APT40 උපදේශනය

PRC MSS ඔත්තු බැලීමේදී භාවිතා කරන ශිල්පීය ක්‍රම ක්‍රියාත්මක වේ

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**

පටුන

විධායක සාරාංශය

පසුබිම

ඔස්ට්‍රේලියානු සංඥා අධ්‍යක්ෂ මණ්ඩලයේ ඕස්ට්‍රේලියානු සයිබර් ආරක්ෂක මධ්‍යස්ථානය (ASD's ACSC), එක්සත් ජනපද සයිබර් ආරක්ෂණ සහ යටිතල පහසුකම් ආරක්ෂක ඒජන්සිය (CISA), එක්සත් ජනපද ජාතික ආරක්ෂක ඒජන්සිය (NSA), එක්සත් ජනපද ෆෙඩරල් විමර්ශන කාර්යාංශය (FBI), එක්සත් රාජධානියේ ජාතික සයිබර් ආරක්ෂක මධ්‍යස්ථානය (NCSC-UK), කැනේඩියානු සයිබර් ආරක්ෂාව සඳහා වූ මධ්‍යස්ථානය (CCCS), නවසීලන්ත ජාතික සයිබර් ආරක්ෂක මධ්‍යස්ථානය (NCSC-NZ), ජර්මානු ෆෙඩරල් බුද්ධි සේවය (BND) සහ ආණ්ඩුක්‍රම ව්‍යවස්ථාව ආරක්ෂා කිරීම සඳහා වූ ෆෙඩරල් කාර්යාලය (BfV), කොරියානු ජනරජයේ ජාතික බුද්ධි සේවය (NIS) සහ NIS හි ජාතික සයිබර් ආරක්ෂක මධ්‍යස්ථානය, සහ ජපානයේ සයිබර් ආරක්ෂාව සඳහා සිදුවීම් සූදානම සහ උපාය මාර්ග පිළිබඳ ජාතික මධ්‍යස්ථානය (NISC) සහ ජාතික පොලිස් ඒජන්සිය (NPA) විසින් නිර්මාණය කරන ලද මෙම උපදේශනය- මින් ඉදිරියට «කර්තෘ ආයතන» ලෙස හඳුන්වනු ලබන - මහජන චීන සමූහාණ්ඩුවේ (PRC) රාජ්‍ය අනුග්‍රහය ලත් සයිබර් කණ්ඩායමක් සහ ඔවුන්ගෙන් ඔස්ට්‍රේලියානු ජාලවලට එල්ලවන වර්තමාන තර්ජනය ගෙනහැර දක්වයි. මෙම උපදේශනය, තර්ජනය පිළිබඳ කර්තෘ ආයතනවල සාමූහික අවබෝධය මෙන්ම ASD හි ACSC සිදුවීම් ප්‍රතිචාර දක්වන විමර්ශන ද උපයෝගී කර ගනී.

PRC රාජ්‍ය අනුග්‍රහය ලත් සයිබර් කණ්ඩායම මීට පෙර ඔස්ට්‍රේලියාව සහ ඇමරිකා එක්සත් ජනපදය ඇතුළු විවිධ රටවල සංවිධාන ඉලක්ක කරගෙන ඇති අතර, පහත ඉස්මතුකර දැක්වෙන ශිල්පීය ක්‍රම අනෙකුත් PRC රාජ්‍ය අනුග්‍රහය ලත් ක්‍රියාකාරීන් විසින් නිතිපතා භාවිතා කරනු ලැබේ. එබැවින්, මෙම කණ්ඩායම සහ ඒ හා සමාන ශිල්පීය ක්‍රම තම රටවල ජාලවලට ද තර්ජනයක් වන බවට කර්තෘ ආයතන විශ්වාස කරති.

මෙම කණ්ඩායම PRC රාජ්‍ය ආරක්ෂක අමාත්‍යාංශය (MSS) වෙනුවන් ද්වේෂසහගත සයිබර් මෙහෙයුම් සිදු කරන බවට කර්තෘ ආයතන තක්සේරු කරති. ක්‍රියාකාරකම් සහ ශිල්පීය ක්‍රම, Advanced Persistent Threat (APT) 40 (කර්මාන්ත වාර්තාකරණයේදී Kryptonite Panda, GINGHAM TYPHOON, Leviathan සහ Bronze Mohawk ලෙසද හැඳින්වේ) ලෙස නිරීක්ෂණය කරන ලද කණ්ඩායම් සමඟ සම්පතනය වේ. මෙම කණ්ඩායම මීට පෙර PRC හි හයිනාන් ප්‍රාන්තයේ, හයිකෝ හි ස්ථානගතව සිටින බවත්, හයිනාන් රාජ්‍ය ආරක්ෂක දෙපාර්තමේන්තුවේ PRC MSS වෙතින් කාර්යයන් ලබා ගන්නා බවත් වාර්තා වී ඇත. වින්දිත ජාල දෙකකට එරෙහිව ක්‍රියාත්මක වන මෙම විරුද්ධවාදියාගේ ශිල්පීය ක්‍රම පිළිබඳ සැලකිය යුතු ප්‍රත්‍යෙක අධ්‍යයනවල සාම්පලයක් පහත උපදේශනය මගින් සපයයි. සයිබර් ආරක්ෂක වෘත්තිකයන්ට තමන්ගේම ජාලවලට එරෙහිව සිදු කෙරෙන APT40 ආක්‍රමණ හඳුනා ගැනීමට, වැළැක්වීමට සහ ඒවාට පිළියම් යෙදීමට ප්‍රත්‍යෙක අධ්‍යයනයන් වැදගත් වේ. තෝරාගත් ප්‍රත්‍යෙක අධ්‍යයනයන් වන්නේ මෙම තර්ජනාත්මක ක්‍රියාකරු හෝ වෙනත් අය විසින් නැවත අයුතු ලෙස ප්‍රයෝජනයට ගැනීමේ අවදානම අඩු කරමින් සුදුසු ප්‍රතිකර්ම සිදු කර ඇති ඒවාය. එබැවින්, සංවිධානවලට ප්‍රතිකර්ම යෙදීමට අවශ්‍ය කාලය ලබාදුන් බව සහතික කිරීමට ප්‍රත්‍යෙක අධ්‍යයනයන් ස්වභාවයෙන්ම පැරණි ස්වභාවයක් ගනී.

ක්‍රියාකාරකම් සාරාංශය

APT40 විසින් ඔස්ට්‍රේලියානු ජාල මෙන්ම කලාපය තුළ රජයේ සහ පුද්ගලික අංශයේ ජාල නැවත නැවතත් ඉලක්ක කර ඇති අතර, ඔවුන් අපගේ ජාලවලට එල්ල කරන තර්ජනය දිගටම පවතී. මෙම උපදේශනයේ විස්තර කර ඇති ඔත්තු බැලීමේදී භාවිතා කරන ශිල්පීය ක්‍රම ඔස්ට්‍රේලියානු ජාලවලට එරෙහිව නිතිපතා නිරීක්ෂණය කෙරේ.

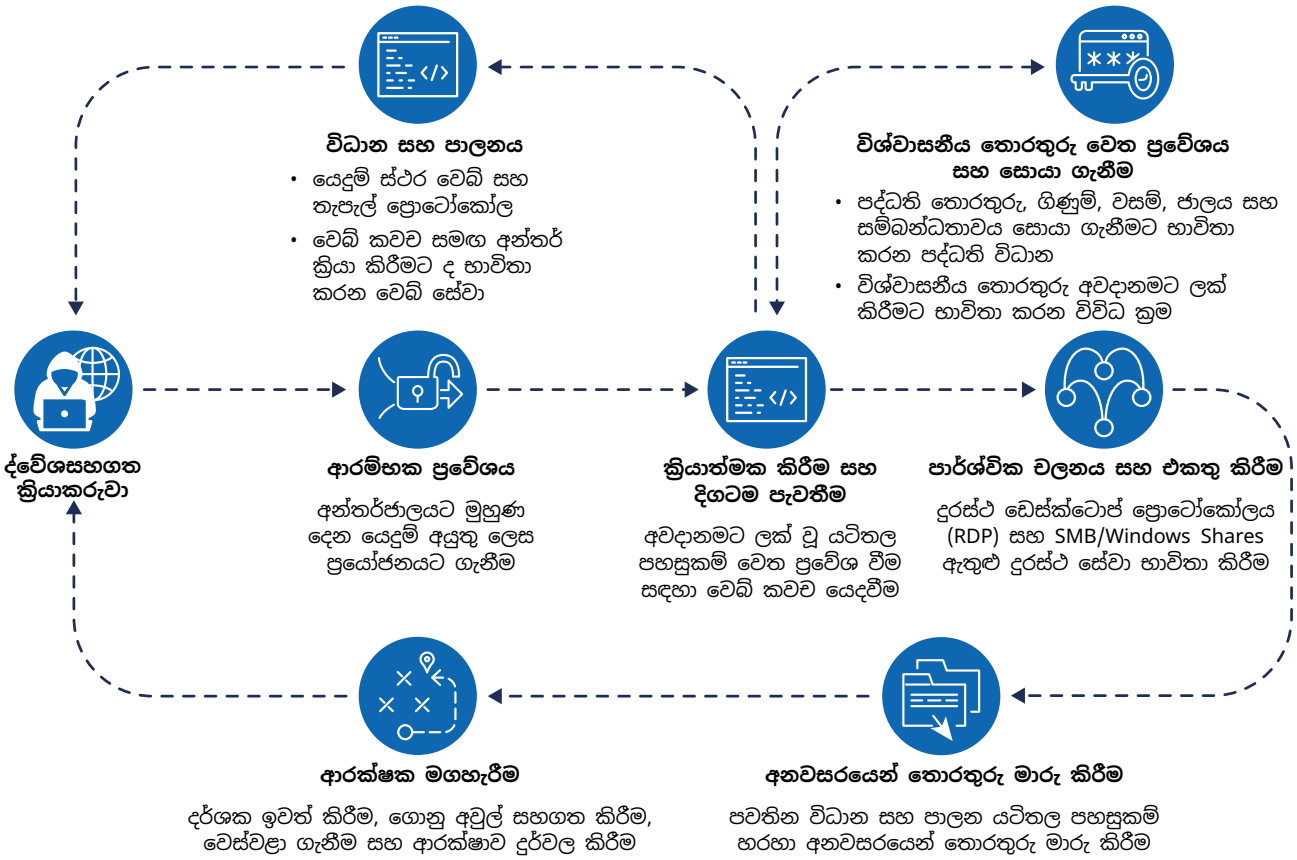
සැලකිය යුතු ලෙස, APT40 සතුව නව අවදානම් පිළිබඳ සංකල්ප-සාධන සාක්ෂි (POC) වේගයෙන් පරිවර්තනය කිරීමට සහ අනුවර්තනය කිරීමට මෙන්ම ඒ ආශ්‍රිත අවදානම් සහගත යටිතල පහසුකම් තිබෙන ඉලක්ක ජාලවලට සම්බන්ධව භාවිතා කිරීමේ හැකියාව ඇත. APT40 උනන්දුවක් දක්වන ජාලවලට, කර්තෘ ආයතන අන්තර්ගත රටවල ජාල ද ඇතුළුව, එරෙහිව ඔත්තු බැලීම සිදු කරන අතර, එහි ඉලක්ක අවදානමට ලක් කිරීමට අවස්ථාව සොයයි. මෙම නිතිපතා ඔත්තු බැලීම මඟින් උනන්දුවක් දක්වන ජාලවල අවදානමට ලක්විය හැකි, ආයු කාලය අවසන් වූ හෝ නඩත්තු නොකරන උපාංග හඳුනා ගැනීමට සහ අයුතු ලෙස ප්‍රයෝජනයට ගැනීමට කණ්ඩායමට ඉඩ සලසයි. 2017 තරම් ඈත කාලයේ සිටම අවදානම් අයුතු ලෙස ප්‍රයෝජනයට ගැනීමට APT40 සාර්ථකත්වය කටයුතු කරයි.

APT40 විසින් Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) සහ Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473) වැනි බහුලව භාවිතා වන මෘදුකාංගවල නව පොදු අවදානම් වේගයෙන් අයුතු ලෙස ප්‍රයෝජනයට ගනියි.

ASD හි ACSC සහ කර්තෘ ආයතන අපේක්ෂා කරන්නේ, ප්‍රසිද්ධියට පත් කිරීමෙන් පැය හෝ දින කිහිපයක් ඇතුළත නව ඉහළ මට්ටමේ අවදානම් සඳහා POC භාවිතා කිරීම කණ්ඩායම දිගටම කරගෙන යනු ඇති බවයි.

2 එක්සත් ජනපද අධිකරණ දෙපාර්තමේන්තුව. 2021. රාජ්‍ය ආරක්ෂක අමාත්‍යාංශය සමඟ වැඩ කරන චීන ජාතිකයන් හතර දෙනෙකුට බෝවන රෝග පර්යේෂණ ඇතුළු බුද්ධිමය දේපළ සහ රහස්‍ය ව්‍යාපාරික තොරතුරු ඉලක්ක කරගත් ගෝලීය පරිගණක වෙත අනවසරයෙන් ප්‍රවේශවන ව්‍යාපාරයක් සම්බන්ධයෙන් චෝදනා එල්ල වී ඇත.

රූපසටහන 1: APT40 ක්‍රියාකාරකම් සඳහා TTP ගැලීම් සටහන



මෙම කණ්ඩායම වංචනිකව සිදු කරන ව්‍යාපාර වැනි පරිශීලක අන්තර්ක්‍රියා අවශ්‍ය කරන ශිල්පීය ක්‍රමවලට වඩා අවදානම් සහගත, පොදු යටිතල පහසුකම් අයුතු ලෙස ප්‍රයෝජනයට ගැනීමට කැමති බව සහ විවිධ පසු විපරම් ක්‍රියාකාරකම් සක්‍රීය කිරීම සඳහා වලංගු විශ්වසනීය තොරතුරු ලබා ගැනීමට ඉහළ ප්‍රමුඛතාවයක් ලබාදෙන බව පෙනේ. APT40 නිතිපතා වෙබ් කවච (T1505.003) දිගටම පවත්වා ගැනීම, විශේෂයෙන් ආක්‍රමණ චක්‍රයේ මුල් අවධියේදී, සඳහා භාවිතා කරයි. සාමාන්‍යයෙන්, සාර්ථක ආරම්භක ප්‍රවේශයකින් පසු APT40 වින්දිතයාගේ පරිසරයට ප්‍රවේශ වීම දිගටම පවත්වා ගැනීම ස්ථාපිත කිරීම කෙරෙහි අවධානය යොමු කරයි. කෙසේ වෙතත්, ආක්‍රමණයක මුල් අවධියේදී දිගටම පැවතීම සිදුවන බැවින්, සියලු ආක්‍රමණයන්හිදී - අවදානමට ලක්වීමේ ප්‍රමාණය හෝ ගනු ලබන ඉදිරි ක්‍රියාමාර්ග නොසලකා - එය නිරීක්ෂණය කිරීමට වැඩි ඉඩක් ඇත.

කැපී පෙනෙන ඔත්තු බැලීමේදී භාවිතා කරන ශිල්පීය ක්‍රම

APT40 මීට පෙර තම මෙහෙයුම් සඳහා විධාන සහ පාලන (C2) ධාරක ලෙස අවදානමට ලක් වූ ඔස්ට්‍රේලියානු වෙබ් අඩවි භාවිතා කර ඇතත්, කණ්ඩායම මෙම තාක්ෂණය (T1594) විකසනය කර ඇත.

