Please Remember to Complete Your Feedback Form

The Rustock Botnet Takedown

OPERATION B107

July 27, 2011

Julia Wolf <julia@fireeye.com>

Alex Lanstein <alex@fireeye.com>

Summary of the Next Hour

- Past: The Rustock Botnet was responsible for over 50% of all spam on Earth, several times since 2006.
- Past: The code evolved significantly over the years.
- Past: It fell down a few times over the years, but then got back up.
- Present: In March of this year, Microsoft et al. successfully shutdown this botnet, and it has not recovered.

The Past

Rustock: The Early Years

- Named 'Rustock' around Jan 2006 by Symantec
- Also named 'RKRustock', 'Costrat', and generic names like 'Meredrop' by others

- Initially used IRC for C&C communications
- The C&Cs hosted on Russian Business Network
- Opened a proxy on the victim to relay spam
- Used Standard Windows Rootkit tricks to hide (SSDT Hooking, ZwOpenKey, ADS, etc.)

Circa 2007

- More-Efficient Template based spambot
- Uses HTTP for C&C communications
- Propagated via drive-by exploits and spam with sensational subject lines
- Spam messages using Microsoft's trademark
- Spam for counterfeit Pfizer pharmaceuticals
- Spam for penny stocks, etc.

LOOK AT OUR RECENT NEWS AT MONDAY, DEC 18!

INVESTORS ALERT!
Monday, Dec 18, DIAAF

Company: Diamant Film Inc.
Symbol: DIAAF.OB

Current Price: $0.0011 (+37.5% Friday Increase!)
5-day Target: $0.02

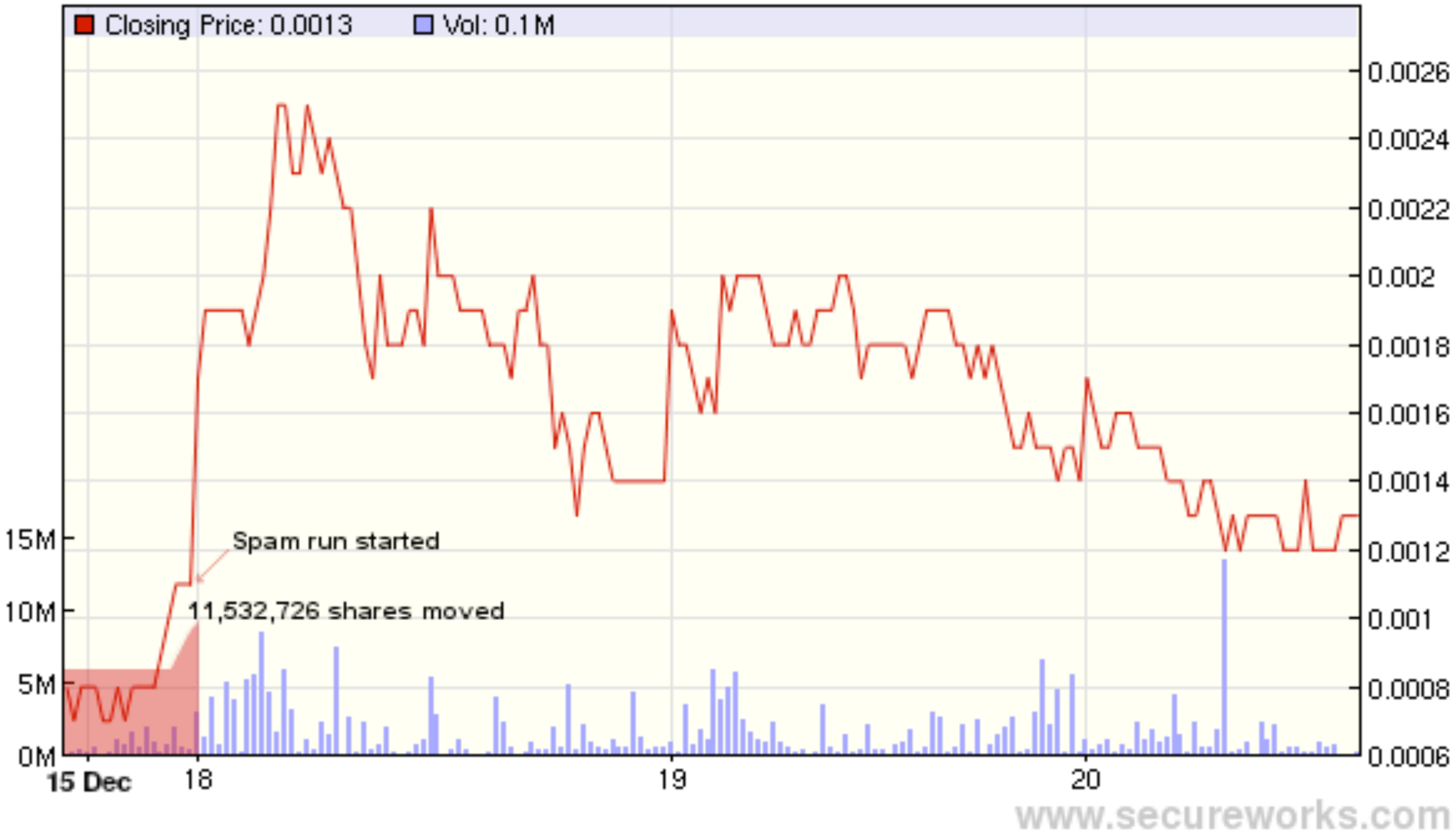
Diamant Film is dedicated to producing environmentally friendly products aimed at minimizing pollution, maximizing the quality of life and preserving the environment.

