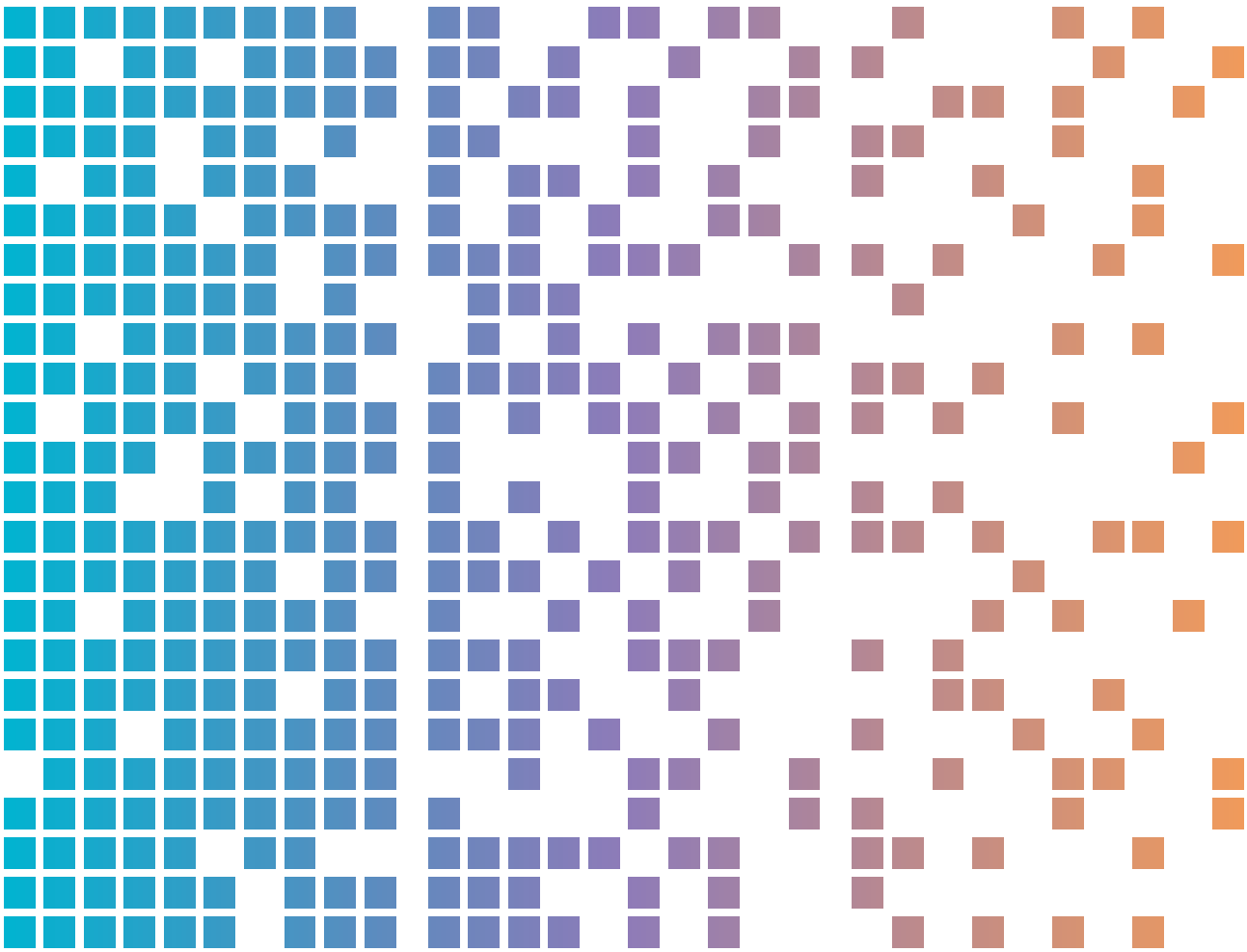
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

मूक चोरी: साइबर अपराधी कॉर्पोरेट नेटवर्कों पर हमला करने के लिए सूचना चोरी करने वाले मैलवेयर का उपयोग करते हैं



सामग्री जटिलता
मध्यम ●●○

विषय-सूची

संदर्भ

इंफो स्टीलर मैलवेयर उपयोगकर्ता के क्रेडेंशियल्स और सिस्टम की जानकारी चुराता है, जिसका दुरुपयोग साइबर अपराधी मुख्यत: आर्थिक लाभ के लिए करते हैं। ऑस्ट्रेलिया सहित पूरी दुनिया-भर में कई संगठनों और क्षेत्रों के प्रति साइबर अपराध हमलों में सूचना चोरी करने वालों की पहचान की गई है। यह प्रकाशन पाठकों को सूचना की चोरी करने वाले मैलवेयर पर साइबर सुरक्षा मार्गदर्शन प्रदान करता है, जिसमें संगठनों और उनके कर्मचारियों के लिए खतरे की गतिविधि और मिटिगेशन के लिए सलाह शामिल है।

प्रमुख बिंदु

- सूचना की चोरी करने वाले मैलवेयर, जिसे इंफो स्टीलर्स के रूप में भी जाना जाता है, एक प्रकार का मैलवेयर होता है, जिसे शिकार व्यक्ति के डिवाइस से जानकारी एकत्र करने के लिए डिज़ाइन किया जाता है। इसमें उपयोगकर्ता नाम और पासवर्ड, क्रेडिट कार्ड के विवरण, क्रिप्टोकरेंसी वॉलेट्स, स्थानीय फाइलें और कुकीज़, उपयोगकर्ता इतिहास और ऑटोफिल फॉर्म विवरणों समेत ब्राउज़र डेटा शामिल हो सकते हैं।
- साइबर अपराधी शिकार बनाए गए व्यक्ति के कार्य-नियोक्ता, उनके ग्राहकों और अन्य उद्यम सिस्टम्स के डिवाइसेज़ में शुरुआती पहुंच प्राप्त करने के लिए कॉर्पोरेट खातों से जुड़े उपयोगकर्ताओं के चोरी किए गए क्रेडेंशियल्स खरीदने और इन्हें इस्तेमाल करने की कोशिश कर सकते हैं। इन संगठनों पर पड़ने वाले प्रभावों में रैंसमवेयर, जबरन वसूली, व्यावसायिक ईमेल हमले और बौद्धिक संपदा की चोरी शामिल हो सकती है।
- ऑस्ट्रेलियाई सिग्नल्स निदेशालय के ऑस्ट्रेलियाई साइबर सुरक्षा केंद्र (एएसडी के एसीएससी) ने ऐसे कर्मचारियों से कॉर्पोरेट नेटवर्क उल्लंघनों की पहचान की है, जो हमला किए गए व्यक्तिगत डिवाइसेज़ के माध्यम से कार्यस्थल संसाधन एक्सेस करते हैं। कई उदाहरणों में, साइबर अपराधियों ने चोरी किए गए वैध उपयोगकर्ता क्रेडेंशियल्स का उपयोग करके कॉर्पोरेट नेटवर्कों में शुरुआती एक्सेस हासिल की। हमारी जांचों से पता चला है कि साइबर अपराधियों द्वारा विशेषाधिकार प्राप्त उपयोगकर्ता खातों को सफलतापूर्वक एक्सेस किए जाने के बाद आमतौर पर व्यापक हमले हुए हैं।
- जो संगठन कर्मचारियों, ठेकेदारों, प्रबंधित सेवा प्रदाताओं या अन्य संस्थाओं को अपने नेटवर्क को दूरस्थ रूप से एक्सेस करने की सुविधा प्रदान करते हैं, जिसमें ब्रिंग यॉर ओन डिवाइस (BYOD) हार्डवेयर शामिल हैं, उन्हें इंफो स्टीलर्स के खतरों के बारे में पता होना चाहिए और खुद को इस खतरे से बचाना चाहिए। साइबर अपराधी फ़िशिंग ईमेल, पायरेटेड सॉफ़्टवेयर डाउनलोड, सर्च इंजन ऑप्टिमाइज़ेशन (एसईओ) तकनीकों, दुर्भावनापूर्ण विज्ञापनों या सोशल मीडिया प्लेटफॉर्मों पर पोस्ट किए गए दुर्भावनापूर्ण लिंक्स सहित कई तकनीकों का उपयोग करके शिकार व्यक्ति के डिवाइसेज़ में इंफो स्टीलर्स को प्रविष्ट करते हैं। सामान्य रूप से, जिन डिवाइसेज़ का उपयोग काम और व्यक्तिगत उद्देश्यों दोनों के लिए किया जाता है, उनके लिए उपयोगकर्ता के व्यवहार और निम्न सुरक्षा नियंत्रणों के कारण इन तकनीकों के माध्यम से इंफेक्शन का ऊंचा जोखिम होता है।
- साइबर अपराधियों के लिए इंफो स्टीलर्स साइबर अपराध गतिविधि का मुद्रीकरण करने का एक आकर्षक मॉडल प्रदान करते हैं, विशेषकर प्रवेश स्तर के साइबर अपराधियों और सीमित तकनीकी दक्षता वाले लोगों के लिए। कुछ साइबर अपराधी मैलवेयर-एस-ए-सर्विस (MaaS) स्टाइल प्रोग्राम के तहत इंफो स्टीलर्स उत्पादों का विपणन करेंगे और उनके उपयोग के लिए मासिक सदस्यता शुल्क लेंगे।

पृष्ठभूमि

साइबर अपराधियों द्वारा इंफो स्टीलर्स का उपयोग ऑस्ट्रेलियाई संगठनों की सुरक्षा और सकुशलता के लिए खतरा प्रस्तुत करता है। इंफो स्टीलर्स संक्रमण आमतौर पर प्रमुख साइबर सुरक्षा घटनाओं की पूर्व-गतिविधि के रूप में मौजूद होते हैं, क्योंकि साइबर अपराधी उपयोगकर्ता क्रेडेंशियल्स को एकत्र करने के लिए इनका उपयोग करते हैं। इन उपयोगकर्ता क्रेडेंशियल्स को, विशेषकर जो इंटरनेट-फेसिंग रिमोट सेवाओं या विशेषाधिकार प्राप्त खातों की एक्सेस प्रदान करते हैं, कॉर्पोरेट सिस्टम और डेटा में शुरुआती एक्सेस को सक्षम बनाने के लिए शोषित किया जाता है।

नोट: शुरुआती एक्सेस ब्रोकर्स चोरी किए गए उपयोगकर्ता क्रेडेंशियल्स को खरीदकर और मान्य बना करके साइबर अपराध इकोसिस्टम के अंदर एक विशेष भूमिका निभाते हैं। फिर वे अधिक मांग वाले कॉर्पोरेट परिवेशों के लिए ऊंची-गुणवत्ता के उपयोगकर्ता क्रेडेंशियल्स की नीलामी ऐसे साइबर अपराधियों को करते हैं, जो संगठन के कॉर्पोरेट नेटवर्क का फायदा उठाने के लिए उपयोगकर्ता क्रेडेंशियल्स का उपयोग करेंगे।

चोरी किए गए वैध उपयोगकर्ता क्रेडेंशियल्स साइबर अपराधियों के लिए अत्यधिक मूल्यवान होते हैं, क्योंकि वे कॉर्पोरेट नेटवर्क और एंटरप्राइज़ सिस्टम की शुरुआती एक्सेस में तेजी लाते हैं। चोरी किए गए वैध उपयोगकर्ता क्रेडेंशियल्स के साथ साइबर अपराधी कई विशिष्ट चुनौतियों और तकनीकों को बायपास कर सकते हैं, जिनमें शामिल हैं:

- लक्ष्य की पहचान करना और उसपर शोध करना
- लक्ष्य के नेटवर्क में कमजोरियों की गणना करना
- शुरुआती एक्सेस के लिए वेक्टर्स विकसित करना, जैसे:
  - फ़िशिंग सामग्री
  - सॉफ़्टवेयर कमजोरियों का शोषण
  - RemoteDesktop प्रोटोकॉल (RDP) या वर्चुअल प्राइवेट नेटवर्क (VPN) सेवाओं सहित दूरस्थ सेवाओं को लक्षित करना
  - उपयोगकर्ता क्रेडेंशियल्स (पासवर्ड का अनुमान लगाने) के प्रति ब्रूट फोर्स के हमले।

इन कदमों के लिए समय के निवेश और तकनीकी योग्यता के ऐसे स्तर की आवश्यकता होती है, जो कुछ साइबर अपराधियों के लिए बाधा प्रस्तुत करता है। विशेष रूप से जो साइबर अपराधी कॉर्पोरेट नेटवर्क सुरक्षा में प्रवेश करने में असमर्थ रहते हैं, वे इंफो स्टीलर्स संक्रमणों से सीधे लाभ उठा सकते हैं, क्योंकि ये संक्रमण वांछनीय कॉर्पोरेट नेटवर्कों के लिए उपयोगकर्ता क्रेडेंशियल्स की त्वरित और आसान एक्सेस प्रदान कर सकते हैं।

दूरस्थ कार्यपरिवेशों में कुछ कर्मचारी काम और व्यक्तिगत इंटरनेट ब्राउज़िंग, दोनों के लिए व्यक्तिगत डिवाइसेज़ का उपयोग करते हैं। ऐसा करने में, कर्मचारी अपने उपयोगकर्ता क्रेडेंशियल्स को अपने वेब ब्राउज़र के पासवर्ड स्टोर और एक्सटेंशन में संग्रहीत करने का विकल्प चुन सकते हैं, या वे वेब ब्राउज़र ऑटोफिल सुविधाओं का उपयोग कर सकते हैं। इंफो स्टीलर्स वेब ब्राउज़र में ऑथेंटिकेशन कुकीज़ और अन्य व्यक्तिगत डेटा के साथ-साथ इन पासवर्ड स्टोर्स को भी लक्षित करते हैं।

कॉर्पोरेट डिवाइसेज़ के विपरीत, व्यक्तिगत डिवाइसेज़ में हमेशा उद्यम सुरक्षा नीतियां लागू नहीं होती हैं, जिससे संगठनों के लिए अधिक जोखिम पैदा होता है। उदाहरण के लिए, कर्मचारी पायरेटेड सॉफ़्टवेयर डाउनलोड करने और ऊंचे जोखिम वाली ऑनलाइन ब्राउज़िंग जैसी गतिविधियों में संलग्न हो सकते हैं, जिससे साइबर खतरों और मैलवेयर संक्रमणों से संपर्क में बढ़ौत्तरी हो सकती है।

इंफो स्टीलर्स, वितरक, शुरुआती एक्सेस ब्रोकर्स और रैंसमवेयर सहयोगी साइबर अपराध इकोसिस्टम का मुख्य हिस्सा बन जाते हैं, जोकि आर्थिक लाभ से प्रेरित होता है। जब साइबर अपराधी किसी हमले के विशेष चरणों को लक्षित करने वाली क्षमताओं में विशेषज्ञता और इनका विकास हासिल कर लेते हैं, तो यह इकोसिस्टम और भी अधिक कुशल बन जाता है और फिर वे इस क्षमता को अन्य आपराधिक सहयोगियों को एक सेवा के रूप में बेचते हैं।

धमकीपूर्ण गतिविधि

एएसडी का एसीएससी विश्व-स्तर पर इंफो स्टीलर गतिविधि के उदय पर दृष्टि रख रहा है और इसकी निगरानी कर रहा है, जोकि ऑस्ट्रेलियाई नेटवर्कों के लिए एक बढ़ता हुआ खतरा प्रस्तुत कर रहा है। उद्योग रिपोर्टिंग इंगित करती है कि 2023 में पूरे साल-भर साइबर अपराध गतिविधि में सबसे लोकप्रिय मैलवेयर वेरिएंट इंफो स्टीलर्स थे। डार्क वेब मार्केटप्लेस पर बिक्री के लिए चोरी किए गए डेटा की बढ़ती हुई मात्रा, और इस डेटा का लाभ उठाने वाली शुरुआती एक्सेस ब्रोकर गतिविधि में वृद्धि इस बढ़ती हुई प्रवृत्ति को दर्शाती है, जो 2024 में तेज हो गई है।

इंफोर्मेशन स्टीलर इकोसिस्टम

चरण 1: मैलवेयर प्राप्त करना

इंफो स्टीलर्स को आमतौर पर साइबर क्रिमिनल मार्केटप्लेस पर MaaS या स्टीलर-एस-ए-सर्विस के रूप में पेश किया जाता है, या सोर्स कोड के रूप में बेचा जाता है। MaaS से संदर्भ ऐसे व्यवसाय मॉडल से है, जिसके तहत एक मैलवेयर डेवलपर वैध सॉफ़्टवेयर-एस-ए-सर्विस प्रस्तावों के समान ही वेब-आधारित प्लेटफ़ॉर्मों के माध्यम से व्यक्ति-विशेषों को अपने दुर्भावनापूर्ण सॉफ़्टवेयर की सदस्यता बेचता है। MaaS मॉडल ने साइबर अपराधियों के लिए प्रवेश की बाधा को कम कर दिया है, क्योंकि यह व्यापक तकनीकी कुशलताओं के बिना भी व्यक्ति-विशेषों को मैलवेयर वितरित करने और साइबर हमलों में उपयोग के लिए चोरी की गई जानकारी एकत्र करने की अनुमति देता है।

MaaS के रूप में प्रस्तुत किए जाने वाले इंफो स्टीलर्स को आमतौर पर अपेक्षाकृत सस्ते मासिक शुल्क पर विज्ञापित किया जाता है, और यह साइबर अपराधियों को एक इंफो स्टीलर डैशबोर्ड की एक्सेस देता है। यह डैशबोर्ड इंफो स्टीलर मैलवेयर के निर्माण की सुविधा प्रदान करता है, चोरी किए गए डेटा को व्यवस्थित करता है और शिकार बनाए गए सिस्टम्स की संख्या का अनुरेखण करता है। MaaS ऑपरेटर्स एंटीवायरस सॉफ़्टवेयर की पहचान में आने से बचने और ग्राहकों को आकर्षित करने और बनाए रखने के लिए फीचर अपडेट्स, टूल्स और तकनीकी सहायता प्रस्तुत करते हैं। कई इंफो स्टीलर्स के पास डेटा एक्सफिल्ट्रेशन करने के बाद शिकार बनाए गए व्यक्ति के डिवाइस से खुद को हटाने की क्षमता होती है।

चरण 2: वितरण

जो साइबर अपराधी इंफो स्टीलर्स का वितरण करते हैं और हमला किए गए डिवाइसेज़ से जानकारी एकत्र करते हैं, उन्हें 'ट्रैफर्स' (ट्रैफिक डिस्ट्रिब्यूटर्स) के नाम से जाना जाता है। ट्रैफ़र्स शिकार बनाए गए लोगों को दुर्भावनापूर्ण लिंक्स की ओर निर्दिष्ट करते हैं, जिससे व्यापक अभियानों के हिस्से के रूप में इंफो स्टीलर्स का फैलाव सुविधाकृत होता है। अधिकांश अभियान अंधाधुंध तरीके से, अवसरवादी संक्रमणों पर निर्भर करते हैं। लेकिन कुछ अभियान विशिष्ट उद्योगों के प्रति अनुरूपित होते हैं और इनमें शिकार बनाने के लिए विशिष्ट व्यक्ति-विशेषों के प्रति लक्षित स्पियरफ़िशिंग शामिल होती है। ट्रैफ़र्स ग्राहकों की मांग के उत्तर में इन अधिक लक्षित अभियानों को चलाते हैं; उदाहरण के लिए, जहां खरीदार ऊंचे मूल्य के विशिष्ट संगठनों या सेक्टरों में एक्सेस की मांग कर रहे हैं।

