS)
T1021		الخدمات المتصلة عن بعد / Remote Services	يستخدم المهاجم الحسابات الصالحة لتسجيل الدخول إلى خدمة مصممة خصيصًا لقبول الاتصالات عن بُعد، مثل telnet و SSH و VNC. قد يقوم المهاجم بعد ذلك بتنفيذ عمليات بانتحاله صفة المستخدم الذي قام بتسجيل الدخول.
T1021	.001	سطح المكتب البعيد / Remote Desktop Protocol	يستخدم المهاجم حسابات صالحة لتسجيل الدخول إلى جهاز كمبيوتر باستخدام بروتوكول سطح المكتب البعيد (RDP). قد يقوم المهاجم بعد ذلك بتنفيذ عمليات بانتحاله صفة المستخدم الذي قام بتسجيل الدخول.

T1021	.002	مشاركة الملفات للويندوز / SMB/Windows Admin Shares	يستخدم المهاجم الحسابات الصالحة للتفاعل مع مشاركة شبكة بعيدة باستخدام SMB) Server Message Block) ويقوم المهاجم بعد ذلك بتنفيذ إجراءات بصفته المستخدم الذي قام بتسجيل الدخول.
T1021	.003	Distributed Component Object Model	يستخدم المهاجم الحسابات الصالحة للتفاعل مع الأجهزة البعيدة من خلال الاستفادة من Distributed Component Object Mode (DCOM) و يقوم المهاجم بعد ذلك بتنفيذ إجراءات بصفته المستخدم الذي قام بتسجيل الدخول.
T1021	.004	SSH	يستخدم المهاجم الحسابات الصالحة لتسجيل الدخول إلى الأجهزة البعيدة باستخدام SSH) Secure Shell). و يقوم المهاجم بعد ذلك بتنفيذ إجراءات بصفته المستخدم الذي قام بتسجيل الدخول
T1021	.005	VNC	يستخدم المهاجم الحسابات الصالحة للتحكم عن بعد في الأجهزة باستخدام حوسبة الشبكة الافتراضية VNC ويقوم المهاجم بعد ذلك بتنفيذ إجراءات بصفته المستخدم الفعلي الذي قام بتسجيل الدخول.
T1021	.006	Windows Remote Management	يستخدم المهاجم الحسابات الصالحة للتفاعل مع الأنظمة البعيدة باستخدامWinRM) Windows Remote Management) ويقوم المهاجم بعد ذلك بتنفيذ إجراءات بصفته المستخدم الفعلي الذي قام بتسجيل الدخول.
T1091		النسخ المتماثل من خلال الوسائط القابلة للإزالة / Replication Through Removable Media	ينتقل المهاجمون إلى الانظمة عن طريق شبكات قد تكون غير متصلة أو مفصولة تماما عن بعضها، وذلك يتم عن طريق نسخ البرامج الضارة إلى وسائط قابلة للإزالة والاستفادة من ميزات التشغيل التلقائي عند إدخال الوسائط في النظام وتشغيلها. في حالة التنقل داخل الشبكة، قد يحدث هذا من خلال تعديل الملفات القابلة للتنفيذ المخزنة على وسائط قابلة للإزالة أو عن طريق نسخ البرامج الضارة وإعادة تسميتها لتبدو وكأنها ملف شرعي لخداع المستخدمين لتنفيذه على نظام منفصل. في حالة الاختراق الأولي، قد يحدث هذا من خلال التعديل اليدوي للوسائط، أو تعديل الأنظمة المستخدمة في تهيئة الوسائط، أو التعديل على البرمجيات الأساسية للوسائط نفسها.
T1072		أدوات تطوير البرامج / Software Tools Deployment	يتمكن المهاجم من الوصول إلى برامج الطرف الثالث المثبتة داخل الشبكة، مثل أنظمة الإدارة والمراقبة والنشر، واستخدامها للتنقل داخل الشبكة. قد تكون تطبيقات وأنظمة نشر البرامج التابعة لطرف ثالث قيد الاستخدام في بيئة الشبكة لأغراض إدارية (على سبيل المثال ، SCCM، HBSS ، Altiris ، إلخ).
T1080		Taint Shared Content	قد يقوم المهاجم بتسليم Payloads إلى الأنظمة البعيدة عن طريق إضافة محتوى إلى مواقع التخزين المشتركة، مثل محركات أقراص الشبكة أو مستودعات البرمجيات الداخلية. قد يكون المحتوى المخزن على محركات أقراص الشبكة أو في مواقع مشتركة أخرى غير سليم (مضاف اليها برمجيات خبيثة) عن طريق إضافة برامج أو نصوص برمجية ضارة أو برمجية لاستغلال ملفات سليمة. بمجرد أن يفتح المستخدم المحتوى المعدل يبدا تشغيل البرنامج الضار على نظام البعيد. وقد يستخدم المهاجم ادوات مشبوه وضاره للتنقل داخل الشبكة.
T1550		ادوات المصادقة البديلة / Use Alternate Authentication Material	يستخدم المهاجمين ادوات مصادقة بديلة، مثل كلمة المرور المختزلة (password hashes) ، وتذاكر Kerberos ، ورموز الوصول إلى التطبيق، من أجل التنقل داخل الشبكة وتجاوز تقنيات التحكم في الوصول إلى الأنظمة.
T1550	.001	رمز الوصول الى التطبيق / Access Application Token	يستخدم المهاجم رموز مسروقة للوصول إلى التطبيقات لتجاوز عملية المصادقة النموذجية والوصول إلى الحسابات أو المعلومات أو الخدمات المقيدة على الأنظمة الأخرى. عادةً ما تتم سرقة هذه الرموز المميزة من المستخدمين واستخدامها بدلاً من بيانات اعتماد تسجيل الدخول.
T1550	.002	Pass the Hash	يقوم المهاجمين باستخدام تقنية Hash Pass The مع كلمات المرور التي تم سرقتها للتحرك داخل الشبكة، متخطين تقنيات التحكم في الوصول إلى الأنظمة. Pass the hash PtH هي طريقة للمصادقة كمستخدم دون الوصول إلى كلمة مرور الغير مشفرة التابعة

			للمستخدم. تتجاوز هذه الطريقة خطوات المصادقة القياسية التي تتطلب كلمة مرور غير مشفرة ، والانتقال مباشرة إلى جزء المصادقة الذي يستخدم كلمة مرور مختزلة.
T1550	.003	Pass the Ticket	قد يقوم المهاجمين باستخدام تقنية Ticket Pass the مع كلمات المرور التي تم سرقتها للتحرك داخل الشبكة، متخطين تقنيات التحكم في الوصول إلى الأنظمة. PtT) Pass the ticket) هي طريقة للمصادقة على نظام يستخدم تذاكر Kerberos دون الوصول إلى كلمة مرور الحساب. يمكن استخدام مصادقة Kerberos كخطوة أولى للحركة داخل أنظمة أخرى .
T1550	.004	Web Session Cookie	يمكن للمهاجمين استخدام ملفات تعريف ارتباط الجلسة المسروقة للمصادقة على تطبيقات وخدمات الويب. تتخطى هذه التقنية بعض بروتوكولات المصادقة متعددة العوامل نظرًا لأن الجلسة قد تمت مصادقتها بالفعل.

جمع البيانات الهامة / Collection

جمع البيانات: يقوم المهاجمين في هذه المرحلة بجمع المعلومات الهامة عن الهدف. ان التقنيات والأساليب في عملية جمع المعلومات متعددة وتختلف باختلاف الأهداف التي لدى المهاجمين. وتكون مرحلة جمع البيانات هي المرحلة الأولى قبل عملية تسريب وسرقة البيانات. وقد يتم جمع البيانات من مصادر مختلفة اما من الأقراص الصلبة او المتصفحات او ملفات فيديو او صوت او حتى البريد الالكتروني وقد تتضمن عملية جمع المعلومات تصوير الشاشة او تسجيل ضربات المفاتيح.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1560		سحب البيانات المؤرشفة / Archive Data Collected	يقوم المهاجم في أرشفة أو تشفير البيانات التي تم جمعها قبل تسريبها. يمكن أن يساعد أرشفة البيانات في تعتيم البيانات التي تم تجميعها وتقليل كمية البيانات المرسلة عبر الشبكة. يمكن استخدام التشفير لإخفاء المعلومات التي يتم تسريبها من عملية الاكتشاف أو جعل التطفل أقل وضوحًا عند الفحص بواسطة المحلل.
T1560	.001	اداة الارشفة Archive via Utility	قد يقوم المهاجم بضغط أو تشفير البيانات التي تم جمعها قبل سحبها من الضحية باستخدام أدوات مساعدة تابعة لطرف ثالث. توجد العديد من الأدوات المساعدة التي يمكنها أرشفة البيانات، بما في ذلك Zip-7 و WinRAR و WinZip.تتضمن معظم الأدوات المساعدة وظائف لتشفير أو ضغط البيانات.
T1560	.002	الارشفة بواسطة المكتبات البرمجية / via Library Archive	قد يقوم المهاجم بضغط أو تشفير البيانات التي تم جمعها قبل سحبها من الضحية باستخدام مكتبات الطرف الثالث. توجد العديد من المكتبات التي يمكنها أرشفة البيانات، بما في ذلك Python rarfile و libzip و zlib.تتضمن معظم المكتبات وظائف لتشفير أو ضغط البيانات.
T1560	.003	الارشفة بواسطة طرق مخصصة / Archive Custom via Method	قد يقوم المهاجم في ضغط أو تشفير البيانات التي تم جمعها قبل سحبها من الضحية باستخدام طريقة مخصصة. قد يختار المهاجمين استخدام أساليب أرشفة مخصصة، مثل التشفير باستخدام XOR أو استخدام ciphers stream التي يتم تنفيذها بدون مراجع مكتبة خارجية أو أداة مساعدة. كما ايضا قد يتم استخدام تطبيقات مخصصة لخوارزميات الضغط المعروفة.
T1123		تسجيل الاصوات / Audio Capture	يمكن للمهاجم الاستفادة من الأجهزة الطرفية للكمبيوتر (مثل الميكروفونات وكاميرات الويب) أو التطبيقات (مثل خدمات مكالمات الصوت والفيديو) لالتقاط التسجيلات الصوتية بغرض الاستماع إلى المحادثات الحساسة لجمع المعلومات.
T1119		تنزيل البيانات بشكل آلي / Automated Collection	بمجرد إنشائه داخل نظام أو شبكة، قد يستخدم المهاجم تقنيات آلية لجمع البيانات الداخلية. يمكن أن تتضمن طرق تنفيذ هذه التقنية استخدام مترجم الأوامر والنصوص للبحث عن المعلومات ونسخها التي تناسب معايير المجموعة مثل نوع,موقع أو الاسم الملف في فترات زمنية محددة. يمكن أيضًا تضمين هذه الوظيفة في أدوات الوصول عن بُعد.
T1115		البيانات المنسوخة / Clipboard Data	قد يقوم المهاجمين بجمع البيانات المخزنة في clipboard من المستخدمين الذين يقومون بنسخ المعلومات داخل أو بين التطبيقات.
T1530		البيانات المخزنة في المخازن السحابية / Data from Cloud Storage Object	قد يصل المهاجمين إلى البيانات التي في التخزين السحابية المؤمَّن بطريقة غير صحيحة.
T1602		بيانات الاعدادات المخزنة في المستودعات Data from / Configuration Repository	قد يقوم المهاجمين بجمع البيانات المتعلقة بالأجهزة المُدارة من المستودعات. يتم استخدام المستودعات بواسطة أنظمة الإدارة من أجل تكوين البيانات وإدارتها والتحكم فيها على الأنظمة البعيدة. قد تسهل المستودعات أيضًا الوصول عن بُعد وإدارة الأجهزة.
T1602	.001	SNMP (MIB Dump)	قد يستهدف المهاجمين قاعدة المعلومات الإدارية (MIB) لجمع أو استخراج معلومات قيمة في شبكة مُدارة باستخدام بروتوكول(SNMP).

