
October, 2018
Who Am I

- Oleg Bondarenko;
- Senior Manager in FireEye;
- (Можу надавати сю рі дані😊 )
- Co-organizer of UISGCONs;
Motivation

▶ APT/Espionage;
▶ eCrime;
▶ Information Operations/Hacktivism;
▶ ICS/SCADA;
eCrime Trends in EMEA in 2018

▶ Threat actors within underground;
▶ Based on Detection;
eCrime Trends in EMEA. Look from Underground.

RU-speaking underground:

- **Ransomware:**
  - GandCrab;
- **Access to infrastructure/Databases for sale:**
  - Fxsmp
- **EK world**
  - Fallout EK;
- **Something from me**
  - Nigerian?
eCrime Trends in EMEA. Look from Underground. GandCrab
eCrime Trends in EMEA. Look from Underground. GandCrab

BUY GANDCRAB Decryptor

What do you need?
You need GandCrab Decryptor.
This software will decrypt all your encrypted files and will delete GandCrab from your PC.
For purchase you need crypto-currency DASH (1 DASH = 765.016 $).
How to buy this currency you can read it here.

How much money you need to pay? Below we are specified amount and our wallet for payment.

Price:
1.5 DASH (1200 USD)

DASH address for payment:
XeCueUcBQ2venzAjvtXwgVM6vEouZGq97N

To make a payment, you have this time:

02 DAYS
02 HOURS
49 MINUTES
03 SECONDS

After this time the amount will double and will be:
3 DASH (2400 USD)
eCrime Trends in EMEA. Look from Underground. GandCrab

- v.5 released in September:
  - integration of Mimikatz;
  - Active Directory brute-force automation;
  - PowerShell builder;
  - CVE-2018-8120 for Windows 7 and Windows Server 2008/2012 (LPE);
  - ALPC-TaskSched-LPE;
eCrime Trends in EMEA. Look from Underground. GandCrab

- Collaboration:
  - Fallout EK;
  - "NTCrypt" crypter service;
eCrime Trends in EMEA. Look from Underground. Fallout EK

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Host</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td><a href="http://www.*.com">www.*.com</a></td>
<td>/ax/?uid=493544&amp;ad=4</td>
</tr>
<tr>
<td>HTTP</td>
<td><em>.</em>.com</td>
<td>/afu.php?zoneid=1809745</td>
</tr>
<tr>
<td>HTTP</td>
<td><em>.</em>.com</td>
<td>/afu.php?zoneid=1809745</td>
</tr>
<tr>
<td>HTTP</td>
<td><em>.</em>.com</td>
<td>/?r=%2Fmb%2Fhan&amp;zoneid=1809745&amp;pbk3=5545538e1460e2a050388e85a8b793a65955</td>
</tr>
<tr>
<td>HTTP</td>
<td>46.101.205.251</td>
<td>/wt/ww.php</td>
</tr>
<tr>
<td>HTTP</td>
<td>hulk.cf</td>
<td>/v3</td>
</tr>
<tr>
<td>HTTP</td>
<td>naosecgomosec.gq</td>
<td>/mQvZT/ucIVQnZ/ooRLO.jsp?Ringnecks=praedial-swindles&amp;R7ryt6=Ceramics-aureity&amp;j2KS=</td>
</tr>
</tbody>
</table>

Figure 1: Malvertisement redirection to Fallout exploit kit landing page
Figure 2: Content within first ad page
eCrime Trends in EMEA. Look from Underground. Fallout EK

Figure 3: 302 redirect to exploit kit-controlled cushion servers
eCrime Trends in EMEA. Look from Underground. Fallout EK

GET/wt/wv.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 46.101.205.251
Connection: Keep-Alive

HTTP/1.1 302 Found
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 30 Aug 2018 18:45:15 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Location: http://huli.cf/v3

Figure 4: Another redirection before exploit kit landing page
eCrime Trends in EMEA. Look from Underground. Fallout EK

Figure 5: Last redirect before user reaches exploit kit landing page
eCrime Trends in EMEA. Look from Underground. Fallout EK
## eCrime Trends in EMEA. Look from Underground. Fallout EK

<table>
<thead>
<tr>
<th>Period</th>
<th>Hits</th>
<th>Loads</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>All time</td>
<td>37828</td>
<td>14863</td>
<td>39.28%</td>
</tr>
<tr>
<td>1 minute</td>
<td>18</td>
<td>6</td>
<td>33.33%</td>
</tr>
<tr>
<td>10 minutes</td>
<td>228</td>
<td>101</td>
<td>44.3%</td>
</tr>
<tr>
<td>30 minutes</td>
<td>735</td>
<td>324</td>
<td>44.08%</td>
</tr>
<tr>
<td>1 hour</td>
<td>1579</td>
<td>673</td>
<td>42.62%</td>
</tr>
<tr>
<td>12 hours</td>
<td>17930</td>
<td>7948</td>
<td>44.33%</td>
</tr>
</tbody>
</table>
Access for sale. Fxmsp.

- What can you do with this data:
  - Simply find out about being compromised;
  - Investigate threat actor/-s TTPs;
  - Find out if your OSP has been compromised to pivot into client networks;
Где, помогите!

O:
To:
On: Friday, 12 October 2018 at 07:27

Я надеюсь, что он достигнет вас вовремя. Я совершил поездку в Николаев, Украина, и моя сумка была украдена, в моей сумке были все важные предметы, такие как телефоны, деньги и мой паспорт. Посольство хочет помочь мне, позволив мне летать без паспорта. Все, что мне нужно сделать, это купить билет на самолет и оплатить мои счета в отеле. К сожалению, у меня нет доступа к моим учетным записям без моей кредитной карты. Я связался с моим банком, но им нужно время, прежде чем они могут дать мне новую кредитную карту, поэтому я хотел попросить вас быстро одолжить мне деньги, которые я вернусь к вам как можно скорее, когда вернусь, я необходимо 2860 евро. Западный союз - это самый быстрый способ перевести деньги мне.

Дайте мне знать, если это возможно.

Я с нетерпением жду вашего ответа.

С уважением,
### eCrime Trends in EMEA in 2018

<table>
<thead>
<tr>
<th></th>
<th>Europe</th>
<th>World</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Pony</td>
<td>Lokibot</td>
<td>Lokibot is credentials stealer</td>
</tr>
<tr>
<td>2</td>
<td>Emotet</td>
<td>Emotet</td>
<td>Emotet is modular credential theft Trojan</td>
</tr>
<tr>
<td>3</td>
<td>Lokibot</td>
<td>Pony</td>
<td>Pony is credentials stealer</td>
</tr>
<tr>
<td>4</td>
<td>Formbook</td>
<td>Chanitor</td>
<td>FormBook is a data stealer/form grabber - keylogger</td>
</tr>
<tr>
<td>5</td>
<td>Chanitor</td>
<td>Formbook</td>
<td>Chanitor is a downloader malware that has been observed loading Pony, Send-Safe spambot, Vawtrak, or Nymaim malware</td>
</tr>
<tr>
<td>6</td>
<td>NanoCore</td>
<td>Ursnif</td>
<td>NanoCore is a publicly available RAT available for purchase</td>
</tr>
<tr>
<td>7</td>
<td>Zeus</td>
<td>NanoCore</td>
<td>Zeus is a banking Trojans</td>
</tr>
<tr>
<td>8</td>
<td>Adwind</td>
<td>Remcos</td>
<td>Adwind is a Java-based, cross-platform RAT</td>
</tr>
<tr>
<td>9</td>
<td>Ursnif</td>
<td>Zeus</td>
<td>Ursnif (aka Gozi and, now, Gozi-ISFB) is a modified modular banking malware with backdoor capabilities</td>
</tr>
<tr>
<td>10</td>
<td>Remcos</td>
<td>Hawkeye</td>
<td>HawkEye is a commercial crimeware tool provider that offers a variety of products, including a keylogger, malware encrypting tool, and a brute-forcing tool</td>
</tr>
</tbody>
</table>

Remcos is a configurable RAT program written in the C++ language that has a large number of implemented features, including: file management, screen capture, access to clipboard data, command shell, arbitrary file access, mouse control, and more.
eCrime in EMEA. Pony

- The Pony tool is a generic platform for downloading and launching arbitrary files on victims' systems, typically used to install additional malware packages. It also collects login credentials from software on the host, including File Transfer Protocol (FTP) user names and passwords.
eCrime in EMEA. FormBook.

- FormBook is a data stealer/form grabber that has been advertised on HackForums by its developer "Ng. Coder" since early 2016. The malware injects itself into various processes and installs function hooks to log keystrokes, steal clipboard contents, and extract data from HTTP sessions.
eCrime in EMEA. FormBook.

- Coded in C and Assembly;
- Lagos Island method;
- Persistence;
- Exe as a service;
- Ng.Coder
eCrime in EMEA. FormBook.

- Works on Windows
  XP/Vista/7/8/8.1/10 (all x86/x64)
  Windows Server 2003/R2, 2008/R2, 2012/R2 (all x86/x64)
- Bin size ~130kb (Uncompressed/raw balloon), ~85kb (compressed)
- Intuitive PHP Panel
- Bugfix, Updates and Support is free.

**PRICING**

- **$29 / Week**
  Full Package/Hosted
- **$59 / Month**
  Full Package/Hosted
- **$99 / 3 Month**
  Full Package/Hosted
- **$299 - Pro**
  Bin for your domain

**PAYMENT METHOD**

- Bitcoin
- Perfect Money
eCrime in EMEA. FormBook.
eCrime in EMEA. Emotet.

- Emotet is a modular credential theft Trojan that primarily collects usernames and passwords for accounts at financial institutions. The malware downloads and executes various modules from hard-coded C&C servers. The modules are not written to disk but loaded directly from memory and include web browser and email client credential harvesters, an email scraper for Microsoft Outlook, and a spam engine.
eCrime in EMEA. Emotet.

▶ collects usernames and passwords for accounts at financial institutions;
▶ downloads and executes various modules from hard-coded C2s;
▶ loaded directly from memory;
▶ include Web browser and email client credential harvesters, an email scraper for Microsoft Outlook, and a spam engine;
▶ Secondary Payloads in 2018 - Trickbot, IcedID, and ZeusPanda;
eCrime in EMEA. LokiBot.

- LokiBot is a .NET launcher that executes an embedded credential stealer. It can download and then drop, load, or execute other binaries to the system. It is also designed to steal private data from infected machines, and then submit that information to a C&C host via HTTP POST.
eCrime in EMEA. LokiBot.
eCrime in EMEA. LokiBot.
## eCrime Trends in EMEA in 2018

<table>
<thead>
<tr>
<th></th>
<th>Europe</th>
<th>World</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Pony</td>
<td>Lokibot</td>
</tr>
<tr>
<td>2</td>
<td>Emotet</td>
<td>Emotet</td>
</tr>
<tr>
<td>3</td>
<td>Lokibot</td>
<td>Pony</td>
</tr>
<tr>
<td>4</td>
<td>Formbook</td>
<td>Chanitor</td>
</tr>
<tr>
<td>5</td>
<td>Chanitor</td>
<td>Formbook</td>
</tr>
<tr>
<td>6</td>
<td>NanoCore</td>
<td>Ursnif</td>
</tr>
<tr>
<td>7</td>
<td>Zeus</td>
<td>Nanocore</td>
</tr>
<tr>
<td>8</td>
<td>Adwind</td>
<td>Remcos</td>
</tr>
<tr>
<td>9</td>
<td>Ursnif</td>
<td>Zeus</td>
</tr>
<tr>
<td>10</td>
<td>Remcos</td>
<td>Hawkeye</td>
</tr>
</tbody>
</table>

Remcos is a configurable RAT program written in the C++ language that has a large number of implemented features, including: file management, screen capture, access to clipboard data, command shell, arbitrary file access, mouse control, and more.
Information Operations and Hacktivism in Europe.

- HK vs. IO;
- Influence Operations via youtube;
- Elections manipulation;
- Fake HK personas are very common here;
Influence Campaign on Youtube.

- YouTube accounts generating U.S., UK, and European politically themed commentary;
- Comments for videos by BBC, RT, RT UK, euronews, the Daily Mail, France 24 English, and Sky News;
- Classic narrative pushing, such as:
  - Defense of Russia, praise of Putin, and accusations of UK;
  - Support for President Trump;
  - Criticism of the EU and European heads of state (DE, FR, EU Commission);
Hacktivism and Information Operations. Fake personas

Fake personas:

- Anonymous Poland/@anpoland (high confidence in nation-state sponsorship);
- Fancy Bears’ Hack Team (high confidence nation-state sponsorship);
- Pravyy Sector/@pravsector (high confidence in nation-state sponsorship);
Information Operations with fake-HK personas

США берут под свой контроль все биологические лаборатории Украины

США в настоящее время устанавливают полный контроль над биологическими объектами, исследованиями и депозитариями смертельно опасных вирусов в Украине.

В дальнейшем это позволит Соединенным Штатам контролировать эпидемиологическую ситуацию в регионе, иметь доступ ко всем разработкам в этой сфере, манипулировать численностью населения и обеспечивать прибыль американским фармакологическим корпорациям.
Information Operations with fake-HK personas
Thank you!