الإنتربول

تقرير الإنتربول عن تقييم التهديدات السيبرية في أفريقيا لعام 2024

لمحة عامة يقدّمها المكتب المعني بعمليات مكافحة الجريمة السيبرية في أفريقيا

الإصدار الثالث

نيسان/أبريل 2024

المحتويات

إخلاء المسؤولية القانونية

مقدمة بقلم مدير إدارة مكافحة الجريمة السيبرية في الإنتربول

ليست التكنولوجيا في عالم اليوم مجرد سلعة ترفيهية، بل هي ركن أساسي من أركان حياتنا اليومية. ويشكّل الإنترنت العمود الفقري لهذا العصر التكنولوجي، وله أهمية حاسمة في إدارة البنى التحتية الحيوية، وإجراء المعاملات المالية على نحو مأمون، والحفاظ على التواصل مع الأحبّة، والتسوّق عبر المواقع الإلكترونية، والوصول إلى كمّ وفير من المعلومات ومواقع التسلية. وبفضل قدرته على تقريب المسافات البعيدة وتسهيل الوصول الفوري إلى البيانات والأنشطة الافتراضية، أصبح الإنترنت أداة لا يُستغنى عنها

بيد أن العصر الرقمي يأتي حاملا في جعبته مجموعةً من الصعوبات الخاصة به، التي تشمل بصورة رئيسية التهديد المتنامي للجريمة السيبرية. فكلما تقدّمت التكنولوجيا، تطورت الأساليب التي يستخدمها مرتكبو الجريمة السيبرية الذين يستعينون بطُرق ما فتئت تزداد ابتكارا لاستغلال مواطن الضعف، مما يعرّض الأشخاص والمؤسسات لمخاطر جمّة. وغالبا ما يُترك الضحايا في حالة مالية ونفسية وعاطفية بائسة. وفي الوقت نفسه، يتفاقم مشهد التهديدات بفعل التطورات الاجتماعية والاقتصادية والسياسية التي تستجد على نطاق أوسع، والتي تشمل، في جملة أمور، اتساع الهوة بين البلدان والمؤسسات والأشخاص القادرين على الصمود في وجه التهديدات السيبرية، وأولئك الذين لا حول لهم ولا قوة. ويستغل مرتكبو الجريمة السيبرية كل هذه الظروف على الصعيد الوطني والإقليمي والعالمي، مما يخلّف عددا لامتناهيا من الضحايا.

وفي مطلع عام 2024، يكتسي تنفيذ الاستراتيجيات الشاملة في مجال الأمن السيبري أهميةً لا يمكن المغالاة فيها. ويتعين على الكيانات، الكبيرة منها والصغيرة، أن تحصّن نفسها ضد مجموعة واسعة من التهديدات السيبرية التي تتراوح بين هجمات تقليدية ومخاطر ناشئة أكثر تعقيدا

وقام الإنتربول على مدى السنوات التسع الماضية قيادة برنامج عالمي متماسك ومتسق لمكافحة الجريمة السيبرية يستند إلى الاستراتيجية العالمية لمكافحة الجريمة السيبرية التي تهدف إلى التخفيف من تبعات هذه الجريمة على الصعيد العالمي وحماية المجتمعات المحلية من أجل عالم أكثر أمانا. ويتولى الإنتربول التنسيق بين بلدانه الأعضاء الـ 196 ويدعمها من خلال أنشطة ترمي إلى منع الجرائم السيبرية، وكشفها، والتحقيق فيها، وتقويضها. وتسبب هذه الجرائم أضرارا كبيرة وتخلّف عواقب وخيمة، أو أنها تُرتكب بوتيرة مرتفعة، أو تثير اهتماما كبيرا في المجتمعات المحلية التي نساعد على حمايتها. وينفَّذ ذلك من خلال إطار عمل ثلاثي الجوانب يوفر الدعم للبلدان الأعضاء في مجالات تبادل المعلومات وتنسيق العمليات والتنمية الاستراتيجية وتطوير القدرات

وفي هذا السياق، أخذ الإنتربول بنهج إقليمي يعرض فيه مساعدة بحسب الطلب من خلال المكاتب الإقليمية المعنية بعمليات مكافحة الجريمة السيبرية. ويمثّل مكتب العمليات المشتركة لمكافحة الجريمة السيبرية في أفريقيا (AFJOC) الذي تموله وزارة الخارجية والكومنولث والتنمية في المملكة المتحدة أحدَ الأمثلة على هذه المبادرة. ويُعنى المكتب بجمع وتحليل المعلومات المتعلقة بالأنشطة التي يضطلع بها مرتكبو الجرائم السيبرية، واتخاذ إجراءات شرطية منسقة تستند إلى البيانات الاستخباراتية، وبشكل عام، تعزيز التعاون وأفضل الممارسات بين البلدان الأعضاء الأفريقية، وإرساء الشراكات مع الجهات المعنية من القطاعين العام والخاص

ومن هذا المنطلق، يشرّفني أن أقدّم أحدث إصدار للتقرير المتعلق بتقييم التهديدات السيبرية في أفريقيا. ويوفّر هذا التقييم دراسة تحليلية شاملة لمشهد التهديدات السيبرية في القارة الأفريقية، وينظر، على وجه الخصوص، في برمجيات انتزاع الفدية، والاحتيال بالبريد الإلكتروني المهني (BEC) وغيره من أشكال الاحتيال الإلكتروني. ولا يكتفي التقرير بتسليط الضوء على هذه التهديدات السيبرية فحسب، بل يرصد أيضا الجهود الوطنية المتواصلة لتحسين القدرة على الصمود في وجه التهديدات السيبرية. ويُختَتم التقرير بتوصيات استراتيجية تمهد الطريق للخطوات المقبلة.

ويتبيّن من خلال الدراسة التحليلية أن الحاجة الماسة إلى تعاون دولي وإقليمي بين أجهزة إنفاذ القانون للتصدي للأنشطة التي يضطلع بها مرتكبو الجرائم السيبرية أمرٌ لا جدال فيه. ويسهم النهج الموحد في تعزيز القدرة على مكافحة التهديدات بفعالية، مما يتيح تبادل البيانات الاستخباراتية، ومشاطرة ممارسات التحقيق، واستخدام التقنيات المتطورة.

ويتعين على الدوام الاضطلاع بالعمل الشرطي على الصعيد المحلي وسيبقى جزءا لا يتجزأ من الخدمات المقدمة لمجتماعتنا المحلية. ولكن بعض الجرائم، كالجريمة السيبرية، تترك بصمة عالمية وقد تفرض علينا جميعا تحديات بفعل حجمها ونطاقها ودرجة تعقيدها. وتقع على عاتقنا مسؤولية جماعية لمنع المجرمين والمجموعات الضالعين في هذه الجرائم، وكشفهم، والتحقيق معهم، وتقويضهم. وسواء كان المتصلون بالإنترنت من الأفراد أو من الشركات، علينا أن نكون أكثر أمانا.

وفي هذا المشهد المعقد، لا يمكن لأي جهة فاعلة، بمفردها، أن تجعلنا قادرين على تأمين سلامتنا الجماعية. والإنتربول، إذ يقر بذلك، يؤدي دور المحاوِر المحايد والجدير بالثقة، مما يوطد التعاون بين أجهزة إنفاذ القانون والقطاعين العام والخاص. ويسعى الإنتربول، من خلال تضافر الجهود وتبادل الخبرات، إلى تعزيز قدراتنا الجماعية على التصدي للتهديدات السيبرية، ويشدد في الوقت نفسه على المسؤولية التي نتقاسمها لحماية عالمنا الرقمي.

وفي الختام، أود أن أعرب عن امتناني لبلداننا الأعضاء في المنطقة الأفريقية ولشركائنا على ثبات دعمهم وتفانيهم في هذا الصدد وعلى إسهامهم في إعداد هذا التقييم. فلا غنى عن جهودهم الحثيثة والتزامهم الراسخ لبلوغ هدفنا المشترك المتمثل في إقامة بيئة رقمية أكثر أمانا للجميع

كريغ جونز
مدير إدارة مكافحة الجريمة السيبرية
الإنتربول

مقدمة بقلم المدير التنفيذي بالوكالة في الأفريبول

في الوقت الذي نستحضر فيه أحداث العام الفائت ونتطلع إلى المستقبل، يواصل مشهد التهديدات السيبرية في أفريقيا، لا بل في العالم أجمع، تغيّره ويزداد تعقيدا. وبين أواخر تسعينيات القرن الماضي حيث كان الوصول إلى الإنترنت خدمة فاخرة لا يمكن إلا لقلة قليلة من الناس دفع كلفتها، ويومنا هذا حيث نشهد طفرة في الاتصالات الإلكترونية، قُطعت أشواط تدل على التقدم المذهل الذي أحرزته التكنولوجيا. بيد أن هذا التقدم لا يخلو من المصاعب. فقد انتشرت التهديدات السيبرية بشكل متصاعد حتى بلغت كل شبر من القارة وطالت الأفراد والحكومات والشركات على حد سواء.

وشكّل عام 2023 منعطفا في بلورة ردنا على هذه التهديدات الناشئة. فقد أحرزت المعركة ضد الجريمة السيبرية تقدما ملحوظا بفضل استنادها إلى الأسس التي وُضعت في السنوات الماضية. وتوثّق تعاوننا مع الإنتربول بشكل غير مسبوق، وهو يتجسد من خلال القيام بمبادرات مبتكرة وتوفير تقنيات متطورة ترمي إلى توطيد دفاعاتنا في المجال السيبري. ويشكّل استحداث مركز البيانات وقواعد البيانات للأدلة الجنائية التابع لأفريبول، فضلا عن تدشين وحدة تحليل البيانات الاستخباراتية الجنائية، محطتين حاسمتين في سعينا إلى تهيئة بيئة سيبرية أكثر أمانا في أفريقيا.

وإطلاق الدورات التدريبية الخاصة بأفريبول والمتعلقة بالتحقيق في الجريمة السيبرية خيرُ دليل على التزامنا ببناء القدرات في القارة. وتوسيع نطاق هذه البرامج لتشمل دروسا من المستوى المتقدم عن تهديدات الأمن السيبري واستراتيجيات الرد قد أسهم في إثراء الترسانة التي يمكن أن نواجه بها مرتكبي الجرائم السيبرية. وكانت مشاركة البلدان الأعضاء إيجابية للغاية، مع ارتفاع كبير في عدد المشاركين وتحسّن ملحوظ في مهارات الموظفين العاملين لدينا والمعنيين بالأمن السيبري.

وفي عام 2023، ازداد عدد شراكائنا وتخطى حلفاءنا التقليديين ليشمل شركات تكنولوجية عملاقة ومؤسسات أكاديمية. وأتاحت لنا علاقات التعاون هذه الاستفادة من أحدث البحوث والتقنيات، وبالتالي تعزيز قدرتنا على التكيف مع المشهد السيبري الدائم التغير. كما قمنا بتوسيع دائرة اهتماماتنا لتشمل التصدي للعواقب الاجتماعية والاقتصادية التي تخلفها التهديدات السيبرية، مع العلم أن الأمن السيبري لا يطرح مشكلة تقنية فحسب، بل هو حجز الزاوية في استقرار اقتصادنا وازدهاره. وتشهد أفريقيا اقتصادا رقميا مزدهرا، وتشكل حماية هذ القطاع حاجة ماسة لتحقيق التنمية المستدامة لدينا

وفي عام 2024، تلتزم أفريبول بمضاعفة جهودها على أربع جبهات استراتيجية:

1. إدراكا منا لطبيعة التهديدات السيبرية التي لا تقف عند حدود، نصبو إلى تعزيز شبكة تعاوننا في جميع أنحاء القارة ومع شركائنا الدوليين. ويشمل ذلك تبادل البيانات الاستخباراتية، وتنفيذ العمليات المشتركة، ومواءمة الأطر القانونية لضمان تشكيل جبهة موحدة ضد الجريمة السيبرية. كما نعمل على تعزيز التعاون مع القطاع الخاص من أجل تنسيق وتوحيد الإجراءات والتقنيات، والسماح بجمع البيانات الاستخباراتية في أنحاء القارة كافة

وفي مطلع عام 2024، أبرمت أفريبول مذكرة تفاهم مع Group-IB، وهي شركة رائدة عالميا في مجال الأمن السيبري. وستسهم هذه الشراكة في تعزيز تبادل البيانات الاستخباراتية وتزويد البلدان الأعضاء في الاتحاد الأفريقي بالتكنولوجيا المتطورة والمعارف المتخصصة في المجالات الحيوية من قبيل التحقيقات السيبرية، والهندسة العكسية، وإدارة الحوادث. وبفضل التعويل على هذه الأدوات والخبرات المتقدمة، ستعزز أفريبول قدراتها في مجال الوقاية من التهديدات السيبرية في القارة. ومن المقرر أيضا أن تبرم أفريبول اتفاقا مع شركة Kaspersky، وهي شريك استراتيجي من القطاع الخاص.

2. يتمثل أحد العناصر الرئيسية من استراتيجيتنا في استحداث فرقة عمل معنية بتبادل المعلومات عن حوادث الجريمة السيبرية وتقديم الدعم اللازم للتحقيق فيها. ونحن ملتزمون بتزويد بلداننا الأعضاء بالمعدات والبرامج اللازمة للتحقيق في الجريمة السيبرية، مع تنظيم دورة تدريب متخصصة بشأن هذه الأدوات. وكأمثلة على مبادراتنا، نذكر العملية الثالثة المشتركة بين الإنتربول وأفريبول لمكافحة الجريمة السيبرية، والمعروفة باسم Africa Cyber Surge 3، ودورتنا التدريبية المتخصصة في مجال الموارد الافتراضية، وتقديم الأدوات الأساسية لإجراء التحقيقات بالاشتراك مع الإنتربول، وكلها مبادرات تبيّن التزامنا الراسخ بتعزيز قدراتنا على مكافحة الجريمة السيبرية في جميع أنحاء القارة.

3. سنواصل استكشاف ودمج الوسائل التكنولوجية الناشئة كالذكاء الاصطناعي وتقنية Blockchain من أجل تعزيز قدراتنا على مكافحة الجريمة السيبرية. وتقدّم هذه التكنولوجيا أدوات واعدة للقيام بتحليل استباقي للتهديدات، وإدارة البيانات على نحو مأمون، وتخصيص الموارد بكفاءة. وبالإضافة إلى ذلك، نعتمد وسائل تكنولوجية مفتوحة المصدر في إطار برامجنا التدريبية، مما يثبت التزامنا بتخطي الصعوبات المالية المرتبطة بالتكاليف الباهظة لمنح التراخيص.

4. نركز بشكل متزايد على مشاركة المجتمعات المحلية ونخطط لإطلاق حملات شاملة للتوعية بالجريمة السيبرية موجهة للفئات الضعيفة، ولا سيما الشباب والشركات الصغيرة والمتوسطة الحجم. فإن توعية هذه المجموعات السكانية الرئيسية بتدابير الوقاية السيبرية هي عنصر حاسم في التخفيف من وطأة التهديدات السيبرية على المستوى الشعبي.

والطريق أمامنا شاق، ولكن عزيمتنا ثابتة. وإذ نستهل عام 2024، تنقشع الغشاوة عن رؤيتنا: جعل أفريقيا قارة رقمية مأمونة وقادرة على الصمود، تُستخدم فيها التكنولوجيا كمنارة للتقدم لا كوسيلة للاستضعاف. ومعا، وبفضل الدعم الراسخ من شركائنا والجهود الجماعية التي تبذلها بلداننا الأعضاء، نحن على أهبة الاستعداد لتحويل هذه الرؤية إلى واقع. فلنسلك هذا الطريق بحزم وتفاؤل لأن أمن فضائنا السيبري أساس ازدهارنا المشترك

السفير جلال شلبا
المدير التنفيذي بالوكالة
أفريبول

الأسماء والتسميات المختصرة

AFJOC	African Joint Operation against Cybercrime
AI	Artificial Intelligence
BEC	Business Email Compromise
BPH	Bulletproof Hosting
CaaS	Crime-as-a-Service
CCP - Operation	Cybercrime Collaborative Platform - Operation
CERT	Computer Emergency Response Teams
CSIRT	Computer Security Incident Response Team
CKE	Cyber Knowledge Exchange
DDoS	Distributed Denial of Service
GLACY+	Global Action on Cybercrime Extended (currently GLACY-e)
IP	Internet Protocol
ISPA	INTERPOL's Support Programme for the African Union
LLM	Large Language Models
MFA	Multi-Factor Authentication
PII	Personally Identifiable Information
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
SMEs	Small and Medium-sized Enterprises

شكر وتقدير

أعدّ هذا التقرير المكتبُ المعني بعمليات مكافحة الجريمة السيبرية في أفريقيا، تحت رعاية مكتب العمليات المشتركة لمكافحة الجريمة السيبرية في أفريقيا (AFJOC) الذي تموله وزارة الخارجية والكومنولث والتنمية في المملكة المتحدة. وأسهم برنامج الإنتربول لدعم الاتحاد الأفريقي (ISPA) أيضا في إعداد هذا التقرير، بدعم من الوزارة الاتحادية للشؤون الخارجية في ألمانيا

ويستند هذا التقرير على تقييم المعلومات الذي قُدّم للإنتربول من قِبل البلدان الأعضاء المعنية وشركاء الإنتربول من القطاع الخاص، بما في ذلك Bi.Zone وFortinet، وGroup-IB، وKaspersky Lab، وTrend Micro

موجز

يقدّم هذا التقرير دراسة تحليلية أجراها الإنتربول بشأن التهديدات السيبرية الرئيسية التي تطال القارة الأفريقية، وذلك استنادا إلى بيانات استخباراتية داخلية، ومعلومات ميدانية، ونتائج دراسة استقصائية، ومساهمات من الجهات الشريكة من القطاع الخاص.

وتشدد الاستنتاجات الرئيسية للتقرير على تفاقم الجريمة السيبرية على مستوى القارة، وتعتبر أن برمجيات انتزاع الفدية والاحتيال بالبريد الإلكتروني المهني، وغير ذلك من أشكال الاحتيال الإلكتروني، هي التهديدات الأسرع انتشارا في عام 2023. واعتُبرت برمجيات انتزاع الفدية، على وجه الخصوص، تهديدا ناشئا بالغ الأهمية يستهدف في غالب الأحيان البنى التحتية الحيوية. أما الاحتيال الإلكتروني، فلا يزال يشكّل الجريمة الرقمية الأكثر شيوعا ضد الأفراد والشركات، مع ما يترتب على ذلك من تداعيات كبرى مالية وعلى صعيد الحجم. ويشير التقرير أيضا إلى سرعة تطور الجهات الفاعلة المسؤولة عن التهديد وأساليبها الإجرامية، ولا سيما الاستغلال المتزايد لشبكات التواصل الاجتماعي، واستخدام برمجيات الذكاء الاصطناعي، وتقنيات الهندسة الاجتماعية المتقدمة.

ويلقي التقرير الضوء على الجهود التي تبذلها البلدان الأفريقية على الصعيد الوطني لمكافحة الجريمة السيبرية، ويركز في الوقت نفسه على تعزيز التشريعات، والنهوض بالقدرات الشرطية، وتوطيد الشراكات، ومشاركة عامة الناس. وعلى الرغم من أن البلدان الأعضاء اتخذت تدابير مهمة لتعزيز قدراتها الدفاعية في المجال السيبري وتحسين ردودها الشرطية، لا تزال هناك مجموعة من العقبات تحول دون اعتماد نهج شامل ومنسق ومستدام لمكافحة الجريمة السيبرية في جميع أنحاء القارة.

ويشير التقرير في مختلف أقسامه إلى التزام الإنتربول بمكافحة الجريمة السيبرية في أفريقيا وتقديم المساعدة إليها في هذا المجال. ويُعتمَد لذلك، بشكل رئيسي، نهجٌ إقليمي متخصص يقوده مكتب الإنتربول المعني بعمليات مكافحة الجريمة السيبرية في أفريقيا، ويُنفَّذ في إطار مشروع " العملية المشتركة لمكافحة الجريمة السيبرية في أفريقيا"، الذي تموله وزارة الخارجية والكومنولث والتنمية في المملكة المتحدة. وتُستكمَل هذه المبادرة بأنشطة أخرى ذات أهمية، ولا سيما تلك التي تُنفَّذ في إطار برنامج الإنتربول لدعم الاتحاد الأفريقي، ومشروع التحرك العالمي الموسَّع لمواجهة الجريمة السيبرية.

ويختتم التقرير بتوصيات استراتيجية من الإنتربول بشأن كيفية التعامل مع مشهد التهديدات السيبرية في أفريقيا، وتعزيز الأمن السيبري في جميع أنحاء القارة. وتشمل التوصيات اعتماد تدابير شاملة وموحدة للأمن السيبري، أو تحسينها، والاستثمار في القدرات السيبرية لأجهزة إنفاذ القانون (الأشخاص والإجراءات والوسائل التكنولوجية)، وتحقيق التآزر في نهج الأمن السيبري المترابط، وتوعية عامة الناس، وتعزيز التعاون الدولي والإقليمي

مقدمة

تشهد البلدان الأفريقية تحولات رقمية ملحوظة. وعلى الرغم من الصعوبات المستمرة في البنى التحتية لتغطية الإنترنت، والوصول إليه، وفيما يتعلق بجودته، لم يتوقف عدد مستخدمي الإنترنت عن الارتفاع في جميع أنحاء القارة، إذ بلغ عدد الأفراد الذين يتصفحون الفضاء السيبري بانتظام في الفترة بين 2019 و2022[1] أكثر من 160 مليون شخص. وتتجلى آثار الرقمنة في العديد من القطاعات، بدءاً من البنى التحتية الحيوية ووصولا إلى الخدمات المصرفية والتجارة الإلكترونية. وتتغلغل التكولوجيا الرقمية أيضا في العديد من جوانب الحياة اليومية للمواطنين الأفارقة، بما في ذلك الارتفاع السريع لعدد المشتريات بالوسائل الرقمية، وزيادة الوقت المخصص لاستخدام الإنترنت، ولا سيما منصات التواصل الاجتماعي. وعلى سبيل المثال، يبلغ حاليا عدد متصفحي فايسبوك، وهي إحدى المنصات الأكثر شعبية في أفريقيا، أكثر من 170 مليون مستخدم. وعلى الصعيد الفردي، فإن الوصول المتزايد إلى الإنترنت يسهّله، على وجه الخصوص، انتشار استخدام الهواتف المحمولة على نطاق واسع، إذ يعتمد أكثر من 650 مليون أفريقي تلك الأجهزة كوسيلة أساسية للوصول إلى الإنترنت.

ولهذه الثورة الرقمية تأثير خاص على الشباب الأفريقي الذين يمثّلون أكثر من 60 في المئة من سكان القارة[2]. ويلجأ الكثيرون منهم، عبر هواتفهم المحمولة في معظم الأحيان، إلى الإنترنت كأداة للتواصل والعمل وتحويل الأموال والتسوق والتعبير عن أفكارهم المبتكرة. وبالنظر إلى تكيّفهم السريع مع التقنيات الرقمية، فإنهم يسهمون في تنمية مجتمع فتيّ يعتمد على الفضاء السيبري. ولئن كان ذلك يتيح للبلدان الأفريقية فرصا ذهبية لمواصلة النمو والابتكار، إلا أنه يعرّضها أيضا لصعوبات ومخاطر لم تشهدهما من قبل في مجال الأمن السيبري.

ولا شك أن ارتفاع عدد الأفريقيين الذين يستخدمون الإنترنت، والاعتماد المتزايد للاقتصادات والمجتمعات على هذه التكنولوجيا، وظهور ما يسمى " بالجيل الرقمي"، هي عواملٌ تؤدي إلى توسيع نطاق الهجمات السيبرية المفتوح أمام المجرمين. وبالتالي، تظهر الجريمة السيبرية في جميع أنحاء أفريقيا وتشكل أحد التهديدات الأسرع انتشارا في القارة. وكان تقرير الإنتربول الأول عن التهديدات السيبرية في أفريقيا (2021) قد قدّر كلفة التداعيات المالية للجريمة السيبرية في المنطقة بأكثر من 4 مليارات دولار أمريكي، أي ما يناهز 10 في المئة من إجمالي ناتج الدخل المحلي لأفريقيا[3]. ومنذ ذلك الحين، والبلدان الأفريقية الـ 54 الأعضاء في الإنتربول تشهد تصاعدا في حجم الصعوبات، وتداعياتها، وتعقيداتها

وتشتد الحاجة إلى معالجة شح المعارف الرقمية، والتصدي لعدم كفاية الاستعدادات في المجال السيبري، والافتقار العام إلى الممارسات الجيدة في مجال تدابير الوقاية السيبرية. ولحسن الحظ، اتخذت البلدان الأفريقية خطوات مهمة في عام 2023 لإرساء اقتصادات رقمية أكثر أمانا ولحماية مجتمعاتها المحلية عبر الإنترنت. والإنتربول ملتزم بدعم بلدانه الأعضاء في تحقيق هذه الأهداف. وهو، إذ يقرّ بالتنوع الهائل الذي تتميز به القارة الأفريقية، ولا سيما مجموعتها الواسعة من الثقافات واللغات والأوضاع الاقتصادية، يقدّم من خلال المشاريع والبرامج الرئيسية كمشروع العملية المشتركة لمكافحة الجريمة السيبرية في أفريقيا (AFJOC) وبرنامج الإنتربول لدعم للاتحاد الأفريقي (ISPA)، أنشطةً بالغة الأهمية تلبي احتياجات مختلف أجهزة إنفاذ القانون الوطنية في أفريقيا.

1 البنك الدولي (2024): https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa

2 المنتدى الاقتصادي العالمي (2023): https://www.weforum.org/agenda/2022/09/why-africa-youth-key-development-potential

3 بحث أجرته Serianu، وهي إحدى الشركات في كينيا التي تعمل في مجال الأمن السيبري لتكنولوجيا المعلومات، ويمكن الاطلاع عليه عبر الموقع الإلكتروني التالي: [https://phys.org/news/2021- 05-rights-group-tool-stem-cybercrime.html]

لمحة عامة عن اتجاهات مشهد التهديدات السيبرية في أفريقيا: 2023

في عام 2023، ظل مشهد التهديدات السيبرية في أفريقيا مرتفع النشاط، مع تغيّر سريع في مستوى الابتكار والنطاق على صعيد الهجمات. واستناداً إلى البيانات الاستخباراتية والمعلومات الميدانية المستقاة من أنشطة الإنتربول الإقليمية، فضلا عن نتائج الاستبيان الذي عُمّم على البلدان الأفريقية الأعضاء والمعلومات التي قدمها الشركاء من القطاع الخاص، حدد الإنتربول التهديدات والاتجاهات الرئيسية التالية:

حجم الجرائم السيبرية وتداعياتها تواصل انتشارها في جميع أنحاء أفريقيا

- يواصل عدد الهجمات التي ينفّذها مرتكبو الجرائم السيبرية ارتفاعه في جميع أنحاء القارة الأفريقية، على نحو ما أفادت به البلدان الأعضاء في الإنتربول[4].
- أكثر من ثلثي البلدان التي أجابت على الاستبيان تعتبر أن الجرائم السيبرية والجرائم التي يسهّل الفضاء السيبري ارتكابها جرائمٌ يتراوح مستوى تهديداتها بين متوسط ومرتفع. وتحديدا، أشارت البلدان إلى ازدياد تأثير هذه الجرائم من الناحية المالية والاجتماعية.
- كمثال آخر على النمو السريع للجريمة السيبرية، تشير التقديرات في عام 2023 إلى أن عدد الهجمات الذي يُشّن أسبوعيا على المؤسسة الواحدة في أفريقيا قد ارتفع بمعدل وسطي قدره 23 في المائة بين سنة وأخرى. وهو المعدل الأعلى المسجل في العالم[5].

برمجية انتزاع الفدية، والاحتيال بالبريد الإلكتروني المهني، وغيرهما من عمليات الاحتيال الإلكتروني، هي التهديدات السيبرية الأسرع نموا في عام 2023

- اعتبرت تقارير الإنتربول السابقة عن تقييم التهديدات السيبرية في أفريقيا أن التهديدات السيبرية التالية هي الأكثر رواجا: الهجمات بالبرمجيات الخبيثة، بما في ذلك برمجيات انتزاع الفدية، وبرمجيات حصان طروادة وسرقة البيانات المصرفية، والتصيد الاحتيالي، والاحتيال الإلكتروني، مثل الاحتيال بالبريد الإلكتروني المهني؛ والابتزاز السيبري، بما في ذلك الهجمات الموزعة لحجب الخدمة (DDoS)؛ والجريمة السيبرية كخدمة، مثل برمجيات التجسس وأدوات التصيد الاحتيالي. وتواصل هذه التهديدات تأثيرها على المشهد السيبري في أفريقيا، مما يسبب أضرارا جسيمة للمجتمعات المحلية في جميع أنحاء القارة.
- في عام 2023، اعتبرت البلدان الأفريقية الأعضاء في المنظمة أن برمجيات انتزاع الفدية، والاحتيال بالبريد الإلكتروني المهني، وعمليات الاحتيال الإلكتروني الأخرى، هي أبرز التهديدات السيبرية.
- وحُددت برمجيات انتزاع الفدية كواحدة من أخطر التهديدات الناشئة في القارة، التي غالبا ما تستهدف البنى التحتية الحيوية، في حين يبقى الاحتيال الإلكتروني أبرز أشكال الجريمة الرقمية التي تستهدف الأفراد والمؤسسات، من حيث عددها وأثرها المالي.

الجهات الفاعلة المسؤولة عن التهديد وأساليبها الإجرامية تتغيران بسرعة – بدءاً من تقنيات الهندسة الاجتماعية الأكثر تطورا ووصولا إلى الاستخدام المتزايد لوسائل التواصل الاجتماعي والذكاء الاصطناعي

- يواصل مرتكبو الجرائم السيبرية الناشطون في أفريقيا وانطلاقا منها، استغلال نقاط الضعف لدى الأشخاص كوسيلة رئيسية للهجوم. ويستخدمون تقنيات الهندسة الاجتماعية التي ما فتئت تزداد تعقيدا من أجل استهداف المؤسسات والأفراد.
- لا يزال التصيد الاحتيالي بالبريد الإلكتروني أحد أبرز وسائل الهجوم الأولي الذي تنطوي عليه مجموعة من الجرائم السيبرية، بما في ذلك برمجيات انتزاع الفدية وأشكال كثيرة من الاحتيال الإلكتروني. وكذلك، يستغل الجناة بصورة تدريجية مختلف قنوات الاتصال، بما في ذلك وسائل التواصل الاجتماعي وتطبيقات المراسلة الآنية، بما يتماشى مع الاتجاهات التكنولوجية والمجتمعية الإقليمية.
- يدمج الجناة الوسائلَ التكنولوجية المتقدمة في أساليبهم الإجرامية. وتتضمن أبرز الأمثلة على ذلك الاستخدام المتزايد لسرقة البيانات كشكل من أشكال الابتزاز، وإساءة استخدام تقنية الذكاء الاصطناعي على نحو متصاعد.

4 تستند هذه المعلومات إلى التقارير التي قدمتها البلدان الأفريقية الأعضاء. وتجدر الإشارة إلى أن تعريف "الجريمة السيبرية" قد يختلف من بلد لآخر.

5 شركة Check Point (2023): https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

استجابةً للتهديدات المتصاعدة التي تطرحها الجرائم السيبرية، اتخذت البلدان الأعضاء الأفريقية تدابير مهمة لتعزيز القدرة على الصمود في وجه التهديدات السيبرية والنهوض بقدرات إنفاذ القانون

- أدى تعزيز الموارد اللازمة لمكافحة الجريمة السيبرية إلى ارتفاع عدد الموقوفين، والإجراءات المتخذة في هذا الصدد، والتحقيقات ذات الصلة. فعلى سبيل المثال، أفاد 19 بلدا عضوا بتوقيف ما مجموعه 10,490 شخصا مرتبطا بالجريمة السيبرية، في الفترة من كانون الثاني/يناير إلى كانون الأول/ديسمبر 2023. وبما أن هذه البلدان لا تمثّل سوى 35 في المائة من مجمل بلدان القارة، فمن المحتمل أن يكون العدد الإجمالي للموقوفين المرتبطين بالجريمة السيبرية أعلى من ذلك بكثير.
- في العامين الماضيين، اعتمدت عشرات البلدان الأفريقية تشريعات جديدة مرتبطة بالجريمة السيبرية أو شرعت في اعتمادها. ويشكل ذلك خطوة استباقية تهدف إلى تعزيز الأطر القانونية اللازمة لمكافحة الجريمة السيبرية.
- تضافرت أيضا بشكل ملحوظ الجهود المبذولة لمكافحة الجريمة السيبرية في القارة، بما في ذلك الجهود المبذولة من البلدان الأفريقية الأعضاء والجهات المعنية من خارج المنطقة. وفي عام 2023، ازداد عدد البلدان التي شكّلت وحدات متخصصة في مكافحة الجريمة السيبرية، قام نصفها تقريبا برفع عدد موظفيه، وأفاد أكثر من 60 في المائة منها بأنه شارك في مبادرات ترمي إلى بناء القدرات في هذا المجال. وبالإضافة إلى ذلك، اتُخذت أكثر من 130 مبادرة في مجال التدريب ونُظّمت أكثر من 40 حملة توعية لعامة الناس في القارة.

بيد أنه لا تزال هناك صعوبات كبرى في مجال التحقيقات تحول دون منع الجريمة السيبرية في جميع أنحاء أفريقيا، وكشفها، والتحقيق فيها، وتعطيلها بشكل فعال

- الاستمرار في عدم الإبلاغ عن الجرائم السيبرية على نحو كاف من شأنه أن يعرقل قدرة أجهزة إنفاذ القانون على التحرك. وفي بعض البلدان، تتفاقم هذه المعضلة بسبب الافتقار إلى منصات محددة أو سهلة الاستخدام للإبلاغ والتسجيل.
- على الرغم من إحراز بعض التقدم، لا يزال التعاون بين أجهزة إنفاذ القانون والجهات المعنية الرئيسية، بما في ذلك القطاع الخاص والأجهزة المعنية بالأمن السيبري، يشكل تحديا في بعض البلدان.
- عدم اتخاذ تدابير الوقاية السيبرية على نحو كاف يواصل تقويض القدرة على الصمود في وجه الجريمة السيبرية في جميع أنحاء القارة، إذ لا يزال مستوى تأهب العديد من المؤسسات والأشخاص في أفريقيا غير كاف للتصدي للهجمات السيبرية.

وتقدم الفقرات التالية دراسة تحليلية معمقة لأبرز اتجاهات التهديدات السيبرية في أفريقيا التي وضعتها البلدان الأعضاء في الإنتربول في الصدارة، وهي: برمجية انتزاع الفدية، والاحتيال الإلكتروني، والاحتيال بالبريد الإلكتروني المهني

برمجيات انتزاع الفدية والابتزاز الرقمي

النقاط الرئيسية:

- ارتفاع عدد الجرائم المرتكبة ببرمجيات انتزاع الفدية والابتزاز الرقمي، حيث أفاد أكثر من نصف البلدان الأفريقية الأعضاء في الإنتربول بوقوع هجمات ضد البنى التحتية الحيوية فيها.
- لا يزال التصيد الاحتيالي بالبريد الإلكتروني وسيلة الهجوم الأكثر شيوعا لتنفيذ هجمات ببرمجيات انتزاع الفدية في أفريقيا، في حين أن طُرق الابتزاز ونماذج العمل التي يستخدمها مرتكبو الجرائم السيبرية تتغير.
- في المجمل، اتخذت البلدان الأفريقية الأعضاء خطوات إيجابية لتعزيز قدرتها على الصمود في وجه الهجمات المرتكبة ببرمجيات انتزاع الفدية، ولكن لا تزال هناك صعوبات عالقة، ولا سيما فيما يتعلق بالإبلاغ عن الهجمات ودفع الفدية.

ارتفاع عدد الجرائم المرتكبة ببرمجيات انتزاع الفدية والابتزاز الرقمي

أفادت البلدان الأعضاء في الإنتربول بأن برمجيات انتزاع الفدية والابتزاز الرقمي هما من أخطر التهديدات السيبرية التي تتعرض لها القارة الأفريقية. وتثير هذه الهجمات قلقا شديدا بسبب التداعيات المالية الكبيرة التي تخلفها، وقدرتها على تعطيل البنى التحتية الحيوية والخدمات الأساسية على نحو خطير، والأضرار التي يمكن أن تلحقها بالمؤسسات والأشخاص المعنيين. وحجم هذه الصعوبات لا لبس فيه، إذ أفادت شركة Chainalysis المتخصصة في الأمن السيبري، بأن الأموال المدفوعة في إطار برمجيات انتزاع الفدية تجاوزت مليار دولار أمريكي على الصعيد العالمي في عام 2023[6]

ويستمر نمو حجم وتواتر وتأثير الهجمات المرتكبة ببرمجيات انتزاع الفدية في أفريقيا. وأفادت البحوث التي أجرتها شركة Check Point المتخصصة في الأمن السيبري بأنه في المتوسط، تعرضت واحدة من أصل 15 مؤسسة لمحاولة هجوم أسبوعي ببرمجية انتزاع الفدية خلال الربع الأول من عام 2023. ولا يزال هذا الرقم أعلى من المعدل الأسبوعي المسجل على الصعيد العالمي والبالغ واحدة من أصل 31 مؤسسة تقريبا[7]. وفي أسبوع واحد من شهر شباط/فبراير 2023، رصدت شركة Kaspersky، وهي شريك للإنتربول من القطاع الخاص، أكثر من 300 محاولة انتزاع فدية في جنوب أفريقيا، مما يشير إلى ارتفاع في وتيرة الهجمات8. ويبدو أن العواقب المالية لهذه الهجمات تتفاقم أيضا، إذ أفادت شركة IBM بأن الكلفة المتوسطة لهجوم ببرمجية انتزاع الفدية بلغت 5,13 ملايين دولار أمريكي في عام 2023، أي بارتفاع نسبته 13 في المائة مقارنةً بعام 2022[9].

البنى التحتية الحيوية في أفريقيا تتعرض للهجوم

من دواعي القلق أنّ ما يناهز نصف البلدان الأفريقية التي أجابت على الاستبيان أفادت بأن البنى التحتية الحيوية فيها قد تعرضت لهجمات ببرمجيات انتزاع الفدية بين كانون الثاني/يناير وكانون الأول/ديسمبر 2023. وتستهدف هذه الهجمات في المقام الأول البنى التحتية الحكومية، والمستشفيات، والمؤسسات المالية، ومزودي خدمة الإنترنت. وعلى سبيل المثال، تعرضت جميع المؤسسات التالية لهذا النوع من الهجمات في السنوات الأخيرة: شركة Electricity Company of Ghana وهي أكبر بائع للكهرباء في غانا، والمصرف الوطني في كل من زامبيا وجنوب السودان، والمؤسسات الحكومية في كل من إثيوبيا والسنغال وزمبابوي، ومزوّد خدمة الإنترنت في جنوب أفريقيا RSAWEB. ولم ينجُ الاتحاد الأفريقي نفسه من هجوم قامت به مجموعة BlackCat (المعروفة أيضا باسم ALPHV) أدى إلى شلّ شبكته الداخلية في عام 2023 وتمكن الإنتربول وشركاؤه من التخفيف من وطأته[10]. واستهداف البنى التحية الحيوية يبعث على القلق الشديد في وقت لا تزال فيه التحولات الرقمية تتسارع في جميع أنحاء القارة وتترابط فيه المنظومات الأساسية على نحو متزايد.

وبالإضافة إلى البنى التحتية الحيوية، أفادت البلدان الأفريقية الأعضاء أيضا بأن الهجمات ببرمجيات انتزاع الفدية قد أصابت مختلف القطاعات. ويشمل ذلك عددا كبيرا من الهجمات ضد الشركات العاملة في قطاعات مثل قطاع المال، والتصنيع، والبيع بالتجزئة. وعلى سبيل المثال، أفادت شركة Sophos لأمن تكنولوجيا المعلومات بأن 78 في المائة من الشركات العاملة في جنوب أفريقيا قد تعرضت لهجمات ببرمجيات انتزاع الفدية في عام 2023[11]. وتشمل الهجمات التي ذاع صيتها تلك التي استهدفت المقر الرئيسي لشركة Porsche في جوهانسبرغ (جنوب أفريقيا)، وفرع المكتب الدولي للائتمان TransUnion في جنوب أفريقيا. وتتواءم هذه الاتجاهات مع المستجدات العالمية. ووفقا للبيانات المجمعة التي قدمها شركاء الإنتربول من القطاع الخاص، إذا كانت قطاعات المصرف، والحكومة، والبيع بالتجزئة، والتكنولوجيا، والصحة، هي الأكثر استهدافا على الصعيد العالمي، فهذا لا يعني أن سائر القطاعات والشركات والمؤسسات بمنأى عن هذه الهجمات.

6 شركة Chainalysis (2024): https://www.chainalysis.com/blog/ransomware-2024/

7 شركة Check Point (2023): https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

8 موقع News24 (2023): https://www.news24.com/fin24/companies/rsaweb-victim-of-cyberattack-as-wave-of-ransomware-attempts-hits-sa-in-past-week-20230206

9 شركة IBM (2023): https://www.ibm.com/reports/data-breach

10 صحيفة لوموند (2023): https://www.lemonde.fr/afrique/article/2023/04/25/vent-de-panique-a-l-union-africaine-apres-une-nouvelle-cyberattaque_6170976_3212.html

11 شركة Sophos (2023): https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/

الاستغلال المتواصل للعنصر البشري

فيما يتعلق بالأساليب الإجرامية، يبدو أن التصيد الاحتيالي بالبريد الإلكتروني هو أسلوب الهجوم ببرمجيات انتزاع الفدية الأكثر شيوعا في أفريقيا، حيث أبلغ ما يناهز نصف البلدان الأفريقية الأعضاء في الإنتربول عن حالات للتصيد الاحتيالي أثناء هذه الهجمات. وتتضمن هذه الرسائل الإلكترونية عادةً ملفات أو عناوين إلكترونية (URL) خبيثة، مصممة لتسهيل وصول إحدى الجهات الفاعلة المسؤولة عن التهديد إلى منظومة ما أو لنشر برمجية خبيثة بصورة آنية عندما يتم النقر على الرابط. وتتضمن أساليب التلوث الشائعة الأخرى التي تستخدمها مجموعات مرتكبي الهجمات ببرمجيات انتزاع الفدية في منطقة أفريقيا استغلالَ الاتصالات غير المأمونة التي تجرى عن طريق بروتوكول سطح المكتب البعيد (RDP)، فضلا عن استغلال ثغرات أخرى. وتتطابق هذه الاتجاهات الإقليمية مع الاستنتاجات العامة لشركة Trend Micro[12]، وهي شريك للإنتربول من القطاع الخاص . ووفقا لهذه الشركة المعنية بالأمن السيبري، فإن وسائل الهجوم الأولي الأكثر استخداما من قبل مجموعات مرتكبي الهجمات ببرمجيات انتزاع الفدية في العالم هي الرسائل الإلكترونية، والويب، وتطبيقات الويب، والبرمجيات الخبيثة مثل التطبيقات المزيفة للهواتف المحمولة، واستغلال ثغرات النظام كالاتصالات غير المأمونة التي تجرى عبر بروتوكول سطح المكتب البعيد.

ولتعزيز الجهود الرامية إلى منع الهجمات، وكشفها، والتخفيف من حدتها، لا بد من فهم كيفية تمكّن الجهات الفاعلة المسؤولة عن التهديد من الدخول الأولي إلى النظام لنشر برمجيات انتزاع الفدية. وعلى وجه الخصوص، تستغل معظم وسائل الهجوم العنصرَ البشري، سواء كان من المستخدمين الذين ينقرون على عنوان إلكتروني خبيث، أو من الموظفين الإداريين في تكنولوجيا المعلومات الذين يخفقون على نحو مستمر في تحديث أو تعديل نظامهم. وبالفعل، تشير الأبحاث التي أجرتها شركة Fortinet للأمن السيبري، وهي أحد شركاء الإنتربول في مشروع Gateway، إلى أن العديد من مجموعات مرتكبي الجرائم ببرمجيات انتزاع الفدية تكرس المزيد من الوقت لاختيار ضحاياها وإجراء البحوث بشأنهم[13]. وتعوّل هذه المجموعات على المعلومات المستقاة من الحسابات الشخصية على وسائل التواصل الاجتماعي، ومواقع الشركات على الويب، وصفحات الويب المخصصة للمؤتمرات، والبيانات القديمة المسربة، من أجل تنفيذ هجمات بتقنيات الهندسة الاجتماعية على نحو أكثر فعالية والتمكن من الدخول الأولي إلى النظام لنشر برمجية انتزاع الفدية.

أساليب الابتزاز الرقمي تتغير

بعد أن تتمكن الجهات الفاعلة المسؤولة عن التهديد ببرمجيات انتزاع الفدية من الدخول الأولي إلى النظام، تسعى عادة إلى إجراء مسح للبنية التحتية للشبكة الخاصة بالضحية وإلى التحرك أفقيا في النظام من خلال استغلال الثغرات وترسيخ مكتسباتها. ثم تقوم بنشر البرمجيات الخبيثة التي تشفّر بيانات الضحية وتطلب منها فدية مقابل إعادة تشغيل ملفاتها. ولممارسة المزيد من الضغط على الضحية، يستخدم العديد من المجموعات برمجيات تخويف أو أساليب ابتزاز إضافية. فعلى سبيل المثال، قد يقوم المهاجمون بتسريب البيانات قبل تشفيرها ثم يهددون بنشر المعلومات الحساسة (ابتزاز مزدوج)، واستخدام هجمات حجب الخدمة لشل عمل الضحية التي ترفض دفع الفدية (ابتزاز ثلاثي)، لا بل يهددون الأطراف الثالثة المتعاقدة مع الضحية لممارسة المزيد من الضغط عليها (ابتزاز رباعي)

ولكن كشف الإنتربول في السنوات الأخيرة عن الاستخدام المتزايد لتسريب البيانات كأداة للابتزاز الرقمي. وبعد التسلل إلى نظام الضحية بشكل أولي، باتت بعض مجموعات مرتكبي الجرائم ببرمجيات انتزاع الفدية تفضل اليوم تجاوز مرحلة التشفير والاكتفاء بتسريب المعلومات الحساسة. ثم تهدد الضحية بنشر هذه المعلومات إذا رفضت دفع الفدية. ونظرا للأضرار المالية والنفسية والمتعلقة بالسمعة التي قد تنجم عن هذا التسريب، فإن العديد من المؤسسات باتت على ما يبدو أكثر استعدادا لدفع هذه الفدية. وقد تصل هذه الأخيرة إلى عدة ملايين من الدولارات على الرغم من أنها لا تنطوي على أيّ شيء يضمن قيام المعتدين بحذف البيانات المسروقة بالفعل. وبالنظر إلى إمكاناته المربحة، سرعان ما يفرض تسريب البيانات نفسه كأسلوب إجرامي لا غنى عنه، ويستعاض به عن تشفير البيانات أو يؤازره، مما يؤدي إلى تحولات في برمجيات انتزاع الفدية والابتزاز الرقمي

لمحة عامة عن نموذج للهجوم ببرمجيات انتزاع الفدية وتسريب البيانات

12 شركة Trend Micro (2023): https://newsroom.trendmicro.com/2022-08-31-Trend-Micro-Warns-of-75-Surge-in-Ransomware-Attacks-on-Linux-as-Systems-Adoptions-Soared

13 شركة Fortinet (2023): https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf

برامج ' التابعين'ونمو نهج الخدمات المترابط لمرتكبي الجرائم السيبرية

بالإضافة إلى تغيّر الأساليب الإجرامية، قد يعزى التأثير المتزايد لبرمجيات انتزاع الفدية، في جزء منه، إلى نشوء نماذج تنظيمية جديدة يستخدمها مرتكبو الجرائم السيبرية. وكشف الإنتربول وشركاؤه عن أن العديد من المجموعات التي تستخدم برمجيات انتزاع الفدية تقوم حاليا بإدارة برامج مبتكرة للتابعين، تنص على استحداث منصات ترمي إلى تقديم برمجيات انتزاع الفدية كخدمة لأطراف ثالثة من الجناة يُعرفون باسم " التابعين". ويتمكن هؤلاء من استخدام المنصات التي توفرها لهم نواة المجموعات التي تستخدم برمجيات انتزاع الفدية، من أجل بث برمجياتهم الخبيثة، ونشر البيانات المسرّبة، وغسل عائدات جرائمهم. ويقوم التابعون، مقابل استخدام المنصة، بدفع رسوم لهذه النواة، إما في شكل اشتراك شهري أو كنسبة مئوية تُقتطَع من أموال الفدية التي حصلوا عليها بفضل المنصة

وكلما أُتقنت هذه العمليات المقدَّمة كخدمة، أتاحت لمرتكبي الجرائم السيبرية تنظيم إجراءاتهم وتكثيف أنشطتهم، وأسهمت أيضا في نشوء أشكال جديدة منها أكثر تطورا وأكثر شراسة. وكشفت شركة Fortinet عن وجود أكثر من 10,600 شكل جديد من برمجيات انتزاع الفدية في النصف الأول من عام 2022، أي ضعف العدد المسجل في الأشهر الستة السابقة[14]. والأهم من ذلك، تعوّل برامج التابعين وغيرها من عمليات انتزاع الفدية المقدَّمة كخدمة على التعزيز المتواصل لنهج الخدمات المترابط لمرتكبي الجرائم السيبرية، وزيادة تخصصه في هذا المجال. ويجند أعضاء نواة المجموعات التي تستخدم برمجيات انتزاع الفدية عدة خبراء لتشغيل برامج التابعين، بما في ذلك مطورو البرامج ومختبروها ومديروها، ومديرو البيانات، والمفاوضون، والمسؤولون عن التجنيد، والخبراء في القانون، والمحاسبون[15]. ويستعينون أيضا بمزودي خدمة خارجيين مثل الوسطاء المتمرسين في مجال الدخول الأولي، وبخدمات غسل الأموال وإيواء المراكز الإلكترونية الخبيثة. وعلى سبيل المثال، قدّم Br0k3r ، وهو أحد الوسطاء الأكثر نشاطا في أفريقيا والشرق الأوسط في مجال الدخول الأولي، أكثر من 60 عرضا لاختراق شبكات مهنية مع بيع حقوق إدارة نطاقها، وذلك عبر موقعه الإلكتروني خلال السنة الماضية[16]. ويمكن للتابعين ومزودي الخدمة، بصفتهم أعضاء في نواة المجموعات، الانتماء إلى عدة مجموعات أخرى، ومن المهم تقويض نهج الخدمات المترابط لمرتكبي الجرائم السيبرية ككل للتمكن من تعطيل الجريمة السيبرية بشكل فعال.

الوسيط في مجال الدخول الأولي	برمجيات انتزاع الفدية للتابعين	مدير البيانات	مشغل برمجيات انتزاع الفدية	مفاوض	المطارد	المحاسب
التمكن من الدخول الأولي إلى نظام المؤسسات مقايضة قيمة الشبكات لبيعها إلى أيّ جهة فاعلة	الثبات/الاستطلاع التحرك الأفقي تصعيد الامتياز نشر برمجيات انتزاع الفدية	توفير بنية تحتية وبرامج لتسريب البيانات تسريب البيانات من مؤسسة ضحية نشر البيانات المسربة عند الاقتضاء	توفير البنية التحتية الخاصة ببرمجيات بانتزاع الفدية والبرامج ذات الصلة	التفاوض مع المؤسسة الضحية	الضغط على المؤسسات الضحية من خلال تهديدها بمواصلة الهجمات وتسريب البيانات المسروقة	غاسل أموال الفدية
داخل	عبر		خارج			

المصدر: Northwave-Cybersecurity.com

لمحة عامة عن نهج الخدمات المترابط لمرتكبي الجريمة السيبرية الذي يكمن وراء برمجيات انتزاع الفدية

14 شركة Fortinet (2023): https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf

15 يوروبول (2023): https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf

16 شركة Group-IB (2024): https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2023-mea/

عملية LANDSLIDE

في بداية عام 2023، أطلق الإنتربول عملية تحمل الاسم الرمزي Landslide وتستهدف البنى التحتية التي تسهّل ارتكاب الجرائم السيبرية، من قبيل برمجيات انتزاع الفدية. وتمثّل الهدف المحدد من هذه العملية في القضاء على أسلوب إجرامي يسهّل ارتكاب الجريمة وبقي لفترة طويلة خارج سيطرة أجهزة إنفاذ القانون، ألا وهو: خدمة إيواء المراكز الإلكترونية الخبيثة (bulletproof hosting). وحدد الإنتربول، بالتعاون مع السلطات في سيشيل وأحد شركائه من القطاع الخاص Trend Micro، عددا من مزودي خدمة الإيواء الضالعين في تسهيل ارتكاب أنشطة غير مشروعة. وبفضل استخدام نتائج الأنشطة الميدانية السابقة، تمكّن الإنتربول من تنظيف البنية التحتية الخبيثة، وتفكيكها. ولا تزال العملية جارية

القدرة على الصمود في وجه برمجيات انتزاع الفدية: تقدّم ملحوظ وصعوبات جارية

اتخذت البلدان الأفريقية الأعضاء في الإنتربول تدابير مهمة لمواجهة التهديد المتواصل الذي تطرحه برمجيات انتزاع الفدية. فعلى سبيل المثال، استحدث أكثر من 60 في المائة من هذه البلدان آلية للإبلاغ عن الهجمات السيبرية للمساعدة على تسهيل كشفها، والتخفيف من حدتها، والتحقيق فيها. وتعمل البلدان أيضا على تعزيز تعاونها مع القطاع الخاص، إذ أرسى ثلثا البلدان الأفريقية الأعضاء التي أجابت على الاستبيان شراكات مع الجهات المعنية من القطاع الخاص للتصدي لبرمجيات انتزاع الفدية. وبالإضافة إلى ذلك، أفادت البلدان الأفريقية بأنها تبذل جهودا إضافية لتوعية الشركات بمخاطر الابتزاز السيبري. وعلى الصعيد الإقليمي، حدث تطور إيجابي آخر يتمثل في إنشاء أفرقة عاملة مشتركة تشارك فيها أجهزة إنفاذ القانون في جميع أنحاء أفريقيا، من أجل التصدي للهجمات ببرمجيات انتزاع الفدية، والتوعية بعواقبها.

وعلى الرغم من هذه الإنجازات الكبيرة، أفادت البلدان الأعضاء بأنها تواجه صعوبات مستمرة. ولا يزال مستوى البلاغات الواردة من ضحايا الهجمات ببرمجيات انتزاع الفدية فيها يطرح مشكلة ويؤثّر في قدرة أجهزة إنفاذ القانون على فتح تحقيقات في هذا الصدد. كما أفادت البلدان الأعضاء بأن 16 في المئة من الضحايا ينتهي بهم الأمر إلى دفع الفدية عند تعرّضهم لهذا النوع من الهجمات. ومع الأسف، لا يضمن دفع الفدية توقف الهجوم ولا حذف البرمجيات الخبيثة من النظام. لا بل إن الضحية، في بعض الحالات، لا تسترجع حتى بياناتها أو تضطر إلى دفع ضعف المبلغ المطلوب منها[17]. وكذلك، فإن دفع الفدية لا يحول دون وقوع الضحية في الشباك مرة أخرى، لا بل إن ذلك من شأنه أن يحفّز مرتكبي الجرائم ببرمجيات انتزاع الفدية على مواصلة أنشطتهم وتوسيع نطاقها، ويمدّهم بالموارد اللازمة. والإنتربول، إذ يدرك هذه المشكلة، أصدر في تشرين الثاني/نوفمبر 2023، وبالتعاون مع خمسين عضوا في المبادرة الدولية لمكافحة برمجيات انتزاع الفدية، بيانا مشتركا يحث فيه بشدة المؤسسات على عدم دفع هذه الفدية[18]

عمليات الاحتيال الإلكتروني

النقاط الرئيسية:

- عمليات الاحتيال الإلكتروني والأساليب الإجرامية المتصلة بها تتغيران باستمرار، ويختار مرتكبو هذه الجرائم ضحاياهم من مختلف الفئات السكانية والقطاعات.
- التصيد الاحتيالي عبر البريد الإلكتروني ووسائل التواصل الاجتماعي يستغل العنصر البشري ويعمل بمثابة بوابة عبور مهمة لارتكاب جرائم سيبرية أخرى.
- الذكاء الاصطناعي يتيح سبلا جديدة للمجرمين لارتكاب ما يُعرف بجريمة تسمين الخنزير قبل ذبحه والحيَل الرومانسية.
- الهواتف الذكية، التي تعكس الاتجاهات الاجتماعية، لا تزال تشكّل هدفا لمرتكبي جرائم الاحتيال بواسطة برمجيات حصان طروادة لسرقة البيانات المصرفية.

17 شركة Sophos (2023): https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/

18 يمكن الاطلاع على هذا البيان عبر الموقع الرسمي على الويب للمبادرة المتعلقة بمكافحة برمجيات انتزاع الفدية : https://counter-ransomware.org/briefingroom/8ed7d1de-1a74-4a36-a2df-d5950624ebd8

عمليات الاحتيال الإلكتروني، أزمة اقتصادية واجتماعية كبرى في أفريقيا

بالإضافة إلى برمجيات انتزاع الفدية، تشكل عمليات الاحتيال الإلكتروني أحد أبرز التهديدات السيبرية التي حددتها البلدان الأفريقية الأعضاء في عام 2023، ولا سيما من حيث الحجم والتداعيات المالية بشكل عام. فهذه العمليات هي فعلٌ أو حيلة تُنفَّذ باستخدام تكنولوجيا المعلومات وعن طريق الإنترنت لغرض سرقة أموال و/أو بيانات شخصية من أشخاص أو مؤسسات . ولتحقيق هذه الغاية، يستعين المجرمون عادة بمجموعة من العناصر التقنية، مثل التصيد الاحتيالي والبرمجيات الخبيثة، المقترنة بتقنيات الهندسة الاجتماعية[19].

ويرتبط النمو الهائل لعمليات الاحتيال الإلكتروني بالتحول الرقمي الذي يجتاح القارة الأفريقية[20]. وبما أن الأفريقيين باتوا يمضون مزيدا من الوقت على الإنترنت، للتواصل، على سبيل المثال، عبر شبكات التواصل الاجتماعي، أو لدفع مشترياتهم عن طريق الخدمات المصرفية المتاحة عبر الهواتف المحمولة، فقد اتسع نطاق الهجوم المتاح أمام المجرمين الذين يحاولون ارتكاب عمليات الاحتيال بالوسائل الرقمية. ومن الصعب تحديد حجم الخسائر الناجمة عن عمليات الاحتيال الإلكتروني في جميع أنحاء القارة الأفريقية، ولكن البلدان الأعضاء في الإنتربول أشارت إلى أن الضحايا يتوزعون على مختلف الفئات العُمرية والأجناس والمهن. وصحيح أن بعض المجموعات قد تكون أكثر عرضة لبعض أشكال الاحتيال الإلكتروني، ولكن أياً من المواطنين قد يصبح ضحية في نهاية المطاف. وكذلك، فإن المؤسسات التي تستهدفها عمليات الاحتيال الإلكتروني تتراوح بين الشركات الصغيرة والمتوسطة الحجم والمؤسسات الكبرى، وتتوزع على مختلف القطاعات والصناعات. وخلاصة القول، يشكل انتشار عمليات الاحتيال الإلكتروني في أفريقيا أزمة اجتماعية واقتصاردية كبرى تصل أصداؤها إلى بلدان المنطقة وما بعدها.

وشملت المجموعة الواسعة لعمليات الاحتيال الإلكتروني خمسة أنواع من المخططات الاحتيالية التي أفادت البلدان الأفريقية الأعضاء في الإنتربول بأنها بالغة الأهمية في عام 2023، وهي، وفقا للترتيب الذي طُرحت فيه للمناقشة، على النحو التالي: الاحتيال بالبريد الإلكتروني المهني، والتصيد الاحتيالي، والحيَل الرومانسية، وجريمة تسمين الخنزير قبل ذبحه، وعمليات الاحتيال عن طريق الهواتف المحمولة. وترد فيما يلي دراسة تحليلية لمختلف أشكال هذه العمليات، باستثناء الاحتيال بالبريد الإلكتروني المهني، الذي تُخصَّص له فقرة نظرا لتفشيه الواسع النطاق في أفريقيا.

التصيد الاحتيالي بالبريد الإلكتروني ووسائل التواصل الاجتماعي يعمل بمثابة بوابة عبور لارتكاب جرائم سيبرية أخرى

حُدد التصيد الاحتيالي من قِبل البلدان الأفريقية الأعضاء كأحد أبرز التهديدات في مجال الاحتيال الإلكتروني، سواء من حيث عدد الحالات المبلَّغ عنها أو الأثر الاجتماعي والاقتصادي الذي يخلفه في جميع أنحاء القارة. والتصيد الاحتيالي نوع من أنواع الاحتيال الإلكتروني ينتحل فيه المجرمون صفة مؤسسة أو كيان مشروع من خلال البريد الإلكتروني أو منصات المراسلة الإلكترونية أو المواقع المزيفة على الويب، وذلك للتمكن من خداع الأشخاص وجعلهم يفصحون عن معلومات شخصية حساسة[21]. وغالبا ما تشمل هذه المعلومات بيانات تسجيل الدخول، وتفاصيل مالية (مثل أرقام بطاقات الائتمان)، وأرقام الضمان الاجتماعي، وغيرها من البيانات التي يمكن استخدامها للوصول غير المشروع إلى حسابات أو القيام بسرقة بيانات الهوية أو سرقة الأموال. وتتضمن محاولات الاحتيال عادة اتصالات عاجلة أو مثيرة للقلق ترمي إلى حث المتلقي على اتخاذ تدابير فورية، مثل النقر على رابط إلكتروني خبيث أو تنزيل ملف مرفق ملوث ببرمجية خبيثة أو تقديم معلومات سرية على نحو مباشر. وإذا كان الهدف الأول من التصيد الاحتيالي هو استغلال سيكولوجيا النفس البشرية للوصول إلى بيانات أو أصول قيّمة، فإن الهجمات بالتصيد الاحتيالي غالبا ما تقوم، من الناحية العملية، مقام بوابة عبور لارتكاب جرائم سيبرية أخرى، بما في ذلك برمجيات انتزاع الفدية ومختلف أنواع عمليات الاحتيال الإلكتروني

وحُدّد في أفريقيا شكلان من أشكال التصيد الاحتيالي استنادا إلى نتائج الدراسة الاستقصائية والبيانات الداخلية للإنتربول، ألا وهما: التصيد الاحتيالي التقليدي، والتصيد الاحتيالي الاجتماعي. وفي هذا السياق، اعتبرت البلدان الأفريقية الأعضاء أن التصيد الاحتيالي التقليدي هو التهديد الأكبر للجريمة السيبرية في المنطقة. وحملات التصيد الاحتيالي التقليدي، التي تُشن عبر البريد الإلكتروني بشكل رئيسي، غالبا ما تنطوي على رسائل إلكترونية تأتي من عناوين ظاهرها مشروع وباطنها زائف. ويتمثل الغرض من ذلك في خداع المتلقين لحثهم على زيارة مواقع احتيالية على الويب، أو النقر على روابط إلكترونية خبيثة، حيث يقوم الجناة فيما بعد بسرقة أيّ بيانات شخصية يتم إدخالها. ومن أشكال التصيد الاحتيالي الشائعة الاحتيال بالبريد الإلكتروني المهني، الذي سيتم التطرق إليه بإسهاب في القسم التالي من هذا التقييم.

19 تتعاون إدارة الإنتربول لمكافحة الجريمة السيبرية تعاونا وثيقا مع مركز الإنتربول لمكافحة الجريمة المالية والفساد، من أجل كبح نمو عمليات الاحتيال الإلكتروني. وللحصول على المزيد من المعلومات عن المركز، يرجى الاطلاع على الصفحة الإلكترونية التالية: https://www.interpol.int/en/Crimes/Financial-crime

20 صحيفة IJSSRR (2023): https://www.ijssrr.com/journal/article/view/1360

21 شركة CSCR (2023): https://csrc.nist.gov/projects/human-centered-cybersecurity/research-areas/phishing

وعلى الرغم من الأهمية المتواصلة للتصيد الاحتيالي التقليدي، تشير البلدان الأعضاء إلى زيادة في استخدام وسائل التواصل الاجتماعي وتطبيقات المراسلة الفورية لارتكاب هجمات بالتصيد الاحتيالي. والأسلوب الإجرامي المستخدَم مشابه لما يجري في التصيد الاحتيالي التقليدي ولكنه يمر عبر منصات مختلفة، حيث يستخدم الجناة حسابات زائفة على وسائل التواصل الاجتماعي ورسائل وهمية كطُعم للحصول على البيانات المالية والمعلومات الشخصية لضحاياهم. ووفقا للبيانات الواردة من البلدان الأعضاء في الإنتربول، فإن المنصات الأكثر استخداما في عمليات التصيد الاحتيالي في أفريقيا هى منصة Meta (المعروفة سابقا باسم فايسبوك)، ومنصتا Messenger وWhatsApp. وتعديل تقنيات التصيد الاحتيالي لتشمل وسائل التواصل الاجتماعي وخدمات المراسلة إنما هو وسيلة لاستهداف طُرق التواصل السائدة في المنطقة، ويبيّن قدرة الجناة على استغلال الاتجاهات التكنولوجية والاجتماعية لتنفيذ مآربهم الخبيثة.

ويرتكز هذان الشكلان للتصيد الاحتيالي على الهندسة الاجتماعية. وفي هذا الصدد، ووفقا لما أفادت به البلدان الأعضاء، فإن استخدام الجهات الفاعلة المسؤولة عن التهديد لأساليب تزداد تعقيدا في مجال الهندسة الاجتماعية في إطار حملات حديثة من التصيد الاحتيالي أمرٌ يبعث على القلق. وعلى سبيل المثال، وأثناء تنفيذ عملية Echoes التي قادها المغرب بدعم من الإنتربول وشركائه من القطاع الخاص، تبيّن أن المجرم المعروف باسم "Ex-Robotos" الذي اشتُهر بإنشائه مجموعة من أدوات التصيد الاحتيالي تحمل الاسم نفسه، كان يختار ضحاياه بدقة من خلال بحث يجريه عبر الإنترنت، ويركز بشكل خاص على رؤساء الشركات وغيرهم من المدراء التنفيذيين. وفي حالات أخرى، كان الجناة يلجؤون إلى خدمات مشروعة ويقومون بالتحكم في النطاقات والحسابات الإلكترونية لتعزيز فرص نجاح هجماتهم بالتصيد الاحتيالي. وأخيرا، تشير البيانات الواردة من البلدان الأعضاء في الإنتربول والجهات الشريكة في مشروع Gateway إلى أن الذكاء الاصطناعي هو أحدث تطور تكنولوجي يستخدمه الجناة للحد، على سبيل المثال، من إشارات التنبيه المتعلقة بالتصيد الاحتيالي التقليدي إلى أدنى مستوى ممكن

عملية Echoes:

في أيار/مايو 2023، تمكنت السلطات المغربية، بالتعاون الوثيق مع الإنتربول وشركتي Microsoft وGroup-IB، من إحباط الجرائم السيبرية التي يرتكبها جناة يُشتبه في استخدامهم مجموعة تطبيقات Microsoft 365 بطريقة احتيالية لاستهداف آلاف الضحايا. وتمكّن الجناة بفضل مجموعة الأدوات هذه من سرقة بيانات الضحايا من أجل، إما مقايضتها لقاء مبلغ من المال فور ذلك مباشرة وإما بيعها على الشبكة الخفية. وتستند هذه العملية المشتركة التي تحمل اسم Echoes إلى تعاون مسبق مع السلطات المغربية، ولا سيما في إطار عملية Lyrebird، وتثبت عزيمة المغرب على مكافحة التهديدات السيبرية

انتحال الهوية والابتزاز الجنسي يسهمان في انتشار آفة الحيَل الرومانسية

كشفت أيضا البيانات التي أحالتها البلدان الأفريقية الأعضاء في الإنتربول عن تفاقم حجم وتأثير وتعقيد عمليات الاحتيال الرومانسي التي حدثت في القارة الأفريقية، وانطلاقا منها، في عام 2023. وقد تتخذ عمليات الاحتيال الرومانسي عدة أشكال، ولكنها تنطوي جميعها على قيام الجناة بالتظاهر بعلاقة عاطفية أو صداقة حميمة لتحقيق مكاسب مالية. وبشكل عام، يقوم الجناة بالتواصل مع ضحاياهم تحت غطاء علاقة رومانسية، وغالبا ما ينتحلون هوية مزيفة عبر الإنترنت. ووفقا للبيانات التي أفادت بها البلدان الأعضاء في الإنتربول، غالبا ما يتقرب الجناة في أفريقيا من الشخص المستهدف من خلال وسائل التواصل الاجتماعي، وخدمة المراسلات الإلكترونية، وتطبيقات المواعدة الإلكترونية. ثم يحاولون إقامة علاقة شخصية مع الضحية التي يستغلون مواطن ضعفها وهشاشتها. وقد تنتهي هذه المرحلة بسرعة شديدة أو قد تدوم لعدة سنوات. وبعد أن يتمكن الجناة من ترسيخ علاقة الثقة الموهومة، يشرعون في التحايل على الضحية و/أو سرقة بياناتها

وفي أفريقيا، سلطت البلدان الأعضاء في الإنتربول الضوء على اتجاهين لهما أهمية خاصة في عمليات الاحتيال الرومانسي: انتحال الهوية والابتزاز الجنسي. وفي سياق هذه العمليات، يحدث انتحال الهوية عندما يستحدث الجناة هوية مزيفة عبر الإنترنت لخداع ضحاياهم[22]. ولهذه الغاية، يقوم الجناة بسرقة معلومات وصور لغيرهم من الأشخاص لابتكار هوية مزيفة لأنفسهم. وتتراوح عمليات الخداع بين استخدام صورة هوية مسروقة لتعزيز المظهر الجذاب والاستيلاء الكامل على هوية شخص آخر، بما في ذلك اسمه، وصورته، وجنسه، وتاريخ ولادته، وموقعه الجغرافي. ووفقا للبلدان الأفريقية الأعضاء في الإنتربول، تهدف جرائم انتحال الهوية إلى اختيار أهداف محددة وتنفيذها يدوم لفترة طويلة من الزمن. وبعد اختيار ضحاياهم، يستخدم الجناة سيناريو معدّا بإحكام لبناء علاقة موثوقة معهم، وذلك قبل محاولة التلاعب بعواطفهم لجعلهم يقدمون على تحويل الأموال. فقد يدّعي الجاني، على سبيل المثال، أنه هو أو أحد المقرّبين إليه، مريض أو مصاب أو محتجز في السجن، أو أنه بحاجة إلى دعم مالي لمقابلة الضحية وجها لوجه، أو أنه يخطط لبناء مستقبل مشترك معها[23]. وما إن يتم تحويل الأموال حتى يختفي الجاني، ويترك وراءه ضحية، ليس فقط مجردة من

22 انتحال الهوية ممارسة موجودة منذ سنوات عديدة، وخصوصا عبر منتديات ومواقع المواعدة الإلكترونية. وقد ينخرط الأشخاص في ذلك لأسباب مختلفة. فمنهم من تكون دوافعه الشعور بعدم الأمان، ومنهم من يتصرف بنيّة خبيثة، للتسلط على الضحية أو الاحتيال عليها، على سبيل المثال.

23 لجنة التجارة الاتحادية في الولايات المتحدة (2023): https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

أموالها بل أيضا في حالة عاطفية ونفسية يرثى لها. ويقوم بعض الجناة، بالإضافة إلى استخدام أساليب الهندسة الاجتماعية التي لا تزال تزداد تعقيدا، بالاستفادة من التقدم التكنولوجي الحاصل في مجال الذكاء الاصطناعي. فبالإضافة إلى ابتكار صور مزيفة لاستقطاب الضحية، يقوم الجناة باستغلال منصات الدردشة المستندة إلى الذكاء الاصطناعي مثل برنامج LoveGPT لإنشاء هوية مزيفة لهم، ومساعدتهم على تحرير النصوص، وتصيد ضحاياهم في نهاية المطاف عبر تطبيقات المواعدة[24].

أما الاتجاه الثاني في مجال عمليات الاحتيال الرومانسي، الذي أبلغت عنه البلدان الأفريقية الأعضاء، فهو ارتفاع في حالات الابتزاز الجنسي. ولهذه الجريمة بعض أوجه الشبه مع أشكال أخرى من الاحتيال الرومانسي. ويستخدم الجناة عادةً هوية مزيفة للاتصال بضحاياهم، الذين يكون معظمهم من الشباب، عن طريق تطبيقات المواعدة، ووسائل التواصل الاجتماعي، وغيرها من المنصات الإلكترونية. ولكن، بعد أن يفوز الجناة بثقة الضحية، يشرعون في إقناعها بإرسال معلومات حميمة أو تنطوي على عناصر جنسية واضحة، ثم يهددون بنشر هذا المحتوى على الإنترنت أو بمشاركته مع الأهل والأصدقاء كشكل من أشكال الابتزاز. ولممارسة مزيد من الضغط على الضحية، يبدأ الجناة بنشر المعلومات الحميمة الخاصة بالضحية على الإنترنت، ثم يطالبون بدفع الأموال مقابل سحبها. وعلى الرغم من أن الابتزاز الجنسي يرتبط في كثير من الأحيان برسائل أو صور أو مقاطع فيديو واضحة، تجدر الإشارة إلى أن الجاني قد لا يحتاج في بعض المجتمعات المحلية إلى أكثر من التهديد بنشر محادثات ذات طابع رومانسي لكي يبتز ضحيته

ويبدو أن الأسلوب الإجرامي المتمثل في الابتزاز الجنسي ناشط جدا. فعلى سبيل المثال، أبلغت بعض البلدان الأعضاء عن حالات ابتزاز جنسي استُخدمت فيها طرق التصيد الاحتيالي لاستهداف المحتوى (غير المنشور) الخاص بالضحايا على حساباتهم على منصة فايسبوك وإنستغرام. وفي هذه الحالات، يصل الجاني على نحو غير مشروع إلى المعلومات الشخصية للضحايا المسجلة على وسائل التواصل الاجتماعي، وهناك يقوم بالبحث عن المحتويات الحميمة ويستخرجها بصورة منهجية. وتبلغ هذه الجريمة ذروتها عندما يقوم الجاني بابتزاز الضحية من خلال تهديدها بنشر المحتوى الخاص بها على وسائل التواصل الاجتماعي أو بمشاطرتها بأشكال مختلفة، ما لم تقم بدفع مبلغ مالي له. وظهر مؤخرا تطور آخر ينطوي على استخدام الذكاء الاصطناعي وسيلةً لإنشاء صور تحتوي على مشاهد جنسية واضحة تكون " أصدق من الحقيقة"من أجل تخويف الضحية وابتزازها، بما في ذلك القُصّر[25]. ونظرا للصعوبات الكبرى التي قد تواجهها الضحية لإزالة هذا المحتوى المتلاعَب به بعد نشره على الإنترنت، يفضل بعضهم دفع المال للمبتزين.

وأثبتت عمليات الاحتيال الرومانسي أنها مربحة للغاية. وتشير التقارير الصادرة عن بعض البلدان الأفريقية الأعضاء إلى أن الأموال المدفوعة ردا على عمليات الاحتيال الرومانسي التي تشمل التصيد الاحتيالي والابتزاز الجنسي ليست مجرد حوادث معزولة. وعلى العكس، يجد الضحايا أنفسهم في كثير من الأحيان مضطرين إلى دفع ما يرقى إلى رسوم شهرية متكررة، إما للحفاظ على علاقتهم الرومانسية الموهومة، وإما لمنع نشر المحتوى الشخصي الخاص بهم. وتشير بعض التقديرات إلى أن الخسائر المرتبطة بهذا التهديد السيبري على المستوى العالمي فاقت 1,3 مليار دولار أمريكي بين عامي 2017 و2022، حيث تخسر الضحية مبلغا وسطيا يعادل 4,400 دولار أمريكي تقريبا لكل عملية احتيال[26]. وبمعزل عن الأثر المالي، قد تستتبع عمليات الاحتيال الرومانسي آثارا عاطفية مدمرة على الضحايا حيث تصل بعض الحالات إلى حد الانتحار. وفي الواقع، وبسبب شعور الضحية بالعار والذنب و/أو الإنكار، والوصمة الاجتماعية المتواصلة، يبقى الكثير من هذه الحوادث طي الكتمان. وذلك يعني أنه، على غرار الجرائم السيبرية الأخرى، قد يكون الأثر الفعلي لعمليات الاحتيال الرومانسي أكبر مما تعلنه الأرقام الرسمية. ومن المتوقع أن يؤدي تزايد حجم عمليات الاحتيال الرومانسي، ومداها، وتعقيدها، إلى طرح عدد متنام من الصعوبات في التحقيقات التي تجريها أجهزة إنفاذ القانون في جميع أنحاء أفريقيا، الأمر الذي يحتم تزويد هذه الأجهزة بالتدريب اللازم والقدرات في مجال الأدلة الجنائية.

عملية Contender: توجيه ضربة لعمليات الاحتيال الرومانسي

تعاون الإنتربول في إطار عملية Contender مع الأجهزة المعنية بمكافحة الجريمة السيبرية في بنن وسويسرا وفنلندا وكوت ديفوار ونيجيريا، ومع عدة جهات شريكة من القطاع الخاص، وذلك من أجل تفكيك شبكات الجريمة السيبرية المنظمة التي تقف وراء عمليات الاحتيال الرومانسي. وأفضت العملية إلى اعتقال ثلاثة مشتبه فيهم في كوت ديفوار وبنن في بداية عام 2023، وإلى مصادرة أجهزة رقمية ومحمولة يتم استخدامها لأغراض خبيثة.

24 شركة Avast (2023): https://decoded.avast.io/threatintel/lovegpt-how-single-ladies-looking-for-your-data-upped-their-game-with-chatgpt/

25 وكالة رويترز (2023): https://www.reuters.com/world/us/fbi-says-artificial-intelligence-being-used-sextortion-harassment-2023-06-07/

26 لجنة التجارة الاتحادية في الولايات المتحدة (2022): https://www.ftc.gov/news-events/blogs/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021

تسمين الخنزير قبل ذبحه، تهديدٌ هجين يتنامى بسرعة

كما هو الحال في سائر المناطق في العالم، كشفت البلدان الأعضاء في الإنتربول عن أن ما يسمى بجريمة "تسمين الخنزير قبل ذبحه" برزت في عام 2023 كأحد أسرع أشكال الاحتيال الإلكتروني نموا. وعلى الرغم من أن هذه الظاهرة حديثة بعض الشيء، أبلغ أكثر من ثلث البلدان الأفريقية الأعضاء في عام 2023 عن حوادث من هذا النوع، ولا سيما في غرب أفريقيا وجنوبها[27]. ووفقا للبيانات الداخلية، تخلّف هذه الجريمة تبعات مالية كبيرة في جميع أنحاء القارة، بما يتماشى مع الأنماط المسجلة عالميا. وتشير الأبحاث إلى أن المبلغ الوسطي الذي يتم تحويله إلى محافظ العملات المشفرة الخاصة بالجناة يتراوح بين 10,000 و100,000 دولار أمريكي، في حين تشير التقديرات إلى أن الخسائر العالمية التي تعزى إلى هذه الجريمة والجرائم الأخرى المرتبطة بالعملات المشفرة قد تضاعفت تقريبا منذ عام 2022، لتتخطى 3,3 مليارات دولار أمريكي في عام 2023[28].

وعلى نحو ما يوضحه تقييم الإنتربول العالمي بشأن تقييم عمليات الاحتيال المالي لعام 2024، فإن جريمة تسمين الخنزير قبل ذبحه هي عملية احتيالية هجينة، أي أنها تجمع بين عناصر الاحتيال في مجال الاستثمار في العملات المشفرة من جهة، والعناصر المرتبطة بعمليات الاحتيال الرومانسي من جهة أخرى. وتتبع هذه المخططات عادةً ثلاث مراحل رئيسية. أولا، يتواصل الجناة مع الأشخاص عن طريق المنصات الرقمية، ولا سيما وسائل التواصل الاجتماعي مثل فايسبوك وإنستغرام، وخدمات المراسلة مثل الرسائل النصية القصيرة (SMS) وواتسأب، وتلغرام، وسيغنال، أو من خلال تطبيقات المواعدة. وقد يزعم الجناة أنهم حصلوا على تفاصيل الاتصال بالضحية من خلال إحدى المرجعيات أو أحد الأصدقاء المشتركين. ولاجتذاب الضحية بشكل أفضل، يستخدم الجناة في كثير من الأحيان حسابا مزيفا، منتحلين هوية شخص جذاب من خلال صور مسروقة من أشخاص آخرين، أو صور استُحدثت بتقنية الذكاء الاصطناعي، وذلك وفقا لأسلوب إجرامي مشابه للأسلوب المستخدم في عمليات الاحتيال الرومانسي. وفي المرحلة الثانية، يقوم الجناة " بتسمين" الضحية من خلال كسب ثقتها، مقدّمين أنفسهم تدريجيا على أنهم خبراء في مجال الاستثمار. وينطوي أسلوب المجرمين على استقطاب الضحايا بلباقة للاستثمار في مشاريع للعملة المشفرة تبدو مشروعة ومربحة. ولكن ما إن تقوم الضحية بتحويل أموال طائلة أو ما إن تبدأ في إدراك أنها تتعرض لعملية احتيالية، يقوم الجناة بقبض هذه الأموال والتواري عن الأنظار. ويسعى الجناة عادة إلى تحويل أموال الضحية باستخدام وسائل الدفع الرقمية أو منصات العملات المشفرة، وذلك لجعل عملية تتبّع الأصول واستردادها أمرا صعبا إلى أقصى حد ممكن. وخلال هذه المرحلة الأخيرة، التي تُعرف أحيانا باسم "الذبح"، يتوقف الجناة عن الرد على رسائل أو مكالمات الضحية، مما يستتبع عواقب مالية ونفسية عليها.

مراحل نمط "تسمين الخنزير قبل الذبح"(المصدر: تقرير الإنتربول 2023 عن اتجاهات الجريمة في العالم)

27 تقرير الإنتربول العالمي بشأن تقييم عمليات الاحتيال المالي لعام 2024: https://www.interpol.int/ar/1/1/2024/2

28 شركة Trend Micro (2023): https://www.trendmicro.com/vinfo/sg/security/news/cybercrime-and-digital-threats/unmasking-pig-butchering-scams-and-protecting-your-financial-future

وفي الحالات التي أبلغت عنها البلدان الأفريقية الأعضاء في مجال الاحتيال بجريمة تسمين الخنزير قبل ذبحه، انقسمت بشكل عام أساليب الاتصال الأولية التي يستخدمها مرتكبو الجرائم السيبرية ما بين منصات الاتصال الاجتماعي (مثل فايسبوك وإنستغرام) وخدمات المراسلة عبر الأجهزة المحمولة (مثل واتسأب، وتلغرام، وسيغنال وSMS)، بما في ذلك استخدام برامج الدردشة الجماعية. وغالبا ما يواجه الأشخاص المستهدفون عبر وسائل التواصل الاجتماعي تقنيات للهندسة الاجتماعية أكثر شراسة مقارنةً بالنهج الأوسع والأقل خصوصية المستخدم عبر منصات المراسلة. وبالإضافة إلى ذلك، سلطت البلدان الأعضاء الضوء على سهولة ارتكاب جرائم تسمين الخنزير قبل ذبحه ومدى توافر مجموعة أدوات التصيد الاحتيالي اللازمة لذلك، واعتبرتهما عنصرين أساسيين في التفاقم المطرد لهذه الحالات طوال عام 2023.

ودفع هذا التفاقم بأجهزة إنفاذ القانون في البلدان الأفريقية الأعضاء إلى تحديد العقبات الخطيرة التي تعترض التحقيقات التي يجرونها، ولا سيما صعوبة الحصول على البيانات من مزودي الخدمات، والعدد الكبير للأجهزة التي تستدعي تحليلا جنائياً. كما أن تكاثر عمليات الاحتيال من خلال تسمين الخنزير قبل ذبحه، يؤدي، مثله مثل سائر الجرائم السيبرية، إلى تفاقم المشكلات القضائية. فعلى سبيل المثال، أظهرت إحدى العمليات التي نفّذها الإنتربول مؤخرا أن بعض الجناة الذين كانوا يرتكبون جرائم تسمين الخنزير قبل ذبحه انطلاقا من مراكز اتصال في ناميبيا، كانوا مرتبطين بشبكات إجرامية صينية معقدة ومتطورة . وللتصدي لهذه الصعوبات، اتخذت البلدان خطوات إيجابية بالفعل. وأُنشئت فرقة عمل خاصة مشتركة لمكافحة جريمة تسمين الخنزير قبل ذبحه في الجنوب الأفريقي وقد حققت بعض الإنجازات الملحوظة في هذا الصدد. ومن جهة أخرى، نظّم الإنتربول سلسلة من الدورات التدريبية وسهّل عقد الاجتماعات مع الجهات المعنية بتقديم الخدمات في القارة من أجل تعزيز الإجراءات الإقليمية المتخذة لمكافحة هذه الجريمة.

الهواتف الذكية، أهداف متنامية لمرتكبي جرائم الاحتيال في أفريقيا

شهدت البلدان الأفريقية الأعضاء عددا متزايدا من عمليات الاحتيال التي تستهدف مستخدمي الهواتف الذكية في عام 2023. ويعكس هذا التطور النمو المستمر في معدل انتشار الهواتف المحمولة في أفريقيا والارتفاع السريع في استخدام الخدمات المصرفية عبر هذه الهواتف في جميع أنحاء القارة[29]. وتنتمي عادةً عمليات الاحتيال الأكثر رواجا التي تُرتكب عبر الهواتف الذكية والتي حددتها أجهزة إنفاذ القانون إلى فئتين أساسيتين مترابطتين في كثير من الأحيان، هما: هجمات التصيد الاحتيالي، وبرمجيات حصان طروادة التي تستهدف البيانات المصرفية.

وتشمل الفئة الأولى توسيع نطاق هجمات التصيد الاحتيالي المذكورة آنفا، التي يحاول فيها الجناة استدراج الضحايا إلى مواقع احتيالية، مثل المواقع المصرفية المزيفة، وذلك من خلال متصفحات الويب المتوفرة على هواتفهم النقالة. وتنطوي الفئة الثانية التي ترصدها أجهزة إنفاذ القانون في أفريقيا بشكل متكرر على استخدام البرمجيات الخبيثة الشبيهة ببرمجيات حصان طروادة التي تستهدف البيانات المصرفية. وهي برمجيات مصممة لسرقة المعلومات المالية وغيرها من المعلومات الحساسة، مثل بيانات التعريف المصرفية على الإنترنت وأرقام الحسابات وبيانات بطاقة الائتمان، من الأجهزة الملوثة. ويمكن نشر هذه البرمجيات بطُرق هجوم متفرقة، ولا سيما من خلال الرسائل الإلكترونية الاحتيالية، أو النقر على المرفقات أو تنزيل البرمجيات المقرصنة، بما في ذلك التطبيقات المزيفة للهواتف المحمولة. وعلى غرار برمجيات حصان طروادة الخبيثة الأخرى، غالبا ما تعمل هذه البرمجيات كبرمجيات مشروعة للتمكن من الوصول إلى الجهاز المعني، مما يعسّر عملية كشفها. وتعمل كذلك كبرمجيات اتصال عن بُعد تسمح لمستخدمها بالتحكم عن بُعد بالنظام الملوث والقيام بهجمات أخرى، بما في ذلك عبر برمجيات انتزاع الفدية[30]. وبعد أن يتم تركيبها، تقوم البرامج الخبيثة بجمع وتسريب البيانات الحساسة من خلال أساليب متعددة من قبيل تسجيل النقر على لوحة المفاتيح، والتقاط صورة الشاشة، وتفريغ بيانات التعريف المستترة، والبحث عن كلمات السر المسجلة في النظام. ويمكن للجهات الفاعلة المسؤولة عن التهديد أن تستخدم لاحقا هذه المعلومات لسرقة الأموال مباشرة من الضحايا، على سبيل المثال، من خلال الوصول عن بُعد إلى تطبيقاتهم المصرفية، أو لارتكاب جرائم أخرى مثل سرقة بيانات الهوية وغيرها من عمليات الاحتيال.

وتطرح برمجيات حصان طروادة التي تستهدف البيانات المصرفية وعمليات الاحتيال الإلكترونية المرتبطة بها صعوبات كبرى على القارة الأفريقية نظرا لارتفاع عدد الحالات المبلَّغ عنها، ولا سيما في الجنوب الأفريقي. ونظرا لاعتماد السكان المتزايد على الهواتف الذكية وخدمات الدفع عبر الهاتف المحمول، أعربت جميع البلدان الأفريقية الأعضاء عن قلقها المتزايد بشأن الأثر الاجتماعي والاقتصادي الذي قد تستتبعه عمليات الاحتيال المرتبطة بهذه الهواتف. وبالإضافة إلى ذلك، تمارس هذه البرمجيات ضغطا متزايدا على القدرات والمهارات في مجال الأدلة الجنائية الرقمية في جميع أنحاء المنطقة. ولمواجهة هذه الصعوبات، قامت عدة بلدان باستثمارات كبرى في أدوات التحليل الجنائي التي سمحت لها بإعداد تقارير عن التحليل الجنائي لمئات الأجهزة خلال فترة الاستعراض. كما أن العديد من البلدان الأفريقية في صدد اتخاذ تدابير مهمة لمنع برمجيات حصان طروادة التي تستهدف البيانات المصرفية عبر الهاتف المحمول بشكل أفضل، والتحقيق فيها، والقضاء عليها. ويشمل ذلك إقامة شراكات مع المصارف لضبط واسترداد عائدات الجريمة، وإطلاق حملات التوعية التي تنبّه المواطنين إلى المخاطر المرتبطة باستخدام الخدمات المصرفية عبر الإنترنت.

29 انظر على سبيل المثال Statista (2023): https://www.statista.com/statistics/1133777/sub-saharan-africa-smartphone-subscriptions/

30 شركة Checkpoint (2023): https://www.checkpoint.com/cyber-hub/cyber-security/what-is-trojan/what-is-a-banking-trojan/

الاحتيال بالبريد الإلكتروني المهني

النقاط الرئيسية:

- الاحتيال بالبريد الإلكتروني المهني يجمع بين العناصر التقنية وأساليب الهندسة الاجتماعية المتطورة، ويشكّل تهديدا متناميا للمؤسسات والأفراد في جميع أنحاء أفريقيا، وخصوصا للعاملين في القطاع المالي
- إن تفاقم هذا التهديد الهجين تغذيه التطورات الحاصلة في المجال التقني، ولا سيما نمو الجريمة السيبرية كخدمة والتأثير الناشىء للذكاء الاصطناعي.
- على الرغم من الإنجازات التي تحققت في مجال إنفاذ القانون، يطرح استمرار الجهات الفاعلة المسؤولة عن الاحتيال بالبريد الإلكتروني المهني في القارة الأفريقية، وانطلاقا منها، صعوبات جمة في مجال التحقيقات.

الاحتيال بالبريد الإلكتروني المهني: تهديد متزايد في أفريقيا

من بين المجموعة الواسعة لعمليات الاحتيال الإلكتروني، حددت البلدان الأفريقية الأعضاء في الإنتربول الاحتيال بالبريد الإلكتروني المهني كأحد أبرز التهديدات في أفريقيا. وينطوي هذا النوع من الجريمة السيبرية على استخدام التصيد الاحتيالي عن طريق البريد الإلكتروني لمهاجمة المؤسسات والأفراد. ويتمثل ذلك عادةً في قيام مرتكبي الجرائم السيبرية باختراق حسابات البريد الإلكتروني المشروعة للمؤسسات والأفراد باستخدام تقنيات الهندسة الاجتماعية و/أو الاختراق المعلوماتي، ومحاولة خداع المؤسسات والأفراد لتحويل أموال غير مرخص بها أو التهديد بنشر المعلومات السرية.

وتتنامى أنشطة مرتكبي الجرائم السيبرية في مجال الاحتيال بالبريد الإلكتروني المهني في جميع أنحاء أفريقيا، وذلك من حيث حجم الهجمات وتأثيرها. وتعكس هذه التطورات الاتجاهات العالمية: ففي الفترة بين نيسان/أبريل 2022 ونيسان/أبريل 2023، كشفت شركة مايكروسوفت 35 مليون محاولة احتيال بالبريد الإلكتروني المهني، وحققت فيها، وهو ما يعادل حوالي 156,000 محاولة هجوم يومية[31]. وفي غضون ذلك، تشير التقارير إلى أن الأثر المالي على الصعيد العالمي لهذا نوع من الاختراقات قد تزايد منذ عام 2013 ليتجاوز 50 مليار دولار أمريكي في عام 2023[32]. ولتوضيح صورة الأضرار الجسيمة التي يمكن أن تخلفها عمليات الاحتيال بالبريد الإلكتروني المهني على الضحايا، تشير تقديرات شركة IBM إلى أن هجوما من هذا النوع يعود على الضحية بكلفة متوسطة تتجاوز 5 ملايين دولار أمريكي . وبالإضافة إلى الخسائر المالية المباشرة، قد تسفر هذه العمليات عن أضرار على المدى البعيد، ولا سيما فقدان البيانات السرية في الحالات التي يتم فيها الإفصاح عن مراسلات حساسة أو متعلقة بالملكية الفكرية. كما يمكن أن تستتبع آثارا نفسية على الضحايا

وفي عام 2023، شكّلت المؤسسات الهدف الأكثر شيوعا لعمليات الاحتيال بالبريد الإلكتروني المهني في البلدان الأفريقية الأعضاء في الإنتربول. ويبدو أن المؤسسات التي تقيم علاقات عمل مع الخارج وتقوم بإبرام صفقات مالية بصورة متكررة تكون فيها الإجراءات الأمنية أقل صرامة، معرضةٌ للتهديد أكثر من غيرها. ولكن المؤسسات المستهدفة قد تتراوح من الشركات الصغيرة والمتوسطة الحجم إلى الشركات الكبرى. وشكّل القطاع المالي القطاع الأكثر معاناة في البلدان الأفريقية الأعضاء، ولكن ما من قطاع أو مؤسسة بمنأى عن عمليات الاختراق هذه. وبالإضافة إلى المصارف والشركات المالية، سُجلت هجمات متكررة ضد شركات تعمل في مجال الاستيراد والتصدير، والنفط والغاز، والمنتجات الصيدلانية، والنقل، والتجارة الإلكترونية. وكذلك، تعرضت كلّ من المؤسسات الحكومية، ولا سيما المؤسسات شبه الحكومية، والقطاع التطوعي، والأفراد، إلى عدد متزايد من الهجمات في جميع أنحاء القارة الأفريقية

31 شركة مايكروسوفت (2023): https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe

32 شركة IBM (2021): https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

الأساليب الإجرامية الشائعة للاحتيال بالبريد الإلكتروني المهني في البلدان الأفريقية

في عام 2023، وفيما يتعلق بالأساليب الإجرامية، حُددت عمليات التصيد الاحتيالي عن طريق الرسائل الإلكترونية كأحد الأساليب الأكثر استخداما للاحتيال بالبريد الإلكتروني المهني، في ما يناهز 80 في المائة من البلدان الأفريقية الأعضاء. وبالمقارنة مع أشكال التصيد الاحتيالي الأخرى، تميل الرسائل الإلكترونية المستخدمة في حالات الاحتيال بالبريد الإلكتروني المهني إلى أن تكون أصعب اكتشافا لأنها لا تتضمن روابط إلكترونية خبيثة ولا تُرسَل بأعداد كبيرة، وبالتالي فهي أقل عرضة للإبلاغ عنها كرسالة إلكترونية غير مرغوب فيها. وأشارت البلدان الأعضاء إلى أنه، بالإضافة إلى التصيد الاحتيالي عبر الرسائل الإلكترونية، يقوم الجناة باستغلال وسائل الإعلام المتفرقة في إطار عملية الاحتيال بالبريد الإلكتروني المهني، ولا سيما الرسائل النصية، والمكالمات الهاتفية، والاجتماعات الافتراضية. فعلى سبيل المثال، انضمت بعض الجهات الفاعلة المسؤولة عن التهديد إلى اجتماعات افتراضية بصفة مستخدم، وذلك لسرقة المعلومات السرية للمؤسسة. ويُساء استخدام وسائل التواصل الاجتماعي وخدمات المراسلة الآنية بشكل متزايد للبحث عن الضحايا و/أو الاتصال بهم[33].

ويمكن تصنيف معظم الحالات التي أبلغت عنها البلدان الأعضاء في الإنتربول في خمس فئات أو مخططات:

1. سرقة البيانات: تخترق الجهات الفاعلة المسؤولة عن التهديد البريد الإلكتروني وبيانات التعريف الخاصة بالموظفين الذين يضطلعون بأدوار محددة، مثل موظفي الموارد البشرية والمحاسبة، للحصول على بيانات شخصية أو بيانات الضرائب التي يعلن عنها سائر الموظفين أو المدراء التنفيذيون. ثم تُستخدم البيانات المجمّعة لشن المزيد من الهجمات في مجال الاحتيال بالبريد الإلكتروني المهني. وأفيدَ بأن هذا السيناريو الأخير آخذ في الارتفاع، إذ يستخدم الجناة البيانات المسربة لابتزاز ضحاياهم مرتين، وحتى ثلاث مرات.
2. اختراق الحساب/انتهاك النظام: من المخططات التي غالبا ما تفيد بها البلدان الأعضاء في مجال الاحتيال بالبريد الإلكتروني المهني، هو قيام الجهات الفاعلة المسؤولة عن التهديد بقرصنة البريد الإلكتروني لأحد الموظفين أو المدراء التنفيذيين، ثم استخدام الحساب المخترَق لإرسال طلبات إلى عدة بائعين من أجل دفع الفواتير. فعلى سبيل المثال، أبلغت عدة بلدان أفريقية عن هجمات تسمى "هجوم الرجل في الوسط" التي يعترض فيها الجناة بطريقة سرية الرسائل المتبادلة بين طرفين ويعيدون نقلها.
3. انتحال صفة رئيس مجلس الإدارة: تُعرف هذه الجريمة أيضا باسم عملية احتيال أو انتحال صفة المدير التنفيذي للمؤسسة، وتتمثل في قيام الجناة بانتحال شخصية مديرين تنفيذيين رفيعي المستوى من أجل تحويل أموال إلى حساب يتحكمون به. وبتطلب هذا النوع من الاحتيال في كثير من الأحيان أن يتحلى الجناة بمستوى معيّن من البحث والاستطلاع إزاء المؤسسة المستهدَفة.
4. انتحال شخصية مسؤول حكومي أو جهاز لإنفاذ القانون أو محام: في هذا النوع من الجرائم، يتصل الجناة بضحاياهم مدّعين أنهم شخصية ذات نفوذ، مثل مسؤول حكومي أو محام، تعامل مسائل سرية وعاجلة. وفي عام 2023، أبلغ العديد من البلدان أيضا عن حالات انتحال شخصية مسؤولين في أجهزة إنفاذ القانون أو في منظمات دولية، بما في ذلك الإنتربول. ثم يستعين الجناة بأساليب متفرقة للضغط على ضحيتهم من أجل أن تقوم بتحويل الأموال بسرعة أو سرّا.
5. مخطط الفاتورة المزورة: يسعى الجناة إلى استغلال العلاقة القائمة بين الضحية وموردها. ويدّعون أنهم أحد هؤلاء الموردين، ويرسلون إليها فاتورة مزيفة ويطلبون من الضحية تحويل الأموال إلى حساب مزيف.

عملية Harrier: توقيف أعضاء في مجموعة للجريمة المنظمة متورطين في عمليات احتيال بالبريد الإلكتروني المهني

لمواجهة المخاطر الجسيمة والمستدامة التي تطرحها الجريمة السيبرية، ولا سيما التداعيات المالية والعاطفية والنفسية المذكورة في التقييم الحالي للتهديدات، أقيمت شراكة استراتيجية بين الإنتربول ومجموعة أطلس التابعة للمنتدى الاقتصادي العالمي. وأرسي هذا التعاون لتحقيق هدفين يتمثلان في تعزيز فهم المشهد العالمي للتهديدات السيبرية، وتسهيل تبادل البيانات الاستخباراتية للتخفيف من التأثير العالمي للجريمة السيبرية.

وتمكّن الإنتربول، بفضل تعاونه مع المشاركين في مبادرة مجموعة أطلس، تحديد هوية أحد مرتكبي عملية متطورة في مجال الاحتيال بالبريد الإلكتروني المهني، تُقدَّر قيمتها بملايين الدولارات واستُخدم فيها الأسلوب الإجرامي المتمثل في تزوير الفواتير. وبفضل تبادل البيانات الاستخباراتية على نطاق واسع، تم ربط الشخص المعني بشبكة إجرامية معقدة مرتبطة بمجموعة Black Axe للجريمة المنظمة، المتمركزة في غرب أفريقيا. وأحيلت هذه المعلومات إلى البلدان الأفريقية المعنية، مما أدى إلى توقيف الجاني.

ولئن كانت أساليب الهجوم الأولية والمخططات العامة لعملية الاحتيال بالبريد الإلكتروني المهني محكمةَ التنظيم، إلا أن أساليب الهندسة الاجتماعية المتغيرة، والبرامج المعلوماتية الإجرامية التي ما فتئت تُستخدَم كخدمة، والذكاء الاصطناعي ذا التأثير الناشىء، كلها عوامل تؤدي إلى تفاقم هذا النوع من الجرائم.

33 مركز أفريقيا (2023): https://africacenter.org/spotlight/africa-evolving-cyber-threats/

أساليب الهندسة الاجتماعية المتغيرة

على غرار الكثير من عمليات الاحتيال الإلكتروني، تعتمد الهجمات بالبريد الإلكتروني المهني، إلى حد بعيد، على استغلال مواطن الضعف لدى الإنسان. وبناء عليه، فإن إبلاغ العديد من البلدان الأفريقية الأعضاء عن تزايد استخدام أساليب الهندسة الاجتماعية المتطورة أمرٌ يبعث على القلق. فعلى سبيل المثال، تُمضي الجهات الفاعلة المسؤولة عن التهديد بالبريد الإلكتروني وقتا طويلا في إجراء البحوث عن الضحايا المحتملين ومراقبتهم، لتحسين طُرق الخداع الأولية أو وسائل الهجوم التي تستخدمها. وتقوم باستغلال المعلومات المنشورة على الملأ أو التي تم الحصول عليها أثناء تسريب سابق للبيانات، لصياغة رسائل تنطوي على طابع شخصي وصادق قدر الإمكان. وفي بعض الحالات، يذهب الجناة إلى حد نسخ أسلوب الكتابة الخاص بالضحية أو يشيرون في الرسالة إلى فعالية مقبلة تكون الضحية مدعوة إليها. ومما يجسد تزايد مستوى التعقيد في الأساليب المستخدمة أن عمليات التصيد الاحتيالي بالبريد الإلكتروني المهني تحقق أهدافها بمعدل يتراوح بين مرتفع إلى مرتفع جدا في أكثر من نصف البلدان الأفريقية الأعضاء في الإنتربول.

ويبدو أيضا أن العديد من هذه الجهات الفاعلة تكرّس مزيدا من الوقت في التحرك بصورة أفقية في النظام الخاص بالضحية، وذلك بعد التمكن من اختراقه بشكل أولي. ويمكن لهذه الجهات استخدام طُرق متعددة لتحقيق الاستمرارية، كإضافة تطبيق مصادقة ثنائية إلى الحساب المخترَق لتجاوز تطبيق المصادقة المتعددة العوامل[34].

ثم يبحث الجناة في مراسلات البريد الإلكتروني الخاص بالضحية أو في تطبيقات تبادل الملفات التي تجرى عن طريق الويب. وتُستخدم المعلومات التي يتم الحصول عليها لإعداد مخططات أكثر إقناعا. فقد نجح بعض الجناة، على سبيل المثال، من خلال تحليل تسلسل رسالة إلكترونية معينة، في استخدام أسماء نطاقات مزورة لإنشاء عدة عناوين مزيفة للبريد الإلكتروني. وتُستخدم هذه العناوين لانتحال صفة عدة شخصيات وتقمّص هوية شركة، مما يوهم الضحية بأنها تتواصل مع مختلف الجهات المتلقية للمراسلة الأصلية.

وفي نفس السياق، لاحظ الإنتربول اتجاها متصاعدا في استخدام المعلومات المسربة في عمليات الاحتيال بالبريد الإلكتروني المهني. وبعد التمكن من اختراق النظام بشكل أولي، يقوم الجناة بتسريب البيانات ليس فقط من أجل إعداد هجمات أكثر فعالية، بل أيضا لابتزاز الضحية بشكل أكبر. ويهدد الجناة بنشر المعلومات الحساسة (ابتزاز مزدوج) أو البيانات المرتبطة بأطراف ثالثة (ابتزاز ثلاثي). والاستخدام المتزايد لاستراتيجيات تسريب البيانات إنما يذكّر مرة أخرى بالتطور المتزايد لمشهد الجرائم المرتكبة عن طريق الاحتيال بالبريد الإلكتروني المهني.

علامات التنبيه الأكثر شيوعا:

01 طلبات دفع مسبق لخدمات غير مطلوبة مسبقًا

02 التواصل عبر البريد الإلكتروني فقط ورفض التواصل بالهاتف أو منصات الصوت أو الفيديو عبر الإنترنت

03 تغييرات آخر لحظة في منصات التواصل القائمة أو في عناوين حسابات البريد الإلكتروني

04 تغييرات آخر لحظة في منصات التواصل القائمة أو في عناوين حسابات البريد الإلكتروني

05 تغييرات آخر لحظة في تعليمات التحويل المصرفي أو معلومات حساب المستلم

06 حالة عاجلة غير موضحة

34 انظر على سبيل المثال الموقع الإلكتروني: https://www.kroll.com/en/insights/publications/cyber/mfa-bypass-leads-to-account-compromise

نمو الجريمة السيبرية كخدمة

يأتي النمو السريع للجريمة السيبرية كخدمة كمؤشر آخر على زيادة تطور النهج المترابط لعمليات الاحتيال بالبريد الإلكتروني المهني، وتنظيمه، وتخصصه. وتجسيدا لهذا النمو، كشفت وحدة مكافحة الجرائم الرقمية في شركة مايكروسوفت أن الجرائم السيربية كخدمة التي تستهدف حسابات البريد الإلكتروني للمؤسسات قد ارتفعت بنسبة 38 في المائة بين عامي 2019 و2022[35]. وتتوفر حاليا مجموعة واسعة من أدوات التصيد الاحتيالي التي تقدّم نماذج وسيناريوهات جاهزة للاستعمال تتيح للجهات الفاعلة المسؤولة عن التهديد بالبريد الإلكتروني المهني تكثيف أنشطتها بسرعة وسهولة. وعلى سبيل المثال، وفي عام 2023، أبلغت مجموعة Group-IB، وهي إحدى الجهات الشريكة للإنتربول في مشروع Gateway، عن عمليات قامت بها مجموعة W3LL، وهي جهة فاعلة إجرامية قامت بتزويد أكثر من 500 من الجهات الفاعلة المسؤولة عن التهديد بالبريد الإلكتروني المهني بمجموعات للتصيد الاحتيالي متكيفة مع احتياجاتها[36]. وقدّمت مجموعة W3LL، من خلال برمجية الجريمة كخدمة الذي حقق رقم مبيعات قدره 500,000 دولار أمريكي، أدوات للمستخدمين تلبي احتياجاتهم إلى حد بعيد لتنفيذ هجمات عن طريق الاحتيال بالبريد الإلكتروني المهني، مما أتاح لهم، في جملة أمور، تجاوز تطبيق المصادقة المتعددة العوامل. وفي الفترة من تشرين الأول/أكتوبر إلى تموز/يوليو 2023، يُقدَّر بأن مجموعة أدوات W3LL للتصيد الاحتيالي قد استُخدمت لاستهداف أكثر من 56,000 حساب مايكروسوفت 365 خاص بالمؤسسات.

وعلاوة على ذلك، حدد الباحثون في مجال الأمن السيبري عددا متزايدا من المنصات غير المشروعة التي تقدم خدمات شاملة، بما في ذلك النماذج، وخدمة الإيواء، وغيرها من الخدمات المؤتمتة، من أجل تنفيذ عدد كبير من عمليات الاحتيال بالبريد الإلكتروني المهني. وتمثل BulletProftLink مثالا على هذا النوع من المنصات التي تسمح للجناة ليس فقط بالحصول على بيانات التعريف وعنوان بروتوكول الإنترنت الخاص بالضحية فحسب، بل أيضا استغلال عناوين بروتوكول الإنترنت المحلية لجعل هجماتهم تبدو وكأنها انبثقت محليا. ويتمكن الجناة، بفضل ذلك، من تجاوز رسائل التنبيه التي تعرض عبارة "ممنوع الدخول"، وهي طريقة تُستخدم كثيرا لكشف الأنشطة المشبوه فيها واعتراضها[37]

التأثير الناشىء للذكاء الاصطناعي

في ظل النمو السريع للذكاء الاصطناعي وانتشار وسائل الإعلام الاصطناعية، أصبحت أساليب الهندسة الاجتماعية التي تتجه نحو المزيد من التطور، والجريمة السيبرية المقدمة كخدمة، أكثر إثارة للقلق. وشهد عام 2023 تطورات جذرية في مجال تقنية الذكاء الاصطناعي بفضل النماذج اللغوية الواسعة النطاق من قبيل ChatGPT، التي استقطبت اهتمام العالم بأسره. ومع الأسف، وعلى الرغم من الحالات الكثيرة التي استُخدم فيها الذكاء الاصطناعي بطريقة إيجابية، ثمة إمكانية لإساءة استخدامه من قبل الجناة، ولا سيما مرتكبي عمليات الاحتيال بالبريد الإلكتروني المهني. واعترافا منه بهذا التهديد الناشىء، أصدر الإنتربول نشرة بنفسجية لتحذير البلدان الأعضاء من مخاطر الذكاء الاصطناعي وتكنولوجيا التزييف العميق التي يستخدمها الجناة من أجل إضفاء مصداقية على عمليات الاحتيال، وتمكينهم على سبيل المثال من إخفاء هوياتهم والادعاء بأنهم أفراد أسرة أو أصدقاء أو في علاقة غرامية[38].

وبشكل مبدئي، يمكن للذكاء الاصطناعي التوليدي أن يسّهل على الجهات الفاعلة المسؤولة عن التهديد استحداث رسائل إلكترونية احتيالية أو رسائل مزورة لطلب مصادقة، وربما على نطاق واسع، ويتيح لها في الوقت نفسه تجنب معايير الكشف الأولية التي تشمل على سبيل المثال الأخطاء الإملائية والنحوية. وعندما تكون النماذج اللغوية الكبرى مزودة بالبيانات الصحيحة، فإن ذلك قد يسمح أيضا للجناة بتقليد الأسلوب والأنماط اللغوية لبعض المؤسسات والأشخاص، ويساعدهم بالتالي على صياغة رسائل إلكترونية أكثر خصوصية وإقناعا لاستقطاب الضحايا وخداعهم[39]. وبالإضافة إلى ذلك، يستغل مرتكبو الجرائم السيبرية بالفعل التقدم السريع لتكنولوجيا التزييف العميق لخداع ضحاياهم، على سبيل المثال، من خلال إعادة تركيب صورة الشخص وصوته أثناء حديثه عبر الهاتف أو الفيديو[40]. وبالنظر إلى سرعة تغيّر تكنولوجيا الذكاء الاصطناعي، وقدرتها الكبيرة على زيادة عدد الهجمات المتصلة بالاحتيال بالبريد الإلكتروني المهني، وتعزيز مستوى تعقيدها، ومصداقيتها، سيتعين على البلدان الأعضاء مراقبة التطورات المستقبلية عن كثب

منع الجهات الفاعلة المسؤولة عن التهديد من ممارسة أنشطتها في أفريقيا

في عام 2023، واصلت البلدان الأفريقية الأعضاء في الإنتربول اتخاذ تدابير ميدانية صارمة لتعطيل أنشطة الجهات الفاعلة المسؤولة عن التهديد الناشطة في المنطقة. وفي عملية Nervone، تمكّن الإنتربول، بالتعاون مع أفريبول وGroup-IB، ومديرية المعلومات والآثار التكنولوجية في كوت ديفوار، من اعتقال عضو بارز في مجموعة يُطلق عليها اسم OPERA1ER. ولهذه المجموعة أيضا أسماء مستعارة مثل NXM وDESKTOP Group وCommon Raven، وهي تنظيم إجرامية منظم للغاية، ويُعتقد أنها استخدمت على نطاق واسع رسائلَ إلكترونية لاختراق البريد الإلكتروني للمؤسسات من أجل سرقة ما يصل إلى 35 مليون دولار أمريكي في 15 بلدا في أفريقيا وآسيا وأمريكا اللاتينية[41]. وفي غضون ذلك، وفي إطار عملية Jackal، قام الإنتربول بتنسيق ودعم قوات الشرطة، ووحدات مكافحة الجريمة المالية، والأجهزة المعنية بمكافحة الجريمة السيبرية في إطار حملة قمع ضد مجموعات الجريمة المنظمة في غرب أفريقيا، بما في ذلك Black Axe، وهي عصابة عنيفة من نوع المافيات تُعرف بارتكاب عمليات احتيال باختراق البريد الإلكتروني للمؤسسات، وغيرها من عمليات الاحتيال الإلكتروني[42]. وتثبت هذه العمليات التزام البلدان الأفريقية الأعضاء بحماية مجتمعاتها المحلية من عواقب عمليات اختراق البريد الإلكتروني للمؤسسات

35 شركة مايكروسوفت (2023): https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe

36 مجموعة Group-IB (2023): https://www.group-ib.com/media-center/press-releases/w3ll-phishing-report/

37 شركة مايكروسوفت (2023): https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe

38 الإنتربول (2023): https://www.interpol.int/ar/1/1/2023/300-500-3

39 وكالة الأمن السيبري في سنغافورة (2023): https://www.csa.gov.sg/Tips-Resource/publications/cybersense/2023/chatgpt---learning-enough-to-be-dangerous

40 الإنتربول (2023): https://www.interpol.int/content/download/20035/file/ChatGPT-Impacts%20on%20Law%20Enorcement-%20August%202023.pdf

41 الإنتربول (2023): https://www.interpol.int/ar/1/1/2023/23

42 الإنتربول (2023): https://www.interpol.int/ar/1/1/2023/2-Jackal

عملية Nervone: اعتقال شخصية بارزة في مجموعة منظمة للجريمة السيبرية

في السنوات الأربع الأخيرة، نظّمت مجموعة إجرامية تُعرف باسم OPERA1ER مخططات واسعة النطاق لعمليات اختراق البريد الإلكتروني للمؤسسات، وحملات تصيّد احتيالي، وهجمات ببرمجيات خبيثة، استهدفت مؤسسات مالية وخدمات مصرفية نقالة في العالم أجمع، مما أتاح لها جني ما يصل إلى 35 مليون دولار أمريكي. وفي بداية شهر حزيران/يونيو 2023، كشف الإنتربول، بالتعاون مع أفريبول وكوت ديفوار والولايات المتحدة وجهات شريكة من القطاع الخاص مثل شركة أورانج وGroup-IB وBooz Allen Hamilton وDarkLabs، هوية أشخاص يُشتبه في كونهم أعضاء بارزين في المجموعة، وقام باعتقالهم. ولم يكن لهذه العملية التي تحمل اسم "Nervone" أن تنجح لولا التبادل الدؤوب للبيانات الاستخباراتية والتعاون الوثيق على مدى عدة سنوات

وبموازاة هذه الإنجازات الميدانية، كثّفت أيضا البلدان الأفريقية الأعضاء جهودها الرامية إلى منع هذه الجرائم والتخفيف من وطأتها. ونظّمت أكثر من 60 في المائة من البلدان الأعضاء التي أجابت على الاستبيان حملات في عام 2023 لتنبيه الأشخاص والمؤسسات إلى مخاطر الهجمات بعمليات الاحتيال بالبريد الإلكتروني المهني. وأُطلقت حملات التوعية هذه من منصات إعلامية متنوعة، ولا سيما الإذاعة والتلفزيون والمواقع الحكومية على الويب وشبكات التواصل الاجتماعي، بهدف تحسين تدابير الوقاية السيبرية ومنع مرتكبي الجرائم السيبرية من مواصلة استغلال العنصر البشري.

وعلى الرغم من هذه التدابير الإيجابية، لا يزال هناك عقبات كبيرة أمام مواصلة التخفيف من وطأة عمليات الاحتيال بالبريد الإلكتروني المهني في أفريقيا. ولا يزال عدد كبير من الجهات الفاعلة في هذا المجال موجودا في أفريقيا، وخصوصا في غرب أفريقيا، ولكنه لا يزال يتزايد أيضا في الأجزاء الجنوبية من القارة، حيث تفيد بعض الدراسات بأن الجزء الأكبر من هذه العمليات يجرى في 11 بلدا فيها[43]. وبعض المجموعات الإجرامية المتورطة تحولت إلى مؤسسات قوامها عدة ملايين من الدولارات[44]. وقد تعوّل على هياكل تنظيمية متطورة تشمل عددا من الأدوار الوظيفية المتخصصة التي تتراوح من مدبّري البنى التحتية إلى مشغّلي البريد الإلكتروني وناقلي الأموال. وبالإضافة إلى ذلك، وللرد جزئيا على إنجازات أجهزة إنفاذ القانون، يتبنى مرتكبو عمليات الاحتيال بالبريد الإلكتروني المهني بشكل متزايد أساليب التعتيم لإخفاء بنيتهم التحتية الإجرامية، وباتوا يوسعون انتشارهم الجغرافي يوما بعد يوم، مما يفاقم الصعوبات التي تعترض أجهزة إنفاذ القانون في مجال التحقيقات.

المناعة السيبرية وقدرات إنفاذ القانون في القارة الأفريقية

لتكوين صورة شاملة عن المشهد الحالي للتهديدات السيبرية، من المهم ألا ندرس فقط التهديدات الأكثر إلحاحا في مجال الجريمة السيبرية، بل أيضا أن نقيّم القدرات المتاحة لردعها. وبناء عليه، يتناول هذا القسم أربع مجالات للمناعة السيبرية في أفريقيا، من خلال استخدام البيانات التي أحالتها البلدان الأعضاء، وهي: الأطر التشريعية، وقدرات إنفاذ القانون، والشراكات، والمشاركة مع الناس

الأطر التشريعية الأفريقية لمكافحة انتشار الجريمة السيبرية

تمثّل الأطر التشريعية الفعالة عنصرا أساسيا في المناعة السيبرية ومعيارا رئيسيا لأنشطة إنفاذ القانون. وفي هذا الصدد، فإن سن القوانين الرامية إلى مكافحة الجريمة السيبرية في جميع أنحاء أفريقيا أمرٌ محفز. وفي عام 2023، وضعت عدة بلدان أفريقية قوانين جديدة حيز التنفيذ، وعدّلت البعض الآخر منها، أو فعّلت التشريعات التي قُدّمت مؤخرا لمكافحة الجريمة السيبرية[45]. ويُذكر في عداد أبرز الأمثلة على ذلك، أنظمة أوغندا بشأن لوائح اعتراض الاتصالات، وقانون الكاميرون لوضع ميثاق حماية الطفل على الإنترنت، وقانون غابون بشأن حماية البيانات الشخصية، وأحكام بوركينا فاسو لمشغلي تكنولوجيا المعلومات والاتصالات في مجال حفظ البيانات، وقانون بوتسوانا بشأن الأصول الافتراضية. وأشارت ستة بلدان أخرى إلى أنها في صدد سن تشريعات جديدة. وتضاف هذه الجهود الحثيثة إلى توسيع نطاق الصكوك الإقليمية والدولية القائمة، بما في ذلك اتفاقية الاتحاد الأفريقي بشأن الأمن السيبري وحماية البيانات الشخصية، المعروفة أيضا باسم اتفاقية مالابو؛ واستراتيجية الاتحاد الأفريقي للتحول الرقمي في أفريقيا (2020-2030)، واتفاقية بودابست بشأن الجريمة السيبرية وبروتوكولاتها الإضافية

ويساند الإنتربول مساندة فعالة جهود البلدان الأعضاء لتحويل تشريعاتها حتى تتمكن من مكافحة الجريمة السيبرية من خلال مبادرات متفرقة. وقد شارك في عام 2023 في تنفيذ مشروع التحرك العالمي الموسّع لمواجهة الجريمة السيبرية (GLACY+) الذي بات يسمى حاليا GLACY-e. وترمي هذه المبادرة، التي هي ثمرة تعاون بين الاتحاد الاوروبي ومجلس أوروبا، إلى تعزيز القدرات السيبرية للبلدان في أفريقيا، وآسيا والمحيط الهادئ، وأمريكا اللاتينية، ومنطقة البحر الكاريبي، ضمن إطار اتفاقية بودابست. ويتمثل أحد طموحات مشروع GLACY+ الأساسية في تطوير التشريعات والسياسات والاستراتيجيات المتسقة في مجال الجريمة السيبرية. ويضطلع الإنتربول بدور حاسم

43 (Agari (2023): ag-acid-geography-of-bec-gd.pdf (fortra.com

44 Agari (2023): https://www.agari.com/resources/videos/scattered-canary-evolution-business-email-compromise-enterprise

45 Lexology (2023): https://www.lexology.com/library/detail.aspx?g=baef72ee-10bd-4eb9-a614-a990c236bb45

في هذا المسعى من خلال تعزيز القدرات والمهارات الميدانية لقوات الشرطة في البلدان المشاركة. وترمي هذه الجهود إلى تحسين كفاءاتها في التحقيق في الجرائم السيبرية والنهوض بالتعاون الشرطي الدولي من خلال سلسلة من الأنشطة.

وفي الوقت نفسه، انخرط الإنتربول طوال عام 2023، وبشكل مسبق، في أبرز الإجراءات الدولية المتخذة في مجال السياسات والتشريعات المتعلقة بالشؤون السيبرية، ولا سيما اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية[46]. وتهدف اللجنة المخصصة إلى إعداد معاهدة دولية جديدة لمكافحة التهديدات السيبرية، من شأنها أن تقدّم، بعد التصديق عليها، أدوات تشريعية معززة إلى البلدان في أفريقيا وخارجها. وسعى الإنتربول، من خلال إسهاماته، إلى ضمان أخذ مصالح واحتياجات بلدانه الأعضاء العديدة في الاعتبار بشكل دقيق في الاتفاقية المقبلة.

وأخيرا، ومنذ استحداث برنامج الإنتربول لمكافحة الجريمة السيبرية، تعمل المنظمة على إعداد صكوك أساسية لمساعدة البلدان الأعضاء على مكافحة هذه الجريمة. ويشمل ذلك القرارات الدولية (التي يتمثل آخرها في قرار عام 2021 المتعلق بمكافحة التهديدات العالمية للجريمة السيبرية من خلال قنوات الإنتربول[47])، واستراتيجية الإنتربول العالمية لمكافحة الجريمة السيبرية للفترة 2022-2025، وفيما يتعلق بأفريقيا على وجه الخصوص، التوصية الإقليمية لعام 2022[48]. وتهيب هذه الأخيرة بالبلدان الأفريقية الأعضاء إلى الاستفادة من موارد الإنتربول إلى أقصى حد ممكن لتعزيز التعاون الميداني، وتبادل البيانات الاستخباراتية، وتحسين القدرات.

تعزيز القدرات السيبرية لأجهزة إنفاذ القانون

تشير البيانات التي تلقاها الإنتربول إلى أن الموارد البشرية المخصصة لمكافحة الجريمة السيبرية لا تزال غير كافية، على الرغم من أن البلدان تتخذ خطوات استباقية لتحسين هذا الوضع. ففي عام 2023، على سبيل المثال، أبلغ ما يقرب من نصف أجهزة إنفاذ القانون في البلدان الأعضاء في الإنتربول عن زيادة في عدد الموظفين المكرسين لمكافحة الجريمة السيبرية. وبالإضافة إلى ذلك، أكدت أربعة بلدان على الأقل أنها أنشأت مؤخرا وحدة لمكافحة الجريمة السيبرية أو أنها في صدد القيام بذلك. وفي غضون ذلك، وعلى مدار عام 2023، أفادت أكثر من نسبة 70 في المائة من أجهزة إنفاذ القانون في البلدان الأفريقية الأعضاء بأنها نفّذت أو شاركت في تنفيذ أنشطة تدريب في المجال السيبري: وبلغ العدد الإجمالي لهذه البلدان 32 بلدا ونُفّذت أكثر من 130 مبادرة في مجال التدريب. ويلقي ذلك الضوء على الجهود المبذولة للاستثمار في الموظفين والمهارات اللازمة لمكافحة الجريمة السيبرية بشكل أفضل، مما يؤكد التزام البلدان الأفريقية الأعضاء بتعزيز المناعة السيبرية في جميع أنحاء القارة.

وعملا بالهدف 3 من استراتيجية الإنتربول العالمية لمكافحة الجريمة السيبرية، تسعى المنظمة إلى المساعدة على تعزيز استراتيجيات البلدان الأعضاء وقدراتها على مكافحة هذه الجريمة. وبناء عليه، يسهم الإنتربول في عدة مبادرات ترمي إلى تعزيز القدرات في القارة الأفريقية، بما في ذلك العملية المشتركة لمكافحة الجريمة السيبرية في أفريقيا (AFJOC) ومشروع GLACY-e، وبرنامج الإنتربول لدعم الاتحاد الأفريقي فيما يتصل بأفريبول (ISPA). وفي عام 2023، أدت هذه الجهود إلى تنظيم ثماني دورات تدريب وحلقات عمل ركزت على أساليب التحقيق في الجريمة السيبرية، وخصوصا فيما يتعلق بالأصول الافتراضية. وبالإضافة إلى ذلك، تم الحصول على 72 من الأدوات المتخصصة والتراخيص اللازمة للقيام بالتحقيقات في الجريمة السيبرية في 22 بلدا عضوا، ورافق ذلك دورةٌ تدريبية مصممة للتدرب على استخدامها. كما يوفر الإنتربول منصتين مخصصتين لضمان سهولة التواصل العالمي بين أجهزة إنفاذ القانون في البلدان الأعضاء، هما منصة تبادل المعارف المتصلة بالجريمة السيبرية، الرامية إلى مشاطرة المعلومات غير الميدانية، ومنصة التعاون لمكافحة الجريمة السيبرية -العمليات، المعنية بتبادل البيانات الاستخباراتية الميدانية على نحو مأمون ومقيَّد. وهاتان المنصتان فعالتان في تنسيق رد دولي على الجريمة السيبرية، وتوفران آلية متطورة للمشاركة الجماعية

46 للمزيد من المعلومات عن اللجنة المخصصة، يرجى الاطلاع على الموقع الإلكتروني: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

47 الإنتربول (2021): https://www.interpol.int/ar/News-and-Events/Events/2021/89th-INTERPOL-General-Assembly

48 الإنتربول (2022): https://www.interpol.int/ar/1/1/2022/28

صعوبات التنسيق في النهج السيبري المترابط

لا بد من إقامة وتعزيز شراكات مفتوحة وشاملة ومتنوعة لتحسين التعاون الفعال في مكافحة الجريمة السيبرية. بيد أن البلدان الأفريقية الأعضاء أبلغت عن صعوبات في تعزيز التعاون بين أجهزة إنفاذ القانون والجهات المعنية المختصة بالنظام السيبري. ويبدو أن العمل مع مزودي الخدمة، وخصوصا عندما يقيمون في الخارج، لا يزال يطرح مشكلة كبيرة فيما يتعلق بالتحقيقات المتصلة بالجريمة السيبرية. وفي الوقت نفسه، أفيدَ بأن التعاون بين القطاعين العام والخاص غالبا ما يستند إلى غرض معيّن ولا يتم من خلال أطر ثابتة وموحدة.

وفي ظل كل هذه الصعوبات التي تعرقل إقامة شراكات ومنصات رسمية بين القطاعين العام والخاص لمساعدة الشركات على مكافحة الجريمة السيبرية، يمكن لمبادرات الإنتربول الاستراتيجية أن تؤدي دورا حاسما في هذا المجال. وتقوم مبادرة الإنتربول الخاصة، التي تحمل اسم Gateway، مقام حجر الزاوية في إجراء دراسات تحليلية معمقة للجريمة السيبرية، بفضل استخدام مجموعة واسعة من مصادر المعلومات اللازمة لتحديد هوية الجهات الفاعلة المسؤولة عن التهديد والضحايا، والإبلاغ عن الهياكل المعرضة للخطر لاتخاذ إجراءات التحرك الضرورية. ومبادرة Gateway، التي تستند إلى القانون الأساسي للإنتربول ومبادئه التوجيهية المتمثلة في تحقيق السيادة، واحترام حقوق الإنسان، والحياد، والتعاون الفعال، تضع إطارا قانونيا لتبادل المعلومات مع كيانات القطاع الخاص من خلال إبرام اتفاقات لتبادل البيانات. وعلاوة على ذلك، يشارك الإنتربول في مبادرات رئيسية لتعزيز التعاون بين مختلف الأطراف المعنية. وتشمل هذه الأطراف مجموعة أطلس التابعة للمنتدى الاقتصادي العالمي[49] التي تجمع بين أجهزة إنفاذ القانون والقطاعين العام والخاص لوضع تصور جديد لنظام الجريمة السيبرية. والتعاون بين هذه المجموعة والإنتربول أدى أيضا إلى تحقيق نتائج ميدانية مذهلة تستند إلى الدراسات التحليلية، بما في ذلك تحديد هوية واعتقال أعضاء في مجموعة تهديد بارزة تُعرف باسم Silver Terrier تنشط بشكل رئيسي انطلاقا من غرب أفريقيا

توعية عامة الناس وتدابير الوقاية السيبرية

استجابة لتزايد استخدام أساليب الهندسة الاجتماعية في ارتكاب الجرائم السيبرية، اتخذت البلدان خطوات مهمة لتوعية الناس بها وبتدابير الوقاية السيبرية. والإبلاغ عن قيام حوالي 80 في المائة من البلدان الأفريقية الأعضاء التي أجابت على الاستبيان بإطلاق حملات توعية للناس ترمي إلى الوقاية من الجريمة السيبرية أمرٌ مشجع. وعلى الرغم من أن هذه الحملات كانت تُطلق عبر الإنترنت في كثير من الأحيان، إلا أنها نُظّمت أحيانا في أماكن مادية، وخصوصا في المؤسسات التربوية، وركزت بالتالي على الشباب وشبكات الدعم المحيطة بهم، ولا سيما أولياء الأمور والأُسر والمربّين. ونُشرت هذه الحملات عبر مختلف المنصات الإلكترونية، بما في ذلك التلفزيون والإذاعة وأخبار الويب ووسائل التواصل الاجتماعي، وفايسبوك الذي حاز على النصيب الأكبر منها. ويشكل التعاون بين أجهزة إنفاذ القانون والكيانات من القطاع الخاص جانبا مهما من جوانب هذه الجهود. وشملت المجالات الرئيسية التي ركزت عليها هذه الحملات تعزيزَ أفضل الممارسات في مجال تدابير الوقاية السيبرية، والتوعية العامّة بعمليات الاحتيال الإلكترونية. وتتماشى هذه الجهود الوطنية مع استراتيجية الاتحاد الأفريقي في مجال التعليم الرقمي[50] التي ترمي في المقام الأول إلى تسريع وتيرة اعتماد التقنيات الرقمية في التدريس والتعلم والبحث والتقييم والإدارة.

وأطلق الإنتربول، في إطار جهود عالمية إضافية، عدة حملات توعية، مثل حملة #YouMayBeNext، و#JustOneClick، و#OnlineCrimeIsRealCrime، من أجل تعزيز انتباه المجتمعات المحلية لمكافحة مرتكبي الجرائم السيبيرية كافة الذين يسعون إلى استغلال مواطن الضعف، أو سرقة البيانات، أو ارتكاب عمليات الاحتيال الإلكتروني، أو إثارة اضطرابات في قلب العالم الرقمي. وشهدت حملة #YouMayBeNext على وجه الخصوص مشاركة عالمية ملحوظة، إذ تلقت دعما من 79 بلدا عضوا، وجهات شريكة من القطاع الخاص، ومنظمات دولية شتى، وكيانات من القطاع الخاص، ومنظمات غير حكومية، الأمر الذي أتاح لها تحقيق انتشار واسع النطاق. ويخطط الإنتربول في عام 2024 لمواصلة هذا الزخم بإطلاق حملة جديدة تركز على التهديد الذي تطرحه البرمجيات الخبيثة

49 للمزيد من العملومات عن مجموعة أطلس التابعة للمندة الاقتصادي العالمي، يرجى الاطلاع على الموقع الإلكتروني: https://initiatives.weforum.org/cybercrime-atlas/home

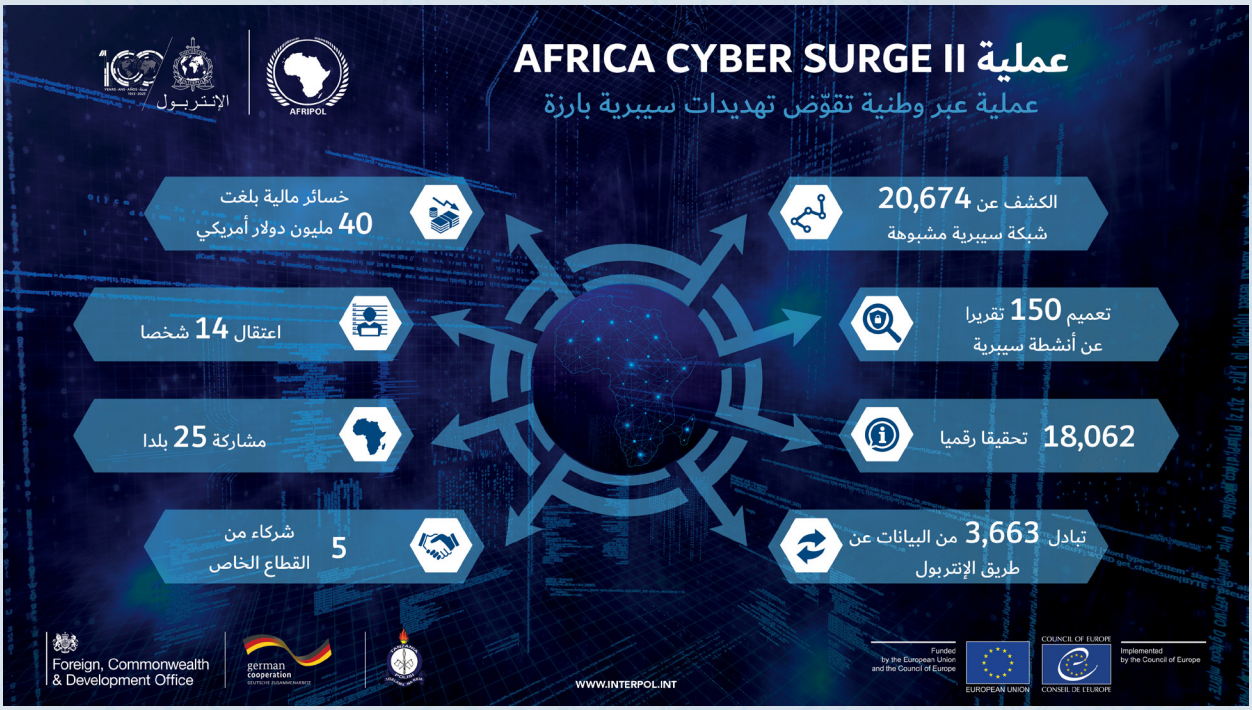
50 استراتيجية الاتحاد الأفريقي في مجال التعليم (2022): https://au.int/en/documents/20221125/digital-education-strategyand-implementation-plan

دعم المناعة السيبرية في أفريقيا: عملية Africa Cyber Surge II للإنتربول

يدعم الإنتربول المناعة السيبرية في أفريقيا من خلال الشراكات، والمنصات، وأنشطة بناء القدرات.

وتشكل عملية Africa Cyber Surge II المثال الأبرز على ذلك:

- قدمّت الجهات الشريكة في مشروع Gateway للإنتربول ومجموعة أطلس التابعة للمنتدى الاقتصادي العالمي معلومات أساسية أسهمت بشكل رئيسي في نجاح هذه العملية.
- استخدمت البلدان المشاركة منصة التعاون لمكافحة الجريمة السيبرية – العمليات لتبادل المعلومات والتنسيق الميداني
- نُظّمت سلسلة من الدورات التدريبية التمهيدية لتعزيز مهارات المحققين في مختلف ميادين التحقيق في الجريمة السيبرية



الخطوات المقبلة

استنادا إلى نتائج التقييم، بما في ذلك تحليل التهديدات السيبرية الأسرع نموا في أفريقيا، والجهود المبذولة لمكافحتها، يقدّم هذا القسم توصيات ترمي إلى التخفيف من وطأة الجريمة السيبرية والأضرار التي تستتبعها على أفريقيا والعالم أجمع.

1. استحداث أدوات راسخة ومتسقة في مجال الأمن السيبري أو تعزيز الموجود منها

يوصي الإنتربول بأن تواصل البلدان الأفريقية الأعضاء عملية استحداث و/أو تعزيز صكوك وطنية راسخة ومتسقة في مجال الأمن السيبري من أجل منع الجريمة السيبرية والتصدي لها. وتشمل هذه الأدوات استراتيجيات وسياسات وأطرا قانونية تهدف إلى تمكين البلدان من مكافحة التهديدات السيبرية بشكل فعال والتخفيف من حدة المخاطر المرتبطة بها. وينطوي ذلك، على سبيل المثال لا الحصر، على إزالة العوائق القانونية أمام المحققين.

2. الاستثمار في القدرات السيبرية لأجهزة إنفاذ القانون: الناس، والعمليات، والتكنولوجيا

يقوم الإنتربول، إدراكا منه لأهمية تعزيز موارد الأمن السيبري في القارة، بتشجيع الجهات المعنية الداخلية والخارجية على زيادة الاستثمار في أجهزة إنفاذ القانون في أفريقيا ودعمها على المدى البعيد. وتستدعي الجريمة السيبرية التي ما لبثت تزداد تعقيدا إنشاء وحدات أكثر تخصصا، وتعيين موظفين ماهرين، وحيازة أدوات ومنصات. لذا، تُشجَّع البلدان على المشاركة بهمّة في أنشطة بناء القدرات الحالية التي تقدمها الكيانات الإقليمية والدولية، مثل تلك التي ينظّمها مكتب الإنتربول لعمليات مكافحة الجريمة السيبرية في أفريقيا

3. إقامة أوجه تآزر بين النهج المترابطة للأمن السيبري

بالنظر إلى الطابع عبر الوطني للجريمة السيبرية، يوصي الإنتربول بشدة بأن تدمج البلدان الأفريقية الأعضاء الجهود التي تبذلها الجهات المعنية بمكافحة الجريمة السيبرية. ويؤدي التعاون مع هذه الجهات الشريكة المعنية مثل القطاع الخاص وأجهزة الأمن السيبري، دورا حاسما في تحسين الاستجابة للحوادث، والوصول إلى البيانات، وتبادل البيانات الاستخباراتية المتعلقة بالتهديدات، وتفكيك البنى التحتية الخبيثة، والتوعية بالأمن السيبري. بالإضافة إلى ذلك، تُشجَّع البلدان على تشكيل أفرقة وطنية للتصدي للطوارئ الحاسوبية وأفرقة للتحرك إزاء الحوادث المتصلة بأمن الحاسوب، والاستعانة بها. وللمساعدة على توطيد أواصر التعاون بين أجهزة إنفاذ القانون وهذه الأفرقة القائمة، استحدث الإنتربول مجموعة اهتمامات خاصة، بالتعاون مع منتدى أفرقة التحرك إزاء الحوادث وأفرقة التحرك إزاء الحوادث المتصلة بأمن الحاسوب

4. تعزيز التعليم الرقمي وأنشطة التوعية

لمواجهة أساليب الهندسة الاجتماعية التي ما لبثت تزداد تعقيدا، يجب تركيز الانتباه مجددا على العنصر البشري، وبالتالي، على تدابير الوقاية. ويشجع الإنتربول البلدان الأفريقية الأعضاء على مواصلة التركيز على تحسين تدابير الوقاية السيبرية، بمؤازرة القطاعين الخاص والعام. وتشمل هذه الاستراتيجية توسيع نطاق توعية عامة الناس من خلال مبادرات حكومية، وحث الأفراد والمؤسسات على تعزيز أمن بريدهم الإلكتروني، واستخدام تطبيق المصادقة المتعددة العناصر، وتنظيم تدريب شامل للموظفين، واعتماد تقنيات الدفع المأمون.

وكذلك، يجب تشجيع المواطنين على إبلاغ سلطات إنفاذ القانون الوطنية كلما وقعوا ضحية لجريمة سيبرية. ولتحقيق هذه الغاية، يوصى بأن تقوم البلدان الأعضاء بتبسيط إجراءات الإبلاغ والتسجيل قدر الإمكان، على سبيل المثال، من خلال استخدام صفحات الويب والمنصات الإلكترونية. ولن تضمن هذه التدابير الاستباقية بيئة رقمية أكثر أمانا فحسب، بل ستسمح أيضا بفهم المشهد السيبري في أفريقيا بشكل أفضل.

5. الاستثمار في القدرات السيبرية لأجهزة إنفاذ القانون: الناس، والعمليات، والتكنولوجيا

التعاون الإقليمي والدولي الفعال أمر حاسم لمواجهة التوسع الجغرافي لمجموعات الجريمة المنظمة وضحاياها. ويهيب الإنتربول بالبلدان الأعضاء إلى المضي في توسيع نطاق تعاونها وتوطيده لتشكيل جبهة موحدة في وجه التهديد العالمي الذي تمثله الجريمة السيبرية. ويشمل ذلك تعزيز تبادل المعلومات، وتنفيذ إجراءات منسقة تستند إلى البيانات الاستخباراتية من خلال مكتب الإنتربول لعمليات مكافحة الجريمة السيبرية في أفريقيا.

وسيواصل الإنتربول دعم البلدان الأفريقية الأعضاء على تعزيز الحد من تأثير الجريمة السيبرية على العالم، وأضرارها، وحماية المجتمعات المحلية من أجل عالم أكثر أمانا.

إطار العمليات المشتركة في أفريقيا

استحدث الإنتربول مكتب أفريقيا للعمليات المشتركة، وهو إطار للعمليات المشتركة للترويج لمقاربة متسقة ومنهجية لتحسين العمليات المنسقة الاستباقية لمكافحة الجريمة السيبرية في القارة. ويتضمن هذا الإطار أربع مراحل.

المرحلة الأولى – الجمع والتحليل

تركز المرحلة الأولى على تحليل معمَّق للمعلومات المتعلقة بالتهديدات السيبرية السائدة، والبنى التحتية الخبيثة، والجهات الفاعلة المسؤولة عن التهديد والعاملة في المجتمع المحلي وضده في المنطقة الأفريقية. وباستخدام البيانات الاستخبارية المستقاة من أجهزة إنفاذ القانون، والبحوث التي تجريها وحدة الاستخبارات لمكافحة الجريمة السيبرية التابعة للإنتربول، واتفاقات تبادل البيانات بشكل مكثف مع شركاء الإنتربول في إطار مشروع Gateway، سينشر مكتب أفريقيا للعمليات المشتركة لمكافحة الجريمة السيبرية التقرير عن تقييم التهديدات السيبرية الأفريقية بغية مساعدة أجهزة إنفاذ القانون في أفريقيا على تكوين فهم أفضل لمشهد التهديدات السيبرية في القارة

المرحلة الثانية – الأولويات والاستراتيجية

سيكون التقرير عن تقييم التهديدات السيبرية الأفريقية الذي نُشر خلال المرحلة الأولى من الدورة بمثابة وثيقة مرجعية لمساعدة البلدان الأفريقية الأعضاء في وضع أو تحديث استراتيجياتها للتحقيق ومقاربتها للتحقيق، وفي توجيه الأولويات الإقليمية للجهود العملياتية المضطلع بها بالاشتراك مع الإنتربول للعام المقبل. واعترافا بتنوع المنطقة الأفريقية، والصعوبات الفريدة التي يواجهها كل بلد، سيقوم مكتب أفريقيا للعمليات المشتركة لمكافحة الجريمة السيبرية بإشراك رئيس مكافحة الجريمة السيبرية في كل بلد خلال هذه المرحلة (بعد الحصول على إذن من المكتب المركزي الوطني المختص) من أجل استكشاف فرص التعاون داخل الأقاليم وبينها. وبحلول نهاية هذه المرحلة، ستكون جاهزةً للنشر خريطةُ طريق إقليمية موضوعة استنادا إلى استراتيجية مشتركة متفق عليها ومشفوعة بنتائج ميدانية واضحة لهذا العام

المرحلة الثالثة – العمليات

سيضع مكتب أفريقيا للعمليات المشتركة لمكافحة الجريمة السيبرية خططا تكتيكية موحدة لتفعيل الاستراتيجية المتفق عليها في المرحلة الثانية. وتوفر الخطط التكتيكية الموحدة مجموعة واضحة من الأهداف والأدوار والمسؤوليات، ومفهوما عملياتيا لمواجهة تهديدات سيبرية محددة. وتتضمن كل خطة تكتيكية موحدة عادةً خططا مفصلة بشأن ما يلي: (1) التخطيط والتحليل؛ (2) التنظيم؛ (3) الأساليب؛ و (4) التقييم. وسيجرى إطلاع البلدان المشاركة على الخطط التكتيكية الموحدة تمهيدا لإقرارها.

وستلتزم وحداتُ مكافحة الجريمة السيبرية المشارِكة التي تعيّنها المكاتبُ المركزية الوطنية بعد ذلك باتخاذ الإجراءات المبينة في الخطط التكتيكية الموحدة وستقدم الدعم الكامل لتحقيق الأهداف والغايات العملياتية المتفق عليها. وبعد إقرار تلك العمليات، سيتولى مكتب أفريقيا للعمليات المشتركة لمكافحة الجريمة السيبرية تنسيق العمليات وسينفذها محققون معيَّنون وفقا للجدول الزمني المبين في تلك الخطط. ويتلقى الإنتربول البيانات المتعلقة بالعمليات من خلال منظومة I-24/7 للاتصالات المأمونة، أو عبر منصة التعاون التابعة له لمكافحة الجريمة السيبرية - العمليات، تمهيدا لتحليلها

وستقوم جهات الاتصال المعيَّنة من كل بلد عضو، فور تلقيها معلومات عملياتية، بالاتصال بمكتب أفريقيا للعمليات المشتركة لمكافحة الجريمة السيبرية بغية تبادل المعلومات وفقا للأهداف والإطار الزمني المحددين للعملية. وسيحتفظ البلد العضو المبادِر بالقيادة الميدانية طوال العملية.

وسيكون تيسير حفظ سجلات الإنترنت (المعلومات الأساسية عن المشتركين، وبيانات الإرسال، والمحتوى، وما إلى ذلك) والكشف عنها، على أساس طوعي وسيجرى تشجيعه في جميع العمليات المتعلقة بمكافحة الجريمة السيبرية، نظرا للطابع المتقلّب للأدلة الإلكترونية. والبلدان الأعضاء مدعوة بشدة، في حدود قوانين وسياسات كل منها، إلى تبادل مستجدات التحقيق والبيانات الاستخبارية المحددة التي قد تساعد بلدانا أعضاء أخرى في تحقيقات خاصة بها. وتيسّر جهات الاتصال، قدر الإمكان، تبادل المعلومات مع الأجهزة الوطنية الأخرى مثل أفرقة التصدي للطوارئ الحاسوبية والمصارف المركزية تبعا لاحتياجات كل عملية.

المرحلة الرابعة – التقييم

خلال المرحلة الرابعة، يجرى استعراضٌ لاحق للعملية بغية تحديد الدروس المستفادة من العمليات. وسيوصي مكتب أفريقيا للعمليات المشتركة لمكافحة الجريمة السيبرية بتعديلات على العمليات المشتركة المقبلة استنادا إلى الاستعراضات والمعلومات الجديدة المستقاة من العمليات. كما سيجرى تقييم المعلومات الاستخبارية التي جُمعت خلال المرحلة الثالثة بغية تعزيز الفهم الإقليمي للتهديدات السيبرية السائدة والاسترشاد بها لدى وضع التقرير المقبل عن تقييم التهديدات السيبرية الأفريقية.

ملاحظات بشأن المنهجية المتّبعة في تقرير الإنتربول عن تقييم التهديدات السيبرية في أفريقيا لعام 2024

يستند تقرير الإنتربول عن تقييم التهديدات السيبرية في أفريقيا لعام 2024 إلى الإصدارات السابقة لتقديم تحليل معمّق لمشهد التهديدات السيبرية على نحو ما اختبرته البلدان الأفريقية الأعضاء. ويقدّم هذا الإصدار تحليلا معمقا يركز على التهديدات الرئيسية من قبيل البرمجيات الخبيثة، والاحتيال بالبريد الإلكتروني المهني، وغيرهما من أشكال عمليات الاحتيال الإلكتروني. ولا يكتفي التقرير بتحديد هذه المشكلات الملحة بل ينظر أيضا في المبادرات الوطنية الجارية التي تهدف إلى تعزيز المناعة السيبرية في جميع أنحاء القارة. ويختتم التقرير بتوصيات يعوَّل عليها لاتخاذ إجراءات ترمي إلى توجيه الجهود التي ستُبذل في المستقبل في مجال الأمن السيبري في القارة

ويرتكز التقرير في المقام الأول على البيانات الاستخباراتية والمعلومات الميدانية المستقاة من مختلف الأنشطة التي يضطلع بها الإنتربول في أفريقيا. وترد معلومات إضافية من دراسة استقصائية أجراها الإنتربول وتتضمن 40 من الأسئلة الكمية والنوعية فيما يتعلق بمنع الأنشطة السيبرية، وكشفها، والتحقيق فيها، وتعطيلها. وفي المجموع، قدم 46 بلدا عضوا معلومات، وهو ما يمثل معدل إجابات يزيد على 80 في المائة

- الجزائر
- أنغولا
- بنن
- بوتسوانا
- بوركينا فاسو
- بوروندي
- الكاميرون
- كابو فيردي
- جزر القمر
- الكونغو
- كوت ديفوار
- جمهورية الكونغو الديمقراطية
- جيبوتي
- غينيا الاستوائية
- إريتريا
- إسواتيني
- إثيوبيا
- غابون
- غامبيا
- غانا
- غينيا
- غينيا-بيساو
- كينيا
- ليسوتو
- ليبريا
- مدغشقر
- ملاوي
- مالي
- موريتانيا
- موريشيوس
- موزامبيق
- ناميبيا
- النيجر
- رواندا
- سان تومي وبرينسيبي
- السنغال
- سيشيل
- سيراليون
- الصومال
- جنوب أفريقيا
- جنوب السودان
- تنزانيا
- توغو
- أوغندا
- زامبيا
- زمبابواي

وأخيرا، استُكملت مجموعة البيانات هذه بمشاورات استراتيجية مع شركاء الإنتربول في إطار مشروع Gateway، مثل Bi.Zone، و Fortinet، وGroup-IB، وKapersky Lab، وTrend Micro.

نبذة عن الإنتربول

الإنتربول هو أكبر منظمة دولية للشرطة في العالم. ويتمثل دوره في مد يد العون إلى أجهزة إنفاذ القانون في بلدانه الأعضاء الـ 196 لمكافحة الجريمة عبر الوطنية بجميع أشكالها. وهو يسعى إلى مساعدة أجهزة الشرطة في العالم أجمع على مواجهة التحديات المتنامية للجريمة في القرن الحادي والعشرين بتزويدها بالدعم التقني والميداني بفضل بنية تحتية متطورة. وتشمل الخدمات التي يقدمها الإنتربول تدريبا محدد الأهداف، ودعما متخصصا لعمليات التحقيق، وقواعد بيانات متخصصة، وقنوات مأمونة للاتصالات الشرطية

رؤية الإنتربول: ربط أجهزة الشرطة لجعل العالم أكثر أماناً

تتمثل رؤية الإنتربول في إقامة عالم يكون فيه كل موظف من موظفي إنفاذ القانون قادرا، من خلال المنظمة، على التواصل بشكل مأمون وعلى تبادل المعلومات الشرطية الحيوية والاطلاع عليها كلما وحيثما دعت الحاجة، من أجل ضمان سلامة المواطنين في العالم. ويقدم الإنتربول باستمرار حلولا جديدة ومتطورة لمواجهة التحديات التي تعترض عمل أجهزة الشرطة والأمن على الصعيد العالمي ويشجع على استخدامها

نبذة عن برنامج الإنتربول لمكافحة الجريمة السيبرية

في عصر رقمي متغير، يتعرض فيه أكثر من نصف البشرية لخطر الوقوع ضحية للجريمة السيبرية، يتولى برنامج الإنتربول العالمي لمكافحة الجريمة السيبرية تقديم الدعم لأجهزة إنفاذ القانون الدولية. ونحن ملتزمون بإعداد وقيادة استجابة عالمية ترمي إلى منع هذه الجريمة، وكشفها، والتحقيق فيها، وتقويضها، بهدف الوصول في نهاية المطاف إلى الحد من تأثيرها على العالم وحماية المجتمعات من أجل عالم أكثر أمانا.

وتركز استراتيجية الإنتربول لمكافحة الجريمة السيبرية على أربعة أهداف رئيسية:

- تبنّي نهج استباقي وديناميكي لمنع الجريمة السيبرية وكبحها عبر تكوين صورة دقيقة عن مشهد تهديدات الجريمة السيبرية من خلال توفير المعلومات وتحليل البيانات الاستخباراتية.
- منع الجريمة السيبرية، التي تسبب ضررا كبيرا على الصعيد الوطني والإقليمي والعالمي، وكشفها، والتحقيق فيها، وكبحها بفعالية، من خلال الإشراف على العمليات عبر الوطنية وتنسيقها ومساعدة البلدان الأعضاء على تنفيذها.
- المساعدة على تطوير استراتيجيات البلدان الأعضاء وقدراتها لمكافحة الجريمة السيبرية وذلك عبر إرساء شراكات مفتوحة وشاملة ومتنوعة، وبناء الثقة في بيئة أمنية سيبرية عالمية.
- تعزيز دور الإنتربول وقدراته في رسم إطار الأمن العالمي من خلال المشاركة في المنتديات الدولية التي تتناول الجرائم السيبرية.

وننفّذ استراتيجيتنا وأهدافنا من خلال نموذج عمل بسيط وبنّاء، يرتكز على ثلاثة أركان أساسية:

- التصدي لتهديدات الجريمة السيبرية: استجابة سريعة ومنسقة لتهديدات الجريمة السيبرية الفورية والناشئة.
- عمليات مكافحة الجريمة السيبرية: تنفيذ استراتيجية ميدانية إقليمية لمكافحة الجريمة السيبرية بشكل فعال.
- بناء القدرات في المجال السيبري: تعزيز الاستراتيجيات والقدرات من خلال مشاريع ومنصات مبتكرة.

وتعوّل هذه الأركان على شبكتنا الواسعة من الشراكات مع القطاعين العام والخاص، مما يؤدي إلى تعزيز التعاون والنهوض بالخبرة الجماعية لمكافحة الجريمة السيبرية.

وللحصول على مزيد من المعلومات، يرجى الاتصال بنا بالبريد الإلكتروني EDPS-CD@interpol.int

نبذة عن مكتب الإنتربول للعمليات المشتركة لمكافحة الجريمة السيبرية في أفريقيا

AFJOC مبادرةٌ أطلقها الإنتربول لتعزيز قدرة أجهزة إنفاذ القانون الوطنية في أفريقيا على منع الجريمة السيبرية والكشف عنها والتحقيق فيها وتعطيلها. ويتحقَّق ذلك من خلال ما يلي

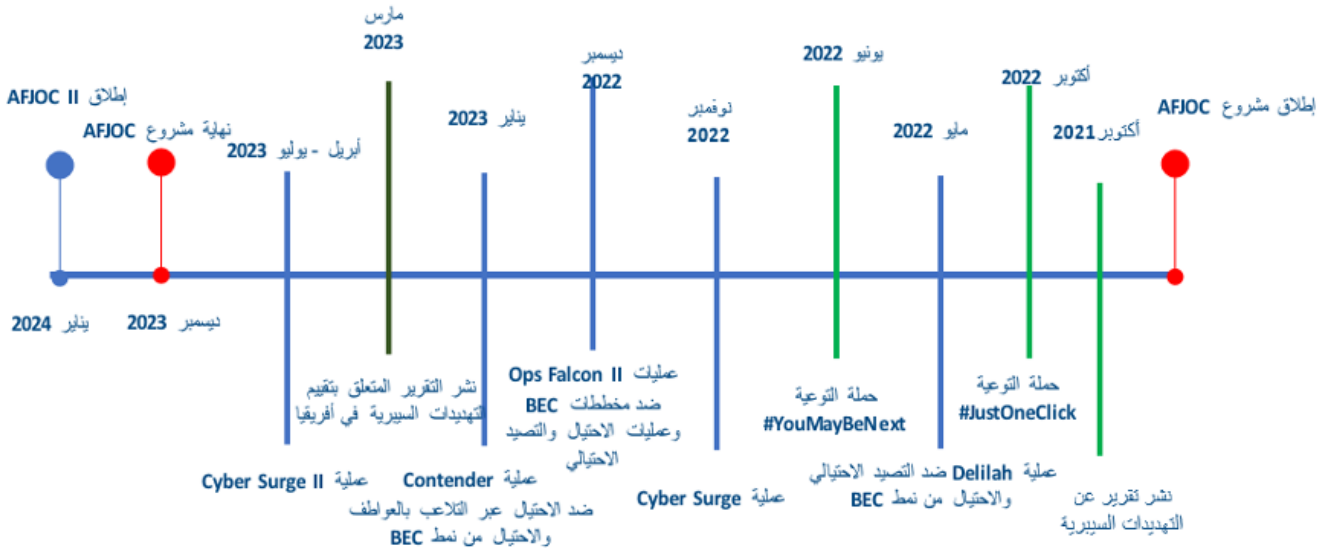
- جمع وتحليل المعلومات المتعلقة بالجرائم السيبرية؛
- تنفيذ عمل منسق يقوم على البيانات الاستخباراتية التي تُجمع؛
- تشجيع التعاون واتباع أفضل الممارسات في أوساط البلدان الأفريقية الأعضاء.

وموّلت المرحلة الأولى من هذه المبادرة وزارةُ الخارجية والكومنولث والتنمية في المملكة المتحدة ونُفّذت في الفترة من عام 2021 إلى عام 2023. وتستند المرحلة الثانية، التي لا تزال تحظى بدعم من وزراة الخارجية والكومنولث والتنمية في المملكة المتحدة، إلى الإنجازات التي تحققت خلال المرحلة الأولى، وتهدف إلى مواصلة تعزيز قدرات أجهزة إنفاذ القانون الوطنية في أفريقيا.

أنشطة المشروع

- الدعم التحليلي والبيانات الاستخباراتية - يشكل الجمع السريع لبيانات استخباراتية دقيقة أمرا حيويا لأيّ تحرك فعال تضطلع به أجهزة إنفاذ القانون لمواجهة الجريمة السيبرية. والتقارير التي يعدّها الإنتربول عن الأنشطة السيبرية هي موارد مهمة لأنها توفر معلومات مفصلة عن التهديدات السيبرية التي تستهدف بلدانا أو مناطق بعينها؛
- تطوير القدرات والإمكانيات الإقليمية لمكافحة الجريمة السيبرية - ثمة منصات تعاونية، مثل منصة التعاون لمكافحة الجريمة السيبرية والمنصة المتعددة الاختصاصات لمكافحة الجريمة السيبرية، تتيح التواصل بشكل مأمون وتبادل بيانات عن العمليات؛
- إطار العمل المشترك - يتيح مواجهة تهديدات الجرائم السيبرية من خلال التعاون بين أجهزة إنفاذ القانون والقطاع الخاص ومنظمات أخرى دولية/مشتركة بين الحكومات؛
- دعم العمليات وتنسيقها - تساهم عملياتنا في تفكيك الشبكات الإجرامية الضالعة في الجريمة السيبرية؛
- حملات التوعية - ترمي إلى تعريف الناس والمؤسسات في أفريقيا بالممارسات الجيدة المعتمدة في المجال السيبري.

ومكتب الإنتربول المعني بعمليات مكافحة الجريمة السيبرية في أفريقيا هو المكلف بتنفيذ مشروع AFJOC. وهو يتعاون على نحو وثيق مع أبرز الجهات المعنية في المنطقة، ولا سيما الاتحاد الأفريقي وأفريبول وأجهزة إنفاذ القانون والقطاع الخاص



الإنتربول

INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510

تابعونا:

INTERPOL HQ

@INTERPOL_HQ

INTERPOL

INTERPOL HQ

INTERPOL_HQ