برنامج خبيث جديد من النوع "برمجيات الفدية"
New Malware: SamSam Ransomware

برمجيات الفدية أو Ransomware هي برمجيات خبيثة تقوم بمنع الوصول إلى الأنظمة والبيانات بالإضافة إلى قيامها بـــ "رهن" هذه الأنظمة بعد منع الوصول إليها والبيانات بعد تشفيرها ريثما يتم دفع الفدية المطلوبة، بالإضافة إلى قدرة هذه البرمجيات على الانتشار إلى محركات التخزين المشتركة Shared Storage Drives والأنظمة التي من الممكن أن تصل إليها Accessible Systems.

وصف البرنامج Summary

تم مؤخراً اكتشاف برنامج خبيث جديد SamSam وهو من نوع برمجيات الفدية التي تستطيع استهداف الأنظمة وبشكل عام أنظمة Windows وخاصة أنظمة Windows Server بالإضافة إلى البيانات المخزنة ضمنها بحيث لن يتمكن مستخدمو هذه الأنظمة من استخدامها بسبب قدرة هذا البرنامج الخبيث على تشفير مختلف ملفات البيانات بتقنيات تشفير متقدمة بواسطة مفاتيح تشفير طويلة نسبياً، مع عدم القدرة تقريباً على فك تشفيرها بدون الحصول على مفاتيح التشفير والتقنيات المستخدمة في عملية التشفير هذه، مع الأخذ بعين الاعتبار أن استهداف المنظومات ذات الشبكات الواسعة والمؤسسات التي تقوم بتقديم خدمات هامة سيمكّن مشغلي هذا البرنامج من طلب فديات أكبر وربما تحصيل هذه الفديات بشكل أسرع وأفضل من استهداف الأنظمة الشخصية.

آلية العمل Access and Exploitation

تعتمد SamSam بشكل أساسي في وصولها إلى الشبكات المستهدَفة على اختراق أنظمة التشغيل Windows Servers، حيث تقوم بعدها باستهداف الأنظمة Hosts ضمن هذه الشبكات، وفق الإحصائيات المتوفرة حتى الآن فإن اختراق المخدمات المركزية للشبكات يتم بواسطة استغلال الثغرات الموجودة في التطبيقات JBoss Applications ويتم ذلك بشكل رئيسي اعتماداً على مجموعة الأدوات JexBoss Exploit Kit والتي هي عبارة عن أداة متقدمة تقوم بالبحث والتحقق من وجود ثغرات معينة ضمن تطبيقات JBoss وذلك في بعض مكوناتها، واستغلال هذه الثغرات لاحقاً وفق طرق وأساليب خاصة. تقوم SamSam أيضاً باستغلال البروتوكول Remote Desktop Protocol RDP من أجل الحصول على وصول مستمر للشبكات المستهدَفة. بالإضافة إلى إمكانية القيام بهجمات القوة الغاشمة Brute Force Attacks على نماذج المصادقة والدخول أو الاعتماد على بيانات دخول قد تم الاستيلاء عليها مسبقاً بطرق مختلفة واستغلال ذلك للوصول إلى الشبكات. بعد تمكن البرنامج من الوصول إلى الشبكات يقوم بعدها برفع سماحيات الوصول Privileges Escalation وذلك من أجل الحصول على سماحيات المدراء Administrator كي يتمكن لاحقاً من تنصيب وتشغيل برنامج تنفيذي على المخدم المستهدَف والبدء بالعمل على استهداف الأنظمة المرتبطة بالشبكة وتشفير ملفات البيانات الموجودة.

البرنامج الخبيث SamSam يحرص على ترك المعلومات التي تتضمن تفاصيل الاتصال بمشغلي البرنامج وهي عادةً عن طريق شبكة Tor، بعد الاتصال يقوم المشغلون بطلب الفدية وتحديد طريقة الدفع والتي تكون غالباً بالعملة Bitcoin، بعد التأكد من دفع الفدية يقوم المشغلون بتزويد الضحية بروابط معينة من أجل تحميل مفاتيح التشفير والأدوات اللازمة من أجل فك تشفير البيانات.

الحماية Mitigations

إن مسؤولية الحماية ضد البرنامج الخبيث SamSam Ransomware تقع على عاتق الجميع، حيث على مالكي المنظومات العمل على دعم أمن الشبكات والنظم والمعلومات بكافة الوسائل المتاحة، وعلى مدراء الأنظمة والمستخدمين اتباع أفضل الطرق والأساليب لتحقيق ذلك، وفيما يلي بعض التوصيات:

- فرض سياسات صارمة على استخدام البروتوكول RDP، تتضمن تحديد المخدمات والأجهزة والمستخدمين المخولين باستخدام خدمة الوصول البعيد RDP، بالإضافة إلى وضع سياسة واضحة من أجل إدارة عمليات تحديث خدمات RDP تتضمن دراسة تفاصيل التحديثات وتأثيراتها المحتملة على المخدمات بشكل خاص قبل الموافقة على تنصيبها.
- في حال الحاجة للاتصال بالبروتوكول RDP من خارج المنظومة External to Internal Connections يفضل عندها استخدام وسائل اتصال آمنة مثل الشبكات الافتراضية VPNs
- التأكد من إيقاف خدمة استقبال الاتصالات البعيدة الخاصة بالبروتوكول RDP وإغلاق المنفذ 3389 على المخدمات والأجهزة التي تشغل الخدمات السحابية إلا في حال الضرورة القصوى ويجب في هذه الحالة اتخاذ الإجراءات الأمنية المناسبة كوضع هذه الأجهزة خلف جدران نارية موثوقة.
- الحد قدر الإمكان من هجمات Brute Force من خلال فرض سياسات لتحديد كلمات مرور قوية وإدارة مناسبة لمختلف أنواع الحسابات Accounts Management
- فرض طرق وأساليب مصادقة متعددة المراحل مثل Two-Factor Authentication إن أمكن.
- متابعة تحديث أنظمة التشغيل والتطبيقات بشكل دوري ومستمر.
- وضع سياسة مناسبة وموثوقة للنسخ الاحتياطي للبيانات واختبارها وتطويرها بشكل مستمر، لعل النسخ الاحتياطي من أهم خطوات الحماية ضد هذا النوع من البرمجيات الخبيثة وذلك كي يتمكن مدراء الأنظمة من استعادة البيانات بشكل مناسب في حال تشفيرها.
- مراقبة ملفات السجلات Log files والتأكد من أن هذه الملفات تقوم بتسجيل التفاصيل المتعلقة بـــ RDP
- تقييد سماحيات تنصيب وتنفيذ البرامج على المخدمات والأجهزة وحصرها بفئة محددة من المستخدمين.
- تنصيب التطبيقات المضادة للبرمجيات الخبيثة المزودة بجدران نارية ومكونات لمسح البريد الالكتروني ومرفقاته وتحديثها بشكل مستمر خاصة على المخدمات، مع الحرص على إجراء مسح دوري للأجهزة.
- التقليل ما أمكن من تشاركية موارد الشبكة كمحركات الأقراص والطابعات، وفي حال الضرورة لذلك يجب فرض كلمات مرور قوية أو إجراء المصادقة بشكل مركزي مثل Active Directory Authentication
- تفعيل تقنية النسخ الاحتياطي Shadow Copies في أنظمة Windows وإعدادها بالشكل الأمثل.