

العطاء الرقمي
Attaa Digital



التعدين الخبيث

ومخاطرة السيرانية

م . صالح الناهي الشكري
مستشار البنية المؤسسية والامن السيران

2021 /Apr/27



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



فايروس لا يضرك ... بل يسرقك وانت لا تعلم



م . صالح الناهي الشكري

مستشار

الامن السيبراني والبنية المؤسسية التقنية
مدرب معتمد في تقنية المعلومات

الخبرات المهنية والعملية والعلمية

- ماجستير علوم حاسب (**Computer Science**) مرتبة الشرف الاولى
- بكالوريوس هندسة حاسب (**Computer Engineer**)
- حاصل على درجة "**مستشار**" من هيئة المهندسين السعوديين
- متخصص في امن الشبكات والامن السيرانى
- خبرة 20 سنة في تقنية المعلومات
- حاصل على العديد من الشهادات المهنية في مجال الشبكات
- وامن المعلومات والبنية المؤسسية التقنية
- CCNA ,CCNP , CISSP, PMP, security + ,ITILv3 , F5 consultant, TOGAF 9.2
- مدرب معتمد من المؤسسة العامة للتدريب المهني والتقني
- في مجال تقنية المعلومات
- حاصل على شهادة TTT للتدريب واعداد المدربين
- دورة امن المعلومات في هيئة المهندسين السعوديين
- العديد من الدورات ومحاضرات توعوية
- مهتم بالاعمال التطوعية والمجتمعية في مجال التقنية

اجندة المحاضرة



الوقاية من التعدين



اعراض التعدين الخبيث



اهم الطرق للتعدين



مقدمة عن التعدين الخبيث



أسئلة الحضور



هجمات التعدين الخبيث

مقدمة عن التعددين الخبيث



العملة الرقمية Digital currency



على شكل رقمي ، وليس لها وجود مادي (مثل الأوراق النقدية والنقود المعدنية)
ولها خصائص مماثلة للعملات المادية، ولكنها تسمح بالمعاملات الفورية ونقل الملكية بلا
حدود
وتشمل الأمثلة العملات الافتراضية والعملات المعماة أو حتى "النقد الإلزامي الرقمي" الصادر
من البنك المركزي
تستخدم لشراء السلع والخدمات ، ولكن يمكن أيضا أن تقتصر على مجتمعات معينة مثل
للاستخدام داخل لعبة على الإنترنت أو شبكة اجتماعية



البنك الدولي

2012 : العملة الافتراضية بأنها نوع من الأموال الرقمية غير الخاضعة للتنظيم

2015 : العملة الافتراضية هي التمثيل الرقمي للقيمة

العملة الرقمية مقابل العملة الافتراضية

فإن العملة الرقمية هي أصول ممثلة في شكل رقمي ولها بعض الخصائص النقدية. يمكن أن

تكون العملة الرقمية مقومة بعملة ذات سيادة وتصدر من قبل الجهة المصدرة المسؤولة عن

استرداد الأموال الرقمية نقدا. وفي هذه الحالة، تمثل العملة الرقمية النقود الإلكترونية. وستعتبر

العملة الرقمية المقومة بوحداتها ذات القيمة أو بإصدار لامركزي أو تلقائي عملة افتراضية.





العملة الافتراضية :

"نوع من الأموال الرقمية غير المنظمة، والتي تصدر وعادة ما يسيطر عليها المطورين، يتم استخدامها وقبولها بين أعضاء مجتمع افتراضي معين".

"وسيلة للتبادل تعمل كعملة في بعض البيئات، ولكنها لا تملك جميع خصائص العملة الحقيقية

أنواع العملات الرقمية





العملة المشفرة :

تعتمد على التشفير لتسلسل مع التوقيعات الرقمية للتحويلات رمزية ، الند للند الشبكات واللامركزية . في بعض الحالات يتم استخدام مخطط إثبات العمل لإنشاء وإدارة العملة

أنواع العملات الرقمية





2009 ساتوشي ناكاموتو قام باختراع اول عملة رقمية البتكوين

تنقل بسهولة ، وموثوقيه ، وافتراضية

10 بتكوين = قيمة معقدة ومشفرة تسمى هاش تتألف من 64 خانة مشفرة بتقنية SHA 256

تحتاج موارد كبيرة - للحماية والتشفير وزيادة الامان

الهاش ينتقل لك من خلال نظام البلوك تشين

البلوك تشين = دفتر حسابات لتسجيل عناوين المالك السابقين والحاليين

مثال
البتكوين وتقنية البلوك تشين





خلال 9 سنوات 2000 عملة مثل الايثيريوم ، بتكوين ، الريفل .. الخ

ليش البتكوين ؟

اول عملة رقمية ، اخرجت اثرياء بسبب ارتفاعه الرهيب ، ارتفعت اكثر من
4000 بالمائة في احد السنوات

