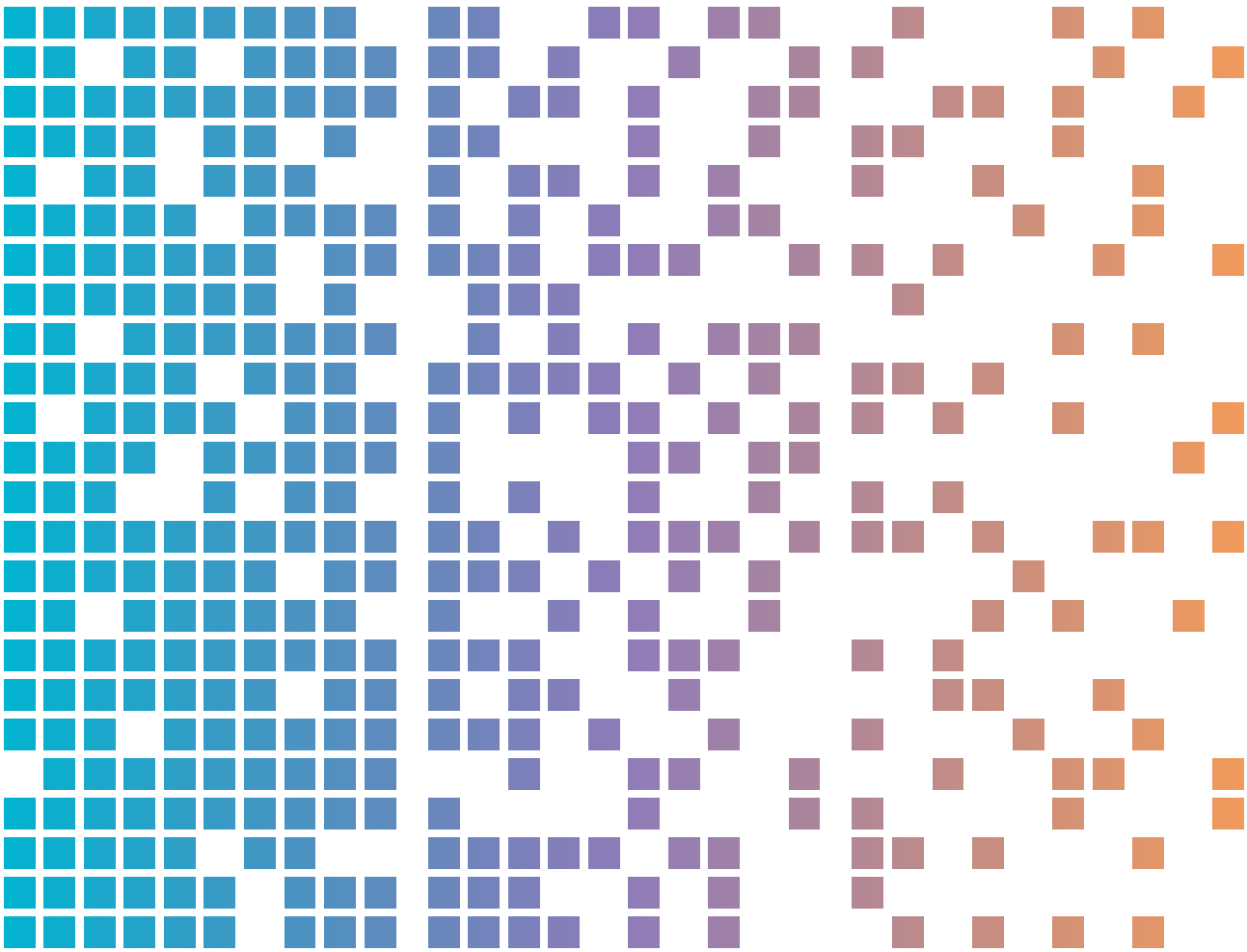
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

அமைதியான கொள்ளை: சைபர் குற்றவாளிகள் நிறுவனங்களின் நெட்வொர்க்குகளை சமரசம் செய்ய தகவல் திருட்டு தீம்பொருளைப் பயன்படுத்துகின்றனர்



உள்ளடக்கத்தின் சிக்கல் தன்மை
நடுத்தரமான

பொருளடக்கம்

சூழ்நிலை

பயனர் நற்சான்றிதழ்கள் மற்றும் கணினி தகவல்களை, தகவல் திருடும் தீம்பொருள் திருடுகிறது. பண ஆதாயத்திற்காக சைபர் திருடர்கள் இதைப் பயன்படுத்துகிறார்கள். ஆஸ்திரேலியா உட்பட உலகெங்கிலும் உள்ள பல நிறுவனங்கள் மற்றும் துறைகளுக்கு எதிரான சைபர் தாக்குதல்களில் தகவல் திருடும் தீம்பொருள் ஈடுபடுத்தப்பட்டுள்ளது கண்டுபிடிக்கப்பட்டுள்ளது. தகவல் திருடும் தீம்பொருள் குறித்த இணைய பாதுகாப்பு வழிகாட்டுதலை இந்த வெளியீடு வாசகர்களுக்கு வழங்குகிறது. நிறுவனங்கள் மற்றும் அவற்றின் ஊழியர்களுக்கு, அச்சுறுத்தல் செயல்பாட்டைக் குறைப்பதற்கான ஆலோசனை இதில் அடங்கும்.

முக்கிய கருத்துகள்

- தகவல் திருடர்கள் (info stealers) என்றும் அழைக்கப்படும் தகவல் திருட்டு தீம்பொருள், பாதிக்கப்பட்டவரின் சாதனத்திலிருந்து தகவல்களைச் சேகரிக்க வடிவமைக்கப்பட்ட ஒரு வகை தீம்பொருள் ஆகும். பயனர் பெயர்கள் மற்றும் கடவுச் சொற்கள், credit card விவரங்கள், cryptocurrency பணப்பைகள், கணினியிலுள்ள கோப்புகள் மற்றும் cookies, உலாவி தரவுகள், பயனர் வரலாறு மற்றும் சமரசம் செய்யப்பட்ட கணினிகளிலிருந்து autofill என்ற தானாக நிரப்பும் படிவங்கள் உள்ளிட்ட பலவற்றை இது உள்ளடக்கும்.
- பாதிக்கப்பட்ட பயனரின் நிறுவனம், அதன் வாடிக்கையாளர்கள் மற்றும் தொடர்புடைய பிற நிறுவனங்களின் சாதனங்களுக்கான ஆரம்ப அணுகலைப் பெற, திருடப்பட்ட பயனர் நற்சான்றிதழ்களை விலை கொடுத்து வாங்கி, பயன்படுத்தவும் சைபர் குற்றவாளிகள் முற்படலாம். Ransomware - தரவைத் திருடி, மிரட்டி, பணம் பறிக்க உதவும் மென்பொருள், மிரட்டி பணம் பறித்தல், வணிக நிறுவனத்தின் மின்னஞ்சல் சமரசம் செய்யப்படுதல் மற்றும் அறிவு சார் சொத்து திருட்டு ஆகியவை இந்த நிறுவனங்களின் அடுத்தடுத்த தாக்கங்களில் அடங்கலாம்.
- சமரசம் செய்யப்பட்ட தனிப்பட்ட சாதனங்களிலிருந்து பணியிட சாதனங்களை ஊழியர்கள் அணுகும் போது நிறுவனத்தின் நெட்வொர்க் மீறல்கள் நடப்பதை ஆஸ்திரேலிய சிக்னல்கள் இயக்குநரகத்தின் ஆஸ்திரேலிய சைபர் பாதுகாப்பு மையம் (ASDயின் ACSC) அடையாளம் கண்டுள்ளது. பல சந்தர்ப்பங்களில், திருடப்பட்ட செல்லுபடியாகும் பயனர் நற் சான்றிதழ்களைப் பயன்படுத்தி சைபர் குற்றவாளிகள் நிறுவனத்தின் நெட்வொர்க்குகளுக்கான ஆரம்ப அணுகலைப் பெற்றனர். சலுகை பெற்ற பயனர் கணக்குகளை சைபர் குற்றவாளிகள் வெற்றிகரமாக அணுகிய பின்னர், மேலதிகமான சமரசங்கள் பொதுவாக நிகழ்ந்தன என்பதை எங்கள் விசாரணைகள் காட்டின.
- ஊழியர்கள், ஒப்பந்ததாரர்கள், நிர்வகிக்கப்படும் சேவை வழங்குநர்கள் அல்லது பிற நிறுவனங்கள்(அவர்களது சொந்த சாதனத்தைப் பயன்படுத்தினாலும்) தங்கள் நெட்வொர்க்கை தொலைவிலிருந்து அணுக உதவும் நிறுவனங்கள், தகவல் திருடர்களின் அபாயங்கள் குறித்து விழிப்புடன் இருக்க வேண்டும் மற்றும் இந்த அச்சுறுத்தலில் இருந்து தங்களைப் பாதுகாத்துக் கொள்ள வேண்டும். Phishing எனப்படும் மின்-தூண்டிலிடல் மின்னஞ்சல்கள், திருட்டு மென்பொருள் பதிவிறக்கங்கள், தேடு பொறி உகப்பாக்க நுட்பங்கள் (SEO), தீங்கிழைக்கும் விளம்பரங்கள் அல்லது சமூக ஊடக தளங்களில் இடுகையிடப்பட்ட தீங்கிழைக்கும் இணைப்புகள் உள்ளிட்ட பரந்த அளவிலான நுட்பங்களைப் பயன்படுத்தி, சைபர் குற்றவாளிகள் பாதிக்கப்பட்ட சாதனங்களில் தகவல் திருடர்கள் (info stealers) என்றும் அழைக்கப்படும் தகவல் திருட்டு தீம்பொருளை பதிவேற்றுகின்றனர். பொதுவாக, பயனர் நடத்தை மற்றும் குறைக்கப்பட்ட பாதுகாப்புக் கட்டுப்பாடுகள் காரணமாக, வேலை மற்றும் தனிப்பட்ட நோக்கங்களுக்காகப் பயன்படுத்தப்படும் சாதனங்கள் இந்த நுட்பங்கள் மூலம் தீம்பொருட்கள் தொற்றுவதற்கான அதிக ஆபத்தில் உள்ளன.
- சைபர் குற்றவாளிகளுக்கு, குறிப்பாக நுழைவு நிலை சைபர் குற்றவாளிகள் மற்றும் குறைந்த தொழில்நுட்ப நிபுணத்துவம் உள்ளவர்கள் சைபர் குற்றச் செயற்பாட்டைப் பணமாக்குவதற்கு, தகவல் திருடும் தீம்பொருட்கள் ஒரு கவர்ச்சிகரமான வழியை வழங்குகின்றன. தகவல் திருடும் தீம்பொருட்களை ஒரு சேவையாக, (Malware-as-a-Service அல்லது MaaS) என்ற திட்டத்தின் கீழ் சில சைபர் குற்றவாளிகள் சந்தைப்படுத்துவார்கள், அவற்றின் பயன்பாட்டிற்கு மாதாந்தர சந்தா கட்டணத்தை வசூலிப்பார்கள்.

பின்னணி

தகவல் திருடர்கள் (info stealers) என்றும் அழைக்கப்படும் தகவல் திருட்டு தீம்பொருளை சைபர் குற்றவாளிகள் பயன்படுத்துவது ஆஸ்திரேலிய நிறுவனங்களின் பாதுகாப்பு மற்றும் நல்வாழ்வுக்கு அச்சுறுத்தலாக இருக்கிறது. பயனர் நற்சான்றிதழ்களை சேகரிக்க சைபர் குற்றவாளிகள் தகவல் திருட்டு தொற்றுகளைப் பயன்படுத்துவதால், பொதுவாக முக்கிய இணைய பாதுகாப்பு சம்பவங்களுக்கு அது முன்னோடி நடவடிக்கைகளாக உள்ளன. இப்படிப் பெறப்பட்ட பயனர் நற்சான்றிதழ்கள், குறிப்பாக இணையத்துடன் இணைக்கப்பட்ட கணினி அமைப்புகள் மற்றும் தொலைநிலை சேவைகள் அல்லது சலுகை பெற்ற கணக்குகளுக்கான அணுகலை வழங்கும் பயனர் சான்றிதழ்கள், பின்னர் பெரு நிறுவன அமைப்புகள் மற்றும் அவற்றின் தரவுகளில் ஆரம்ப அணுகலை ஏற்படுத்த பயன்படுத்தப்படுகின்றன.

குறிப்பு: திருடப்பட்ட பயனர் நற்சான்றிதழ்களை வாங்கி சரிபார்ப்பதன் மூலம், சைபர் குற்றங்கள் செய்பவர்களிடையே ஆரம்ப அணுகல் தரகர்கள் ஒரு தனி பாத்திரத்தை வகிக்கின்றனர். பின்னர், பிரபலமான நிறுவனங்களுக்கான உயர்தர பயனர் நற்சான்றிதழ்களை சைபர் குற்றவாளிகளுக்கு அவர்கள் ஏலம் விடுகிறார்கள். பெரு நிறுவன நெட்வொர்க்கை சுரண்டுவதற்கு பயனர் நற்சான்றிதழ்களை சைபர் குற்றவாளிகள் பயன்படுத்துவார்கள்.

திருடப்பட்ட, செல்லுபடியாகும் பயனர் நற்சான்றிதழ்கள் சைபர் குற்றவாளிகளுக்கு மிகவும் மதிப்புமிக்கவை. ஏனெனில், அவை நிறுவனங்களின் நெட்வொர்க்குகள் மற்றும் நிறுவன கட்டமைப்புகளுக்கான ஆரம்ப அணுகலைத் துரிதப்படுத்துகின்றன. திருடப்பட்ட செல்லுபடியாகும் பயனர் நற்சான்றிதழ்களுடன், சைபர் குற்றவாளிகள் பல பொதுவான பாதுகாப்பு தந்திரோபாயங்களையும் நுட்பங்களையும் புறக்கணிக்க முடியும், அவற்றுள்:

- ஒரு இலக்கை அடையாளம் காணுதல் மற்றும் ஆய்வு செய்தல்
- இலக்கு வைக்கப்பட்ட நெட்வொர்க்கில் பாதிக்கப்படக்கூடிய பகுதிகளைக் கணக்கிடுதல்
- ஆரம்ப அணுகலுக்கான திசையன்களை (vectors) உருவாக்குதல், அவை:
  - Phishing எனப்படும் மின்-தூண்டிலிடல் கருவிகள்
  - மென்பொருளில் உள்ள பாதுகாப்பற்ற தன்மைகள்
  - தொலைவிலிருந்து கணினியை அணுக வழி செய்யும் Remote Desktop Protocol (RDP) மற்றும் Virtual Private Network எனப்படும் மெய் நிகர் தனியார் நெட்வொர்க் (VPN) ஆகிய சேவைகளை இலக்கு வைத்தல்
  - Brute-force என அழைக்கப்படும் முரட்டுத்தனமான தாக்குதல் அல்லது முழுமையான விசை தேடல் என்ற குறியாக்க பகுப்பாய்வுத் தாக்குதலை நடத்தி பல சாத்தியமான விசைகள் அல்லது கடவுச் சொற்களை யூகம் செய்தல்.

