

POSITIVE TECHNOLOGIES

# Типовые ошибки в сетевой безопасности и как их устранить

A network diagram with nodes and connecting lines. One node on the right is highlighted with a red circle and a warning triangle icon. The background is dark with colorful bokeh effects.

Алексей Данилин  
Алексей Леднев

# Утечки данных 2018-2019

## Данные пациентов «скорой» из Подмосквья утекли в Сеть



Теги: [Россия](#), [утечка данных](#)

Данные хранились на незащищенном сервере и были выложены в открытый доступ хактивистами.

На станциях скорой медицинской помощи (ССМП) Подмосквья предположительно произошла утечка данных. Правоохранительные органы начали

[securitylab.ru/news/498730.php](https://securitylab.ru/news/498730.php)

HOME THEATER

## Kanopy privacy breach reveals which movies members have been streaming

[digitaltrends.com/home-theater/kanopy-streaming-data-breach/](https://digitaltrends.com/home-theater/kanopy-streaming-data-breach/)

## 21 млн пользователей сервиса Timehop стали жертвами утечки данных



Теги: [утечка данных](#), [взлом](#), [Timehop](#)

Утекшая база данных содержит порядка 4,7 млн телефонных номеров, а также имена пользователей и электронные адреса.

Администрация сервиса Timehop, позволяющего находить опубликованные ранее материалы в соцсетях, [сообщила](#) о масштабной утечке данных. Инцидент произошел 4 июля

текущего года и затронул 21 млн пользователей.

[securitylab.ru/news/494295.php](https://securitylab.ru/news/494295.php)

## ВЗЛОМЩИКИ ПОХИЩАЮТ АККАУНТЫ OFFICE 365 И G SUITE ЧЕРЕЗ IMAP

[threatpost.ru/office-365-and-g-suite-tenants-attacked-through-imap/31880/?tg\\_rhash=914984d8877f4b](https://threatpost.ru/office-365-and-g-suite-tenants-attacked-through-imap/31880/?tg_rhash=914984d8877f4b)

## The Muncy malware is on the rise

February 19, 2019 By Pierluigi Paganini

Over the last few days, a phishing campaign from DHL and entitled “**DHL Shipment Notification**” has been targeted users worldwide distribution the **Muncy** malware.

[securityaffairs.co/wordpress/81373/malware/muncy-malware-phishing.html](https://securityaffairs.co/wordpress/81373/malware/muncy-malware-phishing.html)

```
Secure | https://delivery.panerabread.com [redacted]
{"accounts": [{"username": "[redacted]", "name": "[redacted]", "cardNumber": "*****6515"},
{"username": "[redacted]@hotmail.com", "name": "[redacted]", "cardNumber": "*****5527"},
{"username": "[redacted]@msn.com", "name": "F B", "cardNumber": "*****7921"},
{"username": "[redacted]@yahoo.com", "name": "C", "cardNumber": "*****7108"},
{"username": "[redacted]", "name": "[redacted]", "cardNumber": "*****6129"},
{"username": "[redacted]@aol.com", "name": "[redacted]", "cardNumber": "*****6061"},
{"username": "[redacted]@yahoo.com", "name": "[redacted]", "cardNumber": "*****8950"},
{"username": "[redacted]", "name": "[redacted]", "cardNumber": "*****4412"},
{"username": "[redacted]", "name": "[redacted]", "cardNumber": "*****8386"},
{"username": "[redacted]@aol.com", "name": "[redacted]", "cardNumber": "*****5384"},
{"username": "[redacted]@optonline.net", "name": "[redacted]", "cardNumber": "*****5144"},
{"username": "[redacted]@hotmail.com", "name": "[redacted]", "cardNumber": "*****7488"},
{"username": "[redacted]", "name": "[redacted]", "cardNumber": "*****6702"},
{"username": "[redacted]", "name": "[redacted]", "cardNumber": "*****7085"}, {"username": "[redacted]@hotmail.com", "name": "[redacted]", "cardNumber": "*****4220"}, {"username": "[redacted]", "name": "[redacted]", "cardNumber": "*****9123"}, {"username": "[redacted]", "name": "[redacted]", "cardNumber": "*****8139"}, {"username": "[redacted]", "name": "[redacted]", "cardNumber": "*****0102"}, {"username": "[redacted]@msn.com", "name": "Sandra", "cardNumber": "*****6851"}, {"username": "[redacted]", "name": "[redacted]", "cardNumber": "*****2654"}]}
```