مثال
البتكوين وتقنية البلوك تشين





الاعتقاد ان الفلوس ممكن تطبع اذا خلصت
البتكوين : 21 مليون

مستقبل البتكوين والتعدين

- عمال التعدين ماطلعوا الا 4.5 مليون حتى بداية 2018

باقي 16 مليون

128 سنة الوقت المقدر لانتهاء البتكوين وصارت بعض الشركات تأجر بعض

الموارد حاسوبية خارقة وبعض المواقع تزرع اكواد تستخدم معالجك





تحقيق \$3,925,863

لكن القيام بعمليات التنقيب

احتاجت إلى 11,388,578 جيجا هاش / الثانية

وهذا يحتاج الى كمية كهرباء ضخمة جدا ومكلفة

مستقبل البتكوين والتعدين





التعدين الخبيث Cryptojacking

تعدين العملة الرقمية المشفرة غير المصرح به ، أو عن الانجليزية الكريبتوجاكنغ، هي عملية
خطف جهاز الضحية بدون علمه/علمها واستغلال قدرات الجهاز الحسابية لتعدين العملات
الرقمية المشفرة Cryptocurrencies





لا تضر برمجيات التعدين غير المصرح به ببيانات الضحية ومعلوماته أو نظام تشغيله أو اتصاله بالإنترنت بل تسرق قدرات المعالجة من وحدة المعالجة المركزية CPU أو من وحدة تسريع الرسومات GPU .

انخفاض أداء الجهاز ما قد إزعاجا لمستخدمي الأجهزة المصابة مع الوقت ارتفاعا في فاتورة الكهرباء، الضروري لتغذية المعالج المنهمك في إجراء العمليات الحسابية الضرورية للتعدين

التعدين الخبيث Cryptojacking





الربح المادي الهدف الرئيسي وراء هذا الهجوم
يتم تحويلها لعملة نقدية (تقليدية) أو كاستخدام العملة الرقمية لشراء الأصول والسلع
والخدمات.

اختيار عملات رقمية مشفرة لا يحتاج تعدينها بكفاءة إلا لوحدة المعالجة المركزية CPU مثل
عملة Monero والتي تعتبر خيار المهاجمين الأول عام 2018.

التعدين الخبيث Cryptojacking





التعدين الخبيث



• 2018 : زيادة في أعداد الهجمات بأكثر من 83%

• إذ تعرّض أكثر من خمسة ملايين مستخدم، لهجمات عبر الإنترنت منذ بداية العام حتى نهاية الربع الثالث، مقارنةً بنحو 2.7 مليون مستخدم خلال الفترة نفسها من العام 2017.

• السبب في الزيادة تركيب البرمجيات والمحتوى غير المرخص واستخدامها في هذا المجال

طرق للتعيين



خداع الضحايا لتحميل برنامج تعدين خبيث Cryptojacking Malware خاص بالمهاجم على حواسيبهم

يستغل المهاجم في ذلك أساليب الهندسة الاجتماعية Social Engineering كأن يتلقى الضحايا بريداً إلكترونياً يبدو حميداً، لكنه يحتوي على رابط خبيث يقوم بتحميل برنامج التعدين على الحاسوب وتشغيله بشكل خفي بحيث يقوم بالتعدين خلال الاستخدام العادي للحاسب المصاب

برامج تعدين خبيث Cryptojacking Malware





ضع سطور البرمجة الخاصة بالتعدين الخبيث على مواقع على الإنترنت بعد إختراقها أو عبر استغلال خدمات الدعاية المتاحة عليها

في هذه الحالة تبدأ عملية التعدين لصالح المهاجم عند زيارة أي مستخدم للموقع المصاب. حيث يتم التعدين ضمن بيئة المتصفح على جهاز الزائر.

إصابة المواقع ببرامج التعدين الخبيثة Malicious Cryptomining Websites



اعراض التعددين الخبيث



اعراض التعدين الخبيث Cryptojacking Symptoms



1. انخفاض أداء وحدة المعالجة المركزية CPU
2. ارتفاع درجة حرارة الجهاز، وذلك يعود إلى أن عملية التعدين تعتمد على إجراء عمليات حسابية بشكل متواصل
3. مراوح الجهاز تعمل بتواتر ولفترات أكبر من المعتاد لكي تحافظ على استقرار درجة حرارة الجهاز

بطء الجهاز أو ارتفاع درجة حرارته ،

إبدا بإجراء خطوات تشخيص التعدين الخبيث Cryptojacking Diagnosis لتحديد ما إذا كان

السبب وراء هذه الأعراض هو فعلا التعدين الخبيث

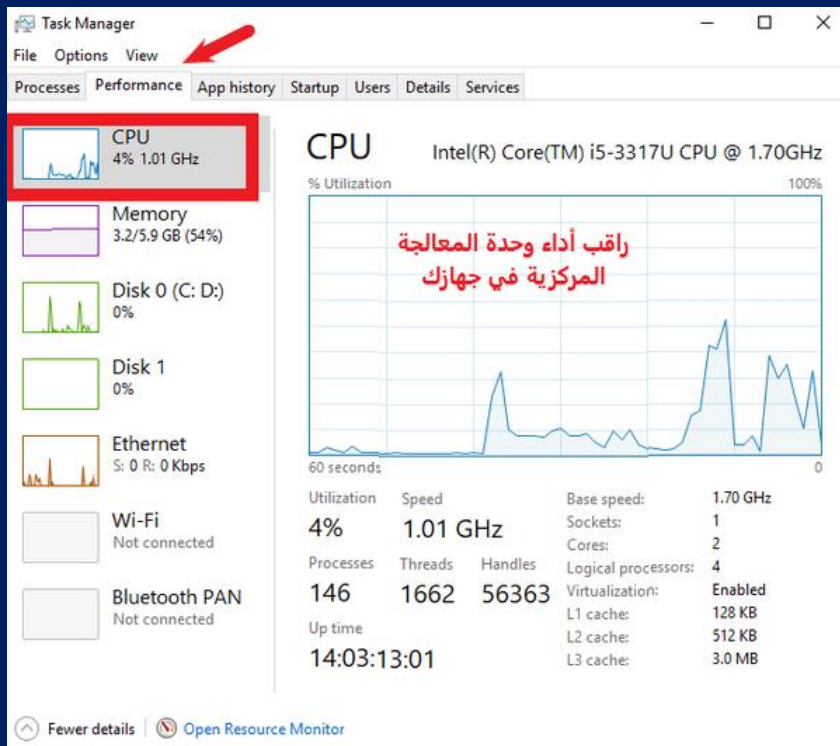
تشخيص التعددين الخبيث



1. قوموا بفتح مدير المهام عن طريق ضغط كل من CTRL و SHIFT و ESC بنفس الوقت
2. اذهبوا الى تبوية الأداء لمراقبة الحمل الواقع على وحدة المعالجة المركزية

تشخيص التعدين الخبيث Cryptojacking Diagnosis





تشخيص التعدين الخبيث Cryptojacking Diagnosis





3. في حال كان بطء الجهاز متربطا مع عمل المتصفح فقد يعني ذلك أن التعدين يحصل عبر المتصفح إما عبر إضافة Addon خبيثة أو عبر زيارة موقع مصاب يقوم بحقن أسطر برمجة التعدين ضمن متصفحكم.

تشخيص التعدين الخبيث Cryptojacking Diagnosis





للتحقق من ذلك على متصفح كروم Chrome أو كروميوم Chromium قوموا بفتح مدير المهام لمتصفح كروم بضغط كلاً من SHIFT وESC

أو من قائمة الإعدادات، قوموا باختيار أدوات أخرى، ثم قوموا باختيار: مدير المهام لتظهر النافذة التالية:

تشخيص التعدين الخبيث Cryptojacking Diagnosis





Task Manager - Google Chrome

Task	Memory footprint	CPU	Network	Process ID
Browser	203,248K	7.8	0	10836
Extension: Adblock	221,820K	1.6	0	12556
Extension: Adblock Plus	204,136K	0.0	0	11720
Extension: AODocs - Smartbar for G Suite	39,008K	0.0	0	9924
Extension: HTTPS Everywhere	136,468K	0.0	0	3824
Extension: LastPass: Free Password Manager	50,316K	0.0	0	11144
Extension: Privacy Badger	48,860K	1.6	0	5716
GPU Process	195,380K	3.1	0	12580
Tab: SalamaTech Wiki ويكي سلامتك	54,704K	0.0	0	6032
	112,260K	0.0	874 B/s	6900

الإضافات

التبويبات المفتوحة

End process

تشخيص التعدين الخبيث Cryptojacking Diagnosis



الوقاية من التعدين الخبيث



الوقاية من التعدين

1. الحذر و الوعي فيما يتعلق بهجمات التّصيد كون هذا النوع من الهجمات وسيلة من الوسائل التي تسمح للقراصنة بالوصول الى جهاز الضحية وزراعة برمجيات التعدين الخبيثة عليه
2. تثبيت إضافات منع الإعلانات على متصفحات الويب طريقة فعّالة لمنع برمجيات التعدين الخبيثة.
3. مراقبة الشبكة للمنظمات والمؤسسات
4. اّطلاع على مستجّدات التعدين الخفيّ





5. عدم تجاهل الأهداف الأقل شأنًا أو وضوحًا، مثل أنظمة إدارة الانتظار، ومحطات نقاط البيع، وحتى أجهزة البيع الآلية، فهذه الأجهزة وما يشابهها يمكن استغلالها في عمليات التعدين الخبيث للعمليات الرقمية، مثلما حدث في هجوم الاستغلال الشهير. EternalBlue

الوقاية من التعدين





6. حماية بيانات العمل في الشركات، ينبغي توعية الموظفين و فرق تقنية المعلومات، والحفاظ على البيانات الحساسة منفصلة، والحرص على تقييد الوصول الموظفين إلى البيانات.

7. استخدام ميزة التحكم في التطبيقات لتتبع الأنشطة المشبوهة التي قد تجري في التطبيقات المشروعة. ويجب أن تكون الأجهزة المتخصصة معدة في نمط Default Deny ويمكن استخدام حل أمني متخصص مثل Kaspersky

Endpoint Security for Business الذي يتضمن هذه المزايا

الوقاية من التعدين





الوقاية من التعدين

8. الحرص على التحديث المستمر للبرمجيات على جميع الأجهزة، لمنع المهاجمين من استغلال الثغرات الأمنية، مع استخدام أدوات يمكنها تلقائيًا اكتشاف الثغرات وتنزيل الإصلاحات البرمجية وتثبيتها.
9. استخدام حل موثوق به لضمان أمن الأجهزة الشخصية مع ضرورة إبقاء المزايا الرئيسية، مثل System Watcher، في وضع التشغيل.



اشهر هجمات التعدين الخبيث



WinstarNssmMiner

عن طريق تشغيل عملية `svchost.exe` أولاً ودس الكود فيها، وضبط صفة العملية الجديدة الناشئة على أنها عملية حرجة أي أساسية لنظام التشغيل. Critical Process. وبالتالي فإن نظام التشغيل يتعطل بمجرد حذفها، ما يدفع المستخدمين إلى الإبقاء عليها، ما يعني مزيداً من التعدين الخبيث.

سياسة الأرض المحروقة





: 2018

هجوم استهدف بشكل رئيسي راوترات مايكروتيك في البرازيل حيث تم استهداف حوالي
170000 جهاز خلال الهجوم

اختراق كبيرة استهدفت
راوترات مايكروتيك MikroTik





Kodi فهو برنامج مجاني ومفتوح المصدر، ويمكن استخدامه لتشغيل مقاطع الفيديو والموسيقى والبودكاست وملفات الوسائط الرقمية الأخرى من وسائط التخزين المحلية وعلى الشبكة ومصادر ال Streaming. يمكن للمستخدمين أيضًا توسيع وظائف البرنامج عن طريق تثبيت بعض الإضافات الموجودة في كل من مستودع Kodi الرسمي وفي مستودعات الطرف الثالث المختلفة. وقام القراصنة بحقن إضافة برمجية تعدين خبيث، وبسبب ميزة التحديث التلقائي للإضافات التي يوفرها كودي، إصيب عدد كبير من أجهزة المستخدمين بالبرمجية الخبيثة التي دفعت أجهزة الضحايا تحت إمرة القراصنة إلى التعدين الخبيث.

منصة كودي Kodi لتشغيل الوسائط





2018 : موقع صحيفة الأهرام المصرية يقوم بالتنقيب عن عملة مونيرو Monero
الرقمية على أجهزة القراء
التعدين الخبيث على أجهزة قراء الموقع كان قد استمر لعدة أيام على الأقل قبل اكتشاف
الحادثة

**موقع صحيفة الأهرام يقوم
بالتعدين على أجهزة القراء**





2018 : موقع صحيفة الأهرام المصرية يقوم بالتنقيب عن عملة مونيرو Monero
الرقمية على أجهزة القراء
التعدين الخبيث على أجهزة قراء الموقع كان قد استمر لعدة أيام على الأقل قبل اكتشاف
الحادثة

**موقع صحيفة الأهرام يقوم
بالتعدين على أجهزة القراء**





شكراً لكم أسئلة واستفسارات

للتواصل للتدريب والاستشارات والاستفسارات



salnahi@gmail.com



0555161888



@salnahi



[linkedin.com/in/salnahi](https://www.linkedin.com/in/salnahi)