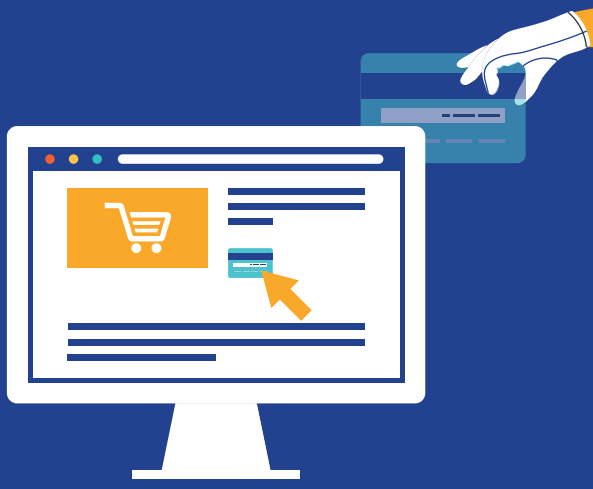
DIGITAALINEN SKIMMAUS

EUROPOL
EC3 | European Cybercrime Centre
POLIISI
POLICE OF FINLAND
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

MITÄ SE ON?

Merkittävä uhka

Digitaalinen skimmaus tarkoittaa verkkokaupan asiakkaiden maksukorttitietojen varastamista. Kortin tapahtumatiedot siepataan verkko-ostoksen maksutapahtuman aikana ilman, että asiakkaat huomaavat mitään tavallisuudesta poikkeavaa.



Rikos tunnetaan monella nimellä

Digitaalisesta skimmauksesta käytetään myös nimityksiä verkkoskimmaus, korttiskimmaus verkossa, digiskimmaus, formjacking eli tapahtumatietojen kaappaus ja Magecart-hyökkäys.

Magecart on yhdistelmä sanoista 'Magento' ja 'shopping cart'. **Magento** oli ensimmäinen hyökkäyksen kohteeksi joutunut avoimen lähdekoodin verkkokauppa-alusta. Magento tarkoittaa myös hyökkäysten takana toimivaa rikollisryhmää.

MITEN SE TOIMII?

Digitaalisessa skimmauksessa on yleensä kolme vaihetta:

Tietomurto
Rikolliset pääsevät käsiksi verkkokaupan lähdekoodiin/palvelimeen tai kolmannen osapuolen työkalun lähdekoodiin. Tämä voi tapahtua haavoittuvuuksien, konfigurointivirheiden tai väsytyshyökkäysten avulla.

Haittaohjelman syöttö
Maksuvirtaan syötetään haittaohjelma.

Tietojen keruu
Asiakas- ja maksutiedot kopioidaan. Tiedot voidaan kerätä välittömästi tai paljastumisriskin minimoimiseksi piilottaa palvelimelle myöhempää keruuta varten.

Asiakas ei tiedä, että hänen korttinsa on kopioitu (skimmattu). Asiakkaan näkökulmasta tilaus on tehty ja tilattu tuote saapuu ajallaan, eikä hänellä ole syytä epäillä, että jotain olisi mennyt pieleen.

DIGITAALINEN SKIMMAUS

EUROPOL
EC3 | European Cybercrime Centre
POLIISI
POLICE OF FINLAND
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

MITÄ PITÄÄ TIETÄÄ?

Digitaalinen skimmaus on kasvussa.
Hyökkäykset voivat jäädä pitkäksi aikaa piiloon.
Kun tietomurto lopulta huomataan,
se voi aiheuttaa verkkokaupalle mainehaittaa, koska käyttäjät kyseenalaistavat palvelun turvallisuuden.

MITÄ TEHDÄ YRITYKSEN SUOJAAMISEKSI?

Kyberrikollisten toimintaa voi vaikeuttaa seuraavasti:

Käytä erityisesti verkkoskimmauksen havaitsemiseen tarkoitettua ohjelmistoa.

Varmista, että työntekijöillä on monivaiheinen tunnistautuminen ja vahvat salasanat käytössä. Kouluta työntekijöitä torjumaan kohdennettuja tietojenkalasteluhyökkäyksiä.

Tarkista verkkokauppa-alusta säännöllisesti automaattisten haavoittuvuusskannausten avulla. Tarkista myös asennetut kolmannen osapuolen komponentit.

Varmista, että verkkokauppa-alustan ohjausnäkymään pääsee vain tietyistä IP-osoitteista. Estä työntekijöiden pääsy ohjausnäkymään tuntemattomista sijainneista.

Varmista, että tietoturvakorjaukset ja kriittiset ohjelmistopäivitykset asennetaan oikea-aikaisesti.

Ota käyttöön sisällön suojauskäytäntö (CSP) ja aliresurssin eheys (SRI). Ne vaikeuttavat haittakoodin syöttämistä verkkokauppaan.

ENTÄ JOS JOUDUT UHRIKSI?

- Jos kyseessä on haittaohjelmatartunta, vaihda heti kaikki ylläpitäjän ja tietokannan salasanat.
- Etsi hyökkääjien mahdollisesti asentamat takaovet haittaohjelmaskannerin avulla.
- Kerää kaikki saatavissa olevat todisteet ja ilmoita hyökkäyksestä poliisille.
- Jos kyseessä on henkilötietoja koskeva tietoturvaloukkaus, toimi sovellettavan tietosuojalainsäädännön mukaisesti.