

Yellow RAT Lab

المحتوى

2.....	Scenario
3.....	Q1
4.....	Q2
5.....	Q3
7.....	Q5
9.....	Q6
10.....	معلومات اضافية
10.....	ما هو RAT (Remote Access Trojan) ؟
12.....	ملفات .dat
13.....	ال C2 Server

Scenario

During a regular IT security check at GlobalTech Industries, abnormal network traffic was detected from multiple workstations. Upon initial investigation, it was discovered that certain employees' search queries were being redirected to unfamiliar websites. This discovery raised concerns and prompted a more thorough investigation. Your task is to investigate this incident and gather as much information as possible.

السيناريو

أثناء فحص دوري لأمن تكنولوجيا المعلومات في شركة GlobalTech، تم رصد حركة مرور غير طبيعية على الشبكة من عدة محطات عمل. وعند إجراء تحقيق أولي، تبين أن استعلامات بحث بعض الموظفين تُعاد توجيهها إلى مواقع ويب غير مألوفة. أثار هذا الاكتشاف مخاوف ودفع إلى إجراء تحقيق أكثر شمولاً. مهمتكم هي التحقيق في هذا الحادث وجمع أكبر قدر ممكن من المعلومات.

Q1

Understanding the adversary helps defend against attacks. What is the name of the malware family that causes abnormal network traffic?

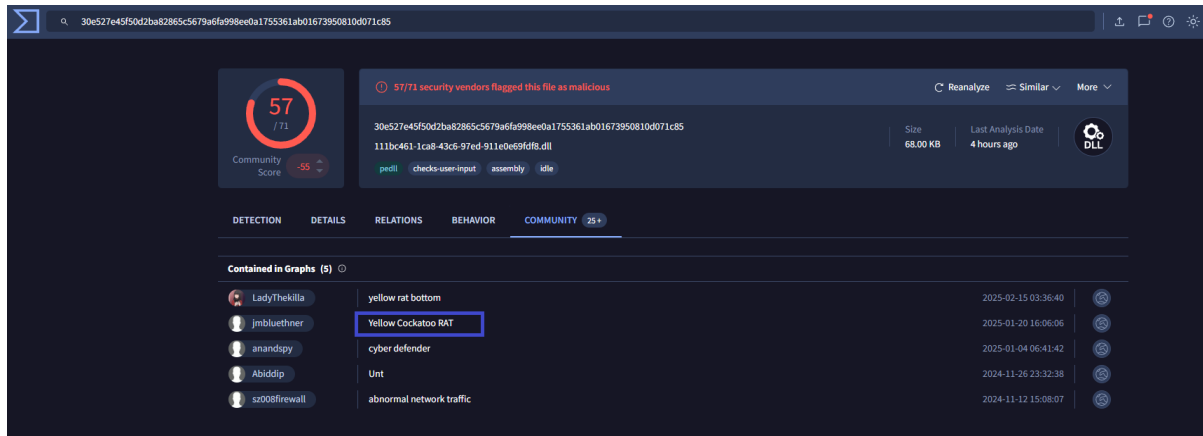
Answer : Yellow Cockatoo RAT

ما اسم عائلة البرمجية الخبيثة؟

الإجابة : Yellow Cockatoo RAT

هذه البرمجية الخبيثة تنتمي إلى عائلة **Yellow Cockatoo RAT** وهي RAT (تروجان وصول عن بُعد). من مهامها التجسس، سرقة البيانات، والسيطرة الكاملة على الجهاز المصاب.

تأخذ الـ **HASH** من الملف الذي قمت بتحميله من الموقع ثم تذهب الى موقع **virostotal** ثم تذهب الى قسم الـ **community** من ثم تبحث في هذا القسم و تجد الجواب [**Yellow Cockatoo RAT**]



30e527e45f50d2ba82865c5679a6fa998ee0a1755361ab01673950810d071c85

57/71
Community Score

57/71 security vendors flagged this file as malicious

30e527e45f50d2ba82865c5679a6fa998ee0a1755361ab01673950810d071c85
111bc461-1ca8-43c6-97ed-911e0e69f0f8.dll

Size: 68.00 KB
Last Analysis Date: 4 hours ago

Reanalyze Similar More

pedi checks-user-input assembly idle

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 26+

Contained in Graphs (5)

File Name	Hash	Date
LadyTheKilla	yellow rat bottom	2025-02-15 03:36:40
jmbiuehner	Yellow Cockatoo RAT	2025-01-20 16:06:06
anandspy	cyber defender	2025-01-04 06:41:42
Abiddip	Unt	2024-11-26 23:32:38
sz008firewall	abnormal network traffic	2024-11-12 15:08:07

Q2

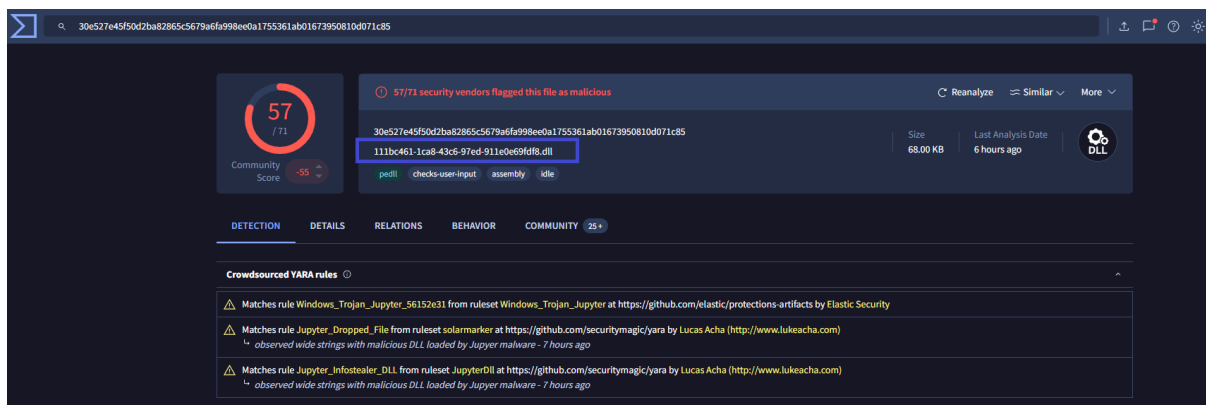
As part of our incident response, knowing common filenames the malware uses can help scan other workstations for potential infection. What is the common filename associated with the malware discovered on our workstations?

Answer : 111bc461-1ca8-43c6-97ed-911e0e69fdf8.dll

ما هو اسم الملف الشائع الذي تستخدمه البرمجية؟

الإجابة : 111bc461-1ca8-43c6-97ed-911e0e69fdf8.dll

تستخدم البرمجيات الخبيثة أسماء ملفات غير ملفتة للانتباه أو عشوائية كوسيلة تمويه. في هذا التحدي، تم اكتشاف ملف DLL تم تحميله في نظام المستخدم ويعمل كـ loader أو وحدة تحميل إضافية لتنفيذ التعليمات الخبيثة.



The screenshot shows the VirusTotal analysis page for the file 111bc461-1ca8-43c6-97ed-911e0e69fdf8.dll. The file is identified as a DLL, 68.00 KB in size, and was last analyzed 6 hours ago. It has a community score of 57/71 and is flagged as malicious by 57/71 security vendors. The analysis shows matches for several YARA rules, including Windows_Trojan_Jupyer_56152e31, Jupyer_Dropped_File, and Jupyer_Infostealer_DLL, all of which are associated with the Jupyer malware family. The file is also associated with the Jupyer malware family.

Q3

Determining the compilation timestamp of malware can reveal insights into its development and deployment timeline. What is the compilation timestamp of the malware that infected our network?

