APT40 ஆலோசனை

சீனாவின் தேசிய பாதுகாப்புத் துறை செயல்படுத்தும் உளவுத் தொழில்நுட்பம்

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**

பொருளடக்கம்

கண்ணோட்டம்

பின்னணி

இந்த ஆலோசனை, ஆஸ்திரேலிய சமிக்ஞைகள் இயக்குநரகத்தின் (ASD) ஒரு பகுதியான ஆஸ்திரேலிய சைபர் பாதுகாப்பு மையம் (ACSC), அமெரிக்காவின் சைபர் பாதுகாப்பு மற்றும் கட்டமைப்பு பாதுகாப்புத் துறை (CISA), அமெரிக்க தேசிய பாதுகாப்பு நிறுவனம் (NSA), அமெரிக்காவின் குற்றப் புலனாய்வுத்துறை (FBI), UKயின் தேசிய சைபர் பாதுகாப்பு மையம் (NCSC UK), சைபர் பாதுகாப்பிற்கான கனேடிய மையம் (CCCS), நியூசிலாந்து தேசிய சைபர் பாதுகாப்பு மையம் (NCSC-NZ), ஜெர்மன் ஃபெடரல் புலனாய்வு சேவை (BND) மற்றும் அரசியலமைப்பின் பாதுகாப்பிற்கான கூட்டாட்சி அலுவலகம் (BfV), கொரிய குடியரசின் தேசிய புலனாய்வு சேவை (NIS) மற்றும் NIS இன் தேசிய சைபர் பாதுகாப்பு மையம், மற்றும் ஜப்பானின் சைபர் பாதுகாப்பிற்கான சம்பவ தயார் நிலை மற்றும் மூலோபாய மையம் (NISC) மற்றும் தேசிய காவல்துறை நிறுவனம் (NPA) - இனிமேல் 'அதிகார முகமைகள்' என்று குறிப்பிடப்படுகிறது - சீன மக்கள் குடியரசின் (PRC) அரச நிதியுதவியுடன் இயங்கும் இணையக் குழு ஆஸ்திரேலியாவின் இணைய மற்றும் பிணையங்களுக்கு ஏற்படுத்தும் தற்போதைய அச்சுறுத்தலைக் கோடிட்டுக் காட்டுகிறது. அச்சுறுத்தல் குறித்து அதிகார முகமைகள் பகிர்ந்து கொண்ட புரிதல், மற்றும் சம்பவங்களுக்கு ASDயின் ACSC நடத்திய விசாரணைகளின் அடிப்படையில் இந்த ஆலோசனை எழுதப்பட்டுள்ளது.

சீன அரச நிதியுதவி பெறும் சைபர் குழு முன்னர் ஆஸ்திரேலியா மற்றும் அமெரிக்கா உட்பட பல்வேறு நாடுகளில் உள்ள நிறுவனங்களைக் குறி வைத்துள்ளது. மேலும், கீழே விவரிக்கப்பட்டுள்ள நுட்பங்கள் உலகளவில் PRC அரசு நிதியுதவி பெறும் மற்றவர்களால் தொடர்ந்தும் பயன்படுத்தப்படுகின்றன. எனவே, இந்த குழு மற்றும் இதே போன்ற நுட்பங்கள் தங்கள் நாடுகளின் நெட்வொர்க்குகளுக்கும் அச்சுறுத்தலாக இருப்பதாக அதிகார முகமைகள் நம்புகின்றன.

இந்தக் குழு, சீனாவின் தேசிய பாதுகாப்புத் துறைக்காக தீங்கிழைக்கும் இணைய நடவடிக்கைகளை நடத்துகிறது என்று இந்த அறிக்கையை எழுதியுள்ள அதிகார முகமைகள் மதிப்பிடுகின்றன. செயல்பாடு மற்றும் நுட்பங்கள், மேம்பட்ட நிலைத்தன்மை அச்சுறுத்தல் - Advanced Persistent Threat (APT) 40 என்று (தொழில்துறை அறிக்கையிடலில் Kryptonite Panda, GINGHAM TYPHOON, Leviathan மற்றும் Bronze Mohawk என்றும்) அழைக்கப்படும் கண்காணிக்கப்பட்ட குழுவுடன் ஒன்றுடன் ஒன்று பொருந்துகின்றன. இந்த குழு முன்னதாக சீனாவின் ஹைனான் மாகாணத்தில் உள்ள ஹைகூவை தளமாகக் கொண்டதாகவும், ஹைனான் மாகாண பாதுகாப்புத் துறை சீனாவின் தேசிய பாதுகாப்புத் துறையிடமிருந்து கட்டளைகள் பெற்றதாகவும் தெரிவிக்கப்பட்டது.[2] இரண்டு பாதிக்கப்பட்ட நெட்வொர்க்குகளுக்கு எதிரான செயல்பாட்டில் இந்த எதிரியின் நுட்பங்களின் குறிப்பிடத்தக்க உத்திகளை விரிவான ஆய்வுகள் மூலம் இந்த அறிக்கை எடுத்துக் காட்டுகிறது. சைபர் பாதுகாப்பு பயிற்சியாளர்கள் தங்கள் சொந்த நெட்வொர்க்குகளுக்கு எதிரான APT40 ஊடுருவல்களை அடையாளம் காணவும், தடுக்கவும் மற்றும் சரி செய்யவும் விரிவான ஆய்வுகள் பயன்படலாம். தேர்ந்தெடுக்கப்பட்ட விரிவான ஆய்வுகள் இந்த அச்சுறுத்தலை முன்னெடுப்பவர்கள் அல்லது மற்றவர்களால் மீண்டும் சுரண்டப்படும் அபாயத்தைக் குறைக்கும் பொருத்தமான தீர்வு மேற்கொள்ளப்பட்டவை. எனவே, விரிவான ஆய்வுகள் இயற்கையாகவே பழமையானவை, நிறுவனங்களுக்கு தீர்வு காண தேவையான நேரம் வழங்கப்படுவதை உறுதி செய்தது.

செயல்பாடுகளின் சுருக்கம்

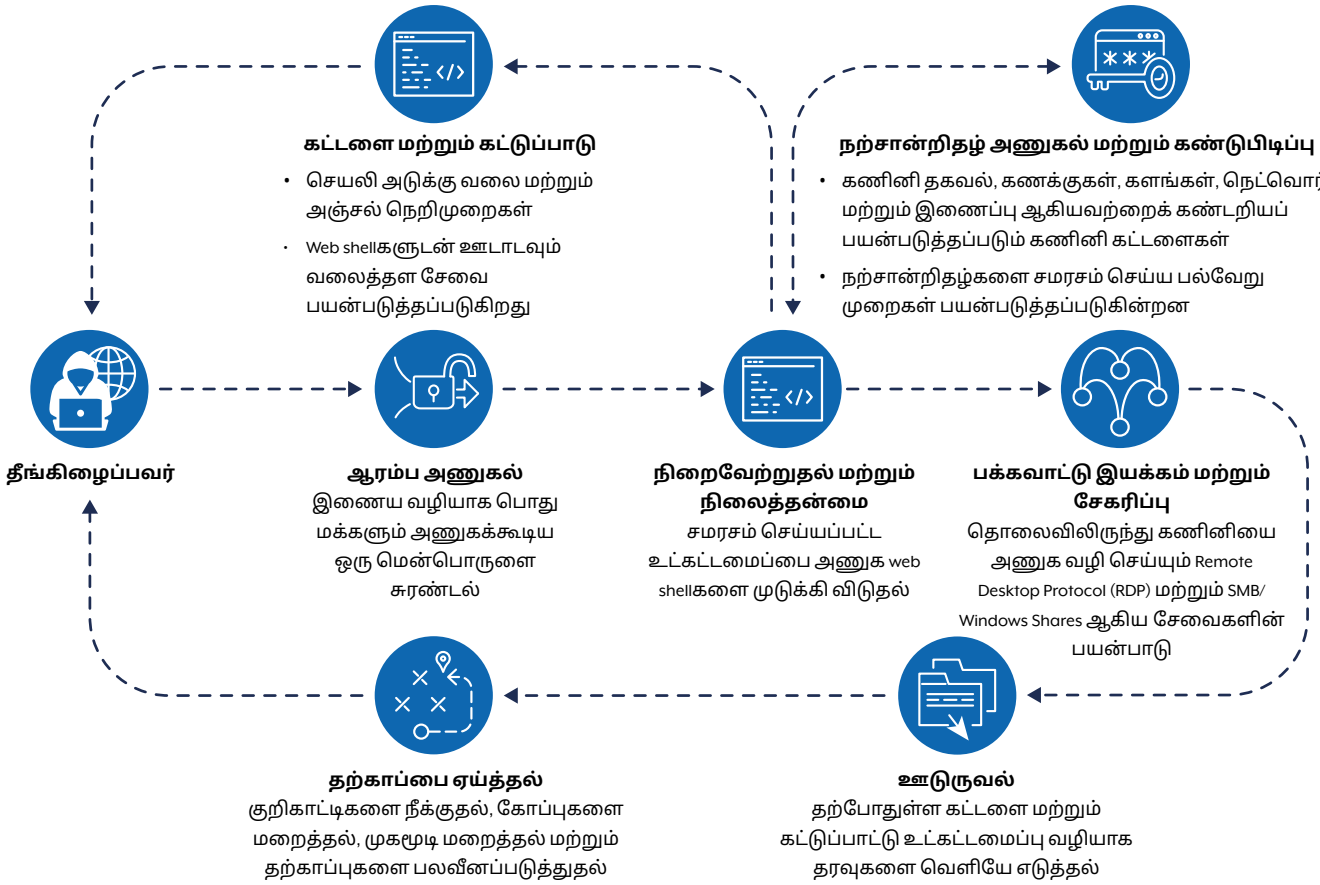
APT40 பலமுறை ஆஸ்திரேலிய நெட்வொர்க்குகள் மற்றும் பிராந்தியத்தில் உள்ள அரசு மற்றும் தனியார் துறை நெட்வொர்க்குகளை குறி வைத்துள்ளது, மேலும் அவை எங்கள் நெட்வொர்க்குகளுக்கு இப்பொழுதும் அச்சுறுத்தலாக உள்ளன. இந்த ஆலோசனையில் விவரிக்கப்பட்டுள்ள உளவு நடவடிக்கை, ஆஸ்திரேலிய நெட்வொர்க்குகளுக்கு எதிராக தொடர்ந்து நடப்பது அவதானிக்கப்படுகிறது.

குறிப்பாக, APT40 ஆனது புதிய பாதிப்புகளின் கருத்தாக்கத்தை (proof-of-concept அல்லது POCஐ) விரைவாக மாற்றியமைக்கும் திறனைக் கொண்டுள்ளது மற்றும் தொடர்புடைய பாதிப்பின் உட்கட்டமைப்பைக் கொண்ட நெட்வொர்க்குகளுக்கு எதிராக உடனடியாக இலக்கு வைத்துப் பயன்படுத்துகிறது. APT40 அதன் இலக்குகளை சமரசம் செய்வதற்கான வாய்ப்புகளைத் தொடர்ந்து தேடுகிறது. அதிகார முகமைகளின் நாடுகளிலுள்ள நெட்வொர்க்குகள் உட்பட பல நெட்வொர்க்குகளுக்கு எதிராகத் தொடர்ந்து உளவு பார்க்கிறது. அப்படி உளவு பார்க்கும் நெட்வொர்க்குகளில் பாதிக்கப்படக்கூடிய, அல்லது இனி பராமரிக்கப்படாத சாதனங்களை அடையாளம் காணவும், சுரண்டல்களை விரைவு படுத்தவும் என்று ஒரு தனி குழுவை நிலை நிறுத்தியுள்ளது. 2017 ஆம் ஆண்டின் முற்பகுதியிலிருந்து, APT40 பாதிப்படையக் கூடிய சாதனங்களைத் தாக்குவதில் தொடர்ந்து வெற்றியைக் காண்கிறது.

Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) மற்றும் Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473) போன்ற பரவலாகப் பயன்படுத்தப்படும் மென்பொருட்களில் புதிதாகக் காணப்பட்ட பொது பாதிப்புகளை APT40 விரைவாகப் பயன்படுத்துகிறது. பொது பாதிப்புகள் புதிதாகக் காணப்பட்ட சில மணி நேரத்திற்குள் அல்லது நாட்களுக்குள், அவற்றைப் பயன்படுத்தி APT40 தாக்குதல்களை நடத்த, குறித்த குழு POCகளை தொடர்ந்து பயன்படுத்தும் என ASD இன் ACSC மற்றும் ஆவணப்படுத்தும் நிறுவனங்கள் எதிர்பார்க்கின்றன.

2 அமெரிக்க நீதித்துறை. 2021. தொற்று நோய் ஆராய்ச்சி உட்பட அறிவு சார் சொத்து மற்றும் ரகசிய வணிகத் தகவல்களை இலக்காகக் கொண்ட உலகளாவிய கணினி ஊடுருவல் பிரச்சாரத்தில் மாநில பாதுகாப்பு அமைச்சகத்துடன் பணிபுரியும் நான்கு சீன நாட்டினர் குற்றம் சாட்டப்பட்டனர்.

படம் 1. APT40 செயற்பாட்டின் தந்திரோபாயங்கள், நுட்பங்கள் மற்றும் நடைமுறைகள்(TTP)



Phishing என்ற மின்-தூண்டிலிடல் போன்ற பயனர் தொடர்பு தேவைப்படும் நுட்பங்களை விட பாதிக்கப்படக்கூடிய, இணைய வழியாக பொது மக்களும் அணுகக்கூடிய உட்கட்டமைப்பை சுரண்டுவதை இந்தக் குழு விரும்புகிறது, மேலும் பலவிதமான பின்தொடர்தல் நடவடிக்கைகளை செயல்படுத்த செல்லுபடியாகும் நற்சான்றிதழ்களைப் பெறுவதற்கு அதிக முன்னுரிமை அளிக்கிறது. Web shellகளை (T1505.003) பயன்படுத்தி, நிலைத்தன்மையுடன் APT40 ஊடுருவ முயற்சிக்கிறது. குறிப்பாக, ஊடுருவலின் வாழ்க்கைச் சுழற்சியின் ஆரம்பத்தில் இதனைப் பயன்படுத்துகிறது. பொதுவாக, வெற்றிகரமான ஆரம்ப அணுகலைத் தொடர்ந்து, பாதிக்கப்பட்டவரின் சூழலில் அணுகலைப் பராமரிக்க நிலைத்தன்மையை நிறுவுவதில் APT40 கவனம் செலுத்துகிறது. இருப்பினும், சமரசம் செய்யப்பட்ட அல்லது எடுக்கப்பட்ட மேலதிக நடவடிக்கைகளின் அளவைப் பொருட்படுத்தாமல் ஒரு ஊடுருவலின் ஆரம்பத்தில் நிலைத்தன்மை ஏற்படுவதால், அனைத்து ஊடுருவல்களிலும் இதைக் கவனிக்க வாய்ப்புள்ளது.

குறிப்பிடத்தக்க ஊடுருவல்

சமரசம் செய்யப்பட்ட ஆஸ்திரேலிய வலைத் தளங்களை அதன் செயல்பாடுகளுக்கு கட்டளை மற்றும் கட்டுப்பாடு (C2) ஹோஸ்ட்களாக APT40 முன்னர் பயன்படுத்தியிருந்தாலும், (T1594) நுட்பத்தை இந்தக் குழு உருவாக்கியுள்ளது.

உலகளாவிய போக்கு போலவே, ஆஸ்திரேலியாவில் அதன் செயல்பாடுகளுக்கு, சிறிய அலுவலகம் (small-office) அல்லது வீட்டுடன் கூடிய அலுவலகம் (home-office) - சுருக்கமாக SOHO, சாதனங்கள் உட்பட சமரசம் செய்யப்பட்ட சாதனங்களை, செயல்பாட்டு உட்கட்டமைப்பு மற்றும் மாறு இணையத் தளத்திற்குத் தாவச் செய்யும் கடைசி இடமாகப் (T1584.008) பயன்படுத்தும் போக்கை APT40 ஏற்றுக் கொண்டுள்ளது. இந்தக் குழுவின் இயக்கங்களை சிறப்பாக வகைப் படுத்தவும் கண்காணிக்கவும் அதிகார முகமைகளுக்கு இது உதவியது.

இந்த SOHO சாதனங்களில் பல, வாழ்க்கையின் இறுதியில் உள்ளவை, மென்பொருள் புதுப்பிக்கப்படாதவை அல்லது புதுப்பிப்பு அறிவிக்கப் பட்டாலும் புதுப்பிக்கப்படாதவை. அவை இலகுவில் தாக்கப் படக்கூடிய இலக்குகளாக அமைகின்றன. சமரசம் செய்யப்பட்டவுடன், SOHO சாதனங்கள் தாக்குதல்களுக்கான தொடக்க புள்ளியை வழங்குகின்றன. முறையான தகவல் பரிமாற்றத்துடன் கலக்கவும் நெட்வொர்க் பாதுகாவலர்களுக்கு சவால் விடவும் அவை (T1001.003) தகுதியடைகின்றன.

உலகெங்கிலும் உள்ள பிற PRC அரச நிதியுதவி பெறுபவர்களால் இந்த நுட்பம் தவறாமல் பயன்படுத்தப்படுகிறது. மேலும், இதை பகிரப்பட்ட அச்சுறுத்தலாக அதிகார முகமைகள் கருதுகின்றன. கூடுதல் தகவலுக்கு, People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices மற்றும் PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure என்ற கூட்டு ஆலோசனைகளைப் பார்க்கவும்.

APT40 எப்போதாவது கொள்முதல் செய்யப்பட்ட அல்லது குத்தகைக்கு எடுக்கப்பட்ட உட்கட்டமைப்பை அதன் செயல்பாடுகளில் பயன்படுத்துகிறது; இருப்பினும் அதன் பயன்பாடு ஒப்பீட்டளவில் வீழ்ச்சியடைந்து வருவதாகத் தெரிகிறது.

கருவிப்படுத்தல்

கீழே கோடிட்டுக் காட்டப்பட்டுள்ள விசாரணைகளின் போது அடையாளம் காணப்பட்ட சில தீங்கிழைக்கும் கோப்புகளை ASD இன் ACSC பகிர்ந்து கொள்கிறது. பரந்த நெட்வொர்க் பாதுகாப்பு மற்றும் சைபர் பாதுகாப்பு சமூகங்கள் அவர்கள் பாதுகாக்க வேண்டிய அச்சுறுத்தல்களை நன்கு புரிந்துகொள்ள இந்த கோப்புகள் VirusTotal இல் பதிவேற்றப்பட்டுள்ளன.

விரிவான ஆய்வுகள்

ASDயின் ACSC இரண்டு அநாமதேய புலனாய்வு அறிக்கைகளைப் பகிர்ந்து கொள்கிறது. இவை, தீங்கிழைப்பவர்கள் தங்கள் கருவிகளையும் ஊடுருவலையும் எவ்வாறு பயன்படுத்துகிறார்கள் என்பது பற்றிய விழிப்புணர்வை வழங்குகின்றன.

MD5	கோப்புப்பெயர்	கூடுதல் தகவல்
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

விரிவான ஆய்வு 1

இந்த அறிக்கை பரவலாகப் பரப்பப்படுவதற்கு உதவும் வகையில் அநாமதேயமாக்கப்பட்டுள்ளது. பாதிக்கப்பட்ட அமைப்பு இனிமேல் 'அமைப்பு' என்று குறிப்பிடப்படுகிறது. இந்த விரிவான ஆய்வில் உள்ள தனிநபர்களின் பெயர்கள் மாற்றப்பட்டுள்ளன, அத்துடன் பாதிக்கப்பட்டவர்களின் அடையாளத்தைப் பாதுகாப்பதற்காக ASD இன் ACSC இல் சம்பவம் குறித்த அறிக்கையிலுள்ள விவரங்கள் அகற்றப்பட்டுள்ளன.

பொழிப்புரை

இந்த அறிக்கை 2022ஆம் ஆண்டு ஜூலை மாதத்திற்கும் செப்டம்பர் மாதத்திற்கும் இடைப்பட்ட காலத்தில் அமைப்பின் நெட்வொர்க்கின் வெற்றிகரமாக சமரசம் செய்யப்பட்ட சம்பவங்கள் குறித்த ASD இன் ACSC விசாரணையின் கண்டுபிடிப்புகளை விவரிக்கிறது. அவதானிக்கப்பட்ட தீங்கிழைக்கும் செயல்பாட்டைச் சுருக்கமாகக் கூறுவதற்கும், தீர்வுக்கான பரிந்துரைகளை வடிவமைப்பதற்கும் இந்த விசாரணை அறிக்கை நிறுவனத்திற்கு வழங்கப்பட்டது. இந்த சமரசம் APT40 ஆல் மேற்கொள்ளப்பட்டது என்பதை கண்டுபிடிப்புகள் சுட்டிக் காட்டுகின்றன.

அமைப்பின் ஒரு சமரசம் செய்யப்பட்ட சாதனத்திலிருந்து அவர்களது நெட்வொர்க்குடன் தீங்கிழைக்கும் குழு இணைப்பை ஏற்படுத்தியிருப்பதை ஆகஸ்ட் மாத நடுப்பகுதியில் ASDயின் ACSC கண்டறிந்து அறிவித்தது. ஆகஸ்ட் மாத பிற்பகுதியில், அமைப்பின் ஒப்புதலுடன், நிறுவனத்தின் நெட்வொர்க்கில் பாதிக்கப்பட்ட ஹோஸ்ட்களுக்கு சென்சார்களை ASDயின் ACSC பொருத்தியது. ASD இன் ACSC ஆய்வாளர்கள் முழுமையான டிஜிட்டல் தடயவியல் விசாரணையை மேற்கொள்ள இந்த சென்சார்கள் அனுமதித்தன. கிடைக்கக்கூடிய சென்சார் தரவைப் பயன்படுத்தி, ASD இன் ACSC ஆய்வாளர்கள் குழுவின் செயல்பாட்டை வெற்றிகரமாக வரைபடமாக்கினர் மற்றும் கவனிக்கப்பட்ட நிகழ்வுகளின் விரிவான கால வரிசையை உருவாக்கினர்.

ஜூலை முதல் ஆகஸ்ட் வரை, ASD இன் ACSC ஆல் கவனிக்கப்பட்ட முக்கிய தீங்கிழைப்பவர் செயல்பாடு பின் வருமாறு:

- ஹோஸ்ட் கணக்கீடு - நெட்வொர்க்கின் வரைபடத்தை, ஒரு தீங்கிழைப்பவர் சொந்தமாக உருவாக்க உதவுகிறது;
- Web shell பயன்பாடு - நெட்வொர்க்கில் ஆரம்ப காலடி வைக்கவும் மற்றும் கட்டளைகளை செயல்படுத்தும் திறனையும் தீங்கிழைப்பவருக்கு அளிக்கிறது; மற்றும்
- தீங்கிழைக்கும் நோக்கங்களுக்காக பிற கருவிப்படுத்தல் நடவடிக்கைகளை தீங்கிழைப்பவர் பயன்படுத்துதல்.

பெரிய அளவிலான முக்கியமான தரவு அணுகப்பட்டதற்கான ஆதாரங்கள் மற்றும் தீங்கிழைப்பவர்கள் நெட்வொர்க் வழியாக பக்கவாட்டில் நகர்ந்ததற்கான ஆதாரங்கள் (T1021.002) விசாரணையில் தெரிய வந்தது. பலவகை அணுகல் பாதைகள் உருவாக்கப்பட்டதும், நெட்வொர்க் ஒரே அடுக்கில் (flat structure) இருப்பதும், மற்றும் அமைப்பினால் உருவாக்கப்பட்ட, ஆனால் பாதுகாப்பற்ற மென்பொருள் பயன்படுத்தப்பட்டதும், இந்த சமரசத்தின் பெரும்பகுதியை எளிதாக்கியது. வெளியேற்றப்பட்ட தரவுகளில், மிகவும் பாதுகாப்பான சிறப்புரிமை அங்கீகார நற்சான்றிதழ்களும் (privileged authentication credentials) மற்றும் நெட்வொர்க் தகவல்களும் அடங்கி இருந்தன, இது குழுவினர் மீண்டும் அனுமதியில்லா அணுகலைப் பெற உதவும். அடிப்படையில் தாக்குதலுக்குள்ளான கணினியில் இருந்தவை தவிர வேறு எந்த கூடுதல் தீய கருவிகளும் கண்டுபிடிக்கப்படவில்லை. இருப்பினும், குழுவினரிடம் முறையான மற்றும் சலுகை பெற்ற நற்சான்றிதழ்களுக்கான அணுகல் இருந்தால், கூடுதல் கருவிகள் தேவையில்லை. இந்த விசாரணை கணிப்புகளின் அடிப்படையில், பகிரங்கமாக அறியப்பட்ட பாதிப்புக்கு சந்தர்ப்பவாதமாக பலியாவதற்கு மாறாக, இந்த நிறுவனம் திட்டமிட்டு APT40 ஆய்வுக்கு இலக்காக தீர்மானிக்கப்பட்டது என்பதைக் குறிக்கிறது,.

விசாரணை முடிவுகள்

ஒரு அரச நிதியுதவி பெற்ற சைபர் குழுவுடன் தொடர்புடையதாக நம்பப்படும் உறுதிப்படுத்தப்பட்ட தீங்கிழைக்கும் IP குறைந்தது ஜூலை மற்றும் ஆகஸ்ட் மாதங்களுக்கு இடையில் அமைப்பின் கணினி நெட்வொர்க்குகளுடன் இணைப்பை மேற்கொண்டதாக, ASD இன் ACSC 2022ஆம் ஆண்டு, ஆகஸ்ட் மாத நடுப்பகுதியில் அமைப்புக்கு அறிவித்தது. சமரசம் செய்யப்பட்ட சாதனம் ஒரு சிறு வணிக அல்லது வீட்டு பயனருக்கு சொந்தமானது.

ஒரு ஹோஸ்ட் அடிப்படையிலான முகவரை அமைப்பின் நெட்வொர்க்கில் ASD-இன் ACSC ஆகஸ்ட் மாத பிற்பகுதியில் அனுப்பியது. சமரசத்தால் பாதிக்கப்பட்டதற்கான ஆதாரங்களை அது காட்டியது.

விசாரணை முயற்சிகளை ஆதரித்திருக்கக்கூடிய சில ஆவணங்கள் (artifacts) பதிவு அமைப்பு அல்லது வலைப்பின்னல் வடிவமைப்பு காரணமாகக் கிடைக்கவில்லை. ஆனால், கிடைக்கின்ற அனைத்து தரவுகளையும் வழங்க அமைப்பு தயார் நிலையில் இருந்ததால், ASD-இன் ACSC ஆய்வாளர்கள் முழுமையான பகுப்பாய்வினை நடத்த முடிந்தது, மற்றும் APT40 செயல்பாட்டைப் பற்றிய புரிதலை உருவாக்கவும் உதவியது.

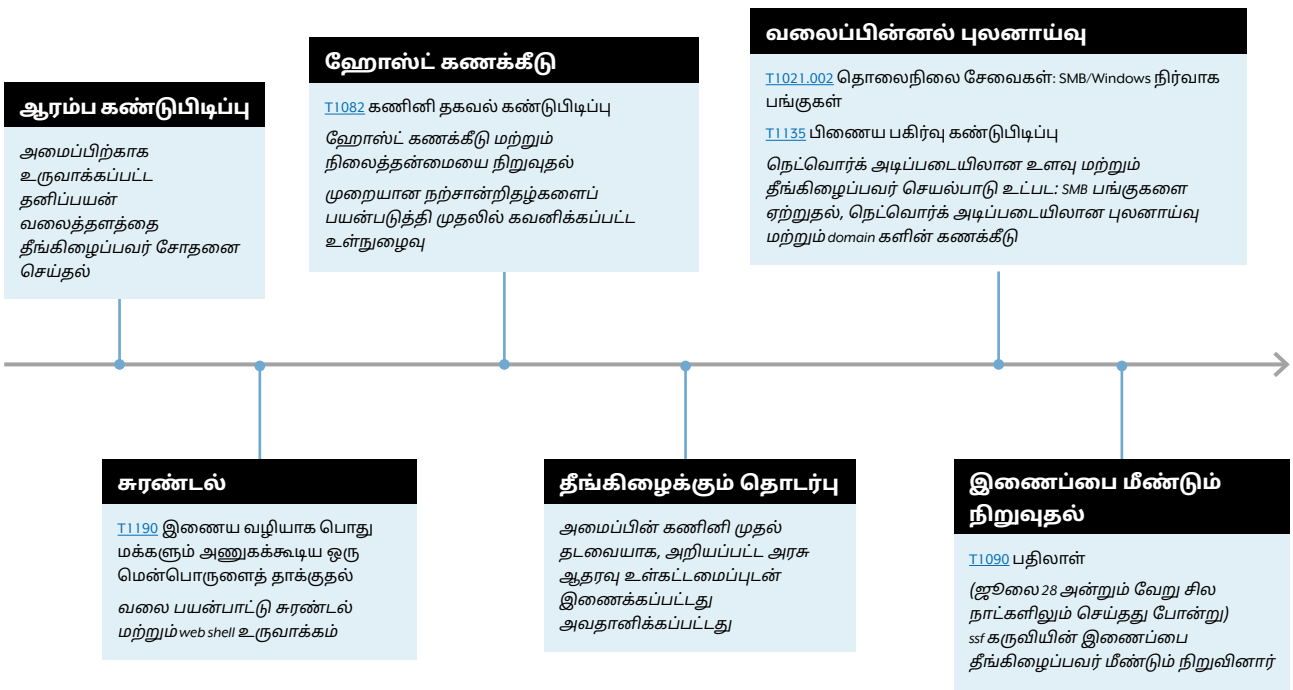
ASDயின் ACSC உடன் செப்டெம்பர் மாதத்தில் கலந்தாலோசித்த பிறகு, ஆரம்ப அறிவிப்பில் அடையாளம் காணப்பட்ட IP-யை மறுக்க அமைப்பு முடிவு செய்தது. குணப்படுத்தும் நடவடிக்கைகளை அக்டோபர் மாதத்தில் தொடங்கியது.

விவரங்கள்

ஜூலை மாதம் முதல், தீங்கிழைப்பவர்கள் `<webapp>2-ext` இல் இயங்கும் தனிப் பயன் வலை பயன்பாட்டை (T1190) சோதித்து வெற்றிகரமாகப் பயன்படுத்த முடிந்தது; இதன்மூலம் DMZ பகுதியில் அவர்களால் காலூன்ற முடிந்தது. நெட்வொர்க் மற்றும் அனைத்து வலைப்பின்னல் மற்றும் எல்லா கணினி பெயர்களையும் கணக்கிட இது பயன்படுத்தப்பட்டது. சமரசம் செய்யப்பட்ட நற்சான்றிதழ்கள் (T1078.002) செயலில் உள்ள கோப்பகத்தை (T1018) வினவவும், DMZ இல் உள்ள பல கணினிகளிலிருந்து கோப்பு பகிர்வுகளை (T1039) ஏற்றுவதன் மூலம் தரவை வெளியேற்றவும் பயன்படுத்தப்பட்டன. சேவையகத்திலிருந்து (T1558.003) செல்லுபடியாகும் உள்நுழைவு தகவல் பெற, அவர்களால் Kerberoasting தாக்குதல் மேற்கொள்ளப்பட்டது. DMZ அல்லது உள்ளமைப்பு வலைப்பின்னலில் அவர்கள் கூடுதல் அணுகல் புள்ளி பெற்றதாக காணப்படவில்லை.

காட்சி கால வரிசை

கீழ் காணும் கால வரிசை, நிறுவனத்தின் வலைப்பின்னலில் தீங்கிழைப்பவர்களின் நடவடிக்கைகளின் முக்கிய கட்டங்களின் பரந்த கண்ணோட்டத்தை வழங்குகிறது.



விரிவான கால வரிசை

ஜூலை: பரிமாற்ற பணியகப் பாதுகாப்பு (transport layer security அல்லது TLS) இணைப்பு (T1102) வழியாக அமைப்பின் (இனிமேல் 'வலை பயன்பாடு' அல்லது '*webapp*' என குறிப்பிடப்படும்) தனிப்பயன் வலை பயன்பாட்டின் (T1190) முகப்புப் பக்கத்திற்கான ஆரம்ப இணைப்பை தீங்கிழைப்பவர்கள் நிறுவினர். வேறு குறிப்பிடத்தக்க நடவடிக்கைகள் எதுவும் காணப்படவில்லை.

ஜூலை: தீங்கிழைப்பவர்கள் இறுதிப்புள்ளிகளைத் தேடும் வலை பயன்பாட்டின் வலைத் தளத்தைத் மேலும் விசாரிக்கத் தொடங்குகிறார்கள்[2].

ஜூலை: ஒரு குறிப்பிட்ட இறுதிப்புள்ளியை சுரண்டுவதற்கான முயற்சிகளில் தீங்கிழைப்பவர்கள் கவனம் செலுத்துகிறார்கள்.

ஜூலை: அநேகமாக மற்றொரு பக்கத்தில் வைக்கப்பட்டுள்ள web shell வழியாக தீங்கிழைப்பவர்கள் வலை சேவையகத்திற்கு வெற்றிகரமாக POST செய்ய முடியும். அதே தீங்கிழைப்பவர்களால் பயன்படுத்தப்படும் இரண்டாவது IPயும் அதே URL இல் இடுகையிடத் தொடங்குகிறது. தீங்கிழைப்பவர்கள் பல சாத்தியமான web shellகளை உருவாக்கி சோதித்தனர்.

சுரண்டல் எப்படி நடத்தப்படுகிறது என்பது தெரியவில்லை, ஆனால் குறிப்பிட்ட இறுதிப்புள்ளி `<webapp>2-ext` இல் கோப்புகளை உருவாக்குவதை இலக்காகக் கொண்டது என்பது தெளிவாகிறது.

இரண்டு IP முகவரி இணைப்புகளும் அவற்றின் பகிரப்பட்ட ஆர்வம் மற்றும் ஆரம்ப இணைப்புகள் சில நிமிட இடைவெளியில் நிகழ்வதன் காரணமாக ஒரே ஊடுருவலின் ஒரு பகுதியாக அவை இருந்தன என்று ASDயின் ACSC நம்புகிறது.

ஜூலை: குழு தொடர்ந்து ஹோஸ்ட் கணக்கீட்டை நடத்துகிறது, சிறப்புரிமை விரிவாக்க வாய்ப்புகளைத் தேடுகிறது மற்றும் வேறுபட்ட web shellலைப் பயன்படுத்துகிறது. தீங்கிழைப்பவர்கள் `<firstname.surname>@<organisation domain>` என்ற சமரசம் செய்யப்பட்ட நற்சான்றிதழ்களைப் பயன்படுத்தி வலை பயன்பாட்டில் உள்நுழைகின்றனர்.

தீங்கிழைப்பவர்களின் செயல்பாடு `<webapp>2-ext` இல் சிறப்புரிமை விரிவாக்கத்தை வெற்றிகரமாக அடைந்ததாகத் தெரியவில்லை. அதற்கு பதிலாக, தீங்கிழைப்பவர்கள் நெட்வொர்க் அடிப்படையிலான செயல்பாட்டிற்கு முன்னுரிமை அளித்தனர்.

ஜூலை: தீங்கிழைப்பவர் ஒரு சேவைக் கணக்கிற்கான சமரசம் செய்யப்பட்ட நற்சான்றிதழ்களை சோதிக்கிறார்[3] இது உள்ளே அணுகக்கூடிய வகையில் உருவாக்கப்பட்டிருப்பதைக் கண்டறிந்திருக்கலாம்.

ஜூலை: தீங்கிழைப்பவர்கள் திறந்த மூல தரவாகும் கருவியான Secure Socket Funnelling (SSF) ஐப் பயன்படுத்துகின்றனர், இது தீங்கிழைக்கும் உள்கட்டமைப்புடன் இணைக்கப் பயன்படுத்தப்பட்டது. இந்த இணைப்பு தீங்கிழைப்பவரின் தாக்குதல் கணினிகளிலிருந்து நிறுவனத்தின் உள் நெட்வொர்க்குகளுக்கு தரவுப் பரிமாற்ற சுரங்கப் பாதையை உருவாக்கப் பயன்படுத்தப்படுகிறது, அதன் இயந்திர பெயர்கள் சேவை கணக்கிற்கான நற்சான்றிதழ்களைப் பயன்படுத்த முயற்சிக்கும் போது நிகழ்வு பதிவுகளில் அம்பலப்படுத்தப்படுகின்றன.

ஆகஸ்ட்: தீங்கிழைப்பவர்கள் சேவைக் கணக்கு சம்பந்தப்பட்ட இணைப்புகளை நிறுவத் தவறியது உட்பட ஒரு குறிப்பிட்ட அளவிலான செயல்பாடுகளை மேற் கொள்வதைக் காணலாம்.

ஆகஸ்ட்: தீங்கிழைப்பவர்கள் குறிப்பிடத்தக்க நெட்வொர்க் மற்றும் செயல்மிகு விவரக் கணக்கெடுப்பை நிகழ்த்துகிறார்கள். DMZ இல் உள்ள Windows கணினிகளில் பங்குகளை[4] ஏற்ற வேறு சமரசம் செய்யப்பட்ட கணக்கு பின்னர் பயன்படுத்தப்படுகிறது, இது வெற்றிகரமான தரவு வெளியேற்றத்தை செயல்படுத்துகிறது.

இது DMZ இல் ஏற்றக்கூடிய இயந்திரங்களில் திருடப்பட்ட நற்சான்றிதழின் சந்தர்ப்பவாத பயன்பாடு என்று தெரிகிறது. இதேபோன்ற செயல்பாட்டுடன் தீங்கிழைப்பவர்கள் உள் நெட்வொர்க்கை குறிவைப்பதிலிருந்து தீச்சுவர்கள் (firewalls) தடுத்தன.

ஆகஸ்ட் – செப்டம்பர்: SSF கருவி தீங்கிழைக்கும் IPயுடன் இணைப்பை மீண்டும் நிறுவியது. அவர்களின் அணுகல் தடுக்கப்படும் வரை கூடுதலாக எந்த நடவடிக்கைகளையும் குழு செய்ததாகக் காணப்படவில்லை.

செப்டம்பர்: தீங்கிழைக்கும் IPயை தங்கள் தீச்சுவர்களில் பட்டியலிட மறுப்பதன் மூலம் அமைப்பு அங்கிருந்து வரும் இணைப்பைத் தடுக்கிறது.

2 இந்த சூழலில், இறுதிப்புள்ளி என்பது வலை பயன்பாட்டின் ஒரு செயல்பாடாகும்

3 சேவைக் கணக்குகள் தனிப்பட்ட பயனர்களுடன் இணைக்கப்படவில்லை, மாறாக சேவைகளுடன் இணைக்கப்பட்டுள்ளன. Microsoft corporate domainனில் பல்வேறு வகையான கணக்குகள் உள்ளன.

4 பங்குகளை ஏற்றுதல் என்பது கோப்பு முறைமை கட்டமைப்பில் உள்ள கோப்புகளை ஒரு பயனர் அல்லது பயனர் குழு அணுகக்கூடிய செயல் முறையாகும்.

தீங்கிழைப்பவர்களின் தந்திரோபாயங்கள் மற்றும் நுட்பங்கள்

MITRE ATT&CK கட்டமைப்பு என்பது சைபர் தாக்குதல்கள் மற்றும் ஊடுருவல்களை வகைப்படுத்துவதற்கும் விவரிப்பதற்கும் ஒரு வழிகாட்டுதலாக இருக்கும், நடைமுறை உலக அவதானிப்புகளை அடிப்படையாகக் கொண்ட, தீங்கிழைப்பவர்களால் பயன்படுத்தப்படும் தந்திரோபாயங்கள் மற்றும் நுட்பங்களின் ஆவணப்படுத்தப்பட்ட தொகுப்பாகும். இந்த கட்டமைப்பை, இலாப நோக்கற்ற அமெரிக்க நிறுவனமான The MITRE Corporation உருவாக்கியது, அத்துடன் இது அச்சுறுத்தல் செய்பவர்களின் நடத்தையை பொதுவான உலகளாவிய மொழியாக செயல்படுகிறது.

தீங்கிழைப்பவர்களின் செயல்பாட்டிற்கு பொருத்தமான பின்வரும் நுட்பங்கள் மற்றும் தந்திரோபாயங்களை ASD இன் ACSC மதிப்பிடுகிறது:

புலனாய்வு

T1594 – பாதிக்கப்பட்டவருக்குச் சொந்தமான இணைய தளங்களைத் தேடுதல்

நெட்வொர்க்கை அணுகுவதற்கான வாய்ப்புகளை அடையாளம் காண தனிப்பயன் வலை பயன்பாட்டின் வலைத்தளத்தை தீங்கிழைப்பவர் பட்டியலிட்டார்.

ஆரம்ப அணுகல்

T1190 – இணைய வழியாக பொது மக்களும் அணுகக்கூடிய ஒரு மென்பொருளை சுரண்டல் (குறிப்பாக, தனிப்பயன் வலை செயலியை சுரண்டுவது)

T1078.002 – செல்லுபடியாகும் கணக்குகள்: Domain கணக்குகள் (நம்பிக்கைச்சான்றுகளுடன் உள்நுழைவது தொடர்பானது)

இணையத்தில் வெளிப்படையாக பெறுவதற்கு வாய்ப்புள்ள தனிப்பயன் வலை பயன்பாடுகளைப் பயன்படுத்துவது, தீங்கிழைப்பவருக்கு ஆரம்ப அணுகல் புள்ளியாக அமைந்தது தீங்கிழைப்பவர் பின்னர் நெட்வொர்க்கிற்கான அணுகலை மேலும் அதிகரிக்க அவர்கள் சமரசம் செய்த நற்சான்றிதழ்களைப் பயன்படுத்த முடிந்தது.

நிறைவேற்றுதல்

T1059 – கட்டளை மற்றும் மென்பொருள் மொழிமாற்றி (web shell மூலம் கட்டளை செயல்படுத்துவது தொடர்பாக)

T1072 – மென்பொருள் வரிசைப்படுத்தல் கருவிகள் (IP உடன் இணைக்க திறந்த மூல கருவியான Secure Socket Funnelling (SSF) ஐப் பயன்படுத்தும் தீங்கிழைப்பவர் தொடர்பாக)

நிலைத்தன்மை

T1505.003 – சேவையக மென்பொருள் உபகரணம்: web shell (அணுகலை நிறுவ web shell மற்றும் SSF ஐப் பயன்படுத்துவது தொடர்பானது)

தகுதிச்சான்றிதழ் அணுகல்

T1552.001 – கடவுச்சொல் கடைகளிலிருந்து நற்சான்றிதழ்கள் (கட்டிட மேலாண்மை அமைப்பு (BMS) தொடர்பான கடவுச்சொல் கோப்புகள் தொடர்பாக)

T1558.003 – Kerberos அனுமதிச்சீட்டைத் திருட அல்லது மோசடி செய்ய: Kerberoasting (பிணைய நற்சான்றிதழ்களைப் பெறுவதற்கான தாக்குதல் தொடர்பாக)

பக்கவாட்டில் நகர்தல்

T1021.002 - தொலைநிலை சேவைகள்: SMB பங்குகள் (பல சாதனங்களிலிருந்து SMB பங்குகளை ஏற்றும் தீங்கிழைப்பவர் தொடர்பாக)

தொகுப்பு

T1213 – தகவல் களஞ்சியங்களிலிருந்து தரவு (BMS சேவையகத்தில் காணப்படும் கையேடுகள்/ ஆவணங்கள் தொடர்பாக)

ஊடுருவல்

T1041 - C2 சேனல் வழியாக தரவு வெளியேற்றம் (செயல்மிகு விவரத் தொகுப்பிலிருந்து தீங்கிழைப்பவர் தரவு வெளியேற்றம் செய்வது மற்றும் பங்குகளை ஏற்றுவது தொடர்பாக)

விரிவான ஆய்வு 2

இந்த அறிக்கை பரவலாகப் பரப்பப்படுவதற்கு உதவும் வகையில் அநாமதேயமாக்கப்பட்டுள்ளது. பாதிக்கப்பட்ட அமைப்பு இனிமேல் 'அமைப்பு' என்று குறிப்பிடப்படுகிறது. இந்த விரிவான ஆய்வில் உள்ள தனிநபர்களின் பெயர்கள் மாற்றப்பட்டுள்ளன, அத்துடன் பாதிக்கப்பட்டவர்களின் அடையாளத்தைப் பாதுகாப்பதற்காக ASD இன் ACSC இல் சம்பவம் குறித்த அறிக்கையிலுள்ள விவரங்கள் அகற்றப்பட்டுள்ளன.

பொழிப்புரை

இந்த அறிக்கை 2022ஆம் ஆண்டு ஏப்ரல் மாதத்தில் அமைப்பின் நெட்வொர்க்கின் வெற்றிகரமாக சமரசம் செய்யப்பட்ட சம்பவங்கள் குறித்த ASD இன் ACSC விசாரணையின் கண்டுபிடிப்புகளை விவரிக்கிறது. அவதானிக்கப்பட்ட தீங்கிழைக்கும் செயல்பாட்டைச் சுருக்கமாகக் கூறுவதற்கும், தீர்வுக்கான பரிந்துரைகளை வடிவமைப்பதற்கும் இந்த விசாரணை அறிக்கை நிறுவனத்திற்கு வழங்கப்பட்டது. இந்த சமரசம் APT40 ஆல் மேற்கொள்ளப்பட்டது என்பதை கண்டுபிடிப்புகள் சுட்டிக் காட்டுகின்றன.

அமைப்பின் நெட்வொர்க்கைப் பாதிக்கும் சந்தேகத்திற்குரிய தீங்கிழைக்கும் செயல்பாட்டை 2022ஆம் ஆண்டு ஏப்ரல் மாதத்திலிருந்து ASDயின் ACSC அவதானித்து வருவதை 2022ஆம் ஆண்டு மே மாதம் அறிவித்தது. பின்னர், அந்த அமைப்பின் இணையத்தில் நேரடியாக இணைக்கப்படும் ஒரு சேவையகத்தில் தீங்கிழைக்கும் மென்பொருளைக் கண்டறிந்திருப்பதாக, ASD இன் ACSCற்குத் தகவல் அளித்தனர். அந்த சேவையகம் அமைப்பின் தொலைநிலை அணுகல் சேவைக்கு உள்நுழைவு வாயிலாக இருந்தது. இந்த சேவையகம் தொலைநிலை அணுகல் உள்நுழைவு மற்றும் அடையாள மேலாண்மை மென்பொருளைப் பயன்படுத்தியது, மேலும் இந்த அறிக்கையில் இனிமேல், 'சமரசம் செய்யப்பட்ட சாதனம்' என்று குறிப்பிடப்படும். ASD இன் ACSC செய்து கொண்ட விசாரணையின் அடிப்படையில் அமைப்பிற்காக மேற்கொள்ளப்பட்ட ஆராய்ச்சி முடிவுகள் மற்றும் தீர்வு ஆலோசனைகளை இந்த அறிக்கை விவரிக்கிறது.

குறைந்தபட்சம் 2022ஆம் ஆண்டு ஏப்ரல் மாதம் முதல் நிறுவனத்தின் தொலைநிலை அணுகல் உள்நுழைவு வாயிலாக சைபர் தீங்கிழைப்பவர்(கள்) மூலம் நிறுவனத்தின் நெட்வொர்க்கின் ஒரு பகுதி சமரசம் செய்யப்பட்டதற்கான சான்றுகள் சுட்டிக் காட்டின. இந்த சேவையகம் பல தீங்கிழைப்பவர்களால் சமரசம் செய்யப்பட்டிருக்கலாம், மேலும் சமரசத்தின் போது பரவலாக பிரசுரிக்கப்பட்ட தொலைதூர குறியீட்டு செயற்பாட்டு (RCE) பாதுகாப்பு குறைபாட்டின் காரணமாக பாதிக்கப்பட்டிருக்க வாய்ப்பு உள்ளது.

ASD இன் ACSC ஆல் கவனிக்கப்பட்ட முக்கிய தீங்கிழைப்பவர் செயல்பாடு பின் வருமாறு:

- ஹோஸ்ட் கணக்கீடு, இது ஒரு தீங்கிழைப்பவர் நெட்வொர்க்கின் சொந்த வரைபடத்தை உருவாக்குவதற்கு உதவுகிறது;
- இணையத்தில் நேரடியாக இணைக்கப்படும் ஒரு சேவையகத்தின் செயலிகள் மற்றும் web shell பயன்பாட்டின் சுரண்டல் - தீங்கிழைப்பவருக்கு நெட்வொர்க்கில் நுழைய அனுமதி மற்றும் கட்டளைகளை செயல்படுத்தும் திறனை அளிக்கிறது;
- மென்பொருள் பாதுகாப்பு குறைபாடுகளை பயன்படுத்தி சிறப்புரிமைகளை அதிகரித்தல்; மற்றும்
- பக்கவாட்டு இயக்கத்தை இயக்க நற்சான்றிதழ் சேகரிப்பு

ASD இன் ACSC ஏப்ரல் 2022 இல் சமரசம் செய்யப்பட்ட சாதனத்தில் பல நூறு தனித்துவமான பயனர் பெயர் மற்றும் கடவுச்சொல் இரண்டையும், தொலைநிலை அணுகல் அமர்வுகள் தொடர்பான பல பன்முக அங்கீகாரக் குறியீடுகள் (MFA) மற்றும் தொழில்நுட்ப பொருட்களையும் பாதிக்கப்பட்ட சாதனத்திலிருந்து எடுக்கப்பட்டதைக் கண்டறிந்தது. அமைப்பின் ஆய்வில், அந்த கடவுச் சொற்கள் செல்லுபடியாக உள்ளன என்பது கண்டறியப்பட்டது. முறையான பயனராக தொலைநிலை உள்நுழைவு அமர்வை கடத்த அல்லது உருவாக்க தீங்கிழைப்பவர் இந்த தொழில்நுட்ப பொருட்களை உண்மையான பயனரின் பெயரில் தொலைதூர உள்நுழைவு அமர்வை கைப்பற்ற அல்லது உருவாக்கப் பயன்படுத்தி நிறுவனத்தின் உள்ளக நெட்வொர்க்கில் நுழைவு பெற்றிருக்கலாம் என்று ASD இன் ACSC மதிப்பீடு செய்கிறது.

விசாரணை முடிவுகள்

விசாரணை சுருக்கம்

நிறுவன ஊழியர்களுக்கு தொலைநிலை உள் நுழைய அனுமதிக்கும் உபகரணங்களை தீங்கிழைப்பவர் சமரசம் செய்ததாக ASDயின் ACSC தீர்மானித்தது, மேலும் இந்த சமரசத்தைப் பயன்படுத்தி மேலதிக நடவடிக்கைகளை நடத்தத் தீங்கிழைப்பவர் முயற்சித்திருக்கிறார். இந்த உபகரணங்கள் மூன்று சுமை-சமநிலை ஹோஸ்ட்களைக் கொண்டுள்ளன, அங்கு சமரசத்திற்கான ஆரம்ப சான்றுகள் கண்டறியப்பட்டன. ஆரம்ப சமரசத்திற்குப் பிறகு மூன்று சுமை சமநிலை ஹோஸ்ட்களில் இரண்டு ஹோஸ்ட்களை அமைப்பு மூடியது. இதனால், அதன்பிறகு நிகழ்ந்த அனைத்து நடவடிக்கைகளும் ஒரு தனி ஹோஸ்டில் நடந்தன. சமரசம் செய்யப்பட்ட சாதனத்துடன் தொடர்புடைய பிற சேவையகங்களும் இதேபோன்ற முறையில் சுமை சமநிலையில் இருந்தன. வாசகத் தன்மைக்காக, இந்த அறிக்கையின் பெரும் பகுதியில் அனைத்து சமரசம் செய்யப்பட்ட சாதனங்களும் 'ஒற்றை சாதனம்' என்று குறிப்பிடப்படுகின்றன.

தீங்கிழைப்பவர் 2022 ஆம் ஆண்டு ஏப்ரல் மாதத்திலிருந்து பொதுவாக அறியப்பட்ட பாதிப்புகளைப் பயன்படுத்தி அந்த சாதனத்தில் web shellகளை நிறுவியதாக நம்பப்படுகிறது. அந்த குழுவின் மோசடி நிகழ்த்தும் நபர்கள் சாதனத்தில் அதிகரித்த உரிமைகளை பெற்றுள்ளனர் என மதிப்பிடப்பட்டுள்ளது. பதிவு செய்வதற்கான வசதி இல்லாத காரணத்தால் நடவடிக்கையின் முழு பரப்பளவை ASD-இன் ACSC இனால் கண்டறிய முடியவில்லை. இருப்பினும், சாதனத்தில் உள்ள சான்றுகள் தீங்கிழைப்பவர் பின் வருமாறு செயல்பட்டார் என்று காட்டுகின்றன:

- பல நூறு உண்மையான பயனாளர் பெயர் மற்றும் கடவுச்சொல் இரண்டையும் சேகரித்தல்; மற்றும்
- தீங்கிழைப்பவர் ஒருவரை, ஒரு முறையான பயனராக மெய்நிகர் உள் கட்டமைப்பு(VDI) அணுக அனுமதித்த தொழில்நுட்ப பொருட்களின் தொகுப்பு.

அமைப்பின் வலையமைப்பில் சமரசத்தை மேலும் அதிகரிக்க தீங்கிழைப்பவர் முயன்றிருப்பார் என்று ASDயின் ACSC மதிப்பிடுகிறது. தீங்கிழைப்பவர் திருடிய கூறுகள் அவர்களுக்கு மெய்நிகர் அமர்வுகளை ஒரு முறையான பயனாளராக அணுக அனுமதித்திருக்கலாம். அவர்களின் விருப்பத்தின்படி அவர்கள் பயனாளராகவோ, நிர்வாகிகளாகவோ இருந்திருக்கலாம். நிலைத்தன்மை மற்றும் பிற இலக்குகளை அடைய நிறுவன சேவைகளை மேலும் சமரசம் செய்ய தீங்கிழைப்பவர் இந்த அணுகல் திசையனைப் பயன்படுத்தியிருக்கலாம்.

ஹோஸ்டிங் வழங்குநர் நிர்வகிக்கும் சூழலில் உள்ள பிற நிறுவன உபகரணங்கள் சமரசத்திற்கான ஆதாரங்களைக் காட்டவில்லை.

அணுகல்

VDI அமர்வுகளுடன் (T1021.001) இணைக்கும் பயனர்களுக்கு, சமரசம் செய்யப்பட்ட சாதனத்துடன் ஹோஸ்ட் செயல்மிகு விவரத் தொகுப்பு மற்றும் webserver வழியாக அங்கீகாரத்தை வழங்கியது.

இடம்	சமரசம் செய்யப்பட்ட சாதன ஹோஸ்ட் பெயர்கள் (சுமை சமநிலை)
தரவு மையம் 1	HOST1, HOST2, HOST3

சாதன உட்கட்டமைப்பில் அணுகல் நுழைவாயில் ஹோஸ்ட்களும் அடங்கும், சாதனத்திலிருந்து உருவாக்கப்பட்ட மற்றும் பதிவிறக்கம் செய்யப்பட்ட அங்கீகார tokenனைப் பெற்றவுடன் அவை பயனருக்கு VDI க்கு ஒரு சுரங்கப் பாதையை வழங்குகின்றன.

இந்த ஹோஸ்ட்களில் எவையும் சமரசம் செய்யப்பட்டதற்கான எந்த ஆதாரமும் இல்லை. இருப்பினும், அணுகல் நுழைவாயில் ஹோஸ்ட்களில் உள்ள பதிவுகள், அறியப்பட்ட தீங்கிழைக்கும் IP முகவரிகளுடன் குறிப்பிடத்தக்க தொடர்புகளின் ஆதாரங்களைக் காட்டின. இந்த ஹோஸ்டில் ஏற்பட்ட செயல்பாடு அல்லது இந்த ஹோஸ்டை அடைந்த அச்சுறுத்தல் தீங்கிழைப்பவர் உள்கட்டமைப்புடன் ஏற்படுத்திய நெட்வொர்க் இணைப்புகளை இது பிரதிபலித்திருக்கலாம். இந்த செயல்பாட்டின் தன்மையை கிடைக்கக்கூடிய ஆதாரங்களைக் கொண்டு தீர்மானிக்க முடியவில்லை, ஆனால் நிறுவனத்தின் நெட்வொர்க்கில் பக்கவாட்டில் செல்ல தீங்கிழைப்பவர் குழு முயன்றது என்பதைக் குறிக்கிறது (TA0008).

உள் ஒழுங்குபடுத்தப்பட்ட கணினிகள்

உள் ஒழுங்குபடுத்தப்பட்ட கணினிகள் நெட்வொர்க் பிரிவிலிருந்து வரையறுக்கப்பட்ட தரவை ASDயின் ACSC விசாரித்தது. உள் நிறுவனத்தின் நெட்வொர்க் பிரிவைப் பாதித்ததாக அறியப்படும் முயற்சி அல்லது வெற்றிகரமான தீங்கிழைக்கும் நடவடிக்கையில் VDI-தொடர்பான பொருட்களைத் தீங்கிழைப்பவர் அணுகல், உள் SQL சேவையகத்தை சுரண்டச் செய்தல் (T1505.001), மற்றும் அறியப்பட்ட தீங்கிழைக்கும் IP முகவரிகளிலிருந்து அணுகல் நுழைவாயில் உபகரணங்கள் (TA0011) ஆகியவை அடங்கும்.

சமரசம் செய்யப்பட்ட சாதனத்திற்கான அணுகலைப் பயன்படுத்தி, உண்மையான பயனர் பெயர்கள், கடவுச் சொற்கள் (T1003), மற்றும் பன்முக அங்கீகார (MFA) token மதிப்புகள் (T1111) ஆகியவற்றை குழு சேகரித்தது. JSON வலை tokenகளையும் (JWTs) குழு சேகரித்தது (T1528), இது மெய்நிகர் உள்நுழைவு அமர்வுகளை உருவாக்கப் பயன்படுத்தப்படும்

அங்கீகாரப் பொருளாகும். மெய்நிகர் அமர்வுகளை (T1563.002) உருவாக்க அல்லது கடத்த தீங்கிழைப்பவர் இவற்றைப் பயன்படுத்த முடியும் மற்றும் உள் நிறுவன நெட்வொர்க் பிரிவை முறையான பயனராக அணுகலாம் (T1078).

நிறுவனத்தின் உள் நெட்வொர்க்கில் வசிக்கும் ஒரு SQL சேவையகத்தை (T1505.001) சுரண்ட, தீங்கிழைப்பவர் சமரசம் செய்யப்பட்ட சாதனத்திற்கான அணுகலைப் பயன்படுத்தினார். தீங்கிழைப்பவருக்கு இந்த தரவு அணுகல் இருந்திருக்கலாம்.

அறியப்பட்ட தீங்கிழைக்கும் IP முகவரிகளிலிருந்து நெட்வொர்க் தரவுப் பரிமாற்றம் இந்த சாதனத்தின் வழியாக அல்லது இந்த சாதனத்திற்கு நிகழ்ந்தது என்பதை அணுகல் நுழைவாயில் சாதனத்திலிருந்து கிடைக்கும் சான்றுகள் வெளிப்படுத்தின. மேலே விவரிக்கப்பட்டுள்ளபடி, தீங்கிழைக்கும் சைபர் தீங்கிழைப்பவர்கள் இந்த சாதனத்தைப் பாதித்து அல்லது பயன்படுத்தி, அமைப்பின் உள் நெட்வொர்க்கில் முன்னோக்கி செல்ல அனுமதித்திருக்கக்கூடும்.

விசாரணை கால வரிசை

கீழேயுள்ள பட்டியல் விசாரணையின் போது கண்டறியப்பட்ட முக்கிய நடவடிக்கைகளின் கால வரிசையை வழங்குகிறது.

நேரம்	நிகழ்வு
2022 ஆம் ஆண்டு ஏப்ரல் மாதம்	அறியப்பட்ட தீங்கிழைக்கும் IP முகவரிகள் அணுகல் நுழைவாயில் ஹோஸ்ட் HOST7 உடன் தொடர்பு கொள்கின்றன. இடைவினைகளின் தன்மையைத் தீர்மானிக்க முடியவில்லை.
2022 ஆம் ஆண்டு ஏப்ரல் மாதம்	அனைத்து ஹோஸ்ட்களும், HOST1, HOST2 மற்றும் HOST3, ஒரு தீங்கிழைக்கும் தீங்கிழைப்பவர் அல்லது தீங்கிழைப்பவர்களால் சமரசம் செய்யப்பட்டன, மேலும் ஹோஸ்ட்கள் மீது web shellகள் வைக்கப்பட்டன. ஒரு பதிவு கோப்பு உருவாக்கப்பட்டது அல்லது HOST2 இல் மாற்றப்பட்டது. இந்தக் கோப்பில் ஒரு தீங்கிழைப்பவரால் கைப்பற்றப்பட்ட நற்சான்றிதழ் உள்ளது. /etc/security/opasswd மற்றும் /etc/shadow கோப்புகள் HOST1 மற்றும் HOST3 இல் மாற்றப்பட்டன, அதாவது கடவுச் சொற்கள் மாற்றப்பட்டன என்பதை இது குறிக்கிறது. HOST1 இல் கிடைக்கும் சான்றுகள் பயனர் 'sshuser' இன் கடவுச் சொல் மாற்றப்பட்டதாகக் கூறுகிறது.
2022 ஆம் ஆண்டு ஏப்ரல் மாதம்	HOST2 அமைப்பால் மூடப்பட்டது. கூடுதல் web shellகள் (T1505.003) HOST1 மற்றும் HOST3 இல் உருவாக்கப்பட்டன. HOST1 மீது SSH brute force முயற்சிகள் HOST3 இலிருந்து நடத்தப்பட்டன. HOST3 இல் ஒரு பதிவு கோப்பு மாற்றியமைக்கப்பட்டது (T1070). இந்தக் கோப்பில் நற்சான்று (T1078) உள்ளது, இது ஒரு தீங்கிழைப்பவரால் கைப்பற்றப்பட்டிருக்கலாம். JWT கள் கைப்பற்றப்பட்டன (T1528) மற்றும் HOST3 இல் ஒரு கோப்பில் வெளியீடு. ஹோஸ்ட் 3 நிறுவனத்தால் மூடப்பட்டது. இதன் பின்னர் அனைத்து செயற்பாடுகளும் HOST1 இல் நிகழ்கின்றன.
2022 ஆம் ஆண்டு ஏப்ரல் மாதம்	கூடுதல் web shellகள் HOST1 இல் உருவாக்கப்பட்டன (T1505.003). JWT கள் கைப்பற்றப்பட்டு HOST1 இல் ஒரு கோப்பில் வெளியிடப்பட்டன.
2022 ஆம் ஆண்டு ஏப்ரல் மாதம்	கூடுதல் web shellகள் HOST1 (T1505.003) இல் உருவாக்கப்படுகின்றன, மேலும் அறியப்பட்ட தீங்கிழைக்கும் IP முகவரி ஹோஸ்டுடன் (TA0011) தொடர்பு கொள்கிறது. அறியப்பட்ட தீங்கிழைக்கும் IP முகவரி அணுகல் நுழைவாயில் ஹோஸ்ட் HOST7 உடன் தொடர்பு கொள்கிறது.
2022 ஆம் ஆண்டு மே மாதம்	அறியப்பட்ட தீங்கிழைக்கும் IP முகவரி அணுகல் நுழைவாயில் ஹோஸ்ட் HOST7 (TA0011) உடன் தொடர்பு கொண்டது. ஒரு பயனருக்கான அங்கீகாரம் வழங்கப்பட்ட நிகழ்வு HOST1 இல் பதிவுகளில் அறியப்பட்ட தீங்கிழைக்கும் IP முகவரியுடன் இணைக்கப்பட்டுள்ளது. இந்த ஹோஸ்டில் ஒரு கூடுதல் web shell உருவாக்கப்படுகிறது (T1505.003).
2022 ஆம் ஆண்டு மே மாதம்	HOST1 இல் ஒரு ஸ்கிரிப்ட் ஒரு தீங்கிழைப்பவரால் மாற்றப்பட்டது (T1543). இந்த ஸ்கிரிப்ட் ஒரு உள் SQL சேவையகத்திலிருந்து தரவை சுரண்டச் செய்திருக்கும் செயல்பாட்டைக் கொண்டுள்ளது.
2022 ஆம் ஆண்டு மே மாதம்	HOST1 இல் கூடுதல் பதிவு கோப்பு கடைசியாக மாற்றப்பட்டது (T1070). இந்த கோப்பில் நிறுவன நெட்வொர்க்கிற்கான பயனர் பெயர் மற்றும் கடவுச்சொல் இரண்டும் உள்ளன, அவை முறையானவை என்று நம்பப்படுகிறது (T1078).
2022 ஆம் ஆண்டு மே மாதம்	ஒரு கூடுதல் குறிப்பேடு கோப்பு கடைசியாக மாற்றப்பட்டது (T1070). இந்த கோப்பில் HOST1 இலிருந்து சேகரிக்கப்பட்ட JWT கள் உள்ளன.
2022 ஆம் ஆண்டு மே மாதம்	கூடுதல் web shellகள் HOST1 இல் உருவாக்கப்பட்டன (T1505.003). இந்த தேதியில், ஏப்ரல் 2022 இல் உருவாக்கப்பட்ட தேதியுடன் ஒரு web shell கண்டுபிடிக்கப்பட்டதை ASD இன் ACSC ற்கு அமைப்பு அறிவித்தது
2022 ஆம் ஆண்டு மே மாதம்	HOST1 இல் பல ஸ்கிரிப்ட்கள் உருவாக்கப்பட்டன, இதில் Log4jHotPatch.jar என்ற பெயரும் அடங்கும்.
2022 ஆம் ஆண்டு மே மாதம்	அணுகல் நுழைவாயில் ஹோஸ்டில் இரண்டு திறந்த 'போர்ட்'களைச் சேர்க்க iptables-save கட்டளை பயன்படுத்தப்பட்டது. அவை போர்ட் 9998 மற்றும் போர்ட் 9999 (T1572) ஆகும்.

தீங்கிழைப்பவர்களின் தந்திரோபாயங்கள் மற்றும் நுட்பங்கள்

விசாரணையின் போது அடையாளம் காணப்பட்ட பல தந்திரோபாயங்கள் மற்றும் நுட்பங்கள் கீழே விவரிக்கப்பட்டுள்ளன.

ஆரம்ப அணுகல்

T1190இணைய வழியாக பொது மக்களும் அணுகக்கூடிய ஒரு மென்பொருளை தாக்குதல்

நெட்வொர்க்கிற்கான ஆரம்ப அணுகலைப் பெறுவதற்கு, remote access login மற்றும் identity management இலுள்ள RCE, சிறப்புரிமை விரிவாக்கம் மற்றும் அங்கீகார சான்றிதழ் தவிர்ப்புத் தளர்வுகளை குழு பயன்படுத்தியிருக்கலாம்.

இந்த ஆரம்ப அணுகல் முறை பின்வருவனவற்றின் காரணமாக மிகவும் சாத்தியமாகக் கருதப்படுகிறது:

- அந்த நேரத்தில் சேவையகம் இந்த CVEகளுக்கு பாதிக்கப்படக்கூடியதாக இருந்தது;
- அறியப்பட்ட தீங்கிழைப்பவர் உள்கட்டமைப்பிலிருந்து இந்த பாதிப்புகளைப் பயன்படுத்துவதற்கான முயற்சிகள் மேற்கொண்டது; மற்றும்
- சுரண்டல் முயற்சிகள் மேற்கொள்ளப்பட்ட சிறிது நேரத்திலேயே முதல் அறியப்பட்ட உள் தீங்கிழைக்கும் நடவடிக்கை நிகழ்ந்தது.

நிறைவேற்றுதல்

T1059.004 கட்டளை மற்றும் ஸ்கிரிப்டிங் மொழிமாற்றி: Unix Shell

மேலே உள்ள பாதிப்புகளை குழு வெற்றிகரமாக பயன்படுத்தியது, பாதிக்கப்பட்ட சாதனத்தில் கிடைக்கும் Unix Shellஇல் கட்டளைகளை இயக்க முடிந்திருக்கலாம். தீங்கிழைப்பவர்களால் இயக்கப்படும் கட்டளைகளின் முழுமையான விவரங்களை வழங்க முடியாது, ஏனெனில் அவை சாதனத்தால் உள்நுழையப்படவில்லை.

நிலைத்தன்மை

T1505.003 சேவையக மென்பொருள் உபகரணம்: Web Shell

பாதிக்கப்பட்ட சாதனத்தின் மீது தீங்கிழைப்பவர்கள் பல web shellகளை வைத்தனர். பல தனித்துவமான தீங்கிழைப்பவர்கள் web shellகளைப் பயன்படுத்தியிருக்கலாம், ஆனால் குறைந்த எண்ணிக்கையிலான தீங்கிழைப்பவர்கள் மட்டுமே இந்த web shellகளைப் பயன்படுத்தி செயல்பாட்டை நடத்தினர். சமரசம் செய்யப்பட்ட சாதனங்களில் தீங்கிழைப்பவர் தன்னிச்சையான கட்டளை செயல்படுத்தலை web shell அனுமதித்திருக்கும்.

சிறப்புரிமை வளர் நிலை

T1068 சிறப்புரிமை மேம்படுத்தலுக்கான சுரண்டல்

கிடைக்கக்கூடிய சான்றுகள் தீங்கிழைப்பவர்கள் அடைந்த சிறப்புரிமையின் அளவை விவரிக்கவில்லை. இருப்பினும், web shellகளைப் பயன்படுத்தி, தீங்கிழைப்பவர்கள் சமரசம் செய்யப்பட்ட சாதனத்தில் வலை சேவையகத்துடன் ஒப்பிடக்கூடிய சிறப்புரிமையின் அளவை அடைந்திருப்பார்கள். சமரசம் செய்யப்பட்ட சாதனத்தில் இருந்ததாக நம்பப்படும் பாதிப்புகள் தீங்கிழைப்பவர்களை ஆகக் கூடிய சலுகைகளை அடைய அனுமதித்திருக்கும்.

தகுதிச்சான்றிதழ் அணுகல்

T1056.003 உள்ளீட்டைக் கைப்பற்றல்: இணைய முகப்பைக் கைப்பற்றல்

தீங்கிழைப்பவர் பல நூறு பயனர் பெயர் மற்றும் கடவுச் சொல் இரண்டையும் தெளிவான உரையில் கைப்பற்றியதை சமரசம் செய்யப்பட்ட சாதனத்தில் உள்ள ஆதாரங்கள் காட்டியது, அவை முறையானவை என்று நம்பப்படுகிறது. ஒரு கோப்பிற்கு நற்சான்றிதழ்களை வெளியிடும் உண்மையான அங்கீகார செயல் முறைக்கு சில மாற்றங்களைப் பயன்படுத்தி இவை கைப்பற்றப்பட்டிருக்கலாம்.

T1111பன்முக அங்கீகாரத்தை இடைமறித்தல்

முறையான உள்நுழைவுகளுடன் தொடர்புடைய பன்முக அங்கீகார (MFA) tokenகளின் மதிப்பையும் தீங்கிழைப்பவர் கைப்பற்றினார். இந்த மதிப்புகளை ஒரு கோப்பில் வெளியேற்ற உண்மையான அங்கீகார செயல்முறையை மாற்றியமைப்பதன் மூலம் இவை கைப்பற்றப்பட்டிருக்கலாம். பன்முக அங்கீகார (MFA) tokenகளின் பாதுகாப்பை வழங்கும் தனித்துவமான மதிப்புகளை சேமிக்கும் 'ரகசிய சேவையகத்தை' சமரசம் செய்வதற்கான எந்த ஆதாரமும் இல்லை.

T1040 வலையமைப்பை மோப்பம் விடுதல்

சமரசம் செய்யப்பட்ட சாதனத்தில் HTTP தரவுப் பரிமாற்றத்தைக் கைப்பற்றுவதன் மூலம் தீங்கிழைப்பவர் JWTகளைக் கைப்பற்றியதாக நம்பப்படுகிறது. சமரசம் செய்யப்பட்ட சாதனத்தில் பயன்பாட்டு tcpdump செயல்படுத்தப்பட்டது என்பதற்கான சான்றுகள் உள்ளன, எனவே தீங்கிழைப்பவர் இந்த JWTகளை இவ்வாறு கைப்பற்றியிருக்கலாம்.

T1539 வலை அமர்வு cookieயைத் திருடல்

மேலே விவரிக்கப்பட்டுள்ளபடி, தீங்கிழைப்பவர் JWT களைக் கைப்பற்றினார், அவை வலை அமர்வு cookieக்களுக்கு ஒத்தவை. இவற்றை தீங்கிழைப்பவர் மீண்டும் பயன்படுத்தி மேலும் அணுகலை நிறுவியிருக்கலாம்.

கண்டுபிடிப்பு

T1046 பிணைய சேவை கண்டுபிடிப்பு

nmap என்ற network scanning utility செயலி அதே நெட்வொர்க் பிரிவில் உள்ள மற்ற சாதனங்களை ஸ்கேன் செய்ய சமரசம் செய்யப்பட்ட சாதனத்தில் செயல்படுத்தப்பட்டதற்கான சான்றுகள் உள்ளன. பக்கவாட்டு இயக்கத்திற்கான வாய்ப்புகளை வழங்கக்கூடிய பிற அணுகக்கூடிய நெட்வொர்க் சேவைகளைக் கண்டறிய இது தீங்கிழைப்பவரால் பயன்படுத்தப்பட்டிருக்கலாம்.

தொகுப்பு

தீங்கிழைப்பவர்கள் எவ்வாறு தரவை சேகரித்தனர் அல்லது சமரசம் செய்யப்பட்ட சாதனத்திலிருந்து அல்லது பிற அமைப்புகளிலிருந்து சரியாக என்ன சேகரிக்கப்பட்டது என்பதை கிடைக்கக்கூடிய சான்றுகள் வெளிப்படுத்தவில்லை. இருப்பினும், கைப்பற்றப்பட்ட நற்சான்றிதழ்கள் (T1003), பன்முக அங்கீகார (MFA) token மதிப்புகள் (T1111) மற்றும் மேலே விவரிக்கப்பட்ட JWTகள் உட்பட சமரசம் செய்யப்பட்ட சாதனத்தில் உள்ள அனைத்து கோப்புகளுக்கும் தீங்கிழைப்பவர்கள் அணுகலைக் கொண்டிருந்தனர்.

கட்டளை மற்றும் கட்டுப்பாடு

T1071.001 செயலி அடுக்கு நெறிமுறை: வலை நெறிமுறைகள்

தீங்கிழைப்பவர்கள் கட்டளை மற்றும் கட்டுப்பாட்டிற்காக web shellகளைப் பயன்படுத்தினர். சாதனத்தில் (T1572) இருக்கும் வலை சேவையகத்தைப் பயன்படுத்தி web shell கட்டளைகள் HTTPS மீது அனுப்பப்பட்டிருக்கும்.

T1001.003 தரவு தெளிவின்மை: நெறிமுறை ஆள்மாறாட்டம்

தீங்கிழைப்பவர்கள் முறையான தரவுப் பரிமாற்றத்துடன் கலக்க வடிவமைக்கப்பட்ட தாக்குதல்களுக்கான தொடக்க புள்ளியாக சமரசம் செய்யப்பட்ட சாதனங்களைப் பயன்படுத்தினர்.

கண்டறிதல் மற்றும் தணிப்பு பரிந்துரைகள்

ASD Essential Eight கட்டுப்பாடுகள் மற்றும் தொடர்புடைய சைபர் பாதுகாப்பு சம்பவங்களைத் தணிப்பதற்கான உத்திகளை செயல்படுத்த ASD இன் ACSC கடுமையாக பரிந்துரைக்கிறது. APT40 மூலம் ஊடுருவல்களைக் கண்டறிந்து தடுக்க எடுக்கப்பட வேண்டிய நெட்வொர்க் பாதுகாப்பு நடவடிக்கைகளுக்கான பரிந்துரைகள் கீழே உள்ளன, அதைத் தொடர்ந்து அட்டவணை 1 இல் சுருக்கமாகக் குறிப்பிடப்பட்டுள்ள நான்கு முக்கிய தந்திரோபாயங்கள், நுட்பங்கள் மற்றும் நடைமுறைகளுக்கான (TTP) குறிப்பிட்ட மட்டுப்படுத்தல்கள்.

கண்டறிதல்

மேலே அடையாளம் காணப்பட்ட சில கோப்புகள் C:\Users\Public* மற்றும் C:\Windows\Temp* போன்ற இடங்களில் கைவிடப்பட்டன. தரவை எழுதுவதற்கு இவை வசதியான இடங்களாக இருக்கலாம், ஏனெனில் அவை வழக்கமாக யாராலும் எழுத அனுமதி உள்ளவை, அதாவது Windowsஸில் பதிவு செய்யப்பட்ட அனைத்து பயனர் கணக்குகளும் இந்த கோப்பகங்கள் மற்றும் அவற்றின் துணை அடைவுகளுக்கு அணுகலைக் கொண்டுள்ளன. பெரும்பாலும், எந்தவொரு பயனரும் இந்த கோப்புகளை பின்னர் அணுகலாம், இது பக்கவாட்டு இயக்கம், பாதுகாப்பு தவிர்ப்பு, குறைந்த சிறப்புரிமை நிறைவேற்றுதல் மற்றும் தரவு வெளியேற்றத்திற்கான ஒத்திகை ஆகியவற்றிற்கான வாய்ப்புகளை அனுமதிக்கிறது.

பின்வரும் Sigma விதிகள் சந்தேகத்திற்கிடமான இடங்களில் இருந்து செயல்படுத்தப்படுவதை ஒழுங்கற்ற செயல்பாட்டின் குறிகாட்டியாக பார்க்கின்றன. எல்லா நிகழ்வுகளிலும், தீங்கிழைக்கும் செயல்பாடு மற்றும் பண்புக்கூறு ஆகியவற்றை உறுதிப்படுத்த அடுத்தடுத்த விசாரணை தேவைப்படுகிறது.

தலைப்பு: World Writable Execution - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

விளக்கம் C:\Windows\Temp. **இலிருந்து செயல்முறை செயல்படுத்தலைக் கண்டறியவும்.**

பின்னணி:

இந்த விதி குறிப்பாக C:\Windows\Temp* இலிருந்து செயல்படுத்துவதைத் தேடுகிறது. தீங்கற்ற பயன்பாடுகளால் மிகவும் பரவலாக C:\Windows\Temp\ பயன்படுத்தப்படுகிறது, இதனால் C:\Windows\ இல் உள்ள பிற யாரும் அணுகக்கூடிய துணை அடைவுகளில் இருந்து செயல்படுத்தப்படுவதை விட குறைந்த நம்பிக்கை தீங்கிழைக்கும் காட்டி ஆகும்.

SYSTEM அல்லது NETWORK SERVICE பயனர்களால் செயல்படுத்தப்பட்ட செயலிகளை அகற்றுவது இந்த விதியால் தேர்ந்தெடுக்கப்பட்ட தீங்கற்ற செயல்பாட்டின் அளவை கணிசமாகக் குறைக்கிறது.

இதன் பொருள் என்னவென்றால், உயர் சலுகை மட்டத்தில் தீங்கிழைக்கும் நிறைவேற்றுதல்களை விதி தவறவிடக்கூடும், ஆனால் ஒரு பயனர் சிறப்புரிமைகளை SYSTEM ற்கு உயர்த்த முயற்சிக்கிறாரா என்பதை தீர்மானிக்க பிற விதிகளைப் பயன்படுத்த பரிந்துரைக்கப்படுகிறது.

ஆராய்ச்சி:

1. இந்த கோப்பு செயல்படுத்தலுடன் நேரடியாக தொடர்புடைய பயனர் சூழல், செயல்படுத்தல் ஒருமைப்பாடு நிலை, உடனடி பின்தொடர்தல் செயல்பாடு மற்றும் கோப்பில் ஏற்றப்பட்ட படங்கள் போன்ற தகவல்களை ஆராயவும்.
2. ஹோஸ்டில் உள்ள சூழ்நிலை செயல்முறை, நெட்வொர்க், கோப்பு மற்றும் பிற ஆதரவு தரவை ஆராய்ந்து செயல்பாடு தீங்கிழைக்கிறதா என்பதை மதிப்பீடு செய்ய உதவுகிறது.
3. தேவைப்பட்டால், அது முறையானதா என்பதை தீர்மானிக்க, தலைகீழ் பொறியியலுக்கான கோப்பின் நகலை சேகரிக்க முயற்சிக்கவும்.

ஒப்பீடுகள்:

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

ஆசிரியர்: ASD யின் ACSC

தேதி: 2024/06/19

நிலை: சோதனை சார்ந்த

குறிச் சொற்கள்:

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

பதிவு மூலம்:

வகை: process_creation
தயாரிப்பு: Windows

கண்டறிதல்:

```
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)

தவறான நேர்மறைகள்:

- அனுமதி பட்டியல் தணிக்கை பயன்பாடுகள் Temp அடைவிலிருந்து இயங்கக்கூடியவைகளை இயக்குவதைக் காணலாம்.
- சட்டபூர்வமாக அமைவு பயன்பாடுகள் மற்றும் துவக்கிகளின் வரிசையை Temp அடைவு கொண்டிருக்கும், எனவே இந்த விதியைப் பயன்படுத்துவதற்கு முன்பு கண்காணிக்கப்பட்ட நெட்வொர்க்கில் இந்த நடத்தை எவ்வளவு பரவலாக உள்ளது (மற்றும் அதை அனுமதிக்க முடியுமா இல்லையா) என்பதைக் கருத்தில் கொள்வது நல்லது.

நிலை: குறைவான

தலைப்பு: World Writable Execution - Non-Temp System Subdirectory

அடையாளம் 5b187157-e892-4fc9-84fc-aa48aff9f997

விளக்கம் Windows OS நிறுவல் இருப்பிடத்தின் துணை அடைவில், யாரும் அணுகக்கூடிய இடத்திலிருந்து செயல்முறை செயல்படுத்தலைக் கண்டறியவும்.

பின்னணி:

தீங்கற்ற பயன்பாடுகளால் மிகவும் பரவலாக C:\Windows\Temp\ பயன்படுத்தப்படுகிறது, இதனால் C:\Windows\ இல் உள்ள பிற யாரும் அணுகக்கூடிய துணை அடைவுகளில் இருந்து செயல்படுத்தப்படுவதை விட குறைந்த நம்பிக்கை தீங்கிழைக்கும் காட்டி ஆகும். இந்த விதி குறிப்பாக C:\Windows\Temp* இலிருந்து செயல்படுத்துவதைத் தேடுகிறது.

ஒரு கோப்பு SYSTEM ஆக இயக்கப்பட்டால் AppData கோப்புறைகள் விலக்கப்படுகின்றன - இது பல தற்காலிக பயன்பாட்டு கோப்புகள் செயல்படுத்தப்படும் ஒரு தீங்கற்ற வழியாகும்.

ஆரம்ப நெட்வொர்க் அடித்தளத்தை முடித்து, இந்த இடங்களிலிருந்து அறியப்பட்ட தீங்கற்ற நிறைவேற்றுதல்களை அடையாளம் கண்ட பிறகு, இந்த விதி அரிதாகவே பயன்படுத்தப்பட வேண்டும்.

ஆராய்ச்சி:

1. இந்த கோப்பு செயல்படுத்தலுடன் நேரடியாக தொடர்புடைய பயனர் சூழல், செயல்படுத்தல் ஒருமைப்பாடு நிலை, உடனடி பின்தொடர்தல் செயல்பாடு மற்றும் கோப்பில் ஏற்றப்பட்ட படங்கள் போன்ற தகவல்களை ஆராயவும்.
2. ஹோஸ்டில் உள்ள சூழ்நிலை செயல்முறை, நெட்வொர்க், கோப்பு மற்றும் பிற ஆதரவு தரவை ஆராய்ந்து செயல்பாடு தீங்கிழைக்கிறதா என்பதை மதிப்பீடு செய்ய உதவுகிறது.
3. தேவைப்பட்டால், அது முறையானதா என்பதை தீர்மானிக்க, தலைகீழ் பொறியியலுக்கான கோப்பின் நகலை சேகரிக்க முயற்சிக்கவும்.

ஒப்பீடுகள்:

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

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

ஆசிரியர்: ASDயின் ACSC.

தேதி: 2024/06/19

நிலை: சோதனை சார்ந்த

குறிச் சொற்கள்:

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

பதிவு மூலம்:

வகை: process_creation

தயாரிப்பு: windows

கண்டறிதல்:

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

தவறான நேர்மறைகள்:

அனுமதி பட்டியல் தணிக்கை பயன்பாடுகள் இந்த அடைவிலிருந்து இயங்கக்கூடியவைகளை இயக்குவதைக் காணலாம்.

கண்காணிக்கப்படும் சூழலில்(களில்) பயன்படுத்தப்படும் ஸ்கிரிப்டுகள் மற்றும் நிர்வாக கருவிகள் இந்த கோப்பகங்களில் ஒன்றில் அமைந்திருக்கலாம், மேலும் அவை ஒவ்வொன்றிற்கும் தனித்தனியாகக் கையாளப்பட வேண்டும் என்று பரிந்துரைக்கப்படுகிறது.

நிலை: உயர்வான

Title: World Writable Execution - Users

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

விளக்கம் C:\Users\Public* மற்றும் பயனர்களுக்கு உரிமையுள்ள, பிற அனைவரும் அணுகக்கூடிய அடைவுகளில் இருந்து செயல்முறை செயல்படுத்தலைக் கண்டறியவும்.

பின்னணி:

ஒரு கோப்பு SYSTEM ஆக இயக்கப்பட்டால் AppData கோப்புறைகள் விலக்கப்படுகின்றன - இது பல தற்காலிக பயன்பாட்டு கோப்புகள் செயல்படுத்தப்படும் ஒரு தீங்கற்ற வழியாகும்.

ஆராய்ச்சி:

1. இந்த கோப்பு செயல்படுத்தலுடன் நேரடியாக தொடர்புடைய பயனர் சூழல், செயல்படுத்தல் ஒருமைப்பாடு நிலை, உடனடி பின்தொடர்தல் செயல்பாடு மற்றும் கோப்பில் ஏற்றப்பட்ட படங்கள் போன்ற தகவல்களை ஆராயவும்.
2. ஹோஸ்டில் உள்ள சூழ்நிலை செயல்முறை, நெட்வொர்க், கோப்பு மற்றும் பிற ஆதரவு தரவை ஆராய்ந்து செயல்பாடு தீங்கிழைக்கிறதா என்பதை மதிப்பீடு செய்ய உதவுகிறது.
3. தேவைப்பட்டால், அது முறையானதா என்பதை தீர்மானிக்க, தலைகீழ் பொறியியலுக்கான கோப்பின் நகலை சேகரிக்க முயற்சிக்கவும்.

ஒப்பீடுகள்:

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

நூலாசிரியர்: ASDயின் ACSC.

தேதி: 2024/06/19

நிலை: சோதனை சார்ந்த

குறிச் சொற்கள்:

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

பதிவு மூலம்:

வகை: process_creation

தயாரிப்பு: windows

கண்டறிதல்:

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

நிபந்தனை: பயனர்கள் ஆனால் AppData அல்ல

தவறான நேர்மறைகள்:

- கண்காணிக்கப்படும் சூழலில்(களில்) பயன்படுத்தப்படும் ஸ்கிரிப்டுகள் மற்றும் நிர்வாக கருவிகள் இந்த கோப்பகங்களில் ஒன்றில் அமைந்திருக்கலாம், மேலும் அவை ஒவ்வொன்றிற்கும் தனித்தனியாகக் கையாளப்பட வேண்டும் என்று பரிந்துரைக்கப்படுகிறது.

நிலை: இடையிலான

மட்டுப்படுத்தல்கள்

பதிவெடுத்தல்

ASDயின் ACSC விசாரணைகளின் போது, வலை சேவையக கோரிக்கை பதிவுகள், Windows event பதிவுகள் மற்றும் இணைய பதிலாள் (proxy) பதிவுகள் உள்ளிட்ட பல பகுதிகளில் விரிவான மற்றும் வரலாற்று பதிவு தகவல் இல்லாதது புலனாய்வு முயற்சிகளின் செயல்திறனையும் வேகத்தையும் குறைக்கும் ஒரு பொதுவான பிரச்சினையாக இருந்தது.

Windows Event Logging and Forwarding இலுள்ள தங்களது வழிகாட்டுதலையும், Windows Event Logging Repository இலுள்ள உள் அமைப்புக் கோப்புகள் மற்றும் ஸ்கிரிப்ட்களையும் மற்றும் the Information Security Manual's Guidelines for System Monitoring ஆகியவற்றில் கூறப்பட்டுள்ள வழிகாட்டுதலையும் மதிப்பாய்வு செய்து செயல்படுத்த ASD இன் ACSC பரிந்துரைக்கிறது.

வழுநீக்கல் மேலாண்மை

வலை சேவையகங்கள், வலை பயன்பாடுகள் மற்றும் தொலைநிலை அணுகல் நுழைவாயில்கள் உட்பட அனைத்து இணையத்தில் வெளிப்படையாகக் காணப்படும் சாதனங்கள் மற்றும் சேவைகளையும் உடனடியாக வழுநீக்கல் செய்யவும். செயல்முறையை தானியக்கமாக்குவதற்கும் விரைவு படுத்துவதற்கும் மையப்படுத்தப்பட்ட வழுநீக்கல் மேலாண்மை அமைப்பை செயல்படுத்துவதைக் கவனியுங்கள். ISM இன் Guidelines for System Management என்ற கணினி மேலாண்மைக்கான வழிகாட்டுதல்கள், குறிப்பாக பொருந்தக்கூடிய இடங்களில் கணினி வழுநீக்கல் கட்டுப்பாடுகளை செயல்படுத்த ASD இன் ACSC பரிந்துரைக்கிறது.

தீங்கிழைப்பவரால் பயன்படுத்தப்பட்ட பெரும்பாலான சுரண்டல்கள் பகிரங்கமாக அறியப்பட்டவை, அத்துடன் அவற்றிற்கான வழுநீக்கல் மற்றும் மட்டுப்படுத்தல்கள் இருந்தன. இணையத்துடன் இணைக்கப்பட்ட உட்கட்டமைப்பில் பாதுகாப்பு வழுநீக்கல் அல்லது மட்டுப்படுத்தல் செயற்பாடுகள் 48 மணி நேரத்திற்குள் மேற்கொள்ளப்படுவதை நிறுவனங்கள் உறுதி செய்ய வேண்டும், மேலும் சாத்தியமான இடங்களில், மென்பொருள் மற்றும் இயக்க முறைமைகளின் சமீபத்திய பதிப்புகளைப் பயன்படுத்த வேண்டும்.

நெட்வொர்க் பிரிவு

நிறுவனத்தின் முக்கியமான தரவுகளைக் கண்டுபிடித்து, அவற்றை சைபர் குற்றவாளிகள் அணுகுவதை நெட்வொர்க் பிரிவுகள் கணிசமாகக் கடினமாக்கும். தேவைப்படாவிட்டால், கணினிகளுக்கு இடையிலான தரவுப் பரிமாற்றத்தை மறுப்பதன் மூலம் பக்கவாட்டு இயக்கத்தை கட்டுப்படுத்த அல்லது தடுக்க நெட்வொர்க்குகளைப் பிரிக்கவும். செயல்மிகு விவரத் தொகுப்பு மற்றும் பிற அங்கீகார சேவையகங்கள் போன்ற முக்கியமான சேவையகங்கள் ஒரு குறிப்பிட்ட எண்ணிக்கையிலான இடைநிலை சேவையகங்கள் அல்லது 'jump server' களிலிருந்து மட்டுமே நிர்வகிக்கப்பட வேண்டும். இந்த சேவையகங்கள் உன்னிப்பாக கண்காணிக்கப்பட வேண்டும், நன்கு பாதுகாக்கப்பட வேண்டும் மற்றும் எந்த பயனர்கள் மற்றும் சாதனங்கள் அவற்றுடன் இணைக்க முடியும் என்பதைக் கட்டுப்படுத்த வேண்டும்.

பக்கவாட்டு இயக்கம் தடுக்கப்படும் நிகழ்வுகளைப் பொருட்படுத்தாமல், தீங்கிழைப்பவர்கள் அணுகவும் பிரித்தெடுக்கவும் முடிந்த தரவின் அளவை கூடுதல் நெட்வொர்க் பிரிவாக்கம் மேலும் மட்டுப்படுத்துவதாக இருக்கலாம்.

கூடுதல் மட்டுப்படுத்தல்கள்

APT40 மற்றும் கீழே உள்ள TTPகளின் மற்றவர்களின் பயன்பாட்டை எதிர்த்துப் போராட பின்வரும் மட்டுப்படுத்தல்களையும் அதிகார முகமைகள் பரிந்துரைக்கின்றன.

- பயன்படுத்தப்படாத அல்லது தேவையற்ற பிணைய சேவைகள், போர்ட்கள் மற்றும் நெறிமுறைகளை முடக்கவும்.
- வலை சேவையகங்கள் மற்றும் பயன்பாடுகளைப் பாதுகாக்க நன்கு வடிவமைக்கப்பட்ட வலை பயன்பாட்டு தீச்சுவர்களை (web application firewalls - WAF) பயன்படுத்தவும்.
- சேவையகங்கள், கோப்பு பகிர்வுகள் மற்றும் பிற ஆதாரங்களுக்கான அணுகலை கட்டுப்படுத்த குறைந்தபட்ச சிறப்புரிமை சலுகைகளை செயல் படுத்தவும்.
- பன்முக அங்கீகாரம் (MFA) மற்றும் நிர்வகிக்கப்பட்ட சேவை கணக்குகளைப் பயன்படுத்தவும், நற்சான்றிதழ்களைத் திருடவும் மீண்டும் பயன்படுத்தவும் கடினமாக்குங்கள். அனைத்து இணைய அணுகல் தொலைநிலை அணுகல் சேவைகளுக்கும் MFA பயன்படுத்தப்பட வேண்டும், அவற்றுள் பின்வருவன அடங்கும்:
  - இணையம் மற்றும் மேகக் கணிமை அடிப்படையிலான மின்னஞ்சல்
  - ஒத்துழைப்பு தளங்கள்
  - Virtual Private Network எனப்படும் மெய் நிகர் தனியார் நெட்வொர்க் (VPN) இணைப்புகள்
  - தொலைவிலிருந்து கணினியை அணுக வழி செய்யும் Remote Desktop சேவைகள்
- அவற்றின் வாழ்க்கையின் இறுதிக் கட்டத்திலுள்ள (end-of-life - EOL) உபகரணங்களை மாற்றவும்.

அட்டவணை 1. தணிப்பு உத்திகள் / நுட்பங்கள்

தந்திரோபாயங்கள், நுட்பங்கள் மற்றும் நடைமுறைகள்(TTP)	அத்தியாவசிய எட்டு மட்டுப்படுத்தல் உத்திகள்	ISM கட்டுப்பாடுகள்
ஆரம்ப அணுகல் T1190 பொதுமக்கள் அணுகக்கூடிய செயலியை சுரண்டல்	வழுநீக்கல் பயன்பாடுகள் வழுநீக்கல் இயக்க முறைமைகள் Multi-Factor Authentication என்ற இரு படி சரிபார்த்தல் செயலி கட்டுப்பாடு	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
நிறைவேற்றுதல் T1059 கட்டளை மற்றும் ஸ்கிரிப்டிங் மொழிமாற்றி	செயலி கட்டுப்பாடு Microsoft Office macroக்களை கட்டுப்படுத்தவும் நிர்வாக சிறப்புரிமைகளை கட்டுப்படுத்தவும்	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
நிலைத்தன்மை T1505.003 சேவையக மென்பொருள் உபகரணம்: Web Shell	செயலி கட்டுப்பாடு நிர்வாக சிறப்புரிமைகளைக் கட்டுப்படுத்தவும்	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
ஆரம்ப அணுகல் / சிறப்புரிமை வளர் நிலை / நிலைத்தன்மை T1078 செல்லுபடியான கணக்குகள்	வழுநீக்கல் இயக்க முறைமைகள் Multi-Factor Authentication என்ற இரு படி சரிபார்த்தல் நிர்வாக சிறப்புரிமைகளைக் கட்டுப்படுத்தவும் செயலி கட்டுப்பாடு பயனர் செயலியை கடினப்படுத்தவும்	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

கூடுதல் கண்டறிதல் மற்றும் மட்டுப்படுத்தல் ஆலோசனைக்கு, இந்த ஆலோசனையின் முடிவில் MITRE ATT&CK திரட்டில் அடையாளம் காணப்பட்ட ஒவ்வொரு நுட்பங்களுக்கும் MITRE ATT&CK நுட்ப வலைப் பக்கத்தில் உள்ள மட்டுப்படுத்தல் மற்றும் கண்டறிதல் பிரிவுகளைப் பார்க்கவும்.

பொறுப்புத் துறப்பு

இந்த வழிகாட்டியில் உள்ள தகவல்கள், "உள்ளது உள்ளபடியே" தகவல் பகிரும் நோக்கங்களுக்காக மட்டுமே வழங்கப்படுகின்றன. இந்த ஆவணத்தில் இணைக்கப்பட்டுள்ள எந்தவொரு நிறுவனங்கள், தயாரிப்புகள் அல்லது சேவைகள் உட்பட எந்தவொரு வணிக நிறுவனம், தயாரிப்பு, நிறுவனம் அல்லது சேவையை இந்த ஆவணத்தை உருவாக்கிய முகவர் ஆதரிக்கவோ, பரிந்துரைக்கவோ இல்லை இதில் கூறப்படும் எந்தவொரு உற்பத்தியாளர் அல்லது வேறு விதமாக குறிப்பிடப்பட்ட வணிக நிறுவனங்கள், தயாரிப்புகள், செயல்முறைகள், வணிகச் சின்னம், சேவைக்கான வணிகச் சின்னம், அல்லது சேவைகளுக்கான எந்தவொரு குறிப்பும், அவற்றை அங்கீகரிப்பதாகவோ, ஒப்புதல், பரிந்துரை அல்லது ஆதரவைக் கொண்டிருப்பதாகவோ குறிக்காது.

இந்த ஆவணம் TLP:CLEAR எனக் குறிக்கப்பட்டுள்ளது. வெளிப்படுத்துவது மட்டுப்படுத்தப்படவில்லை. பொது தளங்களில் வெளியிடுவதற்குப் பொருந்தக்கூடிய விதிகள் மற்றும் நடைமுறைகளுக்கு இணங்க, தகவல் குறைந்தபட்ச அல்லது தவறாகப் பயன்படுத்தப்படுவதற்கான எதிர்பார்க்கக்கூடிய ஆபத்தைக் கொண்டிருக்கும் போது TLP:CLEAR ஐ ஆதாரங்கள் பயன்படுத்தலாம். நிலையான பதிப்புரிமை விதிகளுக்கு உட்பட்டு, TLP:CLEAR தகவல் கட்டுப்பாடு இல்லாமல் விநியோகிக்கப்படலாம். போக்குவரத்து விளக்கு நெறிமுறை பற்றிய கூடுதல் தகவலுக்கு, cisa.gov/tlp ஐப் பார்க்கவும்

MITRE ATT&CK – இதுவரை அறியப்பட்ட APT40 உளவுத் தொழில்நுட்பம்

புலனாய்வு (TA0043)	
பாதிக்கப்பட்டவருக்கு சொந்தமான வலைத் தளங்களைத் தேடுங்கள் (T1594)	பாதிக்கப்பட்டவரின் அடையாளத் தகவலை சேகரிக்கவும்: நற்சான்றிதழ்கள் (T1589.001)
செயல்மிகு நோட்டமிடல்: பாதிப்புக்குள்ளாகுமா என நோட்டமிடல் (T1595.002)	பாதிக்கப்பட்ட ஹோஸ்ட் தகவலை சேகரிக்கவும் (T1592)
திறந்த தேடல் வலைத்தளங்கள் / களங்கள்: தேடல் இயந்திரங்கள் (T1593.002)	பாதிக்கப்பட்ட நெட்வொர்க் தகவலை சேகரிக்கவும்: Domain பண்புகள் (T1590.001)
பாதிக்கப்பட்டவரின் அடையாளத் தகவலை சேகரிக்கவும்: மின்னஞ்சல் முகவரிகள் (T1589.002)	

வள மேம்பாடு (TA0042)	
உள்கட்டமைப்பைப் பெறுதல்: Domains (T1583.001)	உள்கட்டமைப்பைப் பெறுதல் (T1583)
உள்கட்டமைப்பைப் பெறுதல்: DNS Server (T1583.002)	கணக்குகளை சமரசம் செய் (T1586)
திறன்களை வளர்த்துக் கொள்ளுங்கள்: குறியீடு கையொப்பமிடும் சான்றிதழ்கள் (T1587.002)	உள்கட்டமைப்பை சமரசம் செய் (T1584)
திறன்களை வளர்த்துக் கொள்ளுங்கள்: டிஜிட்டல் சான்றிதழ்கள் (T1587.003)	திறன்களை வளர்த்துக் கொள்ளுங்கள்: தீம்பொருள் (T1587.001)
திறன்களைப் பெறுங்கள்: குறியீடு கையொப்பமிடும் சான்றிதழ்கள் (T1588.003)	கணக்குகளை நிறுவுதல்: கிளவுட் கணக்குகள் (T1585.003)
உள்கட்டமைப்பை சமரசம் செய்: நெட்வொர்க் சாதனங்கள் (T1584.008)	திறன்களைப் பெறுங்கள்: டிஜிட்டல் சான்றிதழ்கள் (T1588.004)

ஆரம்ப அணுகல் (TA0001)	
செல்லுபடியாகும் கணக்குகள் (T1078)	Phishing எனப்படும் மின் தூண்டிலிடல் (T1566)
செல்லுபடியாகும் கணக்குகள்: Default Accounts (T1078.001)	Phishing எனப்படும் மின் தூண்டிலிடல் Spearphishing Attachment (T1566.001)
செல்லுபடியாகும் கணக்குகள்: Domain கணக்குகள் (T1078.002)	Phishing எனப்படும் மின் தூண்டிலிடல் மின் தூண்டிலிடல் இணைப்பு (T1566.002)
வெளிப்புற தொலைநிலை சேவைகள் (T1133)	பொதுமக்கள் அணுகக்கூடிய செயலியை சுரண்டல் (T1190)
சமரசம் (T1189)	

நிறைவேற்றுதல் (TA0002)	
Windows மேலாண்மை கருவி (T1047)	கட்டளை மற்றும் ஸ்கிரிப்டிங் மொழிமாற்றி: Python (T1059.006)
திட்டமிடப்பட்ட பணி/வேலை: At (T1053.002)	கட்டளை மற்றும் ஸ்கிரிப்டிங் மொழிமாற்றி: JavaScript (T1059.007)
திட்டமிடப்பட்ட பணி/வேலை: திட்டமிடப்பட்ட பணி (T1053.005)	அதற்கே உரித்தான செயலி நிரலாக்க இடைமுகம் (T1106)
கட்டளை மற்றும் ஸ்கிரிப்டிங் மொழிமாற்றி (T1059)	செயல்முறைகளுக்கு இடையேயான தொடர்பு (T1559)
கட்டளை மற்றும் ஸ்கிரிப்டிங் மொழிமாற்றி: Windows Command Shell (T1059.003)	கணினி சேவைகள்: சேவை செயல்படுத்தல் (T1569.002)
கட்டளை மற்றும் ஸ்கிரிப்டிங் மொழிமாற்றி: PowerShell (T1059.001)	வாடிக்கையாளர் நிறைவேற்றுதலை சுரண்டல் (T1203)
கட்டளை மற்றும் ஸ்கிரிப்டிங் மொழிமாற்றி: Visual Basic (T1059.005)	பயனர் நிறைவேற்றுதல்: தீங்கிழைக்கும் கோப்பு (T1204.002)
கட்டளை மற்றும் ஸ்கிரிப்டிங் மொழிமாற்றி: Unix Shell (T1059.004)	கட்டளை மற்றும் ஸ்கிரிப்டிங் மொழிமாற்றி: Apple Script (T1059.002)
திட்டமிடப்பட்ட பணி/வேலை: Cron (T1053.003)	மென்பொருள் வரிசைப்படுத்தல் கருவிகள் (T1072)

நிலைத்தன்மை (TA0003)	
செல்லுபடியாகும் கணக்குகள் (T1078)	சேவையக மென்பொருள் உபகரணம்: Web Shell (T1505.003)
Office செயலியின் தொடக்கம்: Office Template Macroக்கள் (T1137.001)	கணினி செயல்முறையை உருவாக்கவும் அல்லது மாற்றவும்: Windows Service (T1543.003)
திட்டமிடப்பட்ட பணி/வேலை: At (T1053.002)	துவக்க அல்லது உள்நுழைவு தானியங்கு தொடக்கம் செயல்படுத்தல்: Registry Run Keys / தொடக்க கோப்புறை (T1547.001)
திட்டமிடப்பட்ட பணி/வேலை: திட்டமிடப்பட்ட பணி (T1053.005)	துவக்க அல்லது உள்நுழைவு தானியங்கு தொடக்கம் செயல்படுத்தல்: குறுக்குவழி மாற்றம் (T1547.009)
வெளிப்புற தொலைநிலை சேவைகள் (T1133)	நிறைவேற்றுதலைக் கடத்தல்: DLL தேடல் படிமுறையைக் கடத்தல் (T1574.001)
திட்டமிடப்பட்ட பணி/வேலை: Cron (T1053.003)	நிறைவேற்றுதலைக் கடத்தல்: DLL பக்கவாட்டுக்கு ஏற்றுதல் (T1574.002)
கணக்கு கையாளுதல் (T1098)	செல்லுபடியாகும் கணக்குகள்: மேகக் கணிமை கணக்குகள் (T1078.004)
செல்லுபடியாகும் கணக்குகள்: Domain கணக்குகள் (T1078.002)	

சிறப்புரிமை வளர் நிலை (TA0004)	
திட்டமிடப்பட்ட பணி/வேலை: At (T1053.002)	கணினி செயல்முறையை உருவாக்கவும் அல்லது மாற்றவும்: Windows Service (T1543.003)
திட்டமிடப்பட்ட பணி/வேலை: திட்டமிடப்பட்ட பணி (T1053.005)	துவக்க அல்லது உள்நுழைவு தானியங்கு தொடக்கம் செயல்படுத்தல்: Registry Run Keys / தொடக்க கோப்புறை (T1547.001)
செயல்முறை ஊடுருவல்: நிறைவேற்றும் இழை கடத்தல் (T1055.003)	துவக்க அல்லது உள்நுழைவு தானியங்கு தொடக்கம் செயல்படுத்தல்: குறுக்குவழி மாற்றம் (T1547.009)
செயல்முறை ஊடுருவல்: வெற்று செயல்முறை (T1055.012)	நிறைவேற்றுதலைக் கடத்தல்: DLL தேடல் படிமுறையைக் கடத்தல் (T1574.001)

சிறப்புரிமை வளர் நிலை (TA0004)	
செல்லுபடியாகும் கணக்குகள்: Domain கணக்குகள் (T1078.002)	சிறப்புரிமை மேம்படுத்தலுக்கான சுரண்டல் (T1068)
அணுகல் Token கையாளுதல்: Token ஆள்மாறாட்டம் / திருட்டு (T1134.001)	நிகழ்வு தூண்டப்பட்ட நிறைவேற்றுதல்: Unix Shell உள்ளமைவு மாற்றம் (T1546.004)
செயல்முறை ஊடுருவல்: Dynamic-link Library ஊடுருவல் (T1055.001)	செல்லுபடியாகும் கணக்குகள்: Domain கணக்குகள் (T1078.002)
செல்லுபடியாகும் கணக்குகள்: குறிப்பிட்ட சாதன கணக்குகள் (T1078.003)	

பாதுகாப்பு தவிர்ப்பு (TA0005)	
Rootkit (T1014)	மறைமுக கட்டளை செயல்படுத்தல் (T1202)
குழப்பமான கோப்புகள் அல்லது தகவல் (T1027)	System Binary Proxy செயல்படுத்தல்: Mshta (T1218.005)
குழப்பமான கோப்புகள் அல்லது தகவல்: Software Packing (T1027.002)	System Binary Proxy செயல்படுத்தல்: Regsvr32 (T1218.010)
குழப்பமான கோப்புகள் அல்லது தகவல்: Steganography (T1027.003)	Subvert Trust Controls: Code Signing (T1553.002)
குழப்பமான கோப்புகள் அல்லது தகவல்: வழங்கிய பின்னர் தொகுத்தல் (T1027.004)	கோப்பு மற்றும் கோப்பக அனுமதிகள் மாற்றங்கள்: Linux மற்றும் Mac கோப்பு மற்றும் கோப்பக அனுமதிகள் மாற்றம் (T1222.002)
மாறுவேடம் போடுதல்: சட்ட பூர்வமான பெயர் அல்லது இருப்பிடத்தை சரி பார் (T1036.005)	மெய்நிகராக்கம்/ Sandbox ஏய்ப்பு: கணினி சோதனைகள் (T1497.001)
செயல்முறை உட்செலுத்துதல்: நிறைவேற்றும் இழை கடத்தல் (T1055.003)	மாறுவேடம் போடுதல் (T1036)
பிரதிபலிப்பு குறியீடு ஏற்றுதல் (T1620)	சேதப்படுத்தும் பாதுகாப்புகள்: கணினி தீச்சுவரை முடக்குதல் அல்லது மாற்றியமைத்தல் (T1562.004)
செயல்முறை உட்செலுத்துதல்: வெற்று செயல்முறை (T1055.012)	பொருட்களை மறை: மறைக்கப்பட்ட கோப்புகள் மற்றும் கோப்பகங்கள் (T1564.001)
காட்டி நீக்கம்: கோப்பு நீக்கம் (T1070.004)	பொருட்களை மறை: மறைக்கப்பட்ட Window (T1564.003)
காட்டி நீக்கம்: நேர பதிவு (T1070.006)	நிறைவேற்றுதலைக் கடத்தல்: DLL தேடல் படிமுறையைக் கடத்தல் (T1574.001)
காட்டி நீக்கம்: Windows event பதிவுகளை அழி (T1070.001)	நிறைவேற்றுதலைக் கடத்தல்: DLL பக்க ஏற்றுதல் (T1574.002)
பதிவேட்டை மாற்றுதல் (T1112)	வலை சேவை (T1102)
கோப்புகள் அல்லது தகவல்களை குழப்பமில்லாமல் செய்யவும் -Deobfuscate/Decode (T1140)	மாறுவேடம் போடுதல்: முகமூடிப் பணி அல்லது சேவை (T1036.004)
பழுதடைந்த பாதுகாப்புகள் (T1562)	

சான்றிதழ் அணுகல் (TA0006)	
OSசான்றிதழை எறிதல்: LSASS நினைவகம் (T1003.001)	பாதுகாப்பற்ற நற்சான்றிதழ்கள்: கோப்புகளில் உள்ள நற்சான்றிதழ்கள் (T1552.001)
OSசான்றிதழை எறிதல்: NTDS (T1003.003)	Brute Force: கடவுச்சொல் யூகம் (T1110.001)
நெட்வொர்க்கை மோப்பம் விடுதல் (T1040)	கட்டாய அங்கீகாரம் (T1187)
கடவுச்சொல் கடைகளிலிருந்து நற்சான்றிதழ்கள்: Keychain (T1555.001)	Kerberos டிக்கெட்டுகளைத் திருடுதல் அல்லது போலியாக உருவாக்குதல்: Kerberoasting (T1558.003)

சான்றிதழ் அணுகல் (TA0006)	
உள்ளீடு பிடிப்பு: Keylogging (T1056.001)	பன்முக அங்கீகாரத்தை இடைமறித்தல் (T1111)
வலை அமர்வு cookieயைத் திருடு (T1539)	பயன்பாட்டு அணுகல் tokenனைத் திருடு (T1528)
நற்சான்றிதழ் அணுகலுக்கான சுரண்டல் (T1212)	Brute Force: கடவுச்சொல் விரிசல் (T1110.002)
உள்ளீட்டைக் கைப்படுத்தல்: இணைய முகப்பைக் கைப்பற்றல் (T1056.003)	OSசான்றிதழை எறிதல்: DCSync (T1003.006)
கடவுச்சொல் கடைகளிலிருந்து நற்சான்றிதழ்கள் (T1555)	கடவுச்சொல் கடைகளிலிருந்து நற்சான்றிதழ்கள்: வலை உலாவிகளிலிருந்து நற்சான்றிதழ்கள் (T1555.003)

கண்டுபிடிப்பு (TA0007)	
கணினி சேவை கண்டுபிடிப்பு (T1007)	கணினி தகவல் கண்டுபிடிப்பு (T1082)
பயன்பாட்டு Window கண்டுபிடிப்பு (T1010)	கணக்கு கண்டுபிடிப்பு: உள்ளூர் கணக்கு (T1087.001)
வினவல் பதிவேடு (T1012)	System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®
கோப்பு மற்றும் கோப்பக கண்டுபிடிப்பு (T1083)	கணினி அமைப்பு நேர கண்டுபிடிப்பு (T1124)
நெட்வொர்க் சேவை கண்டுபிடிப்பு (T1046)	கணினி அமைப்பு உரிமையாளர்/பயனர் கண்டுபிடிப்பு (T1033)
தொலைதூர கணினி அமைப்பு கண்டுபிடிப்பு (T1018)	Domain Trust கண்டுபிடிப்பு (T1482)
கணக்கு கண்டுபிடிப்பு: மின்னஞ்சல் கணக்கு (T1087.003)	கணக்கு கண்டுபிடிப்பு: Domain கணக்கு (T1087.002)
கணினி அமைப்பு நெட்வொர்க் இணைப்புகள் கண்டுபிடிப்பு (T1049)	மெய்நிகராக்கம்/ Sandbox ஏய்ப்பு: கணினி அமைப்பு சரிபார்ப்புகள் (T1497.001)
செயல்முறை கண்டுபிடிப்பு (T1057)	மென்பொருள் கண்டுபிடிப்பு (T1518)
அனுமதி குழுக்கள் கண்டுபிடிப்பு: Domain குழுக்கள் (T1069.002)	Network Share Discovery, Technique T1135 - Enterprise | MITRE ATT&CK®
கணினி நெட்வொர்க் உள்ளமைவு கண்டுபிடிப்பு: இணைய இணைப்பு கண்டுபிடிப்பு (T1016.001)	

பக்கவாட்டு இயக்கம் (TA0008)	
தொலை சேவைகள்: Remote Desktop நெறிமுறை (T1021.001)	தொலை சேவைகள் (T1021)
தொலை சேவைகள்: SMB/Windows நிர்வாகப் பங்குகள் (T1021.002)	மாற்று அங்கீகாரப் பொருளைப் பயன்படுத்தவும்: டிக்கெட்டை அனுப்பு (T1550.003)
தொலை சேவைகள்: Windows Remote Management (T1021.006)	பக்கவாட்டு கருவி பரிமாற்றம் (T1570)

சேகரிப்பு (TA0009)	
உள்ளூர் அமைப்பிலிருந்து தரவு (T1005)	சேகரிக்கப்பட்ட தரவை காப்பகப்படுத்தவும்: நூலகம் வழியாக காப்பகம் (T1560.002)
நெட்வொர்க் பகிரப்பட்ட இயக்ககத்திலிருந்து தரவு (T1039)	மின்னஞ்சல் சேகரிப்பு: தொலை மின்னஞ்சல் சேகரிப்பு (T1114.002)

சேகரிப்பு (TA0009)	
உள்ளீட்டைக் கைப்படுத்தல்: Keylogging (T1056.001)	Clipboard தரவு (T1115)
தானியங்கி சேகரிப்பு (T1119)	தகவல் களஞ்சியங்களிலிருந்து தரவு (T1213)
உள்ளீட்டைக் கைப்படுத்தல்: இணைய முகப்பைக் கைப்பற்றல் (T1056.003)	நிலைப் படுத்தப்பட்ட தரவு: தொலைநிலை தரவு நிலைப் படுத்தல் (T1074.002)
நிலைப் படுத்தப்பட்ட தரவு: சாதனத்தில் தரவு நிலைப் படுத்தல் (T1074.001)	சேகரிக்கப்பட்ட தரவை காப்பகம் (T1560)
மின்னஞ்சல் சேகரிப்பு (T1114)	

வெளியேற்றம் (TA0010)	
C2 சேனல் வழியாக வெளியேற்றம் (T1041)	மாற்று நெறிமுறை வழியாக வெளியேற்றம்: சமச்சீரற்ற மறைகுறியாக்கப்பட்ட C2 அல்லாத நெறிமுறை வழியாக வெளியேற்றம் (T1048.002)
மாற்று நெறிமுறை வழியாக வெளியேற்றம் (T1048)	இணைய சேவை மூலம் வெளியேற்றம்: மேக கணிமைக்கு வெளியேற்றம் (T1567.002)

கட்டளை மற்றும் கட்டுப்பாடு (TA0011)	
தரவு தெளிவின்மை: நெறிமுறை ஆள்மாறாட்டம் (T1001.003)	இணைய சேவை: Dead Drop Resolver (T1102.001)
பொதுவாக பயன்படுத்தப்படும் போர்ட் (T1043)	இணைய சேவை: ஒரு வழி தொடர்பு (T1102.003)
பயன்பாட்டு அடுக்கு நெறிமுறை: வலை நெறிமுறைகள் (T1071.001)	நுழைவு கருவி பரிமாற்றம் (T1105)
பயன்பாட்டு அடுக்கு நெறிமுறை: கோப்புப் பரிமாற்ற நெறிமுறைகள் (T1071.002)	பதிலாள்: உள்ளக பதிலாள் (T1090.001)
பதிலாள்: வெளிப்புற பதிலாள் (T1090.002)	தரமற்ற போர்ட் (T1571)
பதிலாள்: பலமுறை தாவும் பதிலாள் (T1090.003)	நெறிமுறை சுரங்கப்பாதை (T1572)
வலை சேவை: இருவழி தொடர்பு (T1102.002)	குறியாக்கப்பட்ட சேனல் (T1573)
குறியாக்கப்பட்ட சேனல்: சமச்சீரற்ற குறியாக்கவியல் (T1573.002)	நுழைவு கருவி பரிமாற்றம் (T1105)
பதிலாள், உத்தி T1090 - நிறுவனம் | MITER ATT&CK®	

தாக்கம் (TA0040)	
சேவை நிறுத்தம் (T1489)	வட்டு துடைப்பு(Disk Wipe) (T1561)
கணினி பணி நிறுத்தம்/மறுதொடக்கம் (T1529)	வள கடத்தல் (T1496)

குறிப்புகள்

பொறுப்புத் துறப்பு

இந்த வழிகாட்டியில் கூறப்பட்டுள்ள விடயங்கள் பொதுவானவை. அவை சட்ட ஆலோசனையாகக் கருதப்படக்கூடாது. மேலும், எந்தவொரு குறிப்பிட்ட சூழ்நிலையில் அல்லது அவசரகால சூழ்நிலையில் நேரடியாக உதவும் என்று நம்பக்கூடாது. எந்தவொரு முக்கியமான விடயத்திலும், உங்கள் சொந்த சூழ்நிலைகள் தொடர்பாக தகுந்த சுயாதீனமான தொழில்முறை ஆலோசனையை நீங்கள் நாட வேண்டும்.

இந்த வழிகாட்டியில் உள்ள தகவல்களை நம்பியதன் விளைவாக ஏற்படும் எந்தவொரு சேதம், இழப்பு அல்லது செலவுக்கும் ஆஸ்திரேலிய காமன்வெல்த் அரசு எந்த பொறுப்பையும் ஏற்காது.

பதிப்புரிமை

ஆஸ்திரேலிய அரசின் Coat of Arms வகை இலச்சினையின் பயன்பாடு

ஆஸ்திரேலிய அரசின் Coat of Arms வகை இலச்சினை எந்தெந்த விதிமுறைகளின் கீழ் பயன்படுத்தப்படலாம் என்பது பிரதமர் துறை மற்றும் அமைச்சரவையின் Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au என்ற இணையதளத்தில் விரிவாக உள்ளது.

மேலும் தகவலுக்கு அல்லது இணைய பாதுகாப்பு முறியடிக்கப்பட்ட நிகழ்வு குறித்துப் புகாரளிக்க, எங்களைத் தொடர்பு கொள்ளவும்:

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

இந்த எண்ணை ஆஸ்திரேலியாவின் உள்ளகப் பயன்பாட்டிற்கு மட்டுமே பயன்படுத்தலாம்.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre