

LESS AGGRESSIVE, MORE EFFECTIVE: SOCIAL ENGINEERING WITH PAID ARCHIVES

Sergey Chernyshev & Daniel Chipiristeanu
Microsoft Malware Protection Center (MMPC)

Microsoft Malware Protection Center

Who, What, & Where

Protection points

Home:

- Microsoft Security Essentials (MSE)
- Malicious Software Removal Tool (MSRT)
- Windows Defender

Corp:

- System Center Endpoint Protection (SCEP)

Cloud:

- Intune
- Hotmail
- Exchange
- Azure

Strategy:

Ensure all of
Microsoft's
customers are
protected

Security vendor agnostic

Disrupt the malware
ecosystem

Support the security
industry

Security content, sharing

Investments:

safe future
systems, processes
scale

Protect through the
cloud

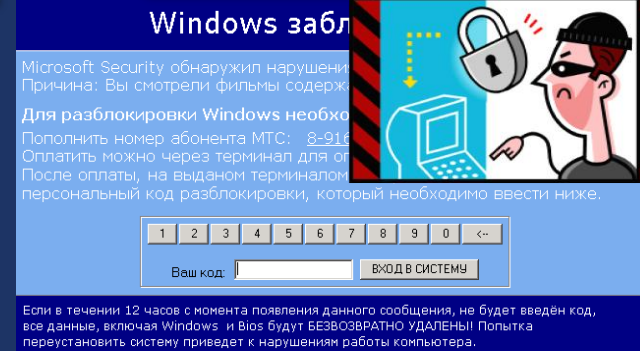
Collaborate with
security industry
Operationalize
research
with BI, automation

Background: social engineering attacks

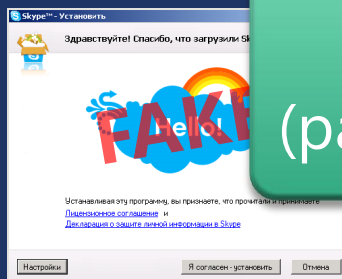
Target

Bogus security solutions

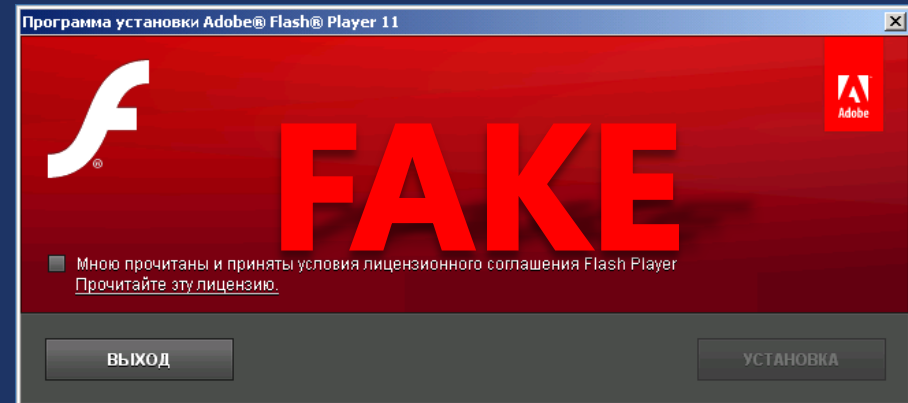
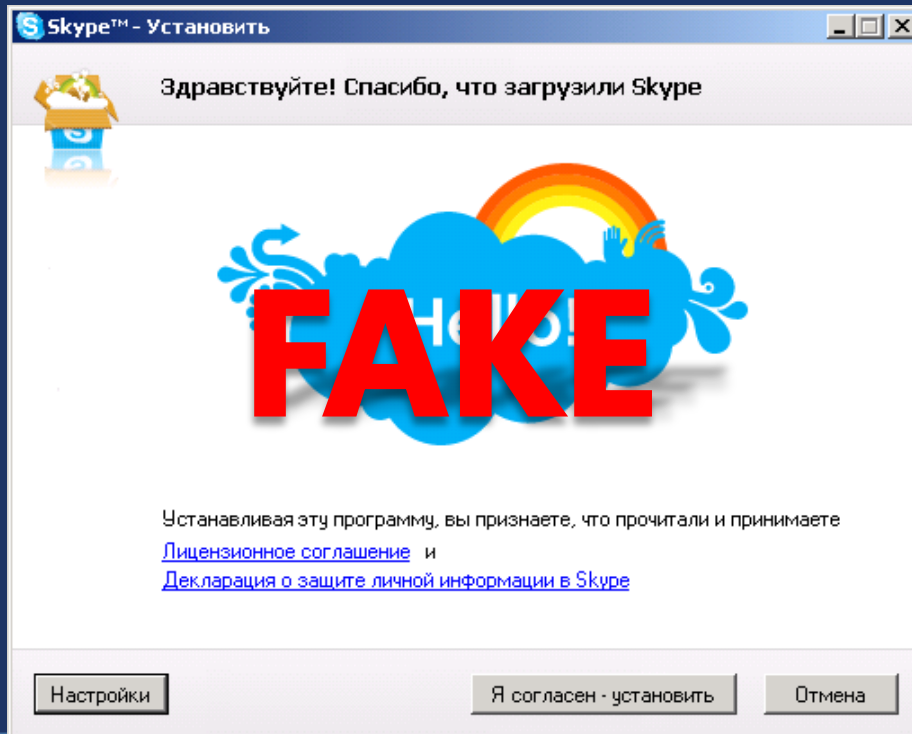
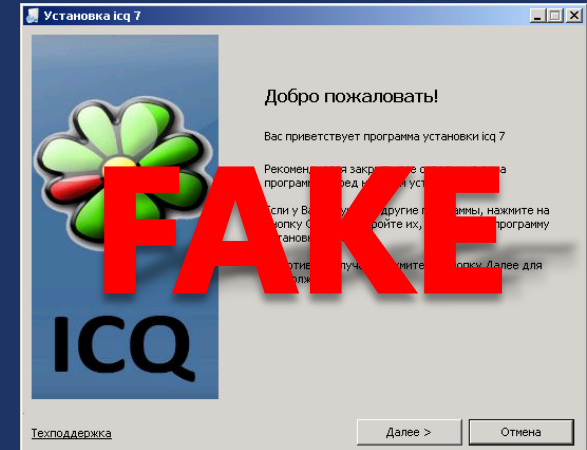
Ransomware



Fake software installers (paid archives)



What are paid archives?



User experience: SKYPE

1. Where can I get SKYPE?

The screenshot shows a Bing search results page for the query "skype download скачать бесплатно". The search bar contains the text "skype download скачать бесплатно" and shows 3,330,000 results. A green arrow points to the first search result, which is a link to "скачать" (download) on the website "www.skype.com/intl/ru/get-skype/on-your-computer/windows/downloading". Below this, there are several other search results, including one from "skypeclub.ru" and another from "skypeclub.ru" with a red arrow pointing to it. The red arrow is labeled "Click". The search results are in Russian and include links to download Skype for Windows, Mac OS X, Linux, and iPhone. The page also shows navigation tabs for "WEB", "IMAGES", "NEWS", and "MORE", and a "Help improve Bing" button at the bottom right.

WEB IMAGES NEWS MORE

bing skype download скачать бесплатно

3,330,000 RESULTS Narrow by language Narrow by region

[скачать](#)
www.skype.com/intl/ru/get-skype/on-your-computer/windows/downloading

[Skype скачать бесплатно русская ...](#) Translate this page
www.skypeclub.ru/skype_windows.htm
Скачать Skype - скачать бесплатную версию скайп. Скачать Skype бесплатно, русская версия Skype.

[skype download - YouTube](#)
www.youtube.com/watch?v=YKHosH-ljys
By Sweasy26ForPeace · 587 views · Added 26/05/2011
26/05/2011 · skype download skype, skype free download, skype скачать, skype скачать бесплатно, skype go to http://www.skype.com/intl/en-us/get ...

[Скачать Skype | Skype Download | skype.ru](#) Translate this page
www.skypeclub.ru/skype_download.htm
Скачать Skype: Skype для Windows; Skype для Windows (Business version) Skype для Mac OS X; Skype для Linux; Skype для iPhone

[Скачать скайп 4.2 skype 5.5 бесплатно ...](#) Translate this page
skype-[nload.ru](#)
Скачать скайп 4.2 и 5.3 (skype) бесплатно ... Скачать скайп (skype) вы можете на нашем ...

[Skype - скачать Skype бесплатно](#) Translate this page
skype.izcity.com

Internal preview Help improve Bing

User experience: SKYPE

1. Where can I get SKYPE?

2. Let me download it ...

Microsoft® | Translator Privacy | Legal
Translator Help

Microsoft® is not responsible for the content below

Powered by Microsoft® Transl

Translate URL http://skype-nload.ru/ Russian (Auto-Detected) English Views

Translated 100% Mouse over text to see original

Download Skype 4.2 or 5.3 (skype) for free

Skype 4.2 (Skype) in Russian

Download Skype (skype) you can on our website, be(c) chargeable! you have noticed a mistake?, of course, we did it deliberately to draw attention. free – means that the program Skype (skype) can be used free of charge and can be downloaded for free on our site. **Downloading the program Skype (skype) version 4.2 or 5.3** you can make worldwide calls to any user. In addition, you can make calls not only to subscribers of Skype (skype), but also any other subscribers to fixed or mobile phones anywhere in the world, even in Antarctica, the Arctic, or in Papua New Guinea. You don't come to the crazy bills because fares Skype (skype) for the lowest and most flexible. And only on our website for you, we offer to

Skype 4.2 GB
Download
Skype 5.3 Eng
Download

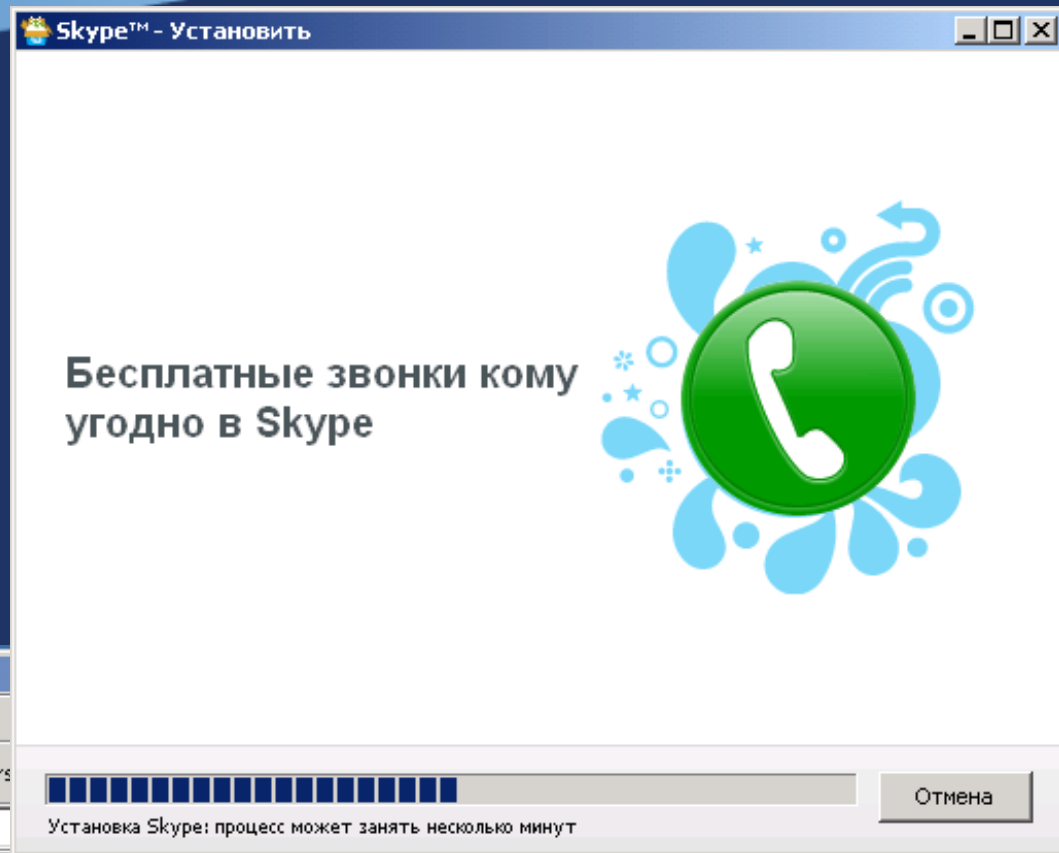
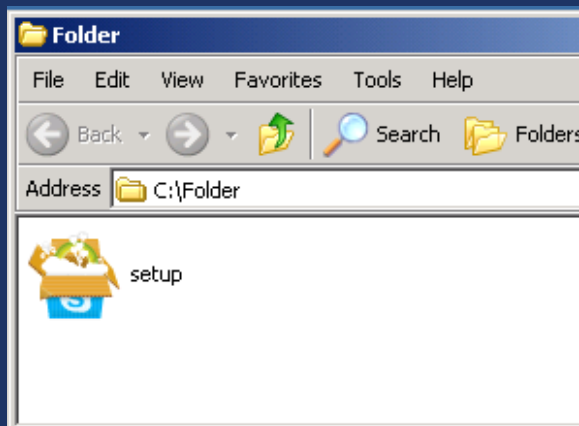
Click