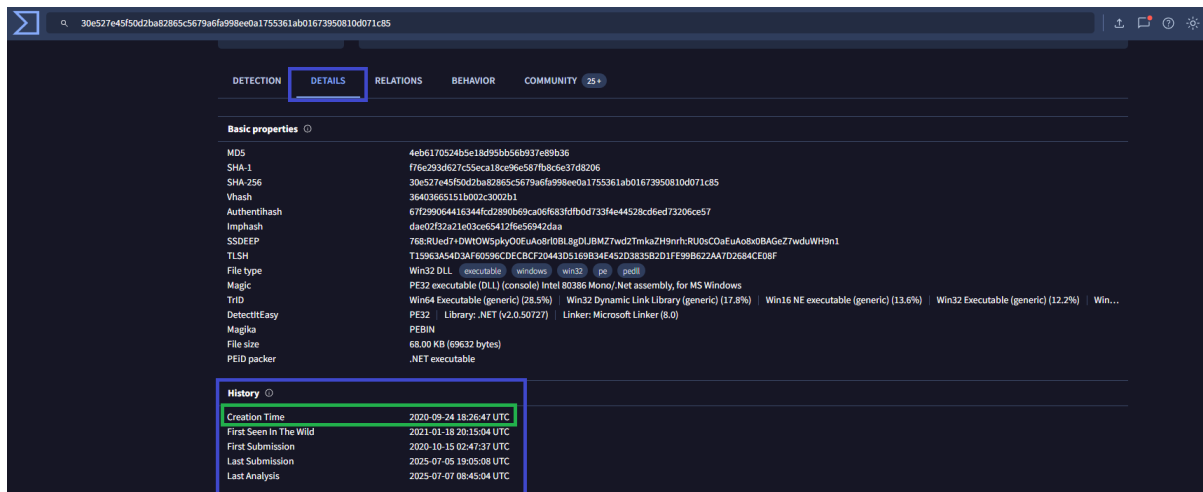
ما هو توقيت تجميع (compilation timestamp) البرمجية؟

الإجابة : 2020-09-24 18:26

توقيت التجميع يُستخرج من رأس ملف PE (مثل ملفات DLL أو EXE). هذا التوقيت يدل على لحظة إنشاء الملف أو آخر مرة تم فيها تجميع الكود، مما يعطي فكرة عن وقت تطوير البرمجية.

تذهب الى **details** ثم تبحث في قسم ال **history** ,

وتجد الإجابة في القسم ال **history** وابحث عن **Creation Time** [Creation Time 2020-09-24 18:26]



The screenshot shows the VirusTotal analysis page for a malware sample. The 'DETAILS' tab is selected, displaying various properties and a history section. The 'Creation Time' in the history is highlighted as 2020-09-24 18:26:47 UTC.

Basic properties	
MD5	4eb170524b5e18d99b5b56b937e89b36
SHA-1	f76e293d627c55eca18ce9e587fb8ce37d8206
SHA-256	30e527e45f50d2ba82865c5679a6fa998ee0a1755361ab01673950810d071c85
Vhash	36403665151b002c3002b1
Authenticash	67f299064416344cd2890b69ca06f683f9fbd733f4e4528cd6ed73206ce57
ImpHash	dae02f32a21e03ce65412f6e56942daa
SSDEEP	768:RUed7+DWTOWSpkyO0EuaO8r10BL8gDUBM27wd2TmkaZH9nrh:RU0sC0aEuA08x0BAGeZ7wdwWH9n1
TLSH	T15963A54D3AF60596CDECBF20443D5169834E452D383582D1FE998622AA7D2684CE08f
File type	Win32-DLL (executable) [Windows] [Win32] [PE] [GUI]
Magic	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
TrID	Win64 Executable (generic) (28.5%) Win32 Dynamic Link Library (generic) (17.8%) Win16 NE executable (generic) (13.6%) Win32 Executable (generic) (12.2%) Win...
DetectItEasy	PE32 Library: .NET (v2.0.50727) Linker: Microsoft Linker (8.0)
Maggika	PEBIN
File size	68.00 KB (69632 bytes)
PEID packer	.NET executable

History	
Creation Time	2020-09-24 18:26:47 UTC
First Seen in The Wild	2021-01-18 20:15:04 UTC
First Submission	2020-10-15 02:47:37 UTC
Last Submission	2025-07-05 19:05:08 UTC
Last Analysis	2025-07-07 08:45:04 UTC

