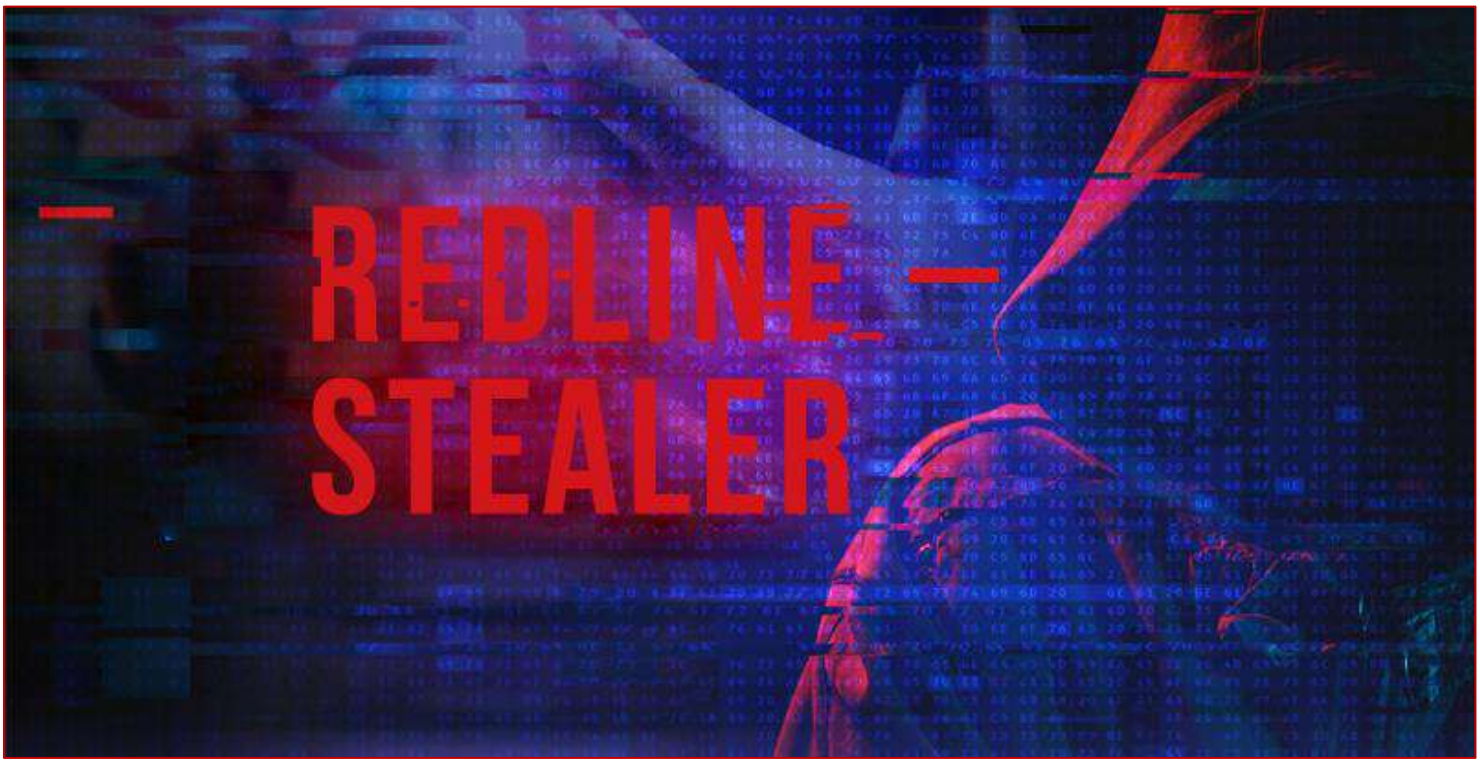
دراسة حول البرمجية الخبيثة Redline Stealer



إعداد م. سليمه كنينه

دائرة الاستجابة للطوارئ المعلوماتية

17/10/2023

الغاية من الدراسة

تهدف هذه الدراسة البسيطة إلى التعريف بالبرنامج الخبيث ريدلاين RedLine ومؤشرات الإصابة وطرق الوقاية منه ومعالجة النظم المصابة به، سيما أنه تم تسجيل العديد من الإصابات على الشبكة السورية في جهات عامة وخاصة، وتركّزت الإصابات بشكل كبير في جهات القطاع الخاص.

ما هو البرنامج الخبيث ريدلاين RedLine؟

What Is RedLine Stealer Malware?

Redline Stealer : عبارة عن برنامج ضار تم برمجته باستخدام لغة البرمجة C# مصمّم لسرقة المعلومات وإصابة نظم تشغيل Windows ببرامج ضارة أخرى (حيث يمكنه تحميل الملفات الضارة وتنفيذها)، يُستخدم لتحقيق الإيرادات عن طريق إساءة استخدام المعلومات التي يتم الحصول عليها. يمكن شراؤه أو الاشتراك به كخدمة (**M**alware–**a**s–**a**–**S**ervice) من منتديات الويب المظلم والويب العميق مقابل 150 دولار أو 200 دولار حسب الإصدار، ومن قناة Telegramوالدفع بعملة Bitcoin و Ethereum و XMR و LTC وUSDT.

يمكن لمجرمي الإنترنت استخدام **RedLine Stealer** لنشر برامج الفدية (Ransomware)، أحصنة طروادة للوصول عن بعد والحصول على صلاحيات إدارية (Remote Access/Administration Trojans) بالإضافة إلى استغلال موارد الأجهزة المصابة في تعدين العملات الرقمية(mine cryptocurrency). وبالتالي يمكن أن يعاني ضحايا RedLine Stealer من فقدان البيانات المالية، ويصبحون ضحايا لسرقة الهوية، ويواجهون مشاكل تتعلق بالخصوصية ومشاكل قانونية، وغيرها من المشكلات الخطيرة. علماً أنه لا يستخدم التشفير لإنشاء قناة آمنة عندما يتصل بخادم التحكم الخاص بالمهاجم، ويمكن التعرف على جميع الحزم والبيانات بسهولة على طبقة الشبكة بواسطة أدوات حماية الشبكة عن طريق إنشاء قواعد مخصصة لاكتشافها.

الهيئة الوطنية لخدمات تقانة المعلومات
مركز أمن المعلومات
دائرة الاستجابة للطوارئ المعلوماتية

الهيئة الوطنية لخدمات تقانة المعلومات
National Authority for IT Services

ملخص

Threat Summary:	
Name	RedLine Stealer virus
Threat Type	Password-stealing virus, banking malware, spyware.
Detection Names	Avast (Win32:DropperX-gen [Drp]), BitDefender (Trojan.GenericKD.33518015), ESET-NOD32 (A Variant Of MSIL/TrojanDownloader.Agent.GAO), Kaspersky (HEUR:Trojan-Downloader.MSIL.Seraph.gen), Full List (VirusTotal)
Malicious Process Name(s)	AddInProcess.exe
Payload	RedLine Stealer can be used to spread a variety of malicious programs.
Symptoms	Software of this kind is designed to stealthily infiltrate the victim's computer and remain silent, and thus no particular symptoms are clearly visible on an infected machine.
Distribution methods	Infected email attachments, malicious online advertisements, social engineering, software 'cracks'.
Damage	Stolen passwords and banking information, identity theft, the victim's computer added to a botnet.

تسميات بعض شركات تطوير برامج مكافحة البرمجيات الخبيثة العالمية:

Avast	Win32:DropperX-gen [Drp]
AVG	Win32:DropperX-gen [Drp]
BitDefender	Trojan.GenericKD.33518015
ESET-NOD32	A Variant Of MSIL/TrojanDownloader.Agent.GAO
Kaspersky	HEUR:Trojan-Downloader.MSIL.Seraph.gen
Malwarebytes	Malware.AI.303897203
Microsoft	Trojan:MSIL/RedLineStealer.ADA!MTB

Tel: +963 11 3937049 **Fax:** +963 11 3937079 P. Box:60 Sabouraa **E-mail:** infoisc@nans.gov.sy

Website: www.nans.gov.sy

بعض أسماء الملفات التنفيذية للبرنامج الخبيث

RedLine Stealer
Malicious Process Name
AddInProcess.exe
BK1VWG1F.exe
mydigitalcoin.info
SynapseX.rar
B2c6fe2d48502fdd3530f2dfcb2d4f6a.exe
https://github.com/abamo12466/alexandro/ra 32bde18a16c416077831b74838f80ad3w/main/Setup.exe
Setup.exe
https://itfolkstechnology.com/wp-download/zip.7z
https://github.com/Jonadesz/LockBit-RansomWare-CRACKED/blob/main/builder.exe
32bde18a16c416077831b74838f80ad3.bin.exe

إجرائيات تنفيذ برنامج ريدلاين RedLine

RedLine execution process

بعد تنفيذ RedLine Stealer على جهاز الضحية، يصبح البرنامج الخبيث قادر على:

1. **جمع المعلومات من جميع متصفحات الويب التي تعتمد على محرك Chromium مثل متصفح Google Chrome، ومتصفح Edge، ومن المتصفحات التي على محرك Gecko مثل متصفح Firefox :**

- تسجيلات الدخول.
- كلمات المرور.
- بيانات الملء التلقائي.
- ملفات تعريف الارتباط.
- تفاصيل بطاقة الائتمان.

يمكن لمجرمي الإنترنت إساءة استخدام هذه المعلومات للوصول إلى حسابات مختلفة على سبيل المثال:

((وسائل التواصل الاجتماعي، البريد الإلكتروني، الحسابات المصرفية، محافظ العملات المشفرة إن وجدت)).

تتضمن قائمة محافظ العملات التي يستهدفها RedLine:

((Armory, AtomicWallet, BitcoinCore, Bytecoin, DashCore, Electrum, Ethereum, LitecoinCore, Monero, Exodus, Zcash, Jaxx)).

تطبيقات وبرامج الشبكات الافتراضية VPN التي يستهدفها RedLine: ((ProtonVPN ,OpenVPN, NordVPN)).

يمكن لمجرمي الإنترنت استخدام البيانات المجمّعة والحسابات التي تم سرقتها:

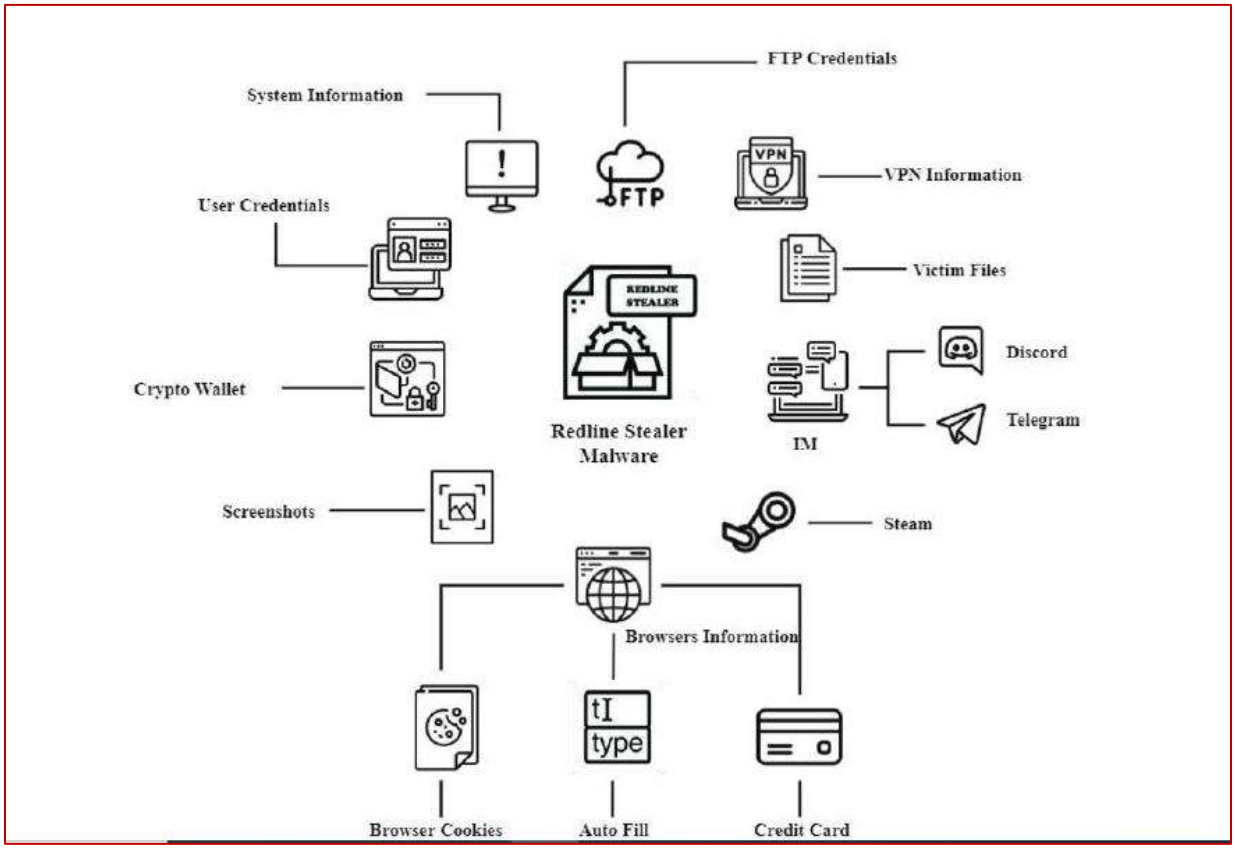
- لنشر البرامج الضارة.
- لإجراء حملات البريد العشوائي.
- لإجراء معاملات ومشتريات احتيالية.
- لخداع أشخاص آخرين لتحويل الأموال.
- لسرقة الهويات وما إلى ذلك.