ट्रैफ़र्स अनेकानेक तकनीकों का उपयोग करके शिकार बनाए गए व्यक्ति के डिवाइसेज़ में इंफो स्टीलर्स को प्रविष्ट करेंगे, जिनमें शामिल हैं:

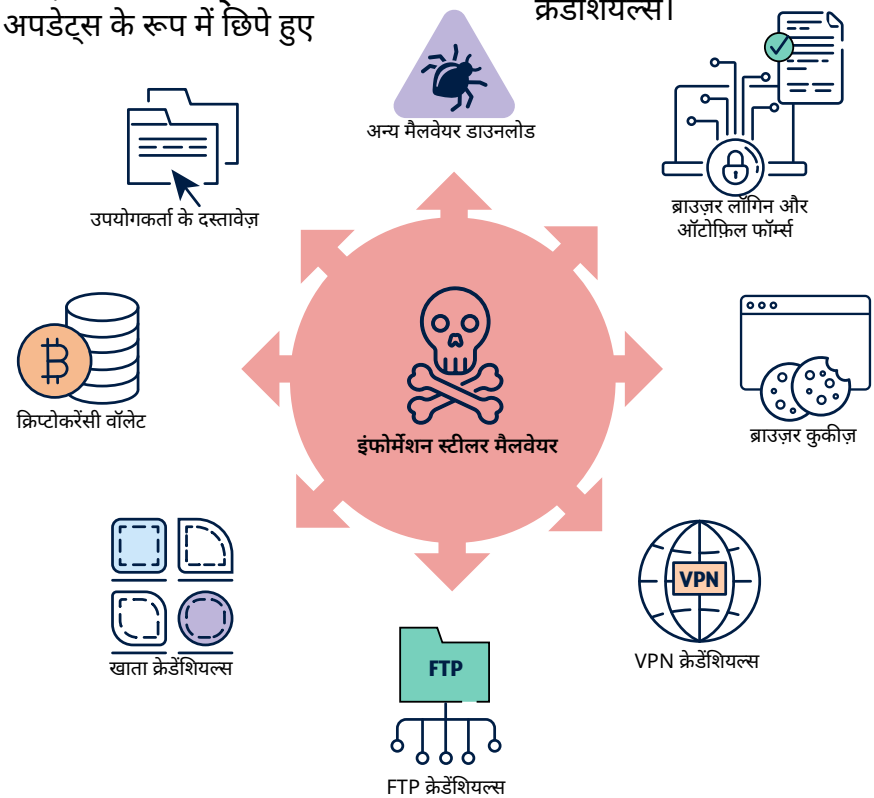
- **बॉटनेट्स**: शिकार बनाए गए कंप्यूटर सिस्टम्स के नेटवर्क्स, जिनका नियंत्रण साइबर अपराधियों द्वारा दुर्भावनापूर्ण कार्यों को अंजाम देने के लिए किया जाता है, जैसे फ़िशिंग मैसेजेस या मैलवेयर वितरित करना

- **फ़िशिंग**: धोखे से संवेदनशील जानकारी प्राप्त करने के प्रयास, जिसमें ईमेल्स या सोशल मीडिया फ़ोरमों और मैसेजिंग ऐप्स पर सीधे मैसेजेस भी शामिल हैं, ऐसी सामान्य वितरण विधियां हैं जिन्होंने साइबर अपराधियों के लिए प्रवेश की बाधा को घटा दिया है:
  - ईमेल में दुर्भावनापूर्ण फ़ाइलों को एटैच करने के बजाय आमतौर पर इन मैसेजेस में एक दुर्भावनापूर्ण लिंक होता है।
- **दुर्भावनापूर्ण खोज परिणाम**: सर्च इंजन ऑप्टिमाइज़ेशन (एसईओ) तकनीकों के माध्यम से वितरित किए जाते हैं, जो लक्ष्यों को वैध सॉफ़्टवेयर या अन्य सामग्री के रूप में छिपे हुए मैलवेयर वितरित करने वाली वेबसाइटों के प्रति निर्दिष्ट करते हैं
- **मैलवर्टाइज़िंग** : हानिकारक कोड का उपयोग, जिसे मैलवेयर वितरित करने के लिए वैध ऑनलाइन विज्ञापनों में इंजेक्ट किया जाता है
- **क्रैक्ड या पायरेटेड सॉफ़्टवेयर**: यूट्यूब वीडियो के माध्यम से साझा किए जाने वाले डाउनलोड्स (वीडियो गेम सहित), जिनमें वीडियो विवरण या कमेंट्स में दुर्भावनापूर्ण लिंक्स होते हैं, या जो अविश्वसनीय साइटों से डाउनलोड किए जाते हैं
- **सोशल मीडिया विज्ञापन और पोस्ट**: जो लक्ष्यों को छिपी हुई मैलवेयर फ़ाइलों के प्रति निर्दिष्ट करते हैं
- **दुर्भावनापूर्ण सॉफ़्टवेयर अपडेट्स**: आमतौर पर वेब ब्राउज़र अपडेट्स के रूप में छिपे हुए

चरण 3: डेटा हार्वेस्टिंग

एक बार जब कोई इंफो स्टीलर शिकार बनाए गए व्यक्ति के डिवाइस पर एक्ज़िक्यूट हो जाता है, तो यह संक्रमित मशीन से संवेदनशील डेटा एकत्र करना शुरू कर देता है। उपयोगकर्ता के क्रेडेंशियल्स चोरी करने के अलावा, ऐसे मामलों में जहां इंफो स्टीलर्स बॉटनेट्स का हिस्सा होते हैं, साइबर अपराधी अतिरिक्त क्षमताओं को सक्रिय करने या अन्य मैलवेयर वितरित करने के लिए कॉन्फ़िगरेशन कमांड भेजकर संक्रमित किए गए डिवाइस को दूरस्थ रूप से नियंत्रित कर सकते हैं। आमतौर पर इंफो स्टीलर्स इनकी चोरी करने में सक्षम होते हैं:

- उपयोगकर्ता नाम और पासवर्ड, विशेषकर जो वेब ब्राउज़र के मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए) उपयोगकर्ता सेशन / टोकन में स्टोर किए हुए हैं
- ऑथेंटिकेशन कुकीज़
- वेब ब्राउज़र ऑटोफ़िल फॉर्म जानकारी
- ईमेल क्रेडेंशियल्स, सामग्री और संपर्क
- वेब ब्राउज़िंग हिस्ट्री
- उपयोगकर्ता दस्तावेज़
- क्रेडिट कार्ड विवरण
- डेस्कटॉप मैसेजिंग ऐप्स से चैट लॉग्स
- सिस्टम जानकारी
- क्रिप्टोकरेंसी वॉलेट्स
- VPN या फ़ाइल ट्रांस्फर प्रोटोकॉल (FTP) क्रेडेंशियल्स।



चित्र 1. इंफो स्टीलर्स की क्षमता

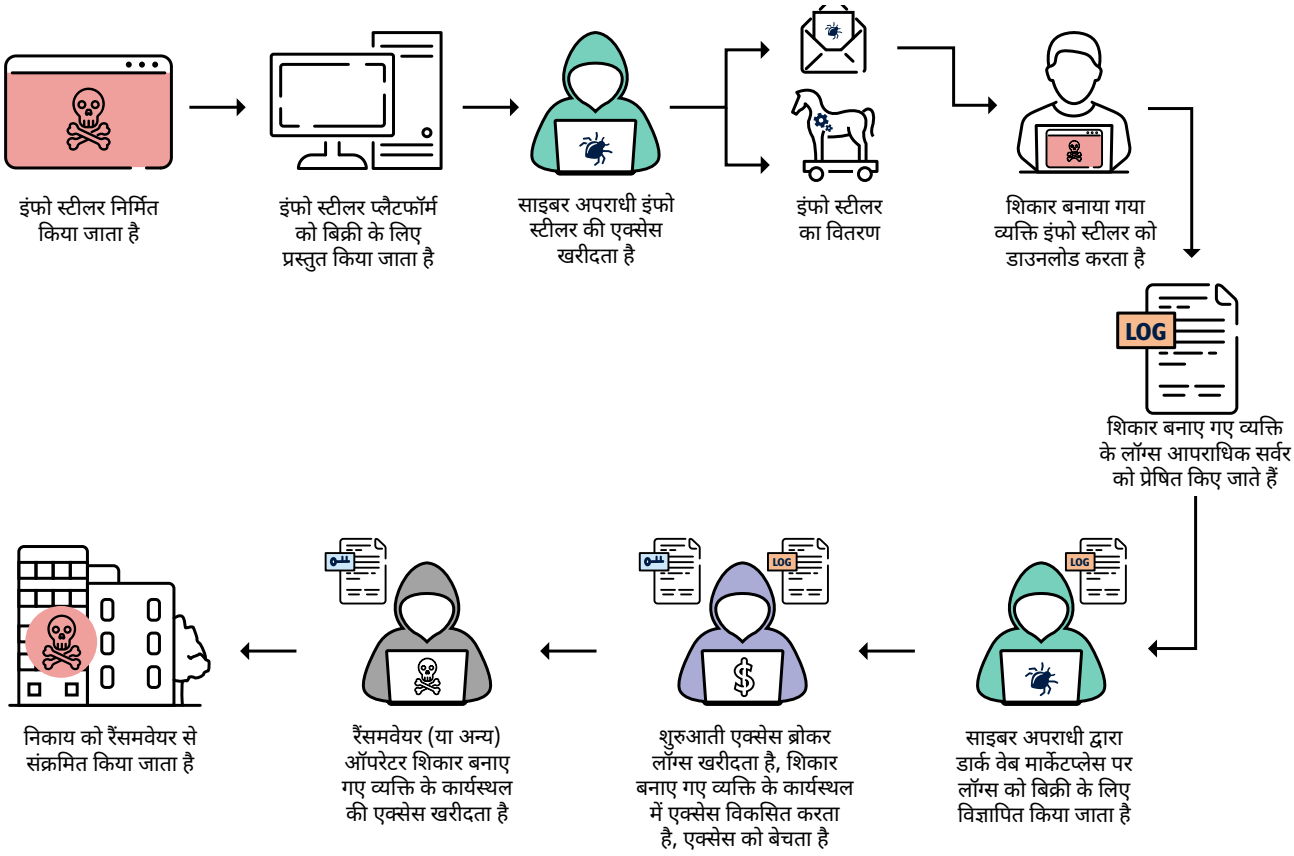
कुछ वेब ब्राउज़र ऑथेंटिकेशन कुकीज़ उपयोगकर्ता को एक समय में कई दिनों के लिए एक खाते या सेवा में लॉग इन करके रखती हैं, ताकि उपयोगकर्ताओं को पुन:प्रमाणित करने की आवश्यकता न हो। यदि चोरी हो जाती है, तो ये ऑथेंटिकेशन कुकीज़ एमएफए आवश्यकताओं को प्रभावी ढंग से बायपास कर सकती हैं और साइबर अपराधियों को शिकार बनाए गए व्यक्तियों के खातों, कॉर्पोरेट नेटवर्क्स और एंटरप्राइज़ सिस्टम्स की एक्सेस प्रदान कर सकती हैं।

चरण 4: डेटा एकत्रीकरण और मुद्रीकरण

इंफो स्टीलर्स को शिकार बनाए गए व्यक्ति की जानकारी को दुर्भावनापूर्ण कमांड-एंड-कंट्रोल सर्वर्स पर बाहर निकालने के लिए कॉन्फ़िगर किया जाता है, जिसे 'लॉग्स' के नाम से जाना जाता है। सामान्य तौर पर, इंफो स्टीलर्स साइबर अपराधियों के साथ लॉग्स की फ़ीड को साझा करने के लिए टेलीग्राम और डिस्कॉर्ड जैसी लोकप्रिय मैसेजिंग ऐप्स का लाभ उठाते हैं।

टेलीग्राम और पूरे डार्क वेब में लॉग्स की बिक्री और व्यापार के लिए विशेष मार्केटप्लेसेज़ मौजूद हैं। साइबर अपराधी अलग-अलग तरीकों से लॉग का मुद्रीकरण करते हैं, जिनमें शामिल हैं:

