



Как информационная безопасность помогает
выжить компании в условиях новых вызовов

Источники угроз

Внешние злоумышленники



Хакерские группировки



Хактивисты и киберармия

NEW



Мелкие пакостники

NEW

Внутренние злоумышленники



Ошибающийся пользователь



Финансово-мотивированный пользователь



Политически-мотивированный пользователь

NEW

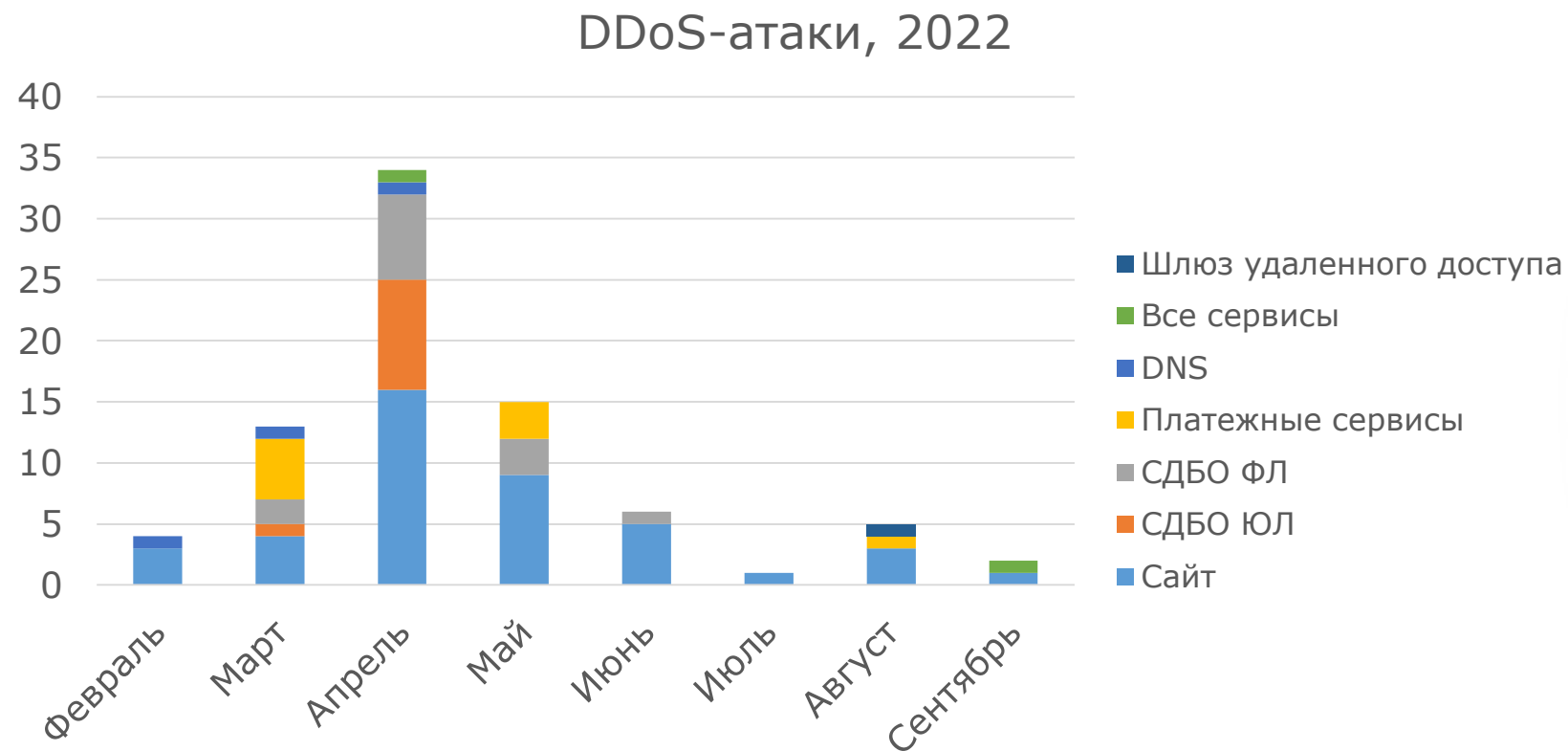
Околосударственные институты



Санкционные активности

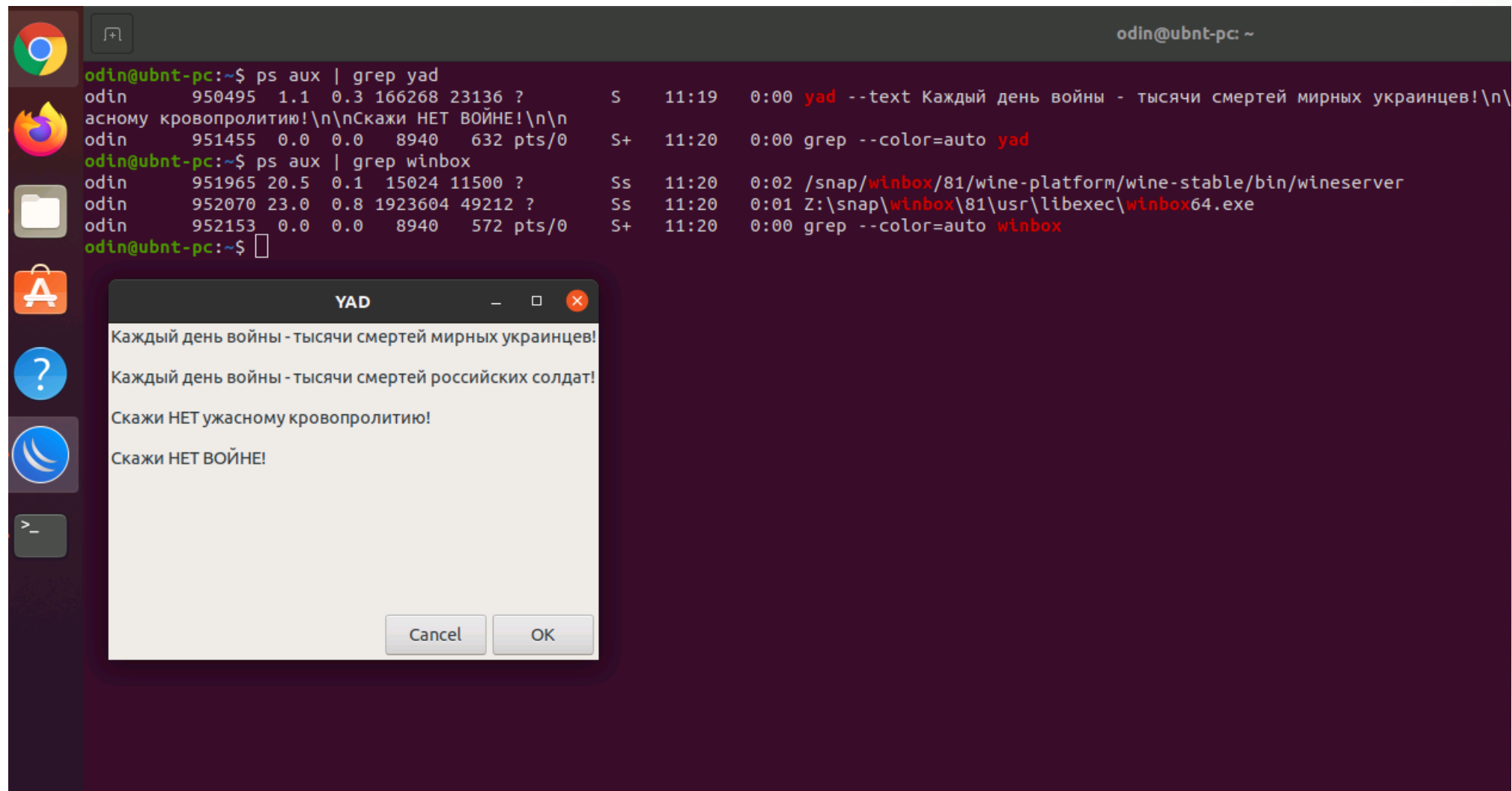
NEW

Попытки реализации угроз



VS 1 атака в 2021

Попытки реализации угроз. Open-source



The screenshot shows a terminal window with the following commands and output:

```
odin@ubnt-pc:~$ ps aux | grep yad
odin    950495  1.1  0.3 166268 23136 ?        S   11:19   0:00 yad --text Каждый день войны - тысячи смертей мирных украинцев!\n\
асному кровопролитию!\n\nСкажи НЕТ ВОЙНЕ!\n\n
odin    951455  0.0  0.0  8940   632 pts/0    S+  11:20   0:00 grep --color=auto yad

odin@ubnt-pc:~$ ps aux | grep winbox
odin    951965 20.5  0.1 15024 11500 ?        Ss  11:20   0:02 /snap/winbox/81/wine-platform/wine-stable/bin/wineserver
odin    952070 23.0  0.8 1923604 49212 ?        Ss  11:20   0:01 Z:\snap\winbox\81\usr\libexec\winbox64.exe
odin    952153  0.0  0.0  8940   572 pts/0    S+  11:20   0:00 grep --color=auto winbox

odin@ubnt-pc:~$
```

A YAD dialog box is open, displaying the output of the 'yad' command:

```
YAD
Каждый день войны - тысячи смертей мирных украинцев!
Каждый день войны - тысячи смертей российских солдат!
Скажи НЕТ ужасному кровопролитию!
Скажи НЕТ ВОЙНЕ!
```

Buttons: Cancel, OK

Попытки реализации угроз. Сертификаты

Хостинг-провайдер DigiCert (Юта, США) отозвал сертификат TLS у сайта Центробанка России, следует из объявления.

"Безопасность вашего соединения снижена. Злоумышленники могут перехватить ваши конфиденциальные данные. Рекомендуется прекратить работу с сайтом", — говорится в сообщении на сайте ЦБ РФ.

С аналогичной проблемой столкнулись сайты некоторых банков. Отзыв сертификатов подтверждает SSLTest.



Переход на домен с недоверенным сертификатом

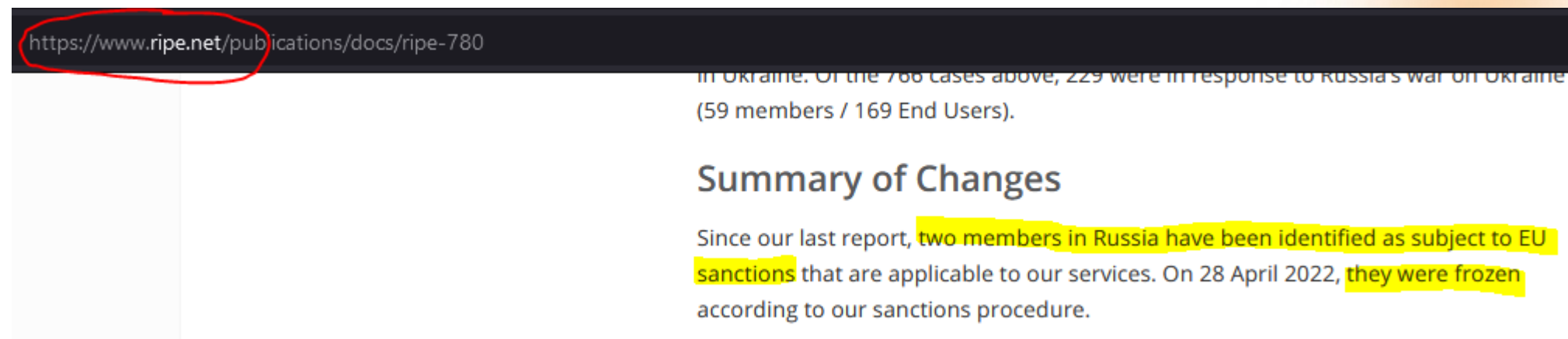
Безопасность вашего соединения снижена. Злоумышленники могут перехватить ваши конфиденциальные данные. Рекомендуется прекратить работу с сайтом.

Веб-адрес:
www.cbr.ru

Попытки реализации угроз. Автономные системы

Внимание вопрос.

Что может случиться с автономной системой при попадании в SDN?



The screenshot shows a document from Ripe.net. The URL <https://www.ripe.net/publications/docs/ripe-780> is circled in red. The document content includes a paragraph about Ukraine: "in Ukraine. Of the 766 cases above, 229 were in response to Russia's war on Ukraine (59 members / 169 End Users)." Below this is a section titled "Summary of Changes" with the following text: "Since our last report, two members in Russia have been identified as subject to EU sanctions that are applicable to our services. On 28 April 2022, they were frozen according to our sanctions procedure."

Попытки реализации угроз. Утечки данных



213 компаний (?) пострадало в РФ за весну-лето 2022

700+ млн. записей в открытом доступе

Попытки реализации угроз. Удаленный доступ



Что объединяет эти программы?

Через каждую из них можно организовать удаленный доступ к инфраструктуре компании без ИТ-скиллов

Попытки реализации угроз. Софт и аппаенсы



We're sorry, something went wrong.

Access denied

You cannot access www.tenable.com. Refresh the page or contact the site owner to request access.



CORTEX XDR

Unauthorized. Error 4011

Dear Palo Alto Networks Customer,

As you know, on a regular basis, the United States (and others) is adopting new restrictions on companies' ability to do business in Russia. The most recent set of US sanctions directly impacts our ability to continue doing business with your company. As a result, Palo Alto Networks is unable to provide your company with products, services and support effective immediately.

Mar 7, 2022: An update on the war in Ukraine

IBM is closely monitoring the war in Ukraine and is taking action to protect its internal operations and to continue delivery of products and services to customers worldwide.

IBM has suspended all business in Russia.

И как же выживать?



Только внешние
сервисы очистки



Закладки в софте



Полноценный SSDLC
(с SAST и DAST)

И как же выживать?



Сертификаты



Резервирование
сертификатов в
разных УЦ



Автономные
системы



Аренда

И как же выживать?



Альтернативная поддержка –
очень плохая идея

Враг снаружи

1. Инвентаризация ИТ-инфраструктуры и способов доступа к ней
2. Защита от вредоносного кода
3. Непрерывное управление уязвимостями
4. Мультифакторная аутентификация
5. Мониторинг
6. Если компания небольшая, рассмотреть аутсорсинг инфобеза

Враг внутри

1. Инвентаризация ИТ-активов
2. Управление доступом
3. Управление уязвимостями
4. Мониторинг
5. DLP
6. Security awareness