APT40 කුඩා-කාර්යාල/නිවාස-කාර්යාල (SOHO) උපාංග ඇතුළු අවදානමට ලක් වූ උපාංග, මෙහෙයුම් යටිතල පහසුකම් ලෙස සහ ඔස්ට්‍රේලියාවේ එහි මෙහෙයුම් සඳහා last-hop redirectors (T1584.008) ලෙස භාවිතා කිරීමේ ගෝලීය ප්‍රවණතාවය අනුගමනය කර ඇත. මෙය කර්තෘ ආයතනවලට මෙම කණ්ඩායමේ චලනයන් වඩා හොඳින් සංලක්ෂණය කිරීමට සහ නිරීක්ෂණය කිරීමට හැකියාව ලබා දී ඇත.

මෙම SOHO උපාංග බොහොමයක් පැවැත්මේ අවසානයට පැමිණ හෝ නොගැලපෙන අතර N-දින අයුතු ප්‍රයෝජන ගැනීමේ මෘදු ඉලක්කයක් වේ. අවදානමට ලක් වූ පසු, SOHO උපාංග මගින් නීත්‍යානුකූල ගමනාගමනය සමඟ මිශ්‍ර වී ජාල ආරක්ෂකයින්ට අභියෝග කිරීමට නිර්මාණය කර ඇති ප්‍රහාර දියත් කිරීමේ අවස්ථාව ලබා දෙයි (T1001.003).

මෙම තාක්ෂණය ලොව පුරා සිටින අනෙකුත් PRC රාජ්‍ය අනුග්‍රහය ලත් ක්‍රියාකාරීන් විසින් නිතිපතා භාවිතා කරනු ලබන අතර, කර්තෘ ආයතන මෙය හවුල් තර්ජනයක් ලෙස සලකති. අතිරේක තොරතුරු සඳහා, ජාල සැපයුම්කරුවන් සහ උපාංග අයුතු ප්‍රයෝජනයට ගන්නා මහජන චීන සමූහාණ්ඩුවේ රාජ්‍ය අනුග්‍රහය ලත් සයිබර් ක්‍රියාකාරීන් සහ එක්සත් ජනපද තීරණාත්මක යටිතල පහසුකම් අවදානමට ලක් කර අඛණ්ඩ ප්‍රවේශයක් දිගටම පවත්වා ගන්නා PRC රාජ්‍ය අනුග්‍රහය ලත් ක්‍රියාකාරීන් යන ඒකාබද්ධ උපදේශනයන් බලන්න.

APT40 විසින් ඇතැම් විට එහි මෙහෙයුම් වලදී වින්දිතයා මුහුණ දෙන C2 යටිතල පහසුකම් ලෙස ප්‍රසම්පාදනය කරන ලද හෝ බදු දී ඇති යටිතල පහසුකම් භාවිතා කරයි; කෙසේ වෙතත්, මෙම ඔත්තු බැලීමේදී භාවිතා කරන ශිල්පීය ක්‍රම සාපේක්ෂව පරිහානියක පවතින බව පෙනේ.

මෙවලම්කරණය

පහත දක්වා ඇති විමර්ශන වලදී හඳුනාගත් ද්වේෂසහගත ගොනු කිහිපයක් ASD හි ACSC විසින් බෙදා ගනිමින් සිටී. පුළුල් ජාල ආරක්ෂණ සහ සයිබර් ආරක්ෂණ ප්‍රජාවන් සඳහා ඔවුන්ට ආරක්ෂා කර ගැනීමට අවශ්‍ය තර්ජන වඩා හොඳින් අවබෝධ කර ගැනීමට හැකි වන පරිදි මෙම ගොනු VirusTotal වෙත උඩුගත කර ඇත.

ප්‍රත්‍යෙක අධ්‍යයනය

ක්‍රියාකරුවෝ ඔවුන්ගේ මෙවලම් සහ ඔත්තු බැලීමේදී ශිල්පීය ක්‍රම භාවිතා කරන ආකාරය පිළිබඳ දැනුවත්භාවය ලබා දීම සඳහා ASD හි ACSC විසින් නිර්නාමික විමර්ශන වාර්තා දෙකක් බෙදා ගනී.

MD5	ගොනු නාමය	අමතර තොරතුරු
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java Source (ජව ජාවා මූලාශ්‍රය)
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Java Bytecode
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Java Bytecode
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Java Source
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Java Bytecode
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Java Bytecode
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Java Bytecode
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Java Bytecode
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | Java Bytecode
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Java Source

ප්‍රත්‍යක්ෂ අධ්‍යයනය 1

පුළුල් ලෙස බෙදා හැරීම සඳහා මෙම වාර්තාව නිර්නාමික කර ඇත. බලපෑමට ලක් වූ සංවිධානය මින් ඉදිරියට 'සංවිධානය' ලෙස හැඳින්වේ. වින්දිතයාගේ අනන්‍යතාවය සහ ASD හි ACSC හි සිදුවීම් ප්‍රතිචාර ක්‍රම වේදයන්ආරක්ෂා කිරීම සඳහා සමහර නිශ්චිත තොරතුරු ඉවත් කර ඇත.

විධායක සාරාංශය

විධායක සාරාංශය?

2022 ජූලි සහ සැප්තැම්බර් අතර සංවිධානයේ ජාලය සාර්ථකව අවදානමට ලක් කිරීම සම්බන්ධයෙන් ASD හි ACSC විමර්ශනයේ සොයාගැනීම් මෙම වාර්තාවෙන් විස්තර කෙරේ. නිරීක්ෂිත ද්වේෂසහගත ක්‍රියාකාරකම සාරාංශගත කිරීමට සහ ප්‍රතිකර්ම නිර්දේශ සකස් කිරීමට මෙම විමර්ශන වාර්තාව සංවිධානයට ලබා දෙන ලදී. සොයාගැනීම්වලින් පෙනී යන්නේ අවදානමට ලක් කිරීම APT40 විසින් සිදු කරන ලද බවයි.

අගෝස්තු මස මැද භාගයේදී, ASD හි ACSC විසින් අගෝස්තු මස අගදී කණ්ඩායම විසින් භාවිතා කරන ලද අවදානමට ලක් වූ උපාංගයකින් සංවිධානයේ ජාලය සමඟ ද්වේෂසහගත අන්තර්ක්‍රියාවල නිරත වූ බව දැනුම් දුන් අතර, සංවිධානයේ කැමැත්ත මත, ASD හි ACSC විසින් සංවිධාන ජාලයේ බලපෑමට ලක් වූ ධාරක වෙත සත්කාරක-පාදක සංවේදක යෙදවීය. මෙම සංවේදක මගින් ASD හි ACSC සිදුවීම් ප්‍රතිචාර විශ්ලේෂකයින්ට සම්පූර්ණ ඩිජිටල් වෝහාරික පරීක්ෂණයක් සිදු කිරීමට ඉඩ ලබා දුන්නේය. පවතින සංවේදක දත්ත භාවිතා කරමින්, ASD හි ACSC විශ්ලේෂකයෝ කණ්ඩායමේ ක්‍රියාකාරකම් සාර්ථකව සිතියම්ගත කර නිරීක්ෂණය කරන ලද සිදුවීම් පිළිබඳ සවිස්තරාත්මක කාලරාමුවක් නිර්මාණය කළහ.

ජූලි සිට අගෝස්තු දක්වා, ASD හි ACSC විසින් නිරීක්ෂණය කරන ලද ප්‍රධාන ක්‍රියාකරුගේ ක්‍රියාකාරකම්වලට ඇතුළත් වූයේ:

- එමඟින් ක්‍රියාකරුට තමන්ගේම ජාලයේ සිතියමක් ගොඩනගා ගැනීමට හැකි වන පරිදි ධාරක ගණන් කිරීම;
- ක්‍රියාකරුට ජාලය වෙත ආරම්භක අඩිතාලමක් සහ විධාන ක්‍රියාත්මක කිරීමේ හැකියාවක් ලබා දෙමින් වෙබ් කවච භාවිතා කිරීම; සහ
- ද්වේෂ සහගත අරමුණු සඳහා ක්‍රියාකරුවා විසින් භාවිතා කරන ලද වෙනත් මෙවලම් යෙදවීම.

සංවේදී දත්ත විශාල ප්‍රමාණයක් ප්‍රවේශ වී ඇති බවට සාක්ෂි සහ ක්‍රියාකරුවන් ජාලය හරහා පාර්ශ්වීයව ඉවත් කළ බවට සාක්ෂි විමර්ශනය මගින් අනාවරණය විය (T1021.002). කණ්ඩායම විසින් ජාලය වෙත බහු ප්‍රවේශය සඳහා දෙශික ස්ථාපිත කිරීම, ජාලයට සමතල ව්‍යුහයක් තිබීම, සහ හිතුමතයට ගොනු උඩුගත කිරීමට භාවිතා කළ හැකි අනාරක්ෂිත අභ්‍යන්තරව සංවර්ධනය කරන ලද මෘදුකාංග භාවිතය මගින් අවදානමට ලක් කිරීම සඳහා වඩාත් පහසුකම් සපයන ලදී. කණ්ඩායමට පරිගණකයට පිවිසීමට ඉඩ සලසන ලද වරප්‍රසාදිතව සත්‍යාපනය කළ විශ්වාසනීය තොරතුරු මෙන්ම මුල් ප්‍රවේශ දෙශිකය අවහිර කළහොත් ක්‍රියාකාරීන්ට අනවසර ප්‍රවේශය නැවත ලබා ගැනීමට ඉඩ සලසන ජාල තොරතුරු ද දත්ත ඇතුළත් ධාරක ගණන් කිරීමට ඇතුළත් විය. මුලින් අයුතු ලෙස ප්‍රයෝජනයට ගත් යන්ත්‍රයේ ඒවා හැර වෙනත් කිසිදු ද්වේෂසහගත මෙවලම් සොයා නොගන්නා ලදී; කෙසේ වෙතත්, නීත්‍යානුකූල සහ වරප්‍රසාද ලත් විශ්වාසනීය තොරතුරු වෙත කණ්ඩායමේ ප්‍රවේශය මගින් අතිරේක මෙවලම් සඳහා අවශ්‍යතාවය නිශේධනය කරනු ඇත. විමර්ශනයේ සොයාගැනීම් වලින් පෙනී යන්නේ ප්‍රසිද්ධියේ දන්නා අවදානමකට අවස්ථාවාදී ලෙස ගොදුරු වීමට වඩා වෙනස් ලෙසින්, APT40 විසින් සංවිධානය හිතාමතාම ඉලක්කගත කිරීමට ඉඩ ඇති බවය.

විමර්ශනයේ සොයා ගැනීම්

2022 අගෝස්තු මැද භාගයේදී, රාජ්‍ය අනුග්‍රහය ලත් සයිබර් කණ්ඩායමක් සමඟ අනුබද්ධ බවට විශ්වාස කෙරෙන තහවුරු කරන ලද ද්වේෂසහගත IP ලිපිනයක් අඩුම වශයෙන් ජූලි සහ අගෝස්තු අතර කාලය තුළ සංවිධානයේ පරිගණක ජාල සමඟ අන්තර් ක්‍රියා කර ඇති බවට ASD හි ACSC විසින් සංවිධානයට දැනුම් දුන්නේය. අවදානමට ලක් වූ උපාංගය සුලු ව්‍යාපාරයකට හෝ ගෘහස්ත පරිශීලකයෙකුට අයත් විය හැකිය.

අගෝස්තු අග භාගයේදී, ASD හි ACSC විසින් සංවිධානයට අයත් ජාලයේ ධාරකයන් වෙත ධාරක-පාදක නියෝජිතයෙකු යෙදවූ අතර එමඟින් ජාලය අවදානමට ලක් වීමේ බලපෑමට ලක් වූ බවට සාක්ෂි පෙන්නුම් කළේය.

විමර්ශනයේ උත්සාහයන්ට සහාය විය හැකි සමහර කෘත්‍යයන් ලොග් වීමේ හෝ ජාල නිර්මාණයේ වින්‍යාසය හේතුවෙන් ලබා ගත නොහැකි විය. කෙසේ වෙතත්, ලබා ගත හැකි සියලු දත්ත සැපයීමට සංවිධානය දැක් වූ සූදානම නිසා ASD හි ACSC හි සිදුවීම් ප්‍රතිචාර දක්වන්නන්ට පුළුල් විශ්ලේෂණයක් සිදු කිරීමට සහ ජාලයේ APT40 ක්‍රියාකාරකම් පිළිබඳ අවබෝධයක් ලබා ගැනීමට හැකි විය.

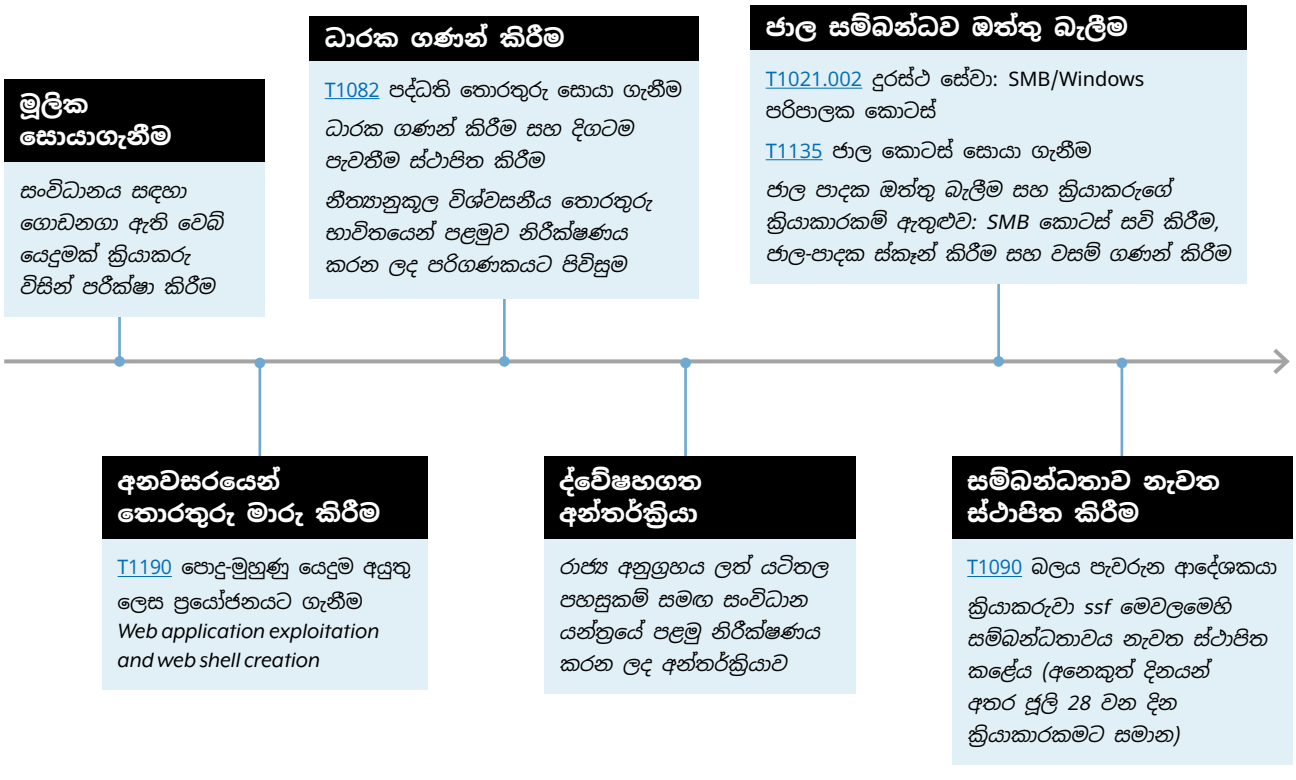
සැප්තැම්බර් මාසයේදී, ASD හි ACSC සමඟ සාකච්ඡා කිරීමෙන් පසු, මූලික දැනුම්දීමේ දී හඳුනාගත් IP ලිපින ප්‍රතික්ෂේප කිරීමට සංවිධානය තීරණය කළේය. ඔක්තෝම්බර් මාසයේදී, සංවිධානය ප්‍රතිකර්ම ආරම්භ කළේය.