T1602	.002	تنزيل اعدادات اجهزة الشبكات المخزنة / Network Device Configuration Dump	قد يصل المهاجمين إلى ملفات تكوين الشبكة لجمع بيانات حساسة حول الجهاز والشبكة. تكوين الشبكة عبارة عن ملف يحتوي على معلمات تحدد تشغيل الجهاز. يخزن الجهاز عادةً نسخة في الذاكرة من التكوين أثناء التشغيل، وتكوين منفصل على وحدة تخزين غير مستقرة للتحميل بعد إعادة ضبط الجهاز. يمكن للمهاجمين فحص ملفات التكوين للكشف عن معلومات حول الشبكة المستهدفة وتخطيطها، وجهاز الشبكة وبرامجه، أو تحديد الحسابات وبيانات الاعتماد الشرعية لاستخدامها لاحقًا.
T1213		البيانات المتوفرة في المستودعات / Data from Information Repositories	قد يستفيد المهاجمين من مستودعات البيانات لاستخراج المعلومات القيمة. مستودعات البيانات هي أدوات تسمح بتخزين المعلومات، عادةً لتسهيل التعاون أو مشاركة المعلومات بين المستخدمين، ويمكن تخزين مجموعة متنوعة من البيانات التي قد تساعد المهاجمين في أهداف أخرى، أو الوصول المباشر إلى المعلومات الهدف.
T1213	.001	مذكرة / Confluence	قد يستفيد المهاجمين من مستودعات Confluence لاستخراج المعلومات القيمة. غالبًا ما توجد في بيئات التطوير جنبًا إلى جنب مع Atlassian JIRA، يتم استخدام Confluence بشكل عام لتخزين الوثائق المتعلقة بالتنمية، ومع ذلك، قد تحتوي بشكل عام على فئات أكثر تنوعًا من المعلومات المفيدة.
T1213	.002	نظام / Sharepoint	قد يستفيد المهاجمين من مستودع SharePoint كمصدر لاستخراج المعلومات القيمة. غالبًا ما يحتوي SharePoint على معلومات مفيدة للمهاجم للتعرف على بنية ووظائف الشبكة والأنظمة الداخلية.
T1005		البيانات من النظام المحلي / Data from Local System	قد يبحث المهاجمين عن مصادر النظام المحلي، مثل أنظمة الملفات أو قواعد البيانات المحلية، للعثور على الملفات ذات الأهمية والبيانات الحساسة قبل عملية الاستخراج.
T1039		البيانات المتوفرة في مجلدات المشاركة / Data from Network Shared Drive	قد يبحث المهاجمين عن مشاركات الشبكة على أجهزة الكمبيوتر التي قاموا باختراقها للعثور على الملفات التي تهمهم. يمكن جمع البيانات الحساسة من أنظمة خارج الشبكة عبر محركات أقراص الشبكة المشتركة(الدليل المشترك المضيف، خادم ملفات الشبكة، إلخ) التي يمكن الوصول إليها من النظام الحالي قبل تسريبها الى خارج الشبكة. قد تكون الأوامر في الطرفية التفاعلية قيد الاستخدام، ويمكن استخدام الوظائف الشائعة داخل cmd لجمع المعلومات.
T1025		البيانات من وسائط التخزين المتنقلة / Data from Removable Media	قد يبحث المهاجمين عن الوسائط القابلة للإزالة المتصلة على أجهزة الكمبيوتر التي قاموا باختراقها للعثور على الملفات التي تهمهم. يمكن جمع البيانات الحساسة من أي وسائط قابلة للإزالة (محرك الأقراص الضوئية ، ذاكرة USB ، إلخ) متصلة بالنظام المخترق قبل عملية الاستخراج. قد تكون الأوامر من الطرفية التفاعلية قيد الاستخدام، ويمكن استخدام الوظائف الشائعة داخل cmd لجمع المعلومات.
T1074		البيانات المخزنة / Data Staged	قد يقوم المهاجمين بتنظيم البيانات التي تم جمعها في مسار مركزي أو مجلد قبل عملية تسريبها الى خارج الشبكة. يمكن الاحتفاظ بالبيانات في ملفات منفصلة أو دمجها في ملف واحد من خلال تقنيات مثل أرشفة البيانات Archive. يمكن استخدام الأوامر الطرفية التفاعلية، ويمكن استخدام الوظائف الشائعة داخل cmd و bash لنسخ البيانات إلى موقع تجريبي.
T1074	.001	البيانات المخزنة محلياً / Staging Local Data	قد يقوم المهاجمين بوضع البيانات التي تم جمعها في موقع مركزي أو مجلد على النظام المحلي قبل عملية تسريبها الى خارج الشبكة. يمكن الاحتفاظ بالبيانات في ملفات منفصلة أو دمجها في ملف واحد من خلال تقنيات مثل أرشفة البيانات Archive. يمكن استخدام الأوامر الطرفية التفاعلية، ويمكن استخدام الوظائف الشائعة داخل cmd و bash لنسخ البيانات إلى موقع تجريبي.
T1074	.002	البيانات المخزنة عن بعد / Remote Data Staging	قد يحاول المهاجمين وضع أنفسهم بين جهازين أو أكثر من الأجهزة المتصلة بالشبكة باستخدام تقنية (man-in-the-middle (MiTM لدعم سلوكيات المتابعة مثل التنصت في الشبكة أو التلاعب في البيانات المنقولة. من خلال إساءة استخدام ميزات بروتوكولات الشبكات