User experience: SKYPE

1. Where can I get SKYPE?

2. Let me download it ...

3. Save & Install ☺ ...



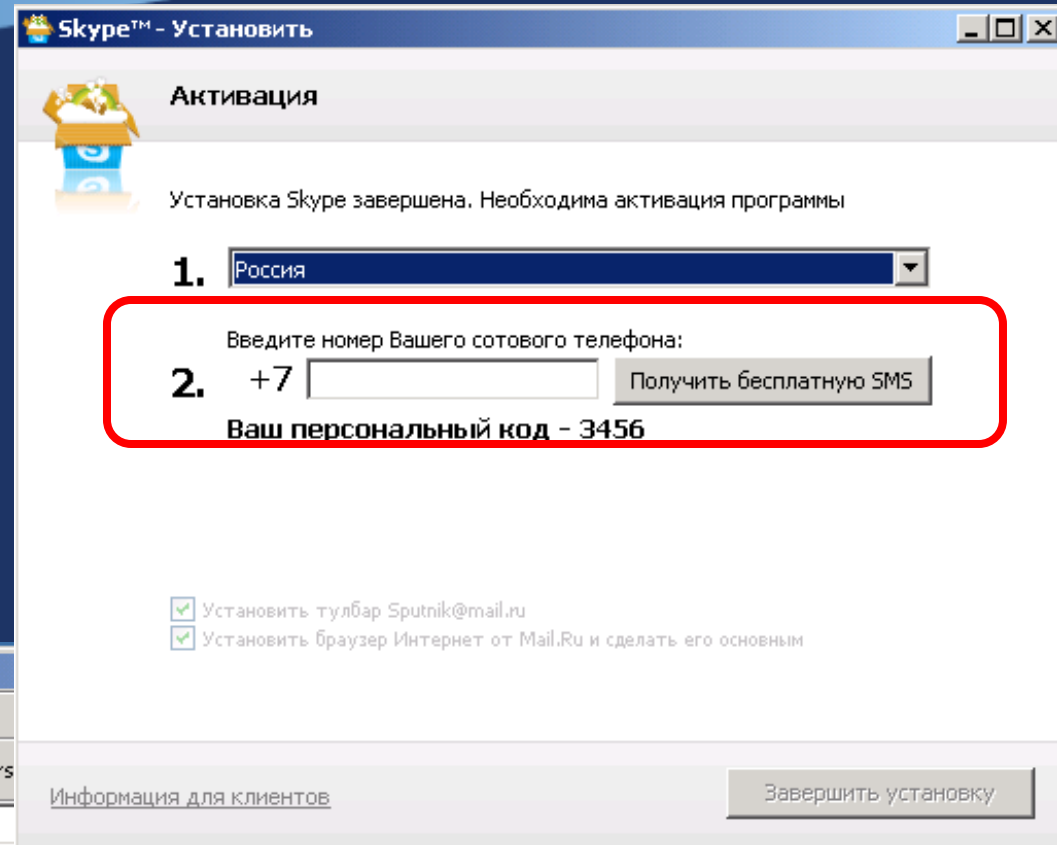
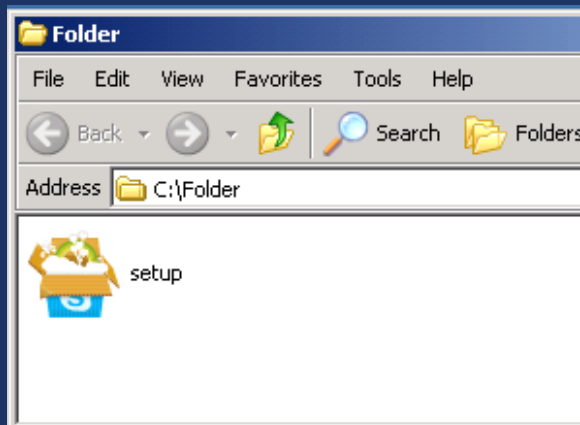
User experience: SKYPE

1. Where can I get SKYPE?

2. Let me download it ...

3. Save & Install ☺ ...

4. Why my Phone # for SMS? ☹



User experience: Adobe Flash Player

1. Where can I get FLASH?

The screenshot shows a Bing search results page for the query "adobe flash player скачать бесплатно". The search results are listed in Russian. A green arrow points to the first result, and a red arrow labeled "Click" points to the second result.

Search Results:

- Result 1 (highlighted in green):** [Adobe - Установить Adobe Flash Player](http://get.adobe.com/ru/flashplayer) Translate this page
get.adobe.com/ru/flashplayer
Главная страница; Скачать; Adobe Flash Player; Adobe Flash Player
- Result 2 (highlighted in red):** [Скачать Adobe Flash Player бесплатно. Adobe...](http://www.besplatnyeprogrammy.ru/adobe-flash-player.html) Translate this page
biblprog.org.ua/ru/flash_player
Скачать Adobe Flash Player. Adobe Flash Player — бесплатный, широко распространенный проигрыватель ...
- Result 3:** [Адобе Флеш Плеер Adobe Flash Player 11 ...](http://www.besplatnyeprogrammy.ru/adobe-flash-player.html) Translate this page
www.besplatnyeprogrammy.ru/adobe-flash-player.html
Скачать бесплатно Adobe Flash Player 11 с каталога легально бесплатных программ. Adobe Flash Player 11 ...
- Result 4:** [Adobe Flash Player 11 скачать бесплатно ...](http://adobe-flash.com) Translate this page
adobe-flash.com
Скачать последнюю версию Adobe Flash Player 11 бесплатно. Просмотр видео, игр - Адоб Флеш Плеер новой ...
- Result 5:** [Adobe Flash Player - скачать бесплатно...](http://www.softportal.com/software-842-a) Translate this page
www.softportal.com/software-842-a
Adobe Flash Player - скачать Adobe Flash Player 11.2.202.235, Adobe Flash Player - кроссплатформенный модуль, который ...
- Result 6:** [Adobe Flash Player — скачать беспла...](http://www.izone.ru/internet/ru/ins/adobe-flash-player.html)
www.izone.ru/internet/ru/ins/adobe-flash-player.html

At the bottom of the page, there are links for "Internal preview" and "Help improve Bing".

User experience: Adobe Flash Player

1. Where can I get FLASH?

2. Let me download it ...



The screenshot shows a Microsoft Translator window with the URL <http://www.adobe-flash.com/> translated from Russian to English. The page content includes:

- Two download buttons for Adobe Flash Player 11: one for Chrome, Opera, and Firefox, and another for Internet Explorer. Both buttons have a red arrow icon and the text "Загрузить сейчас" (Download now).
- A large red banner with the Adobe Flash Player logo and the text "ADOBE® FLASH® PLAYER".
- A heading: "Download Adobe Flash Player 11 free".
- A paragraph describing Adobe Flash as a software product from Adobe, designed for creating web applications and multimedia presentations.
- Two download links: "Download Adobe Flash Player 11 for Internet Explorer" and "Download Adobe Flash Player 11 for Chrome, Opera, Firefox".
- A "Site navigation" section with links to "Adobe Flash Player", "Flash Player Settings", and "Questions and answers".

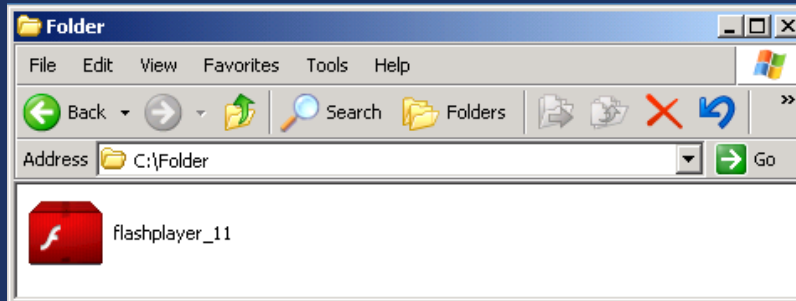
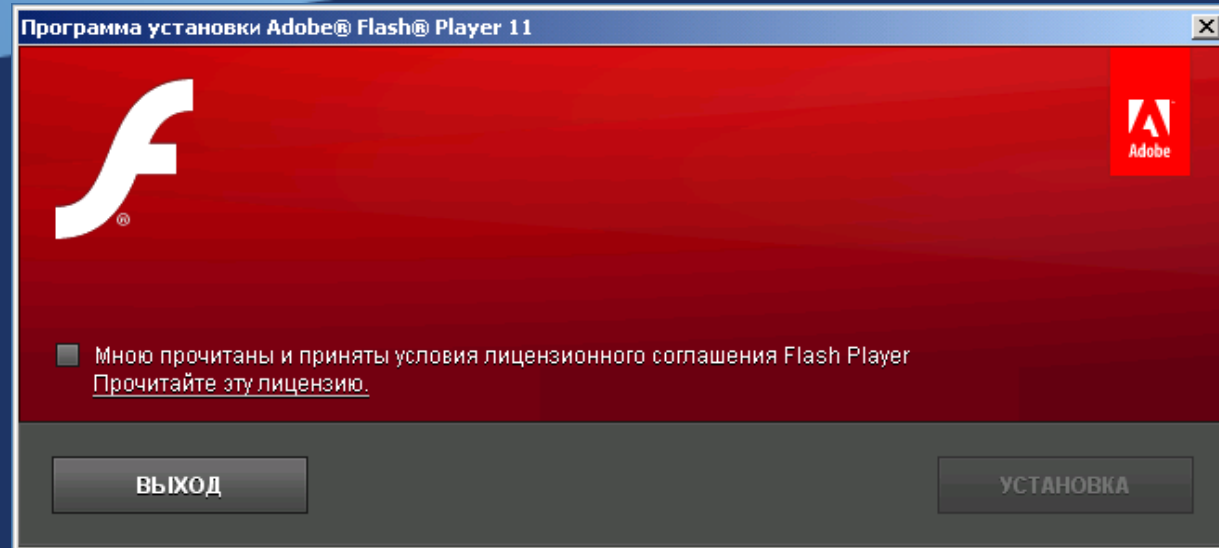
A red arrow labeled "Click" points to the "Download Adobe Flash Player 11 for Internet Explorer" link.

User experience: Adobe Flash Player

1. Where can I get FLASH?

2. Let me download it ...

3. Save & Install 😊 ...

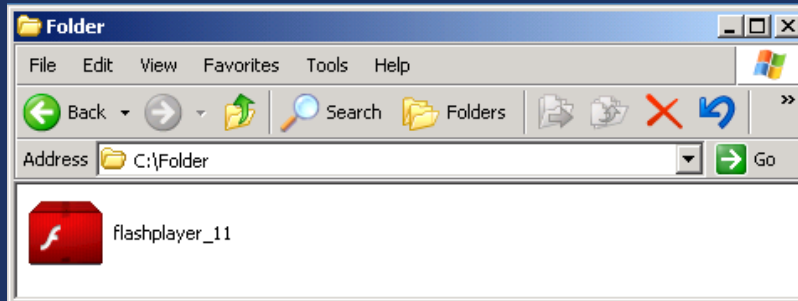
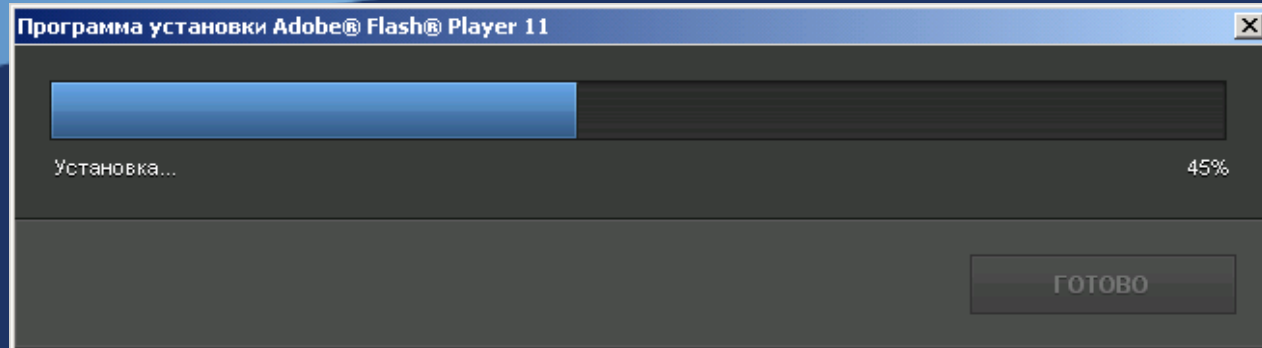


User experience: Adobe Flash Player

1. Where can I get FLASH?

2. Let me download it ...

3. Save & Install 😊 ...



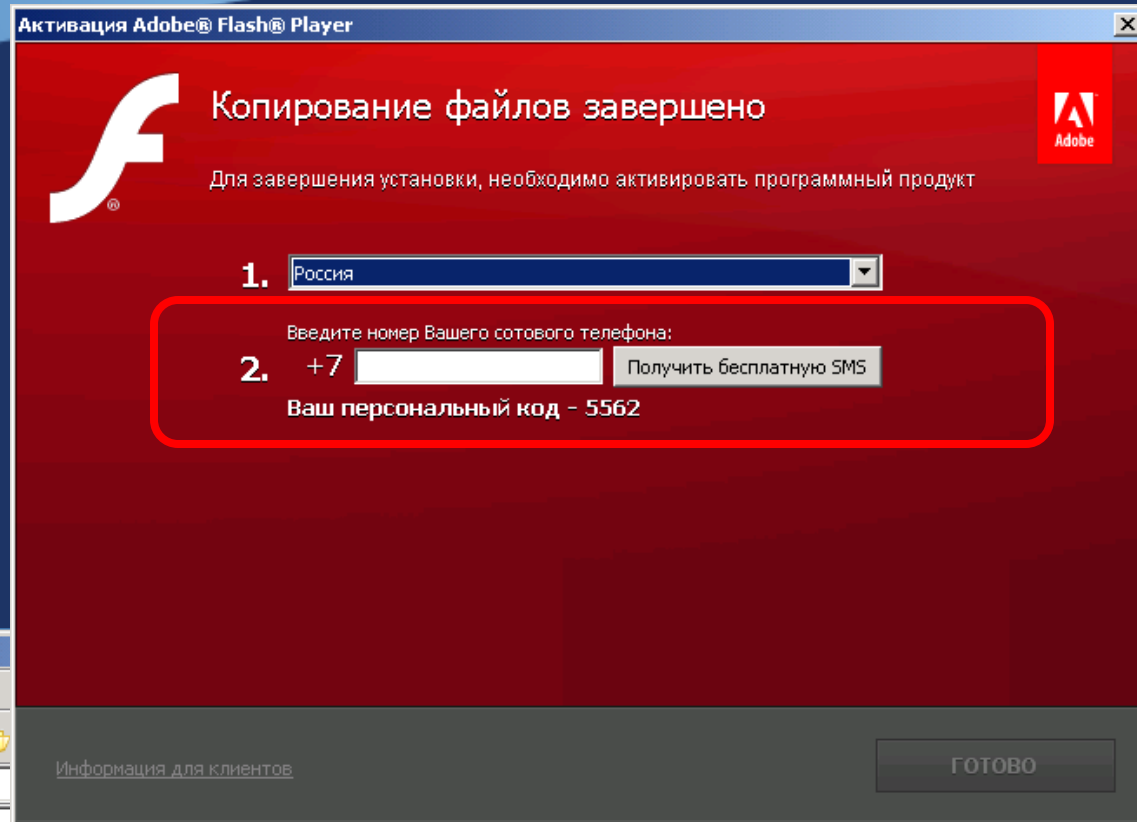
User experience: Adobe Flash Player

1. Where can I get FLASH?

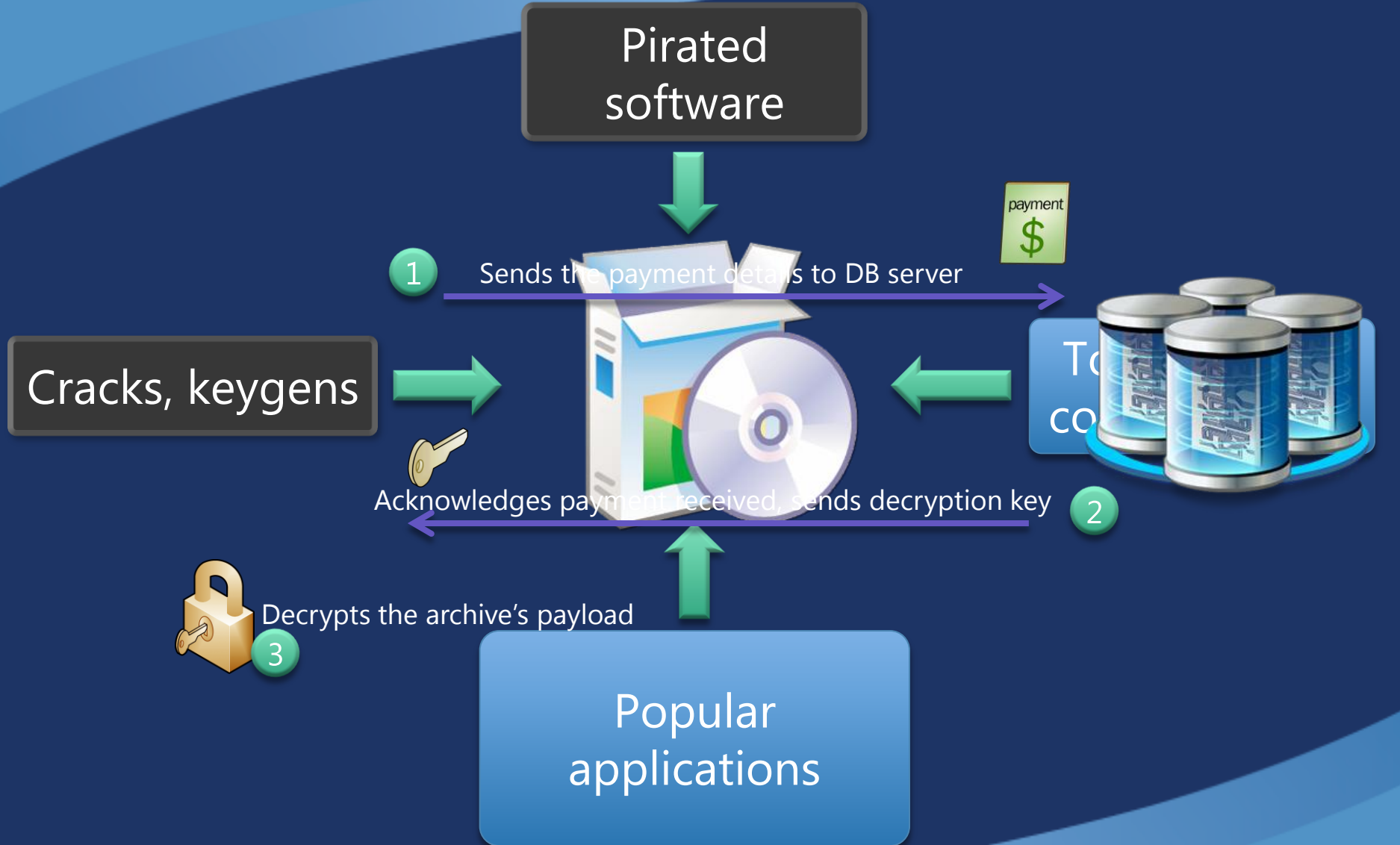
2. Let me download it ...

3. Save & Install 😊 ...

4. Why my Phone # for SMS? 😞



What's the deal with the mechanics

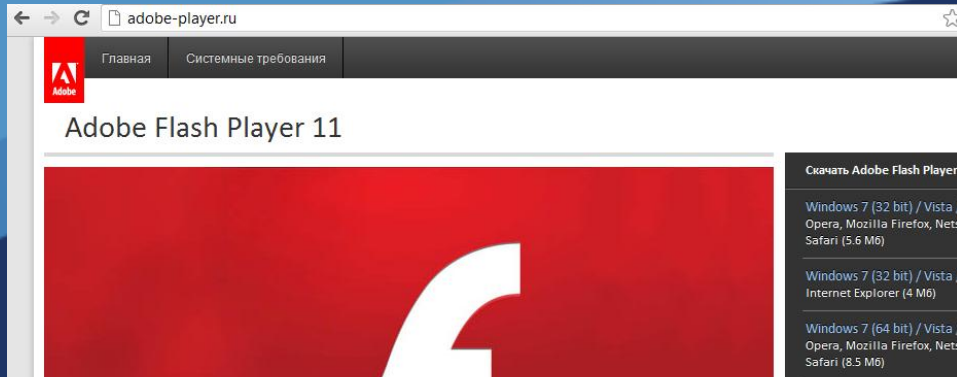


How they are created: builder toolkit

The image displays a software builder toolkit interface with several overlapping windows. The main window, titled "ZIPPRO v3.5", shows a file explorer view of a folder named "arhiver" containing "Adobe Reader.zip". Below this is a list of application templates under the heading "Внешний вид архива" (Archive appearance), including "Doodle Jump", "Download Master", "Far Manager 2", "FL Studio", "Google Chrome", "ICQ", "iTunes", "K-Lite Codec Pack", "Mail.ru Agent", "Mozilla Firefox", "MS ActiveSync", "MS DirectX", "MS Office 2003", "MS Office 2007", "MS Power Point 2007", "MS Power Point 2010", "MS Visio 2007", and "MS Word 2007". A red box highlights this list. To the left, a "ZipMonster Archiver 1.9.1 build 220" window shows a "Master of archive creation" wizard with a "Внешний вид архива" section also highlighted in red, listing various software titles. At the bottom, a "Настройка" (Settings) window shows options for "Тулбары M", "Псевдоподпись", and "Управление шаблонами". A "Создать архив" (Create archive) button is visible at the bottom right.

Integrated Development
Environment (IDE)

How they are created: landing pages



all-freeload.com/bezopasnost/664-microsoft-security-essentials

Microsoft Security

★★★★★ ratings: 3 Category: Antivirus

Screenshots:

Today, surfing the Internet is fraught with many threats and strive to enter the user's computer. Among them are not only familiar to all viruses and Trojans, spyware and worms. Distributed for free antivirus software Microsoft Security Essentials helps you to organize the effective protection of all listed malware.

You can **microsoft security essentials free download** from our site, and the direct link with the resource manufacturer - Microsoft. After installing the software automatically updated daily. In this case, perform some custom action to start the process is not necessary.

Antivirus Microsoft Security Essentials is designed exclusively for home users and small businesses (up to 10 workstations). Despite its rather modest purpose, this product incorporates the best achievements in the field of security, which for years has accumulated a giant in the field of software, like Microsoft. And today the company has created a team of highly qualified professionals, which works on permanent tracking of the latest threats, and developing ways to neutralize them.

The software interface uses color coding to interpret the level of current computer protection. This allows the user to raise that issue, which, according to **Microsoft Security Essentials**, deserves a moment of attention.

Features and benefits of the product Microsoft Security Essentials

- Protection in real time;

Functional Web browser for the Internet. Developed in 1994 by Opera Software ASA (freeware). TDI-built interface, block annoying pop-ups, fraud protection, BitTorrent-Client, RSS-aggregator and a download manager. Plus there is also the same mail client Opera Mail client to work with the IRC-networks. The browser is written in C++ and has a high work rate.

Opera - a convenient, smart and versatile browser. Chances are, you probably already have heard about that for quite some time, Opera is still the fastest browser among others.

Opera browser is equipped with all the necessary tools for your safety and productivity of the Internet, as it contains the protection module Fraud, content blocker, integrated BitTorrent client, download manager files, IRC-Chat, RSS-client, widgets, voice control, and more.

to the combination of reading RSS-flows with email clients and widgets, **Opera** some the universal tool to communicate with the world outside the local area

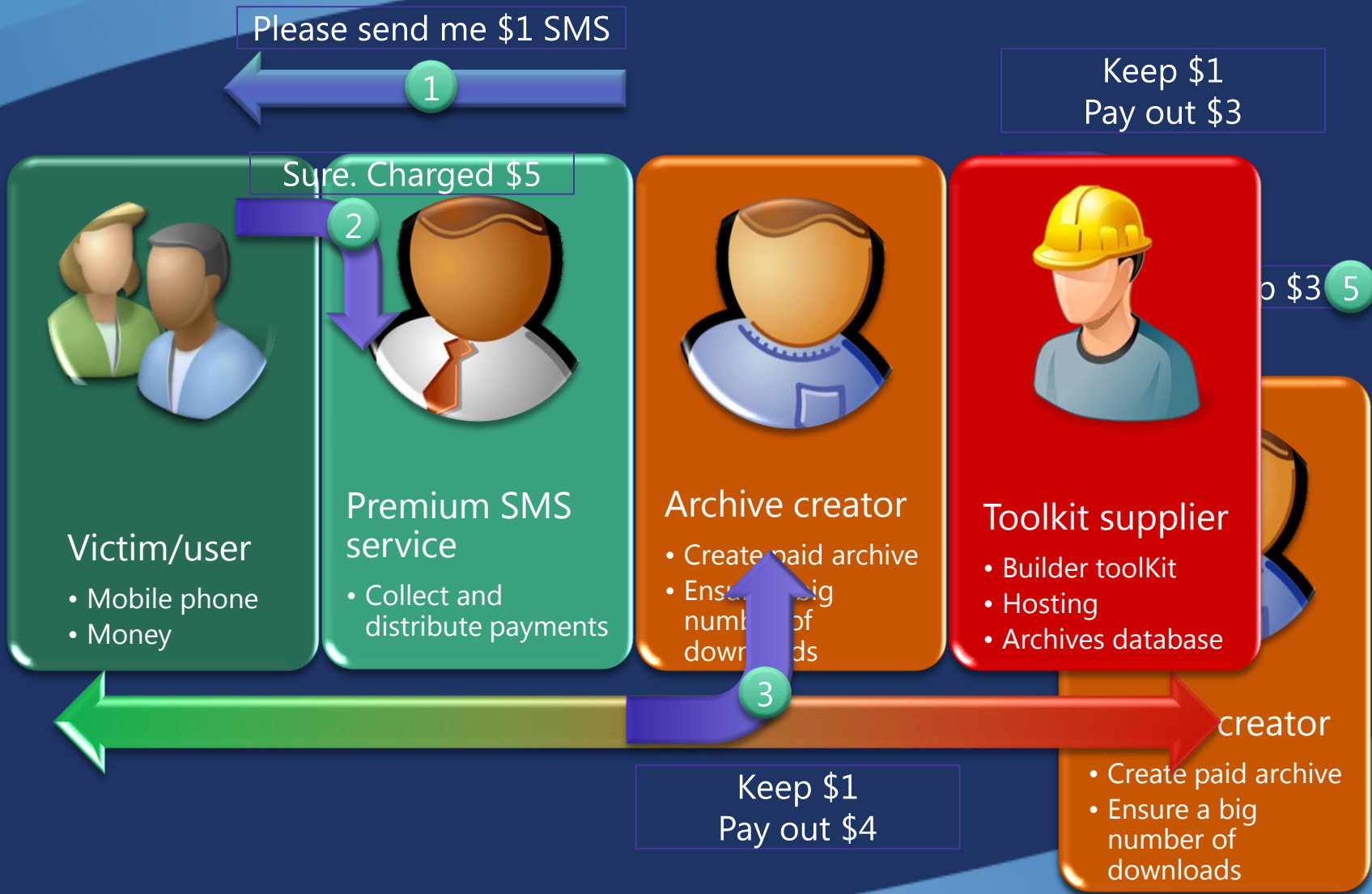
while browsing, and the use of tabs - all these features on the development of as a long time to work its competitors, and a number of similar applications, still missing.

dgets from the site contains Opera everything from watches, games, radio, and search tools to weather forecasts, sports news, web cameras, as well as messaging and email. All these can be easily managed from the Widgets

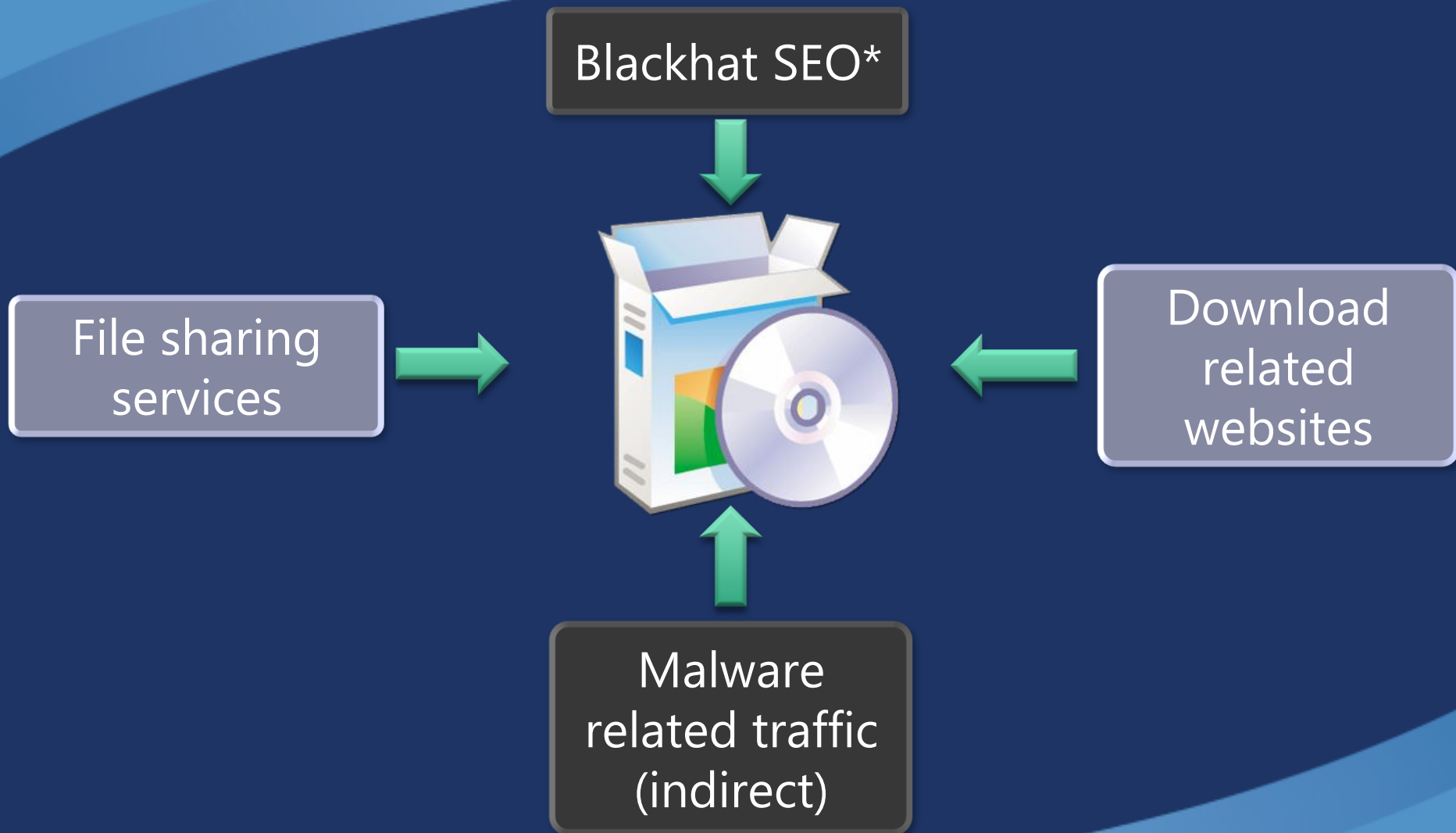
rding to the available categories.

es of Opera:

What happens when you pay for SMS text preparation



Sourcing unwilling victims: web traffic



*SEO – Search Engine Optimization

Profile: ZIP PRO

12 000+ partners from 2009

\$6 400 000 revenue

120 templates

Installs Mail.Ru Sputnik
(\$0.06)

The screenshot displays the ZIPPRO website interface. At the top, there is a navigation bar with links for HOME, RULES, NEWS, CONTACTS, ENTRANCE, and REGISTRATION. The main content area features a large banner for "ZIPPRO" with the tagline "заработай на архивах". Below this, there is a section titled "Создание архива:" (Archive Creation) with a progress bar showing "Шаг: 1 из 2" (Step: 1 of 2). To the right of the banner, there are three promotional boxes: "BACK UP IN THE PAID ARCHIVE!", "POST PAID INTERNET ARCHIVE!", and "ADVERTISE AND EARN MONEY!". At the bottom of the page, there is a section titled "DELPHI 2009 SDK TO CREATE YOUR OWN SKINS!" with three buttons: "WHY ZIPPRO?", "WHAT IS THE PAID ARCHIVES ZIPPRO V 3.5?", and "FOR PROFESSIONALS".

Profile: ZIP Monster

Active since 2010

Offline and online versions

60 templates

AV detection evasion

The screenshot shows a Microsoft Translator window displaying the ZIPMONSTER.RU website. The browser address bar shows the URL <http://www.zipmonster.ru/>. The website header includes navigation links: HOME, ABOUT THE SYSTEM, RULES, FAQ, DOCUMENTATION, OUR ADVANTAGES, and CONTACTS. The main content area features the ZIPMONSTER.RU logo with the tagline "заработай на архивах!". Below the logo is an "AUTHORIZATION" section with a login form containing fields for "Ваш логин" and a password, a "ВОЙТИ" button, and a "Recover password" link. To the right of the login form is a "3 SIMPLE STEPS to EARNING" section with three steps: "Back Up!", "Upload the archive on the Internet!", and "Advertise and earn money!". An illustration of a safe with various items inside and gold coins is positioned to the right of the steps. Below the login form is a world map with the text "Мы принимаем 236 стран Мира". At the bottom, there is a "What is ZIPMONSTER?" section and a "News" section with a date "09.08.2012".

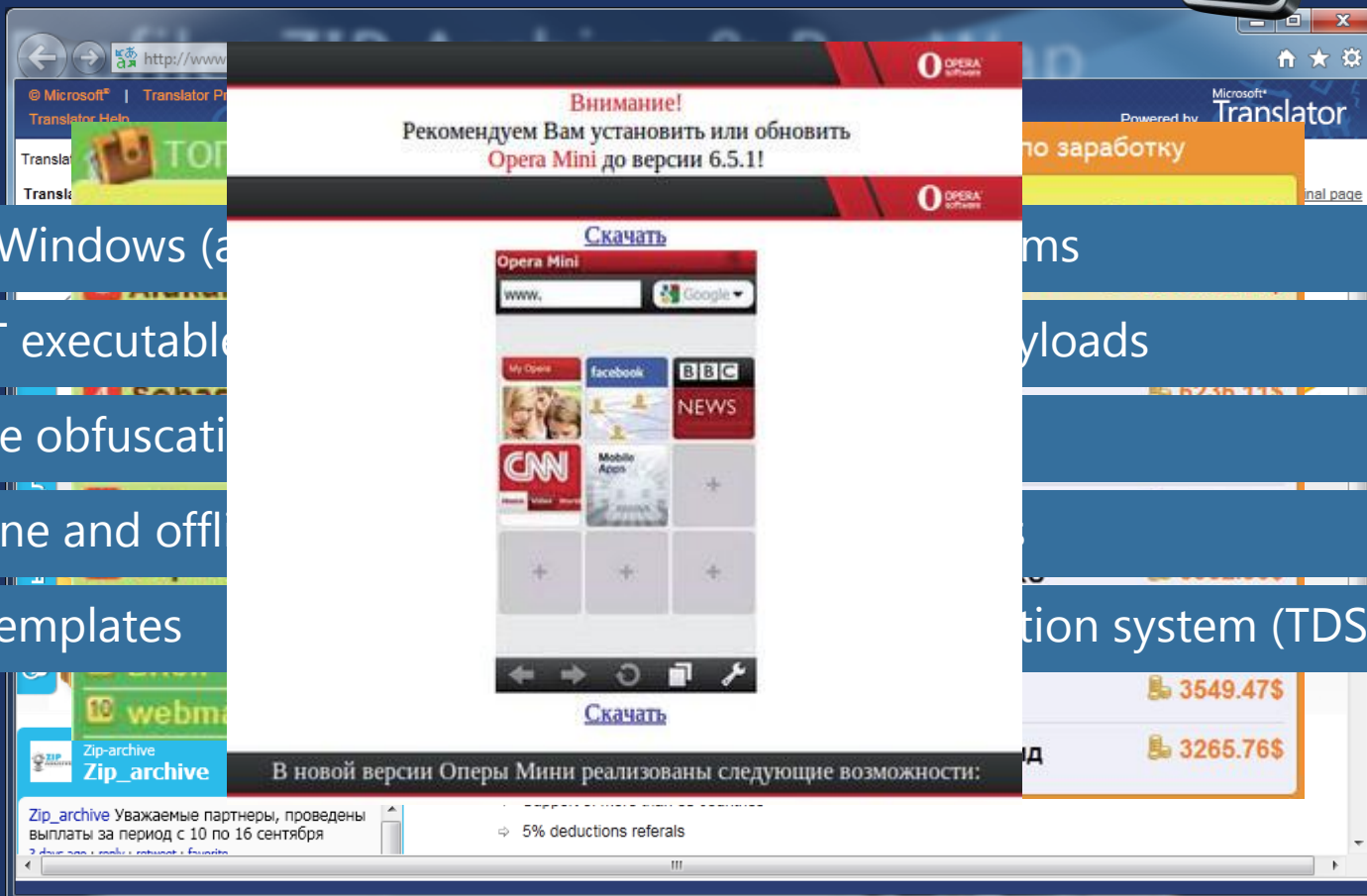
Profile: ZIP Archive & Pro Wap

ZIP Archive

4 000+ webmasters, top 10

Pro Wap

1 200+ webmasters



MS Windows (a

.NET executable

Code obfuscati

Online and offl

80 templates

ms

yloads

tion system (TDS)

3549.47\$

3265.76\$

Zip_archive Уважаемые партнеры, проведены выплаты за период с 10 по 16 сентября

5% deductions referrals

Profile: StimulProfit

StimulProfit

36 000+ registered partners since 2010


Traffic only partnership (server side); paid archives are only seen by users

Plugins for *DataLife Engine* (DLE), *WordPress* and *uCoz*

Domain parking

Пример верхнего блока



Найденные файлы	Закачек	Средняя скорость
 полная версия	↓ 8865	⊕ 7778 кб/сек
 высокая скорость	↓ 8027	⊕ 2021 кб/сек
 Скачать по прямой ссылке	↓ 9848	⊕ 3724 кб/сек
 torrent	↓ 9546	⊕ 2222 кб/сек

Detection evasion methods

Employs obfuscation packers to avoid Detection

- Same packers commonly found in: Zeus (Zbot), Reveton, Kanots, Dofail

Builder Supplier	MS Detection Name	Anti-Detection Techniques
Zip Monster	Program:Win32/Pameseg.BU	<ol style="list-style-type: none">1. Search bytes in system DLLs2. Check OS environment3. Use infinite loops
Zip Pro	Program:Win32/Pameseg.(AK AZ)	<ol style="list-style-type: none">1. Search bytes in system DLLs2. String obfuscation
Zip Archive	Program:MSIL/Pameseg.G	NET assembly obfuscation (use commercial obfuscators)
Pro Wap	Trojan:AndroidOS/VolterSms.A	APK code and string tempering
Stimul Profit	Program:Win32/Pameseg.CF	<i>TCrypt</i> packer

Conclusion

Use less aggressive behaviors

Attract less attention

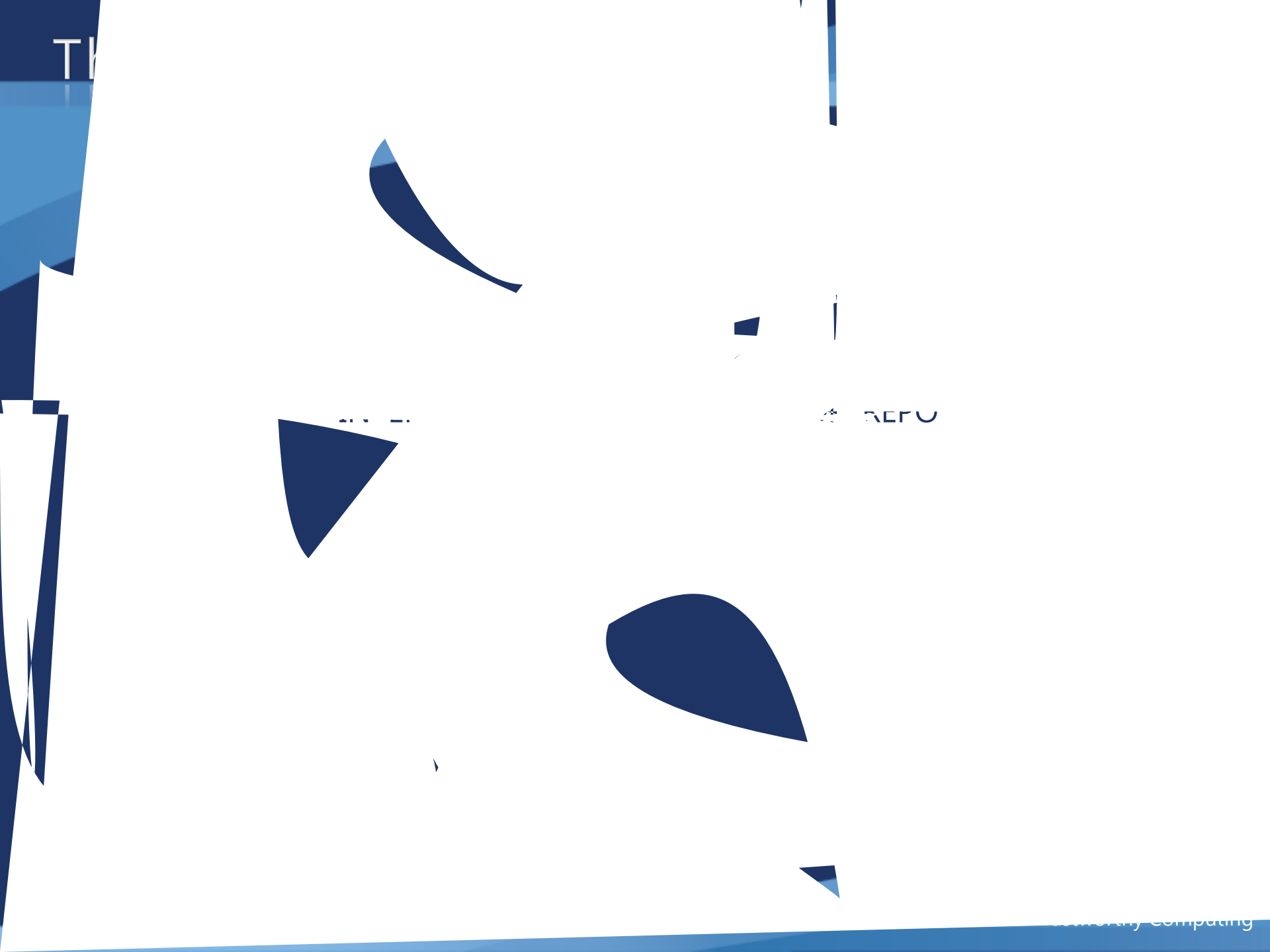
Lower cost for victim

Longer lifetime – longer victim exposure

Long-term effectiveness

Split responsibility

Use EULAs as legal buffers



TH

REFU

Microsoft[®]

Be what's next.[™]

© 2012 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

Trustworthy Computing