المركـز الوطنـــــي
للأمـن السيبرانـــي
National Cyber
Security Center

تقرير المـوقف الأمـني السـيبراني
Cyber Threat Situational Report

الربع الرابـــــع 2025

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

المحتوى

1 الملخص التنفيذي

يقدم هذا التقرير تحليلاً لأبرز التحولات في مشهد التهديدات السيبرانية الوطني، حيث يتم تسليط الضوء على الحوادث السيبرانية التي تم التعامل معها واستعراض أبرز مؤشرات مراقبة الشبكات الحكومية. كما يستعرض التقرير الثغرات الأمنية الشائعة والتي يتم استغلالها على نطاق واسع بهدف تعزيز الوعي السيبراني.

تعد الحوادث المرتبطة بمجموعات برمجيات الفدية من أهم وأبرز التهديدات السيبرانية التي تمت الاستجابة لها ورصدها خلال الربع الرابع من عام 2025. كما تشير الأدلة الى استهداف بعض المؤسسات من قبل جهات تهديد مختلفة مثل مجموعات التهديد المتطورة. تنوعت الأهداف الخاصة بتلك الجهات وشملت تسريب لبيانات المؤسسة الحساسة، او سرقة بيانات الدخول بغرض استخدامها في هجمات سيبرانية او لتحقيق مكاسب مادية عبر بيعها في منصات خاصة بتلك الجهات.

من اهم الأسباب الرئيسية للحوادث السيبرانية هو استخدام أنظمة وبرمجيات غير محدثة او خارجة عن الدعم. تحتوي تلك الأنظمة عادة على ثغرات أمنية والتي عادة ما يتم نشر أكواد برمجية تستغل من قبل المهاجمين لاختراق الأنظمة المتأثرة بتلك الثغرات. من الأسباب الأخرى التي لوحظت، ضعف تطبيق ممارسات الامن السيبراني الفضلى مثل منافذ الخدمات الإلكترونية المفتوحة بشكل غير آمن او عدم استخدام أنظمة وبرمجيات الحماية المناسبة.

على المستوى العالمي، أظهر مشهد التهديدات السيبرانية تطورا وازديادا ملحوظًا في وتيرة الهجمات، حيث سُجِّلت زيادة بنسبة 35% في هجمات برمجيات الفدية التي استهدفت القطاع المالي، إلى جانب رصد أكثر من 1.3 مليون هجوم سيبراني باستخدام برمجيات مصرفية خبيثة خلال عام 2025. كما برزت تهديدات ناشئة تشمل البرمجيات الخبيثة المعززة بقدرات الذكاء الاصطناعي وعمليات الاحتيال التي تعتمد على تقنيات الاتصال قريب المدى (NFC) بالإضافة إلى هجمات واسعة النطاق التي تستهدف سلاسل التوريد (Supply Chain). تجدر الإشارة الى ان الأشهر الأربعة الأولى من عام 2025 شهدت ارتفاعًا في عدد الهجمات السيبرانية التي تعرضت لها المؤسسات مقارنة بالربع الأول من عام 2024، مع وصول حوادث برمجيات الفدية إلى مستويات غير مسبوقة.

2 أبرز الأنشطة والمؤشرات المحلية

- رصد أنشطة سيبرانية ترتبط بمجموعات تهديد متطورة استهدفت عدد من المؤسسات الوطنية.
- ازدياد الهجمات السيبرانية المرتبطة بمجموعات برمجيات الفدية Ransomware
- الكشف عن العديد من نقاط الضعف على شبكات بعض المؤسسات أغلبها يعود لاستخدام برمجيات وأنظمة غير محدثة او خارجة عن الدعم.
- رصد وجود بيانات حساسة مكشوفة بطريقة غير آمنة على شبكة الانترنت

3 احصائيات الحوادث التي تعرضت لها الشبكات الحكومية والوطنية

مؤشرات حول الحوادث السيبرانية التي تم الاستجابة لها

كانت عمليات الاستجابة والتحليل الرقمية للحوادث السيبرانية التي قام بها فريق الاستجابة بالمركز (JoCERT) على النحو التالي:

الشكل رقم(1): عمليات الاستجابة والتحليل الرقمي

في نهج مستمر منذ الربع الثاني من عام 2025، تشير البيانات الخاصة بعمليات الاستجابة للحوادث السيبرانية الى ان أبرز الحوادث السيبرانية المحلية وأكثرها تأثيرا هي هجمات برمجيات الفدية Ransomware مع وجود عدد ملحوظ من حوادث تسريب البيانات Data Leaks. يعد الكشف عن وجود أخطاء في اعدادات بعض الأنظمة Misconfiguration بالإضافة الى استخدام البرمجيات غير المحدثة من أكثر الأسباب الجذرية شيوعًا لهذه الحوادث. كما ان بعض الحوادث ترتبط باستخدام برمجيات مقرصنة (Cracked Software) والتي غالبًا ما تحتوي على برمجيات خبيثة أو ثغرات أمنية يمكن استغلالها لاختراق الأنظمة. ولوحظ أيضا ان استغلال خدمات الاتصال عن بعد RDP من قبل المهاجمين يعد الوسيلة الأكثر شيوعا في الحوادث السيبرانية. بشكل عام تشير المعطيات السابقة الى ازدياد التهديدات السيبرانية المرتبطة بمجموعات برمجيات الفدية وتعكس وجود ضعف في تطبيق معايير وممارسات الامن السيبراني القياسية.

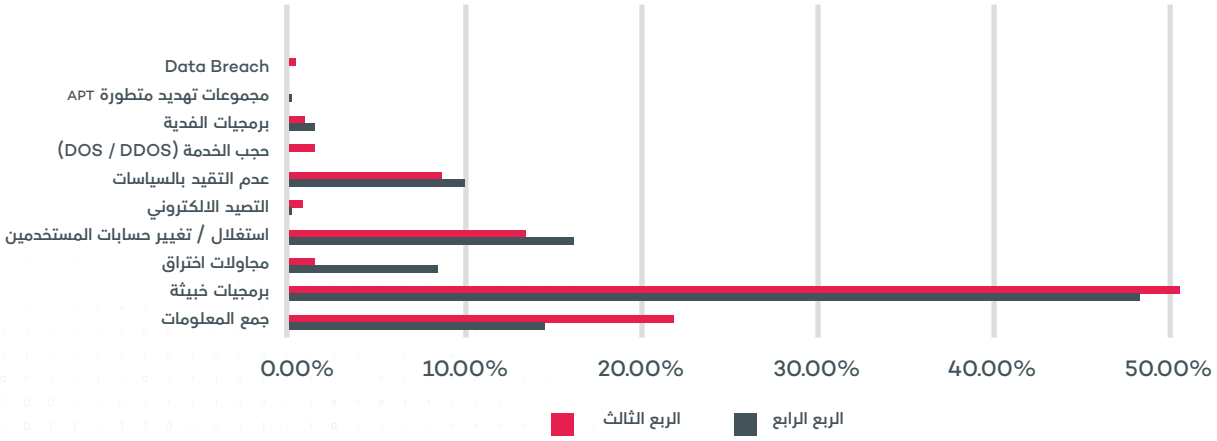
بالإضافة لذلك تجدر الإشارة الى ارتباط بعض تلك الحوادث بمجموعات التهديد المتطورة. تُعد هذه من أخطر الهجمات السيبرانية حيث قد تؤدي إلى اختراقات طويلة الأمد وتسريب بيانات حساسة بالإضافة الى تعطيل العمليات الحيوية للمؤسسة المستهدفة. تعتمد هذه المجموعات غالبًا على استخدام أساليب مثل رسائل التصيد الالكتروني (Phishing) سواء الموجهة او غير الموجهة بالإضافة الى سرقة بيانات الدخول للمستخدمين أو استغلال ثغرات أمنية في خدمات الاتصال عن بُعد.

أبرز ما تشير اليه بيانات مراقبة الشبكات الوطنية

تشير بيانات مراقبة الشبكات الوطنية الى ازدياد في عدد الحوادث السيبرانية المرصودة بنسبة بلغت 20.6% مقارنة بالربع الماضي الا انها ما تزال حول متوسط الحوادث خلال عام 2025. ما تزال نسبة الحوادث الخطيرة تشكل نسبة محدودة (1.8%) من مجموع الحوادث المرصودة والتي تقارب تلك التي تم رصدها في الربع الثالث. تشير البيانات الى ازدياد الحوادث السيبرانية ذات الدوافع المادية بشكل بارز مثل هجمات برمجيات الفدية. من أبرز التغيرات المرصودة انخفاض في نسبة حوادث "التصيد الالكتروني" و"جمع المعلومات" بالإضافة الى ازدياد في الحوادث المرتبطة بمجموعات القرصنة Hacktivists الأمر الذي قد يعزى الى التغيرات في الأوضاع الجيوسياسية التي شهدتها المنطقة خلال تلك الفترة.

الشكل رقم(2): الحوادث السيبرانية

الشكل التالي يوضح التغير في نسبة الحوادث التي تم رصدها خلال الربعين الثالث والرابع. يلاحظ ان بعض الحوادث مثل "البرمجيات الخبيثة" انخفضت فيما ازدادت نسبة حوادث "محاولات الاختراق".



الشكل رقم(3)

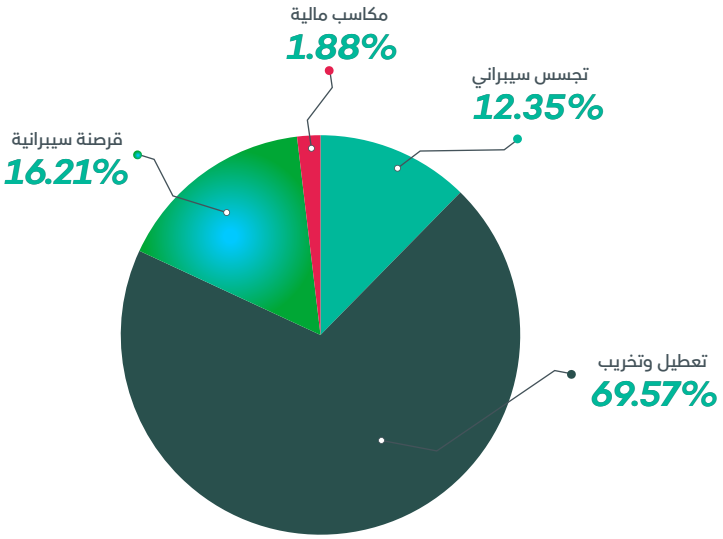
نسبة الحوادث لسيبرانية خلال الربعين الثالث والرابع

فيما يتعلق بالمؤسسات التي يتم مراقبة شبكاتها، كانت أبرز التغيرات ازدياد نسبة المؤسسات التي تعرضت لـ"محاولات اختراق"، حيث بلغت النسبة 47.12% في الربع الرابع مقارنة بـ 11.30% في الربع الثالث من هذا العام. كما لوحظ ارتفاع بسيط في نسبة المؤسسات التي رصدت لديها حوادث "عدم الالتزام بالسياسات". تتسق هذه الاحصائيات مع التغيرات في المشهد العام للتهديدات السيبرانية وارتفاع نسبة الحوادث السيبرانية بشكل عام.

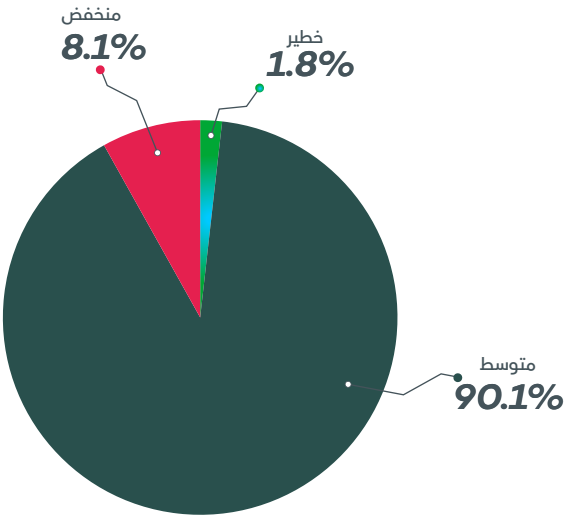
الشكل رقم(4):

ما تشير اليه بيانات الحوادث السيبرانية

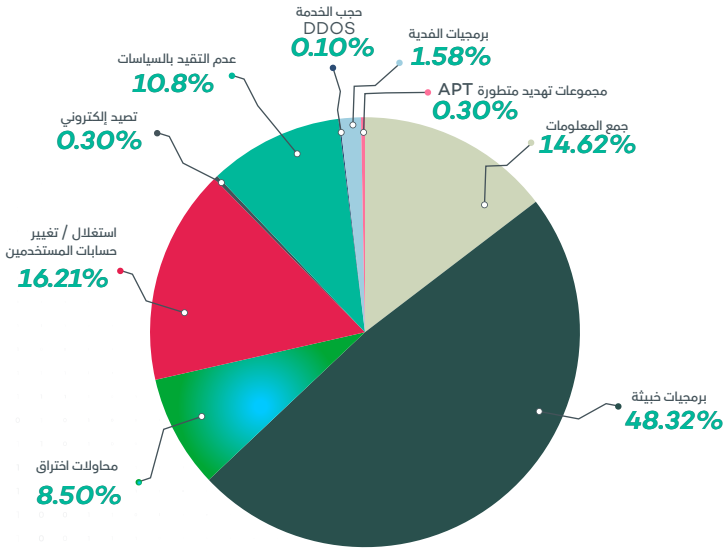
الرسوم البيانية التالية تبين توزيع الحوادث السيبرانية حسب الأهداف، النوع، درجة الخطورة بالإضافة الى توزيع الحوادث السيبرانية التي تم الاستجابة لها حسب القطاع:



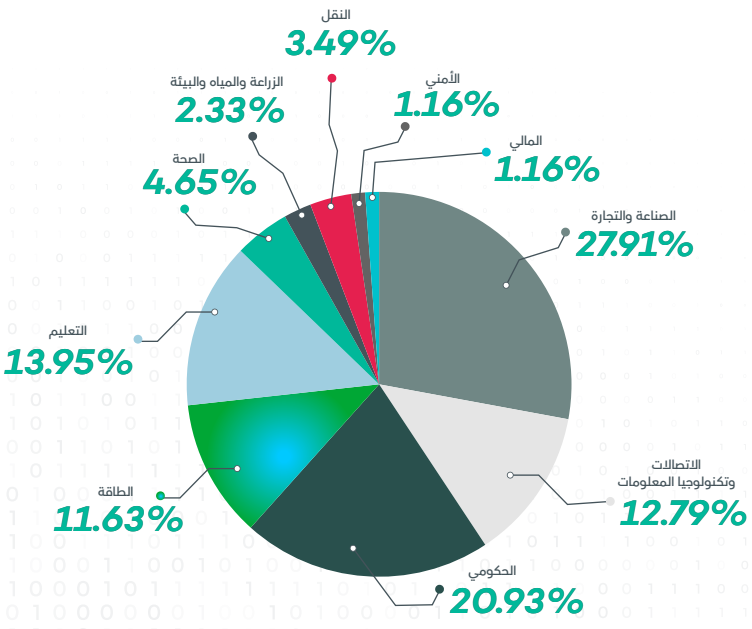
الشكل رقم(5):
توزيع الحوادث السيبرانية (حسب الأهداف)



الشكل رقم(6):
توزيع الحوادث السيبرانية (حسب درجة الخطورة)



الشكل رقم(7):
توزيع الحوادث السيبرانية (حسب النوع)



الشكل رقم(8):
توزيع الحوادث السيبرانية التي تم الاستجابة لها (حسب القطاع)

4 واجهة التهديدات السيبرانية الوطنية

يقصد بـ "**واجهة التهديدات السيبرانية**" نقاط الضعف المكتشفة ضمن أنظمة وشبكات المؤسسات والتي يمكن استغلالها من قبل جهات التهديد في تنفيذ الأنشطة السيبرانية المختلفة. يتناول هذا القسم عرض نقاط الضعف المكتشفة وتسليط الضوء حول مدى خطورتها على المؤسسات الوطنية.

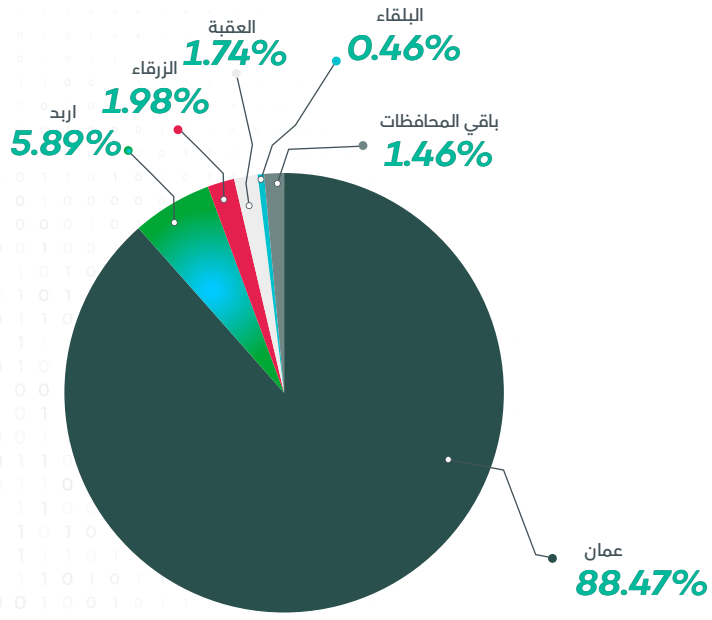
ما تزال نسبة الثغرات الحرجة تقارب تلك في الربع الثالث (9.9% في الربع الرابع مقارنة بـ 10.4% في الربع الثالث). غالبية الثغرات الحرجة ترتبط بخدمات شبكية تستخدم في عملية الاتصال عن بعد بالإضافة لبعض الخوادم شائعة الاستخدام لاستضافة المواقع الالكترونية.

توزعت أصول المؤسسات الوطنية الرقمية على النحو التالي:

39342
أصول رقمية

1.14%
نسبة الأصول الرقمية ذات الثغرات الخطيرة (مرتفعة وحرجة)

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



الشكل رقم(٩):
توزيع الأصول الرقمية على المحافظات

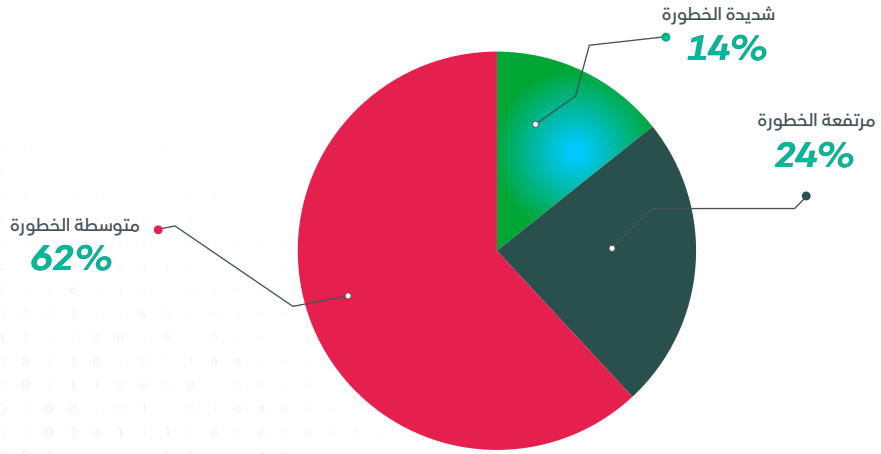
تشير البيانات الى أن نسبة المنافذ الشبكية غير الآمنة المفتوحة على المستوى الوطني ما تزال تشكل نسبة كبيرة من مجموع المنافذ بنسبة بلغت (33.8%). ان استخدام أحد البروتوكولات غير الآمنة المستخدمة في نقل البيانات عبر الانترنت بشكل كبير يلقي الضوء على اهمية تفعيل بروتوكولات النقل الآمن لحماية البيانات من مخاطر عمليات التنصت والسرقة.

33.75%
منافذ البروتوكولات غير الآمنة

من الملاحظ ان العديد من الأنظمة التي تحتوي ثغرات مرتفعة الخطورة او حرجة تعد أنظمة غير محدثة. كما ان عددا كبيرا من تلك الثغرات ترتبط بإعدادات خاطئة او بسبب عدم الالتزام بممارسات الامن السيبراني مثل استخدام اعدادات الأجهزة الافتراضية او الكشف عن الأنظمة التي تحتوي بيانات حساسة على شبكة الانترنت.

5 احصائيات فحوصات الثغرات والاختراق (نطاق حكومي)

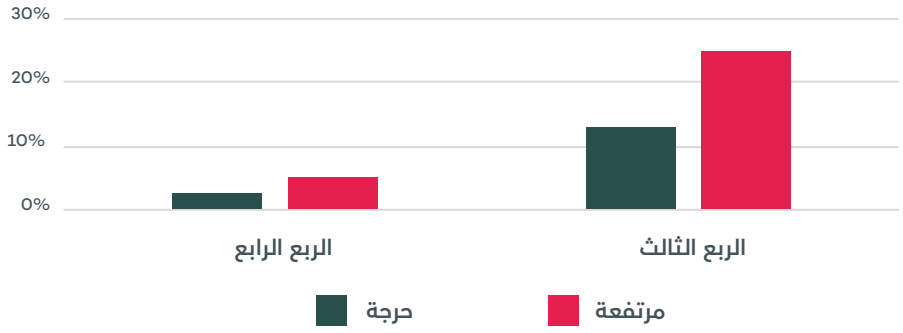
تم إجراء فحوصات لكشف الثغرات على المواقع الإلكترونية للمؤسسات، وكان مجموع الثغرات الأمنية التي تم ايجادها (27) ثغرة (حرجة ومرتفعة الخطورة) على المواقع الالكترونية. يبين الرسم التالي نتائج فحوصات الثغرات للمواقع الرئيسية للمؤسسات الحكومية وعددها 115 مؤسسة.



الشكل رقم(10):
تصنيف الثغرات الأمنية للمواقع الرئيسية للمؤسسات الحكومية
(حسب درجة الخطورة)

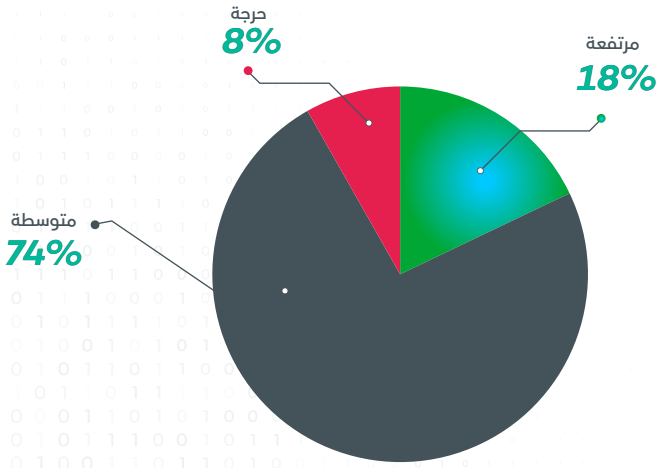
فيما يتعلق بالثغرات الحرجة ومرتفعة الخطورة المرصودة على المواقع الرئيسية للمؤسسات الحكومية بلغت نسبة الثغرات الحرجة 14% في الربع الرابع مقارنة بـ 9% في الربع الثالث فيما بقيت نسبة الثغرات مرتفعة الخطورة تقارب تلك للربع الثالث.

كما لوحظ انخفاض في نسبة المؤسسات التي رصدت لديها ثغرات أمنية حرجة ومرتفعة الخطورة على مواقعها الالكترونية الرئيسية حيث انخفضت النسبة من 21% في الربع الثالث الى 3% في الربع الرابع بالنسبة للثغرات الأمنية الحرجة فيما انخفضت النسبة من 24% في الربع الثالث الى 4% في الربع الرابع بالنسبة للثغرات الأمنية مرتفعة الخطورة.



الشكل رقم(11):
المؤسسات التي رصدت لديها ثغرات أمنية على مواقعها الرئيسية خلال الربعين الثالث والرابع

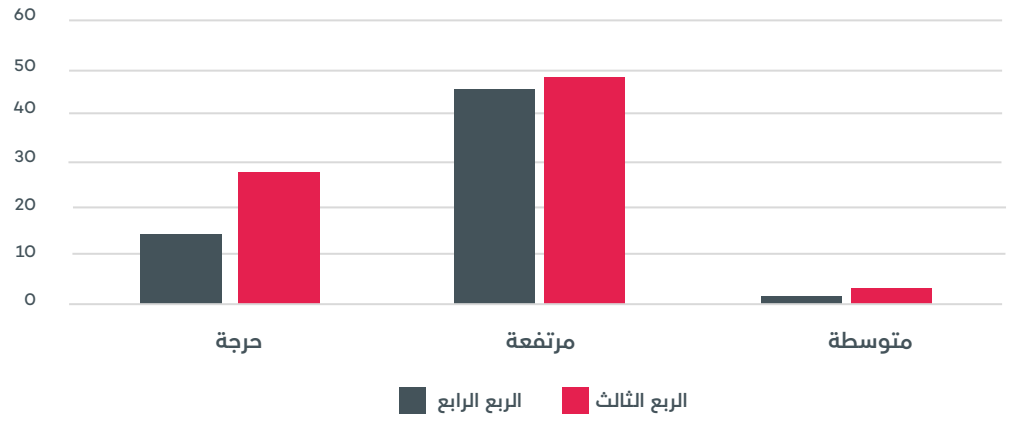
كما قام المركز بإجراء فحوصات اختراق لعدد من المؤسسات الوطنية حيث بلغ عدد المؤسسات التي تم تنفيذ فحص الاختراق لها (20) مؤسسة وبلغ العدد الاجمالي لفحوصات الاختراق (Penetration Testing) المنفذة (56) فحص شملت فحص المواقع والخدمات الالكترونية والتي تم من خلالها الكشف عن وجود (134) ثغرة.



الشكل رقم(12):
توزيع الثغرات المكتشفة من فحوصات الاختراق لبعض المؤسسات
(درجة الخطورة)

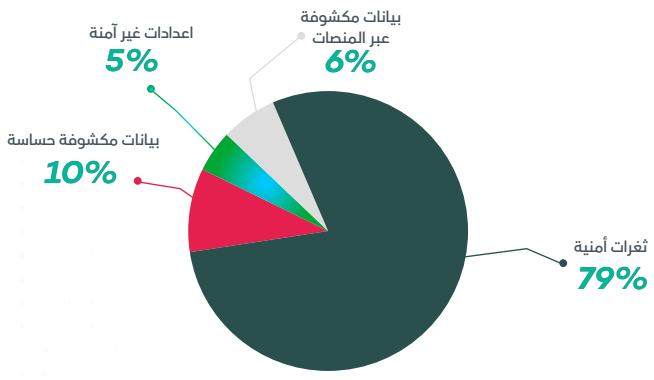
6 نقاط الضعف المرصودة في بعض المؤسسات الوطنية

انخفضت نقاط الضعف المختلفة المرصودة في عدد من المؤسسات الوطنية بنسبة تقارب 21% مقارنة بالربع الثالث من عام 2025. غالبية نقاط الضعف المكتشفة تعود لاستخدام برمجيات غير محدثة تحتوي ثغرات أمنية بعضها تم استغلاله من قبل جهات التهديد المختلفة. تعد معظم الثغرات الأمنية المكتشفة قديمة نسبيا.

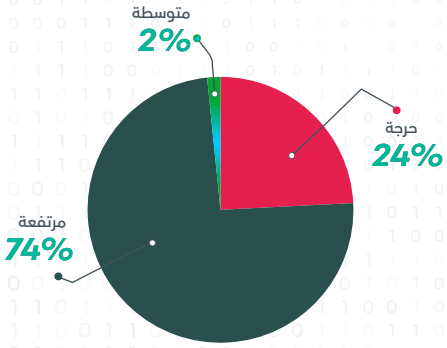


الشكل رقم(13):
نقاط الضعف (حسب الخطورة) خلال الربعين الثاني والثالث

فيما يلي التصنيفات الرئيسية لنقاط الضعف المكتشفة وتوزيعها حسب الخطورة وتوزيع الأنظمة التي تحتوي على نقاط ضعف (حرجة):



الشكل رقم(14):
تصنيف نقاط الضعف المكتشفة



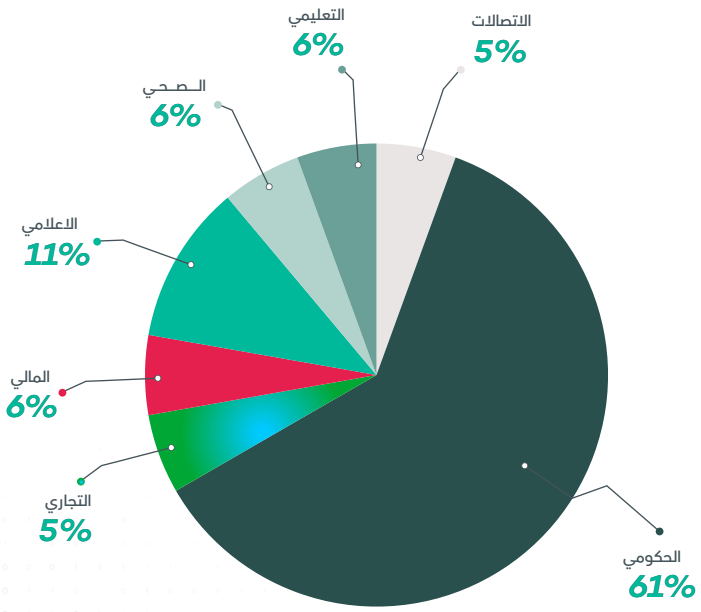
الشكل رقم(15):
توزيع نقاط الضعف المكتشفة حسب درجة الخطورة

7 انتحال الهوية الرقمية للمؤسسات Brand Abusing

تسعى جهات التهديد السيبراني إلى جمع بيانات حساسة تتعلق بالجهة أو المؤسسة المستهدفة، مثل اسم المؤسسة وعلامتها التجارية، إضافةً إلى عناوين البريد الإلكتروني للموظفين، ولا سيما أصحاب المناصب القيادية. غالباً ما تُستغل هذه البيانات في التخطيط لهجمات سيبرانية متنوعة، أو استخدامها دون تصريح بطرق قد تؤثر سلباً على سمعة المؤسسة، وتُلحق ضرراً بإيراداتها. تم رصد (40) من المواقع الإلكترونية او صفحات التواصل الاجتماعي المزيفة والمشابهة لمواقع الكترونية وطنية بازدياد بلغ نسبته 21.21% مقارنة بالربع الثالث.

عادة ما يستهدف القراصنة القطاعات المصرفية والتجارة الالكترونية لسرقة بيانات المستخدمين. فعلى سبيل المثال يمكن ان تؤدي حملات التصيد التي تنتحل صفة احدى الخدمات الإلكترونية لخداع المستخدمين وسرقة بيانات بطاقاتهم الائتمانية او المصرفية. بالإضافة الى ذلك قد تنتحل مجموعات التهديد المتطورة الهوية الرقمية لإحدى المؤسسات المرتبطة بالضحية كجزء من عمليات سيبرانية أوسع نطاقاً يمكن ان تستهدف قطاعات حيوية مثل الحكومي والطاقة والاتصالات.

فيما يلي رسم يوضح توزيع حوادث انتحال الهوية الرقمية حسب القطاع. ما يزال القطاع الحكومي يشكل النسبة الاكبر من القطاعات المستهدفة بنسبة بلغت 61%.



الشكل رقم(16):
القطاعات المستهدفة في عمليات انتحال الهوية الرقمية BRAND ABUSE

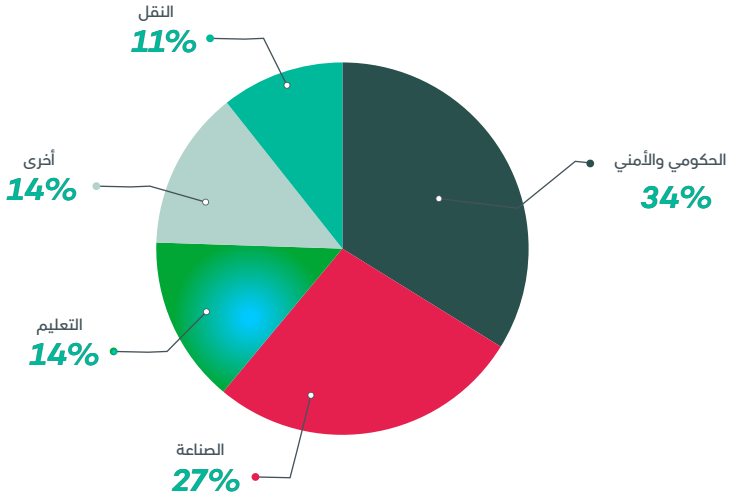
للحد من المخاطر المرتبطة بتلك المواقع يقوم المركز بإزالة تلك المواقع الالكترونية او الصفحات الخاصة بمواقع التواصل الاجتماعي حيث تم إزالة (20) من تلك المواقع الالكترونية او صفحات التواصل الاجتماعي.

توصيات لإدارة واجهة التهديدات السيبرانية للمؤسسة

- إجراء تقييمات دورية للتهديدات السيبرانية وتحليل الثغرات المحتملة
- اغلاق الخدمات والأجهزة غير المستخدمة داخل شبكة المؤسسة
- تقييد صلاحيات المستخدمين والخدمات المتاحة خارج شبكة المؤسسة الا للضرورة
- استخدام حلول الحماية المتقدمة
- تحديث الانظمة والبرمجيات بشكل منتظم
- استخدام البرتوكولات الآمنة لتبادل البيانات

8 المؤشرات الإقليمية والعالمية

يشهد المشهد العالمي والإقليمي للتهديدات السيبرانية تطوراً دائماً ومتسارعاً حيث تم رصد العديد من جهات التهديد السيبرانية الفاعلة خلال الفترة منذ منتصف العام الماضي. تنوعت هذه التهديدات بين هجمات برمجيات الفدية التي استهدفت القطاعات الحيوية في مناطق أمريكا الشمالية وأوروبا وآسيا، ومجموعات القرصنة النشطة التي تنفذ هجمات حجب الخدمة ضد البنية التحتية في أوروبا، بالإضافة إلى مجموعات التهديد المتطورة التي تستغل الثغرات الأمنية الحديثة مثل CVE-2026-21509 في شن هجمات سيبرانية موجهة. إن تتبع التغييرات في هذا المشهد يعد أمراً بالغ الأهمية حيث يمكّن المؤسسات من فهم التكتيكات والتقنيات للمهاجمين، ووضع استراتيجيات دفاعية استباقية تتناسب مع طبيعة تلك التهديدات المتغيرة مما يساهم في تعزيز المرونة السيبرانية وحماية الأصول الرقمية الحيوية.



الشكل رقم(17):
أكثر القطاعات المستهدفة بالهجمات السيبرانية

مجموعات التهديد المتطورة APTs

تمثل مجموعات التهديد المتطورة (APTs)، التهديد السيبراني الأكثر أهمية وتطورًا للأمن القومي والبنية التحتية الحيوية على مستوى العالم. تتميز الأنشطة السيبرانية المرتبطة بتلك المجموعات بسريتها واستمراريتها وتسعى عادة لتحقيق أهداف استراتيجية مثل سرقة الملكية الفكرية أو التجسس او عمليات التخريب وتدمير الأنظمة والبيانات الخاصة بالجهات الحكومية المعادية. كما تتميز هذه المجموعات بتوفر الموارد ومجموعة أدواتها السيبرانية المتعددة مما يسمح لها بتحقيق الوصول بشكل مستمر على المدى الطويل إلى شبكات الضحايا والتي تعد ذات قيمة عالية. تعد عملية الإسناد (Threat Attribution) لتلك المجموعات ومعرفة الضحايا المستهدفين صعبة وليست ممكنة في بعض الاحيان. في أغلب الانشطة تقتصر المعلومات على تأكيد عملية محاولة الاختراق حيث يتم اكتشاف بعض الآثار الرقمية لاحد مراحل الهجوم السيبراني دون وجود سياق وبيانات تتعلق بالمراحل السابقة للهجوم. بالإضافة إلى ذلك، غالبًا ما تتلاعب تلك المجموعات بالأدلة الرقمية وتغير الأساليب والتقنيات الخاصة بها مما يزيد من تعقيد عملية الإسناد.

أبرز أنشطة مجموعات التهديد المتطورة

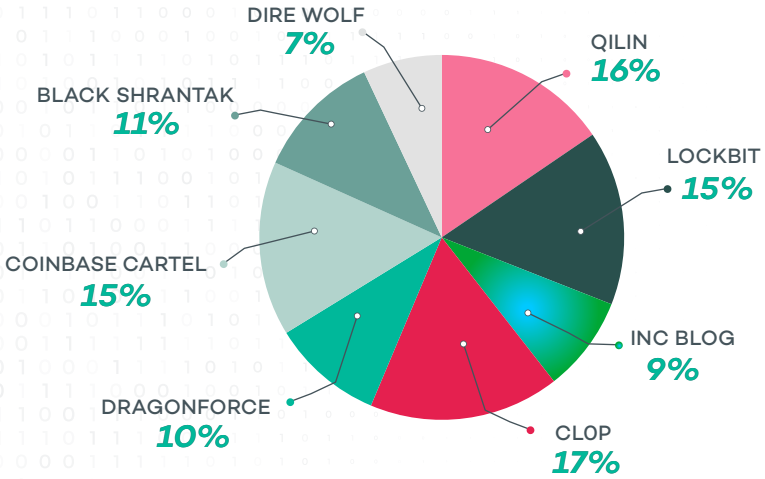
- استمرت احدى مجموعات التهديد الفاعلة في المنطقة بالاعتماد بشكل كبير على عمليات التصيد الالكتروني كوسيلة والذي يُعدّ قناة الوصول الأولية الأبرز حيث يتم الاعتماد بشكل رئيسي على استخدام مستندات تحتوي أكواد برمجية خبيثة تستخدم لتثبيت البرمجيات والأدوات الخبيثة. يأتي هذا الاتجاه امتدادًا لأساليب عمل لوحظت في وقت سابق من عام 2025 حيث شملت أنشطة تلك المجموعة حملات تجسّس دبلوماسي واسعة النطاق استهدفت حكومات ومنظمات دولية في مختلف أنحاء المنطقة وهو ما يعكس استمرار المجموعة في تطوير الأدوات والبرمجيات الخبيثة الخاصة بها. ومن الجدير بالذكر أن هذه المجموعة واكبت الاتجاهات الحديثة في مجال الأمن السيبراني، وحرصت على توظيف التقنيات الجديدة (مثل أسلوب هجمات ClickFix) إضافة إلى وجود أدلة مؤكدة على استخدام حلول النماذج اللغوية الكبيرة (LLM) وغيرها.

- استهدفت احدى الحملات افرادا ومؤسسات في قطاع الامن والدفاع. اعتمدت الحملة على انتحال شخصية عبر تطبيق واتساب، واستخدام خدع تتعلق بالمؤتمرات، بالإضافة إلى روابط مختصرة لإعادة توجيه الضحايا إلى مواقع إلكترونية مزيفة بهدف سرقة بيانات الاعتماد (Credential Harvesting)، وفي بعض الحالات، إيصال ملفات خبيثة.

مجموعات برمجيات الفدية Ransomware

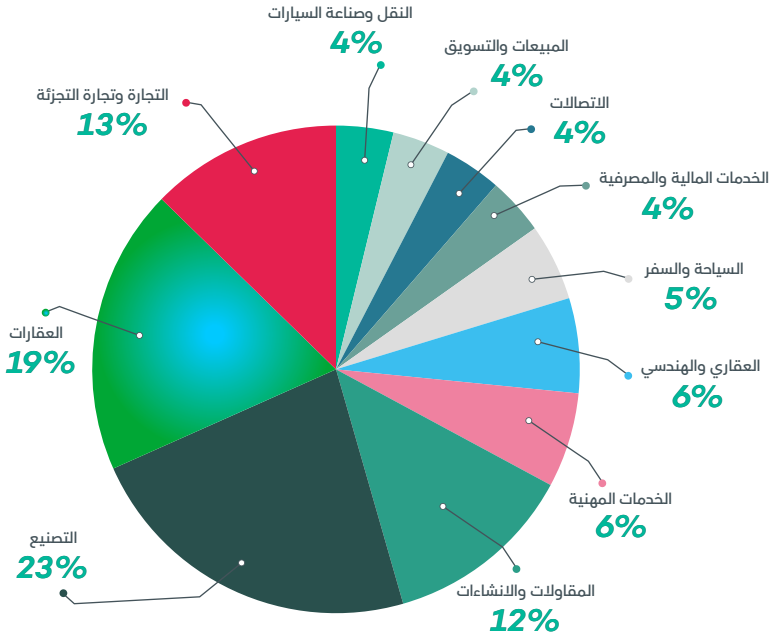
لا تزال برمجيات الفدية تمثل تهديدًا عالميًا بالغ الخطورة، إذ تعمل على تشفير البيانات الحساسة وابتزاز الضحايا من خلال المطالبة بفدية مرتفعة. وقد تطوّر هذا المشهد ليصبح نشاطا سريا معقدا يشمل نماذج (برمجيات الفدية كخدمة RaaS)، ومواقع مخصّصة لنشر البيانات المسربة DLS، إضافة إلى متخصصين كوسطاء وصول أوّليين (IAB) يعملون على تسهيل عملية اختراق الشبكات. يتكوّن نموذج (برمجيات الفدية كخدمة (RaaS)) من شركاء تابعين يتولّون تنفيذ أدوار محددة ضمن مجموعات قرصنة وتركز بشكل أساسي على إيصال ونشر برمجيات الفدية داخل بيئات الشبكات المستهدفة. شهدت هذه البرامج تطورًا ملحوظًا فبعد أن كان اختيار الشركاء يعتمد في البداية على الخبرة والقدرة على الوصول إلى الشبكات المستهدفة، أصبحت اليوم تُدار بأسلوب أقرب إلى الشركات الكبيرة. تجدر الاشارة إلى أن الأنشطة المرتبطة بتلك المجموعات لا تركز فقط على قطاعات أو مناطق جغرافية محددة. لذا فإن مواجهة المخاطر المرتبطة بتلك المجموعات تتطلّب تبنّي نهج دفاعي شمولي يركّز على التهديد بحدّ ذاته، وليس على جهة او مجموعة تهديد محددة

فيما يلي أبرز مجموعات برمجيات الفدية الفاعلة في المنطقة خلال الربع الرابع من عام 2025



الشكل رقم(17):
أبرز مجموعات الفدية الفاعلة في المنطقة خلال الربع الرابع من عام 2025

يعكس التوزيع القطاعي لضحايا هجمات برمجيات الفدية الذي لوحظ خلال الربع الرابع من عام 2025 تأثيراً واسع النطاق عبر قطاعات متعددة في المنطقة كما هو موضح في الرسم البياني أدناه.



الشكل رقم(18):

أكثر القطاعات المستهدفة من قبل مجموعات الفدية خلال الربع الرابع من عام 2025

فيما يلي موجز عن أبرز مجموعات الفدية الفاعلة التي حظيت أنشطتها باهتمام كبير خلال الربع الأخير من عام 2025 في المنطقة.

مجموعة CLOP

- تاريخ النشأة: شباط 2019
- أبرز التقنيات والأساليب والتكتيكات المستخدمة

(T1486)	(T1190)	(T1059)	(T1070)
Data Encrypted for Impact	Exploit Public-Facing Application	Indicator Removal	Command and Scripting Interpreter

(T1083)	(T1057)	(T1059.001)
File and Directory Discovery	Process Discovery	Command and Scripting Interpreter -> PowerShell

الدوافع الرئيسية لهذه المجموعة هو تحقيق مكاسب مادية وتُعرف بتنفيذ عمليات ابتزاز واسعة النطاق، تجمع بين سرقة البيانات وتعطيل الانظمة من خلال عمليات تشفير البيانات. كما ترتبط هذه المجموعة بحملات الاختراق وهجمات سلاسل التوريد واسعة النطاق (مثل حملة Accellion FTA عام 2021 وحملة MOVEit Transfer عام 2023) والتي أدت الى إلحاق الضرر بعدد كبير من الضحايا عبر دول وقطاعات متعددة من خلال استغلال ثغرات في برمجيات نقل الملفات واسعة الانتشار.

مجموعة الفدية LOCKBIT

- تاريخ النشأة: شباط 2019
- أبرز التقنيات والأساليب والتكتيكات المستخدمة

(T1027)	(T1059)	(T1490)	(T1059.001)	(T1486)
Obfuscated Files or Information	Command and Scripting Interpreter	Inhibit System Recovery	Command and Scripting Interpreter -> PowerShell	Data Encrypted for Impact

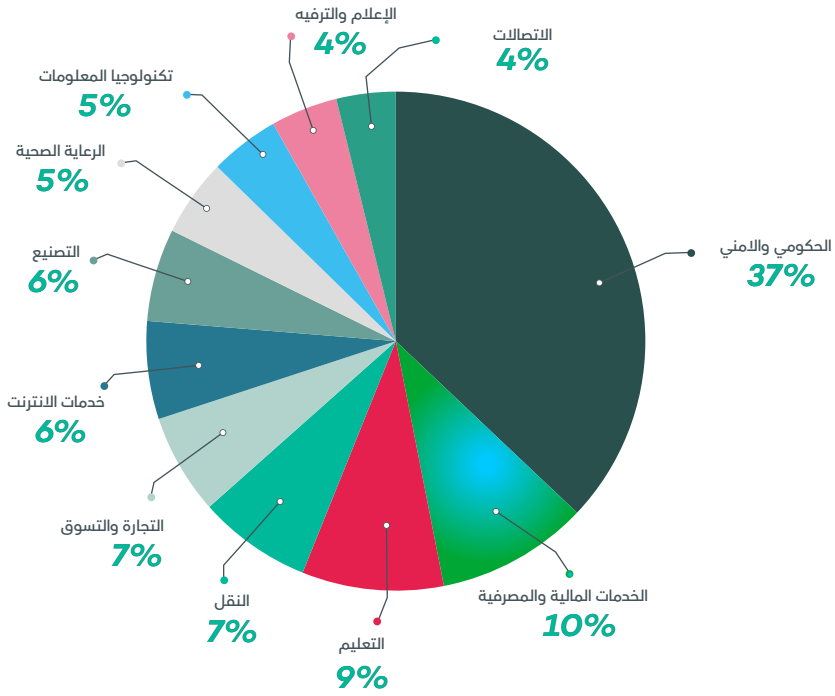
(T1021)	(T1082)	(T1083)	(T1070)	(T1489)
Remote Services	System Information Discovery	File and Directory Discovery	Indicator Removal	Service Stop

تدير المجموعة نموذجًا واسع النطاق لبرمجيات الفدية كخدمة (RaaS) حيث توفّر الأدوات والبنية التحتية للشركاء مقابل حصة من المكاسب المادية. تستهدف هذه المجموعة العديد من المؤسسات حول العالم مما يجعلها واحدة من أكثر مجموعات الفدية نشاطًا حتى اليوم. تعتمد المجموعة على نموذج الابتزاز المزدوج، حيث تقوم بسرقة البيانات الحساسة ومن ثم تقوم بتشفير أنظمة الضحايا. تشير أنشطة المجموعة إلى ان عمليات الاستهداف انتهازية (opportunistic) بشكل كبير وتشمل معظم القطاعات مثل التصنيع والرعاية الصحية والخدمات المالية والحكومات والتعليم والنقل والطاقة وتقنية المعلومات مع الكشف عن ضحايا في جميع أنحاء العالم بما في ذلك منطقة الشرق الأوسط. لا تظهر المجموعة أية دوافع أيديولوجية ويعتقد أن أنشطتها تهدف بشكل رئيسي لتحقيق مكاسب مالية.

مجموعات القرصنة Hacktivism

ازدادت الأنشطة المرتبطة بمجموعات القرصنة تزامنا مع التغيرات والتوترات الجيوسياسية في المنطقة. استهدفت هذه المجموعات بشكل رئيسي القطاعات الحكومية والمالية وقطاع الاتصالات. تهدف هذه المجموعات غالبًا إلى احداث ضجة إعلامية والإضرار بسمعة الجهات المستهدفة ونشر المعلومات المضللة. وتتمثل أبرز أنشطتها في عمليات تشويه المحتوى للمواقع الإلكترونية (Website Defacement) وتسريب البيانات وتنفيذ هجمات حجب الخدمة (DDoS). من الجدير بالذكر ان هذه المجموعات غالبا ما تفتقر إلى القدرات التقنية المتقدمة وتعتمد على استغلال الضعف في تطبيق ممارسات الأمن السيبراني الفضلى واستغلال ثغرات الأنظمة والتطبيقات القديمة غير المحدثة بالإضافة الى استخدام بيانات دخول مسرّبة أو أدوات سيبرانية متاحة بشكل عام. تتسم الأنماط الهجومية لهذه المجموعات بطابع مؤقت ومتقطع حيث تنشط تزامناً مع ازدياد التوترات الجيوسياسية خلال فترات قصيرة في أغلب الأحيان. ومع ذلك لوحظ تحول في سلوك تلك المجموعات في المنطقة عبر استهداف جهات غير متوقعة ما يجعل توسع العمليات خطراً محتملا يتطلب اليقظة والحذر.

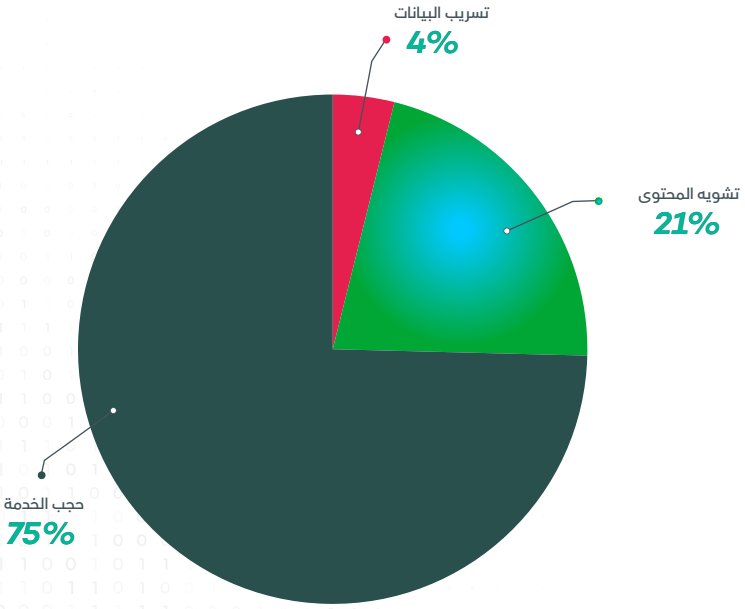
فيما يلي القطاعات المستهدفة في المنطقة من قبل مجموعات القرصنة خلال الربع الرابع من عام 2025



الشكل رقم(19):

أكثر القطاعات المستهدفة من قبل مجموعات الفدية خلال الربع الرابع من عام 2025

كانت هجمات حجب الخدمة هي الأكثر رصدا خلال الربع الرابع من عام 2025 وتوزعت الحوادث المرصودة على النحو التالي:



الشكل رقم(19):

توزيع الحوادث المتربطة بمجموعات القرصنة حسب النوع خلال الربع الرابع 2025

9 أبرز الثغرات الأمنية

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

درجة الخطورة: حرجة 9.3

CVE-2025-14733

الأنظمة المتأثرة:

Fireware OS, including 11.10.2 up to and including 11.12.4_Update1, 12.0 up to and .including 12.11.5, and 2025.1 up to and including 2025.1.3
Firebox models across different product branches, such as T15, T35, T115-W, T125, T145, T185, M295, M395, M495, M595, M695, and others

ثغرة أمنية حرجة تسمح للمهاجم بتنفيذ تعليمات برمجية عشوائية. يتم استغلال هذه الثغرة بشكل نشط حيث أنها تؤثر على كل من شبكة VPN الخاصة بمستخدم ي الأجهزة المحمولة و المكتبية باستخدام بروتوكول IKEv. 2 تم ادراج هذه الثغرة ضمن قائمة الثغرات المستغلة لوكالة CISA الأمريكية.

درجة الخطورة: حرجه 9.8

CVE-2025-59287

الأنظمة المتأثرة:

FortiWeb 8.0.0 through 8.0.1
FortiWeb 7.6.0 through 7.6.4
FortiWeb 7.4.0 through 7.4.9
FortiWeb 7.2.0 through 7.2.11
FortiWeb 7.0.0 through 7.0.11

ثغرة أمنية خطيرة تتيح للمهاجم تجاوز عملية المصادقة وتؤثر على جدران حماية تطبيقات الويب FortiWeb وتسمح بتنفيذ اوامر بصلاحيات مسؤول النظام. وقد أصدرت الشركة Fortinet إجراءات تصحيحات بهذا الخصوص. كما انه اضافت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA)هذه الثغرة الأمنية إلى قائمة الثغرات الامنية المستغلة (KEV) المعروفة نظرا لوجود أدلة على استغلال نشط لها ونظرا لحصولها على تقييم 9.8 في CVSS v 3.1، مما يدل على مستوى تأثيرها الخطر على انظمةFortinet.

درجة الخطورة: حرجة 10.0

CVE-2025-55182

الأنظمة المتأثرة:

React Server Components versions 19.0.0, 19.1.0, 19.1.1, and 19.2.0

ثغرة أمنية خطيرة تعرف ب Shell2React. تم استغلالها بشكل نشط، وحصلت على أعلى درجة خطورة (10.0) وفقا لنظام CVSS. كما قامت وكالة ASIC الأمريكية بإضافة هذه الثغرة الأمنية إلى قائمة الثغرات المستغلة. وقد رصدت أنشطة استغلال هذه الثغرة عبر قنوات متعددة، مع الإشارة إلى استخدامها في هجمات برامج الفدية. تسمح هذه الثغرة تنفيذ التعليمات البرمجية عن بعد (RCE).

درجة الخطورة: حرجة 10.0

CVE-2025-20393

الأنظمة المتأثرة:

Cisco Secure Email Gateway (SEG) – both physical and virtual appliances
Cisco Secure Email and Web Manager (SEWM) – both physical and virtual appliances
All versions of Cisco AsyncOS Software are affected, including up to version 16.0.3-044

ثغرة أمنية حرجة في العديد من منتجات Cisco (Cisco Secure, Cisco Secure Email, Email Gateway, Web Manager) تسمح للمهاجم بتنفيذ أوامر عشوائية عن بعد بامتيازات وصلاحيات مسؤول النظام دون الحاجة لتفاعل المستخدم. يتم استغلال هذه الثغرة بشكل نشط. اضافت وكالة CISA الأمريكية الثغرة إلى قائمة الثغرات المستغلة

درجة الخطورة: مرتفعة

CVE-2025-24990

الأنظمة المتأثرة:

Windows 10 Version 1507, 1607, 1809, 21H2, and 22H2; Windows 11 versions 22H2, 23H2, 24H2, and 25H2; Windows Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022, and 2025, including their Server Core installations

ثغرة امنية في أحد ملفات نظام التشغيل MS Windows. تسمح هذه الثغرة للمهاجمين بالحصول على صلاحيات وامتيازات مسؤول النظام. تم رصد عمليات استغلال واسعة لهذه الثغرة. قامت شركة Microsoft بحذف الملف المرتبط بهذه الثغرة ما أدى الى تأثر بعض أجهزة الفاكس التي تستخدم هذا الملف.

درجة الخطورة: مرتفعة 8.7

CVE-2025-14847

الأنظمة المتأثرة:

MongoDB versions, including 8.2.x (prior to 8.2.3), 8.0.x (prior to 8.0.17), 7.0.x (prior to 7.0.28), 6.0.x (prior to 6.0.27), 5.0.x (prior to 5.0.32), 4.4.x (prior to 4.4.30), and all versions of 4.2.x, 4.0.x, and 3.6.x, with no fixed versions available for the latter

ثغرة أمنية مرتفعة الخطورة تؤثر على خادم MongoDB، وهي قاعدة بيانات NoSQL شائعة الاستخدام في تطبيقات الويب والأنظمة السحابية. تمكن المهاجم من قراءة أجزاء من ذاكرة الخادم بدون صلاحيات مما قد يؤدي لكشف عن بيانات حساسة ورموز Tokens. تم استغلال هذه الثغرة بشكل مكثف، ومع وجود ادلة للاستغلال PoCs اضافت وكالة CISA الأمريكية الثغرة الأمنية إلى قائمة الثغرات المستغلة.

10 نظرة استشرافية

يتوقع ان يشهد الربع الأول من عام 2026 تصاعد ملحوظ في مستوى وتعقيد التهديدات السيبرانية على المستوى العالمي. حيث يعتقد أن يعتمد المهاجمون بشكل أكبر على استخدام تقنيات الذكاء الاصطناعي لأتمتة الهجمات السيبرانية وتوسيع نطاقها. من الممكن ان يؤدي ذلك إلى تنفيذ حملات تصيد الكتروني أكثر إقناعًا وعمليات احتيال تعتمد على التزييف العميق (Deep Fake). كما يُرجّح أن يسهم انتشار نماذج "برمجيات الفدية كخدمة RaaS" في زيادة عدد تلك الهجمات. كما انه من المتوقع ان يتم استهداف قطاعات البنى التحتية الحيوية بشكل أكبر مثل قطاع الطاقة والتصنيع والخدمات اللوجستية من خلال استغلال الثغرات الأمنية في أنظمة التقنيات التشغيلية (OT). إضافة إلى ذلك، ستظل هجمات سلاسل التوريد من أبرز المخاطر مع سعي جهات التهديد المختلفة إلى اختراق موردين والمؤسسات الخارجية 3rd Parties بغرض اختراق عدد أكبر من المؤسسات. للحد من خطورة تلك الهجمات يجب الالتزام بتحديث الأنظمة والتطبيقات بشكل دوري لمعالجة الثغرات الأمنية. كما يُوصى بتأمين خدمات الاتصال عن بعد RDP من خلال تقييد الوصول، واستخدام المصادقة متعددة العوامل أو إغلاقها عند عدم الحاجة. وينبغي تجنب استخدام البرمجيات المقرصنة والاعتماد فقط على البرمجيات المرخصة والمعتمدة. إضافة إلى ذلك، يجب تحسين إعدادات الأنظمة وفق أفضل الممارسات الأمنية.

كما يوصى باتخاذ نهج استباقي لتعزيز منظومة الأمن السيبراني في ظل تصاعد التهديدات السيبرانية وتطورها ويشمل ذلك استخدام حلول أمنية مدعومة بقدرات الذكاء الاصطناعي للكشف المبكر عن الهجمات الحديثة والاستجابة لها بفاعلية. ويجب أيضا تعزيز الحماية من المخاطر المرتبطة بهجمات برمجيات الفدية من خلال عمليات النسخ الاحتياطي المنتظم للبيانات ورفع وعي الموظفين بأساليب التصيد الاحتيالي المبتكرة بالإضافة الى وضع خطط شاملة للتعامل مع كافة أنواع الحوادث السيبرانية.

المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

تـقرير المـوقف الأمـني السـيبراني
Cyber Threat Situational Report

الربـــع الـــرابـــع 2025