مركز البيدر للدراسات والتخطيط
Al-Baidar Center For Studies And Planning

ما هي حرب وسائل التواصل الاجتماعي؟

prevency

ترجمة وتحرير: مركز البيدر للدراسات والتخطيط

عن المركز

مركز البيدر للدراسات والتخطيط منظمة عراقية غير حكوميّة ،وغير ربحّية، تأسس سنة ٢٠١٥م، ومُسجل لدى دائرة المنظمات غير الحكومية في الامانة العامة لمجلس الوزراء.

ويسعى المركز للمساهمة في بناء الدولة، عن طريق طرح الرؤى والحلول العملية للمشاكل والتحديات الرئيسة التي تواجهها الدولة، وتطوير آليات إدارة القطاع العام، ورسم السياسات العامة ووضع الخطط الاستراتيجية، وذلك عن طريق الدراسات الرصينة المستندة على البيانات والمعلومات الموثقة، وعن طريق اللقاءات الدورية مع الجهات المعنية في الدولة والمنظمات الدولية ذات العلاقة. ويسعى المركز لدعم الاصلاحات الإقتصادية والتنمية المستدامة وتقديم المساعدة الفنية للقطاعين العام والخاص، كما يسعى المركز لدعم وتطوير القطاع الخاص، والنهوض به لتوفير فرص عمل للمواطنين عن طريق التدريب والتأهيل لعدد من الشباب، بما يقلل من اعتمادهم على المؤسسة الحكومية، ويساهم في دعم اقتصاد البلد والارتقاء به.

ويسعى ايضاً للمساهمة في بناء الانسان، باعتباره ثروة هذا الوطن، عن طريق تنظيم برامج لاعداد وتطوير الشباب الواعد، وعقد دورات لصناعة قيادات قادرة على طرح وتبني وتطبيق رؤى وخطط مستقبلية، تنهض بالفرد والمجتمع وتحافظ على هوية المجتمع العراقي المتميزة ومنظومته القيمية، القائمة على الالتزام بمكارم الاخلاق، والتحلي بالصفات الحميدة، ونبذ الفساد بانواعه كافة، ادارية ومالية وفكرية واخلاقية وغيرها.

ملاحظة:

الآراء الواردة في هذا المقال لا تعبر بالضرورة عن وجهة نظر المركز، إنما تعبر فقط عن وجهة نظر كاتبها.

www.baidarcenter.org

info@baidarcenter.org

ما هي حرب وسائل التواصل الاجتماعي؟

prevency

وسائل التواصل الاجتماعي كسلاح في عصر المعلومات

من المستحيل تخيل عصر المعلومات اليوم بدون وسائل التواصل الاجتماعي، حيث تخترق وسائل التواصل الاجتماعي حياتنا اليومية، وتحدد اتصالاتنا الخاصة والشركات أو المؤسسات التي تقدم نفسها في شبكة التواصل الاجتماعي. المزايا واضحة جداً: نظرا للطريقة التي تعمل بها وسائل التواصل الاجتماعي، كل شخص – بغض النظر عما إذا كان شخصاً بذاته أو السياسي أو شركة – يمكن أن يحقق توعية هائلة بتكلفة منخفضة وبدون بذل جهد كبير. فلم تعد هناك حاجة إلى حراس البوابات التقليديين مثل مكاتب التحرير الإعلامية التقليدية ويتمتع كل فرد بفرصة توزيع المعلومات والمحتوى بطريقته الخاصة و بتأطيره الخاص. وبهذه الطريقة، يمكن بناء مجتمع عبر الإنترنت وسمعة رقمية مقابلة بسهولة، مما قد يؤدي إلى زيادة مبيعات الشركات ونتائج انتخابات أفضل في السياسة.

ومع ذلك، بالإضافة إلى العديد من الآثار الإيجابية والفرص لاستخدام وسائل التواصل الاجتماعي، فإن الطريقة التي تعمل بها شبكات التواصل الاجتماعي تشكل أيضاً مخاطرَ عديدةً : سهولة الوصول والوصول الواسع وإمكانية إخفاء الهوية تجعل من السهل بشكل متزايد التلاعب بالرأي العام وتشويه سمعة الشركات والمؤسسات والأفراد أو نشر محتوىً كاذب ومضر بالسمعة. وفي ظل هذا الوضع، يمكن للإنترنت وخاصة وسائل التواصل الاجتماعي أن تصبح سلاحاً ومشهداً لحرب افتراضية، تقاتل فيها الجهات الفاعلة لتأكيد مصالحها السياسية أو الاقتصادية أو الاجتماعية أو الثقافية.

