سام
للحقوق والحريات

الأمن الرقمي في اليمن..
الواقع والمهددات

ديسمبر 2022

www.samrl.org

الأمن الرقمي في اليمن..
الواقع والمهددات

سام
للحقوق والحريات

سام
للحقوق والحريات

مشروع الحقوق الرقمية

نافذة حقوقية غير ربحية تابعة لمنظمة سام، بدعم من منظمة إنترنيوز، تهدف إلى التعريف بالحقوق الرقمية، ورصد الانتهاكات الرقمية بحق مستخدمي الفضاء الرقمي، حيث تعمل على مناصرة الحقوق الرقمية لليمنيين، بهدف الوصول إلى فضاء رقمي آمن وعادل وحر. تتيح النافذة تقديم البلاغات عن الانتهاكات الرقمية، كما تساهم في توثيقها وتشكيل قاعدة بيانات عنها. وتعمل على إصدار دراسات وأبحاث حول النشاط الرقمي، والحقوق الرقمية والأمان الرقمي، بالإضافة إلى تخطيط وإدارة حملات المناصرة المحلية والدولية.

violations@samrl.org

مقدمة

الحديث عن الأمن الرقمي ليس ترفًا، بقدر ما هو ضرورة ملحة يفرضها التطور المطرد للتكنولوجيا وما يرافقه من تهديدات ومخاطر، تعجز -أحيانا- أعتى الإمبراطوريات التكنولوجية عن التصدي لها، فما بالك بدولة ذات قدرت سيبرانية هشة وضعيفة للغاية، كاليمن، التي تحتل ذيل التصنيف في مؤشر الأمن السيبراني العالمي.

يواجه مستخدمو الإنترنت في اليمن مخاطر وتهديدات حقيقية تتراوح ما بين الرقابة والتجسس الخارجي، وهجمات القرصنة، بالإضافة إلى هجمات البرمجيات الضارة، والتصيد الاحتيالي عبر وسائل التواصل الاجتماعي، والذي يتخذ أنماطا مخادعة، كصفحات فيسبوك الزائفة، والرسائل المرفقة بـ لينكات خبيثة، وغيرها من الأساليب التي تستهدف الضحايا في اليمن.

سنناقش في هذا التقرير، واقع الأمن الرقمي في اليمن، بالاستناد إلى مؤشرات وإحصائيات عن حجم التهديدات والمخاطر التي يواجهها مستخدمو الإنترنت. كما سنتناول الآليات والإجراءات الكفيلة بتعزيز الأمن المعلوماتي، على المستويين المؤسسي والفردي.

إطار مفاهيمي

-الأمن الرقمي

هو مصطلح جماعي يصف الموارد المستخدمة لحماية هويتك وبياناتك وأصولك الأخرى على الإنترنت، وتتضمن هذه الأدوات خدمات الويب وبرامج مكافحة الفيروسات وبطاقات SIM للهواتف الذكية والقياسات الحيوية والأجهزة الشخصية المؤمنة. Simple Learn.

- الأمن السيبراني

هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، والتي تهدف عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها، أو ابتزاز الأموال من المستخدمين عن طريق برامج الفدية. cisco

السياق التنظيمي

تفتقر اليمن إلى قانون ينظم الفضاء الرقمي، ناهيك عن عدم وجود استراتيجية وطنية للأمن السيبراني، بيد أن ثمة نصوص قانونية عن حماية المعلومات، وحماية الخصوصية، تطرق لها مشروع قانون رقم (13) لسنة 2012م الذي (لم يُنفذ).

تجدر الإشارة إلى أن الخطة الاستراتيجية الوطنية للأمن السيبراني، التي تمخضت عن المؤتمر الوطني الأول للأمن السيبراني، المنعقد في صنعاء خلال الفترة (7-9 يونيو) 2021، هي الإطار الوحيد بهذا الخصوص، وقد تضمنت موجهات بشأن إقرار قوانين الحماية الإلكترونية الفردي ووضع خطة وطنية للاستجابة للحوادث السيبرانية، بالإضافة إلى وضع برنامج حماية الأصول والبنية التحتية للمعلومات الحيوية الخاصة بالدولة، والحوكمة المثالية لإدارة تطبيق الاستراتيجية الوطنية للأمن السيبراني، وأيضا، وضع قوانين ولوائح الأمن السيبراني، والتعاملات الإلكترونية والتجارة الإلكترونية.

مؤشر الأمن الرقمي

تعد اليمن واحدة من أسوأ البلدان في مؤشر الأمن السيبراني العالمي، نظرا لافتقارها للبنى التحتية التكنولوجية، وبحسب مؤشر الأمن السيبراني العالمي (GCI) الصادر عن الاتحاد الدولي للاتصالات بشكل دوري كل عامين، لتصنيف قدرات الأمن السيبراني للدول، فقد احتلت اليمن المرتبة الـ 22 عربيا، والـ 182 عالميا (من أصل 182 دولة) في مؤشر الأمن السيبراني العالمي للعام 2020، بعد أن كانت في المرتبة 21 عربيا، و172 عام 2018.

ويقيس المؤشر التزام الدول بالأمن السيبراني، وتحديد الثغرات لديها، وفيه يتم تقييم مستوى التنمية أو المشاركة لكل بلد على أساس خمس ركائز: التدابير القانونية، التدابير التقنية، التدابير التنظيمية ، تنمية القدرات، والتعاون.

ووفقا لـ تقييم 2020 الصادر عن أكاديمية الحوكمة الإلكترونية NCSI (مؤسسة غير ربحية تساعد مؤسسات القطاع العام في جميع أنحاء العالم في التحول الرقمي) فقد حققت اليمن 6 مؤشرات فقط من أصل 77 مؤشر اعتمد عليها التصنيف، في تقييم القدرات السيبرانية للبلد، وتوزعت كالتالي: مؤشرات الأمن السيبراني العامة (1 من إجمالي 27 مؤشر)، مؤشرات الأمن السيبراني الأساسية (2 من إجمالي 24 مؤشر)، ومؤشرات إدارة الحوادث والأزمات (3 من إجمالي 26 مؤشر).

احتلت اليمن المرتبة الـ 22 عربيا،

والـ 182 عالميا (من أصل 182 دولة) في مؤشر الأمن السيبراني العالمي للعام 2020

مؤشرات الأمن السيبراني العامة

تطوير سياسة الأمن السيبراني	0%
تحليل التهديدات السيبرانية والمعلومات	0%
التعليم والتطوير المهني	0%
المساهمة في الأمن السيبراني العالمي	17%

مؤشرات الأمن السيبراني الأساسية

حماية الخدمات الرقمية	0%
حماية الخدمات الأساسية	0%
خدمات تحديد الهوية والثقة الإلكترونية	11%
حماية البيانات الشخصية	25%

مؤشرات إدارة الحوادث والأزمات

الاستجابة للحوادث السيبرانية	50%
إدارة الأزمات السيبرانية	0%
محاربة الجرائم الإلكترونية	0%
العمليات العسكرية السيبرانية	0%

عوامل الضعف والهشاشة

وجدت شركة ريكورديد فيوتشر Recorded Future -وهي شركة مستقلة تعنى بتقديم المعلومات الاستخبارية للمنظمات حول العالم- حالات متعددة من الأنشطة المشبوهة داخل البنية التحتية للإنترنت في اليمن، حيث يظهر أن عنوان الـ IP لأحد خوادم الأسماء الرئيسية في يمن نت (ns1.yemen.net) يحتوي على وحدة "tenda-backdoor"، والتي تشير إلى باب خلفي للبرامج الثابتة يستخدم الثغرة CVE-2017-16923 لإجراء تنفيذ الأوامر عن بُعد في نماذج أجهزة التوجيه التي تصنعها الشركة المصنعة للشبكات الصينية Tenda، وبالتالي، يمكن للمهاجمين الحكوميين وغير الحكوميين الاستفادة من هذا الباب الخلفي للتسلل إلى مزود خدمة الإنترنت.

بالإضافة إلى ذلك، فإن الخوادم 82.114.162.66 و 82.114.162.10 -وهي سيرفرات استضافة المواقع الإلكترونية- التي يسيطر عليها الحوثيون والتي استضافت حتى يونيو 2018 ما يزيد عن 500 موقع إلكتروني حكومي وتعليمي وشركات يمنية، مليئة بالثغرات القديمة مثل CVE-2003-1582 و CVE-2009-2521 و CVE-2008-1446، والمشكلات الأقدم الأخرى التي لو تُركت دون إصلاح يمكن أن تسمح للمهاجمين بالوصول السهل إلى الأنظمة المذكورة. ريكورديد فيوتشر - نوفمبر 2018.

وفي هذا الصدد، كشفت المؤسسة العامة للاتصالات، في أغسطس 2017، أن شبكة الإنترنت الوطنية تعرضت لتهكير دولي طال الكثير من بلدان العالم ومنها اليمن، وتسببت بإلغاء إعدادات أجهزة مودم الـ ADSL لبعض المشتركين، ما تطلب إعادة تهيئة وتحديث أجهزة المودم، من أجل إعادة استقبال الخدمة. كما أفادت قناة المسيرة (بتاريخ سبتمبر 2021) بتعرض الاتصالات اليمنية لعملية تجسس، من عدد من السفن البريطانية عبر الكابل البحري قبالة الغيضة، مضيفة أنهم سطوا على بيانات شركة الاتصال اليمنية، في عملية تجسس شملت اليمن كله.

وبحسب تقرير صدر في يناير 2018 عن برنامج AGS بجامعة ديوك Duke الأمريكية، فإن الخبراء يتفقون على أن كلاً من "يمن نت" و"عدن نت" مليئة بالثغرات الأمنية [التي تجعلها عرضة للتجسس والاختراق].

المهندس والخبير في تقنية المعلومات علي الصغير فرحان أكد أن سجل اليمن في أمن المعلومات متدنٍ لعدة أسباب، منها: عدم وجود كادر متخصص في الأمن المعلوماتي (السيبراني) وعدم اهتمام قيادات الدولة بقطاع أمن المعلومات والإتصالات بالشكل الكافي، وعدم وجود جهاز حكومي متخصص في تقديم خدمات الدفاع والأمن للفضاء السيبراني، بالإضافة إلى عدم وجود أطر وتشريعات قانونية متكاملة وحديثة تؤسس لقاعدة وطنية فاعلة للأمن السيبراني الوطني، وكذا ضعف التنسيق بين الأجهزة الحكومية ونظائرها في دول الجوار والعالم فيما يخص سبل تدعيم الأمن السيبراني لليمن، بحسب ما نقله موقع مأرب برس - مارس 2013.

إلى ذلك، يشير رئيس جمعية الإنترنت السابق، الاكاديمي وليد السقاف، إلى أن أحد التحديات الرئيسية التي لوحظت هو الافتقار إلى المهارات الكافية من جانب مستخدمي التكنولوجيا للحفاظ على معاملاتهم أكثر أمانًا وحماية مواقعهم الإلكترونية وحساباتهم، وما التهديدات التي يواجهها مستخدمو الإنترنت اليمنيون إلا انعكاس للمخاطر المرتبطة باستخدام الإنترنت بشكل عام. منظمة المراقبة العالمية لمجتمع المعلومات - مصدر سابق.

الأخصائية التقنية نور خالد أشارت -خلال ندوة الابتزاز الإلكتروني لشهر نوفمبر الماضي التي نظمها مشروع الحقوق الرقمية- إلى أن الشركات والمؤسسات المحلية والمنظمات الدولية في اليمن، تعاني من تسيب تقني كبير وتهاون في اتباع إجراءات الأمن السيبراني، على الرغم من أن أي خطأ بسيط يمكن أن يعرض المؤسسة والمنظمة والشركة للاختراق والمساءلة القانونية.

ويمكن القول إن الانقسام بين أطراف الصراع في اليمن، وحالة الاستقطاب بين الفاعلين الإقليميين والدوليين، ألحقت الضرر ببنية الإنترنت في اليمن، إذ وبحسب تقرير صدر في نوفمبر 2018، عن ريكورديد فيوتشر فإن " اللاعبون الدوليون الرئيسيون، بما في ذلك الولايات المتحدة وروسيا والصين، يستخدمون البرامج الضارة والنشاط العسكري والنفوذ السياسي والاستثمارات لتعزيز مصالحهم في الصراع الإقليمي السعودي الإيراني من أجل الهيمنة داخل اليمن.

المهددات والمخاطر

-الرقابة والتجسس الخارجي

أورد تقرير صدر في أكتوبر 2015 عن سيتزن لاب Citizen Lab (وهو مختبر معني بدراسة ضوابط المعلومات التي تؤثر على انفتاح وأمن الإنترنت) أن المراقبة الإلكترونية الخارجية والمحلية منتشرة على نطاق واسع في اليمن، من قبل النزاع المسلح الحالي وخلاله أيضا.

استخدمت الحكومة المعترف بها دوليا شركة هواوي الصينية للمساعدة في بناء مزود خدمة الإنترنت الخاص بها. ومع ذلك، فقد تم اتهام هواوي [من قبل الإدارة الأمريكية] باستخدام تقنيتها للسماح للحكومة الصينية بالتجسس على عملائها. وإذا كان هذا هو الحال في اليمن، فإنه سيشكل تهديدًا خطيرًا لمستقبل الأمن السيبراني اليمني. في الواقع، يتفق الخبراء على أن كلاً من "يمن نت" و "عدن نت" مليئة بالثغرات الأمنية. بحسب برنامج AGS بجامعة ديوك Duke الأمريكية - يناير 2018

تتوقع شركة ريكورديد فيوتشر، أن تكون هناك بعض المراقبة الصينية للنشاط اليمني، حتى لو كانت مجرد وسيلة لمراقبة استثماراتهم. بالإضافة إلى ذلك، فإن حقيقة سيطرة الحوثيين على كمية هائلة من موارد الإنترنت في اليمن، بدعم من إيران، وممارسة سيطرة فعلية على البلاد لا تزال تثير استعداء الحكومة السعودية، وهذا يجعلهم على الأرجح هدفًا للمراقبة السعودية. وتتوقع شركة ريكورديد فيوتشر أن تستخدم هذه المراقبة في المقام الأول لتحديد نوايا الحوثيين وخططهم القتالية للمناوشات في جميع أنحاء اليمن، وستستهدف أجهزة التوجيه والمضيفين التقليديين وأجهزة أندرويد المحمولة. ريكورديد فيوتشر - نوفمبر 2018.

وفي حادثة خطيرة، كشف الموظف السابق في وكالة الأمن القومي الأمريكية NSA إدوارد سنودن، قيام الوكالة بإعادة توجيه حركة مرور الإنترنت الخاصة بـ يمن نت، والاتصالات اليمنية ككل، نحو نقطة تجميع تابعة لوكالة الأمن القومي، عبر مسار جديد أكثر ملاءمة لحركة المرور الواردة، من خلال التلاعب بـ بروتوكول البوابة الحدودية BGP الذي يقوم عليه نظام التوجيه العالمي للإنترنت.

ونظرًا لأنه من الصعب اعتراض اتصالات اليمن الدولية من داخل اليمن نفسه، فقد حاولت الوكالة " تشكيل " حركة المرور عمدًا إلى موقع أكثر ملاءمة من الناحية التشغيلية للمراقبة، بحيث تمر عبر كابلات الاتصالات الموجودة في منطقة صديقة، والأمر أشبه بـ تحويل جزء من النهر إلى موقع يسهل منه صيد الأسماك (أو أكثر قانونية) بحسب دراسة نشرها الباحث شارون غولدبرغ في The Center Foundation، في يونيو 2017.

وعلى الرغم من أن أنشطة التجسس والرقابة الداخلية، خارج سياق تقريرنا، لكن يمكن الإشارة إلى ما أظهرته رسائل البريد الإلكتروني المسربة من شركة برامج التجسس الإيطالية هاكينج تيم Hacking Team حيث تم تقديم طلبات متعددة من شركات في اليمن تسعى للحصول على مساعدة في نشر أدوات المراقبة في البلاد، ففي مايو 2013، تم طلب مزيد من المعلومات حول نظام اعتراض "دافنشي" Da Vinci الخاص بشركة Hacking Team. وبالمثل، في مارس 2015، اتصل عميل بالشركة طالبا المساعدة، بدعوى كونه الرئيس التنفيذي لشركة أمن تكنولوجيا المعلومات التي أبرمت عقدًا مع وكالة الأمن القومي اليمنية "لتطوير الأنظمة والتدريب وإنشاء أداة قوية لمراقبة وتحديد مواقع والتحكم في نطاق الاتصالات الكلي لليمن. إلا أنه ليس من الواضح -من سلاسل البريد الإلكتروني المسربة- ما إذا كانت أي من الشركتين قد اشترت منتجات أو خدمات Hacking Team، ولم تُظهر أي من عمليات الفحص التي أجريت كجزء من بحث سيتزن لاب على هاكينج تيم و فينفيشر دليلًا على خوادم التحكم الموجودة في اليمن. سيتزن لاب - أكتوبر 2015.

-هجمات البرمجيات الضارة

احتلت اليمن المرتبة الثانية ضمن أعلى 10 دول ومناطق من حيث نسبة المستخدمين الذين هاجمتهم البرامج الضارة للأجهزة المحمولة، عند درجة خطورة 18.91، من أصل 26 درجة، بحسب تقرير الشركة المتخصصة في أمن الحواسيب كاسبر سكاي Kaspersky للربع الثالث من العام الجاري 2022. وكان برنامج التجسس Trojan-Spy.AndroidOS. Agent.aas هو التهديد الذي غالبًا ما يواجهه المستخدمون في البلد. إضافة إلى ذلك، فقد تصدرت اليمن قائمة البلدان التي تعرض فيها المستخدمين لهجمات برمجيات الفدية عبر الأجهزة المحمولة، عند درجة خطورة (0.28٪)، وغالبًا ما واجه المستخدمون في اليمن Trojan-Ransom.AndroidOS. .Pigetrl.a

كما احتلت اليمن المرتبة الثانية في قائمة أعلى 10 دول وأقاليم تعرضت لهجوم من قبل برامج الفدية فيروسات طروادة، على اجهزة الكمبيوتر، حيث بلغت نسبة المستخدمين الفرديين الذين تعرضت أجهزة الكمبيوتر خاصتهم للهجوم من قبل برامج تشفير أحصنة طروادة 1.30% (كنسبة مئوية من جميع المستخدمين الفرديين لمنتجات كاسبر سكاي في الدولة)، والمرتبة الخامسة ضمن أكثر 10 بلدان في معدل التعرض لهجمات البرمجيات المالية الخبيثة، بمعدل 2.3%. وبحسب تقرير كاسبر سكاي، للربع الثالث من العام الجاري كانت اليمن في المرتبة 11 في قائمة البلدان التي واجه المستخدمون فيها أكبر مخاطر الإصابة عبر الإنترنت، بمعدل 12.58 من المستخدمين، والمرتبة الثانية من بين البلدان حيث واجه المستخدمون أعلى مخاطر الإصابة المحلية (البرامج الضارة التي تم العثور عليها مباشرة على أجهزة الكمبيوتر الخاصة بالمستخدمين أو الوسائط القابلة للإزالة المتصلة بها) بمعدل 45.12% من المستخدمين بزيادة 2% عن تقرير الربع الثاني.

وبحسب تقرير الربع الثالث للعام 2022 الصادر عن أفاست Avast (وهي شركة تشيكية متعددة الجنسيات لبرامج الأمن السيبراني) كان المستخدمون في اليمن من ضمن أكثر ثلاثة بلدان عرضة لخطر مواجهة برنامج "حصان طروادة الوصول عن بعد" (RATs)، والذي يقوم باستخراج البيانات من الكمبيوتر المصاب وتشغيل الأوامر والتعليمات البرمجية، ومعالجة الملفات على الأجهزة المصابة. كما كان المستخدمون في اليمن من ضمن الأكثر عرضة لخطر التعرض لسرقة المعلومات بواسطة برنامج راكون ستيلر Raccoon Stealer الذي يشق طريقه بشكل أساسي إلى أجهزة الكمبيوتر عبر البرامج "المكركة"، بنسبة مخاطرة (+ 16٪). وكان المستخدمون في اليمن، أيضا، أكثر عرضة لخطر مواجهة برامج الفدية (0.53٪ نسبة مخاطر) بحسب تقرير النصف الثاني لذات العام. كما أن مستخدمي أفاست Avast من اليمن وأربع دول أخرى، كان لديهم أعلى نسبة مخاطر لبرمجيات الاستغلال (إكسبلويت) والتي تعمل على استغلال الأخطاء والثغرات في النظام لتنفيذ تعليمات برمجية ضارة عن بُعد (RCE)، بحسب تقرير أفاست للعام 2021. ووفقا لـ تقرير مخاطر الكمبيوتر الشخصي العالمي لعام 2021، الصادر عن "أفاست"، احتلت اليمن المرتبة الرابعة ضمن الدول العشر الأكثر عرضة لخطر مواجهة التهديدات الإلكترونية في الشرق الأوسط وأفريقيا، بمعدل 46.21% من مستخدمي خدماتها.

وقد مثلت اليمن وكينيا معظم ضحايا برنامج سلينجشوت Slingshot (المقلاع) الذي استُخدم للتجسس الإلكتروني في منطقة الشرق الأوسط وإفريقيا منذ العام 2012 على أقل تقدير وحتى شهر فبراير 2018. وبحسب باحثين لدى كاسبرسكي لاب هاجم البرنامج الضحايا من خلال بعض أجهزة التوجيه الشبكية الرديئة، ومن ثم عمل على جمع لقطات الشاشة وبيانات لوحة المفاتيح وبيانات الشبكة وكلمات المرور ووصلات USB وأنشطة سطح المكتب الأخرى والحافظة والمزيد. كاسبر سكاي - مارس 2018.

-قرصنة المواقع الإلكترونية

ساهمت حقيقة أن اليمن دولة تفتقر إلى الخبرة نسبيًا عندما يتعلق الأمر بالعمليات التقنية المتعلقة بالإنترنت في خلق بيئة خصبة لاختراق مواقع الويب ورسائل البريد الإلكتروني وحسابات وسائل التواصل الاجتماعي، إذ تم استغلال نقص الوعي بكيفية عمل التكنولوجيا وكيفية اتخاذ الاحتياطات المناسبة لمنع الهجمات [التي تعرضت لها العديد من المواقع الإلكترونية في البلاد] خلال 2011-2012، وفقا لـ تقرير صادر عن منظمة المراقبة العالمية لمجتمع المعلومات GISWatch لعام 2014، (وهي منظمة تسعى لإنشاء مجتمع معلومات شامل).

الخبير في الأمن السيبراني كريس بلاسك، نوه في أبريل 2013، بأن مخاطر عدم الاستقرار في اليمن الناجمة عن جرائم الإنترنت والإرهاب السيبراني حقيقية، وأن العديد من الأحداث تسلط الضوء على هذه المخاطر، مستدلا بحادثة اختراق شركة تيليمن، البوابة الدولية الوحيدة لليمن، في صيف عام 2012، والتي ألحقت خسائر مقدرة بأكثر من 20 مليون دولار، بحسب بلاسك، بالإضافة إلى ما تعرض له البنك المركزي اليمني في ذات العام، حيث عانى من العديد من هجمات رفض الخدمة الموزعة وأصيبت مواقعه الإلكترونية عدة مرات ببرامج ضارة مثل الروبوتات (زيوس تروجان Zeus Trojan). مدونة كريس بلاسك.

في نوفمبر 2021، اكتشف باحثون في إسيت ESET (وهي شركة أمن تكنولوجيا المعلومات، ومقرها في براتيسلافا، سلوفاكيا) هجمات اختراق ويب استراتيجية مرتبطة بـ كانديرو Candiru -شركة برامج تجسس إسرائيلية- ضد مواقع بارزة في الشرق الأوسط، مع تركيز قوي على اليمن، حيث تم اختراق موقعي وزارة الإعلام ووكالة الأنباء سبأ، كما تم اختراق موقع يمن نت، وموقعي وزارتي الداخلية والمالية، بالإضافة إلى مواقع كل من: (البرلمان اليمني، الرؤية الوطنية، مصلحة الجمارك اليمنية، وموقع قناة المسيرة)، وكلها خاضعة لسيطرة الحوثيين، في صنعاء.

ونُفذ الهجوم باستخدام (حفرة الري) والذي يؤدي إلى اختراق مواقع الويب التي من المحتمل أن يزورها الأشخاص المستهدفون، مما يفتح الباب أمام غزو جهاز زائر الموقع. وفي هذه الحملة، من المحتمل أن زوار معينين لهذه المواقع قد تعرضوا للهجوم من خلال استغلال المتصفح. ومع ذلك، لم يتمكن باحثو ESET من الحصول على أدلة بشأن هذا الاستغلال، ذلك أن المهاجمين استخدموا المواقع المخترقة فقط كنقطة انطلاق للوصول إلى الأهداف النهائية.

-هجمات التصيد الاحتيالي عبر السوشيال ميديا

يتعرض مستخدمو منصات التواصل الاجتماعي في اليمن، لهجمات تستهدف اختراق حساباتهم الشخصية، إما عبر الهندسة الاجتماعية [والتي "يستخدم فيها المهاجم العاطفة البشرية لخداع الهدف للقيام بعمل ما، مثل الكشف عن بيانات اعتماد المصادقة"، بحسب شركة الأمن الرقمي الأمريكية Proofpoint]. أو عبر النقر على لينكات ضارة، والتي عادة ما تكون مرفقة برسائل مغرية (كالحصول على مساعدة من منظمة ما، أو جوائز مالية، رصيد إنترنت...إلخ) أو تسجيل بيانات الولوج للحساب عبر صفحات زائفة، تم إنشاؤها لهذا الغرض.

فعلى سبيل المثال: كشف الموقع بوست في تقرير نشره بتاريخ أكتوبر 2018، عن تعرض حسابات صحفيين في موقع "تويتر" للقرصنة من قبل جهات تبين أنها تعمل من العاصمة صنعاء، ومارست التهكير لعدة حسابات في تويتر أغلبها لصحفيين يمنيين معروفين، عن طريق استدراجهم بحيل إلكترونية، تعكس في مجملها وجود شبكة تتعلق مهمتها بالقرصنة والاستحواذ على تلك الحسابات لمصالح القائمين على تلك العمليات.

حيث تلقى أحد الصحفيين رسالة من حساب يحمل إسم "صلاح خاشقجي" تنصحه بتوثيق حسابه بالعلامة الزرقاء عبر مراسلة الدعم الفني العربي لتويتر من خلال رقم واتساب تم تخصيصه لهذا الأمر. اتبع الصحفي تلك التعليمات عبر رقم الواتساب، وهو رقم أمريكي جرى تخصيصه لهذه الحيلة، التي تقوم على

مطالبة الضحية بإعطائه البريد الإلكتروني وكلمة السر الخاصة بالبريد، وبيانات الدخول لحساب تويتر، بحجة استكمال عملية التوثيق. وبعد لحظات من المراسلة عبر رقم الواتساب جرى تهكير الحساب، واستبدال البيانات، ثم قام المنفذين للعملية بمراسلة الأصدقاء الذين يتابعون الصحفي ويتابعهم في تويتر وأغلبهم من العاملين في مجال الصحافة. والذين جرى الاحتيال على البعض بنفس الطريقة بعد مراسلتهم من حساب الصحفي الذي جرى تهكيره، مستغلا ثقة الزملاء ببعضهم البعض، واستبعاد مخادعتهم بهذا الشكل.

وعلى الرغم من من أن التصيد الاحتيالي باستخدام برامج المراسلة الفورية المجانية مثل فيسبوك ماسنجر، أو واتساب، لا يندرج تقنيًا ضمن التصيد الاحتيالي، إلا أنه مرتبط ارتباطًا وثيقًا، حيث يستغل المخترق مستوى الراحة المتزايد الذي يتمتع به المستخدمون من خلال فتح الرسائل من الغرباء والرد عليها من خلال منصات التواصل الاجتماعي. تريند مايكرو Trendmicro.

يؤكد الخبير في البرمجة وأمن المعلومات أحمد عسلان، أن غرض من يقفون خلف رسائل الاصطياد الإلكتروني تلك التي تنتشر بشكل عشوائي وتصل إلى مستخدمين غير محددين في مجموعات الدردشات على شبكات وسائل التواصل الاجتماعي وعلى الخاص؛ يتمثل في نجاحهم باستمالة المستخدم ودفعه للنقر على الروابط المرفقة لإيقاعه فيما وصفها بالمصيدة، ليتم تاليا التحكم بهاتفه، ليفضي الأمر في الكثير من الأحيان إلى حدوث جرائم عنف وتنمر تطال الضحايا، تتخذ أشكالا متعددة من تهديدات وابتزازات وجرائم إلكترونية أخرى. الموقع بوست - يوليو 2022

وفي هذا الإطار حذرت اللجنة الدولية للصليب الأحمر في اليمن في يونيو الماضي، من قيام أشخاص مجهولين بإرسال رسائل مضللة عبر تطبيق الواتس آب تتضمن معلومات مزيفة مفادها بأن اللجنة الدولية للصليب الأحمر في اليمن تنفذ برنامجًا طارئًا لمساعدة الأشخاص النازحين والذين تضرروا من النزاع في الحصول على مساعدات نقدية. تطلب هذه الرسائل

المزيفة والمضللة من الناس الدخول إلى رابط إلكتروني لتطبيق مشبوه للحصول على أرقام الحوالات المالية المزعومة. ووفقا للمختصين، قد يترتب عن ذلك قرصنة هواتف من يثبتون ذلك التطبيق على هواتفهم ما يعرض صورهم وبياناتهم الشخصية للخطر.

ومن الملاحظ أن التطبيق، يطلب الأذونات التالية: الوصول إلى الكاميرا، الملفات والوسائط، سجل المكالمات، جهات الاتصال، الميكروفون، رسائل SIM، إدارة المكالمات، الموقع الجغرافي، الأجهزة القريبة) وفي حال تم تثبيت التطبيق فهذا يعني أن الضحية كشف خصوصيته كاملة، وعرض نفسه للخطر.

-التطبيقات والبرامج الخبيثة

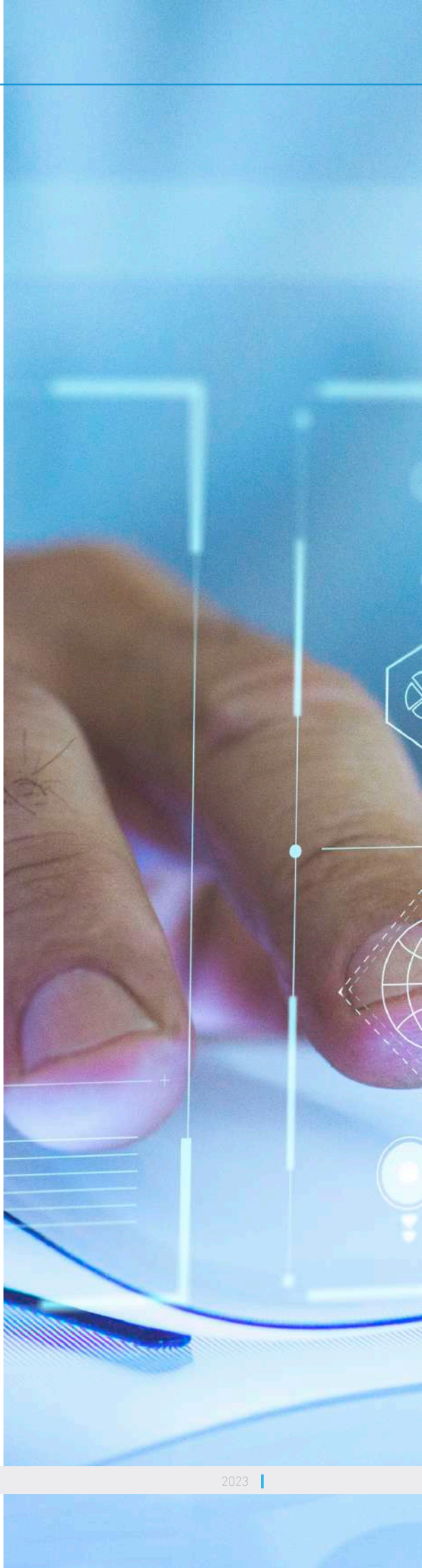
واجه المستخدمون في اليمن أعلى مخاطر الإصابة المحلية (البرامج الضارة التي تم العثور عليها مباشرة على أجهزة الكمبيوتر الخاصة بالمستخدمين أو الوسائط القابلة للإزالة المتصلة بها) بمعدل 45.12% من المستخدمين بزيادة 2% عن تقرير الربع الثاني، يشار إلى أن الشركة احتسبت النسبة المئوية لمستخدمي Kaspersky على أجهزة الكمبيوتر التي تم تشغيل Web Anti-Virus، ولا تتضمن التصنيفات سوى هجمات الكائنات الضارة التي تندرج تحت فئة البرامج الضارة؛ وهي لا تشمل اكتشافات مكافحة فيروسات الويب للبرامج التي يُحتمل أن تكون خطرة أو غير مرغوب فيها. بحسب تقرير كاسبر سكاي، للربع الثالث من العام الجاري.

لاحظت شركة ريكورديد فيوتشر في نوفمبر 2018، زيادة كبيرة في عدد عينات البرامج المقدمة إلى VirusTotal من اليمن، من 13 عينة بين عامي 2015 و 2017 إلى إجمالي 164 عينة في عام 2018... ومن بين هذه العينات، كان نصفها تقريبًا خبيثًا، وكانت الغالبية العظمى من تلك العينات الضارة عبارة عن تطبيقات أندرويد. كما لاحظت الشركة وجود العديد من محافظ العملة الرقمية البديلة البيتكوين Altcoin المزيفة وتطبيقات واتساب المزيفة، وبرامج التجسس التي تتظاهر بأنها مكافحة فيروسات، وبرامج تشغيل الفيديو وتطبيقات

VPN. وبعض عينات من تطبيق AhMyth -يتيح اختراق الهواتف الذكية و التحكم بها بشكل كامل- التي تم العثور عليها، كانت متصلة بعناوين IP الصينية. كما تم العثور على ثلثي تطبيقات برامج التجسس المضادة للفيروسات المزيفة، -المتصلة بعناوين IP الصينية- التي تصل إلى المعلومات من هواتف أندرويد بما في ذلك رسائل البريد الإلكتروني القديمة والرسائل القصيرة وسجلات المكالمات وسجل المتصفح. ومن المحتمل أن يستخدم خدمات إمكانية الوصول للتحكم في التطبيقات المثبتة الأخرى ولديه القدرة على تغيير تكوين الوايفاي وبدء الخدمات أثناء إيقاف تشغيل شاشة الهاتف، إضافة إلى التقاط الصور وحذف الحزم الأخرى. ريكورديد فيوتشر - نوفمبر 2018.

باحثة استخبارات التهديدات في ريكورديد فيوتشر، وينونا ديسومبر، قالت لـ سايبر سكوب CyberScoop في نوفمبر 2018، إنه من غير الواضح ما إذا كانت البرامج الضارة التي لوحظت قد استخدمت إما لأغراض إجرامية أو تجسس في اليمن. ومع ذلك ، قالت: "إن نية المجرمين لاستغلال الناس في منطقة حرب، للقيام بالتجسس ... موجودة".

إلى ذلك، يتزايد حجم استخدام التطبيقات المعدلة في اليمن، كـ واتساب، على سبيل المثال، وهو ما يمثل تهديدا حقيقا للمستخدمين، حيث "يرتبط استخدام هذه الإصدارات المستنسخة بمخاطر أمنية محتملة على الهاتف المحمول وبيانات المستخدمين الشخصية، بالإضافة إلى ذلك، لا توجد طريقة للتأكد من أن ملفات التطبيقات هذه توفر تشفيرًا للمحادثات أو أن الرسائل المرسلة لا تمر عبر خوادم الجهات الخارجية قبل الوصول إلى المستلم، مما قد يعرض الأمان للخطر أو حتى يسهل تسريب المعلومات الشخصية والخاصة. Techidence أكتوبر 2020.



ما الحل؟

لتعزيز الأمن الرقمي/ المعلوماتي في اليمن، يرى رئيس جمعية الإنترنت السابق، الأكاديمي وليد السقاف، في تصريح أدلى به لـ مشروع الحقوق الرقمي، أن يتم التركيز على رفع الوعى لدى العاملين في القطاعين العام والخاص حول كيفية تحديد ومنع التهديدات السيبرانية كلٌ في مجال عمله. كما أنه من المهم تطوير وإنفاذ قوانين ولوائح قوية للأمن السيبراني، والاستثمار في التكنولوجيا المتقدمة، خاصة مفتوحة المصدر التي تم غربلتها من الأخطاء، وينوه السقاف بأهمية التعاون مع المنظمات الدولية والدول الأخرى كـ الإمارات وعمان والأردن -لأن كثيرا من الأنظمة السيبرانية تتطلب تعريبا- للتعلم من تجاربها لا سيما في مجال التعليم والتأسيس للبنى التحتية للخدمات السيبرانية.

ويشدد الخبير في الأمن السيبراني كريس بلاسك على ضرورة معالجة الأمن السيبراني عبر تشكيل فريق يمني للاستجابة لحالات الطوارئ السيبرانية Y-CERT من أجل التخفيف من مخاطر الجرائم الإلكترونية والإرهاب السيبراني والتدهور الاقتصادي، إذ يمكن لوجود بنية تحتية قوية للأمن السيبراني في اليمن أن تمثل نقطة انطلاق للبلاد لمواجهة بعض هذه التحديات من خلال توظيف يمنيين لمعالجة قضايا الأمن السيبراني هذه، مع تحقيق فوائد إضافية قيّمة مثل زيادة فرص التعليم والتوظيف للمواطنين.

المهندس والخبير في تقنية المعلومات علي الصغير فرحان، دعا -في ندوة نظمتها شركة آيتكس للحلول التقنية، بتاريخ 25 مارس 2013، إلى إصدار قوانين وتشريعات وسياسات شاملة تنظم الأمن المعلوماتي وتجرم جرائم الإنترنت والفضاء الرقمي، وشدد على ضرورة توعية الناس بالأمن السيبراني وتدريب القضاة والأمن والبحث الجنائي على كيفية اكتشاف جرائم المعلومات وكيفية التحقيق فيها. كما طالب بضرورة الرفع من الحس الأمني المعلوماتي على مستوى البلاد وعلى المستوى الأفراد (خاصة مستخدمي الفضاء الرقمي). وأكد أن مسؤولية الحكومة تجاه الأمن السيبراني تتمثل في تدريب موظفي الدولة خاصة في قطاعي الأمن والقضاء على إنفاذ قانون جرائم الفضاء الرقمي وتجهيزه للتعامل مع الجرائم السيبرانية. مأرب برس - مارس 2013.

وقد أوصى المشاركون في المؤتمر الأول لأمن المعلومات (الذي نظمته المؤسسة العامة للاتصالات بالتعاون مع الاتحاد الدولي للاتصالات في يونيو 2014) الحكومة بإنشاء مركز السلامة المعلوماتية في اليمن YE – CIRT كنقطة تواصل للاستجابة للمشاكل الأمنية ومعالجتها وإشراك جميع الجهات ذات العلاقة، مع ضرورة الإعداد لبناء استراتيجية وطنية لوضع حلول لازمة في مجال أمن المعلومات بالتعاون مع الاتحاد الدولي للاتصالات، وعمل دراسة لإنشاء هيئة تنظيم الاتصالات ووضع إطار عام على مستوى الدولة لتمويل متطلبات أمن المعلومات، ونشر الوعي المجتمعي بهذا الخصوص عبر وسائل التقنية الحديثة، من خلال البرامج الإعلامية والمناهج التعليمية والمؤتمرات وورش العمل، بالإضافة إلى تخصيص ميزانية ضمن المسؤولية الاجتماعية لشركات الاتصالات، لرعاية ودعم مشاريع التوعية بأمن المعلومات. كما دعوا إلى تشكيل لجنة تحضيرية متخصصة لدراسة القوانين الحالية في اليمن المتعلقة بأمن المعلومات، ومقارنة القوانين المشابهة في الدول الأخرى لإنشاء قوانين وتشريعات لحماية المواطن والمؤسسات. صحيفة الثورة - يونيو 2014.

وعلى المستوى الفردي، نوهت الأخصائية التقنية نور خالد -خلال ندوة الابتزاز الإلكتروني لشهر نوفمبر الماضي التي نظمها مشروع الحقوق الرقمية- بضرورة أن تكون كلمات المرور قوية وألا نستخدم فيها أي معلومات شخصية، وأن تتضمن مزيجا من الرموز والأحرف (كبتل، سمول)، بالإضافة إلى تفعيل المصادقة الثنائية عبر تطبيق جوجل أوثنتيكاتور (Google Authenticator)، وشددت على أهمية أن يكون الشخص شكاكا بشكل كبير، بحيث يفحص كل الروابط الواردة إليه عبر منصات التواصل الاجتماعي باستخدام موقع فايروس توتال Virustotal للتأكد من ما إذا كانت خبيثة أو آمنة، كما حذرت الأخصائية التقنية من تنزيل أي برنامج من موقع غير معروف، أو تثبيت تطبيقات معدلة كالواتس الذهبي وواتس عمر، لأن المحادثات ستمر عبر طرف ثالث، بالإضافة إلى التأكد من الأذونات المطلوبة عند تثبيت أي برنامج أو تطبيق، وفي حال كانت الأذونات المطلوبة غير مرتبطة بالغرض من التطبيق، فينبغي عدم تثبيته.

خاتمة

إن التهديدات والانتهاكات التي يتعرض لها مستخدمو الإنترنت في اليمن، آخذة في الازدياد، وهو ما يستدعي اتخاذ تدابير وقائية على كافة الصعد (تنظيمية، قانونية، تقنية، فنية... إلخ) كما أن تطور تكتيكات مجرمي الإنترنت، يحتم على المؤسسات والأفراد، مواكبة هذا التطور، واتباع أحدث إجراءات الحماية والأمان على الفضاء الرقمي.


سام
للحقوق والحريات

الأمن الرقمي
في اليمن..
الواقع والمهددات

ديسمبر
2022

violations@samrl.org
www.dg.samrl.org

Digital.Rights.Yemen
@SamDigitalRight

سام
للحقوق والحريات

www.samrl.org
info@samrl.org