ÇFARË ËSHTË MALWARE?

Malware i referohet çdo softueri që vendoset në një kompjuter ose rrjet, i krijuar për një qëllim keqdashës. Infektimi me malware zakonisht ndodh pa dijeninë e përdoruesit, sepse ai maskohet si një lloj skedari imazh ose skedar PDF.

Ky lloj softueri mund të prekë kompjuterat edhe celularët. Ai shërben për qëllime të ndryshme si vjedhja e informacionit, gjurmimi i shtypjes së tasteve të tastierës e madje edhe përdorimi i harduerit të një kompjuteri si miniera për kriptomonedhat.

Malware është jashtëzakonisht i përhapur. Shkalla me të cilën shumëfishohen disa lloje malware i bën ata një armik të fuqishëm edhe për profesionistët më të kualifikuar të IT-së. Sukseset e përsëritura të sulmeve malware lënë të kuptohet që ka mjaft aktorë keqdashës të gatshëm për t'i krijuar dhe shpërndarë ato.

Për të qënë efektivë, shumica e malwarëve shfrytëzojnë dobësitë që gjenden në sisteme dhe aplikacione. Përdorimi në rritje eksponenciale i kompjuterit, celularit dhe pajisjeve inteligjente të lidhura në internet, u ofron mjaft opsione sulmuesve kibernetikë për të infektuar dhe kompromentuar teknologjinë.

Cilat janë llojet e malware?

Llojet e malware ndahen në dy kategori: sipas mënyrës së infektimit dhe sipas qëllimi të tij pasi të jetë aktiv.

Më poshtë listohen llojet më të zakonshme të malware:

Mënyra e infektimit

Një nga arsyet pse malware është kaq i përhapur është se ai ka shumë metoda të ndryshme shpërndarjeje. Kryesisht, infektimi me malware ndodh kur përdoruesit gabimisht ose pa kujdes hapin në kompjuterin e tyre një skedar keqdashës të ekzekutueshëm.

Fishing

Mesazhet phishing, janë mënyra më e zakonshme për të vendosur malware në një kompjuter. Skedari bashkëngjitet në mesazh ose përdoruesi drejtohet nëpërmjet një linku të shkarkojë malware nga një vend tjetër në internet ku ai është ruajtur.

USB

Kriminelët kibernetikë shpesh hedhin ose lënë në vend të dukshëm, pajisjet USB që përmbajnë skedarë me emra joshës që kushdo që e gjen të futë USB-në në kompjuter dhe të hapë skedarin per të vendosur malware.

Faqet e internetit

Faqet e internetit mund të përdoren për të vendosur malware tek kompjuteri i një vizitori te saj që nuk ka dyshime per rezikun e infektimit. Kjo bëhet e mundur përmes faqeve të rrjeteve sociale ose web site legjitim të kompromentuar.

Skedarët e infektuar

Skedarët dhe programet legjitime mund të infektohen me virus. Pasi hapen, ato do të funksionojnë siç pritej, dhe pa u vënë re do të instalojnë malware në pajisje pa dijeninë e përdoruesit.

Rrjeti

Ky është lloji malware që përveç infektimit të objektivit të tij kryesor, kërkon të përhapet në pajisje të tjera të lidhura me të në të njëjtin rrjet. Pasi ky malware instalohet nëpërmjet njërës prej menyrave të mësipërme, ai kërkon pajisje të tjera për ti infektuar.

Qëllimi i malware pasi të jetë aktiv

Vjedhja e informacionit

Ky lloj malware regjistron shtypjen e tasteve kur vendosen të dhena sensitive si nformacioni i kartës së kreditit dhe detajet e loginit, ose kërkon në kompjuter për informacione sensitive dhe ia dërgon sulmuesit.

Pengim dhe shkatërrim

Ky lloj malware merr kontrollin e kompjuterit dhe e kyç atë ose skedarët e tij, derisa të paguhet një shpërblim, zakonisht në kriptomonedhë. Ky malware përdoret gjithashtu për të dëmtuar veprimtarine e një organizate ose një agjencie qeveritare, duke i penguar ata të ofrojnë shërbimet e tyre.

Komanda dhe kontrolli

Ky lloj malware është një softuer kqedashës i krijuar për të përdorur burimet e një kompjuteri për të kryer aktivitete të tjera të paligjshme pa e vënë re përdoruesi, të tilla si kryerja e sulmeve kibernetike ndaj pajisjeve të tjerë, shitja e mallrave të paligjshme, mbajtja e skedarëve të paligjshëm, apo edhe mbajtja e minierave të kriptomonedhës.

Si zbulohet dhe hiqet malware

Natyra e malware varet nga fshehja e tij dhe sfida për t'u hequr nga pajisja e infektuar. Malware zbulohet duke identifikuar simptomat e tij, të tilla si, kompjuteri bëhet papritmas më i ngadalshëm, lidhja në internet bëhet më e ngadaltë, skedarët zhduken, dalin reklama pop-up pa hapur një shfletues (browser) ose, në raste ekstreme, kontrolli i plotë i makinës.

Nëse sulmi i malware bëhet me anë të email, mënyra më e mirë për të zbuluar malware është leximi me kujdes i prapashtesave të skedarëve (kujdes nese ka prapashtesën .exe).

Heqja e malware mund të jetë shumë e vështirë, por ndjekja e hapave të mëposhtëm e bën procesin më të lehtë:

1. Shkëputeni makinën e infektuar nga linja e internetit, si dhe nga çdo rrjet ku bën pjesë. Kjo masë paraprake siguron që malware të mos përhapet dhe ndalon dërgimin e informacioneve shtesë tek hakerat.
2. Kryeni një skanim te kompjuterit me programin antivirus. Në shumicën e rasteve, antivirusi jo vetëm që zbulon malware, por gjithashtu do të kujdeset për heqjen e sigurt të tij. Ky hap bëhet në modalitetin e sigurt të Windows dhe nëse skanimi me programin antivirus nuk zbulon gjë.
3. Nëse kompjuteri duket se është ende i infektuar, pastroni skedarët e përkohshëm përmes mjetit Disk Cleanup ndërsa jeni në modalitetin e sigurt të Windows.
4. Kontaktoni komunitete të sigurisë kibernetike për këshilla dhe praktika më të mira, pasi mund të kenë përvojë në heqjen e programeve specifike të dëmshme.
5. Kontaktoni suportin e antivirusit pasi mund të ketë mjete ose shërbime shtesë për t'ju ndihmuar të rikuperoheni nga një infeksion malware.

Si parandalohet infektimi me malware

Parandalimi është mënyra më e mirë e mbrojtjes nga malware. Kjo arrihet përmes përdorimit të softuerit përkatës, dhe kryesisht përmes zbatimit të udhëzimeve me të mira të sigurisë kibernetike nga përdoruesit për të parandaluar infektimet me malware ose për të zvogëluar ndikimin e tyre:

1. Antivirusi duhet të jetë i përditësuar. Antivirusi është një softuer mjaft i mirë pasi ka databazën me malware të nënshkruar (të njohur) me të cilat mund të krahasojë skedarët nëse janë të infektuar. Për të bërë përditësim të rregullt, duhet të aktivizoni përditësimet automatike.
2. Përdorni vetëm softuer legjitim. Metoda tipike e dërgimit të malware tek objektivi është nëpërmjet versioneve të komprometuara të softuerëve të njohur. Në kompjuterët dhe serverët e kompanisë duhen instaluar gjithmonë softuerët që janë të miratuar paraprakisht.
3. Vendosni një politikë të përdorimit të pajisjes celulare. Duhen vendosur rregulla per ndalimin e përdoruesve që të lidhin pajisjet e tyre celulare në çfarëdo lloj mënyre me pajisjet e tyre të punës. Përmes një lidhjeje USB, mund të transmetohen shumë forma të malware nga celulari në desktop.
4. Identifikoni emailet e jashtme. Përdoruesit e postës elektronike të kompanisë suaj duhet të kenë një cilësim që shfaq një etiketë EXTERNAL pranë emaileve që vinë nga një organizatë e jashtme. Ky rikujtues vizual i bën përdoruesit e emailit të jenë tepër vigjilentë me shkarkimet e skedarëve.
5. Mbani të përditësuara sistemet dhe aplikacionet. Sistemet operative dhe softuerët e tjerë duhet të kenë marrë update te versionit më të fundit të tyre për të siguruar që të gjitha patch-et janë instaluar.
6. Ulja e privilegjeve administrative. Përdoruesit nuk duhet të kenë privilegje administrative në vendet e tyre të punës. Kjo masë paraprake parandalon çaktivizimin aksidental të kontrolleve të sigurisë ose instalimin e softuerit të padëshiruar.

7. Rezervoni të dhënat elektronike (backup). Mbrojtja më e mirë ndaj ransomware është strategjia e ruajtjes (backup) të të dhenave.
8. Berja share e skedarëve. Kufizoni vendndodhjet dhe shërbimet për bërjen share dhe shkarkimin e skedarëve. Shërbimet falas dhe publike të ndarjes (share) të skedarëve mund të mbajnë malware të maskuar si skedarë të tjerë.
9. Kryeni simulime të rregullta phishing. Këto simulime lejojnë të identifikohen dobësitë e mundshme përpara se ato të shfrytëzohen nga sulmuesi kibernetik dhe është një mundësi e mire mësimore për përdoruesit.
10. Ndërgjegjësimi. Duhen bërë trajnime të rregullta për ndërgjegjësimin e të gjithë punonjësve për sigurinë e informacionit, që të jenë të informuar se si të parandalojnë infektimin me malware dhe çfarë të bëjnë në rastin e një sistemi të kompromet uar.