قبل ٢٠ عاماً، توقع العلماء بالفعل «حرب شبكة» وتم وصف هذه الظاهرة لأول مرة منذ أكثر من ٢٠ عاماً. في ذلك الوقت، توقع العلماء تطور «حرب شبكة» في القرن الحادي والعشرين، والتي، على عكس الحرب الإلكترونية، لم تكن تهدف إلى التركيز على هجوم أنظمة تكنولوجيا المعلومات أو الاتصالات. ووفقاً للتصور في ذلك الوقت، كان الهدف من حرب الشبكة

هو التلاعب في تصور أو معرفة مجموعة معينة بطريقة متعمدة وبالتالي إلحاق الضرر بالهدف من الهجوم. وبالتالي، فإن مفهوم حرب الشبكة متأصل في نهج محدد للنزاعات في عصر المعلومات: في العصر الرقمي، لم تعد هناك حاجة لإراقة الدماء للقضاء على منافس وكسب الحرب، لأن المعلومات نفسها تصبح أقوى سلاح يمكن استخدامه من قبل الدول والشركات والمجموعات الصغيرة والأفراد على حدٍ سواء.

وسائل التواصل الاجتماعي كجزء من الحرب الهجينة

اليوم، لم تعد هذه الفكرة خيالاً، بل أصبحت حقيقة واقعة: لقد فهم القائمون المختلفون بها واستوعبوا المفهوم الأساسي لحرب الشبكة ويعتمدون بشكل متزايد على استخدام تكتيكات التلاعب بدلاً من الهجمات الجسدية للمضي قدماً في أجنداتهم. اليوم، انحسر مفهوم الحرب الشبكية في الظاهر والباطن في المقام الأول في سياق ما يسمى بالحرب الهجينة. الحرب الهجينة هي مصطلح سياسي–عسكري إلى حد ما يصف مزيجاً من أنواع مختلفة من الحرب العسكرية وغير العسكرية، حيث يتم تنفيذ العمليات والإجراءات في إطار الحرب المختلطة عادة بشكل سري وبدون إعلان رسمي للحرب كاستخدام الهجمات الجسدية السرية أو الهجمات الإلكترونية عبر الإنترنت بالإضافة إلى التكتيكات التواصلية والنفسية مثل الدعاية والمعلومات المضللة. وهذا النهج، على الرغم من أنه يشمل القتال عن طريق وسائل التواصل الاجتماعي، إلّا أنه لا يركز عليه، حيث يختلف الوضع مع مفهوم حرب وسائل التواصل الاجتماعي.

ما هي حرب وسائل التواصل الاجتماعي؟

تصف حرب وسائل التواصل الاجتماعي استخدام وسائل التواصل الاجتماعي كنوع من الأسلحة بهدف إحداث ضرر دائم لبعض الجهات الفاعلة مثل الحكومات أو الشركات. حيث يتم استخدام إستراتيجيات وتكتيكات مختلفة وكذلك الوسائل التكنولوجية من أجل الدفع من خلال أجندة سياسية أو اقتصادية أو اجتماعية أو ثقافية. وتهدف حرب وسائل التواصل الاجتماعي عادةً إلى التلاعب بالمفاهيم، وبالتالي أيضاً في آراء وعواطف وسلوك مجموعة مستهدفة معينة، وبالتالي الإضرار بالهدف الفعلي للهجوم. و تتضمن أمثلة الوسائل في حرب وسائل التواصل الاجتماعي نشر معلومات (خاطئة) في شبكات التواصل الاجتماعي، واستخدام برامج الروبوت الاجتماعية

والتأثير على مجموعات مستهدفة محددة عن طريق الاستهداف الدقيق. ومن هنا، فإن حرب وسائل التواصل الاجتماعي تدور أيضاً حول معركة جذب الانتباه، والتي يتم كسبها من خلال توليد محتوى فيروسي واستغلال آليات اقتصاد الانتباه السائد على الإنترنت. وبالتالي، يقوم المهاجمون بإنشاء روايات ومحتوى يهدف إلى مخاطبة المستخدمين عبر الإنترنت واستقطابهم عاطفياً للتميز عن العرض الزائد للمحتوى على شبكة التواصل الاجتماعي وتحقيق أكبر تأثير ممكن.

من يشارك في حرب وسائل التواصل الاجتماعي؟

في حين اقتصرت المعركة في شبكات التواصل الاجتماعي في البداية على الساحة السياسية، يتم الآن استخدام وسائل التواصل الاجتماعي من قبل جهات فاعلة مختلفة كسلاح إستراتيجي. وبالتالي، يمكن العثور على كل من المهاجمين والأهداف في العديد من قطاعات المجتمع. حيث يمكن تقسيمها تقريباً إلى أربع فئات:

- **السياسيون:** حيث يستخدم الممثلون السياسيون وسائل التواصل الاجتماعي لدفع أجندة سياسية معينة. على سبيل المثال، تهدف حرب وسائل التواصل الاجتماعي إلى التأثير على نتائج الانتخابات أو زعزعة استقرار الأنظمة السياسية أو زعزعة ثقة المجتمع بالحكومة. و تتضمن هذه الجهات السياسية تحالفات الدول أو الدول الفردية أو الأحزاب أو حتى الوحدات العسكرية.

- **الاقتصاديون:** ففي القطاع الاقتصادي، عادة يكون الدافع وراء حرب وسائل التواصل الاجتماعي ذا طبيعة مالية. حيث تسعى المجموعات أو القطاعات الصناعية إلى تأكيد مصالحها من أجل الحصول على ميزة أو إلحاق الضرر بالآخرين. بالإضافة إلى ذلك، تستخدم الشركات أيضاً وسائل التواصل الاجتماعي لتشويه سمعة منافسيها، وللحصول على ميزة تنافسية، وفي نهاية المطاف لتأكيد وجودها في السوق.

- **أصحاب الاهتمامات الخاصة:** إلى جانب المصالح السياسية والاقتصادية، هناك دوافع أخرى للمشاركة في حرب وسائل التواصل الاجتماعي. فهناك مجموعات تحاول، على سبيل المثال، التأثير على الرأي العام من أجل الحصول على لوائح معينة، بينما تحاول الجماعات الدينية أو السياسية تجنيد المزيد من الأتباع لأغراضها.

- **أصحاب الاهتمامات المختلطة:** في النهاية، لا يمكن دائماً تعيين جميع الممثلين لمجموعة معينة، لأن بعض المهاجمين يسعون وراء أهداف متعددة في نفس الوقت أو يعملون فقط نيابة عن جهات أخرى. وتضم مجموعة الهجين هؤلاء المهاجمين بالضبط. ومن أشهر الأمثلة على هؤلاء وكالة أبحاث الإنترنت – وهي شركة روسية شاركت في عمليات معلوماتية مختلفة في الماضي لفرض مصالح كل من الحكومة الروسية والشركات الروسية.

بشكل عام، أصبحت حرب وسائل التواصل الاجتماعي في متناول الجميع في الوقت الحاضر وبدون بذل الكثير من الجهد، لأن القليل من المعرفة التقنية والوصول إلى الإنترنت يكفيان لشن هجوم رقمي على وسائل التواصل الاجتماعي. وبالتالي، يمكن للمستخدم المفرد على شبكة التواصل الاجتماعي جمع معلومات شاملة حول هدف الهجوم بسرعة وسهولة، ومشاركة المحتوى المتلاعب به مع مجموعة مستهدفة واستخدام الاستهداف الدقيق والإعلانات المدفوعة لتشغيله بشكل أكثر تحديداً، أو الاتصال بمجموعة مستهدفة مباشرة عبر رسائل خاصة و مناقشتها معهم وإقناعهم بأمر معين.

حرب وسائل التواصل الاجتماعي كتهديد للشركات؟

يمكن للشركات أن تعلق بسرعة في مرمى النيران الرقمية لهجوم يتم عبر وسائل التواصل الاجتماعي. حيث إنَّ الشركات والمؤسسات الكبيرة معرضة للخطر بشكل خاص، لأنها تتزايد في نظر الجمهور وتكون عرضة بشكل خاص لحملات التشهير. بالإضافة إلى ذلك، تقدم الشركات والمؤسسات الكبيرة عادةً مجالاً أكبر للهجوم، حيث إنها غالباً ما تأخذ في الاعتبار الموضوعات ذات الصلة اجتماعياً مثل المسؤولية الاجتماعية أو المسؤولية الرقمية للشركات بشكل أكبر من الشركات الصغيرة. وبالتالي، فإن سوء السلوك المحتمل أو المزعوم يجذب انتباه مجموعة كبيرة من الناس بسرعة أكبر، ويثير الغضب ويفتح نقاط الهجوم التي يستغلها المنافسون أو مجموعات المصالح. في الوقت نفسه، يمكن للمنافسين والمهاجمين أيضاً استخدام وسائل التواصل الاجتماعي لإلحاق الضرر بالشركة دون مهاجمتها بشكل مباشر. على سبيل المثال، يمكن للمنافسين استخدام الوسائل غير العادلة للحرب على وسائل التواصل الاجتماعي لتعزيز مكانتهم في السوق أو يمكن للمجموعات الصناعية أو جمعيات الضغط التأثير بشكل كبير على ظروف العمل للشركات. في نهاية المطاف، يمكن أن يؤدي التلاعب في مفاهيم المجتمع للقضايا أيضاً إلى فرض شروط تنظيمية معينة وبالتالي يتسبب في أضرار جسيمة للصناعات بأكملها.

ما هي الإستراتيجيات والوسائل في حرب وسائل التواصل الاجتماعي؟

في سياق حرب وسائل التواصل الاجتماعي، يمكن استخدام وسائل التواصل الاجتماعي بطرق مختلفة وبتوجهات إستراتيجية مختلفة. فإذا تم استخدام وسائل التواصل الاجتماعي لمهاجمة الشركات أو المؤسسات أو الأفراد، فهنا يكون الحديث بشكل عام عن إستراتيجيات هجومية. وفي النهاية، ينوي المهاجمون دائماً إتلاف الهدف بطريقة أو بأخرى. ويمكن تمثيلهم بأربع فئات:

الاستهداف وجمع المعلومات

في الاستهداف، تُستخدم وسائل التواصل الاجتماعي لتحديد الأهداف المحتملة للهجوم ،ففي السياق العسكري مثلاً، يعني هذا تحديد مواقع قوات العدو من خلال التحقيق في سلوك وسائل التواصل الاجتماعي لأفراد القوات (على سبيل المثال عن طريق وضع العلامات الجغرافية) أو عن طريق الوصول إلى حسابات وسائل التواصل الاجتماعي. وإذا نظرنا إلى الاستهداف في سياق الهجمات على الشركات، فإن أحد الأهداف هو تحديد الأهداف الفردية داخل المنظمة – من هو، على سبيل المثال، الرئيس التنفيذي للشركة وكيف يمكن استخدام سلوكه على وسائل التواصل الاجتماعي لشن هجوم؟ حيث يرتبط هذا الجانب ارتباطاً وثيقاً بإمكانية استخدام الشبكات الاجتماعية لجمع أكبر قدر ممكن من المعلومات حول الهدف وأصحاب المصلحة من الهدف. فإذا كان، على سبيل المثال، الهدف هو أن يتم التلاعب برأي مجموعة معينة (العملاء، شركاء الأعمال، إلخ)، يتم أولاً تحديد ملفات تعريف الوسائط الاجتماعية وتحليلها، حيث تساعد المعلومات بعد ذلك في تصميم تكتيكات ومحتوى مصمم بدقة من أجل التلاعب بهذه المجموعة بأكبر قدر ممكن من الفعالية. بالإضافة إلى ذلك، يمكن أيضاً استغلال سوء سلوك أصحاب المصلحة الفرديين مثل شركاء العمل أو الموردين للإضرار بسمعة أصحاب المصلحة وبالتالي أيضاً بسمعة الهدف الفعلي للهجوم. و يُعرف هذا الإجراء أيضاً باسم تشويه المصداقية عن طريق الوكيل.

التلاعب من خلال المعلومات

يُعتبر التلاعب بالمجتمعات بأكملها أو بأصحاب المصلحة الأفراد إستراتيجية مركزية في حرب وسائل التواصل الاجتماعي. على سبيل المثال، يجب أن يتأثر رأي وقيم وعواطف وتفكير مجموعة مستهدفة معينة بطريقة تُنشئ تأثيراتٍ تبعيةً تضر بالهدف الفعلي للهجوم. على سبيل المثال، أثر

استخدام الدعاية الرقمية على نتائج الانتخابات أو حث العملاء على التوقف عن الشراء من شركة معينة. ومن أجل الوصول إلى هذا الهدف، يمكن للمهاجمين اتباع أساليب مختلفة:

- **الخداع** : من خلال نشر معلومات أو إشاعات كاذبة، يحاول المهاجمون خداع المجموعة المستهدفة بطريقة منهجية. ومن الشائع أيضاً إنتاج اهتمام مصطنع لموضوع ما من أجل تحويل الانتباه إليه وإبعاده عن موضوع آخر.
- **الارتباك**: من خلال تقديم معلومات متناقضة، يحاول المهاجمون خلق الارتباك والشعور بعدم الأمان في المجموعة المستهدفة. وهذا يجعل المجموعة المستهدفة أكثر عرضة لتبسيط التمثيلات والدعاية المصممة مما يلحق الضرر بالهدف.
- **التقسيم**: يحاول المهاجمون تقسيم المجتمعات أو الجماعات من خلال نشر الآراء المتطرفة وكذلك الكراهية والتحريض على الإنترنت. وهذا الصراع العام، بدوره، من المفترض أن يؤدي إلى مشاعر سلبية قوية وقابلية أعلى لأحداث معينة.
- **التعرّض**: ينشر المهاجمون معلومات أو بيانات سرية (خاطئة) من أجل فضيحة علنية لهدف الهجوم.
- **تشويه السمعة والتشهير**: حيث يهاجم المعتدون سمعة الهدف وينشرون محتوىً مسيئاً للسمعة وتشهيرياً في وسائل التواصل الاجتماعي.

و بغض النظر عن الهدف والنهج الذي يتبعه المهاجمون، فإن احتمالات استخدام المعلومات كسلاح في حرب وسائل التواصل الاجتماعي شاسعة: فمنها ما يسمى بالطرق المفتوحة، على سبيل المثال، توزيع الشائعات والمعلومات الخاطئة أو السرية وغيرها من المحتويات عبر حسابات وسائل التواصل الاجتماعي الرسمية للمؤثرين وقادة الرأي مثل السياسيين أو المشاهير أو موظفي الشركة، ومن خلال هذا النوع من توزيع المحتوى المستقطب أو المعلومات المضللة أو الاتهامات، يمكن للمهاجمين الوصول بسرعة إلى جمهور عريض وإثارة حرب مشتعلة وحتى لفت الانتباه إلى وسائل الإعلام التقليدية. بالإضافة إلى ذلك، عادة ما يكون للمؤثرين «الحقيقيين» تأثير كبير على رأي المجموعة المستهدفة لأنهم يتمتعون بدرجة عالية من المصداقية.

إذا استمر المهاجمون في السر، فعادةً ما ينشئون هوياتٍ مزيفةً في وسائل التواصل الاجتماعي – ما يسمى بحسابات دمى الجورب – أو يستأجرون متصيدين عبر الإنترنت لتوزيع محتوى مستقطب. ويتراوح هذا المحتوى من التعليقات والتقييمات السلبية الفردية إلى حملات اغتيال الشخصيات الرقمية واسعة النطاق والعناوين المستهدفة للمستخدمين الفرديين عبر المنشورات والإعلانات المدفوعة للتأثير على آرائهم في اتجاه أو آخر، ما يسمى بالروبوتات الاجتماعية وشبكات الروبوتات هي أيضاً وسيلة شائعة للتأثير على الرأي. حيث يمكنهم تحقيق وصول هائل للمحتوى في غضون وقت قصير جداً، لأن الروبوتات تنشر أو تربط أو تعلق أو تشارك تلقائياً وكل ثانية، وبالتالي تضخيم وصول المحتوى بشكل مصطنع. ويمكن أيضاً استخدام الروبوتات لغرض إرسال البريد العشوائي الكلاسيكي لإنشاء نوع من «التحميل الزائد للمعلومات» لمجموعة مستهدفة محددة على شبكة التواصل الاجتماعية.