For more information please visithttp://www.diamantfilm.com/

CALL YOUR BROKER NOW!

Rustock Manipulation of DIAAF.OB

Rustock Manipulation of DIAAF.OB



Dear lucky winner,
This is to inform you that your email has won a consolation prize of the Microsoft Corporation EMAIL DRAW Today. Your email has won you 1,000.000.00 (One Million Great british Pounds) To claim your prize, please contact your fiduciary agent Barr.Arthur James Esq with your Batch #:409978E and Reference No:FL/668530092 and contact him via email immediately within 24hrs.with the information below.

Barr Arthur James Esq
Email:barr.arthurjamesesq01@hotmail.com.hk
Tel: +44-792-404-9532
Tel: +44-703-192-4594

You are to send the below required details;
1.Full Name:.....
2.Address:.....
3..Occupation :.....`
4.Age:.....
5.Sex:.....
6.Tel:.....
Sincerely,
Mrs Marilyn Berger Head Customercare Service
Microsoft Promotion.

Circa 2008

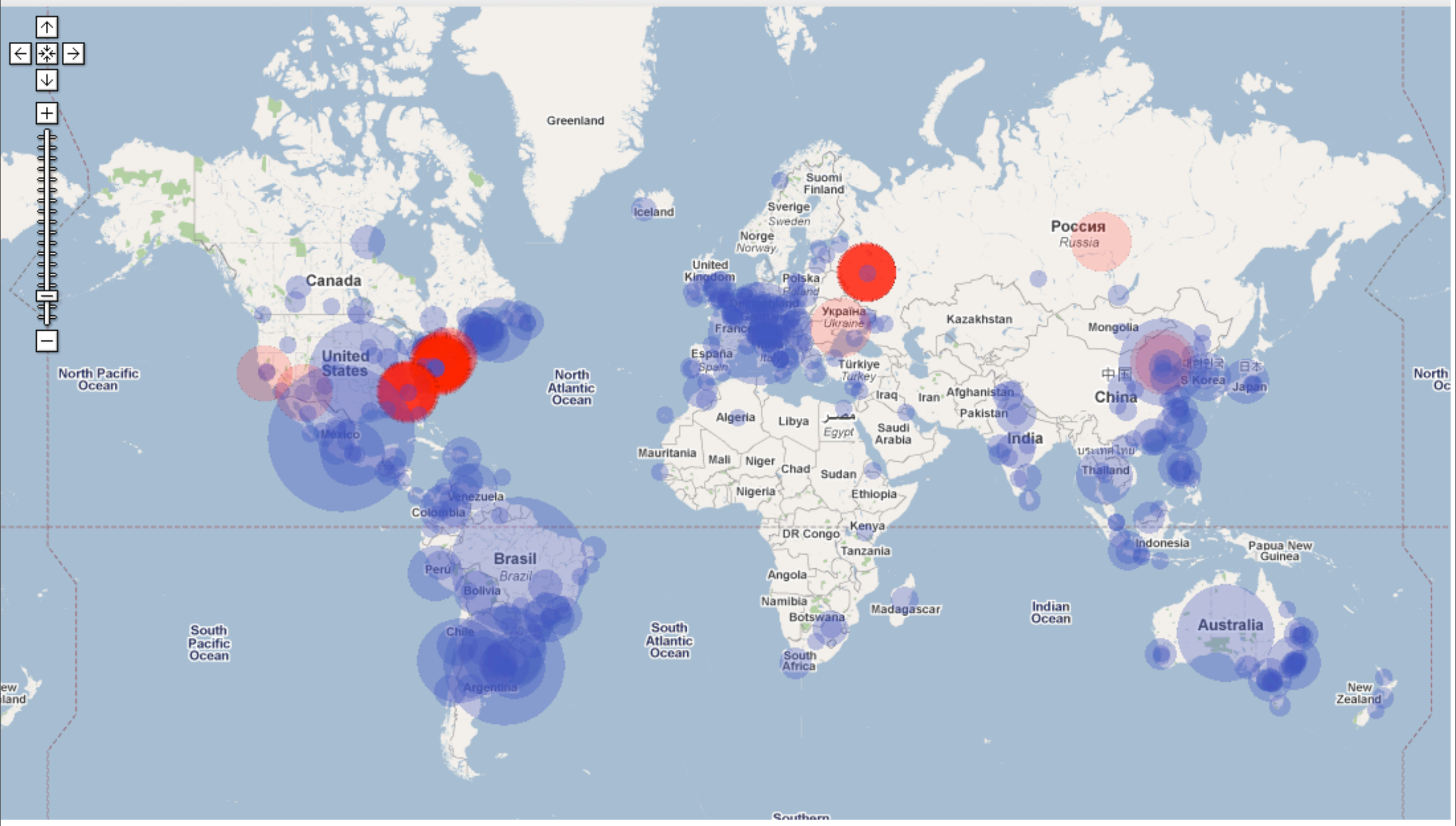
- C&Cs mostly hosted at Atrivo/Intercage... Until September 2008
- ...Then C&Cs mostly hosted at McColo... Until November 2008
- Joe Stewart estimated about 130,000 bots in Rustock at the time.

FireEye

FireEye BotMap Service

Logged in as **monitor** | Log out

Show all botnets | Show all bots | Both | All links | Rustock Botnet | Mode: Manual | 2 | Rescale | (07/21/09 07:30:33 GMT)



Circa 2008

- Rustock used hard-coded IPs for C&Cs, after McColo it switched to using static DNS
- On the weekend of Nov 15, McColo regained peering through TeliaSonera for about twelve hours
- An update was pushed out to the botnet, relocating the C&C servers in Russia

Circa 2009

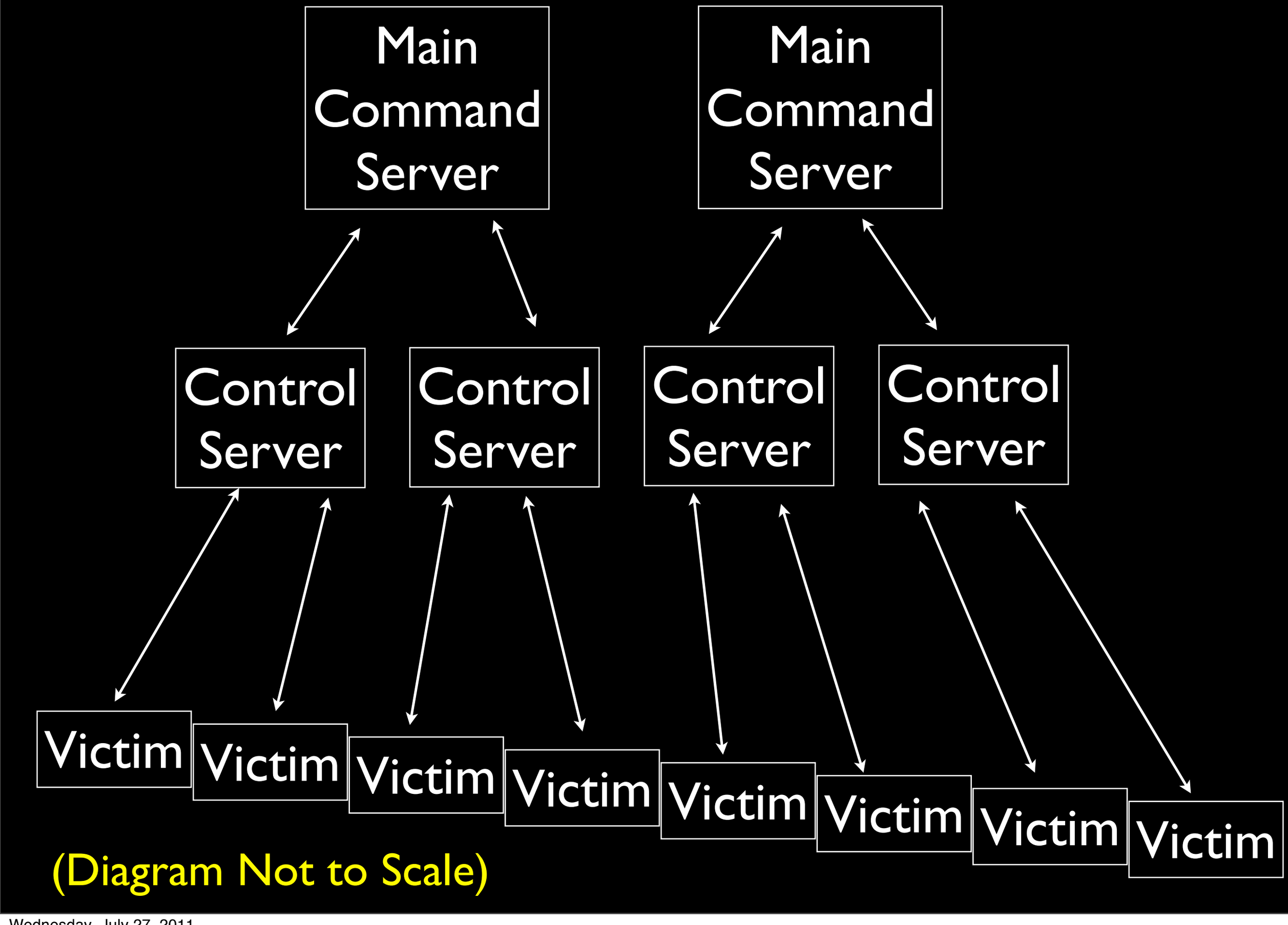
- Propagated via Pay-Per-Install [Piptea]
- Propagated via drive-by-download attacks
- Pharmacy spam...
- Blah, blah, more of the same...
- Oh yeah, and sending about 50% of all spam on Earth

Circa 2010

- Stopped sending spam approximately between Dec 25, 2010 and Jan 9, 2011
- No one is certain why yet, but lots of speculation:
- May have had something to do with "SpamIt/Glavmed" going down in Oct.
- Maybe someone involved got arrested
- Maybe the botnet operator(s) went on vacation [or were abducted by aliens...]