இதை செய்வதற்கு நேர முதலீடு மற்றும் தொழில்நுட்ப திறன் தேவைப்படுகிறது, சில சைபர் குற்றவாளிகளுக்கு இது ஒரு தடையாக உள்ளது. குறிப்பாக, நிறுவனத்தின் நெட்வொர்க் பாதுகாப்பு கட்டமைப்புகளை ஊடுருவ முடியாத சைபர் குற்றவாளிகள் தகவல் திருட்டு தீம்பொருளிலிருந்து நேரடியாக பயனடையலாம், ஏனெனில் இந்த தீம்பொருள், நிறுவனத்தின் நெட்வொர்க்குகளுக்கு விரைவான மற்றும் எளிதான பயனர் நற்சான்றிதழ் அணுகலை வழங்க முடியும்.

தொலைவிலிருந்து கணினியை அணுக வழி உள்ள சில ஊழியர்கள், வேலை மற்றும் தனிப்பட்ட இணைய உலாவல் இரண்டிற்கும் ஒரே தனிப்பட்ட சாதனங்களைப் பயன்படுத்துகின்றனர். அவ்வாறு செய்யும்போது, ஊழியர்கள் தங்கள் பயனர் நற்சான்றிதழ்களை தங்கள் வலை உலாவிகளின் கடவுச் சொற்களை கணினியில் சேமித்து வைத்திருக்கலாம் மற்றும் autofill என்ற தானாக நிரப்பும் படிவங்கள் உள்ளிட்ட பலவற்றில் அவற்றை சேமித்து வைத்திருக்கலாம். தகவல் திருடும் தீம்பொருள், வலை உலாவியில் உள்ள அங்கீகார cookieக்கள் மற்றும் பிற தனிப்பட்ட தரவுடன் இந்த கடவுச் சொற்களைக் குறி வைக்கின்றனர்.

நிறுவனத்தின் சாதனங்களைப் போலன்றி, தனிப்பட்ட சாதனங்கள் எப்போதும் நிறுவன பாதுகாப்புக் கொள்கைகளை நடைமுறைப்படுத்துவதில்லை, இது நிறுவனங்களுக்கு அதிக ஆபத்தை ஏற்படுத்துகிறது. எடுத்துக்காட்டாக, திருட்டு மென்பொருளைப் பதிவிறக்குதல் மற்றும் அதிக ஆபத்துள்ள இணைய உலாவல் போன்ற நடவடிக்கைகளில் ஊழியர்கள் ஈடுபடலாம், இணைய அச்சுறுத்தல்கள் மற்றும் தீம்பொருள் தொற்றுகள் ஏற்படும் வாய்ப்புகளை அவர்கள் அதிகரிக்கலாம்.

தகவல் திருடுபவர்கள், அதை விநியோகிப்பவர்கள், ஆரம்ப அணுகல் தரகர்கள் மற்றும் ransomware துணை நிறுவனங்கள் இப்போது நிதி ஆதாயத்தால் இயக்கப்படும் சைபர் குற்றவாளிகள் கூட்ட அமைப்பின் முக்கிய பகுதியை உருவாக்குகின்றன. ஒரு தாக்குதலின் குறிப்பிட்ட கட்டங்களைக் குறி வைக்கும் திறன்களை நிபுணத்துவம் பெற்று சைபர் குற்றவாளிகள் வளர்த்துக் கொள்கிறார்கள். பின்னர் அவர்கள் அந்த திறனை மற்ற குற்றவியல் துணை நிறுவனங்களுக்கு ஒரு சேவையாக விற்கிறார்கள்.

அச்சுறுத்தல் நடவடிக்கை

உலகளாவிய அளவில் தகவல் திருடும் தீம்பொருளின் செயல்பாடு அதிகரிப்பதை ASDயின் ACSC கண்காணித்து வருகிறது, இது ஆஸ்திரேலிய நெட்வொர்க்குகளுக்கு வளர்ந்து வரும் அச்சுறுத்தலை முன்வைக்கிறது. சைபர் குற்றச் செயல்பாட்டிற்கு 2023 முழுவதும் தகவல் திருடும் தீம்பொருள் மிகவும் பிரபலமான தீம் பொருளாக இருந்தது என்று தொழில்துறை அறிக்கை சுட்டிக் காட்டுகிறது. திருடப்பட்ட தரவுகள் இருண்ட வலை சந்தைகளில் விற்பனைக்கு விடப்படும் அளவு, மற்றும் இந்தத் தரவைப் பயன்படுத்தும் ஆரம்ப அணுகல் தரகர் செயற்பாட்டின் எண்ணிக்கையும் அதிகரிக்கும் போக்கை பிரதிபலிக்கிறது. 2024ஆம் ஆண்டில் இது மேலும் துரிதப்படுத்தப்பட்டுள்ளது.

தகவல் திருட்டு கட்டமைப்பு

நிலை 1: தீம்பொருளைக் கையகப்படுத்தல்

தகவல் திருடும் தீம்பொருட்கள் வழக்கமாக சைபர் குற்றவாளி சந்தைகளில், MaaS அல்லது Stealer-as-a-Service என வழங்கப்படுகின்றன அல்லது மூலக் குறியீடாக விற்கப்படுகின்றன. MaaS என்பது ஒரு வணிக மாதிரியைக் குறிக்கிறது, இதன் மூலம் ஒரு தீம்பொருளை உருவாக்குபவர், தங்கள் தீங்கிழைக்கும் மென்பொருளுக்கான சந்தாவை இணைய அடிப்படையிலான தளம் வழியாக தனி நபர்களுக்கு விற்கிறார். முறையான Software-as-a-Service போன்று மென்பொருட்களை விற்பது போன்ற ஒரு கட்டமைப்பு இது. MaaS முறை மூலம் தீம்பொருட்கள் விற்கப்படுவதால், தீம்பொருளை விநியோகிக்கவும், சைபர் தாக்குதல்களில் பயன்படுத்த திருடப்பட்ட தகவல்களை சேகரிக்கவும் விரிவான தொழில்நுட்ப திறன்கள் இல்லாத நபர்களை இலகுவில் அனுமதிப்பதால் சைபர் குற்றவாளிகள் இதில் நுழைவதற்கான தடை குறைந்துள்ளது.

MaaS ஆக வழங்கப்படும் தகவல் திருடும் தீம்பொருட்கள் பொதுவாக ஒப்பீட்டளவில் மலிவான மாதாந்தர கட்டணத்திற்கு விளம்பரப் படுத்தப்படுகிறது, மேலும் சைபர் குற்றவாளிகளுக்கு தகவல் திருடும் 'தகவல் திரட்டு திரை' -dashboardற்கான அணுகலை வழங்குகிறது. தகவல் திருட்டு தீம்பொருளை உருவாக்க 'தகவல் திரட்டு திரை' உதவுகிறது. மேலும், திருடப்பட்ட தரவை ஒழுங்கமைக்கிறது மற்றும் சமரசம் செய்யப்பட்ட அமைப்புகளின் எண்ணிக்கையைக் கண்காணிக்கிறது. வைரஸ் தடுப்பு மென்பொருளால் கண்டறிவதைத் தவிர்ப்பதற்கும் சந்தாதாரர்களை ஈர்ப்பதற்கும் தக்க வைத்துக் கொள்வதற்கும் புதுப்பிப்புகள், கருவிகள் மற்றும் தொழில்நுட்ப ஆதரவை MaaS சேவை வழங்குநர்கள் வழங்குகிறார்கள். பல தகவல் திருடும் தீம்பொருட்கள் தரவுகளை வெளியே எடுத்த பின்னர் பாதிக்கப்பட்டவரின் சாதனத்திலிருந்து தங்களை நீக்கும் திறனைக் கொண்டுள்ளன.

நிலை 2: விநியோகம்

தகவல் திருடும் தீம்பொருட்களை விநியோகிக்கும் மற்றும் சமரசம் செய்யப்பட்ட சாதனங்களிலிருந்து தகவல்களைச் சேகரிக்கும் சைபர் குற்றவாளிகள் Traffers (traffic distributors) என்று அழைக்கப்படுகிறார்கள். பாதிக்கப்பட்டவர்களை தீங்கிழைக்கும் இணைப்புகளுக்கு Traffers வழி நடத்துகிறார்கள், பரந்த செயற்பாடுகளின் ஒரு பகுதியாக தகவல் திருடும் தீம் பொருட்களின் பரவலை எளிதாக்குகிறார்கள். பெரும்பாலான செயற்பாடுகள் கண்மூடித்தனமாக, சந்தர்ப்பவாத வகையில் தொற்று ஏற்படுத்துவதை நம்பியுள்ளன. இருப்பினும், சில செயற்பாடுகள் குறிப்பிட்ட தொழில்களுக்கு ஏற்ப வடிவமைக்கப்பட்டுள்ளன மற்றும் குறிப்பிட்ட பாதிக்கப்பட்டவர்களுக்கு எதிராக இலக்கு வைக்கப்பட்ட ஈட்டி முனையில் நடத்தப்படும் மின்-தூண்டிலிடல் நடவடிக்கையும் - அடங்கும். வாடிக்கையாளர் தேவைக்கு பதிலளிக்கும் வகையில் Traffers இந்த அதிக இலக்கு செயற்பாடுகளை நடத்துகிறார்கள்; உதாரணமாக, வாங்குபவர்கள் குறிப்பிட்ட உயர் மதிப்பு நிறுவனங்கள் அல்லது துறைகளுக்கான அணுகலைத் தேடும் போது.

பலவிதமான நுட்பங்களைப் பயன்படுத்தி, பாதிக்கப்பட்ட சாதனங்களுக்கு தகவல் திருடும் தீம்பொருட்களை Traffers பயன்படுத்துவார்கள், அவற்றுள்:

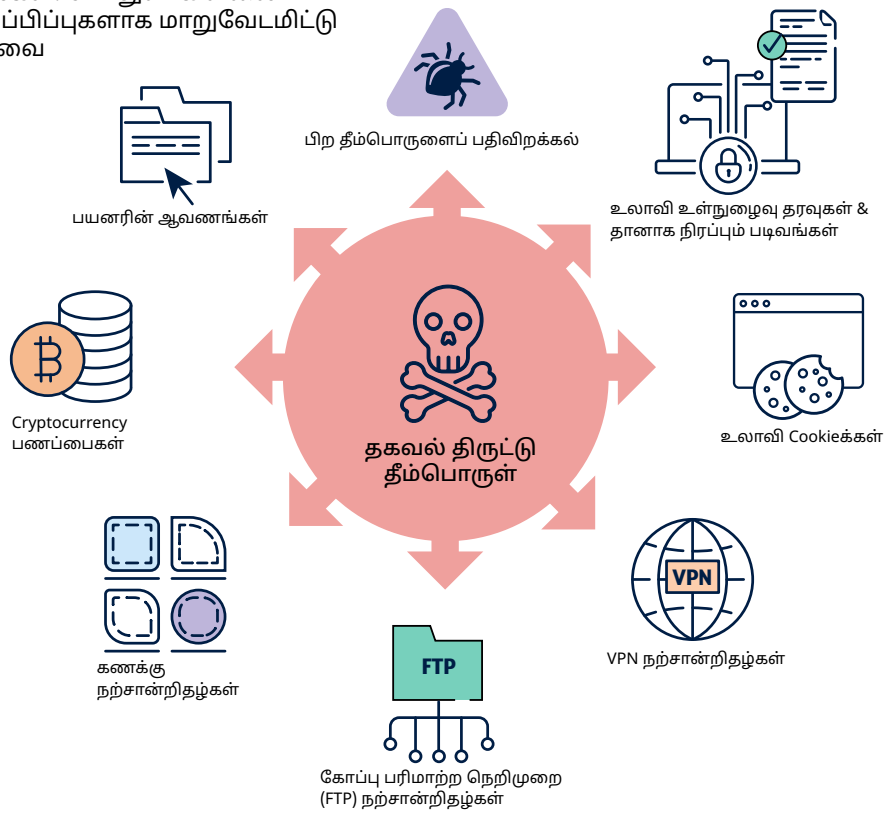
- **botnetகள்**: மின்-தூண்டிலிடல் செய்திகள் அல்லது தீம்பொருளை வழங்குவது போன்ற தீங்கிழைக்கும் செயல்களைச் செய்ய சைபர் குற்றவாளிகளால் கட்டுப்படுத்தப்படும் சமரசம் செய்யப்பட்ட கணினி அமைப்புகளின் நெட்வொர்க்குகள்

- **phishing எனப்படும் மின்-தூண்டிலிடல்:** சமூக ஊடகங்கள், மன்றங்கள் மற்றும் செய்தியிடல் பயன்பாடுகளில் மின்னஞ்சல்கள் அல்லது நேரடி செய்திகள் மூலம் ஏமாற்றி, முக்கியமான தகவல்களைப் பெறுவதற்கான முயற்சிகள்; இவை குறைந்த தடைகளுடன் சைபர் குற்றவாளிகள் குற்றச் செயலில் ஈடுபடுவதற்கான பொதுவான விநியோக முறைகள்:
  - இந்த மின்-தூண்டிலிடல் செய்திகள் பொதுவாக தீங்கிழைக்கும் கோப்புகளை மின்னஞ்சலுடன் இணைப்பதை விட, தீங்கிழைக்கும் இணைப்புகளைக் கொண்டுள்ளன.
- **தீங்கிழைக்கும் தேடல் முடிவுகள்:** தேடல் பொறி உகப்பாக்கம் (SEO) நுட்பங்கள் மூலம் வழங்கப்படும் இந்த முடிவுகள், இலக்குகளை முறையான மென்பொருள் அல்லது பிற உள்ளடக்கம் போல வேடமிட்டுள்ள தீம்பொருள் வழங்கும் வலைத் தளங்களுக்கு இட்டுச் செல்கின்றன
- **தீங்கு விளைவித்தல்:** தீம்பொருளை விநியோகிக்க முறையான ஆன்லைன் விளம்பரங்களில் உட்செலுத்தப்பட்ட தீங்கு விளைவிக்கும் குறியீட்டைப் பயன்படுத்துதல்
- **crack செய்யப்பட்ட அல்லது திருட்டு மென்பொருள்:** வீடியோ gameகள் உட்பட பதிவிறக்கங்கள், YouTube வீடியோக்கள் வழியாக பகிரப்பட்ட, வீடியோ விளக்கம் அல்லது கருத்துகளில் தீங்கிழைக்கும் இணைப்புகளுடன் அல்லது நம்பத்தகாத பதிவிறக்க தளங்களிலிருந்து பெறப்பட்டவை
- **சமூக ஊடக விளம்பரங்கள் மற்றும் இடுகைகள்:** மாறுவேடமிட்ட தீம்பொருள் கோப்புகளுக்கு இலக்குகளை இயக்குதல்
- **தீங்கிழைக்கும் மென்பொருள் புதுப்பித்தல்கள்:** பொதுவாக வலை உலாவி புதுப்பிப்புகளாக மாறுவேடமிட்டு பகிரப்படுபவை

நிலை 3: தரவு அறுவடை

பாதிக்கப்பட்டவரின் சாதனத்தில் தகவல் திருட்டு தீம்பொருள் செயல்பட ஆரம்பித்தவுடன், அது சமரசம் செய்யப்பட்ட சாதனத்திலிருந்து முக்கியமான தரவுகளை சேகரிக்கத் தொடங்குகிறது. பயனர் நற்சான்றிதழ்களைத் திருடுவதைத் தவிர, botnetடின் ஒரு பகுதியாக தகவல் திருட்டு தீம்பொருள் இருக்கும் சந்தர்ப்பங்களில், கூடுதல் திறன்களைச் செயல்படுத்த அல்லது பிற தீம்பொருளை வழங்க உள்ளமைவு கட்டளைகளை அனுப்புவதன் மூலம் சமரசம் செய்யப்பட்ட சாதனத்தை சைபர் குற்றவாளிகள் தொலைவிலிருந்து கட்டுப்படுத்தலாம். பொதுவாக, தகவல் திருடும் தீம்பொருட்கள் பின்வருவனவற்றைத் திருடும் திறன் கொண்டவை:

- பயனர் பெயர்கள் மற்றும் கடவுச் சொற்கள், குறிப்பாக வலை உலாவிகளின் ஒன்றுக்கு மேற்பட்ட வழியில் அங்கீகாரம் வழங்கும் கடவுச் சொற்கள் (MFA), பயனர் அமர்வுகள் அல்லது tokenகளில் சேமிக்கப்பட்டவை
- அங்கீகாரம் வழங்கும் cookieக்கள்
- autofill என்ற தானாக நிரப்பும் இணைய உலாவி படிவ தரவுகள்
- மின்னஞ்சல் நம்பிக்கைச்சான்றுகள், உள்ளடக்கங்கள் மற்றும் தொடர்புகள்
- வலை உலாவல் வரலாறு
- பயனர் ஆவணங்கள்
- கிரெடிட் கார்ட் விவரங்கள்
- கணினியிலுள்ள செய்தியிடல் பயன்பாடுகளிலிருந்து அரட்டை பதிவுகள்
- கணினி தகவல்
- cryptocurrency பணப்பைகள்
- VPN அல்லது கோப்பு பரிமாற்ற நெறிமுறை (FTP) நற்சான்றிதழ்கள்.



படம் 1. தகவல் திருடும் தீம்பொருளின் திறன்

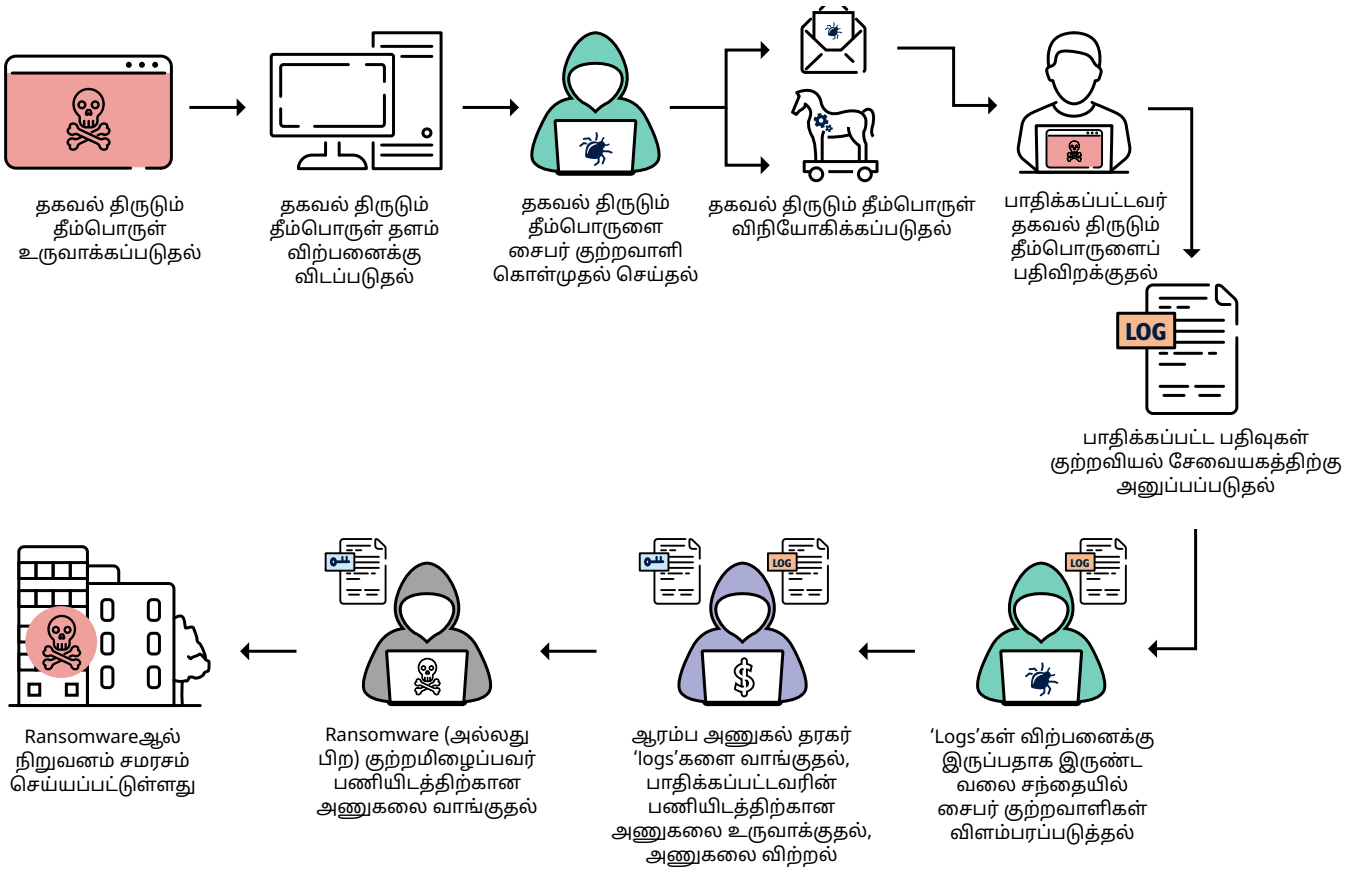
சில வலை உலாவி அங்கீகார cookieக்கள் ஒரு பயனரை ஒரே நேரத்தில் பல நாட்களுக்கு, அவரது கணக்கு அல்லது சேவையில் இணைய அனுமதியளித்திருக்கும், இதனால் பயனர்கள் மீண்டும் அங்கீகாரம் வழங்கத் தேவையில்லை. அங்கீகார cookieக்கள் திருடப்பட்டால், MFA தேவைகளை திறம்படக் கடந்து, பாதிக்கப்பட்ட கணக்குகள், நிறுவனத்தின் நெட்வொர்க்குகள் மற்றும் நிறுவன கட்டமைப்புகளை சைபர் குற்றவாளிகள் அணுக அனுமதி வழங்கக்கூடும்.

நிலை 4: தரவு ஒருங்கிணைப்பு மற்றும் பணமாக்குதல்

பாதிக்கப்பட்ட சாதனத்திலிருந்து, தீங்கிழைக்கும் கட்டளை மற்றும் கட்டுப்பாட்டு சேவையகங்களுக்குத் தகவல்களை 'logs' என்று வெளியேற்றும் வகையில் தகவல் திருடும் தீம்பொருட்கள் கட்டமைக்கப்பட்டுள்ளன. பொதுவாக, தகவல் திருடும் தீம்பொருள் சைபர் குற்றவாளிகளுடன் 'logs' பதிவுகளின் ஊட்டத்தைப் பகிர்ந்து கொள்ள, Telegram மற்றும் Discord போன்ற பிரபலமான செய்தியிடல் செயலிகளைப் பயன்படுத்துகிறார்கள்.

Telegram மற்றும் இருண்ட வலை முழுவதும், இந்த 'logs' பதிவுகளின் விற்பனை மற்றும் வர்த்தகத்திற்காக, சிறப்பு சந்தைகள் உள்ளன. சைபர் குற்றவாளிகள் 'logs'களை பல்வேறு வழிகளில் பணமாக்குகிறார்கள், அவற்றுள்:

- ஆரம்ப அணுகல் தரகர்கள் உட்பட குற்றவியல் சந்தைகளில் 'logs'களை விற்பனை செய்தல்
- அடையாள திருட்டு மற்றும் மிரட்டி பணம் பறித்தல் மூலம் பாதிக்கப்பட்டவரை நேரடியாக சுரண்டுதல்
- Ransomware செயற்பாட்டிற்காக, நிறுவனங்களின் நெட்வொர்க்குகளில் ஆரம்ப அணுகலுக்கான தகவலைப் பயன்படுத்துதல்.



படம் 2. தகவல் திருடும் தீம்பொருளின் அமைப்பு மற்றும் ஒரு நிறுவனத்தில் அது ஏற்படுத்தும் சாத்தியமான தாக்கம்

தாக்கங்கள்

தகவல் திருடும் தீம்பொருட்கள் தனிநபர்கள் மற்றும் நிறுவனங்கள் மீது கடுமையான தாக்கங்களை ஏற்படுத்தலாம். தகவல் திருடும் தீம்பொருட்கள் பயனர் நற்சான்றிதழ்களைச் சேகரிக்கும் அதே வேளை, நிறுவனத்தின் நெட்வொர்க்குகள் அல்லது செல்லுபடியாகும் பயனர் கணக்குகளுடன் இணைக்கப்பட்டுள்ள நிறுவன கட்டமைப்புகளை அணுக, இந்த பயனர் நற்சான்றிதழ்களை சைபர் குற்றவாளிகள் பயன்படுத்தலாம். பெரும்பாலும், கணினி உரிமையாளர்கள் இதைக் கண்டறிவதைத் தாமதப்படுத்துகிறது.

தகவல் திருடும் தீம்பொருட்களால் பாதிக்கப்பட்ட **நிறுவனங்கள்**, எதிர்கொள்ளும் பின்விளைவுகளில் பின்வருவன அடங்கும்:

- ransomware - தரவைத் திருடி, மிரட்டி, பணம் பறிக்க உதவும் மென்பொருள்
- தரவு மீறல்
- வணிக மின்னஞ்சல் சமரசம்
- அறிவு சார் சொத்து திருட்டு
- முக்கியமான தகவல்களின் திருட்டு.

தகவல் திருடும் தீம்பொருட்களால் பாதிக்கப்பட்ட **தனிநபர்கள்**, எதிர்கொள்ளும் பின்விளைவுகளில் பின்வருவன அடங்கும்:

- தனிப்பட்ட மின்னஞ்சல் அல்லது சமூக ஊடக கணக்குகளுக்கு அங்கீகரிக்கப்படாத அணுகல்
- அடையாள திருட்டு அதிகரிக்கும் ஆபத்து
- phishing என்ற மின்-தூண்டிலிடல் தாக்குதல்களின் ஆபத்து அதிகரித்துள்ளது
- நிதி இழப்பு அல்லது நிதிக் கணக்குகளுக்கான அங்கீகரிக்கப்படாத அணுகல்
- தனியுரிமை இழப்பு.

விரிவான ஆய்வு:

இந்த விரிவான ஆய்வு பொது பரவலாக்கத்தை செயல்படுத்த அநாமதேயமாக்கப்பட்டுள்ளது. ASDயின் ACSCற்கு அறிக்கை சமர்ப்பித்த ஆஸ்திரேலிய நிறுவனங்களைப் பாதித்த, இணைய பாதுகாப்பு முறியடிக்கப்பட்ட சம்பவங்களின் அடிப்படையில் இது அமைகிறது. இனிமேல், 'அமைப்பு' என்று பாதிக்கப்பட்ட நிறுவனம் குறிப்பிடப்படுகிறது. இந்த விரிவான ஆய்வில் உள்ள தனிநபர்களின் பெயர்கள் மாற்றப்பட்டுள்ளன, அத்துடன் பாதிக்கப்பட்டவர்களின் அடையாளத்தைப் பாதுகாப்பதற்காக விவரங்கள் அகற்றப்பட்டுள்ளன.

இந்த அமைப்பு ஒரு ஆஸ்திரேலிய வணிக நிறுவனமாகும். அதன் ஊழியர்களை, தனிப்பட்ட சாதனங்களிலிருந்து நிறுவனத்தின் கட்டமைப்புகளை அணுக அனுமதிக்கிறது. Alice தொலை தூரத்திலிருந்து பணிபுரியும் ஒரு ஊழியர்.

வீட்டிலிருந்து வேலை செய்யும் போது, Alice தனது தனிப்பட்ட மடிக்கணினியைப் பயன்படுத்தி தனது நிறுவனத்தின் நெட்வொர்க்கைத் தொலைவிலிருந்து அணுகுகிறார். Notepad++ என்ற (ஒரு வகை குறிப்பு எடுக்கும்) மென்பொருள் முறையானது என்று நம்பிய Alice, அதன் வலைத் தளத்திலிருந்து அவரது **தனிப்பட்ட மடிக்கணினிக்குப், பதிவிறக்கம்** செய்தார். Notepad ++ மென்பொருளுக்கான நிறுவியாக ஒரு **தகவல் திருட்டு தீம்பொருள்** மாறுவேடத்தில் இருந்தது.

மென்பொருளை Alice நிறுவ முயன்றபோது, தகவல் திருடும் தீம்பொருள் செயல்படுத்தப்பட்டு, அவரது மடிக்கணினியிலிருந்து பயனர் நற்சான்றிதழ்களை அறுவடை செய்யத் தொடங்கியது. அவரது வலை உலாவியில் சேமித்து வைக்கப்பட்டிருந்த அவரது பணியிட பயனர் பெயர் மற்றும் கடவுச்சொல் ஆகியவை அதில் அடங்கும். பின்னர் அந்த பயனர் நற்சான்றிதழ்களை சைபர் குற்றவாளி குழுவால் கட்டுப்படுத்தப்படும் தொலைநிலை கட்டளை மற்றும் கட்டுப்பாட்டு சேவையகத்திற்குத் தகவல் திருடும் தீம்பொருள் அனுப்பியது.

இதிலிருந்து திருடப்பட்ட 'log'கள் மற்றவர்களிடமிருந்து திருடப்பட்டவற்றுடன் தொகுக்கப்பட்டு பின்னர் இருண்ட வலை சந்தை வழியாக சைபர் குற்றவாளிகளுக்கு **விற்கப்பட்டன.**

Bob என்ற சைபர் குற்றவாளி Aliceஇன் பயனர் நற்சான்றிதழ்களை வாங்கினார். அந்த நிறுவனத்தின் நெட்வொர்க்கில் சேவைகளுக்கான பயனர் நற்சான்றிதழ்களை அவர் அடையாளம் கண்டார். Aliceஇன் அமைப்பு இந்த சேவைகளுக்காக MFAயை கட்டமைக்கவில்லை, அதாவது நிறுவனத்தின் நெட்வொர்க்கை வெற்றிகரமாக **அங்கீகரிக்கவும் அணுகவும்** திருடப்பட்ட பயனர் நற்சான்றிதழ்களை மட்டுமே Bob பயன்படுத்த வேண்டி இருந்தது.

திருடப்பட்ட **செல்லுபடியாகும் பயனர் நற்சான்றிதழ்களைப்** பயன்படுத்தி Aliceஇன் நிறுவனத்தின் பெரு நிறுவன நெட்வொர்க்கை Bob அணுகினார். நிறுவனத்தின் நெட்வொர்க்கில் பக்கவாட்டில் Bob செல்ல முடிந்தது. நிறுவனத்திற்கு சொந்தமான முக்கியமான தரவை அடையாளம் கண்டு, நிறுவனத்தை மிரட்டி பணம் பறிப்பதற்காக அவற்றை அவரால் வெளியே எடுக்க முடிந்தது.

முக்கியமான தரவுகளைத் திருடிய Bob, நிறுவனத்தின் **தரவுத் தளங்கள் மற்றும் கோப்பு முறைமைகளை** அணுக முடியாதபடி **குறியாக்கம்** (encrypt) செய்தார்.

மட்டுப்படுத்தல்கள்

தங்கள் நெட்வொர்க்குடன் இணைக்கும் சாதனங்களில், குறிப்பாக தொலை தூரத்தில் பணிபுரியும் ஊழியர்களால் பயன்படுத்தப்படும் தனிப்பட்ட சாதனங்களில் கட்டுப்பாடுகளை நிறுவனங்கள் செயல்படுத்த முடியாமல் போகலாம். பயனர் நற்சான்றிதழ்களை குறி வைக்கும் தகவல் திருடும் தீம்பொருட்களின் அபாயத்திலிருந்து தங்களைப் பாதுகாத்துக் கொள்வதற்கான கட்டுப்பாடுகளை செயல்படுத்துவதில் நிறுவனங்கள் கவனம் செலுத்த ASDயின் ACSC பரிந்துரைக்கிறது. இந்த மட்டுப்படுத்தல் நடவடிக்கைகளில் பின்வருவன அடங்கும்:

ஊழியர்களுக்கு சைபர் பாதுகாப்பு விழிப்புணர்வு பயிற்சி வழங்குதல்

- ஊழியர்களுக்குப் பயனுள்ள பயிற்சியை வழங்குவதன் மூலம் வெற்றிகரமான இலக்கு வைக்கப்பட்ட தாக்குதல்களையும் தீங்கிழைக்கும் கோப்பு பதிவிறக்கங்களையும் தடுக்கவும்.
- தகவல் திருடும் தீம் பொருட்கள் குறித்தும், அவற்றின் விநியோக முறைகள் மற்றும் உங்கள் நிறுவனத்திற்கு மின்-தூண்டிலிடல் அச்சுறுத்தல்கள் பற்றிய விழிப்புணர்வை ஏற்படுத்துங்கள்.

பாதுகாப்பான நிறுவன கணக்குகள்

- MFA ஐ செயல் படுத்தவும்:
- வெளிப்புற மற்றும் நிறுவனத்துள் வழங்கப்படும் சேவைகள், கட்டமைப்புகள் மற்றும் முக்கியமான தரவுக் களஞ்சியங்கள், குறிப்பாக இணைய வழியாக அணுகக்கூடிய மின்னஞ்சல், VPNகள் மற்றும் முக்கியமான அமைப்புகளை அணுகும் சலுகை பெற்ற பயனர் கணக்குகள் ஆகியவற்றில் MFA என்ற இரு படி சரிபார்த்தல் முறையை செயல் படுத்தவும். எந்த கணினி அணுகலுக்கும் phishing-resistant Multi-Factor Authentication என்ற மின்-தூண்டிலிடலை எதிர்க்க வல்ல இரு படி சரிபார்த்தல் முறையை செயல் படுத்துவதே சிறந்த நடைமுறை.
- பயனர் கணக்குகள் இனி தேவைப்படாத போது அவற்றை முடக்க வேண்டும்.
- நிர்வாகி சிறப்புரிமைகளைக் கட்டுப்படுத்தவும்:
- நெட்வொர்க் நிர்வாகம் மற்றும் பிற சலுகை பெற்ற பணிகளை ஒரு பிரத்தியேக, அதிக பாதுகாப்பு கொண்ட கணினி நிலையத்தை மட்டுமே பயன்படுத்தி செய்யுங்கள் (அதாவது secure admin workstation).
- நிர்வாகி அமைப்புகளை நிர்வகிக்க சலுகை பெற்ற பயனர் கணக்குகளையும், நிர்வாகமற்ற பணிகளுக்கு நிலையான பயனர் கணக்குகளையும் பயன்படுத்த வேண்டும் என்று கோருவதன் மூலம் குறைந்த-சலுகை வழங்கும் சிறந்த நடைமுறையைப் பின்பற்றவும்.
- (ஆன்லைன் சேவைகளை அணுகுவதற்கு வெளிப்படையாக அங்கீகரிக்கப்பட்டவை தவிர,) இணையம், மின்னஞ்சல் மற்றும் வலை சேவைகளை அணுகுவதிலிருந்து சிறப்புரிமை பெற்ற பயனர் கணக்குகளைத் தடுத்தல்.
- அமைப்புகள் மற்றும் செயலிகளுக்கு just-in-time என்ற நேரச் சிக்கன நிர்வாகத்தைச் செயல்படுத்துவதைக் கவனத்தில் கொள்ளுங்கள்.
- சிறப்புரிமை பெற்ற பயனர் கணக்குகளுக்கு மேலாண்மை மற்றும் தணிக்கைகளை செயல் படுத்தவும்.
- குறிப்பாக வெளிப்புற அணுகலை எதிர்கொள்ளும் மற்றும் தொலைநிலை அணுகல் கணக்குகளுக்கு, கடவுச் சொற்களை அவ்வப்போது புதுப்பிக்கவும்.
- அமர்வுக்கான குறி அடையாளம் மற்றும் cookieக்களின் ஆயுள் காலம் மற்றும் அவை எப்போது காலாவதியாகும் என்பன குறித்த கொள்கைகளை செயல் படுத்தவும்.

பணியிடத்திற்கு வெளியே சாதனங்களின் இயக்கத்தை கடினமாக்குங்கள்

- நிறுவனத்தின் சாதனங்கள் வெளியே இயக்கப்படுவதால் ஏற்படும் இடர் மதிப்பீட்டைச் செய்து, பணியிடத்திற்கு வெளியே சாதனங்களின் இயக்கத்தை கடினப்படுத்தும் வழிகாட்டுதல்களை செயல் படுத்தவும்.
- நிர்வகிக்கப்படாத தனிப்பட்ட சாதனங்களை விட நிறுவனத்தால் நிர்வகிக்கப்படும் சாதனங்கள் மிகவும் பாதுகாப்பானவை என்பதால், தனிப்பட்ட சாதனங்களை ஊழியர்கள் வேலைக்குப் பயன்படுத்த அனுமதித்தால் அதற்கான (BYOD) கொள்கையை செயல் படுத்தவும்.

மென்பொருளை சேவையாக வழங்கும் (Saas) விற்பனையாளர்கள் மற்றும் நிர்வகிக்கப்பட்ட சேவை வழங்குநர்கள் உட்பட உங்கள் நெட்வொர்க்குகளை அணுகும் விற்பனையாளர்களிடமிருந்து விநியோகச் சங்கிலி அபாயங்களை மதிப்பாய்வு செய்து மதிப்பிடுங்கள். நிர்வகிக்கப்பட்ட சேவை வழங்குநரை ஈடுபடுத்தும் போது உங்கள் பாதுகாப்பை எவ்வாறு நிர்வகிப்பது.

உங்கள் நிறுவனத்தின் நெட்வொர்க்கைப் பாதுகாக்கவும்

- செயலிகள் மற்றும் இயக்க முறைமைகளை புதுப்பித்த நிலையில் வைத்திருங்கள்.
- கண்டிப்பான அனுமதிப் பட்டியலுடன் பயன்பாட்டுக் கட்டுப்பாட்டை நடைமுறைப் படுத்த உங்கள் பாதுகாப்புக் கொள்கைகளைப் பயன்படுத்தவும்.
- ஒருவரின் தொழில் நிலை மற்றும் செயற்பாட்டின் அடிப்படையில் பிரிவு படுத்தப்பட்ட நெட்வொர்க், தேவையான அளவு கண்காணிப்பு என்பவற்றை செயல் படுத்தவும்.
- பயனர் செயல்பாடுகளை, குறிப்பாக தொலைதூர ஊழியர்களின் செயல்பாடுகளை தணிக்கை செய்து கண்காணிக்கவும்,
- முக்கியமான தரவுக்கான அங்கீகரிக்கப்படாத அணுகல் அல்லது வெளிப்புற நெட்வொர்க்கில் பதிவேற்றப்பட்ட பெரிய அளவிலான தரவு போன்ற அசாதாரண தரவு பரிமாற்ற செயல்பாடுகளை சிறப்புரிமை பெற்ற கணக்குகளைக் கண்காணிப்பதன் மூலம் வெளிப்படுத்தலாம்.
- அங்கீகரிக்கப்படாத தரவு இடமாற்றங்களைத் தடுக்க தரவு இழப்பு தடுப்பு கொள்கைகள் மற்றும் கருவிகளை செயல் படுத்தவும்.

ASDயின் சைபர் பாதுகாப்பு குழுமத்தில் இணைந்து, Cyber Threat Intelligence Sharing (CTIS) என்ற சைபர் அச்சுறுத்தல் புலனாய்வு பகிர்வு சேவையில் சேரவும்

- CTIS என்பது இருவழி பகிர்வுத் தளமாகும். தீங்கிழைக்கும் இணைய செயல்பாடு பற்றிய தகவல்களைப் பெறவும் பகிர்ந்து கொள்ளவும் இது அரசின் தொழில்துறை கூட்டாளர்களுக்கு உதவுகிறது.
- ASD இன் ACSC தகவல் திருடும் செயல்பாட்டைக் கண்காணித்து CTIS இயங்கு தளத்தின் மூலம் செயலில் உள்ள கட்டளை மற்றும் கட்டுப்பாட்டு உட்கட்டமைப்பின் விவரங்களைப் பகிர்ந்து கொள்கிறது.
- ஒரு பங்குதாரராக பதிவு செய்து, உங்கள் நிறுவனம் மற்றும் வாடிக்கையாளர் தரவை சைபர் குற்றவாளிகளின் அச்சுறுத்தல்களிலிருந்து பாதுகாக்கவும்.

ஒரு சமரசத்திற்குத் தயாராகுங்கள்

- தகவல் திருட்டு சமரசம் ஏற்பட்டால் பயன்படுத்தக் கூடிய 'சைபர் பாதுகாப்பு எதிர்வினைத் திட்டம்' ஒன்றை உருவாக்கவும். சந்தேகத்திற்கிடமான கோப்பை பதிவிறக்கம் செய்ததாக ஊழியர்கள் சந்தேகித்தால், என்ன செய்ய வேண்டும், யாரைத் தொடர்பு கொள்ள வேண்டும் என்பதை அவர்கள் அறிந்திருப்பதை உறுதிப்படுத்தவும்.

ASD இன் ACSC இன் 'அத்தியாவசிய எட்டு' செயற்பாடுகளை நடைமுறைப்படுத்தவும்

- மேலே குறிப்பிட்டுள்ள மட்டுப்படுத்தல்கள் நடவடிக்கைகளுக்கும் மேலதிகமாக, ASD இன் ACSC இன் 'அத்தியாவசிய எட்டு' செயற்பாடுகளில் கூறப்பட்டுள்ள மீதமுள்ளவற்றை செயல் படுத்த ASD இன் ACSC கடுமையாகப் பரிந்துரைக்கிறது.

தொலை தூரத்தில் பணிபுரியும் போது உங்கள் ஊழியர்களுக்கான ஆலோசனை

- உங்கள் தனிப்பட்ட சாதனங்களில் உள்ள தகவலைப் பாதுகாக்கவும்
  - நல்ல இணைய பழக்கங்களை வளர்த்துக் கொள்ளுங்கள், மற்றும் சந்தேகத்திற்கிடமான இணைப்புகள் அல்லது pop-upகளைக் கிளிக் செய்யாதீர்கள் அல்லது அறியப்படாத அல்லது நம்பத்தகாத மூலங்களிலிருந்து கோப்புகள் அல்லது மென்பொருளைப் பதிவிறக்க வேண்டாம்.
  - பணி மற்றும் தனிப்பட்ட கணக்குகளுக்கு தனித்துவமான கடவுச் சொற்களைப் பயன்படுத்தவும். முடிந்தவரை தனிப்பட்ட கணக்குகளுக்கு MFA ஐப் பயன்படுத்தவும்.
  - உங்கள் நிறுவனத்தால் வெளிப்படையாக அங்கீகரிக்கப்படாவிட்டால் உங்கள் பணி நற்சான்றிதழ்களை தனிப்பட்ட கடவுச்சொல் நிர்வாகியில் சேமிக்க வேண்டாம். இதில் உங்கள் இணைய உலாவியின் கடவுச்சொல் நிர்வாகியும் அடங்கும். **சந்தேகம் இருந்தால், உங்கள் நிறுவனம் பரிந்துரைக்கும் கடவுச்சொல் நிர்வாகியை வழங்குமாறு கோருங்கள்.**
  - பகிரப்பட்ட அல்லது சமூக கணினி சாதனங்களிலிருந்து உங்கள் வேலை கணக்குகளில் உள் நுழைய வேண்டாம்.
  - உங்கள் இணைய உலாவியின், autofill என்ற தானாக நிரப்பும் இணைய உலாவி படிவத்தில் என்ன சேமிக்கப்படுகிறது என்பதை அறிந்து கொள்ளுங்கள். தகவல் திருடும் தீம்பொருட்கள் autofill என்ற தானாக நிரப்பும் இணைய உலாவி படிவத்தில் சேமிக்கப்படும் தரவை குறி வைக்கின்றன. வலை படிவங்களை நிரப்பும் போது, உங்கள் வலை உலாவியின் autofill என்ற தானாக நிரப்பும் படிவத்தில் சேமிப்பதை விட, கிரெடிட் கார்ட் எண்கள் போன்ற முக்கியமான தரவை ஒவ்வொரு முறையும் நீங்களே உள்ளிடுங்கள்.
  - தகவல் திருடும் தீம்பொருளுக்குக் கிடைக்கும் தகவல்களைக் குறைப்பதற்காக, இணையத்தில் உலாவல் அமர்வு முடிந்தவுடன் அனைத்து ஆன்லைன் சேவைகளிலிருந்தும் வெளியேறி, வலை உலாவி cookieக்களை அழிக்கவும்.
  - உங்கள் இயக்க முறைமையின் உள்ளமைக்கப்பட்ட வைரஸ் தடுப்பு செயலி இயக்கப்பட்டுள்ளதா என்பதை உறுதிப்படுத்தவும். நீங்கள் மூன்றாம் தரப்பு வைரஸ் தடுப்பு தீர்வைப் பயன்படுத்தினால், அது புதுப்பித்த நிலையில் வைக்கப்பட்டுள்ளதா மற்றும் புகழ்பெற்ற விற்பனையாளர் உருவாக்கியதா என்பதை உறுதிப்படுத்தவும்.

உதவி

சைபர் பாதுகாப்பு சம்பவம் தொடர்பாக பாதிக்கப்பட்ட அல்லது உதவி தேவைப்படும் ஆஸ்திரேலிய நிறுவனங்கள் ASD இன் ACSC ஐ 1300 CYBER1 (1300 292 371) வழியாக அல்லது cyber.gov.au/report வழியாக அறிக்கையைச் சமர்ப்பிப்பதன் மூலம் தொடர்பு கொள்ளலாம்.

நிறுவனங்கள் சந்தேகத்திற்கிடமான நெட்வொர்க் செயல்பாடு மற்றும் தகவல் திருடும் தீம் பொருட்களுடன் தொடர்புடைய சமரசத்தின் குறிகாட்டிகளை, அந்த சம்பவம் கட்டுப்படுத்தப்பட்டதாகக் கருதப்பட்டாலும் கூட, புகாரளிக்க வேண்டுமென்று ASD இன் ACSC ஊக்குவிக்கிறது. சைபர் அச்சுறுத்தல் நடவடிக்கைகளில் ஈடுபடுபவர்களின் தந்திரோபாயங்கள், நுட்பங்கள் மற்றும் நடைமுறைகள் பற்றிய எங்கள் புரிதலை மேம்படுத்த நீங்கள் வழங்கிய தகவலைப் பயன்படுத்துகிறோம், இதே வழியில் இலக்கு வைக்கப்பட்டுள்ள பிற ஆஸ்திரேலிய நிறுவனங்களை எச்சரிக்க இது எங்களுக்கு உதவுகிறது.

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 ஆஸ்திரேலியாவிற்குள் மட்டுமே பயன்படுத்த முடியும்.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre