கணினி வைரஸ்களை அறிந்து கொள்வோம்

கணினி வைரஸ் என்றால் என்ன?

கணினி வைரஸ் என்பது, ஒரு கணினியிலிருந்து மற்றொரு கணினிக்கு தாவ வல்ல, தன்னைத்தானே விருத்தி செய்து கொள்ளும், கணினிக்கு கேடு விளைவிக்கும் ஒரு *சிறிய செய்நிரலாகும்*. இந்த *செய்நிரல்* உங்கள் கணினியிலுள்ள முக்கியமான தரவுகளை மாற்றவோ அல்லது அழிக்கவோ வல்லது. அனேகமான வைரஸ்கள் நிறைவேற்றுத்தகு கோப்புக்களின் இணைப்பாக (attachment to executable files) நமது கணினிக்குள் நுழைகின்றன.

ஆகையால் நாம் இந்த கோப்புக்களை இயக்கும் போதோ அல்லது திறக்கும் போதோ வைரஸ்கள் செயல்பட ஆரம்பித்து விடுகின்றன.

அதிகமாகக் காணப்படும் வைரஸ் வகைகள்

கணினி வைரஸ், ஸ்பைவெயார், ட்ரோஜன் ஹோர்ஸ், எட்வெயார், வ(ர்)ம் பொன்ற அனைத்தும் மெல்வெயார் வகையைச் சார்ந்தவையாகும். உங்கள் கணினிக்கு கேடு விளைவிக்கும் அல்லது நீங்கள் *அறியாவண்ணம்* உங்கள் கணினியிலுள்ள தரவுகளை திருடிக்கொள்ளும் வைரஸ்கள் இவ்வகையைச் சார்ந்ததாகும்.

ஸ்பைவெயார்(Spyware) – அதிகமாகக் காணப்படும் வைரஸ் வகையாகும். இவ்வைரஸ் ஒரு நபரின் கணினியின் செயல்பாடுகளை அவர் *அறியாவண்ணம்* சேகரித்து வைக்கும்.

எட்வெயார் (Adware) – உங்கள் அனுமதியின்றியே கணினியில் தன்னை நிறுவி விளம்பரங்களைத் திரையில் காண்பிக்கும். மேலும் இதன் மூலம் ஒருவரின் இணையச் செயற்பாடுகளின் தரவுகள் சேகரிக்கப்படும்.

ட்ரோஜன் ஹோர்ஸ் (Trojen Horse) - இவை நன்மை பயக்கும் மென்பொருள் போல் தோற்றமளித்து கணினியில் உட்புகுந்து பின்னர் தீங்கு விளைவிப்பனவாகும். இவ்வைரஸ்களுக்குத் தன்னைத்தானே விருத்தி செய்து கொள்ளும் ஆற்றல் இல்லை. ஆனால் இது உங்கள் கணினியிலுள்ள முக்கியமானத் தகவல்களைத் திருட வல்லதோடு *மட்டுமல்லாமல்* ஒரு குறிப்பிட்ட திகதியில் அல்லது நேரத்தில் கணினியைச் சேதப்படுத்திவிடும் ஆற்றல் கொண்டது.

வ(ர்)ம் (Worm) - இவை பொதுவான வைரஸ்களை விட வேறுபட்டவையாகும். இவை ஒரு *கணினியிலிருந்து* மற்றொரு கணினிக்கு மனிதனின் உதவியின்றியே தாவி விடும். இவ்வைரஸ்கள் தன்னைத்தானே *விருத்தி* செய்து கொள்ளும் ஆற்றல் கொண்டவை. உதாரணம்: இவ்வகை வைரஸ் உங்கள் கணினியில் பல்கிப் *பெருகி* பின்னர் உங்களது இ-மெயில் முகவரி புத்தகத்தைப் பயன்படுத்தி இ-மெயிலாக பலரது கணினிகளுக்குப் பரவி விடும். பின்னர் அந்த கணினிகளிலிருந்து மீண்டும் பல கணினிகளுக்குப் *பரவ* ஆரம்பித்து விடும். *ஆகவே* இத்தகைய வ(ர்)ம்கள் கணினி வலையமைப்பூடாக சுயமாகவே பரவும் ஆற்றல் கொண்டவை.

வைரஸ் உங்கள் கணினிக்குள் எவ்வாறு உட்புகுகின்றது?

கணினி வைரஸ்கள் இ-மெயில் மூலமாக அல்லது இ-மெயில் இணைப்பாக எளிதாக உட்புகுகின்றன. இ-மெயில் மூலமாக பரவும் வைரஸ்கள் மனங்கவரும் படங்களாகவோ, வாழ்த்துக்களாகவோ அல்லது செவிப்புல-கட்புல கோப்புகளாகவோ உங்களை வந்தடையும். ஆகவே எதிர்பாராவிதமாகவோ அல்லது அனுப்புனர் யார் என்று அறியமுடியாத இ-மெயில்களையோ அதன் இணைப்புகளையோ *திறவாமல்* இருத்தல் சாலச்சிறந்ததாகும்.

நீங்கள் இணையத்தில் பதிவிறக்கம் செய்யும் போது கூட இவ்வகை வைரஸ்கள் உங்கள் கணினிக்குள் உட்புக வாய்ப்புண்டு.

கணினி வைரஸ்களின் தாக்கத்தின் அறிகுறிகள்:

1. கணினியின் இயக்க வேகம் குறைவடைதல்
2. கணினி அடிக்கடி தானாகவே மீள் துவக்கமடைதல் அல்லது அசாதாரன முறையில் செயற்படுதல்
3. கணினியிலுள்ள செய்நிரல்கள் சரிவர செயல்படாமை

4. வழக்கத்திற்கு *மாறான* செய்திகள் (messages) தென்படுதல்
5. உங்களால் நிறுவப்படாத படவுருகள் (Icons) *திரையில்* தென்படுதல்
6. உங்களால் அழிக்கப்படாத செய்நிரல்கள் அழிக்கப்பட்டதாக தோன்றுதல்

உங்கள் கணினியை வைரஸ்களின் தாக்கத்திலிருந்து காப்பது எப்படி?

1. இணைய பாவணைக்காக சுவாலைச்சுவரை (Firewall) பயன்படுத்துதல்.
2. கணினியின் பணிசெயலமைப்பு (Operating System) மற்றும் அனைத்து மென்பொருட்களையும் இற்றைப்படுத்துதல் (update)
3. இற்றைப்படுத்தப்பட்ட நம்பகமான எதிர்-வைரஸ் மென்பொருளைப் பயன்படுத்துதல்.
4. அறியா மூலங்களிலிருத்து வரும் இ-மெயில்களைத் திறவாதிருத்தல்
5. தெரிந்த மூலத்திலிருத்து வரும் இ-மெயில்களாயிருந்தாலும் உள்ளடக்கத்தை அறியாத இணைப்புக்களைத் திறவாதிருத்தல்.
6. இ-மெயில்களின் இணைப்புக்களைத் திறப்பதற்கு முன் வைரஸ் பரிசோதனை செய்தல்.
7. சந்தேகத்திற்குரிய *வலைத்தளங்களுக்கு* சஞ்சரிப்பதைத் தவிர்த்தல்
8. இணையத்தில் அறியா மூலங்களுக்குத் தம்மைப்பற்றிய தனிப்பட்ட விபரங்களை (இ-மெயில் முகவரி, வங்கிக் கணக்கு எண்கள், கடனட்டை எண்கள்) வழங்காதிருத்தல்
9. இணையத்திலிருந்து பதிவிறக்கம் செய்யும்போது நம்பிக்கைக்குரிய இணையத்தளங்களிலிருந்து மட்டும் பதிவிறக்கம் செய்தல்.

சுவாலைச்சுவர் (Firewall) என்றால் என்ன?

சுவாலைச்சுவர் என்பது வேறொரு வலையமைப்பிலிருந்து நமது *வலையமைப்பிற்குள்* நுழைய முற்படும் தரவுகளுக்கு வழிவிடுதலோ அல்லது தடுத்தலோ செய்யும் ஒரு மென்பொருளோ அல்லது வன்பொருளாகும். உதாரணம்: ஒரு நிறுவனத்தின் கணினி வலையமைப்பின் மூலம் இணையத்திற்கு பிரவேசிக்கும் போது, வெளி நபர்கள் நிறுவனத்தின் தரவுகளை *இணையத்தினூடாக* கையகப்படுத்தலைத் தடுப்பதற்கும், இணையத்திலிருந்து நிறுவனத்திற்குள் பிரவேசிக்கும் தரவுகளைக் கட்டுப்படுத்துவதற்கும் சுவாலைச்சுவர் பயன்படுத்தப்படும்.

இதே போன்று நமது தனிநபர் கணினிகளுக்கும் சுவாலைச்சுவரை நிறுவுவதன் மூலம் இணையத்திலிருந்து வரும் வைரஸ் தாக்கத்திலிருந்து பாதுகாத்துக்கொள்ள முடியும். சுவாலைச்சுவர் மூலம் அதனூடாக செல்லும் அனைத்து தரவுகளும் பரிசோதனைச் செய்யப்பட்டு அவற்றின் சேரிடங்களுக்கான அனுமதி வழங்கப்படும். இவை அனைத்தும் பாவனையாளர் வழங்கும் விதிமுறைக்கு அமையவே செய்யப்படும்.

எதிர்வைரஸ் (Anti-Virus) மென்பொருள் என்றால் என்ன?

எதிர்வைரஸ் (Anti-Virus) மென்பொருள் என்பது ஸ்பைவெயார், ட்ரோஜன் ஹோர்ஸ், எட்வெயார், வ(ர்)ம் பொன்ற அனைத்து கணினி வைரஸ் மென்பொருள்கள் நமது கணினியில் நுழையா *வண்ணம்* தடுத்தல் முதல் அவற்றை அடையாளங் கண்டு நீக்குதல் போன்ற முக்கியமான காரியங்களைச் செய்வதற்காக உருவாக்கப்பட்ட *மென்பொருளாகும்*.

எதிர்வைரஸ் (Anti-Virus) மென்பொருள் எவ்வாறு செயல்படுகிறது?

எதிர்வைரஸ் (Anti-Virus) மென்பொருள் கணினி வைரஸ்களை *சோதனை* செய்யும் மற்றும் அடையாளங் காணும் முறையில் 2 விதமாகச் செயல்படுகிறது:

- முன்பெ அறியப்பட்ட வைரஸ்கள் உள்ளனவா என்று ஆராய்தல்
- வைரஸ் எனச் சந்தேகம் ஏற்படும் வகையில் செயல்படும் கணினி செய்நிரல்களை ஆராய்தல்

முன்பே அறியப்பட்ட வைரஸ்கள் உள்ளனவா என்று ஆராய்தல்

இதன்போது எதிர்வைரஸ் மென்பொருளை உருவாக்கும் போதே இனங்காணப்பட்டிருந்த வைரஸ் வகைகளின் அடையாளங்கள் அடங்கிய தரவுத்தளம் ஒன்று உபயோகப்படுத்தப்படும். புதியதொரு கோப்பைப் பரிசோதனைச் செய்யும் போது *முன்பே* அறியப்பட்ட வைரஸ்கள் உள்ளனவா என்று பரிசோதனை செய்து, அத்தகைய வைரஸ் காணப்பட்டால் அதனை அழித்தல் அல்லது தனிமைப்படுத்துதல் (Quarantine) அல்லது கோப்பு செம்மையாக்கம் செய்யப்படும். இதன் மூலம் அந்த வைரஸ் பரவுதல் தடுக்கப்படும். ஒவ்வொரு நிமிடமும் புதுப்புது வைரஸ்கள் இனங்காணப்படுவதால் வைரஸ் வகைகளின் அடையாளங்கள் அடங்கிய தரவுத்தளம் இற்றைப்படுத்தப்படுகிறது. ஆகவே நாமும் நமது எதிர்வைரஸ் (Anti-Virus) மென்பொருளை *இற்றைப்படுத்தல்* மூலம் புதிய வைரஸ்களின் தாக்கத்திலிருந்து எமது கணினியைப் பாதுகாத்துக் கொள்ளலாம்.

எதிர்வைரஸ் மென்பொருளொன்றை நிறுவிய பின்னர், நமது கணினியை துவக்கும் போதே எதிர்வைரஸ் மென்பொருளும் செயல்பட ஆரம்பித்துவிடும்.

வைரஸ் என சந்தேகம் ஏற்படும் வகையில் செயல்படும் கணினி செய்நிரல்களை ஆராய்தல்

இதன்போது *முன்பே* அறியப்பட்ட வைரஸ்கள் உள்ளனவா என்று பரிசோதனை செய்வதற்குப் பதிலாக ஒவ்வொரு *கோப்பும்*, ஒவ்வொரு செய்நிரலும் பரிசோதனை செய்யப்படும். உதாரணமாக ஒரு செய்நிரல் மூலம் கணினியின் நிறைவேற்றுத்தகு கோப்பினுள் (Executable File) எழுத முற்படும் போது அச்செய்நிரல் சந்தேகத்திற்குரிய செய்நிரலாக அடையாளங் காணப்பட்டு எச்சரிக்கை விடுக்கப்படும். பாவனையாளரின் முடிவைப் பொறுத்து அச்செய்நிரல் தொடர்ந்து செயலாற்ற அனுமதிப்பதா அல்லது கணினியிலிருந்து நீக்கப்பட வேண்டுமா எனத் தீர்மானம் செய்யப்படும். இந்தத் தொழில்நுட்பத்தைப் பயன்படுத்தும் எதிர்வைரஸ் மென்பொருளின் மூலம் இதுவரை இனங்காணப்படாத வைரஸ்களின் தாக்கத்தின் அளவைக் குறைக்கலாம்.

எதிர்வைரஸ் (Anti-Virus) மென்பொருள் ஒன்றைத் தெரிவு செய்யும் போது கருத்தில் கொள்ள வேண்டிய விடயங்கள் எவை?

இன்று உலகில் பலவகையான எதிர்வைரஸ் மென்பொருள்கள் காணப்படுகின்றன. ஆகவே உங்களது தேவைக்கேற்ற எதிர்வைரஸ் மென்பொருளைத் தேர்ந்தெடுக்க வேண்டும். ஆயினும் எந்தவொரு சிறந்த எதிர்வைரஸ் மென்பொருளுக்கும் *பொருத்தமான* விடயங்களாவன யாதெனில்:

1. சுயமாகவே இற்றைப்படுத்திக் கொள்ளும் ஆற்றல்
2. சுயமாகவே வைரஸ் பரிசோதனை செய்யும் ஆற்றல்
3. எதிர்வைரஸ் மென்பொருள் நமது இ-மெயில் *செய்நிரலோடு* இயைந்து செயலாற்றுதல்
4. எதிர்வைரஸ் மென்பொருள் உற்பத்தியாளர் இற்றைப்படுத்தப்பட்ட வைரஸ் வரையறைகளைத் தொடர்ச்சியாக வழங்குதல்.
5. எதிர்வைரஸ் மென்பொருள் உற்பத்தியாளரால் புதிதாக இனங்காணப்படும் வைரஸ் பற்றிய சரியானதும் காலத்துக்கு பொருத்தமானதுமான தகவல்களை வெளியிடுதல்

இன்றைய உலகில் பிரசித்திப் பெற்ற சில எதிர்வைரஸ் மென்பொருள்கள்:

1 Kaspersky Lab	6 Trend Micro
2 McAfee	7 F-Secure
3 Symantec	8 Sophos
4 Avast	9 Bitdefender
5 ESET	10 Microsoft Security Essentials

உங்கள் கணினியின் பாதுகாப்புப் பற்றியோ அல்லது ஏதெனும் வைரஸ் சம்பந்தமாகவோ கேள்விகள் இருப்பின் கீழ்காணும் முகவரியுடன் தொடர்பு கொள்ளவும்.

If you have any questions, please inform us:

https://techcert.lk/en/report-form
தொலைபேசி - +94 11 4 462 562
மின்னஞ்கல் - help@techcert.lk

This document was prepared by the Training Division of LK Domain Registry in collaboration with the Internet Society Sri Lanka Chapter.
For more details please visit http://nic.lk/index.php/training-materials.