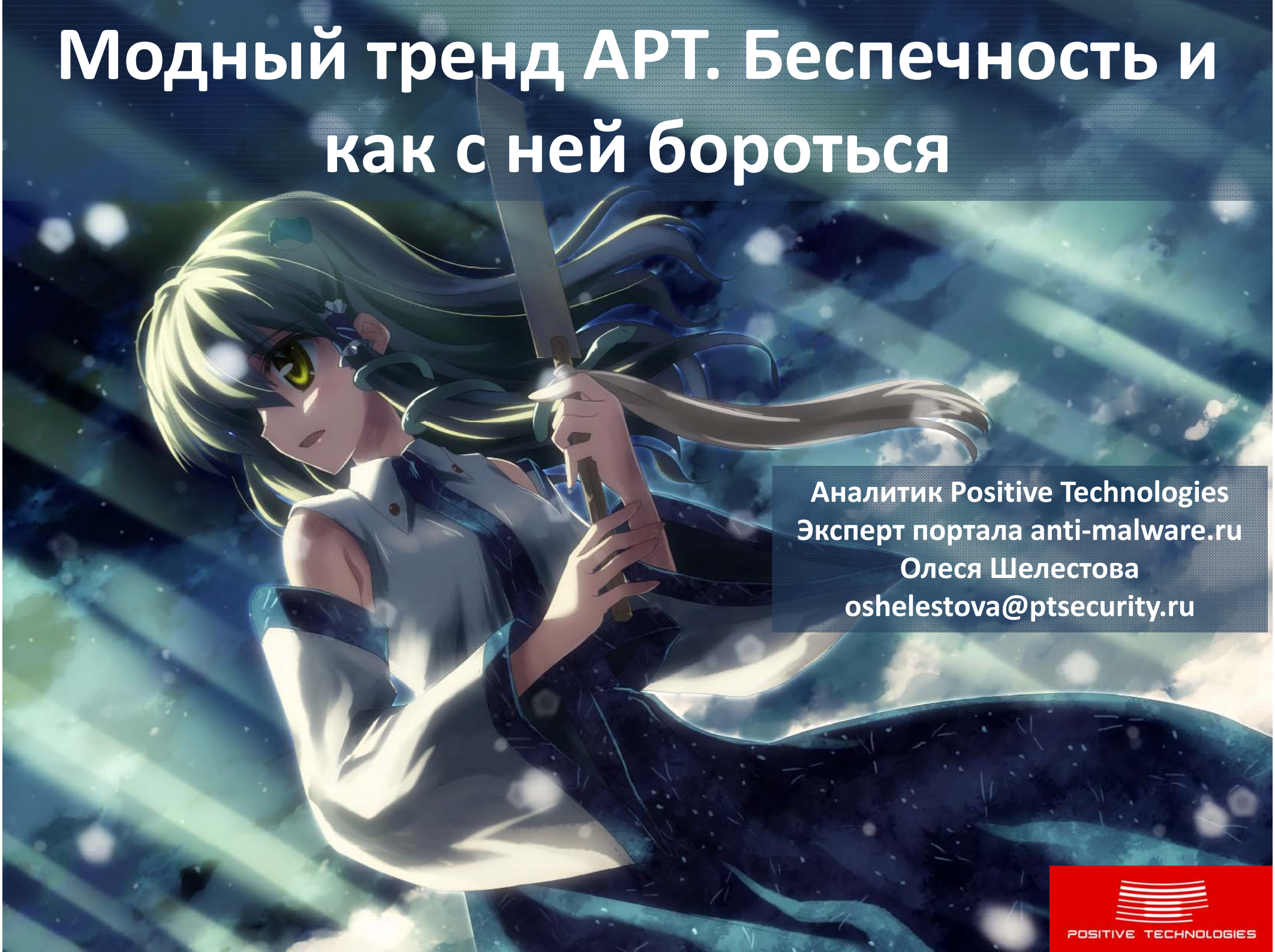
Модный тренд APT. Беспечность и как с ней бороться



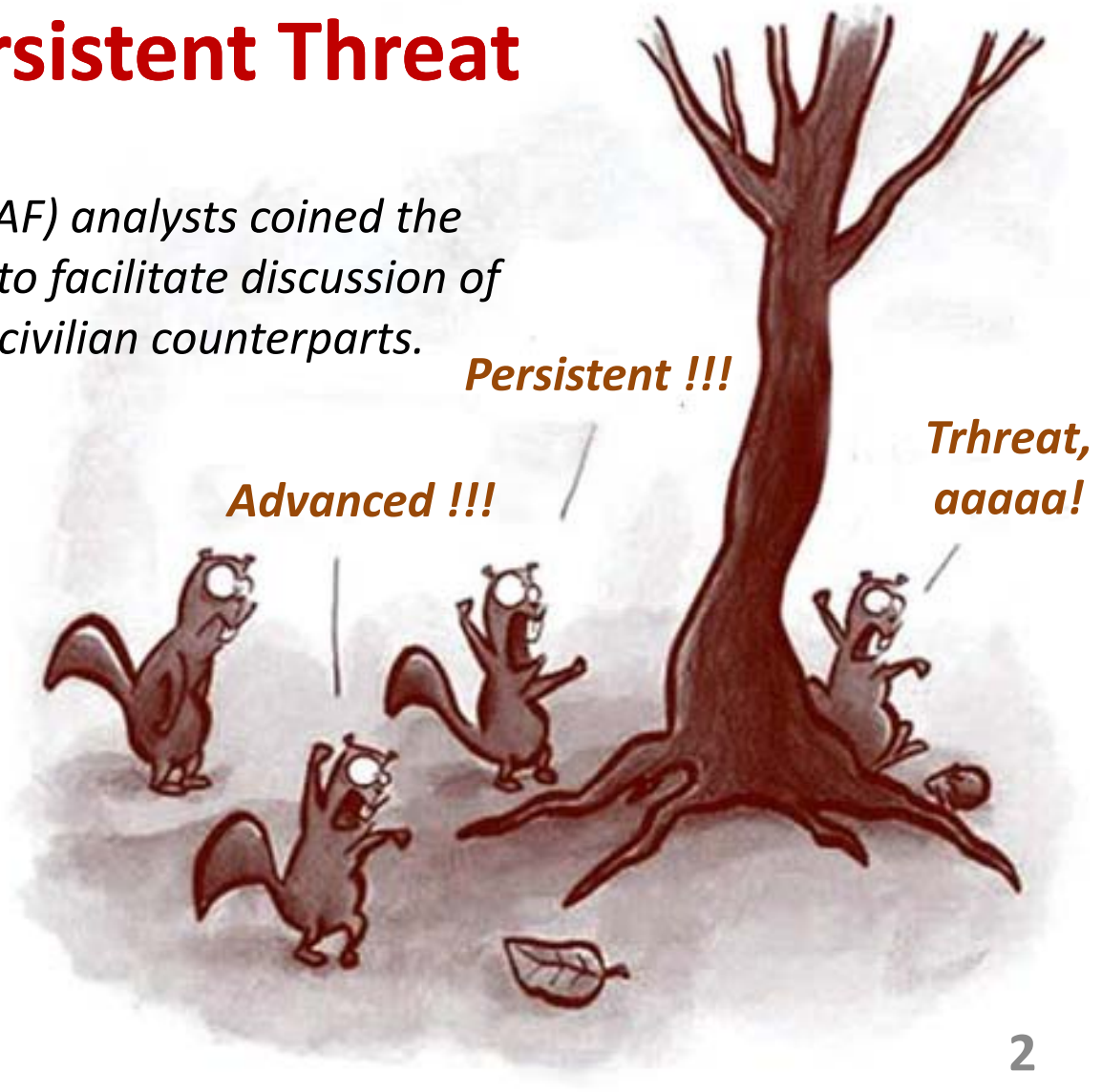
Аналитик Positive Technologies
Эксперт портала anti-malware.ru
Олеся Шелестова
oshelestova@ptsecurity.ru

POSITIVE TECHNOLOGIES

Что такое APT

APT – Advanced Persistent Threat

*In 2006, the United States Air Force (USAF) analysts coined the term **advanced persistent threat** (APT) to facilitate discussion of intrusion activities with their uncleared civilian counterparts.*



Следует понимать, что APT – Это НЕ malware! Это вид, парадигма атаки.

Чем отличается от других атак

- Атакующих – группа
- Индивидуальный подход к жертве
- Использование старых уязвимостей, 0-day совместно с социальной инженерией
- Цель – получение ценной информации
- Получают полный доступ над жертвой
- Не останавливаются на неудачной попытке
- Долго и тщательно скрывают свое присутствие
- Не фокусируются на ROI
- Возвращаются «I'll be back»
- Что хотят: «critical data and assets, for example, card holder data, source code, and trade secrets» (SANS)

SANS: "Even the best monitoring mindset and methodology may not guarantee discovery of the actual APT attack code. Instead, the power of more comprehensive analysis and correlation can discover behavior indicative of APT-related attacks and data exfiltration."

Как все шумно начиналось …

Operation Aurora.

Начало:
On January 12, 2010, Google revealed on its blog that it had been the victim of a cyber attack. The company said the attack occurred in mid-December and originated from China.

Google были первыми кто заявил об атаке.

Почему Aurora:
Aurora was part of the filepath on the attacker's machine that was included in two of the malware binaries that have since been associated with the attack. The filepath is typically inserted by code compilers to indicate where debug symbols and source code are located on the developer's machine. (McAfee)

Вообще-то, интерес изначально был к Китайским диссидентам

Нападавшие получили доступ к всего лишь двум аккаунтам китайских борцов за права человека. Один из них – Ai Weiwei.

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Interaction

Article Talk

Ai Weiwei

From Wikipedia, the free encyclopedia

This is a Chinese name; the family name is Ai.

