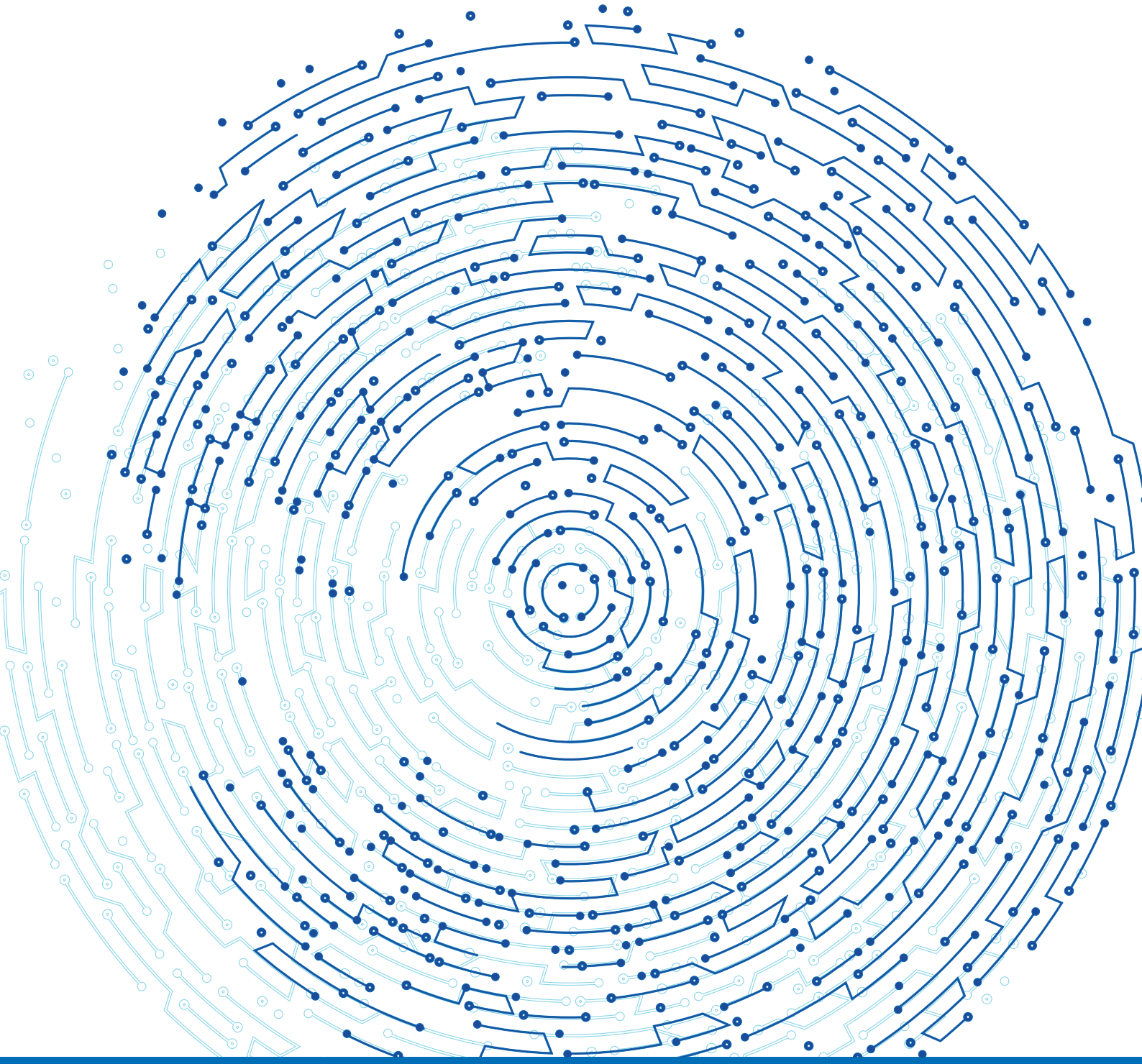
APT40 مەسلىھەت

خ خ ج دۆلەت بىخەتەرلىك مىنىستىرلىقىنىڭ ھۇنەرلىرى ھەربىكەتتە



Australian Government

Australian Signals Directorate

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

National Cyber Security Centre

a part of GCHQ

Bundesnachrichtendienst

National Cyber Security Centre

PART OF THE GCSB

Bundesamt für Verfassungsschutz

警察庁

National Police Agency

NISC

内閣サイバーセキュリティセンター

National center of Incident readiness and Strategy for Cybersecurity

مۇندەرىجە

ئومۇمىي چۈشەنچە

ئارقا كۆرۈنۈش

ئاۋسترالىيە سىگنال ئىدارىسى قارمىقىدىكى ئاۋسترالىيە تور بىخەتەرلىكى مەركىزى (ASD's ACSC)، ئامېرىكا تور بىخەتەرلىكى ۋە ھۆل مۇئەسسە بىخەتەرلىكى (CISA)، ئامېرىكا دۆلەت بىخەتەرلىك ئىدارىسى (NSA)، ئامېرىكا فېدېراتسىيە تەكشۈرۈش ئىدارىسى (FBI)، ئەنگلىيە دۆلەتلىك تور بىخەتەرلىكى مەركىزى (NCSC-UK)، كانادا تور بىخەتەرلىكى مەركىزى (CCCS)، يېڭى زېلاندىيە دۆلەتلىك تور بىخەتەرلىكى مەركىزى (NCSC-NZ)، گېرمانىيە فېدېراتسىيە ئىستىخبارات مۇلازىمىتى (BND) ۋە ئاساسىي قانۇننى قوغداش فېدېراتسىيە ئىشخانىسى (BfV)، كورىيە جۇمھۇرىيىتى دۆلەتلىك ئىستىخبارات مۇلازىمىتى (NIS) ۋە ئۇنىڭ قارمىقىدىكى دۆلەتلىك تور بىخەتەرلىكى مەركىزى، ياپونىيە ۋەقەلەرگە تەييارلىق كۆرۈش ۋە تور بىخەتەرلىك ئىستراتېگىيەسى مىللىي مەركىزى (NISC) ۋە دۆلەتلىك ساقچى ئىدارىسى (NPA) نىڭ كوللېكتىپ ئاپتورلۇقىدا (تۆۋەندە ئۇلار «ئاپتور ئورگانلار» دېيىلىدۇ) تەييارلاپ چىقىلغان مەزكۇر مەسلىھەت خىتاي خەلق جۇمھۇرىيىتى (خ خ ج) نىڭ دۆلەت ھامىيلىقىدىكى تور گۇرۇپپىسى ۋە ئۇلارنىڭ ئاۋسترالىيە تور بىخەتەرلىكىگە كەلتۈرۈۋاتقان نۆۋەتتىكى تەھدىتلىرىنى بايان قىلىپ بېرىدۇ. مەزكۇر مەسلىھەت ئاپتور ئورگانلارنىڭ تەھدىتلەر ھەققىدىكى ئومۇمى چۈشەنچىسىگە، شۇنىڭدەك ASD قارمىقىدىكى ACSC نىڭ تورلۇك ھادىسىلەرگە جاۋابەن تەكشۈرۈشلىرىگە ئاساسەن تەييارلاندى.

خ خ ج ھامىيلىقىدىكى تور گۇرۇپپىسى ئىلگىرىكى ۋاقىتلاردا ئوخشىمىغان مەملىكەتلەرددىكى، جۈملىدىن ئاۋسترالىيە ۋە ئامېرىكىدىكى تەشكىلاتلارنى نىشانغا ئالغان. شۇنىڭدەك خ خ ج ھامىيلىقىدىكى باشقا تور ئارتىستلىرى تۆۋەندە تەكىتلەپ ئۆتۈلگەن ئۇسۇللارنى دۇنيا مىقياسىدا مۇنتىزىم رەۋىشتە قوللانغان. شۇڭا ئاپتور ئورگانلار مەزكۇر گۇرۇپپا ۋە مۇشۇ خىلدىكى ئۇسۇللارنى ئۆز مەملىكەتلىرىدىكى تور ساھەسى ئۈچۈن تەھدىت، دەپ قارايدۇ.

ئاپتور ئورگانلار مەزكۇر گۇرۇپپىنى خ خ ج دۆلەت بىخەتەرلىك ئىدارىسى (MSS) گە ۋاكالىتەن زىيانلىق مەشغۇلاتلارنى قىلىۋاتىدۇ، دەپ ئىشىنىدۇ. بۇ پائالىيەتلەر ۋە ھۇنەرلەر «يۇقىرى دەرىجىلىك دائىمىي تەھدىت» (APT) 40 (بۇ يەنە بۇ ساھەدىكى دوكلاتلاردا Leviathan، GINGHAM TYPHOON، Kryptonite Panda ۋە Bronze Mohawk دەپمۇ ئاتىلىدۇ) نامىلىق گۇرۇپپىنىڭ پائالىيەتلىرى بىلەنمۇ ئۆزئارا ماس كېلىدۇ. ئىلگىرىكى دوكلاتلاردا كۆرسىتىلىشچە، مەزكۇر گۇرۇپپا خەينەن ئۆلكىسىنىڭ خەيكو شەھرىگە جايلاشقان بولۇپ، خ خ ج دۆلەت بىخەتەرلىك مىنىستىرلىقى ۋە خەينەن ئۆلكىلىك دۆلەت بىخەتەرلىك نازارىتىدىن ۋەزىپە تاپشۇرۇۋېلىپ كەلگەن. تۆۋەندىكى مەسلىھەتلەر بۇ دۇشمەن كۈچنىڭ زىيانكەشلىكىگە ئۇچرىغان ئىككى تور باشتىن كەچۈرگەن ھۇنەرلەر ھەققىدىكى دېلو مىسالىرىنى ئۆلگە سۈپىتىدە بايان قىلىپ بېرىدۇ. بۇ دېلو مىسالىرى تور بىخەتەرلىكى بىلەن شۇغۇللانغۇچىلارنىڭ ئۆز تور ساھەسىگە APT40 نىڭ قىلغان ھۇجۇملىرىنى ئېنىقلاش، ئۇنىڭ ئالدىنى ئېلىش ۋە زىيان-زەخمەتنى تۆۋەنلەشتە زور ئەھمىيەتكە ئىگە. تاللانغان بۇ دېلو مىسالىرى ئاشۇ تور ئارتىستلىرى ياكى باشقىلارنىڭ قايتىدىن ئاشۇ يوسۇندا خېيىم-خەتەر تۇغدۇرۇشىدىن ساقلىنىش مەقسىتىدە مۇڭاپىق بولغان تۆۋەنلەتىش تەدبىرلىرى ئېلىنغان دېلولار ھېسابلىنىدۇ. شۇڭا بۇ دېلو مىسالىرى خاراكتېر جەھەتتە تەبىئىيلا كونا بولۇپ، ئورگانلار بۇ ئارقىلىق زىيانلارنى تۆۋەنلەتىشكە يېتەرلىك ۋاقىت چىقىرالايدۇ.

پائالىيەت خۇلاسىسى

APT40 توختاۋسىز رەۋىشتە ئاۋسترالىيە تورلىرىنى، شۇنىڭدەك بۇ رايوندىكى ھۆكۈمەت ۋە خۇسۇسىي تارماقلارنىڭ تورلىرىنى نىشان قىلىۋاتقان بولۇپ، ئۇلارنىڭ تور ساھەسىگە سېلىۋاتقان تەھدىتلىرى ھېلىمۇ داۋام قىلماقتا. بۇ مەسلىھەتتە بايان قىلىنغان ھۇنەرلەر ئاۋسترالىيە تورلىرىغا قارشى پائالىيەتلەردە كۆپلەپ ئۇچرايدۇ.

دەققەت قىلىشقا تېگىشلىك بولغىنى شۇكى، APT40 تېزدىن ئۆزگىرىش ۋە ئۇقۇملارنى تەھقىلەش (POC) ئارقىلىق يېڭىدىن ئوتتۇرىغا چىقىۋاتقان ئاجىزلىقلارغا ماسلىشىش ئىقتىدارىغا ئىگە. ئۇلار مۇشۇ ئالاھىدىلىكلىرى ئارقىلىق مۇناسىۋەتلىك ئاجىزلىقلار مەۋجۇت بولۇۋاتقان ھۆل مۇئەسسەلەرنى نىشان قىلغان ھالدا تورلارغا ھۇجۇم قىلىپ كەلگەن.

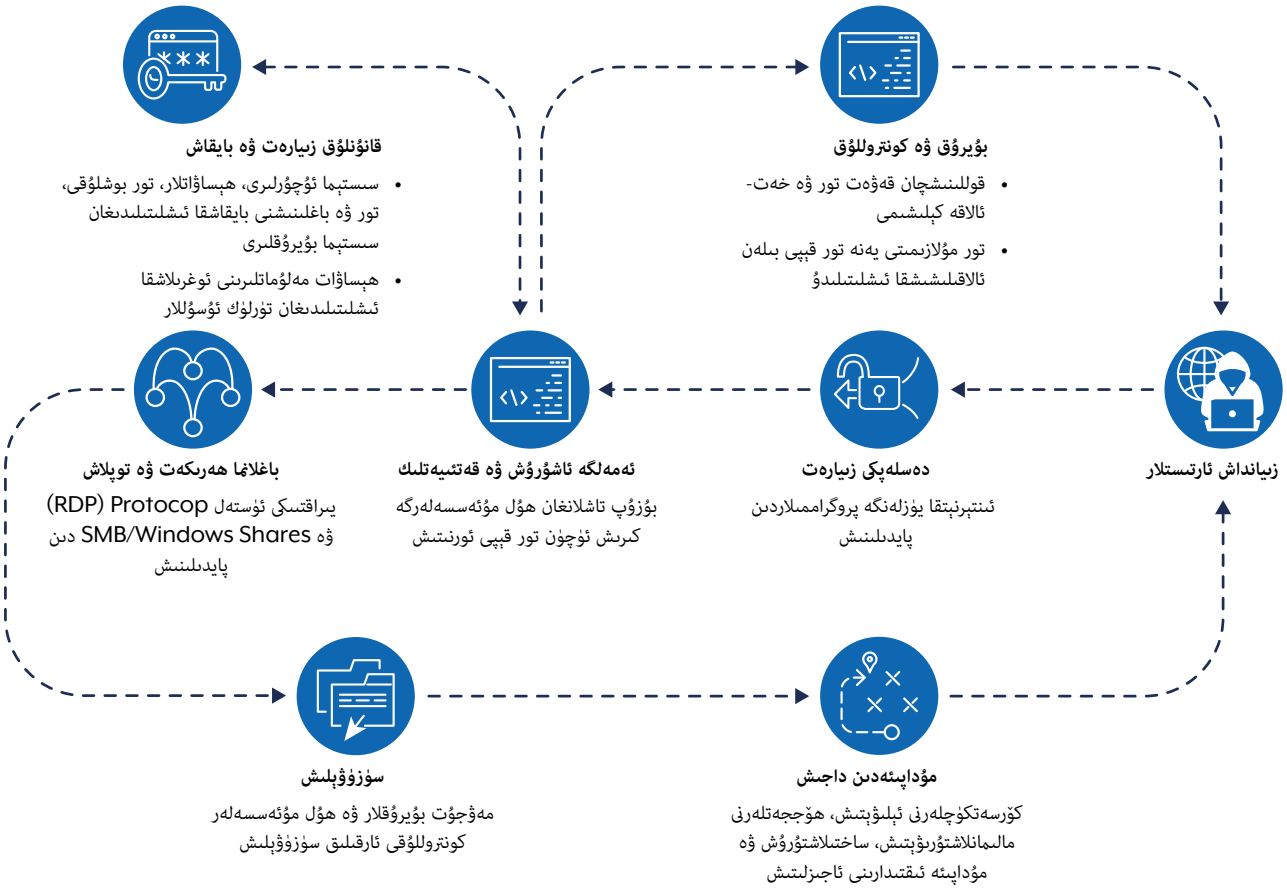
APT40 مۇنتىزىم رەۋىشتە ئۆزلىرى قىزىقىدىغان تور ساھەسىنى، جۈملىدىن ئاپتور ئورگانلار مەنسۇپ دۆلەتلەرنىڭ تور دۇنياسىنى رازۋېدكا قىلىپ كەلگەن ھەمدە ئۆز نىشانلىرىنى ۋەيران قىلىشنىڭ پۈرسەتلىرىنى ئىزلىگەن.

مۇشۇ خىلدىكى دائىمىي رازۋېدكا ئارقىلىق بۇ گۇرۇپپا ئۆزلىرى قىزىقىدىغان تورلاردىكى ئاجىزلىقلارنى، خىزمەت مۇددىتى ئاخىرلاشقان ياكى ئاسراشتىن قالغان ئۇسكۇنىلەرنى بايقاش ھەمدە تېزدىن ئۇلاردىكى يوچۇقلاردىن پايدىلىنىشقا ئۆتكەن. -2017يىلدىن بۇيان APT40 مۇشۇ يوسۇندا تورلاردىكى ئاجىزلىقلارنى تېپىشتا توختاۋسىز ئۇتۇقلارغا ئېرىشىپ كەلگەن.

APT40 تېزدىن كەڭ كۆلەمدە قوللىنىلىدىغان يۇمتاللاردىن Log4J (CVE 2021 44228)، Atlassian Confluence (CVE-2021-31207، CVE-2021-26084) ۋە Microsoft Exchange (CVE-2021-31207؛ CVE-2021-34523؛ CVE-2021-34473) قاتارلىقلاردىكى يېڭى يوچۇقلارنى تېپىپ چىققان. ASD قارمىقىدىكى ACSC ۋە ئاپتور ئورگانلارنىڭ پەملىشچە، بۇ گۇرۇپپا تور يوچۇقلىرى ئاممىغا ئاشكارىلانغاندىن كېيىنكى بىرنەچچە سائەت ياكى بىرنەچچە كۈن ئىچىدە ئۇقۇملارنى تەھقىلەش (POC) ئارقىلىق بۇ يوچۇقلارغا تاقابىل تۇرۇشنىڭ كويىغا چۈشىدۇ.

2 ئامېرىكا ئەدلىيە مىنىستىرلىقى. 2021. خىتاي دۆلەت بىخەتەرلىك مىنىستىرلىقى بىلەن خىزمەت ھەمكارلىقى بولغان تۆت نەپەر خىتاي پۇقراسى ئەقلىي مۇلۇك ۋە مەخپىي سودا مەلۇماتلىرىنى جۈملىدىن پۇقۇملۇق كېسەللىكلەر تەتقىقاتىنى نىشان قىلغان دۇنياۋى كومپيۇتېر تاجاۋۇزكارلىقى قىلمىشىدا ئەيىبلەندى.

1-رەسىم. APT40 پائالىيەتلىرىنىڭ ئاقما دىئاگرامى



بۇ گۇرۇپپا تورلاردىكى قوللانغۇچىلارنىڭ ئۆزئارا تەسىر كۆرسىتىشى تەلەپ قىلىنىدىغان قارماق سېلىش دېگەندەك ئۇسۇللاردىن كۆرە ئاجىز ۋە ئاممىغا يۈزلەنگەن ئاممىۋى مۇئەسسەسەلەردىن پايدىلىنىشنى ئەۋزەل كۆرىدۇ. شۇنداقلا كېيىنكى بىر قاتار تەدبىرلەرنى ئەمەلگە ئاشۇرۇش ئۈچۈن ئىناۋەتلىك ھېسابات ئۇچۇرلىرىنى توپلاشنى ئالدىنقى ئورۇنغا قويىدۇ. APT40 ھەرقاچان ئىزچىل مەۋجۇتلۇق ئۈچۈن تور قېپى (Web Shell) دىن (T1505.003) پايدىلىنىدۇ. بولۇپمۇ ئۆزلىرىنىڭ مۇداخىلە پائالىيەتلىرىنىڭ دەسلەپكى باسقۇچىدا شۇنداق قىلىدۇ. ئومۇمەن قىلىپ ئېيتقاندا، دەسلەپكى زىيارەت ئۈكۈشلۇق بولغاندىن كېيىن APT40 نۇقتىلىق قىلىپ زىيانكەشلىككە ئۇچرىغۇچىنىڭ تور مۇھىتىغا ئۆزۈن مۇددەتكە كىرىۋەيدىغان بولۇشقا ئۇرۇنىدۇ. دەرۋەقە، تور مۇداخىلىسىنىڭ دەسلەپكى مەزگىللىرىدە ئۆزۈن مۇددەتلىك زىيارەت كۆرۈلىدىغانلىقى ئۈچۈن مۇداخىلىنىڭ قانداق شەكىل ئېلىشى ياكى كېيىنكى پائالىيەتلىرىنىڭ قانداق بولۇشىدىن قەتئىنەزەر بۇ ھال مۇداخىلىنىڭ ھەممىسىدىلا كۆزگە چېلىقىدۇ.

دىققەتكە سازاۋەر ھۇنەرلەر

گەرچە APT40 ئىلگىرى ئاۋستىرالىيە تورلىرىغا ھۇجۇم قىلىشتا بۇيرۇق ۋە كونتروللۇق (C2) ئۈچۈن ئىشلىتىلگەن بولسىمۇ، بۇ گۇرۇپپا بۇ ھۇنەرلىرىنى ئاللىقاچان يېڭىلىپ چىققان(T1594).

APT40 يۇقۇملانغان ئۇسكۇنىلەرنى، جۈملىدىن كىچىك ئىشخانا ياكى ئۆي ئىشخانىلىرى (SOHO)دىكى ئۇسكۇنىلەرنى ئىشلىتىۋېرىشتەك دۇنياۋى يۈزلىنىشكە ماسلىشىپ، بۇنى ئۆزلىرىنىڭ ئاۋستىرالىيەدىكى پائالىيەتلىرىنى قانات يايدۇرۇشنىڭ مەشغۇلات ھۇل مۇئەسسەسى ۋە ئاخىرقى قايتا يۆللەندۇرگۈچىسى (T1584.008) قىلىۋالغان. بۇ ھال ئاپتور ئورگانلارنى مەزكۇر گۇرۇپپىنىڭ ھەرىكەتلىرىنى تېخىمۇ ياخشى تەسۋىرلەش ۋە ئۇلارنىڭ ھەرىكەتلىرىنى تېخىمۇ ياخشى ئىز قوغلاش ئىمكانىيىتىگە ئىگە قىلىدۇ.

كۆپلىگەن SOHO ئۇسكۇنىلىرىنىڭ ئىشلەش مۇددىتى ئاخىرلاشقان ياكى ياماللىمغان بولغاچقا N-كۇنلۇك ھۇجۇم ئۇچۇن يۇمشاق نىشان بولۇپ قالغان. ھۇجۇمغا ئۇچرىغان ھامان SOHO ئۇسكۇنىلىرى ھۇجۇمنىڭ باشلىنىش نۇقتىسى بولۇپ قالىدۇ. بۇنداق ھۇجۇملارنىڭ مەقسىتى بولسا قانۇنىي ئېقىم مىقدارى بىلەن ئارىلىشىپ كېتىش ھەمدە تور بەت ھېمايىچىلىرىغا خىرىس قىلىشتۇر (T1001.003).

بۇ خىل تېخنىكىلارنى خ خ ج نىڭ دۆلەت ھامىيلىقىدىكى تور ئارتىستلىرى دۇنيا مىقياسىدا قوللىنىپ كېلىۋاتقان بولۇپ، ئاپتور ئورگانلار بۇنى بىر تۈرلۈك ئورتاق تەھدىت، دەپ قارايدۇ. بۇ ھەقتىكى تېخمۇ تەپسىلى مەلۇماتلار ئۇچۇن بىرلەشمە مەسلىھەتتىكى «خ خ ج نىڭ دۆلەت ھامىيلىقىدىكى تور ئارتىستلىرىنىڭ تور ۋە ئۇسكۇنە بىلەن تەمىنلىگۈچىلەرگە ھۇجۇم قىلىشى» ۋە «خ خ ج دۆلەت ھامىيلىقىدىكى تور ئارتىستلىرىنىڭ ئامېرىكىدىكى ئاچقۇچلۇق ھۇل مۇئەسسەسە ئەسلىھەلىرىگە زىيان سېلىشى ۋە ئۇزۇن مۇددەتلىك ئىزچىل زىيارىتى» گە قارالسۇن.

APT40 ئادەتتە پات-پاتلا ئۆز مەشغۇلاتى جەريانىدا سېتىۋالغان ياكى ئىجارىگە ئالغان ھۇل مۇئەسسەسەلەردىن زىيانكەشلىككە ئۇچرىغۇچىغا يۈزلەنگەن C2 ھۇل مۇئەسسەسە قۇرۇلۇشى سۈپىتىدە پايدىلىنىدۇ؛ ھالبۇكى بۇنداق ھۇنەرلەر ھازىر ئاللىقاچان «تەيىنەمنىڭ زامانىسى»دىكى نەرسىلەرگە ئايلىنىپ قالغان.

ۋاستىلار

ASD قارمىقىدىكى ACSC بولسا تۆۋەندە بايان قىلىنغان تەكشۈرۈشلەر داۋامىدا ئېنىقلانغان بەزى زىيانلىق ھۆججەتلەرنى بىز بىلەن ھەمبەھىرلەيدۇ. بۇ ھۆججەتلەر VirusTotalغا يۈكلەنگەن بولۇپ، كەڭ مەنىدىكى تور مۇداپىئەسى ۋە تور بىخەتەرلىكى ساھەسىنى مۇداپىئە كۆرۈشى زۆرۈر بولغان تەھدىتلەرنى تېخىمۇ ياخشى چۈشىنىش ئىمكانىيىتىگە ئىگە قىلىدۇ.

دېلو مىساللىرى

ASD قارمىقىدىكى ACSC تور ئارتىستلىرىنىڭ ئۆز ۋاستىلىرى ۋە ھۇنەرلىرىنى قانداق ئىشقا سالىدىغانلىقىدىن خەۋەردار قىلىش مەقسىتىدە ئىككى تۈرلۈك نامسىز تەكشۈرۈش دوكلاتىنى ھەمبەھىرلىگەن.

MD5	ھۆججەت نامى	قوشۇمچە مەلۇماتلار
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java Source
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

1-دېلو مسالى

بۇ دوكلاتنىڭ تېخمۇ كەڭ تارقىلىشى ئۈچۈن نامسىز شەكىل قوللىنىلدى. تەسىرگە ئۇچرىغان ئورگان تۆۋەندە «ئورگان» دەپ ئېلىندۇ. زىيانكەشلىككە ئۇچرىغۇچىنىڭ كىملىكىنى قوغداش ۋە ASD قارمىقىدىكى ACSC نىڭ ھادىسىلەرگە ئىنكاس قايتۇرۇش ئۇسۇللىرىنى ھېمايە قىلىش ئۈچۈن بۇنىڭدىكى بەزى ئېنىق تەپسىلاتلار ئۆچۈرۈۋېتىلدى.

قىسقىچە خۇلاسە

بۇ دوكلاتتا ASD قارمىقىدىكى ACSC نىڭ 2022-يىلى ئېيۇلدىن سېنتەبىرگىچە بولغان ئارىلىقتا ئورگانىنىڭ تورلىرى نىشان قىلىنغان ئۇتۇقلۇق بۇزغۇنچىلىقلار ھەققىدە بايقىغانلىرى تەپسىلى بايان قىلىنغان. بايقالغان يامان غەرەزلىك پائالىيەتلەرنى خۇلاسىلەش، شۇنىڭدەك بۇنىڭغا دەرمان بولىدىغان چارە ۋە تەۋسىيەلەرنى تۈزۈپ چىقىش ئۈچۈن بۇ تەكشۈرۈش دوكلاتى ئاشۇ ئورگانغا يوللاپ بېرىلگەن. تەكشۈرۈش نەتىجىسى بۇ قېتىمقى بۇزغۇنچىلىقنىڭ جاۋابكارى APT40 ئىكەنلىكىنى كۆرسىتىدۇ.

ASD قارمىقىدىكى ACSC ئاۋغۇستىنىڭ ئوتتۇرىلىرىدا بۇ ئورگانغا مەزكۇر ئورگان ئاۋغۇستىنىڭ ئاخىرقى مەزگىللىرىدە ئىشلەتكەن بىر ئۈسكۈنىنىڭ تاجاۋۇزغا ئۇچرىغان بولۇشى مۇمكىنلىكىنى، ئۇلارنىڭ بولسا مۇشۇ ئۈسكۈنە ئارقىلىق يامان غەرەزلىك ئالاقدا بولغانلىقىنى ئۇقتۇرغان. شۇنىڭدەك مەزكۇر ئورگانىنىڭ ئىجازىتىنى ئالغاندىن كېيىن ASD قارمىقىدىكى ACSC مەزكۇر ئورگانىنىڭ تورىدىكى يۇقۇملىنىش ئېھتىماللىقى بولغان ماشىنىلارغا باش ماشىننىڭ ئاساس قىلغان سۈزگۈچ ئورناتقان. بۇ سۈزگۈچلەر بولسا ASD قارمىقىدىكى ACSC نىڭ ھادىسىلەرگە ئىنكاس قايتۇرۇش مۇتەخەسسىسلىرىنىڭ بۇ ھەقتە ئۈزۈل-كېسىل بولغان رەقەملىك ئىسپات توپلاش تەكشۈرۈشىگە ئىمكانىيەت يارىتىدۇ. مەزكۇر بولغان سۈزگۈچ ئۇچۇرلىرىدىن پايدىلىنىش ئارقىلىق ASD قارمىقىدىكى ACSC نىڭ تەھلىلچىلىرى بۇ گۇرۇپپىنىڭ پائالىيەت خەرىتىسىنى ئۇتۇقلۇق سىزىپ چىقتى ھەمدە بايقالغان ھادىسىلەرنىڭ تەپسىلى ۋاقىت جەدۋىلىنى تۈزۈپ چىقتى.

ئىيۇل ئېيىدىن تارتىپ ئاۋغۇست ئېيىغىچە بولغان ئارىلىقتا ASD قارمىقىدىكى ACSC تەرىپىدىن كۆزىتىلگەن مۇھىم ئارتىستلارنىڭ پائالىيەتلىرى تۆۋەندىكىلەرنى ئۆز ئىچىگە ئالىدۇ:

- ئارتىستقا ئۆزلىرىنىڭ تور خەرىتىسىنى سىزىپ چىقىش ئىمكانىيىتى يارىتىپ بېرىدىغان ئاساسلىق ماشىنىلارنىڭ سانىنى ئېلىش؛
- تور قېپىنىڭ قوللىنىلىشى بولسا تور ھوجۇمچىلىرىنى توردا پۈت دەسسەپ تۇرىدىغان ئەڭ دەسلەپكى نۇقتىلار بىلەن تەمىنلەيدۇ ھەمدە بۇيرۇقلارنى ئىجرا قىلىش ئىقتىدارىغا ئىگە قىلىدۇ؛ يەنە
- تور ھوجۇمچىلىرىنىڭ يامان غەرەزلىك قىلمىشلىرىغا كېرەكلىك باشقا قوراللارنى ئورۇنلاشتۇرىدۇ.

تەكشۈرۈشتە زور ساندىكى سەزگۈر سانلىق مەلۇماتلارنىڭ زىيارەت قىلىنغانلىقى، شۇنىڭدەك بۇ ئارتىستلارنىڭ تور ساھەسىنى توغرىسىغا مېڭىپ ئۆتكەنلىكى بايقالغان(T1021.002). تور مۇداخىلىسىنىڭ كۆپ قىسمى مەزكۇر گۇرۇپپىنىڭ تورلاردا كۆپلىگەن زىيارەت ۋېكتور نۇقتىلىرىنى بەرپا قىلىپ چىقىشى، تورلارنىڭ تۈپ-تۈز قۇرۇلمىلىق بولۇشى، شۇنىڭدەك ئېچىق قىسمدا ياساپ چىقىلغان ھەمدە بىخەتەر بولمىغان يۇمتاللار ئارقىلىق ھۆججەتلەرنىڭ تورلارغا يۈكلىنىشى سەۋەبىدىن كېلىپ چىققان. سۈزۈۋېلىنغان سانلىق مەلۇماتلار بۇ گۇرۇپپىنىڭ ئاشۇ تورلارغا كىرىشىگە ئىمكان بەرگۈچى نوپۇز ئىجازەتلىرىنى، شۇنىڭدەك دەسلەپكى كىرىش ۋېكتورى توسۇۋېتىلگەن بولسا تور ئارتىستلىرىغا ئىجازەتسىز كىرىش يوللىرىنى ئېچىپ بەرگۈچى تور ئۇچۇرلىرىنى ئۆز ئىچىگە ئالىدۇ. ئەڭ دەسلەپ ھوجۇم قىلىنغان ماشىنىلارنىڭ سىرتىدا باشقا يامان غەرەزدىكى قوراللار ھازىرچە بايقالمىغان. ئەمما بىرەر گۇرۇپپىنىڭ قانۇنلۇق ۋە ئالاھىدە ئىمتىيازلىق ئىجازەتلەرنى قولغا چۈشۈرەلىشى بۇنىڭدا قوشۇمچە قوراللارنى ئىشلىتىشىنىڭ ھاجەتسىز ئىكەنلىكىنى كۆرسىتىپ بېرىدۇ. تەكشۈرۈش نەتىجىسىدىن قارىغاندا مەزكۇر ئورگان تورلاردىكى كۆپچىلىككە مەلۇم بولغان ئاجىزلىقلارنىڭ تەسادىپىي قۇربانى بولۇپ كەتكەن ئەمەس، ئەكسىچە APT40 ئۇلارنى غەرەزلىك ھالدا نىشانغا ئالغاندەك قىلىدۇ.

تەكشۈرۈش نەتىجىلىرى

2022-يىلى ئاۋغۇست ئېيىنىڭ ئوتتۇرىسىدا ASD قارمىقىدىكى ACSC بۇ ئورگانىغا جەزملەشتۈرۈلگەن بىر زىيانلىق IP ئادرېسىنىڭ ئاز دېگەندىمۇ ئىيۇل ۋە ئاۋغۇست ئايلىرى ئارىلىقىدا مەزكۇر ئورگانىڭ كومپيۇتېر تور سىستېمىسى بىلەن ئالاقىدا بولغانلىقىنى، بۇ IP ئادرېسىنى دۆلەت هامىيلىقىدىكى تور گۈرۈپپىسى بىلەن ئالاقىسى بار، دەپ قارايدىغانلىقىنى ئۇقتۇرغان. مۇداخىلىگە ئۈچرىغان ئۈسكۇنە بەلكىم بىرەر كىچىك شىركەتكە ياكى ئۆيدە ئولتۇرۇشلۇق بىرەر قوللانغۇچىغا تەۋە بولغان بولۇشى مۇمكىن.

ئاۋغۇستنىڭ ئاخىرلىرىدا ASD قارمىقىدىكى ACSC ئورگانىنىڭ تور بېتىدىكى ماشىنىلارغا باش ماشىننى ئاساس قىلغان بىر ۋاكالەتچىنى ئورۇنلاشتۇرۇپ قويغان بولۇپ، بۇ هال بۇزغۇنچىلىققا ئۇچرىغانلىقىنىڭ ئىسپاتى بولغان ئىدى.

خاتىرىلەرنى سەرەمجانلاشتۇرۇش ۋە تورلارنى لايىھىلەش سەۋەبىدىن تەكشۈرۈشكە ياردەم بېرىشى مۇمكىن بولغان بەزى بۇيۇملاردىن پايدىلىنىش ئىمكانىيتى يوق ئىدى. شۇنداق بولسىمۇ ئورگانىنىڭ بارچە مەۋجۇت مەلۇماتلار بىلەن تەمىن ئېتىشكە تەييار بولۇشى ASD قارمىقىدىكى ACSC نىڭ ھادىسىلەرگە ئىنكاس قايتۇرغۇچىلىرىغا كەڭ كۆلەملىك تەھلىل ۋە APT40 نىڭ توردىكى پائالىيەتلىرى ھەققىدە چوڭقۇنچە ھاسىل قىلىش ئىمكانىيتى يارىتىپ بەردى.

سېنتەبىرنىڭ ئاخىرىدا ASD قارمىقىدىكى ACSC بىلەن مەسلىھەتلەشكەندىن كېيىن ئورگان ئۆزلىرىنىڭ دەسلەپكى ئۇقتۇرۇشىدا ئېنىقلانغان IP نى ئىنكار قىلىش ھەققىدە قارار ئالدى. ئۆكتەبىردە ئورگان بۇ ھەقتىكى تۇزىتىش خىزمىتىنى باشلىدى.

تەپسىلاتى

ئىيۇل ئېيىدىن باشلاپ تور ئارتىسىتلىرى `<webapp>2-ext` تە ئىشلەيدىغان مەخسۇس تور پروگراممىلىرى (T1190) نى سىناق قىلىش ۋە ئۇنىڭدىن پايدىلىنىش ئىمكانىيىتىگە ئىگە بولدى. بۇ بولسا ئۆز نۆۋىتىدە بۇ گۇرۇپپىغا توردىكى قوراللسزلاندۇرۇلغان رايوندا پۈت تىرەپ تۇرۇش ئىمكانىيتى يارىتىپ بەرگەندى. بۇلار بولسا تور بەت ۋە كۆرۈنىدىغان تور بوشلۇقلىرىنىڭ سانىنى ئېلىشقا ئىشلىتىلگەن. ئوغرىلانغان ھېساۋات مەلۇماتلىرى (T1078.002) بولسا Active Directory (T1018) نى سۈرۈشتە قىلىش ۋە DMZ ئېچىدىكى بىرنەچچە ماشىنىغا ھۆججەت ھەمبەھرلىگۈچى (T1039) ئورنىتىپ قويۇش ئارقىلىق ئۇچۇرلارنى سۈزۈۋېلىشقا ئىشلىتىلگەن. تور ئارتىسىتلىرى مۇلازىمىتېردىن(T1558.003) ئىناۋەتلىك تور ئىجازەت ھېساۋاتىغا دائىر ئۇچۇرلارنى قولغا چۈشۈرۈش ئۈچۈن Kerberoasting ھۇجۇمىنى ئىشقا سالغان. بۇ گۇرۇپپىنىڭ DMZ دا ياكى ئېچىكى تورلاردا قوشۇمچە مەۋجۇتلۇق نۇقتىلىرىغا ئىگە بولغانلىقى زادىلا بايقالمىغان.

كۆرۈنمە تەرتىپ

تۆۋەندىكى ۋاقىت جەدۋىلى ئورگانىنىڭ توردا بايقالغان زىيانلىق تور ئارتىسىتلىرىنىڭ پائالىيەتلىرى، شۇنىڭدەك بۇنىڭ ئاساسىي باسقۇچلىرى ھەققىدە كەڭ دەرىجىدە مەلۇمات بېرىدۇ.

دەسلەپكى بايقاش

ئارتىست مەزكۇر ئورگان ئۇچۇن مەخسۇس ياسالغان تور پروگراممىلىرىغا سىناق يۈرگۈزدى

ساھىبخانىنىڭ سانىنى ئېلىش

T1082 سىستېما ئۇچۇرلىرىنىڭ بايقىلىشى

ئاساسىي ماشىننىڭ سانىنى ئېلىش ۋە ئۇزۇن مۇددەتلىك زىيارەتنى باشلاش

قانۇنىي ھېساۋات ئۇچۇرلىرى ئارقىلىق تىزمىغا كىرىشنىڭ تۇنجى قېتىم بايقىلىشى

تور رازۋېدكىسى

T1021.002 يىراق مۇسايىلىك مۇلازىمەتلەر: SMB/Windows باشقۇرغۇچىنىڭ ھەمبەھرلىشى

T1135 توردىكى ھەمبەھرلەشنىڭ بايقىلىشى

تور ئاساسىدىكى رازۋېدكا ۋە ئارتىستلارنىڭ پائالىيىتى تۆۋەندىكىلەرنى ئۆز ئىچىگە ئالىدۇ: SMB ھەمبەھرلىكىنى ئورۇنلاشتۇرۇش، تور ئاساسىدىكى سىكەنىرلەش ۋە تور بوشلۇقلىرىنىڭ سانىنى ئېلىش

تىمسىقلاش

T1190 ئاممىغا يۈزلەندۈرۈلگەن پروگراممىلاردىن پايدىلىنىش

تور پروگراممىلىرىنى تىمسىقلاش ۋە تور قېپىنى يارىتىش

زىيانلىق ئۆزگارا تەسىر

ئورگان ماشىنىسىنىڭ مەلۇملۇق دۆلەت ھامىيلىقىدىكى ھۇل مۇئەسسە بىلەن ئۆزئارا تەسىر كۆرسىتىشىنىڭ تۇنجى قېتىم بايقىلىشى

قايتىدىن باغلىنىش

T1090 Proxy

ئارتىست ssf قوراللىرىنىڭ باغلىنىشىنى قايتىدىن ئورناتقان (28-ئىيۇل قاتارلىق كونا‌ردىكى باشقا پائالىيەتلەر بىلەن ئوخشاپ كېتىدۇ)

تەپسىلى ۋاقىت جەدۋىلى

ئىيۇل: ئارتىستلار قاتناش قاتلام بىخەتەرلىكى (TLS) ئۇلىنىشى (T1102) ئارقىلىق ئورگان ئۇچۇن قوزغۇلغان مەخسۇس تور (T1190) (تۆۋەندە «تور» ياكى «تور ئەپ» دەپبىلىدۇ) نىڭ باش سەھىپىسىگە دەسلەپكى ئۇلىنىشنى ۋۇجۇتقا چىقارغان. باشقا دىققەتكە سازاۋەر بولغىدەك پائالىيەتلەر بايقالمىدى.

ئىيۇل: ئارتىستلار تېخمۇ چوڭقۇر تەكشۈرۈش ئۇچۇن ئاخىرقى نۇقتىلارنىئىزلەپ، تور پروگراممىلىرىنىڭ تور بەتلىرىنى ساناشقا ئۆتكەن.

ئىيۇل: ئارتىستلار مەلۇم بىر يەكۇنىي نۇقتىنى قېزىش ئۇرۇنۇشىغا پۈتۈن دىققىتىنى مەركەزلەشتۈرگەن.

ئىيۇل: تور ئارسىتلىرى تور مۇلازىمىتېرىگە مۇۋاپىقىيەتلىك ھالدا `POST` قىلالىشى مۇمكىن بولۇپ، بۇنىڭدا باشقا سەھىپىلەرگە جايلاشتۇرۇلغان تور قېپىدىن پايدىلانغان بولسا كېرەك. خۇددى شۇ ئارتىستلار قوللانغان، دەپ قارىلۇاتقان ئىككىنچى IP مۇ ئەينى URL مەنزىلگە مەزمۇن چاپلاشقا باشلىغان. ئارتىستلار ئوخشىشپ كېتىدىغان بىرنەچچە تور قېپى ياساپ چىققان ۋە ئۇلارن سىناق قىلغان.

بۇنى قوللىنىشنىڭ ئېنىق ئۇسۇلى ھازىرچە ئېنىق ئەمەس. ئەمما شۇ نەرسە ئېنىقكى، يەكۇنىي نۇقتا `ext-2<webapp>` دا ھۆججەت ياساش ئۇچۇن نىشانغا ئېلىنغان.

ASD قارمىقىدىكى ACSC نىڭ پىكرىچە، ئورتاق قىزىقىش ۋە دەسلەپكى ئۇلىنىشنىڭ بىرنەچچە مىنۇتلۇق ۋاقىت پەرقى بىلەن سادىر بولغانلىقىدىن قارىغاندا ئىككى IP ئادرېسىنىڭ مەنزىل ئۇلىنىشلىرى ئوخشاش تور مۇداخىلىسىنىڭ بىر قىسمى.

ئىيۇل: بۇ گۇرۇپپا ئاساسىي ماشىنىلارنىڭ سانىنى ئېلىشنى داۋام قىلغان ھەمدە ئىمتىيازلارنى ئاشۇرۇشنىڭ ئىمكانىيەتلىرىنى ئىزلەشكە ۋە باشقا تور قېپىنى ئورنىتىشقا ئۇرۇنغان. ئارتىستلار ئوغرىلانغان ھېساۋات مەلۇماتلىرى ئارقىلىق `<firstname.surname>@<organisation domain>` غا كىرگەن.

ئارتىستلارنىڭ پائالىيەتلىرى `ext-2<webapp>` دىكى ئىمتىيازنى ئاشۇرۇشتەك ئۇتۇقلارغا ئېرىشەلمىگەندەك قىلىدۇ. ئەكسىچە، ئارتىستلار تور ئاساسىدىكى پائالىيەتلەرنى مۇھىم ئورۇنغا قويغان.

ئىيۇل: ئارتىستلار ئوغرىلانغان ھېساۋات ئۇچۇرلىرىنى مۇلازىمەت ھېساۋاتىدا سىناق قىلغان بولۇپ، بۇنى قاتتىق كود ئارقىلىق ئىچكى جەھەتتە كېرىشكە بولىدىغان ئىككى قاتلاملىق ھۆججەتلەردىن تېپىۋالغان بولۇشى مۇمكىن.

ئىيۇل: ئارتىستلار ئوچۇق مەنبەلىك قوراللاردىن Secure Socket Funnelling ئارقىلىق يامان غەرەزلىك ھۇل مۇئەسسەسگە باغلانغان.

بۇ ئۇلىنىش ئارتىستنىڭ ھۇجۇم ماشىنىلىرىدا ئورگاننىڭ ئىچكى تورلىرىغا ھۇجۇم قىلىشقا ئىشلىتىلىدۇ. ئۇلارنىڭ ماشىنا نامىلرى مۇشۇ ئىجازەتلەر ئارقىلىق مۇلازىمەت ھېساۋاتىغا كىرىشكە ئۇرۇنغاندىكى ھادىسىلەر خاتىرىسىدە كۆرىستىلگەن.

ئاۋغۇست: ئارتىستلار چەكلىك مىقداردىكى پائالىيەتنى ئەمەلگە ئاشۇرغان بولۇپ، شۇ قاتاردا ئۇلارنىڭ مۇلازىمەت ھېساۋاتى بىلەن ئالاقە ئورنىتىشى مەغلۇبىيەتكە ئۇچرىغان.

ئاۋغۇست: ئارتىستلار مۇھىم تورلار ۋە Active Directoryنىڭ سانىنى ئېلىش بىلەن مەشغۇل بولغان. ئارقىدىنلا ئوغرىلانغان يەنە بىر ھېساۋات DMZ دائىرىسىدىكى «كۆزنەك» (Windows) ماشىنىلىرىغا ھەمبەھرلەش مەزمۇنلىرىنى چىقىرىشقا ئىشلىتىلگەن. بۇ بولسا ئۇچۇرلارنى ئۇتۇقلۇق سۈزۈۋېلىشقا شارائىت ياراتقان.

قارىغاندا بۇ ھال ئوغرىلانغان ھېساۋات مەلۇماتلىرىنى DMZ دىكى ئورنىتىشقا بولىدىغان ماشىنىلاردا پۈرسەتپەرەسلىك شەكلىدە قوللىنىشتەك قىلىدۇ. خەۋپسىزلىك تاملىرى بولسا ئارتىستنىڭ مۇشۇ خىلدىكى ئىچكى تور پائالىيەتلىرىنى توسۇالدۇ.

ئاۋغۇست – سېپتەبىر: SSF قورالى زىيانلىق IP بىلەن بولغان ئالاقىنى قايتىدىن ئەمەلگە ئاشۇرىدۇ.

تىزمغا كىرىشى توسۇپ قېلىنمىغىچە بۇ گۇرۇپپىنىڭ باشقا قوشۇمچە پائالىيەتتە بولغانلىقى كۆزگە چېلىقمايدۇ.

سېپتەبىر: ئورگان ئادەتتە زىيانلىق IPنى خەۋپسىزلىك تاملىرىدا رەت قىلىش ئارقىلىق توسۇپ قويىدۇ.

2 بۇنداق ئەھۋالدا يەكۇنىي نۇقتا بولسا تور پروگراممىسىنىڭ بىر مۇھىم رولى ھېسابلىنىدۇ.

3 مۇلازىمەت ھېساۋاتلىرى بولسا خۇسۇسىي قوللانغۇچىلارغا ئەمەس، بەلكى مۇلازىمەتلەرگە باغلانغان بولىدۇ. «مىكروسوفت» شىركىتىنىڭ تور بوشلۇقىدا ھەر خىل تۈردىكى ھېساۋاتلار مەۋجۇت.

4 ھەمبەھرلەنگەن مەزمۇنلارنى ئورنىتىش بولسا ھۆججەت سىستېمىسى قۇرۇلمىسىدىكى ھۆججەتلەرنى پايدىلانغۇچىلار ياكى پايدىلانغۇچى گۇرۇپپا ئوچۇن كۆرگىلى بولىدىغان قىلىپ بېرىش جەريانىدۇر.

ئارتىستلارنىڭ تاكتىكىسى ۋە ھۈنەرلىرى

MITRE ATT&CK رامكىسى تور ماكانىدىكى تەھدىت ئارتىستلىرى قوللىنىدىغان تاكتىكا ۋە ھۈنەرلەرنىڭ ھۆججەتلەشتۈرۈلگەن توپلىمى ھېسابلىنىدۇ. بۇ رامكىنى ئامېرىكىدىكى تىجارەتسىز MITRE شىركىتى ئىشلەپ چىققان بولۇپ، تەھدىت ئارتىستلىرىنىڭ قىلمىش-ئەتمىشلىرىنى بايان قىلغۇچى دۇنياۋى تىل سۈپىتىدە قوللىنىلىدۇ.

ASD قارمىقىدىكى ACSC ئارتىستلارنىڭ زىيانلىق پائالىيەتلىرى ھەققىدە تۆۋەندىكى تېخنىكا ۋە تاكتىكىلارنى باھالاپ چىقىدۇ:

رازۋېدكا

T1594 - زىيانكەشلىككە ئۇچرىغۇچىغا مەنسۇپ تور بەتلەرنى ئىزلەش

ئاشۇ تورلارغا كىرىش ئىمكانىيىتىنى ئېنىقلاش ئۈچۈن ئارتىستلار مەخسۇس تور پروگراممىلىرىنى ساناش بىلەن مەشغۇل بولىدۇ.

دەسلەپكى زىيارەت

T1190 - ئاممىغا يۈزلەنگەن پروگراممىلارنى تىمسىقلاش (مەخسۇس تور پروگراممىلىرىدىن پايدىلىنىش بويىچە)

T1078.002 - ئىناۋەتلىك ھېسابئاتلار: تور بوشلۇقى ھېسابئاتلىرى (ئوغرىلانغان ھېسابقا مەلۇماتلىرى خاتىرىسى بويىچە)

ئىنتېرنېت پاش قىلغان مەخسۇس تور پروگراممىلىرىدىن پايدىلىنىش ئارتىستلارنى دەسلەپكى كىرىش نۇقتىسى بىلەن تەمىنلەيدۇ. ئارتىست كېيىنچە تېخمۇ ئىچكىرىلەپ تورلارغا كىرىشنى داۋاملاشتۇرۇش ئۈچۈن ئۆزلىرى ئوغرىلىغان ھېسابقا مەلۇماتلىرىدىن ئوكۇشلۇق پايدىلانغان.

ئىجرائىيات

T1059 - بۇيرۇق ۋە يېزىق تەرجىمانى (تور قېپى ئارقىلىق بۇيرۇقلارنى ئىجرا قىلىش بويىچە)

T1072 - يۆتكىلىدىغان ئورنىتىش ۋاستىلىرى (IP غا ئۇلىنىش ئۈچۈن ئوچۇق مەنبە قورالى بولغان Secure Socket Funnelling (SSF) دىن پايدىلىنىدىغان ئارتىست ھەققىدە)

قەتئىيلىك

T1505.003 - مۇلازىمەت يۆتكىلىنىڭ تەشكىلىي قۇرۇلمىسى تور قېپى (كىرىش ئىجازىتى ئېلىش ئۈچۈن تور قېپى ۋە SSF دىن پايدىلىنىش بويىچە)

قانۇنلۇق زىيارەت

T1552.001 - مەخپىي نومۇر دۆكىنىدىكى ھېسابقا مەلۇماتلىرى (بىنا باشقۇرۇش تىزىمى (BMS) بىلەن باغلىنىشلىق بولغان مەخپىي نومۇر ھۆججەتلىرى بويىچە)

T1558.003 - Kerberos تالۇنلىرىنى ئوغرىلاش ياكى ساختىلاشتۇرۇش: Kerberoasting (تور ھېسابئاتلىرىنى ئوغرىلاش ئۈچۈن قىلىنغان ھۇجۇملار)

باغلانما ھەرىكەت

T1021.002 - يىراق مۇسابىلىك مۇلازىمەت: SMB ھەمبەھرلىگەنلەر (بىر نەچچە ئۈسكۈنىگە SMB ھەمبەھرلىگەن مەزمۇنلارنى ئورناتقان ئارتىست ھەققىدە)

توپلاش

T1213 - ئۇچۇر ئامبارلىرىدىكى مەلۇماتلار (BMS مۇلازىمىتىردا بايقالغان قوللانمىلار\ھۆججەتلەر بويىچە)

سۈزۈۋېلىش

T1041 - قانىلى ئارقىلىق سۈزۈۋېلىش (ئارتىستنىڭ Active Directory ۋە ھەمبەھرلەشنى ئورنىتىشتىن ئۇچۇرلارنى سۈزۈۋېلىشى)

2-دېلو مسالى

بۇ دوكلاتنىڭ تېخىمۇ كەڭ تارقىلىشى ئۈچۈن نامسىز شەكىل قوللىنىلدى. تەسىرگە ئۇچرىغان ئورگان تۆۋەندە «ئورگان» دەپ ئېلىندۇ. زىيانكەشلىككە ئۇچرىغۇچىنىڭ كىملىكىنى قوغداش ۋە ASD قارمىقىدىكى ACSC نىڭ ھادىسىلەرگە ئىنكاس قايتۇرۇش ئۇسۇللىرىنى ھېمايە قىلىش ئۈچۈن بۇنىڭدىكى بەزى ئېنىق تەپسىلاتلار ئۆچۈرىۋېتىلدى.

قىسقىچە خۇلاسە

بۇ دوكلاتتا ASD قارمىقىدىكى ACSC نىڭ 2022-يىلى ئاپرېلدا ئورگاننىڭ تورلىرىنى نىشان قىلغان ئۇنۇقلۇق بۇزغۇنچىلىقلار ھەققىدە بايقىغانلىرى تەپسىلى بايان قىلىنغان. بايقالغان يامان غەرەزلىك پائالىيەتلەرنى خۇلاسىلەش ھەمدە بۇنىڭغا دەرمان بولىدىغان چارە ۋە تەۋسىيەلەرنى تۇزۇپ چىقىش ئۈچۈن بۇ تەكشۈرۈش دوكلاتى ئاشۇ ئورگانلارغا يوللاپ بېرىلگەن. تەكشۈرۈش نەتىجىسى بۇ قېتىمقى بۇزغۇنچىلىقنىڭ جاۋابكارى APT40 ئىكەنلىكىنى كۆرسىتىدۇ.

2022-يىلى مايدا ASD قارمىقىدىكى ACSC شۇبھىلىك زىيانداش پائالىيەتلەرنىڭ 2022-يىلى ئاپرېل ئېيىدىن بۇيان ئورگان تورىغا تەسىر كۆرسىتىپ كېلىۋاتقانلىقىنى بۇ ئورگانلارغا ئۇقتۇردى. ئارقىدىنلا ئورگان ASD قارمىقىدىكى ACSCغا ئۆزلىرىنىڭ ئىنتېرنېتقا يۈزلەنگەن مۇلازىمېتىردىكى زىيانداش يۇمىتاللارنى بايقىغانلىقىنى، بۇ مۇلازىمېتىرنىڭ مەزكۇر ئورگاننىڭ كارخانا مۇلازىمىتىگە يېراقتىن كىرىش مەسلىسىنى ھەل قىلىشتا تىزىملىتىپ كىرىش ئېغىزى بىلەن تەمىن ئېتىدىغانلىقىنى ئۇقتۇرغان. بۇ مۇلازىمېتىر يېراقتىن كىرىش ۋە كىملىكنى باشقۇرۇش مەھسۇلاتىنى ئىشلىتىدىغان بولۇپ، بۇ دوكلاتتا «ئوغرىلانغان قۇرۇلما» دەپ ئاتىلىدۇ. مەزكۇر دوكلاتتا ASD قارمىقىدىكى ACSCنىڭ تەكشۈرۈشىگە جاۋابەن ئورگان ئۈچۈن تەييارلاپ چىقىلغان تەكشۈرۈش نەتىجىلىرى ۋە تۈزىتىش مەسلىھەتلىرى تەپسىلى بايان قىلىنغان.

دەللەر شۇنى كۆرسىتىدۇكى، ئەڭ ئاز دېگەندىمۇ 2022-يىلى ئاپرېل ئېيىدىن باشلاپ زىيانلىق تور ئارتىستلىرى ئورگان تورىغا يېراقتىن كىرىش ئېغىزى ئارقىلىق ئورگان تورىغا ھۇجۇم قىلىپ كەلگەن. مەزكۇر مۇلازىمېتىر بەلكىم بىرنەچچە ئارتىستنىڭ بۇزغۇنچىلىقىغا ئۇچرىغان بولۇشى مۇمكىن، شۇنداقلا ئاشۇ بۇزغۇنچىلىق مەزگىلىدە ھەممىگە مەلۇم بولغان يېراق مۇسابىلىك كود ئىجرا قىلىش (RCE) نىڭ زەئىپلىكى بۇنىڭغا تەسىر كۆرسەتكەن بولۇشى مۇمكىن.

ASD قارمىقىدىكى ACSCئاساسلىق ئارتىستلارنىڭ تۆۋەندىكى قىلمىشلىرىنى بايقىغان:

- ئارتىستقا ئۆزلىرىنىڭ تور خەرىتىسىنى سىزىپ چىقىش ئىمكانىيىتى يارىتىپ بېرىدىغان ئاساسلىق ماشىنىلارنىڭ سانىنى ئېلىش؛
- ئىنتېرنېتقا يۈزلەنگەن پروگراممىلارنى تىمسىقلاش ۋە تور قاپلىرىدىن پايدىلىنىش، ئارتىستقا تور ساھەسىدە دەسلەپكى تايانچ نۇقتىسى يارىتىش ۋە بۇيرۇقلارنى بېجىرىش قابىلىيىتىنى ئاتا قىلىش؛
- ئىمتىيازلارنى ئاشۇرۇش ئۈچۈن يۇمتاللارنىڭ زەئىپلىكلىرىنى تېپىپ چىقىش؛
- باغلانما ھەرىكەتنى ئەمەلگە ئاشۇرۇش ئۈچۈن ھېسابات ئۇچۇرلىرىنى توپلاش

ASD قارمىقىدىكى ACSC 2022-يىلى ئاپرېل ئېيىدا زىيانداش ئارتىستنىڭ ھۇجۇمغا ئۇچرىغان ئۇسكۇنىدە بىرنەچچە يۈز جۈپ يىگانە قوللانغۇچى ئىسمى ۋە مەخپىي نومۇرىنى، شۇنىڭدەك يېراقتىن كىرىشكە ئالاقدار كۆپ-ئامىللىق دەللەلەش كودلىرىنى ۋە تېخنىكىلىق بۇيۇملارنى ئۆچۈرۈپ تاشلىغانلىقىنى بايقىغان. ئورگان بۇ ھالنى تەكشۈرۈپ كۆرگەندە مەخپىي نومۇرلارنىڭ قانۇنىي ئىكەنلىكى مەلۇم بولغان. ASD قارمىقىدىكى ACSCنىڭ باھالىشىچە، تور ئارتىسى بۇ تېخنىكىلىق بۇيۇملارنى قانۇنلۇق پايدىلانغۇچى سۈپىتىدە يېراقتىن كىرىش باسقۇچى يارىتىش ياكى ئۇنى ئوغرىلاش، شۇنىڭدەك ئورگاننىڭ ئىچكى شىركەت تورىغا قانۇنلۇق قوللانغۇچىلارنىڭ ھېساۋاتى ئارقىلىق كىرىش ئۈچۈن توپلىغان بولۇشى مۇمكىن.

تەكشۈرۈش نەتىجلىرى

تەكشۈرۈش خۇلاسىسى

ASD قارمىقىدىكى ACSC نىڭ ئېنىقلىشىچە، ئارتىست ئەملىيەتتە ئورگان خادىملىرىنى يىراقتىن كىرىش مەزگىلى بىلەن تەمىن ئەتكۈچى ئۈسكۇنە (لەر) گە بۇزغۇنچىلىق قىلغان ھەمدە مەزكۇر بۇزغۇنچىلىق ئارقىلىق كېيىنكى قىلمىشلىرىنى ئەمەلگە ئاشۇرۇشقا ئۇرۇنغان. مەزكۇر ئۈسكۇنىلەر يۈك تەڭپۇڭلاشتۇرۇلغان ئۇچ ماشىنىدىن تۈزۈلگەن بولۇپ، ئۇلاردا بۇزغۇنچىلىقنىڭ دەسلەپكى دەللىلىرى بايقالغان. دەسلەپكى بۇزغۇنچىلىقتىن كۆپ ئۆتمەي ئورگان يۈك تەڭپۇڭلاشتۇرۇلغان ئۇچ ماشىنىنىڭ ئىككىسىنى تاقىۋەتكەن. نەتىجىدە كېيىنكى بارلىق ھەرىكەتلەر بىرلا ماشىنىدا تاماملانغان. ھۇجۇمغا ئۇچرىغان ئۈسكۇنە بىلەن باغلىنىشلىق بولغان باشقا مۇلازىمىتىرلارمۇ خۇددى شۇ تەرىقىدە تۈك تەڭپۇڭلۇقىدا بولىدۇ. ئۇقۇمنىڭ ئېنىق بولۇشى ئۈچۈن مەزكۇر دوكلاتنىڭ كۆپ قىسىم جايلىرىدا بۇزغۇنچىلىققا ئۇچرىغان بارلىق ئۈسكۇنىلەر «يەككە ئۈسكۇنە» دەپ ئاتالدى.

ئارتىست 2022-يىلى ئاپرېلدىن باشلاپ بۇزۇلغان ئۈسكۇنىلەرگە تور قاپلىرىنى ئورنىتىش ئۈچۈن كۆپچىلىككە مەلۇم بولغان زەئىپلىكلەردىن پايدىلانغان، دەپ قارالماقتا. بۇ گۇرۇپپىدىكى تەھدىت ئارتىستلىرى بولسا ئۈسكۇنىدە تېخمۇ كېڭەيتىلگەن ئىمتىيازلارغا ئىگە بولۇۋالغان، دەپ قارىلىدۇ. ASD قارمىقىدىكى ACSCپايدىلىنىشقا بولىدىغان خاتىرىلەرنىڭ كەمچىل بولۇشى تۈپەيلىدىن بۇ قىلمىشنىڭ تولۇق كۆلىمىنى ئېنىقلاشقا ئىلاجسىز قالدى. ھالبۇكى، ئۈسكۇنىدىكى دەللىلەر ئارتىستنىڭ تۆۋەندىكىلەرنى قولغا چۈشۈرگەنلىكىنى كۆرسىتىدۇ:

- نەچچە يۈز جۈپ ھەقىقى قوللانغۇچى ئىسمى ۋە ئۇلارنىڭ مەخپى نومۇرى؛ ۋە
- زىياندىش ئارتىستلارنىڭ مەۋھۇم ئۈستەل كومپيۇتېرى قۇرۇلمىسى (VDI) غا قانۇنىي قوللانغۇچى سۈپىتىدە كىرىشىگە ئىجازەت بەرگەن تېخنىكىلىق بۇيۇملار توپلىمى.

ASD قارمىقىدىكى ACSCنىڭ باھالىشىچە، ئارتىست ئورگان تورىنى تېخمۇ ئىلگىرىلىگەن ھالدا بۇزۇشقا ئۇرۇنۇپ كۆرگەن. ئارتىست ئوغرىلاپ چىققان ئۇچۇرلار ئۇلارنى قانۇنلۇق پايدىلانغۇچىلار (ئېھتىمال ئۇلار تاللىغان قوللانغۇچىلار، جۈملىدىن باشقۇرغۇچىلار) سۈپىتىدە مەۋھۇم ئىش ئۈستىلىدىكى سۆھبەت مەزمۇنلىرىنى ئوغرىلاش ياكى يېغىنىنى باشلاش ئىمكانىيىتىگە ئىگە قىلغان. ئارتىست يەنە ئورگان مۇلازىمىتىنى تېخمۇ ئېچىكىرلەپ ۋەيران قىلىش، ئۇزۇن مۇددەتكە كىرىش ۋە باشقا مەقسەتلەر ئۈچۈن مۇشۇ كىرىش ۋېكتورىدىن پايدىلانغان بولۇشى مۇمكىن.

ئۈسكۇنە بىلەن تەمىن ئەتكۈچىنىڭ باشقۇرۇش مۇھىتىغا ھاۋالە قىلىنغان ئورگان ئۈسكۇنىلىرىدە بولسا بۇ خىل بۇزغۇنچىلىققا ئۇچرىغانلىقىنىڭ ھېچقانداق دەللىلى كۆزگە چېلىقمايدۇ.

كىرىش

ئۈسكۇنىلىرى بۇزغۇنچىلىققا ئۇچرىغان باش ماشىنا Active Directory ۋە تور مۇلازىمىتېرى ئارقىلىق VDI يېغىنىغا ئۇلانماقچى بولغان قوللانغۇچىلارنىڭ كىملىكىنى دەللىلەيدۇ. (T1021.001)

ئورنى	بۇزغۇنچىلىققا ئۇچرىغان ئۈسكۇنىنىڭ باش ماشىنا ناملىرى (يۈك تەڭپۇڭلۇقى)
1-سانلىق مەلۇمات مەركىزى	HOST1, HOST2, HOST3

ئۈسكۇنە ھۆل مۇئەسسەلىرى يەنە كىرىش دەرۋازىسى باش ئاپاراتىنى ئۆز ئىچىگە ئالىدۇ. مەزكۇر باش ئاپارات ئۈسكۇنە چەمبرىپ بەرگەن ۋە ئۇنىڭدىن چۈشۈرۈۋېلىنغان قوللانغۇچىلار كىملىكى قوللانغۇچىلارنىڭ قولىغا ئۆتكەندىن كېيىن ئۇلارنى VDI غا باردىغان تونىل بىلەن تەمىن ئېتىدۇ.

بۇ خىلدىكى ماشىنىلارنىڭ بۇزغۇنچىلىققا ئۇچرىغانلىقى ھەققىدە ھېچقانداق دەلىل مەۋجۇت ئەمەس. ھالبۇكى، كىرىش دەرۋازىسىدىكى ئاساسلىق ماشىنىلارنىڭ خاتىرىلىرى مەلۇم بولغان زىيانلىق ئادرېسلار بىلەن ئۇلارنىڭ زور كۆلەملىك ئالاقىدە بولغانلىقىنى ئىسپاتلايدۇ. بۇ ئەھۋال بەلكىم مەزكۇر ماشىنىدىكى پائالىيەتلەرنى ياكى بولمىسا مەزكۇر ماشىنىغا قول سوزغان تەھدىت ئارتىسىنىڭ تور ئالاقىلىرىنى ئەكس ئەتتۈرۈشى مۇمكىن. ھازىرقى مەۋجۇت دەللىلەر ئارقىلىق بۇ قىلمىشنىڭ خاراكتېرىنى بېكىتىشكە ئامالسىزمىز. ئەمما بۇ ئەھۋال ئاشۇ گۇرۇپپىنىڭ ئورگان توربىدا توغرىسىغا يۆتكەلگەنلىكىنى كۆرسىتىپ بېرىدۇ (TA0008).

ئىچكى ماشىنىلار

ASD قارمىقىدىكى ACSCئىچكى ئورگان تور بېتىدىن ئېلىنغان چەكلىك ساندىكى مەلۇماتلارنى تەكشۈرۈپ چىقتى. ئىچكى ئورگان توربىدىكى ئۆتۈقلۇق تاماملانغان زىيانلىق بۇزغۇنچىلىق قىلمىشلىرىدىن ھازىرچە مەلۇم بولغانلىرى تۆۋەندىكىچە: ئارتىستنىڭ VDI بىلەن ئالاقىدار بۇيۇملارنى زىيارەت قىلىشى، ئىچكى قىسمىدىكى SQL مۇلازىمىتېرىغا (T1505.001) قول تىقىپ بېقىشى، شۇنىڭدەك مەلۇملۇق زىياندىش IP ئادرېسىنىڭ زىيارەت دەرۋازىسىدىكى ئۈسكۇنىلەردىن (TA0011) ئۆتۈشى سەۋەبىدىن كېلىپ چىققان ئېقىم مىقدارىنى چۈشەندۈرۈشكە ئىلاج بولماسلىق.

مەزكۇر گۇرۇپپا ئۆزلىرىنىڭ بۇزغۇنچىلىققا ئۇچرىغان ئۈسكۇنىلەرگە كىرەلەيدىغانلىقىدىن پايدىلىنىپ ھەقىقى قوللانغۇچىلارنىڭ ئىسمى، ئۇلارنىڭ مەخپىي نومۇرى(T1003) ۋە كۆپ ئاممىللىق جەزملەشتۈرۈش قىممىتى (MFA) دېگەنلەرنى توپلىغان (T1111). بۇ گۇرۇپپا يەنە JSON Web قىممىتى (JWTs) (T1528) نى توپلىغان بولۇپ، بۇ ئەملىيەتتە مەۋھۇم ئۈستەل يۈزىگە كىرىش باسقۇچىنى يارىتىشقا ئىشلىتىلىدىغان جەزملەشتۈرۈش ۋاستىسى ئىدى. تور ئارتىستلىرى بۇلاردىن مەۋھۇم ئۈستەل يۈزىدە (T1563.002) يىراقتىن

كىرىش باسقۇچى ياىرتىش ياكى ئۇنى ئوغرىلاش، شۇنىڭدەك ئورگان تورىغا قانۇنلۇق قوللانغۇچى سۈپىتىدە كىرىشكە ئىشلەتكەن بولۇشى مۇمكىن (T1078).

ئارتىست يەنە بۇزغۇنچىلىققا ئۇچرىغان ئۇسكۇنىگە بولغان زىيارەت ھوقۇقىنى ئورگانىنڭ ئىچكى تورىغا جايلاشقان SQL مۇلازىمىتېرنى (T1505.001) قولغا چۈشۈرۈشكە ئىشلەتكەن. ئارتىست بەلكىم بۇ سانلىق مەلۇماتلارنى زىيارەت قىلغان بولۇشى مۇمكىن.

ئۇسكۇننىڭ تور دەرۋازىسىغا كىرىشتە قولغا كەلتۈرۈلگەن ئىسپاتلار شۇنى كۆرسىتىدۇكى، توردىكى ئېقىم مىقدارى بىزگە مەلۇم بولغان زىيانلىق IP ئادرېسىدىن كەلگەن ياكى شۇ ئادرېس ئارقىلىق ۋۇجۇتقا چىققان. يۇقىردا بايان قىلىنغاندەك، بۇ بەلكىم زىيانداش تور ئارتىسىنڭ مەزكۇر ئۇسكۇنىگە تەسىر كۆرسەتكەنلىكى ياكى ئۇنى ئىچكى تورغا كىرىشكە دەسمىي قىلماقچى بولغانلىقىنى كۆرسىتىشى مۇمكىن.

تەكشۈرۈشنىڭ ۋاقىت جەدۋىلى

تۆۋەندىكى تىزىملىك تەكشۈرۈش داۋامىدا ئېنىقلانغان ئاساسىي پائالىيەتلەرنىڭ ۋاقىت تەرتىۋىنى كۆرسىتىپ بېرىدۇ.

ۋاقىت	ۋەقە
2022-يىلى ئاپرېل	مەلۇم بولغان زىيانلىق IP ئادرېسى كىرىش دەرۋازىسىدىكى ماشىنا HOST7 بىلەن ئۆزئارا ئۇچراشقان. ئەمما بۇ ئۇچرىشىشنىڭ خاراكتېرىنى بېكىتىشكە ئىلاجسىزمىز.
2022-يىلى ئاپرېل	بارلىق ئاساسىي ماشىنىلار، HOST2 ،HOST1 ۋە HOST3 زىيانداش ئارتىستنىڭ بۇزغۇنچىلىقىغا ئۇچرىغان بولۇپ، بۇ ماشىنىلارغا تور قېپى ئورۇنلاشتۇرۇپ قويۇلغان. HOST2 دا بولسا بىر پائالىيەت خاتىرىسى يارىتىلغان ياكى ئۆزگەرتىلگەن. بۇ ھۆججەت زىيانداش ئارتىست قولغا چۈشۈرگەن ھېسابات ئۇچۇرلىرىنى ئۆز ئىچىگە ئالىدۇ. etc/security/opasswd and /etc/shadow/ قاتارلىق ھۆججەتلەر HOST1 ۋە HOST3 دە ئۆزگەرتىلگەن بولۇپ، بۇ مەخپىي نومۇرلارنىڭ ئۆزگەرتىلگەنلىكىنى كۆرسىتىدۇ. HOST1 دا مەۋجۇت بولغان دەللەر «sshuser» نامىدىكى قوللانغۇچىنىڭ مەخپىي نومۇرى ئۆزگەرتىلگەنلىكىنى كۆرسىتىدۇ.
2022-يىلى ئاپرېل	HOST2 ئورگان تەرىپىدىن تاقۇلىتىلگەن. HOST1 ۋە HOST3 دە قوشۇمچە تور قاپلىرى (T1505.003) ياساپ چىقىلغان. HOST1 بولسا HOST3 تىن كەلگەن زورلۇق خاراكتېرىدىكى شىددەتلىك SSH ئۇرۇنۇشىغا دۇچ كەلگەن. HOST3 دىكى بىر پائالىيەت خاتىرىسى ئۆزگەرتىلگەن (T1070). بۇ ھۆججەت زىيانداش ئارتىست قولغا چۈشۈرۈلگان ھېسابات مەلۇماتلىرىنى (T1078) ئۆز ئىچىگە ئالىدۇ. JWT لار بولسا قولغا چۈشۈرۈلگەن (T1528) ۋە HOST3 تىكى ھۆججەتلەرگە يوللانغان. HOST3 ئورگان تەرىپىدىن تاقۇلىتىلگەن. مۇشۇ ۋاقىتتىن كېيىنكى بارلىق پائالىيەتلەر HOST1 دا سادىر بولغان.
2022-يىلى ئاپرېل	HOST1دا قوشۇمچە تور قاپلىرى ياسالغان (T1505.003). JWT لار قولغا چۈشۈرۈلگەن ۋە HOST1 تىكى ھۆججەتلەرگە يوللانغان.
2022-يىلى ئاپرېل	HOST1 دا (T1505.003) قوشۇمچە تور قاپلىرى ياساپ چىقىلغان ھەمدە بىزگە مەلۇملۇق زىيانداش IP ئادرېسى ئاساسلىق ماشىنا بىلەن ئۆزئارا ئۇچراشقان (TA0011). مەلۇملۇق زىيانداش IP ئادرېسى HOST7 دىكى كىرىش دەرۋازىسى بىلەن ئۇچراشقان.
2022-يىلى ماي	مەلۇملۇق زىيانداش IP ئادرېسى HOST7 دىكى كىرىش دەرۋازىسى بىلەن ئۇچراشقان(TA0011). قوللانغۇچىنىڭ كىملىكىنى دەللەش ۋەقەسى HOST1 نىڭ پائالىيەت خاتىرىسىدىكى زىيانداش IP ئادرېسى بىلەن مۇناسۋەتلىك. بۇ ماشىنىدا قوشۇمچە تور قېپى ياساپ چىقىلغان(T1505.003).
2022-يىلى ماي	HOST1 دىكى يېزىقلارنى ئارتىست ئۆزگەرتىۋەتكەن (T1543). بۇ يېزىقلار ئىچكى SQL مۇلازىمىتېرىدىن مەلۇماتلارنى ئېلىپ بېرىش ئىقتىدارىنى ئۆز ئىچىگە ئالىدۇ.
2022-يىلى ماي	HOST1 دىكى قوشۇمچە پائالىيەت خاتىرىسى ئاخىرقى قېتىم ئۆزگەرتىلگەن (T1070). بۇ ھۆججەت ئورگان توردىكى قوللانغۇچىلار ئىسمى ۋە ئۇلارنىڭ مەخپىي نومۇرلىرىنى ئۆز ئىچىگە ئالىدىغان بولۇپ، بۇلار قانۇنلۇق، دەپ قارىلىدۇ (T1078).
2022-يىلى ماي	قوشۇمچە پائالىيەت خاتىرىسى ئاخىرقى قېتىم ئۆزگەرتىلگەن (T1070). بۇ ھۆججەت HOST1 دىن توپلانغان JWT لارنى ئۆز ئىچىگە ئالىدۇ.
2022-يىلى ماي	HOST1 دا قوشۇمچە تور قاپلىرى ياسالغان (T1505.003). مۇشۇ كۆندە ئورگان -2022يىلى ئاپرېلدا ياسالغان تور قېپىنىڭ بايقالغانلىقىنى ASD قارمىقىدىكى ACSC غا مەلۇم قىلغان.
2022-يىلى ماي	HOST1 دا كۆپلىگەن يېزىقلار ياساپ چىقىلغان بولۇپ، ئۇلارنىڭ بىرىگە Log4jHotPatch.jar دەپ نام قويۇلغان.
2022-يىلى ماي	iptables-save بۇيرۇقى كىرىش دەرۋازىسىغا ئىككى دانە ئوچۇق ئېغىز قوشۇش ئۈچۈن ئىشلىتىلگەن. بۇ ئېغىزلار 9998 ۋە 9999 ئىدى (T1572).

ئارتىستلارنىڭ تاكتىكىسى ۋە ھۇنەرلىرى

تۆۋەندە تەكتىلەنگەنلىرى تەكشۈرۈش داۋامىدا ئېنىقلانغان بىرنەچچە تاكتىكا ۋە ھۇنەرلەر ھېسابلىنىدۇ.

دەسلەپكى زىيارەت

T1190 ئاممىغا يۈزلەنگەن پروگراممىلاردىن پايدىلىنىش

بۇ گۇرۇپپا يىراقتىن كىرىش ۋە كىملىكنى دەللەلەش مەھسۇلاتلىرىدىكى RCE، ئىمتىيازلارنى ئاشۇرۇش ۋە قوللانغۇچىنىڭ كىملىكىنى دەللەلەشتىكى زەئىپلىكلەردىن پايدىلىنىش ئارقىلىق تورغا قارىتىلغان دەسلەپكى زىيارەت ھوقۇقىنى قولغا چۈشۈرىۋالغاندەك قىلىدۇ.

تۆۋەندىكى سەۋەبلەر تۆپەيلىدىن بۇ خىل دەسلەپكى زىيارەت ئۇسۇلىنىڭ ئەمەلگە ئېشىشى ئەڭ زور دەرىجىدە مۇمكىن بولغان:

- شۇ ۋاقىتلاردا مۇلازىمېتىر بۇ CVE لارغا نىسبەتەن ئاجىز بولغان؛
- بۇ خىل ئاجىزلىقلاردىن پايدىلىنىش ئۈرۈنۈشلىرى مەلۇملۇق ئارتىستنىڭ مۇئەسسەسلىرىدىن كەلگەن.
- تۈنجى قېتىم مەلۇم بولغان ئېچىكى زەرەرلىك پائالىيەت ئاجىزلىقلاردىن پايدىلىنىش ئۈرۈنىشىدىن ئۈزۈن ئۆتمەي سادىر بولغان.

ئىجرائىيات

T1059.004 بۇيرۇق ۋە يېزىق تەرجىمانى: Unix Shell

بۇ گۇرۇپپا يۇقىرىقى ئاجىزلىقلاردىن مۇۋەپپەقىيەتلىك پايدىلانغان بولۇشى مۇمكىن، شۇڭا تەسىرگە ئۇچرىغان ئۇسكۇنىدە Unix Shell بۇيرۇقلىرىنى ئىجرا قىلىشقا مۇۋاپىق بولغان. ئارتىستلار ئىجرا قىلغان بۇيرۇقلارنى ئۇسكۇنە خاتىرىگە ئالمىغانلىقى ئۈچۈن ئۇلارنىڭ تەپسىلاتى ھەققىدە ھازىرچە مەلۇمات بەرگىلى بولمايدۇ.

قەتئىيلىك

T1505.003 مۇلازىمېتىر يۈمتال زاپچاسلىرى: تور قېپى

ئارتىستلار زەرەرلەنگەن ئۇسكۇنىگە بىرنەچچە تور قېپى ئورنىتىپ قويغان. ئېھتىمال بىرنەچچە ئالاھىدە ئارتىست تور قېپىنى ئورۇنلاشتۇرغان بولۇشى مۇمكىن، ئەمما ئاز ساندىكى ئارتىستلار بۇ تور قاپلىرىدىن پايدىلىنىپ مەشغۇلات قىلغان. تور قاپلىرى ئادەتتە ھۇجۇمچىلارنىڭ ھۇجۇمغا ئۇچرىغان ئۇسكۇنىلەردە خالىغانچە قىلغان بۇيرۇقلارنى ئىجرا قىلىشىغا ئىمكان بېرىدۇ.

ئىمتىيازلارنى ئاشۇرۇش

T1068 ئىمتىيازلارنى ئاشۇرۇش ئۈچۈن پايدىلىنىش

ھازىرقى مەۋجۇت دەللىل-ئىسپاتلار بۇ ئارتىستلار قولغا كەلتۈرىۋالغان ئىمتىيازلارنىڭ دەرىجىسىنى تەسۋىرلەپ بەرمەيدۇ. دەرۋەقە، ئارتىستلار تور قاپلىرى ئارقىلىق بۇزغۇنچىلىققا ئۇچرىغان ئۇسكۇنىدىكى تور مۇلازىمېتىردا مۇئەييەن دەرىجىدىكى ئىمتىيازلارنى قولغا كەلتۈرەلەيدۇ. ئارتىستلار نورمالدا بۇزغۇنچىلىققا ئۇچرىغان ئۇسكۇنىلەردىكى ئاجىزلىقلاردىن پايدىلىنىپ يىلتىز ئىمتىيازى (root privileges)نى قولغا چۈشۈرەلەيدۇ.

قانۇنلۇق زىيارەت

T1056.003 كىرگۈزۈشتىن قولغا چۈشۈرۈش: Web Portal دىن قولغا چۈشۈرۈش

بۇزغۇنچىلىققا ئۇچرىغان ئۇسكۇنىدىكى دەللىلەر ئارتىستلارنىڭ قانۇنلۇق قانۇنلۇق دەپ قارىلىدىغان نەچچە يۈزلىگەن قوللانغۇچىلار ئىسمى ۋە ئۇلارنىڭ مەخپىي نومۇرلىرىنى ئېنىق تېكىست ھالىتىدە قولغا چۈشۈرىۋالغانلىقىنى كۆرسىتىدۇ. ئېھتىمال بۇ ئۇچۇرلار ھېسابات مەلۇماتلىرىنى ھۆججەتكە چىقىرىدىغان ھەقىقىي جەرياننى ئۆزگەرتىش ئارقىلىق قولغا چۈشۈرىۋالغان بولۇشى مۇمكىن. كۆپ ئاممىلىق جەرياننى ساقلاپ بەرگۈچى «مەخپىي مۇلازىمېتىر»نىڭ بۇزغۇنچىلىققا ئۇچرىغانلىقى ھەققىدە ھېچقانداق دەلىل يوق.

T1111 كۆپ ئاممىلىق جەرياننى چەكلەش

ئارتىست يەنە قانۇنلۇق كىرىشكە ماس كېلىدىغان كۆپ ئاممىلىق جەرياننى قىممەتنى قولغا چۈشۈرىۋالغان. ئۇلار بۇ قىممەتلەرنى ھۆججەتكە چىقىرىش ئۈچۈن ھەقىقى يوسۇندىكى كىملىكنى جەرياننى ئۆزگەرتىش ئارقىلىق قولغا چۈشۈرىۋالغان بولۇشى مۇمكىن. كۆپ ئاممىلىق جەرياننى خەۋپسىزلىكى بىلەن تەمىن ئېتىدىغان يېگانە قىممەتلەرنى ساقلاپ بەرگۈچى «مەخپىي مۇلازىمېتىر»نىڭ بۇزغۇنچىلىققا ئۇچرىغانلىقى ھەققىدە ھېچقانداق دەلىل يوق.

T1040 تورنى ھىدلاش

ئارتىستلار بۇزغۇنچىلىققا ئۇچرىغان ئۇسكۇنىدە HTTP ئېقىم مىقدارىنى چۈشۈرۈۋېلىش ئارقىلىق JWT لارنى قولغا كەلتۈرىۋالغان، دەپ قارىلىدۇ. دەللەلەر شۇنى كۆرسىتىدۇكى، ئەمىلىي قوللىنىلىدىغان پروگراممىلاردىن tcpdump بۇزغۇنچىلىققا ئۇچرىغان ئۇسكۇنىدە ئىجرا قىلىنغان. قارىغاندا ئارتىستلار مۇشۇ ئۇسۇل ئارقىلىق JWT لارنى قولغا كەلتۈرىۋالغان بولسا كېرەك.

T1539 Web Session Cookie لارنى ئوغرىلاش

يۇقىردا بايان قىلىنغاندەك ئارتىست JWT لارنى قولغا كەلتۈرىۋالغان بولۇپ، بۇلار Web Session Cookie غا ئوخشاپ كېتىدۇ. ئارتىست بۇلارنى قايتا ئىشلىتىش ئارقىلىق تېخىمۇ چوڭ زىيارەت ئىمتىيازى يارىتالايدۇ.

بايقاش

T1046 تور مۇلازىمىتىنى بايقاش

دەللل-ئىسپاتلار شۇنى كۆرسىتىدۇكى، تورنى سكەنىرلەيدىغان nmap پروگراممىسى بۇزغۇنچىلىققا ئۇچرىغان ئۇسكۇنىدە قوللىنىلغان. بۇنىڭ بىلەن خۇددى شۇ تور بەت بۆلىكىدىكى باشقا ئەپلەرنى سكەنىرلەشمۇ ئىشقا ئاشقان. قارىغاندا ئارتىست مۇشۇلاردىن پايدىلىنىپ زىيارەت قىلىشقا بولىدىغان ۋە توغرىسىغا يۆتكىلىش ئىمكانىيەتلىرى بىلەن تەمىن ئېتىدىغان باشقا تورلارغا قول سوزغاندەك قىلىدۇ.

توپلاش

هازىرقى مەۋجۇت دەللل-ئىسپاتلار ئارتىستلارنىڭ ئۇچۇرلارنى قانداق توپلىغانلىقىنى كۆرسىتىپ بېرەلمەيدۇ، شۇنىڭدەك بۇزغۇنچىلىققا ئۇچرىغان ئۇسكۇنىلەردىن ياكى باشقا سىستېمىلاردىن زادى نېمىلەرنىڭ توپلانغانلىقىنىمۇ دەپ بېرەلمەيدۇ. ئەمما، ئارتىستلار بۇزغۇنچىلىققا ئۇچرىغان ئۇسكۇنىدىكى بارلىق هۆججەتلەرگە، جۇملىدىن قولغا چۈشۈرۈلگەن كىملىك ئىجازىتى (T1003)، كۆپ ئامىللىق جەزىملەش قىممىتى (T1111) ۋە يۇقىرىدا بايان قىلىنغان JWT لارنىڭ هەممىسىنى زىيارەت قىلغاندەك قىلىدۇ.

بۇيرۇق ۋە كونترولluق

T1071.001 قوللىنىشچان قاتلام كېلىشىمى: تور كېلىشىمى

ئارتىستلار تور قاپلىرىنى بۇيرۇق ۋە كونترولluققا ئىشلەتكەن.

تور قاپلىرىنىڭ بۇيرۇقلىرى ئادەتتە HTTPS نى بويلاپ ئۇسكۇنىدىكى مەۋجۇت تور مۇلازىمىتېرى ئارقىلىق يوللانغان. (T1572).

T1001.003 مەلۇماتلارنى خىرەلەشتۇرۇش: كېلىشىم تەقلىدچىلىكى

ئارتىستلار بۇزغۇنچىلىققا ئۇچرىغان ئۇسكۇنىلەرنى هۇجۇمنىڭ باشلىنىش نۇقتىسى قىلىدۇ هەمدە بۇ هۇجۇملارنى قانۇنلۇق ئېقىم مىقدارى بىلەن ئارىلاشتۇرىۋېتىدۇ.

بايقاش ۋە ئېھتىيات تەۋسىيەلىرى

ASD قارمىقىدىكى ACSC ئادەتتە ASD نىڭ تۆۋىكى سەككىز خىل كونتروللۇق تەدبىرى ۋە مۇناسىۋەتلىك تور بىخەتەرلىكى ھادىسلىرىگە قارىتىلغان تەھدىسىە ئىستراتېگىيەسىنى ئىجرا قىلىشنى كۆچلۈك تەۋسىيە قىلىدۇ. تۆۋەندىكىلەر APT40 تەرىپىدىن تور مۇداخىلىسىنى ئېنىقلاش ۋە ئۇنىڭ ئالدىنى ئېلىش ئۈچۈن ئەمەلگە ئاشۇرۇلۇشى كېرەك بولغان تور بىخەتەرلىكى چارىلىرى ھەققىدىكى تەۋسىيەلەردۇر. ئاندىن قالسا 1-جەدۋەلدە خۇلاسىلەنگەن تۆت ئاساسىي تەۋسىيە ھېسابلىنىدۇ.

بايقاش

يۇقىرىدا ئېنىقلانغان بەزى ھۆججەتلەر C:\Users\Public* and C:\Windows\Temp* قاتارلىق جايلارغا چوشۇرۈلگەن. بۇ جايلار ئۇچۇرلارنى يېزىشقا قولاي جايلار بولۇشى مۇمكىن. چۈنكى ئادەتتە دۇنيادا يېزىلىشى مۇمكىن بولغان، يەنى «كۆزنەك» (Windows) تە تىزىمغا ئېلىنغان بارلىق قوللانغۇچىلار ھېسابقا ئالىدىغان مۇشۇ مۇندەرىجىنى ھەمدە ئۇنىڭ ئاستىدىكى ئىككىلەمچى مۇندەرىجىلەرنى زىيارەت قىلالايدۇ. كۆپىنچە، ھەرقانداق پايدىلانغۇچى ئۇلارنىڭ بۇ ھۆججەتلەرگە كىرەلەيدىغان بولۇپ، بۇ ھال توغرىسىغا يۆتكىلىش، مۇداپىئەدىن داجىش، تۆۋەن ئىمتىيازدىكى ئىجرائات ۋە سۈزۈۋېلىنغان ئۇچۇرلارنى ساقلىۋېلىشقا سەھنە يارىتىدۇ.

تۆۋەندىكى Sigma قائىدىلىرى گۇمانلىق جايلاردىن كەلگەن بۇيرۇقلارنى بىنورمال قىلمىشلارنىڭ بەلگىسى سۈپىتىدە ئىزلەيدۇ. بارچە ئەھۋالدا ئۇلارنىڭ بىر تەكشۈرۈش ئارقىلىق زىيانلىق قىلمىشلار ۋە ئۇنىڭ سەۋەبلىرىنى جەزملەشتۈرۈش زۆرۈر بولىدۇ.

ماۋزۇ: دۇنياۋى يېزىشقا مۇمكىن بولىدىغان بۇيرۇقلار-ۋاقىتلىق

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

تەسۋىرى: تىن ئىجرا بولىدىغان بۇيرۇقلارنىڭ جەريانىنى ئېنىقلاش C:\Windows\Temp.

ئارقا كۆرۈنۈشى:

بۇ قائىدە مەخسۇس C:\Windows\Temp* تىن ئىجرا بولىدىغان بۇيرۇقلارنى ئىزدەيدۇ. ۋاقىتلىق (Temp) بولسا كۆپىنچە ئىجابىي خاراكتېردىكى پروگراممىلار ئۈچۈن ئىشلىتىلىدۇ. شۇڭا C:\Windows تىكى دۇنياۋى يېزىشقا مۇمكىن بولىدىغان باشقا ئىككىلەمچى بۇيرۇقلارغا سېلىشتۇرغاندا Temp ئىشەنچلىك دەرىجىسى تۆۋەنرەك بولغان يامان نىيەتلىك كۆرسەتكۈچلەر ھېسابلىنىدۇ.

«سىستېما» (SYSTEM) ياكى «تور مۇلازىمىتى» (NETWORK SERVICE) قوللانغۇچىلىرى ئىجرا قىلغان پروگراممىلارنى ئۇچۇرۇۋېتىش بولسا مەزكۇر قائىدە تاللىغان ئىجابىي خاراكتېردىكى پائالىيەتلەرنىڭ سانىنى كۆرۈنەرلىك دەرىجىدە ئازايتىۋېتىدۇ.

بۇ ھال بۇ قائىدىنىڭ يۇقىرىراق دەرىجىدىكى ئىمتىياز دائىرىسىدە زىيانلىق بۇيرۇقلارنى قاچۇرۇپ قويۇشى مۇمكىنلىكىدىن دېرەك بېرىدۇ. ئەمما بۇ ھال باشقا قائىدىلەرنى ئىشلىتىش ئارقىلىق قوللانغۇچىنىڭ ئىمتىيازىنى SYSTEM دەرىجىسىگە يۈكسەلدۈرۈشكە ئۇرۇنغان ياكى ئۇرۇنمىغانلىقى ھەققىدە قارار قىلىشنى تەۋسىيە قىلىدۇ.

تەكشۈرۈش:

1. مەزكۇر ھۆججەتنىڭ ئىجرا قىلىنىشى بىلەن بىۋاستە مۇناسىۋەتلىك بولغان ئۇچۇلارنى تەكشۈرۈپ بېقىڭ. مەسىلەن، قوللانغۇچى مەزمۇنى، ئىجرا قىلىشنىڭ مۇكەممەللىك دەرىجىسى، ئۇلاپلا ئەگىشىش پائالىيىتى ۋە ھۆججەت يۈكلەپ چىققان رەسىملەر.
2. قىلمىشنىڭ زىيانلىق ياكى ئەمەسلىكىنى باھالاشقا ياردەمى بولۇشى ئۈچۈن ماشىنىدىكى مەزمۇن جەريانى، تور، ھۆججەت ۋە بۇنى قوللايدىغان باشقا سانلىق مەلۇماتلارنى تەكشۈرۈپ بېقىڭ.
3. زۆرۈر بولسا ئەكسىي ئىنژېنېرلىق شەكلىدە ئۇنىڭ قانۇنلۇق ياكى ئەمەسلىكىنى ئېنىقلاش ئۈچۈن ھۆججەتنىڭ كۆپەيتىلگەن نۇسخىسىنى يېغىشقا ھەرىكەت قىلىڭ.

پايدىلانمىلار:

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

ئاپتور: ASD قارمىقىدىكى ACSC

ۋاقتى: 2024/06/19

ھالىتى: تەجرىبە خاراكتېرلىك

خەتكۈچ:

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

خاتىرە مەنبەسى:

كاتېگورىيە: process_creation

مەھسۇلات: كۆزنەك

بايقاش:

```
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)
```

ساختا ئىجابىيلىقلار:

- ئىجازەت بېرىلگەن تىزىملىكنى تەكشۈرۈش پروگراممىلىرىنىڭ Temp دىن كېلىۋاتقان بۇيرۇقلارنى ئىجرا قىلىدىغانلىقى بايقالدى.
- Temp قانۇنىي رەۋىشتە بىر يۇرۇش تەڭشەك پروگراممىلار ۋە باشلىغۇچى پروگراممىلارنى ئۆز ئىچىگە ئالىدۇ. شۇڭا مەزكۇر قائىدىنى باشلاشتىن ئاۋۋال بۇ خىل ھەرىكەتلەر نازارەت قىلىنىدىغان توردا قانچىلىك دائىرىگە تارقالغانلىقى (ۋە رۇخسەت بېرىلگەن تىزىملىككە كىرگۈزۈلۈشى مۇمكىن ياكى ئەمەسلىكىنى) نى ئويلىنىپ كۆرۈش بەكمۇ مۇھىم.

دەرىجىسى: تۆۋەن

ماۋزۇ: دۇنياۋى يېزىشقا بولىدىغان بۇيرۇقلار - Non-Temp System Subdirectory

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

تەسۋىرى: بۇيرۇقنىڭ ئىجرا بولۇش جەريانىنى «كۆزنەك» (Windows) مەشغۇلات سىستېمىسى ئورنىتىلغان ئىككىلەمچى مۇندەرىجىدىكى دۇنياۋى يېزىلىدىغان جايدىن ئېنىقلاش.

ئارقا كۆرۈنۈشى:

بۇ قائىدە مەخسۇس *\C: \ and particularly C: \Windows دىكى دۇنياۋى يېزىلىدىغان مۇندەرىجىدىن بۇيرۇقنىڭ ئىجرا بولۇشىنى ئىزدەيدۇ. ئەمما C: \Windows\Temp بولسا بۇنىڭدىن مۇستەسنا (بۇنى ئىجابىي پروگراممىلار كۆپرەك قوللىنىدىغانلىقى ئۈچۈن بۇنىڭ زىياندا‌شلىق كۆرسەتكۈچ دەرىجىسىمۇ تۆۋەنرەك بولىدۇ).

ئەگەر ھۆججەت SYSTEM سۈپىتىدە ئىشقا سېلىنسا AppData خالتىلىرى بۇنىڭدىن مۇستەسنا بولىدۇ. بۇ بولسا كۆپلىگەن ۋاقتىلىق پروگرامما ھۆججەتلىرىنى ئىجرا قىلىدىغان قولاي ئۇسۇل.

تورنىڭ ھۇل لىنىيەسىنى دەسلەپكى قەدەمدە تاماملىغاندىن ھەمدە ئاشۇ جايلاردىن كېلىۋاتقان ئىجابىي بۇيرۇقلارنى ئايدىڭلاشتۇرغاندىن كېيىن بۇ قائىدە كەمدىن-كەم تەدبىقلىنىدۇ.

تەكشۈرۈش:

1. مەزكۇر ھۆججەتنىڭ ئىجرا قىلىنىشى بىلەن بىۋاستە مۇناسىۋەتلىك بولغان ئۇچۇرلارنى تەكشۈرۈپ بېقىڭ. مەسىلەن، قوللانغۇچى مەزمۇنى، ئىجرا قىلىشنىڭ مۇكەممەللىك دەرىجىسى، ئۇلاپلا ئەگىشىش پائالىيىتى ۋە ھۆججەت يۈكلەپ چىققان رەسىملەر.
2. قىلمىشنىڭ زىيانلىق ياكى ئەمەسلىكىنى باھالاشقا ياردىمى بولۇشى ئۈچۈن ماشىنىدىكى مەزمۇن جەريانى، تور، ھۆججەت ۋە بۇنى قوللايدىغان باشقا سانلىق مەلۇماتلارنى تەكشۈرۈپ بېقىڭ.
3. زۆرۈر بولسا ئەكسىي ئىنژېنېرلىق شەكلىدە ئۇنىڭ قانۇنلۇق ياكى ئەمەسلىكىنى ئېنىقلاش ئۈچۈن ھۆججەتنىڭ كۆپەيتىلگەن نۇسخىسىنى يېغىشقا ھەرىكەت قىلىڭ.

پايدىلانمىلار:

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

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

ئاپتور: ASD قارمىقىدىكى ACSC

ۋاقتى: 2024/06/19

ھالىتى: تەجرىبە خاراكتېرلىك

خەتكۈچ:

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

خاتىرە مەنبەسى:

كاتېگورىيە: process_creation

مەھسۇلات: كۆزنەك

بايقاش:

```
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

ساختا ئىجابىيلىقلار:

ئىجازەت بېرىلگەن تىزىملىكنى تەكشۈرۈش پروگراممىلىرىنىڭ مۇشۇ مۇئندەرىجىدىن كېلىۋاتقان بۇيرۇقلارنى ئىجرا قىلىدىغانلىقى بايقالدى.

نازارەت قىلىنىدىغان مۇھىت (لار) دا پايدىلىنىلىدىغان يېزىقلار ۋە مەمۇرىي ۋاستىلارنىڭ مۇشۇ مۇئندەرىجىلەرنىڭ بىرىگە جايلاشقان بولۇشى مۇمكىن بولۇپ، ئۇلارنىڭ ھالىتىگە بىر-بىرلەپ قاراپ چىقىش توغرا كېلىدۇ.

دەرىجىسى: يۇقىرى

ماۋزۇ: دۇنياۋى يېزىلىدىغان بۇيرۇقلار-قوللانغۇچىلار

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

تەسۋىرى: بۇيرۇقنىڭ ئىجرا بولۇش جەريانىنى C:\Users\Public* ۋە «قوللانغۇچىلار»دىكى باشقا دۇنياۋى يېزىشقا بولىدىغان خالتىلاردىن ئېنىقلاڭ.

ئارقا كۆرۈنۈشى:

ئەگەر ھۆججەت SYSTEM سۈپىتىدە ئىشقا سېلىنسا AppData خالتىلىرى بۇنىڭدىن مۇستەسنا بولىدۇ. بۇ بولسا كۆپلىگەن ۋاقىتلىق پروگراممىلا ھۆججەتلىرىنى ئىجرا قىلىدىغان قولاي ئۇسۇل.

تەكشۈرۈش:

1. مەزكۇر ھۆججەتنىڭ ئىجرا قىلىنىشى بىلەن بىۋاستە مۇناسىۋەتلىك بولغان ئۇچۇرلارنى تەكشۈرۈپ بېقىڭ. مەسىلەن، قوللانغۇچى مەزمۇنى، ئىجرا قىلىشنىڭ مۇكەممەللىك دەرىجىسى، ئۇلاپلا ئەگىشىش پائالىيىتى ۋە ھۆججەت يۈكلەپ چىققان رەسىملەر.
2. قىلمىشنىڭ زىيانلىق ياكى ئەمەسلىكىنى باھالاشقا ياردەمى بولۇشى ئۈچۈن ماشىنىدىكى مەزمۇن جەريانى، تور، ھۆججەت ۋە بۇنى قوللايدىغان باشقا سانلىق مەلۇماتلارنى تەكشۈرۈپ بېقىڭ.
3. زۆرۈر بولسا ئەكسىي ئىنژېنېرلىق شەكلىدە ئۇنىڭ قانۇنلۇق ياكى ئەمەسلىكىنى ئېنىقلاش ئۈچۈن ھۆججەتنىڭ كۆپەيتىلگەن نۇسخىسىنى يېغىشقا ھەرىكەت قىلىڭ.

پايدىلانمىلار:

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

ئاپتور: ASD قارمىقىدىكى ACSC

ۋاقتى: 2024/06/19

ھالىتى: تەجرىبە خاراكتېرلىك

خەتكۈچ:

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

خاتىرە مەنبەسى:

كاتېگورىيە: process_creation

مەھسۇلات: كۆزنەك

بايقاش:

```
users:
  Image|contains:
  - ': \\Users\\All Users\\'
  - ': \\Users\\Contacts\\'
  - ': \\Users\\Default\\'
  - ': \\Users\\Public\\'
  - ': \\Users\\Searches\\'
appdata:
  Image|contains: '\\AppData\\'
  User: 'SYSTEM'
```

شەرت: قوللانغۇچى ۋە appdata ئەمەس

ساختا ئىجابىيلىقلار:

- نازارەت قىلىندىغان مۇھىت (لار)دا پايدىلىنىلىدىغان يېزىقلار ۋە مەمۇرىي ۋاستىلارنىڭ ئاممىۋى ياكى قوشۇمچە مۇنەدەرىجىگە جايلاشقان بولۇشى مۇمكىن بولۇپ، ئۇلارنىڭ ھالىتىگە بىر-بىرلەپ قاراپ چىقىش توغرا كېلىدۇ.

دەرىجىسى: ئوتتۇراھال

ئازايتىش

خاتىرىلەر

ASD قارمىقىدىكى ACSC نىڭ تەكشۈرۈشلىرى داۋامىدا تەكشۈرۈش تىرىشچانلىقىنىڭ ئۇنۇمى ۋە سۈرئىتىنى تۆۋەنلىتىدىغانلىقىنى ئۇرتاق مەسىلە كۆپلىگەن ساھەلەر، جۈملىدىن تور مۇلازىمىتېرى خاتىرىسى، Windows ئىنتېرنېت ۋەقەلىرى خاتىرىسى ۋە ئىنتېرنېت ژاكالەتچىلىك خاتىرىسىنى ئۆز ئىچىگە ئالغان تولۇق ۋە تارىخىي خاتىرىلەرنىڭ كەملىكى بولغان.

ASD قارمىقىدىكى ACSC ئۆزلىرىنىڭ تۆۋەندىكى ساھەلەرگە قارىتا مەسلىھەتلىرىنى كۆرۈپ چىقىشنى ۋە تەدبىقلاشنى تەۋسىيە قىلىدۇ. Windows ۋەقەلىرى خاتىرىسى ۋە ئۇلارنى يوللاپ مېڭىش، جۈملىدىن بۇ Windows ۋەقەلىرى خاتىرە ئامبىرى ۋە ئۇچۇر بىخەتەرلىكى قوللانمىسىدىكى سىستېما نازارىتى مەسلىھەتچىلىكى، خاتىرىلەرنى مەركەزلەشتۈرۈش ۋە مۇئەييەن مۇددەتكە خاتىرىلەرنى ساقلاپ قېلىش قاتارلىقلارنى ئۆز ئىچىگە ئالىدۇ.

ياماقلارنى باشقۇرۇش

ئىنتېرنېتقا تەسىر قىلىدىغان بارلىق ئوسكۇنىلەر ۋە مۇلازىمەتلەرنى، شۇ جۈملىدىن تور مۇلازىمىتېرى، تور پروگراممىلىرى ۋە يېراقتىن كىرىش دەرۋازىسىنى تېزدىن تۈزىتىشكە تىرىشىڭ. جەريانىنى ئاپتوماتلاشتۇرۇش ۋە تېزلەشتۈرۈش ئۈچۈن مەركەزلەشتۈرۈلگەن ياماقلارنى باشقۇرۇش سىستېمىسىنى ئىجرا قىلىشنى ئويلىشىپ كۆرۈڭ. ASD قارمىقىدىكى ACSC نادەتتە ISM نىڭ «سىستېما باشقۇرۇش كۆرسەتكۈچى»نى، بولۇپمۇ زۆرۈر بولغاندا سىستېما ياماشنى كونترول قىلىشنى تەۋسىيە قىلىدۇ.

ئارتىست قوللانغان بۈزغۇنچىلىق ۋاستىلىرىنىڭ كۆپ قىسمى ئاممىغا مەلۇملۇق بولۇپ، ئۇلاردا ياماقلار يېڭى زىيانىنى تۆۋەنلىتىش تەدبىرلىرى مەۋجۇت ئىدى.

ئورگانلار 48 سائەت ئىچىدە ئىنتېرنېتقا يۈزلەنگەن ھۇل مۇئەسسەلەرگە قارىتا بىخەتەرلىك ياماقلىرى يېڭى زىيانىنى تۆۋەنلىتىش تەدبىرلىرى قوللىنىشقا كاپالەتلىك قىلىشى، شۇنىڭدەك ئىلاجى بولسا يۇمتال ۋە مەشغۇلات سىستېمىسىنىڭ ئەڭ يېڭى نۇسخىسىنى ئىشلىتىشى لازىم.

تورنى بۆلەكلەرگە ئاجرىتىش

تورنى بۆلەكلەرگە ئاجرىتىۋەتكەندە رەقىبلەر ئۇچۇن توردىكى سەزگۈر مەلۇماتلارنى تېپىش ۋە ئۇلارنى قولغا چۈشۈرۈۋېلىش زور دەرىجىدە قىيىنلىشىدۇ. تەلەپ قىلىنمىغان ئەھۋالدا تورنى بۆلەكلەرگە ئاجرىتىۋېتىش كومپيۇتېرلار ئارىسىدىكى توغرىسىغا يۆتكىلىشنى چەكلەپ قويىدۇ ياكى توسۇپ قويىدۇ. Active Directory ۋە باشقا كىملىكنى جەزملەشتۈرۈش مۇلازىمىتېرلىرىغا ئوخشاش مۇھىم مۇلازىمىتېرلار پەقەت چەكلەنگەن مىقداردىكى ۋاستىچى مۇلازىمىتېرلار ياكى «ئۆتكۈنچى مۇلازىمىتېرلار» تەرىپىدىن باشقۇرۇلۇشى مۇمكىن. بۇ مۇلازىمىتېرلار دىققەت بىلەن كۆزىتىلىشى، ياخشى مۇداپىئەلەنگەن بولۇشى، شۇنىڭدەك قايسى قوللانغۇچى ۋە ئوسكۇنىنىڭ ئۇلارغا ئۇلىنىشىنى چەكلىشى لازىم.

توغرىسىغا يۆتكىلىشنىڭ ئالدىنى ئېلىش ھالەتلىرىدىن قەتئىنەزەر تورنى بۆلەكلەرگە ئاجرىتىۋېتىش ئۆز نۆۋىتىدە يەنە ئارتىستلارنىڭ كىرىشى ۋە ئېلىشى مۇمكىن بولغان ئۇچۇر مىقدارىنى زور دەرىجىدە چەكلەپ قويىدۇ.

قوشۇمچە زىيانىنى ئازايتىش چارىلىرى

- ئاپتور ئورگانلار تۆۋەندىكىچە زىيانىنى ئازايتىش چارىلىرى ئارقىلىق APT40 ۋە باشقىلارنىڭ TTP لارنى ئىشلىتىشىگە قارشى تۇرۇشنى تەۋسىيە قىلىدۇ.
- ئىشلىتىلمەيدىغان ياكى كېرەكسىز تور مۇلازىمىتىنى، پورتلارنى ۋە كېلىشىملەرنى ئۆچۈرىۋېتىڭ.
- تور مۇلازىمىتېرلىرى ۋە پروگراممىلىرىنى قوغداش ئۈچۈن ياخشى ئاسرالغان تور پروگراممىسى مۇداپىئە تاملىرى (WAF لار) دىن پايدىلىنىڭ.
- مۇلازىمىتېرلارغا، ھۆججەت ھەمبەھىرلەشكە ۋە باشقا مەنبەلەرگە كىرىشكە بېرىلگەن ئىمتىيازنى ئەڭ تۆۋەن دەرىجىگە چۈشۈرۈپ قويۇڭ.
- ھېسباۋات مەلۇماتلىرىنى ئوغرىلاش ۋە ئۇنى قايتا قوللىنىشنى قىيىنلاشتۇرۇش ئۈچۈن كۆپ ئاممىللىق جەزملەشتۈرۈش (MFA) ۋە باشقۇرۇلىدىغان مۇلازىمەت ھېسابلىرىدىن پايدىلىنىڭ.
- كۆپ ئاممىللىق جەزملەشتۈرۈش ئىنتېرنېتقا كىرىش مۇمكىن بولغان بارلىق يېراقتىن كىرىش مۇلازىمىتىگە قوللىنىلىشى كېرەك. جۈملىدىن:
  - تور ۋە بۇلۇت ئاساسىدىكى ئېلخەتلەر
  - ھەمكارلىق سۇپىلىرى
  - مەۋھۇم خۇسۇسىي تور ئۇلىنىشلىرى
  - يېراق مۇسايىلىك ئۈستەل مۇلازىمىتى
- پايدىلىنىش مۇددىتى تۈگىگەن ئوسكۇنىنى ئالماشتۇرۇۋېتىڭ.

1-جەدۋەل. زىياننى ئازايتىش ئىستراتېگىيەلىرى\تېخنىكىلار

TTP	زىياننى ئازايتىشنىڭ ئاساسلىق سەككىز ئىستراتېگىيەسى	ISM كونترولىلۇقى
دەسلەپكى زىيارەت T1190 ئاممىغا يۈزلەنگەن پروگراممىلاردىن پايدىلىنىش	ياماق پروگراممىلىرى ياماق مەشغۇلات سىستېمىسى كۆپ ئامىللىق جەزملەشتۈرۈش پروگرامما كونترولىلۇقى	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
ئىجرائىيات T1059 بۇيرۇق ۋە يېزىق تەرجىمانى	پروگرامما كونترولىلۇقى Microsoft Office macros نى چەكلەش مەمۇرىي ئىمتىيازلارنى چەكلەش	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
قەتئىيلىك T1505.003 مۇلازىمېتىر يۇمتال زاپچاسلىرى: تور قېپى	پروگرامما كونترولىلۇقى مەمۇرىي ئىمتىيازلارنى چەكلەش	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
دەسلەپكى زىيارەت / ئىمتىيازنى ئاشۇرۇش / قەتئىيلىك T1078 ئىناۋەتلىك ھېسابئاتلار	ياماق مەشغۇلات سىستېمىسى كۆپ ئامىللىق جەزملەشتۈرۈش مەمۇرىي ئىمتىيازلارنى چەكلەش پروگرامما كونترولىلۇقى قوللانغۇچىلار پروگراممىسىنى كۆچەيتىش	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

ناۋادا ئومۇمىي تەرىقىدىكى ئېنىقلاش ۋە زىياننى ئازايتىش ھەققىدە تېخىمۇ كۆپ مەسلىھەتكە ئېھتىياجلىق بولسىڭىز مەزكۇر كۆرسەتمىنىڭ ئاخىرىدىكى MITRE ATT&CK خۇلاسىسىدە بەلگىلەنگەن ھەر بىر تېخنىكا ئۈچۈن MITRE ATT&CK تېخنىكا تور بېتى ھەققىدىكى بۆلەكنىڭ «زىياننى ئازايتىش ۋە بايقاش» دېگەن قىسمىغا قاراڭ.

بايانات

مەزكۇر دوكلاتتىكى ئۇچۇرلار «ئەسلى قانداق بولسا شۇنداق» دېگەن شەكىلدە پەقەت مەلۇمات بېرىشنىلا مەقسەت قىلىدۇ. ئاپتور ئورگانلار ھېچقانداق سودا تەشكىلاتى، مەھسۇلاتلار، شىركەت ياكى مۇلازىمەت، جۈملىدىن مەزكۇر ھۆججەت بىلەن ئالاقىدار بولغان ھەرقانداق تەشكىلات، مەھسۇلات ياكى مۇلازىمەتنى ئېتىراپ قىلمايدۇ. مۇلازىمەت ماركىسى، سودا ماركىسى، ئىشلەپچىقارغۇچى ياكى باشقا يوللار ئارقىلىق بۇ مەزمۇنلارنى مەلۇم سودا ئورگانلىرىغا، مەھسۇلاتلارغا، جەريانغا ياكى مۇلازىمەتكە نەقىل تەرقىسىدە سۆنۈش ئاپتور ئورگانلارنىڭ نەزىردە ھېچقاچان يوللۇق ھېسابلانمايدۇ، شۇنىڭدەك ئېتىراپمۇ قىلىنمايدۇ ياكى ئۇلارنى مەمنۇن قىلمايدۇ.

مەزكۇر ھۆججەتكە TLP: CLEAR دەپ بەلگە قويۇلغان. بۇنى ئاشكارا قىلىش چەكلىمىگە ئۇچرىمايدۇ. مەنبەلەرنىڭ TLP: CLEAR دىكى مەلۇماتلاردىن خاتا پايدىلىنىش خەۋپى ئەڭ تۆۋەن دەرىجىدە بولسا ياكى ئومۇمەن بۇنداق خەۋپ مەۋجۇت بولمىسا تەدبىقلاشقا بولىدىغان قائىدىلەرگە ۋە ئاممىغا ئاشكارىلاش تەرتىپىگە مۇۋاپىق كېلىدىغان شەكىلدە پايدىلانسا بولىدۇ. ئۆلچەملىك نەشر ھوقۇقى قائىدىلىرىگە رىئايە قىلغان ئاساستا TLP: CLEAR دىكى مەلۇماتلارنى ھېچقانداق چەكلىمسىز تارقىتىشقا بولىدۇ. ئېقىم چىراقلىرى كېلىشىمى ھەققىدە تېخىمۇ تەپسىلى مەلۇمات ئالماقچى بولسىڭىز cisa.gov/tlp غا قاراڭ.

MITRE ATT&CK - تارىخىي APT40 دىكى كىشىنى قىزىقتۇرىدىغان ھۇنەرلەر

رازۋېدكا (TA0043)	
زىيانكەشلىككە ئۇچرىغۇچىغا مەنسۇپ تور بەتلەرنى ئىزلەش (T1594)	زىيانكەشلىككە ئۇچرىغۇچىنىڭ شەخسىي مەلۇماتلىرىنى يىغىش: ھېساپ مەلۇماتلىرى (T1589.001)
ئاكتىپ سكەنىرلەش: ئاجىزلىقنى سكەنىرلەش (T1595.002)	زىيانكەشلىككە ئۇچرىغۇچى ماشىنا ھەققىدە مەلۇمات توپلاش (T1592)
ئوچۇق تور بەتلەر\تور بوشلۇقلىرىنى ئىزدەش: ئىزدەش ماتورى (T1593.002)	زىيانكەشلىككە ئۇچرىغۇچ تور ئۇچۇرلىرىنى توپلاش: تور بوشلۇقىنىڭ خۇسۇسىيەتلىرى (T1590.001)
زىيانكەشلىككە ئۇچرىغۇچىنىڭ شەخسىي مەلۇماتلىرىنى يىغىش: ئېلخەت ئادرېسى (T1589.002)	

مەنبە تەرەققىياتى (TA0042)	
ھۇل مۇئەسسەسىنى سېتىۋېلىش: تور بوشلۇقلىرى (T1583.001)	ھۇل مۇئەسسەسىنى سېتىۋېلىش (T1583)
ھۇل مۇئەسسەسىنى سېتىۋېلىش: DNS مۇلازىمېتىرى (T1583.002)	ھېساۋاتلارنى ئوغرىلاش (T1586)
ئىقتىدار يېتىلدۈرۈش: كود ئىمزالاش گۇۋاھنامىلىرى (T1587.002)	ھۇل مۇئەسسەسىنى ئوغرىلاش (T1584)
ئىقتىدار يېتىلدۈرۈش: رەقەملىك گۇۋاھنامىلار (T1587.003)	ئىقتىدار يېتىلدۈرۈش: زىيانداش يۇمتال (T1587.001)
ئىقتىدارنى قولغا كەلتۈرۈش: كود ئىمزالاش گۇۋاھنامىلىرى (T1588.003)	ھېساۋات تۈرغۈزۈش: بۇلۇت ھېساۋاتى (T1585.003)
ھۇل مۇئەسسەسىنى ئوغرىلاش: تور ئۆسكۈنىلىرى (T1584.008)	ئىقتىدارنى قولغا كەلتۈرۈش: رەقەملىك گۇۋاھنامىلار (T1588.004)

دەسلەپكى زىيارەت (TA0001)	
ئىناۋەتلىك ھېساۋاتلار (T1078)	قارماق سېلىش (T1566)
ئىناۋەتلىك ھېساۋاتلار: ئۆلچەملىك ھېساۋاتلار (T1078.001)	قارماق سېلىش: نىشانلانغان قوشۇمچە ھۆججەت (T1566.001)
ئىناۋەتلىك ھېساۋاتلار: تور بوشلۇقى ھېساۋاتلىرى (T1078.002)	قارماق سېلىش: نىشانلانغان ئۇلانما (T1566.002)
تاشقى يىراق مۇسابىلىك مۇلازىمەت (T1133)	ئاممىغا يۈزلەنگەن پروگراممىلارنى تىمسىقلاش (T1190)
ھەربىكەتلەنمە شەكىللىك بۆرۈنچىلىق (T1189)	

ئىجرائىيات (TA0002)	
Windows باشقۇرۇش قوراللىرى (T1047)	بۇيرۇق ۋە يېزىق تەرجىمانى: Python (T1059.006)
پلانلانغان ۋەزىپە\ئىش: At (T1053.002)	بۇيرۇق ۋە يېزىق تەرجىمانى: JavaScript (T1059.007)
پلانلانغان ۋەزىپە\ئىش: پلانلانغان ۋەزىپە (T1053.005)	يەرلىك API (T1106)
بۇيرۇق ۋە يېزىق تەرجىمانى (T1059)	جەريانلار ئارا ئالاقە (T1559)
بۇيرۇق ۋە يېزىق تەرجىمانى: Windows بۇيرۇق قېپى (T1059.003)	سىستېما مۇلازىمەتلىرى: مۇلازىمەتنى بېجىرىش (T1569.002)
بۇيرۇق ۋە يېزىق تەرجىمانى: PowerShell (T1059.001)	خېرىدار ئىجراسى ئۈچۈن يوچۇقتىن پايدىلىنىش (T1203)
بۇيرۇق ۋە يېزىق تەرجىمانى: Visual Basic (T1059.005)	قوللانغۇچىنىڭ ئىجرا قىلىشى: زەھەرلىك ھۆججەت (T1204.002)
بۇيرۇق ۋە يېزىق تەرجىمانى: Unix Shell (T1059.004)	بۇيرۇق ۋە يېزىق تەرجىمانى: ئالما يېزىقى (T1059.002)
پلانلانغان ۋەزىپە\ئىش: Cron (T1053.003)	يۇمتاللارنى ئورنىتىش ۋاستىلىرى (T1072)

قەتئىيلىك (TA0003)	
ئىناۋەتلىك ھېساۋاتلار (T1078)	مۇلازىمېتىر يۇمتال زاپچاسلىرى: تور قېپى (T1505.003)
ئىشخانا پروگراممىلىرىنى قوزغىتىش: Office Template Macros (T1137.001)	سىستېما جەريانىنى يارىتىش ياكى ئۆزگەرتىش: Windows مۇلازىمىتى (T1543.003)
پلانلانغان ۋەزىپە\ئىش: At (T1053.002)	قوزغىتىش ياكى تىزىمغا كىرىشنى ئاپتوماتىك ئىجرا قىلىش: تىزىملىتىشنى ئىشقا كىرىشتۇرۇش ئاچقۇچلىرى\قوزغىتىش خالتىسى (T1547.001)
پلانلانغان ۋەزىپە\ئىش: پلانلانغان ۋەزىپە (T1053.005)	قوزغىتىش ياكى تىزىمغا كىرىشنى ئاپتوماتىك ئىجرا قىلىش: تېزلەتمىنى ئۆزگەرتىش (T1547.009)
تاشقى يىراق مۇسابىلىك مۇلازىمەت (T1133)	ئوغرىلاشنىڭ ئىجرا ئېقىمى: DLL ئوغرىلىق بۇيرۇتمىسىنى ئىزدەش (T1574.001)
پلانلانغان ۋەزىپە\ئىش: Cron (T1053.003)	ئوغرىلاشنىڭ ئىجرا ئېقىمى: DLL يانداش يۈكلەش (T1574.002)
ھېساۋات باشقۇرۇش (T1098)	ئىناۋەتلىك ھېساۋاتلار: بۇلۇت ھېساۋاتى (T1078.004)
ئىناۋەتلىك ھېساۋاتلار: تور بوشلۇقى ھېساۋاتلىرى (T1078.002)	

ئىمتىيازنى ئاشۇرۇش (TA0004)	
پلانلانغان ۋەزىپە\ئىش: At (T1053.002)	سىستېما جەريانىنى يارىتىش ياكى ئۆزگەرتىش: Windows مۇلازىمىتى (T1543.003)
پلانلانغان ۋەزىپە\ئىش: پلانلانغان ۋەزىپە (T1053.005)	قوزغىتىش ياكى تىزىمغا كىرىشنى ئاپتوماتىك ئىجرا قىلىش: تىزىملىتىشنى ئىشقا كىرىشتۇرۇش ئاچقۇچلىرى\قوزغىتىش خالتىسى (T1547.001)
كىرگۈزۈش جەريانى: لىنىيە ئىجراسىنىڭ ئوغرىلىنىشى (T1055.003)	قوزغىتىش ياكى تىزىمغا كىرىشنى ئاپتوماتىك ئىجرا قىلىش: تېزلەتمىنى ئۆزگەرتىش (T1547.009)
كىرگۈزۈش جەريانى: جەريانىنى ئېچىش (T1055.012)	ئوغرىلاشنىڭ ئىجرا ئېقىمى: DLL ئوغرىلىق بۇيرۇتمىسىنى ئىزدەش (T1574.001)

ئىمتىيازنى ئاشۇرۇش (TA0004)

ئىناۋەتلىك ھېسابات: تور بوشلۇقى ھېساۋاتلىرى (T1078.002)	ئىمتىيازنى ئاشۇرۇش ئۆچۈن پايدىلىنىش (T1068)
كىرىش تەمتىكىنى باشقۇرۇش: تەمتەك تەقلىدچىلىكى\ئوغرىلىقى (T1134.001)	ھادىسە قوزغاتقان ئىجرائات: Unix Shell سەپلىمىسىنى ئۆزگەرتىش (T1546.004)
كىرگۈزۈش جەريانى: دىنامىكلىق باغلانغان ئامبارغا كىرگۈزۈش (T1055.001)	ئىناۋەتلىك ھېسابات: تور بوشلۇقى ھېساۋاتلىرى (T1078.002)
ئىناۋەتلىك ھېسابات: يەرلىك ھېساۋاتلار (T1078.003)	

مۇداپىئەدىن داجىش (TA0005)

Rootkit (T1014)	ۋاستىلىك بۇيرۇقنى ئىجرا قىلىش (T1202)
خىرەلەشتۈرۈلگەن ھۆججەتلەر ياكى مەلۇماتلار (T1027)	سىستېمىدىكى ئىكلىك ۋاكالەتچى ئىجراسى: Mshta (T1218.005)
خىرەلەشتۈرۈلگەن ھۆججەتلەر ياكى مەلۇماتلار: يۇمتال ئورالمىسى (T1027.002)	سىستېمىدىكى ئىكلىك ۋاكالەتچى ئىجراسى: Regsvr32 (T1218.010)
خىرەلەشتۈرۈلگەن ھۆججەتلەر ياكى مەلۇماتلار: Steganography (T1027.003)	ئىشەنچ كونتروللۇقىنى بۇزۇش: كود ئىمزالاش (T1553.002)
خىرەلەشتۈرۈلگەن ھۆججەتلەر ياكى مەلۇماتلار: يەتكۈزۈلگەندىن كېيىن تۈزۈپ چىقىش (T1027.004)	ھۆججەت ۋە مۇندەرىجە ئىجازەتنامىلىرىنى ئۆزگەرتىش: Linux ۋە Mac تېكى ھۆججەت ۋە مۇندەرىجە ئىجازەتنامىلىرىنى ئۆزگەرتىش (T1222.002)
نىقابلىنىش: قانۇنلۇق ئىسىم ۋە ئورۇنلارنى پار كەلتۈرۈش (T1036.005)	مەۋھۇملاشتۇرۇش\قۇم ساندۇقتىن داجىش: سىستېما تەكشۈرۈشلىرى (T1497.001)
كىرگۈزۈش جەريانى: لىنىيە ئىجراسىنىڭ ئوغرىلىنىشى (T1055.003)	نىقابلىنىش (T1036)
ئەكسى كودلارنى قاچىلاش (T1620)	مۇداپىئەنى بۇزۇش: تور بىخەتەرلىك تېمىنى ئۆچۈرۈش ياكى ئۆزگەرتىۋېتىش (T1562.004)
كىرگۈزۈش جەريانى: جەريانىنى ئېچىش (T1055.012)	بۈيۇملارنى يوشۇرۇش: يوشۇرۇن ھۆججەتلەر ۋە مۇندەرىجىلەر (T1564.001)
كۆرسەتكۈچنى ئىلىۋېتىش: ھۆججەتنى ئۆچۈرۈش (T1070.004)	بۈيۇملارنى يوشۇرۇش: يوشۇرۇن كۆزنەك (T1564.003)
كۆرسەتكۈچنى ئىلىۋېتىش: Timestomp (T1070.006)	ئوغرىلاشنىڭ ئىجرا ئېقىمى: DLL ئوغرىلىق بۈيرۇقىمىسىنى ئىزدەش (T1574.001)
كۆرسەتكۈچنى ئىلىۋېتىش: Windows ۋەقەلەر خاتىرىسىنى تازىلاش (T1070.001)	ئوغرىلاشنىڭ ئىجرا ئېقىمى: DLL يانداش يۈكلەش (T1574.002)
تىزىملىتىشنى ئۆزگەرتىش (T1112)	تور مۇلازىمىتى (T1102)
ھۆججەت ياكى ئۇچۇرلاردىكى خىرەلىكنى يوقىتىش\كودنى يېشىش (T1140)	نىقابلىنىش: ۋەزىپە ياكى مۇلازىمەتنى نىقابلاش (T1036.004)
مۇداپىئەنى بۇزۇش (T1562)	

قانۇنلۇق زىيارەت (TA0006)

OS مەخپىي نومۇر ئوغرىلىقى: LSASS خاتىرىسى (T1003.001)	ئىشەنچسىز ھېسابات مەلۇماتلىرى: ھۆججەتلەردىكى ھېسابات مەلۇماتلىرى (T1552.001)
OS مەخپىي نومۇر ئوغرىلىقى: NTDS (T1003.003)	زورلۇق كۆچى: مەخپىي نومۇرنى تەخمىن قىلىش (T1110.001)
تورنى ھىدلاش (T1040)	مەجبۇرىي دەللەلەش (T1187)

قانۇنلۇق زىيارەت (TA0006)	
مەخپىي نومۇر دۆكانلىرىددىكى ھېسابات مەلۇماتلىرى: ئاچقۇچ زەنجىرى (T1555.001)	Kerberos تالۇنلىرىنى ئوغرىلاش ياكى ساختىلاشتۇرۇش: Kerberoasting (T1558.003)
كىرگۈزۈشتىن قولغا چۈشۈرۈش: كۇنۇپكا تاختىسى خاتىرىسى (T1056.001)	كۆپ ئامىللىق جەزملەشتۈرۈشنى توسۇش (T1111)
Steal Web Session Cookie لارنى ئوغرىلاش (T1539)	پروگراممىغا كىرىش تەمتكىنى ئوغرىلاش (T1528)
ھېسابات مەلۇماتلىرى ئوغرىلاش (T1212)	زورلۇق كۈچى: مەخپىي نومۇرنى بۇزۇش (T1110.002)
كىرگۈزۈشتىن قولغا چۈشۈرۈش: Web Portal نى سۈرەتكە ئېلىش (T1056.003)	OS مەخپىي نومۇر ئوغرىلىقى: DCSync (T1003.006)
مەخپىي نومۇر دۆكانلىرىددىكى ھېسابات مەلۇماتلىرى: تور كەزگۈچتىكى ھېسابات مەلۇماتلىرى (T1555.003)	مەخپىي نومۇر دۆكىنىددىكى ھېسابات مەلۇماتلىرى (T1555)

بايقاش (TA0007)	
سىستېما مۇلازىمىتىنى بايقاش (T1007)	سىستېما ئۇچۇرلىرىنى بايقاش (T1082)
پروگراممىا كۆزنىكىنى بايقاش (T1010)	ھېساۋاتنى ئېنىقلاش: يەرلىك ھېساۋات (T1087.001)
تىزىملىكنى تەكشۈرۈش (T1012)	سىستېما ئۇچۇرى ۋە تېخنىكىلارنى بايقاش T1082 – كارخانا | MITRE ATT&CK®
ھۆججەت ۋە مۇندەرىجىنى ئېنىقلاش (T1083)	سىستېما ۋاقتىنى ئېنىقلاش (T1124)
تور مۇلازىمىتىنى ئېنىقلاش (T1046)	سىستېما ئىگىسى\ قوللانغۇچىنى ئېنىقلاش (T1033)
يىراق مۇسابىلىك سىستېمىنى ئېنىقلاش (T1018)	تور بوشلۇقى ئىشەنچىنى ئېنىقلاش (T1482)
ھېساۋاتنى ئېنىقلاش: ئېلخەت ھېساۋاتى (T1087.003)	ھېساۋاتنى ئېنىقلاش: تور بوشلۇقى ھېساۋاتى (T1087.002)
سىستېما تور ئۇلىنىشىنى ئېنىقلاش (T1049)	مەۋھۇملاشتۇرۇش\قۇم ساندۇقتىن داجىش: سىستېما تەكشۈرۈشلىرى (T1497.001)
جەريانىنى ئېنىقلاش (T1057)	يۆمتالنى ئېنىقلاش (T1518)
رۇخسەت گۇرۇپپىسىنىڭ بايقىغانلىرى: تور بوشلۇقى گۇرۇپپىلىرى (T1069.002)	سىستېما ھەمبەھرلىكى ۋە تېخنىكىلارنى بايقاش T1135 – كارخانا | MITRE ATT&CK®
سىستېما تورىنى ماسلاشتۇرۇشتا بايقالغانلار: ئىنتېرنېت ئۇلىنىشىنى ئېنىقلاش (T1016.001)	

توغرىسىغا يۆتكىلىش (TA0008)	
يىراق مۇسابىلىك مۇلازىمەتلەر: يىراق مۇسابىلىك ئۈستەل يۈزى كېلىشىمى (T1021.001)	يىراق مۇسابىلىك مۇلازىمەتلەر (T1021)
يىراق مۇسابىلىك مۇلازىمەتلەر: SMB/Windows باشقۇرغۇچىلىرىنىڭ ھەمبەھرلىكى (T1021.002)	ۋاكالىتەن دەللەلەش ماتېرىياللىرىنى ئىشلىتىش : بېلەت تاپشۇرۇش (T1550.003)
يىراق مۇسابىلىك مۇلازىمەتلەر: Windows نى يىراق مۇسابىلىك باشقۇرۇش (T1021.006)	توغرىسىغا قورال يۆتكەش (T1570)

توپلام (TA0009)	
يەرلىك سىستېمىدىن ئېلىنغان ئۇچۇرلار (T1005)	يىغىلغان مەلۇماتلارنى ئارخىپلاشتۇرۇش: كۈتۈپخانا ئارقىلىق ئارخىپلاشتۇرۇش (T1560.002)
ئورتاق سىستېمىدىن ئېلىنغان مەلۇماتلار (T1039)	ئېلخەت توپلىمى: يىراق مۇسابىدىن ئېلخەت توپلاش (T1114.002)

توپلام (TA0009)

كىرگۈزۈشتىن قولغا چۈشۈرۈش: كۇنۇپكا تاختىسى خاتىرسى (T1056.001)	كېسىپ چاپلاش تاختىسىدىكى ئۇچۇرلار (T1115)
ئاپتوماتىك توپلاش (T1119)	ئۇچۇر ئامبارلىرىدىكى مەلۇماتلار (T1213)
كىرگۈزۈشتىن قولغا چۈشۈرۈش: Web Portal نى سۈرەتكە ئېلىش (T1056.003)	ئۇچۇرلارنى ۋاقىتلىق ساقلاش: يىراق مۇساپىدىن ئۇچۇرلارنى ۋاقىتلىق ساقلاش (T1074.002)
ئۇچۇرلارنى ۋاقىتلىق ساقلاش: يەرلىك ئۇچۇرلارنى ۋاقىتلىق ساقلاش (T1074.001)	يىغىلغان مەلۇماتلارنى ئارخىپلاشتۇرۇش (T1560)
ئېلخەت توپلىمى (T1114)	

سۈزۈۋېلىش (TA0010)

C2 قانىلى ئارقىلىق سۈزۈۋېلىش (T1041)	ۋاكالەتچى كېلىشىم ئارقىلىق سۈزۈۋېلىش : سىممېترىك شىفىرلاشمىغان C2 كېلىشىمى ئارقىلىق سۈزۈۋېلىش كېلىشىمى (T1048.002)
ۋاكالەتچى كېلىشىم ئارقىلىق سۈزۈۋېلىش (T1048)	تور مۇلازىمىتى ئارقىلىق سۈزۈۋېلىش: بۇلۇت ئامبىرىغا يوللاش (T1567.002)

بۇيرۇق ۋە كونترولluق (TA0011)

مەلۇماتلارنى خىرەلەشتۈرۈش: كېلىشىم تەقلىدچىلىكى (T1001.003)	تور مۇلازىمىتى: ئۆلۈك نۇقتا قىلتىقى (T1102.001)
ئورتاق ئىشلىتىلىدىغان ئېغىز (T1043)	تور مۇلازىمىتى: تاق يۆنىلۈشلۈك ئالاقە (T1102.003)
قوللىنىشچان قاتلام كېلىشىمى: تور كېلىشىملىرى (T1071.001)	كىرىش قورالىلىرىنى يۆتكەش (T1105)
قوللىنىشچان قاتلام كېلىشىمى: ھۆججەت يۆتكەش كېلىشىملىرى (T1071.002)	ۋاكالەتچى: ئىچكى ۋاكالەتچى (T1090.001)
ۋاكالەتچى: تاشقى ۋاكالەتچى (T1090.002)	ئۆلچەمسىز ئېغىز (T1571)
ۋاكالەتچى: كۆپ-نۇقتىلىق ۋاكالەتچى (T1090.003)	كېلىشىم تونىلى (T1572)
تور مۇلازىمىتى: قوش يۆنىلۈشلۈك ئالاقە (T1102.002)	شىفىرلانغان قانال (T1573)
شىفىرلانغان قانال: سىممېترىك بولمىغان شىفىرلىق رەسىم (T1573.002)	كىرىش قورالىلىرىنى يۆتكەش (T1105)
ۋاكالەتچى، تېخنىكا T1090 – كارخانا | MITRE ATT&CK®	

تەسىرى (TA0040)

مۇلازىمەتنىڭ توختىشى (T1489)	دىسكا سۈرتۈش (T1561)
سىستېمىنى ئۆچۈرۈش\قايتا قوزغىتىش (T1529)	مەنبەلەر ئوغرىلىقى (T1496)

ئىزاھلار

بايانات

مەزكۇر قوللانمىدىكى ماتېرىياللار ئومۇمىي خاراكتېرگە ئىگە بولۇپ، ھەرقانداق ۋەزىيەتتە ياكى جىددىي ئەھۋاللاردا قانۇنىي مەسلىھەت سۈپىتىدە قارالماسلىقى ياكى ياردەم رولىنى ئوينىماسلىقى لازىم. ھەر قانداق مۇھىم مەسىلە كۆرۈلسە ئۆز شارائىتىڭىز بويىچە تېگىشلىك بولغان مۇستەقىل كەسىپ ئىگىلىرىدىن مەسلىھەت سورىشىڭىز لازىم.

ئاۋسترالىيە ھەمدوستلۇقى مەزكۇر قوللانمىدا بايان قىلىنغان مەلۇماتلارغا تايىنىش نەتىجىسىدە كۆرۈلگەن ھەرقانداق زىيان، يوقتىش ياكى خراجەتلەر ئۈچۈن جاۋابكارلىقنى ياكى مەسئۇلىيەتنى ئۈستىگە ئالمايدۇ.

نەشر ھەققى

ھەربىي گېربنى ئىشلىتىش ھەققىدە

ھەربىي گېربدىن پايدىلىنىش شەرتلىرى باش مىنىستر مەھكىمىسى ۋە كابىنېت تور بېتىدە تەپسىلى بايان قىلىنغان. «ھەمدوستلۇق ھەربىي گېربى ھەققىدىكى ئۇچۇرلار ۋە كۆرسەتمىلەر» | pmc.gov.au.

قوشۇمچە مەلۇماتلار ياكى تور بېكەتەرلىكى ھادىسىسى ھەققىدە خەۋەر بەرمەكچى بولسىڭىز بىز بىلەن ئالاقىلىشىڭ:

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

بۇ نۇمۇر پەقەت ئاۋسترالىيەدىلا ئىشلىتىلىدۇ.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre