APT40 परामर्श-सूचना

पीआरसी एमएसएस ट्रेडक्राफ्ट के काम करने का तरीके

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

विषय-सूची

अवलोकन

पृष्ठभूमि

यह परामर्श सूचना, जिसका लेखन इन एजेंसियों ने किया है: ऑस्ट्रेलियाई सिग्नल निदेशालय के ऑस्ट्रेलियाई साइबर सुरक्षा केंद्र (एएसडी के एसीएससी), संयुक्त राज्य साइबर सुरक्षा एवं इंफ्रास्ट्रक्चर सुरक्षा एजेंसी (सीआईएसए), संयुक्त राज्य अमेरिका की राष्ट्रीय सुरक्षा एजेंसी (एनएसए), संयुक्त राज्य संघीय जाँच ब्यूरो (एफबीआई), यूनाइटेड किंगडम राष्ट्रीय साइबर सुरक्षा केंद्र (एनसीएससी-यूके), कनाडाई साइबर सुरक्षा केंद्र (सीसीसीएस), न्यू ज़ीलैंड राष्ट्रीय साइबर सुरक्षा केंद्र (एनसीएससी-एनजेड), जर्मन संघीय खुफिया सेवा (बीएनडी) और संविधान संरक्षण संघीय कार्यालय (बीएफवी), कोरिया गणराज्य की राष्ट्रीय खुफिया सेवा (एनआईएस) और एनआईएस के राष्ट्रीय साइबर सुरक्षा केंद्र, और जापान के राष्ट्रीय साइबर सुरक्षा घटना तत्परता एवं रणनीति केंद्र (एनआईएससी) और राष्ट्रीय पुलिस एजेंसी (एनपीए) – जिन्हें इसके बाद "लेखन एजेंसियों" के रूप में संदर्भित किया जाएगा - पीपल्स रिपब्लिक ऑफ चाइना (पीआरसी) के राज्य-प्रायोजित साइबर समूह को और ऑस्ट्रेलियाई नेटवर्क के लिए उनके वर्तमान खतरे को रेखांकित करती है। यह परामर्श-सूचना संलेखन एजेंसियों की खतरे की साझा समझ के साथ-साथ एएसडी की एसीएससी घटना प्रतिक्रिया जाँचों पर आधारित है।

पीआरसी के राज्य-प्रायोजित साइबर समूह ने पहले ऑस्ट्रेलिया और संयुक्त राज्य अमेरिका समेत कई देशों में स्थित संगठनों को लक्षित किया है, और अन्य पीआरसी राज्य-प्रायोजित हमलावरों द्वारा विश्व-स्तर पर नीचे दी गई तकनीकों का नियमित उपयोग किया जाता है। इसलिए संलेखन एजेंसियों का मानना है कि यह समूह, और इसी तरह की तकनीकें उनके देशों के नेटवर्कों के लिए भी खतरा बनी हुई हैं।

संलेखन एजेंसियों का आकलन है कि यह समूह पीआरसी मिनिस्ट्री ऑफ स्टेट सिक्योरिटी (एमएसएस) के लिए दुर्भावनापूर्ण साइबर ऑपरेशन्स चलाता है। इसकी गतिविधि और तकनीकें एडवांस्ड पर्सिस्टेंट थ्रेट (APT) 40 के रूप में ट्रैक किए गए समूहों के साथ ओवरलैप होती है (जिसे उद्योग रिपोर्टिंग में क्रिप्टोनाइट पांडा, गिंगहम टाइफून, लेविएथन और ब्रॉन्ज़ मोहॉक के नाम से भी जाना जाता है)। इस समूह के बारे में रिपोर्ट किया गया है कि यह पहले हाइकू, हैनान प्रांत, पीआरसी में स्थित था और इसे पहले हैनान प्रांत के सुरक्षा विभाग, पीआरसी एमएसएस से काम दिया जाता था।[2] निम्नलिखित परामर्श-सूचना इस विरोधी द्वारा शिकार बनाए गए दो नेटवर्कों के प्रति कार्रवाई की तकनीकों के महत्वपूर्ण मामले के अध्ययन का एक नमूना प्रदान करती है। इन मामला अध्ययनों के परिणाम साइबर सुरक्षा पेशेवरों के लिए महत्वपूर्ण हैं, ताकि वे अपने खुद के नेटवर्कों में APT40 के हस्तक्षेप की पहचान, रोकथाम और उपचार कर सकें। चुने हुए मामले अध्ययनों में इस धमकीपूर्ण हमलावर, या किसी अन्य के द्वारा फिर से दुरुपयोग के जोखिम को कम करने के लिए उपयुक्त उपचार लागू किया गया है। इस तरह से ये मामले अध्ययन स्वाभाविक रूप से पुरानी प्रकृति के हैं, ताकि यह सुनिश्चित हो सके कि संगठनों को उपचार के लिए आवश्यक समय दिया गया था।

गतिविधि सारांश

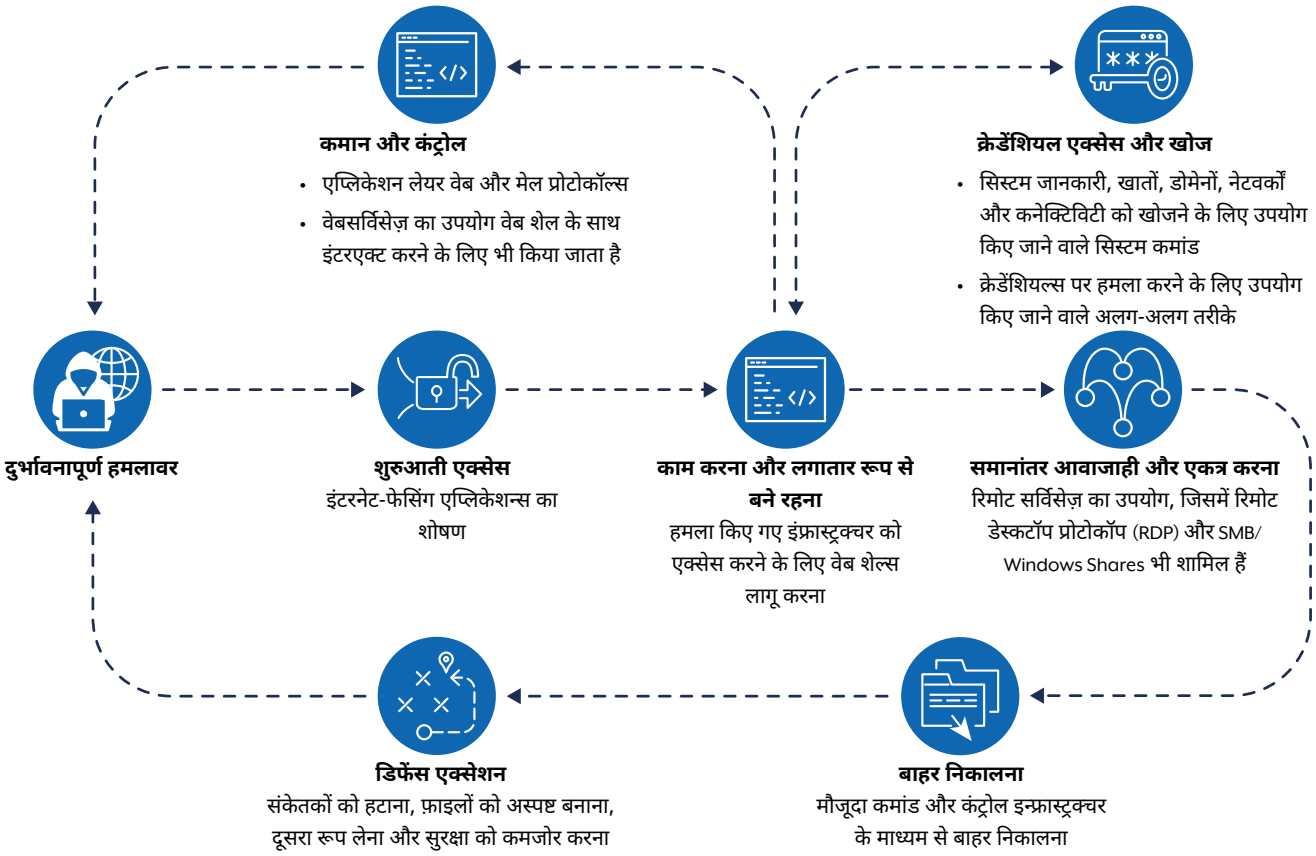
APT40 ने बार-बार ऑस्ट्रेलियाई नेटवर्कों, तथा साथ ही इस क्षेत्र में सरकारी और निजी सेक्टर के नेटवर्कों को भी लक्षित किया है, और ये हमारे नेटवर्क के लिए जारी खतरा बने हुए हैं। इस परामर्श-सूचना में वर्णित ट्रेडक्राफ्ट को नियमित रूप से ऑस्ट्रेलियाई नेटवर्कों के प्रति देखा जाता है।

विशेषकर APT40 में नई कमजोरियों के प्रूफ-ऑफ-कॉन्सेप्ट (पीओसी) का तेजी से रूपांतरण और अनुकूलन करने की क्षमता है और इससे संबंधित कमजोरियों वाले इंफ्रास्ट्रक्चर को लक्ष्य नेटवर्कों के प्रति तुरंत इस्तेमाल किया जा सकता है। APT40 नियमित रूप से अभिरुचि के नेटवर्कों की टोह लगाता है और अपने लक्ष्यों पर हमला करने के अवसरों की तलाश करता है, जिसमें संलेखन एजेंसियों के देशों में स्थित नेटवर्क भी शामिल हैं। यह नियमित टोही इस समूह के लिए अभिरुचि के नेटवर्कों पर कमजोर, जीवन-के-अंत या ठीक से बनाए न रखे जाने वाले डिवाइसेज़ की पहचान करना और शोषणों को तेजी से लागू करना आसान बना देती है। APT40 को 2017 की शुरुआत से ही कमजोरियों का फायदा उठाने में सफलता मिल रही है।

APT40 व्यापक रूप से उपयोग किए जाने वाले सॉफ़्टवेयर का त्वरित शोषण करता है, जैसे Log4J (CVE 2021 44228), एटलैस्सियन कॉन्फ्लुएँस (CVE-2021-31207, CVE-2021-26084) और माइक्रोसॉफ़्ट एक्सचेंज (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473)। एएसडी की एसीएससी और संलेखन एजेंसियों को उम्मीद है कि यह समूह सार्वजनिक रिलीज़ होने के बाद कुछ ही घंटों या दिनों के अंदर नई हाई-प्रोफ़ाइल कमजोरियों के लिए पीओसी का उपयोग करना जारी रखेगा।

2 अमेरिकी न्याय विभाग। 2021. चार चीनी नागरिकों पर, जो राजकीय सुरक्षा मंत्रालय के साथ काम कर रहे थे, संक्रामक रोग अनुसंधान सहित बौद्धिक संपदा और गोपनीय व्यावसायिक जानकारी को लक्षित करने वाले वैश्विक कंप्यूटर हस्तक्षेप अभियान का आरोप लगाया गया।

चित्र 1. APT40 गतिविधि के लिए TTP फ़्लोचार्ट



ऐसा प्रतीत होता है कि यह समूह उन तकनीकों पर कमजोर, पब्लिक-फेसिंग इंफ्रास्ट्रक्चर का शोषण करना पसंद करता है, जिनके लिए उपयोगकर्ता इंटरएक्शन की आवश्यकता होती है - जैसे फ़िशिंग अभियान, और यह अनेकानेक फॉलो-अप गतिविधियों को सक्षम बनाने के लिए वैध क्रेडेंशियल्स प्राप्त करने को ऊँची प्राथमिकता देता है। APT40 लगातार रूप से बने रहने के लिए नियमित रूप से वेब शेल (T1505.003) का उपयोग करता है, विशेषकर हस्तक्षेप के जीवन चक्र की शुरुआत में। आमतौर पर, शुरुआत में सफलतापूर्वक एक्सेस करने के बाद APT40 शिकार के परिवेश में एक्सेस बनाए रखने के लिए लगातार रूप से बने रहने पर फोकस करता है। चूंकि लगातार रूप से बने रहने की प्रकृति हस्तक्षेप के आरंभिक समय में पैदा होती है, इसलिए सभी हस्तक्षेपों में इसके पहचान में आने की संभावना अधिक है - चाहे हमले की सीमा या आगे के कार्य कुछ भी हों।

उल्लेखनीय ट्रेडक्राफ्ट

APT40 ने पूर्व में हमला की गई ऑस्ट्रेलियाई वेबसाइटों को अपने ऑपरेशन्स के लिए कमांड और कंट्रोल (C2) होस्ट के रूप में इस्तेमाल किया है, फिर भी समूह ने इस तकनीक का क्रमिक विकास किया है (T1594)।

APT40 ने ऑस्ट्रेलिया में अपने ऑपरेशन्स के लिए ऑपरेशनल इंफ्रास्ट्रक्चर और लास्ट-हॉप रिडायरेक्टर्स (T1584.008) के रूप में संक्रमित डिवाइसेज़ का उपयोग करने की वैश्विक प्रवृत्ति अपनाई है, जिसमें छोटे-कार्यालय/गृह-कार्यालय (SOHO) डिवाइसेज़ भी शामिल हैं। इसने संलेखन एजेंसियों को इस समूह की गतिविधियों को बेहतर ढंग से चिह्नित करने और इसका अनुरेखण करने में सक्षम बनाया है।

इनमें से कई SOHO डिवाइसेज़ अपने जीवन-के-अंत में हैं या अनपैच्ड हैं और ये एन-डे शोषण के लिए एक आसान लक्ष्य उपलब्ध कराते हैं। एक बार संक्रमित हो जाने के बाद SOHO डिवाइसेज़ हमलों के लिए एक लॉन्चिंग पॉइंट प्रदान करते हैं, जिसे वैध ट्रैफ़िक के साथ घुलने-मिलने और नेटवर्क डिफेंडर्स को चुनौती देने के लिए डिज़ाइन किया जाता है (T1001.003)।

पीआरसी के अन्य राज्य-प्रायोजित हमलावरों द्वारा इस तकनीक का उपयोग दुनिया-भर में नियमित रूप से भी किया जाता है, और संलेखन एजेंसियाँ इसे एक साझा खतरा मानती हैं। अतिरिक्त जानकारी के लिए संयुक्त परामर्श-सूचनाएँ देखें: पीपल्स रिपब्लिक ऑफ चाइना के राज्य-प्रायोजित साइबर हमलावर नेटवर्क प्रदाताओं और डिवाइसेज़ का दुरुपयोग करते हैं और पीआरसी के राज्य-प्रायोजित हमलावर यू.एस. के अतिमहत्वपूर्ण इन्फ्रास्ट्रक्चर पर हमला करते हैं और लगातार एक्सेस बनाए रखते हैं।

APT40 कभी-कभी अपने ऑपरेशन्स में विक्टिम-फेसिंग C2 इंफ्रास्ट्रक्चर के रूप में खरीदे गए या कॉन्ट्रैक्ट पर दिए गए इंफ्रास्ट्रक्चर का उपयोग करता है; किंतु इस ट्रेडक्राफ्ट में सापेक्ष रूप से गिरावट प्रतीत होती है।

टूलिंग

एएसडी का एसीएससी नीचे रेखांकित जाँचों के दौरान पहचान में आई कुछ दुर्भावनापूर्ण फ़ाइलों को साझा कर रहा है। इन फ़ाइलों को VirusTotal पर अपलोड किया गया है, ताकि व्यापक नेटवर्क सुरक्षा और साइबर सुरक्षा समुदायों को उन खतरों को बेहतर ढंग से समझ पाने में सक्षम बनाया जा सके, जिनसे उन्हें बचाव करने की आवश्यकता है।

मामले अध्ययन

एएसडी का एसीएससी दो अज्ञात जाँच रिपोर्टें साझा कर रहा है, ताकि इस बारे में जागरुकता बनाई जा सके कि हमलावर अपने डिवाइसेज़ और ट्रेडक्राफ्ट को कैसे नियोजित करते हैं।

MD5	फ़ाइलनेम	अतिरिक्त जानकारी
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | जावा सोर्स
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | जावा बाइटकोड
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | जावा बाइटकोड
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | जावा सोर्स
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | जावा बाइटकोड
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | जावा बाइटकोड
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | जावा बाइटकोड
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | जावा बाइटकोड
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | जावा बाइटकोड
e02be0dc614523dddd7a28c9e9d500cff	Nova_jsp.java	15 kB | जावा सोर्स

मामला अध्ययन 1

व्यापक फैलाव को सक्षम बनाने के लिए इस रिपोर्ट में से नाम हटा दिए गए हैं। प्रभावित संगठन को इसके बाद 'संगठन' के रूप में संदर्भित किया जाएगा। शिकार की पहचान और एएसडी के एसीएससी की घटना प्रतिक्रिया विधियों की सुरक्षा के लिए कुछ विशिष्ट विवरण हटा दिए गए हैं।

कार्यकारी सारांश

यह रिपोर्ट जुलाई और सितंबर 2022 के बीच संगठन के नेटवर्कों के सफल हमले में एएसडी के एसीएससी की जाँच के निष्कर्षों के विवरण देती है। यह खोजी रिपोर्ट दुर्भावनापूर्ण गतिविधि को सारांशित करने और उपचारात्मक सलाहों का ढांचा बनाने के लिए प्रदान की गई थी। निष्कर्षों से संकेत मिलता है कि हमला APT40 द्वारा किया गया था।

अगस्त के मध्य में, एएसडी के एसीएससी ने अगस्त के अंत में समूह द्वारा उपयोग किए जा रहे संभावित रूप से संक्रमित डिवाइस से संगठन के नेटवर्कों के साथ दुर्भावनापूर्ण इंटरएक्शन के बारे में संगठन को सूचित किया और संगठन की सहमति के साथ, एएसडी के एसीएससी ने संगठन के नेटवर्कों पर संभावित प्रभावित होस्ट्स के लिए होस्ट-आधारित सेंसर लागू किए। इन सेंसरों ने एएसडी के एसीएससी घटना प्रतिक्रिया विश्लेषकों को पूरी तरह से डिजिटल फोरेंसिक जाँच करने की अनुमति दी। एएसडी के एसीएससी विश्लेषकों ने उपलब्ध सेंसर डेटा का उपयोग करते हुए समूह की गतिविधि को सफलतापूर्वक मैप किया और देखी गई घटनाओं की एक विस्तृत समयरेखा बनाई।

एएसडी के एसीएससी द्वारा जुलाई से अगस्त तक देखी गई प्रमुख हमलावर गतिविधि में शामिल हैं:

- होस्ट एन्युमरेशन, जो हमलावर को नेटवर्कों का अपना नक्शा बनाने में सक्षम करता है;
- वेब शेल का उपयोग, जो हमलावर को नेटवर्कों पर शुरुआती रूप से पैर जमाने और कमांड्स चलाने की क्षमता प्रदान करता है; और
- दुर्भावनापूर्ण उद्देश्यों के लिए हमलावर द्वारा उपयोग किए गए अन्य टूलिंग का लागूकरण।

जाँच में बड़ी मात्रा में संवेदनशील डेटा को एक्सेस किए जाने का पता चला और इस बात का सबूत मौजूद है कि हमलावरों ने नेटवर्कों में समानांतर रूप से आवाजाही की (T1021.002)। हमला अधिकांशत: नेटवर्कों में समूह द्वारा एक्सेस वेक्टर्स स्थापित करने, सपाट संरचना वाला नेटवर्क होने और असुरक्षित आंतरिक रूप से विकसित सॉफ़्टवेयर के उपयोग से सुविधाकृत हुआ था, जिसे मनमाने ढंग से फ़ाइलें अपलोड करने के लिए इस्तेमाल किया जा सकता था। बाहर निकाले गए डेटा में प्रिविलेज-प्राप्त ऑथेंटिकेशन क्रेडेंशियल्स शामिल थे जो समूह को लॉग इन करने में सक्षम बनाते थे, और साथ ही इसमें नेटवर्क के बारे में जानकारी भी शामिल थी, जो मूल एक्सेस वेक्टर के अवरुद्ध होने की स्थिति में हमलावरों को अनधिकृत एक्सेस प्राप्त करने की अनुमति देती थी। शुरू में शोषित मशीन पर उन लोगों से परे कोई अतिरिक्त दुर्भावनापूर्ण टूलिंग की पहचान नहीं हो पाई थी; लेकिन किसी समूह की वैध और प्रिविलेज-प्राप्त क्रेडेंशियल्स की एक्सेस अतिरिक्त टूलिंग की आवश्यकता नकार देती है। जाँच के निष्कर्षों से संकेत मिलता है कि संगठन के सार्वजनिक रूप से ज्ञात कमजोरियों के अवसरवादी रूप से शिकार बनने के बजाय उसे संभवत: APT40 द्वारा जानबूझकर लक्षित किया गया था।

जाँच के निष्कर्ष

अगस्त 2022 के मध्य में, एएसडी के एसीएससी ने संगठन को सूचित किया कि एक राज्य-प्रायोजित साइबर समूह से संबद्ध पुष्टि किए गए दुर्भावनापूर्ण आईपी ने कम से कम जुलाई और अगस्त के बीच संगठन के कंप्यूटर नेटवर्कों के साथ इंटरएक्शन किया था। हमला किया गया डिवाइस शायद एक छोटे व्यवसाय या घरेलू उपयोगकर्ता का था।

अगस्त के अंत में, एएसडी के एसीएससी ने संगठन के नेटवर्कों पर होस्ट्स के लिए एक होस्ट-आधारित एजेंट लागू किया, जिससे हमले से प्रभावित होने का सबूत प्रदर्शित हुआ।

जाँच के प्रयासों को समर्थन दे सकने वाली कुछ चीजें लॉगिंग या नेटवर्क डिज़ाइन के कॉन्फ़िगरेशन के कारण उपलब्ध नहीं थीं। इसके बावजूद भी सभी उपलब्ध डेटा प्रदान करने की संगठन की तत्परता ने एएसडी के एसीएससी के घटना उत्तरदाताओं को व्यापक विश्लेषण करने और नेटवर्कों पर संभावित APT40 गतिविधि को समझ पाने में सक्षम बनाया।

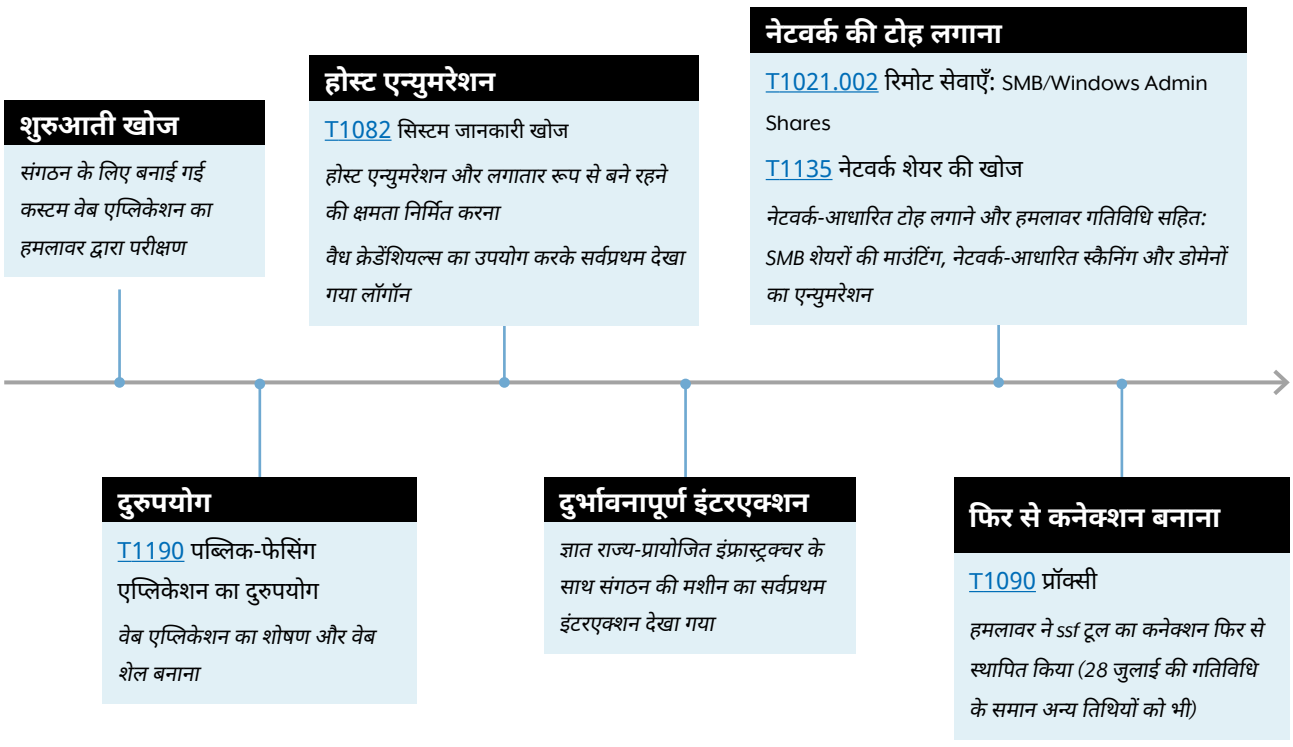
सितंबर में, एएसडी के एसीएससी से परामर्श के बाद संगठन ने शुरुआती अधिसूचना में पहचाने गए आईपी को अस्वीकार करने का निर्णय लिया। अक्टूबर में, संगठन ने यह उपचार शुरू किया।

विवरण

जुलाई की शुरुआत में हमलावर `<webapp>2-ext` पर चलने वाली एक कस्टम वेब एप्लिकेशन (T1190) का परीक्षण और शोषण करने में सक्षम थे, जो समूह को नेटवर्क डिमिलिटरीकृत ज़ोन (DMZ) में पैर जमाने में सक्षम बनाता है। इसे नेटवर्कों के साथ-साथ सभी दृश्यमान डोमेनों, इन दोनों का एन्युमरेशन करने के लिए लिवरेज किया गया था। संक्रमित क्रेडेंशियल्स (T1078.002) का उपयोग एक्टिव डायरेक्टरी (T1018) को क्वेरी करने और DMZ के अंदर एकाधिक मशीनों से फ़ाइल शेयर्स (T1039) को माउंट करके डेटा को बाहर निकालने के लिए किया गया था। हमलावर ने सर्वर से वैध नेटवर्क क्रेडेंशियल प्राप्त करने के लिए एक केर्बेरोस्टिंग हमला किया (T1558.003)। समूह को DMZ या आंतरिक नेटवर्कों में उपस्थिति के कोई भी अतिरिक्त बिंदु प्राप्त करते हुए नहीं देखा गया था।

दृश्य समयरेखा

नीचे दी गई समयरेखा संगठन के नेटवर्कों पर देखी गई दुर्भावनापूर्ण हमलावर गतिविधि के प्रमुख चरणों का व्यापक अवलोकन प्रदान करती है।



विस्तृत समयरेखा

जुलाई: हमलावरों ने संगठन के लिए निर्मित कस्टम वेब एप्लिकेशन (T1190) के फ्रंट पेज पर ट्रांसपोर्ट लेयर सिक्योरिटी (TLS) कनेक्शन (T1102) के माध्यम से एक शुरुआती कनेक्शन स्थापित किया (जिसे इसके बाद 'वेब एप्लिकेशन' या '*webapp*' के रूप में संदर्भित किया जाएगा)। कोई अन्य उल्लेखनीय गतिविधि नहीं देखी गई।

जुलाई: हमलावर आगे जाँच करने के लिए एँडपॉइंट्स की तलाश में वेब एप्लिकेशन की वेबसाइट का एन्युमरेशन शुरू करते हैं।[2]

जुलाई: हमलावर एक विशिष्ट एँडपॉइंट का दुरुपयोग करने के प्रयासों पर फोकस करते हैं।

जुलाई: हमलावर वेब सर्वर पर सफलतापूर्वक पोस्ट करने में सक्षम होते हैं, शायद किसी अन्य पृष्ठ पर मौजूद वेब शेल के माध्यम से। एक अन्य आईपी को संभवतः उन्हीं हमलावरों द्वारा इस्तेमाल किया जाता है। वह भी उसी यूआरएल पर पोस्ट करना शुरू कर देता है। हमलावरों ने कई संभावित वेब शेल बनाए और उनका परीक्षण किया।

दुरुपयोग का सटीक तरीका अज्ञात है, लेकिन यह स्पष्ट है कि विशिष्ट एँडपॉइंट को `<webapp>2-ext` पर फ़ाइलें बनाने के लिए लक्षित किया गया था।

एएसडी के एसीएससी का मानना है कि दो आईपी पते कनेक्शन्स अपने साझा हित और शुरुआती कनेक्शन के कारण एक ही हस्तक्षेप के हिस्सा थे।

जुलाई: समूह होस्ट एन्युमरेशन करना जारी रखता है, प्रिविलेज एस्केलेशन के अवसरों की तलाश करता है, और एक अलग वेब शेल लागू करता है। हमलावर `<firstname.surname>@<organisation domain>` के संक्रमित क्रेडेंशियल्स का उपयोग करके वेब एप्लिकेशन में लॉग इन करते हैं।

हमलावरों की गतिविधि `<webapp>2-ext` पर सफलतापूर्वक प्रिविलेज एस्केलेशन हासिल करने के लिए प्रकट नहीं होती है। इसके बजाय हमलावरों ने नेटवर्क-आधारित गतिविधि की ओर रुख किया।

जुलाई: हमलावर एक सेवा खाते के लिए संक्रमित क्रेडेंशियल्स का परीक्षण करता है,[3] जिसे संभवतः आंतरिक रूप से सुलभ बायनेरीज़ में हार्डकोड किया गया पाया गया।

जुलाई: हमलावर ओपन-सोर्स टूल सिक्योर सॉकेट फ़नलिंग लागू करते हैं, जिसे दुर्भावनापूर्ण इंफ्रास्ट्रक्चर से कनेक्ट आउट करने के लिए इस्तेमाल किया गया था। इस कनेक्शन का उपयोग हमलावर की हमला करने वाली मशीनों से संगठन के आंतरिक नेटवर्कों में ट्रैफ़िक की टनलिंग के लिए किया जाता है। इनके मशीन नेम्स इवेंट लॉग में उजागर होते हैं, जब वे सेवा खाते के लिए क्रेडेंशियल्स का उपयोग करने का प्रयास करते हैं।

अगस्त: हमलावरों को सीमित मात्रा में गतिविधि करते हुए देखा जाता है, जिसमें सेवा खाते से जुड़े कनेक्शन्स स्थापित न कर पाना शामिल है।

अगस्त: हमलावर महत्वपूर्ण नेटवर्कों और एक्टिव डायरेक्टरी का एन्युमरेशन करते हैं।[4] इसके बाद एक अन्य संक्रमित खाते को DMZ के अंदर विंडोज़ मशीनों पर शेयर्स की माउंटिंग के लिए इस्तेमाल किया जाता है, जिससे सफलता के साथ डेटा को बाहर निकालना एनेबल हो जाता है।

यह DMZ में माउंटेबल मशीनों पर चोरी किए गए क्रेडेंशियल का अवसरवादी उपयोग प्रतीत होता है। फ़ायरवॉल ने हमलावर को इसी गतिविधि के साथ आंतरिक नेटवर्कों को लक्षित करने से अवरुद्ध कर दिया।

अगस्त - सितंबर: SSF टूल ने एक दुर्भावनापूर्ण IP से कनेक्शन को फिर से स्थापित किया। समूह को तब तक कोई अतिरिक्त गतिविधि करते हुए नहीं देखा जाता है, जब तक कि उनकी एक्सेस अवरुद्ध नहीं हो जाती है।

सितंबर: संगठन दुर्भावनापूर्ण आईपी को अपने फ़ायरवॉल पर लिस्ट करने से मना करके ब्लॉक कर देता है।

2 इस संदर्भ में, एँडपॉइंट एक वेब एप्लिकेशन का फंक्शन है

3 सेवा खाते व्यक्तिगत उपयोगकर्ताओं से बंधे हुए नहीं हैं, बल्कि ये सेवाओं से जुड़े हैं। माइक्रोसॉफ़्ट कॉर्पोरेट डोमेन में अलग-अलग तरह के खाते होते हैं।

4 शेयर्स को माउंट करना एक उपयोगकर्ता या उपयोगकर्ता समूह के लिए सुलभ फ़ाइल सिस्टम स्ट्रक्चर पर फ़ाइलें निर्मित करने की प्रक्रिया है।

हमलावर की चालबाजियाँ और तकनीकें

MITRE ATT&CK फ्रेमवर्क साइबरस्पेस में हमलावरों द्वारा इस्तेमाल की जाने वाली चालबाजियों और तकनीकों का एक प्रलेखित संग्रह है। यह ढांचा अमेरिका के गैर-लाभकारी संगठन MITRE कॉर्पोरेशन द्वारा बनाया गया था और यह धमकी देने वाले हमलावरों के व्यवहार के इर्द-गिर्द एक सामान्य वैश्विक भाषा के रूप में काम करता है।

एएसडी का एसीएससी हमलावर की दुर्भावनापूर्ण गतिविधि के साथ प्रासंगिक होने के लिए निम्नलिखित तकनीकों और चालबाजियों का आकलन करता है:

टोह लगाना

T1594 – शिकार के स्वामित्व वाली वेबसाइटों की खोज करना

हमलावर ने नेटवर्कों को एक्सेस करने के अवसरों की पहचान के लिए कस्टम वेब एप्लिकेशन की वेबसाइट का एन्युमरेशन किया।

शुरुआती एक्सेस

T1190 – पब्लिक-फेसिंग एप्लिकेशन का दुरुपयोग (कस्टम वेब एप्लिकेशन के दुरुपयोग के संबंध में)

T1078.002 – मान्य खाते: डोमेन खाते (संक्रमित क्रेडेंशियल्स के साथ लॉग ऑन करने के संबंध में)

इंटरनेट पर उजागर कस्टम वेब एप्लिकेशन्स का दुरुपयोग हमलावर के लिए एक्सेस का एक शुरुआती बिंदु प्रदान करता है। बाद में हमलावर उन क्रेडेंशियल्स का उपयोग करने में सक्षम था, जिन्हें उसने नेटवर्कों में अपनी एक्सेस को आगे बढ़ाने के लिए संक्रमित किया था।

काम करना

T1059 – कमांड और स्क्रिप्टिंग इंटरप्रेटर (वेब शेल के माध्यम से कमांड के काम करने के संबंध में)

T1072 – सॉफ़्टवेयर लागूकरण टूल्स (हमलावर द्वारा ओपन-सोर्स टूल सिक्योर सॉकेट फ़नललिंग (SSF) का उपयोग करके आईपी से कनेक्ट करने के बारे में)

लगातार रूप से बने रहना

T1505.003 – सर्वर सॉफ़्टवेयर घटक: वेब शेल (एक्सेस स्थापित करने के लिए वेब शेल और SSF के उपयोग के संबंध में)

क्रेडेंशियल एक्सेस

T1552.001 – पासवर्ड स्टोर्स से क्रेडेंशियल्स (बिल्डिंग मैनेजमेंट सिस्टम (BMS) से संबंधित पासवर्ड फ़ाइलों के संबंध में)

T1558.003 – चोरी या जाली Kerberos टिकट: Kerberoasting (नेटवर्कों क्रेडेंशियल्स हासिल करने के लिए हमले के संबंध में)

समानांतर आवाजाही

T1021.002 – रिमोट सेवाएँ: SMB शेयर्स (हमलावर द्वारा कई डिवाइसेज़ से SMB शेयर्स को माउंट करने के संबंध में)

एकत्र करना

T1213 – सूचना रिपॉज़िटरीज़ से डेटा (BMS सर्वर पर पाए जाने वाले मैन्युअल्स/दस्तावेजों के संबंध में)

बाहर निकालना

T1041 – C2 चैनल पर बाहर निकालना (एक्टिव डायरेक्टरी और बढ़ते शेयरों से हमलावर के डेटा को बाहर निकालने के संबंध में)

मामला अध्ययन 2

व्यापक फैलाव सक्षम बनाने के लिए इस रिपोर्ट में से नाम हटा दिए गए हैं। प्रभावित संगठन को इसके बाद 'संगठन' के रूप में संदर्भित किया जाता है। शिकार की पहचान और एएसडी के एसीएससी की घटना प्रतिक्रिया विधियों के संरक्षण के लिए कुछ विशिष्ट विवरण हटा दिए गए हैं।

कार्यकारी सारांश

इस रिपोर्ट में अप्रैल 2022 में संगठन के नेटवर्कों के सफल हमले में एएसडी की एसीएससी जाँच के निष्कर्षों का विवरण दिया गया है। यह खोजी रिपोर्ट देखी गई दुर्भावनापूर्ण गतिविधि को सारांशित करने और उपचारात्मक सलाह का ढांचा बनाने के लिए संगठन को प्रदान की गई थी। निष्कर्षों से संकेत मिलता है कि हमला APT40 द्वारा किया गया था।

मई 2022 में, एएसडी के एसीएससी ने एक संगठन के नेटवर्कों को अप्रैल 2022 से प्रभावित करने वाली संदिग्ध दुर्भावनापूर्ण गतिविधि के बारे में संगठन को सूचित किया। इसके बाद, संगठन ने एएसडी के एसीएससी को सूचित किया कि उन्होंने एक इंटरनेट-फेसिंग सर्वर पर दुर्भावनापूर्ण सॉफ़्टवेयर की खोज की है, जो संगठन के कॉर्पोरेट रिमोट एक्सेस समाधान के लिए लॉगिन पोर्टल प्रदान करता है। इस सर्वर ने रिमोट एक्सेस लॉगिन और पहचान प्रबंधन उत्पाद का उपयोग किया और इस रिपोर्ट में इसे 'संक्रमित डिवाइस' के रूप में संदर्भित किया जाएगा। यह रिपोर्ट एएसडी के एसीएससी द्वारा की गई जाँच के उत्तर में संगठन के लिए विकसित किए गए जाँच निष्कर्षों और उपचार सलाह का विवरण देती है।

साक्ष्य से संकेत मिला कि संगठन के नेटवर्कों के हिस्से पर दुर्भावनापूर्ण साइबर हमलावर(रों) द्वारा कम से कम अप्रैल 2022 से संगठन के रिमोट एक्सेस लॉगिन पोर्टल के माध्यम से हमला किया गया था। यह सर्वर एकाधिक हमलावरों द्वारा संक्रमित किया गया हो सकता है, और यह संभवतः रिमोट कोड एक्ज़िक्यूशन (RCE) कमजोरियों से प्रभावित था, जिनके बारे में हमला होने के समय व्यापक रूप से प्रचार किया गया था।

एएसडी के एसीएससी द्वारा देखी गई प्रमुख हमलावर गतिविधि में शामिल हैं:

- होस्ट एन्युमरेशन, जो किसी हमलावर को नेटवर्कों का अपना नक्शा बनाने में सक्षम करता है;
- इंटरनेट-फेसिंग एप्लिकेशन्स और वेब शेल उपयोग का दुरुपयोग, जो हमलावर को नेटवर्कों पर शुरुआती पैर जमाने और कमांड्स चलाने की क्षमता प्रदान करता है;
- प्रिविलेजेस को बढ़ाने के लिए सॉफ़्टवेयर कमजोरियों का दुरुपयोग; और
- समानांतर आवाजाही को सक्षम बनाने के लिए क्रेडेंशियल का संग्रह

एएसडी के एसीएससी ने पाया कि एक दुर्भावनापूर्ण हमलावर ने अप्रैल 2022 में हमला किए गए डिवाइसेज़ पर कई सौ अनन्य उपयोगकर्ता नामों और पासवर्ड जोड़ों के साथ-साथ रिमोट एक्सेस सेशन्स से संबंधित कई मल्टी-फैक्टर ऑथेंटिकेशन कोड्स और तकनीकी आर्टिफैक्ट्स को बाहर निकाल दिया था। संगठन द्वारा समीक्षा करने पर पासवर्ड वैध पाए गए। एएसडी के एसीएससी का आकलन है कि हमलावर ने इन तकनीकी आर्टिफैक्ट्स को एक वैध उपयोगकर्ता के रूप में रिमोट लॉगिन सेशन को हाइजैक करने के उद्देश्य से एक नया सेशन बनाने के लिए एकत्र किया हो सकता है, और एक वैध उपयोगकर्ता खाते के इस्तेमाल से संगठन के आंतरिक कॉर्पोरेट नेटवर्कों को एक्सेस किया हो सकता है।

जाँच के निष्कर्ष

जाँच सारांश

एएसडी के एसीएससी ने पता लगाया कि हमलावर ने संगठन के कर्मचारियों के लिए रिमोट लॉगिन सेशन्स प्रदान करने वाले डिवाइस(सों) पर हमला किया, और फिर आगे की गतिविधि करने के प्रयास में इस हमले का उपयोग किया। इन डिवाइसेज़ में तीन लोड-बैलेंस्ड होस्ट्स होते हैं, जहां हमले के सबसे शुरुआती सबूत का पता चला था। संगठन ने शुरुआती हमले के तुरंत बाद तीन लोड-बैलेंस्ड होस्ट्स में से दो को बंद कर दिया। इसके परिणामस्वरूप बाद की सभी गतिविधियाँ एक ही होस्ट पर घटित हुई। संक्रमित डिवाइस से जुड़े अन्य सर्वर भी इसी तरह से लोड-बैलेंस्ड थे। सुगमता के लिए इस रिपोर्ट में अधिकांश संक्रमित डिवाइसेज़ को 'सिंगल डिवाइस' के रूप में संदर्भित किया गया है।

ऐसा माना जाता है कि हमलावर ने अप्रैल 2022 के बाद हमला किए गए डिवाइस में वेब शेल चलाने के लिए सार्वजनिक रूप से ज्ञात कमजोरियों का उपयोग किया। समूह के धमकीपूर्ण हमलावरों के लिए यह आकलन किया जाता है कि उन्होंने डिवाइस पर प्रिविलेज प्राप्त किए। एएसडी का एसीएससी लॉगिंग उपलब्धता की कमी के कारण गतिविधि की संपूर्ण सीमा नियत नहीं कर सका। किंतु डिवाइस पर मौजूद सबूत इंगित करता है कि एक हमलावर ने यह हासिल कर लिया:

- कई सौ वास्तविक उपयोगकर्ता नामों और पासवर्ड जोड़ों को एकत्र करना; और
- ऐसी तकनीकी आर्टिफैक्ट्स को एकत्र करना, जिन्होंने दुर्भावनापूर्ण हमलावर को एक वैध उपयोगकर्ता के रूप में वर्चुअल डेस्कटॉप इन्फ्रास्ट्रक्चर (VDI) सेशन एक्सेस करने की अनुमति दी हो सकती है।

एएसडी के एसीएससी का आकलन है कि हमलावर संगठन के नेटवर्कों के संक्रमण को आगे बढ़ाने का इच्छुक रहा होगा। हमलावर द्वारा बाहर निकाली गई आर्टिफैक्ट्स ने उन्हें एक वैध उपयोगकर्ता के रूप में वर्चुअल डेस्कटॉप सेशन्स को हाईजैक करने या शुरू करने की अनुमति दी हो सकती है, संभवत: उनकी पसंद के उपयोगकर्ता के रूप में, जिसमें एडमिनिस्ट्रेटर्स भी शामिल हैं। हमलावर ने लगातार रूप से बने रहने और अन्य लक्ष्य प्राप्त करने के उद्देश्य से संगठन की सेवाओं पर हमला करने के लिए इस एक्सेस वेक्टर का उपयोग किया हो सकता है।

होस्टिंग प्रदाता के प्रबंधित परिवेश के अंदर संगठन के अन्य डिवाइसेज़ पर हमले का सबूत प्रदर्शित नहीं हुआ।

एक्सेस

संक्रमित डिवाइस वाले होस्ट ने VDI सेशन्स से कनेक्ट होने वाले उपयोगकर्ताओं के लिए एक्टिव डायरेक्टरी और एक वेबसर्वर के माध्यम से ऑथेंटिकेशन किया (T1021.001)।

स्थान	संक्रमित डिवाइस के होस्टनेम्स (लोड-बैलेंस्ड)
डेटासेंटर 1	HOST1, HOST2, HOST3

डिवाइस के इंफ्रास्ट्रक्चर में एक्सेस गेटवे होस्ट भी शामिल थे, जो डिवाइस से जेनरेट और डाउनलोड किया गया ऑथेंटिकेशन टोकन हासिल करने के बाद उपयोगकर्ता को VDI के लिए एक टनल प्रदान करते थे।

इनमें से किसी भी होस्ट के संक्रमित होने का कोई सबूत नहीं था। किंतु एक्सेस गेटवे होस्ट लॉग्स ने इस बात का प्रमाण प्रदर्शित किया कि ज्ञात दुर्भावनापूर्ण IP पतों के साथ काफी अधिक इंटरएक्शन्स हुए थे। संभावित है कि यह इस होस्ट पर हुई गतिविधि या खतरापूर्ण हमलावर के इंफ्रास्ट्रक्चर के साथ नेटवर्क कनेक्शन्स का प्रतिबिंबन करता है, जिनसे होस्ट तक पहुंच स्थापित हुई थी। इस गतिविधि की प्रकृति को उपलब्ध साक्ष्य का उपयोग करके नियत नहीं किया जा सकता है, लेकिन यह इंगित करती है कि समूह संगठन के नेटवर्कों (TA0008) में समानांतर आवाजाही करने का इच्छुक था।

आंतरिक होस्ट्स

एएसडी के एसीएससी ने आंतरिक संगठन के नेटवर्क सेगमेंट से सीमित डेटा की जाँच की। आंतरिक संगठन के नेटवर्क सेगमेंट को प्रभावित करने के ज्ञात प्रयास या सफल दुर्भावनापूर्ण गतिविधि में शामिल हैं - VDI से संबंधित आर्टिफैक्ट्स में हमलावर की एक्सेस, आंतरिक SQL सर्वर (T1505.001) की स्क्रेपिंग, और एक्सेस गेटवे डिवाइसेज़ (TA0011) के माध्यम से ज्ञात दुर्भावनापूर्ण IP पतों से निर्गत होने वाला अस्पष्टीकृत ट्रैफ़िक।

संक्रमित डिवाइस में एक्सेस का उपयोग करके समूह ने वास्तविक उपयोगकर्ता नाम, पासवर्ड्स (T1003), और MFA टोकन वैल्यूज़ (T1111) एकत्र की। समूह ने JSON वेब टोकन को (JWTs) (T1528) भी एकत्र किया, जो वर्चुअल डेस्कटॉप लॉगिन सेशन बनाने के लिए इस्तेमाल किया जाने वाला एक ऑथेंटिकेशन आर्टिफैक्ट है। इस बात की संभावना है कि हमलावर एक वर्चुअल डेस्कटॉप सेशन (T1563.002) बनाने या हाईजैक करने के लिए इनका उपयोग करने, और एक वैध उपयोगकर्ता के रूप में

आंतरिक संगठन नेटवर्क सेगमेंट को एक्सेस करने में सक्षम हुआ हो (T1078)।

हमलावर ने संगठन के आंतरिक नेटवर्क में मौजूद एक SQL सर्वर (T1505.001) को स्क्रेप करने के लिए भी संक्रमित डिवाइस में एक्सेस का उपयोग किया। यह संभव है कि हमलावर के पास इस डेटा की एक्सेस थी।

एक्सेस गेटवे डिवाइस से उपलब्ध साक्ष्य से पता चला है कि ज्ञात दुर्भावनापूर्ण आईपी पते से या इस डिवाइस के माध्यम से नेटवर्क ट्रैफ़िक की आवाजाही हुई थी। जैसा कि ऊपर वर्णित है, इससे यह संकेत मिल सकता है कि दुर्भावनापूर्ण साइबर हमलावरों ने संभवत: आंतरिक नेटवर्क में घुसने के लिए इस डिवाइस को प्रभावित या इसका उपयोग किया हो।

जाँच की समयरेखा

नीचे दी गई सूची जाँच के दौरान खोजी गई प्रमुख गतिविधियों की समयरेखा प्रदान करती है।

समय	घटना
अप्रैल 2022	ज्ञात दुर्भावनापूर्ण आईपी पते एक्सेस गेटवे होस्ट HOST7 के साथ इंटरएक्ट करते हैं। इंटरएक्शन की प्रकृति निर्धारित नहीं की जा सकी।
अप्रैल 2022	सभी होस्ट्स, HOST1, HOST2 और HOST3, एक दुर्भावनापूर्ण हमलावर या हमलावरों द्वारा संक्रमित किए गए थे, और होस्ट्स पर वेब शेल्स लगाए गए थे। HOST2 पर एक लॉग फ़ाइल बनाई या संशोधित की गई थी। इस फ़ाइल में ऐसी क्रेडेंशियल सामग्री है, जो संभवत: एक दुर्भावनापूर्ण हमलावर द्वारा कैप्चर की गई है। /etc/security/opasswd और /etc/shadow फ़ाइलों को HOST1 और HOST3 पर संशोधित किया गया था, जो यह दर्शाता है कि पासवर्ड बदल दिए गए थे। HOST1 पर उपलब्ध साक्ष्य बताते हैं कि उपयोगकर्ता 'sshuser' के लिए पासवर्ड बदल दिया गया था।
अप्रैल 2022	HOST2 को संगठन द्वारा बंद कर दिया गया था। HOST1 और HOST3 पर अतिरिक्त वेब शेल्स (T1505.003) बनाए गए थे। HOST1 को HOST3 से SSH ब्रूट फोर्स प्रयासों का अनुभव हुआ। HOST3 पर एक लॉग फ़ाइल (T1070) संशोधित की गई थी। इस फ़ाइल में ऐसी क्रेडेंशियल सामग्री (T1078) है, जो संभवत: किसी दुर्भावनापूर्ण हमलावर द्वारा कैप्चर की गई है। JWTs को कैप्चर किया गया (T1528) और HOST3 पर एक फ़ाइल में आउटपुट किया गया। HOST3 को संगठन द्वारा बंद कर दिया गया था। इस समय के बाद सभी गतिविधियाँ HOST1 पर होती हैं।
अप्रैल 2022	HOST1 (T1505.003) पर अतिरिक्त वेब शेल्स बनाए गए। JWTs कैप्चर किए गए और HOST1 पर एक फ़ाइल में इन्हें आउटपुट किया गया।
अप्रैल 2022	HOST1 (T1505.003) पर अतिरिक्त वेब शेल्स बनाए जाते हैं, और एक ज्ञात दुर्भावनापूर्ण आईपी पता होस्ट (TA0011) के साथ इंटरएक्ट करता है। एक ज्ञात दुर्भावनापूर्ण आईपी पता एक्सेस गेटवे होस्ट HOST7 के साथ इंटरएक्ट करता है।
मई 2022	एक ज्ञात दुर्भावनापूर्ण आईपी पता एक्सेस गेटवे होस्ट HOST7 (TA0011) के साथ इंटरएक्ट करता है। उपयोगकर्ता के एक ऑथेंटिकेशन प्रकरण को HOST1 पर मौजूद लॉग्स में ज्ञात दुर्भावनापूर्ण आईपी पते से जोड़ा जाता है। इस होस्ट पर एक अतिरिक्त वेब शेल बनाया जाता है (T1505.003)।
मई 2022	HOST1 पर मौजूद एक स्क्रिप्ट को एक हमलावर (T1543) द्वारा संशोधित किया गया। इस स्क्रिप्ट में आंतरिक SQL सर्वर से डेटा को स्क्रैप करने की फंक्शनैलिटी थी।
मई 2022	HOST1 पर एक अतिरिक्त लॉग फ़ाइल अंतिम बार संशोधित की गई (T1070)। इस फ़ाइल में संगठन नेटवर्क के लिए उपयोगकर्ता नाम और पासवर्ड जोड़े मौजूद हैं, जिन्हें वैध माना जाता है (T1078)।
मई 2022	एक अतिरिक्त लॉग फ़ाइल अंतिम बार संशोधित की गई (T1070)। इस फ़ाइल में HOST1 से एकत्रित JWTs हैं।
मई 2022	HOST1 (T1505.003) पर अतिरिक्त वेब शेल्स बनाए गए। इस तिथि को संगठन ने अप्रैल 2022 में निर्माण तिथि वाली एक वेब शेल की खोज की सूचना एएसडी के एसीएससी को दी।
मई 2022	HOST1 पर कई स्क्रिप्ट्स बनाई गईं, जिनमें से एक का नाम Log4jHotPatch.jar था।
मई 2022	एक्सेस गेटवे होस्ट में दो ओपन पोर्ट जोड़ने के लिए iptables-save कमांड का उपयोग किया गया। ये पोर्ट 9998 और 9999 (T1572) थे।

हमलावर की चालबाजियाँ और तकनीकें

जाँच के दौरान पहचानी गई कई चालबाजियाँ और तकनीकें नीचे दी गई हैं।

शुरुआती एक्सेस

T1190 पब्लिक-फेसिंग एप्लिकेशन का दुरुपयोग करना

समूह ने नेटवर्क में शुरुआती एक्सेस हासिल करने के लिए रिमोट एक्सेस लॉगिन और पहचान प्रबंधन उत्पाद में RCE, प्रिविलेज एस्केलेशन्स और ऑथेंटिकेशन बाईपास कमजोरियों का दुरुपयोग किया।

निम्नलिखित के कारण शुरुआती एक्सेस के इस तरीके को सबसे अधिक संभावित माना जाता है:

- उस समय सर्वर इन CVE के प्रति कमजोर था;
- ज्ञात हमलावर इंफ्रास्ट्रक्चर की ओर से इन कमजोरियों का फायदा उठाने की कोशिशें; और
- दुरुपयोग के प्रयास किए जाने के तुरंत बाद पहली ज्ञात आंतरिक दुर्भावनापूर्ण गतिविधि हुई।

काम करना

T1059.004 कमांड और स्क्रिप्टिंग इंटरप्रेटर: यूनिक्स शेल

समूह ने उपरोक्त कमजोरियों का सफलतापूर्वक दुरुपयोग किया, और संभव है कि वह प्रभावित डिवाइस पर उपलब्ध यूनिक्स शेल में कमांड्स चलाने में सक्षम हुआ हो। हमलावरों द्वारा चलाई गई कमांड्स का पूरा विवरण नहीं दिया जा सकता है, क्योंकि इन्हें डिवाइस द्वारा लॉग नहीं किया गया था।

लगातार रूप से बने रहना

T1505.003 सर्वर सॉफ़्टवेयर घटक: वेब शेल

हमलावरों ने प्रभावित डिवाइस पर कई वेब शेल्स लागू किए। यह संभव है कि कई अलग-अलग हमलावरों ने वेब शेल्स लागू किए होंगे, लेकिन केवल कुछ ही हमलावरों ने इन वेब शेल्स को इस्तेमाल करके गतिविधि की। हमलावर द्वारा मनमाने ढंग से कमांड देकर वेब शेल्स ने संक्रमित डिवाइसेज़ पर काम करने की अनुमति दी होगी।

प्रिविलेज एस्केलेशन

T1068 प्रिविलेज एस्केलेशन के लिए दुरुपयोग

उपलब्ध साक्ष्य हमलावरों द्वारा प्राप्त प्रिविलेज के स्तर का वर्णन नहीं करते हैं। किंतु हमलावरों ने वेब शेल्स के उपयोग से संक्रमित डिवाइस पर वेब सर्वर की तुलना में प्रिविलेज का एक स्तर हासिल किया होगा। माना जाता है कि संक्रमित डिवाइस पर मौजूद कमजोरियों ने हमलावरों को रूट प्रिविलेजेस हासिल करने की अनुमति दी होगी।

क्रेडेंशियल एक्सेस

T1056.003 इनपुट कैप्चर: वेब पोर्टल कैप्चर

संक्रमित डिवाइस पर साक्ष्य से पता चला है कि हमलावर ने स्पष्ट टेक्स्ट में कई सौ वैध माने जाने वाले उपयोगकर्ता नाम-पासवर्ड जोड़ों को कैप्चर कर लिया था। यह संभावित है कि इन्हें वास्तविक ऑथेंटिकेशन प्रक्रिया में कुछ संशोधन का उपयोग करके कैप्चर किया गया था, जोकि किसी फ़ाइल में क्रेडेंशियल्स को आउटपुट करता है।

T1111 मल्टी-फैक्टर ऑथेंटिकेशन इंटरसेप्शन

हमलावर ने वैध लॉगिन के अनुरूप MFA टोकन्स की वैल्यू को भी कैप्चर कर लिया। इन वैल्यूज़ को किसी फ़ाइल में आउटपुट करने के लिए वास्तविक ऑथेंटिकेशन प्रक्रिया को संशोधित करके इन्हें कैप्चर किया गया था। 'सीक्रेट सर्वर' में संक्रमण होने का कोई सबूत नहीं है ,जो MFA टोकन्स की सुरक्षा के लिए उपलब्ध कराए जाने वाले अनन्य मानों को स्टोर करता है।

T1040 नेटवर्क स्निफिंग

माना जाता है कि हमलावर ने संक्रमित डिवाइस पर HTTP ट्रैफ़िक को कैप्चर करके JWTs को कैप्चर किया था। इस बात के सबूत मौजूद हैं कि यूटिलिटी tcpdump को संक्रमित डिवाइस पर एक्ज़िक्यूट किया गया था, और हो सकता है कि हमलावर ने इस प्रकार से इन JWTs को कैप्चर किया हो।

T1539 वेब सेशन कुकी की चोरी करना

जैसा कि ऊपर वर्णित है, हमलावर ने JWTs को कैप्चर कर लिया, जो वेब सेशन कुकीज़ के समरूप हैं। आगे की एक्सेस प्राप्त करने के लिए हमलावर द्वारा इनका पुन: उपयोग किया जा सकता था।

खोज

T1046 नेटवर्क सेवा की खोज

इस बात के प्रमाण मौजूद हैं कि संक्रमित डिवाइस पर नेटवर्क स्कैनिंग यूटिलिटी nmap को एक्ज़िक्यूट किया गया था, ताकि उसी नेटवर्क सेगमेंट में अन्य डिवाइसेज़ को स्कैन किया जा सके। संभवत: हमलावर द्वारा इसका इस्तेमाल एक्सेस करने योग्य अन्य नेटवर्क सेवाओं की खोज के लिए किया गया था, जो समानांतर आवाजाही के अवसर प्रस्तुत कर सकती हैं।

एकत्र करना

उपलब्ध साक्ष्य यह नहीं बताते हैं कि हमलावरों ने डेटा को कैसे एकत्र किया था या फिर संक्रमित डिवाइस या अन्य सिस्टम्स से वास्तव में क्या एकत्र किया गया था। किंतु इस बात की संभावना है कि हमलावरों के पास संक्रमित डिवाइस पर सभी फ़ाइलों की एक्सेस थी, जिसमें कैप्चर किए गए क्रेडेंशियल्स (T1003), MFA टोकन वैल्यूज़ (T1111), और ऊपर वर्णित JWTs शामिल हैं।

कमांड और कंट्रोल

T1071.001 एप्लिकेशन लेयर प्रोटोकॉल: वेब प्रोटोकॉल्स

हमलावरों ने कमांड और कंट्रोल के लिए वेब शेल्स का इस्तेमाल किया। वेब शेल कमांड्स को डिवाइस (T1572) पर मौजूदा वेब सर्वर का उपयोग करके HTTPS पर पारित किया गया होगा।

T1001.003 डेटा को अस्पष्ट बनाना: प्रोटोकॉल का प्रतिरूपण

हमलावरों ने वैध ट्रैफ़िक के साथ घुलने-मिलने के उद्देश्य से डिज़ाइन किए गए हमलों के लिए लॉन्चिंग पॉइंट के रूप में संक्रमित डिवाइसेज़ का उपयोग किया।

खोज करने और मिटिगेशन के लिए सलाह

एएसडी का एसीएससी पुरजोर सलाह देता है कि एएसडी के अनिवार्य आठ कंट्रोल्स और संबद्ध साइबर सुरक्षा घटनाओं को मिटिगेट करने के लिए रणनीतियाँ लागू किए जाएँ। APT40 के हस्तक्षेपों की खोज करने और इनकी रोकथाम के लिए नेटवर्क सुरक्षा कार्रवाइयों की सलाह नीचे दी गई है, और इसके बाद तालिका 1 में चार प्रमुख TTPs के लिए संक्षेप में जोखिम कम करने के लिए कदम दिए गए हैं।

खोज

ऊपर पहचानी गई कुछ फ़ाइलों को C:\Users\Public* और C:\Windows\Temp* जैसे स्थानों में छोड़ दिया गया था। ये स्थान डेटा लिखने के लिए सुविधाजनक स्थान हो सकते हैं, क्योंकि ये आमतौर पर वर्ल्ड राइटेबल होते हैं, यानि विंडोज़ में रजिस्टर्ड सभी उपयोगकर्ता खातों के पास इन डायरेक्टरीज़ और उनकी सबडायरेक्टरीज़ की एक्सेस उपलब्ध होती है। अक्सर, बाद में कोई भी उपयोगकर्ता इन फ़ाइलों को एक्सेस सकता है, जिससे समानांतर आवाजाही, सुरक्षा से बचाव, लो-प्रिविलेज एक्ज़िक्यूशन और बाहर निकालने के लिए स्टेजिंग के अवसर मिलते हैं।

निम्नलिखित सिग्मा नियम विषम गतिविधि के संकेतक के रूप में संदिग्ध स्थलों से काम किए जाने की खोज करते हैं। सभी मामलों में दुर्भावनापूर्ण गतिविधि और एट्रिब्यूशन की पुष्टि के लिए बाद में जाँच की आवश्यकता होती है।

शीर्षक: वर्ल्ड राइटेबल एक्ज़िक्यूशन – TEMP

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

विवरण: C:\Windows\Temp से प्रक्रिया काम करना का पता लगाएँ।

पृष्ठभूमि:

यह नियम विशेषकर C:\Windows\Temp* से एक्ज़िक्यूशन के लिए ध्यान रखता है। TEMP का इस्तेमाल अधिक व्यापक रूप से सौम्य एप्लिकेशन्स द्वारा किया जाता है और इस प्रकार से यह C:\Windows में अन्य वर्ल्ड राइटेबल सबडायरेक्टरीज़ से एक्ज़िक्यूशन किए जाने की तुलना में निम्नतर विश्वास का दुर्भावनापूर्ण संकेतक है।

सिस्टम या नेटवर्क सर्विस उपयोगकर्ताओं द्वारा एक्ज़िक्यूट की गई एप्लिकेशन्स को हटाने से इस नियम द्वारा चयनित सौम्य गतिविधि की मात्रा काफी कम हो जाती है।

इसका अर्थ है कि नियम ऊँचे प्रिविलेज स्तर पर दुर्भावनापूर्ण एक्ज़िक्यूशन्स से चूक सकता है, लेकिन इस बात का पता लगाने के लिए अन्य नियमों का उपयोग करने की सलाह दी जाती है कि क्या उपयोगकर्ता सिस्टम के लिए प्रिविलेजेस को बढ़ाने का प्रयास कर रहा है।

जाँच:

1. इस फ़ाइल के एक्ज़िक्यूशन से सीधे संबद्ध जानकारी की जाँच करें, जैसे उपयोगकर्ता संदर्भ, एक्ज़िक्यूशन इंटेग्रिटी स्तर, तत्काल फॉलो-ऑन गतिविधि और फ़ाइल द्वारा लोड की गई इमेजेस।
2. प्रासंगिक प्रक्रिया, नेटवर्क, फ़ाइल और होस्ट पर मौजूद अन्य समर्थनकारी डेटा की जाँच करें, ताकि इस बात का आकलन करने में सहायता मिल सके कि गतिविधि दुर्भावनापूर्ण है या नहीं।
3. यदि आवश्यक हो, तो रिवर्स इंजीनियरिंग के लिए फ़ाइल की एक कॉपी एकत्र करने का प्रयास करें, ताकि नियत किया जा सके कि क्या यह वैध है।

संदर्भ:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

लेखक: एएसडी के एसीएससी

तिथि: 2024/06/19

स्टैटस: प्रयोगात्मक

टैग्स:

- tlp.green
- classification.au.official
- attack.execution

लॉग सोर्स:

```
category: process_creation
product: windows
```

खोज:

```
temp:
    Image|startswith: 'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase: 'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
system_user:
    User:
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

```
dismhost:
    Image|endswith: 'dismhost.exe'
known_parent:
    ParentImage|endswith:
    - '\\esif_uf.exe'
    - '\\vmtoolsd.exe'
    - '\\cwainstaller.exe'
    - '\\trolleyexpress.exe'
condition: temp and not (common_temp_path or system_user or dismhost or known_parent)
```

असत्य सकारात्मक:

- Allowlist ऑडिटिंग एप्लिकेशन्स को Temp से एक्ज़िक्यूटेबल्स चलाते हुए देखा गया है।
- Temp वैध रूप से सेटअप एप्लिकेशन्स और लॉन्चर्स का एक एरे शामिल करेगा, इसलिए यह विचार करने योग्य होगा कि इस नियम को लागू करने से पहले यह व्यवहार ऐसे किसी नेटवर्क पर कितना प्रचलित है, जिसकी निगरानी की जाती है (और क्या इसे allowlisted किया जा सकता है या नहीं)।

स्तर: low

शीर्षक: World Writable Execution - Non-Temp System Subdirectory

आईडी: 5b187157-e892-4fc9-84fc-aa48aff9f997

विवरण: Windows OS इंस्टॉल स्थान की एक सबडायरेक्टरी में एक वर्ल्ड राइटेबल स्थान से प्रक्रिया के एक्ज़िक्यूशन का पता लगाएँ।

पृष्ठभूमि:

यह नियम विशेषकर C:\, और खासकर C:\Windows* के अंदर वर्ल्ड राइटेबल डायरेक्टरीज़ से एक्ज़िक्यूशन के लिए दिखता है, जिसमें C:\Windows\Temp के लिए अपवाद है (इसका उपयोग अधिक व्यापक रूप से सौम्य एप्लिकेशन्स द्वारा किया जाता है और इस प्रकार से यह निम्नतर विश्वास का दुर्भावनापूर्ण संकेतक है)।

यदि कोई फ़ाइल SYSTEM के रूप में चलाई जाती है, तो AppData फ़ोल्डर्स को बाहर रखा जाता है - यह एक सौम्य तरीका है, जिसमें कई अस्थायी एप्लिकेशन फ़ाइलें एक्ज़िक्यूट की जाती हैं।

शुरुआती नेटवर्क बेसलाइन को पूरा करने और इन स्थानों से ज्ञात सौम्य एक्ज़िक्यूशन्स की पहचान करने के बाद यह नियम शायद ही कभी गलती करेगा।

जाँच:

1. इस फ़ाइल एक्ज़िक्यूशन से सीधे संबद्ध जानकारी की जाँच करें, जैसे उपयोगकर्ता संदर्भ, एक्ज़िक्यूशन इंटेग्रिटी स्तर, तत्काल फॉलो-ऑन गतिविधि और फ़ाइल द्वारा लोड की गई इमेजेस।
2. प्रासंगिक प्रक्रिया, नेटवर्क, फ़ाइल और होस्ट पर मौजूद अन्य समर्थनकारी डेटा की जाँच करें, ताकि इस बात का आकलन करने में सहायता मिल सके कि गतिविधि दुर्भावनापूर्ण है या नहीं।
3. यदि आवश्यक हो, तो रिवर्स इंजीनियरिंग के लिए फ़ाइल की एक कॉपी एकत्र करने का प्रयास करें, ताकि नियत किया जा सके कि क्या यह वैध है।

संदर्भ:

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

लेखक: एएसडी का एसीएससी

तिथि: 2024/06/19
स्टैटस: प्रयोगात्मक

टैग्स:

- tlp.green
- classification.au.official
- attack.execution

लॉग सोर्स:

```
category: process_creation
product: windows
```

खोज:

```
writable_path:
    Image|contains:
    - ':\\$Recycle.Bin\\'
    - ':\\AMD\\Temp\\'
    - ':\\Intel\\'
    - ':\\PerfLogs\\'
    - ':\\Windows\\addins\\'
    - ':\\Windows\\appcompat\\'
    - ':\\Windows\\apppatch\\'
    - ':\\Windows\\AppReadiness\\'
    - ':\\Windows\\bcastdvr\\'
    - ':\\Windows\\Boot\\'
    - ':\\Windows\\Branding\\'
    - ':\\Windows\\CbsTemp\\'
    - ':\\Windows\\Containers\\'
    - ':\\Windows\\csc\\'
    - ':\\Windows\\Cursors\\'
    - ':\\Windows\\debug\\'
    - ':\\Windows\\diagnostics\\'
    - ':\\Windows\\DigitalLocker\\'
    - ':\\Windows\\dot3svc\\'
    - ':\\Windows\\en-US\\'
    - ':\\Windows\\Fonts\\'
    - ':\\Windows\\Globalization\\'
    - ':\\Windows\\Help\\'
    - ':\\Windows\\IdentityCRL\\'
    - ':\\Windows\\IME\\'
    - ':\\Windows\\ImmersiveControlPanel\\'
```

- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Image|contains: '\\AppData\\'
User: 'SYSTEM'

condition: writable_path and not appdata

असत्य सकारात्मक:

Allowlist ऑडिटिंग एप्लिकेशन्स को Temp से एक्ज़िक्यूटेबल्स चलाते हुए देखा गया है।

यह संभव है कि निगरानी किए जाने वाले परिवेश(शों) में उपयोग की जाने वाली स्क्रिप्ट्स और एडमिनिस्ट्रेटिव टूल्स इनमें से किसी एक डायरेक्टरी में स्थित हो सकते हैं और इन्हें मामला-दर-मामला आधार पर संबोधित किया जाना चाहिए।

स्तर: high

शीर्षक: वर्ल्ड राइटेबल एक्ज़िक्यूशन - उपयोगकर्ता

आईडी: 6DDA3843-182A-4214-9263-925A80B4C634
विवरण: C:\Users\Public* और Users के अंदर मौजूद अन्य वर्ल्ड राइटेबल फ़ोल्डर्स से प्रक्रिया एक्ज़िक्यूशन का पता लगाएँ।
पृष्ठभूमि:

यदि कोई फ़ाइल SYSTEM के रूप में चलाई जाती है, तो AppData फ़ोल्डर्स को बाहर रखा जाता है - यह एक सौम्य तरीका है, जिसमें कई अस्थायी एप्लिकेशन फ़ाइलें एक्ज़िक्यूट की जाती हैं।

जाँच:

1. इस फ़ाइल एक्ज़िक्यूशन से सीधे संबद्ध जानकारी की जाँच करें, जैसे उपयोगकर्ता संदर्भ, एक्ज़िक्यूशन इंटेग्रिटी स्तर, तत्काल फॉलो-ऑन गतिविधि और फ़ाइल द्वारा लोड की गई इमेजेस।
2. प्रासंगिक प्रक्रिया, नेटवर्क, फ़ाइल और होस्ट पर मौजूद अन्य समर्थनकारी डेटा की जाँच करें, ताकि इस बात का आकलन करने में सहायता मिल सके कि गतिविधि दुर्भावनापूर्ण है या नहीं।
3. यदि आवश्यक हो, तो रिवर्स इंजीनियरिंग के लिए फ़ाइल की एक कॉपी एकत्र करने का प्रयास करें, ताकि नियत किया जा सके कि क्या यह वैध है।

संदर्भ:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

लेखक: एएसडी का एसीएससी
तिथि: 2024/06/19
स्टैटस: प्रयोगात्मक
टैग्स:

- tlp.green
- classification.au.official
- attack.execution

लॉग सोर्स:

category: process_creation
product: windows

खोज:

```
users:
    Image|contains:
    - ':\\Users\\All Users\\'
    - ':\\Users\\Contacts\\'
    - ':\\Users\\Default\\'
    - ':\\Users\\Public\\'
    - ':\\Users\\Searches\\'
appdata:
    Image|contains: '\\AppData\\'
    User: 'SYSTEM'
condition: users and not appdata
```

असत्य सकारात्मक:

- यह संभव है कि निगरानी किए जाने वाले परिवेश(शों) में उपयोग की जाने वाली स्क्रिप्ट्स और एडमिनिस्ट्रेटिव टूल्स इनमें से किसी एक डायरेक्टरी में स्थित हो सकते हैं और इन्हें मामला-दर-मामला आधार पर संबोधित किया जाना चाहिए।

स्तर: medium

मिटिगेशन्स

लॉगिंग

एएसडी की एसीएससी जाँचों के दौरान खोजी प्रयासों की प्रभाविता और गति को कम बनाने वाला एक आम मुद्दा कई क्षेत्रों में व्यापक और ऐतिहासिक लॉगिंग जानकारी की कमी है, जिसमें वेब सर्वर रिक्वेस्ट लॉग्स, विंडोज़ इवेंट लॉग्स और इंटरनेट प्रॉक्सी लॉग्स शामिल हैं।

एएसडी का एसीएससी विंडोज़ इवेंट लॉगिंग और फॉरवर्डिंग के बारे में उनके मार्गदर्शन की समीक्षा और लागूकरण की सलाह देता है, जिसमें विंडोज़ इवेंट लॉगिंग रिपॉज़िटरी और सूचना सुरक्षा मैनुअल के सिस्टम मॉनिटरिंग के लिए दिशानिर्देश में निहित कॉन्फ़िगरेशन फ़ाइलें और स्क्रिप्ट्स शामिल हैं, ताकि लॉग्स को केंद्रीकृत किया जा सके और लॉग्स को एक उपयुक्त अवधि के लिए सहेजकर रखा जा सके।

पैच प्रबंधन

इंटरनेट के प्रति उजागर डिवाइसेज़ और सेवाओं को तुरंत पैच करें, जिसमें वेब सर्वर्स, वेब एप्लिकेशन्स और रिमोट एक्सेस गेटवे शामिल हैं। प्रक्रिया को स्वचालित और तेज बनाने के लिए एक केंद्रीकृत पैच प्रबंधन प्रणाली लागू करने पर विचार करें। एएसडी का एसीएससी ISM के सिस्टम प्रबंधन के लिए दिशानिर्देश लागू करने की सलाह देता है, विशेषकर उपयुक्ततानुसार सिस्टम पैचिंग कंट्रोल्स।

हमलावर द्वारा उपयोग किए गए अधिकांश दुरुपयोग सार्वजनिक रूप से ज्ञात थे और इनके लिए पैचेस या मिटिगेशन्स उपलब्ध थे। संगठनों को सुनिश्चित करना चाहिए कि सुरक्षा पैचेस या मिटिगेशन्स को 48 घंटों के अंदर इंटरनेट फेसिंग इंफ्रास्ट्रक्चर पर लागू किया जाता है, और जहां संभव हो, सॉफ़्टवेयर व ऑपरेटिंग सिस्टम के नवीनतम संस्करणों का उपयोग किया जाए।

नेटवर्क सेगमेन्टेशन

नेटवर्क सेगमेन्टेशन से हमलावरों के लिए संगठन के संवेदनशील डेटा का पता लगाना और इसकी एक्सेस प्राप्त करना काफी अधिक कठिन बन सकता है। कंप्यूटरों के बीच ट्रैफ़िक यदि आवश्यक न हो, तो इसे अस्वीकार करके समानांतर आवाजाही को सीमित या अवरुद्ध करने के लिए नेटवर्क का सेगमेन्टेशन करें। एक्टिव डायरेक्टरी और अन्य ऑथेंटिकेशन सर्वर्स जैसे महत्वपूर्ण सर्वर्स केवल सीमित संख्या में मध्यस्थ सर्वर्स या 'जंप सर्वर्स' से प्रशासित होने में सक्षम होने चाहिए। इन सर्वर्स की बारीकी से निगरानी की जानी चाहिए, इन्हें अच्छी तरह से संरक्षित करना चाहिए और कौन से उपयोगकर्ता व डिवाइसेज़ इनसे कनेक्ट करने में सक्षम हैं, इसे सीमित करना चाहिए।

समानांतर आवाजाही को अवरुद्ध किए जाने के पहचान में आए उदाहरणों के बावजूद भी अतिरिक्त नेटवर्क सेगमेन्टेशन से उस डेटा की मात्रा को और भी अधिक सीमित किया जा सकता था, जिसे हमलावर एक्सेस करने और बाहर निकालने में सक्षम थे।

अतिरिक्त मिटिगेशन्स

संलेखन एजेंसियाँ APT40 और अन्य लोगों द्वारा नीचे दिए गए TTP के उपयोग का सामना करने के लिए निम्नलिखित मिटिगेशन्स की सलाह भी देती हैं।

- अप्रयुक्त या अनावश्यक नेटवर्क सर्विसेज़, पोर्ट्स और प्रोटोकॉल्स को अक्षम बनाएँ।
- वेब सर्वर्स और एप्लिकेशन्स की सुरक्षा के लिए अच्छी तरह से ट्यून किए गए वेब एप्लिकेशन फ़ायरवॉल्स (WAFs) का उपयोग करें।
- सर्वर्स, फ़ाइल शेयर्स, और अन्य संसाधनों की एक्सेस को सीमित करने के लिए निम्नतम प्रिविलेज लागू करें।
- क्रेडेंशियल्स की क्रैकिंग करने और पुन:उपयोग को कठिन बनाने के लिए मल्टी-फैक्टर ऑथेंटिकेशन (MFA) और प्रबंधित सेवा खातों का उपयोग करें। सभी इंटरनेट एक्सेसिबल रिमोट एक्सेस सेवाओं के लिए MFA लागू किया जाना चाहिए, जिनमें शामिल हैं:
  - वेब और क्लाउड-बेस्ड ईमेल
  - सहयोग प्लैटफॉर्म्स
  - वर्चुअल प्राइवेट नेटवर्क कनेक्शन्स
  - रिमोट डेस्कटॉप सर्विसेज़
- जीवन-के-अंत में डिवाइसेज़ को बदलें।

तालिका 1. मिटिगेशन रणनीतियाँ/तकनीकें

TTP	अनिवार्य आठ मिटिगेशन रणनीतियाँ	ISM कंट्रोल
शुरुआती एक्सेस T1190 पब्लिक-फेसिंग एप्लिकेशन का दुरुपयोग	पैच एप्लिकेशन्स पैच ऑपरेटिंग सिस्टम्स मल्टी-फैक्टर ऑथेंटिकेशन एप्लिकेशन कंट्रोल	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
एक्ज़िक्यूशन T1059 कमांड एंड स्क्रिप्टिंग इंटरप्रेटर	एप्लिकेशन कंट्रोल Microsoft Office के मैक्रोज़ को अवरुद्ध करें एडमिनिस्ट्रेटिव प्रिविलेजेस को अवरुद्ध करें	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
लगातार रूप से बने रहना T1505.003 सर्वर सॉफ़्टवेयर घटक: वेब शेल	एप्लिकेशन कंट्रोल एडमिनिस्ट्रेटिव प्रिविलेजेस को अवरुद्ध करें	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
शुरुआती एक्सेस / प्रिविलेज एस्केलेशन / लगातार रूप से बने रहने T1078 वैध खाते	पैच ऑपरेटिंग सिस्टस मल्टी-फैक्टर ऑथेंटिकेशन एडमिनिस्ट्रेटिव प्रिविलेजेस को प्रतिबंधित करें एप्लिकेशन कंट्रोल उपयोगकर्ता एप्लिकेशन सख्त	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

अतिरिक्त सामान्य पहचान और मिटिगेशन सलाह के लिए, कृपया MITRE ATT&CK सारांश में पहचानी गई प्रत्येक तकनीक के लिए MITRE ATT&CK तकनीक वेबपेज पर मिटिगेशन्स एवं खोज अनुभाग देखें, जोकि इस परामर्श-सूचना के अंत में दिया गया है।

अस्वीकरण

इस रिपोर्ट में दी गई जानकारी केवल सूचना प्रयोजनों के लिए "जैसा है, वैसे ही" स्वरूप में प्रदान की जा रही है। लेखन एजेंसियाँ किसी भी वाणिज्यिक निकाय, उत्पाद, कंपनी या सेवा का समर्थन नहीं करती हैं, जिसमें इस दस्तावेज़ में लिंक की गई कोई भी संस्था, उत्पाद या सेवाएँ भी शामिल हैं। सेवा चिह्न, ट्रेडमार्क, विनिर्माता, या अन्यथा द्वारा विशिष्ट वाणिज्यिक निकायों, उत्पादों, प्रक्रियाओं या सेवाओं के लिए कोई भी संदर्भ, लेखन एजेंसियों द्वारा समर्थन, अनुशंसा, या पक्षपात का गठन नहीं करता है या इनके लिए संकेत नहीं देता है।

यह दस्तावेज़ TLP:CLEAR चिह्नित है। प्रकटीकरण असीमित है। यदि जननिर्गति के लागू नियमों और प्रक्रियाओं के अनुरूप इस जानकारी के दुरुपयोग के लिए न्यूनतम या कोई भी पूर्वानुमानित जोखिम नहीं है, तो स्रोत TLP:CLEAR का उपयोग तब कर सकते हैं। मानक कॉपीराइट नियमों के अधीन TLP:CLEAR जानकारी बिना किसी प्रतिबंध के वितरित की जा सकती है। ट्रैफिक लाइट प्रोटोकॉल के बारे में और अधिक जानकारी के लिए cisa.gov/tlp देखें।

MITRE ATT&CK – रुचिकर ऐतिहासिक APT40 ट्रेडक्राफ्ट

टोह लगाना (TA0043)	
शिकार बनाए गए व्यक्ति के स्वामित्व वाली वेबसाइटों की खोज करना (T1594)	शिकार बनाए गए व्यक्ति की पहचान जानकारी एकत्र करना: क्रेडेंशियल्स (T1589.001)
सक्रिय स्कैनिंग: कमजोरियों की स्कैनिंग (T1595.002)	शिकार बनाए गए होस्ट्स की जानकारी एकत्र करना (T1592)
ओपन वेबसाइटों/डोमेन्स की खोज: खोज इंजन्स (T1593.002)	शिकार बनाए गए नेटवर्क की जानकारी एकत्र करना: डोमेन की प्रॉपर्टीज़ (T1590.001)
शिकार बनाए गए व्यक्ति की पहचान जानकारी एकत्र करना: ईमेल पते (T1589.002)	

संसाधन विकास (TA0042)	
इंफ्रास्ट्रक्चर का अधिग्रहण: डोमेन्स (T1583.001)	इन्फ्रास्ट्रक्चर का अधिग्रहण करना (T1583)
इंफ्रास्ट्रक्चर का अधिग्रहण: DNS सर्वर (T1583.002)	खातों का संक्रमण करना (T1586)
क्षमताएँ विकसित करना: कोड साइनिंग सर्टिफिकेट्स (T1587.002)	इंफ्रास्ट्रक्चर को संक्रमित करना (T1584)
क्षमताएँ विकसित करना: डिजिटल सर्टिफिकेट्स (T1587.003)	क्षमताएँ विकसित करना: मैलवेयर (T1587.001)
क्षमताएँ प्राप्त करना: कोड साइनिंग सर्टिफिकेट्स (T1588.003)	खाते बनाना: क्लाउड खाते (T1585.003)
इंफ्रास्ट्रक्चर को संक्रमित करना: नेटवर्क डिवाइसेज़ (T1584.008)	क्षमताएँ प्राप्त करना: डिजिटल सर्टिफिकेट्स (T1588.004)

शुरुआती एक्सेस (TA0001)	
वैध खाते (T1078)	फ़िशिंग (T1566)
वैध खाते: डिफ़ॉल्ट खाते (T1078.001)	फ़िशिंग: स्पियरफ़िशिंग एटैचमेंट (T1566.001)
वैध खाते: डोमेन खाते (T1078.002)	फ़िशिंग: स्पियरफ़िशिंग लिंक (T1566.002)
बाहरी रिमोट सर्विसेज़ (T1133)	पब्लिक-फेसिंग एप्लिकेशन का दुरुपयोग करना (T1190)
ड्राइव-बाय हमला (T1189)	

एक्ज़िक्यूशन (TA0002)	
विंडोज़ मैनेजमेंट इंस्ट्रूमेन्टेशन (T1047)	कमांड और स्क्रिप्टिंग इंटरप्रेटर: पायथन (T1059.006)
शेड्यूल्ड टास्क/जॉब: एट (T1053.002)	कमांड और स्क्रिप्टिंग इंटरप्रेटर: जावास्क्रिप्ट (T1059.007)
शेड्यूल्ड टास्क/जॉब: शेड्यूल्ड टास्क (T1053.005)	नेटिव API (T1106)
कमांड और स्क्रिप्टिंग इंटरप्रेटर (T1059)	इंटर-प्रोसेस कम्युनिकेशन (T1559)