Technical Advancements 2009-2010

- Began using pseudo-random DNS names for C&C backup
- Used a slight variation of RC4 to encrypt communications
- DNS answers for C&Cs would return an obfuscated IP address, which Rustock would transform into the real thing
  1.2.3.4 -> 5.6.7.8
- C&C Server Hierarchy...


Main Command Server
Main Command Server
Control Server
Control Server
Control Server
Control Server
Victim
Victim
Victim
Victim
Victim
Victim
Victim
Victim
(Diagram Not to Scale)

Main Command Server

Main Command Server

Publicly Visible

Control Server

Control Server

Control Server

Control Server

Victim

Victim

Victim

Victim

Victim

Victim

Victim

Victim

(Diagram Not to Scale)

Invisible

Main Command Server

Main Command Server

Control Server

Control Server

Control Server

Control Server

Victim

Victim

Victim

Victim

Victim

Victim

Victim

Victim

(Diagram Not to Scale)

Technical Advancements 2009-2010

- Began using TLS/SSL for SMTP transport, and then stopped using it after several months, possibly for performance reasons.
- Fast-Flux DNS
- Mix random text from http://wikipedia.org/wiki/Special:Random into spam

Domains Answering with False IPs

- godlovesme.org
- chernomorsky.name
- hollybible.com
- hollyjesus.com
- muza-flowers.biz

Example Random Spam

From: Super Offers onViagra <ibabuyaz9927@comcastbusiness.net>
Subject: julia, cut prices all week. Roman a Planet present Forest

From: Super Offers onViagra <pesipahep8838@vt.edu>
Subject: julia, cut prices all week. the rates received

From: Super Offers onViagra <uxupeidi1999@alicedsl.de>
Subject: julia, cut prices all week. d The

From: Super Offers onViagra <okysoy7918@charter.com>
Subject: julia, cut prices all week. Executive

From: Super Offers onViagra <yavehawygo7373@rr.com>
Subject: julia, cut prices all week. the the

From: Super Offers onViagra <nuufuigu2455@comcast.net>
Subject: julia, cut prices all week. as sequential The After

From: "Pfizer PillsTrader" <seruky3597@mchsi.com>
Subject: Hi julia, Sale-Over Reminder. area volcanic Movies

From: "Pfizer PillsTrader" <iliowi9398@comcast.net>
Subject: Hi julia, Sale-Over Reminder. is the b IB on

From: "Pfizer PillsTrader" <pocisyxu4643@2sex899.com>
Subject: Hi julia, Sale-Over Reminder. more Please the A members

Rustock Command & Control Network Locations

Search

Map

Google 200 km 200 mi

Map data ©2011 Europa Technologies, Google, INEGI, LeadDog Consulting - Terms of Use

Wednesday, July 27, 2011

2011

- March 16, 2011: US Federal Marshals and the Dutch High Tech Crime Unit seize all Rustock C&C physical servers

The Present

Operation b107

- Operation b49, Waledac takedown in 2010
  - DNS name transfer to Microsoft
- Not applicable to Rustock
- Richard Boscovich had a great idea:
- Lanham Trademark Act (15 U.S.C.)
- And also, Computer Fraud and Abuse Act (18 U.S.C) and CAN-SPAM Act (15 USC)

Operation b107

"Enter a preliminary and permanent injunction isolating and securing the botnet infrastructure, including the software operating from and through the Command and Control IP Addresses/ Domains and placing that infrastructure outside of the control of the Defendants or their representatives or agents."

TL;DR We want to to seize all the computers.

Lanham Trademark Act

- Allows companies to seize [alleged] counterfeit goods and trademark infringing materials

- The Rustock C&C servers [are believed to] contain spam templates for emails claiming to be from Microsoft, and for counterfeit Pfizer pharmaceuticals

- ...Which are all fraudulently using Microsoft and Pfizer's trademarks

Since March

- Brian Krebs may have found at least one person behind the operation of the Rustock Botnet: Vladimir Alexandrovich Shergin (who doesn't pay his hosting bills)
- Another suspect associated with SpamIt goes by "Cosma2k," possibly named Dmitri A. Sergeev, Artem Sergeev, or Sergey Vladomirovich Sergeev
- Name is kinda like "John Smith" in English

I want to work in

Google™

Sergeev Dmitri A.

Summary:

Experience

June 2006 - present

Experience

June 2006 - present
Software Engineer - Itransition (software development)
Duties, functions, achievements:
software development for C + + (ActiveX, STL, MFC, ATL, COM) and C # (MMC 3.0 SnapIns, PowerShell scripts, install projects, GUI application, SharePoint Services and others), problem-solving on a project with customers (English). Serve as experts in the field of installations (InstallShield, InstallAnywhere and a little IsPack, InnoSetup) (for Windows XP x32 and x64, Windows Vista x32 and x64 and other types). Partial participation in the Java project.

June 2005 - October 2005
Software Engineer - Individual (web sites)
Duties, functions, achievements:
development of sites with admin's part, the scripts to collect information from websites.

June 2005 - June 2006
Software Engineer, Mathematician - Agileo (software development)
subordinate to a man
Duties, functions, achievements:
Defining the implementation of a 3D model in Microsoft Office (Word Art) and the introduction of this algorithm in the application that converted rtf files (c + + and java projects).

December 2004 - June 2005
Software Engineer - Internet Service Provider Magistral (providing access to the Internet)
subordinate to a man
Duties, functions, achievements:
Technical Support Internet Service

February 2003 - December 2004
Software Engineer - Individual (trade)
Duties, functions, achievements:
Writing in the old VB 6.0 program that was written in Clipper.
Professional skills, abilities, competencies
The long experience of programming in C + + / C #. Investigation of new technologies, solutions for special problems, no problems with foreign code, an expert in the field of installations (InstallShield, InstallAnywhere and a little IsPack, InnoSetup) (for Windows XP x32 and x64, Windows Vista x32 and x64 and other types) .
Information about education

2000 - 2002 (top)
Belarusian State University
Faculty: Faculty of Applied Mathematics and Computer Science - Evening Study
Profession: Programmer
Qualifications: engineer

1996 - 2001 (higher technical)
Belarusian State University
Faculty: Physics - daily study
Specialty: Nuclear electronics and metrology red diploma
Qualifications: Master's degree and postgraduate studies from 2001 to 2004 BSU day department

Languages
English *(can pass the interview)*
French *(basic knowledge)*

Other information
Hobbies, Sports
interested in useful technologies and capabilities in C + + / C #, weekend sports (gym and pool)

Additional information
executive and executive

Waiting for your job:

ger-mes@ger-mes.ru

Since March

- Microsoft has been running advertisements in the newspapers circulated near where the operators are believed to be
- They have also been trying to contact all of the alleged operators via email, phone, and ICQ; Basically saying: "Hey, we have your stuff, tell us if we're mistaken."
- So far, no one has contacted Microsoft complaining about their servers being sized

Задолженность по грандам

Испанские регионы увеличивают долговое бремя страны

Ольга Шамина
o.shamina@mn.ru

115,5 млрд евро *составили долги испанских регионов в 2010 году*

Долговые проблемы Испании серьезнее, чем до сих пор думали, полагает агентство Fitch. Значительная часть долга сосредоточена в регионах. Администрация крупнейшей автономной области Кастилия-Ла-Манча задолжала €2 млрд поставщикам товаров и услуг и не может выплатить зарплаты 76 тыс. госслужащих. Центральное правительство тоже не знает, как разрешить финансовые проблемы.

Спокойной жизни испанской провинции угрожает призрак дефолта

В первом квартале 2011 года общий дефицит бюджетов всех 17 автономных областей Испании составил почти €5 млрд, или 0,46% ВВП, оценило агентство Fitch. Главными должниками стали Мадрид и Андалузия. Бюджету Мадрида в первом квартале не хватило €1,18 млрд, или 0,6% валового регионального продукта, Андалузии — €1,1 млрд, или 0,75% ВРП. Небольшой профицит наблюдался в первом квартале лишь в трех областях – Арагоне, Риохе и Галиции.

По меркам госбюджетов стран ЕС это небольшие проблемы, но важна тенденция. В 2011 году дефицит региональных бюджетов не должен, по планам испанского правительства, превышать 1,3% местных ВРП. Но есть риск превысить этот рубеж, полагают Фернандо Майорга и Гильхем Костес из Fitch. Уже в первом квартале многие сообщества подошли к предельному уровню. Например, дефицит бюджетов Кастилии-Ла-Манчи и Балеарских островов составил 0,97% ВРП. Главная причина — рост расходов. Совокупные расходы местных администраций в первом квартале выросли на 5,56%, а за весь 2010 год — на 4,81%.

У агентства Moody's на прошлой неделе вызвала беспокойство Каталония, где дефицит бюджета в 2011 году составит 2,66% ВРП. Это угрожает попыткам правительства сократить дефицит всего бюджета страны с 9,24% ВВП в 2010-м до 6% в 2011 году, полагает Moody's.

В 2010 году долг испанских регионов составил €115,5 млрд. У правительства есть возможность контролировать рост долгосрочной задолженности — регионы должны согласовывать такие заимствования. Но для краткосрочных кредитов этого не нужно, а они уже составляют до четверти всей задолженности.

Вскрыть масштаб проблемы иногда помогает приход к власти оппозиции. В конце мая в Кастилии-Ла-Манче на выборах победила оппозиционная Народная партия. До этого регионом в течение нескольких десятилетий правили социалисты. По данным Bloomberg, лидер оппозиционной партии Винсент Тирабо заявил, что у региона фактически нет средств, а оплатить работу госслужащих и поставщиков администрация не может.

Члены Социалистической партии назвали эти заявления «хулиганством». Долг региона составляет около €7 млрд, правительство не оплатило различных контрактов на €2 млрд, сообщила испанская газета elEconomista. Примерно 76 тыс. госслужащих может не получить в этом месяце зарплату, добавляет Bloomberg. Кастилию-Ла-Манчу уже называют «маленькой Грецией».

Кредиторы уже предъявляют испанским должникам счета. По данным Испанской ассоциации фармакологических компаний, госсистема здравоохранения страны должна поставщикам €5,2 млрд. В одних регионах поставщикам не платили за лекарства для больниц уже больше года, а в других — более полутора лет. Система здравоохранения и закупки полностью контролируются региональными правительствами.

Из-за роста скрытого долга испанскому правительству будет сложно сократить дефицит бюджета до 6% в 2011 году, считает Лавиния Сантоветти из банка Nomura. На самом деле дефицит достигнет 6,7%, полагают в банке. Но катастрофа Испании не грозит. Даже если ситуация в трех крупнейших регионах — Каталонии, Мадриде и Андалузии — будет развиваться по греческому сценарию (там в 2010 году дефицит бюджета оказался в пять раз больше первоначальных оценок), это добавит лишь 3,5 п.п. к общей долговой нагрузке страны, пояснила «МН» Сантоветти. #

Агентство Fitch fitchratings.ru

Майские каникулы бюджета

Расходы правительства все сильнее отстают от доходов

Андрей Сусаров
a.susarov@mn.ru

По данным Минфина, к лету профицит федерального бюджета достиг 355,8 млрд руб. — 1,8% ВВП. Но благостную картину во многом обеспечили длинные майские праздники — из-за них уменьшились расходы бюджета. А вот доходов собрано уже почти половина от годового плана.

Доходы федерального бюджета по итогам января–мая составили почти 4,2 трлн руб., сообщил в минувшую пятницу Минфин. Израсходовало правительство 3,8 трлн руб. В прошлом году в это самое время в бюджете был дефицит в 463 млрд рублей.

Экономию этого года правительство вряд ли может считать своим достижением. Если доходы поступают в бюджет с явным опережением от плана, и за пять месяцев их сборы уже составили почти половину — 47,5% — от намеченной на весь год суммы, то расходы заметно отстают, едва превысив треть годовой росписи — 36%.

Особенно резко бюджетные расходы оказались зажаты в мае, сократившись почти на треть по сравнению с апрелем. Меньше чем в мае бюджет в этом году тратил только в январе, да и то всего на 1%. Получается, что майские каникулы на активности бюджетных распорядителей сказались не меньше, чем рождественские. Благодаря этому в федеральном бюджете и возник столь существенный профицит — 4,6% ВВП. В прошлом году сокращение расходов в мае тоже фиксировалось, но было заметно меньше — на 24%.

Неравномерность расходов внутри года Минфину пока победить не удается. В прошлом году за первые пять месяцев в федеральный бюджет было собрано 46% от первоначального годового плана, зато расходы не дотянули и до 37%. Казалось бы, сейчас отставание небольшое. Но прошлый год завершился декабрьским аккордом, который оказался рекордным для последних пяти лет: расходы в декабре были в 2,1 раза больше ноябрьских и в 2,4 раза превзошли средние за предыдущие 11 месяцев. Очевидно, попытки Минфина добиться более плавного исполнения бюджета в этом году (см. «МН» от 28 марта) пока не увенчались успехом, и прошлогодний рекорд может быть побит.

Бюджетный процесс у нас устроен так, что расходный «навес» к концу года неизбежен, отмечает Елена Пенухина из Центра макроэкономического анализа и краткосрочного прогнозирования. Минфин попытался в начале прошлого года перечислить сразу почти в полном объеме межбюджетные трансферты в регионы. За счет этого в прошлом году исполнение бюджета по расходам было более равномерным, чем прежде, соглашается Сергей Дробышевский из Института Гайдара. «Но через несколько месяцев стало понятно, что все идет как обычно. У нас всегда расходы запаздывают, а потом в течение нескольких последних месяцев года, разгоняя инфляцию, в бешеном темпе исполняются», — делает вывод Пенухина. К концу года мы неизбежно выйдем на бюджетный дефицит, считает Дробышевский.

Бюджет по-прежнему выручает выгодная конъюнктура. Если в целом, по данным Федерального казначейства, доходы января–мая этого года больше прошлогодних на 31,4%, фискальные сборы с импорта увеличились на 42,6%. Опережающим темпом растут и сырьевые налоги. На 41% больше поступило экспортных пошлин, собираемых преимущественно с нефти, газа и нефтепродуктов. На 39,3% больше собрано налога на добычу полезных ископаемых (НДПИ).

Наибольший прирост сборов НДПИ обеспечил природный газ. По итогам пяти месяцев поступления превзошли прошлогодние на 49,4%. Правда, ставка этого налога для газа была с 1 января 2011 года увеличена на 61%, а нефтяники обеспечили прирост сборов НДПИ на 40% и без изменения ставки, только за счет высоких цен на рынке. Так что увеличение поступлений газового НДПИ на самом деле скромнее того, что можно было ожидать.

В идеале сборы НДПИ с газа должны были увеличиться соразмерно росту ставки, соглашается президент Института энергетики и финансов Леонид Григорьев, если не упала добыча. По данным Минэнерго, за пять месяцев добыча газа по сравнению с аналогичным периодом прошлого года выросла на 2,9%. Но Григорьев указывает, что рост сборов вполне сопоставим с увеличением ставки.

Поступления по сборам, зависимым от внутреннего производства, выросли заметно слабее: поступление налога на прибыль выросло по сравнению с прошлым годом на 34,8%, внутреннего НДС — на 32,6%. Этот прирост в значительной степени связан с благоприятной для нас конъюнктурой на внешнем рынке, уверена Пенухина.

То, что общие доходы федерального бюджета в этом году выросли меньше, чем поступления по основным разделам, Пенухина объясняет снижением доходов от размещения средств Резервного фонда. На начало 2010 года в нем было 1,83 трлн руб., а к 1 января этого года — 0,78 трлн руб. (на 1 июня, по данным Минфина, с учетом курсовой переоценки, — 0,746 трлн руб.). В итоге, по данным Казначейства, доходы от размещения средств Резервного фонда сократились с 52 млрд руб. за пять месяцев прошлого года до 16 млрд в этом. А обслуживание госдолга, наоборот, стало дороже: расходы увеличились с 84,5 млрд до 99 млрд рублей. ■

В мае российское правительство уменьшило расходы и обеспечило высокий профицит бюджета

31%
составило уменьшение бюджетных расходов в мае

Налог с Турции

С момента совещания у Владимира Путина по налогообложению газовой отрасли, после которого министр финансов Алексей Кудрин объявил, что с газовиков в 2012 году планируется дополнительно взять 150 млрд руб., причем 80–90% — за счет роста НДПИ для «Газпрома», прошла неделя. Но ясности, как именно будет увеличиваться фискальное бремя в отрасли, нет.

Вчера профильный вице-премьер Игорь Сечин, который неделю назад отсутствовал на совещании, заявил, что «надо работать над оптимизацией налогообложения в газовой отрасли». «НДПИ может повлиять на уровень добычи, а нам нужно уровень добычи поддерживать, — сказал он Интерфаксу. — И мне представляется более целесообразным все-таки обратить внимание на сверхдоходы, которые дает экспорт». Он также оговорился, что и здесь понадобится сбалансированный подход, «обязательно с учетом реализации инвестиционной программы «Газпрома». Позднее источник в Минэнерго подтвердил, что в качестве одной из мер обсуждается введение экспортной пошлины на газ, который идет в Турцию через «Голубой поток». Но, по его словам, этот шаг придется согласовывать на межправительственном уровне с Турцией, которая вряд ли согласится с тем, что газ для нее подорожает на 30%.

Алексей Гривач

Задолженность по грандам

Испанские регионы увеличивают долговое бремя страны

Ольга Шамина
o.shamina@mn.ru

115,5 млрд евро
составил долг испанских регионов в 2010 году

Долговые проблемы Испании серьезнее, чем до сих пор думали, полагает агентство Fitch. Значительная часть долга сосредоточена в регионах. Администрация крупнейшей автономной области Кастилия-Ла-Манча задолжала €2 млрд поставщикам товаров и услуг и не может выплатить зарплаты 76 тыс. госслужащих. Центральное правительство тоже не знает, как разрешить финансовые проблемы.

В первом квартале 2011 года общий дефицит бюджетов всех 17 автономных областей Испании составил почти €5 млрд, или 0,46% ВВП, оценило агентство Fitch. Главными должниками стали Мадрид и Андалузия. Бюджету Мадрида в первом квартале не хватило €1,18 млрд, или 0,6% валового регионального продукта, Андалузии — €1,1 млрд, или 0,75% ВРП. Небольшой профицит наблюдался в первом квартале лишь в трех областях – Арагоне, Риохе и Галиции.

По меркам госбюджетов стран ЕС это небольшие проблемы, но важна тенденция. В 2011 году дефицит региональных бюджетов не должен, по планам испанского правительства, превышать 1,3% местных ВРП.

О спокойной жизни испанской провинции угрожает призрак дефолта

позиции. В конце мая в Кастилии-Ла-Манче на выборах победила оппозиционная Народная партия. До этого регионом в течение нескольких десятилетий правили социалисты. По данным Bloomberg, лидер оппозиционной партии Винсент Тирабо заявил, что у региона фактически нет средств, а оплатить работу госслужащих и поставщиков администрация не может.

Члены Социалистической партии назвали эти заявления «хулиганством». Долг региона составляет около €7 млрд, правительство не оплатило различных контрактов на €2 млрд, сообщила испанская газета elEconomista. Примерно 76 тыс. госслужащих может не получить

From The Court Filing

- I find this quote hilarious:

"No Customers of the IP addresses in question, or the domains in question have requested that the IP addresses and domains be reinstated."

Current Botnet Size

- Data Measured by Microsoft's Sinkhole
  - Mar 20-26, 2011: 1,601,619
  - June 12-18, 2011: 702,860

In Related News...

- Similar tactics have been used to takedown CoreFlood botnet after Rustock

The Future

Yet To Be Written...

I'm not being poetic, I mean I just haven't written this slide yet. It'll be done in the next few days.

Credits

- Microsoft Digital Crimes Unit & Richard Boscovich
- David Dittrich at University of Washington
- Patrick Ford of Pfizer Global Security
- Atif Mushtaq, et al. at FireEye
- Joe Stewart, Brian Krebs, M86Security, Messagelabs, and everyone else.

Questions?

http://blog.fireeye.com/

Bonus Fun Slides!

Let's read us some hex dumps!

Technical Stuff

Rustock C&C c. 2007-2008

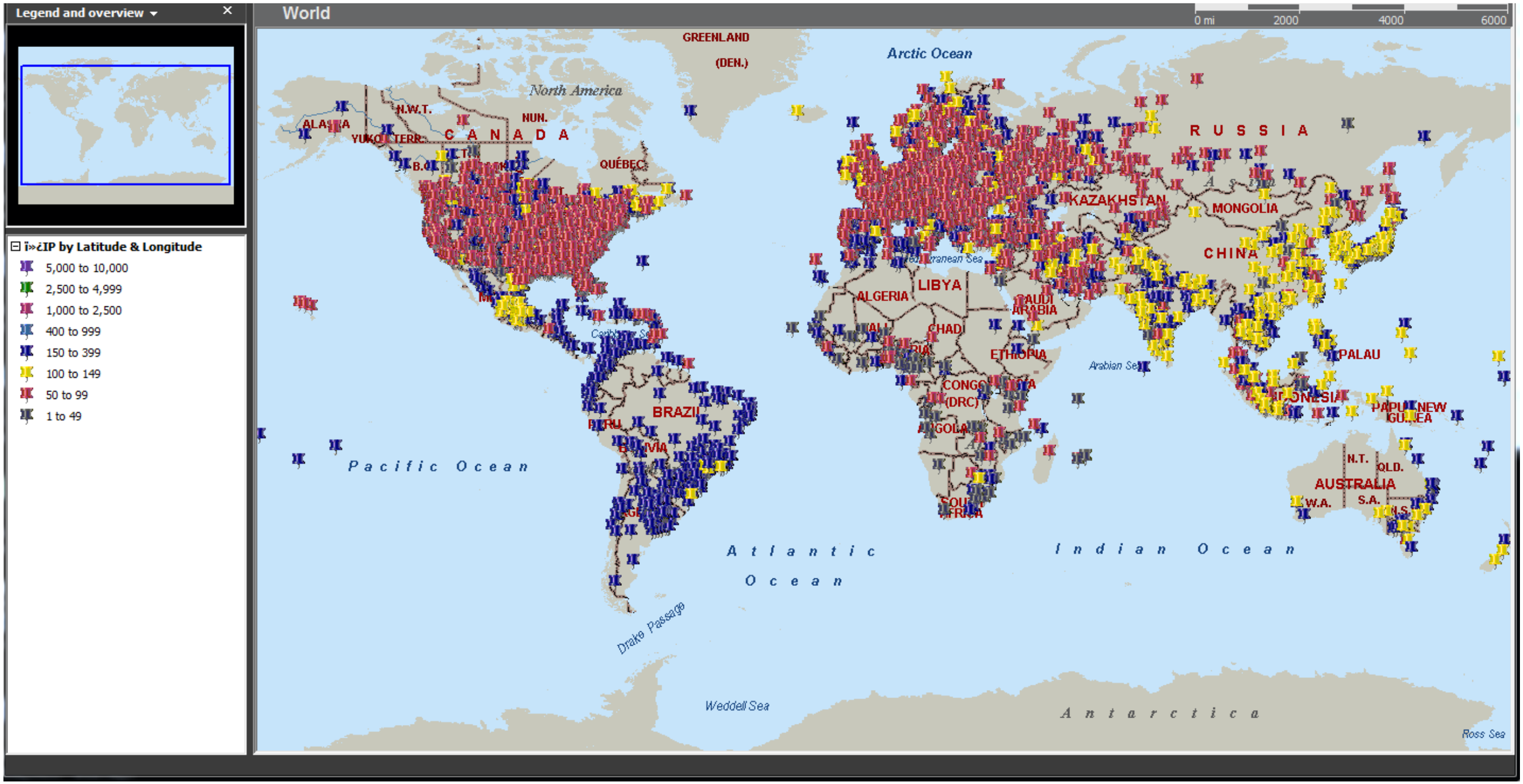
```
POST /data.php HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Accept-Language: en
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Host: 208.66.194.22
Content-Type: multipart/form-data
Content-Encoding: gzip
Content-Length: 135
Connection: Close
Pragma: no-cache
```

Rustock C&C c. 2009-2010

```
POST /index.php?topic=3D33.117 HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://go-thailand-now.com
Content-Type: application/x-www-form-urlencoded
Content-Encoding: gzip
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Host: go-thailand-now.com
Content-Length: 214
Connection: Keep-Alive
Cache-Control: no-cache
```

By Contrast, Spyeye

```
GET /web/map/gate.php?guid=3Dusers1!AJKLPQ!
JU1232&ver=3D10280&stat=ONLINE&plg=ftpbc;socks5;t2p&cpu=0&ccrc=JKLAF24&md5=9012ab902413dcf8gg
a89 HTTP/1.0
User-Agent: Microsoft Internet Explorer
Host: hahsdhsl.com
Pragma: no-cache
```


Legend and overview
World
0 mi
2000
4000
6000
ï»¿IP by Latitude & Longitude
5,000 to 10,000
2,500 to 4,999
1,000 to 2,500
400 to 999
150 to 399
100 to 149
50 to 99
1 to 49
GREENLAND
(DEN.)
Arctic Ocean
North America
N.W.T.
NUN.
C A N A D A
QUÉBEC
RUSSIA
KAZAKHSTAN
MONGOLIA
CHINA
LIBYA
ALGERIA
CHAD
ETHIOPIA
PALAU
BRAZIL
Arabian Sea
N.T.
QLD.
AUSTRALIA
W.A.
S.A.
Pacific Ocean
Atlantic Ocean
Indian Ocean
Drake Passage
Weddell Sea
Antarctica
Ross Sea


black hat®
BRIEFINGS & TRAINING
USA + 2011
EMBEDDING SECURITY

Please Remember to Complete Your Feedback Form