Helaas heb ik niet meer alle data in bezit. Ik repareer af en toe pc's van mensen zoals meerdere tweakers, en had laatst een klant met dit virus.

Had een hele logboek opgebouwd voor ING, wat ze trouwens niet wilde hebben...

Maar kort samengevat:
Klant logt in (ik heb het ook kunnen zien) en krijgt popup over dat een elektronische handtekening geverifieerd moet worden. Op dat moment is het virus al actief. De popup is geen echte popup, maar gewoon een overlay in de pagina van mijn ing. Wil even benadrukken dat het echt geen nieuw browser venster is.

Eigenaardigheden:
Is een nette SSL verbinding, met goede URL en goed ING certificaat. AVG ziet het virus niet. Speciale cleanup tool van ING zelf ziet het virus ook niet. Heb deze verwijderd door Malwarebytes anti-malware samen met Kaspersky te draaien.

Hoe het virus (volgens mij werkt):
Op een nog onbekende manier "inject" het virus de html pagina zodra je ingelogd bent en include een of meerdere javascript files van een externe server. (in dit geval zag ik volgens mij twee verschillende, op apache draaiende servers)
.
Heb dit met Firebug kunnen traceren en waren een paar hostnames die ineens tussen de lijst voor kwamen.
In die javascript staan simpelweg het rekeningnummer van, het rekeningnummer naar het bedrag en uiteraard wat code om het uit te voeren.
Heb zelf nooit het scherm van de TAN code kunnen zien, want het rekeningnummer was al bevroren.
In het geval van deze klant was het rekeningnummer waar het heen ging gewoon een ander ING nummer (begon met dezelfde cijfers). Het bedrag wat afgeschreven was, was zo'n €1750,-

Dit is ongeveer rond 12-7-2011 geweest (vorige maand dus).

Het virus wat erop zat:
Spy Eye.

Hij zat zijn saldo te bekijken op de start pagina van "mijn ing". Er verscheen een pop-up melding met de vraag of hij zijn digitale handtekening aan wilde vragen en of hij daarbij een aantal gegevens door wilde spelen. De gegevens heeft hij niet ingevuld (inlognaam, telefoonnummer,wachtwoord). Hierna kwam er opeens een sms binnen met een tan code, in de pop up verscheen de melding "om uw digitale handtekening te bevestigen voert u nu de tancode in", dit heeft hij wel gedaan. Vervolgens was idd 90% van zijn rekening afgeschreven. Aangifte gedaan bij de politie, die wisten te vertellen dat er aardig wat meldingen binnen waren gekomen van verschillende banken waaronder rabobank en abn met de bekende aparte kastjes. Na een aantal ingevulde formulieren van de ing heeft hij na ongeveer 2 weken het geld terug gehad.

Vorige week vrijdag had ik een computer van een klant op onze TD met problemen met ING bankieren. Deze problemen deden zich voor het eerst vorige week woensdag voor. We hebben de computer opgeschoond met o.a. Combofix en Mcafee Stinger, handmatig en automatische schijfopruiming, internetopties reset, firewall reset, er

draaide op deze PC de PC Veilig software van KPN. In msconfig-opstarten stonden wat verwijzingen naar bestanden die verwijderd zijn. We hadden het idee dat de PC 100% schoon was. Zodra er werd ingelogd op ING Bankieren stond er echter direct een transactie klaar van (inderdaad) zo'n 90% van het saldo. Ik testte dit met mijn eigen ING rekening en kreeg netjes een TAN code in mijn SMS. Die heb ik uiteraard maar even niet gebruikt. Ik was ondertussen al uitgelogd op de besmette PC. Ik ben op mijn eigen notebook weer ingelogd en de betaling stond niet meer in de verzendlijst. We hebben van de klant niet de mogelijkheid gehad de computer nader te onderzoeken, ze hebben direct een nieuwe gekocht om geen enkel risico meer te lopen en hebben besloten de ander enkel nog offline te gaan gebruiken voor hun werkzaamheden. Het was al met al wel een ervaring, klant voelde zich er erg naar onder, omdat ze het als een persoonlijke aanval opvatte, een beetje het gevoel alsof iemand bij je inbreekt.

Overigens is dit niet de eerste keer dat deze melding zich voordoet. We hadden zo'n 5 weken terug een klant met exact dezelfde melding 'de betaling stond al klaar'. We hebben die PC rigoureus geformatteerd en opnieuw geinstalleerd. De problemen waren daarna (uiteraard) ook de wereld uit. Klant had hierover destijds contact gehad met ING, die adviseerden de klant om de PC door een expert na te laten kijken.

Voor 3 weken geleden kreeg mijn schoonzoon (Monnickendam), elk moment dat hij inlogde, via IE, een scherm om een transactie door te zetten, dus niet het inlogscherm, maar het scherm om de TANcode in te voeren.
Teven ontving hij op de GSM een SMS met de TANcode.

Hij vond dit gek en heeft die handeling niet uitgevoerd, toen ik bij hun op visite was, had ik dat ook geconstateerd en ik heb toen ingelogd bij ING via Google Chrome en kreeg toen gewoon het inlogscherm.

Er was niks te vinden via scannen aan maleware en/of virus, ik heb toen de laptop gereset naar fabrieks-instellingen (WinXP schoon erop) daarna geen problemen meer.

Hij heeft geen idee waar het "virus" vandaan kwam, ik ben er ook niet meer ingedoken, alles werkt weer normaal, hij gebruikte AVast en PC Tools Spyware Doctor.

Ook mijn rekening werd geplunderd op de door U beschreven manier, en wel op 29 juli j.l.

Gevonden virus: trojan 9AOB33BiED6.exe op c:Romano.bin

Ontdekt en verwijderd door malwarebytes.

Div. scanners geven infectievrij aan maar daar ben ik niet zeker van omdat de computer traag blijft.

Geld overgeboekt naar iban: GB14loyd[xxxxxxxxxxx]

Naam: Sergejs B.

Omschrijving: Diets Fee

Ik kan melden dat er op 15/16 augustus een ongewenste overboeking van mijn ING-rekening naar Roemenie heeft plaatsgevonden. IBAN nummer begint met RO.

de gegevens en omschrijving luidde:

IBAN:RO48BTRL00904xxxxxxxxx
naam:MARIAN C.
OMSCHRIJVING:00904201W83229XX

In eerste instantie verscheen de overboeking niet op mijn overzicht. De ING kon deze wel zien.
op mijn PC vond ik een virus ***spyware.passwords.xgen*** *en na scannen met www.ing.nl/cleaner een* ***MEBroot infectie****, die niet de verwijderen was volgens de ING cleaner.*

door helpdesk-aan-huis.nl , een gespecialiseerd bedrijf wat voor mij als systeembeheerder optreedt, zijn beide virussen daarop verwijderd. (combofix en symantec MBR)

echter na nogmaals scannen met de ING cleaner blijft deze een mebroot infectie vaststellen.

de malvercatie heeft plaatsgevonden vanuit een site waarnaar ik op voor mij onverklaarbare wijze naar toe geloodst ben. knappe imitatie van de ING site. het enige wat ik gemerkt heb is een langere identificatie tijd.

daarna werd, omdat ik een aanmerkelijk bedrag wilde overboeken, een tweede maal een TANcode gevraagd. hiermee heb ik waarschijnlijk de transactie naar het buitenland geautoriseerd.

hoe men wist welke nog niet gebruikte TANcode men moest vragen begrijp ik niet.

zover mijn ervaring van afgelopen maandag en dinsdag met de ING

en nu maar hopen dat mijn geld snel terug is.

Ik ben dit exacte virus namelijk een maand geleden al bij een klant van mij tegengekomen. Ze zat op ING.nl en er verscheen een pop-up. Daarna ontving ze een TAN code per sms waar een groot bedrag van haar rekening zou worden afgeschreven. Ze heeft deze code ook ingevuld, maar gelukkig heeft de ING direct haar mijn.ing.nl en haar TAN codes geblokkeerd.

Volgens mij is een familielid van mij hier ook slachtoffer van geworden en ik stond er naast toen het gebeurde.

Ik weet niet of het exact hetzelfde virus betreft.

Hoe het virus op de xp computer is gekomen weet ik niet.
Ik weet ook niet welk virus het was.
Al deze informatie is verloren gegaan omdat ik vlak voordat de leegroof werd ontdekt, ik die pc helemaal heb geherinstalleerd.

De werking van het virus hebben sommige reageerders al correct uit de doeken gedaan.
Het virus nestelt zich en wacht rustig af tot je gaat internetbankieren.
Het inloggen bij de ING verloopt normaal alleen gelijk daarna, staat er een bericht dat er vanwege een extra beveiligingscontrole er een TAN-code moet worden ingevoerd.

Ik weet niet helemaal exact meer of dat bericht werd geladen in een pop-up of niet maar ik heb niet een pop-up op zien komen en als dat al wel zo was, was het een pop-up op volledige scherm-grootte.
Het bericht werd dus volgens mij gewoon in het open bankier-scherm geplaatst en qua uiterlijk en speling van teksten, was er niets verdachts aan op te merken.

Bij haast of niet goed opletten, valt het dus maar minimaal buiten de normale procedure.
Verschil in SSL certificaat of adres heb ik niet gemerkt maar of daar verschil in zat, weet ik niet meer.
Vervolgens kan er prima een normale transactie worden aangemaakt en hiervoor moet ook een andere TAN-code woorden ingevoerd.
Het virus houdt hier rekening mee en laat eerst de legitieme boeking afgeboekt worden, zodat het virus niet een te hoge boeking doet en dus effectief niet kan worden gedaan door de saldo-controle van de bank.
Na overboeking van de legitieme boeking, wordt de stiekem verstopte boeking (de boeking is niet te zien in het boekingsoverzicht voor verzending), doorgevoerd.

Het virus houdt zelfs rekening met de rood-staan ruimte van de rekening en boekt echt het maximale bedrag af dat mogelijk is.

Ik heb het virus ook gehad, maar dat is al ruim een maand geleden (ik ben er gelukkig niet ingetrapt). ING wist ervan, ik moest nieuwe tan-activatie ophalen bij het postkantoor (de TAN-functionaliteit had ING al geblokkeerd, omdat ze dit blijkbaar konden dedecteren) en via de scanner op de site www.ing.nl/cleaner het virus verwijderen.

Mijn schoonvader heeft vermoedelijk te maken gehad met dit virus, hij is op de beschreven manier een hoop geld kwijt geraakt.

De symptomen waren regelmatig BSOD meldingen waarvan er een de foutcode 0x000000D1 op scsiport.sys had en een extreem traag opstartend en werkend systeem.

Omdat ik aanvankelijk dacht dat het een defecte hdd was heb ik de hdd rigoreus doorgetest en daarmee ook de volledige schijf gewist. 1 ding was iig zeker, het virus was weg hiermee.

Geïnstalleerd was AVG Free en Webroot Spysweeper. Beide waren niet in staat om het virus buiten de deur te houden.

De bron van de inlogpagina is iets anders. Bij standaard internetbankieren is deze heel kort en verwijst naar een applicatie van ING. Bij de gehackte versie is de site optisch hetzelfde. Alleen het laadscherm na inloggen is een ronddraaiend oranje icoontje. Deze is ook exact nagemaakt, maar wel groter. Ze vragen om bevestiging van je adresgegevens met gelijk je tancode. Prompt krijg je een SMS. Gelukkig staat daar tegenwoordig het bedrag in, maar de adresgegevens pagina was voor mij al reden genoeg om af te blazen.

De bronpagina van de gehackte versie is wel langer met meer code en deze verwijst naar some.post.com of iets dergelijks.

Hoe ik het ben opgelopen is mij nog onduidelijk, het enige wat ik vermoed is dat deze door een gehackte bekende site is gekomen. Ik herinner me dat ik bij een engelstalig Honda VFR forum een nare pop-up kreeg ondanks alle maatregelen die ervoor zijn. Dit heeft het progje er denk ik snel opgezet.

Wat mij nu extra scherp maakt is, als ik telkens opnieuw in moet loggen bij sites. Dat is de makkelijkste herkenning, waarschijnlijk door gerommel met de cookies. Ook is HTTPS in de url niet voldoende veilig, er moet een certificaat bijstaan wil het echt veilig zijn. Zij faken blijkbaar een certificaat zodat het wel zogenaamd een beveiligde verbinding is. Er staat geen bedrijfsnaam in de url balk, wat je normaal bij ABN en ING wel ziet.

De cleaner van ING werkte feilloos (www.ing.nl/cleaner). McAfee stond duimen te draaien, terwijl deze toch dit soort dingen moet onderscheppen.