5 SITUASJONER DER DU IKKE VISSTE DU KUNNE BLI INFISERT MED VIRUS, SKADE-PROGRAMMER, ELLER BLI HACKET

De fleste er kjent med de vanligste typene skadeprogrammer: nettfisking, reklameprogrammer, spionprogrammer, virus, ormer og lignende. Men etter som teknologien forbedres, blir også nettkriminelle smartere. De forsøker å angripe under radaren for å få tak i informasjonen din. Derfor dukker det stadig opp nye former for skadeprogrammer, som du kanskje ikke er oppmerksom på.

SVINDEL OG SKADE-PROGRAMMER PÅ SOSIALE MEDIER

Gråvare er en type skadeprogram som ikke direkte skader dataene dine fysisk, slik som andre skadeprogrammer. De har en mer irriterende virkemåte som likner på reklameprogrammer og spion-programmer. Gråvare oppstår ofte på sosiale medier, vanligvis i form av "klikk agn", der en fristende artikkel tar deg til et nettsted der du blir bedt om å fylle ut en rask undersøkelse før du får tilgang til mediet. Denne informasjonen samles inn og selges til nettkriminelle, og kan deretter brukes til å hacke inn på de personlige kontoene dine. Hvis du vil lære mer om denne typen svindel og hvordan du kan beskytte deg mot den, kan du se artikkelen "Social Media Scams Based on Current Events" (Svindel på sosiale medier, basert på aktuelle hendelser) som er tilgjengelig på Norton.com.

Ikke bare er gråvare vanlig på disse plattformene, men det er også høy risiko for komme i kontakt med farlige skade-programmer på sosiale nettverk.

Da TV-showet Breaking Bad var i populært, fantes det en populær Twit-ter-svindel som forårsaket kaos. Koblinger ble lagt ut for å lokke brukere til å laste ned en neste uviste episode. Hvis brukerne klikket på koblingen, ble de omdirigert til en side som lastet ned en fil. Siden ledet brukerne til en annen kobling for å installere et program for å spille av videoen. Koblingen sendte brukere til et affiliate-program, som spammerne tjente penger på. Denne svindelen så ut til å være ganske ufarlig for brukernes datamaskiner, men det finnes andre tilfeller der det som lastes ned kan være et farlig skadeprogram. Vær alltid forsiktig når du klikker på ukjente koblinger og prøver å laste ned ukjente filer.

UTNYTTINGSVERKTØY

Utnyttingssett er generelt hva navnet tilsier, dvs. et skadelig verktøysett som gjennomsøker datamaskinen din for å se etter programvare som ikke er oppdatert. Disse verktøyene leter etter sikkerhet-shull i programvare, med det formål å plassere skadeprogrammer på brukerens datamaskiner. Dette kan skje når brukerne besøker nettsteder som inneholder skadelig reklame. Malvertis-ing finnes på alle typer nettsteder, både klarerte og ukjente, og det bruker elektronisk annonsering ved å bygge inn skadelig kode i legitime annonser. Nylig ble Yahoo utsatt for dette. De ble brukt som vert for skadelige annonser som omdirigerte brukerne til nettsteder som styrer disse verktøyene. Utnyttingssett finnes imidlertid ikke alltid i malvertising. Det populære nettstedet, Askmen.com, ble nylig kompromittert ved å omdirigere brukere til et nettsted som brukte et utnyttelsesverktøy. Derfor er det svært viktig å sørge for at alle programmene dine er oppdatert til enhver tid.

MOBIL RANSOMWARE

Ransomware på datamaskiner er ikke en ny trussel, men nylig har den begynt å migrere til populære mobilplattformer. Ransomware er et program som angriper viktige filer, for eksempel bilder og dokumenter, og krypterer dem, slik at brukeren ikke lenger får tilgang til dem. Brukeren mottar deretter en melding som ber om betaling for å låse opp filene. De første versjonene av mobil ransomware ble oppdaget tidligere i år. Du utsettes for ransomware når du besøker et infisert nettsted. Det lastes automatisk ned til telefonen eller via nedlasting av en skadelig app. Hvis enheten din blir infisert, må du ikke betale gebyret! I stedet må du sørge for å sikkerhets-kopiere regelmessig og gjenopprette telefonen fra den nyeste sikkerhets-kopien. Du kan finne ut hvordan du oppdager falske mobilapper ved å lese "Hvordan gjenkjenne en falsk Android-app" på Norton.com.

SKADEPROGRAMANGREP UNDER NETTBASERT SPILLING

Flere tilfeller av skadeprogrammer for spill er rapportert i nyhetene i det siste. Denne typen skadeprogram koster deg kanskje ikke penger, men det kan føre til bortkastet tid. Nettpratrommene til Twitch.tv, et nettsted som brukes til å strømme direkte nettbasert spilling, ble nylig infiltrert av en bot som lokket brukere ved hjelp av loddtrekninger. Når brukerne klikker på koblingen for å delta i loddtrekningen, vises et tomt Java-skjema. Når brukeren fyller ut skjemaet, installeres skadeprogrammet på brukerens datamaskin, der det angriper brukerens Steam-konto og sletter hele Steam-lommeboken og annet innhold. Deretter selger de nettkriminelle brukerens eiendeler i Steam-fellesskapet. På samme måte oppsto det et problem med en skadelig trojansk hest i det populære World of Warcraft-spillet, der den var maskert som et legitimt spill-tillegg. Når den trojanske hesten er installert, overtar den helt kontroll over brukerens konto. Vi anbefaler sterkt at brukerne ikke deaktiverer antivirusprogrammer når de spiller nettbaserte spill.

REKLAMEPROGRAMMER OG SKADEPROGRAMMER I LESERUTVIDELSER

Leserutvidelser er veldig populære tilleggsprogrammer som brukes til å utføre en rekke oppgaver mens du surfer på Internett. Men vi vedder på at du ikke er klar over at enkelte av dem kan stjele informasjonen din! Noen skadelige utvidelser vil enten spore alle nettstedene du besøker, eller de vil sette inn reklame-programmer på disse nettstedene. Selv om dette ikke er et stort problem når det gjelder dataene på datamaskinen, er det et ganske stort problem når det gjelder personvern. Angripere kan bruke disse utvidelsene til å utføre klikksvindel ved å legge til falske annonser på nettsteder og omdirigere deg til disse nettstedene. Selv om dette har et lavere trusselnivå, kan denne nyere formen for skadeprogram-mer utvikle seg til noe som er mye mer invaderende. Faktisk har ENISA (Euro-pean Union Agency for Network and Information Security) utstedt advarsler om at det har vært en økning i skadelige leserutvidelser som prøver å overta kontrollen av kontoer på sosiale nettverk. Så, selv om de for øyeblikket ikke er øverst på trusselslisten, bør du definitivt holde øye med dem.

Internett-trusler kan dukke opp i alle former og størrelser, og det finnes mange du sikkert ikke er oppmerksom på. Vi beskytter deg så du ikke trenger å bekymre deg om den minste detalj. Dermed kan du i stedet fokusere på hverdagen din og overlate de kompli-serte tingene til oss.