الجمهورية العربية السورية
وزارة الاتصالات والتقانة
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

الرقم:43/ت/2019

الموضوع: تقرير حول هجمات اختطاف أسماء النطاقات المسماة بهجمات السلاحف البحرية

أشار تقرير لشركة سيسكو بتعرض عدد من الدول إلى هجمات الكترونية واسعة لاختطاف أسماء النطاقات DNS hijackings campaign في الأسابيع القليلة الماضية، قامت بها منظمة إجرامية تحت رعاية إحدى الحكومات التي لم يسمها التقرير والذي نشر على الرابط التالي:

https://blog.talosintelligence.com/2019/04/seaturtle.html#more

تبدأ الهجمات من خلال استغلال الثغرات الأمنية في شبكات ونظم الأهداف واستخدام تقنيات أخرى كالتصيد الالكتروني وبرمجيات خبيثة كمرفقات لرسائل البريد الالكتروني (spam) وأي تقنيات أخرى تتيح لهم الحصول على بيانات دخول للتسلل إلى المنظومة المستهدفة.

وحددت شركة سيسكو عدد من الثغرات –على سبيل المثال لا الحصر –استغلها المنظمون لهجمات السلاحف البحرية في اختراق أهدافهم:

- CVE-2009-1151 ثغرة أمنية تسمح بحقن كود برمجي يصيب تطبيق phpMyAdmin.
- CVE-2014-6271 ثغرة أمنية لتنفيذ التعليمات البرمجية عن بُعد في نظام GNU bash في نظام التشغيل UNIX، ويتأثر بها بروتوكول نقل البريد الإلكتروني (SMTP).
- CVE-2017-3881: ثغرة أمنية تمكن من تنفيذ التعليمات البرمجية عن بُعد من قِبل مستخدم غير مصادق له مع إمكانية زيادة صلاحياته وهي موجودة في مبدلات Cisco.
- CVE-2017-6736 ثغرة أمنية تمكن من تنفيذ التعليمات البرمجية عن بُعد في أجهزة التوجيه Cisco 2811.
- CVE-2017-12617 ثغرة أمنية لتنفيذ التعليمات البرمجية عن بُعد في مخدمات الويب Apache.
- CVE-2018-0296 ثغرة التنقل عبر المجلدات تسمح بالدخول غير المصرح به إلى تجهيزات حماية خاصة بشركة cisco.
- CVE-2018-7600 ثغرة في نظام إدارة محتوى Drupal تسمح بتنفيذ التعليمات البرمجية عن بُعد.

وبمجرد أن يحصل متسللو السلاحف البحرية على اختراق جزئي لمنظومة الهدف، فإنهم يتابعون الانتشار والبحث بشكل أفقي عبر الشبكة حتى يحصلوا على بيانات الدخول اللازمة لتعديل سجلات DNS للنطاقات ذات الاهتمام.

ويقومون بذلك وفق طريقتين: إما أن يستهدفوا منظومة النطاق العلوي بشكل مباشر حيث إدارة النطاق أو من خلال استهداف منظومات الشركات(المسجلين) المرخص لها ببيع وإدارة النطاقات والتي تتصل بمنظومة النطاق العلوي

Tel: +963 11 3937049 Fax: +963 11 3937079 P. Box:60 Sabouraa E-mail: infoisc@nans.gov.sy
Website: www.nans.gov.sy

الحكومي من خلال بروتوكول (EPP) ولديهم صلاحيات تسجيل نطاقات جديدة والتعديل في سجلات أسماء النطاقات (DNS Records).

وفي الحالتين يتم التلاعب بسجلات النطاقات بحيث يتم إعادة توجيه النطاقات للعناوين IPs الشبكية الخاصة بالمهاجمين بدلاً من العناوين المخصصة لها بحيث يتم إجبار المستخدمين على المرور بمخدمات خاصة بالمخترقين قبل وصولهم إلى الخدمات أو المواقع الاصلية التي قاموا بطلبها، وعندها ومن خلال هجمات الرجل في الوسط MITM يحصلون على بيانات الدخول الخاصة بالمستخدمين الشرعيين الذين يقومون بتسجيل الدخول إلى الخدمات والتطبيقات أو المواقع الالكترونية.

تم استخدام مخدمات الأسماء التالية في هجمات السلاحف البحرية لإعادة التوجيه:

ns1[.]intersecdns[.]com

ns2[.]intersecdns[.]com

ns1[.]lcjcomputing[.]com

ns2[.]lcjcomputing[.]com

الأمر الملفت في هذه الهجمات استخدام شهادات رقمية شرعية خاصة بالمهاجمين لاختراق الخدمات التي تستخدم الشهادات الرقمية مثل المواقع الالكترونية ومخدمات الشبكات الافتراضية وواجهات التطبيقات وذلك من خلال توجيه الضحية إلى صفحة مزورة بشهادة رقمية شرعية من جهة موثوقة وعندها يمكن خداع المستخدمين بسهولة ولن يلاحظوا أي فرق أو أي مشكلة عند رؤيتهم رمز القفل بجانب الشهادة على المتصفح باللون الأخضر وعندها يقومون بإدخال بياناتهم للدخول إلى الخدمة والنتيجة حصول المخترقين على بيانات الدخول إلى هذه الخدمات.

ولضمان تحكمهم المستمر بهذه الأهداف المخترقة يقوم المهاجمون أولاً بتغيير إعدادات DNS لمسجلي DNS المستهدفين وشركات الاتصالات ومقدمي خدمات الإنترنت ثم يستخدم المهاجمون سيطرتهم على هذه الخدمات لمهاجمة الأهداف الأساسية التي تستخدم خدمات DNS وتشمل الأهداف الرئيسية منظمات الأمن القومي ووزارات الخارجية ومنظمات الطاقة البارزة، وتركزت هذه الهجمات في الشرق الأوسط وشمال إفريقيا وبعض دول أوروبا.

تكمن خطورة هذه الهجمات أن داعميها يسعون لاختراق دائم للشبكات والأنظمة الحساسة للجهات المستهدفة.

ويشير التقرير إلى أنه تم اختطاف النطاقات السورية التالية في الأسابيع الستة الماضية:

- mofa.gov.sy وزارة الخارجية السورية
- syriatel.sy شركة الاتصالات السورية سيريتل

Tel: +963 11 3937049 Fax: +963 11 3937079 P. Box:60 Sabouraa E-mail: infoisc@nans.gov.sy
Website: www.nans.gov.sy

- وزارة الداخلية السورية syriamoi.gov.sy

وذكر التقرير بعض العناوين الشبكية التي استخدمت في الهجمات على النطاقات العلوية السورية:

45.77.137.65 ، 142.54.164.189 ،159.89.101.204

وهي عناوين خارجية ومجهولة.

إجراءات الحماية:

إن هذه الحملات مستمرة كما تشير التقارير، ويقوم المهاجمون بتنسيق هذه الهجمات بأساليب متجددة وبطرق أكثر فاعلية وللحماية منها يمكن اتخاذ مجموعة من الإجراءات:

1- يجب زيادة مناعة منظومات مخدمات أسماء النطاقات DNS ضد كل أشكال الهجمات المعروفة من خلال كشف ومعالجة الثغرات الأمنية.

2- المراقبة المستمرة لسجلات مخدمات أسماء النطاق والإبلاغ عن أي نشاط مشبوه في عمل هذه الخدمات من قبل الجهات المستهدَفة.

3- اعتماد سياسات أمنية صارمة تشدد على عمليات مصادقة المستخدمين من خلال أكثر من مرحلة للمصادقة، إضافة لاستخدام كلمات مرور قوية يتم تغييرها بشكل دوري واستخدام تجهيزات للحماية وإعدادها بالشكل الأمثل.

4- الانتباه والحذر من الصفحات المزورة، خصوصاً صفحات إدخال بيانات الدخول، ويمكن لمدراء المواقع الالكترونية تمييزها من خلال وجود اختلاف بسيط في الشكل وبطء في الاستجابة عن المعتاد وفحص الروابط التي تحتويها الصفحة المزورة، كذلك في حال استخدام شهادات رقمية للمواقع الالكترونية يجب التأكد من مصدر الشهادة الرقمية لأن المهاجمين يعتمدون شهادات رقمية شرعية للصفحات المزورة ولكن من مصدر يختلف عن مصدر الشهادة الأصلية للموقع أو للخدمة.

5- استخدام برامج مضادة للبرمجيات الخبيثة والانتباه من رسائل البريد الواغل (spam) وخصوصاً بالنسبة للمستخدمين الذين لا يملكون خبرات في هذا المجال.

6- إبلاغ الهيئة الوطنية لخدمات الشبكة عن أي حالة أو مشكلة تطرأ على عمل مخدمات أسماء النطاقات لأن أي معلومة قد تكون مفيدة لنا في تجنب حدوث اختراق أو العبث بأسماء النطاقات العلوية السورية.

رئيس مركز أمن المعلومات

م. سلمان سليمان

سلمان علي سليمان
Digitally signed by سلمان علي سليمان
DN: c=SY, ou=مركز أمن المعلومات, o=National Agency for Network Services (NANS), 0.9.2342.19200300.100.1.1=1017000 9529, cn=سلمان علي سليمان
Date: 2019.06.10 10:48:44 +03'00'

2019/5/22

Tel: +963 11 3937049 Fax: +963 11 3937079 P. Box:60 Sabouraa E-mail: infoisc@nans.gov.sy
Website: www.nans.gov.sy