المركـز الوطنـــي
للأمـن السيبرانـي
National Cyber
Security Center

تقرير المـوقف الأمـني السـيبراني
Cyber Threat Situational Report

الربع الثاني 2024

المركز الوطني للأمن السيبراني
Info@ncsc.jo +(962) 65 900 501 +(962) 5 900 500

الملخص التنفيذي

كانت التهديدات المتعلقة بسرقة بيانات الدخول تمثل النشاط الأكثر انتشارا والذي استهدف العديد من القطاعات في منطقة الشرق الأوسط. ما تزال برمجيات سرقة المعلومات "Info stealers" الوسيلة الفعالة وبشكل متزايد لجمع بيانات الدخول في المؤسسات الوطنية، حيث بلغت الزيادة في الحسابات المسروقة 39% مقارنة بالربع الثاني من العام الماضي. غالبا ما يتم استخدام بيانات الدخول المسروقة من قبل المهاجمين في بداية الهجوم السيبراني. يعد استخدام آلية المصادقة المتعددة (MFA) هو الخيار الأفضل للوقاية والحد من خطورة الحوادث السيبرانية الناشئة من حوادث تسريب او سرقة بيانات الدخول.

استهدفت مجموعات التهديد المتطورة ومجموعات القرصنة أهدافا تتماشى مع الأغراض الاستخبارية والايدولوجيات السياسية او الدينية لديها. على سبيل المثال العديد من الحوادث السيبرانية في المنطقة نشأت بسبب الحرب على قطاع غزة والظروف السياسية في المنطقة، ومن المرجح أن تستمر هذه الحوادث في المستقبل المنظور مادامت هذه الحرب مستمرة.

كانت عمليات التأثير الإعلامي (Influence Operations) هي السمة السائدة لأنشطة جهات التهديد وذلك نتيجة للأحداث الجيوسياسية الجارية. تضمنت تلك العمليات حملات تضليل اعلامي واستخدام وتوظيف لتقنيات الذكاء الاصطناعي لنشر معلومات مغلوطة او المبالغة في طريقة عرض المعلومات. بالرغم من محدودية عدد الحوادث السيبرانية التي نتجت بسبب تلك الظروف والاحداث، يعتقد أن عمليات التأثير الإعلامي يمكن ان يكون لها العديد من الآثار السلبية مثل التلاعب بالرأي العام وفقد الثقة لديه، ونشر الخوف بين المواطنين، أو الإضرار بالسمعة، أو التأثير في عملية تنفيذ السياسات والأنظمة.

خلال الربع الثاني تم رصد بعض الحوادث المحلية التي قد تعود لمجموعات التهديد المتطورة وتشير الأدلة الى ان الغرض الأساسي من هذه العمليات محاولة الوصول بشكل دائم للأنظمة وجمع المعلومات. كما تم رصد بعض الحوادث من قبل مجموعات القرصنة وكان السبب الرئيسي لتلك الحوادث وجود ثغرات أمنية للأنظمة المستهدفة.

أبرز الأنشطة والمؤشرات المحلية

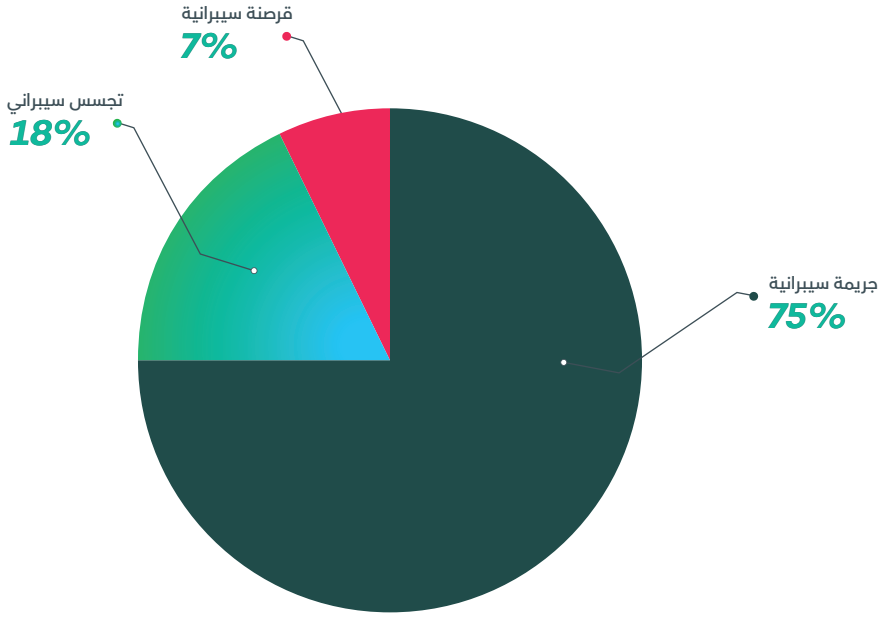
- رصد عدد من الحوادث الوطنية يعتقد أنها من قبل مجموعات تهديد متطورة بغرض جمع المعلومات.
- غالبية الأنظمة التي تحتوي ثغرات خطيرة/حرجة هي أنظمة وبرمجيات غير محدثة او خارجة عن الدعم.
- الكشف عن (6) حوادث لتغيير محتوى المواقع الإلكترونية للمؤسسات الأردنية.
- الحوادث السيبرانية المرتبطة بمجموعات القرصنة (Hacktivists) كانت الاكثر رصدا خلال الربع الثاني.
- تم رصد بيانات دخول مسربة لحسابات تابعة لمؤسسات أردنية.
- أكثر الأنظمة انتشارا على المستوى الوطني وتحتوي ثغرات عالية الخطورة هي: Apache HTTP Server, Nginx, PHP.
- تعد أساليب ووسائل الهندسة الاجتماعية من أكثر الوسائل استخداماً من قبل جهات التهديد المختلفة.
- أبرز سمات حملات التأثير والتضليل الإعلامي هي استخدام تقنيات الذكاء الاصطناعي بغرض نشر معلومات مغلوطة او مبالغ فيها عبر وسائط التواصل الاجتماعي المختلفة.
- أكثر التكتيكات والأساليب استخداماً من قبل المهاجمين هي: سرقة البيانات، تعطيل الأنظمة والخدمات، عمليات الاستكشاف للأنظمة الداخلية وهجمات تشفير البيانات (هجمات الفدية).

احصائيات الحوادث التي تعرضت لها الشبكات الحكومية والوطنية

بلغ عدد الحوادث السيبرانية التي تعامل معها المركز خلال الربع الثاني من العام 2024 (1582) حادثة استهدفت عدد من الوزارات والمؤسسات الحكومية بالإضافة لعدد من المؤسسات الحيوية.

لوحظ انخفاض في عدد الحوادث السيبرانية المكتشفة بنسبة بلغت 23% مقارنة بالربع الأول من هذا العام. من الممكن أن يرجع السبب في ذلك الى زيادة التزام المؤسسات بتطبيق السياسات والتدابير الأمنية، الا ان الاتجاه العام للحوادث لا زال مرتفعاً مقارنة بالسنوات السابقة بالرغم من انخفاضه مقارنه مع الربع الفائت. .

توزعت أهداف الحوادث السيبرانية على النحو التالي:

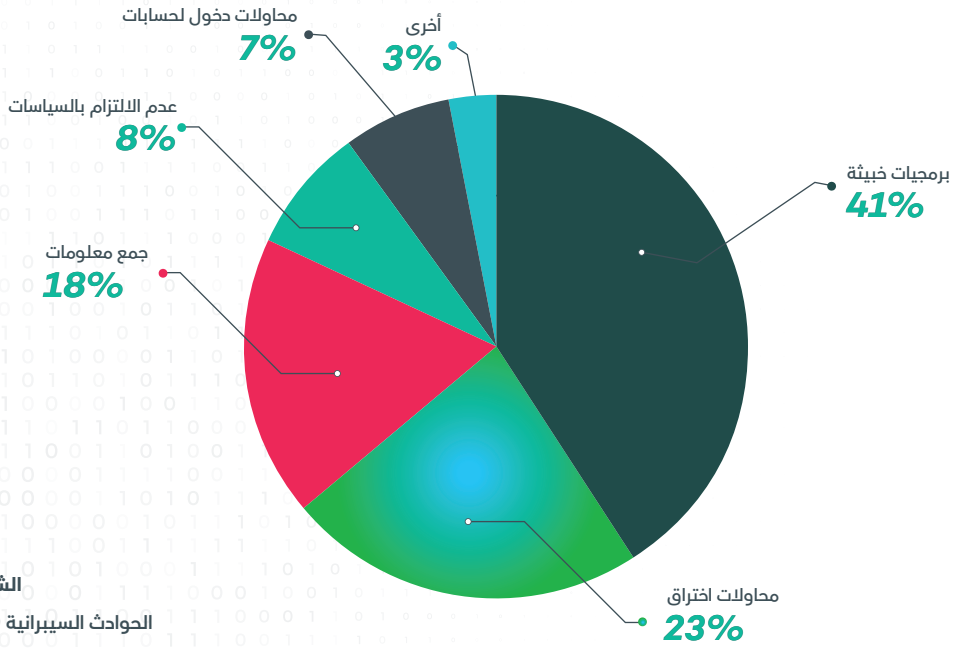


الشكل رقم(1):
توزيع الحوادث السيبرانية (حسب الأهداف)

الجريمة السيبرانية

يشير مصطلح الجرائم السيبرانية إلى الأفعال غير القانونية التي يتم ارتكابها باستخدام أجهزة الكمبيوتر أو الإنترنت مثل سرقة البيانات، المطالبة بدفع المال، تثبيت برمجيات خبيثة واختراق الأجهزة بشكل عام.

ويوضح الرسم التالي توزيع الحوادث السيبرانية حسب نوعها:



الشكل رقم(2):
الحوادث السيبرانية (حسب النوع)

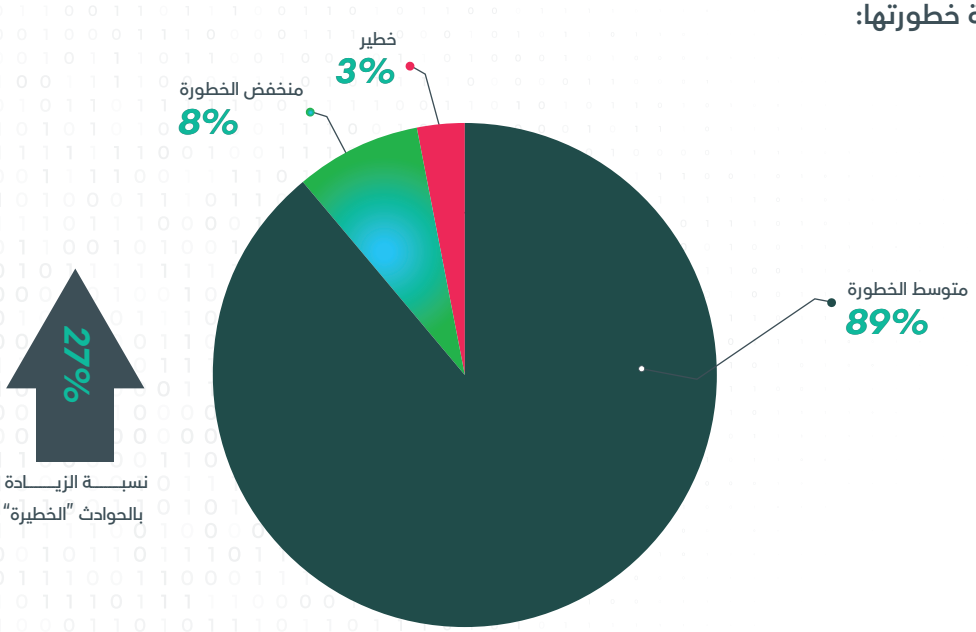
كما هو مبين ما تزال غالبية الحوادث المرصودة تعود للإصابة ببرمجيات خبيثة بنسبة ثابتة مقارنة بالربع الأول من هذا العام. تعمل مجموعات التهديد باستمرار على تطوير برمجيات خبيثة يمكن استخدامها لسرقة البيانات أو تجاوز ضوابط الحماية بهدف إلحاق الضرر بجهاز مستهدف أو بياناته أو تطبيقاته. هناك عدة طرق شائعة يمكن من خلالها الإصابة بالبرمجيات الخبيثة، ومعرفة طرق الاصابة تساعد في اتخاذ تدابير وقائية ضد التهديدات المحتملة.
فيما يلي بعض الطرق الأكثر شيوعًا للإصابة بالبرمجيات الخبيثة:

1. رسائل البريد الإلكتروني التي تحتوي على روابط أو مرفقات ضارة
2. محركات الأقراص القابلة للإزالة المصابة ببرمجية خبيثة، مثل محركات أقراص فلاش USB
3. الثغرات الامنية في البرامج أو أنظمة التشغيل
4. تنزيل البرمجيات الخبيثة دون موافقة المستخدم أو علمه عند زيارة موقع ويب مخترق أو الضغط على إعلانات خادعة
5. اختراق مواقع الويب المشروعة لتثبيت البرمجيات الخبيثة عند زيارة الموقع

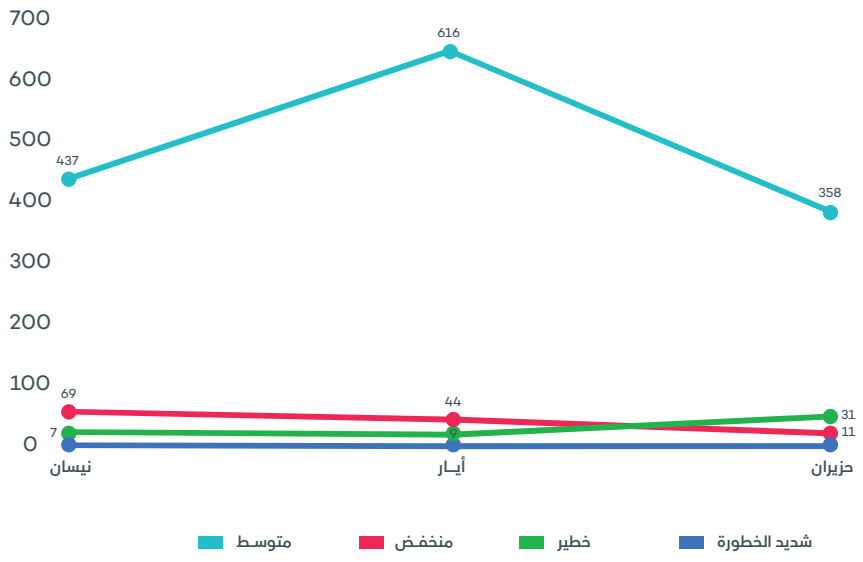
41%
برمجيات خبيثة

للوقاية من الإصابة من البرمجيات الخبيثة ينصح بتطبيق ممارسات الأمن السيبراني الفضلى، مثل توخي الحذر من رسائل البريد الإلكتروني والمرفقات، التأكد من تحديث البرامج بانتظام، استخدام الحلول الموثوقة لمكافحة الفيروسات، الاحتفاظ بنسخ احتياطية للبيانات الحساسة، تنزيل الملفات والتطبيقات فقط من مصادر موثوقة، استخدام جدران الحماية، استخدام كلمات مرور قوية ومعقدة، مراقبة حركة مرور الشبكة بانتظام بحثًا عن أي نشاط مشبوه، واعطاء صلاحيات للمستخدم حسب الحاجة.

لم يتم تسجيل أية حوادث "شديدة الخطورة" وغالبية الحوادث المرصودة "متوسطة الخطورة" كما لوحظ ارتفاع في الحوادث المصنفة بـ "خطير" بنسبة تقارب 27% مقارنة بالربع الاول من هذا العام. يمكن الاطلاع على "تعليمات تصنيف حوادث الامن السيبراني" لمزيد من التفاصيل حول هذه التصنيفات.
تالياً تصنيف الحوادث من حيث درجة خطورتها:



الشكل رقم(3):
تصنيف الحوادث (حسب درجة الخطورة)



الشكل رقم(4):

توزيع الحوادث السيبرانية حسب درجة الخطورة خلال الربع الثاني/٢٠٢٤

أبرز ما تشير اليه بيانات الحوادث السيبرانية:

43%

من المؤسسات رصدت لديها حوادث

عدم الالتزام بالسياسات

السياسات الأمنية تشمل مجالات عدة مثل التحكم في امكانية الوصول لأصول المؤسسة، وعمليات المصادقة (Authentication)، والتشفير، وإجراءات النسخ الاحتياطي للبيانات، وإدارة تحديث الأنظمة والبرمجيات. يمكن أن تحدث هذه الحوادث نتيجة لهجمات خبيثة، أو أخطاء بشرية، أو إهمال. لوحظ انخفاض بنسبة تُقارب 21% في عدد حوادث "عدم الالتزام بالسياسات" الامر الذي قد يكون أحد الأسباب التي أدت للانخفاض في عدد الحوادث الإجمالي.

74%

من المؤسسات رصدت لديها حوادث

محاولات اختراق

تحدث هذه الحوادث عندما يحاول أحد المهاجمين الوصول إلى أحد الأنظمة من خلال استغلال ثغرة أمنية أو خطأ أمني دون تصريح. يتم الكشف عن هذه الثغرات بشكل عام. قد لا يتم اصدار حزم التصحيح لتلك الثغرات مباشرة الامر الذي يؤدي لاستغلالها قبل تطبيق تلك التصحيحات.

69%

من المؤسسات رصدت لديها حوادث

جمع معلومات

تهدف هذه العملية لجمع معلومات تقنية للمؤسسة المستهدفة بهدف الكشف عن نقاط الضعف المحتملة للمساعدة في التخطيط لتنفيذ العمليات السيبرانية في المستقبل.

كما بلغ عدد عمليات الاستجابة الميدانية التي قام بها فريق الاستجابة للحوادث السيبرانية (46)، قام خلالها فريق التحقيقات الرقمية بإجراء (15) عملية تحليل رقمي للأدلة المرتبطة بهذه الحوادث.

46
عملية إستجابة

15
عملية تحليل رقمي

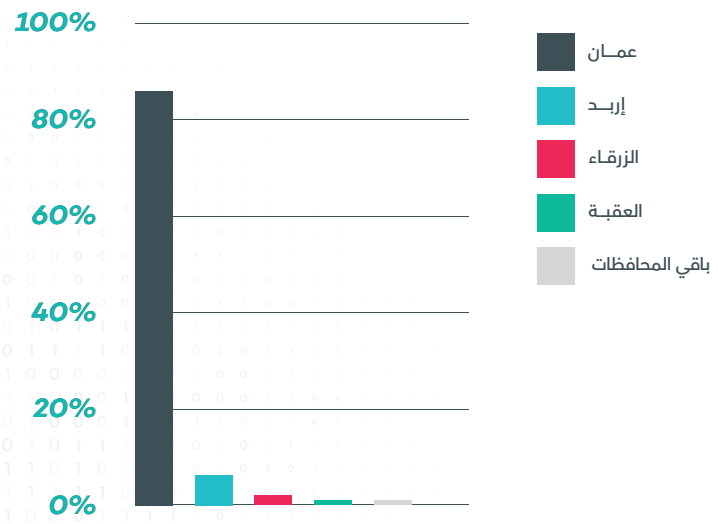
واجهة التهديدات السيبرانية الوطنية

تشكل واجهة التهديدات مجموعة من العوامل التي تعد مصدراً للتهديدات السيبرانية ويمكن استغلالها من قبل المهاجمين لتنفيذ عملياتهم المختلفة. تساعد هذه المعلومات في التصدي للهجمات السيبرانية المختلفة من خلال عرض لأبرز الأخطاء أو الثغرات المكتشفة خلال الربع الثاني. تجدر الإشارة الى أنه من الممكن الحد وتجنب هذه المخاطر باتباع وتنفيذ إجراءات الحماية بشكل روتيني ومنتظم.

بلغ العدد الإجمالي للأصول الرقمية للمؤسسات على المستوى الوطني: 43,580 احتوى منها ما نسبته 1.1% على ثغرات خطيرة.

توزعت أصول المؤسسات على النحو التالي:

الأصول الرقمية
تعرف الأصول الرقمية بأنها مجموع البيانات والأجهزة وأنظمة المعلومات التي تمكن المؤسسة من تحقيق أهداف للعمل.



الشكل رقم(5):
توزيع الأصول الرقمية للمؤسسات على المحافظات

43580
أصول رقمية

1.1%
نسبة الأصول الرقمية
ذات الثغرات الخطيرة

كما تم رصد العديد من الخدمات الإلكترونية على المستوى الوطني التي تستخدم بروتوكولات غير آمنة (يتم نقل البيانات بشكل غير مشفر) بلغت نسبتها 33% من اجمالي الخدمات.

33%
الخدمات غير الآمنة

فيما يلي أكثر الأنظمة انتشارا على المستوى الوطني وتحتوي ثغرات عالية الخطورة وحرجة، والتي يجب على المؤسسات الوطنية معالجتها بشكل فوري:

- Apache HTTP Server
- Nginx
- PHP
- OpenSSH
- Microsoft Exchange

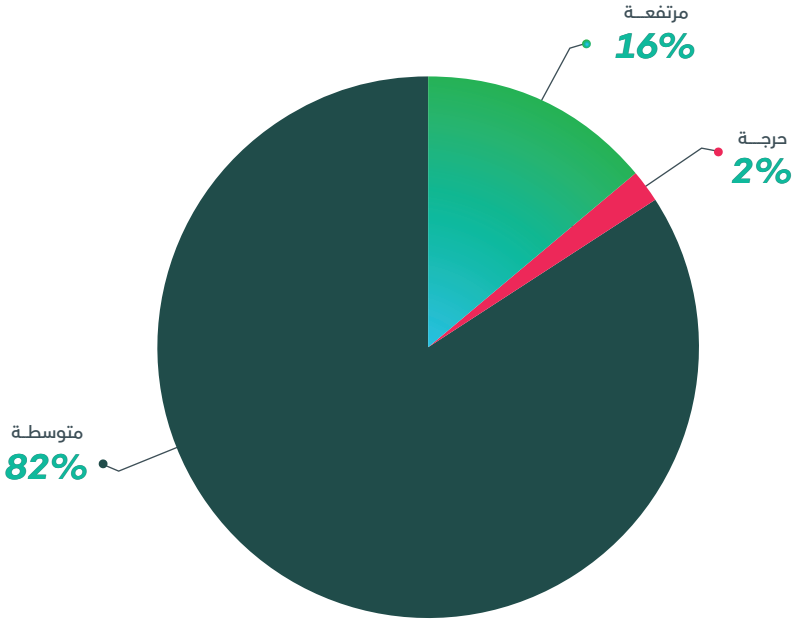
فيما يلي أهم الثغرات الحرجة والجديدة التي تم رصدها وترتبط بتقنيات وبرمجيات تستخدم في المؤسسات الوطنية وتم الكشف عن عملية استغلال واسعة النطاق لتلك الثغرات على مستوى العالم:

الخطورة	النظام المتأثر	رمز الثغرة
تمكن المهاجم من تنفيذ أوامر وتعليمات بصلاحيات عالية	(pan-os (Palo Alto	3400-CVE-2024
يمنح المهاجم إمكانية تنفيذ التعليمات البرمجية عن بعد	Google Chrome	4671-CVE-2024
تمكن المهاجم من تنفيذ أوامر وتعليمات بصلاحيات عالية	(MS Windows (10, 11, Server	30051-CVE-2024
تسمح للمهاجم بتجاوز أحد مزايا الحماية في منتجات Office وتنفيذ أوامر	(MS Windows (10, 11, Server	30040-CVE-2024

من الملاحظ أن المنتجات الخاصة بشركة "Microsoft" تعد الأكثر عرضة لعمليات الاستغلال والذي يمكن أن يعزى لكون منتجاتها هي الأكثر استخداما وانتشارا مثل أنظمة التشغيل ويندوز والمجموعة المكتبية اوفيس. غالبا ما يتم استغلال تلك الثغرات في بداية عملية الاختراق او في تنفيذ بعض العمليات الخبيثة الاخرى مثل تثبيت برمجيات خبيثة وجمع المعلومات.

احصائيات فحوصات الثغرات والاختراق

تم إجراء فحوصات لكشف الثغرات على عدد من المواقع الإلكترونية الوطنية بمتوسط بلغ (42) موقع الكتروني في كل شهر وبلغ متوسط عدد الثغرات الأمنية التي تم ايجادها (838) ثغرة ومتوسط عدد المؤسسات (36) مؤسسة في كل شهر.
تم اعلام المؤسسات بهذه الثغرات وضرورة معالجتها بأسرع وقت.
الرسم التالي يبين نتائج فحوصات الثغرات للمواقع الرئيسية للمؤسسات الحكومية وعددها 115 مؤسسة:



الشكل رقم(6):
تصنيف الثغرات الأمنية للمواقع الرئيسية للمؤسسات الحكومية

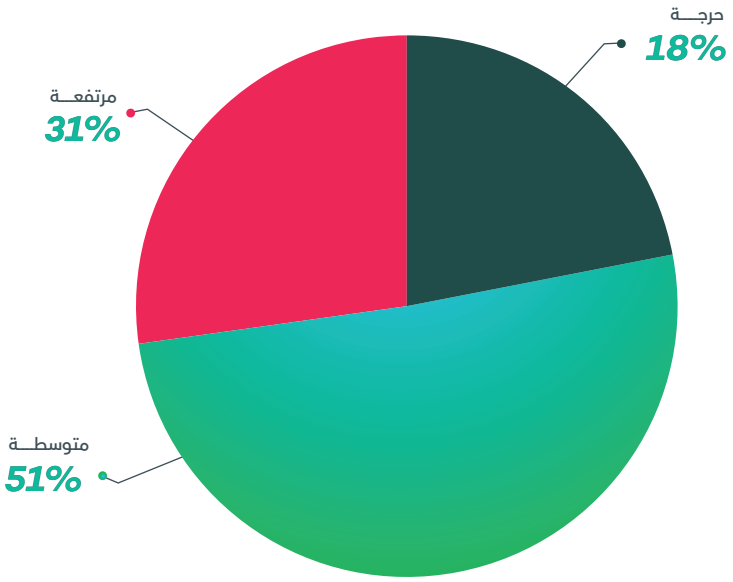
8%
من المؤسسات رصدت لديها ثغرات
حرجة

40%
من المؤسسات رصدت لديها ثغرات
مرتفعة الخطورة

تم إجراء فحوصات لكشف الثغرات في الخوادم في (44) مؤسسة حكومية في الربع الثاني. بلغ متوسط عدد الثغرات الأمنية التي تم ايجادها (840) ثغرة في كل شهر ومتوسط عدد المؤسسات (38) مؤسسة ومتوسط عدد الخوادم التي تم فحصها (3752) خادم، شهرياً خلال الربع الثاني. من الملاحظ أن غالبية الأنظمة التي تحتوي ثغرات حرجة هي أنظمة وبرمجيات غير محدثة او خارجة عن الدعم.

> 90%
من الثغرات الحرجة لانظمة وبرمجيات غير محدثة او منتهية الدعم

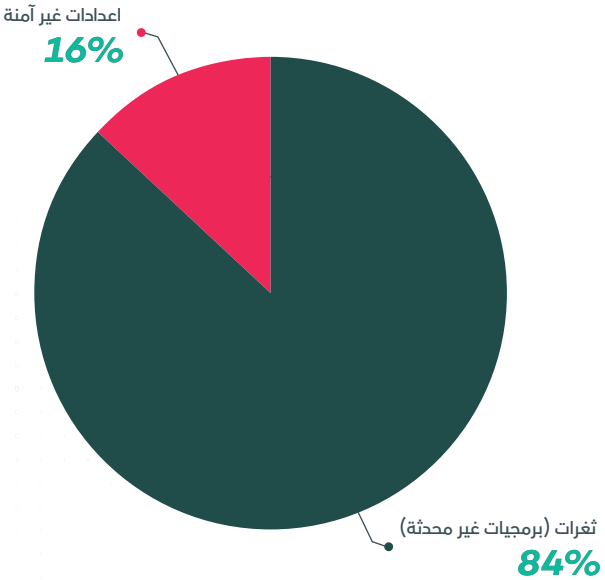
وبلغ العدد الاجمالي لفحوصات الاختراق (Penetration Testing) المنفذة (43) فحص شملت فحص المواقع والخدمات الالكترونية. بلغ مجموع الثغرات التي تم ايجادها (271) ثغرة توزعت على النحو التالي:



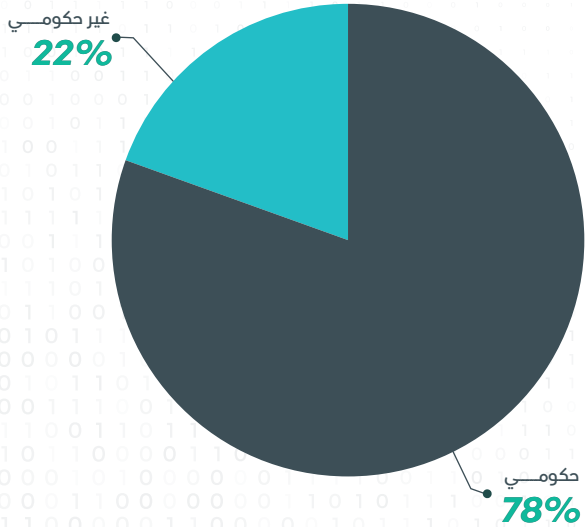
الشكل رقم(7):
تصنيف الثغرات المكتشفة من فحوصات الاختراق

نقاط الضعف المرصودة في عدد من المؤسسات الحكومية:

تم رصد عدد (49) من نقاط الضعف المختلفة في عدد من المؤسسات الحكومية. الرسوم التالية توضح التصنيفات الرئيسية لنقاط الضعف المكتشفة وتوزيع نقاط الضعف المكتشفة حسب القطاع.



الشكل رقم(8):
تصنيف نقاط الضعف المكتشفة



الشكل رقم(9):
توزيع نقاط الضعف المكتشفة (حسب القطاع)

فيما يلي قائمة بالأنظمة التي تحتوي نقاط ضعف "حرجـة":

النظام
PHP
Microsoft Exchange Server
Apache Tomcat Server
Apache HTTP Server
Palo Alto Networks PAN-OS software
WordPress
OpenSSH

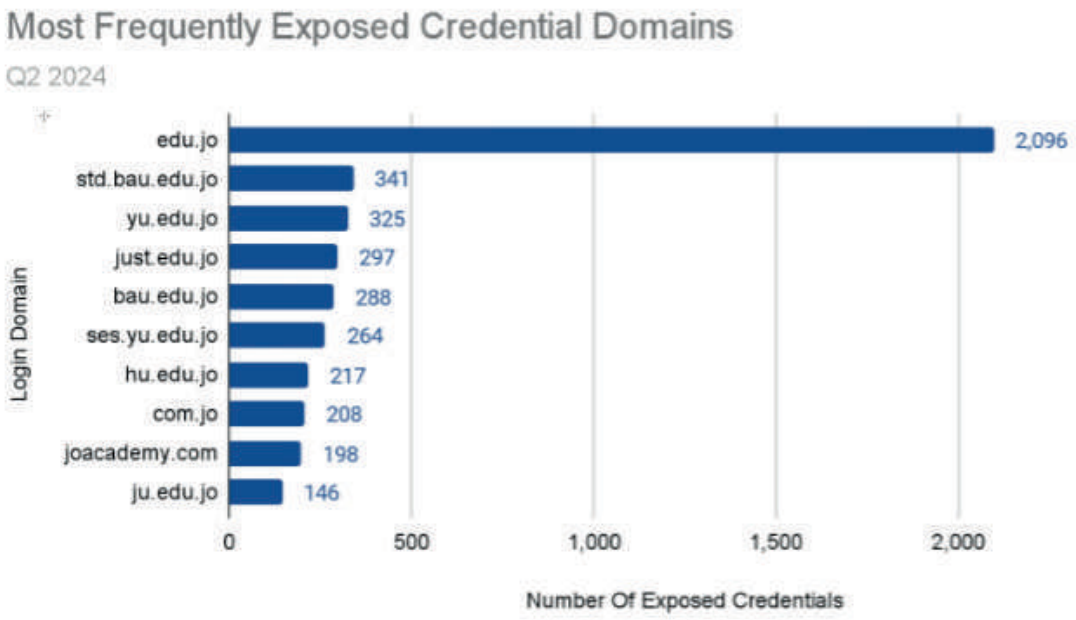
البيانات المكشوفة

تم الكشف عن وجود بعض الملفات التي تحوي معلومات فنية خاصة بالعمل مكشوفة على شبكة الانترنت. يتم كشف تلك البيانات عادة نتيجة لخطأ في الاعدادات الأمنية تسمح بالكشف عنها او لعدم تطبيق أفضل الممارسات الأمنية من قبل المبرمجين والفنيين. من الممكن ان يتم استغلال تلك البيانات من قبل القراصنة وجهات التهديد المختلفة في التخطيط لشن هجمات سيبرانية.

الحسابات المسربة

تم رصد العديد من بيانات الدخول (Credentials) لحسابات تابعة لمؤسسات أردنية. غالبا ما يتم سرقة بيانات الدخول من خلال برمجيات سرقة المعلومات (Info Stealer) وتتم الإصابة بهذه البرمجيات من خلال استخدام برمجيات غير مرخصة او من خلال تصفح المواقع غير الموثوقة. تهدف تلك البرمجيات بشكل رئيسي لجمع بيانات الدخول للمواقع الإلكترونية المحفوظة في متصفحات الانترنت في الحواسيب والأجهزة الذكية. يتم عرض البيانات المسروقة على المواقع والمنتديات الخاصة المتداولة بين المهاجمين والتي يمكن أن يتم استخدامها في عملية اختراق أنظمة المؤسسة المستهدفة. يجب على مسؤولي الأنظمة تغيير بيانات الدخول المسربة وفحص لشبكة المؤسسة للتأكد من خلوها من أية برمجيات خبيثة. اضافة لأهمية الالتزام بتطبيق ممارسات آمنة لبيانات الدخول، يبقى استخدام طرق المصادقة متعددة العوامل MFA من أفضل الطرق للحد من خطورة بيانات الدخول المكشوفة او المسربة.

الرسم التالي يبين أكثر النطاقات المرتبطة ببيانات الدخول المسربة، حيث يظهر النطاق الأكاديمي كأكثر النطاقات الوطنية التي تعرضت لتسريب بيانات المستخدمين:



الشكل رقم(10):

المواقع المرتبطة بالبيانات المسربة

المؤشرات الإقليمية والعالمية

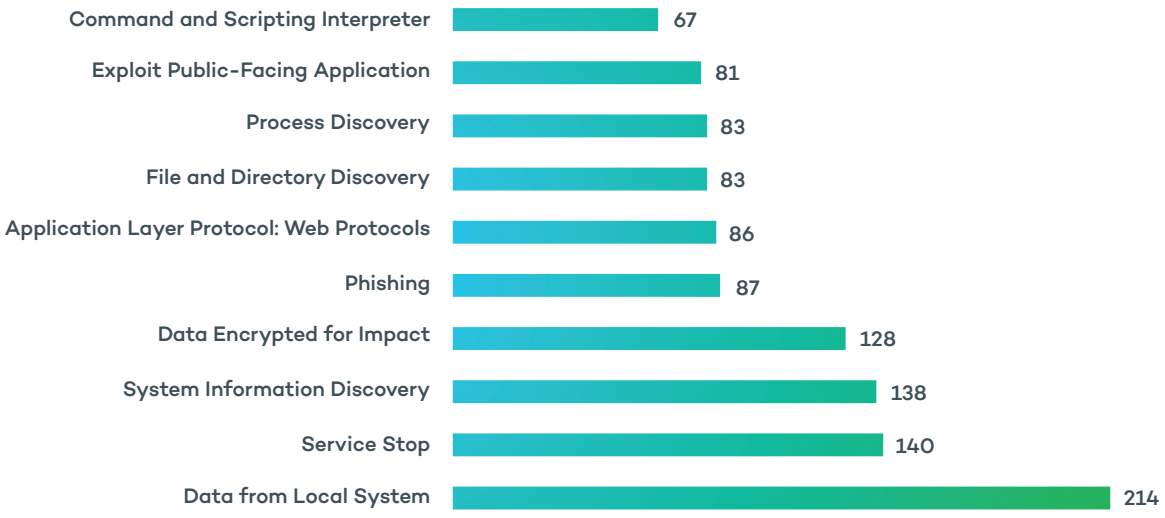
تمثل عملية متابعة ومراقبة التغيرات في بيئة التهديدات السيبرانية تحديًا هائلاً نظرا للعديد من العوامل التي تؤثر في الدوافع لتنفيذ الهجمات السيبرانية المختلفة. يعد الحرص على تطبيق الآليات وتقنيات الحماية الفعالة من الهجمات السيبرانية القائمة على مبادئ الأمن السيبراني الأساسية سببا رئيسيا للتخفيف من مخاطر تلك التهديدات.

أشارت بعض التقارير المتخصصة الى ان المخاطر المرتبطة بهجمات التصيد الإلكتروني غالبا ما تؤدي الى تحمل الجهات المستهدفة تكاليف مالية ضخمة للتعامل مع الأضرار الناجمة التي تنشأ نتيجة للتعطل في أعقاب الهجوم ويتعين على المؤسسات تخصيص جزء من الموارد المالية لتحديد المتطلبات التنظيمية وعملية الاستشارة والاستعانة بالخبراء الخارجيين.

أبرز التكتيكات المستخدمة من قبل جهات التهديد المختلفة هي:

1. سرقة البيانات
2. تعطيل الخدمة
3. جمع المعلومات
4. تشفير البيانات

الرسم التالي يوضح أكثر التكتيكات المستخدمة من قبل المهاجمين خلال الربع الماضي:



الشكل رقم(11):
أكثر التكتيكات المستخدمة من قبل المهاجمين

أهم الحوادث السيبرانية

ما تزال أساليب ووسائل الهندسة الاجتماعية من أبرز الطرق وأكثرها شيوعا التي تستخدم من قبل المهاجمين في عملية الوصول الأولي للمؤسسات المستهدفة حيث يستخدم المهاجم البريد التصيدي الذي يتضمن موضوعات ذات علاقة بالجهة المستهدفة. كان الهدف الأساسي لغالبية الهجمات المرصودة هو التجسس وجمع المعلومات أو لتثبيت برمجية خفية. بعض الهجمات كانت تهدف لإلحاق اضرار بالغة او تدمير الأنظمة المستهدفة وأخرى كانت بغرض دعم ايدولوجيات وتوجهات معينة قد ترتبط بأسباب تتعلق بالأحداث الجارية في المنطقة. أكثر المؤسسات التي تعرضت لتلك الحوادث كانت تتبع لقطاعات حساسة وحيوية مثل القطاع الحكومي، المالي، القانوني، وقطاع تكنولوجيا المعلومات وذلك نظرا لطبيعة المعلومات التي تمتلكها تلك المؤسسات.

رصدت احدى شركات الامن السيبراني انشاء منصة جديدة تُستخدم للتصيد الاحتيالي كخدمة (PHaaS) بغرض استهداف إحدى المؤسسات المالية من خلال سرقة حسابات المؤسسة على منصة الاوفيس السحابية التابعة شركة Microsoft. انتحلت حملة التصيد التي تم اطلاقها باستخدام تلك المنصة صفة دائرة الموارد البشرية للمؤسسة وتضمنت ارسال بريد الكتروني يحتوي على ملفات PDF تضمنت اكواد الاستجابة السريعة QR. بمجرد مسح تلك الأكواد يتم تحويل الضحية لصفحة احتيالية شبيهه بصفحة الدخول الى حسابات اوفيس السحابية.

كشف باحثون عن حملة سميت بـ"DuneQuixote" استهدفت مؤسسات حكومية في المنطقة من قبل مجموعة تهديد متطورة. البرمجية الخبيثة المستخدمة في الحملة كانت تحاكي احدى البرمجيات الشرعية وتستخدم تقنيات متقدمة لتجنب الاكتشاف. الغرض الرئيسي من البرمجية هو تمكين المهاجم من تنفيذ أوامر على جهاز الضحية.

عمليات التأثير الإعلامي Influence Operations

كانت عمليات التأثير الإعلامي التي تهدف الى احداث تغيير بالرأي العام السمة السائدة لأنشطة جهات التهديد وذلك نتيجة للأحداث الجيوسياسية خلال الربع الثاني. تتضمن تلك العمليات تنفيذ حملات تضليل اعلامي واستخدام لتقنيات الذكاء الاصطناعي لنشر معلومات مغلوطة او المبالغة في طريقة عرض المعلومات. على الرغم من محدودية عدد الحوادث السيبرانية التي نتجت من هذه العمليات، يعتقد أنه يمكن ان يكون لها العديد من الآثار السلبية مثل التلاعب بالرأي العام وفقد الثقة لديه، ونشر الخوف بين المواطنين، أو الإضرار بالسمعة، أو التأثير في عملية تنفيذ السياسات او اتباع الأنظمة. تجدر الإشارة الى أن شركة OpenAI كشفت عن قيامها بتعطيل عمليات التأثير والتلاعب التي تستخدم نماذج الذكاء الاصطناعي الخاصة بها. حيث قامت الشركة باكتشاف خمس عمليات بغرض التأثير بالرأي العام وقامت بإيقاف مجموعة من الحسابات المرتبطة بتلك العمليات.

مجموعات القرصنة (Hacktivism)

تم رصد عدد من العمليات السيبرانية المرتبطة بهذه المجموعات والتي كانت تهدف بشكل رئيسي لتسريب بيانات ودعم أحد طرفي النزاع في الصراعات الدائرة على المستوى الإقليمي والعالمي. استهدفت احدى المجموعات أنظمة التكنولوجيا التشغيلية المطورة من قبل الشركات التالية: Schneider, Unitronics, Siemens.. كما تضمنت العديد من تلك الهجمات تشهير بالمؤسسات المستهدفة وادعاء الوصول لبيانات حساسة دون وجود أدلة. وتم رصد بعض الهجمات الأخرى مثل حجب الخدمة، تشويه المحتوى للموقع الإلكتروني، تسريب بيانات حساسة بالإضافة لعمليات تعطيل لأنظمة التكنولوجيا التشغيلية (ICS). احدى المجموعات نفذت هجوما واسع النطاق استهدف مواقع إلكترونية وأنظمة حساسة وخوادم البريد الإلكتروني وخوادم نقل الملفات لمؤسستين حيوتين في المنطقة.

هجمات برمجيات الفدية

أبرز مجموعات برمجيات الفدية التي استهدفت منطقة الشرق الأوسط خلال الربع الماضي هي: LockBit Gang, Daixin Team, and Stormous. أبرز هجمات الفدية التي رصدت استهدفت احدى المدن الرئيسية في المنطقة وأدت الى تسريب قواعد بيانات تحتوي على ما يقرب من 30 ألف سجل من المعلومات الحساسة. وبلغت البيانات المسروقة ما بين 60 إلى 80 جيجابايت تضمنت: بطاقات الهوية، بيانات جواز السفر ورخص القيادة ومعلومات الوظيفة والمعلومات الشخصية. كما ادعت المجموعة انها قامت بتدمير بعض البيانات الاحتياطية للمدينة.

كانت مجموعة برمجية الفدية LockBit Gang واحدة من أكثر المجموعات نشاطًا وفقا لعمليات الابتزاز المنشورة خلال الربع الثاني. يشير استمرار أنشطة مجموعة برمجية الفدية LockBit المشهورة الى قدرتها على متابعة تنفيذ عملياتها على الرغم من عملية إنفاذ القانون التي عطلت بنيتها التحتية عبر عملية تعرف باسم "Cronos" في شهر شباط الماضي. لم يكن من الواضح فيما إذا كانت المجموعة قادرة على تنفيذ هجمات جديدة خاصة بعدما تم الاستحواذ على برمجية جديدة تحت التطوير. ومع ذلك، يبدو أن المجموعة قد استعادت بعضًا من حجم هجماتها السابقة. حيث أظهرت المجموعة مرونة تمثلت في إنشاء بنية تحتية جديدة بشكل متسارع وإدراج الضحايا على موقع الابتزاز الجديد (DLS) الخاص بهم. يتوجب على مسؤولي الامن السيبراني في المؤسسات ان يكونوا على دراية بأحدث أنشطة المجموعة والعمل على تعزيز وسائل الحماية التقنية ورصد وجود نسخ البرمجية المحدثة للمجموعة LockBit-NG-Dev

قامت مجموعة برمجية الفدية BlackSuit بمهاجمة مزود البرمجيات (CDK Global) الخاص بإحدى شركات صناعة السيارات الأمريكية. أدى الهجوم الى إغلاق مركزي البيانات (Data centers) وأنظمة الشركة مما أدى إلى تعطيل الخدمات لحوالي 15000 وكالة سيارات في جميع أنحاء أمريكا الشمالية وتعطيل عمليات شركات السيارات Lithia Motors وGroup 1 Automotive وPenske وSonic Automotive. عادة ما تستخدم المجموعة أدوات التحكم عن بعد RMM لإنشاء الاتصال بالأنظمة المستهدفة مثل برمجيات AnyDesk و MobaXterm. كما تستغل الثغرات في البرمجيات والأنظمة وتستخدم تقنيات تشفير قوية وأدوات خاصة لنقل البيانات عبر الشبكة بطريقة خفية لتجاوز أنظمة جدار الحماية.

اكتشف باحثون حملة مستمرة منذ شهر أيار من عام 2021 من قبل مجموعة التهديد " Mallox". استهدفت الحملة خوادم قواعد البيانات من شركة Microsoft المكشوفة على شبكة الإنترنت وقواعد البيانات Postegre. في عام 2022، قامت المجموعة بإنشاء وتقديم نموذج الفدية ككخدمة (Ransomware-as-a-service).

أهم الثغرات الأمنية

أبرز الثغرات التي تم اكتشافها خلال الربع الماضي وتم استغلالها على نطاق واسع كانت للأنظمة التالية:

1- Firewall (CVE-2024-3400) Palo Alto
2- PHP (CVE-2024-4577)
3- Google Chrome (CVE-2024-4671)
4- Google Pixel (CVE-2024-32896)

تعد الثغرة المكتشفة على متصفح Google Chrome (CVE-2024-4671) خامس ثغرة جديدة (Zero day) منذ مطلع العام الحالي. من الجدير بالذكر أنه تم اكتشاف 8 ثغرات جديدة عام 2023 لمتصفح Google ما يشير الى وجود اتجاه لدى جهات التهديد باستهداف الأنظمة والبرمجيات الأكثر شيوعا، حيث تشير الاحصائيات الى أن الحصة السوقية للمتصفح تصل الى 65% على مستوى العالم. كما تم استغلال ثغرة في برمجية PHP ضمن سلسلة هجمات برمجية الفدية تعرف باسم "TellYouThePass". نظرا لان الثغرة تؤثر على جميع إصدارات PHP على نظام ويندوز التي تستخدم الواجهة البرمجية (CGI)، من الممكن ان يؤدي ذلك لزيادة احتمالية استهداف المهاجمين لتلك الأنظمة.

نظرة استشرافية

تشكل عمليات التأثير الإعلامي تهديدا نظرًا لكونها تعتمد على التلاعب والاحتيال النفسي. كما أن توظيف تقنيات الذكاء الاصطناعي في هذه الحملات يشير الى استغلاله بشكل متزايد من قبل جهات التهديد بالنظر للزيادة الملحوظة في استخدام عمليات التزييف العميق (Deep Fake) أو انتحال الشخصية على قنوات التواصل الاجتماعي. في حين أن حملات نشر المعلومات غير الدقيقة و/أو المضللة عبر وسائل التواصل الاجتماعي أو عبر الإنترنت ليست جديدة في العالم الرقمي، الا أنه يجب التنبه لها بشكل خاص تبعا للتغيرات والصراعات الجيوسياسية. قد تؤدي المعلومات الكاذبة او المضللة إلى إثارة العنف أو أعمال انتقامية، أو تصعيد الصراع، أو تفاقم التوترات الدولية. نتيجة لذلك، ينبغي أن يتوخى المستخدمون والمؤسسات على حد سواء الحذر عند قراءة المقالات والمنشورات المتعلقة بالأحداث والصراعات الجيوسياسية على الإنترنت، مثل التنبه للعناوين المثيرة أو المحتوى الذي يؤدي لأثارة العواطف والانفعالات.

يعد استغلال الثغرات الأمنية من أكثر التكتيكات شيوعا لدى جهات التهديد المختلفة. من المتوقع ان يستمر الاتجاه السائد باستغلال الثغرات الخاصة بالأنظمة والبرمجيات الأكثر استخداما. لذا يجب على المؤسسات العمل على تطبيق سياسة فعالة لتحديث الأنظمة والبرمجيات وترتيب الأولويات تبعا لأهمية الأنظمة المستخدمة. كما ينصح بتطبيق عدد من التدابير مثل متابعة المعلومات حول الثغرات المستغلة وخاصة التي ترتبط بأنظمة المؤسسة واستخدام أدوات للكشف عن وجود الثغرات بشكل مستمر وخاصة للأنظمة الحيوية او الحساسة الأمر الي يساعد في عملية الكشف وإصلاح هذه الثغرات في أقرب وقت ممكن.

يجب على مسؤولي الأنظمة في المؤسسات التي رصد لديها تسريبات لبيانات الدخول العمل على فحص أجهزة المؤسسة للتأكد من إزالة هذه البرمجيات الخبيثة وإعادة ضبط بيانات الدخول. كما يعد وجود سياسة فعالة لاستخدام بيانات الدخول وتطبيق عملية المصادقة المتعددة من أفضل الطرق للحماية من الحوادث الناتجة من عمليات تسريب بيانات الدخول.

من المرجح أن الصراعات الجيوسياسية المستمرة، مثل الحرب على قطاع غزة، والتوترات العامة في منطقة الشرق الأوسط سوف تستمر في دفع مجموعات التهديد ومجموعات القرصنة لزيادة عملياتها وحملاتها. كما يحتمل أن الشركات والمؤسسات التي لديها او تتعامل مع البيانات المرتبطة بالدول المعنية في صراعات جيوسياسية أن تواجه مخاطر متزايدة لحدوث تلك الانشطة.

على الرغم من أن الأنشطة الخاصة بمجموعات القرصنة تعرف عمومًا بأنها عمليات مبالغ فيها أو مضللة، الا أنه يجب على المؤسسات العمل على تعزيز حماية البنية التحتية من هجمات تلك المجموعات والتي غالبا ما تكون بغرض التعطيل (على سبيل المثال، هجمات حجب الخدمة DDoS، وتشويه محتوى الموقع Defacement). يجب أن تعطى الأولوية لتطبيق الإجراءات الضرورية مثل إغلاق أي منافذ مفتوحة غير ضرورية على الشبكة.

المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

تـقرير المـوقف الأمـني السـيبراني
Cyber Threat Situational Report

الربع الثاني 2024