Ai Weiwei (born 18 May 1957) is a Chinese conten
Swiss architects Herzog & de Meuron as the artistic
Government's stance on democracy and human righ
schools" in the 2008 Sichuan earthquake.[4] In 2011
"economic crimes" (tax evasion). In October 2011 A
spokesman Liu Weimin responded, "China has man
magazine".[5]

n, and social, political and cultural criticism.[1][2] Ai collaborated with
activist, he has been highly and openly critical of the Chinese
an schools corruption scandal following the collapse of so-called "tofu-skin
hout any official charges being filed; officials alluded to their allegations of
n was criticised by the Chinese authorities. Chinese Foreign Ministry
a political bias and perspective has violated the objectives of the

Как проводилась атака

Несколько сотрудников получали письма от доверенных адресатов

Письмо содержало ссылку на сайт, расположенный в Тайване

На сайте был размещен JavaScript, эксплуатирующий уязвимость в Internet Explorer (Memory Corruption)

На инфицированную систему устанавливался бэкдор

Инфицированная система подключалась к C&C по 443 порту, используя шифрование трафика

На момент обнаружения атаки не было информации о том какая уязвимость используется и в каком продукте

Шаг за шагом, инфицировались другие внутренние ресурсы в этой сети, которые также использовались в атаке и далее для получения доступа к конечным целям (pivoting)

А потом…

Спустя недел

уязвимости M

Microso

Cumulativ

Published: Thurs

В марте 2010 Symantec, помогавший в

что S (12 миллиард ils» разосланных по

всем

В ма м что также по PT

RSA, Google, Morgan Stanley, HBGarry, Adob r Networks, Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical were also among the targets.

В APT Aurora атакующими для закрепления на протяжении многих месяцев во внутренней сети жертвы использовались системы software-configuration management (SCM) (Google, Adobe и другие компании в «Fortune 100 companies»).

Причин для этого было множество:

1) Там было много «вкусного»;
2) SCM более надежен в отличие от рабочих станций;
3) Много уязвимостей.

Много. Очень много уязвимостей.

PerForce.

PERFORCE

Company | Contact | Search

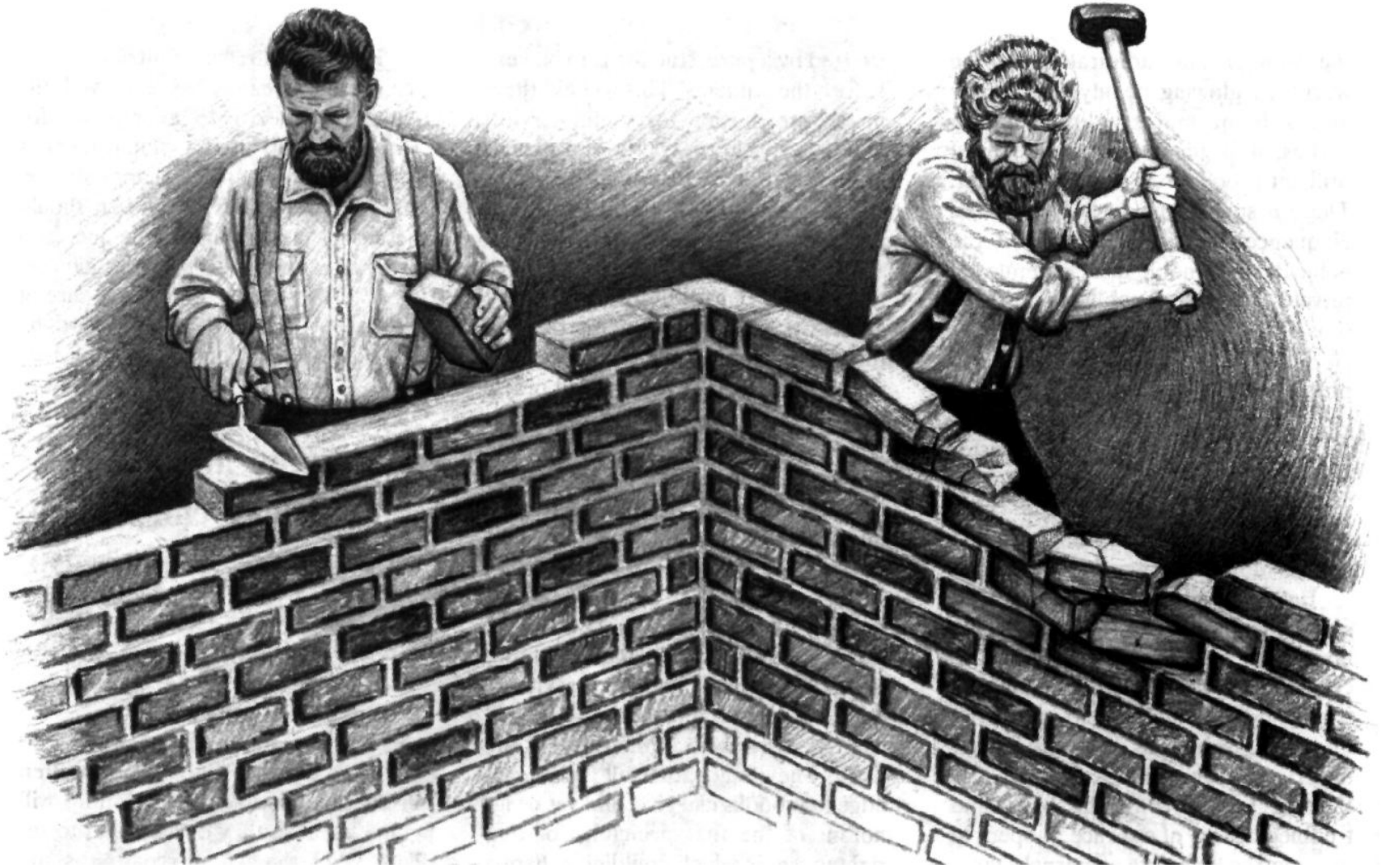
Products | Downloads | Documentation | Multimedia | Customers | Services | Purchase | Support

Create. Develop.

Version everything with Perforce.

Software and firmware. Digital assets and games. Websites and documents. More than 400,000 users in over 5,500 organizations trust Perforce to version their work. Discover fast, scalable effortless version management with the Perforce platform.

RSA attack



- Начало атаки пришлось на две небольшие группы сотрудников.
- Злоумышленники обходя спам фильтры в течение двух дней отсылали им фишинговые письма.
- Письмо содержало файл MS Excel с 0-day||уязвимостью Adobe Flash (CVE 2011-069)
- Естественно, при открытии файла – эксплойт устанавливал RAT
- RAT устанавливал реверс коннект на tcp порт 3460 C&C сервера

«the victim workstations installed a remote access toolkit (RAT) known as Poison Ivy; referred to here as PI-RAT»

“A —zero-day exploit for a vulnerability is created before, or on the same day, as a vendor learns about a particular vulnerability and no patch or remediation is available yet.”

The PI-RAT toolkit has been extensively used in other attacks, including GhostNet

И военным стало очень страшно, поскольку алгоритмы и продукты RSA используются много где))

GhostNet (ShadoNet). Introduction.

Между июне ...ружил двух
фазовую ата
Жертвы атак ...ике.

Жертвами ок ...ра в Лондоне,
Нью Йорке, Б ...одали как
злоумышлен

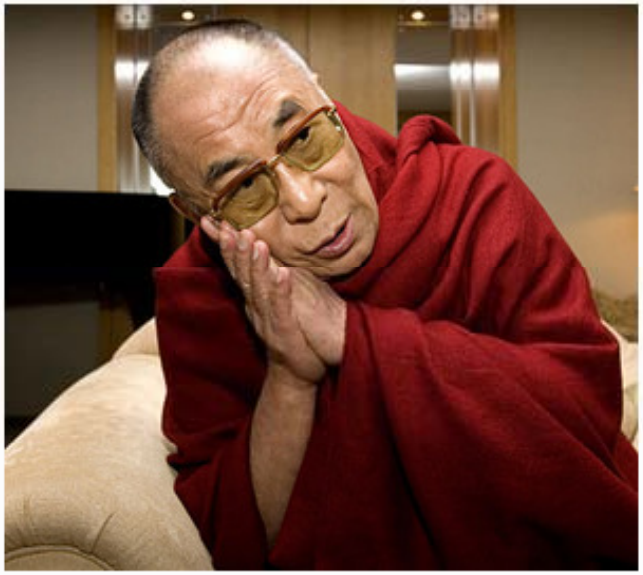
China Is Scary

Somebody Hacked the Dalai Lama

By Jen Doll Tue., Apr. 6 2010 at 1:59 PM
Categories: China Is Scary, Cybercrime, Jen Doll, Technology

Comments (3)

Like Send Tweet 0 Submit Pin it +1 0



Can you guess this man's password?

Let's say you're part of a gang of infamous, powerful Chinese hackers with a really cool name, say, "the Shadow Network." You've busted through the fortified security systems of sensitive targets "including foreign ministries, embassies, and even a computer at NATO headquarters." All in all, you've stolen confidential, privileged information from 103 countries and almost 1,300 computers.

But what do you *really* want?

Ah yes, the personal e-mails of the man behind the following Yoda-like nuggets of wisdom:

"Happiness is not something ready made. It comes from your own actions."

- Web интерфейс управлял четырьмя C&C.
- Когда эксперты обнаружили его, выяснилось что инфицированными оказались 1,295 компьютера в 103 странах

«close to 30% of the infected computers can be considered high-value and include the ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan; embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation), and the Asian Development Bank; news organizations; and an unclassified computer located at NATO headquarters»

«In 2009 and 2010, researchers from the University of Toronto published reports on two cyberespionage networks known as “GhostNet” and “ShadowNet” that included malware and command and control infrastructure connected with the Enfal Trojan.»

Enfal использовался еще в давние времена. Активность его была замечена с 2002 года и была известна как “Byzantine Hades”, “Byzantine Anchor,” “Byzantine Candor” и “Byzantine Foothold.

Как распространялся

- Сформирова
  campaigns@f
- Аттач был в ф
  ID Book for Ti

ement

From: "campaigns@freetibet.org" <campaigns@freetibet.org>
Date: 25 July 2008
Subject: Translation of Freedom Movement ID Book for Tibetans in Exile

Translation of Freedom Movement ID Book for Tibetans in Exile.

Front Cover

Emblem of the Tibetan government in Exile

Script: Voluntary Contribution into common fund for Tibetan Freedom Movement

Inside Cover

Resolution was passed in the preliminary general body meeting of the Tibetan Freedom Movement held on July 30, 1972 that the Tibetan refugees in exile would promise for each individual,Äôs share of the voluntary contribution into the Tibetan Freedom Movement Receipt book. This resolution was later reaffirmed by the 11th Tibetan People,Äôs Deputies and passed into the law on April 01, 1992 (Tibetan King Year 2119)

Until the last page of this book is used, the book stands valid until August 15, 2012

Date: August 16, 2008
Emblem of the Tibetan Government in Exile

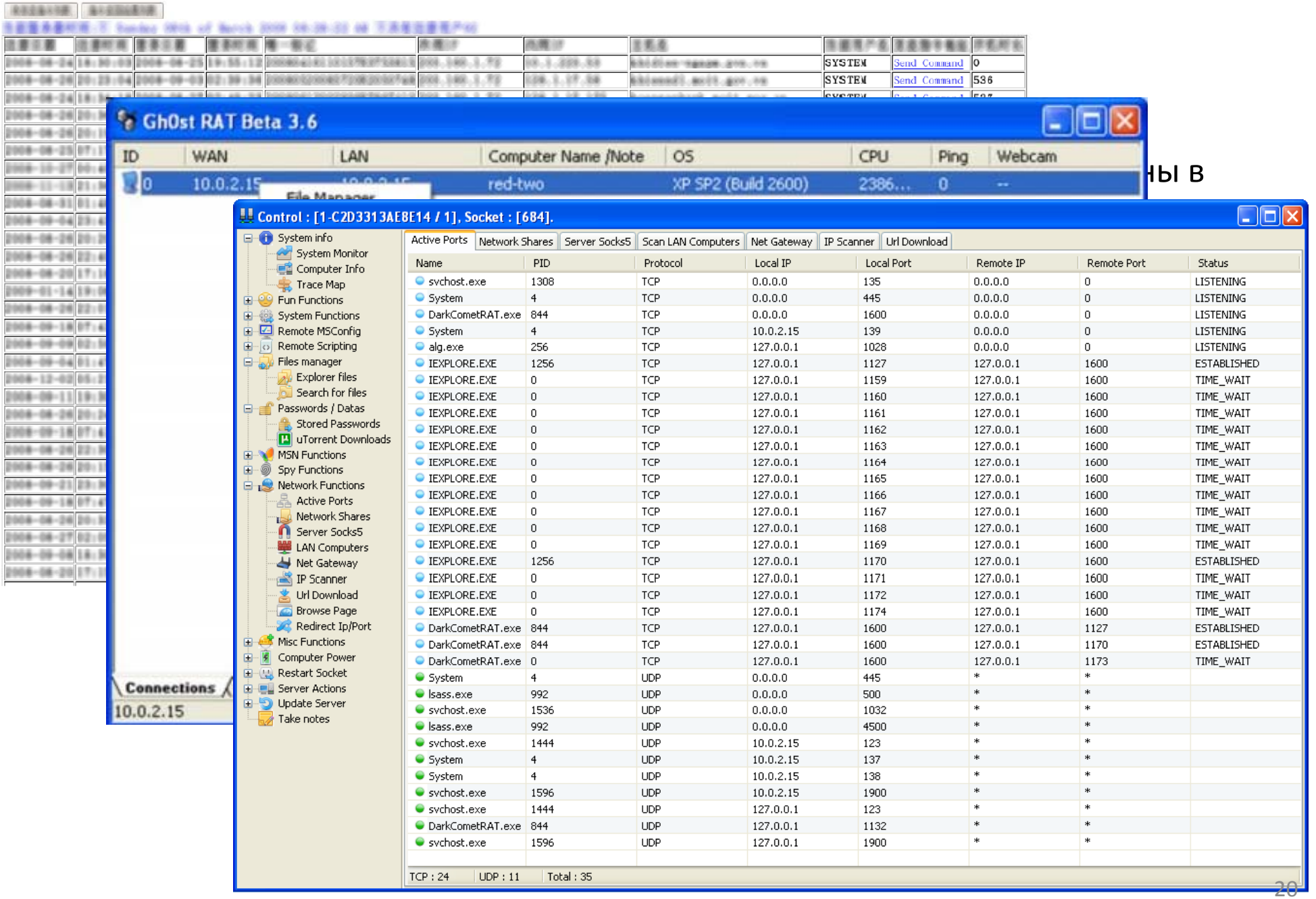
Official Signature

Attachment: Translation of Freedom Movement ID Book for Tibetans in Exile.doc

- При открытии письма или ссылки использовалась уязвимость и устанавливался бэкдор

“I July 2008, Only 11 of the 34 anti-virus programs provided by Virus Total38 recognized the malware embedded in this document”

Antivirus	Version	Last Update	Result
AntiVir	-	-	EXP/Word.Dropper.Gen
Authentium	-	-	CVE-2006-2492
Avast	-	-	MW97:CVE-2006-2492
eTrust-Vet	-	-	W97M/SmartTags!exploit
F-Prot	-	-	CVE-2006-2492
Fortinet	-	-	MSWord/ObjPointer.A!exploit.M20062492
GData	-	-	MW97:CVE-2006-2492
Ikarus	-	-	Virus.MW97.CVE.2006.2492
Microsoft	-	-	Exploit:Win32/Wordjmp.gen
Sophos	-	-	Troj/MalDoc-Fam
Webwasher-Gateway	-	-	Exploit.Word.Dropper.Gen

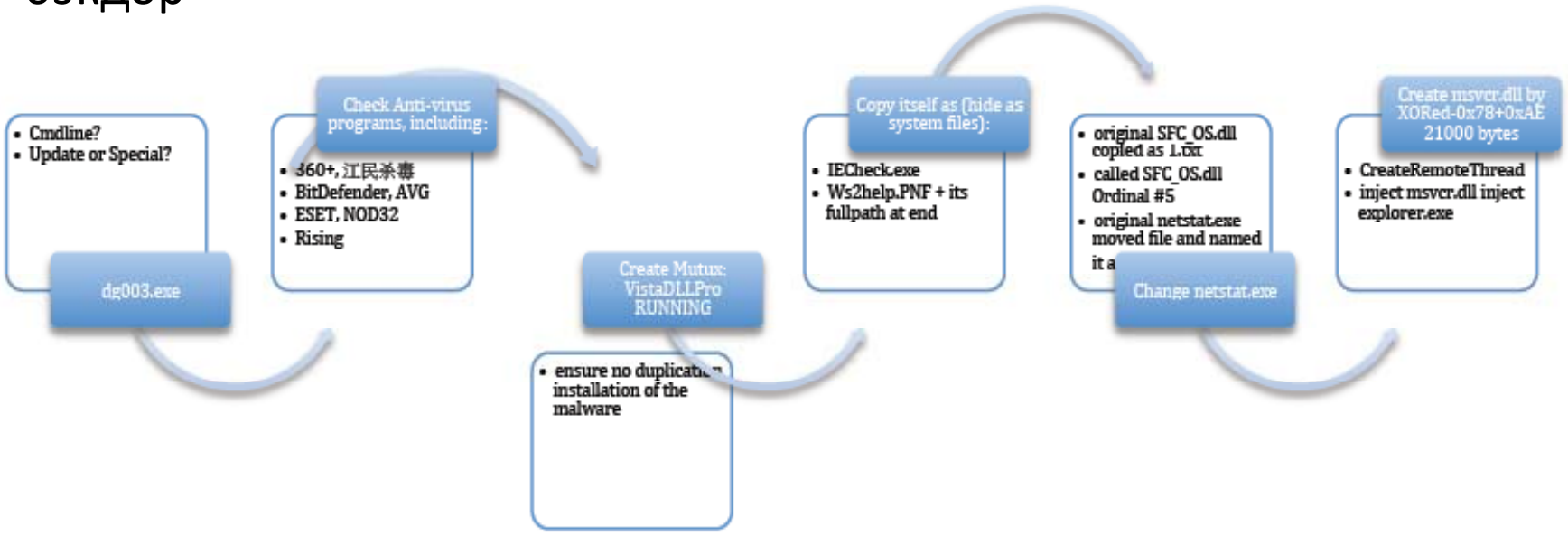

GhOst RAT Beta 3.6
ID
WAN
LAN
Computer Name /Note
OS
CPU
Ping
Webcam
0
10.0.2.15
red-two
XP SP2 (Build 2600)
2386...
0
--
Control : [1-C2D3313AE8E14 / 1], Socket : [684].
System info
System Monitor
Computer Info
Trace Map
Fun Functions
System Functions
Remote MSConfig
Remote Scripting
Files manager
Explorer files
Search for files
Passwords / Datas
Stored Passwords
uTorrent Downloads
MSN Functions
Spy Functions
Network Functions
Active Ports
Network Shares
Server Socks5
LAN Computers
Net Gateway
IP Scanner
Url Download
Browse Page
Redirect Ip/Port
Misc Functions
Computer Power
Restart Socket
Server Actions
Update Server
Take notes
Connections
10.0.2.15
Active Ports
Network Shares
Server Socks5
Scan LAN Computers
Net Gateway
IP Scanner
Url Download
Name
PID
Protocol
Local IP
Local Port
Remote IP
Remote Port
Status
svchost.exe 1308 TCP 0.0.0.0 135 0.0.0.0 0 LISTENING
System 4 TCP 0.0.0.0 445 0.0.0.0 0 LISTENING
DarkCometRAT.exe 844 TCP 0.0.0.0 1600 0.0.0.0 0 LISTENING
System 4 TCP 10.0.2.15 139 0.0.0.0 0 LISTENING
alg.exe 256 TCP 127.0.0.1 1028 0.0.0.0 0 LISTENING
IEXPLORE.EXE 1256 TCP 127.0.0.1 1127 127.0.0.1 1600 ESTABLISHED
IEXPLORE.EXE 0 TCP 127.0.0.1 1159 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1160 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1161 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1162 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1163 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1164 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1165 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1166 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1167 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1168 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1169 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 1256 TCP 127.0.0.1 1170 127.0.0.1 1600 ESTABLISHED
IEXPLORE.EXE 0 TCP 127.0.0.1 1171 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1172 127.0.0.1 1600 TIME_WAIT
IEXPLORE.EXE 0 TCP 127.0.0.1 1174 127.0.0.1 1600 TIME_WAIT
DarkCometRAT.exe 844 TCP 127.0.0.1 1600 127.0.0.1 1127 ESTABLISHED
DarkCometRAT.exe 844 TCP 127.0.0.1 1600 127.0.0.1 1170 ESTABLISHED
DarkCometRAT.exe 0 TCP 127.0.0.1 1600 127.0.0.1 1173 TIME_WAIT
System 4 UDP 0.0.0.0 445 * *
lsass.exe 992 UDP 0.0.0.0 500 * *
svchost.exe 1536 UDP 0.0.0.0 1032 * *
lsass.exe 992 UDP 0.0.0.0 4500 * *
svchost.exe 1444 UDP 10.0.2.15 123 * *
System 4 UDP 10.0.2.15 137 * *
System 4 UDP 10.0.2.15 138 * *
svchost.exe 1596 UDP 10.0.2.15 1900 * *
svchost.exe 1444 UDP 127.0.0.1 123 * *
DarkCometRAT.exe 844 UDP 127.0.0.1 1132 * *
svchost.exe 1596 UDP 127.0.0.1 1900 * *
TCP : 24
UDP : 11
Total : 35

Operation Shady RAT

On April 11, 2009, researchers at the Information Warfare Monitor released a report that uncovered a suspected cyber espionage network of over 1,295 infected hosts in 103 countries.

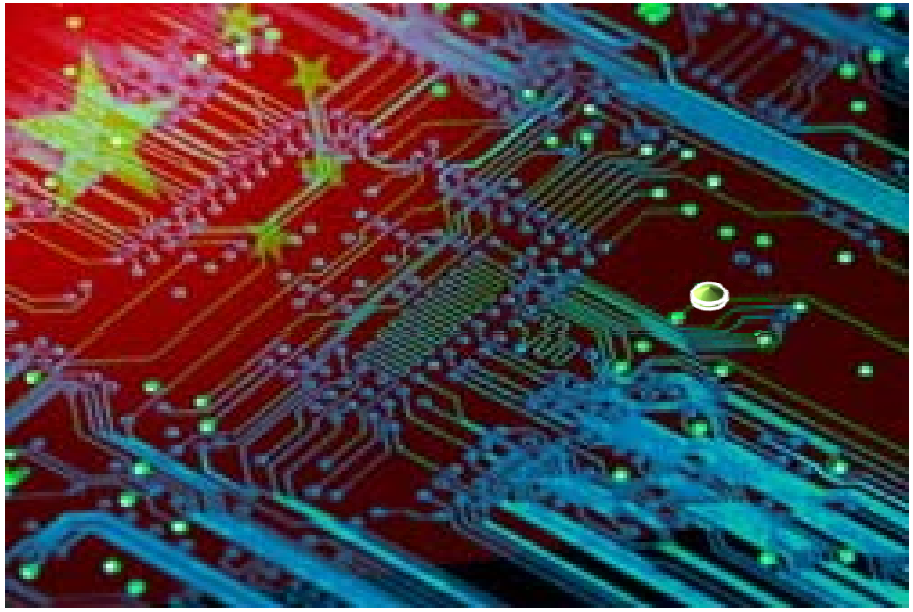
Эта атака не была чем то новым. “McAfee has detected the malware variants and other relevant indicators for years with Generic Downloader.x and Generic BackDoor.t heuristic signatures”

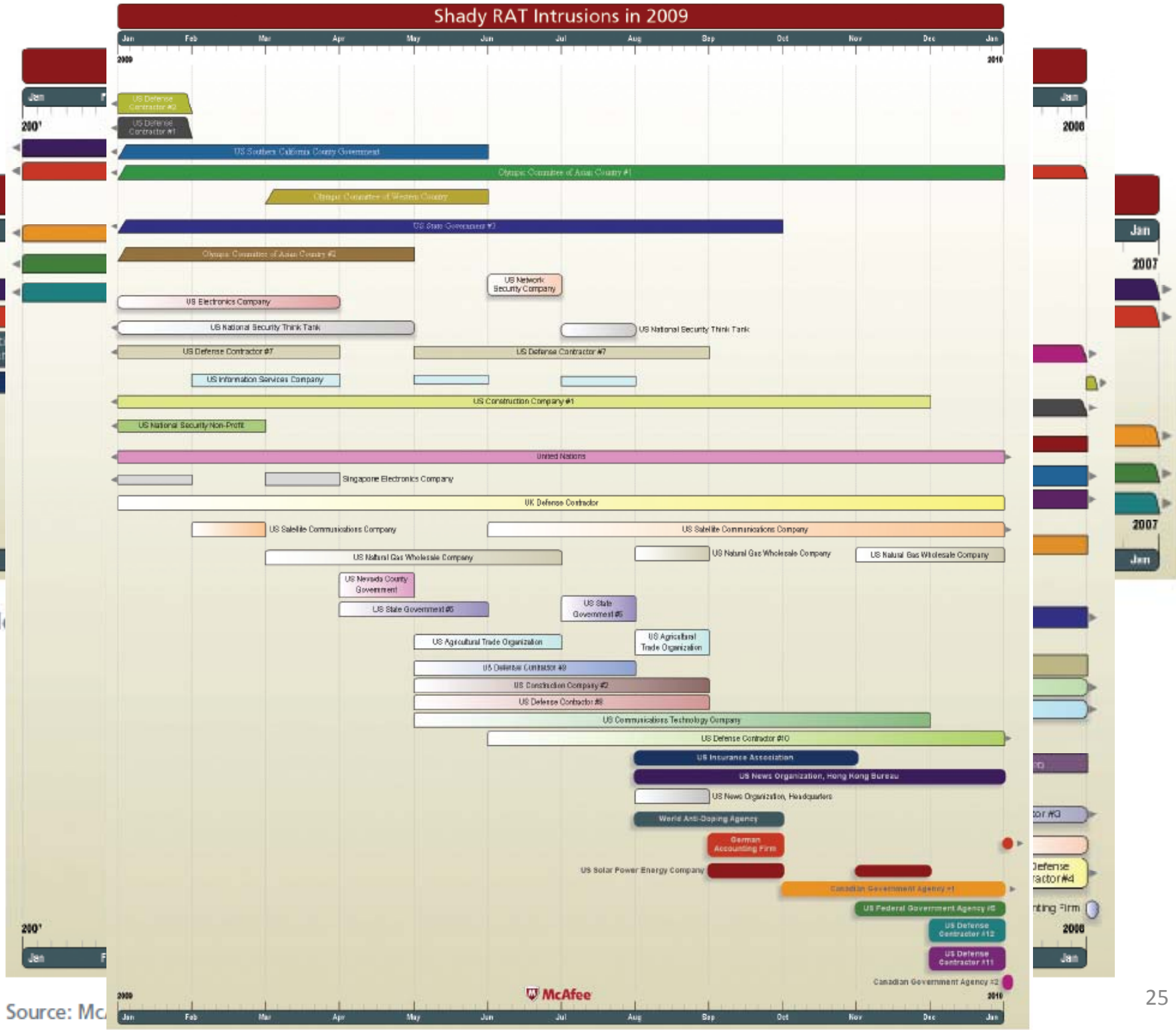
- Атакующие сначала компрометировали Web сервер с помощью SQL инъекции
- Создавали там страницу “drive by” exploit code, которая инфицировала посетителей
- И целенаправленно направляли на эту страницу целевых пользователей, используя email phishing
- Использовали те же фишинговые письма с вложениями в формате *.PDF и *.DOC открывая которые, через уязвимость устанавливался бэкдор



gh0st RAT соединялся к IP адресам DSL провайдера в Китае по доменным именам:

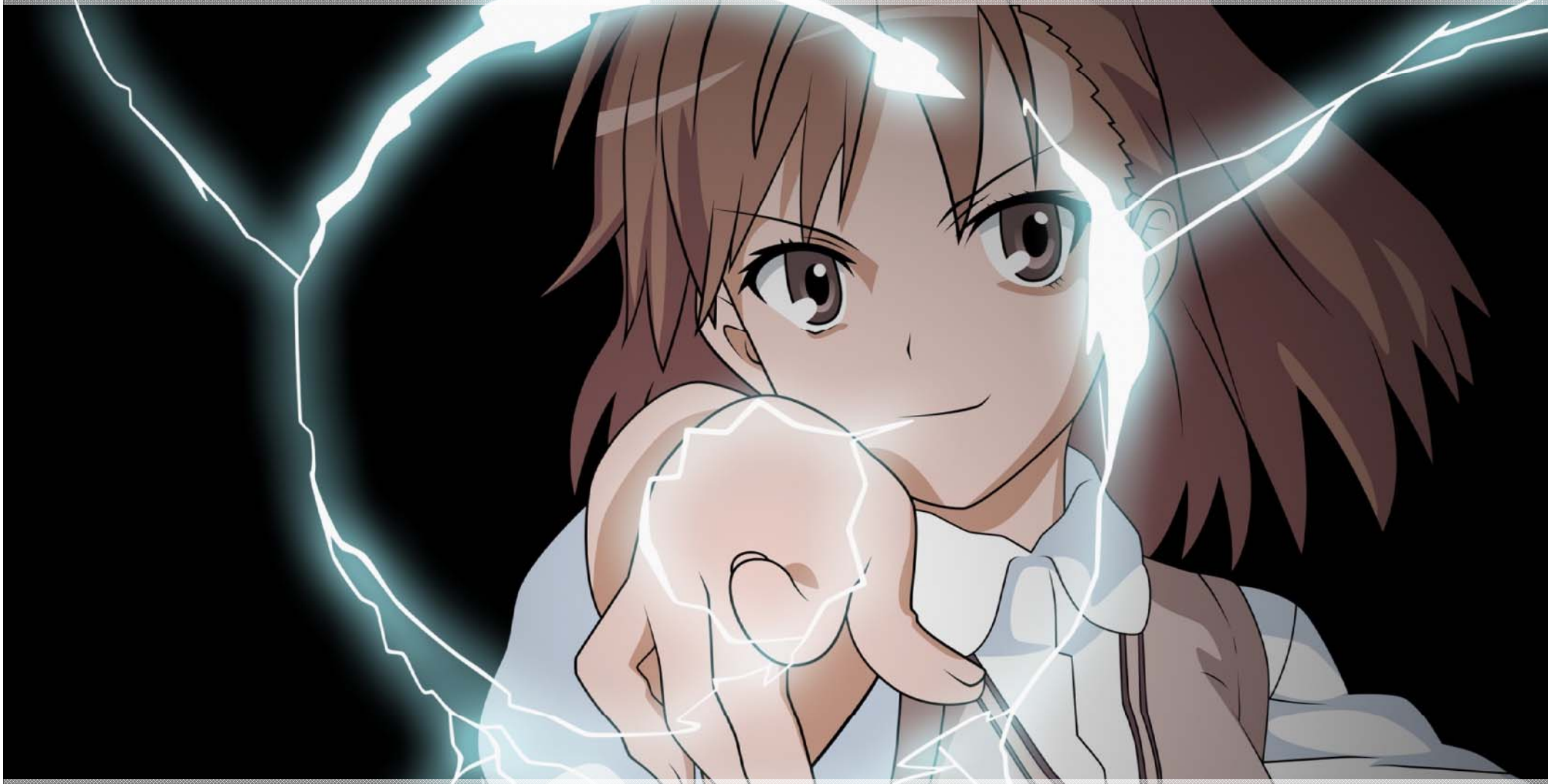
**.broad.hk.hi.dynamic.163data.com.cn*
**.broad.hk.hi.dynamic.163data.com.cn*
**.broad.hk.hi.dynamic.163data.com.cn*
**.broad.hk.hi.dynamic.163data.com.cn*
**.broad.hk.hi.dynamic.163data.com.cn*
**.broad.hk.hi.dynamic.163data.com.cn*