Q4

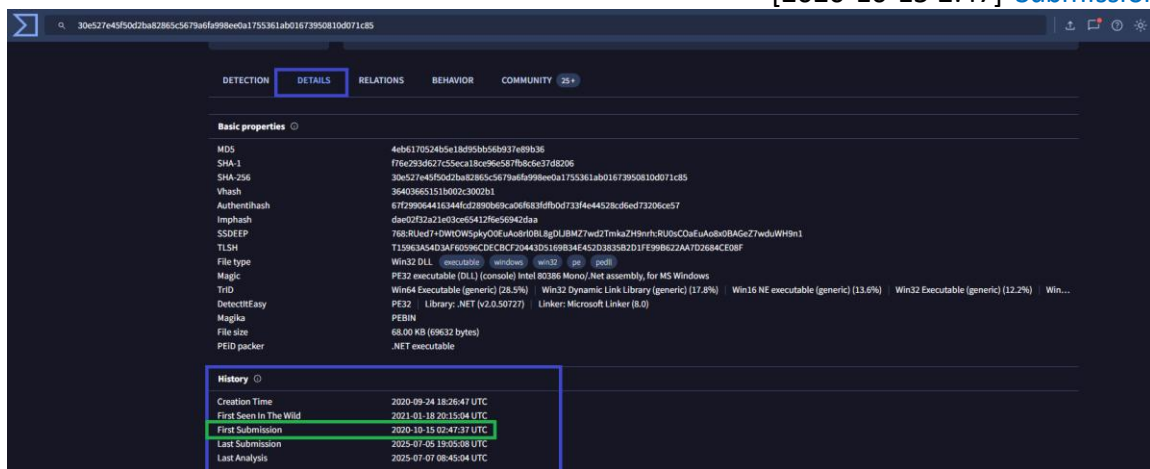
Understanding when the broader cybersecurity community first identified the malware could help determine how long the malware might have been in the environment before detection. When was the malware first submitted to VirusTotal?

متى تم إرسال البرمجية لأول مرة إلى VirusTotal؟

الإجابة : 2020-10-15 02:47

تاريخ أول رفع للملف على VirusTotal يُظهر متى اكتشف المجتمع الأمني هذه البرمجية الخبيثة. يمكن مقارنته بتاريخ التسلسل لمعرفة مدة "الإقامة" داخل الشبكة قبل اكتشافها.

تذهب إلى **details** ثم تبحث في قسم ال **history** , وتجد الإجابة في القسم ال **history** وابحث عن **First Submission** [2020-10-15 2:47]



Property	Value
MD5	4eb6170524b5e18d99bb5b937e89b36
SHA-1	f76e293d627c55eca18ce9e587b8ce37d8206
SHA-256	30e527e45f50d2ba82865c5679a6fa998e0a1755361ab01673950810d071c85
Vhash	36403665151b002c3002b1
Authenthash	67f299064416344fc2890b69ca06f631fbb0d7334e44528cd6ed73206ce57
Imphash	d4e02f3d2210310e541278e69f42daa
SSDEEP	768:Rl4d71-DWOW5phYQ8UAsvI0RL8pJRMZ7wd2Tmkaz7H9rhRj0uCOafoABAGz7wduWH9n1
TLSH	T3963A54D3AF60594CDECBCF20443D5169B34E45D3838201FE998622AA70268ACE08F
File type	Win32 DLL (executable) windows win32 pe (pdf)
Magic	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
TrID	Win64 Executable (generic) (28.5%) Win32 Dynamic Link Library (generic) (17.8%) Win16 NE executable (generic) (13.6%) Win32 Executable (generic) (12.2%) Win...
DetectItEasy	PE32 Library: .NET (v2.0.50727) Linker: Microsoft Linker (8.0)
Magika	PEBIN
File size	68.00 KB (6932 bytes)
PEID packer	.NET executable

History	Date
Creation Time	2020-09-24 18:26:47 UTC
First Seen In The Wild	2021-01-18 20:15:04 UTC
First Submission	2020-10-15 02:47:37 UTC
Last Submission	2025-07-05 19:05:08 UTC
Last Analysis	2025-07-07 08:45:04 UTC

