



Quarantine

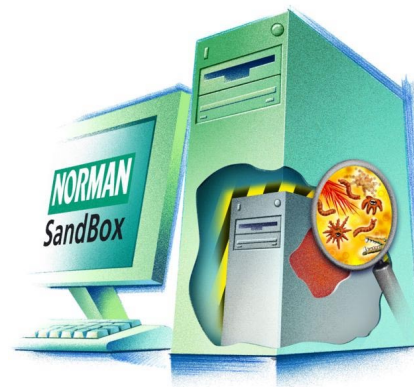


Statistics



Unread mail

Norman SandBox v2



Toisen sukupolven Norman SandBox –virustorjuntateknologia sisältää useita merkittäviä parannuksia edelliseen versioon verrattuna. Tietoverkkojen jäljittely sekä edistyneempi tunnistamiskyky auttavat sinua havaitsemaan ja suojautumaan ennalta tuntemattomilta madoilta aikaisemmassa vaiheessa kuin koskaan ennen.

Norman SandBox tukee sekä SMTP:tä että MAPI:a. Se tukee kaikkia tunnettuja menetelmiä, joilla virukset etsivät sähköpostiosoitteita (tiedostojärjestelmän tutkiminen, WAB tiedostot, WAB32.DLL ja rekisterit).

Norman SandBox tukee kaikkia näitä tekniikoita täydellisesti.

Todiste teknologian toimivuudesta

- Norman SandBox v2 -teknologian laatu on varmistettu pitkäaikaisissa käyttötesteissä normaalissa käyttöympäristössä. Testien aikana Norman SandBox v2 pysäytti useita uusia, ennalta tuntemattomia matoja. Epäilyttävien ohjelmien suorittaminen simuloidussa (teeskennellyssä) tietoverkossa tuottaa uuden virustorjuntamekanismin, joka ei perustu tunnettujen virusten jälkiä etsiviin tekniikoihin, kuten heuristiikkaan tai päivitettäviin virusmääritetiedostoihin.

Massapostimatojen leviämistekniikat

- Sähköpostimadot käyttävät periaatteessa kahta leviämistapaa. Ne menevät joko WinSock/WinSock2 –kirjastoa hyödyntäen suoraan SMTP-palvelimelle tai MAPI-kirjaston kautta. Osa madoista käyttää molempia tapoja. Madot hakevat esim. sähköpostiosoitteet, viestin otsikon ja viestikentän MAPI:sta ja lähettävät «version» itsestään SMTP:n kautta. Toiset madot kytkeytyvät kiinteästi ohjelmoituihin laitteisiin (IP tai DNS kautta) eri syistä. Ne saattavat lisätä tietoturva-aukkoja sähköpostin tunnistamiseen esim. niin, että Outlook Express avaa liitetiedostot automaattisesti. Se, miten mato etsii sähköpostiosoitteita järjestelmästä, vaihtelee. Osa madoista tutkii tiedostojärjestelmää ja yrittää löytää EML, HTML ja muita sähköpostiosoitteita sisältäviä tekstitiedostoja. Toiset paikantavat Windows-osoitekirjan tarkastelemalla rekisteriasetuksia ja toiset käyttävät WAB32 –kirjastoa hakeakseen Windows-osoitekirjaan tallennetut osoitteet.

Tietoverkoissa leviävät madot

- Tietoverkkojen jaoissa leviävät virukset voivat käyttää useita eri tekniikoita etäkoneen tartuttamiseen. DLL Kernel32 sisältää API:t, joista ilmenevät kaikki levyasemat sekä tietoa levyasemien tyypeistä. Toiset virukset yksinkertaisesti kopioivat itsensä levyasemiin tai tutkivat levyasemilla sijaitsevia tiedostojärjestelmiä löytääkseen itselleen sopivan paikan.

MPR.DLL avaa sovelluksille pääsyn Wnet-toimintoihin. Nämä toiminnot antavat viruksille ja madoille mahdollisuuden tutkia verkkoa; jakoja, kirjoittimia tai tietokantoja, joista ilmenee muiden koneiden yhteyksiä. Kun mato löytää sopivia verkkoresursseja, se kopioi itsensä kyseisiin resursseihin suoraan tai käyttämällä UNC-polkuja.

- Toiset madot (kuten W32/Opaserv) käyttävät SMB protokollaa etäkoneen tartuttamiseen. Ne lähettävät portin 137 kautta viestejä aliverkkoihin ja odottavat vastauksia verkkoihin liitettyiltä tietokoneilta. Kun tietokone vastaa, mato selvittää sen jakonimen, muodostaa uuden yhteyden ja tartuttaa etäkoneen portin 139 kautta.

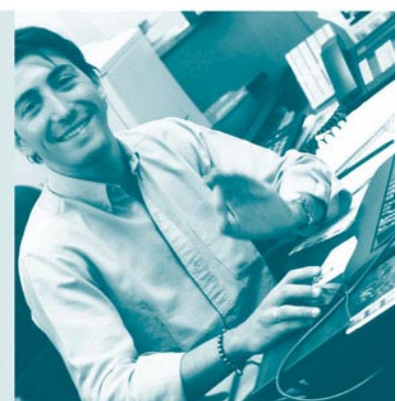


Peace of Mind

Norman is one of the world's leading companies within the field of data security. With products for virus control, spam control, email control, download control, personal firewall, encryption, data recovery, certified data erasure and computer forensics, the company plays an important role in the data industry.

NORMAN®

www.norman.com



Norman SandBox havaitsee yritykset muuttaa tai lisätä scriptejä tai suoritettavia ohjelmia P2P lataushakemistoihin.

Norman SandBox reagoi moniin erilaisiin ennalta määriteltyihin tapahtumiin ja huomauttaa «tietoturvahista». Niitä ei määritetä viruksiksi vaan haitallisiksi ohjelmiksi.

Mitä viruksia Norman SandBox tunnistaa?

Onko Norman SandBox turvallinen?

Paljonko resursseja Norman SandBox vaatii?

Mitä minun pitää tehdä kun Norman SandBox havaitsee viruksen?

Missä Norman SandBox:ia pitäisi käyttää?

Vaatiiko Norman SandBox päivittämistä?

Havaitseeko Norman SandBox KAIKKI virukset?

Peer2Peer (P2P) verkkomadot

Monet madot ovat tietoisia P2P verkoista ja pyrkivät leviämään hyödyntäen niiden mekanismeja esimerkiksi sijoittamalla itsensä «mielenkiintoisella tiedostonimellä» lataushakemistoon. Tällaiset madot voidaan jäljittää tarkastelemalla joitakin rekisteriarvoja. P2P-verkkoja on useita, joista yleisin lienee Kazaa.

Takaovet ja muut vahingolliset ohjelmat

Takaovi on ohjelma, joka avaa portteja tietojärjestelmääsi. Sen jälkeen järjestelmä odottaa ulkopuolista yhteydenottoa. Yhteydenottaja suorittaa yleensä piilotoimintoja, kuten tietokoneesi luvaton etähallinnointia. Toiset Troijalaiset saattavat lähettää tietokoneestasi tietoja sinun tietämättäsi, esimerkiksi tiedostoja, näppäinpainalluksia ja verkkolevyasemien tai numerovalitsimien (dialer) salasanoja.

Usein esitettyjä kysymyksiä

Norman SandBox havaitsee useimmat eri virustyyppit. Näyte, josta viruksille ominaista toimintaa etsitään, suoritetaan teeskennellyssä tietokonejärjestelmässä ja verkkoympäristössä. Virus voi olla paikallisesti leviävää tai muita tietokoneita tartuttavaa tyyppiä. Virus voi käyttää myös etäkoneen palveluja, kuten SMTP, News, IRC, DNS, jne.

Kyllä. Koska kaikki toimenpiteet suoritetaan teeskennellyssä ympäristössä, mitään ei suoriteta oikeassa järjestelmässäsi. Jos virus tai Troijalainen pyrkii tuhoamaan kaikki järjestelmätiedostosi, se tuhoaa ne teeskennellyllä levyllä, ei oikealla levylläsi. Sen takia ratkaisu on ehdottoman turvallinen.

Norman SandBox käyttää skannerikoneiston emulaattoria ja virtuaalimuistin hallintamoduulia. Norman SandBox:in ohjelmakomponentit sijaitsevat virusmääritetietokannassa (NVCBIN.DEF). Norman SandBox -komponenttien koko pakattuna on alle 160 kB. Muistitarve per skannaus on noin 4 MB. Koska toimenpiteet suoritetaan jäljitelyssä tilassa, nopeus on erittäin tärkeä. Tietokoneessa, jossa on 700 MHz PIII, jäljitellään yli miljoona käskyä sekunnissa. Tietokoneessa, jossa on 2 GHz P4, jäljitellään yli kolme miljoonaa käskyä sekunnissa. Norman SandBox on kehitetty minimoimaan suoritettavat toimenpiteet varsinkin puhtaissa tiedostoissa ja kehitystyö jatkuu. Kun normaailta kiintolevyllä skannattiin kaikki ohjelmatiedostot, Norman SandBox kasvatti suorituskykyestiemme perusteella skannausaikaa noin 40%. Verrattaessa käytettyä aikaa ja tuntemattomien virusten ja matojen havaitsemisesta saavutettua hyötyä, emme pidä nopeuskysymystä ongelmallisena.

Kun Norman SandBox havaitsee viruksen, sen nimi voi olla joku seuraavista:

W32/EMailWorm	Sähköpostimato
W32/NetworkWorm	Jaetussa verkossa leviävä mato
W32/FileInfector	Virus, joka tartuttaa tavallisia ohjelmatiedostoja
W32/P2PWorm	P2P verkoissa leviävä mato
W32/Malware	Yleinen havainto haitallisena pidettävästä ohjelmasta

Jos Norman SandBox havaitsee jotain tuntematonta, emme ilmeisesti ole nähneet sellaista aiemmin ja sen takia sille ei ole määritetty tunnistekoodia. Tällaisissa tapauksissa pyydämme teitä ystävällisesti lähettämään tiedostonäytteen osoitteeseen analysis@norman.no. Norman SandBox:in pitäisi aina tuottaa lyhyt kuvaus, miksi se pitää koodia matona tai viruksena. Kuvaus löytyy lokitiedostosta tai viestikonsolistamme.

Norman SandBox:ia pitäisi käyttää kaikissa sähköpostia skannaavissa tuotteissa, kuten NIP (Norman Internet Protection), Lotus Notes, Exchange ja MailSweeper. Voit käyttää sitä säännöllisissä manuaalisissa virusskannauksissa ja voit luoda omia tehtävä-tiedostoja, jolloin voit suorittaa Norman SandBox -virusskannauksia tarpeen mukaan. Emme tarjota sitä reaaliaikaiseen virusskannaukseen, vaikka se siinä toimii.

Kyllä. Norman SandBox muodostuu useista ohjelmakomponenteista, kuten esimerkiksi kernel32, wsock32 ja msvcr, jotka sijaitsevat binäärimääritetiedostossa (NVCBIN.DEF). Kehitämme näitä ohjelmakomponentteja jatkuvasti. Muutokset vaikuttavat tiedostoon, jonka nimi on NVCINCR.DEF. Näin ollen toimitamme muutosten jälkeen ainoastaan pienen päivityspaketin sen sijaan, että toimittaisimme koko SandBox:in kaikkine ohjelmamoduuleineen.

Ei. Norman SandBox:in tarkoitus on havaita järjestelmääsi nykyisin uhkaavat koodit. Se keskittyy havaitsemaan binääriset sähköposti- ja verkkomadot, jotka ovat nykyisin yleisimpiä ja vaarallisimpia viruksia. Norman SandBox ei tunnista "historiallisia" DOS COM -viruksia tai muita ei-suoritettavia viruksia (makrot ja skriptit).

Norman solutions for clients/workstations: Norman Virus Control for Microsoft Windows 95, 98, Me, NT4.0, 2000, XP, OS/2, Linux (On-Demand scanning) | Norman Internet Control for Microsoft Windows 95, 98, Me, NT4.0, 2000, XP | Norman Personal Firewall | Norman Privacy

Norman solutions for servers: Norman Virus Control for Microsoft Windows XP, 2000, NT40 | Norman Virus Control Firebreak for Novell Netware 4.11 and later | Norman Virus Control for Linux | Norman Virus Control for Lotus Domino (Win32, OS/2) | Norman Virus Control for Firewall-1 (and next generation version)

Norman solutions for web, gateways and mailservers: Norman Spam Control | Norman Email Control | Norman Download Control | Norman Virus Control Net | Norman Virus Control for Microsoft Internet Information Server | Norman Virus Control for MIMESweeper | Norman Virus Control for Microsoft Exchange

NORMAN®

www.norman.com