المركز الوطني للأمن السيبراني

National Cyber Security Center

الموقف الأمني

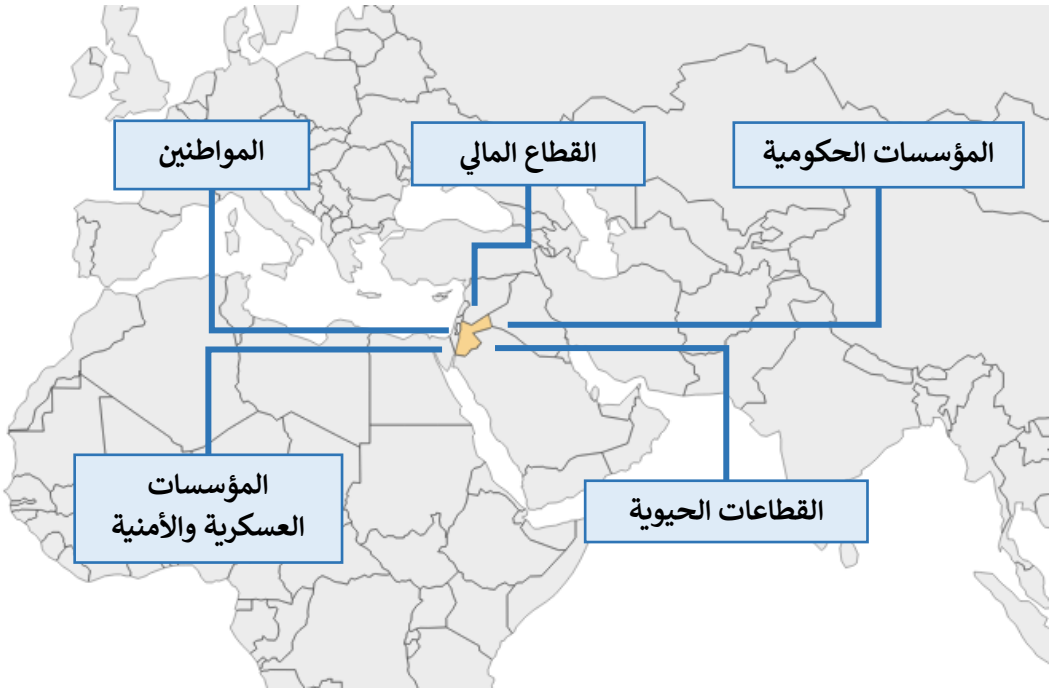
الربع الأول ٢٠٢٢

تصنيف الوثيقة: متاح

قائمة المحتويات

المقدمة

من خلال التقرير التالي يتم تسليط الضوء على حالة الأمن السيبراني على الصعيدين المحلي والدولي خلال الربع الأول من عام ٢٠٢٢، بالإضافة لاستعراض بعض الإحصائيات حول أبرز جهات التهديد نشاطاً وأكثر البرمجيات الخبيثة والثغرات الأمنية انتشاراً خلال الفترة المذكورة، والشكل التالي يبين أبرز الجهات الوطنية المتأثرة من الهجمات السيبرانية.



الشكل (١): أبرز الجهات الوطنية المتأثرة بالهجمات السيبرانية

الساحة المحلية

- ما زالت المؤسسات الحكومية على رأس الجهات المستهدفة من خلال الهجمات السيبرانية المرصودة ضمن مراكز الاستجابة لحوادث الأمن السيبراني في القطاعات الوطنية المختلفة، حيث تنشط في هذا النطاق مجموعات القرصنة المدعومة من الدول (State-Sponsored) والتي يكون الغاية من عملياتها السيبرانية الهجومية التجسس وسرقة المعلومات، ويتوقع أن تستمر هذه المجموعات في نشاطها خلال الفترة القادمة.
- فيما يخص القطاع المالي والخاص فإن الهجمات المرتبطة بالجرائم الإلكترونية مثل هجمات الفدية (Ransomware) ما زالت تمثل التهديد الأكبر لهذه المؤسسات، حيث يكون الدافع عادة وراء هذه الهجمات تحصيل الأموال من خلال ابتزاز المؤسسات المستهدفة لدفع الفدية المطلوب، أو بيع المعلومات التي يتم تحصيلها إلى جهات تهديد أخرى من خلال عرضها على المتاجر والمنتديات الخاصة بالجرائم الإلكترونية على الانترنت المظلم (Dark Web).

الساحة الدولية

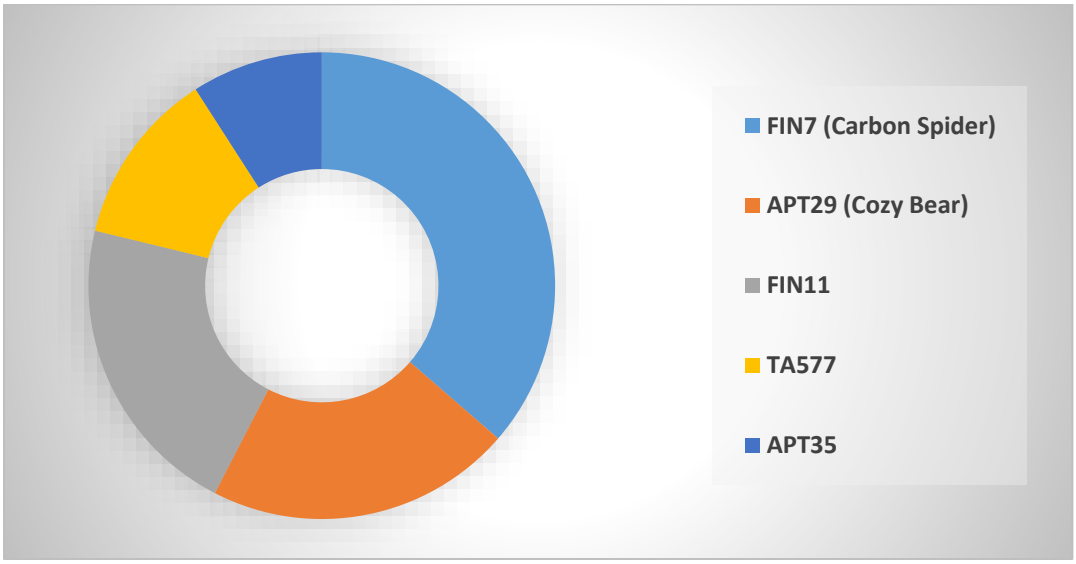
- رصدت مراكز الأبحاث والشركات العالمية المختصة في الأمن السيبراني ارتفاعاً كبيراً لوتيرة الهجمات السيبرانية التي تم التبليغ عنها أو تسجيلها ضد المؤسسات الأوكرانية المختلفة وذلك بالتزامن مع العملية العسكرية التي تشنها القوات الروسية ضد النظام الأوكراني منذ نهاية شهر شباط من هذا العام. ومن اللافت للنظر أن بعض هذه الهجمات حمل طابعاً تدميرياً وتخريبياً، حيث تم فيها استهداف الشبكات الحيوية الأوكرانية مثل بعض شركات الكهرباء ببرمجيات خبيثة تؤدي في حال تثبيتها إلى تعطيل الأجهزة المستهدفة بشكل كامل من خلال تشفير البيانات أو محوها بشكل غير قابل للاسترداد، مما قد يكون ذو عواقب وخيمة خصوصاً في حال استهداف أنظمة التحكم مثل نظام (SCADA).

- شهدت الأشهر الماضية ارتفاعاً ملحوظاً بهجمات الأمن السيبراني المرتبطة ببرامج الفدية المعقدة عالية التأثير ضد مؤسسات البنية التحتية الحرجة على مستوى العالم، حيث استهدفت هذه الهجمات قطاعات مختلفة مثل الرعاية الصحية والطبية والخدمات المالية والأسواق والتعليم العالي والبحث العلمي وقطاعات الطاقة والمرافق الحكومية. أظهرت جهات التهديد التي تقف وراء هذه الهجمات توجهات جديدة في طبيعة الهجوم، فعلى سبيل المثال ابتعد المهاجمون عن استهداف الشركات العملاقة واتجهوا نحو الضحايا من الحجم المتوسط للتقليل من عمليات التدقيق والتحري، كما استخدم المهاجمون أساليب مختلفة لابتزاز الأموال مثل التهديد بنشر البيانات المسروقة وإبلاغ عملاء الضحية.

- اجتذبت الثغرة الأمنية (Spring4Shell) والمرتبطة بإطار العمل (Spring) الخاص بلغة (Java) اهتمام الباحثين في مجال الأمن السيبراني، حيث أن هذا الإطار مفتوح المصدر مستخدم بكثرة في مجال تطوير التطبيقات والمواقع الإلكترونية. يمكن أن يؤدي استغلال هذه الثغرة الى تنفيذ أوامر بصلاحيات متقدمة في النظام المستهدف، وقد قام عدد من الشركات المصنعة للبرمجيات الحاسوبية بالإبلاغ عن تأثرها بهذه الثغرة، ومن المتوقع أن يتم الكشف عن المزيد من البرمجيات المتأثرة بهذه الثغرة الخطيرة التي اعتبرها عدد من الباحثين مقاربة في مستوى الخطورة لثغرة (Log4Shell) البرمجية التي تم اكتشافها نهاية العام الماضي.

جهات التهديد

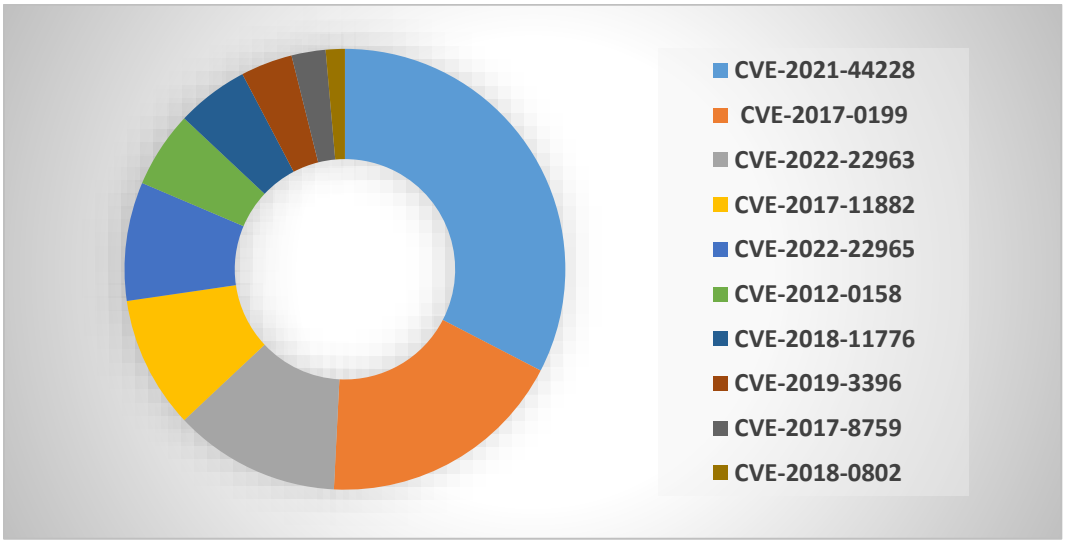
تصدرت مجموعة القرصنة المدعوة باسم (FIN7) والتي يطلق عليها أيضاً (Carbon Spider) أكثر مجموعات القرصنة نشاطاً على الساحة الدولية خلال الربع الأول من هذا العام. يعتبر الدافع الرئيسي وراء عمليات القرصنة التي تقوم بها هذه المجموعة هو الدافع المادي، حيث أنها تقوم باستهداف المؤسسات المختلفة بهدف تشفير وسرقة البيانات الخاصة بهذه المؤسسات من خلال برمجية (Carbanak) الخبيثة والمرتبطة ارتباطاً وثيقاً بهذه المجموعة. قامت المجموعة مؤخراً بتطوير برمجيات خبيثة تقوم باستهداف نقاط البيع (POS) وسرقة البيانات المالية المخزنة عليها، والشكل رقم (٢) بين أكثر مجموعات القرصنة نشاطاً على الساحة العالمية خلال الربع الأول من هذا العام.



الشكل (٢): أكثر مجموعات القرصنة نشاطاً على المستوى العالمي خلال الربع الأول من عام ٢٠٢٢

الثغرات الأمنية

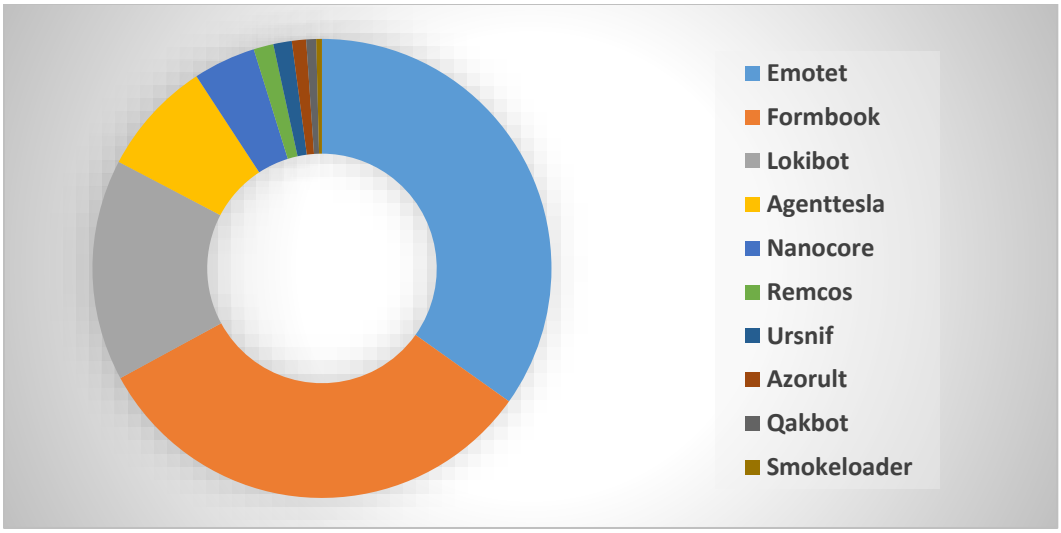
تصدرت الثغرة الأمنية رقم (CVE-2021-44228) والتي تم اكتشافها نهاية العام الماضي وأطلق عليها الباحثون اسم (Log4Shell) أكثر الثغرات البرمجية استهدافاً خلال الربع الأول من هذا العام. يعتبر تصنيف هذه الثغرة على أنها شديدة الخطورة حيث أنه يمكن استغلالها بسهولة من قبل جهات التهديد وهي ترتبط ببرمجية (Apache Log4j) المنتشرة في العديد من التطبيقات والأنظمة المختلفة، والشكل رقم (٣) يبين أكثر الثغرات البرمجية استغلالاً على المستوى العالمي خلال الربع الأول من عام ٢٠٢٢.



الشكل (٣): أكثر الثغرات الأمنية استهدافاً على المستوى العالمي خلال الربع الأول من عام ٢٠٢٢

البرمجيات الخبيثة

احتلت برمجية (Emotet) الخبيثة أكثر البرمجيات الخبيثة انتشاراً على المستوى العالمي خلال الربع الأول من هذا العام. هذه البرمجية المكتوبة بلغة (C/C++) تتصل بخادم السيطرة (C&C) من خلال بروتوكول (HTTP) وتتميز بأنها لا تقوم بكتابة أي بيانات على الجهاز المصاب (File-less Malware) وإنما تقوم بتنفيذ أوامرها في الذاكرة المؤقتة (RAM) مما يساعدها على تفادي أنظمة الحماية الموجودة على الجهاز وتثبيت برمجيات لاحقة تقوم بسرقة البيانات وكلمات السر من الجهاز المصاب وتمكين المهاجم من الانتقال لباقي الأجهزة في الشبكة، والشكل رقم (٤) يبين أكثر البرامج الخبيثة انتشاراً على المستوى العالمي خلال الربع الأول من هذا العام.



الشكل (٤): أكثر البرمجيات الخبيثة انتشاراً على المستوى العالمي خلال الربع الأول من عام ٢٠٢٢

التوقعات المستقبلية

ما زال زخم الهجمات السيبرانية الناتج عن الأزمة الروسية – الأوكرانية محصوراً بشكل رئيسي بين هاتين الدولتين خصوصاً بعض الهجمات السيبرانية التدميرية التي يكون الغرض منها الإضرار بالقطاعات الحيوية كشبكات الكهرباء والاتصالات المحلية، إلا أنه لا يستبعد أن تكون بعض الدول في مرمى نيران هذه الهجمات في المرحلة المقبلة، خصوصاً في حال دخول هذه الدول على خط هذه الأزمة والتأثير فيها لصالح أحد الأطراف سواءً من الناحية السياسية أو الاقتصادية.

إن الثغرات الأمنية التي ظهرت في الأشهر القليلة الماضية ضمن بعض البرمجيات المستخدمة بكثرة في الأنظمة والتطبيقات المختلفة مثل برمجية (Java) و (Apache) أظهرت خطورة هجمات سلاسل التوريد والتي لا تستهدف منتج بعينه وإنما برمجية مدمجة في هذا المنتج وفي العديد من الأنظمة الأخرى، ويعتقد أن يزيد تركيز جهات التهديد على مثل هذا النوع من الهجمات السيبرانية خلال الفترة القادمة.