कमांड और स्क्रिप्टिंग इंटरप्रेटर: विंडोज़ कमांड शेल (T1059.003)	सिस्टम सर्विसेज़: सर्विस एक्ज़िक्यूशन (T1569.002)
कमांड और स्क्रिप्टिंग इंटरप्रेटर: पावरशेल (T1059.001)	क्लायंट एक्ज़िक्यूशन के लिए दुरुपयोग (T1203)
कमांड और स्क्रिप्टिंग इंटरप्रेटर: विज़ुअल बेसिक (T1059.005)	उपयोगकर्ता एक्ज़िक्यूशन: दुर्भावनापूर्ण फ़ाइल (T1204.002)
कमांड और स्क्रिप्टिंग इंटरप्रेटर: यूनिक्स शेल (T1059.004)	कमांड और स्क्रिप्टिंग इंटरप्रेटर: एप्पल स्क्रिप्ट (T1059.002)
शेड्यूल्ड टास्क/जॉब: क्रॉन (T1053.003)	सॉफ़्टवेयर लागूकरण टूल्स (T1072)

लगातार रूप से बने रहना (TA0003)	
वैध खाते (T1078)	सर्वर सॉफ़्टवेयर घटक: वेब शेल (T1505.003)
ऑफिस एप्लिकेशन स्टार्टअप: ऑफिस टेम्पलेट मैक्रोज़ (T1137.001)	सिस्टम प्रक्रिया निर्मित या संशोधित करना: विंडोज़ सर्विस (T1543.003)
शेड्यूल्ड टास्क/जॉब: एट (T1053.002)	बूट या लॉगऑन ऑटोस्टार्ट एक्ज़िक्यूशन: रजिस्ट्री रन कीज़ / स्टार्टअप फ़ोल्डर (T1547.001)
शेड्यूल्ड टास्क/जॉब: शेड्यूल्ड टास्क (T1053.005)	बूट या लॉगऑन ऑटोस्टार्ट एक्ज़िक्यूशन: शॉर्टकट संशोधन (T1547.009)
बाहरी रिमोट सर्विसेज़ (T1133)	एक्ज़िक्यूशन फ्लो को हाइजैक करना: DLL सर्च ऑर्डर की हाइजैकिंग (T1574.001)
शेड्यूल्ड टास्क/जॉब: क्रॉन (T1053.003)	एक्ज़िक्यूशन फ्लो को हाइजैक करना: DLL साइड-लोडिंग (T1574.002)
खाते में हेरफेर (T1098)	वैध खाते: क्लाउड खाते (T1078.004)
वैध खाते: डोमेन खाते (T1078.002)	

प्रिविलेज एस्केलेशन (TA0004)	
शेड्यूल्ड टास्क/जॉब: एट (टी1053.002)	सिस्टम प्रक्रिया निर्मित या संशोधित करना: विंडोज़ सर्विस (T1543.003)
शेड्यूल्ड टास्क/जॉब: शेड्यूल्ड टास्क (T1053.005)	बूट या लॉगऑन ऑटोस्टार्ट एक्ज़िक्यूशन: रजिस्ट्री रन कीज़ / स्टार्टअप फ़ोल्डर (T1547.001)
प्रोसेस इंजेक्शन: थ्रेड एक्ज़िक्यूशन की हाइजैकिंग (T1055.003)	बूट या लॉगऑन ऑटोस्टार्ट एक्ज़िक्यूशन: शॉर्टकट संशोधन (T1547.009)
प्रोसेस इंजेक्शन: प्रोसेस हॉलोइंग (T1055.012)	एक्ज़िक्यूशन फ्लो को हाइजैक करना: DLL सर्च ऑर्डर की हाइजैकिंग (T1574.001)

प्रिविलेज एस्केलेशन (TA0004)	
वैध खाते: डोमेन खाते (T1078.002)	प्रिविलेज एस्केलेशन के लिए दुरुपयोग (T1068)
एक्सेस टोकन में हेरफेर: टोकन का प्रतिरूपण/चोरी (T1134.001)	घटना द्वारा आरंभ होने वाला एक्ज़िक्यूशन: यूनिक्स शेल कॉन्फ़िगरेशन संशोधन (T1546.004)
प्रोसेस इंजेक्शन: डायनामिक-लिंक लाइब्रेरी इंजेक्शन (T1055.001)	वैध खाते: डोमेन खाते (T1078.002)
वैध खाते: स्थानीय खाते (T1078.003)	

सुरक्षा से बचाव (TA0005)	
रूटकिट (T1014)	इनडायरेक्ट ऑर्डर एक्ज़िक्यूशन (T1202)
अस्पष्ट फ़ाइलें या सूचना (T1027)	सिस्टम बाइनरी प्रॉक्सी एक्ज़िक्यूशन: Mshta (T1218.005)
अस्पष्ट फ़ाइलें या जानकारी: सॉफ़्टवेयर पैकिंग (T1027.002)	सिस्टम बाइनरी प्रॉक्सी एक्ज़िक्यूशन: Regsvr32 (T1218.010)
अस्पष्ट फ़ाइलें या जानकारी: स्टेगानोग्राफ़ी (T1027.003)	ट्रस्ट कंट्रोल्स को नष्ट करना: कोड साइनिंग (T1553.002)
अस्पष्ट फ़ाइलें या जानकारी: डिलीवरी के बाद कंपाइल करना (T1027.004)	फ़ाइल और डायरेक्टरीज़ की पर्मिशन्स में संशोधन: लाइनेक्स और मैक फ़ाइल और डायरेक्टरी पर्मिशन्स में संशोधन (T1222.002)
रूपांतरण करना: वैध नाम या स्थान का मिलान करना (T1036.005)	वर्चुअलाइज़ेशन/सैंडबॉक्स से बचाव: सिस्टम जाँचें (T1497.001)
प्रोसेस इंजेक्शन: थ्रेड एक्ज़िक्यूशन की हाइजैकिंग (T1055.003)	रूपांतरण: (T1036)
रिफ्लेक्टिव कोड लोडिंग (T1620)	सुरक्षाओं का बिगड़ाव: सिस्टम फ़ायरवॉल को अक्षम या संशोधित करना (T1562.004)
प्रोसेस इंजेक्शन: प्रोसेस हॉलोइंग (T1055.012)	आर्टिफैक्ट्स छिपाना: छिपी हुई फ़ाइलें और डायरेक्टरीज़ (T1564.001)
संकेतक हटाना: फ़ाइल हटाना (T1070.004)	आर्टिफैक्ट्स छिपाना: छिपी हुई विंडो (T1564.003)
संकेतक हटाना: टाइमस्टॉम्प (T1070.006)	एक्ज़िक्यूशन फ्लो को हाइजैक करना: DLL सर्च ऑर्डर की हाइजैकिंग (T1574.001)
संकेतक हटाना: विंडोज़ इवेंट लॉग साफ़ करना (T1070.001)	एक्ज़िक्यूशन फ्लो को हाइजैक करना: DLL साइड-लोडिंग (T1574.002)
रजिस्ट्री संशोधन (T1112)	वेब सर्विस (T1102)
फ़ाइलों या जानकारी को स्पष्ट/डिकोड करना (T1140)	रूपांतरण: टास्क या सर्विस का रूपांतरण (T1036.004)
सुरक्षाओं का बिगड़ाव (T1562)	

क्रेडेंशियल एक्सेस (TA0006)	
OS क्रेडेंशियल डंपिंग: LSASS मेमोरी (T1003.001)	असुरक्षित क्रेडेंशियल्स: फ़ाइलों में क्रेडेंशियल्स (T1552.001)
OS क्रेडेंशियल डंपिंग: NTDS (T1003.003)	ब्रूट फोर्स: पासवर्ड का अनुमान लगाना (T1110.001)
नेटवर्क स्निफिंग (T1040)	जबरन ऑथेंटिकेशन (T1187)
पासवर्ड स्टोर्स से क्रेडेंशियल्स: कीचेन (T1555.001)	Kerberos टिकट की चोरी या जालसाजी: केर्बेरोस्टिंग (T1558.003)

क्रेडेंशियल एक्सेस (TA0006)	
इनपुट कैप्चर: कीलॉगिंग (T1056.001)	मल्टी-फैक्टर ऑथेंटिकेशन हस्तक्षेप (T1111)
वेब सेशन कुकी की चोरी (T1539)	एप्लिकेशन एक्सेस टोकन की चोरी (T1528)
क्रेडेंशियल एक्सेस के लिए दुरुपयोग (T1212)	ब्रूट फोर्स: पासवर्ड क्रैकिंग (T1110.002)
इनपुट कैप्चर: वेब पोर्टल कैप्चर (T1056.003)	OS क्रेडेंशियल डंपिंग: DCSync (T1003.006)
पासवर्ड स्टोर्स से क्रेडेंशियल्स (T1555)	पासवर्ड स्टोर्स से क्रेडेंशियल्स: वेब ब्राउज़र्स से क्रेडेंशियल्स (T1555.003)

खोज (TA0007)	
सिस्टम सर्विस खोज (T1007)	सिस्टम जानकारी खोज (T1082)
एप्लिकेशन विंडो खोज (T1010)	खाता खोज: स्थानीय खाता (T1087.001)
रजिस्ट्री में क्वेरी (T1012)	सिस्टम सूचना खोज, तकनीक T1082 - एंटरप्राइज़ | MITRE ATT&CK®
फ़ाइल और डायरेक्टरी की खोज (T1083)	सिस्टम टाइम की खोज (T1124)
नेटवर्क सर्विस की खोज (T1046)	सिस्टम ओनर/यूज़र की खोज (T1033)
रिमोट सिस्टम की खोज (T1018)	डोमेन ट्रस्ट की खोज (T1482)
खाता खोज: ईमेल खाता (T1087.003)	खाता खोज: डोमेन खाता (T1087.002)
सिस्टम नेटवर्क कनेक्शन्स की खोज (T1049)	वर्चुअलाइज़ेशन/सैंडबॉक्स से बचाव: सिस्टम जाँचें (T1497.001)
प्रोसेस की खोज (T1057)	सॉफ़्टवेयर की खोज (T1518)
पर्मिशन ग्रुप्स की खोज: डोमेन ग्रुप्स (T1069.002)	नेटवर्क शेयर की खोज, तकनीक T1135 - एंटरप्राइज़ | MITRE ATT&CK®
सिस्टम नेटवर्क कॉन्फ़िगरेशन की खोज: इंटरनेट कनेक्शन की खोज (T1016.001)	

समानांतर आवाजाही (TA0008)	
रिमोट सर्विसेज़: रिमोट डेस्कटॉप प्रोटोकॉल (T1021.001)	रिमोट सर्विसेज़ (T1021)
रिमोट सर्विसेज़: SMB/Windows एड्मिन शेयर्स (T1021.002)	वैकल्पिक ऑथेंटिकेशन सामग्री का उपयोग: टिकट पास करना (T1550.003)
रिमोट सर्विसेज़: विंडोज़ रिमोट मैनेजमेंट (T1021.006)	लैटरल टूल ट्रांसफर (T1570)

एकत्र करना (TA0009)	
स्थानीय सिस्टम से डेटा (T1005)	एकत्र किए गए डेटा को आर्काइव करना: लायब्रेरी के माध्यम से आर्काइव करना (T1560.002)
नेटवर्क शेयर्ड ड्राइव से डेटा (T1039)	ईमेल एकत्र करना: रिमोट ईमेल एकत्र करना (T1114.002)

एकत्र करना (TA0009)	
इनपुट कैप्चर: कीलॉगिंग (T1056.001)	क्लिपबोर्ड डेटा (T1115)
स्वचालित रूप से एकत्र करना (T1119)	सूचना रिपॉज़िटरी से डेटा (T1213)
इनपुट कैप्चर: वेब पोर्टल कैप्चर (T1056.003)	डेटा स्टेज्ड: रिमोट डेटा स्टेजिंग (T1074.002)
डेटा स्टेज्ड: स्थानीय डेटा स्टेजिंग (T1074.001)	एकत्र किए गए डेटा को आर्काइव करना (T1560)
ईमेल एकत्र करना (T1114)	

बाहर निकालना (TA0010)	
C2 चैनल पर बाहर निकालना (T1041)	वैकल्पिक प्रोटोकॉल पर बाहर निकालना: एसिमेट्रिक एन्क्रिप्टेड नॉन-C2 प्रोटोकॉल (T1048.002) पर बाहर निकालना
वैकल्पिक प्रोटोकॉल पर बाहर निकालना (T1048)	वेब सर्विस पर बाहर निकालना: क्लाउड स्टोरेज में बाहर निकालना (T1567.002)

कमांड और कंट्रोल (TA0011)	
डेटा का अस्पष्टीकरण: प्रोटोकॉल प्रतिरूपण (T1001.003)	वेब सर्विस: डेड ड्रॉप रिज़ॉल्वर (T1102.001)
सामान्य रूप से प्रयुक्त किया जाने वाला पोर्ट (T1043)	वेब सर्विस: एक-तरफा संचार (T1102.003)
एप्लिकेशन लेयर प्रोटोकॉल: वेब प्रोटोकॉल्स (T1071.001)	इंग्रेस टूल ट्रांस्फर (T1105)
एप्लिकेशन लेयर प्रोटोकॉल: फ़ाइल ट्रांस्फर प्रोटोकॉल्स (T1071.002)	प्रॉक्सी: आंतरिक प्रॉक्सी (T1090.001)
प्रॉक्सी: बाहरी प्रॉक्सी (T1090.002)	गैर-मानक पोर्ट (T1571)
प्रॉक्सी: मल्टी-हॉप प्रॉक्सी (T1090.003)	प्रोटोकॉल टनलिंग (T1572)
वेब सर्विस: दो-तरफा संचार (T1102.002)	एन्क्रिप्टेड चैनल (T1573)
एन्क्रिप्टेड चैनल: एसिमेट्रिक क्रिप्टोग्राफी (T1573.002)	इंग्रेस टूल ट्रांस्फर (T1105)
प्रॉक्सी, तकनीक T1090 - एंटरप्राइज़ | MITRE ATT&CK®	

प्रभाव (TA0040)	
सर्विस स्टॉप (T1489)	डिस्क वाइप (T1561)
सिस्टम शटडाउन/रिबूट (T1529)	रिसोर्स की हाइजैकिंग (T1496)

नोट्स

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 करना:

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