

MUST READ TrueCrypt is safer than previous examinations suggest

Kaspersky gives a close look to the Russian underground

November 23, 2015 By [Pierluigi Paganini](#)



According to Kaspersky Lab, bad actors in the Russian underground have stolen more than \$790 Million over 3 years, from 2012 to 2015.

According to the experts at Kaspersky Lab, Russian criminal rings have stole roughly \$790 Million over 3 years (from 2012 to 2015), more than \$500 million of that is from victims located outside the Russian.

The cyber gangs targeted individuals, businesses, and financial institutions across the world, a new report from Moscow-based Kaspersky Lab shows.

The experts at Kaspersky estimated the losses by analyzing the information gathered from over 160 arrests of Russian-language speaking cybercriminals as well as data gathered during their investigation. Unfortunately, this data could represent only the tip of the iceberg, in many cases attacks are undetected and it is not easy to provide an estimation of the losses.

"With online financial transactions becoming more common, the organizations supporting such operations are becoming more attractive to cybercriminals. Over the last few years, cybercriminals have been increasingly attacking not just the customers of banks and online stores, but the enabling banks and payments systems directly. The story of the [Carbanak cybergroup](#) which specializes in attacking banks and was exposed earlier this year by Kaspersky Lab is a clear confirmation of this trend." reads the [Kaspersky's report](#).

The experts noticed that the [Russian underground](#) has become even more crowded and despite the numerous arrests made by law enforcement a growing number of bad actors is finding cybercrime an attractive and profitable business.

More than 1,000 individuals have been recruited by the Russian cyber criminal rings over the last three years, most of them involved in the development of malware and set up of control infrastructure.

The researchers at Kaspersky have identified at least five cyber gangs focused specifically on financial crimes. We are facing with organized structures composed of 10 to 40 people which are operating for at least two years.

Pl
it

"At least two of them are actively attacking targets not only in Russia but also in the USA, the UK, Australia, France, Italy and Germany." continues the report.

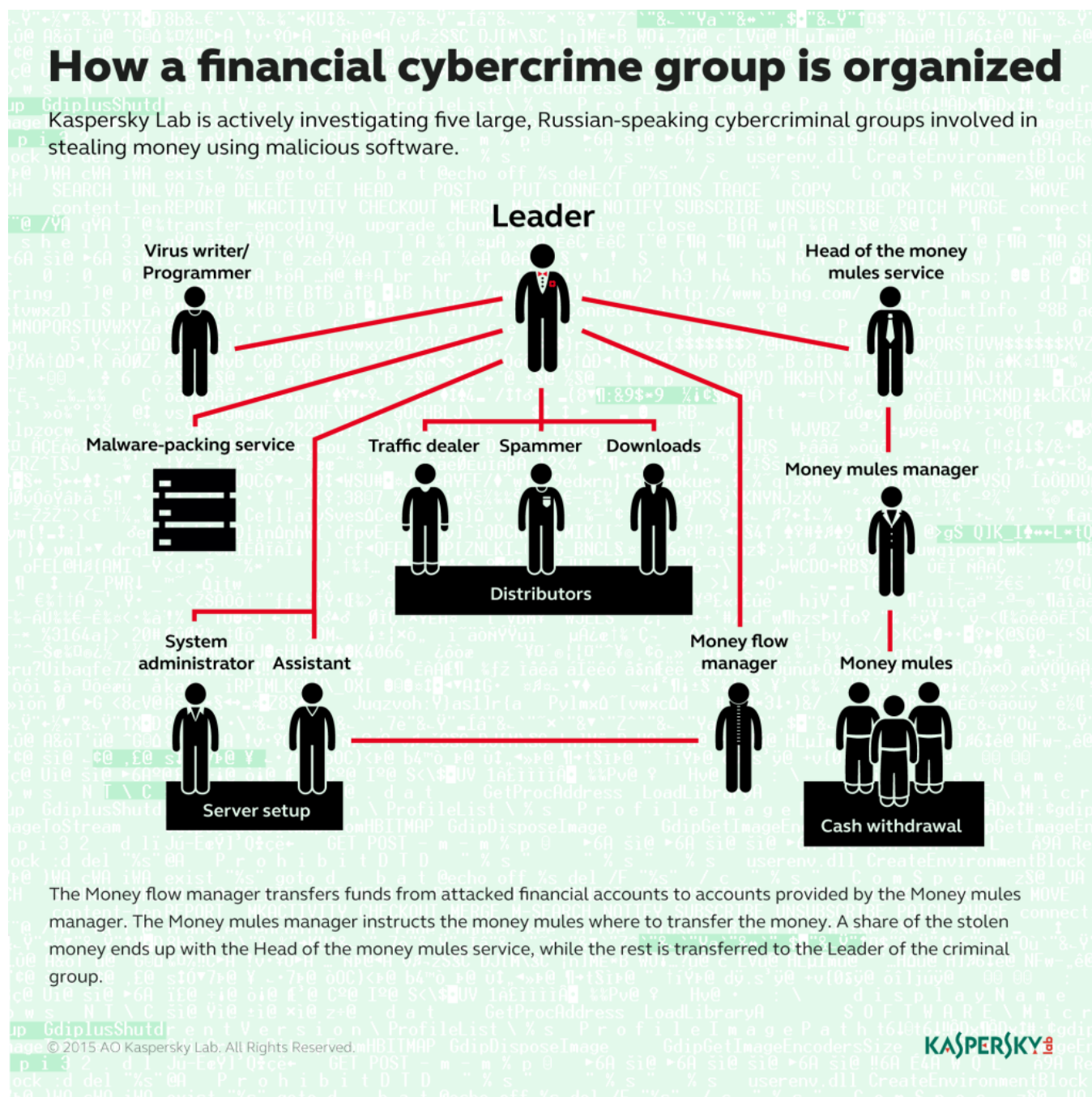
These organizations operate like regular businesses offering a large number of services and products. The Russian underground focuses its offer on [hacking solutions](#) and [credit card frauds](#).

"All of these "products" and "services" are bought and sold in various combinations in order to enable four main types of crime. These types can also be combined in various ways depending on the criminal group:"

- *DDoS attacks (ordered or carried out for the purpose of extortion);*
- *Theft of personal information and data to access e-money (for the purpose of resale or money theft);*
- *Theft of money from the accounts of banks or other organizations;*
- *Domestic or corporate espionage;*
- *Blocking access to data on the infected computer for the purpose of [extortion](#);*

The experts observed that preferred currencies for transactions in Russian underground include [Bitcoin](#), Perfect Money, and WebMoney.

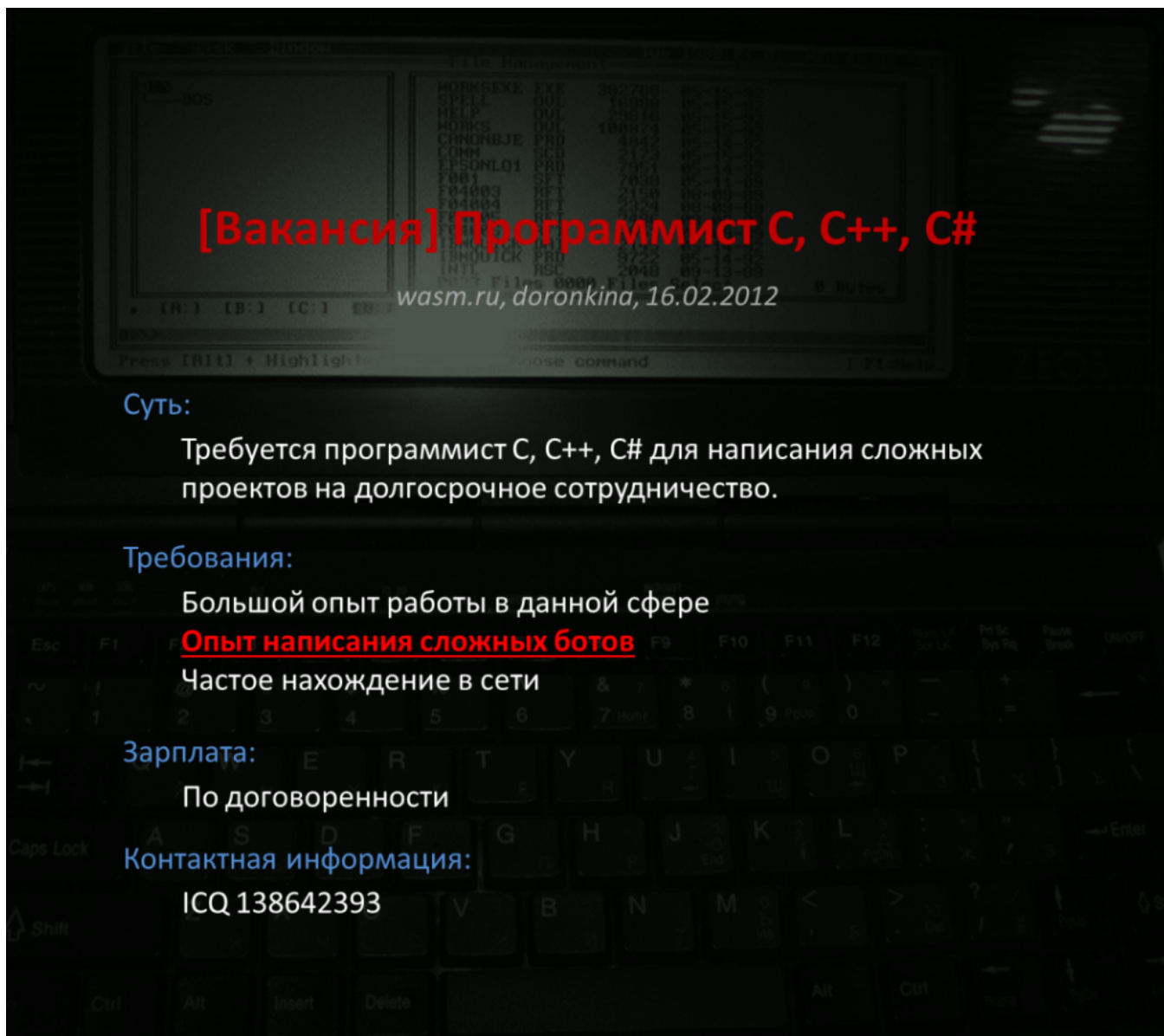
The Russian cyber underground offers a lot of job opportunities for wannabe cybercriminals, there are offers for both skilled and novice people.



Skilled professionals can be recruited for programming and virus writing, web designing for phishing pages, and testing. A category of individuals that is also requested are the cryptographers, which are hired as 'cryptors' for packing malicious code so as to evade malware detection.

"In general, employees involved in cybercrime can be divided into two types: those who are aware of the illegality of the project or the work they are offered, and those who (at least in the beginning) know nothing about it. In the latter case, these are usually people performing relatively simple operations such as copying the interface of banking systems and sites," states the report. "By

advertising “real” job vacancies, cybercriminals often expect to find employees from the remote regions of Russia and neighboring countries (mostly Ukraine) where problems with employment opportunities and salaries for IT specialists are quite severe.”



[Вакансия] Программист С, С++, С#
wasm.ru, doronkina, 16.02.2012

Суть:
Требуется программист С, С++, С# для написания сложных проектов на долгосрочное сотрудничество.

Требования:
Большой опыт работы в данной сфере
Опыт написания сложных ботов
Частое нахождение в сети

Зарплата:
По договоренности

Контактная информация:
ICQ 138642393

Skilled professionals can be recruited for programming and virus writing, web designing for phishing pages, and testing. A category of individuals that is also requested are the cryptographers, which are hired as ‘cryptors’ for packing malicious code so as to evade malware detection.

Give a look to the [report](#) ... it is fully of interesting information on the Russian underground.

Pierluigi Paganini

(**Security Affairs** – Russian underground, *cybercrime*)

Share it please ...        

 [cybercrime card frauds](#) [extortion](#) [hacking services](#) [Kaspersky Lab](#) [malware](#)

[Russian Underground](#)[Breaking News](#)[Cyber Crime](#)

SHARE ON



Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".



PREVIOUS ARTICLE

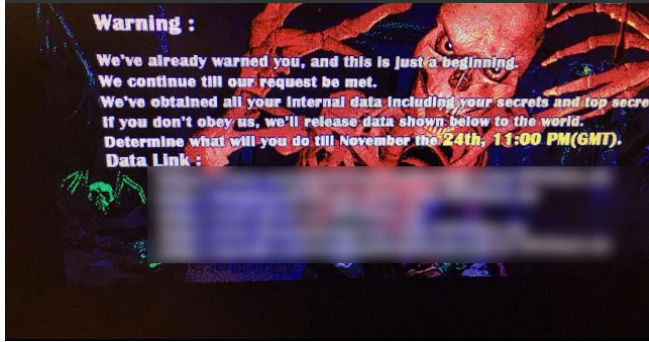
[Security Affairs newsletter Round 36 –
Best of the week from best sources](#)

NEXT ARTICLE

[Ransomware will target also Medical
Devices](#)



YOU MIGHT ALSO LIKE



Damballa revealed the secrets behind the Destover malware that infected the Sony Pictures

November 23, 2015 By [Pierluigi Paganini](#)





Police Body Cameras come with Conficker Worm

November 22, 2015 By [Pierluigi Paganini](#)



MORE STORY



ty Affairs Newsletter - Best of the v

if the best security articles published this week by the principal sources field.

Security Affairs newsletter Round 36 – Best of the week from best sources

A new round of the weekly Security Affairs newsletter arrived! Every week