Q5

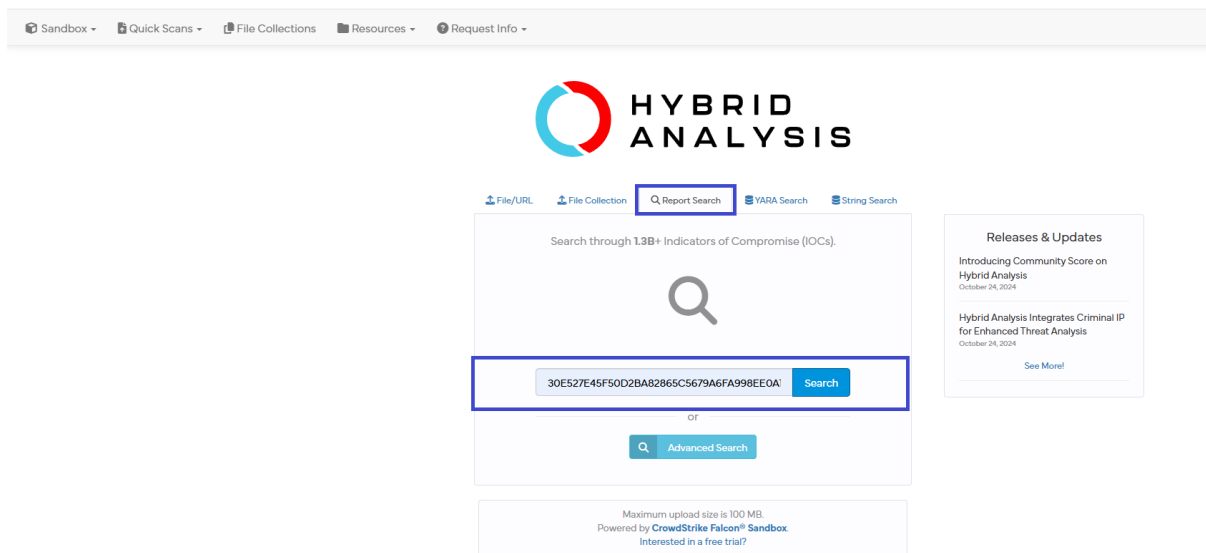
To completely eradicate the threat from Industries' systems, we need to identify all components dropped by the malware. What is the name of the .dat file that the malware dropped in the AppData folder?

ما هو اسم ملف الـ .dat الذي تم إنشاؤه داخل مجلد AppData ؟

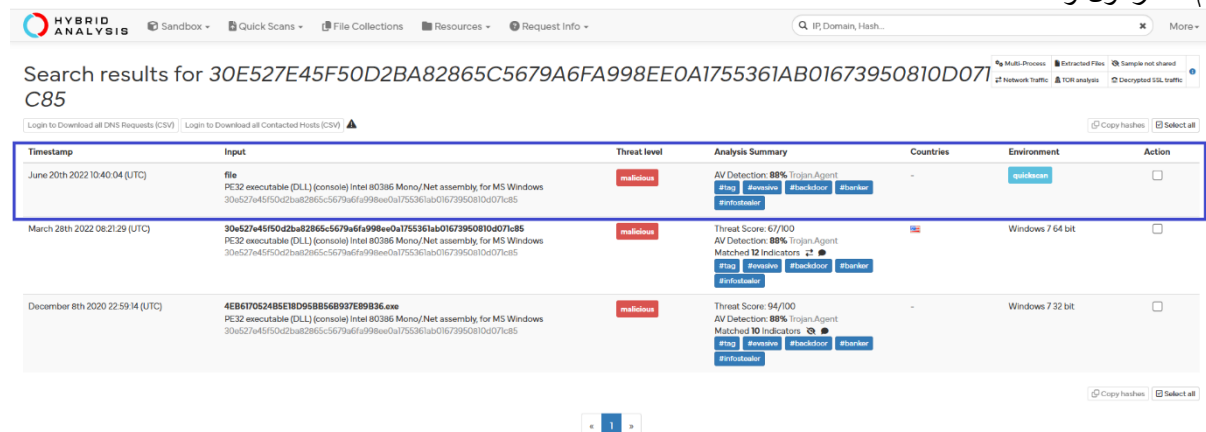
الإجابة : solarmaker.dat

هذا الملف يتم إسقاطه من قبل البرمجية كجزء من حفظ البيانات أو الإعدادات، وقد يحتوي على مفاتيح التهيئة أو بيانات مسروقة، وغالبًا يكون مشفرًا أو مضغوطًا لتجنب الكشف.

نذهب الى موقع hybrid-analysis من ثم نذهب الى خانة الـ Report Search ونضع الـ Hash في خانة البحث



ثم نختار اول واحد



Timestamp	Input	Threat level	Analysis Summary	Countries	Environment	Action
June 20th 2022 10:40:04 (UTC)	file PE32 executable (DLL) (console) Intel 80386 Mono/Net assembly for MS Windows 30e527e45f50d2ba82865c5679a6fa998ee0a1755361ab01673950810d071c85	malicious	AV Detection: 88% Trojan.Agent #tag #analysis #backdoor #torster	-	quiescent	<input type="checkbox"/>
March 28th 2022 08:21:29 (UTC)	30e527e45f50d2ba82865c5679a6fa998ee0a1755361ab01673950810d071c85 PE32 executable (DLL) (console) Intel 80386 Mono/Net assembly for MS Windows 30e527e45f50d2ba82865c5679a6fa998ee0a1755361ab01673950810d071c85	malicious	Threat Score: 67/100 AV Detection: 88% Trojan.Agent Matched 12 indicators +1 #tag #analysis #backdoor #torster	GB	Windows 7 64 bit	<input type="checkbox"/>
December 8th 2020 22:59:14 (UTC)	4EB6170624B5E18D9B856B937E89B36.exe PE32 executable (DLL) (console) Intel 80386 Mono/Net assembly for MS Windows 30e527e45f50d2ba82865c5679a6fa998ee0a1755361ab01673950810d071c85	malicious	Threat Score: 94/100 AV Detection: 88% Trojan.Agent Matched 30 indicators +3 #tag #analysis #backdoor #torster	-	Windows 7 32 bit	<input type="checkbox"/>

ثم نذهب الى خانه Falcon Sanbox reports ثم نختار الثاني

Falcon Sandbox Reports (2)

Characteristics Legend Show All As List Submit

Windows 7 32 bit

f76e293d627c55eca18ce96e587fb...
December 8th 2020 22:57:57 (UTC)

Malicious

Threat Score: 94/100
Labeled As: Trojan.Agent
Indicators: 3 2 5
Characteristics: 2

Windows 7 64 bit

111bc461-1ca8-43c6-97ed-911e0e6...
October 15th 2020 02:23:24 (UTC)

Malicious

Threat Score: 67/100
Labeled As: Trojan.Agent
Indicators: 1 3 4
Characteristics: 2

ثم نبحت عن ملف نهايته تكون [.dat] في خانه All Strings

Extracted Strings

Search

All Strings (656) Interesting (183) 30e527e45f50d2ba92865... regsvr32.exe (1) screen_1.png (2) screen_0.png (2)

<Run>b__137
??_e_0_?v_u
?_???_q0_...
?_...
?v_?_?_...
\\AppData\\Roaming\\solarmarker.dat
0...
0...?
_0_0_...l_...
??...0_...
?...?_...

نجد الملف الذي كنا نبحت عنه هنا [\\AppData\\Roaming\\solarmarker.dat]

Q6

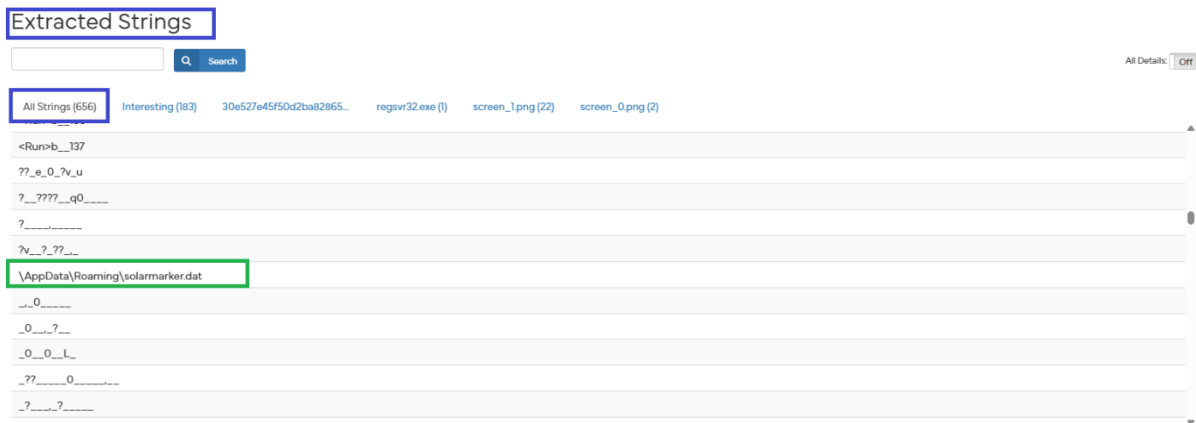
It is crucial to identify the C2 servers with which the malware communicates to block its communication and prevent further data exfiltration. What is the C2 server that the malware is communicating with?

ما هو عنوان سيرفر C2 ؟

الإجابة: <https://gogohid>

خادم التحكم والسيطرة (C2 server) هو المكان الذي تتصل به البرمجية الخبيثة للحصول على أوامر أو لرفع البيانات المسروقة. حظر هذا الدومين في الجدار الناري أمر ضروري لمنع استمرار الاتصال.

اكمل الخطوة السابقة ونبحث عن عنوان السيرفر



نجد الموقع الذي كنا بحث عنه [<https://gogohid.com>]

معلومات إضافية

ما هو RAT (Remote Access Trojan) ؟

RAT هو اختصار لـ **Remote Access Trojan**، ويُترجم إلى "حصان طروادة للتحكم عن بُعد". هو نوع من البرمجيات الخبيثة (**Malware**) يُصنّف ضمن **Trojan horses** لأنه يخدع الضحية بالظهور كبرنامج عادي أو شرعي، لكنه في الواقع يُمكن المُهاجم (**attacker**) من التحكم الكامل في جهاز الضحية عن بُعد.

كيف يعمل RAT تقنيًا؟

- المرحلة الأولى – الإصابة (**Infection**):
 - يتم خداع الضحية لتحميل برنامج أو فتح ملف يحتوي على RAT، غالبًا ممويه داخل ملف Word، PDF، أو برنامج كراك.
- المرحلة الثانية – التثبيت (**Persistence**):
 - نسخ نفسه داخل مجلدات النظام مثل %APPDATA% أو %TEMP%.
 - يُعدل إعدادات الريجستري ليعمل مع بدء تشغيل النظام.
- المرحلة الثالثة – الاتصال بالمُهاجم (**C2 Communication**):
 - يتصل بخادم تحكم وتحكم (**Command & Control**).
 - ينتظر أوامر المُهاجم أو يُرسل تقارير عن نشاط الجهاز.
- المرحلة الرابعة – تنفيذ الأوامر:
 - يبدأ بتنفيذ الأوامر القادمة من المُهاجم مثل فتح كاميرا، تحميل ملفات، تشغيل **Keylogger**، إلخ.

ما أضرار RAT ؟

- انتهاك صارخ للخصوصية: يمكنه مراقبتك صوتًا وصورة بدون علمك.
- سرقة الملفات الشخصية والبيانات الحساسة: مثل الصور، المشاريع، الوثائق المالية.
- خسائر مالية مباشرة: سرقة حسابات بنكية أو معلومات بطاقات ائتمان.
- ابتزاز إلكتروني: تسجيلات كاميرا أو ميكروفون قد تُستخدم لتهديد الضحية.
- تحميل برمجيات خبيثة إضافية: يمكنه تنزيل **Ransomware** أو برامج تجسس أخرى.
- بطء الجهاز واستهلاك موارده: نتيجة العمليات في الخلفية.
- استخدام جهازك في جرائم إلكترونية: مثل هجمات **DDoS** أو سرقة بيانات من جهات أخرى.

أمثلة شهيرة على RATs معروفة

- **njRAT**: شائع جدًا في الدول العربية، واجهة رسومية، برمجة VB.NET.
- **DarkComet**: سهل الاستخدام وواجهة رسومية، لكنه قديم نوعًا ما.
- **QuasarRAT**: مفتوح المصدر، مكتوب بـ **C#**، يُستخدم في اختبارات الاختراق أحيانًا.
- **NanoCore**: قوي جدًا، يحتوي على إضافات كثيرة، منتشر بين مجرمي الإنترنت.
- **Remcos**: تجاري ومدفوع، يُستخدم بكثرة في حملات تجسس صناعي وتجاري.
- **PlugX**: معقد جدًا، يُستخدم من قبل مجموعات **APTs** وله تقنيات إخفاء متقدمة.

