Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

AFP

cyber.gov.au

“புல்லெட் ப்ரூப்” ஹோஸ்டிங் வழங்குநர்கள்: இணைய குற்றவாளிகளின் உள்கட்டமைப்பு கவசத்தில் விரிசல்கள்

வெற்றிகரமான இணைய குற்றவாளிகள் பாதுகாப்பான, கண்டறிய முடியாத மற்றும் மீள்தன்மை கொண்ட உள்கட்டமைப்பை நம்பியுள்ளனர். ஒரு நெட்வொர்க் முறிந்து அதில் குற்றவாளிகள் நுழையும்போதும், சான்றுகள் திருடப்படும்போதும், மென்பொருள் அல்லது தரவுகள் திருடப்பட்டு சட்டவிரோத இணைய தளங்களில் விற்பனை செய்வதன் பின்னாலும், இணைய குற்றவாளிகள் மறைந்திருந்து செயல்படும் உள்கட்டமைப்பு உள்ளது.

இருப்பினும், கண்டறிய முடியாதவர்களாக இயங்குவதும், பிறரால் கண்டுபிடிக்க கடினமாக இருக்கவைப்பதும், இணைய குற்றவாளிகளுக்கு ஒரு சவாலாக மாறிவருகிறது. அரசுகள், சட்ட அமலாக்க நிறுவனங்கள் மற்றும் தனியார் துறைக்கு இடையிலான உலகளாவிய ஒத்துழைப்பு, இணையத்தில் பெயர் தெரியாமல் இயங்குவதை இணைய குற்றவாளிகளுக்கு கடினமாக்குகிறது. மேலும், மிகச் சில இணைய குற்றவாளிகள் மட்டுமே பாதுகாப்பான உள்கட்டமைப்பைத் தாங்களாகவே நிர்வகிக்கவும், பராமரிக்கவும் தேவையான திறன்களையும் நிபுணத்துவத்தையும் கொண்டுள்ளனர். இதனால், இணைய குற்றவாளிகள் தங்களின் செயல்பாடுகளை பிற சட்டவிரோத உள்கட்டமைப்பு வழங்குநர் மூலம் நிறைவேற்றி, பிறரை ஏமாற்றி, தாங்கள் லாபமீட்டுவதில் அதிக கவனம் செலுத்துகின்றனர்.

‘சைபர் கிரைம்-அஸ்-எ-சர்வீஸ்’ என்பது பல்வேறு வகையான தீங்கிழைக்கும் இணைய குற்றவாளிகளை ஆதரிக்கும் வகையில் உருவாக்கப்பட்ட ரகசியமான சந்தையைக் குறிக்கிறது. இந்த ரகசிய சந்தை, ஆன்லைன் திருட்டுகளை நடத்த உதவும் மென்பொருள், சேவைகள் மற்றும் பொதுமக்களை குறிவைத்து ஏமாற்றும் தகவல்களை இணைய குற்றவாளிகளுக்கு வழங்குகிறது. இணைய குற்றவாளிகளாக மாறக்கூடியவர்கள், நெட்வொர்க்குகளை ஊடுருவக்கூடிய, பாதுகாப்பு பொறிமுறைகளை தவிர்க்க உதவும் கருவிகளை வாங்கலாம். அதேபோன்று, அப்பாவி பொதுமக்களின் தனிப்பட்ட தகவல்களைத் திருடும் மென்பொருளையும் வாங்கலாம். புல்லெட் ப்ரூப் ஹோஸ்டிங் (BPH) வழங்குநர்கள் இணைய குற்றச் சூழல் அமைப்பின் ஒரு பகுதியாகும். இணைய குற்றவாளிகளுக்கு இவர்கள் பாதுகாப்பான உள்கட்டமைப்பை வழங்குகிறார்கள். முக்கியமாக, உலகம் முழுவதும் அப்பாவிகளை குறிவைக்க நூற்றுக்கணக்கான இணைய குற்றவாளிகளை ஒரே நேரத்தில் அனுமதிக்க ஒரு BPH வழங்குநரால் முடியும்.

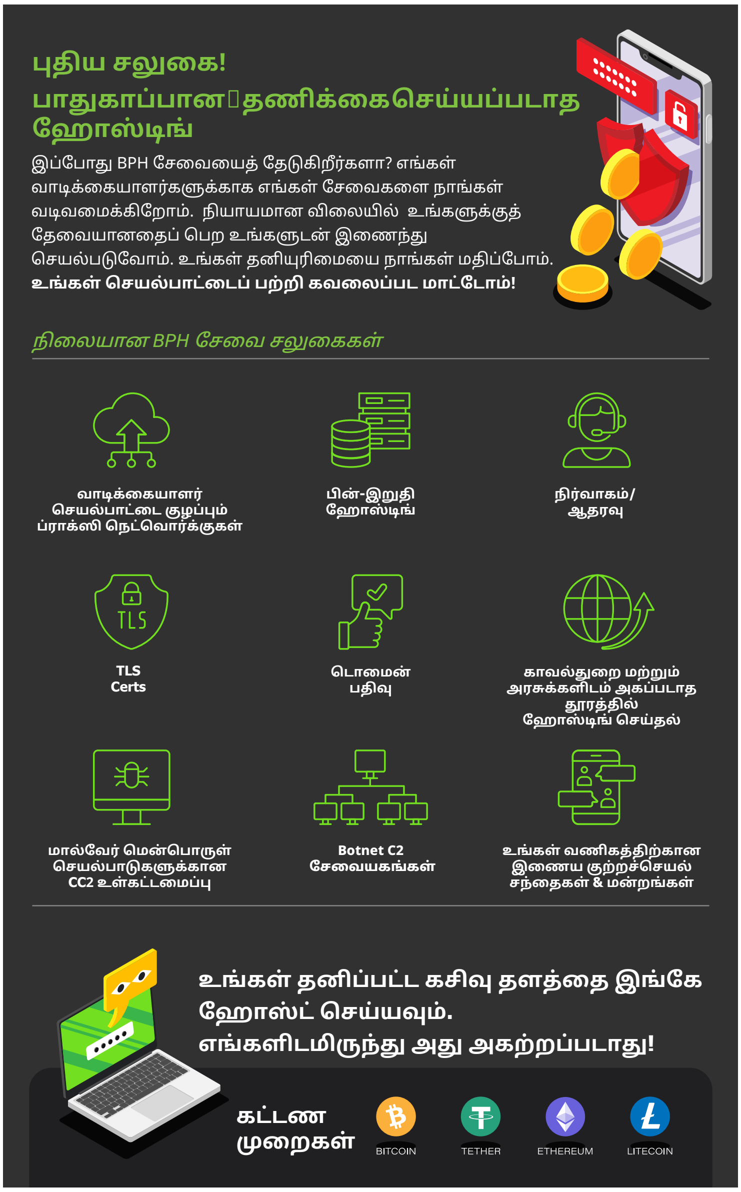
“புல்லெட் ப்ரூப்” ஹோஸ்டிங் வழங்குநர் என்றால் என்ன?

எளிமையாகச் சொன்னால், BPH வழங்குநர்கள் இணைய குற்றவாளிகள் இயங்குவதற்கு ஒரு மெய்நிகர் மற்றும்/அல்லது நேரடியான உள்கட்டமைப்பை குத்தகைக்கு விடுகின்றனர். BPH வழங்குநர்கள், இணைய உள்கட்டமைப்பு சேவையின் ஒரு குறிப்பிட்ட பிரிவாகும். இவர்கள், தீங்கிழைக்கும் இணைய குற்றவாளிகள் தங்களின் சட்டவிரோத உள்ளடக்கத்தை இணையத்தில் இயங்கவும், செயல்படவும் அனுமதிக்கின்றனர்.

"புல்லெட் ப்ரூப்” என்பது சந்தைப்படுத்துவதற்காக பயன்படுத்தப்படும் சொல். உண்மையில், இந்த சேவைகள் மற்ற உள்கட்டமைப்பு வழங்குநர்களைப் போலவே இடையூறுகளுக்கு ஆளாகின்றன. ஆனால் வித்தியாசம் என்னவெனில், BPH வழங்குநர்கள் சட்ட அமலாக்கம் மற்றும் பிற உள்ளடக்க நீக்குதல் கோரிக்கைகளுக்கு கீழ்ப்படிய மறுக்கிறார்கள். மேலும் பாதிக்கப்பட்டவர்களிடமிருந்து வரும் துஷ்பிரயோக புகார்களையும், சந்தாதாரரின் கோரிக்கைகளையும் புறக்கணிக்கிறார்கள். இப்படி இணைய குற்றவாளிகள் தங்களுக்குள் தொடர்புகளை தொடரவும், சட்டவிரோத இணைய குழுக்களையும், வலைத்தளங்களை இயக்கவும், திருட்டை மேற்கொள்ளும் மென்பொருள் மற்றும் ஃபிஷிங் போன்றவற்றை பயன்படுத்தவும், சட்ட அமலாக்கம் அல்லது பிற கோரிக்கைகளின் அடிப்படையில் தங்கள் குத்தகையை ஆபரேட்டர் முடித்துவிடுவார் என்ற அச்சமின்றி பணத்தை மோசடி செய்யவும் அனுமதிக்கின்றனர்.

BPH வழங்குநர்கள் தெரிந்தே இணைய குற்றவாளிகளின் அமைப்பில் பங்கேற்கிறார்கள், அதன்மூலம் கடுமையான நிதி மோசடி செய்யும் இணைய குற்றவாளிகள் இயங்க அனுமதிக்கின்றனர். ஆஸ்திரேலிய நிறுவனங்கள் மற்றும் அவற்றின் வாடிக்கையாளர்களைப் பாதிக்கும் முக்கிய இணைய திருட்டு சம்பவங்களை இணைய குற்றவாளிகள் BPH வழங்குநர்களை பயன்படுத்தியே நடத்தியுள்ளனர். இந்த திருட்டு சம்பவங்களில் ரேன்சம்வேர் தாக்குதல்கள், தரவு பறிப்பு மற்றும் முக்கியமான தகவல்களைத் திருடுதல் ஆகியன அடங்கும்.

**"புல்லெட் ப்ரூப்" ஹோஸ்டிங்
வழங்குநர்களின் ரகசிய விளம்பரத்தின் ஒரு மாதிரி:**

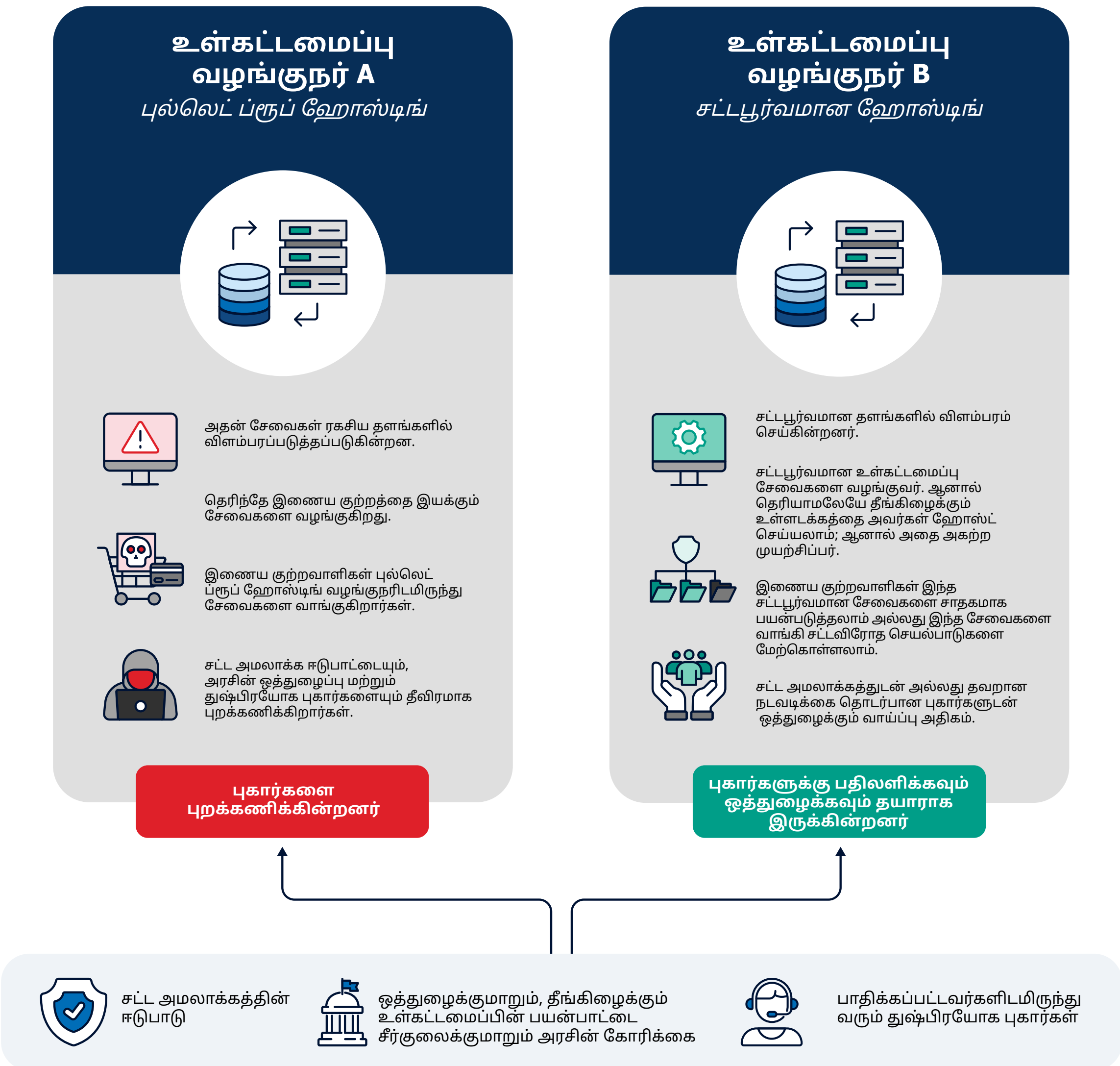


BPH வழங்குநர்கள் எவ்வாறு செயல்படுகிறார்கள்?

BPH வழங்குநர்களிடையே வணிக செயல்பாடு வேறுபடுகிறது. மிகவும் பொதுவான முறை என்பது இணைய குற்றவாளிகளுக்கு இணையத்தின் IP முகவரிகளை குத்தகைக்கு விடுவதும், குற்றவாளிகளின் இருப்பிடங்கள், அடையாளங்கள் மற்றும் செயல்பாடுகளை மறைக்க சிக்கலான நெட்வொர்க் முறைகளை அவர்களுக்கு வழங்குவதும் ஆகும். பல சந்தர்ப்பங்களில், BPH வழங்குநர்கள் பிற முறையான ஹோஸ்டிங் வழங்கும் சேவை, தரவு மையங்கள் அல்லது இணைய சேவைகளின் (ISP) IP முகவரிகளையும், சேவைகளையும் மறுவிற்பனை செய்கிறார்கள் அல்லது குத்தகைக்கு விடுகிறார்கள். BPH வழங்குநர்கள் தருகின்ற உள்கட்டமைப்பு, இணைய குற்றவாளிகளுக்கு 'டவுன்ஸ்ட்ரீம்" சேவைகளை வழங்குகிறது என்பதை இந்த 'அப்ஸ்ட்ரீம்' வழங்குநர்கள் அறியாமல் இருக்கலாம்.

தங்கள் வாடிக்கையாளர்களை அடையாளம் காண்பதை கடினமாக்கும் வகையில் தங்கள் நெட்வொர்க்குகள் மற்றும் அமைப்பு கட்டமைப்பை BPH வழங்குநர்கள் உள்ளமைக்கின்றனர். உதாரணமாக, வாடிக்கையாளரின் செயல்பாட்டுடன் தொடர்புடைய இணைய அடையாளங்காட்டிகளை - அவர்களுக்கு ஒதுக்கப்பட்ட IP முகவரிகள் மற்றும் டொமைன் பெயர் போன்றவற்றை - அவர்கள் அடிக்கடி மாற்றுகிறார்கள். இத்தகைய BPH வழங்குநர்களின் நுட்பங்கள், பாதுகாப்புத்துறை மற்றும் புலனாய்வாளர்களுக்கு சவாலாக இருக்கின்றன. ஏனெனில் குறிப்பிட்ட நேரமொன்றில் நடந்த ஒரு சம்பவத்தையும், ஒரு திருடன் அல்லது வாடிக்கையாளர் பயன்படுத்தியுள்ள IP முகவரியையும் இணைப்பதை இந்த நுட்பங்கள் கடினமாக்குகின்றன. மேலும், BPH வழங்குநர்கள் பெரும்பாலும் அதிக கட்டுப்பாடுகளின்றி இணையங்கள் இயங்க அனுமதிக்கும் நாடுகளின் உள்கட்டமைப்பைப் பயன்படுத்துகின்றனர். இந்த நாடுகளில் இணைய திருட்டை விசாரித்து தடுப்பதற்கான முறையான நடவடிக்கைகள் மென்மையாக இருக்கும் அல்லது இல்லாமலிருக்கும்.

புல்லெட் ப்ரூப் ஹோஸ்டிங் வழங்குநர்கள் சட்டபூர்வமான உள்கட்டமைப்பு வழங்குநர்களிடமிருந்து எவ்வாறு வேறுபடுகிறார்கள்?



BPH வழங்குநர்களை குறிவைப்பது இணைய குற்றவாளிகளின் அச்சுறுத்தலை எவ்வாறு பாதிக்கிறது

BPH வழங்குநர்கள் நூற்றுக்கணக்கான அல்லது ஆயிரக்கணக்கான இணைய குற்றவாளிகளை ஒரே நேரத்தில் சீர்குலைக்ககூடிய ஒரு மதிப்புமிக்க வாய்ப்பை தருகின்றனர். பல்வேறு இணைய குற்றவாளிகளும் பிற தீங்கிழைக்கும் இணைய மோசடியாளர்களும் தங்கள் குற்றங்களை எளிதாக செய்ய இந்த சேவைகளைப் பயன்படுத்துகின்றனர். இணையத்திலிருந்து நீக்கும் கோரிக்கைகள் அல்லது துஷ்பிரயோக புகார்களை அவர்கள் எதிர்கொள்ளும் போது அவர்களின் செயல்பாடு கண்டுபிடிக்க இயலாததாக இருக்கலாம் அல்லது தொடர்ந்து செயல்படலாம் என்றும் நம்புகிறார்கள்.

இருப்பினும், சட்ட அமலாக்கம், அரசு நிறுவனங்கள் மற்றும் தனியார் துறை ஆகியவை இந்த சட்டவிரோத உள்கட்டமைப்பு வழங்குநர்களை குறிவைத்து சீர்குலைக்க ஒன்றிணைந்து செயற்படுகின்றனர். இதில் அறியப்பட்ட BPH வழங்குநர்களிடமிருந்து இணைய போக்குவரத்தை முன்கூட்டியே தடுப்பது போன்ற தற்காப்பு நடவடிக்கைகளும் அடங்கும். இந்த நடவடிக்கைகள் ஆஸ்திரேலிய மற்றும் அதன் கூட்டணி நெட்வொர்க்குகளுடன் தொடர்பு கொள்ளும் இணைய குற்றங்களின் அளவைக் குறைக்க உதவுகின்றன. மேலும் BPH வழங்குநர்களுக்கு தருகின்ற உள்கட்டமைப்பு இணைய குற்றவாளிகளுக்கு 'டவுன்ஸ்ட்ரீம்" சேவைகளை வழங்குகிறது என்பதை, இந்தசட்டபூர்வமான 'அப்ஸ்ட்ரீம்' வழங்குநர்கள் மற்றும் ISP கள் அறியாமல் இருப்பதையும் குறைக்கிறது.

சைபர் கிரைம்-அஸ்-எ-சர்வீஸ் எனும் அமைப்பில் BPH வழங்குநர்கள் மட்டுமே உள்கட்டமைப்பு வழங்குநர் வகை அல்ல. இந்த சேவைகள், இணைய திருட்டு அச்சுறுத்தல்களை தீவிரமாக ஆதரித்து, சட்டப்பூர்வமான விசாரணை மற்றும் பதில் தருவதை வேண்டுமென்றே தடுத்து ஆஸ்திரேலியாவில் இணைய திருட்டு அச்சுறுத்தலை தொடர்ந்து நிலைநிறுத்துகின்றன. BPH வழங்குநர்களுக்கு எதிரான நடவடிக்கை, அந்த சேவைகளின் பலவீனத்தையும், அவற்றைப் பயன்படுத்தும் தீய நோக்கமுள்ள இணைய குற்றவாளிகளையும் வெளிப்படுத்துகிறது.