الجمهورية العربية السورية
وزارة الاتصالات والتقانة
الهيئة الوطنية لخدمات الشبكة

National Agency for Network Services
Information Security Center

دراسة حول البرمجية الخبيثة EMOTET

ملخص

برمجيات خبيثة من نوع أحصنة طروادة من طراز متقدم مخصصة لمهاجمة البنوك والمؤسسات المالية، وتعتبر البرمجيات الخبيثة من هذا النوع شديدة الخطورة بسبب ميزاتها الشبيهة بالديدان البرمجية من ناحية سرعة الانتشار وصعوبة معالجة الإصابة بعد وقوعها، كذلك تتمتع بالقدرة على التحول وتغيير طبيعتها لتجنب الاكتشاف القائم على تحديد الشيفرة الخبيثة الخاصة بها (البصمة) المعرفة لدى البرامج المضادة للبرمجيات الخبيثة، تستهدف نظم التشغيل windows بشكل أساسي ومؤخراً تم تسجيل إصابات بنظم تشغيل MAC من شركة APPLE.

تحافظ على نشاطها في النظام المصاب من خلال عدة طرق منها: التعديل في قيم مفاتيح التسجيل في مسجل النظام Registry، كذلك العمل بشكل تلقائي مع كل عملية إقلاع للنظام المضيف، واستخدام مكتبات الارتباط الديناميكي (DLL)لتطوير وتحديث قدراتها باستمرار.

الدراسة الفنية:

أ. التسميات حسب المرجعيات العالمية:

Trojan.Emotet,Trojan:W32/Emotet,Trojan.GenericKD.40123048

ب. الانتشار:

- عبر رسائل البريد الإلكتروني الواغل SPAM كملفات مرفقة وبأشكال متنوعة.
- يعتمد أدوات ومنهجيات عديدة للانتشار في الشبكة بعد الإصابة يقوم بتحميلها ومنها:
  - NetPass.exe
  - Credential enumerator
  - WebBrowserPassView

- Outlook scraper
- Mail PassView
- SMB Accounts brute force

ج. الإصابة:

تحدث الإصابة عند فتح الملف الحامل للفيروس أو ملف الفيروس ووفق المراحل التالية:

- إنشاء مفاتيح جديدة في مسجل النظام تمكن الفيروس من العمل بشكل تلقائي مع إعادة إقلاع نظام التشغيل.
- يحقن نفسه في واحدة أو أكثر من إجرائيات نظام التشغيل الفعالة مثل explorer.exe.
- الاتصال بالمخدم الخاص به عبر عنوان شبكي ومنفذ معين وانتظار تلقي تعليمات المهاجم.
- محاولة الانتشار في الشبكة المحيطة ونقل العدوى.

د. أعراض الإصابة:

- وجود المفاتيح التالية في مسجل النظام:

- HKLM\SYSTEM\ControlSet001\services\[Dropped_Filename]\Type: 0x00000010
- HKLM\SYSTEM\ControlSet001\services\[Dropped_Filename]\Start: 0x00000002
- HKLM\SYSTEM\ControlSet001\services\[Dropped_Filename]\ErrorControl: 0x00000000
- HKLM\SYSTEM\ControlSet001\services\[Dropped_Filename]\ImagePath: %windir%\System32|SysWOW64\[Dropped_Filename].exe
- HKLM\SYSTEM\ControlSet001\services\[Dropped_Filename]\DisplayName: [Dropped_Filename]
- HKLM\SYSTEM\ControlSet001\services\[Dropped_Filename]\ObjectName: LocalSystem
- HKLM\SYSTEM\ControlSet001\services\[Dropped_Filename]\Description:

- وجود ملفات بأسماء غريبة مثل المسار التالي:

C:\Users\<username>\AppData\Local\Microsoft\Windows**shedaudio.exe**

System root directories:

- C:\Windows\11787416.exe
- C:\Windows\System32\46615275.exe
- C:\Windows\System32\shedaudio.exe
- C:\Windows\WOW64\f9jwqSbS.exe

- الاتصال بالعناوين الشبكية التالية:

- 71.244.60[.]231:4143
- 84.200.208[.]98:80
- 91.217.66[.]130:443
- 193.169.54[.]12:8080
- 80.82.115[.]164:4143
- 186.103.199[.]252:4143
- 213.108.33[.]44:80
- 27.254.150[.]53:4143
- 189.51.144[.]3:80
- 159.203.94[.]198:4143
- 178.62.39[.]238:443
- 178.62.253[.]139:4143
- 52.4.64[.]240:4143

هـ. الوقاية من الإصابة:

- حماية نظم التشـــغيل من خلال البرامج المضـــادة للبرمجيات الخبيثة وتحديثها بشـــكل مســـتمر وعدم منح الصلاحيات للمستخدمين بإيقاف برامج الحماية لأي سبب كان.
- إبطال عمل البروتوكول SMB في حال عدم اســـتخدامه، وفي حال الحاجة إليه يتم تطبيق قواعد حماية على الجدار الناري لنظام تشغيل ويندوز بحيث لا يتم السماح بتمرير الطلبات الواردة إلى خدمة SMB كما يمكن استخدام أجهزة أو برمجيات كشف ومنع التطفل IPDS لفحص حركة بيانات الشبكة.
- إيقاف تنفيذ برمجيات الماكرو بالنسبة لبرامج الأوفيس وعدم منح الصلاحيات للمستخدمين بتمكين تنفيذها.
- اســـتخدام برمجيات أو تجهيزات فلترة وفحص البريد الإلكتروني Anti-spam لمنع وصـــول مرفقات البريد الإلكتروني المشبوهة إلى المستخدمين وحجب مصدرها.
- تحديث نظم التشغيل بشكل دوري.
- توعية وتدريب العاملين وتعريفهم بأنماط رســـائل البريد الإلكتروني الواغل وتقنيات الهندســـة الاجتماعية وإيجاد آليات لإعلام مسؤولي الشبكات والنظم المعلوماتية بأي حالة مشبوهة.

هـ. المعالجة:

في حال تم اكتشاف وجود إصابة بهذا البرنامج الخبيث من خلال ظهور أحد أعراض الإصابة المبينة أعلاه، يمكن اتخاذ مجموعة من الإجراءات وهي تختلف بحسب درجة الانتشار ويمكن تلخيصها بشكل عام في عدة نقاط:

- عزل الأجهزة المصابة عن الشبكة.
- الكشف على بقية الأجهزة المتصلة ضمن نفس الشبكة المحلية، والأجهزة المتصلة من خارج الشبكة المحلية وعزلها.
- تحديد العناوين الشبكية لمخدمات المهاجم من خلال تعليمة netstat –a في موجه الأوامر لنظام تشغيل windows وحجبها من خلال تجهيزات الحماية.
- الإزالة اليدوية لجميع ملفات الفيروس من نظام تشغيل الأجهزة المصابة بالإضافة لحذف قيم مفاتيح مسجل النظام التي أنشأها أو عدلها الفيروس وذلك يتطلب خبرة وممارسة في هذا المجال ولا مجال لسردها في هذا البحث – خصوصاً أن هذا الفيروس يمكنه اكتشاف البيئات الافتراضية _ ، وإن لم يكن ذلك متاح يجب الاعتماد على تنصيب برمجيات مضادة للبرامج الخبيثة ذات سمعة وتصنيف جيد وتنصيب آخر التحديثات وإجراء المسح الشامل ومعالجة الإصابة.

رئيس مركز أمن المعلومات

م. سلمان سليمان