Redacted records from Panera's site, which let anyone search by a variety of customer attributes, including [krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/](https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/)

# Сетевая «антигигиена»

## Типовые нарушения в 9 из 10 организаций:

1. Учетные записи в открытом виде
2. Нешифрованные почтовые сообщения
3. Использование утилит для удаленного доступа
4. Применение протоколов LLMNR и NetBios
5. Ошибки в конфигурации сети
6. TOR, VPN-туннели и прочие инструменты скрытия активности в сети
7. Майнеры, торренты и онлайн-игры



- Снижение эффективности эксплуатируемых средств защиты
- Косвенное содействие развитию атаки
- Утечка конфиденциальных данных

# PT Network Attack Discovery — ЭТО ...

PT

## **PT Network Attack Discovery** —

система глубокого анализа  
сетевого трафика  
для выявления  
и расследования атак

[ptsecurity.com/ru-ru/products/network-attack-discovery/](http://ptsecurity.com/ru-ru/products/network-attack-discovery/)

- **Мониторинг сети**  
Видит все, что происходит  
в трафике в режиме  
реального времени
- **Выявление атак в реальном  
времени и в ретроспективе**  
Пополнение сигнатур  
и репутационных списков  
2 раза в неделю
- **Расследования атак**  
Хранит сырой трафик  
и 1200 параметров сессий



# PT Expert Security Center

PT



- Исследуем угрозы
- Отвечаем за экспертизу в продуктах: сигнатуры, корреляции и IoC
- Расследуем инциденты ИБ
- Оказываем экспертную поддержку при реагировании на инцидент
- Проводим threat hunting в инфраструктуре заказчика

# Открытые учетные данные

## Чем опасно:

В случае компрометации сети,  
злоумышленник сможет перехватить  
учетные данные

# Открытые учетные данные



## Чем опасно:

В случае компрометации сети, злоумышленник сможет перехватить учетные данные

## Как выявить:

Демо

# Открытые учетные данные

## Чем опасно:

В случае компрометации сети, злоумышленник сможет перехватить учетные данные

## Как устранить:

- WEB серверы: переход с протокола http на https
- LDAP: настроить клиентов на использование защищенной версии протокола Secure LDAP или Kerberos
- Почта: настроить клиенты и сервера на использование TLS
- Telnet: использовать SSH
- FTP: перейти на SFTP или FTPS



# Почта в открытом виде

## Чем опасно:

- Компрометация конфиденциальных данных
- Помощь в развитии атаки
- Сбор данных об организации в целом и о конкретных пользователях в частности

# Почта в открытом виде

## Чем опасно:

- Компрометация конфиденциальных данных
- Помощь в развитии атаки
- Сбор данных об организации в целом и о конкретных пользователях в частности

## Как выявить:

Демо

# Почта в открытом виде

## Чем опасно:

- Компрометация конфиденциальных данных
- Помощь в развитии атаки
- Сбор данных об организации в целом и о конкретных пользователях в частности

## Как устранить:

- Принудительное использование TLS
- PGP и S/MIME

# Средства удаленного доступа

## Чем опасно:

Может использоваться злоумышленниками для получения удаленного доступа к хостам внутри организации

# Средства удаленного доступа

## Чем опасно:

Может использоваться злоумышленниками для получения удаленного доступа к хостам внутри организации

## Как выявить:

Демо

# Средства удаленного доступа

## Чем опасно:

Может использоваться злоумышленниками для получения удаленного доступа к хостам внутри организации

## Как устранить:

- Разграничение прав локальных пользователей
- Whitelist для ПО (AppLocker)

# Подверженные спуфингу протоколы

## Чем опасно:

Использование протоколов LLMNR и NetBios, может поспособствовать проведению атаки MITM

# Подверженные спуфингу протоколы

PT

## Чем опасно:

Использование протоколов LLMNR и NetBios, может поспособствовать проведению атаки MITM