Source: McAfee

Operation Lurid



Enfal. To russia with love …

С августа 2010 года обнаружилась новая атака. Но теперь инфицированными оказались организации в России, Казахстане, Украине, Вьетнаме и других странах.

«At least 50 victim organizations ranging from government ministries and agencies, diplomatic missions, research institutions, and commercial entities have been hit in the former Soviet Union region and other countries.» (McAfee)

Атакующие развернули C&C инфраструктуру общим объемом в 15 доменов на 10 IP адресах.

1,465 unique hosts (host name + MAC address as stored by the C&C)
2,272 unique external IP addresses

The top 10 countries based on number of victims (2,272 IP addresses) were: Russia had 1,063 IP addresses hit in the attacks; Kazakhstan, 325; Ukraine, 102; Vietnam, 93; Uzbekistan; 88; Belarus, 67; India, 66; Kyrgyzstan, 49; Mongolia, 42; and China, 39.

Всего затронутых стран: 61

Как это не банально, но эта серия атак также использовала серию уязвимостей Adobe Reader *CVE-2009-4324* , *CVE-2010-2883*

CVE-ID

CVE-2010-2883
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Stack-based buffer overflow in CoolType.dll in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a PDF document with a long field in a Smart INdependent Glyphlets (SING) table in a TTF font, as exploited in the wild in September 2010. NOTE: some of these details are obtained from third party information.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:http://blog.metasploit.com/2010/09/return-of-unpublished-adobe.html
- MISC:http://community.websense.com/blogs/securitylabs/archive/2010/09/10/brief-analysis-on-adobe-reader-sing-table-parsing-vulnerability-cve-2010-2883.aspx
- CONFIRM:http://www.adobe.com/support/security/advisories/apsa10-02.html

National Cyber-Alert System

Vulnerability Summary for CVE-2009-4324

Original release date: 12/15/2009
Last revised: 08/21/2010
Source: US-CERT/NIST

Overview

Use-after-free vulnerability in the Doc.media.newPlayer method in Multimedia.api in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, allows remote attackers to execute arbitrary code via a crafted PDF file using ZLib compressed streams, as exploited in the wild in December 2009.

Impact

CVSS Severity (version 2.0):
CVSS v2 Base Score: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 8.6

CVSS Version 2 Metrics:
Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

CVSS Access Vector: Network exploitable

Как проводилась атака

- Опять же – письма по электронной почте.
- Письмо не содержало какого либо контента. Была указана тема письма и вложенный аттач.
- Subject: “Tibetan Losar Event on 6 March 2011”
- Attach: “LOSAR FLYER_edited-3.pdf”
- По данным McAfee – 2 версии Enfal.

“The email was sent using an email provider called Gawab (gawab.com) which is popular in the Middle East. The server used was info3.gawab.com (66.220.20.18) and the email address was emb107@gawab.com. The originating IP address was: 96.46.11.88 (INTERNETXTUSA). While this IP address is assigned to the US, it is used by a VPN provider in China”

Следует отметить основное отличие от других APT:

- Были развернуты индивидуальные компании атак.
- Под каждую – был заведен разный URL на C&C

Campaign	Count	Countries
strong	668	All 68 of the compromised counters were in Vietnam.
ejun0708	63	5 in Russia, 3 in Ukraine and 1 each in Czech Republic, Kazakhstan, Switzerland, Tajikistan and Belarus
ejun0614	42	27 in Russia, 3 in China, 3 in Kyrgyzstan, 2 in Tajikistan and 1 each in UK, US, S. Korea, Czech republic, Pakistan, Germany and Kazakhstan.
strongNewDns	34	All 34 of the compromised counters were in Vietnam.
ejun0509	32	31 in Russia, 1 in Ukraine
ejun0511	29	21 in Russia, 4 in Ukraine, 2 in Kazakhstan, and 1 each in Czech Republic and Azerbaijan
7-28	28	24 in Vietnam and one each in UAE, Cambodia ,Thailand and China
ejun0503	25	23 in Russia and 1 each in Ukraine and Czech Republic
0dayaug12.exe	22	20 in Belarus and 2 in Kazakhstan
C:\WINDOWS\ system32\desp.exe	22	12 in US, 5 in Russia, 3 in The Netherlands, and 1 each in Switzerland and the European Union.

- C&C Сервера теперь находились и в Соединенных Штатах и в Англии, но доменные имена зарегистрированы на Китай.

Country	Sector	Date	Camapign
France	GOV	Sat Jun 18 10:22:22 2011	0dayjun14.exe
Switzerland	GOV	Mon Jul 11 11:28:02 2011	LOGO076
UK	MEDIA	Thu Jun 16 08:18:44 2011	0dayapr13.exe
Germany	SPACE	Mon Jun 20 09:43:48 2011	6-7
Spain	SPACE	Mon Jul 4 11:38:35 2011	6-27
Russia	GOV	Tue Jun 7 12:15:34 2011	lh0603hy
Russia	GOV	Mon Jul 11 07:17:46 2011	ejun0708
Russia	GOV	Tue Jun 28 00:54:16 2011	110608
Russia	SPACE/GOV	Wed Jul 13 04:21:20 2011	aoo526pdf
Russia	SPACE	Wed Jul 13 07:14:38 2011	winupdate712
Russia	SPACE	Mon Jul 25 08:43:40 2011	6-7
Russia	SPACE	Wed Jul 13 02:45:59 2011	coo328xls
Russia	RESEARCH/GOV	Wed Jul 13 06:06:06 2011	aoo0516pdf
Russia	RESEARCH	Tue Jun 14 02:49:58 2011	winupdate

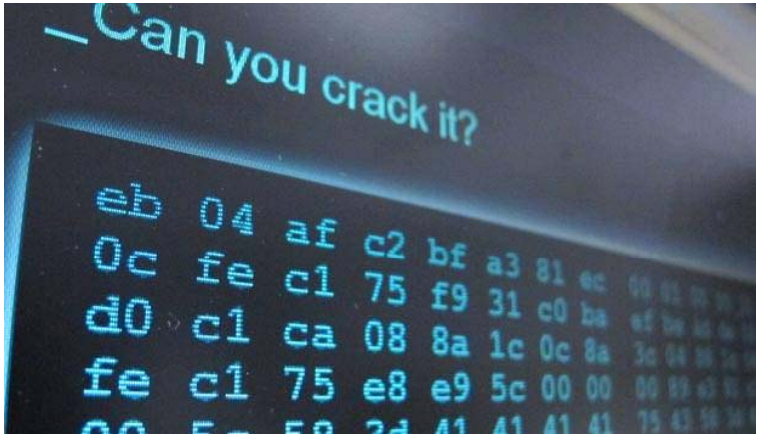
«After the initial connection, the malware makes two kinds of connections to the command and control server every 2 minutes. The fi rst connection is a KEEPALIVE connection to the URL path "/cgI-bin/Owpq4.cgi". The malware posts information to the command and control server that identifi es the compromised machine: OS and version, "campaign ID" and malware version. The second connection is an ASKCMD connection to a URL with the path "/trandocs/mm/<machine_name>:<MAC address>/Cmwhite". The contents of "Cmwhite" contain commands that are sent by the attackers to the compromised computer.»

Operation Night Dragon

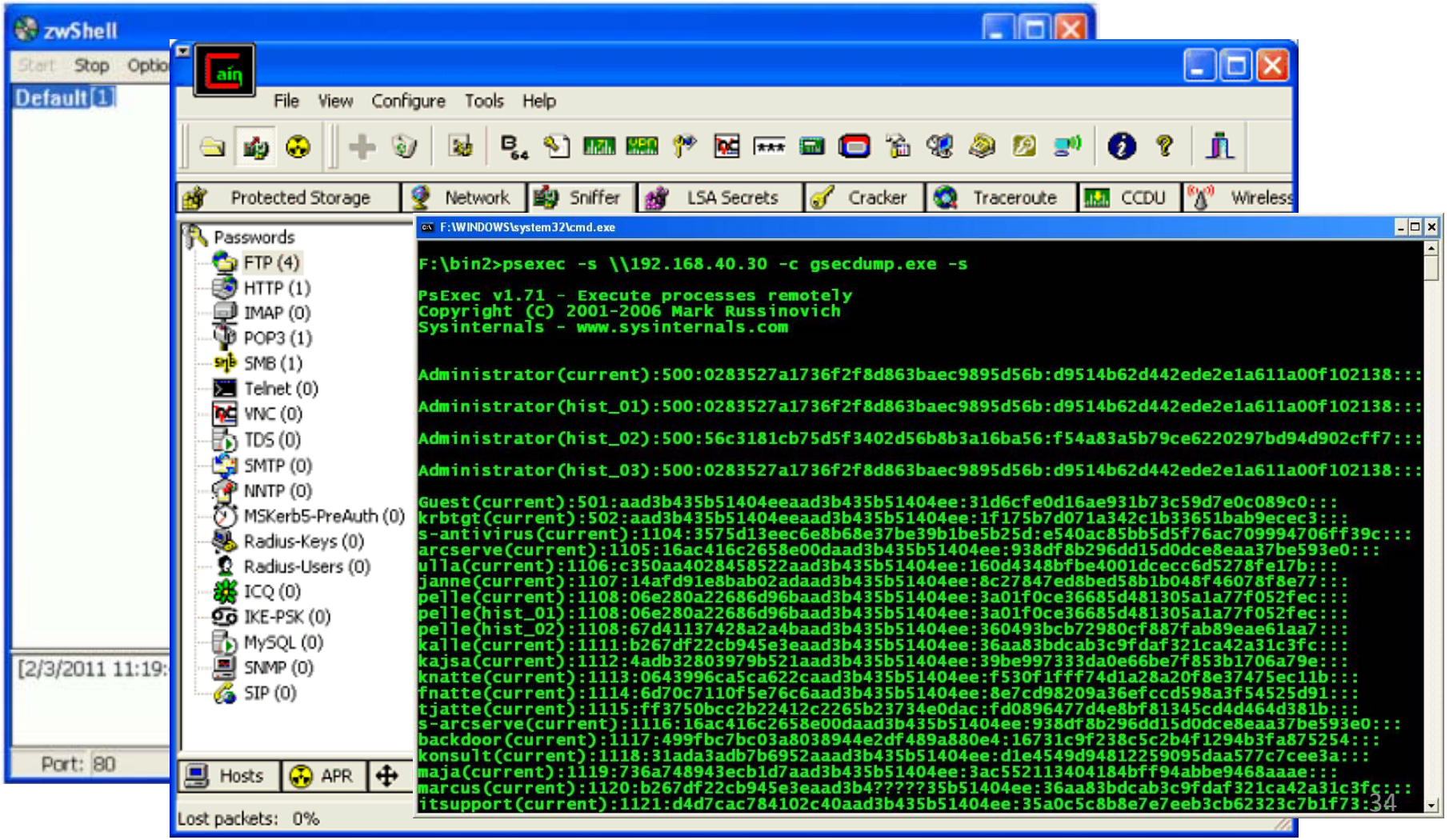
Истоки Night Dragon были замечены с ноября 2009 года

Night Dragon was another attack revealed by McAfee in early 2011 that targeted global oil, gas, and petrochemical companies. Again sourced from China and targeting sensitive industry specific intellectual property.

- *Company extranet web servers compromised through SQL-injection techniques, allowing remote command execution*
- *Commonly available hacker tools are uploaded on compromised web servers, allowing attackers to pivot into the company's intranet and giving them access to sensitive desktops and servers internally*
- *Using password cracking and pass-the-hash tools, attackers gain additional usernames and passwords, allowing them to obtain further authenticated access to sensitive internal desktops and servers*
- *Initially using the company's compromised web servers as command and control (C&C) servers, the attackers discovered that they needed only to disable Microsoft Internet Explorer (IE) proxy settings to allow direct communication from infected machines to the Internet*
- *Using the RAT malware, they proceeded to connect to other machines (targeting executives) and exfiltrating email archives and other sensitive documents*



- Атакующие использовали утилиту zwShell (написана на Delphi) для генерации уникального трояна
- Были использованы Cain & Abel и консольная утилита gsecdump для взлома дампов паролей



К чему может привести?

AT&T Data
discuss the

История

Компания была основана в
сигнализаций и устройств
Cable была образована *No*

В 1922 — начато производ
В 1953 — на базе трубок R
В 1966 — исследовательск
В 1976 — фирма сменила
В 2009 — с целью реструк
опубликованном заявлени
высокий запланированный

По итогам 1-го квартала 20
осенью 2009 года.[1]

В июне 2009 руководство

phone Company of Canada было выделе
ластинок (вместо обычных в то время в

Торонто.

Nortel Networks.

1 федерального закона США «О банкр
ение рынка на фоне мирового финансов

состояния защиты от кредиторов и верн

а компания будет ликвидирована.

ing to a

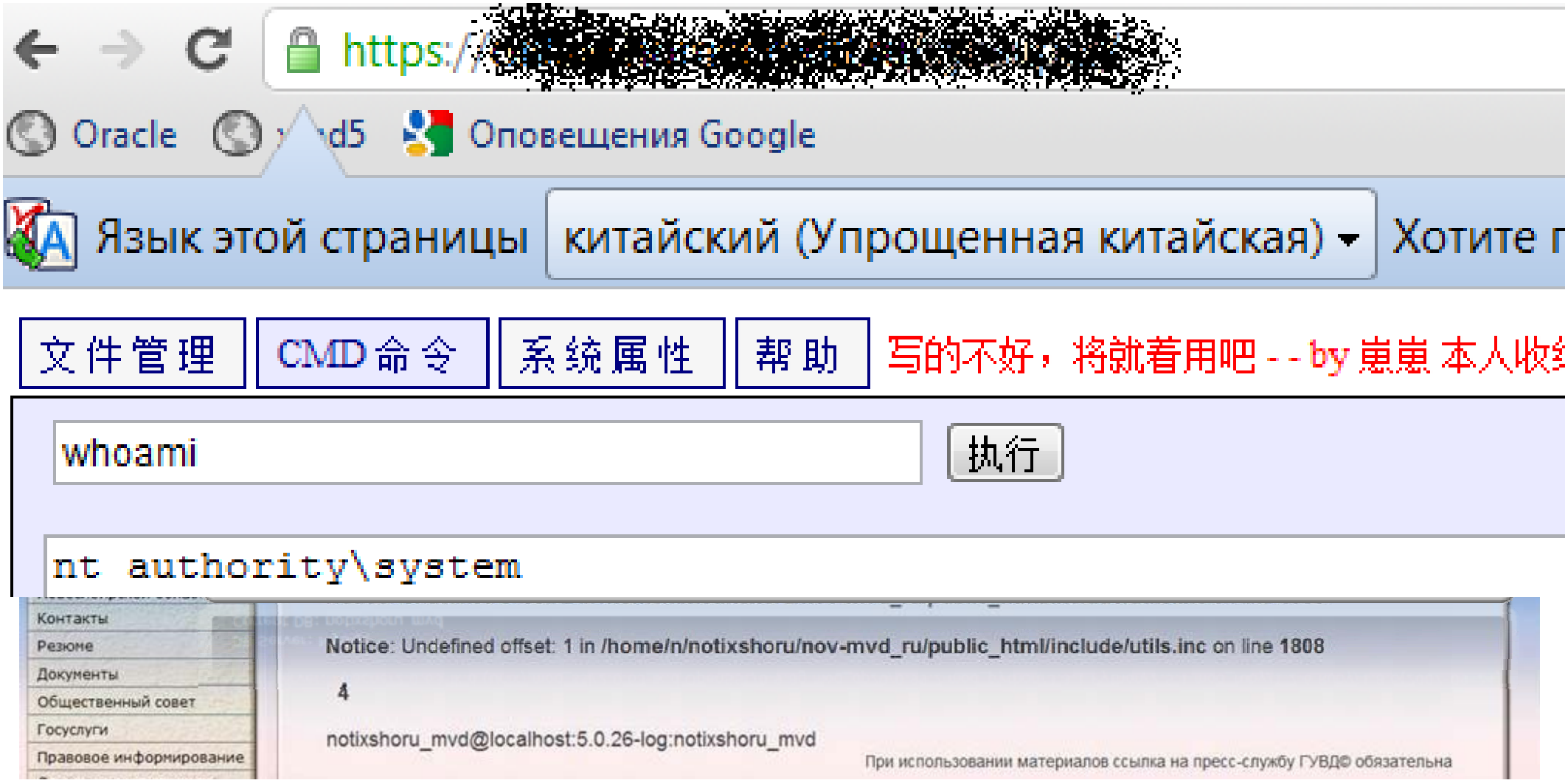
on of

2011 GCN Awards
Federal Budget
GCN Lab Reviews
Cloud/Virtualization

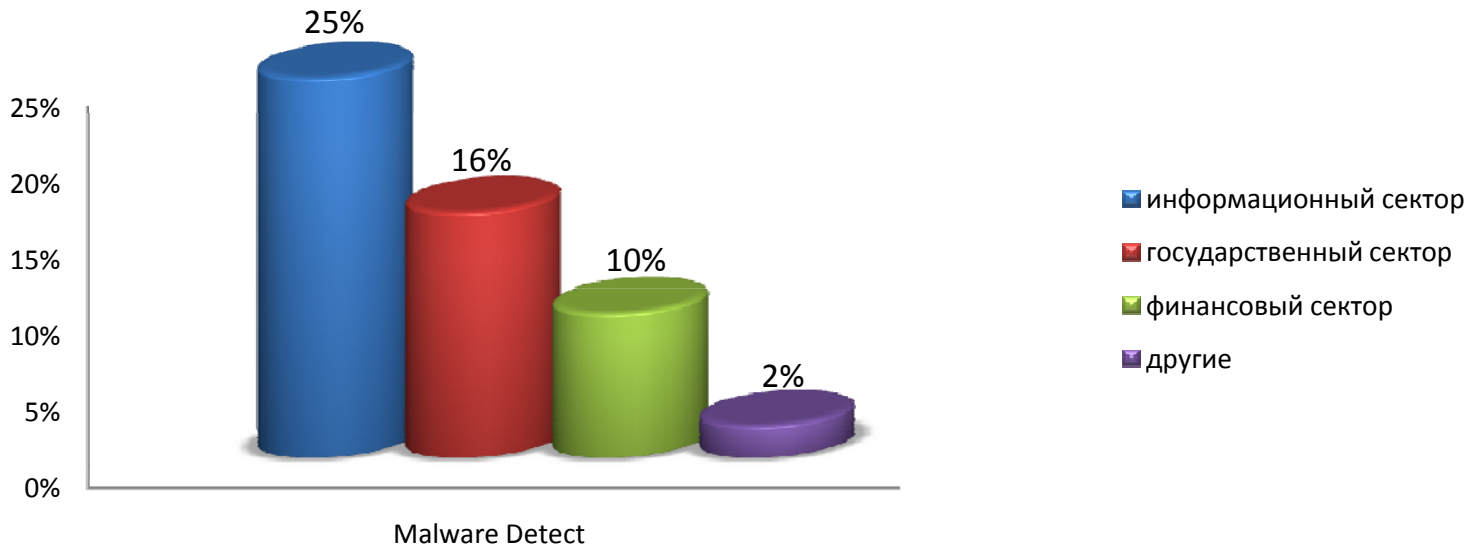
the hacking, told the WSJ that the company discovered the breach in 2004 but allowed the hacks to continue for years afterwards. Five years after the breach was discovered, in 2009, Shields found rootkits in laptops using an encrypted channel to send e-mail and other sensitive information to servers near Beijing.

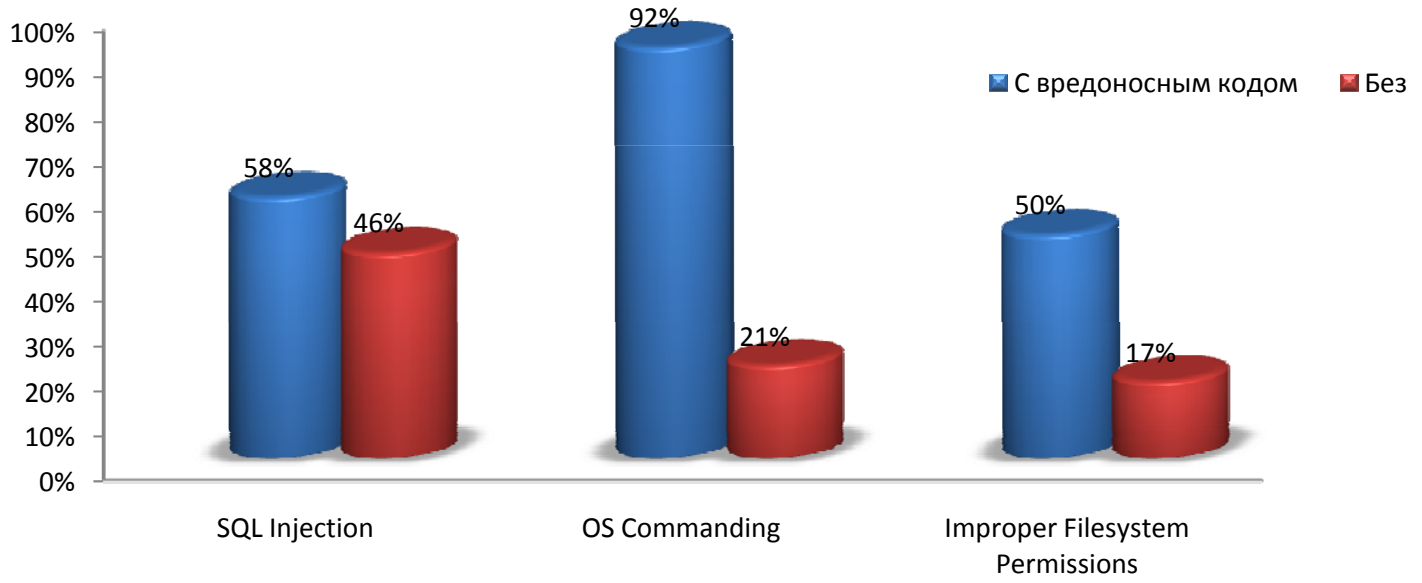
Другие примеры последствий?
(не совсем АРТ ☺)

«Шутки-шутками, но в каждой шутке есть море правды»



Суровая российская правда






but what
can I do?
但我能做些什麼
呢？

Что делать то?!

Prevent:

- *Процессная составляющая*
- *Техническая составляющая*
- *Организационная составляющая*

Post factum:

- Анализ трафика
- Антивирусная проверка
- Контроль целостности
- Контроль политик
- Выявить уязвимости
- Выявить слабые места в инфраструктуре
- Выявлять симптомы

Анализ трафика

- Например, в случае с Night Dragon, можно составить сигнатурку на IDS\IPS:

  plain text signature of “hW$.” (or “\x68\x57\x24\x13”) at the byte offset 0x42 within the TCP packet

- В случае с другими APT, равно как и для выявлений аномалий полезно заглянуть в fast flux и dyn dns запросы

No.	Time	Source	Destination	Protocol	Info
1	2011-05-07 06:19:04.913420	192.168.1.121	192.168.1.8	DNS	Standard query response A 192.118.40.97
2	2011-05-07 06:19:25.751097	192.168.1.121	192.168.1.8	DNS	Standard query response A 192.180.99.59
3	2011-05-07 06:19:46.841776	192.168.1.121	192.168.1.8	DNS	Standard query response A 192.106.178.136
4	2011-05-07 06:20:07.852046	192.168.1.121	192.168.1.8	DNS	Standard query response A 192.31.7.237
5	2011-05-07 06:20:28.880871	192.168.1.121	192.168.1.8	DNS	Standard query response A 192.232.239.160
6	2011-05-07 06:20:49.743262	192.168.1.121	192.168.1.8	DNS	Standard query response A 192.114.123.242
7	2011-05-07 06:21:10.860840	192.168.1.121	192.168.1.8	DNS	Standard query response A 192.151.178.111
8	2011-05-07 06:21:31.846147	192.168.1.121	192.168.1.8	DNS	Standard query response A 192.161.62.145
9	2011-05-07 06:21:52.855336	192.168.1.121	192.168.1.8	DNS	Standard query response A 192.10.144.119

- Не надейтесь на удачу! Проверьте наличие сигнатур или добавьте сами!

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ET TROJAN Aurora C&C Checkin"; flow:established,to_server; content:"|ff ff ff ff ff ff 00 00 fe ff ff ff ff ff ff ff ff 88 ff|"; offset:0; depth:20; classtype:trojan-activity; reference:url, www.avertlabs.com/research/blog/index.php/2010/01/18/an-insight-into-the-aurora-communication-protocol/; sid:10000000001; rev:1;)
```

- Не надейтесь на удачу! Проверьте наличие сигнатур или добавьте сами!

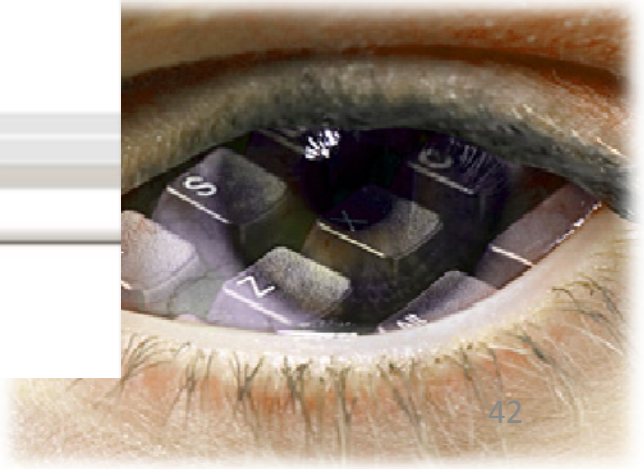
```
Transmission Control Protocol, Src Port: http (80), Dst Port: remote-as (1053), Seq: 1, Ack: 17, Len: 16
    Source port: http (80)
    Destination port: remote-as (1053)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 17    (relative sequence number)]
    Acknowledgement number: 17    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size: 64224
  ⊞ Checksum: 0x0bba [validation disabled]
  ⊞ [SEQ/ACK analysis]
Hypertext Transfer Protocol
  ⊟ Data (16 bytes)
      Data: 01600111000000190000000068572413
      [Length: 16]

0000  00 0c 29 1d 8f f6 00 0c  29 86 d1 e7 08 00 45 00   ..)..... ).....E.
0010  00 38 8e d7 40 00 80 06  8d 7b ac 10 c3 25 ac 10   .8..@... .{...%..
0020  c3 26 00 50 04 1d aa 3d  cf 5e 7e d0 3e e6 50 18   .&.P...= .^~.>.P.
0030  fa e0 0b ba 00 00 01 60  01 11 00 00 00 19 00 00   .......` ........
0040  00 00 68 57 24 13                                 ..hW$.
```

- Если еще не контролируете чувствительную информацию – пора начать

```
Transmission Control Protocol, Src Port: http (80), Dst Port: remote-as (1053), Seq: 17, Ack: 17, Len: 17
    Source port: http (80)
    Destination port: remote-as (1053)
    [Stream index: 0]
    Sequence number: 17    (relative sequence number)
    [Next sequence number: 34    (relative sequence number)]
    Acknowledgement number: 17    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size: 64224
  ⊞ Checksum: 0xb3a7 [validation disabled]
  ⊞ [SEQ/ACK analysis]
Hypertext Transfer Protocol
  ⊟ Data (17 bytes)
      Data: 078C00000061646D696E002D0000110000
      [Length: 17]

0000  00 0c 29 1d 8f f6 00 0c  29 86 d1 e7 08 00 45 00   ..)..... )....E.
0010  00 39 8e d8 40 00 80 06  8d 79 ac 10 c3 25 ac 10   .9..@... .y...%..
0020  c3 26 00 50 04 1d aa 3d  cf 6e 7e d0 3e e6 50 18   .&.P...= .n~.>.P.
0030  fa e0 b3 a7 00 00 07 8c  00 00 00 61 64 6d 69 6e   ........ ...admin
0040  00 2d 00 00 11 00 00                              .-.....
```



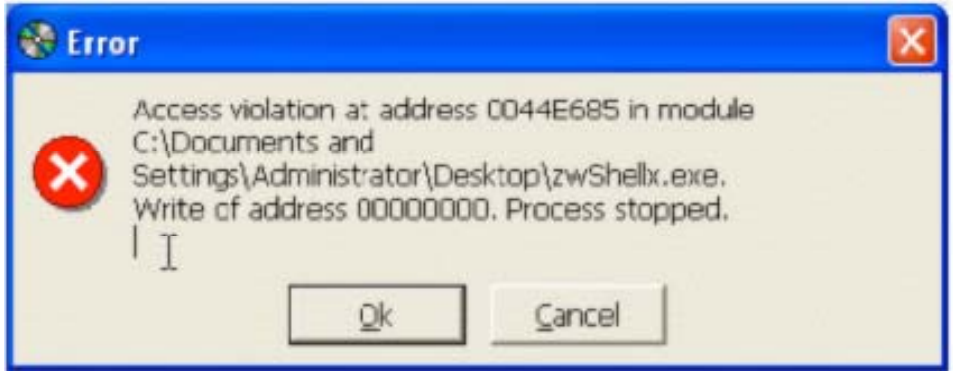
- Не забывайте о сопутствующих дырах! (по моей проверке через простейший запрос через google - Lizamoon еще очень живет ;)

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"SPECIFIC-THREATS lizamoon script injection"; flow:established,to_client; content:"script src=http|3A 2F 2F|"; nocase; content:"|2F|ur.php"; within:50; fast_pattern; nocase; reference:url,isc.sans.edu/diary.html?storyid=10642; classtype:misc-activity; sid:18604; rev:1;)
```

- Проверьте наличие основных ключей в реестре, проверьте файловые системы!

PI-RAT is installed on a Windows system, it creates the following file and registry keys:
- C:\Documents and Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk\rasphone.pbk
- HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\Location Awareness
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\Location Awareness

- Проведите сканирование уязвимостей
- Обратите внимание на хиты в логах прокси
- Отключите доступ к Интернету для ваших серверов по ip\mac адресам
- Не забывайте о мобильных пользователях
- Ограничьте HTTP POST size
- Ограничьте использование неконтролируемых выходов из интрасети (отключение прокси в настройках, проброс портов)
- Не все «операторы и креаторы APT » - гении




Prevention

Предотвращение

1) Процессная составляющая:

- Patch management
- Vulnerability management
- Policy management
- Configuration management

2) Техническая составляющая:

- Сканеры уязвимостей
- IDS\IPS
- Honeypots
- Создайте «ловушки»
- Контроль антивирусной защиты
- SIEM
- Двухфакторная аутентификация
- DLP\IRM

3) Организационная составляющая:

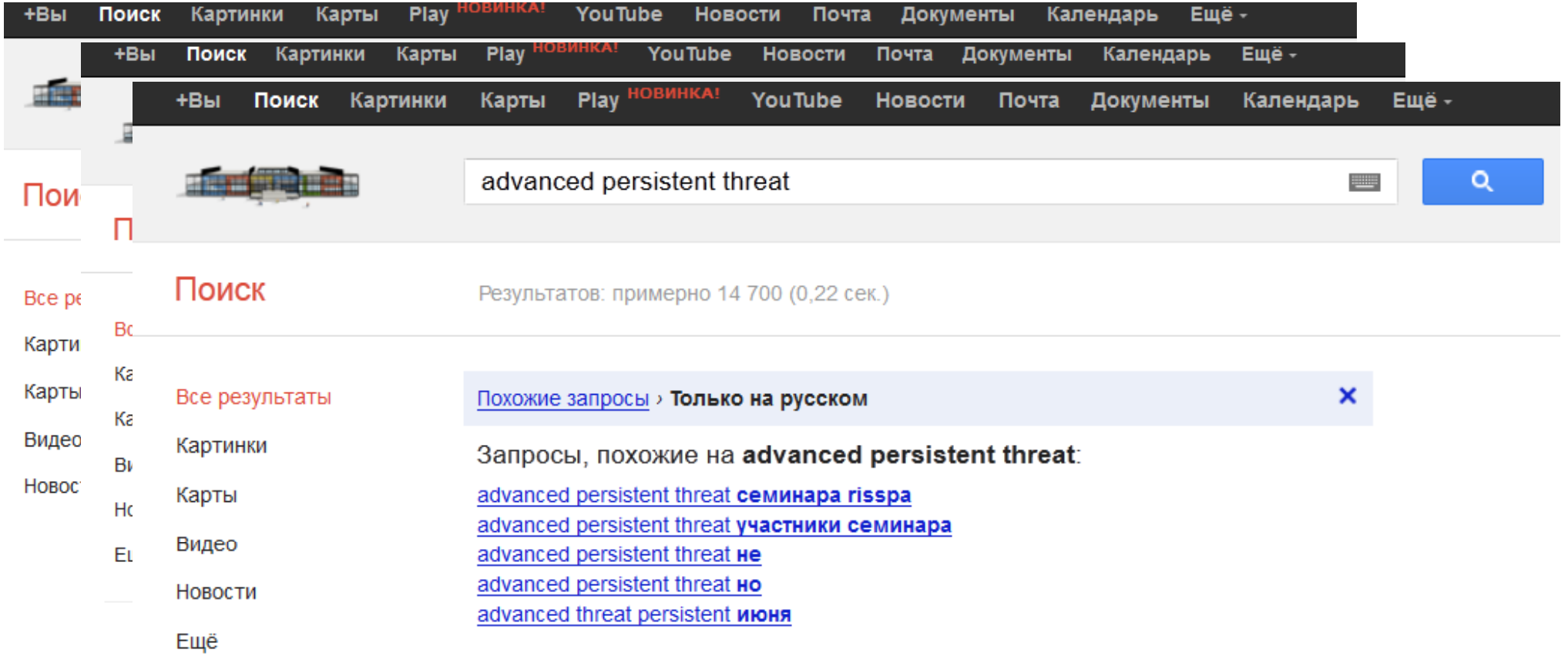
- Внешнее и внутреннее сканирование, тесты на проникновение
- Обучение персонала
- Инцидент-менеджмент
- Реагируйте на угрозы. Будьте на чеку.

Спасибо за внимание

POSITIVE TECHNOLOGIES

Is not interested this…

ога … ☺



Почему China?

- 41% пользователей Интернета находится в Азии
- В China более 500 миллионов пользователей Интернета
- Большинство пользователей находится он-лайн 24 часа в сутки
- .....

— 17.01.2012 01:07 —

Число пользователей интернета в Китае превысило полмиллиарда человек, больше двух миллионов сайтов

Число пользователей интернета в Китае на конец декабря 2011 года перешагнуло за 500 млн и достигло 513 млн человек, отмечается в сводке, опубликованной Китайским информационным центром интернета (КИЦИ), чьи данные приводит **«Синьхуа»**.

Согласно сводке КИЦИ, число пользователей за 2011 год увеличилось на 55,8 млн человек. На конец декабря уровень охвата интернетом населения Китая вырос на четыре процентных пункта по сравнению с концом 2010 года и достиг 38,3%. Количество пользователей мобильного интернета составило 356 млн человек с приростом на 17,5%.

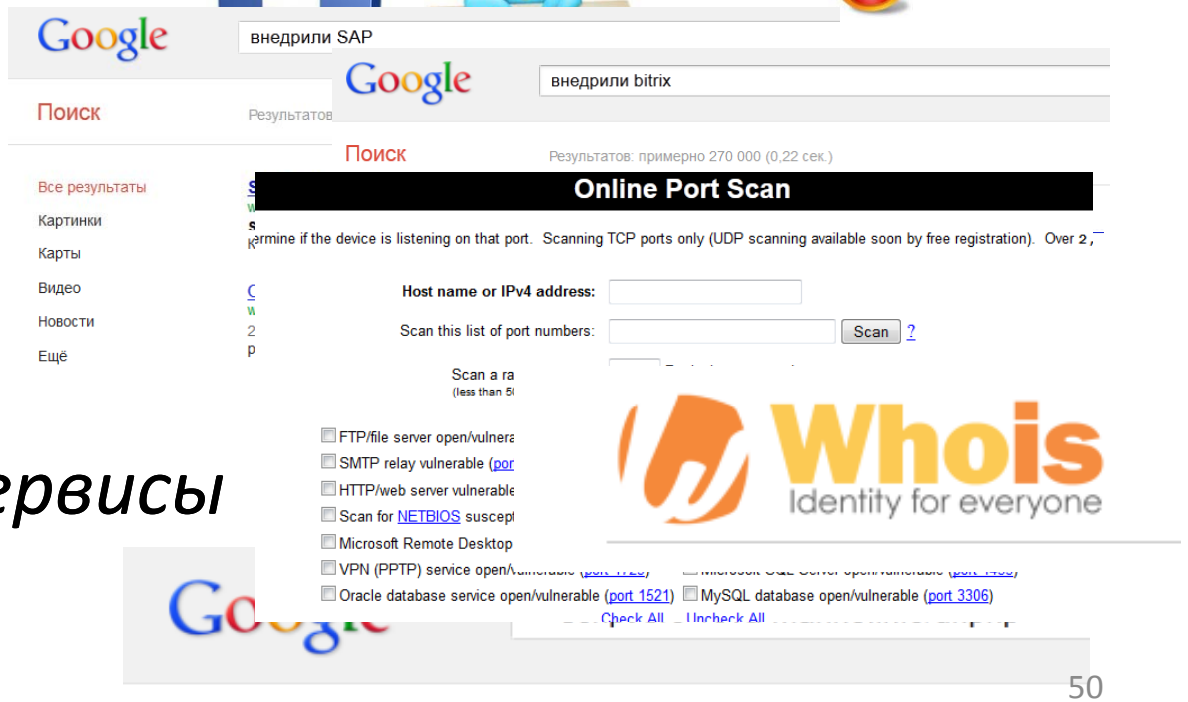
При этом на конец 2011 года в Китае насчитывалось 2,296 млн веб-сайтов, что на 20% больше, чем в конце 2010 года.

▪ «Газета.Ru»

Структура атаки

1 Этап. Сбор данных о жертве

- *Сканирования*
- *Социальные сети*
- *Поисковик*
- *Служебные сервисы*



Структура атаки

2 Этап. Вторжение

- *Социалка*
- *malware*
- *Vulnerabilities*
- *0-day exploits*

Структура атаки

3 Этап. Закрепление влияния

- *SCM*
- *MS AD*
- *Proxy*
- *Source code*
- *«тот незаметный сервер в углу»*
- *филиал\клиент\субподрядчик*

Структура атаки

4 Этап. Сохранение влияния

- *Удаление логов*
- *Использование нового кода*
- *Подстраивание под СЗИ*
- *Опережение ваших действий*