النتيجة: تواجه المجموعة المستهدفة في كثير من الأحيان وبشكل منتظم قصة أو إشاعة أو معلومات معينة تدور حول التعود و تأثير الذاكرة وتبدأ المجموعة المستهدفة في تصديق المحتوى (ما يسمى بتأثير التعرض المجرد).

من أجل الاستمرار في توزيع المحتوى والرسائل الخاصة بالفرد بأكبر قدر ممكن من الوصول، لا يزال يتم استخدام ما يسمى ب «الاختطاف» وهو الهاشتاج. هنا، يقوم المهاجمون أي «المختطفون» الموجودين بالفعل المعروفين جيداً بنشر المحتوى الخاص بهم فيما بينهم بقوةٍ وتكرارٍ هائلين. النتيجة: يتم حجب المحتوى الفعلي للهاشتاج ويواجه المستخدمون الذين يبحثون عن الهاشتاج في الغالب المحتوى المتلاعب به للمهاجمين.

التعبئة والالتزام

بالإضافة إلى التأثير على الإدراك والتفكير والعواطف، تدور حرب وسائل التواصل الاجتماعي أيضاً حول التلاعب بالسلوك – حتى خارج الشبكة الاجتماعية. فهو لا يحاول فقط التأثير على ما يحبه الناس أو يشاركونه أو يعلقون عليه، ولكن أيضاً كيف يتصرفون بعيداً عن العالم الرقمي. حيث يحاول المهاجمون الرقميون، على سبيل المثال، إقناع مجموعة مستهدفة معينة بالانخراط في حملة ضد الهدف الفعلي، وعلى سبيل المثال، الدعوة للاحتجاج على الخطط السياسية أو مقاطعة

الشركات أو المنتجات. و للقيام بذلك، يلجأ الخصوم إلى نوع من تكتيك الحشد: بمساعدة وسائل غير عادلة مثل الروبوتات التي تعطي مظهرَ كتلةٍ رقميةٍ غاضبة وتحاول إصابةَ المستخدمين الحقيقيين بغضبها وسخطها. النتيجة: يصبح المستخدمون الحقيقيون جزءاً من الغوغاء عبر الإنترنت، وبالتالي يحشدون المزيد والمزيد من المستخدمين (الحقيقيين) الآخرين. و يمكن أن تكون النتيجة احتجاجاً (وهمياً) أو مقاطعة (وهمية)، والتي لم تكن لتحدث لولا تدخل المهاجمين. في هذه المرحلة، يستخدم المهاجمون أيضاً ما يسمى بالتسويق الماكر "Astroturfing".

ويستخدم هذا النوع من التسويق تدابير تواصلية لتزييف الاحتجاجات الموجودة بالفعل أو «الحركات الشعبية» – دائمًا بهدف تمكين الأشخاص الحقيقيين من الانضمام إلى هذه الحركة الوهمية وبالتالي فرض أجندة معينة.

ومن الوسائل الأخرى للتلاعب بالسلوك ما يسمى بالهندسة الاجتماعية. و هذه محاولة لاستخدام التلاعب النفسي لإقناع الأهداف باتخاذ إجراءات معينة، مثل الكشف عن المعلومات والبيانات السرية. وقد أصبحت الهندسة الاجتماعية معروفة في عام ٢٠١٠ من قبل خبير تكنولوجيا المعلومات توماس رايان Thomas Ryan، من بين آخرين. حيث أنشأ رايان الشخصية الفنية الافتراضية Robin Sage ، وأنشأ ملفاً شخصياً لها في الشبكات الاجتماعية واستخدمها في الاتصال بالسياسيين ورؤساء الشركات من أجل استخراج معلومات سرية منهم – وبنجاح كبير. وتُعرف هذه العملية والتي يتظاهر فيها الأشخاص (المزيفون) بعلاقة مع هدف الهجوم من أجل الحصول على معلومات أو بيانات أو حتى صور للشخص الذي لم يتم تصنيفه بشكل كامل، باسم محاصرة العسل.

الهجمات الإلكترونية الاجتماعية

هذه فئة خاصة من حرب وسائل التواصل الاجتماعي وهي مزيج من الهجمات الإلكترونية الكلاسيكية وأساليب التلاعب في شبكة التواصل الاجتماعي، أو ما يسمى بالهجمات الإلكترونية الاجتماعية. حيث يستخدم مجرمو الإنترنت الكلاسيكيون أيضاً وسائل التواصل الاجتماعي بشكل متزايد ويحاولون إرسال البرامج الخبيثة والبرامج الضارة عبر المنشورات العامة للحسابات المزيفة أو الرسائل المباشرة في تطبيقات المراسلة الخاصة بالشبكات أو للوصول إلى البيانات المهمة

بمساعدة الهندسة الاجتماعية. بالإضافة إلى ذلك، أصبحت حسابات وسائل التواصل الاجتماعي بشكل متزايد هدفاً للمتسللين للوصول إلى المعلومات (على سبيل المثال من المحادثات الخاصة) عبر الملفات الشخصية أو لمشاركة المحتوى عبر الملفات الشخصية المخترقة. ومن ناحية أخرى، يلجأ المحاربون في حرب وسائل التواصل الاجتماعي أيضاً إلى أساليب الحرب الإلكترونية الكلاسيكية مثل القرصنة، على سبيل المثال، للوصول إلى البيانات والمعلومات التي يتم توزيعها بعد ذلك عبر وسائل التواصل الاجتماعي على نطاق واسع. و هناك إشارات على زيادة في مثل هذه الهجمات المختلطة، والتي يجب أن تكون الشركات على وجه الخصوص مستعدة لها.

أخيراً، هناك شيء واحد يجب توضيحه: الأساليب المذكورة هنا ليست سوى أمثلة، لأنه في حرب وسائل التواصل الاجتماعي هناك مجموعة غير محدودة من الإستراتيجيات والوسائل، و يتزايد عددها وتطورها باستمرار مع التطور التكنولوجي المستمر. فقط أولئك الذين هم على دراية بأساليب الهجوم الحالية ويبقون دائماً على إطلاع دائم بأحدث التقنيات يمكنهم حماية أنفسهم ومعرفة ما يجب فعله في حالة الطوارئ من أن يصبحوا جزءاً من حرب وسائل التواصل الاجتماعي.

كيف تدير خطر حرب وسائل التواصل الاجتماعي؟

أصبحت الحماية والدفاع ضد الهجمات في أو من خلال شبكة التواصل الاجتماعي أكثر تعقيداً. إذ يمكن تنفيذ الهجمات بالاستفادة من مجرد عدد قليل من الشبكات الاجتماعية . ويضاف إلى ذلك مشكلة ما يسمى بالتطبيقات الاجتماعية المظلمة – التطبيقات التي لا يمكن تتبع حركة المرور الخاصة بها وتشمل هذه تطبيقات المراسلة (messenger) مثلWhatApp أو Telegram فقد أصبحت هذه أيضاً ساحة للّعب بشكل متزايد في حرب وسائل التواصل الاجتماعي.

النتيجة: الرصد الفعال غير ممكن بدون الخبرة والمعرفة الشاملة بهذه المشاكل، ممّا يقلل بشكل كبير من قدرة المؤسسات أو الشركات أو الأفراد على التصرف في حالة وقوع هجوم .

وحتى لا يصبح شخص ضحية لهجوم ويقع بسرعة في وضع رد فعل سلبي، فإنه من الضروري الحصول على نظرة عامة على منصات وإستراتيجيات وتكتيكات المهاجمين والإجراءات المضادة المحتملة – ويمكن أن تتغير هذه مرة أخرى ومرة أخرى في وقت قصير جداً. ومن أجل منع مثل هذا

العجز عن التصرف في حالات الطوارئ بشكل أفضل، من الضروري زيادة الوعي بالموضوع، ودمج خطر «حرب وسائل التواصل الاجتماعي» في إدارة المخاطر الخاصة بالفرد وإعداد إستراتيجيات دفاعية مضادة للطوارئ. و يسعدنا مساعدتك في هذه الإجراءات.