## Как выявить:

Демо



# Подверженные спуфингу протоколы

## Чем опасно:

Использование протоколов LLMNR и NetBios, может поспособствовать проведению атаки MITM

## Как устранить:

### 1. Отключить LLMNR

GPO: **Computer Configuration -> Administrative Templates -> Network -> DNS Client**

Значение **Turn Off Multicast Name Resolution** выставить в **enable**

### 2. Отключить NetBios

Через настройку **dhcpcmgmt.msc. Server Options** (или Scope Option)

Вкладка **Advanced -> Microsoft Windows 2000 Options -> 001 Microsoft Disable Netbios Option**  
выставить значение **0x2**

# Ошибки конфигурирования

## Чем опасно:

- Несанкционированный сетевой доступ между подсетями
- Не использование внутреннего DNS
- Наружу выставлено то, чего не должно быть

# Ошибки конфигурирования

## Чем опасно:

- Несанкционированный сетевой доступ между подсетями
- Не использование внутреннего DNS
- Наружу выставлено то, чего не должно быть

## Как выявить:

Демо

# Ошибки конфигурирования

## Чем опасно:

- Несанкционированный сетевой доступ между подсетями
- Не использование внутреннего DNS
- Наружу выставлено то, чего не должно быть

## Как устранить:

- Настройка ACL
- GPO: **User Configuration\Administrative Templates\Network\Network Connections**
- Настройка межсетевого экрана

# Соккрытие трафика

## Чем опасно:

- Снижение эффективности использования средств защиты в организации
- Потеря контроля за контентом, передаваемым вовне

## Инструменты

- VPN
- TOR
- Proxy
- etc.

# Соккрытие трафика

## Чем опасно:

- Снижение эффективности использования средств защиты в организации
- Потеря контроля за контентом, передаваемым вовне

## Как выявить:

Демо

## Инструменты

- VPN
- TOR
- Proxy
- etc.

# Соккрытие трафика

## Чем опасно:

- Снижение эффективности использования средств защиты в организации
- Потеря контроля за контентом, передаваемым вовне

## Как устранить:

- Разграничение прав локальных пользователей
- Whitelist для ПО (AppLocker)
- Настройка межсетевого экрана

## Инструменты

- VPN
- TOR
- Proxy
- etc.

# Майнеры, торренты...

## Чем опасно:

- Нагрузка на сеть и оборудование
- Риск установки ВПО



# Майнеры, торренты...

## Чем опасно:

- Нагрузка на сеть и оборудование
- Риск установки ВПО

## Как выявить:

Демо

# Майнеры, торренты...

## Чем опасно:


- Нагрузка на сеть и оборудование
- Риск установки ВПО

## Как устранить:

- Своевременное обновление AV баз
- Разграничение прав локальных пользователей
- Whitelist для ПО (AppLocker)

# Сетевая гигиена

1. Учетные записи в открытом доступе
2. Нешифрованные почтовые сообщения
3. Использование утилит для удаленного доступа
4. Применение протоколов LLMNR и NetBios
5. Ошибки в конфигурации сети
6. TOR, VPN-туннели и прочие инструменты скрытия активности в сети
7. Майнеры, торренты и онлайн-игры

- 
- Минимизировать использование открытых протоколов
  - Контролировать разграничение сетевого доступа
  - Разграничивать права пользователей

# Что дальше

## 1 Пилот PT Network Attack Discovery

с отчетом от PT Expert Security Center:

- Ошибки в сетевой безопасности в вашей компании
- Внутренние атаки
- Внутрисетевая активность злоумышленников

[ptsecurity.com/ru-ru/products/network-attack-discovery/](https://ptsecurity.com/ru-ru/products/network-attack-discovery/)

## 2 Welcome to PHDays!

Живая работа продуктов PT в условиях, максимально приближенных к реальности:

- MaxPatrol SIEM
- PT Network Attack Discovery
- PT MultiScanner
- PT Application Firewall

[phdays.com](https://phdays.com)



**Спасибо**

**за внимание!**

[adanilin@ptsecurity.com](mailto:adanilin@ptsecurity.com)  
[alednyov@ptsecurity.com](mailto:alednyov@ptsecurity.com)

[ptsecurity.com](http://ptsecurity.com)