كيف أحمي نفسي من RAT ؟

- لا تفتح ملفات من مصادر غير موثوقة حتى لو كانت بصيغة PDF أو DOC.
- استخدم برنامج مكافحة فيروسات مُحدث دائماً، وخصوصاً الذي يدعم تحليل السلوك (Heuristic/Behavior-based).
- راقب تشغيل البرامج عند الإقلاع (Startup Items) وملفات الـ رجستري.
- استخدم جدار ناري (Firewall) لمنع الاتصال العشوائي بالسيرفرات البعيدة.
- افحص استهلاك الشبكة ببرامج مثل Wireshark أو GlassWire.
- قم بتحديث نظام التشغيل وبرامجك باستمرار لسد الثغرات الأمنية.
- افصل الإنترنت عند الشك بأي نشاط مشبوه لتقليل الضرر.
- افحص العمليات الجارية على الجهاز باستخدام أدوات مثل Process Explorer أو Autoruns من Sysinternals.

ملفات .dat

ملفات [.dat] هي ملفات بيانات عامة تُستخدم لتخزين معلومات محددة تتعلق بالبرنامج الذي أنشأها، وغالبًا ما تحتوي على بيانات نصية عادية أو بيانات ثنائية (Binary) مثل إعدادات البرامج، بيانات الألعاب، أو حتى ملفات فيديو.

خصائص ملفات .dat:

- ملفات بيانات عامة: لا تلتزم ببنية محددة أو نوع محتوى معين، بل يعتمد ذلك على البرنامج الذي أنشأها.
- تُستخدم داخليًا: غالبًا ما تُستخدم هذه الملفات من قبل البرامج نفسها ولا يُفترض أن يفتحها المستخدم يدويًا.
- أنواع المحتوى: قد تحتوي على نص عادي، إعدادات تكوين، بيانات الألعاب، مرفقات بريد إلكتروني، أو ملفات فيديو.
- مرتبطة ببرامج محددة: مثل ألعاب Minecraft التي تستخدم ملفات .dat لتخزين بيانات المستويات، أو برامج مثل CCleaner و Microsoft Exchange Server.

هل تعتبر خبيثة؟

- ملفات .dat نفسها ليست خبيثة بطبيعتها.
- لكنها قد تُستخدم كوسيلة لإخفاء ملفات ضارة أو تعليمات خبيثة، خاصة في هجمات التصيد الاحتيالي.
- يجب الحذر عند استقبال ملفات .dat من مصادر غير موثوقة، وعدم فتحها أو تشغيل محتوياتها دون التأكد.
- استخدام برامج مكافحة الفيروسات وأنظمة الحماية المتقدمة يساعد في كشف مثل هذه الهجمات.
- بالتالي، ملفات .dat ليست ضارة بحد ذاتها، لكنها قد تكون جزءًا من هجوم خبيث إذا استُخدمت بطريقة مخادعة.

ال C2 Server

C2 Server (اختصار لـ **Command and Control Server**) هو خادم تحكم وسيطرة يُستخدم من قِبل المهاجمين الإلكترونيين لإدارة الأجهزة المصابة بالبرمجيات الخبيثة عن بُعد. بعد إصابة جهاز الضحية ببرمجية خبيثة مثل **RAT**، يتصل الجهاز المصاب بخادم **C2** ليبدأ في تلقي الأوامر وتنفيذها أو إرسال بيانات مسروقة للمهاجم.

الوظائف الأساسية لخادم C2:

- إرسال الأوامر للأجهزة المصابة (مثل سرقة البيانات، حذف الملفات، تثبيت برمجيات إضافية).
- استقبال البيانات المسروقة من الأجهزة المصابة.
- إدارة شبكة من الأجهزة المصابة (**botnet**) لتنفيذ هجمات واسعة مثل هجمات حجب الخدمة (**DDoS**).
- إخفاء الاتصالات ومحاولة التمويه لتجنب اكتشافه من قبل أنظمة الحماية.

كيف يعمل خادم C2؟

- إصابة الجهاز: يُصاب الجهاز ببرمجية خبيثة عبر البريد الإلكتروني، روابط ضارة، أو ثغرات.
- الاتصال بخادم C2: البرمجية الخبيثة تنشئ اتصالاً بخادم C2 عبر الإنترنت.
- تنفيذ الأوامر: يتلقى الجهاز المصاب أوامر من الخادم، مثل سرقة كلمات المرور أو تعطيل النظام.
- إرسال النتائج: يرسل الجهاز المصاب البيانات أو نتائج الأوامر إلى الخادم.

خوادم C2 تُعد من العناصر الأساسية في الهجمات السيبرانية الحديثة، وتُمكن المهاجمين من التحكم الكامل بالشبكات المصابة وتنفيذ أهدافهم بسرية وفعالية.