			الشائعة التي يمكنها تحديد تدفق حركة مرور الشبكة (مثل ARP و DNS و LLMNR وما إلى ذلك)، قد يجبر المهاجمين جهازًا على الاتصال من خلال نظام يتم التحكم فيه من قِبل المهاجم حتى يتمكنوا من جمع المعلومات أو تنفيذ اهداف إضافية.
T1114		تنزيل البريد الالكتروني / Email Collection	قد يستهدف المهاجمين البريد الإلكتروني للمستخدم لجمع معلومات حساسة. قد تحتوي رسائل البريد الإلكتروني على بيانات حساسة، بما في ذلك الأسرار التجارية أو المعلومات الشخصية، والتي يمكن أن تكون مفيدة للمهاجمين. يمكن للمهاجمين جمع البريد الإلكتروني أو إعادة توجيهه من خوادم البريد أو العملاء.
T1114	.001	تنزيل البريد الداخلي / Local Email Collection	قد يستهدف المهاجمين البريد الإلكتروني للمستخدم على الأنظمة المحلية لجمع معلومات حساسة. يمكن الحصول على الملفات التي تحتوي على بيانات البريد الإلكتروني من النظام المحلي للمستخدم، مثل تخزين Outlook أو ملفات ذاكرة التخزين المؤقت.
T1114	.002	تنزيل البريد عن بعد / Remote Email Collection	قد يقوم المهاجمين بإعداد قواعد إعادة توجيه البريد الإلكتروني لجمع المعلومات الحساسة. قد يسيء المهاجمين استخدام قواعد إعادة توجيه البريد الإلكتروني لمراقبة أنشطة الضحية، وسرقة المعلومات، واكتساب المزيد من المعلومات الاستخبارية عن الضحية أو منظمة الضحية لاستخدامها كجزء من عمليات استغلال أو عمليات أخرى. يسمح Outlook و OWA (Outlook Web App) للمستخدمين بإنشاء قواعد علبة الوارد لوظائف البريد الإلكتروني المختلفة، بما في ذلك إعادة التوجيه إلى مستلم مختلف. وبالمثل ، يمكن لمستخدمي أو مسؤولي Workspace Google إعداد قواعد إعادة توجيه البريد عبر واجهة ويب Google Workspace. يمكن إعادة توجيه الرسائل إلى مستلمين داخليين أو خارجيين، ولا توجد قيود تحد من مدى هذه القاعدة. يمكن للمسؤولين أيضًا إنشاء قواعد إعادة التوجيه لحسابات المستخدمين بنفس الاعتبارات والنتائج.
T1114	.003	قواعد تمرير البريد / Email Forwarding Rule	قد يستخدم المهاجمين طرقًا لجمع مدخلات المستخدم للحصول على بيانات الحسابات أو جمع المعلومات. أثناء الاستخدام العادي للنظام، غالبًا ما يوفر المستخدمون بيانات اعتماد لمواقع مختلفة ، مثل صفحات أو بوابات تسجيل الدخول أو مربعات حوار النظام. قد تكون آليات الجمع المدخلات شفافة للمستخدم (مثل ربط واجهة برمجة تطبيقات بيانات الحسابات) أو تعتمد على خداع المستخدم لتقديم مدخلات فيما يعتقدون أنه خدمة أصلية (مثل Portal Capture Web).
T1056		تسجيل وجمع المدخلات / Input Capture	قد يقوم المهاجمين بتسجيل ضربات مفاتيح المستخدم لاعتراض بيانات الاعتماد أثناء قيام المستخدم بكتابتها. من المحتمل أن يتم استخدام Keylogging للحصول على بيانات حسابات المستخدم لفرص وصول جديدة عندما لا تكون عملية Dumping بيانات حسابات نظام التشغيل فعالة، وقد تتطلب من المهاجم اعتراض ضربات المفاتيح على النظام لفترة طويلة من الوقت قبل التمكن من التقاط بيانات الحسابات المستخدم بنجاح.
T1056	.001	تسجيل ضربات المفاتيح / Keylogging	قد يقوم المهاجمين بتسجيل ضربات مفاتيح المستخدم لاعتراض بيانات حسابات المستخدم أثناء قيامه بكتابتها. من المحتمل أن يتم استخدام Keylogging للحصول على بيانات حسابات المستخدم لفرص وصول جديدة عندما لا تكون عملية الDumping بيانات حسابات مستخدم نظام التشغيل فعالة، وقد تتطلب من المهاجم اعتراض ضربات المفاتيح على النظام لفترة طويلة من الوقت قبل التمكن من التقاط بيانات حسابات المستخدمين بنجاح.
T1056	.002	تسجيل واجهة التطبيقات / GUI Input Capture	قد يحاكي المهاجمين مكونات واجهة المستخدم الرسومية GUI لنظام التشغيل الشائعة لمطالبة المستخدمين ببيانات حسابات الوصول مع مطالبة تبدو مشروعة. عندما يتم تنفيذ البرامج التي تحتاج إلى امتيازات إضافية غير الموجودة في سياق المستخدم الحالي، فمن الشائع لنظام التشغيل مطالبة المستخدم ببيانات حساب الوصول المناسبة لتفويض الامتيازات للمهمة (على سبيل المثال: تجاوز التحكم في حساب المستخدم).
T1056	.003	Web Portal Capture	قد يقوم المهاجمين بتثبيت برمجية على بوابات خارجية، مثل صفحة تسجيل الدخول إلى VPN، لالتقاط ونقل بيانات حسابات الوصول للمستخدمين الذين يحاولون تسجيل الدخول إلى الخدمة. على سبيل المثال، قد تسجل صفحة تسجيل الدخول المخترقة بيانات حساب المستخدم قبل تسجيل دخول المستخدم إلى الخدمة.

T1056	.004	سرقة بيانات / API Credential API Hooking	قد يرتبط المهاجمين بوظائف واجهة برمجة تطبيقات (API Windows) لجمع بيانات حسابات الوصول للمستخدم. قد تلتقط آليات الربط الضارة استدعاءات واجهة برمجة التطبيقات API التي تتضمن معلمات تكشف عن بيانات حسابات الوصول لمصادقة المستخدم. على عكس Keylogging، تركز هذه التقنية بشكل خاص على وظائف API التي تتضمن المعلمات التي تكشف عن بيانات حسابات المستخدم.
T1185		اعتراض البيانات من خلال المتصفح / Man in the Browser	قد يرتبط المهاجمين بوظائف واجهة برمجة تطبيقات (API Windows) لجمع بيانات حسابات المستخدم. قد تلتقط آليات الربط الضارة استدعاءات API التي تتضمن معلمات تكشف عن بيانات حسابات مصادقة المستخدم. على عكس Keylogging، تركز هذه التقنية بشكل خاص على وظائف API التي تتضمن المعلمات التي تكشف عن بيانات حسابات المستخدم.
T1557		اعتراض البيانات / Man-in-the-Middle	يمكن للمهاجمين الاستفادة من الثغرات الأمنية والوظائف الرئيسية في برنامج المتصفح لتغيير المحتوى وتعديل السلوك واعتراض المعلومات كجزء من تقنيات Man in The browser.
T1557	.001	LLMNR/NBT-NS Poisoning and SMB Relay	من خلال الاستجابة لحركة مرور شبكة NBT-NS / LLMNR ، قد ينتحل المهاجمين مصدرًا موثوقًا لتحليل الاسم لفرض الاتصال بنظام يتم التحكم فيه من قبل المهاجم. يمكن استخدام هذا النشاط لجمع أو نقل مواد المصادقة.
T1557	.002	ARP Cache Poisoning	قد يسمم المهاجمين بروتوكول(ARP) لوضع أنفسهم بين اتصال جهازين أو أكثر من الأجهزة المتصلة بالشبكة. يمكن استخدام هذا النشاط لتمكين سلوكيات المتابعة مثل التنصت في الشبكة أو التلاعب في البيانات المنقولة.
T1113		تسجيل الشاشة / Screen Capture	قد يحاول المهاجمين أخذ لقطات شاشة لسطح المكتب لجمع المعلومات على مدار العملية. قد يتم تضمين وظيفة التقاط الشاشة كميزة لأداة الوصول عن بعد المستخدمة في عمليات ما بعد الاختراق. عادةً ما يكون التقاط لقطة شاشة ممكنًا من خلال الأدوات المساعدة الأصلية أو استدعاءات واجهة برمجة التطبيقات ، مثل CopyFromScreen أو xwd أو screencapture.
T1125		تسجيل الفيديو / Video Capture	يمكن للمهاجم الاستفادة من الأجهزة الطرفية للكمبيوتر (على سبيل المثال ، الكاميرات المدمجة أو كاميرات الويب) أو التطبيقات (مثل خدمات مكالمات الفيديو) لالتقاط تسجيلات الفيديو بغرض جمع المعلومات. يمكن أيضًا التقاط الصور من الأجهزة أو التطبيقات، في فترات زمنية محددة، بدلاً من ملفات الفيديو.