විස්තර

ජූලි මාස ආරම්භයේදී, <webapp>2-ext මත ක්‍රියාත්මක වන වෙබ් යෙදුමක් වන (T1190) පරීක්ෂා කර අයුතු ලෙස ප්‍රයෝජනයට ගැනීමට ක්‍රියාකාරීන්ට හැකි වූ අතර එමඟින් කණ්ඩායමට network demilitarized zone (DMZ) හි අඩිතාලමක් ස්ථාපිත කිරීමට හැකිය. ජාලය මෙන්ම සියලුම දෘශ්‍ය වසම් ගණනය කිරීම සඳහා මෙය උත්තෝලනය කරන ලදී. DMZ තුළ බහු යන්ත්‍රවලින් ගොනුවල කොටස් (T1078.002) සවි කිරීම මඟින්, ක්‍රියාකාරී නාමාවලිය (T1018) විමසීමට සහ දත්ත අනවසරයෙන් මාරු කිරීමට අවදානමට ලක් වූ විශ්වසනීය තොරතුරු (T1039) භාවිතා කරන ලදී. (T1558.003) සේවාදායකයකින් ජාලයේ වලංගු විශ්වසනීය තොරතුරු ලබා ගැනීමට ක්‍රියාකරු Kerberoasting ප්‍රහාරයක් සිදු කළේය. DMZ හෝ අභ්‍යන්තර ජාලය තුළ කණ්ඩායමට පැවැත්ම හා සම්බන්ධ අමතර ස්ථාන ලබා ගැනීමට නොහැකි වූ බව නිරීක්ෂණය විය.

දෘශ්‍ය කාලරේඛාව

පහත දැක්වෙන කාලරේඛාවමඟින් සංවිධාන ජාලය තුළ නිරීක්ෂණය කරන ලද ද්වේෂසහගත ක්‍රියාකරුගේ ක්‍රියාකාරකම්වල ප්‍රධාන අවධීන් පිළිබඳ පුළුල් විග්‍රහයක් සපයයි.



සවිස්තරාත්මක කාලරේඛාව

ජුලි: ක්‍රියාකරුවන් විසින් සංවිධානය සඳහා ගොඩනගා ඇති අභිරුචි වෙබ් යෙදුමක (T1190) මුල් පිටුවට ප්‍රවාහන ස්ථර ආරක්ෂණ (TLS) සම්බන්ධතාවයක් (T1102) හරහා මූලික සම්බන්ධතාවයක් ස්ථාපිත කරන ලදී. (මින් ඉදිරියට 'වෙබ් යෙදුම' හෝ 'වෙබ් යෙදුම' ලෙස හැඳින්වේ) වෙනත් කිසිදු කැපී පෙනෙන ක්‍රියාකාරකමක් නිරීක්ෂණය නොවීය.

ජුලි: වැඩිදුර විමර්ශනය කිරීම සඳහා ක්‍රියාකාරීන් වෙබ් යෙදුමේ වෙබ් අඩවිය ගණන් කිරීමට පටන් ගන්නේ අන්ත ලක්ෂ්‍ය සොයමිනි.

ජුලි: සුවිශේෂ අන්ත ලක්ෂයකින් අයුතු ප්‍රයෝජන ගැනීමේ උත්සාහයන් වෙත ක්‍රියාකරුවෝ අවධානය යොමු කරති.

ජුලි: ක්‍රියාකරුවන්ට වෙබ් සේවාදායකයට සාර්ථකව `POST` සිදු කිරීමට, බොහෝ විට වෙනත් පිටුවක තබා ඇති වෙබ් කවචයක් හරහා, හැකි වේ,.

එකම ක්‍රියාකරුවන් විසින් භාවිතා කිරීමට ඉඩ ඇති, දෙවන IP ලිපිනයක් ද එම URL එකට ස්ථාපනය කිරීම ආරම්භ කරයි.

ක්‍රියාකරුවෝ විසින් සුදුසු ලෙස හැඟෙන වෙබ් කවච ගණනාවක් නිර්මාණය කර පරීක්ෂා කළෝය.

අයුතු ලෙස ප්‍රයෝජන ගැනීමේ නිශ්චිත ක්‍රමය නොදන්නා නමුත්, නිශ්චිත අන්ත ලක්ෂ්‍යය `<webapp>2-ext` හි ගොනු නිර්මාණය කිරීමට ඉලක්ක කර ඇති බව පැහැදිලි වේ.

ASD හි ACSC විශ්වාස කරන්නේ ඔවුන්ගේ බෙදාගත් උනන්දුව සහ මිනිත්තු කිහිපයක් අතරදී සිදුවන ආරම්භක සම්බන්ධතා හේතුවෙන් IP ලිපින සම්බන්ධතා දෙක එකම ආක්‍රමණයක කොටසක් බවයි.

ජුලි: සමූහය විසින් ධාරක ගණන් බැලීම දිගටම කරගෙන යන අතර, වරප්‍රසාද තීව්‍ර කිරීමේ අවස්ථා සොයමින් සහ වෙනස් වෙබ් කවචයක් යෙදවීම සිදු කරයි. ක්‍රියාකරුවෝ `<firstname.surname>@<organisation domain>` සඳහා අවදානමට ලක් වූ විශ්වාසනීය තොරතුරු භාවිතා කරමින් වෙබ් යෙදුමට පිවිසෙති.

ක්‍රියාකරුවන්ගේ ක්‍රියාකාරකම් `<webapp>2-ext` හි වරප්‍රසාද තීව්‍ර කිරීම සාර්ථකව මුදුන්පත් කරගෙන ඇති බවක් නොපෙනේ.

ඒ වෙනුවට, ක්‍රියාකරුවෝ ජාල-පාදක ක්‍රියාකාරකම් වෙනස් කිරීමට යොමු වෙති.

ජුලි: ක්‍රියාකරුවා අවදානමට ලක් වූ විශ්වසනීය තොරතුරු සේවා ගිණුමක් සඳහා පරීක්ෂා කර එය අභ්‍යන්තරව ප්‍රවේශ විය හැකි ද්විමය ගොනුවල දෘඪ කේතනය කර ඇති බව සොයා ගැනීමට ඉඩ ඇත.

ජුලි: ක්‍රියාකරුවන් විසින් ද්වේෂසහගත යටිතල පහසුකම් වෙත සම්බන්ධ වීමට භාවිතා කරන විවෘත මූලාශ්‍ර මෙවලම, Secure Socket Funnelling යොදවයි. මෙම සම්බන්ධතාවය ක්‍රියාකරුගේ ප්‍රහාරක යන්ත්‍රවලින් සංවිධානයේ අභ්‍යන්තර ජාල වෙත ගමනාගමනය සිදු කිරීමට භාවිතා කරන අතර, සේවා ගිණුම සඳහා විශ්වාසනීය තොරතුරු භාවිතා කිරීමට උත්සාහ කරන විට සිදුවීම් ලොග් වල යන්ත්‍ර නාම නිරාවරණය වේ.

අගෝස්තු: ක්‍රියාකාරීන් විසින් සේවා ගිණුමේ සම්බන්ධතා ස්ථාපිත කිරීමට නොහැකි වීම ඇතුළු සීමිත ක්‍රියාකාරකම් ගණනාවක් සිදු කරන බව පෙනේ.

අගෝස්තු: ක්‍රියාකරුවෝ සැලකිය යුතු ජාල සහ ක්‍රියාකාරී නාමාවලි ගණන් කිරීම සිදු කරති. DMZ තුළ ඇති Windows යන්ත්‍රවලට කොටස් සවි කිරීම සඳහා අවදානමට ලක් වූ වෙනස් ගිණුමක් පසුව භාවිතා කරනු ලැබේ. එමඟින් සාර්ථක දත්ත අනවසරයෙන් මාරු කිරීම සක්‍රීය කරයි.

මෙය DMZ තුළ සවි කළ හැකි යන්ත්‍රවල සොරකම් කරන ලද විශ්වාසනීය තොරතුරු අවස්ථාවාදී ලෙස භාවිතා කිරීමක් ලෙස පෙනේ. ක්‍රියාකරුවා විසින් සමාන ක්‍රියාකාරකම් සහිත අභ්‍යන්තර ජාලය ඉලක්ක කර ගැනීම ෆයර්වෝල් මඟින් අවහිර කරන ලදී.

අගෝස්තු - සැප්තැම්බර්: SSF මෙවලම අනිෂ්ට IP ලිපිනය හා සම්බන්ධතාවයක් නැවත ස්ථාපිත කළේය. කණ්ඩායමේ ප්‍රවේශය අවහිර කරන තුරු ඔවුන් කිසිදු අමතර ක්‍රියාකාරකම් සිදු නොකරන බව නිරීක්ෂණය වී ඇත.

සැප්තැම්බර්: සංවිධානය ඔවුන්ගේ ෆයර්වෝල් මත ද්වේෂසහගත IP ලිපිනය ප්‍රතික්ෂේප කිරීම මඟින් එය අවහිර කරයි.

2 මෙම සන්දර්භය තුළ, අන්ත ලක්ෂ්‍යයක් යනු වෙබ් යෙදුමේ කාර්යයකි

3 සේවා ගිණුම් තනි පරිශීලකයින් සමඟ නොව සේවාවන් සමඟ බැඳී ඇත. මයික්‍රොසොෆ්ට් ආයතනික වසමක, විවිධ ආකාරයේ ගිණුම් තිබේ.

4 පරිශීලකයෙකුට හෝ පරිශීලක කණ්ඩායමකට ප්‍රවේශ විය හැකි ගොනු පද්ධති ව්‍යුහයක් තුළ ගොනු තැන්පත් කිරීමේ ක්‍රියාවලිය කොටස් සවි කිරීම වේ.

ක්‍රියාකාරක උපක්‍රම සහ ශිල්පීය ක්‍රම

MITRE ATT&CK රාමුව යනු සයිබර් අවකාශයේ තර්ජනාත්මක ක්‍රියාකාරීන් විසින් භාවිතා කරන උපක්‍රම සහ ශිල්පීය ක්‍රම පිළිබඳ ලේඛනගත එකතුවකි. මෙම රාමුව එක්සත් ජනපදයේ ලාභ නොලබන MITRE සංස්ථාව විසින් නිර්මාණය කරන ලද අතර තර්ජනාත්මක ක්‍රියාකාරී හැසිරීම වටා පොදු ගෝලීය භාෂාවක් ලෙස ක්‍රියා කරයි. ASD හි ACSC විසින් ක්‍රියාකරුගේ ද්වේෂසහගත ක්‍රියාකාරකම් වලට අදාළ වන පහත සඳහන් ශිල්පීය ක්‍රම සහ උපක්‍රම තක්සේරු කරයි:

ඔත්තු බැලීම

T1594 – වින්දිතයා සතු වෙබ් අඩවි සොයන්න

ජාලයට ප්‍රවේශ වීමේ අවස්ථා හඳුනා ගැනීම සඳහා ක්‍රියාකරුඅභිරුචි වෙබ් යෙදුමේ වෙබ් අඩවිය ලැයිස්තුගත කළේය.

ආරම්භක ප්‍රවේශය

T1190 – පොදු-මුහුණු යෙදුම අයුතු ලෙස ප්‍රයෝජනයට ගැනීම (අභිරුචි වෙබ් යෙදුම අයුතු ලෙස ප්‍රයෝජනයට ගැනීම සම්බන්ධයෙන්)

T1078.002 – වලංගු ගිණුම්: වසම් ගිණුම් (අවදානමට ලක් වූ විශ්වසනීය තොරතුරු සමඟ ලොග් වීම සම්බන්ධයෙන්)

අන්තර්ජාලයට නිරාවරණය වන අභිරුචි වෙබ් යෙදුම් අයුතු ලෙස ප්‍රයෝජනයට ගැනීම මගින් ක්‍රියාකරුවාට ප්‍රවේශ වීමේ ආරම්භක ලක්ෂ්‍යයක් සපයයි. පසුව ක්‍රියාකරුවාට ජාලයට ප්‍රවේශය තවදුරටත් පුළුල් කිරීම සඳහා ඔවුන් අවදානමට ලක් කළ විශ්වාසනීය තොරතුරු භාවිතා කිරීමට හැකි විය.

ක්‍රියාත්මක කිරීම

T1059 – විධාන සහ පිටපත් කිරීමේ පරිවර්තකයා (වෙබ් කවචය හරහා විධාන ක්‍රියාත්මක කිරීම සම්බන්ධයෙන්)

T1072 – මෘදුකාංග යෙදවුම් මෙවලම් (ක්‍රියාකරුවා IP ලිපිනයට සම්බන්ධ වීමට Secure Socket Funnelling (SSF) විවෘත මූලාශ්‍ර මෙවලම කිරීම සම්බන්ධයෙන්)

දිගටම පැවතීම

T1505.003 – සේවාදායක මෘදුකාංග සංරචකය:

වෙබ් කවචය (ප්‍රවේශය ස්ථාපිත කිරීම සඳහා වෙබ් කවචයක් සහ SSF භාවිතා කිරීම සම්බන්ධයෙන්)

විශ්වසනීය තොරතුරු වෙත ප්‍රවේශ වීම

T1552.001 – මුරපද ගබඩාවලින් විශ්වාසනීය තොරතුරු (ගොඩනැගිලි කළමනාකරණ පද්ධතියට (BMS) අදාළ මුරපද ගොනු සම්බන්ධයෙන්)

T1558.003 – Kerberos ටිකට්පත් සොරකම් කිරීම හෝ ව්‍යාජ ලෙස සකස් කිරීම: Kerberoasting (ජාලයේ විශ්වාසනීය තොරතුරු ලබා ගැනීම සඳහා සිදු කරන ප්‍රහාරය සම්බන්ධයෙන්)

පාර්ශ්වික චලනය

T1021.002 – දුරස්ථ සේවා: SMB කොටස් (බහු උපාංග මගින් SMB කොටස් සවි කරන ක්‍රියාකරුවා සම්බන්ධයෙන්)

එකතු කිරීම

T1213 – තොරතුරු ගබඩාවලින් ලබා ගන්නා දත්ත (BMS හි අඩංගු සේවාදායකයේ ඇති අත්පොත්/ලේඛන සම්බන්ධයෙන්)

අනවසරයෙන් තොරතුරු මාරු කිරීම

T1041 – C2 නාලිකාව හරහා බැහැර කිරීම (ක්‍රියාකාරී නාමාවලියෙන් සහ සවිකිරීමේ කොටස් වලින් ක්‍රියාකරුගේ දත්ත බැහැර කිරීම සම්බන්ධයෙන්)

ප්‍රත්‍යක අධ්‍යයනය 2

පුළුල් ලෙස බෙදා හැරීමට හැකිවන පරිදි මෙම වාර්තාව නිර්නාමික කර ඇත. බලපෑමට ලක් වූ සංවිධානය මින් ඉදිරියට 'සංවිධානය' ලෙස හැඳින්වේ. ASD හි ACSC හි වින්දිතයාගේ අනන්‍යතාවය සහ සිදුවීම් ප්‍රතිචාර ක්‍රම ආරක්ෂා කිරීම සඳහා සමහර විශේෂිත තොරතුරු ඉවත් කර ඇත.

විධායක සාරාංශය

2022 අප්‍රේල් මාසයේදී සංවිධාන ජාලය සාර්ථකව අවදානමට ලක් කිරීම පිළිබඳ ASD හි ACSC විමර්ශනයේ සොයාගැනීම් මෙම වාර්තාවෙන් විස්තර කෙරේ. නිරීක්ෂිත ද්වේෂසහගත ක්‍රියාකාරකම් සාරාංශගත කිරීමට සහ ප්‍රතිකර්ම නිර්දේශ සකස් කිරීමට මෙම විමර්ශන වාර්තාව සංවිධානයට ලබා දෙන ලදී. සොයාගැනීම්වලින් පෙනී යන්නේ අවදානමට ලක් කිරීම APT40 විසින් සිදු කර ඇති බවයි.

2022 මැයි මාසයේදී, ASD හි ACSC විසින් 2022 අප්‍රේල් මාසයේ සිට සංවිධානයේ ජාලයට බලපාන සැක සහිත ද්වේෂසහගත ක්‍රියාකාරකම් පිළිබඳව සංවිධානයකට දැනුම් දෙන ලදී. පසුව, අන්තර්ජාල මුහුණත් සේවාදායකයක ද්වේෂසහගත මෘදුකාංගයක් සොයා ගත් බව සංවිධානය ASD හි ACSC වෙත දැනුම් දුන්නේය. එය සංවිධානයේ ආයතනික දුරස්ථ ප්‍රවේශ විසඳුම සඳහා පිවිසුම් වීමේ පෝටලය සැපයුවේය. මෙම සේවාදායකය දුරස්ථ ප්‍රවේශ පිවිසුම් සහ අනන්‍යතා කළමනාකරණ නිෂ්පාදනයක් භාවිතා කළ අතර එය මෙම වාර්තාවේ 'අවදානමට ලක් වූ උපකරණය' ලෙස හඳුන්වනු ලැබේ.

ASD හි ACSC විසින් සිදු කරන ලද විමර්ශනයට ප්‍රතිචාර වශයෙන් සංවිධානය සඳහා සංවර්ධනය කරන ලද විමර්ශන සොයාගැනීම් සහ ප්‍රතිකර්ම උපදෙස් මෙම වාර්තාවෙන් විස්තර කෙරේ.

අඩුම වශයෙන් 2022 අප්‍රේල් මාසයේ සිට සංවිධානයේ දුරස්ථ ප්‍රවේශ පිවිසුම් පෝටලය හරහා ද්වේෂසහගත සයිබර් ක්‍රියාකරුවන් විසින් සංවිධාන ජාලයේ කොටසක් අවදානමට ලක් කර ඇති බව සාක්ෂිවලින් පෙනී ගියේය. මෙම සේවාදායකය බහු ක්‍රියාකාරීන් විසින් අවදානමට ලක් කර ඇති අතර, අවදානමට ලක් වූ කාලය පුරා පුළුල් ලෙස ප්‍රචාරය කරන ලද දුරස්ථ කේත ක්‍රියාත්මක කිරීමේ (RCE) අවදානමකින් එය බලපෑමට ලක් විය හැකිය.

ASD හි ACSC විසින් නිරීක්ෂණය කරන ලද ක්‍රියාකාරීන්ගේ ප්‍රධාන ක්‍රියාකාරකම් අතරට ඇතුළත් වන්නේ:

- ධාරක ගණන් කිරීම, එමඟින් ක්‍රියාකරුවෙකුට තමන්ගේම ජාලයේ සිතියමක් ගොඩනගා ගැනීමට හැකි වේ;
- ක්‍රියාකරුට ජාලය වෙත ආරම්භක අඩිතාලමක් දැමීමේ සහ විධාන ක්‍රියාත්මක කිරීමේ හැකියාව ලබා දෙමින්, අන්තර්ජාලයට මුහුණ දෙන යෙදුම් සහ වෙබ් කවච භාවිතය අයුතු ලෙස ප්‍රයෝජනයට ගැනීම;
- වරප්‍රසාද තීව්‍ර කිරීම සඳහා මෘදුකාංග අවදානම් අයුතු ලෙස ප්‍රයෝජනයට ගැනීම; සහ
- පාර්ශ්වික චලනය සක්‍රීය කිරීම සඳහා විශ්වසනීය තොරතුරු එකතු කිරීම; සහ

2022 අප්‍රේල් මාසයේදී, ද්වේෂසහගත ක්‍රියාකරුවෙකු අවදානමට ලක් වූ උපකරණයේ අනන්‍ය පරිශීලක නාම සහ මුරපද යුගල සිය ගණනක් මෙන්ම දුරස්ථ ප්‍රවේශ සැසිවලට අදාළ බහු-සාධක සත්‍යාපන කේත සහ තාක්ෂණික කෞතුක වස්තු ගණනාවක් ඉවත් කර ඇති බව ASD හි ACSC විසින් සොයා ගන්නා ලදී. සංවිධානය විසින් කරන ලද සමාලෝචනයකින් පසු, මුරපද නීත්‍යානුකූල බව සොයා ගන්නා ලදී. නීත්‍යානුකූල පරිශීලකයෙකු ලෙස දුරස්ථ පිවිසුම් සැසියක් පැහැර ගැනීමට හෝ නිර්මාණය කිරීමට සහ නීත්‍යානුකූල පරිශීලක ගිණුමක් භාවිතයෙන් සංවිධානයේ අභ්‍යන්තර ආයතනික ජාලයට ප්‍රවේශ වීමට ක්‍රියාකරුවා මෙම තාක්ෂණික කෞතුක වස්තු එකතු කර ඇති බව ASD හි ACSC තක්සේරු කරයි.

විමර්ශනයේ සොයා ගැනීම්

විමර්ශනයේ සාරාංශය

ASD හි ACSC විසින් තීරණය කළේ සංවිධානයේ කාර්ය මණ්ඩලයට දුරස්ථ පිවිසුම් සැසි සපයන උපාංගය(යන්) ක්‍රියාකරුවා අවදානමට ලක් කළ බවත්, වැඩිදුර ක්‍රියාකාරකම් සිදු කිරීමට මෙම අවදානම භාවිතා කළ බවත්ය. මෙම උපකරණ ප්‍රවේශන-සමතුලිත ධාරක තුනකින් සමන්විත වන අතර එහිදී අවදානමට කළ කිරීමේ මුල්ම සාක්ෂි අනාවරණය විය. ආරම්භක අවදානමට ලක් කිරීමෙන් ටික කලකට පසු සංවිධානය ප්‍රවේශන-සමතුලිත ධාරක තුනෙන් දෙකක් වසා දැමීය. එහි ප්‍රතිඵලයක් ලෙස, සියලු පසුකාලීන ක්‍රියාකාරකම් තනි ධාරකයක් සිදු විය. අවදානමට ලක් වූ උපකරණය හා සම්බන්ධ අනෙකුත් සේවාදායකයන් ද ඒ හා සමාන ආකාරයකින් ප්‍රවේශන-සමතුලිත කරන ලදී. කියවීමට පහසුව සඳහා, මෙම වාර්තාවේ බොහෝ අවස්ථාවලදී සියලුම අවදානමට ලක් වූ උපකරණ 'තනි උපකරණයක්' ලෙස හැඳින්වේ.

2022 අප්‍රේල් සිට අවදානමට ලක් වූ උපාංගයට වෙබ් කවච යෙදවීම සඳහා ක්‍රියාකරුවා හොඳින් දන්නා අවදානම් භාවිතා කර ඇති බවට විශ්වාස කෙරේ. කණ්ඩායමේ තර්ජනාත්මක ක්‍රියාකාරීන් උපාංගයේ ඉහළ වරප්‍රසාද ලබාගෙන ඇති බවට තක්සේරු කෙරේ. ලොග් වීමේ හැකියාව නොමැතිකම හේතුවෙන් ASD හි ACSC හට ක්‍රියාකාරකම්වල සම්පූර්ණ ප්‍රමාණය තීරණය කිරීමට නොහැකි විය. කෙසේ වෙතත්, උපාංගයේ සාක්ෂි වලින් පෙන්නුම් කරන්නේ කියකරුවෙකු පහත සඳහන් දෑ සපුරාගත් බවයි:

- අව්‍යාජ පරිශීලක නාම සහ මුරපද යුගල සිය ගණනක් එකතු කිරීම; සහ
- ද්වේෂසහගත ක්‍රියාකරුවෙකුට නීත්‍යානුකූල පරිශීලකයෙකු ලෙස අතථ්‍ය ඩෙස්ක්ටොප් යටිතල පහසුකම් (VDI) සැසියකට ප්‍රවේශ වීමට ඉඩ ලබාදිය හැකි තාක්ෂණික කෞතුක වස්තු එකතු කිරීම.

ASD හි ACSC විසින් තක්සේරු කරන්නේ ක්‍රියාකරුවා සංවිධාන ජාලයේ අවදානමට ලක් කිරීම තවදුරටත් ශක්තිමත් කිරීමට උත්සාහ කරන බවය. ක්‍රියාකරුවා විසින් අනවසරයෙන් මාරු කරන ලද කෞතුක වස්තු මගින් ඔවුන්ට නීත්‍යානුකූල පරිශීලකයෙකු ලෙස, සමහරවිට පරිපාලකයින් ඇතුළු ඔවුන් කැමති පරිශීලකයෙකු ලෙස, පෙනී සිටීමින් අතථ්‍ය ඩෙස්ක්ටොප් සැසි පැහැර ගැනීමට හෝ ආරම්භ කිරීමට ඉඩ දිය හැකිය. ක්‍රියාකරු මෙම ප්‍රවේශ දෙශිකය භාවිතා කර දිගටම පැවතීම සහ අනෙකුත් ඉලක්ක සපුරා ගැනීම සඳහා සංවිධාන සේවාවන් තවදුරටත් අවදානමට ලක් කර ඇති බව පෙනේ.

ධාරක සපයන්නා කළමනාකරණය කරන පරිසරය තුළ ඇති අනෙකුත් සංවිධාන උපකරණ අවදානමට ලක් වූ බවට සාක්ෂි පෙන්නුම් කළේ නැත.

ප්‍රවේශය

අවදානමට ලක් වූ උපකරණය සහිත ධාරකය, VDI සැසිවලට සම්බන්ධ වන පරිශීලකයින් සඳහා Active Directory සහ වෙබ් සේවාදායකයක් හරහා සත්‍යාපනය සපයන ලදී (T1021.001).

ස්ථානය	අවදානමට ලක් වූ උපකරණවල ධාරක නාම (ප්‍රවේශන-සමතුලිත)
දත්ත මධ්‍යස්ථානය 1	ධාරක1, ධාරක2, ධාරක3

පරිශීලකයා විසින් උපකරණය භාවිතයෙන් ජනනය කර බාගත කරන ලද සත්‍යාපන ටෝකනයක් ලබා ගත් පසු, VDI වෙත උමං මාර්ගයක් සපයන ප්‍රවේශ ද්වාර ධාරක ද උපකරණ යටිතල ව්‍යුහයෙහි ඇතුළත් විය.

මෙම ධාරකයන්ගෙන් කිසිවක් අවදානමට ලක් වී ඇති බවට සාක්ෂි නොමැත. කෙසේ වෙතත්, ප්‍රවේශ ද්වාර ධාරක ලොග් මගින් දැන හඳුනන අනිෂ්ට IP ලිපින සමඟ සැලකිය යුතු අන්තර්ක්‍රියා ඇති බවට සාක්ෂි පෙන්නුම් කළේය. මෙම ධාරකයේ සිදු වූ ක්‍රියාකාරකම්, හෝ මෙම ධාරක වෙත ළඟා වූ තර්ජනාත්මක ක්‍රියාකරුවාගේ යටිතල පහසුකම් සමඟ ජාල සම්බන්ධතා මෙයින් පිළිබිඹු විය හැකිය. මෙම ක්‍රියාකාරකමේ ස්වභාවය ලබාගත හැකි සාක්ෂි භාවිතයෙන් තීරණය කළ නොහැකි නමුත්, සංවිධානයේ ජාලය තුළ පාර්ශ්වීයව ගමන් කිරීමට සමූහය උත්සාහ කළ බව පෙන්නුම් කරයි (TA0008).

අභ්‍යන්තර ධාරක

ASD හි ACSC අභ්‍යන්තර සංවිධානයේ ජාල අංශයෙන් සීමිත දත්ත විමර්ශනය කළේය. අභ්‍යන්තර සංවිධානයේ ජාල අංශයට බලපා ඇති කළ බව දන්නා උත්සාහයන් හෝ සාර්ථක ද්වේෂසහගත ක්‍රියාකාරකම් අතරට VDI-ආශ්‍රිත කෞතුක වස්තු වෙත ක්‍රියාකරුගේ ප්‍රවේශය, අභ්‍යන්තර SQL සේවාදායකයක් අමාරුවෙන් ලබා ගැනීම (T1505.001), සහ දැන හඳුනන ද්වේෂසහගත IP ලිපින වලින් ප්‍රවේශ ද්වාර උපකරණ (TA0011) හරහා යන බව නිරීක්ෂණය කරන ලද පැහැදිලි කළ නොහැකි ගමනාගමනය ඇතුළත් වේ.

අවදානමට ලක් වූ උපකරණයට ඒවායේ ප්‍රවේශය භාවිතා කරමින්, කණ්ඩායම අව්‍යාජ පරිශීලක නාම, මුරපද (T1003) සහ MFA ටෝකන් අගයන් (T1111) එකතු කළේය. කණ්ඩායම JSON වෙබ් ටෝකන් (JWTs) (T1528) ද එකතු කළේ අතර එය අතථ්‍ය ඩෙස්ක්ටොප් පිවිසුම් සැසි නිර්මාණය කිරීමට භාවිතා කරන සත්‍යාපන කෞතුක වස්තුවක් වේ. අථත්‍ය ඩෙස්ක්ටොප් සැසි (T1563.002) නිර්මාණය කිරීමට හෝ පැහැර ගැනීමට, සහ නීත්‍යානුකූල පරිශීලකයෙකු

ලෙස අභ්‍යන්තර සංවිධාන ජාල අංශයට ප්‍රවේශ වීමට (T1078) ක්‍රියාකරුට මේවා භාවිතා කිරීමට හැකි වන්නට ඇත.

සංවිධානයේ අභ්‍යන්තර ජාලයේ පැවති SQL සේවාදායකයක් (T1505.001) අමාරුවෙන් ලබා ගැනීම සඳහා ක්‍රියාකරුවා අවදානමට ලක් වූ උපකරණය වෙත ප්‍රවේශය ද භාවිතා කළේය. ක්‍රියාකරුවාට මෙම දත්ත වෙත ප්‍රවේශය තිබූ බව පෙනේ.

ප්‍රවේශ ද්වාර උපකරණයෙන් ලබා ගත හැකි සාක්ෂිවලින් හෙළි වූයේ දැන හඳුනන ද්වේෂසහගත IP ලිපින වලින් මෙම උපාංගය හරහා හෝ ජාල ගමනාගමනය වෙතින් සිදු වූ බවයි. ඉහත විස්තර කර ඇති පරිදි, මෙයින් ඇඟවෙන්නේ ද්වේෂසහගත සයිබර් ක්‍රියාකාරීන් අභ්‍යන්තර ජාලයේ ලොකු වෙනස් කිරීමක් සඳහා මෙම උපාංගයට බලපෑම් සිදු කළ බව හෝ භාවිතා කළ බවය.

විමර්ශන කාලරේඛාව

විමර්ශනය අතරතුර සොයාගත් ප්‍රධාන ක්‍රියාකාරකම්වල කාලරාමුවක් පහත ලැයිස්තුවෙන් සපයයි.

වේලාව	සිදුවීම
2022 අප්‍රේල්	දන්නා ද්වේෂසහගත IP ලිපින ප්‍රවේශ ද්වාර සත්කාරක HOST7 සමඟ අන්තර් ක්‍රියා කරයි. අන්තර්ක්‍රියා වල ස්වභාවය තීරණය කළ නොහැකි විය.
2022 අප්‍රේල්	ධාරක1, ධාරක 2 සහ ධාරක 3 යන සියලුම ධාරක, ද්වේෂසහගත ක්‍රියාකරුවෙක් හෝ ක්‍රියාකරුවෝ විසින් අවදානමට ලක් කරන ලද අතර, වෙබ් කවච ධාරක මත තබා ඇත. ධාරක2 හි ලොග් ගොනුවක් නිර්මාණය කිරීම හෝ වෙනස් කිරීම සිදු විය. මෙම ගොනුවේ ද්වේෂසහගත ක්‍රියාකරුවෙකු විසින් ග්‍රහණයකර ගන්නා ලද විශ්වාසනීය තොරතුරු අඩංගු ද්‍රව්‍ය ඇතුළත් වේ. /etc/security/opasswd සහ /etc/shadow ගොනු ධාරක1 සහ ධාරක3 හි වෙනස් කළ අතර, මුරපද වෙනස් කර ඇති බව එයින් පෙන්නුම් කරයි. ධාරක1 හි ඇති සාක්ෂිවලින් පෙනී යන්නේ 'sshuser' පරිශීලකයා සඳහා මුරපදය වෙනස් කර ඇති බවය.
2022 අප්‍රේල්	සංවිධානය විසින් ධාරක2 වසා දමන ලදී. ධාරක1 සහ ධාරක3 මත අමතර වෙබ් කවච (T1505.003) නිර්මාණය කරන ලදී. ධාරක1 හට ධාරක3 වෙතින් එල්ල වූ SSH ප්‍රචන්ඩ බල උත්සාහයන් අත්විඳීමට සිදුවිය. ධාරක3 මත ලොග් ගොනුවක් වෙනස් කරන ලදී (T1070). මෙම ගොනුවේ ද්වේෂසහගත ක්‍රියාකරුවෙකු විසින් ග්‍රහණයකර ගන්නා ලද (T1078) විශ්වාසනීය තොරතුරු අඩංගු ද්‍රව්‍ය ඇතුළත් වේ. (T1528) විසින් JWTs ග්‍රහණය කරගෙන එය ධාරක3 මත ගොනුවකට ප්‍රතිදානය කරන ලදී. සංවිධානය විසින් ධාරක3 වසා දමන ලදී. මෙම කාලයෙන් පසු සියලුම ක්‍රියාකාරකම් සිදු වන්නේ ධාරක1 මත.
2022 අප්‍රේල්	ධාරක1 (T1505.003) හි අතිරේක වෙබ් කවච නිර්මාණය කරන ලදී. JWT ග්‍රහණය කරගෙන එය HOST1 හි ගොනුවකට ප්‍රතිදානය කරන ලදී.
2022 අප්‍රේල්	ධාරක1 (T1505.003) මත අතිරේක වෙබ් කවච නිර්මාණය කර ඇති අතර, දැන හඳුනන ද්වේෂසහගත IP ලිපිනයක් (TA0011) ධාරකය සමඟ අන්තර්ක්‍රියා සිදු කරයි. දැන හඳුනන ද්වේෂසහගත IP ලිපිනයක් ප්‍රවේශ ද්වාර ධාරකය වන ධාරක7 සමඟ අන්තර්ක්‍රියා සිදු කරයි.
2022 මැයි	දැන හඳුනන ද්වේශසහගත IP ලිපිනයක් ප්‍රවේශ ද්වාර ධාරකය වන ධාරක7 (TA0011) සමඟ අන්තර්ක්‍රියා සිදු කළේය. පරිශීලකයෙකු සඳහා සත්‍යාපන සිදුවීමක් HOST1 හි ලොග් වල දැන හඳුනන ද්වේශසහගත IP ලිපිනයකට සම්බන්ධ කර ඇත. මෙම සත්කාරකයේ (T1505.003) අතිරේක වෙබ් කවචයක් නිර්මාණය කර ඇත.
2022 මැයි	HOST1 හි පිටපතක් ක්‍රියාකරුවෙක් විසින් වෙනස් කරන ලදී (T1543). මෙම පිටපතේ අභ්‍යන්තර SQL සේවාදායකයකින් දත්ත ඉවත් කළ හැකි ක්‍රියාකාරීත්වයක් අඩංගු වේ.
2022 මැයි	HOST1 හි අතිරේක ලොග් ගොනුවක් අවසන් වරට වෙනස් කරන ලදී (T1070). මෙම ගොනුවේ සංවිධාන ජාලය සඳහා පරිශීලක නාමය සහ මුරපද යුගල අඩංගු වන අතර ඒවා නීත්‍යානුකූල යැයි විශ්වාස කෙරේ (T1078).
2022 මැයි	අතිරේක ලොග් ගොනුවක් අවසන් වරට වෙනස් කරන ලදී (T1070).අතිරේක ලොග් ගොනුවක් අවසන් වරට වෙනස් කරන ලදී (T1070).
2022 මැයි	HOST1 (T1505.003) හි අමතර වෙබ් කවච නිර්මාණය කරන ලදී. මෙම දිනයේදී, සංවිධානය 2022 අප්‍රේල් මාසයේ නිර්මාණ දිනය සහිත වෙබ් කවචයක් සොයා ගැනීම ASD හි ACSC වෙත වාර්තා කළේය
2022 මැයි	LOg4jHotPatch.jar ලෙස නම් කරන ලද එකක් ඇතුළුව HOST1 හි පිටපත් ගණනාවක් නිර්මාණය කරන ලදී.
2022 මැයි	විවෘත ද්වාර දෙකක් ප්‍රවේශ ද්වාර ධාරකයට එකතු කිරීමට iptables-save විධානය භාවිතා කරන ලදී. ද්වාරයන වූයේ 9998 සහ 9999 (T1572) ය.

ක්‍රියාකරුගේ උපක්‍රම සහ ශිල්පීය ක්‍රම

විමර්ශනය අතරතුර දී හඳුනාගත් උපක්‍රම සහ ශිල්පීය ක්‍රම කිහිපයක් පහත දැක්වේ

ආරම්භක ප්‍රවේශය

T1190 පොදු මුහුණ දීමේ යෙදුම අයුතු ලෙස ප්‍රයෝජනයට ගැනීම

ආරම්භක ප්‍රවේශය ලබා ගැනීම සඳහා කණ්ඩායම විසින් දුරස්ථ ප්‍රවේශ පිවිසුම් සහ අනන්‍යතා කළමනාකරණ නිෂ්පාදිතය තුළ RCE, වරප්‍රසාද තීව්‍ර කිරීම, සහ සත්‍යාපන මඟ හැරීමේ අවදානම්, අයුතු ලෙස ප්‍රයෝජනයට ගැනීමට බොහෝ දුරට ඉඩක් තිබුණි.

පහත සඳහන් හේතු මත, මෙම ආරම්භක ප්‍රවේශ ක්‍රමවේදය භාවිතා කිරීමට බොහෝ දුරට ඉඩ ඇති බව සැලකේ:

- ඒ වනවිට සේවාදායකය මෙම CVE වලට ගොදුරුවීමේ අවදානමක් තිබුණි:
- දැන හඳුනන යටිතල පහසුකම් මගින් මෙම අවදානම් අයුතු ලෙස ප්‍රයෝජනයට ගැනීමට උත්සාහ කිරීම; සහ
- පළමු දැන හඳුනන අභ්‍යන්තර ද්වේෂසහගත ක්‍රියාකාරකම සිදු වූයේ අයුතු ලෙස ප්‍රයෝජන ගැනීමේ උත්සාහයන් සිදු කිරීමෙන් ටික කලකට පසුවය.

ක්‍රියාත්මක කිරීම

T1059.004 විධාන සහ පිටපත් කිරීමේ පරිවර්තකයා: Unix Shell

ඉහත අවදානම් සාර්ථකව ප්‍රයෝජනයට ගත් කණ්ඩායමට බලපෑමට ලක් වූ උපකරණයෙන් ලබාගත් Unix කවචයක තිබූ විධාන ක්‍රියාත්මක කිරීමට හැකි වන්නට ඇත. ක්‍රියාකරුවන් විසින් ක්‍රියාත්මක කරන විධාන උපකරණය මගින් ලොග් කර නොමැති බැවින්, ඒවා පිළිබඳ සම්පූර්ණ විස්තර සැපයිය නොහැක.

දිගටම පැවතීම

T1505.003 සේවාදායක මෘදුකාංග සංරචකය: Web Shell

බලපෑමට ලක් වූ උපකරණය මත ක්‍රියාකරුවන් විසින් වෙබ් කවච කිහිපයක් යොදවා ඇත. විවිධ නිශ්චිත ක්‍රියාකාරීන් විසින් වෙබ් කවච යෙදවූ බව සිතිය හැකි නමුත්, මෙම වෙබ් කවච භාවිතා කරමින් ක්‍රියාකාරකම් සිදු කළේ කියකරුවන් කුඩා සංඛ්‍යාවක් පමණි. වෙබ් කවච මගින් අවදානමට ලක් වූ උපකරණ මත ක්‍රියාකරුට හිතුමතයට විධාන ක්‍රියාත්මක කිරීමට ඉඩ දුන්න විය හැකිය.

වරප්‍රසාද තීව්‍ර කිරීම

T1068 වරප්‍රසාද තීව්‍ර කිරීම සඳහා අයුතු ප්‍රයෝජන ගැනීම

ලබාගත් හැකි සාක්ෂි මගින් ක්‍රියාකරුවා ලබා ගන්නා වරප්‍රසාද මට්ටම විස්තර නොකෙරේ. කෙසේ වෙතත්, වෙබ් කවච භාවිතා කිරීමෙන්, ක්‍රියාකරුවන්ට අවදානමට ලක් වූ උපාංගයේ වෙබ් සේවාදායකය හා සමාන වරප්‍රසාද මට්ටමක් ලබා ගැනීමට හැකිය ඇත. අවදානමට ලක් වූ උපාංගයේ තිබූ බවට විශ්වාස කෙරෙන අවදානම් හේතුවෙන් ක්‍රියාකරුවන්ට මූල වරප්‍රසාද ලබා ගැනීමට හැකි වනු ඇත.

විශ්වසනීය තොරතුරු වෙත ප්‍රවේශ වීම

T1056.003 ඇතුළු කිරීමේ ග්‍රහණය: වෙබ් පෝටල් ග්‍රහණය

අවදානමට ලක් වූ උපකරණයේ සාක්ෂිවලින් පෙනී ගියේ ක්‍රියාකරුවා නීත්‍යානුකූල යැයි විශ්වාස කරන පැහැදිලි පාඨයකින් පරිශීලක නාම-මුරපද යුගල සිය ගණනක් ග්‍රහණය කරගත් බවය. ගොනුවකට විශ්වාසනීය තොරතුරු ප්‍රතිදානය කරන අව්‍යාජ සත්‍යාපන ක්‍රියාවලියේ යම් වෙනස් කිරීමක් භාවිතා කරමින් මේවා ග්‍රහණය කරගෙන ඇති බව පෙනේ.

T1111 බහු-සාධක සත්‍යාපන අන්තර්ග්‍රහණය

ීත්‍යානුකූල පිවිසුම් වලට අනුරූප වන MFA ටෝකනවල අගය ද ක්‍රියාකරුවා ග්‍රහණය කර ගත්තේය. මෙම අගයන් ගොනුවකට ප්‍රතිදානය කිරීම සඳහා අව්‍යාජ සත්‍යාපන ක්‍රියාවලිය වෙනස් කිරීම මගින් ඒවා ග්‍රහණය කර ගැනීමට ඉඩ තිබුණි. MFA ටෝකනවල ආරක්ෂාව සඳහා සපයන අද්විතීය අගයන් ගබඩා කරන 'රහස් සේවාදායකය' අවදානමට ලක් වූ බවට කිසිදු සාක්ෂියක් නොමැත.

T1040 ජාල ආඝ්‍රාණය

ක්‍රියාකරුවා විසින් අවදානමට ලක් වූ උපකරණයේ HTTP ගමනාගමනය ග්‍රහණය කර ගැනීමෙන් JWT ග්‍රහණය කරගත් බවට විශ්වාස කෙරේ. අවදානමට ලක් වූ උපකරණය මත utility tcpdump ක්‍රියාත්මක කළ බවට සාක්ෂි තිබේ, ක්‍රියාකරුවා විසින් මෙම JWT ග්‍රහණය කරගත් ආකාරය එසේ සිදු විය හැකිය.

T1539 වෙබ් සැසි කුකිය සොරකම් කිරීම

ඉහත විස්තර කළ පරිදි, ක්‍රියාකරුවා වෙබ් සැසි කුකීස් වලට සමාන JWT ග්‍රහණය කර ගත්තේය. වැඩිදුර ප්‍රවේශය ස්ථාපිත කිරීම සඳහා ක්‍රියාකරුවා විසින් මේවා නැවත භාවිතා කර තිබිය හැකිය.

සොයා ගැනීම

T1046 ජාල සේවා සොයාගැනීම

එකම ජාල කොටසේ අනෙකුත් උපකරණ ස්කෑන් කිරීම සඳහා ජාල පරිලෝකන උපයෝගිතා nmap අවදානමට ලක් වූ උපාංගය මත ක්‍රියාත්මක කර ඇති බවට සාක්ෂි තිබේ. පාර්ශ්වීය චලනය සඳහා අවස්ථා ඉදිරිපත් කළ හැකි වෙනත් ළඟා විය හැකි ජාල සේවා සොයා ගැනීමට නළුවා විසින් මෙය භාවිතා කර ඇති බව පෙනේ.

එකතු කිරීම

පවතින සාක්ෂි මගින් ක්‍රියාකරුවන් දත්ත රැස් කළ ආකාරය හෝ අවදානමට ලක් වූ උපකරණයෙන් හෝ වෙනත් පද්ධතිවලින් හරියටම එකතු කළ දේ හෙළි නොකරයි. කෙසේ වෙතත්, ග්‍රහණය කරගත් විශ්වාසනීය තොරතුරු (T1003), MFA ටෝකන් අගයන් (T1111) සහ ඉහත විස්තර කර ඇති JWT ඇතුළුව අවදානමට ලක් වූ උපකරණයේ සියලුම ගොනු වෙත ක්‍රියාකරුවන්ට ප්‍රවේශය තිබූ බව පෙනේ.

විධාන සහ පාලනය

T1071.001 යෙදුම් ස්ථර ප්‍රොටෝකෝල: වෙබ් ප්‍රොටෝකෝල

විධාන සහ පාලනය සඳහා ක්‍රියාකරුවෝ වෙබ් කවච භාවිතා කළෝය. උපකරණයේ දැනට පවතින වෙබ් සේවාදායකය (T1572). භාවිතයෙන් වෙබ් කවච විධාන HTTPS නොසලකා හරින්නට ඇත

T1001.003 දත්ත අපැහැදිලි කිරීම: ප්‍රොටෝකෝල අනුකරණය

නීත්‍යනුකූල ගමනාගමනය සමඟ මිශ්‍ර වීම සඳහා නිර්මාණය කර ඇති ප්‍රහාර සඳහා ආරම්භක ස්ථානයක් ලෙස ක්‍රියාකරුවෝ අවදානමට කළ වූ උපාංග භාවිතා කළෝය.

හඳුනාගැනීමේ සහ ලිහිල් කිරීමේ නිර්දේශ

ASD හි ACSC දැඩි ලෙස නිර්දේශ කරන්නේ ASD Essential Eight පාලන සහ ඒ ආශ්‍රිත සයිබර් ආරක්ෂණ සිදුවීම් අවම කිරීම සඳහා උපාය මාර්ග ක්‍රියාත්මක කිරීමයි. APT40 මගින් ආක්‍රමණයන් හඳුනා ගැනීමට සහ වැළැක්වීමට ගත යුතු ජාල ආරක්ෂක ක්‍රියාමාර්ග සඳහා නිර්දේශ පහත දැක්වේ. ඉන්පසු ප්‍රධාන TTP හතර සඳහා නිශ්චිත ලිහිල් කිරීම් 1 වගුවේ සාරාංශ කර ඇත.

සොයා ගැනීම

ඉහත හඳුනාගත් සමහර ගොනු C:\Users\Public* සහ C:\Windows\Temp* වැනි ස්ථානවල ද බැහැර කර ඇත. සාමාන්‍යයෙන් දත්ත සෑමට ප්‍රවේශ විය හැකි බැවින් ඒවා ලිවීම සඳහා මෙම ස්ථාන පහසු ස්ථාන විය හැකිය. එනම්, Windows හි ලියාපදිංචි කර ඇති සියලුම පරිශීලක ගිණුම් වලට මෙම නාමාවලි සහ ඒවායේ උප නාමාවලි වෙත ප්‍රවේශය තිබේ. බොහෝ විට, ඕනෑම පරිශීලකයෙකුට පසුව මෙම ගොනු වෙත ප්‍රවේශ විය හැකි අතර පාර්ශ්වීය චලනය, ආරක්ෂක මගහැරීම, අඩු වරප්‍රසාද ක්‍රියාත්මක කිරීම සහ අනවසරයෙන් තොරතුරු මාරු කිරීම සඳහා අවස්ථා ලබා දේ.

පහත දැක්වෙන Sigma නීති මගින් අසාමාන්‍ය ක්‍රියාකාරකම්වල දර්ශකයක් ලෙස සැක සහිත ස්ථානවලින් කෙරෙන ක්‍රියාත්මක කිරීම ගැන සොයා බලයි. සෑම අවස්ථාවලදීම, ද්වේෂසහගත ක්‍රියාකාරකම් සහ ආරෝපණය තහවුරු කිරීම සඳහා පසුකාලීන විමර්ශනයක් අවශ්‍ය වේ.

ලේඛනයේ නාමය: ලෝකයේ ලිවීමට හැකි දේ ක්‍රියාත්මක කිරීම - තාවකාලික

අනන්‍යතාවය: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

විස්තරය: C:\Windows\Temp. වෙතින් ක්‍රියාවලි ක්‍රියාත්මක කිරීම ඉවත් කිරීම

පසුබිම:

මෙම රීතිය විශේෂයෙන් C:\Windows\Temp* වෙතින් ක්‍රියාත්මක කිරීම සඳහා සොයා බලයි. Temp වඩාත් පුළුල් ලෙස භාවිතා කරනු ලබන්නේ benign යෙදුම් මගින් වන අතර එබැවින් එය C:\Windows හි අඩංගු සෑමට ප්‍රවේශ විය කැකි අනෙකුත් උප බහලුම් වලින් ක්‍රියාත්මක කිරීමට වඩා අඩු විශ්වාසනීය ද්වේෂසහගත දර්ශකයකි.

SYSTEM හෝ NETWORK SERVICE පරිශීලකයින් විසින් ක්‍රියාත්මක කරන ලද යෙදුම් ඉවත් කිරීමෙන් මෙම රීතිය මගින් තෝරාගත් benign ක්‍රියාකාරකමේ ප්‍රමාණය සැලකිය යුතු ලෙස අඩු කරයි.

මෙයින් අදහස් කරන්නේ රීතියට ඉහළ වරප්‍රසාද මට්ටමකින් ද්වේෂසහගත ක්‍රියාත්මක කිරීම් මග හැරිය හැකි නමුත් පරිශීලකයෙකු SYSTEM වෙත වරප්‍රසාද ඉහළ නැංවීමට උත්සාහ කරන්නේද යන්න තීරණය කිරීමට වෙනත් නීති භාවිතා කිරීම නිර්දේශ කෙරෙන බවයි.

විමර්ශනය:

1. පරිශීලක සන්දර්භය, ක්‍රියාත්මක කිරීමේ අඛණ්ඩතා මට්ටම, ක්ෂණික පසු විපරම් ක්‍රියාකාරකම් සහ ගොනුව මඟින් දමන ලද රූප වැනි මෙම ගොනු ක්‍රියාත්මක කිරීම සමඟ සෘජුවම සම්බන්ධ තොරතුරු පරීක්ෂා කරන්න.
2. ක්‍රියාකාරකම ද්වේෂසහගත ද යන්න තක්සේරු කිරීමට උපකාර කිරීම සඳහා සන්දර්භීය ක්‍රියාවලිය, ජාලය, ගොනුව සහ ධාරකයේ අනෙකුත් සහායක දත්ත විමර්ශනය කරන්න.
3. අවශ්‍ය නම්, එය නීත්‍යානුකූලද යන්න තීරණය කිරීමට ප්‍රතිවර්ත ඉංජිනේරු විද්‍යාව සඳහා ගොනුවේ පිටපතක් එකතු කිරීමට උත්සාහ කරන්න.

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

කර්තෘ: ASD හි ACSC

දිනය: 2024/06/19

තත්ත්වය: පර්යේෂණාත්මක

ටැග්:

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

ලොග් මූලාශ්‍රය:

ප්‍රභේදය: process_creation
නිෂ්පාදිතයproduct: windows

සොයා ගැනීම:

```
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:
    පරිශීලකයා:
    - 'පද්ධතිය'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

තත්ත්වය: temp වන අතර (common_temp_path හෝ system_user හෝ dismhost හෝ known_parent) නොවේ

අසත්‍ය ධනාත්මක කරුණු:

- Temp වෙතින් ක්‍රියාත්මක කළ හැකි ඒවා Allowlist විගණන යෙදුම් මගින් ක්‍රියාත්මක වන බව නිරීක්ෂණය වී ඇත.
- Temp හි නීත්‍යානුකූලව සැකසුම් යෙදුම් සහ දියත් කිරීම් මාලාවක් අඩංගු වේ. එබැවින් මෙම රීතිය යෙදවීමට පෙර නිරීක්ෂණය කරන ලද ජාලයක මෙම හැසිරීම කෙතරම් ප්‍රචලිතද යන්න (සහ එය අවසර ලැයිස්තු ගත කළ හැකිද නැද්ද යන්න) සලකා බැලීම වටී.

මට්ටම: පහල

ලේඛනයේ නාමය: පරිශීලකයින්ට ප්‍රවේශ විය හැකි දේ ක්‍රියාත්මක කිරීම - Non-Temp පද්ධතියේ උප නාමාවලිය

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

විස්තරය: Windows OS ස්ථාපන ස්ථානයේ උප නාමාවලියක පරිශීලකයින්ට ප්‍රවේශ විය හැකි ස්ථානයකින් ක්‍රියාත්මක කෙරෙන ක්‍රියාවලිය සොයා ගන්න.

පසුබිම:

මෙම රීතිය C:\ සහ විශේෂයෙන් C:\Windows* තුළ අඩංගු පරිශීලකයින්ට ප්‍රවේශ විය හැකි නාමාවලි, C:\Windows\Temp හැර (එය benign යෙදුම් මගින් වඩාත් පුළුල් ලෙස භාවිතා කරන අතර එම නිසා අඩු විශ්වාසනීය ද්වේෂසහගත දර්ශකයකි), ක්‍රියාත්මක කිරීම සඳහා ය. ගොනුවක් SYSTEM ලෙස ක්‍රියාත්මක කරන්නේ නම් AppData ෆෝල්ඩර බැහැර කරනු ලැබේ - මෙය බොහෝ තාවකාලික යෙදුම් ගොනු ක්‍රියාත්මක කිරීමේ හිතකර ක්‍රමයකි.

ආරම්භක ජාල මූලික රේඛාවක් සම්පූර්ණ කිරීමෙන් සහ මෙම ස්ථාන වලින් දන්නා ලද හිතකර ක්‍රියාත්මක කිරීම් හඳුනා ගැනීමෙන් පසු, මෙම රීතිය කලාතුරකින් ක්‍රියාත්මක විය යුතුය.

විමර්ශනය:

1. පරිශීලක සන්දර්භය, ක්‍රියාත්මක කිරීමේ අඛණ්ඩතා මට්ටම, ක්ෂණික පසු විපරම් ක්‍රියාකාරකම සහ ගොනුව මඟින් දමන ලද රූප වැනි මෙම ගොනු ක්‍රියාත්මක කිරීම සමඟ සෘජුවම සම්බන්ධ තොරතුරු පරීක්ෂා කරන්න.
2. ක්‍රියාකාරකම ද්වේෂ සහගතද යන්න තක්සේරු කිරීමට උපකාර කිරීම සඳහා සන්දර්භීය ක්‍රියාවලිය, ජාලය, ගොනුව සහ ධාරකයේ අනෙකුත් සහායක දත්ත විමර්ශනය කරන්න.
3. අවශ්‍ය නම්, එය නීත්‍යානුකූලද යන්න තීරණය කිරීම සඳහා ප්‍රතිවර්ත ඉංජිනේරු විද්‍යාව සඳහා ගොනුවේ පිටපතක් එකතු කිරීමට උත්සාහ කරන්න.

යොමු කිරීම්:

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

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

කර්තෘ: ASD හි ACSC

දිනය: 2024/06/19

තත්ත්වය: පර්යේෂණාත්මක

ටැග්:

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

ලොග් මූලාශ්‍රය:

ප්‍රභේදය: process_creation
නිෂ්පාදිතය: windows

සොයා ගැනීම්:

ලිවිය හැකි_මාර්ගය:
රූපය|අඩංගු දේ:

- ':\\$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:
  රූපය|අන්තර්ගතයන්:'\\AppData\\'
  පරිශීලකයා: 'පද්ධතිය'

තත්වය: writable_path වන අතර appdata නොවේ

අසත්‍ය ධනාත්මක කරුණු:

අවසර ලැයිස්තු විගණන යෙදුම් මෙම නාමාවලි වලින් ක්‍රියාත්මක කළ හැකි ඒවා ක්‍රියාත්මක වන බව නිරීක්ෂණය වී ඇත.

නිරීක්ෂණය කරන ලද පරිසරය(ය) තුළ භාවිතා කරන ස්ක්‍රිප්ට් සහ පරිපාලන මෙවලම් මෙම නාමාවලි වලින් එකක පිහිටා තිබිය හැකි අතර ඒවා එක් එක් සිද්ධිය අනුව ආමන්ත්‍රණය කළ යුතුය

මට්ටම: ඉහළ

ලේඛනයේ නාමය: ලෝක ලිවිය හැකි ක්‍රියාත්මක කිරීම - පරිශීලකයින්

අනන්‍යතාවය: 6dda3843-182a-4214-9263-925a80b4c634

විස්තර: C:\Users\Public* වෙතින් ක්‍රියාවලි ක්‍රියාත්මක කිරීම සහ පරිශීලකයින් තුළ ඇති සැමට ප්‍රවේශ විය කැකි අනෙකුත් ෆෝල්ඩර හඳුනා ගන්න.

පසුබිම

ගොනුවක් SYSTEM ලෙස ක්‍රියාත්මක කරන්නේ නම් AppData ෆෝල්ඩර බැහැර කරනු ලැබේ - මෙය බොහෝ තාවකාලික යෙදුම් ගොනු ක්‍රියාත්මක කරන හිතකර ක්‍රමයකි.

විමර්ශනය:

4. පරිශීලක සන්දර්භය, ක්‍රියාත්මක කිරීමේ අඛණ්ඩතා මට්ටම, ක්ෂණික පසු විපරම් ක්‍රියාකාරකම් සහ ගොනුව මඟින් දමන ලද රූප වැනි මෙම ගොනු ක්‍රියාත්මක කිරීම සමඟ සෘජුවම සම්බන්ධ තොරතුරු පරීක්ෂා කරන්න.
5. ක්‍රියාකාරකම ද්වේෂසහගතද යන්න තක්සේරු කිරීමට උපකාරී වන සන්දර්භීය ක්‍රියාවලිය, ජාලය, ගොනුව සහ ධාරකයේ අනෙකුත් සහායක දත්ත විමර්ශනය කරන්න.
6. අවශ්‍ය නම්, එය නීත්‍යානුකූලද යන්න තීරණය කිරීම සඳහා ප්‍රතිලෝම ඉංජිනේරු විද්‍යාව සඳහා ගොනුවේ පිටපතක් එකතු කිරීමට උත්සාහ කරන්න.

යොමු කිරීම්:

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

කර්තෘ: ASD හි ACSC

දිනය: 2024/06/19

තත්ත්වය: පර්යේෂණාත්මක

ටෑග්:

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

ලොග් මූලාශ්‍රය:

ප්‍රභේදය: process_creation
නිෂ්පාදිතයproduct: windows

සොයා ගැනීම:

පරිශීලකයා:

රූපය|අඩංගු දේ:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:

රූපය|අන්තර්ගතයන්: '\\AppData\\'
පරිශීලකයා: 'පද්ධතිය '

කොන්දේසිය: යෙදුම් දත්ත නොව පරිශීලකයින්

අසත්‍ය ධනාත්මක කරුණු:

- අධීක්ෂිත පරිසරය(යන්) තුළ භාවිතා කරන පිටපත් සහ පරිපාලන මෙවලම් පොදු හෝ උප නාමාවලියක පිහිටා තිබිය හැකි අතර ඒවා සිද්ධියෙන් සිද්ධියට අනුව ආමන්ත්‍රණය කළ යුතුය.

මට්ටම: මධ්‍යම

ලිහිල් කිරීම්

ලොග් වීම

ASD හි ACSC විමර්ශන අතරතුර, විමර්ශන උත්සාහයන්හි කාර්යක්ෂමතාව සහ වේගය අඩු කරන පොදු කරුණක් වන්නේ වෙබ් සේවාදායක ඉල්ලීම් ලොග්, Windows සිදුවීම් ලොග් සහ අන්තර්ජාල ප්‍රොක්සි ලොග් ඇතුළු ක්ෂේත්‍ර ගණනාවක් හරහා පුළුල් හා ඓතිහාසික ලොග් තොරතුරු නොමැති වීමය.

Windows සිදුවීම් ලොග් කිරීමේ ගබඩාවේ සහ තොරතුරු ආරක්ෂණ අත්පොතෙහි පද්ධති අධීක්ෂණය සඳහා මාර්ගෝපදේශයේ අඩංගු වින්‍යාස ගොනු සහ පිටපත් ඇතුළුව Windows සිදුවීම් ලොග් කිරීම සහ ඉදිරිපත් කිරීම මත ඔවුන්ගේ මාර්ගෝපදේශ සමාලෝචනය කර ක්‍රියාත්මක කිරීම ය.

පැච් කළමනාකරණය

වෙබ් සේවාදායක, වෙබ් යෙදුම් සහ දුරස්ථ ප්‍රවේශ ද්වාර ඇතුළුව සියලුම අන්තර්ජාලයට නිරාවරණය වූ උපාංග සහ සේවාවන් වහාම පැච් කරන්න. ක්‍රියාවලිය ස්වයංක්‍රීය කිරීමට සහ කඩිනම් කිරීමට මධ්‍යගත පැච් කළමනාකරණ පද්ධතියක් ක්‍රියාත්මක කිරීම සලකා බලන්න. ASD හි ACSC නිර්දේශ කරන්නේ ISM හි පද්ධති කළමනාකරණය සඳහා මාර්ගෝපදේශ, විශේෂයෙන් අදාළ වන විට පද්ධති පැච් කිරීමේ පාලනයන්, ක්‍රියාත්මක කිරීම ය.

ක්‍රියාකරුවා විසින් භාවිතා කරන බොහෝ අයුතු ලෙස ප්‍රයෝජනයට ගැනීම් හොඳින් දන්නා අතර පැච් හෝ අවම කිරීම් ලබා ගත හැකි විය. පැය 48ක් ඇතුළත අන්තර්ජාල මුහුණත යටිතල පහසුකම් සඳහා ආරක්ෂක පැච් හෝ ලිහිල් කිරීම් යොදන බවට සංවිධාන සහතික විය යුතු අතර, හැකි සෑම විටම, මෘදුකාංග සහ මෙහෙයුම් පද්ධතිවල නවතම අනුවාදයන් භාවිතා කළ යුතුය.

ජාල ඛණ්ඩනය

ජාල ඛණ්ඩනය මඟින් විරුද්ධවාදීන් සංවිධානයේ සංවේදී දත්ත සොයා ගැනීම සහ ඒවාට ප්‍රවේශය ලබා ගැනීම සැලකිය යුතු ලෙස දුෂ්කර කළ හැකිය. අවශ්‍ය නොමැති නම් පරිගණක අතර ගමනාගමනය ප්‍රතික්ෂේප කිරීම මඟින් පාර්ශ්වීය චලනය සීමා කිරීම හෝ අවහිර කිරීම සඳහා ජාල ඛණ්ඩනය කරන්න. Active Directory සහ අනෙකුත් සත්‍යාපන සේවාදායක වැනි වැදගත් සේවාදායකයන් සීමිත අතරමැදි සේවාදායකයන් ගණනකින් හෝ 'jump servers' මඟින් පමණක් පරිපාලනය කළ යුතුය.

මෙම සේවාදායකයන් සමීපව නිරීක්ෂණය කිරීම, හොඳින් ආරක්ෂා කිරීම සහ ඒවාට සම්බන්ධ විය හැකි පරිශීලකයින් සහ උපාංග සීමා කිරීම කළ යුතුය.

පාර්ශ්වීය චලනයක් වළක්වන අවස්ථා හඳුනාගැනීම නොසලකමින්, අතිරේක ජාල ඛණ්ඩනය මඟින් ක්‍රියාකාරීන්ට ප්‍රවේශ වීමට සහ බලහත්කාරයෙන් ලබා ගැනීමට හැකි වූ දත්ත ප්‍රමාණය තවදුරටත් සීමා කළ හැකිය.

අතිරේක ලිහිල් කිරීම්

APT40 සහ අනෙකුත් අය පහත සඳහන් TTP භාවිතයට එරෙහිව සටන් කිරීම සඳහා කර්තෘ ආයතන පහත සඳහන් ලිහිල් කිරීම් ද නිර්දේශ කරයි.

- භාවිතයට නොගත් හෝ අනවශ්‍ය ජාල සේවාවන්, ද්වාරයන් සහ ප්‍රොටෝකෝල අක්‍රීය කරන්න.
- වෙබ් සේවාදායකයන් සහ යෙදුම් ආරක්ෂා කිරීම සඳහා හොඳින් සුසර කරන ලද වෙබ් යෙදුම් ෆයර්වෝල් (WAF) භාවිතා කරන්න.
- සේවාදායක, ගොනු කොටස් සහ අනෙකුත් සම්පත් වෙත ප්‍රවේශය සීමා කිරීමට අවම වරප්‍රසාද බලාත්මක කරන්න.
- විශ්වසනීය තොරතුරු පළුදු කිරීම සහ නැවත භාවිතා කිරීම අපහසු කිරීම සඳහා බහු-සාධක සත්‍යාපනය (MFA) සහ කළමනාකරණය කළ සේවා ගිණුම් භාවිතා කරන්න. අන්තර්ජාලයෙන් ප්‍රවේශ විය හැකි සියලුම දුරස්ථ ප්‍රවේශ සේවාවන් සඳහා MFA යෙදිය යුතුය. ඒවා අතරට ඇතුළත් වන්නේ:
  - වෙබ් සහ ක්ලවුඩ්-පාදක ඊමේල්
  - සහයෝගීතා වේදිකා
  - අතථ්‍ය පුද්ගලික ජාල සම්බන්ධතා
  - දුරස්ථ ඩෙස්ක්ටොප් සේවා
- ආයු කාලය අවසන් වන උපකරණ ප්‍රතිස්ථාපනය කරන්න.

1 වැනි වගුව: ලිහිල් කිරීමේ උපාය මාර්ග/තාක්ෂණ

TTP	අත්‍යවශ්‍ය අවම කිරීමේ උපාය මාර්ග අට	ISM පාලනයන්
ආරම්භක ප්‍රවේශය T1190 පොදු-මුහුණු යෙදුම අයුතු ලෙස ප්‍රයෝජනයට ගැනීම	පැච් යෙදුම් පැච් මෙහෙයුම් පද්ධති සූරාකෑම බහු-සාධක සත්‍යාපනය යෙදුම් පාලන	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
ක්‍රියාත්මක කිරීම T1059 විධාන සහ පිටපත් කිරීමේ පරිවර්තකයා	යෙදුම් පාලනය Microsoft Office මැක්‍රෝ සීමා කරන්න පරිපාලන වරප්‍රසාද සීමා කරන්න	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
දිගටම පැවතීම T1505.003 සේවාදායක මෘදුකාංග සංරචකය: වෙබ් කවචය	යෙදුම් පාලනය පරිපාලන වරප්‍රසාද සීමා කරන්න	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
මූලික ප්‍රවේශය / වරප්‍රසාද තීව්‍ර කිරීම / දිගටම පැවතීම T1078 වලංගු ගිණුම්	පැච් මෙහෙයුම් පද්ධති බහු-සාධක සත්‍යාපනය පරිපාලන වරප්‍රසාද සීමා කරන්න යෙදුම් පාලනය පරිශීලක යෙදුම් දැඩි කිරීම	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

අතිරේක සාමාන්‍ය හඳුනාගැනීමේ සහ අවම කිරීමේ උපදෙස් සඳහා, මෙම උපදේශනයේ අවසානයේ ඇති MITER ATT&CK සාරාංශයේ හඳුනාගෙන ඇති එක් එක් ශිල්පීය ක්‍රම සඳහා MITER ATT&CK තාක්ෂණික වෙබ් පිටුවේ අවම කිරීම් සහ අනාවරණය කොටස් බලන්න.

හිමිකම් අත්හැරීම

මෙම වාර්තාවේ තොරතුරු “පවතින ආකාරයට” සපයනු ලබන්නේ තොරතුරු අරමුණු සඳහා පමණි. කර්තෘ ආයතන විසින් කිසිදු වාණිජ ආයතනයක්, නිෂ්පාදිතයක්, සමාගමක්, හෝ සේවාවක් අනුමත නොකරයි. එයට මෙම ලේඛනය තුළ සම්බන්ධ කර ඇති ඕනෑම වාණිජ ආයතනයක්, නිෂ්පාදිතයක්, හෝ සේවාවක් ඇතුළත් වේ. සේවා සලකුණු, වෙළඳ ලකුණු, නිෂ්පාදකයෙකු හෝ වෙනත් ආකාරයකින් නිශ්චිත වාණිජ ආයතන, නිෂ්පාදන, ක්‍රියාවලීන් හෝ සේවාවන් වෙත යොමු කිරීම, කර්තෘ ආයතන විසින් අනුමත කිරීම, නිර්දේශ කිරීම හෝ අනුග්‍රහය දැක්වීමක් අදහස් නොකරයි.

මෙම ලේඛනය TLP:CLEAR ලෙස සලකුණු කර ඇත. හෙළිදරව් කිරීම සීමා නොවේ. මහජන නිකුතුව සඳහා අදාළ නීති සහ ක්‍රියා පටිපාටිවලට අනුකූලව, තොරතුරු අනිසි ලෙස භාවිතා කිරීමේ අවම හෝ පුරෝකථනය කළ නොහැකි අවදානමක් ඇති විට මූලාශ්‍ර TLP:CLEAR භාවිතා කළ හැකිය. සම්මත ප්‍රකාශන හිමිකම් නීතිවලට යටත්ව, TLP:CLEAR තොරතුරු සීමාවකින් තොරව බෙදා හැරිය හැක. රථවාහන ආලෝක ප්‍රොටෝකෝලය පිළිබඳ වැඩිදුර තොරතුරු සඳහා, cisa.gov/tlp බලන්න

MITER ATT&CK – ඓතිහාසික APT40 උනන්දුවක් දක්වන වෙළඳ ශිල්පය

ඔත්තු බැලීම (TA0043)	
විඳිතයා සතු වෙබ් අඩවි සොයන්න (T1594)	විඳිතයාගේ අනන්‍යතා තොරතුරු රැස් කරන්න: විශ්වාසනීය තොරතුරු (T1589.001)
ක්‍රියාකාරී ස්කෑන් කිරීම: අවදානම ස්කෑන් කිරීම (T1595.002)	විඳිත ධාරක තොරතුරු රැස් කරන්න (T1592)
Search Open Websites/Domains: සෙවුම් යන්ත්‍ර (T1593.002)	විඳිත ජාල තොරතුරු රැස් කරන්න: වසම් ලක්ෂණ (T1590.001)
විඳිත අනන්‍යතා තොරතුරු රැස් කරන්න: ඊමේල් ලිපින (T1589.002)	

සම්පත් සංවර්ධනය (TA0042)	
යටිතල පහසුකම් ලබා ගැනීම: ධාරක (T1583.001)	යටිතල පහසුකම් ලබා ගන්න (T1583)
යටිතල පහසුකම් ලබා ගැනීම: DNS සේවාදායකය (T1583.002)	අවදානමට ලක් වූ ගිණුම් (T1586)
හැකියාවන් වර්ධනය කිරීම: කේත අත්සන් කිරීමේ සහතික (T1587.002)	අවදානමට ලක් වූ යටිතල පහසුකම් (T1584)
හැකියාවන් වර්ධනය කිරීම: ඩිජිටල් සහතික (T1587.003)	හැකියාවන් වර්ධනය කිරීම: අනිෂ්ට මෘදුකාංග (T1587.001)
ලබා ගැනීමේ හැකියාවන්: කේත අත්සන් කිරීමේ සහතික (T1588.003)	ස්ථාපිත ගිණුම්: ක්ලවුඩ් ගිණුම් (T1585.003)
අවදානමට ලක් වූ යටිතල පහසුකම්: ජාල උපාංග (T1584.008)	ලබා ගැනීමේ හැකියාවන්: ඩිජිටල් සහතික (T1588.004)

මූලික ප්‍රවේශය (TA0001)	
වලංගු ගිණුම් (T1078)	වංචනිකව යවනු සන්නිවේදනයන් (T1566)
වලංගු ගිණුම්: කොන්දේසි කඩකරන ගිණුම් (T1078.001)	වංචනිකව යවන සන්නිවේදනයන්: ඉල්ලක්කගතව වංචනික සන්නිවේදයන් යැවීමේ ඇමුණුම (T1566.001)
වලංගු ගිණුම්: ධාරක ගිණුම් (T1078.002)	වංචනිකව යවන සන්නිවේදනයන්: ඉල්ලක්කගතව වංචනික සන්නිවේදයන් යැවීමේ සබැඳිය (T1566.002)
බාහිර දුරස්ථ සේවා (T1133)	පොදු-මුහුණු යෙදුම අයුතු ලෙස ප්‍රයෝජනයට ගැනීම (T1190)
Drive-by Compromise (T1189)	

ක්‍රියාත්මක කිරීම (TA0002)

Windows කළමනාකරණ උපකරණ (T1047)	විධාන සහ ස්ක්‍රිප්ටින් පරිවර්තකය: Python (T1059.006)
කාලසටහන්ගත කාර්යය/රැකියාව: (T1053.002) හි	විධාන සහ ස්ක්‍රිප්ටින් පරිවර්තකය: JavaScript (T1059.007)
Scheduled Task/Job: Scheduled Task (T1053.005)	Native API (T1106)
විධාන සහ පිටපත් කිරීමේ පරිවර්තකයා (T1059)	අන්තර්-ක්‍රියාවලි සන්නිවේදනය (T1559)
විධාන සහ පිටපත් කිරීමේ පරිවර්තකයා: Windows විධාන කවචය (T1059.003)	පද්ධති සේවා: සේවා ක්‍රියාත්මක කිරීම (T1569.002)
විධාන සහ පිටපත් කිරීමේ පරිවර්තකයා: PowerShell (T1059.001)	සේවාදායක ක්‍රියාත්මක කිරීම සඳහා අයුතු ලෙස ප්‍රයෝජන ගැනීම (T1203)
විධාන සහ ස්ක්‍රිප්ටින් පරිවර්තකය: Visual Basic (T1059.005)	පරිශීලකයන් ක්‍රියාත්මක කිරීම: අනිෂ්ට ගොනුව (T1204.002)
විධාන සහ පිටපත් කිරීමේ පරිවර්තකයා: Unix Shell (T1059.004)	විධාන සහ පිටපත් කිරීමේ පරිවර්තකයා: Apple Script (T1059.002)
නියමිත කාර්යය/රැකියාව: Cron (T1053.003)	මෘදුකාංග යෙදවුම් මෙවලම් (T1072)

දිගටම පැවතීම (TA0003)

වලංගු ගිණුම් (T1078)	සේවාදායක මෘදුකාංග සංරචකය: කවචය (T1505.003)
කාර්යාල යෙදුම් ආරම්භය: කාර්යාල සැකිලි මැක්‍රෝස් (T1137.001)	පද්ධති ක්‍රියාවලිය සාදන්න, නිතිනම් වෙනස් කරන්න: Windows සේවාව (T1543.003)
නියමිත කාර්යය/රැකියාව: (T1053.002) හි	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
නියමිත කාර්යය/රැකියාව: නියමිත කාර්යය/රැකියාව (T1053.005)	Boot හෝ Logon ස්වයංක්‍රීයව ආරම්භ කිරීම ක්‍රියාත්මක කිරීම: කෙටි ක්‍රමයෙන් වෙනස් කිරීම (T1547.009)
බාහිර දුරස්ථ සේවා (T1133)	ක්‍රියාත්මක කිරීමේ ප්‍රවාහය පැහැර ගැනීම: DLL සෙවුම් ඇණවුම් Hijacking (T1574.001)
නියමිත කාර්යය/රැකියාව: Cron (T1053.003)	ක්‍රියාත්මක කිරීමේ ප්‍රවාහය පැහැර ගැනීම: DLL පැති-පූරණය (T1574.002)
ගිණුම් හැසිරවීම (T1098)	වලංගු ගිණුම්: ක්ලවුඩ් ගිණුම් (T1078.004)
වලංගු ගිණුම්: වසම් ගිණුම් (T1078.002)	

වරප්‍රසාද තීව්‍ර කිරීම (TA0004)

නියමිත කාර්යය/රැකියාව: (T1053.002) හි	පද්ධති ක්‍රියාවලිය සාදන්න, නැතහොත් වෙනස් කරන්න: Windows සේවාව (T1543.003)
නියමිත කාර්යය/රැකියාව: නියමිත කාර්යය (T1053.005)	ආරම්භක හෝ පිවිසුම් ස්වයංක්‍රීයව ක්‍රියාත්මක කිරීම: රෙජිස්ට්‍රි ධාවන යතුරු / ආරම්භක ෆෝල්ඩරය (T1547.001)
ක්‍රියාවලි ඇතුළත් කිරීම: Thread ක්‍රියාත්මක කිරීමේ පැහැරගැනීම (T1055.003)	Boot හෝ Logon ස්වයංක්‍රීයව ආරම්භ කිරීමේ ක්‍රියාත්මක කිරීම: කෙටි ක්‍රමයෙන් වෙනස් කිරීම (T1547.009)
ක්‍රියාවලි ඇතුළත් කිරීම: ක්‍රියාවලි හිස් කිරීම (T1055.012)	ක්‍රියාත්මක කිරීමේ ප්‍රවාහය පැහැරගැනීම: DLL සෙවුම් ඇණවුම් පැහැරගැනීම (T1574.001)

වරප්‍රසාද තීව්‍ර කිරීම (TA0004)

වලංගු ගිණුම්: වසම් ගිණුම් (T1078.002)	වරප්‍රසාද තීව්‍ර කිරීම සඳහා අයුතු ලෙස ප්‍රයෝජන ගැනීම (T1068)
ප්‍රවේශ ටෝකන් හැසිරවීම: ටෝකන් අනුකරණය/සොරකම (T1134.001)	සිදුවීම් අවුලුවන ක්‍රියාත්මක කිරීම: Unix Shell (යුනික්ස් ෂෙල්) වින්‍යාස වෙනස් කිරීම (T1546.004)
ක්‍රියාවලි ඇතුළත් කිරීම: ගතික-සබැඳි පුස්තකාලය ඇතුළත් කිරීම (T1055.001)	වලංගු ගිණුම්: වසම් ගිණුම් (T1078.002)
වලංගු ගිණුම්: දේශීය ගිණුම් (T1078.003)	

ආරක්ෂාව මගහැරීම (TA0005)

Rootkit (T1014)	අනියමිත විධාන ක්‍රියාත්මක කිරීම (T1202)
අපැහැදිලි ගොනු හෝ තොරතුරු (T1027)	පද්ධති ද්විමය ප්‍රොක්සි ක්‍රියාත්මක කිරීම: Mshta (T1218.005)
අපැහැදිලි ගොනු හෝ තොරතුරු: මෘදුකාංග ඇසුරුම්කරණය (T1027.002)	පද්ධති ද්විමය ප්‍රොක්සි ක්‍රියාත්මක කිරීම: Regsvr32 (T1218.010)
අපැහැදිලි ගොනු හෝ තොරතුරු: Steganography (T1027.003)	භාර පාලනයන් යටපත් කිරීම: කේත අත්සන් කිරීම (T1553.002)
අපැහැදිලි ගොනු හෝ තොරතුරු: බෙදාහැරීමෙන් පසු සම්පාදනය කිරීම (T1027.004)	ගොනු සහ නාමාවලි අවසර වෙනස් කිරීම්: Linux සහ Mac ගොනු සහ නාමාවලි අවසර වෙනස් කිරීම (T1222.002)
වෙනත් වේශයකින් පෙනී සිටීම: නීත්‍යානුකූල නම හෝ ස්ථානය ගැළපීම (T1036.005)	Virtualisation/Sandbox මග හැරීම: පද්ධති පරීක්ෂාවන් (T1497.001)
ක්‍රියාවලි ඇතුළත් කිරීම: Thread ක්‍රියාත්මක කිරීමේ පැහැරගැනීම (T1055.003)	වෙනත් වේශයකින් පෙනී සිටීම (T1036)
පරාවර්තක කේත පූරණය (T1620)	ආබාධ ආරක්ෂණ: පද්ධති ෆයර්වෝලය අක්‍රිය කිරීම හෝ වෙනස් කිරීම (T1562.004)
ක්‍රියාවලි ඇතුළත් කිරීම: ක්‍රියාවලි හිස් කිරීම (T1055.012)	කෞතුක වස්තු සැඟවීම: සැඟවුණු ගොනු සහ නාමාවලි (T1564.001)
දර්ශකය ඉවත් කිරීම: ගොනු මකා දැමීම (T1070.004)	කෞතුක වස්තු සැඟවීම: සැඟවුණු Window (T1564.003)
දර්ශකය ඉවත් කිරීම: Timestomp (T1070.006)	ක්‍රියාත්මක කිරීමේ ප්‍රවාහය පැහැර ගැනීම: DLL සෙවුම් ඇණවුම් පැහැර ගැනීම (T1574.001)
දර්ශකය ඉවත් කිරීම: Windows Event Logs හිස් කිරීම (T1070.001)	ක්‍රියාත්මක කිරීමේ ප්‍රවාහය පැහැර ගැනීම: DLL Side-Loading (T1574.002)
රෙජිස්ට්‍රිය වෙනස් කරන්න (T1112)	වෙබ් සේවාව (T1102)
ගොනු හෝ තොරතුරු නිරවුල් කිරීම/විකේතනය කරන්න (T1140)	වෙනත් වේශයකින් පෙනී සිටීම: කාර්යය හෝ සේවාව වෙනත් වේශයකින් පෙන්වීම (T1036.004)
දුෂ්කරතා ආරක්ෂාවන් (T1562)	

විශ්වාසනීය තොරතුරු වෙත ප්‍රවේශය (TA0006)

OS විශ්වසනීය තොරතුරු අත්හැර දැමීම: LSASS Memory (T1003.001)	අනාරක්ෂිත විශ්වාසනීය තොරතුරු: ගොනු වල අඩංගු විශ්වාසනීය තොරතුරු (T1552.001)
OS විශ්වසනීය තොරතුරු අත්හැර දැමීම: NTDS (T1003.003)	ප්‍රචන්ඩ බලය: මුරපද අනුමාන කිරීම (T1110.001)
ජාල ආඝ්‍රාණය (T1040)	බලහත්කාර සත්‍යාපනය (T1187)

විශ්වාසනීය තොරතුරු වෙත ප්‍රවේශය (TA0006)

මුරපද ගබඩා මගින් විශ්වාසනීය තොරතුරු: Keychain (T1555.001)	Kerberos ටිකට්පත් සොරකම් කිරීම හෝ ව්‍යාජ ලෙස සකස් කිරීම: Kerberoasting (T1558.003)
ආදාන ග්‍රහණය කිරීම: Keylogging (T1056.001)	බහු-සාධක සත්‍යාපන අන්තර්ග්‍රහණය (T1111)
වෙබ් සැසි කුකී සොරකම් කිරීම (T1539)	යෙදුම් ප්‍රවේශ ටෝකනය සොරකම් කිරීම (T1528)
විශ්වාසනීය තොරතුරු වෙත ප්‍රවේශය සඳහා අයුතු ප්‍රයෝජන ගැනීම (T1212)	ප්‍රචන්ඩ බලය: මුරපද පළුදු කිරීම (T1110.002)
ආදාන ග්‍රහණය කිරීම: වෙබ් ද්වාර ග්‍රහණය කිරීම (T1056.003)	OS විශ්වාසනීය තොරතුරු අත්හැර දැමීම: DCSync (T1003.006)
මුරපද ගබඩා මගින් විශ්වාසනීය තොරතුරු (T1555)	මුරපද ගබඩා මගින් විශ්වාසනීය තොරතුරු: වෙබ් බ්‍රව්සර් මගින් විශ්වාසනීය තොරතුරු (T1555.003)

සොයා ගැනීම (TA0007)

පද්ධති සේවා සොයා ගැනීම (T1007)	පද්ධති තොරතුරු සොයා ගැනීම (T1082)
Application Window සොයා ගැනීම (T1010)	ගිණුම් සොයා ගැනීම: දේශීය ගිණුම (T1087.001)
විමසුම් රෙජිස්ට්‍රිය (T1012)	පද්ධති තොරතුරු සොයාගැනීම, තාක්ෂණය T1082 - Enterprise | MITRE ATT&CK®
ගොනු සහ නාමාවලි සොයා ගැනීම (T1083)	පද්ධති කාල සොයා ගැනීම (T1124)
ජාල සේවා සොයා ගැනීම (T1046)	පද්ධති හිමිකරුවා/පරිශීලකයා සොයා ගැනීම (T1033)
දුරස්ථ පද්ධති සොයා ගැනීම (T1018)	වසම් භාර සොයා ගැනීම (T1482)
ගිණුම් සොයා ගැනීම: ඊමේල් ගිණුම (T1087.003)	ගිණුම් සොයා ගැනීම: වසම් ගිණුම (T1087.002)
පද්ධති ජාල සම්බන්ධතා සොයා ගැනීම (T1049)	Virtualisation/Sandbox මග හැරීම: පද්ධති පරීක්ෂාවන් (T1497.001)
ක්‍රියාවලි සොයා ගැනීම (T1057)	මෘදුකාංග සොයා ගැනීම (T1518)
අවසරය තිබෙන කණ්ඩායම් සොයා ගැනීම: වසම් කණ්ඩායම් (T1069.002)	ජාල බෙදාගැනීම සොයා ගැනීම, තාක්ෂණය T1135 - Enterprise | MITRE ATT&CK®
පද්ධති ජාල වින්‍යාස සොයා ගැනීම: අන්තර්ජාල සම්බන්ධතා සොයා ගැනීම (T1016.001)	

පාර්ශ්වික චලනය (TA0008)

දුරස්ථ සේවා: දුරස්ථ ඩෙස්ක්ටොප් ප්‍රොටෝකෝලය (T1021.001)	දුරස්ථ සේවා (T1021)
දුරස්ථ සේවා: SMB/Windows පරිපාලක කොටස් (T1021.002)	විකල්ප සත්‍යාපන ද්‍රව්‍ය භාවිතා කිරීම: ටිකට් පත ලබා දෙන්න (T1550.003)
දුරස්ථ සේවා: Windows දුරස්ථ කළමනාකරණය (T1021.006)	පාර්ශ්වික මෙවලම් හුවමාරුව (T1570)

එකතුව (TA0009)

දේශීය පද්ධතිය වෙතින් දත්ත (T1005)	එකතු කරන ලද දත්ත සංරක්ෂණය කිරීම: පුස්තකාලය හරහා සංරක්ෂණය කිරීම (T1560.002)
ජාල බෙදාගත් ධාවකයෙන් දත්ත (T1039)	ඊමේල් එකතුව: දුරස්ථ ඊමේල් එකතුව (T1114.002)

එකතුව (TA0009)

ආදාන ග්‍රහණය කිරීම: Keylogging (T1056.001)	Clipboard දත්ත (T1115)
ස්වයංක්‍රීය එකතු කිරීම (T1119)	තොරතුරු ගබඩා මගින් දත්ත (T1213)
ආදාන ග්‍රහණය කිරීම: වෙබ් ද්වාර ග්‍රහණය කිරීම (T1056.003)	දත්ත එළි දැක්වීම: දුරස්ථ දත්ත එළි දැක්වීම (T1074.002):
දත්ත එළි දැක්වීම: දේශීය දත්ත එළි දැක්වීම (T1074.001)	එකතු කළ දත්ත සංරක්ෂිත කිරීම (T1560)
ඊමේල් එකතු කිරීම (T1114)	

අනවසරයෙන් තොරතුරු මාරු කිරීම (TA0010)

C2 නාලිකාව හරහා අනවසරයෙන් තොරතුරු මාරු කිරීම (T1041)	විකල්ප ප්‍රොටෝකෝලය හරහා අනවසරයෙන් තොරතුරු මාරු කිරීම: අසම්මිතික සංකේතනය කළ C2 නොවන ප්‍රොටෝකෝලය හරහා අනවසරයෙන් තොරතුරු මාරු කිරීම (T1048.002)
විකල්ප ප්‍රොටෝකෝලය හරහා අනවසරයෙන් තොරතුරු මාරු කිරීම (T1048)	වෙබ් සේවාව හරහා අනවසරයෙන් තොරතුරු මාරු කිරීම: ක්ලවුඩ් ගබඩාවට අනවසරයෙන් තොරතුරු මාරු කිරීම (T1567.002)

විධානය සහ පාලනය (TA0011)

දත්ත අපැහැදිලි කිරීම: ප්‍රොටෝකෝල අනුකරණය (T1001.003)	වෙබ් සේවාව: Dead Drop Resolver (T1102.001)
පොදුවේ භාවිතා වන ද්වාරය (T1043)	වෙබ් සේවාව: ඒක දිශා සන්නිවේදනය (T1102.003)
යෙදුම් ස්ථර ප්‍රොටෝකෝලය: වෙබ් ප්‍රොටෝකෝල (T1071.001)	ඇතුළත් කිරීමේ මෙවලම් මාරු කිරීම (T1105)
යෙදුම් ස්ථර ප්‍රොටෝකෝලය: ගොනු හුවමාරු ප්‍රොටෝකෝල (T1071.002)	බලය පැවරුන ආදේශකයා: අභ්‍යන්තර බලය පැවරුන ආදේශකයා (T1090.001)
බලය පැවරුන ආදේශකයා: බාහිර බලය පැවරුන ආදේශකයා (T1090.002)	ප්‍රමිතියක් නොමැති ද්වාර (T1571)
බලය පැවරුන ආදේශකයා: Multi-hop (දත්ත අතරමැදි නෝඩ් එකක් හෝ කිහිපයක් හරහා ගමන් කරන සන්නිවේදන පද්ධතියක්) බලය පැවරුන ආදේශකයා (T1090.003)	ප්‍රොටෝකෝල උමං මාර්ග (T1572)
වෙබ් සේවාව: ද්වී දිශා සන්නිවේදනය (T1102.002)	සංකේතනය කළ නාලිකාව (T1573)
සංකේතනය කළ නාලිකාව: අසම්මිතික ගුප්ත ලේඛන විද්‍යාව (T1573.002)	ඇතුළත් කිරීමේ මෙවලම් මාරු කිරීම (T1105)
බලය පැවරුන ආදේශකයා, තාක්ෂණය T1090 - ව්‍යවසාය | MITER ATT&CK®	

බලපෑම (TA0040)

සේවා නැවත් වීම (T1489)	Disk Wipe (T1561)
පද්ධතිය වසා දැමීම/නැවත ආරම්භ කිරීම (T1529)	සම්පත් පැහැර ගැනීම (T1496)

සටහන්

හිමිකම් අත්හැරීම

මෙම මාර්ගෝපදේශයේ ඇති තොරතුරු සාමාන්‍ය ස්වභාවයක් ගන්නා අතර එය නීති උපදෙසක් ලෙස හෝ කිසියම් විශේෂිත අවස්ථාවකදී හෝ හදිසි අවස්ථාවකදී සහාය සඳහා විශ්වසනීය දෙයක් ලෙස නොසැලකිය යුතුය.

ඕනෑම වැදගත් කාරණයකදී, ඔබ ඔබේම තත්වයන් සම්බන්ධව සුදුසු ස්වාධීන වෘත්තීය උපදෙස් ලබා ගත යුතුය.

මෙම මාර්ගෝපදේශයේ අඩංගු කරුණු මත විශ්වාසය තැබීමේ ප්‍රතිඵලයක් ලෙස සිදුවන ඕනෑම හානියක්, අලාභයක් හෝ වියදමක් සඳහා මධ්‍යම රජය කිසිදු වගකීමක් හෝ වගකීමක් භාර නොගනී.

ප්‍රකාශන හිමිකම

රාජ්‍ය ලාංඡනය භාවිතා කිරීම

රාජ්‍ය ලාංඡනය භාවිතා කළ හැකි නියමයන් අගමැති සහ කැබිනට් දෙපාර්තමේන්තුවේ වෙබ් අඩවියේ Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au විස්තර කර ඇත.

වැඩි විස්තර සඳහා, හෝ සයිබර් ආරක්ෂණ සිදුවීමක් වාර්තා කිරීමට, අපව අමතන්න:

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

මෙම අංකය භාවිතයට ලැබෙනුයේ ඔස්ට්‍රේලියාව තුළ පමණි.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre