المركـز الوطنـــــي
للأمـن السيبرانـــي
National Cyber
Security Center

تقرير المـوقف الأمـني السـيبراني
Cyber Threat Situational Report

الربع الثـــالـث 2025

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

المحتوى

1 الملخص التنفيذي

يهدف هذا التقرير لإعطاء نظرة واضحة حول مشهد التهديدات السيبرانية على المستوى الوطني وعرض أبرز الحوادث السيبرانية التي تم الاستجابة لها بالإضافة الى أبرز ما تشير اليه البيانات الخاصة بمراقبة الشبكات الحكومية والوطنية. كما يتم عرض أبرز الثغرات الأمنية ونقاط الضعف الشائعة التي تم الكشف عنها والتي يمكن ان يتم استغلالها من قبل المهاجمين في تنفيذ الهجمات السيبرانية المختلفة.

تجدر الإشارة الى ان مشهد التهديدات السيبرانية يتغير باستمرار والمعلومات الواردة في هذا التقرير تسهم في نشر ثقافة الوعي السيبراني على المستوى الوطني حيث أن هذا التقرير يسلط الضوء على أكثر القطاعات المعرضة لمثل هذه التهديدات. كما ان التقرير لا يهدف الى التطرق الى الجهود المبذولة من قبل المركز الوطني للأمن السيبراني وكافة النواحي الأخرى للأمن السيبراني والتي تساهم بشكل عام في الحد من خطورة الهجمات السيبرانية بشكل فعال.

أن مشهد التهديدات السيبرانية خلال الربع الثالث من هذا العام اتسم ببروز هجمات برمجيات الفدية وازدياد وتيرتها كأكثر التهديدات السيبرانية خطورة وتطورا. كما تعد الحوادث السيبرانية المرتبطة بالقراصنة كأفراد او مجموعات من أكثر التهديدات شيوعا وتهدف هذه المجموعات بشكل أساسي لإحداث عمليات تأثير اعلامي من خلال هجمات حجب الخدمة او تغيير المحتوى وغيرها من الهجمات. ان وجود أنظمة وبرمجيات غير محدثة أو خارجة عن الدعم قد يؤدي في العديد من الحالات الى تمكن جهات التهديد من استغلال الثغرات الأمنية ونقاط الضعف فيها لاستهداف المؤسسات الوطنية للوصول واختراق أنظمتها وشبكاتها.

2 أبرز الأنشطة والمؤشرات المحلية

- رصد عدد من الهجمات السيبرانية المرتبطة بمجموعات القرصنة Hacktivists استهدفت عددا من المؤسسات الوطنية.
- رصد العديد من الهجمات السيبرانية المرتبطة بمجموعات برمجيات الفدية Ransomware
- رصد تسريب حسابات دخول رسمية خاصة بموظفي بعض المؤسسات الحكومية
- الكشف عن العديد من الثغرات الأمنية التي ترتبط بأنظمة وبرمجيات غير محدثة او خارجة عن الدعم
- الكشف عن العديد من نقاط الضعف على الشبكات الخاصة ببعض المؤسسات الوطنية:

✓ الكشف عن العديد من أنظمة الإدارة والتحكم ومنصات إدارة قواعد البيانات مكشوفة على شبكة الإنترنت
✓ رصد بعض الخدمات الالكترونية التي تستخدم بروتوكولات غير آمنة
✓ الكشف عن وجود اعدادات خاطئة وغير آمنة الخاصة بخدمات الشبكة الافتراضية VPN

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

شكلت حوادث برمجيات الفدية Ransomware كأبرز الحوادث السيبرانية المرصودة محليا حيث لوحظ ازدياد في تلك الحوادث نسبة للربع الثاني من هذا العام. تعد هجمات برمجيات الفدية من أكثر التهديدات الشائعة والتي لها تأثيرات ضارة على المؤسسات من حيث الاضرار بالسمعة او الخسائر المادية المرتبطة بتعطل الخدمات او في حال الاستجابة ودفع الفدية.

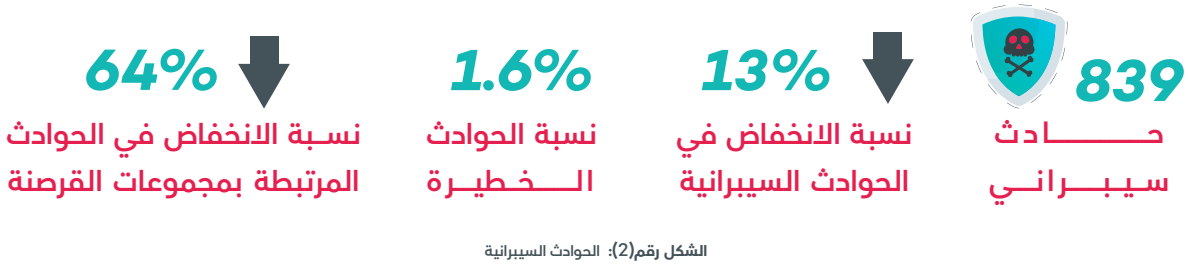
بالإضافة لذلك تم رصد عدد محدود من الحوادث المرتبطة بمجموعات التهديد المتطورة APTs والتي استهدفت بعض المؤسسات الوطنية الحيوية. تؤكد المؤشرات والأدلة الرقمية على أن الغرض الرئيسي للأنشطة السيبرانية المرتبطة بتلك المجموعات والتي تتمثل في اختراق مؤسسات محددة هو البقاء والتخفي وجمع المعلومات وسرقتها لدعم الأهداف الاستراتيجية والجهات الداعمة لتلك المجموعات.

من اهم الأسباب الرئيسية المؤدية للحوادث السيبراني المرصودة محليا:

✓ عدم تحديث الانظمة والبرمجيات بشكل مستمر.
✓ استخدام برمجيات وأنظمة غير مرخصة او خارجة عن الدعم.
✓ استخدام إعدادات افتراضية او خاطئة وغير آمنة.
✓ ضعف في تطبيق سياسات الامن السيبراني الفضلى.
✓ نقص وعي الأفراد بمخاطر التهديدات السيبرانية.

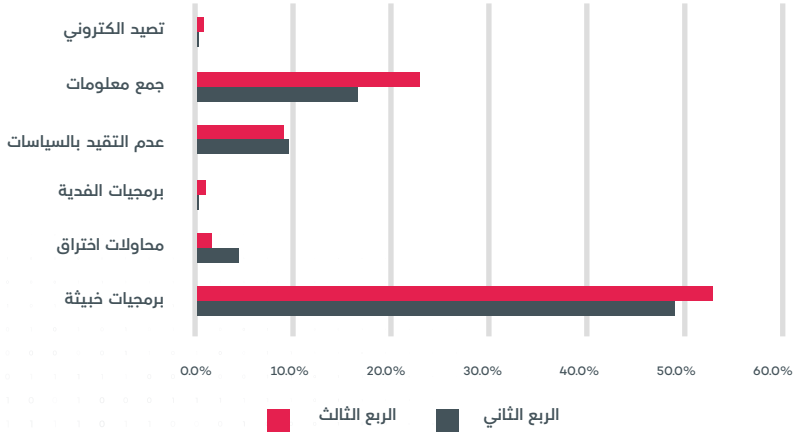
أبرز ما تشير اليه بيانات مراقبة الشبكات الوطنية

تشير بيانات مراقبة الشركات الوطنية الى انخفاض في عدد الحوادث السيبرانية المرصودة بنسبة بلغت 13% مقارنة بالربع الماضي وما تزال نسبة الحوادث الخطيرة تشكل نسبة محدودة (1.6%) من مجموع الحوادث المرصودة والتي تقارب تلك التي تم رصدها في الربع الثاني. لوحظ انخفاض في نسبة حوادث "محاولات الاختراق" حيث بلغت نسبتها 1.6% مقارنة ب 4.1% في الربع الثاني. كما تشير البيانات الى ازدياد الحوادث السيبرانية ذات الدوافع المادية بشكل بارز مثل هجمات برمجيات الفدية.
من أبرز التغيرات المرصودة انخفاض الحوادث المرتبطة بمجموعات القرصنة Hacktivists بنسبة تقارب 64% نسبة للربع الثاني من هذا العام. قد يعود ذلك الى التغيرات في الأوضاع الجيوسياسية التي شهدتها المنطقة خلال تلك الفترة.



الشكل رقم(2): الحوادث السيبرانية

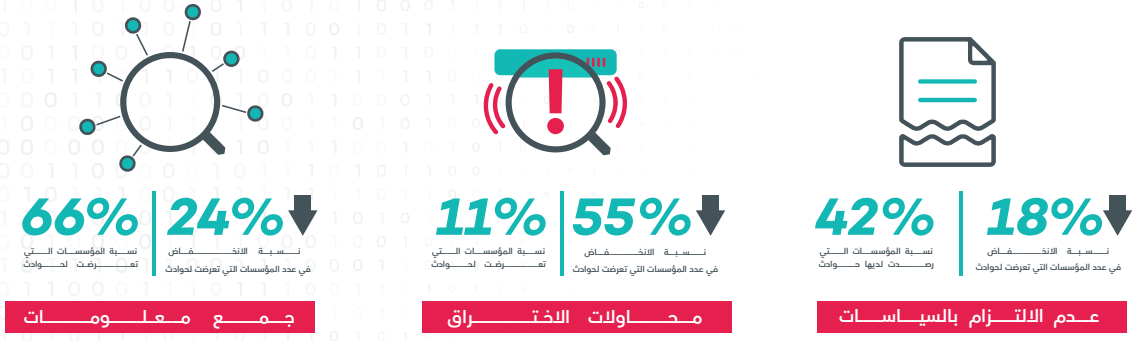
الشكل التالي يوضح التغير في نسبة الحوادث التي تم رصدها خلال الربعين الثاني والثالث. يلاحظ ان حوادث "جمع المعلومات" و"البرمجيات الخبيثة" ازدادت بنسبة قليلة فيما انخفضت نسبة حوادث "محاولات الاختراق".



الشكل رقم(3)

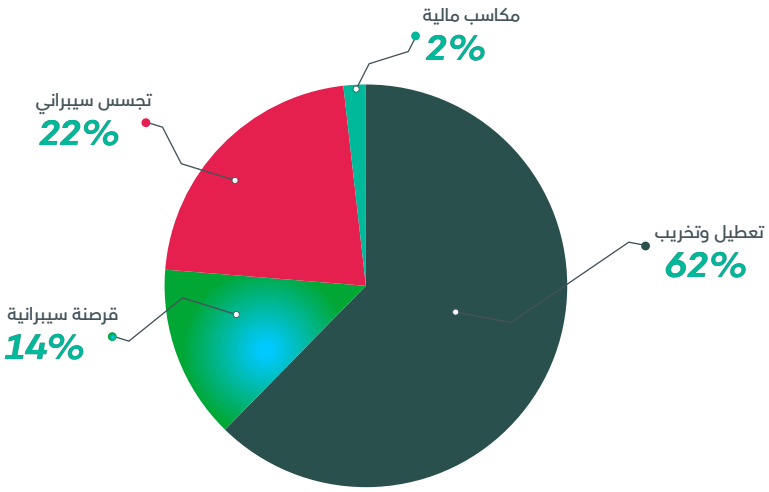
نسبة الحوادث لسيبرانية خلال الربعين الثاني والثالث

فيما يتعلق بالمؤسسات التي يتم مراقبة شبكاتها، كانت أبرز التغيرات انخفاض في نسبة المؤسسات التي تعرضت لـ"محاولات اختراق"، حيث بلغت النسبة 11% في الربع الثالث مقارنة بـ 25% في الربع الثاني من هذا العام. كما لوحظ ارتفاع بسيط في نسبة المؤسسات التي رصدت لديها حوادث "عدم الالتزام بالسياسات" حيث بلغت 42% في الربع الثالث مقارنة بـ 36% في الربع الثاني. تتسق هذه الاحصائيات مع التغيرات في المشهد العام للتهديدات السيبرانية وانخفاض نسبة الحوادث السيبرانية.

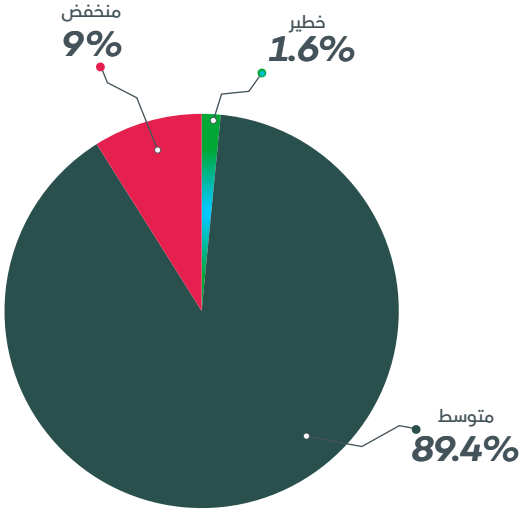


الشكل رقم(4):
ما تشير اليه بيانات الحوادث السيبرانية

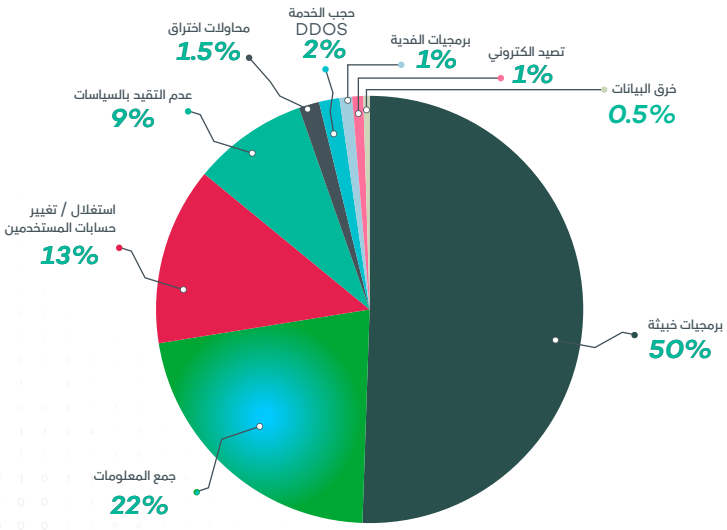
الرسوم البيانية التالية تبين توزيع الحوادث السيبرانية حسب الأهداف، النوع، درجة الخطورة بالإضافة الى توزيع الحوادث السيبرانية التي تم الاستجابة لها حسب القطاع:



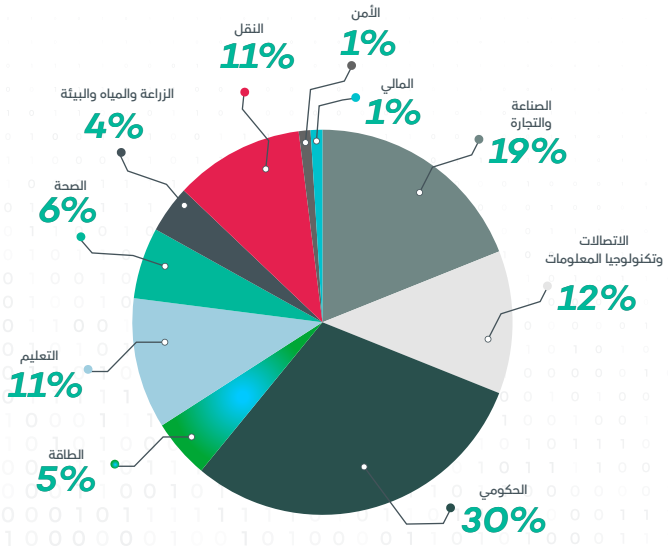
الشكل رقم(5):
توزيع الحوادث السيبرانية (حسب الأهداف)



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 الجزء عرض نقاط الضعف المكتشفة وتسليط الضوء حول مدى خطورتها على المؤسسات الوطنية.

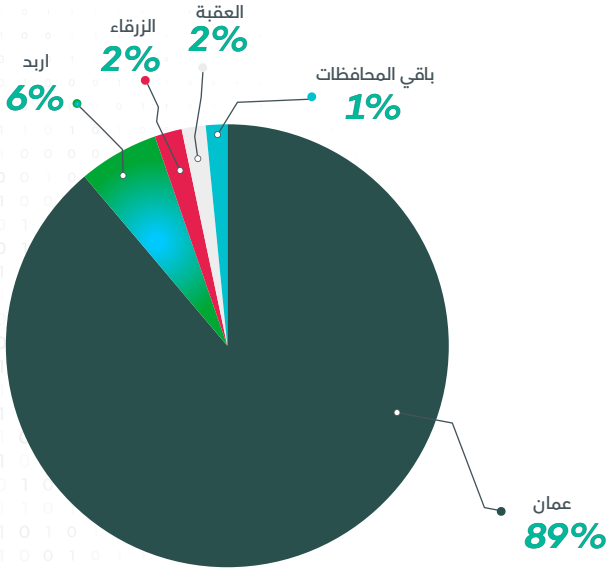
انخفضت نسبة الثغرات الحرجة الى 11% مقارنة بـ 17% في الربع الثاني من هذا العام. من الملاحظ ان النسبة الأكبر من الثغرات الحرجة في أحد أنظمة البريد الالكتروني شائعة الاستخدام انخفضت بشكل كبير (من 9.9% في الربع الثاني الى 0.7% في الربع الثالث).

توزعت أصول المؤسسات الوطنية الرقمية على النحو التالي:

42725
أصول رقمية

1.18%
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

ما تزال المنافذ المفتوحة غير الآمنة تشكل نسبة كبيرة (33.7%) من المنافذ الشبكية Network Ports التي تم رصدها على المستوى الوطني والتي تقارب بيانات الربع السابق. يشكل بروتوكول HTTP المستخدم بشكل كبير في الخوادم التي تستضيف المواقع والخدمات الإلكترونية النسبة الأكبر (16%) من مجموع تلك المنافذ.

33.7%
منافذ البروتوكولات غير الآمنة

16%
نسبة منفذ برتوكول HTTP المفتوح

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.

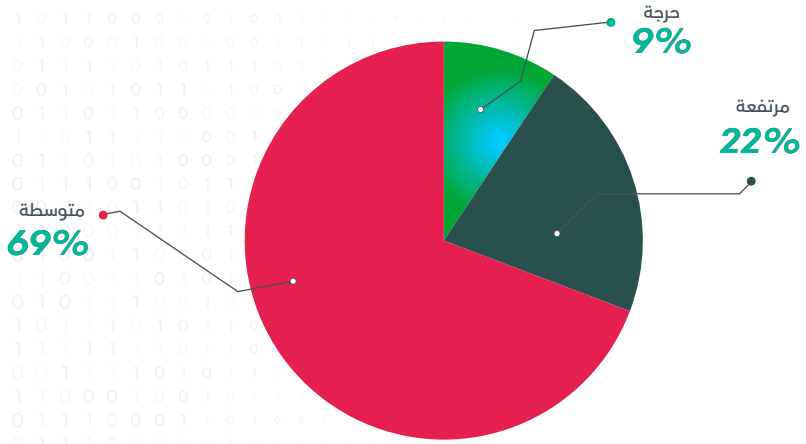
كانت أكثر الأنظمة انتشارا على المستوى الوطني وتحتوي على ثغرات مرتفعة الخطورة وحرجة:

- WordPress
- Apache HTTP Server
- OpenSSH
- Exim

5 احصائيات فحوصات الثغرات والاختراق (نطاق حكومي)

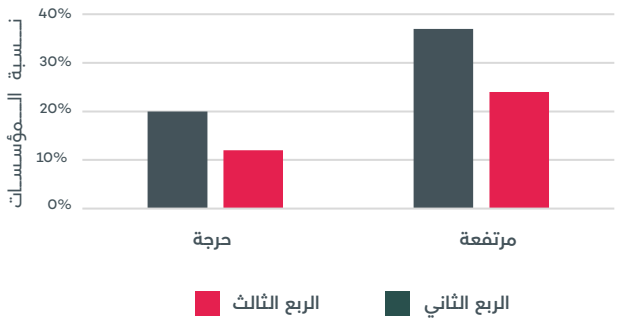
تم إجراء فحوصات لكشف الثغرات على المواقع الإلكترونية للمؤسسات، وكان مجموع الثغرات الأمنية التي تم ايجادها (64) ثغرة (حرجة ومرتفعة الخطورة) على المواقع الالكترونية.

يبين الشكل التالي نتائج فحوصات الثغرات للمواقع الرئيسية للمؤسسات الحكومية وعددها 115 مؤسسة.
انخفضت نسبة الثغرات الحرجة والخطيرة المرصودة على المواقع الرئيسية للمؤسسات الحكومية. حيث بلغت نسبة الثغرات الحرجة 9% في الربع الثالث مقارنة بـ 14% في الربع الثاني فيما انخفضت نسبة الثغرات مرتفعة الخطورة الى 22% مقارنة بـ 38% في الربع الثاني. قد تشير هذه البيانات الى تحسن ملحوظ في التدابير المتخذة من قبل تلك المؤسسات لتعزيز الامن السيبراني لديها.



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

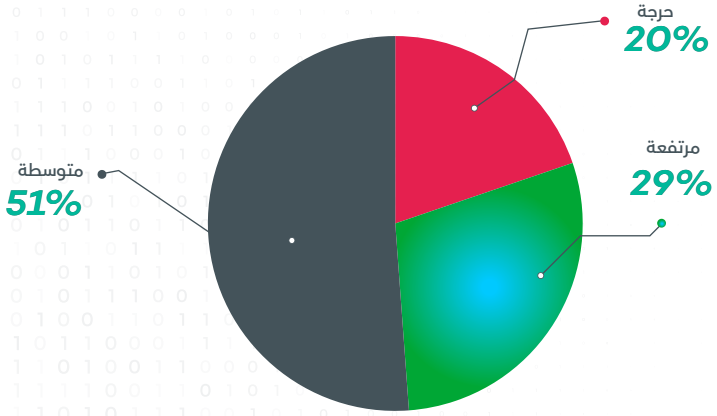
كما لوحظ انخفاض في عدد المؤسسات التي رصدت لديها ثغرات أمنية حرجة ومرتفعة على مواقعها الرئيسية حيث انخفضت نسبة المؤسسات من 20% في الربع الثاني الى 12% في الربع الثالث بالنسبة للثغرات الأمنية الحرجة فيما انخفضت النسبة من 37% في الربع الثاني الى 24% في الربع الثالث بالنسبة للثغرات الأمنية مرتفعة الخطورة.



الشكل رقم(11):
المؤسسات التي رصدت لديها ثغرات أمنية على مواقعها الرئيسية خلال الربعي الثاني والثالث

تم إجراء فحوصات لكشف الثغرات للخوادم في مركز البيانات الحكومي لعدد من المؤسسات الحكومية بلغ عددها (70) مؤسسة. بلغ مجموع الثغرات الأمنية الخطيرة التي تم ايجادها (512) ثغرة وعدد الخوادم والأجهزة التي تم فحصها (18167) خادم/جهاز. ما تزال الغالبية العظمى من الثغرات الحرجة تعد قديمة نسبيا. مع نسبة انخفاض بلغت 3% للثغرات القديمة (سنتين فأكثر)

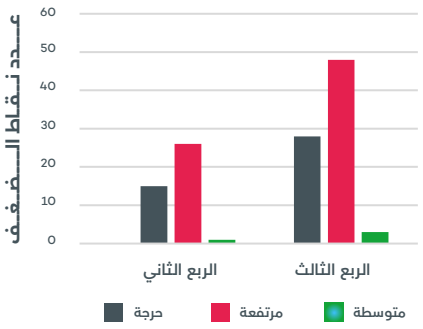
كما قام المركز بإجراء فحوصات اختراق لعدد من المؤسسات الوطنية حيث بلغ عدد المؤسسات التي تم تنفيذ فحص الاختراق لها (14) مؤسسة وبلغ العدد الاجمالي لفحوصات الاختراق (Penetration Testing) المنفذة (42) فحص شملت فحص المواقع والخدمات الالكترونية والتي تم من خلالها الكشف عن وجود (86) ثغرة.



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

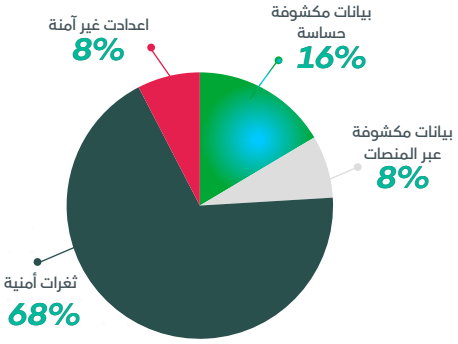
6 نقاط الضعف المرصودة في بعض المؤسسات الوطنية

تم رصد العديد من نقاط الضعف المختلفة في عدد من المؤسسات الوطنية. تشير البيانات الى ارتفاع ملحوظ وبارز في عدد نقاط الضعف المكتشفة خلال الربع الثالث. حيث ارتفعت من 42 خلال الربع الثاني لتصل الى 79 نقطة ضعف بنسبة تقارب 88%. غالبية نقاط الضعف المكتشفة بسبب استخدام برمجيات غير محدثة أو خارجة عن الدعم. من الملاحظ ان غالبية الثغرات الأمنية المرتبطة بهذه البرمجيات ترتبط بعدد محدود من المؤسسات ما قد يشير الى عمليات تثبيت واستحداث لأنظمة مستجدة لدى تلك المؤسسات. كما أن غالبية الأنظمة التي تحتوي ثغرات أمنية حرجة تستخدم في إدارة المحتوى وتقديم خدمات الويب.

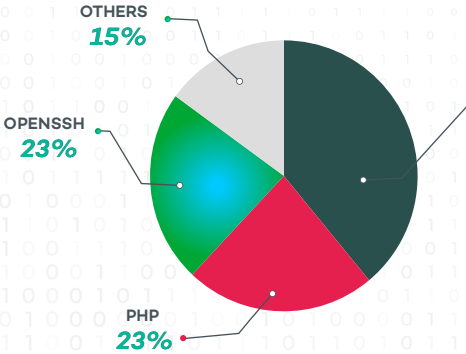


الشكل رقم(13):
نقاط الضعف (حسب الخطورة) خلال الربعين الثاني والثالث

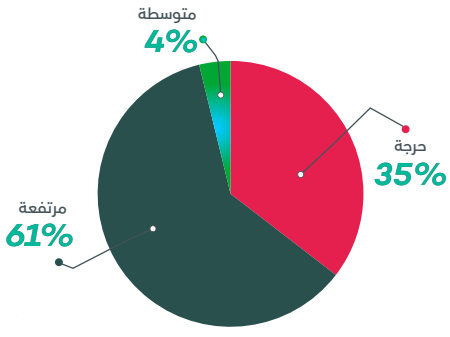
التصنيفات الرئيسية لنقاط الضعف المكتشفة وتوزيع نقاط الضعف المكتشفة حسب الخطورة وتوزيع الأنظمة التي تحتوي على نقاط ضعف (حرجة) وكما هو مبين أدناه:



الشكل رقم(14):
تصنيف نقاط الضعف المكتشفة



الشكل رقم(16):
توزيع الأنظمة التي تحتوي نقاط ضعف (حرجة)



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

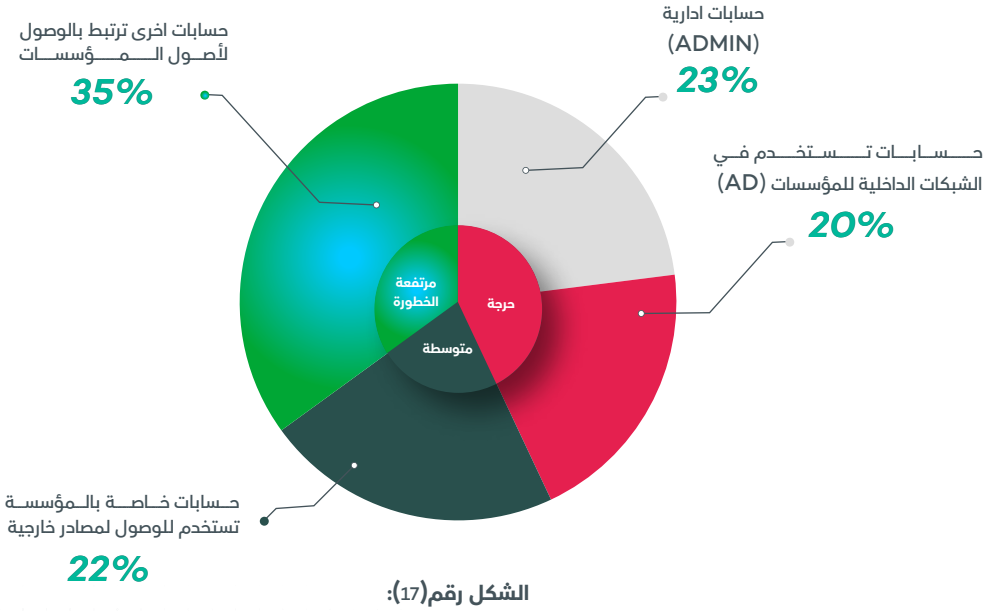
كما تم رصد نقاط الضعف التالية:

- رصد بعض البيانات المكشوفة على منصات مشاركة الملفات المتاحة على الانترنت مثل GitHub.
- بعض الخدمات الالكترونية والأنظمة تستخدم اعدادات غير آمنة مما يسمح للمهاجم باستغلالها.
- بعض المواقع الالكترونية تسمح بعرض محتويات الموقع مما قد يؤدي للكشف عن بيانات حساسة.

7 البيانات المسربة والمكشوفة *Leaked & Exposed Data*

تم رصد ازدياد في تسريب الحسابات المرتبطة بأنظمة وخدمات الكترونية للمؤسسات الحكومية. بعض هذه الحسابات تخص موظفين أو المستخدمين الخارجيين (العملاء) الذين يملكون صلاحية الوصول لموارد أو تطبيقات المؤسسات. غالبا ما يتم تسريب بيانات الحسابات من خلال الإصابة ببرمجيات "سرقة المعلومات Infostealers" الخبيثة عن طريق تثبيت برمجيات مقرصنة وغير مرخصة يتم توزيعها ونشرها من قبل المهاجمين عبر العديد من الوسائل المختلفة.

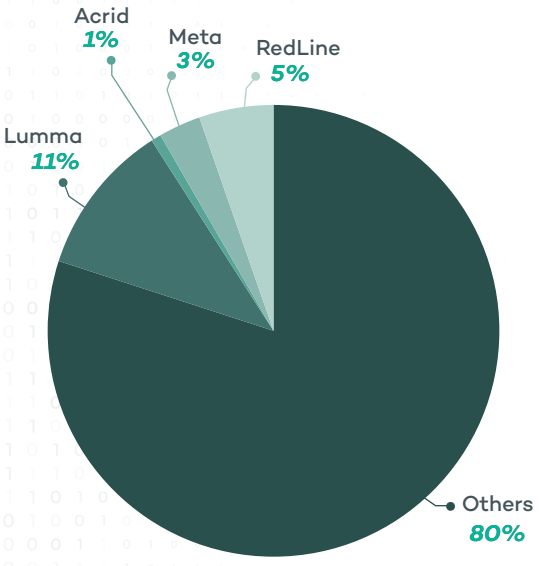
يبين الشكل التالي توزيع لتلك الحسابات المسربة حسب نوع الحساب ودرجة خطورة التسريب:



الشكل رقم(17):

توزيع الحسابات المسربة (حسب نوع الحساب ودرجة الخطورة)

يوضح الشكل التالي برمجيات سرقة المعلومات المرتبطة بالحسابات المسربة



الشكل رقم(18):

توزيع الحسابات المسربة حسب نوع برمجيات سرقة المعلومات

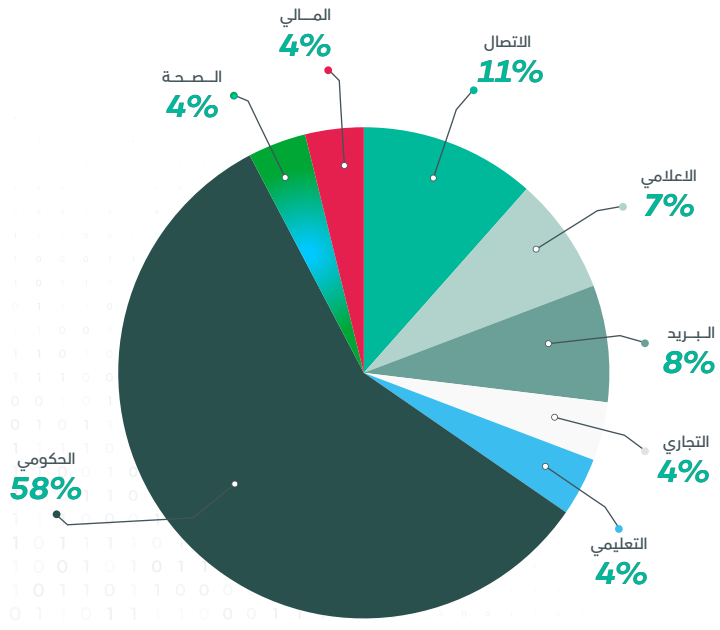
توصيات للحد من مخاطر الحسابات المسربة

- اجراء فحص شامل للجهاز المرتبط بالتسريب للكشف عن وجود برمجيات خبيثة.
- تغيير كلمات المرور المستخدمة في الحسابات الأخرى.
- تطبيق سياسة كلمات المرور القوية.
- عقد ورشات توعية وتدريب الموظفين حول طرق الإصابة بالبرمجيات الخبيثة

8 انتحال الهوية الرقمية للمؤسسات Brand Abusing

تسعى جهات التهديد السيبرانية 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 (33) من المواقع الإلكترونية او صفحات التواصل الاجتماعي المزيفة والمشابهة لمواقع الكترونية وطنية بانخفاض بلغت نسبتها 39% مقارنة بالربع الثاني. يعود السبب الرئيسي في ذلك الانخفاض الى الأنشطة المرتبطة بمجموعات القرصنة نظرا للتغيرات في الأوضاع الإقليمية في ذلك الوقت. شكل القطاع الحكومي ما نسبته 58% من القطاعات المستهدفة.



الشكل رقم(19):
القطاعات المستهدفة في عمليات انتحال الهوية الرقمية BRAND ABUSE

للحد من المخاطر المرتبطة يتم إزالة تلك المواقع الالكترونية او الصفحات الخاصة بمواقع التواصل الاجتماعي حيث تم إزالة (19) من تلك المواقع الالكترونية او صفحات التواصل الاجتماعي.

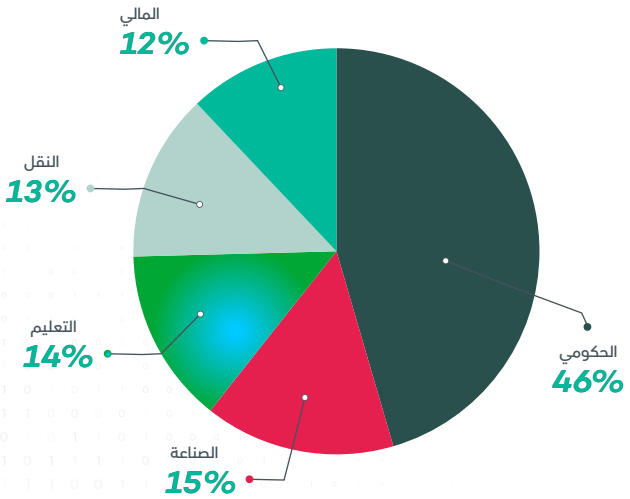
توصيات لإدارة واجهة التهديدات السيبرانية للمؤسسة

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

9 المؤشرات الإقليمية والعالمية

تتميز بيئة التهديدات السيبرانية بالتعقيد والتغير بشكل مستمر. يعد رصد الاتجاهات السائدة وتحليل المتغيرات التي تطرأ على مشهد التهديدات السيبرانية أمرا ضروريا نظراً لاختلاف جهات التهديد وتقنيات الهجوم. كما يُعد الاطلاع المنتظم على التقارير الأمنية والمعلومات الفنية الحديثة أمراً محورياً لفهم الأساليب والتقنيات الجديدة التي توظفها جهات التهديد. تدعم هذه البيانات المحدثة قدرة المؤسسات في تعزيز عمليات الاستجابة للحوادث السيبرانية وفي اتخاذ التدابير الوقائية المناسبة.

خلال الربع الثالث كانت غالبية الهجمات السيبرانية تستهدف القطاع الحكومي. يوضح الشكل التالي أكثر القطاعات المستهدفة بالهجمات السيبرانية.



الشكل رقم(20):
أكثر القطاعات المستهدفة بالهجمات السيبرانية

كما كانت اكثر التقنيات الشائعة والتي تستخدم من قبل المهاجمين في الوصول الى الأنظمة المستهدفة:

- خدمات الاتصال عن بعد Remote Services
- حسابات مستخدمين داخل شبكة المؤسسة Domain Accounts
- حسابات المستخدمين المحلية Local Accounts
- التصيد الالكتروني Phishing

مجموعات التهديد المتطورة APTs

كشف الباحثون عن عدد من التهديدات السيبرانية المؤثرة المرتبطة بتلك المجموعات. استخدم المهاجمون التقنيات مثل استغلال الثغرات الامنية Zero-day. كما استمر المهاجمون في استخدام وسائل الهندسة الاجتماعية والتصيد الإلكتروني كوسيلة فعالة للوصول الى الشبكات والأنظمة المستهدفة.

طور المهاجمون أساليب وطرق أكثر اقناعا للضحايا للاستجابة ودفعهم لتفعيل البرمجيات الخبيثة من خلال استخدام ملفات وثائق ذات صلة بالأحداث الجيوسياسية. كما استخدم المهاجمون بريد الكتروني مخترق لخداع الضحايا وإعطاءهم موثوقية أكبر للمحتوى التصيدي واستخدم في حالات أخرى علامات تجارية مألوفة، وبنية تحتية قابلة للتوسع وموثوقة وتدعم عمليات سرقة بيانات الاعتماد وعمليات الوصول الاولي من خلال اتمتة عمليات نشر برمجيات وأدوات خبيثة متخصصة لسرقة هذه البيانات. لوحظ استغلال المهاجمون لمنصات مشاركة الملفات العامة بغرض استضافة ونشر الملفات الخبيثة من خلال ارسال روابط إلكترونية مشبوهة عبر البريد التصيدي.

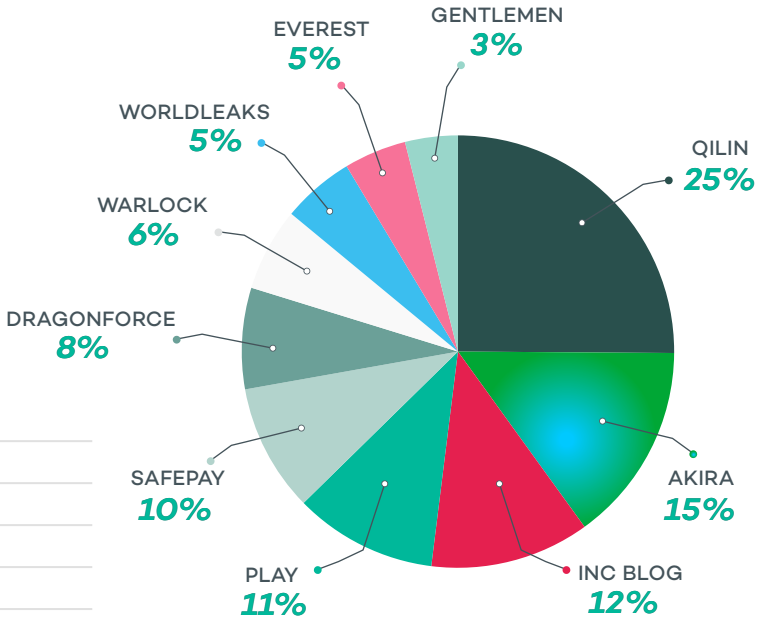
أبرز أنشطة مجموعات التهديد المتطورة

- لوحظ استخدام احدى مجموعات التهديد المتطورة الإقليمية بشكل متزايد لحسابات مستخدمين مخترقة ذات صلة بمؤسسات حساسة وكما استخدم مرفقات تحتوي على ملفات نصية تتضمن أكواد برمجية خبيثة.
- استخدمت احدى هذه المجموعات وسائل التخزين USB Devices كوسيلة للدخول واختراق الشبكات المستهدفة.
- لوحظ استخدم العديد من هذه المجموعات أسلوب التحايل على الضحايا من خلال ارسال برمجيات ذات صفة موثوقة لخداعهم والايقاع بهم.
- استخدمت احدى هذه المجموعات بريد تصيدي موجه Spearphishing يتضمن ملفات وثائق تنتحل صفة رسمية .
- استغلت احدى هذه المجموعات واجهات برمجة التطبيقات API لاستخدام تقنيات الذكاء الاصطناعي AI في عمليات انشاء وتشغيل الأوامر البرمجية الخبيثة بشكل تفاعلي ومرن.

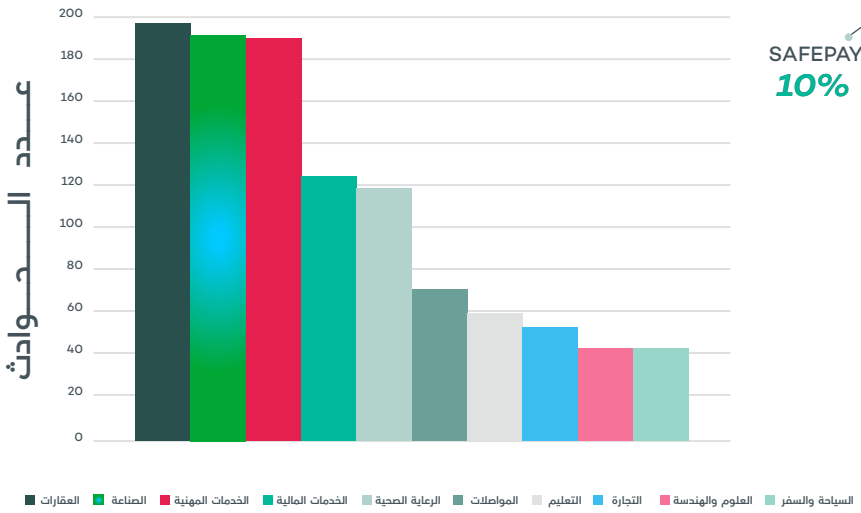
مجموعات برمجيات الفدية Ransomware

يعد نموذج برامج الفدية كخدمة (RaaS) من أبرز الأسباب الرئيسية لانتشار وتوسع عمليات وهجمات برمجيات الفدية. من خلال مراقبة تطور هذا النموذج ومتابعة المواقع الإلكترونية الخاصة بمجموعات برمجيات الفدية يمكن الكشف عن نطاق هذه العمليات ومدى تأثيرها في جميع أنحاء العالم. يعتمد نموذج البرمجية كخدمة على إيجاد قراصنة تابعين من ذوي الخبرة متخصصين في تنفيذ أدوار ومراحل محددة من الهجوم السيبراني.

تشير البيانات الخاصة بمنصات مجموعات برمجيات الفدية المخصصة لنشر بيانات الضحايا الى تنفيذ عدد متقارب من الهجمات خلال الربع الثاني والثالث من هذ العام. من الجدير بالملاحظة ان عدد مجموعات برمجيات الفدية النشطة التي قامت بنشر بيانات عبر تلك المنصات كان أكثر بنسبة تقارب 14% خلال الربع الثالث مقارنة بالربع الثاني.



الشكل رقم(21):
أبرز مجموعات الفدية خلال الربع الثالث من عام 2025



الشكل رقم(22):
أكثر القطاعات المستهدفة من قبل مجموعات الفدية خلال الربع الثالث من عام 2025.

مجموعات القرصنة Hacktivism

تم رصد عدد كبير من الهجمات المرتبطة بمجموعات القرصنة، بما في ذلك هجمات حجب الخدمة (DDoS)، وهجمات تغيير المحتوى (Defacements)، وعمليات التأثير الإعلامي (Information Operations). غالباً ما تتأثر العمليات الخاصة بهذه المجموعات بفعل التغييرات والأوضاع الجيوسياسية، وتهدف عادة لتحقيق أهداف سياسية أو مكاسب مادية.

فيما يلي أبرز بعض الحوادث السيبرانية المكتشفة:

- استغل مهاجمون منصة تيليغرام Telegram لإنشاء صفحات تصيد تحاكي منصات لشركات مشهورة مثل DHL, FedEx وغيرها، تستخدم هذه الصفحات الوهمية بهدف جمع معلومات الضحية، البيانات المالية وفي بعض الأحيان بيانات الدخول للحسابات البنكية.
- استخدمت احدى مجموعات القرصنة منصة تيليغرام لإنشاء ونشر برمجيات خبيثة متطورة بهدف سرقة الرسائل النصية للضحايا (SMS) واستغلالها.
- استهدفت احدى هذه المجموعات أنظمة صناعية ICS في العديد من الدول حيث تم الكشف عن 82 حادث في عدد من الدول الأوروبية بشكل رئيسي والتي تهدف الى تعطيل عمليات تشغيل الأنظمة.
- تم الكشف عن استهداف احدى هذه المجموعات لمنصة Salesforce المستخدمة على نطاق واسع عالميا. قام المهاجمون بإرسال بريد تصيدي موجه لموظفين في مناصب عليا بهدف الحصول على بيانات الدخول لهذه الحسابات ذات الصلاحيات العالية.

10 أبرز الثغرات الأمنية

فيما يلي أبرز الثغرات الأمنية المكتشفة خلال الربع الثالث من هذا العام والتي تم استغلالها على نطاق واسع:

درجة الخطورة: حرجة

CVE-2024-8963

الأنظمة المتأثرة:
Ivanti CSA 4.6 and prior versions

ثغرة أمنية حرجة يؤدي استغلالها الى السماح للمهاجم بتنفيذ وظائف مقيدة (Restricted) على النظام المستهدف. تشير درجة الخطورة إلى وجود احتمال كبير للتأثير على سرية البيانات ودقتها. كما يمكن الدمج بين استغلال هذه الثغرة بالإضافة الى ثغرات أخرى لتحقيق تأثيرات اكثر خطورة مثل تنفيذ التعليمات البرمجية عن بعد، سرقة بيانات الدخول ونشر البرمجيات الخبيثة.

درجة الخطورة: حرجة

CVE-2025-53770

الأنظمة المتأثرة:
Microsoft SharePoint Server Subscription Edition - patch is available
Microsoft SharePoint Server 2019- patch is available
Microsoft SharePoint Server 2016 patch is NOT available yet

ثغرة امنية جديدة (Zero-day) ذات خطورة حرجة تسمح بتنفيذ تعليمات برمجية عن بعد (RCE) دون أي تفاعل من قبل المستخدم الامر الذي يؤدي الى السيطرة الكاملة على الخادم المستهدف. من الجدير بالذكر ان المهاجمين غالبا ما يقومون بسرقة مفاتيح تشفير والتي تسمح لهم بالحفاظ على إمكانية الوصول للخادم حتى بعد تنفيذ عملية التصحيح. لذا يجب على المؤسسات التي تستخدم هذه الأنظمة المتأثرة تنفيذ التوصيات الفنية الصادرة من قبل الشركة.

درجة الخطورة: حرجة

CVE-2025-7775

الأنظمة المتأثرة:
NetScaler ADC and Gateway versions 13.1 before 13.1-59.22, 14.1 before 14.1-47.48, 13.1-FIPS and NDcPP before 13.1-37.241-FIPS and NDcPP, and 12.1-FIPS and NDcPP before 12.1-55.330-FIPS and NDcPP

ثغرة أمنية جديدة تسمح للمهاجم بتنفيذ تعليمات برمجية عن بعد وتنفيذ عمليات حجب الخدمة DoS. تم رصد عمليات استغلال على نطاق واسع لهذه الثغرة مع وجود تقارير تفيد بتثبيت المهاجم لأدوات بغرض البقاء داخل الأنظمة المستهدفة. يوصى بشدة بأن تقوم المؤسسات بالتحديث إلى الإصدارات الاخيرة، حيث إن الإصدارين 12.1 و13.0 توقف الدعم الفني لهما (EOL) ويجب التحديث إلى الإصدارات الجديدة المدعومة.

درجة الخطورة: حرجة

CVE-2025-20333

الأنظمة المتأثرة:
Cisco ASA (9.16, 9.17, 9.18, 9.19, 9.20, 9.22)
Cisco FTD (7.0, 7.2, 7.4, 7.6)

ثغرة أمنية تسمح للمهاجم لديه بيانات دخول VPN صالحة بتنفيذ تعليمات برمجية عشوائية بصلاحيات عالية. تم استغلال الثغرة بشكل نشط وتمت إضافتها إلى أرشيف الثغرات المستغلة المعروفة (KEV) التابع لوكالة الأمن السيبراني وأمن البنى التحتية الأمريكية CISA

درجة الخطورة: مرتفعة (Zero-day)

CVE-2025-6554

الأنظمة المتأثرة:
جميع الاصدارات ما قبل 138.0.7204.96
كما قد تتأثر المتصفحات الأخرى المستندة إلى الكروم، مثل Microsoft Edge وBrave وOpera وVivaldi

ثغرة أمنية مرتفعة جديدة (Zero-day) في متصفح Google Chrome تتيح للمهاجم تنفيذ عمليات برمجية عن بعد. تم استغلال هذه الثغرة على نطاق واسع مع وجود أدلة تشير إلى استخدامها في تنفيذ هجمات محددة الاهداف قد ترتبط بمجموعات التهديد المتطورة او لأغراض تجسسية.

درجة الخطورة: مرتفعة

CVE-2025-52970

الأنظمة المتأثرة:
7.6.3 and below - 7.4.7 and below - 7.2.10 and below - 7.0.10 and below

ثغرة امنية في نظام Fortinet FortiWeb تسمح للمهاجم بالحصول على صلاحيات مسؤول النظام. لا يوجد أي دليل على وجود عمليات استغلال او كود برمجي Exploit لاستغلال هذه الثغرة. لكن تجدر الإشارة الى أن التأثير المحتمل لاستغلالها خطير، وقد يؤدي الى سيطرة كاملة على نظام FortiWeb، واختراق الشبكة والوصول إلى بيانات حساسة.

درجة الخطورة: مرتفعة

CVE-2025-53786

الأنظمة المتأثرة:
Microsoft Exchange Server 2016 (Cumulative Update 23)
Microsoft Exchange Server 2019 (Cumulative Update 14 and Cumulative Update 15)
Microsoft Exchange Server Subscription Edition RTM

ثغرة أمنية مرتفعة الخطورة في بيئة خوادم MS Exchange قد تسمح للمهاجم بترقية الصلاحيات Privilege Escalation وامكانية اختراق نطاق المؤسسة (Domain) بشكل كامل.

درجة الخطورة: مرتفعة

CVE-2025-55234

الأنظمة المتأثرة:
Windows 10, Windows 11, and Windows Server, including Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, and Windows Server 2025

ثغرة أمنية تسمح للمهاجم بتنفيذ هجمات إعادة توجيه "Relay Attacks" عند استغلاله لهذه الثغرة في برتوكول SMB (Server Message Block) الخاصة بأنظمة MS Windows مما يؤدي إلى رفع الامتيازات وربما الوصول الكامل للنظام.

درجة الخطورة: مرتفعة

CVE-2025-38352

الأنظمة المتأثرة:
Linux distributions and systems, including Debian, Ubuntu, Red Hat, CentOS, SUSE Linux Enterprise, openSUSE, Amazon Linux, and Android devices running vulnerable kernel versions

ثغرة أمنية تسمح للمهاجم بتخطي جدار الحماية (FW) وتنفيذ تعليمات برمجية خبيثة ما يمكن أن تؤدي الى عدم استقرار النظام واحتمال حدوث حجب للخدمة (DoS). أشارت عدة تقارير الى وجود عمليات استغلال واسعة النطاق لهذه الثغرة.

11 نظرة استشرافية

يعد رصد الاتجاهات السائدة وتحليل المتغيرات التي تطرأ على مشهد التهديدات السيبرانية أمرا ضروريا نظراً لاختلاف جهات التهديد وتقنيات الهجوم. كما يُعد الاطلاع المنتظم على التقارير الأمنية والمعلومات الفنية الحديثة أمراً محورياً لفهم الأساليب والتقنيات الجديدة التي توظفها جهات التهديد، سواء كانت جهات إجرامية، أو مجموعات ذات دوافع سياسية، أو حتى تهديدات ناتجة عن أخطاء بشرية أو ثغرات تقنية.

ما تزال برمجيات الفدية أحد أكبر التهديدات السيبرانية المستمرة التي تواجه المؤسسات المختلفة. من المتوقع أن تستمر هجمات برمجيات الفدية في الازدياد وكما أنه من المرجح ان تستمر مجموعات برمجيات الفدية في استغلال الثغرات الأمنية (Zero-day) كطريقة لاختراق الأنظمة والشبكات المستهدفة وستظل القطاعات الوطنية الحيوية منها أهدافًا رئيسية لتلك المجموعات. تتغير أنشطة مجموعات القرصنة بالتغيرات في الأوضاع الجيوسياسية حيث يتوقع ان تزاد وتيرتها في حال تصاعد الأوضاع في المنطقة. قد يتم تشكيل تحالفات بين تلك المجموعات مما قد يؤدي إلى تنفيذ أنشطة سيبرانية أكثر تنسيقًا وتطورًا. من المتوقع أن تشهد الهجمات المرتبطة بمجموعات التهديد المتطورة ارتفاعًا مستمرًا. يعتقد أن هذه المجموعات سوف تركز بشكل أكبر على استهداف قطاعات البنية التحتية الحرجة، وأن تستخدم تقنيات أكثر تطوراً وتعقيدا وقد يتم استغلال قدرات الذكاء الاصطناعي بشكل أكبر لتعزيز عملياتها وانشطتها الخبيثة. كما ستظل تلك المجموعات تسعى لاستغلال الثغرات الأمنية على نطاق واسع كطريقة أساسية للوصول الى الأنظمة والشبكات المستهدفة.

بشكل عام من المتوقع أن تشهد الفترة القادمة بروز تهديدات سيبرانية أكثر تطورا وتعقيدًا مما يستلزم تطوير استراتيجيات أمنية استباقية متقدمة من خلال تطبيق الحلول الأمنية المناسبة من تنفيذ عمليات تدقيق وتقييم أمني للأصول الرقمية بالإضافة الى استخدام أدوات رصد ومراقبة متطورة للأنظمة والشبكات وتحديث آليات وتقنيات الكشف لمثل هذا النوع من الهجمات ومتابعة أحدث المعلومات للوقاية والحماية من التهديدات والحد منها.

المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

تـقرير المـوقف الأمـني السـيبراني
Cyber Threat Situational Report

الربـــع الـــثـالـث 2025