التحكم والسيطرة / Command and Control

التحكم والسيطرة: يقوم المهاجم باستخدام وسائل متعددة لتحكم والسيطرة بالنظام المستهدف وتختلف التقنيات والأساليب المتبعة في هذه المرحلة. وعادة ما يقوم المهاجمين باستخدام طرق متقدمة لمحاكات حركة المرور الطبيعية لتجنب عمليات الرصد والاكتشاف. وهناك العديد من الأساليب والتقنيات التي يستطيع المهاجم استخدامها لكي يقوم بإنشاء قناة مخفية لتحكم والسيطرة على البنية التحتية ولا يتم اكتشافها من قبل أجهزة وأنظمة وبرمجيات الحماية.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1071		برتوكولات التطبيقات / Application Layer Protocol	قد يتواصل المهاجمين باستخدام بروتوكولات لApplication Layer لتجنب الكشف/ الحجب في الشبكة عن طريق التخفي مع حركة المرور الحالية. سيتم تضمين أوامر عن بعد للأنظمة، ونتائج هذه الأوامر غالبًا مضمنة في حركة مرور البروتوكول بين العميل والخادم.
T1071	.001	برتوكولات الويب / Web Protocols	قد يتواصل المهاجمين باستخدام بروتوكولات Application Layer المرتبطة بحركة مرور الويب لتجنب الكشف / الحجب في الشبكة من خلال التخفي مع حركة المرور الحالية. سيتم تضمين أوامر عن بعد للأنظمة، ونتائج هذه الأوامر غالبًا مضمنة في حركة مرور البروتوكول بين العميل والخادم.
T1071	.002	بروتوكول نقل الملفات / File Transfer Protocols	قد يتواصل المهاجمين باستخدام بروتوكولات Application Layer المرتبطة بنقل الملفات لتجنب الكشف / الحجب في الشبكة عن طريق التخفي مع حركة المرور الحالية. سيتم تضمين أوامر عن بعد للأنظمة، ونتائج هذه الأوامر غالبًا مضمنة في حركة مرور البروتوكول بين العميل والخادم.
T1071	.003	بروتوكول البريد Mail Protocols	قد يتواصل المهاجمين باستخدام بروتوكولات Application Layer المرتبطة بتسليم البريد الإلكتروني لتجنب الكشف / الحجب في الشبكة عن طريق التخفي مع حركة المرور الحالية. سيتم تضمين أوامر عن بعد للأنظمة، ونتائج هذه الأوامر غالبًا مضمنة في حركة مرور البروتوكول بين العميل والخادم.
T1071	.004	برتوكول اسماء النطاقات / DNS	قد يتواصل المهاجمين باستخدام بروتوكول Application Layer من خلال نظام أسماء النطاقات (DNS) لتجنب الكشف / الحجب في الشبكة عن طريق التخفي مع حركة المرور الحالية. سيتم تضمين أوامر عن بعد للأنظمة، ونتائج هذه الأوامر غالبًا مضمنة في حركة مرور البروتوكول بين العميل والخادم.
T1092		الاتصال من خلال الوسائط القابلة للازالة / Communication Through Removable Media	يمكن المهاجمين تنفيذ الأوامر والتحكم بين الأنظمة المخترقة على الشبكات التي يُحتمل أن تكون غير متصلة بالشبكة باستخدام وسائط قابلة للإزالة لنقل الأوامر من نظام إلى نظام. لنجاح الهجمة يجب اختراق كلا النظامين، مع احتمال تعرض النظام المتصل بالإنترنت للاختراق أولاً والثاني من خلال التنقل داخل الشبكة بواسطة النسخ عبر الوسائط القابلة للإزالة. سيتم نقل الأوامر والملفات من النظام غير المتصل إلى النظام المتصل بالإنترنت الذي يتمتع المهاجم بوصول مباشر إليه.
T1132		تشفير البيانات / Data Encoding	قد يقوم المهاجمين بتشفير البيانات لجعل محتوى حركة التحكم والسيطرة أكثر صعوبة في الكشف. يمكن تشفير معلومات التحكم والسيطرة (C2) باستخدام نظام تشفير البيانات القياسي. قد يلتزم استخدام ترميز البيانات بمواصفات البروتوكول الحالية ويتضمن استخدام ASCII أو Unicode أو Base64 أو MIME أو أنظمة تشفير ثنائية إلى نص أو رموز أخرى. قد تعمل بعض أنظمة تشفير البيانات أيضًا إلى ضغط البيانات، مثل gzip.
T1132	.001	ترميز قياسي / Standard Encoding	قد يقوم المهاجمين بتشفير البيانات باستخدام نظام ترميز بيانات قياسي لجعل محتوى حركة التحكم والسيطرة أكثر صعوبة في اكتشافه. يمكن تشفير معلومات التحكم والسيطرة (C2) باستخدام نظام تشفير بيانات قياسي يلتزم بمواصفات البروتوكول الحالية. تتضمن مخططات تشفير البيانات الشائعة ASCII و Unicode و hexadecimal و Base64 و MIME. قد تؤدي بعض أنظمة تشفير البيانات أيضًا إلى ضغط البيانات، مثل gzip.
T1132	.002	ترميز غير قياسي / Non-Standard Encoding	قد يقوم المهاجمين بتشفير البيانات باستخدام نظام ترميز بيانات غير قياسي لجعل محتوى حركة التحكم والسيطرة أكثر صعوبة في اكتشافه. يمكن تشفير معلومات التحكم والسيطرة (C2) باستخدام نظام ترميز بيانات غير قياسي يختلف عن مواصفات البروتوكول الحالية. قد تستند مخططات ترميز البيانات غير القياسية إلى أنظمة تشفير البيانات القياسية أو مرتبطة بها، مثل ترميز Base64 المعدل لنص رسالة طلب داخل بروتوكول HTTP.

T1001		تشفير وتعمية البيانات / Data Obfuscation	قد يقوم المهاجمين بتشويش حركة التحكم والسيطرة(C2) لجعل اكتشافها أكثر صعوبة. يتم إخفاء اتصالات (C2) 'ولكن ليس بالضرورة أن تكون مشفرة' في محاولة لجعل المحتوى أكثر صعوبة في اكتشافه أو فك تشفيره ولجعل طريقة الاتصال أقل وضوحًا وإخفاء الأوامر وعدم التمكن من رؤيتها. يشمل ذلك العديد من الطرق، مثل إضافة البيانات غير المرغوب فيها إلى حركة مرور البروتوكول، أو استخدام إخفاء المعلومات steganography، أو انتحال صفة البروتوكولات الشرعية.
T1001	.001	البيانات الغير هامة / Junk Data	قد يضيف المهاجمين بيانات غير مهمة إلى البروتوكولات المستخدمة للتحكم والسيطرة لجعل عملية اكتشافه أكثر صعوبة. من خلال إضافة بيانات عشوائية أو لا معنى لها إلى البروتوكولات المستخدمة للتحكم والسيطرة، يمكن للمهاجمين منع الأساليب البسيطه لفك تشفير أو تحليل حركة المرور بأي طريقة أخرى. قد تتضمن الأمثلة إلحاق البيانات مسبقًا بأحرف غير مهمة أو كتابة أحرف غير مهمة بين الأحرف المهمة.
T1001	.002	اخفاء البيانات / Steganography	قد يستخدم المهاجمين تقنيات إخفاء المعلومات لإخفاء حركة مرور التحكم والسيطرة لجعل محاولات اكتشافه أكثر صعوبة. يمكن استخدام تقنيات Steganographic لإخفاء البيانات في الرسائل الرقمية التي يتم نقلها بين الأنظمة. يمكن استخدام هذه المعلومات المخفية في التحكم والسيطرة في الأنظمة المخترقة. في بعض الحالات ، يمكن استخدام تمرير الملفات المضمنة باستخدام تقنية إخفاء المعلومات، مثل ملفات الصور أو المستندات ، للتحكم والسيطرة.
T1001	.003	انتحال البروتوكول / Protocol Impersonation	قد ينتحل المهاجمين صفة البروتوكولات المشروعة أو حركة مرور خدمة الويب لإخفاء نشاط التحكم والسيطرة وإحباط جهود المحللين. من خلال انتحال صفة البروتوكولات المشروعة أو خدمات الويب، يمكن للمهاجمين جعل حركة مرور التحكم والسيطرة الخاصة بهم منسجمة مع حركة مرور الشبكة المشروعة.
T1568		الاستجابة التلقائية / Dynamic Resolution	قد ينشئ المهاجمين بشكل ديناميكي اتصالات بالبنية التحتية التحكم والسيطرة لتفادي الاكتشاف والطرد من الشبكة. يمكن تحقيق ذلك باستخدام البرامج الضارة التي تشترك في خوارزمية مشتركة مع البنية التحتية التي يستخدمها المهاجم لتلقي اتصالات البرامج الضارة. يمكن استخدام هذه الحسابات لضبط المعلمات ديناميكيًا مثل اسم المجال أو عنوان IP أو رقم المنفذ الذي تستخدمه البرامج الضارة للتحكم والسيطرة.
T1568	.001	Fast Flux DNS	قد يستخدم المهاجمين Fast Flux DNS لإخفاء قناة التحكم والسيطرة خلف مجموعة من عناوين IP المتغيرة بسرعة والمرتبطة بدقة مجال واحدة. تستخدم هذه تقنية FQDN، مع عناوين IP متعددة مخصصة لها والتي يتم تبديلها بتردد عالٍ، باستخدام مجموعة من عناوين IP الخاصة بـ robin و TTL) Time-To-Live) لسجل مورد DNS.
T1568	.002	توليد النطاقات بشكل آلي Domain / Generation Algorithms	قد يستفيد المهاجمين من توليد النطاقات بشكل آلي (DGAs) لتحديد مجال الوجهة ديناميكيًا لحركة مرور التحكم والسيطرة بدلاً من الاعتماد على قائمة عناوين IP الثابتة أو المجالات. يتميز هذا بميزة أنه يجعل الأمر أكثر صعوبة على المحللين في حظر أو تتبع أو الاطاحة بقناة التحكم والسيطرة، حيث من المحتمل أن يكون هناك آلاف المجالات التي يمكن أن تتحقق منها البرامج الضارة بحثًا عن التعليمات.
T1568	.003	جمع بيانات اسماء النطاقات / DNS Calculation	قد يقوم المهاجمين بإجراء جمع بيانات اسماء النطاقات التي يتم إرجاعها في نتائج DNS لتحديد المنفذ وعنوان IP الذي يجب استخدامه للتحكم والسيطرة، بدلاً من الاعتماد على رقم منفذ محدد مسبقًا أو عنوان IP الفعلي الذي تم إرجاعه. يمكن استخدام حساب IP أو رقم المنفذ لتجاوز الحماية عند الخروج لقناة C2.
T1573		تشفير القناة / Encrypted Channel	قد يستخدم المهاجمين خوارزمية تشفير معروفة لإخفاء حركة التحكم والسيطرة بدلاً من الاعتماد على أي حماية متأصلة يوفرها بروتوكول الاتصال. على الرغم من استخدام خوارزمية آمنة، قد تكون هذه التطبيقات عرضة للهندسة العكسية إذا تم تشفير المفاتيح السرية أو إنشاؤها داخل البرامج الضارة/ملفات التكوين.

T1573	.001	Symmetric Cryptography	قد يستخدم المهاجمين خوارزمية تشفير متماثل معروفة لإخفاء حركة التحكم والسيطرة بدلاً من الاعتماد على أي حماية متأصلة يوفرها بروتوكول الاتصال. تستخدم خوارزميات التشفير المتماثل نفس المفتاح لتشفير النص العادي وفك تشفير النص المشفر. تتضمن خوارزميات التشفير المتماثل الشائعة AES و DES و DES3 و Blowfish و RC4.
T1573	.002	Asymmetric Cryptography	قد يستخدم المهاجمين خوارزمية معروفة للتشفير غير المتماثل لإخفاء حركة التحكم والسيطرة بدلاً من الاعتماد على أي حماية متأصلة يوفرها بروتوكول الاتصال. يستخدم التشفير غير المتماثل ، المعروف أيضًا باسم تشفير المفتاح العام، زوج مفاتيح لكل طرف: الأول يعتبر عام يمكن توزيعه للعامة والآخر خاص. نظرًا لكيفية إنشاء المفاتيح، يقوم المرسل بتشفير البيانات باستخدام المفتاح العام للمستقبل ويفك المتلقي تشفير البيانات بمفتاحه الخاص. هذا يضمن أن المستلم المقصود فقط يمكنه قراءة البيانات المشفرة. تتضمن خوارزميات تشفير المفتاح العام الشائعة RSA و ElGamal.
T1008		Fallback Channels	قد يستخدم المهاجمين قنوات اتصال بديلة أو احتياطية إذا تم اختراق القناة الأساسية أو تعذر الوصول إليها من أجل الحفاظ على قناة التحكم والسيطرة ولتجنب عتبات نقل البيانات.
T1105		Ingress Tool Transfer	قد يقوم المهاجمين بنقل أدوات أو ملفات أخرى من نظام خارجي إلى بيئة تم الاستيلاء عليها. يمكن نسخ الملفات من نظام يتم التحكم فيه عن طريق المهاجم الخارجي من خلال قناة التحكم والسيطرة لإحضار الأدوات إلى شبكة الضحية أو من خلال بروتوكولات بديلة باستخدام أداة أخرى مثل FTP. يمكن أيضًا نسخ الملفات على نظامي Mac و Linux باستخدام أدوات مضمنة في الأنظمة مثل scp و rsync و sftp.
T1104		Multi-Stage Channels	قد ينشئ المهاجمين مراحل متعددة للتحكم والسيطرة ليتم توظيفها في ظل ظروف مختلفة أو لوظائف معينة. قد يؤدي استخدام مراحل متعددة إلى تشويش قناة التحكم والسيطرة لجعل عملية الاكتشاف عن التطفل أكثر صعوبة.
T1095		Non-Application Layer Protocol	قد يستخدم المهاجمين بروتوكول non-application layer للاتصال بين المضيف وخادم C2 أو بين المضيفين المصابين داخل الشبكة. قائمة البروتوكولات الممكنة واسعة النطاق. تتضمن الأمثلة المحددة استخدام بروتوكولات network layer، مثل بروتوكول رسائل التحكم في الإنترنت (ICMP)، وبروتوكولات طبقة النقل "transport layer"، مثل بروتوكول مخطط بيانات المستخدم (UDP)، وبروتوكولات session layer، مثل (Socket Secure (SOCKS ، وكذلك إعادة التوجيه / البروتوكولات النفقية ، مثل (Serial over LAN (SOL.
T1571		المنافذ الغير متعارف عليها / Port Non-Standard	قد يتواصل المهاجمين باستخدام بروتوكول ومنفذ غير مرتبطة مع بعضها عادةً. على سبيل المثال، HTTPS عبر المنفذ 8088 أو المنفذ 587 على عكس المنفذ التقليدي 443. قد يقوم المهاجمين بإجراء تغييرات على المنفذ المتعارف عليه و المستخدم بواسطة البروتوكول لتجاوز الحماية أو تحليل الاختلاف أو تحليل بيانات الشبكة.
T1572		برتوكولات النقل الخاصة / Tunneling Protocol	قد يقوم المهاجمين بنقل اتصالات الشبكة الخاصة من وإلى نظام الضحية ضمن بروتوكول منفصل لتجنب الكشف أو حماية الشبكة أو لتمكين الوصول إلى أنظمة لا يمكن الوصول إليها بأي طريقة أخرى. يتضمن الاتصال الخاص تغليف بروتوكول داخل بروتوكول آخر. قد يخفي هذا السلوك حركة المرور البيانات الضارة عن طريق المزج مع حركة المرور الحالية أو توفير طبقة خارجية من التشفير (على غرار VPN). يمكن للنفق أو النقل الخاص أيضًا تمكين توجيه حزم الشبكة التي لن تصل إلى وجهتها المقصودة لولا ذلك ، مثل SMB أو RDP أو حركة مرور أخرى تتم حجبها بواسطة أجهزة الشبكة أو لا يتم توجيهها عبر الإنترنت.
T1090		الوكيل / Proxy	قد يستخدم المهاجمين وكيل اتصال لتوجيه حركة مرور الشبكة بين الأنظمة أو العمل كوسيط لاتصالات الشبكة إلى خادم التحكم والسيطرة لتجنب الاتصالات المباشرة ببنيتهم التحتية المستخدمة. توجد العديد من الأدوات التي تتيح إعادة توجيه حركة المرور من خلال الوكلاء أو إعادة توجيه المنفذ، بما في ذلك HTRAN و ZXProxy و ZXPortMap. يستخدم المهاجمين هذه الأنواع من الوكلاء لإدارة اتصالات التحكم والسيطرة، وتقليل عدد اتصالات الشبكة الخارجية المتزامنة، وتوفير المرونة في مواجهة أي فقدان في الاتصال،

			أو تجاوز الاتصالات الموثوقة القائمة بين الضحايا لتجنب الشك. قد يربط المهاجمين معًا عدة وكلاء لإخفاء مصدر حركة المرور بيانات الضارة.
T1090	.001	الوكيل الداخلي / Internal Proxy	قد يستخدم المهاجمين وكيلًا داخليًا لتوجيه حركة التحكم والسيطرة بين نظامين أو أكثر في بيئة تم أختراقها. توجد العديد من الأدوات التي تتيح إعادة توجيه حركة المرور من خلال الوكلاء أو إعادة توجيه المنفذ، بما في ذلك HTRAN و ZXProxy و ZXPortMap. يستخدم الخصوم وكلاء داخليين لإدارة اتصالات التحكم والسيطرة داخل بيئة مخترقة، لتقليل عدد اتصالات الشبكة الخارجية المتزامنة ، لتوفير المرونة في مواجهة أي فقدان في الاتصال، أو تجاوز الاتصالات الموثوقة الحالية بين الأنظمة المصابة لتجنب الشك. قد تستخدم اتصالات الوكيل الداخلية بروتوكولات شبكات نظير إلى نظير (p2p) الشائعة، مثل SMB، للاندماج بشكل أفضل مع البيئة.
T1090	.002	الوكيل الخارجي / External Proxy	قد يستخدم المهاجمين وكيلًا خارجيًا للعمل كوسيط لاتصالات الشبكة إلى خادم التحكم والسيطرة لتجنب الاتصالات المباشرة ببنيتهم التحتية المستخدمة. توجد العديد من الأدوات التي تتيح إعادة توجيه حركة المرور من خلال الوكلاء أو إعادة توجيه المنفذ، بما في ذلك HTRAN و ZXProxy و ZXPortMap. يستخدم المهاجمين هذه الأنواع من الوكلاء لإدارة اتصالات التحكم والسيطرة، بالإضافة لتوفير المرونة في مواجهة أي فقدان في الاتصال، أو لتجاوز مسارات الاتصالات الموثوقة الحالية لتجنب الاكتشاف.
T1090	.003	Multi-hop Proxy	لإخفاء مصدر حركة مرور البيانات الضارة، قد يربط المهاجمين عدة وكلاء. عادةً ما يكون المدافع قادرًا على تحديد آخر حركة مرور للوكيل التي تم اجتيازها قبل أن يدخل الشبكة؛ قد يكون المدافع قادرًا أو غير قادر على تحديد أي وكلاء سابقين قبل وكيل آخر قفزة تمت. تجعل هذه التقنية تحديد المصدر الأصلي لحركة المرور الضارة أكثر صعوبة من خلال مطالبة المدافع بتتبع حركة المرور الضارة من خلال عدة وكلاء لتحديد مصدرها. نوع معين من هذا السلوك هو استخدام شبكات onoin routing ، مثل شبكة TOR المتاحة للعامة.
T1090	.004	Domain Fronting	قد يستفيد المهاجمين من مخططات الموجه(Routing Schemes) في شبكات توصيل المحتوى (CDNs) والخدمات الأخرى التي تستضيف مجالات متعددة لإخفاء الوجهة المقصودة لحركة مرور HTTPS أو حركة المرور عبر HTTPS. تتضمن Domain fronting استخدام أسماء نطاقات مختلفة في حقل SNI لرأس TLS والحقل المضيف ل HTTP. إذا تم تقديم كلا النطاقين من نفس CDN ، فقد يقوم CDN بالتوجيه إلى العنوان المحدد في HTTP بعد إلغاء التفاف رأس TLS. يتم استخدام أحد أشكال التقنية واجهة "domainless" ، حقل SNI الذي تم تركه فارغًا؛ قد يسمح هذا للواجهة بالعمل حتى عندما تحاول CDN التحقق من تطابق حقول SNI و Host HTTP (إذا تم تجاهل حقول SNI الفارغة).
T1219		الوصول للبرمجيات عن بعد / Remote Access Software	قد يستخدم المهاجم برامج شرعية للوصول لسطح المكتب والوصول عن بُعد، مثل Team Viewer و Go2Assist و LogMein و AmmyyAdmin وغيرها، لإنشاء قناة تفاعلية للتحكم والسيطرة لاستهداف الأنظمة داخل الشبكات. تُستخدم هذه الخدمات بشكل شائع كبرامج للدعم الفني، وقد يُسمح بها من خلال سياسة التحكم في التطبيقات داخل البيئة. تُستخدم أدوات الوصول عن بُعد مثل VNC و Ammyy و Teamviewer بشكل متكرر عند مقارنتها بالبرامج الشرعية الأخرى التي يشيع استخدامها من قبل المهاجمين.
T1205		Traffic Signaling	قد يستخدم المهاجمين Traffic Signaling لإخفاء المنافذ المفتوحة أو غيرها من الوظائف الضارة المستخدمة للبقاء في الشبكة أو التحكم والسيطرة. تتضمن Traffic Signaling استخدام القيمة السحرية أو تسلسل يجب إرساله إلى النظام لإطلاق استجابة خاصة، مثل فتح منفذ مغلق أو لتنفيذ مهمة ضارة. إرسال سلسلة من الحزم بخصائص معينة قبل فتح المنفذ تتيح للمهاجم استخدامه في التحكم والسيطرة. عادةً ما تتكون هذه السلسلة من الحزم من محاولات توصيل بتسلسل محدد مسبقًا من المنافذ المغلقة (مثل Port Knocking) ، ولكن يمكن أن تتضمن أعلامًا غير عادية أو سلاسل محددة أو خصائص فريدة أخرى. بعد اكتمال التسلسل ، قد يتم فتح منفذ بواسطة جدار الحماية الخاص بالمضيف، ولكن يمكن أيضًا تنفيذه بواسطة برنامج مخصص.

T1205	.001	Port Knocking	قد يستخدم المهاجمين طريقة Porting Knocking لإخفاء المنافذ المفتوحة المستخدمة للبقاء في الشبكة أو للتحكم والسيطرة. لتمكين منفذ، يرسل المهاجم سلسلة من محاولات للاتصال إلى منافذ مغلقة تم تحديدها مسبقاً. بعد اكتمال التسلسل، غالبًا ما يتم فتح منفذ بواسطة جدار حماية المضيف، ولكن يمكن أيضًا تنفيذه بواسطة برنامج مخصص.
T1102		خدمات الويب / Web Service	قد يستخدم المهاجمين خدمة ويب خارجية شرعية قائمة كوسيلة لنقل البيانات إلى/ من نظام مخترق. قد توفر مواقع الويب الشعبية ووسائل التواصل الاجتماعي التي تعمل كآلية لـ C2 قدرًا كبيرًا من التغطية نظرًا لاحتمال اتصال المضيفين داخل الشبكة بهم بالفعل. إن استخدام الخدمات المشتركة ، مثل تلك التي تقدمها Google أو Twitter ، يسهل على المهاجمين الاختباء في الضوضاء المتوقعة. يستخدم مقدمو خدمات الويب عادةً تشفير SSL / TLS ، مما يمنح المهاجمين مستوى إضافيًا من الحماية.
T1102	.001	Dead Drop Resolver	قد يستخدم المهاجمين خدمة ويب خارجية موجودة وشرعية لاستضافة المعلومات التي تشير إلى بنية تحتية إضافية للتحكم والسيطرة (C2). قد ينشر المهاجمين محتوى، يُعرف باسم محلل الإسقاط 'dead drop resolver' ، على خدمات الويب مع نطاقات أو عناوين IP مضمنة (وغالبًا ما تكون مشفرة /مشوهة). بمجرد الإصابة، سيتواصل الضحايا مع هؤلاء المحللون ويعيدون توجيههم.
T1102	.002	الاتصال من الطرفين / Bidirectional Communication	قد يستخدم المهاجمين خدمة ويب خارجية موجودة وشرعية كوسيلة لإرسال أوامر إلى نظام مخترق واستلامه عبر قناة خدمة الويب. قد تستفيد الأنظمة المخترقة من مواقع الويب الشائعة ووسائل التواصل الاجتماعي لاستضافة تعليمات التحكم والسيطرة (C2). يمكن لهذه الأنظمة المصابة بعد ذلك إرسال المخرجات من هذه الأوامر مرة أخرى عبر قناة خدمة الويب. قد يحدث الرجوع بعدة طرق، اعتمادًا على خدمة الويب المستخدمة. على سبيل المثال ، قد تأخذ حركة الرجوع في قيام النظام المخترق بنشر تعليق على منتدى، أو إصدار طلب سحب لمشروع تطوير، أو تحديث مستند مستضاف على خدمة ويب، أو عن طريق إرسال تغريدة.
T1102	.003	الاتصال من طرق واحد / One-Way Communication	قد يستخدم المهاجمين خدمة ويب خارجية موجودة وشرعية كوسيلة لإرسال أوامر إلى نظام مخترق دون تلقي مخرجات قادمة من خلال خدمة الويب. قد تستفيد الأنظمة المخترقة من مواقع الويب الشائعة ووسائل التواصل الاجتماعي لاستضافة تعليمات التحكم والسيطرة (C2). قد تختار هذه الأنظمة المصابة إرسال المخرجات من تلك الأوامر مرة أخرى عبر قناة C2 مختلفة، بما في ذلك إلى خدمة ويب أخرى. بدلاً من ذلك ، قد لا تُرجع الأنظمة المخترقة أي مخرجات على الإطلاق في الحالات التي يرغب فيها المهاجمين في إرسال تعليمات إلى الأنظمة ولا يريدون ردًا.

تسريب البيانات / Exfiltration

تسريب البيانات: يتكون من عدة تقنيات قد يستخدمها المهاجمين لسرقة البيانات من شبكتك. بمجرد أن يتم جمع البيانات غالبا يتم حزمها/ضغطها لتفادي الاكتشاف عندما يتم نقلها. وذلك يتم أما عبر الأرشفة أو التشفير. ان التقنيات المستخدمة لتسريب البيانات لخارج الشبكة هي بالغالب تتم عبر قناة التحكم والسيطرة (C&C)أو من خلال قناة أخرى وكذلك من المحتمل وضع قيود على حجم النقل.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1020		تسريب البيانات بشكل آلي / Exfiltration Automated	قد يقوم المهاجمين بتسريب البيانات ، مثل المستندات الحساسة و الملفات ، من خلال استخدام عمليات مؤتمتة بعد جمعها.
T1020	.001	البيانات المتكررة / Traffic Duplication	قد يستفيد المهاجمين من انعكاس حركة المرور traffic mirroring من أجل أتمتة تسريب البيانات عبر البنية التحتية للشبكة المستهدفة. تعد ميزة انعكاس حركة المرور ميزة مضمنة لبعض أجهزة الشبكة وتستخدم لتحليل الشبكة ويمكن تهيئتها لتكرار حركة المرور وإعادة التوجيه إلى وجهة واحدة أو أكثر لتحليلها بواسطة محلل الشبكة أو جهاز مراقبة آخر.
T1030		نقل البيانات بواسطة احجام محددة / Transfer Data Size Limits	قد يقوم المهاجم بتسريب البيانات من خلال تجزئة البيانات الى احجام موحدة بدلاً من تسريب الملفات كاملة أو من الممكن أن يحد من أحجام الحزم التي تقل عن عتبات 'Threshold' معينة لكي لا يتم اكتشافها. ويمكن استخدام هذا الأسلوب لتجنب التنبيهات من خلال مركز مراقبة بيانات الشبكة.
T1048		تسريب البيانات بواسطة بروتوكول بديل / Exfiltration Over Alternative Protocol	قد يسرق المهاجمين البيانات عن طريق تسريبها عبر بروتوكول مختلف عن بروتوكول قناة التحكم والسيطرة (C&C)الحالية. يمكن أيضًا إرسال البيانات إلى شبكة بديلة عن خادم التحكم والسيطرة الرئيسي.
T1048	.001	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	قد يسرق المهاجمين البيانات عن طريق تسريبها عبر بروتوكول شبكة مشفرة من نوع متماثل بخلاف بروتوكول قناة التحكم و السيطرة الموجودة. يمكن أيضًا إرسال البيانات إلى شبكة بديلة عن خادم التحكم والقيادة الرئيسي.
T1048	.002	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	قد يسرق المهاجمين البيانات من خلال تسريبها عبر بروتوكول شبكة مشفرة من النوع غير متماثل بخلاف بروتوكول قناة التحكم والسيطرة الموجودة. يمكن أيضًا إرسال البيانات إلى شبكة بديلة عن خادم التحكم والسيطرة الرئيسي.
T1048	.003	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	قد يسرق المهاجمين البيانات عن طريق تسريبها عبر بروتوكول شبكة غير مشفرة بخلاف بروتوكول قناة التحكم والسيطرة الموجودة. يمكن أيضًا إرسال البيانات إلى شبكة بديلة عن خادم التحكم والسيطرة الرئيسي.
T1041		تسريب البيانات من خلال قناة تحكم وسيطرة / Exfiltration Over C2 Channel	قد يسرق المهاجمين البيانات عن طريق تسريبها عبر قناة التحكم والسيطرة الموجودة. البيانات المسروقة يتم ترميزها من خلال قناة الاتصالات العادية باستخدام نفس بروتوكول اتصالات التحكم والسيطرة.
T1011		تسريب البيانات من خلال الشبكات البديلة Exfiltration Over Other Network Medium	قد يحاول المهاجمين بتسريب البيانات عبر شبكة وسيطة مختلفة عن قناة التحكم والسيطرة. إذا كانت شبكة التحكم والسيطرة عبارة عن اتصال سلكي متصل بالإنترنت، فقد يحدث التسريب ، على سبيل المثال ، عبر اتصال WiFi أو مودم أو اتصال بيانات خلوية أو Bluetooth أو قناة تردد راديو مختلفة (RF).
T1011	.001	تسريب البيانات من خلال البلوتوث / Exfiltration Over Bluetooth	قد يحاول المهاجمين بتسريب البيانات عبر البلوتوث بدلاً من قناة التحكم والسيطرة. إذا كانت شبكة التحكم والسيطرة عبارة عن اتصال سلكي متصل بالإنترنت ، فقد يختار المهاجم سرقة البيانات باستخدام قناة اتصال مثل Bluetooth.

T1052		تسريب البيانات من خلال وسائط فيزيائية / Exfiltration Over Physical Medium	قد يحاول المهاجمين بتسريب البيانات عبر وسيط مادي ، مثل محرك أقراص قابل للإزالة. أمثلة على ذلك، اختراق الشبكة المعزولة عن الانترنت Air-gapped network ، ويمكن أن يحدث التسريب عبر وسيط مادي أو جهاز مقدم من قبل المستخدم. يمكن أن تكون هذه الوسائط عبارة عن محرك أقراص ثابت خارجي أو محرك أقراص USB أو هاتف خلوي أو مشغل MP3 أو أي أجهزة تخزين أخرى. يمكن استخدام الوسيط المادي أو الجهاز كنقطة خروج نهائية أو للتنقل بين الأنظمة غير المتصلة.
T1052	.001	تسريب البيانات من خلال USB over USB / Exfiltration	قد يحاول المهاجمين بتسريب البيانات عبر جهاز مادي متصل بـ USB. أمثلة على ذلك، اختراق الشبكة المعزولة عن الانترنت Air-gapped network، ويمكن أن يحدث التسريب عبر جهاز USB مقدم من قبل المستخدم. يمكن استخدام جهاز USB كنقطة خروج نهائية أو للتنقل بين الأنظمة غير المتصلة.
T1567		تسريب البيانات من خلال خدمات الويب / Exfiltration Over Web Service	قد يستخدم المهاجمين خدمة ويب خارجية موجودة وشرعية لتسريب البيانات بدلاً من قناة التحكم والسيطرة الخاصة بهم. قد توفر خدمات الويب الشائعة التي تستخدم لتسريب البيانات قدرًا كافيا من التغطية نظرًا لاحتمال وجود اتصال مسبق بين المستخدمين و الشبكة الداخلية قبل حدوث الاختراق. بالإضافة قد يوجد هناك سياسات في جدار الحماية تسمح في حركة المرور لهذه الخدمات.
T1567	.001	تسريب البيانات الى مستودع الاكواد / Exfiltration to Code Repository	قد يقوم المهاجمين بتسريب البيانات إلى مستودع الأكواد البرمجية بدلاً من قناة التحكم والسيطرة الخاصة بهم. غالبًا ما يمكن الوصول إلى مستودعات الأكواد عبر واجهة برمجة التطبيقات (على سبيل المثال: https://api.github.com). غالبًا يتم الوصول إلى واجهات برمجة التطبيقات هذه عبر بروتوكول HTTPS ، مما يمنح المهاجم مستوى إضافي من الحماية.
T1567	.002	تسريب البيانات الى الخدمات السحابية / Exfiltration to Cloud Storage	قد يقوم المهاجمين بتسريب البيانات إلى خدمة التخزين السحابية بدلاً من قناة التحكم والسيطرة الخاصة بهم. تتيح خدمات التخزين السحابية تخزين البيانات وتحريرها واستردادها من خادم تخزين سحابي خارجي عبر الإنترنت.
T1029		جدولة نقل البيانات / Scheduled Transfer	قد يقوم المهاجمين بجدولة تسريب البيانات ليتم عملها فقط في أوقات محددة في اليوم أو على فترات زمنية معينة. يمكن القيام بذلك مع الأنشطة العادية في الشبكة لتجنب الاكتشاف.
T1537		تسريب البيانات الى الحسابات السحابية / Transfer Data to Cloud Account	قد يقوم المهاجمين بتسريب البيانات عن طريق نقل البيانات ، بما في ذلك النسخ الاحتياطية من البيئات السحابية إلى حساب سحابي آخر يتم التحكم فيه في نفس الخدمة لتجنب عمليات نقل/تنزيلات الملفات وذلك لتفادي اكتشاف التسريب البيانات في الشبكة.

التأثير / Impact

التأثير: يسعى المهاجمون دائماً الى تدمير البيانات واحداث تأثير على البيانات او الخدمات او على الوصول لها او من خلال التلاعب بها او التأثير على سلامة الاعمال والعمليات التشغيلية. وتختلف التقنيات والأساليب المتبعة في احداث الأثر اما ان تكون تدميرية او عبث بالبيانات. وقد يقوم المهاجم بالتأثير على المنظمة من خلال التعديل على البيانات لتحقيق أهدافه مما يحدث تأثير على النظام او الجهة التي تم العبث بالبيانات الخاصة بها. وعادة ما يكون احداث الأثر هو هدف المهاجمون النهائي او لتغطية الاختراق الذي حدث.

ID / المعرف	المعرف الفرعي	Name /الاسم	Description / الوصف
T1531		مسح الحسابات / Account Access Removal	يقطع المهاجمون توفر الوصول للموارد الشبكية أو الانظمة وذلك لمنع الوصول للمستخدمين المصرح لهم. الحسابات من المحتمل حذفها, اقفالها أو يتم التلاعب بها عن طريق تغيير الحساب لمنع الوصول للحسابات .
T1485		تدمير البيانات / Data Destruction	يقوم المهاجمين بتدمير البيانات والملفات في نظام محدد او عدد كبير في الشبكة وذلك لمنع التوافرية للأنظمة, الخدمات وموارد الشبكة. تدمير البيانات هي عملية حذف بيانات غير قابلة للاسترجاع عن طريق تقنيات الطب الشرعي الرقمي وذلك من خلال الكتابة فوق الملفات المحذوفة لمنع امكانية استرجاعها. في نظم التشغيل المعروفة يتم حذف الملفات من خلال أوامر del, rm وهنا يتم حذف المؤشر الخاص بالملف من غير حذف المحتوى بداخل الملف, مما يجعل أمكانية استعادة الملفات ممكنة من خلال أدوات الطب الشرعي الرقمي. الطريقة سوف تختلف عند استخدام wipe لأنها تقوم بحذف الملف مباشرة.
T1486		تشفير البيانات لتعظيم الاثر / Data Encrypted for Impact	يقوم المهاجمين بتشفير البيانات والملفات في الأنظمة المستهدفة او عدد كبير منها في الشبكة وذلك لمنع التوافرية في الأنظمة, الخدمات وموارد الشبكة. كذلك يجعلون الوصول غير ممكن للبيانات المحفوظة في القرص الصلب المحلي أو المتصلة عن بعد وذلك دون معرفة مفتاح فك التشفير. يتم عمل ذلك ليتم الزام الضحية بالتعويض المالي لأجل اعطاءه مفتاح فك التشفير الملفات أو لمنع الوصول للملفات بشكل دائم. في حال الفدية، يتم غالبا تشفير ملفات مستندات الأوفس, الصور, الفيديو, صوتيات وغيرها وفي بعض الأحيات يتم تشفير ملفات حساسة بالنظام ومنها MBR, Disk Partion.
T1565		التلاعب بالبيانات / Data Manipulation	من الممكن أن يقوم المهاجمين بأضافة، حذف أو التلاعب بالبيانات من أجل تغيير المخرجات أو لأخفاء نشاطه. التلاعب بالبيانات قد يؤثر على عملية الأعمال أو متخذين القرار.
T1565	.001	التلاعب بمخزن البيانات / Stored Data Manipulation	من الممكن أن يقوم المهاجمين بأضافة، حذف أو التلاعب بالبيانات المخزنة من أجل تغيير المخرجات أو لأخفاء نشاطه. التلاعب بالبيانات المخزنة قد يؤثر على عملية الأعمال أو متخذين القرار.
T1565	.002	التلاعب بالبيانات المنقولة / Data Transmitted Manipulation	من الممكن أن يقوم المهاجمين في تبديل البيانات المتجه للتخزين أو انظمة أخرى من أجل تغيير المخرجات أو لأخفاء نشاطه. التلاعب بالبيانات المنقولة قد يؤثر على عملية الأعمال أو متخذين القرار
T1565	.003	التلاعب بالبيانات وقت العمل والتشغيل / Runtime Data Manipulation	من الممكن أن يقوم المهاجمين في تعديل الأنظمة للتلاعب بالبيانات حين وصولها وعرضها للمستخدم. التلاعب بالبيانات وقت العمل والتشغيل قد يؤثر على عملية الأعمال أو متخذين القرار
T1491		التشوية او التغير / Defacement	يقوم المهاجمين بتعديل المحتوى الظاهري المتوفر داخليا أو خارجيا لشبكة المنظومة. الأسباب وراء التشويه يتضمن توصيل رسالة، تخويف أو التفاخر بالتطفل. تستخدم صور هجومية أو مزعجة لتسبب للمستخدم عدم الراحة أو الضغط للأمتثال للرسائل المصاحبة.

