الخليج

اقتصاد, تقنية وسيارات

17 فبراير 2024 23:31 مساء

التزييف العميق.. حاجة ملحّة لأطر قانونية وتنظيمية

أسهمت تطورات الذكاء الاصطناعي الكبيرة في ارتفاع وتيرة هجمات الهندسة الاجتماعية باستخدام «التزييف العميق»، وصولاً إلى انتحال صفة المسؤولين المصرفيين لتحويل الأموال، ما أثار مخاوف المؤسسات والشركات على حد سواء في حصول هجمات سيبرانية وإلكترونية متقنة ومدروسة، مستغلة عدم الاستعداد لهذه النوعية من الهجمات.

وقال خبراء في الحماية السيبرانية والإلكترونية لـ«الخليج»: إن قراصنة المعلومات وعصابات طلب الفدية، استخدموا فعلياً تقنيات «التزييف العميق» في العديد من الهجمات، خلال عام 2023، كما سيواصلون ذلك، خلال 2024، في ظل الثورة الرقمية التي يشهدها العالم حالياً، ما يستدعي من المؤسسات والشركات الاستعداد جيداً للتعامل الاستباقي مع هذه الهجمات.

ويقول الخبراء تواجه المنطقة مجموعة من التحديات بشأن تطور تقنيات التزييف العميق، واستغلالها في تكتيكات الهندسة الاجتماعية لقرصنة البيانات، أو تخريب الشبكات وتعطيلها وطلب أموال أو لغرض الابتزاز الإلكتروني، ما يستلزم وضع أطر قانونية ولوائح رسمية، لاستخدام هذه التقنيات بشكل قانوني ومعاقبة من يستغلها لارتكاب جرائم.

الصورة

أكد الدكتور هاو لي، الأستاذ المشارك في قسم الرؤية الحاسوبية، ومدير مختبر «الميتافيرس» في جامعة محمد بن زايد للذكاء الاصطناعي، أن التهديدات المتعلقة بالتزييف العميق موجودة دائماً، حيث قدرتها على توليد محتوى واقعي بسهولة كبيرة، ما يعني قدرة، حتى الأفراد العاديين، على استخدام هذه التقنية لأغراض مشبوهة وهو ما أصبحنا نراه يتكرر الآن بوتيرة أكبر. وأضاف: يعد هذا النوع من تقنيات التزييف العميق أحد الأسباب، التي دفعت الجامعة إلى إجراء أبحاث حول الكيفية التي يمكن ضبط انتشار هذا النوع من المحتوى ومنعه، وبالطبع، فإن التقنية المستخدمة لتوليد التزييف العميق، يمكن استخدامها بطريقة قانونية في مجالات متعدد مثل توليد المؤثرات البصرية في الأفلام، وفي الاتصالات الغامرة، وإنتاج مواد تعليمية وغيرها.

توظيف الذكاء الاصطناعي •

وأضاف: من المهم على المستوى التكنولوجي فهم الفروق الدقيقة والتعقيدات، التي تنطوي عليها تكنولوجيا التزييف العميق، وذلك حتى نتمكن من ضبط التهديدات الناتجة عنها وفي حقيقة الأمر، فقد شهدنا مراحل سابقة كان من السهل فيها اكتشاف أي تلاعب يتم القيام به، لكن التكنولوجيا تطورت إلى حد كبير، ولذلك فإن كشفها يحتاج إلى توظيف الذكاء الاصطناعي.

وتتسم أدوات كشف التزييف العميق المتوفرة في الوقت الحالي بفاعليتها في كشف أكثر أنواع المحتوى المعروفة، والتي يتم توليدها باستخدام الذكاء الاصطناعي مثل: مقاطع الفيديو التي تشتمل على تبديل الوجوه ومزامنة الشفاه باستخدام الذكاء الاصطناعي، والصور التي يظهر فيها الأفراد بهيئة مثالية غير معقولة، أو التي تبدو العناصر الثانوية الظاهرة فيها مثل الملابس غير منطقية.

وقال لي: نقوم في الجامعة بأخذ هذه التكنولوجيا المستخدمة في توليد المحتوى الواقعي المنتج حاسوبياً، ومن ثم تكييفها حتى تتمكن من كشف التزييف العميق والمحتوى، الذي يتم التلاعب به ويعمل باحثو الذكاء الاصطناعي على إيجاد نوع جديد من منصة YouTube يمكن للمستخدم فيه كتابة ما يريده، لتقوم المنصة بتوليد مقطع فيديو من الأوامر، التي حصلت عليها من المستخدم.

وعلى الرغم من وجود العديد من التطبيقات والمنصات، التي تقوم بمهام مماثلة في الوقت الحالي وبعضها في حقيقة الأمر مقدم من شركات تكنولوجيا عملاقة، فإن هذه الجهود التي يتم بذلها في هذا السياق، ستسهم في تحسين هذه التكنولوجيا بصورة ملحوظة.

توصيات •

وعن أهم التوصيات المتعلقة بالتعامل مع عمليات التزييف العميق والتخفيف من آثارها رأى لي: أن الخطوة الأولى تتمثل في نشر الوعي حول مسألة وجود هذا النوع من التزييف، فعلى سبيل المثال، إذا شاهد شخص ما محتوى معين يعرض بطريقة مختلفة عن الواقع، يجب حينها على المشاهد التنبّه والتحقق من مصدر الفيديو؛ إذ لا يجب تصديق أي شيء نراه ونعتبره حقيقة.

الخطوة الثانية هي أن التكنولوجيا أصبحت أفضل في كشف محتوى الفيديو الذي يتم التلاعب به؛ إذ شهدت خلال العامين الماضيين تطوراً ملموساً.

• القوانين المناسبة

وأخيراً، يجب العمل مع الجهات التشريعية والمنصات الإعلامية لوضع القوانين المناسبة، التي تستخدم هذه التكنولوجيا ومن أمثلة ذلك قيام الولايات المتحدة بتطبيق قوانين وتشريعات خاصة بالتزييف العميق، وحظر الاستخدامات غير القانونية لها، كما تعمل أوروبا والمملكة المتحدة على وضع تشريعات جديدة للتزييف العميق، والتي تعد جزءاً من قانون الذكاء الاصطناعي. إلا أن التشريعات في حقيقة الأمر متأخرة عن عملية إنتاج الصور بالذكاء الاصطناعي، وذلك من حيث الآثار الضارة مثل الاحتيال والخداع والنشر المتعمد للمعلومات المضللة.

وبيّن لي: من جانبها بدأت بعض شركات التكنولوجيا مثل «جوجل» و«ميتا» تطبيق سياسات تنظيم ذاتي من أجل إدارة التزييف العميق، لكننا لا نزال بحاجة إلى المزيد من القوانين المدروسة والأكثر صرامة. وكما هي الحال مع جميع التقنيات، فإن التزييف العميق هو أداة يمكن استخدامها في الجانب الجيد والسيئ، ولذلك من الأهمية بمكان أن يقوم المجتمع بإدارة الدفة نحو الاتجاه الصحيح.

• قلق متزايد

يقول حيدر باشا، الرئيس التنفيذي لأمن المعلومات لدى شركة «بالو ألتو نتوركس» لمنطقة أوروبا والشرق الأوسط وإفريقيا وأمريكا اللاتينية: أصبحت تقنية التزييف العميق، مصدر قلق متزايداً على مستوى العالم، خاصة بسبب احتمالية إساءة استخدامها.

ويشير تقرير المخاطر العالمية لعام 2024 الصادر عن المنتدى الاقتصادي العالمي، إلى أن أكبر خطر قصير المدى ينبع من المعلومات المضللة وتشكل تدخلات التزييف العميق جزءاً كبيراً من هذا الخطر.

وأضاف: أحد الاتجاهات التي شهدناها في الشرق الأوسط، هو زيادة تعقيد الهجمات الإلكترونية، مع تطور تكنولوجيا التزييف العميق، بحيث أصبحت أكثر إحكاماً وإقناعاً، ما يجعل من الصعب تحديد المخاطر والتخفيف من حدتها.

وتُستخدم تقنية التزييف العميق أيضاً في الكثير من عمليات الاحتيال المالي، عن طريق انتحال شخصية الأفراد للوصول إلى معلومات حساسة أو السماح بمعاملات احتيالية.

ووفقاً لبحث أجرته مؤسسة «جارتنر» فإن 30% من المؤسسات، بحلول 2026، لن تعتبر حلول التحقق من الهوية والمصادقة موثوقة بمعزل عن غيرها، وذلك في ظل الهجمات الإلكترونية، التي تستخدم التزييف العميق المعتمد على الذكاء الاصطناعي.

• أمان المؤسسات

ويعد التعرف إلى تعقيدات تكنولوجيا التزييف العميق أمراً محورياً في صياغة تدابير مضادة قوية. وعندما يتعلق الأمر بالأمن السيبراني، يعد اكتشاف التزييف العميق أمراً بالغ الأهمية، لأسباب عديدة للحفاظ على أمان المؤسسات والأفراد.

ومن خلال اكتشاف هذه التهديدات في الوقت المناسب، يمكن للشركات منع هجمات الهندسة الاجتماعية، والحماية من المعاملات الاحتيالية، وضمان حماية البيانات الحساسة.

ويمكن أيضاً استخدام التزييف العميق كجزء من حملات التصيد الاحتيالي والبرامج الضارة، ويمكن أن يساعد اكتشافها مسبقاً المؤسسات على الاستجابة بشكل استباقي لهذه التهديدات وتخفيف تأثيرها قبل حدوث أي ضرر.

ويؤكد باشا: من المهم لرؤساء الأمن ومديري أمن المعلومات، وضع استراتيجيات قوية مسبقاً، والتي تشمل تحديد الجهاز والتحليلات السلوكية، والتي يمكن أن تزيد من فرص اكتشاف الهجمات.

ومع انتشار التحول الرقمي، من المهم للمؤسسات أن تفهم التهديدات المحتملة لتقنيات التزييف العميق، وأن تقوم بالتثقيف وزيادة الوعي حول كيفية التمييز بين الحقيقي والمزيف، وفهم أفضل الممارسات للاستفادة من المعلومات الموثوقة.

ويجب على الشركات الاستفادة من شريك إلكتروني مبتكر، يمكنه المساعدة على دمج كل ما سبق، مع التركيز على نتائج الأمان المستقلة في الوقت الفعلي، مع تحسين البساطة والتكامل. من المهم أيضاً الدمج مع المنصات التي تدعم الذكاء الاصطناعي، وتلعب دوراً مهماً في مكافحة التزييف العميق.

- **نماذج اللغات الكبيرة**

وشهدت قطاعات الصناعة والأسواق مستويات مختلفة من التأثير، بعد قيام الجهات الفاعلة بالتهديد بالاستفادة من تقنيات التزييف العميق في الهجمات الإلكترونية. وبالنظر إلى المستقبل، سيستمر المهاجمون في الاستفادة من نماذج اللغات الكبيرة (LLMs) والذكاء الاصطناعي التوليدي لتطوير رسائل البريد الإلكتروني، لأغراض التصيّد الإلكتروني والإيقاع بالضحايا، ودمجها مع الهجمات المزيفة العميقة وغيرها من الهجمات، التي تدعم الذكاء الاصطناعي لزيادة معدلات نجاحها.

ويشير باشا إلى أنه نتيجة لذلك، يلعب الذكاء الاصطناعي دوراً مزدوجاً في الأمن السيبراني، سواء للحماية أو لشن الهجمات الإلكترونية. من المهم للمؤسسات توحيد أدوات الأمان الخاصة بها، لتحسين أوقات الاستجابة وتقليل التعقيد.

- **تزوير الصوت والفيديو**

قال كانديد ويست، نائب رئيس أبحاث الحماية السيبرانية في أكرونيس: تم استخدام الذكاء الاصطناعي التوليدي في العديد من الهجمات، التي تستهدف البريد الإلكتروني للشركات، لتزييف مكالمات صوتية أو مكالمات الفيديو من الرؤساء التنفيذيين.

وكانت هناك زيادة في عدد المهاجمين، الذين ينشئون صوراً فاضحة بواسطة التزييف العميق، بهدف الابتزاز أو التزييف العميق لأفراد من الأسرة والادعاء بأنهم تعرضوا لحادث من أجل الحصول على الأموال.

وتُستخدم تكتيكات مماثلة لنشر المعلومات المضللة، والتي يمكن أن تؤدي إلى الإضرار بالعلامات التجارية للشركات، عند نشر معلومات غير صحيحة أو الهجمات السيبرانية، كما شهدنا حالات استخدم فيها المحتالون التزييف العميق، أثناء إجراء مقابلة العمل بهدف الحصول على وظيفة.

وأضاف ويست، من المهم فهم الذكاء الاصطناعي التوليدي، لكن العديد من التدابير المضادة، لا تتطلب المعرفة بآلية عمل نماذج الذكاء الاصطناعي خلف الكواليس، كما يصعب معرفة البيانات أو المعايير، التي تم استخدامها لتدريب نماذج الذكاء الاصطناعي. وعلى الشركات التي تقع ضحية هذه الهجمات، والتي هي ببساطة الطرف المتلقي، وضع 3 خطوات مهمة في الاعتبار وهي: لا تثق بشكل أعمى بأي محتوى رقمي، وتحقق من الأصالة والهوية، قبل القيام بأي إجراءات واستخدم أدوات وإجراءات إضافية للتخفيف من الأضرار.

وإلى جانب وعي المستخدم والتدابير القانونية والتنظيمية، هناك بعض الأشياء التي يجب على الشركات مراعاتها، ويجب ألاّ تعتمد فقط على المعايير البيومترية للتحقق، حيث يمكن على سبيل المثال تزوير أنماط الصوت.

وعدم السماح لأي كان بالوصول إلى بياناتك، واعتماد المصادقة متعددة العوامل لزيادة الأمان. بالنسبة للمعاملات الحساسة، مثل المعاملات المالية المستعجلة، يجب أن تكون هناك إجراءات محددة، حتى في حالات الاستثناءات، والتي يجب أن تتطلب التحقق من خارج النطاق. للأسف، لم تعد رسائل البريد الإلكتروني أو الرسائل الصوتية جيدة، بما يكفي للحصول على الموافقات المهمة.

تحول •

قال عاكف خان، نائب الرئيس للتحليلات لدى «جارتنر»: «شهد العقد الماضي ظهور عدة نقاط تحول في مجالات الذكاء الاصطناعي، أتاحت إمكانية توليد صور اصطناعية لوجوه بشرية حقيقية في ما بات يُعرف بالتزييف العميق.

وأضاف خان، يجب على رؤساء أمن المعلومات وإدارة المخاطر اختيار مزودي الخدمات، الذين يتمتعون بالقدرات اللازمة ولديهم الخطط المناسبة، التي تتخطى المعايير الحالية المطبقة وعلى المؤسسات البدء في تحديد الضوابط المطلوبة، عبر التعاون مع مزودي الخدمة، الذين طوروا آليات تساعد على التخفيف من حدة التهديدات القائمة على التزييف العميق، عبر استخدام مزيج من أدوات كشف هجمات الحقن الرقمي لبيانات الوجه البيومترية وفحص الصور.

ويجب على الرؤساء التنفيذيين لشؤون أمن المعلومات وقادة إدارة المخاطر، بعد تحديد الاستراتيجية وخط الأساس، إدراج مؤشرات إضافية خاصة بالمخاطر وأساليب التعرف، تشمل التحقق من هوية الأجهزة وتحليل السلوك، وذلك بهدف زيادة فرص كشف الهجمات، التي تتعرض لها إجراءات التحقق من الهوية في مؤسساتهم.

التهديدات الكامنة •

إيفجينيا بوبوفا

تقول إيفجينيا بوبوفا، مديرة تطوير الأعمال الدولية في «بوزيتف تكنولوجيز»: مع الانتشار الواسع للتكنولوجيا الرقمية والذكاء الاصطناعي، في ظل المشهد الرقمي المتطور الذي نشهده حالياً، بات من الضروري التوعية بخطورة التهديدات الكامنة في التعقيد المتزايد، الذي تشهده تقنيات الهندسة الاجتماعية. حيث أثار الارتفاع الكبير في عدد الهجمات، التي تستخدم تقنية التزييف العميق، خلال عام 2023، مخاوف الكثيرين من أصحاب الأعمال والمستخدمين

.الأفراد، وأحدثت صدمة كبيرة في مشهد الأمن السيبراني في مختلف أنحاء العالم

وأضافت بوبوفا، تعد دولة الإمارات من أهم المراكز التكنولوجية في المنطقة، وهنا تبرز الحاجة الماسة إلى زيادة الوعي بمخاطر هذه التكنولوجيا، وكان البرنامج الوطني للذكاء الاصطناعي في الدولة، أطلق عام 2021 دليل «التزييف .العميق»، ضمن مبادرات مجلس جودة الحياة الرقمية

ويهدف الدليل إلى تعزيز الوعي المجتمعي بالاستخدامات الإيجابية والسلبية لتكنولوجيا التزييف العميق، وتأثيرها في جودة حياة الأفراد، وتعريفهم بسبل الحماية من مختلف التحديات الناجمة عن الاستخدام غير الصحيح لهذه التطبيقات .والوسائل التكنولوجية الحديثة

وقالت بوبوفا: شهدت الهجمات السيبرانية، التي تستخدم أساليب الهندسة الاجتماعية، وتحديداً هجمات التزييف (Sumsub) العميق، زيادة كبيرة خلال العام الماضي، حيث رصد تقرير الاحتيال السنوي الثالث الصادر عن شركة . %زيادة هائلة بنسبة بلغت 450

الصورة