



LIETUVOS KRIMINALINĖS POLICIJOS BIURO
NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE TYRIMO VALDYBA

**„Nusikalstamų veikų, susijusių su
atsiskaitymų elektroninėmis mokėjimo
priemonėmis, tendencijos Lietuvoje“**

Vilnius

2012-03-01

NEETV struktūra

Valdyba esama sudėtimi įkurta 2009-01-01. Nuo 2001 iki 2009 m. 5 žmonių skyrius ekonominės policijos sudėtyje. Steigiant valdybą viso buvo numatyta 14 etatų. Realiai šiuo metu dirba 10 žmonių.

- 1-asis skyrius: ikiteisminiai, operatyviniai tyrimai.
- 2-asis skyrius: techninis palaikymas, elektroninė žvalgyba.

Elektroninio nusikalstamumo iššūkiai ir NEETV „fokusas“

- Sparčiai augantis nusikaltėlių mentalitetas - socialinė inžinerija, tai naujas veiksmingas būdas išvilioti duomenis. Žmogiškasis faktorius labai svarbus, nes viskas prasideda nuo vartotojo, o baigiasi sukompromituotu IT kompanijos tinklu.
- Tobulėjantis “modus operandi” (M.I.T.M, virusai)
- Tobulėjančios informacinės technologijos
- Botnet tinklai

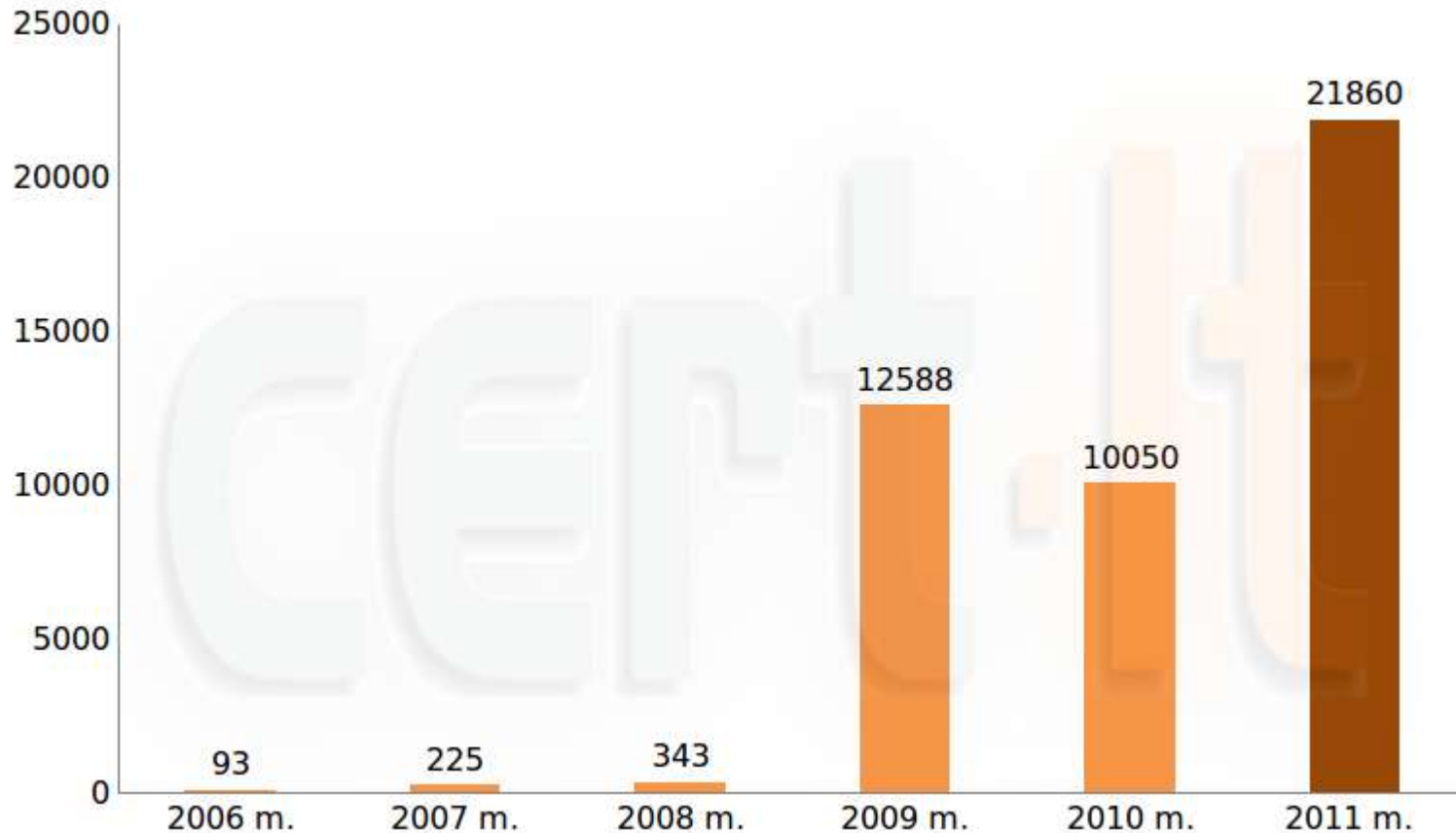
NEETV fokusas - sunkių ir sudėtingų nusikaltimų elektroninėje erdvėje tyrimas. Iš jų nemaža tyrimų dalis sukoncentruota į nusikalstamas veikas elektroninėje erdvėje, susijusiomis su neteisėtu atsiskaitymu elektroninėmis mokėjimo priemonėmis.

Latentiškumas ir incidentų tipai

Atkreiptinas dėmesys, kad elektroninių nusikaltimų latentiškumas yra labai aukštas ir sudaro apie 95 %.

- **Užvaldymas** - nesankcionuotas naudojimas informacinės sistemos ištekliais, neteisėtas informacinės sistemos išteklių naudojimas.
- **System Compromise/Intrusion** – neteisėtas prisijungimas prie informacinės sistemos ar elektroninių ryšių tinklo.
- **Elektroninių duomenų klastojimas** (angl. phishing). Sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.
- **Manipuliacija** (angl. spyware) - elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.

CERT-LT incidentų statistika

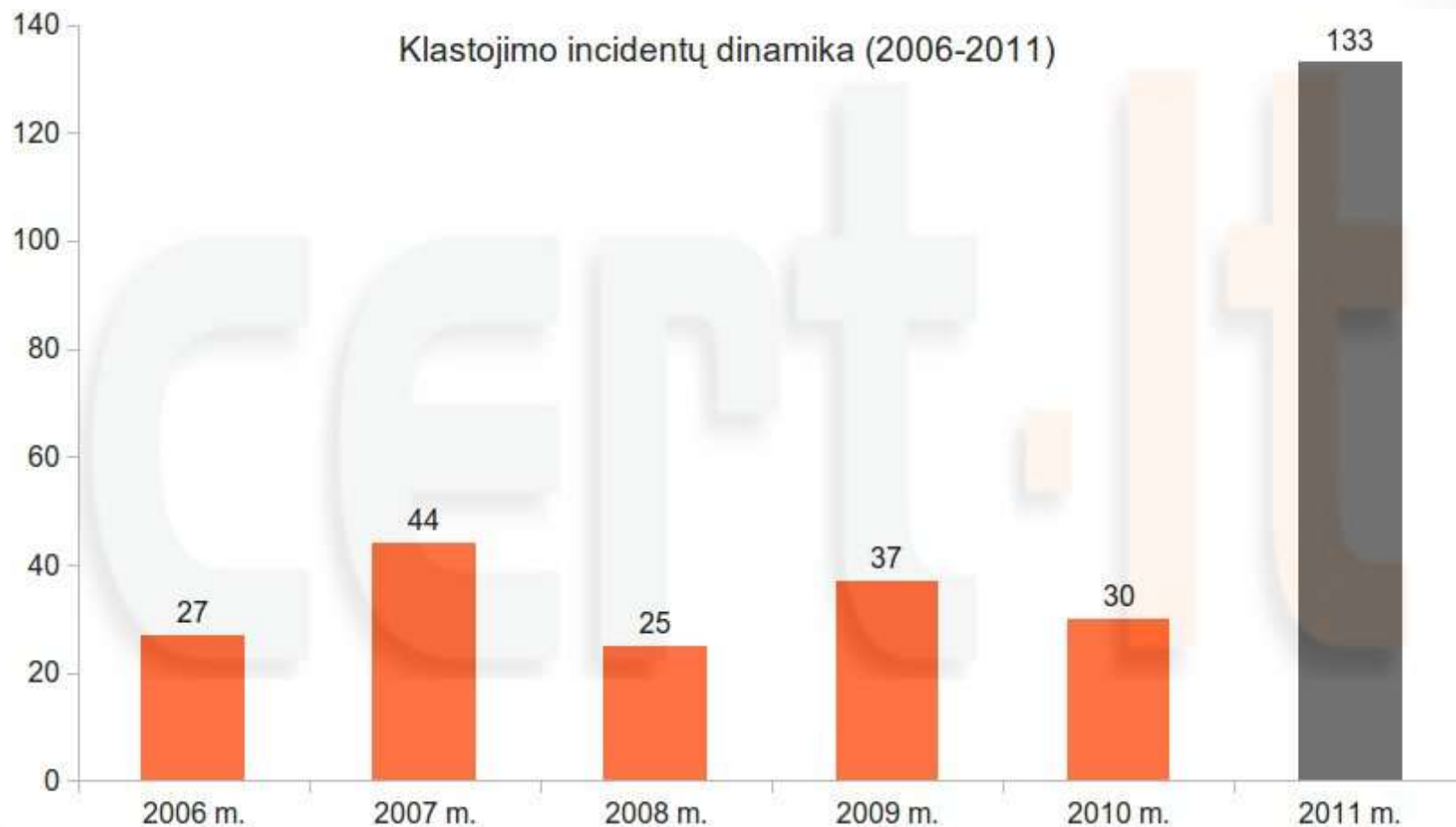


2009-2010 m. dominuoja destruktivus kodas - Win32/Conflicker/Downadup.

2011 m. registruoti 8507 užvaldymo incidentai. 18 kartų daugiau nei 2010 m.

2011 m. registruoti 133 klastojimo (angl. Phishing) incidentai. 4 kartus daugiau nei 2010 m.

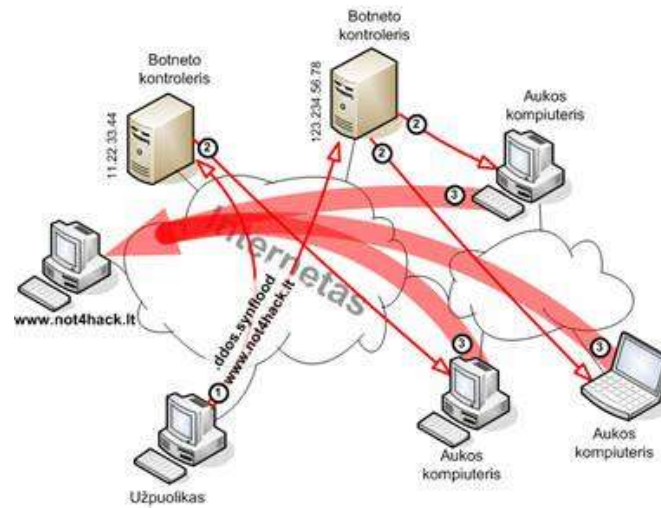
CERT-LT „phishing“ statistika



Didžiausios grėsmės – finansų sistema ir „silpnoji grandis“

Pavojingiausi atvejai, tiesiogiai nukreipti prieš finansų sistemas ir bankinį sektorių.

- BotNet atakos (sisteminis)
- Key Logger (end user)
- Phishing (end user)



Operacija - Cardingworld.cc ir Callservice.biz

Išardytas vienas didžiausių Rusijos forumų

1. JAV kasmet patiria 67,2 milijardo dolerių nuostolių. Tai oficiali JAV FTB statistika. Vien per 2008-2010 m. dėl virusų, botnet'ų, phishingo veiklos JAV klientai prarado daugiau nei 8 milijardus USD.
2. Deja Lietuvoje tokios statistikos nėra, tačiau LKPB NEETV darbo patirtis rodo, kad jau dabar bankų ir finansinių institucijų patiriami nuostoliai yra ženklūs. Pagal mūsų tiriamas bylas virš 1.000.000 litų.



The screenshot shows a news article from USA Today. The navigation bar includes links for Home, News, Travel, Money, Sports, Life, Tech, and W. The article is in the Tech section, specifically 'Inside Tech'. The title is 'Cybercrime flourishes in online hacker forums', posted on 10/11/2006 at 10:27 PM ET. The author is Byron Acohido and Jon Swartz. The article discusses the growth of cybercrime forums and the damage they cause to U.S. businesses and consumers. It includes a photo of Dan Clements, founder of CardCops, and a section titled 'CYBERCRIME BY THE NUMBERS' with two bullet points: \$67.2 billion in annual business losses and \$8 billion in consumer losses over two years.

USA TODAY ■ Home ■ News ■ Travel ■ Money ■ Sports ■ Life ■ Tech ■ W

Tech = Cars = E

Cybercrime flourishes in online hacker forums

Posted 10/11/2006 10:27 PM ET E-mail | Save | Print | Reprints & Permissions | **RSS**

By Byron Acohido and Jon Swartz, USA TODAY

SEATTLE — Criminals covet your identity data like never before. What's more, they've perfected more ways to access your bank accounts, grab your Social Security number and manipulate your identity than you can imagine.

Want proof? Just visit any of a dozen or so thriving cybercrime forums, websites that mirror the services of Amazon.com and the efficiencies of eBay. Criminal buyers and sellers convene at these virtual emporiums to wheel and deal in all things related to cyberattacks — and in the fruit of cyberintrusions: pilfered credit and debit card numbers, hijacked bank accounts and stolen personal data.

The cybercrime forums gird a criminal economy that robs U.S. businesses of \$67.2 billion a year, according to an FBI projection. Over the past two years, U.S. consumers lost more than \$8 billion to viruses, spyware and online fraud schemes, *Consumer Reports* says.

In 2004, a crackdown by the FBI and U.S. Secret Service briefly disrupted growth of the forums. But they soon regrouped, more robust than ever. Today, they are maturing — and consolidating — just like any other fast-rising business sector, security experts and law enforcement officials say. In fact, this summer a prominent forum leader who calls himself Iceman staged a hostile takeover of four top-tier rivals, creating a megaforum.

Enlarge Robert Hanashiro, USA TODAY

Dan Clements, of CardCops, tracks cyber crime transactions taking place in IRC chat rooms and hacker forums.

■ CYBERCRIME BY THE NUMBERS

- **\$67.2 billion:** FBI estimate of what U.S. businesses lose annually because of computer-related crimes.
- **\$8 billion:** *Consumer Reports* estimate of what U.S. consumers lost the past two years because of viruses, spyware and Internet scams.

Dar viena sėkminga tarptautinė operacija - puikaus trišalio policijos bendradarbiavimo pavyzdys



Po bendrai organizuoto pasitarimo Vilniuje LKPB NEETV kartu su partneriais iš JAV FTB ir Baltarusijos milicijos pradėjo bendrą tyrimą, tikslu sunaikinti plačiai išgarsėjusius interneto forumus.

Bendra operacija truko 2 metus ir po daugybės atliktų paruošiamųjų darbų 2010 metais vienu metu pavyko sulaikyti forumų organizatorius skirtingose pasaulio vietose. Išjungti serveriai bei servais, surasti skirtingose vietose įrodymai. Forumų veikla sustabdyta visam laikui, nes uždaryti servais, neleido migruoti kitur. Sulaikyta daug įtariamųjų, tyrimai tęsiasi.



AČIŪ UŽ DĖMESĮ

Lietuvos kriminalinės policijos biuro
Nusikaltimų elektroninėje erdvėje tyrimo valdyba
2-ojo skyriaus viršininkas
DONATAS VILIAMAS

Kontaktinis telefonas 8~5 271 9612

cyberpolice@policija.lt