



RAPPORT

# **FORSVARET MOD MALWARE - BESKYT JERES NETBUTIK, KUNDERNE OG BUNDLINJEN**

## INDHOLD

3 MALWARE KRYBER IND PÅ WEBSTEDER OVERALT

3 HVAD ER MALWARE?

4 MØNSTRENE FOR MALWARE-ANGREB

5 “FORRETNINGSMODELLEN” FOR MALWARE

6 KONKLUSION

6 OM VERISIGN



# FORSVARET MOD MALWARE – BESKYT JERES NETBUTIK, KUNDERNE OG BUNDLINJEN

## MALWARE KRYBER IND PÅ WEBSTEDER OVERALT

I denne rapport forklares truslen fra malware, og hvordan denne kan påvirke jeres netbutik. Der gives en beskrivelse af, hvilke motivationer kriminelle har for at distribuere malware på nettet, og hvordan de inficerer webservere for at muliggøre distributionen. Desuden fremhæves de metoder, som administratorer kan anvende til at registrere, hvornår og hvordan hackere har inficeret en netbutiks webserver.

Desuden gennemgås øvrige kritiske punkter vedrørende malware:

- Hvordan hackere distribuerer malware via webbrowsere i stedet for med traditionelle metoder, som f.eks. inficerede vedhæftede filer i e-mails.
- Hvilke økonomiske motivationer moderne kriminelle har for at inficere slutbrugersystemer.
- Hvordan malware distribueres ved at inficere legitime websteder.
- Hvilke programmer der findes til at inficere så mange websider som muligt.
- Hvordan netkriminelle har udviklet angrebsteknikker, der gør det muligt for malware at inficere tusindvis af websteder på én gang ved at udnytte sårbarheder på websteder.
- Hvordan hackere distribuerer skadelig kode via falske annoncer med det formål at inficere de mest populære og ofte godt beskyttede websteder.

## HVAD ER MALWARE?

Malware er en generel betegnelse for skadelig software, og dette er et voksende problem på internettet. Hackere installerer malware ved at udnytte svagheder i sikkerheden på jeres webserver for at få adgang til jeres websted. Malware omfatter alt fra adware, som popper uønskede reklamer op, til trojanske heste, der kan hjælpe kriminelle med at stjæle fortrolige oplysninger, som f.eks. legitimationsoplysninger til netbanker.

Malware distribueres i stigende omfang via webbrowsere. Denne taktik er blevet mere udbredt i de senere år, fordi filtrering af e-mail har gjort det vanskeligere for hackere at distribuere deres programmer via spammail. Og fordi

firewalls desuden er blevet mere udbredt på arbejdspladsen og i hjemmet, er det blevet sværere for malware at sprede sig fra system til system via netværk. Via internettet har hackere mulighed for at trænge ind på jeres websted og bruge det som vært til at sprede malware til jeres kunder.

Malware-kode er vanskelig at opdage og kan inficere kundernes computere blot ved, at de går ind på jeres websted. Denne form for malware kaldes "drive-by" malware, og brugerne er stort set ikke (eller overhovedet ikke) klar over, at deres computere er blevet inficeret, hvilket gør det til et særligt lumsk problem. Hackere bruger drive-by malware til at sprede vira, gøre ulovlig brug af computere eller stjæle følsomme data, som f.eks. kreditkortnumre eller andre personlige oplysninger.

## Hvordan fungerer drive-by malware, og risikerer små websteder at blive ramt?

Drive-by malware downloader sig selv på en brugers computer uden dennes tilladelse. Netkriminelle udnytter svagheder i browsere og/eller plug-ins til at overføre malware ved at skjule den skadelige kode i websider som usynlige elementer (f.eks. en iframe eller obfuscator) eller ved at indlejre den i et billede (f.eks. en flash- eller PDF-fil), som uset kan overføres fra webstedet til den besøgendes computer. Alle websteder er i farezonen. Små websteder kan være mere sårbare, fordi der her sandsynligvis er færre ressourcer og mindre ekspertise til rådighed til at opdage og reagere hurtigt på angreb.

Malware kan inficere jeres kunders computere blot ved, at de besøger jeres websted. Ved at udvælge websteder med få besøgende kan der gå længere tid, inden hackere bliver opdaget, så de kan nå at forvolde mere skade.



## MØNSTRENE FOR MALWARE-ANGREB

For at inficere en computer via en webbrowser skal en hacker først gøre to ting. For det første skal han/hun finde på en måde at få forbindelse til ofret på. Dernæst skal hackeren installere malware på ofrets computer. Begge dele kan ske meget hurtigt og uden ofrets viden afhængig af hackerens taktik.

En metode, som en hacker kan benytte til at få et offers browser til at køre den skadelige kode, er ganske enkelt ved at invitere ofret til at besøge et websted, som er inficeret med malware. Selvfølgelig vil næppe nogen besøge et websted, hvis de får at vide, at det er inficeret. Derfor må hackeren skjule sine lumske hensigter med webstedet. Avancerede hackere anvender de nyeste overføringsmetoder og sender ofte malware-inficerede meddelelser via sociale netværk, som f.eks. Facebook, eller via instant messaging-systemer. Denne metode giver ganske vist resultater til en vis grad, men den er afhængig af, at brugerne bliver lokket til at besøge et bestemt websted.

Andre hackere udvælger websteder, som potentielle ofre besøger af sig selv. I dette tilfælde bryder hackeren ind på det udvalgte websted og indsætter en stump html-kode, der har forbindelse til hackerens server. Denne kode kan indlæses hvor som helst fra, f.eks. et helt andet websted. Hver gang en bruger besøger et websted, som er inficeret på denne måde, har hackerens kode mulighed for at inficere brugerens computer med malware.

---

### Typiske metoder til overføring af malware:

- **Bannerannoncer:** Med denne metode (som også kaldes "malvertising") klikker brugerne intetanende på en bannerannonce, som dernæst forsøger at installere skadelig kode på brugerens computer. Alternativt kan annoncen henvise brugerne til et websted, hvor de bliver bedt om at downloade en PDF med skadelig kode, som er vanskelig at opdage, eller de bliver bedt om at udlevere betalingsoplysninger for at få adgang til at downloade en PDF.
  - **Dokumenter til at downloade:** Brugere lokkes til at åbne et velkendt program, f.eks. Microsoft Word eller Excel, som indeholder en forinstalleret trojansk hest.
  - **Man-in-the-middle:** Med denne metode forledes brugerne til at tro, at de befinder sig på et websted, de kan have tillid til. I realiteten indsamler en netkriminal de data, som brugeren udleverer på webstedet, f.eks. brugernavn og adgangskode. Eller en kriminel kan ulovligt overtage en session og holde den åben, efter at brugerne tror, at de har lukket den. Derefter kan den kriminelle foretage sine ondsindede transaktioner. Hvis brugeren har brugt en netbank, kan den kriminelle overføre penge. Hvis brugeren har bestilt varer, kan den kriminelle få adgang til og stjæle det kreditkortnummer, som er brugt ved transaktionen.
  - **Softwareopdateringer:** Malware opslår invitationer på sociale mediewebsteder, hvor brugerne tilbydes at se en video. Linket forsøger at narre brugerne til at tro, at de er nødt til at opdatere deres nuværende software for at kunne se videoen. Den tilbudte softwareopdatering er skadelig.
  - **Keylogger:** Brugere narres til at downloade keylogger-software ved hjælp af en af ovennævnte metoder. Derefter overvåger keyloggeren bestemte brugerhandlinger, f.eks. brug af musen eller tastaturet, og tager billeder af skærmen for at opsnappe personlige bank- eller kreditkortoplysninger.
- 



## “FORRETNINGSMODELLEN” FOR MALWARE

Hvordan bruger hackere malware til personlig vinding? De kan bruge inficerede computere til at få økonomisk gevinst på mange måder. En af de enkleste måder er ved hjælp af annoncer. Akkurat som mange websteder får en indtægt ved at opslå annoncer, kan malware vise annoncer, som giver den netkriminelle en indtægt.

Eller det kan ske i form af afpresning. Et stort netværk af inficerede computere kan opnå stor processorkraft, og nogle hackere anvender denne trussel til at afpresse penge fra webstedsejere. En gruppe computere, som er under enkelt hackers kontrol (et såkaldt “botnet”), kan sende store mængder netværkstrafik til et udvalgt websted, hvilket kan resultere i et DoS-angreb (Denial of Service). Derefter tager den kriminelle kontakt til webstedets ejer og forlanger penge for at stoppe angrebet. Kriminelle anvender desuden ofte inficerede computere til at indsamle brugbare brugeroplysninger, som f.eks. legitimationsoplysninger til netbanker. Denne type malware, der kaldes en infostealer (trojansk hest til afluring af bankdata), er en af de mest avancerede og bedst skjulte former for malware. Derefter kan den kriminelle bruge de private oplysninger til sine ondsindede planer eller sælge dem videre til en tredjepart, som derefter bruger dem til at få økonomisk gevinst.

---

## Hvad er sortlistning, og hvorfor er det vigtigt at undgå?

På grund af de mulige skadevirkninger, som malware kan forårsage, sætter Google, Yahoo, Bing og andre søgemaskiner websteder, hvor der er konstateret malware, på en spærreliste (også kaldet at “sortliste”). Hvis et websted bliver sortlistet, advarer søgemaskinen potentielle besøgende om, at webstedet ikke er sikkert, eller udelukker helt links til webstedet i søgeresultater.

Uanset hvor meget et websted er søgemaskineoptimeret, kan det have katastrofale konsekvenser, hvis webstedet bliver sortlistet. Sortlistning kan ske uden varsel, det sker ofte uden webstedsejerens vidende, og det er meget vanskeligt at genoprette webstedets renommé igen. Det er afgørende for et websteds succes – også på sigt – at tage de korrekte foranstaltninger for at undgå, at det bliver sortlistet i søgemaskiner.

---

## VERISIGN ER FORTSAT DEN FØRENDE LEVERANDØR AF NETSIKKERHED

VeriSign var pioneren, der lancerede den første kommercielle SSL-løsning midt i 1990'erne, og er i dag markedets førende leverandør af SSL-certifikater. Desuden er VeriSign det kendteste internetsikkerhedsmærke i verden i dag. Dette omdømme blandt både forbrugere og netbutikker er opbygget gennem mange år ved at være på forkant i branchen og anvende markedets mest avancerede teknologi til VeriSigns førende SSL-løsninger.



Ud over at tilbyde trygheden ved et anerkendt SSL-certifikat har VeriSign løbende opfyldt sine kunders behov ved konstant at udbygge og forbedre sit SSL-løsningsassortiment via understøttelse af nye standarder og integrering med supplerende teknologier og løsninger. VeriSign fortsætter traditionen med at tilbyde daglig scanning af websteder for malware som en del af sine SSL-løsninger for at beskytte jeres websted, jeres værdifulde brand og jeres kunders fortrolige oplysninger mod det konstant skiftende trusselsbillede på internettet.



## KONKLUSION

Netbutikker og udbydere af tjenester på nettet har oplevet en utrolig vækst i løbet af det seneste årti. Men den stadigt mere udbredte brug af internettet i almindelige menneskers hverdag har samtidig medført en stigning i netkriminalitet. Malware er blevet mere omsiggribende og bringer væksten i e-handel i fare ved at skabe frygt for misbrug af personlige oplysninger. Det forringer tilliden og giver netbutikker dårligere resultater. Der er brug for en effektiv metode til at bekæmpe brugen af malware, hvis e-handlen skal kunne udnytte sit fulde potentiale.

VeriSign tilbyder en komplet netsikkerhedsløsning, som kan hjælpe med at sikre jeres succes som e-handelsfirma ved at kombinere markedets bedste SSL-certifikater med innovative funktionaliteter, som bl.a. sørger for regelmæssig overvågning af jeres offentligt tilgængelige websider for malware. Sammen med VeriSign-seglet, som er verdens mest anerkendte tillidsmærke, hjælper VeriSign jer med at give kunderne fuld tillid til sikkerheden på jeres websted. Hvis I vil sikre jer, at forbrugerne opfatter jeres websted som et sikkert sted at handle, er VeriSign SSL-certifikater den rigtige løsning for jer.

## OM VERISIGN

VeriSign er den digitale verdens anerkendte leverandør af infrastruktur tjenester til internettet. Flere milliarder gange hver eneste dag benytter firmaer og forbrugere vores internetinfrastruktur til at kommunikere og handle trygt på nettet.

**Få mere at vide på [www.Verisign.eu](http://www.Verisign.eu).**

