

Artikel Phishers vangen meer dan 3 miljard dollar in VS

Automatiseringsgids woensdag 19 december 2007, Stamford, 11:15 uur

Alleen al in de Verenigde Staten hebben phishers - lieden die nietsvermoedende computergebruikers via emails proberen op te lichten - dit jaar 3,2 miljard dollar 'verdiend' met hun activiteiten. Dat concludeert Gartner uit onderzoek. Het aantal slachtoffers groeide van 2,3 naar 3,6 miljoen, in de 12 maanden gerekend tot eind augustus.

De phishers worden niet talrijker, maar wel inventiever, want 3,3 procent van de ondervraagden zegt nu geld te hebben verloren na de ontvangst van een phishing-email, terwijl dat een jaar geleden 2,3 procent was (en 2,9 procent in 2005).

Volgens Gartner worden phishing-aanvallen vaker gebruikt om meteen malwareprogramma's op de pc van het beoogde slachtoffer te dumpen. Beschermende software wordt vaak niet gebruikt. Elf procent van de volwassenen gebruikt volgens Gartner helemaal geen beveiligingssoftware en nog eens 45 procent gebruikt dergelijke software alleen voor zover die gratis is te verkrijgen.

Doorgaans zijn de slachtoffers niet meer dan zo'n 200 dollar kwijt. Een aantal gevallen met grotere verliezen tillen het feitelijke gemiddelde schadebedrag het afgelopen jaar naar 866 dollar. Wel slaagden meer mensen er in (een deel van) hun geld terug te krijgen. (Freek Blankena)

UBM Global: Gebruik DriveLock Applicatie Launch Filter en voorkom daarmee het opstarten van niet geautoriseerde applicaties

- *Autoriseren en controleren van applicaties*
 - *Op client PC's*
 - *Binnen Terminal Services client sessies*
 - *Die actief zijn in het netwerk*
 - *Ter bescherming tegen aanvallen, inclusief zero-day attacks, waarvoor nog geen patches verkrijgbaar zijn*

- *Keuze uit operationele modes*
 - » *Whitelist mode: alleen specifieke applicaties zijn toegestaan*
 - » *Blacklist mode: specifieke applicaties worden geblokkeerd*
 - » *Scan mode: opstarten van applicaties wordt gelogd zonder toepassingsregels*
 - » *Test mode: regelverwerking is gelogd zonder blokkering van applicaties*

- *Templates kunnen worden gecreëerd van huidige lopende applicaties*
- *Blacklist en whitelist regels kunnen worden gecombineerd om uitzonderingen te creëren*
- *Werkingsprincipe*
 - » *Onderschept elke start van een applicatie*
 - » *Verwerkt een hash van de executable*

» *Vergelijkt deze hash met alle beschikbare whitelist en blacklist regels*