- आपराधिक मार्केटप्लेसेज़ पर लॉग्स को बेचना, जिसमें शुरुआती एक्सेस ब्रोकर्स भी शामिल हैं
- पहचान की चोरी और जबरन वसूली के माध्यम से शिकार बनाए गए व्यक्ति का सीधे शोषण करना
- रैंसमवेयर गतिविधि के उद्देश्य से कॉर्पोरेट नेटवर्क्स में शुरुआती एक्सेस के लिए जानकारी का लाभ उठाना।



चित्र 2. इंफो स्टीलर इकोसिस्टम और किसी संगठन पर संभावित प्रभाव

निहितार्थ

व्यक्ति-विशेषों और संगठनों, इन दोनों के लिए इंफो स्टीलर्स के गंभीर प्रभाव हो सकते हैं। यदि इंफो स्टीलर्स उपयोगकर्ता क्रेडेंशियल्स एकत्र करते हैं, तो साइबर अपराधी इन उपयोगकर्ता क्रेडेंशियल्स का उपयोग कॉर्पोरेट नेटवर्क्स या एंटरप्राइज़ सिस्टम्स को वैध उपयोगकर्ता खातों के माध्यम से एक्सेस करने के लिए कर सकते हैं, और अक्सर सिस्टम ओनर्स को इनका पता चलने में देरी होती है।

इंफो स्टीलर्स से प्रभावित होने वाले **संगठनों** के लिए परिणामों में शामिल हो सकते हैं:

- रैंसमवेयर
- डेटा उल्लंघन
- व्यावसायिक ईमेल संक्रमण
- बौद्धिक संपदा की चोरी
- संवेदनशील जानकारी की चोरी।

इंफो स्टीलर्स से प्रभावित होने वाले **व्यक्ति-विशेषों** के लिए परिणामों में शामिल हो सकते हैं:

- व्यक्तिगत ईमेल या सोशल मीडिया खातों की अनधिकृत एक्सेस
- पहचान की चोरी का संवृद्ध खतरा
- फ़िशिंग हमलों का संवृद्ध खतरा
- आर्थिक नुकसान या आर्थिक खातों की अनधिकृत एक्सेस
- गोपनीयता की हानि।

मामला अध्ययन

सार्वजनिक फैलाव को सक्षम करने के लिए इस मामला अध्ययन को गुमनाम बनाया गया है। यह ऑस्ट्रेलियाई संस्थाओं को प्रभावित करने वाली एकाधिक साइबर सुरक्षा घटनाओं पर आधारित है, जिन्हें एएसडी के एसीएससी के पास रिपोर्ट किया गया है। इसके बाद से प्रभावित इकाई को 'संगठन' के रूप में संदर्भित किया गया है। इस मामला अध्ययन में शामिल व्यक्ति-विशेषों के नाम काल्पनिक हैं और पीड़ितों की पहचान के संरक्षण के लिए विवरण हटा दिए गए हैं।

यह संगठन एक ऑस्ट्रेलियाई व्यवसाय है, जो कर्मचारियों को व्यक्तिगत डिवाइसेज़ से कॉर्पोरेट सिस्टम को एक्सेस करने की अनुमति देता है। ऐलिस इस संगठन की एक कर्मचारी है, जो दूरस्थ रूप से काम करती है।

घर से काम करते समय ऐलिस अपने निजी लैपटॉप का उपयोग करके अपने संगठन के कॉर्पोरेट नेटवर्क को दूरस्थ रूप से एक्सेस करती है। ऐलिस ने अपने **व्यक्तिगत लैपटॉप** पर नोटपैड++ का संस्करण (एक प्रकार का नोट-टेकिंग सॉफ़्टवेयर) ऐसी वेबसाइट से **डाउनलोड** किया, जिसे वह वैध मानती थी। इस नोटपैड++ सॉफ़्टवेयर के इंस्टॉलर के रूप में एक **इंफो स्टीलर** छिपा हुआ था।

जब ऐलिस ने सॉफ़्टवेयर इंस्टॉल करने का प्रयास किया, तो इंफो स्टीलर सक्रिय हो गया और उसने लैपटॉप से **उपयोगकर्ता क्रेडेंशियल्स** की हार्वेस्टिंग शुरू कर दी। इसमें उसके कार्यस्थल का उपयोगकर्ता नाम और पासवर्ड शामिल था, जिसे उसने अपने वेब ब्राउज़र के सेव्ड लॉगिन्स फीचर में सेव करके रखा था। इसके बाद इंफो स्टीलर ने उपयोगकर्ता क्रेडेंशियल्स को एक साइबर आपराध समूह द्वारा नियंत्रित किए जाने वाले रिमोट कमांड-एंड-कंट्रोल सर्वर पर भेज दिया।

चोरी किए गए लॉग्स को दूसरों के साथ पैक किया गया और फिर **एक डार्क वेब मार्केटप्लेस के माध्यम से इन्हें साइबर अपराधियों को बेच दिया गया**।

बॉब नाम के एक साइबर अपराधी ने ऐलिस के उपयोगकर्ता क्रेडेंशियल्स खरीद लिए, जिससे उसे ऐलिस के संगठन के नेटवर्क पर सेवाओं के लिए उपयोगकर्ता क्रेडेंशियल्स की पहचान मिल गई। ऐलिस के संगठन ने इन सेवाओं के लिए **एमएफए कॉन्फ़िगर नहीं किया था,** जिसका अर्थ था कि कॉर्पोरेट नेटवर्क पर सफलतापूर्वक ऑथेंटिकेट और एक्सेस करने के लिए बॉब इन चोरी किए गए उपयोगकर्ता क्रेडेंशियल्स को इस्तेमाल कर सकता था।

बॉब ने चोरी किए गए **वैध उपयोगकर्ता क्रेडेंशियल्स** के इस्तेमाल से ऐलिस के संगठन के कॉर्पोरेट नेटवर्क को बिना पकड़ में आए एक्सेस किया। बॉब कॉर्पोरेट नेटवर्क में समानांतर रूप से इधर-उधर देख पाने में सक्षम बन गया और उसने संगठन से संबंधित संवेदनशील डेटा की पहचान करके इसे कंपनी से बाहर निकाल लिया, ताकि वह जबरन वसूली कर सके।

संवेदनशील डेटा की चोरी करने के बाद, बॉब ने संगठन के **डेटाबेस और फाइल सिस्टम्स** को इनेक्सेसिबल बनाने के लिए इन्हें **एन्क्रिप्ट** कर दिया।

मिटिगेशन्स

यह संभव है कि संगठन अपने कॉर्पोरेट नेटवर्क से कनेक्ट होने वाले डिवाइसेज़ पर नियंत्रणों को लागू न कर पाएं, विशेषकर जो दूरस्थ रूप से काम करने वाले कर्मचारियों द्वारा उपयोग किए जाने वाले व्यक्तिगत डिवाइस होते हैं। एएसडी के एसीएससी ने संगठनों को नियंत्रण लागू करने पर ध्यान केंद्रित करने की सलाह दी है, ताकि वे उपयोगकर्ता क्रेडेंशियल्स को लक्षित करने वाले इंफो स्टीलर्स के जोखिम से खुद को सुरक्षित रख सकें। इन जोखिमों को कम करने के कदमों में शामिल हैं:

कर्मचारियों को साइबर सुरक्षा जागरुकता प्रशिक्षण उपलब्ध कराएँ

- कर्मचारियों को प्रभावी प्रशिक्षण देकर सफल लक्षित सोशल इंजीनियरिंग और दुर्भावनापूर्ण फ़ाइल डाउनलोड्स की रोकथाम करना।
- इंफो स्टीलर्स, उनके वितरण के तरीकों और अपने संगठन के लिए फ़िशिंग के खतरों के बारे में जागरुकता बढ़ाना।

कॉर्पोरेट खाते सुरक्षित करें

- एमएफए लागू करें
- बाहरी और आंतरिक सेवाओं, सिस्टम्स और संवेदनशील डेटा रिपॉज़िटरीज़ में एमएफए लागू करें, विशेषकर महत्वपूर्ण सिस्टम्स को एक्सेस करने वाली वेबमेल, वीपीएन और विशेषाधिकार प्राप्त उपयोगकर्ता खाते। सभी खातों के लिए फ़िशिंग-रोधी एमएफए लागू करना सबसे अच्छी कार्यप्रथा है।
- जब उपयोगकर्ता खातों की आवश्यकता न हो, तो उन्हें अक्षम कर दें।
- एडमिनिस्ट्रेटर विशेषाधिकारों को प्रतिबंधित करें:
- केवल एक समर्पित लॉक्ड-डाउन वर्कस्टेशन (यानि एक सुरक्षित एडमिनिस्ट्रेशन वर्कस्टेशन) के उपयोग से नेटवर्क एडमिनिस्ट्रेशन और अन्य विशेषाधिकार प्राप्त कार्य पूरे करें।
- गैर-एडमिनिस्ट्रेशन कार्यों के लिए सिस्टम्स और मानक उपयोगकर्ता खातों के प्रबंधन के उद्देश्य से विशेषाधिकार प्राप्त उपयोगकर्ता खातों का उपयोग आवश्यक बनाने के माध्यम से एडमिनिस्ट्रेटर्स के लिए निम्नतम-विशेषाधिकार सर्वोत्तम कार्यप्रथा का पालन करें।
- विशेषाधिकार प्राप्त उपयोगकर्ता खातों को इंटरनेट, ईमेल और वेब सेवाओं को एक्सेस करने से रोकें (ऑनलाइन सेवाओं की एक्सेस के लिए स्पष्टत: अधिकृत लोगों के अलावा)।
- सिस्टम्स और एप्लिकेशन्स के लिए जस्ट-इन-टाइम एडमिनिस्ट्रेशन लागू करने पर विचार करें।
- विशेषाधिकार प्राप्त उपयोगकर्ता खातों के लिए प्रबंधन और ऑडिटिंग लागू करें।
- समय-समय पर पासवर्डों को अपडेट करें, विशेषकर एक्सटर्नल-फेसिंग रिमोट-एक्सेस खातों के लिए।
- सेशन टोकन्स और कुकीज़ के लिए लाइफस्पैन टाइमआउट्स और सनसेट नीतियाँ लागू करें।

उद्यम में गतिमयता को सख्त बनाएँ

- उद्यम गतिमयता जोखिम आकलन करें और उद्यम गतिमयता को सख्त बनाने के लिए दिशानिर्देश लागू करें।
- यदि आप कर्मचारियों को काम के लिए व्यक्तिगत डिवाइसेज़ का इस्तेमाल करने की अनुमति देते/ती हैं, तो अपना खुद का डिवाइस लाएँ बीवाईओडी नीति लागू करें, क्योंकि कॉर्पोरेट रूप से प्रबंधित डिवाइसेज़ अप्रबंधित व्यक्तिगत डिवाइसेज़ की तुलना में अधिक सुरक्षित होते हैं।

अपने नेटवर्क्स को एक्सेस करने वाले विक्रेताओं की ओर से आपूर्ति श्रृंखला जोखिमों की समीक्षा और आकलन करें, जिनमें सॉफ़्टवेयर-एस-ए-सर्विस (Saas) विक्रेता और प्रबंधित सेवा प्रदाता शामिल हैं। किसी प्रबंधित सेवा प्रदाता को संलग्न करते समय अपनी सुरक्षा का प्रबंधन कैसे करें।

अपने कॉर्पोरेट नेटवर्क को सुरक्षित करें

- एप्लिकेशन्स और ऑपरेटिंग सिस्टम्स को अप टु डेट रखें।
- एप्लिकेशन्स नियंत्रण लागू करने के लिए सख्त अनुमति सूची के साथ स्थानीय सुरक्षा नीतियाँ लागू करें।
- भूमिका और कार्यात्मकता के आधार पर नेटवर्क सेगमेंट्स को अलग-अलग करने के लिए नेटवर्क सेगमेंटेशन लागू करें।
- उपयोगकर्ता गतिविधियों का ऑडिट और निगरानी करें, विशेषकर दूरस्थ कर्मचारियों के लिए।
- विशेषाधिकार प्राप्त खातों की निगरानी से संवेदनशील डेटा या असामान्य डेटा ट्रांस्फर गतिविधियों के लिए अनधिकृत एक्सेस प्रकट हो सकती है, जैसे किसी बाहरी नेटवर्क पर अपलोड किए गए डेटा की बड़ी मात्राएं।
- अनधिकृत डेटा ट्रांस्फर को रोकने के लिए डेटा-हानि रोकथाम नीतियाँ और संसाधन लागू करें।

एएसडी साइबर सिक्योरिटी नेटवर्क पार्टनर बनें और एएसडी की साइबर थ्रेट इंटेलिजेंस शेयरिंग (सीटीआईएस) सेवा में शामिल हों

