البرنامج الخبيث *ACbackdoor*

اكتشف الباحثون مؤخراً برنامجًا ضارًا يُطلق عليه اسم *ACbackdoor* حيث يستهدف جميع إصدارات نظم التشغيل Windowsبالإضافة إلى نظام التشغيل Linux وذلك لسرقة معلومات حساسة من الأجهزة المخترقة.

تأتي خطورة هذا النوع في أنّ المستخدم العادي لا يُدرك بأنّ حاسبه قد تمّ اختراقه بسبب أنّ ملف payload الضار سيتمّ تشغيله ضمن خلفية نظام التشغيل Background لكن بالتأكيد سيُلاحظ الآثار المترتّبة على هذا الاختراق حيث سيصيب الحاسب بعض البرمجيات الخبيثة الأخرى أو تتمّ سرقة بيانات الحاسب.

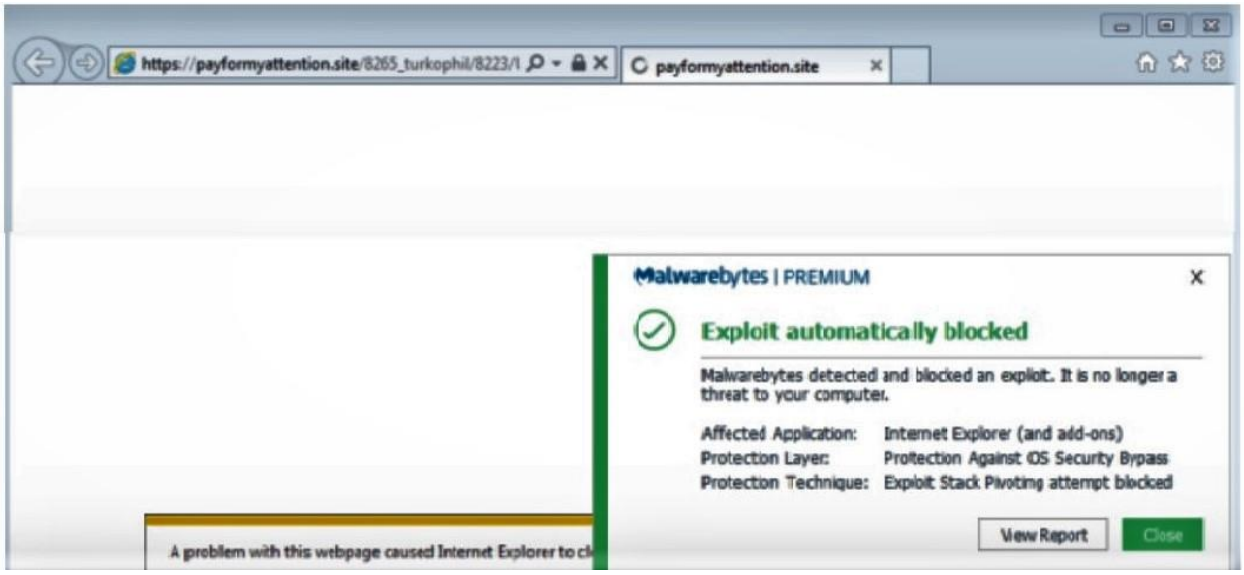
معدّل اكتشاف هذه البرمجية الخبيثة في أنظمة التشغيل Linux ضئيل جداً مقارنةً مع نظام التشغيل Windows فباستخدام 70 أداة مسح anti-malware scanning tools تمّ اكتشاف وجود البرمجية الخبيثة بواسطة أداة واحدة فقط في نظام التشغيل Linux بينما في نظام التشغيل Windows تمّ اكتشافها بواسطة 37 أداة.

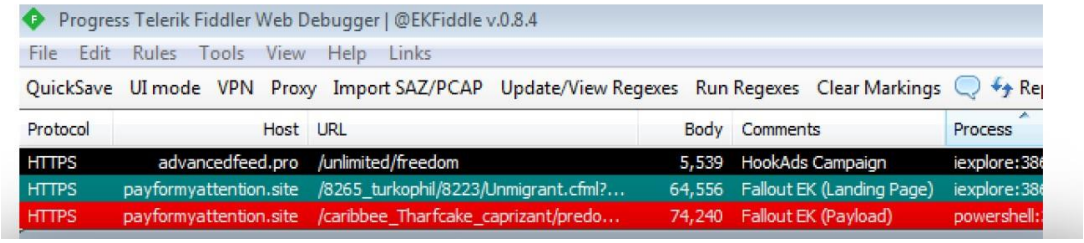
الوصف Description

الملف التنفيذي للبرمجية الخبيثة يكون مرتبط ديناميكياً بملفات PE (Portable Executable) في نظم التشغيل Windows بينما يكون مرتبط ستاتيكياً بملفات ELF (Executable and Linkable Format) في نظم التشغيل Linux، بالرغم من أنّ كلاهما يؤدّيان نفس الوظيفة بالإضافة الى اتّصالهم بمخدّمات التحكم والإدارة Command and Control Servers إلا أنّهما يختلفان بطرق التأثير في الأجهزة الضحية حيث في نظم التشغيل Windows يستخدم المهاجمون أداة استغلال *Fallout Exploit Kit*، التي تتضمّن كود خبيث يُعرّض صفحة الويب للخطر بينما في نظم التشغيل Linux لم تُعرف الطريقة بعد.

الجديد في أداة الاستغلال *Fallout* هو :

- استخدام رمازات برمجية نوع *powershell* لتنفيذ الرماز الخبيث payload بدلاً من استخدام *VBScript* كلغة برمجية يدعمها متصفح internet explorer فقط والذي أصبح قادراً على اكتشافها بعد الهجمات السابقة باستخدام الملف التنفيذي الخبيث iexplore.exe.
- يتمّ إرسال ملف payload المرمّز بتقنية BASE64 باستخدام برتوكول النقل HTTPS كقناة اتصال إلى مخدّمات command and control servers الخاصّة بالمهاجمين كما توضّح الصورة أدناه.

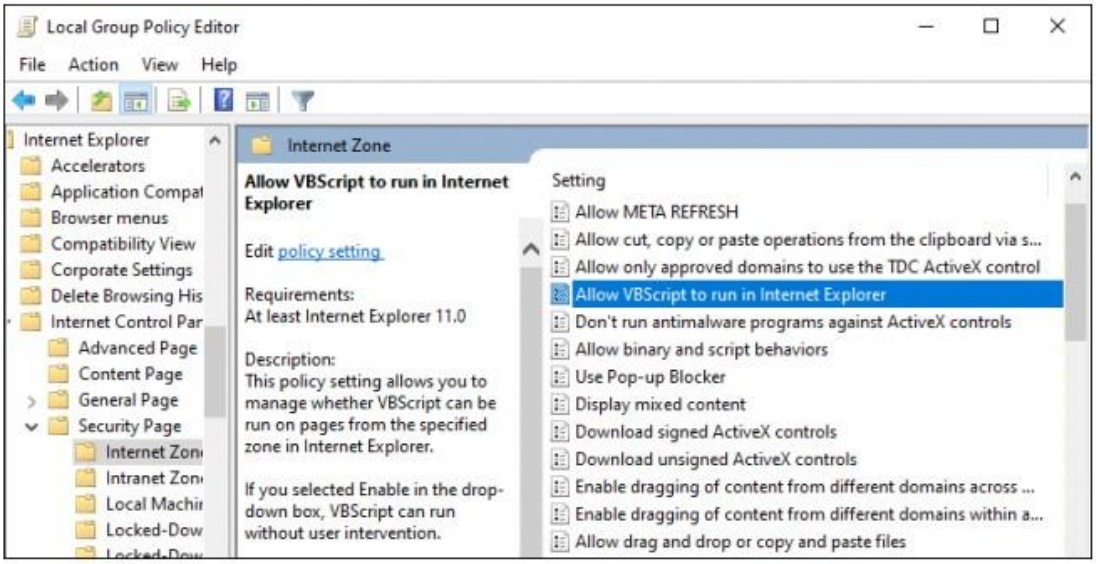




تاريخ ظهور أداة الاستغلال "*Fallout exploit kit*"

ظهرت أداة الاستغلال Fallout exploit kit لأوّل مرة منذ أواخر عام 2018 كنوع من برمجيات الفدية *Ransomware* من خلال القدرة على تنفيذ التعليمات البرمجية الخبيثة نوع *VBScript* عن بعد بصلاحيات مدير النظام Windows Administrator داخل متصفح الويب Internet Explorer وصنّفت الثغرة بالرمز CVE-2018-8174 وبعدها ظهرت من خلال استغلال ثغرة CVE-2018-15982 في مواقع تستخدم تطبيق Flash Player بالإصدارات 31.0.0.153 and earlier, and 31.0.0.108 and earlier وبهذا أثّرت الثغرة على جميع الزائرين لمثل هذه المواقع المصابة والمتحكَّم بها من قبل المهاجمين.

تمّ حل المشكلة الموجودة في متصفح الويب بعد قيام شركة Microsoft بتحديث نظم التشغيل Windows، حيث تمّ تعطيل خيار تمكين المحتوى البرمجي نوع *VBScript* بالحالة الافتراضيّة كما توضّح الصورة أدناه، وهذا يوضّح مدى أهميّة تطبيق تحديثات البرامج والتي غالباً تعمل على تصحيح الأخطاء ونقاط الضعف ولذلك فإنّ خيار تشغيل إيقاف التحديث التلقائي ليس فكرة جيدة.



النشر Dissemination

Fallout exploit kit تهاجم مواقع الويب ويتمّ اختيارها بحيث تكون الأكثر شعبية وذلك لضمان إصابة عدد كبير من الضحايا بهذه البرمجية الخبيثة. هذه المواقع تعاني عادةً من ثغرات محددة مثل ثغرة XSS في إحدى صفحاتها، يتمّ استغلال هذه الثغرة بحيث يتمّ حقن رمازات خبيثة بمجرّد دخول المستخدم لصفحة الويب المصابة بالبرمجية الخبيثة عندها يتمّ تلقائياً تحميل برنامج خبيث في متصفح الزائر وتشغيل ملف payload في خلفية نظام التشغيل Background داخل جهاز الضحية بدون إذن أو علم من قبل مستخدم النظام، هذا البرنامج الخبيث هو برنامج قابل للتنفيذ باستخدام موجه الأوامر *PowerShell* الذي سيقوم بتنفيذ أوامر مرمّزة بترميز BASE64.

الإقلاع وبدء العمل Starting Up

- يبدأ البرنامج الخبيث *ACBackdoor* عمله على الأنظمة المصابة بإجراء عدد من الاختبارات للتأكّد من أنّ النظام الحالي ليس بيئة اختبارية Sandbox ثم يعمل على تمويه نفسه لتجنّب كشفه من قبل التطبيقات المضادّة للبرمجيات الخبيثة Antimalware Scan Interface AMSI من خلال إجرائية عاملة باسم *MsMpEng.exe* في نظم التشغيل Windowsبينما في نظم Linux فإنّ اسم الإجرائية هو *[kworker/u8:7-ev]*.
- يتمّ تأسيس اتصال عكسي من خلال فتح باب خلفي في النظام (backdoor) للاتصال مع مخدّمات command and control servers الخاصّة بالمهاجمين وبهذا يمكنه أن يستقبل، يشغل، ينفّذ وأيضاً ويحدّث البرمجيات الخبيثة التي سيتمّ استقبالها من هذه المخدّمات بشكلٍ تلقائي في كلّ عملية اقلاع لنظام التشغيل المصاب.
- مهمّة ملف payload هي جمع معلومات مهمّة عن الضحية، (مثل بيانات تسجيل الدخول، العنوان الفيزيائي للجهاز MAC Address، ملفات الارتباط web cookies ..) وإرسالها إلى المهاجمين حيث يتمّ جمع المعلومات باستخدام أدوات خاصّة، كتوابع Application Programming Interface (API) في نظم التشغيل Windows، وفي نظم التشغيل Linux باستخدام أمر *uname [OPTION]* لإظهار معلومات عن النظام.

- إذا كان تقييم المهاجمين لجهاز الضحية مناسباً عندها يتمّ تنفيذ ملف payload النهائي باستخدام موجّه الأوامر *PowerShell* الذي سيقود الضحيّة إلى موقع آخر مستضاف في مخدّمات الإدارة والتحكم الخاصّة بالمهاجمين ويتمّ تشفير جهاز الضحيّة بهدف الحصول على فدية مالية باستخدام العملة الرقمية bitcoin.

على الرغم من أنّ أدوات الاستغلال ليست جديدة إلا أنّ المهاجمين يقومون باستخدام أدوات استغلال أكثر تطوّراً تجمع بين تقنياتٍ مختلفة حتى البرمجية الخبيثة payload يتمّ ترقيتها باستمرار.

أعراض الإصابة الأكثر شيوعاً:

- بطء في عمل جهاز الكمبيوتر.
- تعطّل البرامج المنصّبة على النظام على الفور.
- يتّصل الحاسب بالإنترنت ويقوم بتحميل برمجيات بدون إذن المستخدم.
- عدم إمكانية إزالة البرمجيات الخبيثة التي تمّ تحميلها، وذلك بالطرق الاعتيادية.

التوصيات والحماية Recommendations and Mitigations

- ✓ يتعيّن على المستخدمين أن يبقوا حذرين عند تصفحهم لمواقع الويب لأنّ مثل هذه البرمجيات الخبيثة منتشرة بشكلٍ واسع على شبكة الإنترنت.
- ✓ تحميل وتطبيق تحديثات أنظمة التشغيل بشكلٍ مستمر.
- ✓ التحديث المستمر للبرامج المتأثرة ومراقبة حركة مرور الشبكة إن أمكن.
- ✓ تنصيب تطبيقات مكافحة البرمجيات الخبيثة والتأكّد من تحديثها بشكلٍ مستمر وتلقائياً.

المصادر References

- https://www.bleepingcomputer.com/news/security/linux-windows-users-targeted-with-new-acbackdoor-malware/
- https://nvd.nist.gov/vuln/detail/CVE-2018-15982
- https://www.cybereason.com/blog/watch-where-you-browse-the-fallout-exploit-kit-stays-active
- https://www.deepworkmagazine.com/cyber-crime/malware/fallout-exploit-kit-is-back-with-new-vulnerabilities-and-payloads/

إعداد

م. نوره قادري