Prepared by:

Hamza Al-Dorafi

Nezar Al-Hamady

Abdulrahman Al-Halaqi

Amr Al-Awadhi

Documentation For

No Trust

Digital Forensics Case

February 01, 2025

المحتويات

[2. المقدمة 3](#_Toc189219001)

[3. أهداف المشروع 3](#_Toc189219002)

[4. نطاق المشروع وحدوده 5](#_Toc189219003)

[نطاق المشروع 5](#_Toc189219004)

[حدود المشروع: 5](#_Toc189219005)

[5. آلية الهجوم باستخدام الفيروس المرسل عبر البريد الإلكتروني 5](#_Toc189219006)

[إرسال بريد إلكتروني احتيالي (Phishing) 5](#_Toc189219007)

[الهدف: 5](#_Toc189219008)

[التنفيذ: 5](#_Toc189219009)

[إخفاء الملف الضار: 6](#_Toc189219010)

[تنفيذ الفيروس في الخلفية 6](#_Toc189219011)

[الهدف: 6](#_Toc189219012)

[التنفيذ: 6](#_Toc189219013)

[جمع البيانات المهمة 7](#_Toc189219014)

[الهدف: 7](#_Toc189219015)

[التنفيذ: 7](#_Toc189219016)

[إرسال البيانات إلى الخادم 7](#_Toc189219017)

[الهدف: 7](#_Toc189219018)

[التنفيذ: 7](#_Toc189219019)

[التحسينات: 7](#_Toc189219020)

[6. التحضير لعملية التحقيق الجنائي الرقمي 8](#_Toc189219021)

[الإجراءات الأولية: 8](#_Toc189219022)

[7. جمع الأدلة الرقمية وتحليلها 8](#_Toc189219023)

[8. تحليل صورة الذاكرة العشوائية (RAM) للجهاز المخترق 8](#_Toc189219024)

[9. استخراج البيانات المسروقة وتحليل الفيروس المستخدم 9](#_Toc189219025)

[10. تحديد اتصال المهاجم بالجهاز المخترق 9](#_Toc189219026)

[11. تحديد هوية المهاجم ومصدر الهجوم 10](#_Toc189219027)

[12. الأدوات المستخدمة في التحري 10](#_Toc189219028)

[13. إيقاف الفيروس ومنع سرقة البيانات مستقبلاً 10](#_Toc189219029)

[14. التحديات والصعوبات التي واجهت التحقيق 11](#_Toc189219030)

[15. الجانب القانوني والأخلاقي في التحقيق الرقمي 11](#_Toc189219031)

[16. التوصيات لتعزيز أمن الأنظمة ومنع الاختراقات المستقبلية 11](#_Toc189219032)

[17. النتائج النهائية والخاتمة 12](#_Toc189219033)

# المقدمة

أصبحت الهجمات السيبرانية أكثر تطورًا، حيث يعتمد المهاجمون على تقنيات متقدمة لاختراق الأجهزة وسرقة البيانات الحساسة. يتناول هذا المشروع تحليل هجوم تم من خلال بريد إلكتروني يحتوي على مرفق ضار، حيث قام الفيروس بجمع الملفات والصور والمعلومات المهمة من جهاز الضحية وإرسالها إلى جهاز آخر. من خلال التحليل الجنائي الرقمي، نسعى إلى استخراج الأدلة الرقمية، كشف هوية المهاجم، وفهم طبيعة الهجوم لمنع تكراره في المستقبل.

# أهداف المشروع

1. تحليل فيروس خبيث أُرسل كمرفق في بريد إلكتروني.
2. جمع الأدلة الرقمية من جهاز الضحية لتحديد البيانات التي تم سرقتها.
3. ****تحليل** DNS و IP**: يمكن استخدام MXToolbox للتحقق من سجلات DNS الخاصة بالمرسل، والتأكد مما إذا كان هناك أي نشاط مريب مرتبط بعناوين IP مشبوهة. هذا يمكن أن يساعد في تتبع البريد الإلكتروني الذي يحتوي على المرفق الضار.
4. ****تحليل الشبكة****: استخدام Wireshark لمراقبة حركة مرور الشبكة أثناء الهجوم. يمكن فحص الحزم لرصد أي اتصالات مشبوهة بين جهاز الضحية والخوادم المشبوهة. قد يساعد ذلك في تحديد اسم الفيروس وأي بيانات يتم إرسالها.
5. تحليل صورة الذاكرة العشوائية (RAM) لتحديد العمليات النشطة أثناء الهجوم.
6. مراقبة العمليات: يمكن استخدام Process Hacker للكشف عن العمليات المشبوهة النشطة على النظام. هذه العمليات قد تشمل تلك المرتبطة بالفيروسات أو البرامج الخبيثة التي تم تنفيذها أثناء الهجوم.
7. جمع الأدلة الرقمية: Redline يساعد في جمع الأدلة الرقمية من جهاز الضحية، ويقدم تفاصيل حول العمليات، والملفات المفتوحة، وذاكرة النظام. يمكن استخدامها لتحديد الفيروسات أو البرمجيات الخبيثة التي تم تثبيتها.
8. تحديد اسم الفيروس والاتصالات التي قام بها مع جهاز المهاجم.
9. الكشف عن هوية المهاجم والمسار الذي استخدمه لسرقة البيانات.
10. فحص الملفات: يمكن رفع المرفقات المشبوهة على VirusTotal لفحصها عبر العديد من محركات الفيروسات المختلفة للكشف عن البرمجيات الخبيثة. يساعد هذا في تحديد نوع الفيروس وطرق انتشاره.
11. إيقاف الفيروس ومنع حدوث هجمات مماثلة في المستقبل.
12. تقديم تقرير كامل عن الحادثة

# نطاق المشروع وحدوده

## نطاق المشروع

1. يشمل المشروع تحليل جهاز كمبيوتر يعمل بنظام التشغيل Windows تم اختراقه عبر فيروس وصل كمرفق في بريد إلكتروني.
2. التركيز على تحليل ملفات النظام، الذاكرة العشوائية (RAM)، والاتصالات الشبكية الخاصة بالفيروس.
3. محاولة استرجاع البيانات المسروقة.

## حدود المشروع:

1. لا يشمل المشروع تحليل الهجوم على مستوى الشبكة بالكامل.
2. لا يتناول التحقيق في حملات التصيد الاحتيالي بشكل موسع، وإنما يركز فقط على الهجوم محل الدراسة.

# آلية الهجوم باستخدام الفيروس المرسل عبر البريد الإلكتروني

## إرسال بريد إلكتروني احتيالي (Phishing)

### الهدف:

محاكاة هجوم تصيد احتيالي لاختبار استجابة الضحية في بيئة آمنة.

### التنفيذ:

1. إنشاء بريد إلكتروني وهمي:
   * الأداة: انشاء حساب gmail مشابهة للموقع الرسمي
   * نموذج الرسالة:
2. السيد/ ....
3. .أتمنى أن تكون في تمام الصحة والعافية
4. يسرني أن أبلغكم بأنه تم إرسال نسخة من تطبيق تفعيل Microsoft Office بنجاح إلى جهازكم. للاستفادة من هذا التفعيل، يمكنك الضغط على الرابط ادناه والاستمتاع بتجربة مجانية واستثنائية

### إخفاء الملف الضار:

* 1. الطريقة:
     1. إنشاء ملف EXE وهمي باستخدام  PyInstaller.
     2. إخفاء الكود داخل الملف.

## تنفيذ الفيروس في الخلفية

### الهدف:

فهم كيفية عمل البرامج الضارة في الخلفية دون أن يلاحظها المستخدم.

### التنفيذ:

1. تجنب الاكتشاف:
   1. إخفاء العملية: استخدم مكتبات مثل PyWin32  لإخفاء النافذة في أنظمة Windows:

## جمع البيانات المهمة

### الهدف:

سرقة البيانات لتحليل كيفية حدوثها.

### التنفيذ:

1. تحديد الملفات المستهدفة:
   1. أي بيانات قد يكون لها أهمية مثل كلمات سر او مستندات وغيره.
2. تشفير البيانات المسروقة:  
   استخدم خوارزمية AES-256 قبل الإرسال

## إرسال البيانات إلى الخادم

### الهدف:

نقل البيانات المسروقة عبر الشبكة.

### التنفيذ:

1. استخدام بروتوكول HTTP:
2. التخفي عبر HTTPS:
   1. استخدم شهادة SSL مع أداة مثل Let's Encrypt  لتشفير الاتصال.

### التحسينات:

1. التنكر كحركة مرور شرعية:  
   أرسل البيانات عبر منافذ شائعة مثل 443 لـ HTTPS مع تمويه الحزم كطلبات ويب عادية.

# التحضير لعملية التحقيق الجنائي الرقمي

## الإجراءات الأولية:

1. إنشاء صورة رقمية (Forensic Image) للذاكرة RAM باستخدام FTK Image للحفاظ على الأدلة.
2. استخراج صورة الذاكرة العشوائية (RAM) باستخدام Volatility لتحليل العمليات النشطة وقت الهجوم.
3. تحليل حركة الشبكة والبيانات المرسلة
4. مراقبة السجلات والأنشطة المشبوهة
5. عزل الجهاز المخترق عن الإنترنت والشبكة المحلية لمنع المزيد من سرقة البيانات.

# جمع الأدلة الرقمية وتحليلها

الأدلة التي سيتم جمعها تشمل:

1. المرفق الضار الذي استُخدم لنشر الفيروس.
2. سجلات النظام (Event Logs) لتحديد وقت تشغيل الفيروس.
3. سجلات الاتصال (Firewall & Network Logs) للكشف عن أي اتصال بجهاز المهاجم.

# تحليل صورة الذاكرة العشوائية (RAM) للجهاز المخترق

باستخدام Volatility Framework، سنقوم بتحليل الذاكرة لاستخراج:

1. البرامج الضارة التي تعمل حاليًا.
2. مفاتيح تسجيل الدخول (Credentials) التي قد تكون مخزنة في الذاكرة.
3. الاتصالات المفتوحة بالجهاز المهاجم (TCP/UDP Connections).

# استخراج البيانات المسروقة وتحليل الفيروس المستخدم

1. استخراج الملفات المؤقتة التي أنشأها الفيروس أثناء سرقة البيانات.
2. مقارنة الفيروس بقاعدة بيانات البرمجيات الضارة لتحديد مصدره ونوعه.

# تحديد اتصال المهاجم بالجهاز المخترق

باستخدام أدوات تحليل الشبكات مثل Wireshark و IP Location

وغيرها، سنقوم بـ:

1. تحديد عناوين الـ IP التي تم الاتصال بها.
2. تحليل البيانات المرسلة لمعرفة نوع الملفات التي تم تهريبها.
3. البحث عن أنماط مشبوهة في حركة المرور الشبكية.

# تحديد هوية المهاجم ومصدر الهجوم

1. تحليل الـ IP المرتبط بالاتصال للكشف عن الموقع الجغرافي للمهاجم.
2. البحث في السجلات الرقمية لمعرفة ما إذا كان هناك أي معلومات مسربة تشير إلى المهاجم.
3. تحليل البريد الإلكتروني المستخدم في الهجوم باستخدام أدوات مثل email headers analysis.

# الأدوات المستخدمة في التحري

## Mxtoolbox

## Wireshark

## ip location

## Process Hacker

## virustotal

## Redline

## LogParser

## volatility

## Procmon

## Recuva

# إيقاف الفيروس ومنع سرقة البيانات مستقبلاً

1. عزل وإزالة الفيروس باستخدام برامج مكافحة الفيروسات المتقدمة.
2. إغلاق المنافذ الشبكية المفتوحة التي استغلها الفيروس.
3. إعادة ضبط بيانات تسجيل الدخول وكلمات المرور.
4. تحديث النظام وإغلاق أي ثغرات أمنية استغلها الهجوم.

# التحديات والصعوبات التي واجهت التحقيق

1. إخفاء الفيروس نفسه داخل العمليات الشرعية للنظام.
2. استخدام التشفير لحماية البيانات المسروقة أثناء نقلها.
3. حذف السجلات بعد الاختراق لإخفاء أثر الهجوم.

# الجانب القانوني والأخلاقي في التحقيق الرقمي

1. ضرورة الحصول على إذن قانوني قبل تحليل الجهاز.
2. مراعاة سرية البيانات وعدم استخدامها خارج نطاق التحقيق.
3. الامتثال للقوانين المتعلقة بالجرائم الإلكترونية وحماية البيانات الشخصية.

# التوصيات لتعزيز أمن الأنظمة ومنع الاختراقات المستقبلية

1. استخدام برامج كشف التهديدات المتقدمة (EDR & SIEM).
2. تدريب الموظفين على كيفية التعرف على رسائل التصيد الاحتيالي.
3. إجراء عمليات نسخ احتياطي دورية للبيانات المهمة.
4. تفعيل المصادقة الثنائية (2FA) على جميع الحسابات الحساسة.

# النتائج النهائية والخاتمة

يؤكد التحقيق أن الهجوم تم من خلال تصيد احتيالي باستخدام بريد إلكتروني يحتوي على مرفق ضار، حيث تمكن الفيروس من جمع البيانات وإرسالها إلى جهاز المهاجم. بعد التحليل، تم تحديد هوية المهاجم وإيقاف الهجوم بنجاح.