T1491	.001	التشوية والتغير الداخلي / Internal Defacement	يقوم المهاجمين بتشويه الأنظمة الداخلية للمنظمة لمحاولة تخويف وتضليل المستخدمين. قد يكون على شكل تعديلات على مواقع الويب الداخلية ، أو على أنظمة المستخدم مباشرة باستبدال خلفية سطح المكتب. تستخدم صور هجومية أو مزعجة لتسبب للمستخدم عدم الراحة أو الضغط للامتثال للرسائل المصاحبة. نظرًا لأن طريقة التشويه الداخلي تكشف وجود المهاجم ، فغالبًا ما يحدث ذلك بعد تحقيق أهداف أخرى
T1491	.002	التشوية و التغير الخارجي / External Defacement	يقوم المهاجمين بتشويه الأنظمة الخارجية للمنظمة لمحاولة توصيل رسالة أو تخويف وتضليل المستخدمين أو المنظمة. التشويه الخارجي يعتبر هو الأكثر شيوعا من ضحايا التشويه وذلك لأن المهاجمين أو مجموعات القراصنة تستخدمها لتوصيل رسالة سياسية أو نشر دعايات. التشويه الخارجي تستخدم غالبا كمحفز لتحريك أحداث معينة ، أو ردت فعل على الإجراءات التي تتخذها منظمة أو حكومة. وبالمثل ، يمكن أيضًا استخدام تشويه موقع الويب كإعداد أو مقدمة للهجمات المستقبلية مثل Drive-by Compromise
T1561		محي القرص الصلب / Disk Wipe	يقوم المهاجمين بمحي أو تخريب البيانات الخام في القرص الصلب في أنظمة محددة أو عدد كبير في الشبكة وذلك لمنع التوافرية في الأنظمة, الخدمات وموارد الشبكة. وذلك بالقيام بالكتابة بشكل مباشر في القرص الصلب على البيانات المخزنة بداخلها. في بعض الأحيان يتم تشفير ملفات حساسة بالنظام ومنها MBR. قد تتم محاولة مسح كامل لجميع أجزاء القرص
T1561	.001	محي محتوى البيانات من القرص الصلب / Content Disk Wipe	يقوم المهاجمين بأزالت المحتويات المخزنة في الأجهزة في أنظمة محددة أو عدد كبير في الشبكة وذلك لمنع التوافرية في الأنظمة, الخدمات وموارد الشبكة
T1561	.002	محي هيكلة القرص الصلب Disk Structure Wipe	قد يقوم المهاجمين بإتلاف أو محي هياكل بيانات القرص الموجودة على محرك الأقراص الثابتة اللازمة لتشغيل النظام، وذلك بأستهداف أنظمة حساسة أو عدد كبير منها في الشبكة وذلك لمنع التوافرية في الأنظمة, الخدمات وموارد الشبكة
T1499		حجب الخدمة للطرفية / Endpoint Denial of Service	قد يقوم المهاجمين في هجوم حجب الخدمة لمنع التوافرية في الوصول لخدمات المستخدمين. هجوم حجب الخدمة يمكن قيامه عبر استهلاك موارد النظام التي يتم استخدامها أما من قبل الخدمات المستضافة بداخله أو استغلال النظام لإحداث حالة تعطل مستمرة. مثال على ذلك خدمات تتضمن خدمة البريد، المواقع، نظام أسماء النطاقات DNS والتطبيقات وغيرها، ومن خلال وجود هذي الخدمات قد يتمكن المهاجم من استغلالها لعمل هجوم حجب الخدمة لأغراض سياسة أو تهديدات أو ابتزاز.
T1499	.001	استهلاك موارد النظام / OS Exhaustion Flood	قد يقوم المهاجمين في أستهداف نظم التشغيل في الهجوم نظرا لأنها هي المسؤولة في أدارة الموارد المحدودة في النظام.بالأضافة لا تحتاج هذه الهجمات إلى استنفاد الموارد الفعلية على النظام حيث يمكنها ببساطة استنفاد الحدود التي يفرضها نظام التشغيل ذاتيًا وذلك لمنع النظام بأكمله من أن يتأثر بسبب المطالب المفرطة على قدرته.
T1499	.002	استهلاك موارد الشبكة Service / Flood Exhaustion	يقوم المهاجمين في أستهداف خدمات شبكية مختلفة مزودة من قبل النظام لعمل DOS. المهاجمين كثيرا ما يستهدفون خدمة الويب أو خدمة نظام أسماء النطاقات. برامج خادم الويب أيضا من الممكن استهدافه بطرق متنوعه وذلك اعتمادا على الخدمة المزودة فيه.
T1499	.003	استهلاك موارد التطبيقات / Application Exhaustion Flood	قد يستهدف المهاجمين تطبيقات ويب تتميز بموارد عالية جدا للتسبب في حجب الخدمة DoS. قد تكون الميزات المحددة في تطبيقات الويب عالية جدا لاستخدام الموارد. قد تتمكن الطلبات المتكررة لهذه الميزات من استنفاد موارد النظام ورفض الوصول إلى التطبيق أو الخادم نفسه

T1499	.004	اختراق التطبيقات او البرمجيات / Application or System Exploitation	قد يستغل المهاجمين ثغرات البرامج التي يمكن أن تتسبب في تعطيل تطبيق أو نظام ومنع توافره للمستخدمين. قد تقوم بعض الأنظمة بإعادة تشغيل التطبيقات والخدمات الهامة تلقائيًا عند حدوث أعطال ، ولكن من المحتمل إعادة استغلالها بشكل مستمر للتسبب في استمرارية حجب الخدمة
T1495		عطب النظام الثابت او الداخلي / Firmware Corruption	قد يقوم المهاجمين بالكتابة فوق أو إتلاف محتويات ذاكرة الفلاش الخاصة بنظام BIOS أو البرامج الثابتة الأخرى في الأجهزة المتصلة بالنظام من أجل جعلها غير قابلة للتشغيل أو غير قادرة على الأقلاع. البرنامج الثابت هو برنامج يتم تحميله وتنفيذه من ذاكرة غير مستقرة على الأجهزة من أجل تهيئة وظائف الجهاز وإدارتها. يمكن أن تتضمن هذه الأجهزة اللوحة الأم أو محرك الأقراص الثابتة أو بطاقات الفيديو.
T1490		منع استرداد النظام / Inhibit System Recovery	قد يقوم المهاجمين بحذف أو إزالة بيانات نظام التشغيل المضمنة وإيقاف تشغيل الخدمات المصممة للمساعدة في استرداد النظام التالف وذلك من أجل منع الاسترداد. قد تحتوي أنظمة التشغيل على ميزات يمكن أن تساعد في إصلاح الأنظمة التالفة ، مثل كتالوج النسخ الاحتياطي والنسخ الاحتياطية لوحدة التخزين volume shadow copies وميزات الإصلاح التلقائي. قد يقوم المهاجمين بتعطيل أو حذف ميزات استرداد النظام لزيادة تأثيرات تدمير البيانات وتشفير البيانات من أجل التأثير.
T1498		حجب خدمات الشبكة / Network Denial of Service	قد ينفذ المهاجمين هجمات حجب الخدمة عبر الشبكة DoS لتقليل أو منع توافر الموارد المخصصة للمستخدمين. يمكن إجراء DoS للشبكة عن طريق استنفاد خدمات معدل نقل البيانات bandwidth للشبكة التي تعتمد عليها. أمثلة على الموارد هي مواقع ويب وخدمات البريد الإلكتروني ونظام أسماء النطاقات. لقد لوحظ أن الأعداء يشنون هجمات حجب الخدمة على الشبكة لأغراض سياسية ولدعم الأنشطة الخبيثة الأخرى ، بما في ذلك الإلهاء والقرصنة والابتزاز
T1498	.001	فيضان الشبكة المحدد / Direct Network Flood	قد يحاول المهاجمين التسبب في حجب الخدمة DoS عن طريق إرسال حجم كبير من حركة مرور الشبكة إلى الهدف المراد. يحدث Direct Network Flood عندما يتم استخدام نظام واحد أو أكثر لإرسال عدد كبير من حزم الشبكة نحو خدمة الشبكة المستهدفة. يمكن استخدام أي بروتوكول شبكة تقريبًا للإغراق. يتم استخدام البروتوكولات مثل UDP أو ICMP بشكل شائع ولكن يمكن أيضًا استخدام البروتوكولات مثل TCP.
T1498	.002	تضخيم الانعكاس / Reflection Amplification	قد يقوم المهاجمين بالتسبب في حجب الخدمة من خلال عكس حجم كبير لحركة مرور الشبكة على الهدف المراد. يستفيد هذا النوع من Network DoS من وسيط خادم تابع لجهة خارجية يستضيف ويستجيب لعنوان الشبكي IP المنتحل Spoof. عادةً ما يُطلق على خادم الطرف الثالث هذا اسم عاكس. يعمل المهاجم هجومًا انعكاسيًا عن طريق إرسال حزم إلى عاكسات تحتوي على العنوان الشبكي المنتحل الخاص بالضحية. على غرار Direct Network Floods ، يمكن استخدام أكثر من نظام واحد لتنفيذ الهجوم ، أو يمكن استخدام الروبوتات. وبالمثل ، يمكن استخدام عاكس واحد أو أكثر لتركيز حركة المرور على الهدف.
T1496		Resource Hijacking	قد يستفيد المهاجمين من موارد الأنظمة المختارة من أجل حل مشكلات الموارد العالية التي قد تؤثر على النظام أو توافرية الخدمة المستضافة.
T1489		ايقاف الخدمات / Service Stop	قد يقوم المهاجمين بإيقاف الخدمات أو تعطيلها على النظام لجعل هذه الخدمات غير مفعلة لدى المستخدمين. يمكن أن يؤدي إيقاف الخدمات أو العمليات المهمة إلى منع الاستجابة للحادثة في حال وقوعها. وفي حال ايقاف الخدمات قد ينتفع المهاجمين بتحقيق الأهداف المرادة وذلك لإلحاق الضرر بالمنظمة.
T1529		ايقاف او اعادة تشغيل الانظمة / System Shutdown/Reboot	قد يقوم المهاجمين بإغلاق/إعادة تشغيل الأنظمة لمنع الوصول إلى هذه الأنظمة أو المساعدة في تدميرها. قد تحتوي أنظمة التشغيل على أوامر لبدء إيقاف تشغيل/ إعادة تشغيل الجهاز. في بعض الحالات ، يمكن أيضًا استخدام هذه الأوامر لبدء إيقاف تشغيل/إعادة تشغيل جهاز كمبيوتر عن بعد. قد يؤدي إيقاف تشغيل الأنظمة أو إعادة تشغيلها إلى تعطيل الوصول إلى موارد الكمبيوتر للمستخدمين المصرح لهم.

إنتهى بفضل الله.