المركز الوطني
للأمن السيبراني
National Cyber
Security Center

تقرير الموقف الأمني السيبراني
Cyber Threat Situational Report

الربع الثاني 2026

المركز الوطني للأمن السيبراني
عمّان - الدوار السابع +(962) 6 900 500 +(962) 65 300 265 Info@ncsc.jo

المحتوى

الملخص التنفيذي

يستعرض هذا التقرير ملامح المشهد الوطني للتهديدات السيبرانية مع تحليل للحوادث التي تم التصدي لها ورصد مؤشرات الأداء للشبكات الحكومية. كما يسلط الضوء على نقاط الضعف والثغرات الأكثر استغلالاً بهدف رفع كفاءة الوعي الأمني وتعزيز الحماية.

على المستوى الوطني لوحظ ازدياد في عدد الحوادث السيبرانية المرصودة خلال الربع الثاني بنسبة بلغت 22% تقريبا مقارنة بالربع الأول. ترتبط غالبية الزيادة في الحوادث المرصودة بعمليات "جمع المعلومات"، "محاولات الاختراق" و"عمليات استغلال حسابات المستخدمين". يمكن إرجاع ذلك لأسباب منها عدم الاستقرار واستمرار التوترات الجيوسياسية في المنطقة والتي تؤثر في طبيعة أنشطة جهات التهديد بشكل عام. كما ان ظهور ثغرات أمنية في أنظمة شائعة الاستخدام قد يدفع العديد من المهاجمين لتنفيذ محاولات اختراق.

من الجدير بالذكر ان الأنشطة السيبرانية المرتبطة بمجموعات القرصنة انخفضت بشكل كبير عما كانت عليه بنسبة بلغت 73.7%. من الممكن ان يرجع ذلك الى انخفاض في حدة التوترات خاصة في الشهر الأخير من الربع.

شهدت البيئة الرقمية المحلية استمراراً ملحوظاً في رصد هجمات برمجيات الفدية (Ransomware) التي استهدفت قطاعات عدة مثل الصحي، الصناعي والتجاري.

كما تم رصد ازدياد في الأنشطة السيبرانية المرتبطة بمجموعات التهديد المتقدمة المدعومة من دول والتي تشكل تهديدا مرتفعا على المؤسسات الوطنية نظرا للأهداف الخاصة بها والتي ترتبط بالدول الداعمة لها.

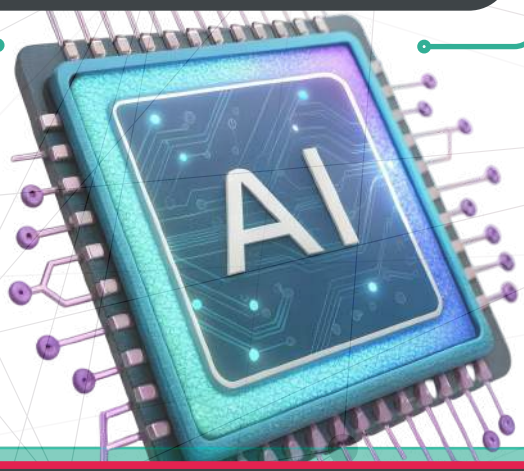
82.6%

من رسائل التصيد الالـكتروني يتم اعدادها باستخدام الذكاء الاصطناعي

اتسم الربع الثاني من عام 2026 بتصاعد وتيرة التحولات والاتجاهات التي تم تتبعها في مشهد التهديدات السيبرانية على مستوى العالم. حيث لوحظ تلاشي الفروقات تماماً بين المخاطر الناشئة من العمليات التجارية وبين الصراعات الجيوسياسية والجرائم السيبرانية. كما أصبحت أدوات الذكاء الاصطناعي جزء أساسي من تكتيكات المهاجمين بدلا من كونها مجرد أداة وبرزت 'الهوية الرقمية' كأهم عنصر في الهجمات السيبرانية.

73.7%

انـخفاض الـهجمات المرتبطة بـمـجموعـات الـقرصـنة



تنعكس التحولات المتسارعة في بيئة التهديدات السيبرانية العالمية بشكل مباشر ومتسارع على المشهد السيبراني المحلي، مما يفرض تحديات معقدة على البنى التحتية الحيوية.

ففي المدى القريب، يتصاعد دور الذكاء الاصطناعي التوليدي والوكيل (Agentic AI) كأداة هجومية تمكن القراصنة من أتمتة عمليات الاختراق، وتطوير برمجيات خبيثة ذاتية التكيف، وصياغة حملات تصيد احتيالي فائقة الدقة والتخصيص يصعب كشفها بالوسائل التقليدية. تشير التقارير إلى أن 82.6% من رسائل التصيد الالكتروني تستخدم الذكاء الاصطناعي لمحاكاة أساليب كتابة يصعب كشفها بالطرق التقليدية. تشير المعلومات المتوفرة أن 87% من قادة الأمن السيبراني اعتبروا أن الثغرات المرتبطة بالذكاء الاصطناعي تشكل الخطر الأسرع نمواً.

على المدى المتوسط، تبرز مخاطر الحوسبة الكمية التي تهدد بكسر خوارزميات التشفير الحالية؛ حيث تتبنى جهات التهديد المتقدمة تكتيك "خزّن الآن وفك التشفير لاحقا" (HNDL) لجمع البيانات الحساسة والمشفرة حالياً تمهيداً لفك تشفيرها فور نضوج التقنية الكمية. هذا التداخل المتطور يفرض على المؤسسات المحلية الإسراع في تبني استراتيجيات دفاعية مرنة والتحول الفوري نحو التشفير المقاوم للكم (PQC) لحماية الأمن القومي والسيادة الرقمية.

مشهد التهديدات السيبرانية الوطنية

لوحظ انخفاض الحوادث السيبرانية المرتبط بمجموعات القرصنة مقارنة بالربع السابق الامر الذي يعزى للتغيرات في الأوضاع الجيوسياسية في المنطقة حيث غالبا ما تكون هذه الهجمات بهدف دعم اتجاهات سياسية واحداث تأثير اعلامي واسع النطاق. كما ازدادت الحوادث السيبرانية المرتبطة بمجموعات التهديد المتقدمة APTs بشكل محدود فيما لم يطرأ تغيير يُذكر على معدل هجمات برمجيات الفدية. تأثر المشهد السيبراني بعوامل أخرى مثل ادزياد الثغرات الأمنية المكتشفة خاصة في ظل التطور المتسارع لأدوات الذكاء الاصطناعي التي تسهل من عملية اكتشاف الثغرات الأمنية واستغلالها.

مجموعات التهديد المتقدمة APTs (التجسس السيبراني)

تشير البيانات المتوفرة الى استمرار التهديدات المرتبطة بمجموعات التهديد المتقدمة بشكل عام. تسعى هذه الجهات لتحقيق أهداف استراتيجية من خلال عمليات الاختراق وجمع المعلومات بشكل أساسي. لوحظ أيضا اتجاه هذه المجموعات خلال التوترات الجيوسياسية نحو تنفيذ عمليات تخريبية تهدف لمسح البيانات الخاصة بالمؤسسات وتعطيل الأنظمة.
كما لوحظ تحول بعض المجموعات نحو استهداف أنظمة التكنولوجيا التشغيلية (OT) ودمج أدوات الذكاء الاصطناعي لأتمتة وتوسيع نطاق الهجمات. تجدر الإشارة الى بروز اتجاه لدى بعض المجموعات نحو استخدام جهات الواجهة المقنّعة تحت مسمى "نشطاء الاختراق" (Hacktivist personas) بهدف إخفاء المسؤولية وراء هذه الهجمات.

محليا رصدت بعض الهجمات التي يرجح ان ترتبط بعدد من مجموعات التهديد المتقدمة استهدفت عدد محدود من المؤسسات الوطنية. تشير البيانات الى ان غالبية هذه الهجمات كانت تهدف لتحقيق آلية وصول بالمؤسسات المستهدفة بهدف جمع معلومات يتم استغلالها في هجمات مستقبلا.

الجريمة السيبرانية (برمجيات الفدية)

تستغل مجموعات الفدية (Ransomware) بشكل أساسي الثغرات الأمنية في أنظمة وشبكات المؤسسات المستهدفة. تُظهر المؤشرات الأخيرة للحوادث السيبرانية وجود عدة نقاط ضعف محتملة تزيد من فرص نجاح هذه الهجمات. من أبرز هذه النقاط استخدام كلمات مرور ضعيفة تعود لمسؤول النظام (Admin) واستغلال منافذ بروتوكول سطح المكتب (RDP) المفتوحة وغير المحمية. كما أن عدم وجود أنظمة الحماية الأساسية، مثل برامج مكافحة الفيروسات (AV) وجدران الحماية يضاعف تلك المخاطر. بالإضافة الى ذلك، لوحظ استخدام أنظمة تشغيل وأنظمة حماية غير محدثة مما ينشئ ثغرات أمنية ويمنح المهاجمين الفرصة المناسبة لتنفيذ هجوم الفدية.

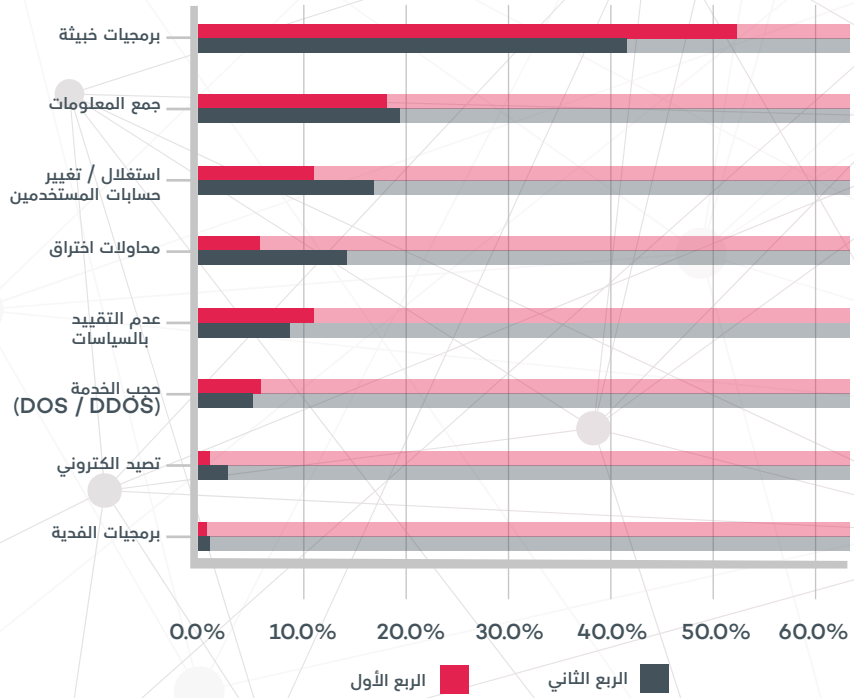
منذ بداية عام 2026، كثفت مجموعات الفدية عملياتها التي استهدفت الشركات المتوسطة والكبيرة، متبعةً نموذج "الابتزاز المزدوج". تكمن الميزة الأبرز للمجموعات في استخدام تقنية "EtherHiding"، حيث تستغل العقود الذكية اللامركزية على شبكة بلوكشين "" (Polygon) لتجاوز حظر جدران الحماية التقليدية. بعد تمكنها من اختراق الشبكة تستخدم المجموعات أسلوب (BYOVD) لتعطيل أنظمة الحماية مثل نظام كشف التهديدات (EDR).

مجموعات القرصنة

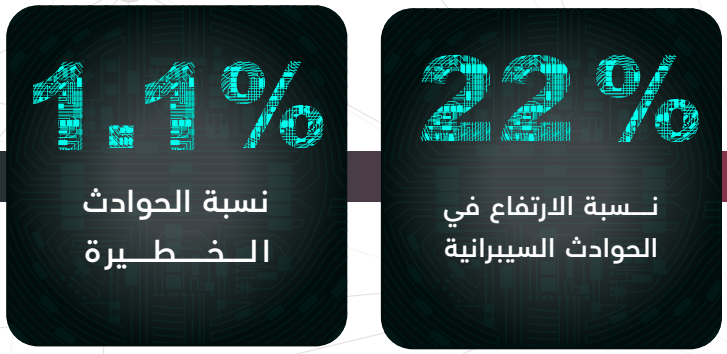
شهدت منطقة الشرق الأوسط منذ بداية هذا العام نشاطا بارزا لمجموعات القرصنة (Hacktivism) والتي تتماشى بصورة مباشرة مع التغيرات في الاوضاع الاقليمية. خلال هذه الفترة لوحظ ابتعاد هذه المجموعات عن استخدام الأساليب التقليدية مثل عمليات تغيير محتوى المواقع الإلكترونية، لتنتقل إلى تبني تقنيات متطورة وعالية التأثير تشمل نشر برمجيات المسح المخصصة (Wipers) واستخدام نموذج الابتزاز ببرمجيات الفدية بالإضافة إلى استهداف أنظمة التحكم الصناعي الحيوية (ICS).
على المستوى الوطني، لوحظ ان الأنشطة السيبرانية المرتبطة بتلك المجموعات انخفضت بشكل كبير عما كانت عليه. من الممكن ان يرجع ذلك الى انخفاض في حدة التوترات خاصة في الشهر الأخير من الربع.

مؤشرات الحوادث السيبرانية المحلية

ازدادت عدد الحوادث السيبرانية بنسبة بلغت 22% مقارنة بالربع الأول من هذا العام وبلغت نسبة الحوادث الخطيرة 1.1%.

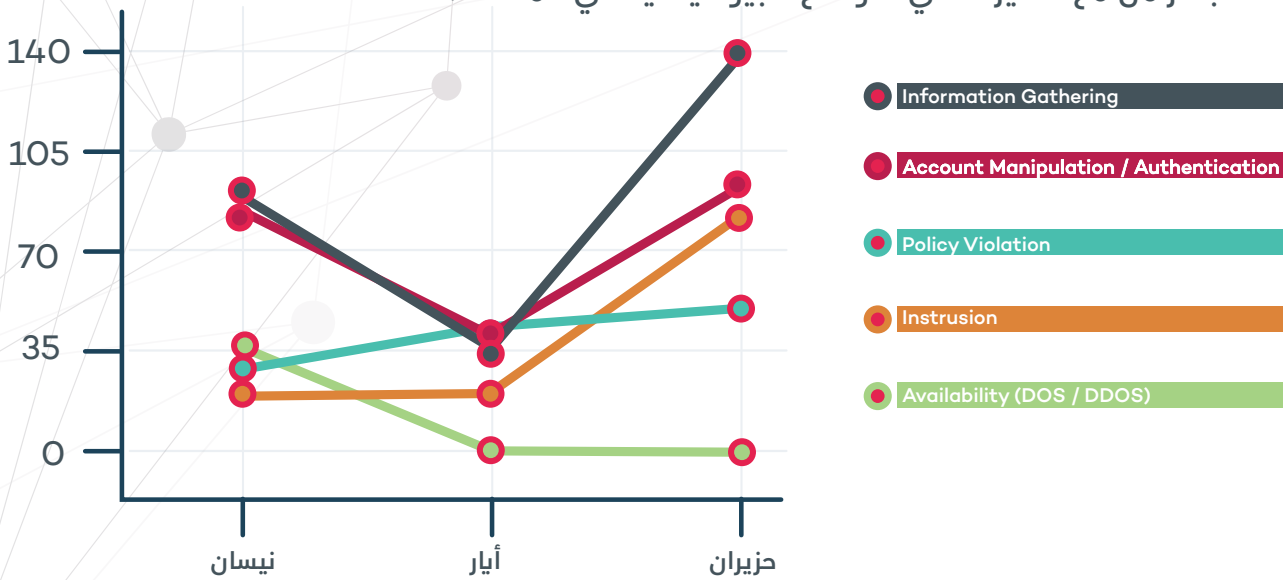


الشكل رقم :(1) نسبة الحوادث التي تم رصدها خلال الربعين الأول والثاني



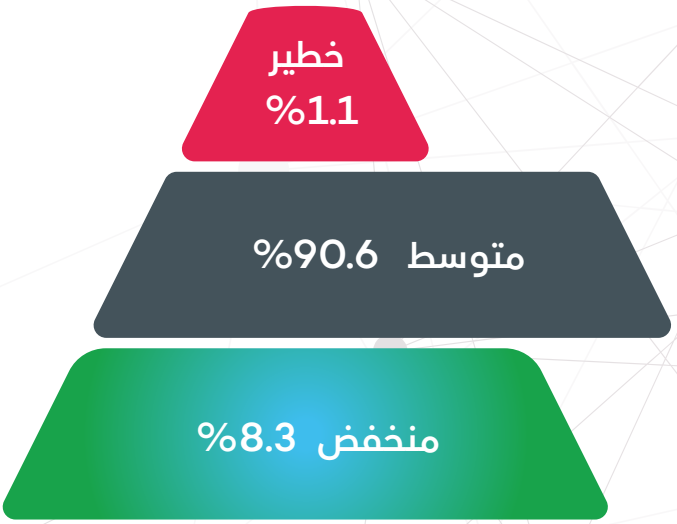
الشكل رقم :(2) الحوادث السيبرانية

لوحظ انخفاض عدد الحوادث في منتصف الربع الثاني بشكل عام مع ملاحظة انخفاض كبير في حوادث حجب الخدمة DDoS بالتزامن مع التغيرات في الأوضاع الجيوسياسية في المنطقة.



الشكل رقم :(3) الحوادث المرصودة خلال الربع الثاني

تتسق بيانات الحوادث بشكل عام مع تلك المرصودة في الفترات السابقة حيث تعد غالبية الحوادث ذات خطورة متوسطة بنسبة بلغت 90.6%. ما تزال البرمجيات الخبيثة تشكل النسبة الأكبر من الحوادث السيبرانية المرصودة بنسبة بلغت 40% من مجموع الحوادث الإجمالي.

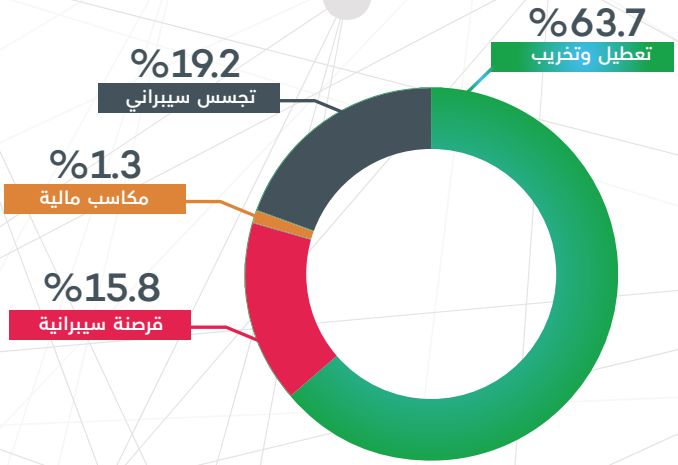


الشكل رقم :(4) توزيع الحوادث السيبرانية (حسب درجة الخطورة)

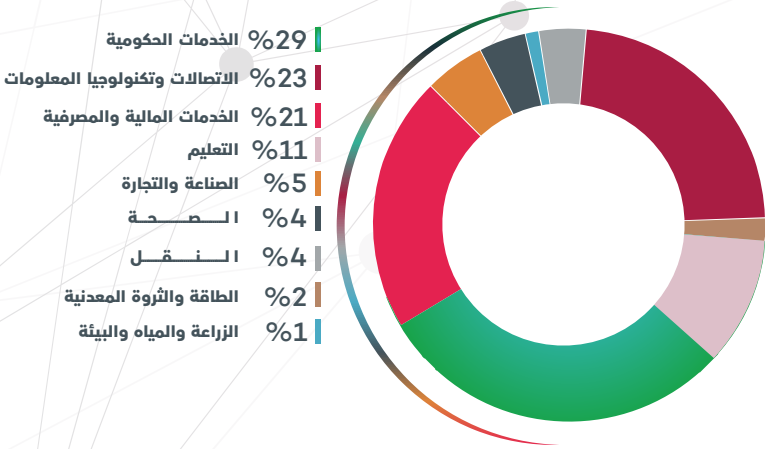
تتم الإصابة بالبرمجيات الخبيثة في المؤسسات عادة من خلال:

- **أساليب الهندسة الاجتماعية** مثل رسائل التصيد الالكتروني التي تتضمن روابط أو مرفقات خبيثة.
- **ضعف اجراءات التحديثات الدورية** للأنظمة والتطبيقات.
- **ضعف الوعي** لدى المستخدمين حول أفضل الممارسات الأمنية وضعف سياسات التحكم في صلاحيات الوصول الممنوحة للمستخدمين.

قد يؤدي الإصابة بالبرمجيات الخبيثة الى احداث تأثيرات خطيرة مثل تسريب البيانات الحساسة وسرقة الملكية الفكرية، وتعطيل العمليات التشغيلية، بالإضافة إلى الخسائر المادية المصاحبة لعمليات الإصلاح.



الشكل رقم :(5) توزيع الحوادث السيبرانية (حسب الأهداف)



الشكل رقم :(6) توزيع الحوادث السيبرانية التي تم الاستجابة لها (حسب القطاع)

تشير بيانات عمليات الاستجابة الميدانية للحوادث السيبرانية الى أن أبرز أسباب الإصابة بالحوادث السيبرانية يتعلق بأخطاء مستخدمين أو ضعف في تطبيق السياسات الأمنية والاجراءات المرتبطة بها. كما تجدر الإشارة الى ازدياد خطورة عمليات التصيد الالكتروني نظرا للاعتماد المتزايد على تقنيات الذكاء الاصطناعي الذي يمكن المهاجمين من استخدام أساليب احتيالية شديدة الإقناع وخالية من الأخطاء اللغوية وباستخدام لغات مختلفة. يمكن تجنب العديد من هذه الحوادث من خلال:

- تحديث الأنظمة والتطبيقات بشكل مستمر
- توعية المستخدمين حول مخاطر استخدام البرمجيات المقرصنة.
- التأكد من توافق الأنظمة والأجهزة المستخدمة في المؤسسة مع معايير الأمن السيبراني وفق متطلبات الشركة الموردة.

واجهة التهديدات السيبرانية الوطنية

تمنح العناصر المشكّلة لواجهة التهديدات السيبرانية (Attack Surface) المؤسسات رؤية واضحة حول جميع نقاط الضعف والثغرات المحتملة التي قد يتم استغلالها من قبل المهاجمين سواء كانت أجهزة، أو برمجيات، أو حسابات موظفين، أو حتى شركاء خارجيين. ان معرفة هذه العناصر تساعد في تحديد أولويات الحماية وتوزيع الموارد الأمنية بشكل فعال. كما تتيح تـقليص مساحة الهجوم عبر إغلاق الـمنافذ Ports غـير المستخدمة وتحديث الأنظمة، مما يرفع فعالية عـمليـات الاسـتجابة للـحوادث ويـقلل بـشكل كبير من احتمالية نجاح الاختراقات السيبرانية وتقليص سطح الهجوم وضمان استمرارية الأعمال.

1.19%
نسبة الأصول الرقمية ذات الثغرات الخطيرة (مرتفعة وحرجة)

على المستوى الوطني بلغت نسبة التغير في عدد الأصول الـرقمية بـانخـفاض 1.76% وارتـفعت نـسبة الأصول الرقمية ذات الثـغرات الـخطيرة بنـسبة 1.5%. لـم يلاحظ تـغير فـي البيانات عما تم رصده في فـترات سابقة حيث ما تزال المنافذ غير الآمنة تشكل نسبة تقارب 34.2% من مجموع المنافذ المفتوحة على شبكة الانترنت على المستوى الوطني نظراً لاتساع الخدمات الرقمية للمؤسسات الوطنية.

34.2%
منافذ البروتوكولات غير الآمنة

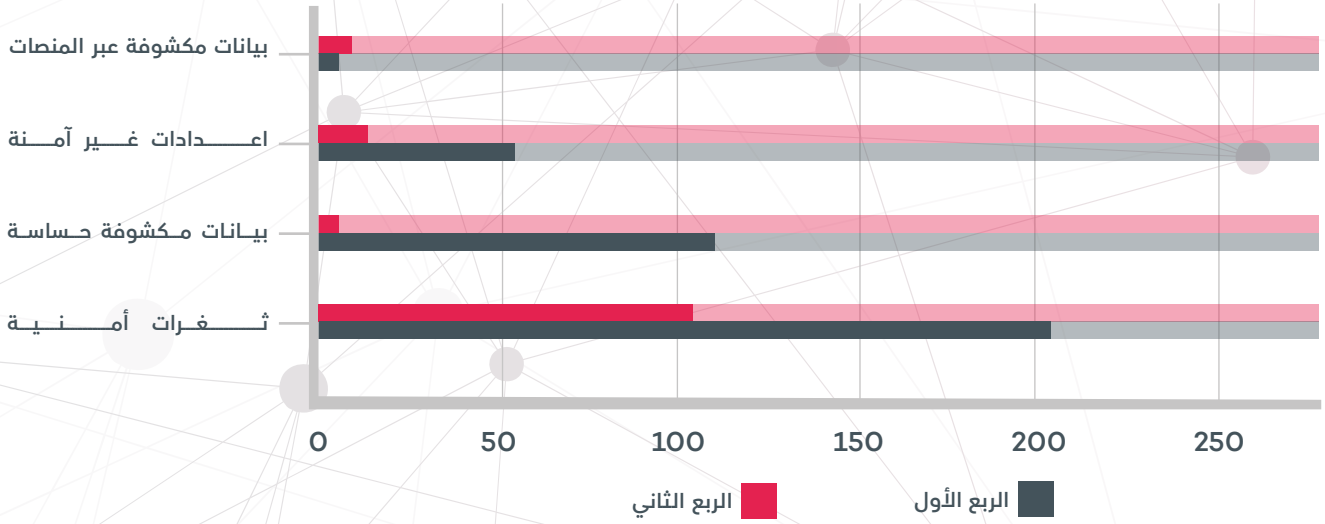
لوحظ استمرار تكرار ظهور الثغرات ذات الخطورة الشديدة التي تم الإشارة اليها في الفترات السابقة بنسب متقاربة. يؤكد هذا النمط المتكرر أهمية إدارة الثغرات وتسريع عمليات تطبيق التحديثات الأمنية، واجراء تقييمات دورية للتحقق من إجراءات المعالجة والحد من ظهور الثغرات الخطيرة.

ان الانتشار الواسع لبروتوكولات غير آمنة مثل HTTP وFTP وTELNET يشير الى ضعف في الوعي بمخاطرها الأمنية ويرفع احتمالية تعرضها لتسريب البيانات. يستخدم بروتوكول Telnet لإدارة أجهزة الشبكة القديمة (Network Switches) لعدم دعمها لبروتوكول SSH الآمن كما يتم استخدام بروتوكول FTP في تحديث الطابعات والآلات الصناعية القديمة (PLC) بالإضافة إلى استخدام بروتوكول HTTP في أنظمة نقاط البيع والمخازن (POS) لنقل بيانات الفواتير ما يسهل عملية اختراقها.
تظهر البيانات أن غالبية الثغرات ذات الخطورة الحرجة ومرتفعة الخطورة ترتبط بخدمات Apache و OpenSSH.

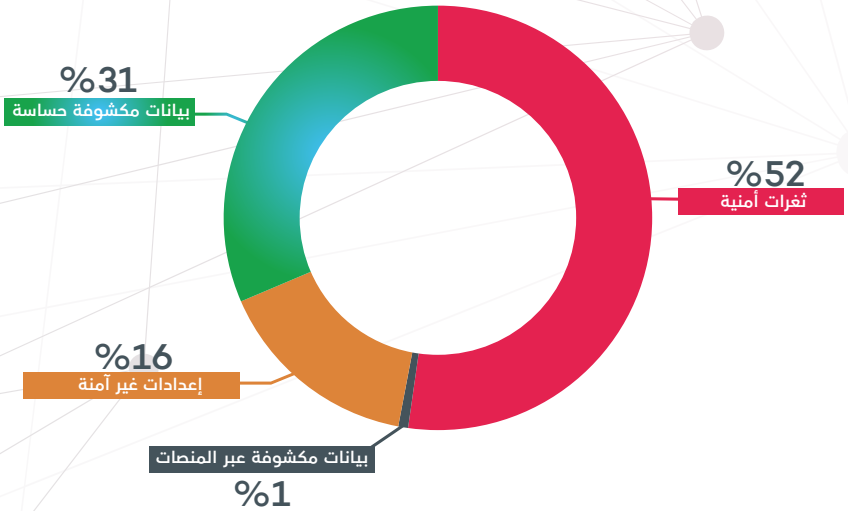
نقاط الضعف المرصودة في بعض المؤسسات الوطنية

يقوم المركز بمراقبة ورصد التغيرات في نقاط الضعف لدى بعض المؤسسات الوطنية بشكل دوري. تهدف هذه العملية المنتظمة لحماية تلك المؤسسات بشكل استباقي للحد من خطورة التهديدات السيبرانية التي قد ينشأ عنها آثار جسيمة نظرا لطبيعة البيانات والأنظمة الخاصة لتلك المؤسسات.

لوحظ ازدياد كبير في نسبة نقاط الضعف المكتشفة لدى بعض المؤسسات الوطنية. تشير البيانات الى ارتباط ازدياد نقاط الضعف بازدياد وتيرة الكشف عن الثغرات الأمنية خلال هذا الربع نظرا لتعزيز قدرات المركز في الكشف عن التهديدات السيبرانية باستخدام أنظمة مدعومة بالذكاء الاصطناعي. كما قد ترتبط هذه الزيادة بحادثة تسريب بيانات FortiBleed الشهيرة واكتشاف ثغرات على نظام ادارة المحتوى Joomla وثغرة في تطبيقات cPanel.



الشكل رقم :(8) تصنيف نقاط الضعف المكتشفة في بعض المؤسسات



الشكل رقم :(9) نقاط الضعف المرصودة

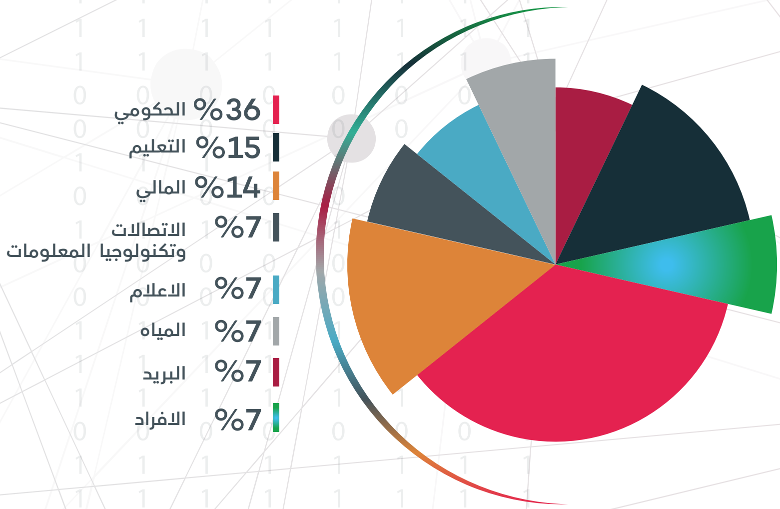
تم رصد عدد محدود من الثغرات الأمنية الحرجة على المواقع الالكترونية الرئيسية للمؤسسات الحكومية ما يشير الى عملية تحديث مستمرة للخوادم المستضيفة لتلك المواقع. كما يشار ايضا الى عدم ملاحظة تكرار في المؤسسات التي رصدت لديها ثغرات أمنية مرتفعة الخطورة وحرجة منذ الربع الرابع من عام 2025.

انتحال الهوية الرقمية للمؤسسات Brand Abusing

تُمثّل العلامة التجارية للمؤسسة في البيئة الرقمية المعاصرة عاملا أساسيا يؤثر في قيمتها السوقية مما يبين أهمية المراقبة الاستباقية لإساءة استخدامها كأولوية إستراتيجية لإدارة المخاطر وحوكمة الأمن السيبراني للمؤسسة. إن رصد محاولات انتحال الهوية الرقمية هو ضرورة إستراتيجية للمؤسسة تضمن استمرارية الأعمال. بالاضافة الى ذلك، تُسهم هذه الرقابة في الحد من خطورة التهديدات وحماية الأصول المالية للمؤسسة.

بشكل عام تتسق البيانات الحالية مع النتائج التي تم التوصل إليها في الربع السابق حيث ما يزال القطاع الحكومي هو الأكثر استهدافاً. تستغل جهات التهديد باستمرار الثقة بالقطاع العام لشن حملات سرقة بيانات الاعتماد، والتصيد الالكتروني.

خلال الربع الثاني من عام 2026 لوحظ ازدياد كبير في أنشطة انتحال الهوية الرقمية مقارنة بالربع الأول حيث. تم الكشف عن 122 من المواقع الإلكترونية التي تنتحل صفة مؤسسات وطنية. من الجدير بالذكر ان غالبية هذه الأنشطة تعود لاحدى المؤسسات بنسبة بلغت 86% من المجموع الكلي لعمليات الانتحال ما قد يشير لعملية استهداف موجهة ومنسقة لأغراض مالية



الشكل رقم: (10) القطاعات المستهدفة في عمليات انتحال الهوية الرقمية Brand Abusing

توصيات لإدارة واجهة التهديدات السيبرانية للمؤسسة

1. اغلاق منافذ الشبكة Ports غير الضرورية وتقييد الوصول إلى واجهات إدارة الأجهزة مثل RDP وSSH) لتكون متاحة فقط من خلال شبكات موثوقة.
2. المراقبة المستمرة لحركة مرور البيانات للاكتشاف المبكر لهجمات حجب الخدمة (DDoS).
3. تطبيق المصادقة متعددة العوامل (MFA) القائمة على المفاتيح الأمنية (FIDO2) بدلاً من الرموز SMS القابلة للسرقة.
4. تحديث البنية التحتية الأمنية، وزيادة الوعي بالأمن السيبراني
5. الاحتفاظ بنسخ من البيانات الحساسة في بيئة معزولة عن الشبكة الرئيسية

المؤشرات الإقليمية والعالمية

شهد الربع الثاني من عام 2026 استمراراً في تصاعد مستوى التهديدات السيبرانية التي تستهدف تطبيقات الويب باعتبارها أحد أكثر الأصول عرضة للهجوم داخل المؤسسات، حيث أصبحت التطبيقات السحابية، وواجهات برمجة التطبيقات (APIs)، والخدمات الرقمية أهدافاً رئيسية للمهاجمين. وقد اتسمت هذه الفترة بارتفاع وتيرة استغلال الثغرات الأمنية الحرجة، وتزايد هجمات سرقة الهوية الرقمية والتصيد الاحتيالي. كما ساهمت التوترات الجيوسياسية، ولا سيما في منطقة الشرق الأوسط في زيادة نشاط مجموعات الاختراق ذات الدوافع السياسية وعمليات التجسس الالكتروني التي استهدفت المؤسسات الحكومية والبنية التحتية الحيوية. تعكس هذه المؤشرات الحاجة الى تبني نهج استباقي لإدارة المخاطر السيبرانية، وتسريع معالجة الثغرات وتعزيز أمن الهوية، ورفع جاهزية المؤسسات لمواجهة التهديدات المتطورة.

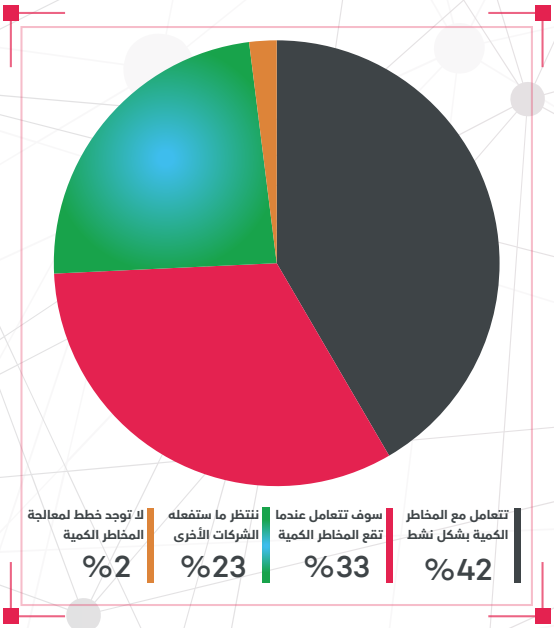
42% **فقط**

نسبة المؤسسات التي تتعامل مع المخاطر الكمية بشكل نشط

أبرز الاتجاهات في مشهد التهديدات السيبرانية العالمي

المخاطر المرتبطة بتقنيات الحوسبة الكمية Quantum Computing

تشير التطورات في الحوسبة الكمّية إلى انتقالها من مرحلة البحث النظري إلى استخدامات عملية مبكرة، ما يفرض تحولًا استراتيجيًا في مشهد التهديدات السيبرانية، خصوصًا في مجالات التشفير وإدارة الهوية الرقمية وسرية البيانات طويلة الأمد. يتمثل التهديد الأساسي في احتمال ظهور حواسيب كمّية ذات صلة بالتشفير (CRQCs) قادرة مستقبلاً على كسر خوارزميات المفاتيح العامة الحالية، مما قد يؤدي إلى تقويض البنية التحتية للتشفير وموثوقية الأنظمة الرقمية على نطاق واسع، كما تشير المؤشرات إلى أن نشاط "اجمع الآن وفك التشفير لاحقًا" (Harvest Now, Decrypt Later) يمثل مخاطرة قائمة تستهدف البيانات طويلة العمر حتى قبل توفر قدرات فك التشفير الكمّي، في حين تُظهر المتطلبات التنظيمية ومعايير الصناعة تسارعًا في تبني التشفير ما بعد الكمّي (PQC) بما يجعل الجاهزية الكمّية أولوية استراتيجية للامتثال واستمرارية الأعمال. أظهرت احدى الدراسات ان ما نسبته 42% فقط من المؤسسات تتعامل مع المخاطر الكمية بشكل نشط.



مقترحات لإدارة المخاطر المتعلقة بالتشفير الكمي

1. إنشاء جرد شامل للتشفير ومراقبة الخوارزميات والأصول التشفيرية المعرضة للمخاطر الكمّية
2. تبني مبدأ "المرونة التشفيرية" (Cryptographic Agility) لتمكين استبدال الخوارزميات بسهولة دون إعادة تصميم الأنظمة
3. تطوير خارطة طريق للانتقال الى التشفير ما بعد الكمي (PQC) مع تحديد الأولويات حسب حساسية البيانات
4. تعزيز حوكمة الموردين وسلاسل الامداد لضمان التوافق مع المعايير التشفيرية الناشئة

المخاطر المرتبطة بتطور تقنيات الذكاء الاصطناعي

تحولت الهجمات السيبرانية القائمة على الذكاء الاصطناعي إلى أسلوب عمل معتاد للمخترقين. وفقاً للتقرير السنوي الأول لاستخبارات التهديدات الصادر عن شركة "أنثروبيك" (Anthropic) في يونيو 2026، تم رصد قرابة 14,000 نشاط خبيث ترتبط بـ 832 حساب. كما أشارت الشركة الى تعطيل محاولة استغلال جهات التهديد لنماذج الذكاء الاصطناعي الخاصة بها في عمليات ابتزاز الضحايا وسرقة البيانات على نطاق واسع، ما يقدم دليلاً على أن "الذكاء الاصطناعي الوكيل" (Agentic AI) يتم توظيفه في كافة مراحل الهجمات السيبرانية.

تشير التقارير إلى أن 82.6% من رسائل التصيد الالكتروني تستخدم الذكاء الاصطناعي لمحاكاة أساليب كتابة يصعب كشفها بالطرق التقليدية. في احدى الدراسات الاستطلاعية، اعتبر 87% من قادة الأمن السيبراني أن الثغرات المرتبطة بالذكاء الاصطناعي تشكل الخطر الأسرع نمواً. كما تجدر الإشارة الى رصد تضاعف ظهور الثغرات البرمجية بمعدل 4 أضعاف نتيجة لاستغلال الذكاء الاصطناعي في الكشف عن الأخطاء في البرمجيات الأمر الذي دفع 64% من المؤسسات لفحص أمان أدوات الذكاء الاصطناعي المدمجة لديها.

82.6%
من رسائل التصيد الالـكتروني يتم اعدادها باستخدام الذكاء الاصطناعي

توصيات للتعامل مع مخاطر الذكاء الاصطناعي

1. تبني مبدأ "عدم الثقة المطلقة" Zero-Trust: الاعتماد دائماً على وسيلة تواصل بديلة ومستقلة لتأكيد الهوية في العمليات ذات المخاطر المرتفعة (مثل تحويل الأموال).
2. تسريع معالجة الثغرات الأمنية من خلال أتمتة وتحديث الأنظمة والبرمجيات خلال فترة قصيرة
3. استخدام المصادقة الثنائية المدعومة بالأجهزة باستخدام مفاتيح الأمان مثل YubiKeys) أو ميزة Passkeys.
4. تطبيق سياسات أمنية للأنظمة الذكية بوضع حواجز تصفية (Guardrails) للمدخلات والمخرجات لمنع هجمات حقن الأوامر (Prompt Injections).

ارتفاع ملحوظ في استغلال الثغرات الأمنية

واصل المهاجمون تقليص الفترة الزمنية بين الإعلان عن الثغرات واستغلالها، حيث أصبحت العديد من الثغرات الحرجة تُستغل خلال 24 إلى 48 ساعة فقط من نشر التحديثات الأمنية. كما أظهر تقرير Verizon لعام 2026 أن ما نسبته 31% من حوادث الاختراق بدأت باستغلال ثغرات أمنية، متجاوزة لأول مرة حوادث سرقة بيانات الاعتماد كوسيلة للوصول الأولي. أدى ذلك إلى تشديد متطلبات تحديث الأنظمة وتقليص فترات الاستجابة للثغرات الحرجة.

31%
من حوادث الاختراق بدأت باستغلال ثغرات أمنية

تطور العمليات السيبرانية المرتبطة بالصراعات الجيوسياسية

تصاعدت العمليات السيبرانية المرتبطة بالصراعات الجيوسياسية لتتجاوز أنشطة التجسس التقليدي إلى تنفيذ هجمات مدمرة تستهدف البنى التحتية الحيوية والتكنولوجيا التشغيلية (OT). أبرز الأنشطة شملت استخدام برمجيات خبيثة متنكرة في هيئة برامج فدية لمسح الأجهزة عن بُعد، بالتوازي مع حملات تسريب بيانات وعمليات تأثير وإضرار بالسمعة. كما استمرت حملات التجسس طويلة الأمد المدعومة من الدول ضد شبكات الاتصالات، بينما كثفت بعض المجموعات عملياتها المالية عبر استهداف منصات العملات المشفرة، مما يعكس استمرار توظيف القدرات السيبرانية لتحقيق أهداف استراتيجية وسياسية واقتصادية.

يصعب تحديد مسؤولية الهجمات السيبرانية بدقة أو تحليل جميع ضحاياها، حيث يقتصر الرصد في كثير من الحالات على التأكد من تنفيذ محاولة الاختراق واكتشاف مؤشرات الهجوم دون توفر سياق جنائي كامل لجميع المراحل. تعمل مجموعات التهديد المتقدمة أو تلك المدعومة من الدول على إخفاء آثارها وتغيير أساليبها وتكتيكاتها باستمرار، مما يزيد من تعقيد عمليات الإسناد وتحديد المسؤولية. مع هذه التحديات، يعتمد تقييم جهات التهديد على تحليل الأدلة الرقمية، وأنماط السلوك، ومؤشرات الاختراق المتاحة للوصول إلى تقديرات أكثر دقة.

فيما يلي أبرز اتجاهات أنشطة مجموعات التهديد المتقدمة في المنطقة خلال الربع الثاني:

- تم رصد عدة حملات تصيد إلكتروني اعتمدت على انتحال هويات تجارية موثوقة واستخدام رسائل مرتبطة بالمشاريع لنشر برمجيات خبيثة.

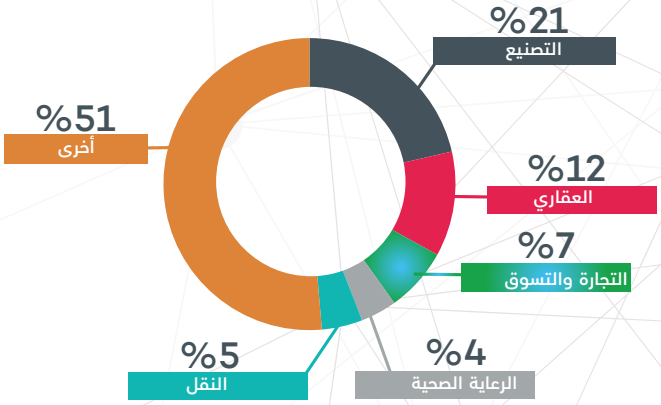
- قامت احدى مجموعات التهديد بارسال رسائل احتيالية مستوحاة من مشاريع خاصة بالمؤسسات المستهدفة مثل مشاريع البناء والبنية التحتية وغيرها مع استخدام بنية تحتية خبيثة تشمل خدمات مخترقة.

- تم رصد حملة تصيد الكتروني انتحلت صفة مسؤول في احدى شركات قطاع الطاقة حيث استخدم المهاجمون ملفات مزيفة تتعلق بمستندات المناقصات والموردين مزيفة لنشر البرمجيات الخبيثة.

مجموعات برمجيات الفدية Ransomware

تعد برمجيات الفدية Ransomware من أبرز التهديدات السيبرانية التي تواجه المؤسسات حول العالم. تطورت هذه الهجمات من عمليات تشفير للبيانات وطلب الفدية إلى منظومة إجرامية متكاملة تشمل نماذج الفدية كخدمة (RaaS)، مواقع تسريب البيانات (DLS) ووسطاء الوصول الأولي (IABs) الذين يسهلون عملية اختراق الشبكات المستهدفة.

تتجاوز تداعيات هجمات برمجيات الفدية مجرد التعطيل التقني المؤقت لتشمل عدة جوانب أخرى. فمن الناحية المادية، تتكبد المؤسسات خسائر باهظة تمتد لتشمل تكاليف استعادة الأنظمة وتعطل العمليات الإنتاجية، كما قد يتم فرض غرامات تنظيمية نتيجة لانتهاك خصوصية البيانات. من ناحية أخرى يؤثر الهجوم على سمعة المؤسسة ويزعزع ثقة العملاء والشركاء ويتفاقم هذا الخطر مع تبني المهاجمين استراتيجية "الابتزاز المزدوج"، حيث يتم تهديد المؤسسة بنشر بياناتها الحساسة وأسرارها التجارية بشكل عام.

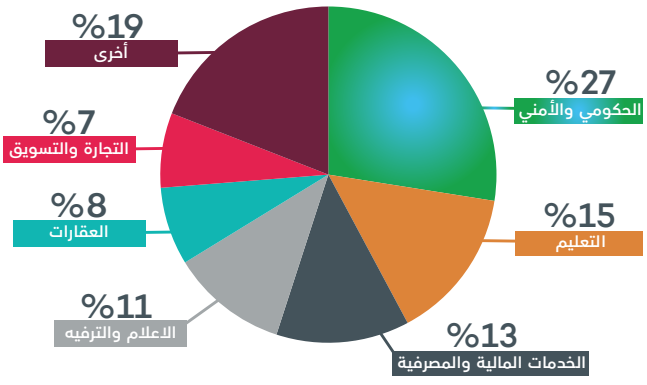


الشكل رقم :(11) أكثر القطاعات المستهدفة في المنطقة من قبل مجموعات الفدية خلال الربع الثاني

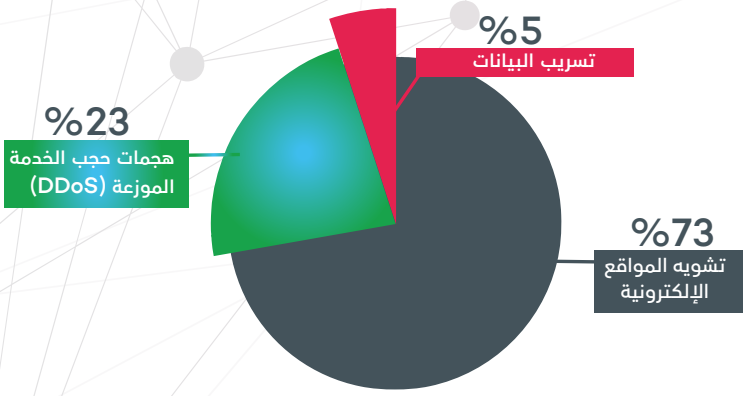
مجموعات القرصنة Hacktivism

تعد الأنشطة السيبرانية لمجموعات القرصنة ذات أبعاد اجتماعية وسياسية وذات سياقات ترتبط بالصراعات والتغيرات في الأوضاع الجيوسياسية. تسعى هذه المجموعات إلى دعم قضايا معينة وجذب الانتباه وإحداث تأثير نفسي بدلاً من تحقيق مكاسب مالية وتعتمد غالبًا على استغلال منصات التواصل الاجتماعي للتنسيق والترويج لأنشطتها. من أكثر أساليب الهجوم شيوعًا، هجمات حجب الخدمة (DDoS)، تشويه المواقع (Defacement) ونشر البيانات المسربة.

تتميز معظم مجموعات القرصنة بقدرات تقنية محدودة وتعتمد غالبًا على استخدام أدوات وتقنيات متاحة علنًا بالإضافة الى استغلال الثغرات المعروفة في الأنظمة غير المحدثة، مع ندرة امتلاكها قدرات تطوير أدوات خاصة أو استغلال الثغرات الجديدة Zero-day. تبقى هجمات حجب الخدمة DDoS النشاط الأكثر انتشارًا، بينما تعد عمليات تشويه المواقع أقل شيوعًا. غالبًا ما تهدف هذه العمليات إلى تحقيق تأثير إعلامي أكثر من تحقيق اختراقات معقدة أو طويلة الأمد



الشكل رقم :(12) أكثر القطاعات المستهدفة في المنطقة من قبل مجموعات القرصنة خلال الربع الثاني



الشكل رقم :(13) توزيع الحوادث المرتبطة بمجموعات القرصنة حسب النوع خلال الربع الثاني

أبرز الثغرات الأمنية

فيما يلي أبرز الثغرات المكتشفة في الأنظمة شائعة الاستخدام على المستوى العالمي خلال الربع الثاني من هذا العام والتي تم استغلالها على نطاق واسع:

FORTINET	CVE-2026-35616	حرجة 9.8
Microsoft	CVE-2026-33824	حرجة 9.8
cPanel	CVE-2026-41940	حرجة 9.8
Windows	CVE-2026-41089	حرجة 9.8
cisco	CVE-2026-20182	حرجة 10.0
ivanti	CVE-2026-10520	حرجة 10.0
paloalto NETWORKS	CVE-2026-0257	حرجة 9.1
Joomla!	CVE-2026-48907	حرجة 9.8
Adobe	CVE-2026-34621	مرتفعة 8.6
Linux	CVE-2026-31431	مرتفعة 7.8
NGINX	CVE-2026-42945	مرتفعة 8.1
TREND MICRO	CVE-2026-34926	متوسطة 6.7

الثغرات الأمنية التي تم استغلالها في حملات سيبرانية نشطة عالميًا

حملة "FortiBleed": استهداف 86 ألف جدار حماية FortiGate لسرقة البيانات

تعد حملة «FortiBleed» أحد أبرز التهديدات الممنهجة لسرقة بيانات الاعتماد، حيث استهدفت ما يصل إلى 86,000 من أنظمة جدران الحماية FortiGate حول العالم. تكشف هذه الحملة عن «مفارقة» خطيرة في عملية معالجة الثغرات، حيث تفشل عملية تطبيق التحديثات للبرامج الثابتة (firmware) في حماية كلمات المرور القديمة المخزنة في النسخ الاحتياطية للإعدادات والتي يسهل فك تشفيرها باستخدام معدات حاسوبية قوية، يمكن فك تشفير هذه الكلمات دون الاتصال بالإنترنت ما يسمح للمهاجمين بتجاوز أنظمة الحماية والانتقال للشبكة الداخلية Active Directory لضمان وصول طويل الأمد. لمواجهة هذا التهديد، يجب على المؤسسات إجراء إعادة تعيين شاملة وفورية لكلمات مرور المسؤولين، وفرض المصادقة متعددة العوامل (MFA)، وترقية البرامج الثابتة وتفعيل الانتقال إلى تشفير أقوى، والبحث النشط عن أي مؤشرات أنشطة خبيثة داخل الشبكة.

اكتشاف عدد من الثغرات في نظام إدارة المحتوى Joomla

شهد الربع الثاني من عام 2026 اكتشاف سلسلة من الثغرات الأمنية الحرجة التي استهدفت نظام إدارة المحتوى Joomla وبيئته البرمجية، وتحديداً عبر إضافاته (Extensions) الأكثر شيوعاً. من أبرز هذه الثغرات (CVE-2026-48908) و (CVE-2026-56290) بحجم خطورة بلغ الحد الأقصى (10/10)؛ حيث سمحت لجهات غير مصرح لها برفع ملفات عشوائية وتنفيذ برمجيات PHP ضارة عن بُعد للسيطرة الكاملة على المواقع المستهدفة من خلال إضافات شهيرة مثل SP Page Builder وPage Builder CK. كما تم رصد ثغرة حرجة (CVE-2026-48904) في النواة الأساسية للنظام عبر واجهة API لتعديل المجموعات، وثغرات أخرى في محررات شائعة مثل JCE (CVE-2026-48907) استُغلت في هجمات نشطة، مما دفع هيئات الأمن السيبراني مثل CISA لإصدار تحذيرات عاجلة بضرورة التحديث الفوري.

ثغرة CVE-2026-41940 تهدد 1.5 مليون خادم cPanel

تُعد ثغرة CVE-2026-41940 خللاً أمنياً حرِجاً (CVSS 9.8) في نظام إدارة الخوادم cPanel & WHM وتكتسب أهمية نظراً لانتشارها الهائل حول العالم (نحو 1.5 مليون خادم) متصل بالإنترنت. تتيح هذه الثغرة تجاوز آلية المصادقة وتخطي آليات التحقق وتسمح للمخترق بالسيطرة الكاملة وامتلاك صلاحيات مسؤول النظام (Root)ما قد يؤدي الى حدوث تسريب للبيانات وتثبيت لبرمجيات الفدية. للحد من هذه المخاطر يجب القيام بعمليات تحديث فوري إلى الإصدارات الآمنة وتقييد منافذ إدارة الظام بالجدار الناري وإعادة تعيين كلمات المرور.

النظرة الاستشرافية للمشهد السيبراني

تشير التوقعات إلى ازدياد اعتماد مجموعات التهديد السيبرانية على وسائل الهندسة الاجتماعية المدعومة بالذكاء الاصطناعي، لتصبح من أبرز أساليب الهجوم عالية التأثير. أثبت هذا النمط القدرة على تجاوز الضوابط التقنية التقليدية عبر استهداف العنصر البشري عوضا عن استغلال الثغرات البرمجية. كما برز التصيّد الصوتي كأسلوب رئيسي والذي يتوقع أن يشهد تطورًا كبيرًا عبر دمج تقنيات استنساخ الصوت بالذكاء الاصطناعي لإنتاج انتحالات صوتية واقعية خصوصا للمدراء التنفيذيين أو موظفي تكنولوجيا لمعلومات. إلى جانب ذلك، يمكن أن يتم استخدام الذكاء الاصطناعي في مراحل ما قبل الهجوم مثل عمليات الاستطلاع الآلية وجمع البيانات المفتوحة وصياغة رسائل تصيّد مخصصة وواقعية. يعكس ذلك الأمر تحولًا استراتيجيًا من استغلال الثغرات التقنية إلى استهداف وهندسة الثقة البشرية كطبقة اختراق مركزية، بما يتيح تنفيذ هجمات أكثر قابلية للتوسع مع تقليل فعالية أساليب الكشف التقليدية المعتمدة على عمليات التحليل التقني.

من المتوقع أن يؤدي تبني المؤسسات الواسع للذكاء الاصطناعي الى اعادة تشكيل أدوار محللي الأمن السيبراني، حيث ستتحول مراكز العمليات الأمنية من الاعتماد على المعالجة اليدوية للتنبيهات إلى انشاء بيئات تشغيل ذكية قائمة على الأتمتة والذكاء الاصطناعي (Agentic SOC). كما يتوقع أن تصبح التنبيهات الأمنية مدعومة بتحليلات آلية متقدمة تشمل ملخصات الحوادث، وفك الأوامر والبرمجيات المموهة Obfuscated، وربطها بإطار MITRE ATT&CK مع تسريع عمليات الاحتواء والاستجابة المؤتمتة عبر أنظمة SOAR.

للحفاظ على الهوية الثقافية واللغوية للدول والابتعاد عن الانحيازات الثقافية التي قد تفرضها النماذج العالمية للذكاء الاصطناعي، تتجه الدول نحو بناء مراكز حوسبة فائقة وتطوير نماذج لغوية ضخمة (LLMs) بلغاتها الأم ومبنية على قيمها المحلية ما يعرف باسم الذكاء الاصطناعي السيادي (Sovereign AI). من أبرز الأمثلة العالمية في هذا الاتجاه إطلاق دولة الإمارات العربية المتحدة لنماذج مفتوحة المصدر مثل عائلة نماذج "فالكون" (Falcon) ونموذج "جيس" المخصص للغة العربية، إلى جانب المبادرات الاستراتيجية للمملكة العربية السعودية، وتوجهات الاتحاد الأوروبي واليابان نحو تشييد بنى تحتية حوسبية مستقلة.

ستظل هجمات برمجيات الفدية المصحوبة بسرقة البيانات والابتزاز المتعدد في عام 2026، من أبرز التهديدات ذات الأثر المالي المرتفع، نظرًا لقدرتها على تعطيل العمليات وتسريب البيانات وإطالة فترات التعافي. كما تمتد آثار هذه الهجمات إلى الموردين والعملاء وسلاسل التوريد، مما يضاعف الخسائر الاقتصادية حيث تسببت الحوادث في عام 2025 في خسائر كبيرة وأدت الى حدوث اضطرابات واسعة في قطاعات حيوية.

يرجح أن تظل مجموعات التهديدات المستمرة المتقدمة (APT) من أكثر الجهات السيبرانية تطورًا وقدرة وتنفيذا لعمليات التجسس السيبراني، جمع المعلومات الاستخباراتية، الهجمات التخريبية وحملات التأثير لتحقيق أهداف أمنية وسياسية واقتصادية وعسكرية كما يعتقد ان تستمر في استهداف بيئات التحكم الصناعي (ICS) والتقنيات التشغيلية (OT). كما يتوقع ان تستهدف هجمات مجموعات الفدية بشكل محدد الأنظمة الحيوية مثل ERP لتعطيل العمليات وسلاسل الإمداد. ستظل نقاط الضعف في ممارسات الأمن السيبراني، خاصة آليات الوصول عن بُعد غير الآمن، عاملًا رئيسيًا في انتشار البرمجيات الخبيثة.

المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

تـقرير المـوقف الأمـني السـيبراني
Cyber Threat Situational Report
الربـــع الثاني 2026