2. جمع معلومات النظام :

- العناوين الشبكية (IP addresses).
- أسماء المستخدمين (usernames).
- إعدادات UAC (user account control)

- الحلول الأمنية المطبّقة (security solutions).

3. جمع البيانات من مختلف التطبيقات والبرامج التي تستخدم بروتوكول FTP (File Transfer Protocol) ومن مختلف التطبيقات والبرامج الخاصة بالمراسلة الفورية عبر الانترنت IM (Instant Messaging) والاستيلاء على الملفات المخزّنة على أجهزة الكمبيوتر المصابة.



طرق الإصابة بالبرنامج الخبيث ريدلاين RedLine

RedLine Stealer Distribution Method

يتسلل RedLine Stealer إلى جهاز الكمبيوتر بواسطة:

- ✓ الهندسة الاجتماعية لحملات البريد الإلكتروني العشوائي(spam): عادةً ما يقوم مجرمو الإنترنت بإرسال رسائل بريد إلكتروني تحتوي على مرفقات ضارة، حيث يتم إرفاق مستندات Microsoft Office و PDF ، وملفات الأرشيف (RAR و ZIP) والملفات القابلة للتنفيذ (exe. وغيرها) وملفات (JavaScript) إذا تم فتحها، فسيقوم RedLine بتثبيت برامج ضارة أخرى.
- ✓ أدوات كسر حماية البرامج (Crack): تستخدم لتفعيل البرامج بطريقة غير شرعية، إلا أنها غالبًا ما تقوم بتثبيت البرامج الضارة بدلاً من ذلك.
- ✓ الأدوات المزيفة لتحديث البرامج (fake updates): تتسبب في حدوث ضرر عن طريق تثبيت برامج ضارة بدلاً من التحديثات أو تقوم باستغلال الأخطاء/العيوب في البرامج القديمة المثبتة على نظام التشغيل.
- ✓ روابط المواقع غير الرسمية و شبكات (torrent clients) وأدوات تحميل البرامج (third party) لتحميل وتثبيت البرامج المجانية: تقوم بخداع المستخدمين لتثبيت برامج ضارة عن طريق إخفائها ضمن حزم البرامج الحقيقية.
- ✓ أحصنة طروادة (Trojans): يجب تثبيتها أولاً، غالبًا ما تتكاثر وتقوم بتثبيت برامج ضارة أخرى وتسبب عدوى متسلسلة.
- ✓ يستخدم مجرمو الانترنت موقع YouTube لنشر برنامج RedLine الخبيث: حيث يقومون بتحميل مقاطع فيديو للعبة Valorant مع رابط موقع الويب في الوصف الخاص بهم والذي من المفترض أن يقوم هذا الرابط بتحميل بوت للتصويب التلقائي (يستخدم للغش في اللعبة، حيث يتم الغش باستخدام برامج النقر التلقائي والتصويب التلقائي، وغيرها من البرامج غير المصرح بها التي تمنح اللاعبين أفضلية غير عادلة في اللعبة)، إلا أنه يقوم بتحميل ملف مضغوط يحتوي على ملف تنفيذي ضار مصمم لإصابة أجهزة الكمبيوتر ببرنامج RedLine الخبيث.

لعبة Valorant فالورانت: هي لعبة فيديو مجانية متعددة اللاعبين من تطوير ونشر شركة ريوت غيمز وصدرت على نظام التشغيل مايكروسوفت ويندوز.

الهيئة الوطنية لخدمات تقانة المعلومات
مركز أمن المعلومات
دائرة الاستجابة للطوارئ المعلوماتية

الهيئة الوطنية لخدمات تقانة المعلومات
National Authority for IT Services

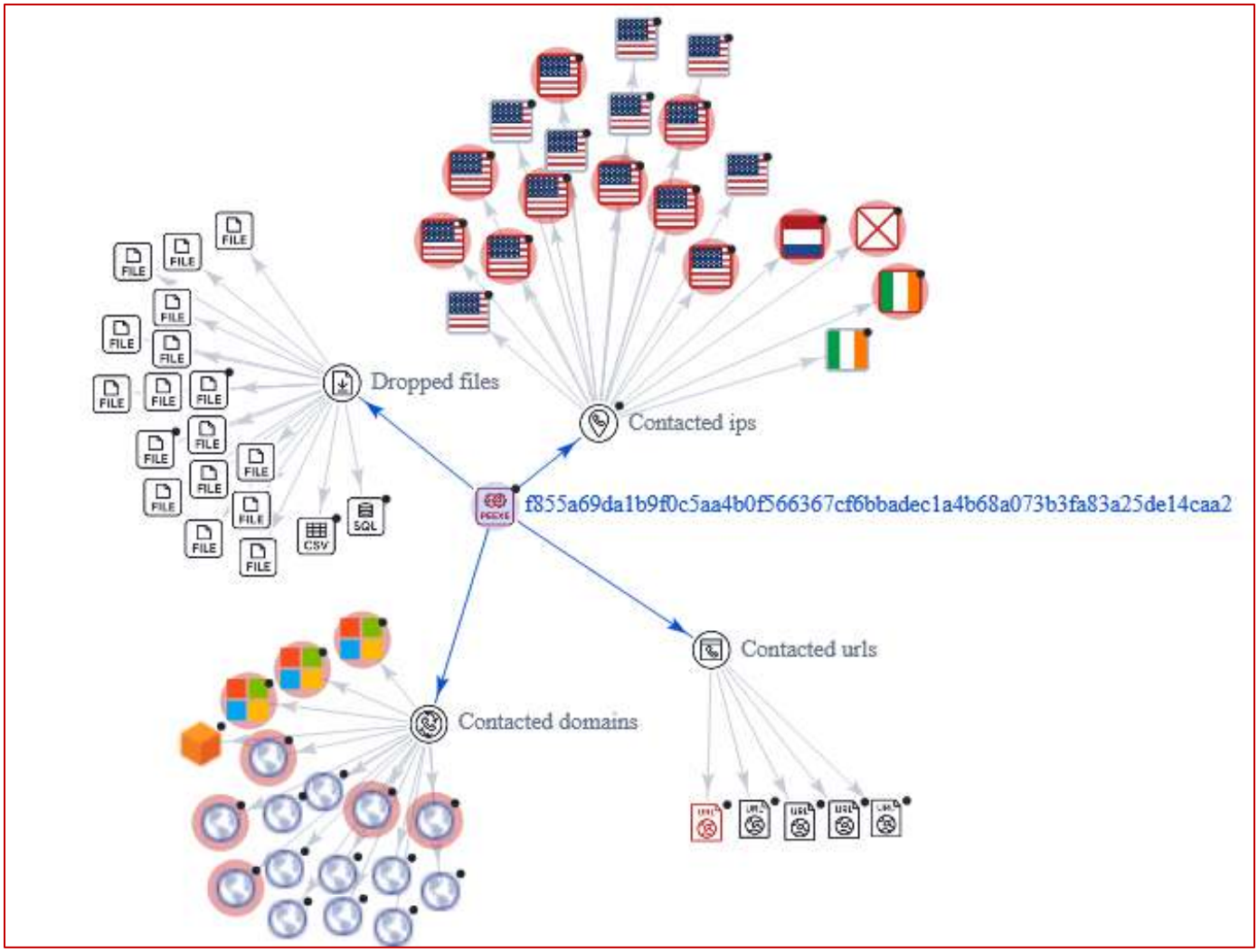
حملات نشر برمجية ريدلاين RedLine Stealer

الوقت	الحملة
تحديث 20 -3- 2020	حملة عبر البريد الإلكتروني العشوائي لتوزيع RedLine Stealer حيث يقوم مجرمو الانترنت بإرسال آلاف من الرسائل المخادعة التي تطلب المساعدة في إجراء بحث طبي يتعلق بفيروس كورونا. ظهور موقع ويب احتيالي(mydigitalcoin.info) للحصول علىBitcoin بتكوين مجانًا!
تحديث 3 -11- 2020	أدوات تثبيت Inno Setup المزيفة لبرنامج TeamViewer حيث يتم تنفيذ الملف'wmiprvse.exe' ، الذي يقوم بتبيث الملف الضار 'msi.dll' الذي يتصل بعنوان URL الضار الذي يستضيف البرنامج الضار RedLine لسرقة كلمات المرور. تطبيقات العملات المشفرة المزيفة المستخدمة لإخفاء البرمجيات الخبيثةRedLine Stealer
تحديث 9-11-2021	وجود صفحة لتحميل LastPass مزيفة تُستخدم لتوزيع ملف ISO بلاحقة يؤدي إلى حقن برنامج RedLine الخبيث. يتمتع الآن أحدث إصدار من برنامج RedLine الخبيث بقدرات إضافية فهو يجمع المزيد من المعلومات العامة (مثل الرمز البريدي والمنطقة الزمنية والمدينة والأجهزة المثبتة)، ويفحص النظام بحثًا عن العمليات الجارية والمتصفحات المثبتة واتصالات FTP والبيانات الأخرى. كما أنه يتحقق من وجود Discord و VPN و Steam و Telegramوغيرهم من العملاء ومحافظ العملات المشفرة.
تحديث 16-3-2022	يستخدم مجرمو الانترنت موقع YouTube لتوزيع برنامج RedLine الخبيث. حيث يقومون بتحميل مقاطع فيديو للعبة Valorant مع رابط موقع الويب في الوصف الخاص بهم، من المفترض أن يقوم هذا الرابط بتحميل بوت للتصويب التلقائي، إلا أنه يقوم بتحميل ملف مضغوط يحتوي على ملف تنفيذي ضار مصمم لإصابة أجهزة الكمبيوتر ببرنامج RedLine الخبيث.
تحديث 17-3-2023	حملة بريد عشوائي جديدة تحت عنوان Adobe Acrobat Sign لنشر RedLine Stealer

Tel: +963 11 3937049 **Fax:** +963 11 3937079 P. Box:60 Sabouraa **E-mail:** infoisc@nans.gov.sy

Website: www.nans.gov.sy

RedLine Infostealer اتصالات



RedLine malware
يتصل بالروابط التالية
http://45.153.184.122:6677/IRemotePanel
http://www.geoplugin.net/json.gp?ip=95.222.165.118
http://checkip.amazonaws.com
http://www.geoplugin.net/json.gp?ip=95.211.190.199
http://www.microsoft.com/pki/certs/MicRooCerAut_2010-06-23.crt
http://express-vpns.biz
http://express-vpns.cloud
http://express-vpns.fun
http://express-vpns.online
http://express-vpns.pro
http://express-vpns.xyz
http://45.137.22.152:55615
http://copy-marco.gl.at.ply.gg:51589
http://raizen.serveftp.com:48770
http://jul-nelson.gl.at.ply.gg:47198
http://103.202.55.51:55615
http://185.241.208.44:35361
http://siyatermi.duckdns.org:17044
http://103.202.55.11:55615
http://103.202.55.172:65012
http://45.154.98.129:35361
http://15.228.188.221:4483

http://185.159.129.168/clpr/OWUsN2UsODMsOWIsOWUsODIsOTAsOTEsNjQsN2Ys
http://185.237.15.169:27164
http://45.95.168.220:55615
http://176.42.9.192:20331
http://2.56.254.150:35955
http://185.147.34.178:55615
http://81.161.229.45:47652
http://172.177.156.145:33325
http://16.16.126.164:48082
يتصل بالعناوين التالية
130.155.190.20.in-addr.arpa
14.110.152.52.in-addr.arpa
210.31.213.23.in-addr.arpa
226.101.242.52.in-addr.arpa
254.129.249.8.in-addr.arpa
41.69.35.23.in-addr.arpa
alabamasan.ru
amazonaws.com
arc.msn.com
checkip.amazonaws.com
fp2e7a.wpc.2be4.phicdn.net
fp2e7a.wpc.phicdn.net
geoplugin.net

login.live.com
microsoft.com
prda.aadg.msidentity.com
www.geoplugin.net
www.microsoft.com
7.tcp.eu.ngrok.io
0.tcp.eu.ngrok.io
afgantrophy.top
vikaneleneer.shop
5.tcp.eu.ngrok.io
6.tcp.eu.ngrok.io
isahelyria.site
2.tcp.eu.ngrok.io
mcth.xyz
copy-marco.gl.at.ply.gg
siyatermi.duckdns.org
raizen.serveftp.com
gbsbreakes.com
0.tcp.in.ngrok.io
4.tcp.eu.ngrok.io
jul-nelson.gl.at.ply.gg
marduk.top
amadapi.tuktuk.ug
tttmundo2022.eastus.cloudapp.azure.com

sept6amd.tuktuk.ug
afterburners-msi.com
afterburner-download.org
anydesk24.com
يتصل بالعناوين الشبكية التالية
104.86.182.43
178.237.33.50
18.214.132.216
18.233.90.151
18.235.112.207
192.168.0.1
192.229.211.108
192.229.221.95
20.190.159.134
20.82.210.154
20.99.132.105
20.99.133.109
20.99.184.37
20.99.185.48
20.99.186.246
23.216.147.76
23.40.197.184
3.224.145.145
34.192.250.175

34.196.181.158
34.197.12.81
34.198.132.204
34.236.80.17
40.126.31.1
40.126.31.135
40.126.31.137
40.126.31.139
40.126.31.141
40.126.31.6
40.126.31.8
45.153.184.122
52.0.197.231
52.200.161.135
52.206.178.1
81.177.141.52
135.181.7.171
54.91.200.119
94.142.138.4
85.209.176.171
185.209.22.181
185.215.113.69
194.104.136.5
194.50.153.135

193.106.191.253
92.42.47.244
91.121.67.60
135.181.129.119
77.232.38.156
45.9.20.20
65.108.69.168
159.69.246.184
77.91.124.82
77.91.68.56
185.225.74.51
5.42.65.101
يقوم بتحميل المكتبات التالية
mscoree.dll : CorExeMain

الوقاية من الإصابة

كيفية تجنب الإصابة بالبرمجيات الخبيثة

How to avoid malware

كما هو الحال مع أي برامج ضارة أخرى، من الأفضل اتخاذ الإجراءات الوقائية لمنع الإصابة، بدلاً من علاج المشكلات التي تلي الإصابة، ولذلك يوصى بالتالي:

- ✓ التحديث الدوري لنظم التشغيل (تفعيل خدمة التحديثات التلقائية).
- ✓ تثبيت برامج مكافحة البرمجيات الخبيثة ذات السمعة الجيدة والتحديث الدوري لها.

- ✓ فحص أنظمة التشغيل بانتظام بحثًا عن التهديدات باستخدام برامج مكافحة الفيروسات أو برامج مكافحة التجسس.
- ✓ استخدام برمجيات أو تجهيزات لفحص البريد الالكتروني **(Anti-Spam)** لمنع وصول مرفقات البريد المشبوهة وحجب مصدرها.
- ✓ إعداد تكوين بروتوكولات الإنترنت لمصادقة البريد الإلكتروني وعناصر التحكم الأمنية مثل **DKIM** و **DMARC** و **SPF**. (يساعد نظام التعرف على هوية المرسل في مصادقة مرسلي البريد الإلكتروني من خلال التحقق من أن رسائل البريد الإلكتروني جاءت من النطاق الذي يدعون أنهم منه. تعد طرق المصادقة الثلاثة هذه مهمة لمنع البريد العشوائي وهجمات التصيد الاحتيالي ومخاطر أمان البريد الإلكتروني الأخرى).
- ✓ ضبط المنافذ المفتوحة وحركة البيانات من خلال استخدام الجدران النارية **(Firewall)**.
- ✓ استخدام أجهزة أو برمجيات كشف ومنع التطفل**(IPDS,IDS)** لفحص حركة البيانات على الشبكة.
- ✓ تقسيم الشبكة إلى **VLANs** لعزل الشبكات والخدمات ومستخدميها حسب الأهمية والحاجة.
- ✓ مراقبة حركة البيانات من الأجهزة والشبكات لاكتشاف الأنشطة المشبوهة والأنماط غير المعتادة.
- ✓ عدم استخدام شبكة Wi-Fi مفتوحة مجهولة المصدر للوصول إلى الانترنت.
- ✓ إدارة المستخدمين والموارد والصلاحيات على مستوى نظم التشغيل والخدمات الإلكترونية وحسابات التواصل الاجتماعي.
- ✓ عدم منح المستخدمين الأذونات لإيقاف برنامج مكافحة الفيروسات أو جدار الحماية.
- ✓ عدم منح المستخدمين العاديين الأذونات لتحميل وتثبيت البرامج.
- ✓ تحميل البرامج من المواقع الرسمية وعبر الروابط المباشرة.
- ✓ تجنب حفظ البيانات المهمة عن طريق الملفات النصية في مجلد على سطح المكتب، والمستندات، وما إلى ذلك، ويجب حفظها في مجلدات مقفولة بكلمات مرور.
- ✓ يجب تحديث البرامج المثبتة وتفعيلها من خلال الأدوات أو الوظائف التي صممها المطورون الرسميون.
- ✓ تقييد المستخدمين عند تصفح الويب.

- ✓ تثبيت إضافة (Ad blocker)على المتصفح لإيقاف الإعلانات الضارة – أحصنة طروادة – التصيد الاحتيالي – والمحتويات غير المرغوب بها.
- ✓ توعية وتدريب المستخدمين بتقنيات الهندسة الاجتماعية والتهديدات سواء فيما يتعلق بالبريد الالكتروني – رسائل SMS – برامج المراسلة أو أي تطبيقات أخرى.
- ✓ توخي الحذر عند فتح مرفقات البريد الالكتروني حتى لو كان المرفق متوقع ويبدو أن المرسل معروف.
- ✓ لا ينبغي الوثوق برسائل البريد الإلكتروني غير ذات الصلة التي يتم تلقيها من عناوين مشبوهة وغير معروفة وتحتوي على مرفقات/روابط (لا تفتح المحتويات).
- ✓ الحد من استخدام ميّزة حفظ كلمة المرور على متصفح الويب وذلك للحد من خطر تسرّب المعلومات.
- ✓ تغيير كلمات المرور بانتظام، كما يجب فرض سياسات كلمة مرور قوية لجميع الموظفين.
- ✓ تفعيل ميزات الحماية التي توفرها وسائط التواصل الاجتماعي والبريد الإلكتروني للحسابات الحكومية مثل المصادقة متعددة العوامل (**MFA**) وآليات استعادة الحساب ومنح الصلاحيات المناسبة حسب طبيعة العمل والخبرة الفنية والتأكد من إمكانية استعادة الحسابات في حال اختراقها:
- ✓ الحد من إعادة استخدام كلمات المرور نفسها على منصات مختلفة.
- ✓ تعطيل تنفيذ وحدات الماكرو في MS Office وعدم منح المستخدمين الأذونات لتنفيذ برمجيات الماكرو.

المعالجة

كيفية إزالة البرنامج الخبيث ريد لاين

How to remove RedLine Stealer

- ✓ عزل الجهاز المصاب عن الشبكة.
- ✓ إعادة تشغيل الكمبيوتر واختيار الوضع الآمن مع الشبكة **Safe Mode with Networking**

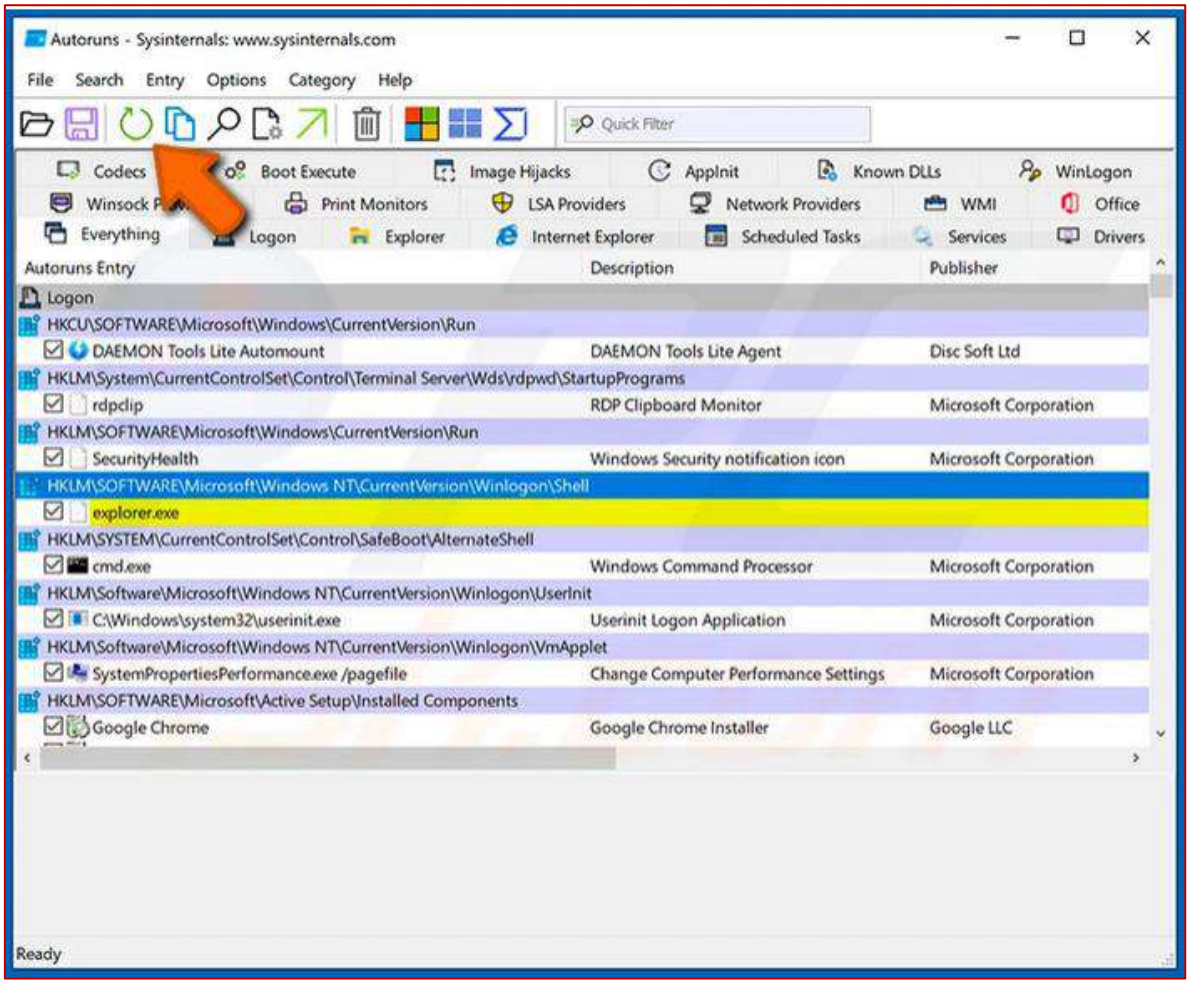
(يعمل الوضـع الآمن على تشـغيل نظام التشـغيل Windows بالحد الأدنى فقط من عدد برامج التشغيل والخدمات اللازمة للتشغيل، يؤدي هذا غالبًا إلى منع تحميل البرامج الضارة أو غيرها من البرامج التي تعمل بشكل سيء، كما يسهل عملية تنظيفها).

بمجرد تشغيل البرامج الضارة في ذاكرة جهاز الكمبيوتر الخاص بك، قد يكون من الصعب إزالتها، غالبًا ما يتم إنشاء البرامج الضارة باستخدام ما نسميه خاصية 'الاستمرارية'("persistence")، مما يعني أنه إذا تم تشـــغيلها ولاحظت أن ملفاتها قد تم حذفها أو عزلها بواســـطة برنامج الأمان، فستحاول البرامج الضارة إعادة كتابة الملفات على القرص الصلب للجهاز، تتيح لنا إعادة التشغيل في الوضـع الآمن فرصـة تحميل نظام التشـغيل Windows دون تحميل البرامج الضـارة، حتى نتمكن من تنظيف الملفات من محرك الأقراص دون أن تحاول البرامج الضارة الموجودة في الذاكرة إعادة تثبيت نفسها.

- ✓ استخدم أداة إزالة البرامج الضارة من **Kaspersky** :
  - ➢ https://www.kaspersky.com/downloads/free-virus-removal-tool
- ✓ استخدم أداة **Microsoft Safety Scanner** :
  - ➢ https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download?view=o365-worldwide
- ✓ إذا تعذر اكتشـاف البرنامج الخبيث أو إزالته باسـتخدام Microsoft Safety Scanner أو أداة إزالة البرامج الضارة لنظام التشغيلWindows ، فجرّب الخطوات التالية((إنّ إزالة التهديدات يدويًا تتطلب مهارات كمبيوتر متقدمة)):

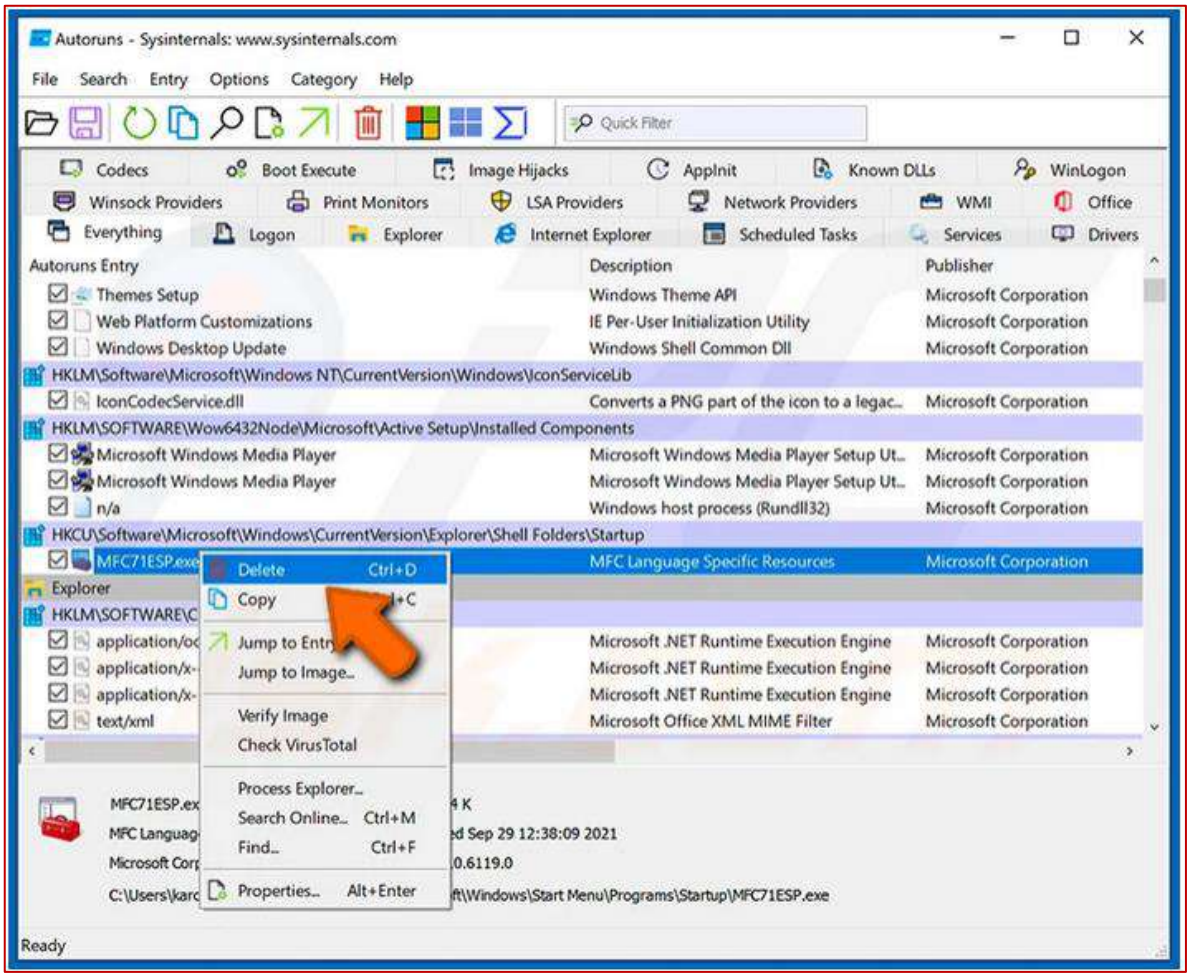
1. قم بتحميل برنامج **Autoruns.exe** من الرابط التالي وقم بتشغيله
   - ➢ https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns

- انقر فوق 'Options' في الجزء العلوي وقم بإلغاء تحديد 'Hide Empty Locations' وخيارات 'Hide Windows Entries' بعد هذا الإجراء، انقر فوق أيقونة 'Refresh'

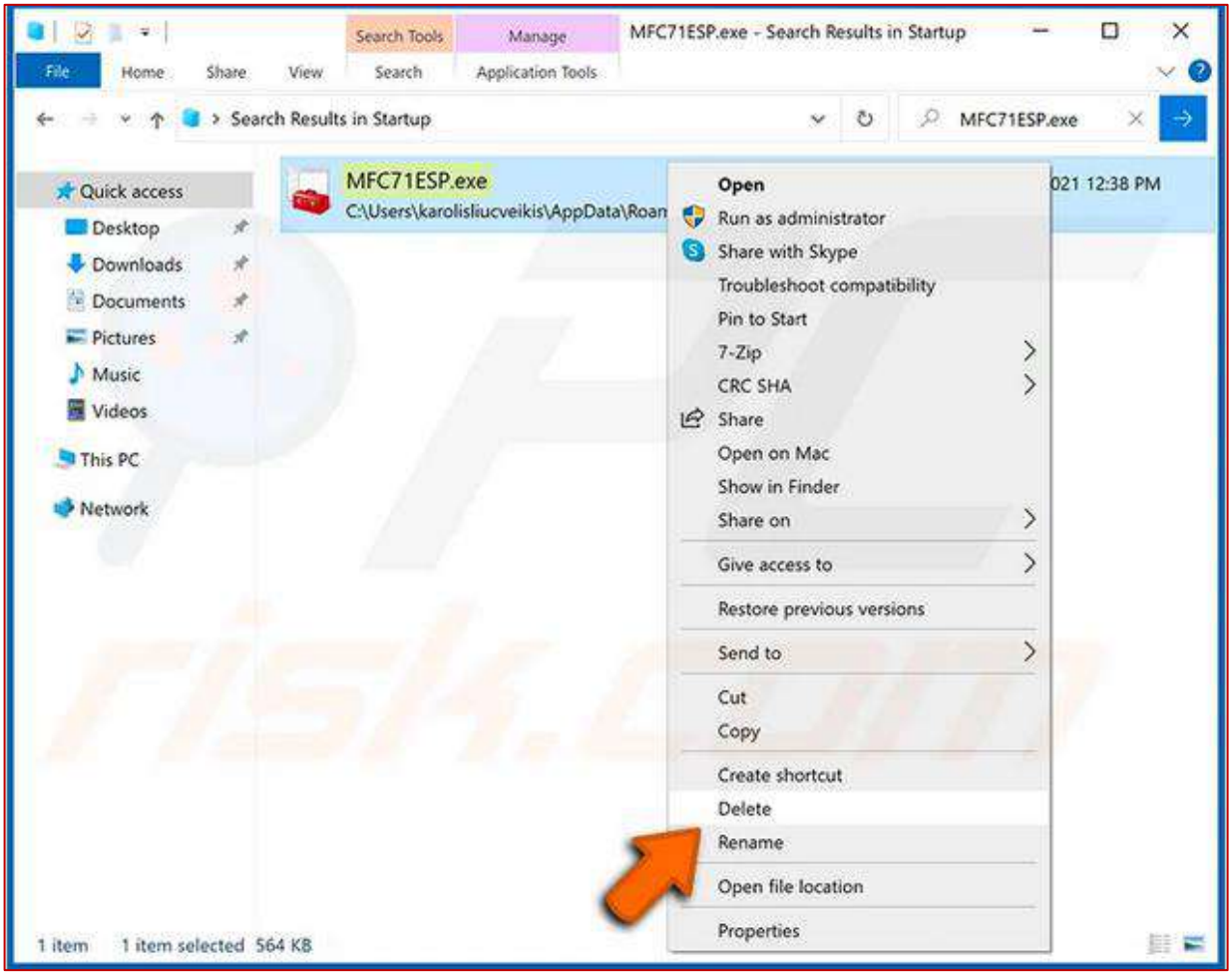


- تحقق من القائمة المقدّمة من تطبيق Autoruns وحدّد موقع ملف البرامج الضـــارة الذي تريد إزالته.
- يجب عليك كتابة المسار الكامل والاسم. لاحظ أنّ بعض البرامج الضارة تخفي أسماء العمليات تحت أسماء عمليات Windows الشرعية، في هذه المرحلة من المهم جدًا تجنّب إزالة ملفات النظام.

- بعد تحديد موقع البرنامج المشـبوه الذي ترغب في إزالته، انقر بزر الماوس الأيمن فوق اسـمه واختر 'Delete'.



- بعد إزالة البرامج الضارة من خلال تطبيق Autoruns ، يجب عليك البحث عن اسم البرامج الضارة على جهاز الكمبيوتر الخاص بك. تأكد من تمكين الملفات والمجلدات المخفية قبل المتابعة (enable hidden files and folders) إذا وجدت اسم ملف البرامج الضارة فتأكد من إزالته .



كما يمكننا اتباع خطوات إضافية للتأكد ولإزالة البرمجيات الخبيثة:

2. البحث عن الحسابات غير العادية التي تم إنشاؤها، خاصة في مجموعة المسؤولين:
   C:\> lusrmgr.msc
3. البحث ضمن المجلدات والملفات:
   - عن الملفات التي حجمها أكبر من 5 ميغا.
   - البحث عن الملفات غير العادية التي تمت إضافتها مؤخرًا في مجلدات النظام، وخاصة C:WINDOWS/system32
   - البحث ضمن الملفات المخفية.C:\> dir /S /A:H
4. البحث عن وجود أي مكونات للبرمجيات الخبيثة ضمن مسجل النظام (Registry).
   بمجرد الدخول، اضغط على CTRL و F معًا واكتب اسم البرنامج الخبيث ثم انقر بزر الماوس الأيمن واحذف أي إدخالات تجدها تحمل اسمًا مشابهًا.
5. التحقق من مجلد التشغيل التلقائي للمستخدم (Startup) .
6. البحث عن أي (Processes) و (Services) غير اعتيادية وبشكل خاص التي تتبع حسابات "SYSTEM" ، "ADMINISTRATOR" من خلال C:\> taskmgr.exe
7. البحث عن خدمات الشبكة غير العادية/غير المتوقعة التي تم تثبيتها وبدء تشغيلها
   C:\> services.msc
8. التأكد من أي نشاط غير عادي على الشبكة:
   - التحقق الملفات التي تم مشاركتها والتأكد من أن كل منها مرتبط بنشاط عادي
     C:\> net view \\127.0.0.1
   - إلقاء نظرة إلى الجلسات المفتوحة على الجهاز. C:\> net session
   - إلقاء نظرة على الجلسات التي فتحها الجهاز مع الأنظمة الأخرى C:\> net use
   - التحقق من وجود أي اتصال NetBIOS مشبوه C:\> nbtstat –S
   - البحث عن أي نشاط مشبوه على منافذ النظام C:\> netstat –na 5
     (5 يجعلها يتم تحديثها كل 5 ثواني)

9. النظر إلى قائمة المهام المجدولة بحثًا عن أي إدخال غير عادي C:\>schtasks.exe
10. مراقبة ملفات السجل (log files) بحثًا عن الإدخالات غير المعتادة C:\> eventvwr.msc

- البحث عن الأحداث التي تؤثر على جدار الحماية أو برنامج مكافحة الفيروسات أو حماية الملفات أو أي خدمة جديدة مشبوهة .
- البحث عن عدد كبير من محاولات تسجيل الدخول الفاشلة أو الحسابات المقفلة.
- مراقبة ملفات سجل جدار الحماية وملفات برامج/أجهزة كشف ومنع التطفل (إن وجدت) بحثًا عن أي نشاط مشبوه.

11. (Rootkit check) من الأفضل دائمًا تشغيل العديد من الأدوات بدلاً من تشغيل أداة واحدة فقط.
12. (Malware check) تشغيل منتج واحد على الأقل لمكافحة الفيروسات على القرص بأكمله، إذا أمكن، استخدم العديد من برامج مكافحة الفيروسات، يجب أن يكون برنامج مكافحة الفيروسات محدثًا تمامًا.
13. حذف وإزالة البرامج التي تم تحميلها من الانترنت من مصادر غير موثوقة قبل تنفيذها.
14. البحث ضمن البرامج وحذف جميع البرامج التي تظهر بأسماء غريبة.

✓ الكشف عن بقية الأجهزة المتصلة على نفس الشبكة المحلية.

المراجع:

- https://www.pcrisk.com/removal-guides/17280-redlinestealer-malware
- https://www.virustotal.com/gui/file/f855a69da1b9f0c5aa4b0f566367cf6bbadec1a4b68a073b3fa83a25de14caa2/relations
- https://any.run/malware-trends/redline
- https://resources.infosecinstitute.com/topics/malware-analysis/redline-stealer-malware-full-analysis