



NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

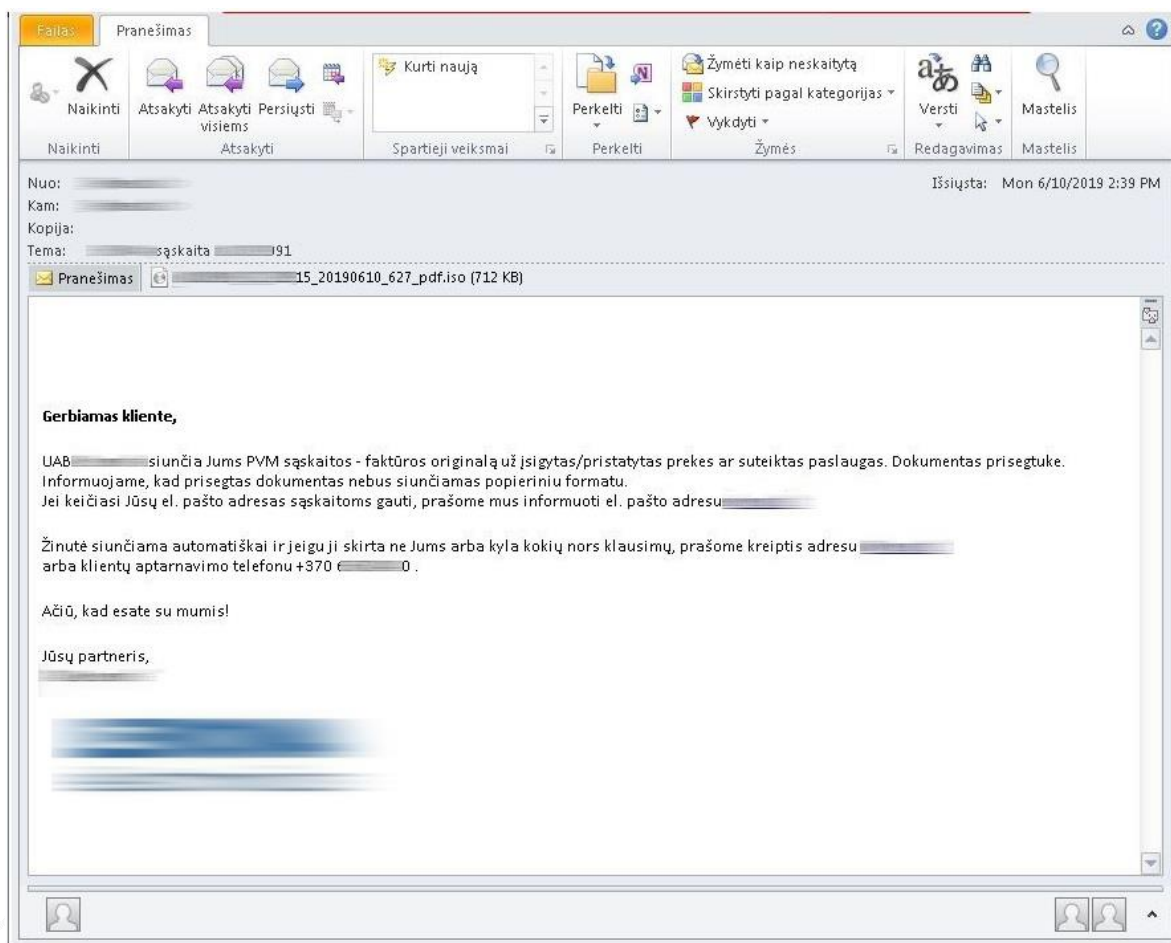


INFORMACINIS BIULETENIS
LIETUVOJE ŽINOMŲ ĮMONIŲ VARDU SIUNČIAMY EL. LAIŠKAI
SU KENKSMINGU PROGRAMINIŲ KODŲ

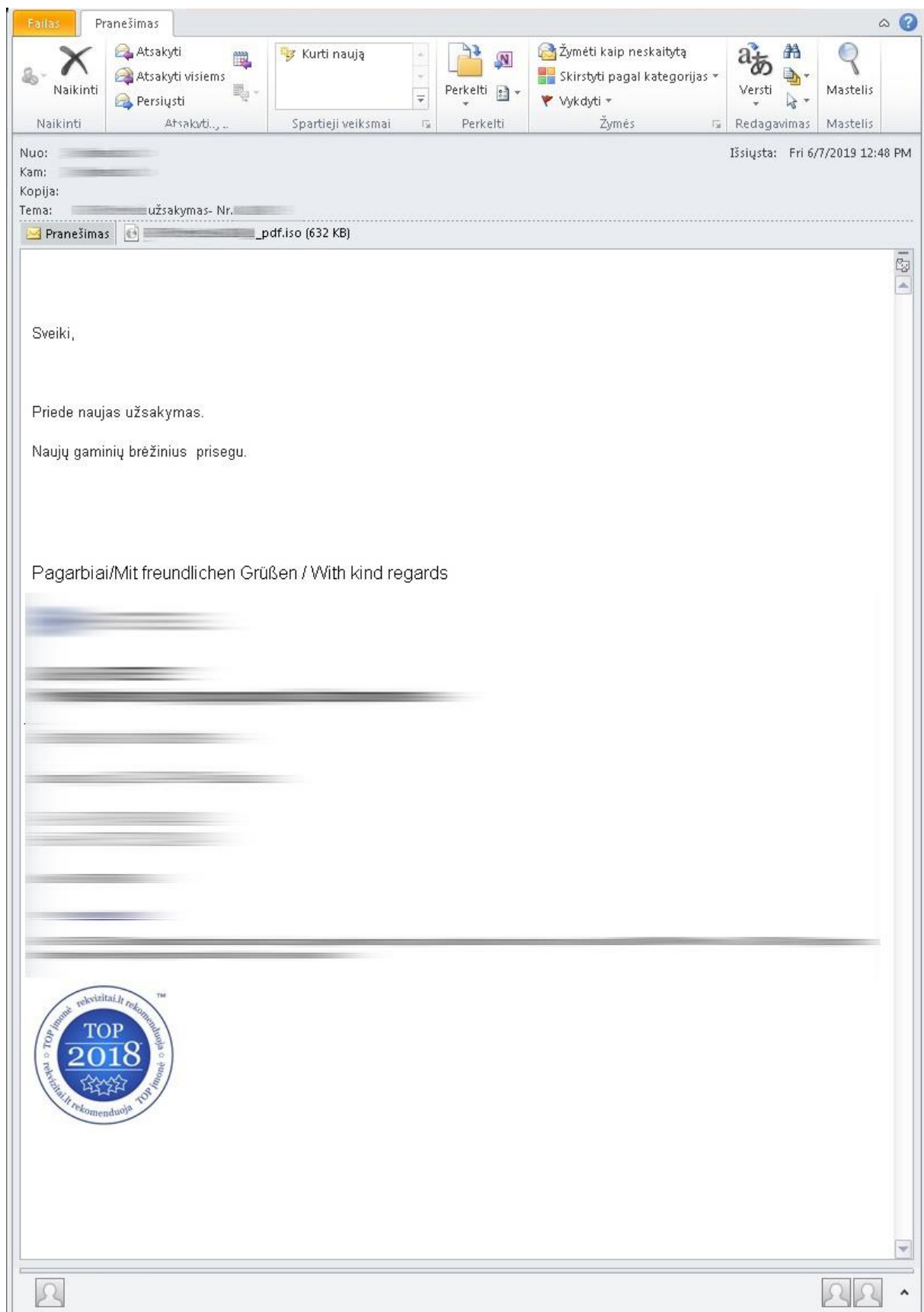
2019 m. birželio 26 d.

Vilnius

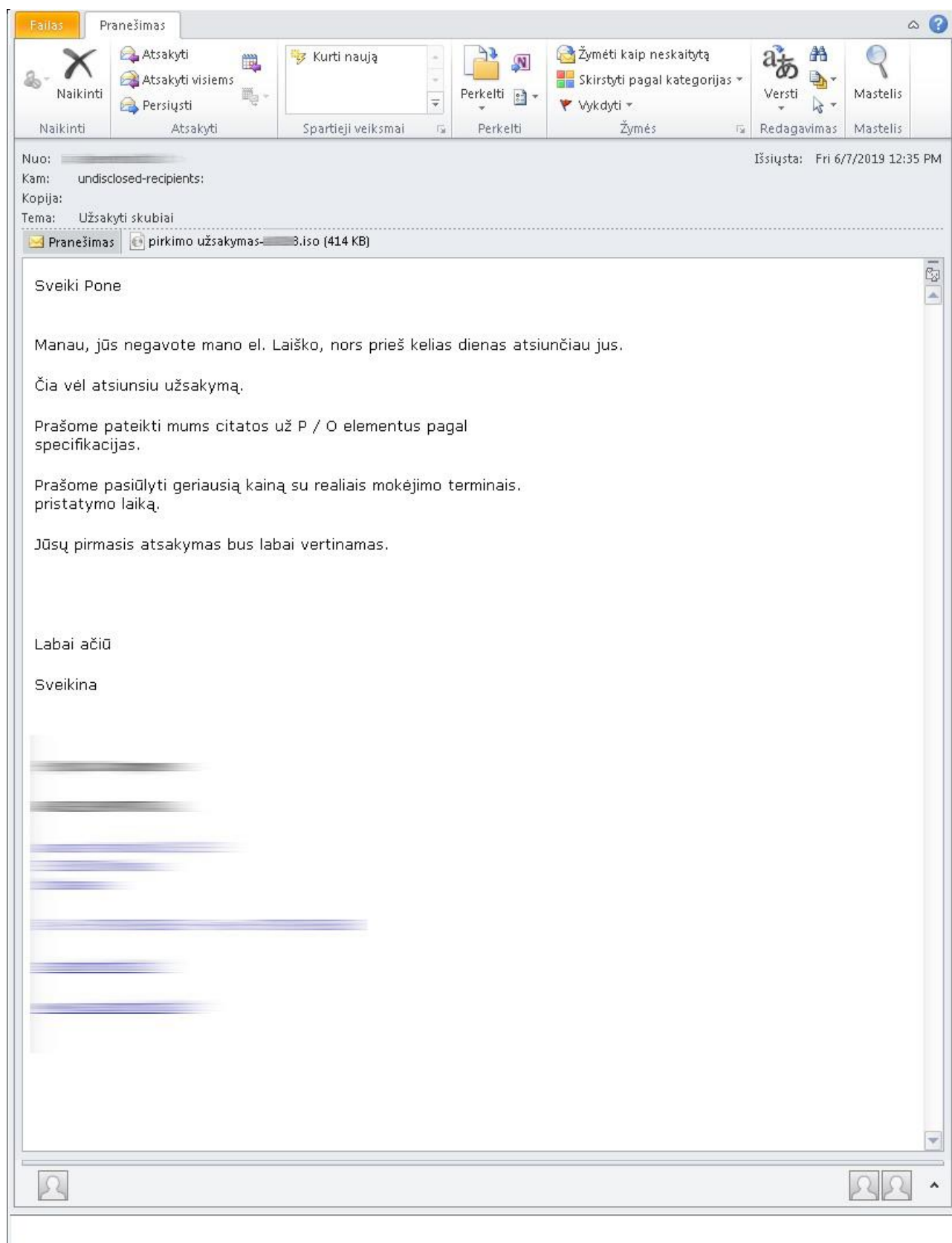
Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (NKSC) informuoja, kad Lietuvoje plinta el. laiškai su kenksmingu programiniu kodu. Pastarosiomis dienomis NKSC fiksuoja atvejus, kuomet klastojant žinomų Lietuvos ir užsienio įmonių el. pašto adresus, naudojant jų logotipus ir kontaktinę informaciją, platinamas kenksmingas programinis kodas.



1. Pav. Suklastoto el. laiško pavyzdys, imituojantis tiekėją



2. Pav. Suklastoto el. laiško pavyzdys, imituojantis tiekėją



3. Pav. Suklastoto el. laiško pavyzdys, imituojantis tiekėją



Kenkimo kodas talpinamas *.iso formato bylose, kurios būna prisegtos prie el. laiško. Prisegtoje byloje yra talpinamas vykdomasis *.exe failas. Atidarius prisegtą bylą ir paleidus vykdomąjį *.exe failą, kenksmingas programinis kodas iš kompiuterio bando surinkti asmeninę naudotojo informaciją, nuskaito kompiuterio vardą, bando identifikuoti, ar kompiuterį galima pasiekti nuotoliniu būdu (ar įgalintas „Remote Desktop“ funkcionalumas), siunčia informaciją į nutolusią tarnybinę stotį ir atlieka kitus žvalgybos veiksmus.

El. laiško tekstas dažniausiai būna parašytas lietuvių kalba. Laiškas gavėjui atrodo tikroviškas, kadangi siunčiamas iš žinomo ir patikimo adresato, tačiau iš tiesų būna suklastotas.

Rekomendacijos

Tikrinkite laiško antraštes (angl. headers), kuriose matoma, kas yra tikrasis laiško siuntėjas (laukelis From). Analizuojant antraštę, reikėtų žiūrėti į pirmą Received parametrą nuo apačios. Šis parametras pasakys, iš kurio serverio buvo išsiųstas el. laiškas. Jeigu From laukas yra siuntejas@imone.lt, tai ir Received laukelyje turi matytis adresų sritis (domenas) „imone.lt“. Šio sukčiavimo atveju laukelyje Received matomi visai kiti duomenys, iš kur buvo išsiųstas laiškas. Žr. pav. 4.

```
Received: from setentaycuatro47.nspirmario.com (Not Verified[188.93.74.47]) by [redacted] with [redacted] (using TLS: TLSv1.2, ECDHE-RSA-AES256-GCM-SHA384)
id <B5cF4d1740000>; Mon, 10 Jun 2019 14:39:32 +0300
Received: from webmail.embalpacklevante.com (localhost [IPv6:::1])
by setentaycuatro47.nspirmario.com (Postfix) with ESMTPSA id 90B123E23272;
Mon, 10 Jun 2019 13:39:05 +0200 (CEST)
Authentication-Results: setentaycuatro47.nspirmario.com;
spf=pass (sender IP is ::1) smtp.mailfrom=neatsakyt1[redacted] smtp.helo=webmail.embalpacklevante.com
Received-SPF: pass (setentaycuatro47.nspirmario.com: connection is authenticated)
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="=_fc3676c3ea2907e14704b57724269733"
Date: Mon, 10 Jun 2019 12:39:05 +0100
From: Rex SQL Server <neatsakyt1[redacted]>
To: undisclosed-recipients:;
Subject: =?UTF-8?Q?[redacted]?=
Organization: [redacted]
In-Reply-To: <AMOPRO[redacted]@AMOPRO8MB4081.eurprd08.prod.outlook.com>
References: <AMOPRO[redacted]@AMOPRO8MB4081.eurprd08.prod.outlook.com>
Message-ID: <846f832c236c367754e1e51928963909@imona.lt>
X-Sender: neatsakyt1[redacted]
User-Agent: Roundcube webmail/1.3.8
```

Pav. 4. Suklastoto el. laiško tikrasis siuntėjas

Priklausomai nuo el. pašto programos, antraščių peržiūros galimybė skiriasi.

Atkreipiame dėmesį, kad kibernetiniai nusikaltėliai nuolat platina ir kitus kenkimo kodus, kurie išnaudoja įvairios programinės įrangos pažeidžiamumus, todėl rekomenduojame nuolatos atlikti tiek antivirusinių, tiek operacinių sistemų, tiek kitos naudojamos programinės įrangos atnaujinimus.

Siekiant apsisaugoti nuo el. pašto adresatų klastojimo, rekomenduojame įgalinti ir tinkamai sukonfigūruoti „SPF“ (Sender Policy Framework) funkcionalumą. Ši priemonė turėtų būti naudojama su papildoma atsarga, kadangi neteisingi nustatymai gali nulemti kai kurių laiškų nepristatymą jų gavėjams.

Primename, kad pagrindinis dalykas – nuolatos būti atidiems ir kritiškai vertinti gaunamus laiškus.