- सीटीआईएस दो-तरफा साझाकरण प्लैटफॉर्म है, जो सरकार और उद्योग भागीदारों को दुर्भावनापूर्ण साइबर गतिविधि के बारे में जानकारी हासिल करने और इसे साझा करने में सक्षम बनाता है।
- एएसडी का एसीएससी इंफो स्टीलर गतिविधि पर नज़र रख रहा है और सीटीआईएस प्लेटफॉर्म के माध्यम से सक्रिय कमांड और कंट्रोल इंफ्रास्ट्रक्चर के विवरण साझा करता है।
- भागीदार बनने और अपने संगठन व ग्राहक डेटा को साइबर अपराध के खतरों से सुरक्षित रखने के लिए साइन अप करें।

हमले के लिए तैयार रहें

- एक इंफो स्टीलर हमला होने की स्थिति में उपयोग के लिए एक साइबर सुरक्षा घटना प्रतिक्रिया योजना विकसित करें। यदि कर्मचारियों को संदेह है कि उन्होंने कोई संदिग्ध फ़ाइल डाउनलोड की है, तो सुनिश्चित करें कि उन्हें पता रहे कि क्या करना है और किससे संपर्क करना है।

एएसडी के एसीएससी के अनिवार्य आठ लागू करें

- ऊपर वर्णित मिटिगेशन्स के अलावा, एएसडी का एसीएससी अपने बाकी के अनिवार्य आठ लागू करने की पुरजोर सलाह देता है।

आपके कर्मचारियों के लिए दूरस्थ काम करते समय सलाह

- अपने व्यक्तिगत डिवाइसेज़ पर अपनी जानकारी को सुरक्षित रखें
  - अच्छी साइबर स्वच्छता विकसित करें और संदिग्ध लिंक्स या पॉप-अप्स पर क्लिक न करें, अथवा अज्ञात या अविश्वसनीय स्रोतों से फ़ाइलें या सॉफ़्टवेयर डाउनलोड न करें।
  - कार्य और व्यक्तिगत खातों के लिए अलग-अलग पासवर्डों का उपयोग करें। जहां संभव हो, व्यक्तिगत खातों के लिए एमएफए का उपयोग करें।
  - अपने कार्यस्थल के क्रेडेंशियल्स को व्यक्तिगत पासवर्ड मैनेजर में तब तक स्टोर न करें, जब तक कि ऐसा करना आपके कार्य-नियोक्ता द्वारा स्पष्ट रूप से अनुमोदित न हो। इसमें आपके वेब ब्राउज़र का पासवर्ड मैनेजर शामिल है। **यदि संदेह हो, तो अपने कार्य-नियोक्ता से कॉर्पोरेट रूप से समर्थित पासवर्ड मैनेजर उपलब्ध कराने के लिए निवेदन करें।**
  - साझा किए जाने वाले या अन्य लोगों द्वारा इस्तेमाल किए जाने वाले कार्यस्थलों से अपने कार्य खातों में लॉग इन न करें।
  - आपके वेब ब्राउज़र की ऑटोफ़िल सुविधा में क्या स्टोर किया जा रहा है, इससे अवगत रहें। फ़ॉर्म्स को ऑटोफ़िल करने के लिए ब्राउज़र्स जो डेटा सेव करते हैं, इंफो स्टीलर्स उस डेटा को लक्षित करते हैं। वेब फ़ॉर्म्स भरते समय क्रेडिट कार्ड नंबर जैसे संवेदनशील डेटा को अपने वेब ब्राउज़र की ऑटोफ़िल सुविधा में सेव करने के बजाय इसे स्वयं एंटर करने के बारे में विचार करें।
  - इंफो स्टीलर्स के लिए उपलब्ध जानकारी घटाने के उद्देश्य से ब्राउज़िंग सेशन समाप्त होने के बाद सभी ऑनलाइन सेवाओं से लॉग आउट करें और वेब ब्राउज़र कुकीज़ को क्लियर करें।
  - यह सुनिश्चित करें कि आपके ऑपरेटिंग सिस्टम का अंतर्निहित एंटीवायरस सॉल्युशन एनेबल्ड है। यदि आप किसी तृतीय-पक्ष एंटीवायरस सॉल्युशन का उपयोग करते/ती हैं, तो यह सुनिश्चित करें इसे अप टु डेट रखा जाता है और यह किसी प्रतिष्ठित विक्रेता की ओर से है।

सहायता

किसी इंफो स्टीलर हमले से प्रभावित हुए या इसके संबंध में सहायता प्राप्त करने के इच्छुक ऑस्ट्रेलियाई संगठन **1300 CYBER1 (1300 292 371)** के माध्यम से या cyber.gov.au/report पर रिपोर्ट जमा करके एएसडी के एसीएससी से संपर्क कर सकते हैं।

एएसडी का एसीएससी निकायों को संदिग्ध नेटवर्क गतिविधि और इंफो स्टीलर्स से जुड़े हमले के संकेतकों की रिपोर्ट करने के लिए प्रोत्साहित करता है, भले ही किसी घटना को हल किया गया माना जाए। हम आपके द्वारा प्रदान की गई जानकारी को साइबर हमलावरों की चालबाजियों, तकनीकों और प्रक्रियाओं के बारे में अपनी समझ के बेहतरीकरण के लिए इस्तेमाल करते हैं, जिससे हमे इसी तरह से लक्षित किए गए अन्य ऑस्ट्रेलियाई संगठनों को चेतावनी देने में सहायता मिलती है।

अस्वीकरण

इस संदर्शिका में दी गई सामग्री सामान्य प्रकृति की है और इसे कानूनी सलाह के रूप में नहीं लिया जाना जाना चाहिए अथवा किसी विशेष परिस्थिति या आपात स्थिति में इसपर सहायता के लिए भरोसा नहीं किया जाना चाहिए। किसी भी महत्वपूर्ण मामले में आपको अपनी परिस्थितियों के संबंध में उपयुक्त स्वतंत्र पेशेवर सलाह लेनी चाहिए।

इस संदर्शिका में निहित जानकारी पर निर्भरता के परिणामस्वरूप होने वाले किसी भी क्षति, हानि या खर्चे के लिए राष्ट्रमंडल कोई भी जिम्मेदारी या दायित्व को स्वीकार नहीं करता है।

और अधिक जानकारी या किसी साइबर सिक्योरिटी घटना की रिपोर्ट करने के लिए हमसे संपर्क करें:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

यह नंबर केवल ऑस्ट्रेलिया में उपयोग के लिए उपलब्ध है।

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre