positive technologies

PT KNOCKIN

PT SANDBOX

ВРЕДОНОСНОЕ ПО: ИССЛЕДОВАНИЕ ПОВЕДЕНИЯ И КАНАЛОВ РАСПРОСТРАНЕНИЯ

PT SANDBOX
SANDBOX PT
PT SANDBOX
SANDBOX PT
PT SANDBOX
SANDBOX PT
PT SANDBOX
SANDBOX PT

СОДЕРЖАНИЕ

ЦЕЛИ И МЕТОДЫ ИССЛЕДОВАНИЯ

Вредоносные программы наносят значительный ущерб пользователям и организациям. Они зашифровывают либо удаляют важные данные, крадут учетные данные аккаунтов в различных сервисах, интернет-банкинге или криптовалютных кошельков, останавливают работу компаний.

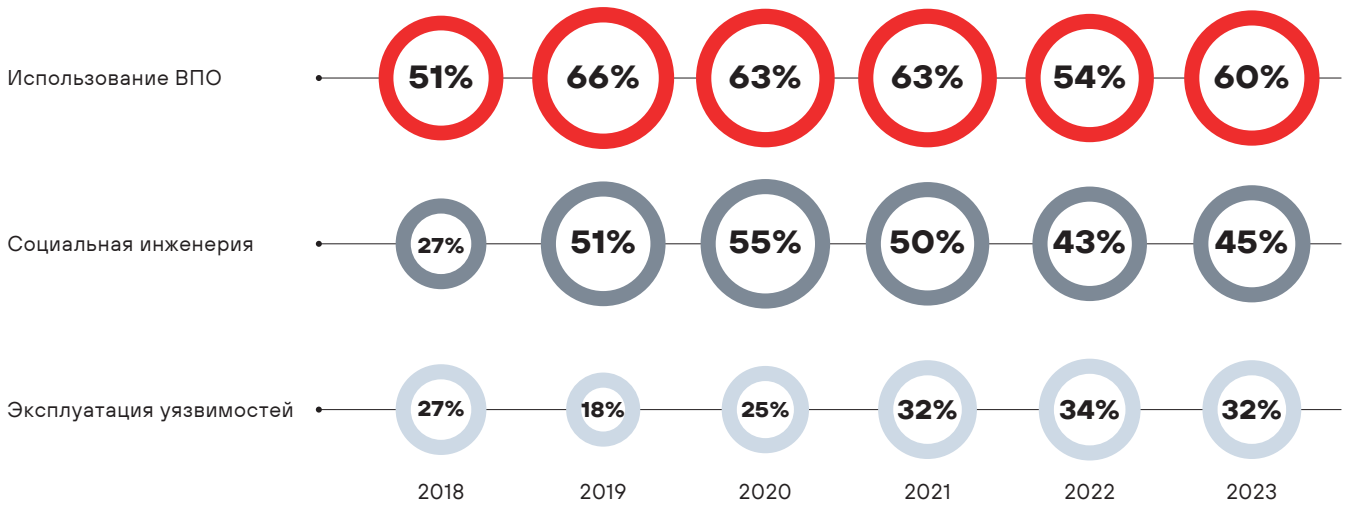


Рисунок 1. Частота использования различных методов атак с 2018 по 2023 год

Одна из причин популярности ВПО (вредоносное программное обеспечение) — относительная простота в использовании и распространении. Злоумышленники могут создавать и распространять его с невысокими затратами и минимальными усилиями. Кроме того, ВПО обеспечивает атакующему большую вариативность действий в ходе атаки.

Существует множество каналов распространения вредоносного ПО, многие из них основаны на человеческом факторе. Например, это фишинговые атаки с использованием электронной почты, вредоносных веб-сайтов и социальных сетей.

Цели этого исследования — установить:

- самые популярные у злоумышленников типы ВПО;
- каналы, по которым злоумышленники доставляют вредоносы;
- принципы действия вредоносных программ;
- соотношение этих действий с техниками MITRE ATT&CK[1] 1.

Мы также предложим меры, которые помогут защититься от атак с использованием вредоносов.

Исследование основано на публичных сведениях об инцидентах ИБ, собственной экспертизе Positive Technologies, результатах анализа вредоносного ПО продуктом PT Sandbox на территории РФ, а также на других исследованиях авторитетных источников.

ВПО в 2023 г.
Цифры и факты

60% атак основаны на использовании ВПО. Это самый популярный метод преодоления периметра компании

57% атак с применением ВПО приходится на шифровальщики. Это наиболее распространенный тип вредоносного ПО

18% атак, реализуемых с помощью программ-вымогателей, приходится на медицинские учреждения. Это самая атакуемая отрасль

57% атак с применением ВПО реализованы через электронную почту. Это самый популярный способ распространения ВПО

56% атак через почту реализованы с помощью файловых вложений с вредоносным содержимым. Это наиболее распространенный вид вредоносной нагрузки

1

[1] MITRE ATT&CK — это база знаний с открытым исходным кодом о тактиках и методах противника, основанная на реальных наблюдениях. ATT&CK предоставляет общую таксономию тактик и техник для лучшей классификации поведения противника.

СОВРЕМЕННОЕ ВПО: КАКОЕ ОНО?

Данные на рис. 2 свидетельствуют о том, что атаки с применением вредоносов в 2023 году являлись наиболее распространенным методом.

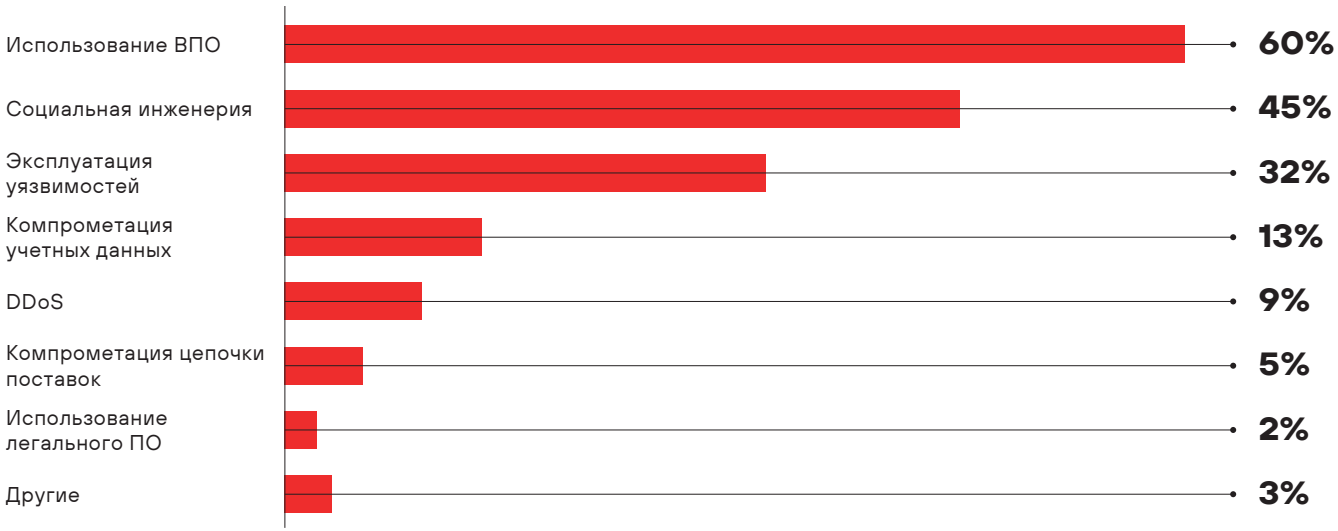


Рисунок 2. Методы атак (доля успешных атак, 2023 год) [2]

Существует несколько видов вредоносных программ:

- **Вымогательское ПО (ransomware)** — программы для блокировки доступа пользователей к данным путем шифрования отдельных файлов или файловой системы в целом. Обычно доступ возвращается после выплаты злоумышленникам выкупа в цифровой валюте, однако известны случаи, когда файлы так и не были расшифрованы.

- **Шпионское ПО (spyware)** — средства для скрытного отслеживания действий пользователей системы и кражи различной конфиденциальной информации, например учетных записей, финансовых данных, данных криптокошельков.

- **ВПО для удаленного управления (remote access trojan, RAT)** — программы для управления устройством, на которое они были установлены. Такое ВПО может быть использовано для кражи, изменения или удаления информации на устройстве, а также служить точкой входа в сеть и использоваться для дальнейшего развития атаки. Важно отметить, что большинство троянов удаленного доступа имеют функции шпионского ПО — такие программы умеют скрытно записывать экран пользователя и определять его местоположение, регистрировать ввод данных с клавиатуры.

- **Загрузчики (downloader)** — вспомогательное ПО для загрузки дополнительных компонентов с управляющих серверов злоумышленника или сторонних интернет-ресурсов. В качестве загрузчика могут быть использованы легитимные утилиты, с которыми обычно работают администраторы сети. Это позволяет замаскировать вредоносные действия и скрыть присутствие злоумышленника в сети.

- **Майнеры (miner)** — программы, использующие аппаратные мощности устройства для добычи криптовалюты. Такие вредоносы работают скрытно и имеют функции для маскировки своей деятельности и предотвращения обнаружения.

- **Банковские трояны (banking trojan)** — программы, разработанные специально для кражи с устройства финансовой информации и учетных данных банковских приложений и сервисов.

- **Рекламное ПО (adware)** — программы, которые отображают нежелательную или даже вредоносную рекламу на экране зараженного устройства. Кроме того, такие утилиты умеют перенаправлять результаты поиска на рекламные сайты и собирать данные пользователей, которые впоследствии будут отправлены рекламодателям без согласия этих пользователей[3].

Виды вредоносных программ:

- Вымогательское ПО (ransomware)
- Шпионское ПО (spyware)
- ВПО для удаленного управления (remote access trojan)
- Загрузчики (downloader)
- Майнеры (miner)
- Банковские трояны (banking trojan)
- Рекламное ПО (adware)

[2] В рамках одной атаки могли быть использованы как один, так и несколько методов.

[3] Не все рекламные программы являются вредоносными, некоторые из них легальны и безопасны для использования.

Популярность ВПО среди злоумышленников обусловлена низким порогом вхождения: многие программы продаются в даркнете за относительно небольшие суммы или даже распространяются на бесплатной основе, часто с подробной инструкцией. Популярна бизнес-модель «Вредоносное ПО как услуга» (malware-as-a-service, MaaS): злоумышленники предоставляют своим партнерам доступ к ВПО и инфраструктуре за определенную плату. Есть несколько вариантов оплаты: единоразовая покупка ВПО, оформление подписки на определенный срок или выплата процента от прибыли (например, доли от выкупа) в случае проведения успешной атаки.

По нашим данным, в 2023 году среди используемых типов ВПО лидировали программы-шифровальщики (см. рис. 3). Кроме того, по сравнению с 2022 годом доля успешных атак на организации с их участием выросла[2] с 54 до 57%.

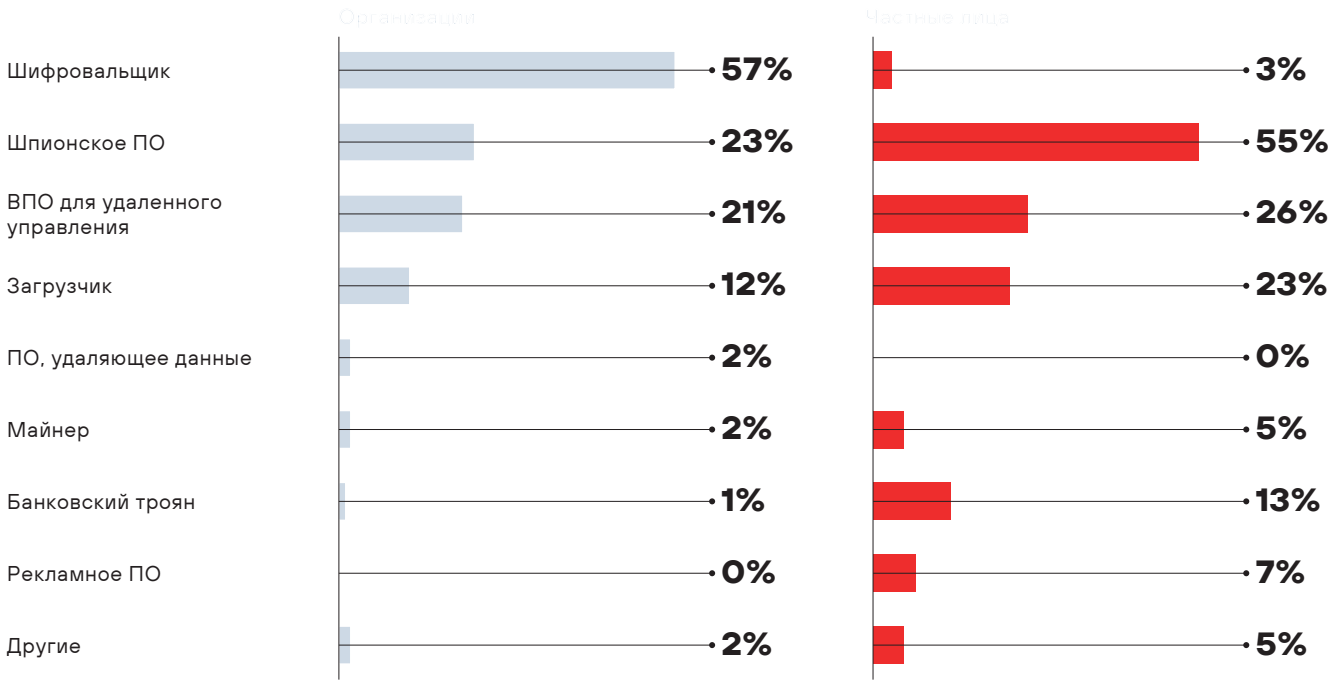


Рисунок 3. Типы вредоносного ПО (доля успешных атак с использованием ВПО, 2023 год)

В 2023 году атакам с использованием шифровальщиков наиболее часто подвергались медицинские учреждения: атаки на них составили 18% от общего числа. Организации в сфере науки и образования оказались на втором месте с долей 14%, промышленные организации заняли третье место с 12% от общего числа атак.

Рисунок 4. Категория жертв среди организаций (доля успешных атак с использованием вымогательского ПО, 2023 год)

Один из самых распространенных шифровальщиков, используемых в атаках на организации, — LockBit. LockBit распространяется по модели RaaS (ransomware-as-a-service — одна из разновидностей модели MaaS) и отличается широкой партнерской программой. Решение кросс-платформенное, поэтому опасно для компьютеров на базе ОС Windows, macOS, Linux и других, менее распространенных операционных систем. Стоит отметить, что любой тип вредоносного ПО может быть написан в кросс-платформенном исполнении. Это опровергает устоявшийся миф о том, что в опасности только пользователи ОС Windows.

Цена на ВПО
(на основе анализа сообщений в дарквебе)

От 50 до 80 000 долл. США

50 долл. США — стилер с функционалом кражи данных из браузеров, cookie, истории, паролей, а также файлов с компьютера

500 долл. США — drainer[4], dropper[5] или reverse shell[6]

500 – 80 000 долл. США — покупка загрузчика (downloader), от 1500 долл. США в месяц — его аренда

6000 долл. США — готовое ВПО для банков, банкоматов и POS-терминалов

От 10 000 долл. США — разработка индивидуального шпионского ПО под конкретные цели

Стоимость разработки вредоносного ПО под заказ в десятки раз выше, чем покупка готового вредоноса, так как от разработчика требуются специфические знания о сетевых технологиях и операционных системах, а также в других областях

Также выросла популярность шпионского ПО: с 12 до 23% (организации), с 44 до 51% (частные лица). Такие программы умеют скрытно записывать экран пользователя и определять местоположение устройства, регистрировать ввод данных с клавиатуры и многое другое.

Одни из наиболее распространенных представителей данного типа ВПО — AgentTesla и Formbook. AgentTesla — это ВПО для удаленного доступа, впервые замеченное еще в 2014 году. Изначально это был обычный кейлоггер, собиравший введенную с клавиатуры информацию, однако с тех пор ПО подверглось значительным изменениям и усовершенствованиям. Сейчас AgentTesla может делать снимки экрана рабочего стола пользователя, записывать нажатия клавиш на клавиатуре, регистрировать нажатия клавиш виртуальной клавиатуры, красть данные из буфера обмена, собирать учетные данные из различных приложений (например, Google Chrome, Mozilla Firefox, Microsoft Outlook, IceDragon и FileZilla), делать снимки с помощью веб-камеры пользователя и автоматически переносить свои копии на USB-накопители, чтобы распространять их среди других компьютеров.

FormBook — вредоносное ПО, впервые обнаруженное в 2016 году. Средство крадет различные типы данных из зараженных систем, включая учетные данные, кэшированные в веб-браузерах, снимки экрана и нажатия клавиш. Оно также может выступать в качестве загрузчика, что позволяет ему загружать и запускать дополнительные вредоносные файлы. FormBook работает по модели MaaS.

[4] Drainer — набор инструментов для кражи средств с криптокошельков.

[5] Dropper — ВПО, предназначенное для доставки и скрытой установки на зараженное устройство другого вредоносного ПО.

[6] Reverse shell — инструмент для создания обратной оболочки и управления скомпрометированным устройством.

ПРИМЕРЫ АТАК С ИСПОЛЬЗОВАНИЕМ LOCKBIT

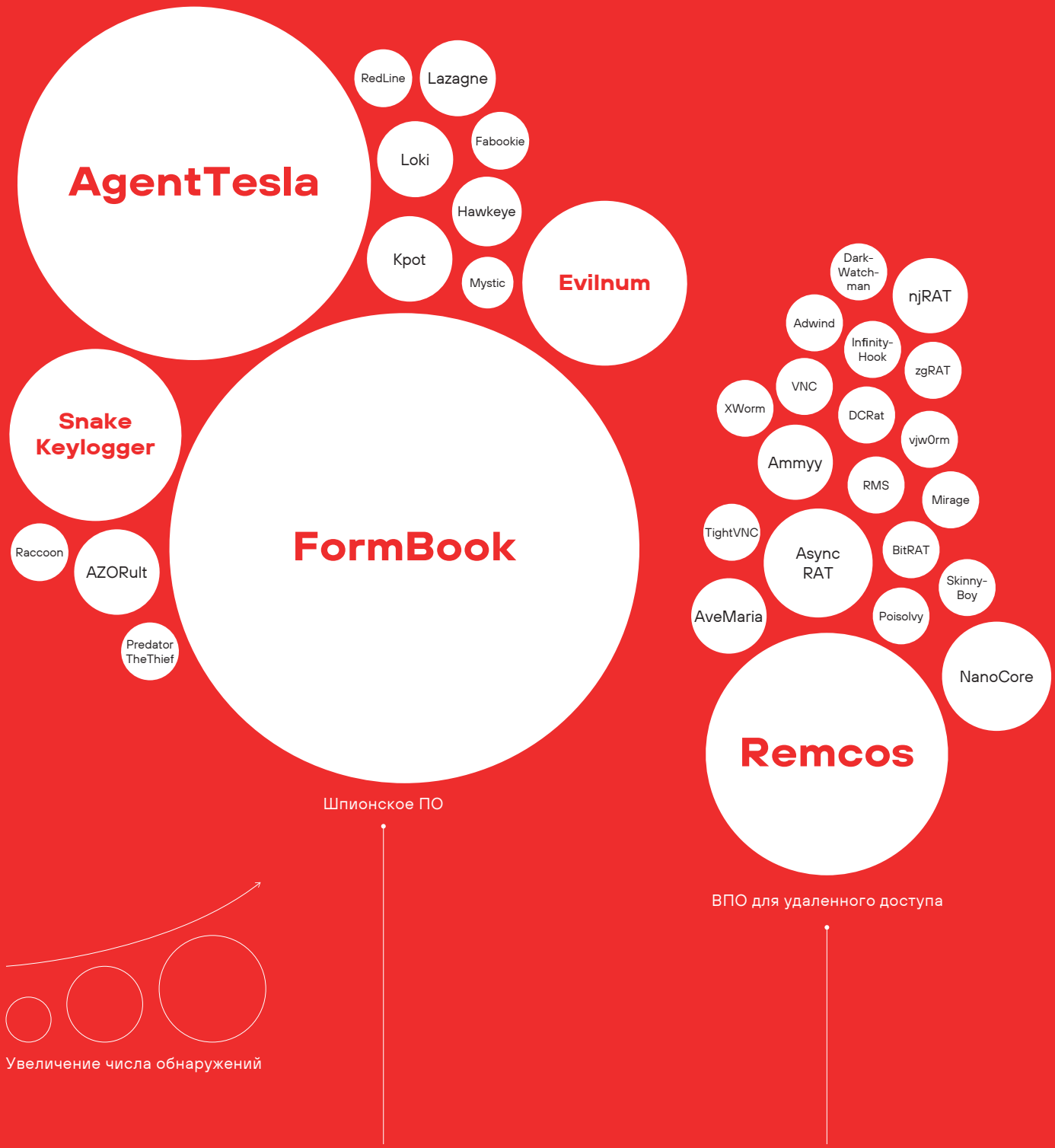
РАСПРОСТРАНЕННЫЕ СЕМЕЙСТВА ВПО И ИХ ПОВЕДЕНИЕ

Продукт PT Sandbox проанализировал в изолированной среде вредоносные программы, используемые на территории РФ, и их поведение. На основании этих данных были выявлены наиболее часто встречающиеся семейства ВПО (см. рис. 5). Прослеживается региональная специфика, а именно: наиболее часто встречаются представители шпионского ВПО, в частности уже упомянутые семейства FormBook и AgentTesla; шифровальщики используются значительно реже.

Благодаря полученным данным удалось выявить наиболее часто наблюдаемое поведение вредоносов и отразить его на матрицу MITRE ATT&CK (см. рис. 6). В то время как тактика определяет цель, которой пытается достичь противник, техника показывает, как именно злоумышленник достигает ее, выполняя то или иное действие. Компания Positive Technologies перевела[3] бóльшую часть матрицы MITRE на русский язык и продолжает адаптировать данный инструмент.

[3]

Рисунок 5. Основные семейства ВПО, обнаруженные PT Sandbox



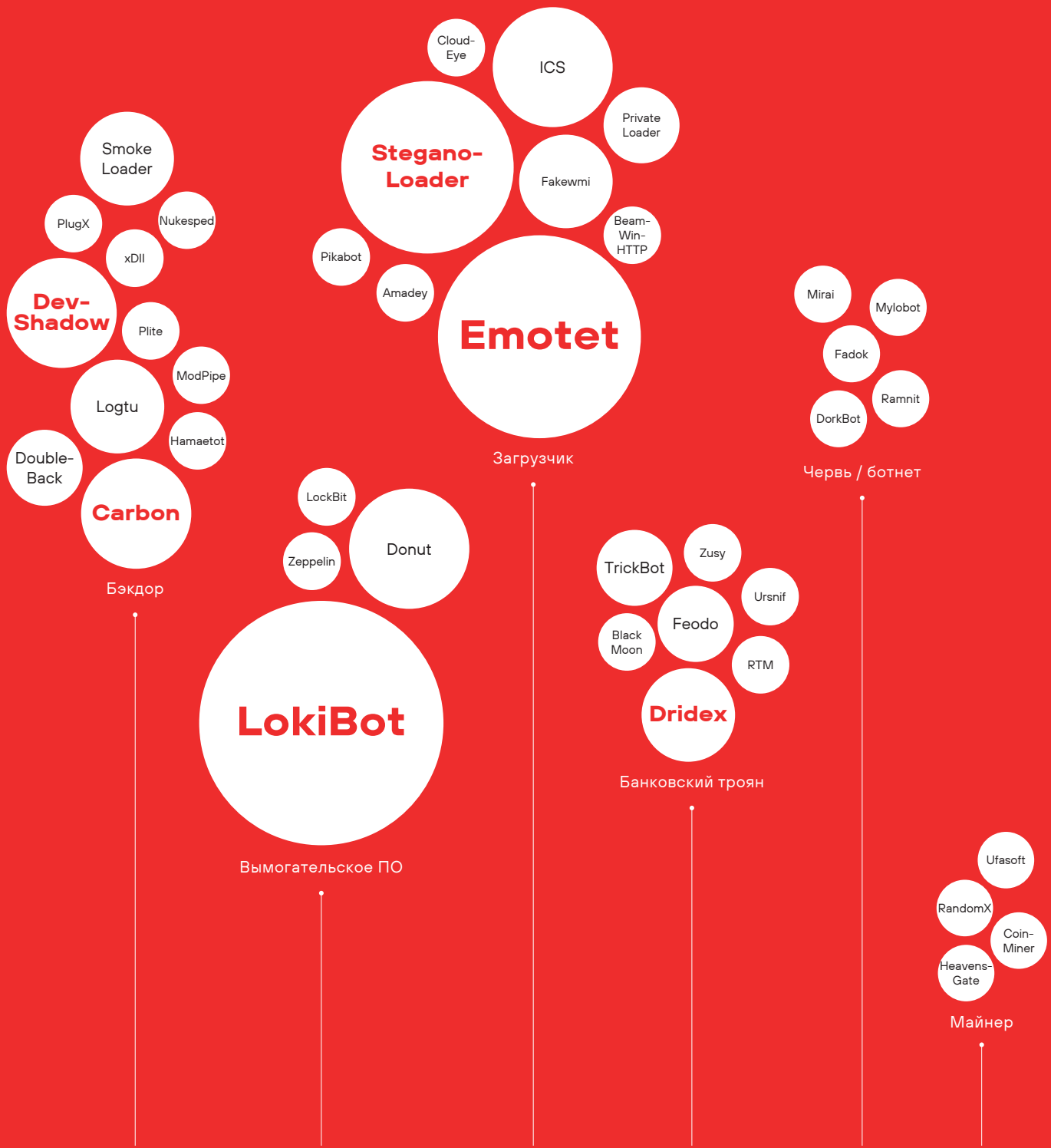

Cloud-Eye
ICS
Private Loader
Stegano-Loader
Fakewmi
Beam-Win-HTTP
Pikabot
Amadey
Emotet
Загрузчик
Smoke Loader
PlugX
Nukesped
xDll
Dev-Shadow
Plite
ModPipe
Logtu
Hamaetot
Double-Back
Carbon
Бэкдор
Mirai
Mylobot
Fadok
Ramnit
DorkBot
Червь / ботнет
LockBit
Donut
Zeppelin
LokiBot
Вымогательское ПО
TrickBot
Zusy
Ursnif
Feodo
Black Moon
RTM
Dridex
Банковский троян
Ufasoft
RandomX
Coin-Miner
Heavens-Gate
Майнер

Рисунок 6. Тепловая карта техник MITRE ATT&CK

Тактика	Техника				
Initial Access	T1091 Replication Through Removable Media				
Execution	T1106 Native API	T1047 Windows Management Instrumentation	T1559 Inter-Process Communication	T1129 Shared Modules	T1204 User Execution
Persistence	T1068 Account Manipulation	T1137 Office Application Startup	T1546 Event Triggered Execution	T1543 Create or Modify System Process	T1136 Create Account
Privilege Escalation	T1068 Exploitation for Privilege Escalation				
Defence Evasion	T1574 Hijack Execution Flow	T1497 Virtualization/Sandbox Evasion	T1622 Debugger Evasion	T1006 Direct Volume Access	T1202 Indirect Command Execution
	T1112 Modify Registry	T1564 Hide Artifacts	T1036 Masquerading	T1211 Exploitation for Defense Evasion	T1027 Obfuscated Files or Information
	T1620 Reflective Code Loading				
Credential Access	T1555 Credentials from Password Stores	T1556 Modify Authentication Process	T1003 OS Credential Dumping	T1552 Unsecured Credentials	
Discovery	T1057 Process Discovery	T1016 System Network Configuration Discovery	T1518 Software Discovery	T1135 Network Share Discovery	T1 007 System Service Discovery
	T1082 System Information Discovery	T1083 File and Directory Discovery	T1010 Application Window Discovery	T1120 Peripheral Device Discovery	T1201 Password Policy Discovery
Lateral Movement	T1021 Remote Services	T1563 Remote Service Session Hijacking			
Collection	T1560 Archive Collected Data	T1025 Data from Removable Media	T1119 Automated Collection	T1123 Audio Capture	T1115 Clipboard Data
Command and Control	T1219 Remote Access Software	T1205 Traffic Signaling			
Exfiltration	T1048 Exfiltration Over Alternative Protocol				
Impact	T1490 Inhibit System Recovery	T1531 Account Access Removal	T1529 System Shutdown/ Reboot	T1561 Disk Wipe	T1485 Data Destruction

> 500 000 срабатываний 100 000 – 500 000 срабатывыний 10 000 – 100 000 срабатываний

T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter	T1569 System Services	T1053 Scheduled Task/Job	
T1176 Browser Extensions	T1547 Boot or Logon Autostart Execution	T1037 Boot or Logon Initialization Scripts		

T1553 Subvert Trust Controls	T1548 Abuse Elevation Control Mechanism	T1218 System Binary Proxy Execution	T1222 File and Directory Permissions Modification	T1055 Process Injection
T1562 Impair Defenses	T1140 Deobfuscate/Decode Files or Information	T1134 Access Token Manipulation	T1197 BITS Jobs	T1070 Indicator Removal

T1069 Permission Groups Discovery	T1613 Container and Resource Discovery	T1018 Remote System Discovery	T1087 Account Discovery	T1614 System Location Discovery
T1012 Query Registry	T1217 Browser Information Discovery	T1049 System Network Connections Discovery		

T1056 Input Capture	T1113 Screen Capture

T1489 Service Stop	T1499 Endpoint Denial of Service	T1565 Data Manipulation

1000 – 10 000 срабатываний < 1000 срабатываний

Мы выявили десять наиболее популярных техник, выполняемых вредоносными программами:

1. T1010 Изучение открытых приложений

Как реализуется

Вредоносное ПО пытается получить список открытых окон приложений. Список окон позволяет определить потенциальные данные для сбора, а также собрать информацию об инструментах безопасности (Security Software Discovery), которые следует обойти.

Пример

Троян удаленного доступа njRAT собирает информацию об открытых окнах во время первичного заражения.

2. T1562 Ослабление защиты

Как реализуется

ВПО может модифицировать компоненты среды жертвы, чтобы нарушить работу защитных механизмов или отключить их. Это включает в себя не только ослабление превентивных средств защиты, таких как межсетевые экраны, IPS и антивирусы, но и функций обнаружения, которые могут использоваться для аудита активности и выявления вредоносного поведения. Это может затрагивать как штатные средства защиты, так и дополнительные возможности, установленные пользователями и администраторами.

Пример

Вредоносное ПО TangoDelta из семейства Lazarus Group пытается завершить различные процессы, связанные со средствами защиты от McAfee. Кроме того, вредоносное ПО SHARPKNOT из того же семейства отключает службы уведомлений и предупреждений о системных событиях Microsoft Windows.

3. T1497 Обход виртуализации или песочницы

Как реализуется

Вредоносные программы могут использовать различные средства для обнаружения и обхода сред виртуализации и песочниц. Установив наличие артефактов, указывающих на среду виртуальной машины (VME) или песочницу, программа может изменить свое поведение, чтобы скрыть вредоносную сущность. Также ВПО может искать артефакты VME перед сбросом вторичных или дополнительных полезных данных. Для обхода виртуализации или песочницы могут использоваться различные методы, такие как проверка наличия средств мониторинга безопасности (например, Sysinternals, Wireshark и другие). ВПО может проверять и действия легитимных пользователей, чтобы определить, находится ли система в виртуальной среде. Чтобы вредоносное ПО не обнаружили во временной песочнице, злоумышленники могут использовать таймеры и циклы в его коде.

Пример

ВПО для удаленного управления EvilBunny продолжает работу только в том случае, если в среде запущено не менее 15 процессов.

4. T1057 Изучение процессов

Как реализуется

Вредоносные программы часто пытаются получить информацию о процессах, которые запущены на компьютере или сетевом устройстве. Эта информация помогает понять, какие программы и приложения используются на компьютерах внутри сети. Получив эти данные, ВПО может выбирать варианты дальнейшего развития атаки, в том числе заражать ли целевой компьютер полностью или выполнить только определенный список действий, например, для дальнейшего распространения в сети. Для получения этой информации вредоносы могут использовать утилиту *tasklist*, запустив ее в Windows через командную строку *(cmd)* или оболочку *PowerShell*, а на устройствах с MacOS и Linux — с помощью специальных команд. Также они могут проверить процессы на сетевых устройствах, например, через команду командной строки (CLI) *show processes*.

Пример

ВПО Brute Ratel C4 может перечислять все процессы и находить определенные идентификаторы процессов (PID).

5. T1016 Изучение конфигурации сети

Как реализуется

Вредоносное ПО способно искать информацию о конфигурации сети и сетевых настройках, таких как IP- и (или) MAC-адреса компьютеров, к которым они получили доступ, или о системах на удаленных устройствах. Для этого они могут использовать различные утилиты администрирования ОС, например *arp, ipconfig/ifconfig, nbtstat* и *route*. Кроме того, вредоносные программы умеют обращаться к интерфейсу командной строки сетевых устройств для получения сведений об их настройках, таких как IP-адреса настроенных интерфейсов и статические или динамические маршруты. Для этого могут использоваться команды *show ip route* и *show ip interface*. Информация, полученная в результате обнаружения сетевой конфигурации системы, может быть использована вредоносами для дальнейших автоматических действий, включая определение доступа внутри целевой сети и планирование следующих шагов.

Пример

Вредоносное ПО Empire может получать сведения о конфигурации сети — например, информацию о DNS-серверах и сетевых прокси-серверах, используемых хостом, публичные IP-адреса

6. T1529 Завершение работы или перезагрузка системы

Как реализуется

ВПО способно выключать или перезагружать зараженные компьютеры или сетевые устройства, для того чтобы нарушить доступ к ним или даже вывести их из строя. Обычно ОС предоставляют специальные команды для выполнения таких действий. Иногда эти команды можно использовать

даже для удаленного выключения либо перезагрузки компьютеров или серверов с помощью интерфейса командной оболочки, а также сетевых устройств через их интерфейс командной строки.

Подобные действия могут создать проблемы для легитимных пользователей, лишая их доступа к ресурсам зараженного устройства. Кроме того, выключение или перезагрузка могут затруднить процессы реагирования на инциденты и восстановления после атаки. Вредоносы могут использовать выключение или перезагрузку системы в сочетании с другими действиями, например удалением данных с диска или блокированием возможности восстановления системы, чтобы ускорить нарушение доступности системы.

Пример

ВПО Shamoon перезагружает зараженную систему после того, как завершается функция удаления данных.

7. T1059 Интерпретаторы командной строки и сценариев

Как реализуется

ОС предоставляют пользователям встроенные интерфейсы командной строки. Например, в macOS и дистрибутивах Linux есть Unix shell, а в Windows — Command shell и PowerShell. Также есть кросс-платформенные языки программирования, например Python, а также языки, часто используемые в клиентских приложениях, например JavaScript и Visual Basic. Вредоносное ПО может использовать эти инструменты для выполнения различных команд и скриптов как способа запуска произвольных действий. Команды и сценарии могут быть встроены в первоначальную полезную нагрузку, которая доставляется жертвам, например, через фишинговые документы, или могут быть частью полезной нагрузки, загружаемой из уже зараженных систем. Они могут выполнять команды через интерактивные терминалы и оболочки, а также использовать различные удаленные сервисы для выполнения команд на удаленных компьютерах.

Пример

ВПО Fox Kitten использует обратную оболочку Perl для связи с C&C-серверами.

8. T1053 Запланированная задача (задание)

Как реализуется

Большинство ОС имеют утилиты для запланированного выполнения программ или сценариев в определенные дату и время. Кроме того, запланировать выполнение задачи можно на удаленной системе при наличии определенных прав доступа (например, через RPC и общий доступ к файлам и принтерам в среде Windows). Чтобы запланировать задачу на удаленной системе, обычно нужно принадлежать к администраторской или другой привилегированной группе на удаленном устройстве. ВПО может использовать функционал планирования задач для выполнения вредоносного кода, например, при старте системы или по определенному расписанию для обеспечения регулярного запуска вредоносных действий. Кроме того, механизм планирования задач может быть использован для их запуска от имени указанной учетной записи (например, с более высокими привилегиями). Еще один вариант использования данной технологии — маскировка одноразового выполнения команд под доверенный системный процесс.

Пример

Планировщик задач часто используется рекламным ВПО, для того чтобы усложнить его удаление с зараженного устройства.

9. T1012 Запросы к реестру

Как реализуется

Реестр Windows содержит много информации об ОС, ее настройках, установленных программах и параметрах безопасности. Для получения этих данных часто используется утилита *reg*, но есть и другие способы доступа к реестру. Вредоносная программа может обращаться к реестру для получения информации о системе, ее конфигурации и установленном ПО. Эта информация может помочь злоумышленникам в их дальнейших действиях в сети. Например, она поможет решить, является ли захваченное устройство целевым и стоит ли его заражать или лучше использовать его как промежуточный узел для дальнейшего перемещения по сети.

Пример

Троян удаленного доступа gh0st RAT умеет проверять наличие сервисного ключа в реестре, чтобы определить, был ли он ранее установлен в системе.

10. T1547 Автозапуск при загрузке или входе в систему

Как реализуется

ОС имеют механизмы автоматического запуска программы при загрузке системы или входе в учетную запись. Эти механизмы могут включать в себя автоматический запуск программ, которые размещены в определенных каталогах или указаны в реестре Windows, где хранится информация о настройках системы. Злоумышленники могут добиться того же эффекта, модифицируя или расширяя функционал ядра ОС. Вредоносное ПО может внести в список автозагрузки себя или другое ВПО для обеспечения постоянного присутствия в системе. Это может быть сделано, например, путем добавления ссылки на свою программу в реестр Windows или в другие системные каталоги. Кроме того, поскольку некоторые программы, которые запускаются автоматически при загрузке системы или входе в учетную запись, работают с повышенными привилегиями, злоумышленники могут использовать их для повышения привилегий.

Пример

ВПО xCaon после установки на зараженное устройство добавляет запись о себе в раздел реестра, в котором хранится список автозапуска.

Таким образом, ВПО использует легитимные функции ОС:

- **для проведения разведки: изучение открытых приложений, процессов, конфигурации сети;**
- **для выполнения вредоносных действий: обход виртуализации или песочницы, интерпретаторы командной строки и сценариев, запросы к реестру;**
- **для закрепления на захваченном устройстве: ослабление защиты, завершение работы или перезагрузка системы, запланированная задача (задание), автозапуск при загрузке или входе в систему.**

ЭЛЕКТРОННАЯ ПОЧТА КАК СПОСОБ РАСПРОСТРАНЕНИЯ ВПО

Есть несколько наиболее популярных способов доставки вредоносных программ в сеть организации. В 2023 году ВПО чаще всего доставлялось через электронную почту (больше половины успешных случаев атак с использованием вредоносов) (см. рис. 7).

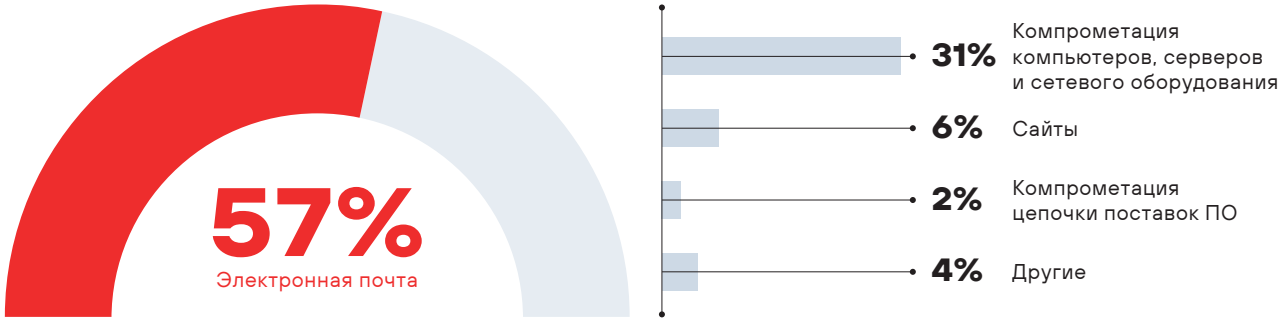


Рисунок 7. Способы распространения ВПО (организации)

Несмотря на то что этот метод доставки ВПО уже давно известен, пользователи продолжают открывать неизвестные файлы, кликать по ссылкам и картинкам. Кроме того, злоумышленники часто маскируют фишинговые письма под легитимные и опираются на эмоции людей — страх, жадность, любопытство и желание помочь. Например, увидев письмо с пометкой «срочно», пользователь забеспокоится, что не успеет что-то сделать, в спешке откроет вредоносное вложение и заразит свою рабочую станцию. Другой пример: злоумышленники присылают уведомление о недошедшем письме, в котором содержится информация об отпусках, зарплатах или платежах. Это те сведения, которые рядовой сотрудник знать не должен, но из любопытства захочет с ними ознакомиться. Так, эксперты Positive Technologies обнаружили у одного клиента рассылку писем под видом претензии с требованием возврата средств.

МЕТОДЫ СОКРЫТИЯ ВРЕДОНОСНОЙ ПОЛЕЗНОЙ НАГРУЗКИ

Для доставки вредоносной полезной нагрузки злоумышленники обычно используют файловые вложения, приложенные к письмам, ссылки в теле письма, а также QR-коды. В настоящее время наиболее популярным методом являются файловые вложения (более половины успешных случаев) (см. рис. 8).

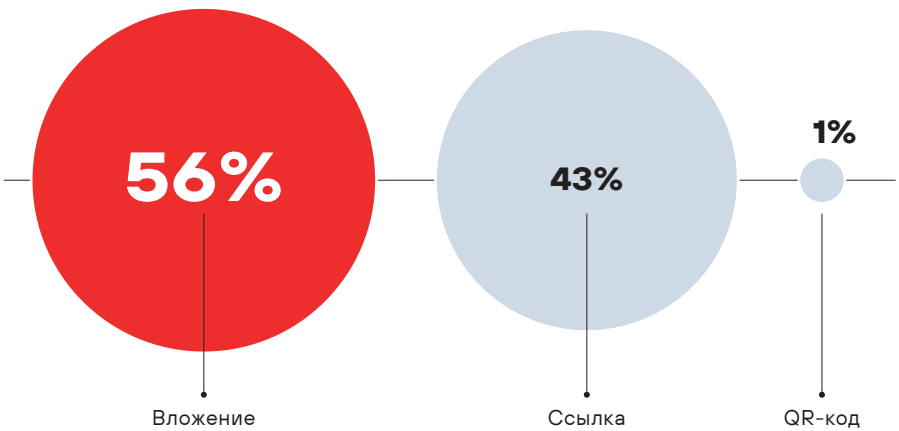


Рисунок 8. Виды вредоносной нагрузки

Самые распространенные типы отправляемых файлов — это архивы (форматы .zip, .rar, .7z и подобные). В них злоумышленники могут легко скрыть вредоносное ПО от средств проверки безопасности, маскируя его под безобидные документы или изображения. Поскольку многие сотрудники регулярно используют архивы для обмена файлами или хранения данных, получение архивированных вложений не вызывает у них подозрений.

Тренды фишинговых атак на организации в 2022—2023 годах

Вредоносное ПО в корпоративной сети: угрозы и способы обнаружения

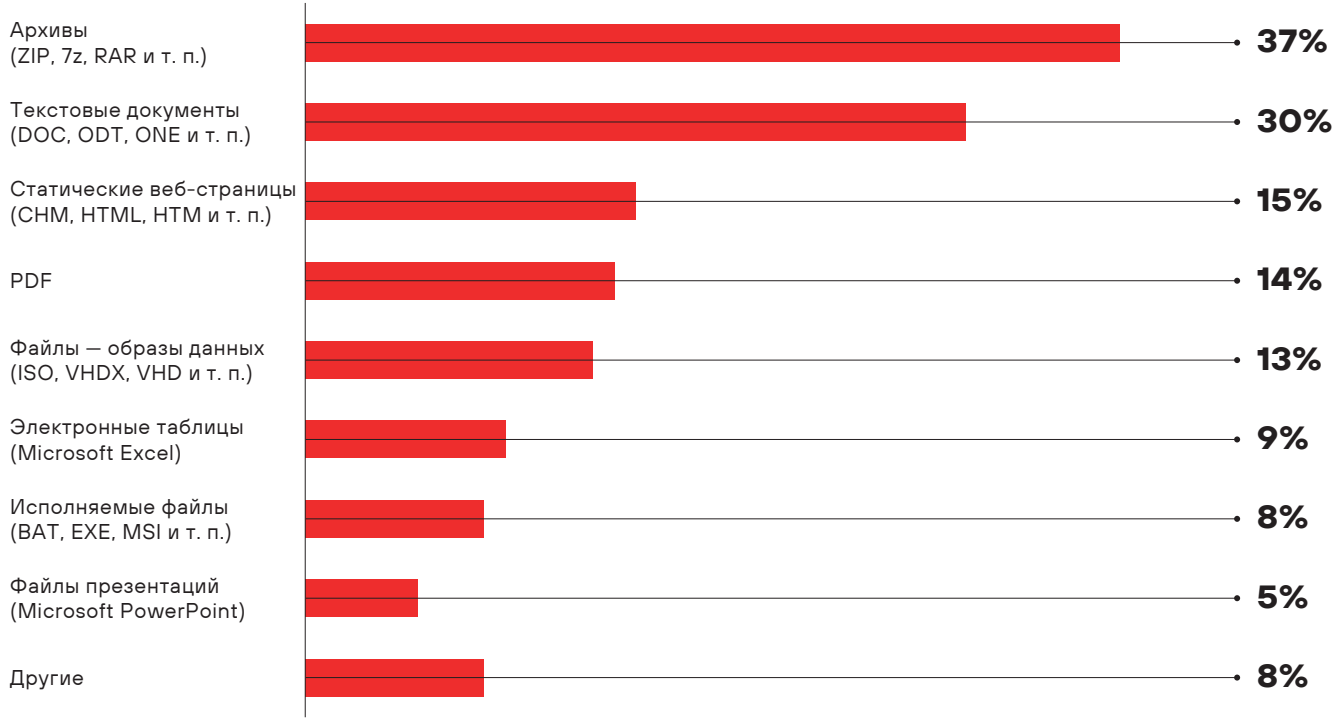


Рисунок 9. Расширения вредоносных файлов

Согласно исследованию, довольно часто вложениями фишинговых писем являются статические веб-страницы (файлы с расширениями .html, .htm и другие). Они могут быть как поддельными формами ввода персональных или учетных данных, так и частью атак с использованием HTML-контрабанды. Она основана на принципе сокрытия вредоносного кода внутри безобидных данных, таких как строки, изображения или другие типы контента, которые могут передаваться по сети. Злоумышленник создает полезную нагрузку, которая кодирует вредоносный HTML-код, что делает его безопасным для действующих механизмов обеспечения ИБ. Когда пользователь открывает зараженную страницу в браузере, инициируется выполнение скрытого вредоносного кода, который собирает полезную нагрузку на устройстве.

Довольно часто в фишинговых атаках встречались файлы с расширениями обычных офисных таблиц и документов — таких как .doc, .pdf, .xls и .pptx. Такие вложения, как правило, не вызывают подозрений у пользователя. Одна из техник — внедрение в офисные документы скриптов с вредоносной полезной нагрузкой, которые при активации в фоновом режиме загружают и разворачивают ВПО. Кроме того, в отчете[4] об актуальных киберугрозах за 3-й квартал 2023 года мы рассказывали, что злоумышленники стали чаще использовать .pdf-документы в фишинговых атаках, встраивая в них вредоносные ссылки, дополнительно маскируя их с помощью QR-кодов. Еще одно нововведение в фишинге с помощью PDF-файлов — использование техники MalDoc[5] (встраивание word-файлов в документ формата PDF). Суть в том, что передаваемое вложение имеет формат .pdf, однако открываться оно будет в редакторе текстовых файлов Word, что вызовет срабатывание вредоносных макросов и загрузку полезной нагрузки.

Если говорить о ссылках, то при переходе по ним происходит автоматическая загрузка ВПО в фоновом для пользователя режиме. Чтобы избежать обнаружения средствами защиты, злоумышленники могут реализовать несколько последовательных переадресаций с одного ресурса на другой. Но в конечном счете это приведет на страницу загрузки вредоноса. Еще один способ — использование домена .zip, который с недавнего времени доступен для покупки. Доменное имя с таким расширением может запутать пользователя, особенно если у него нет технических знаний. Так, например, имя сайта outlook365update[.]zip выглядит как вполне легитимное. Кроме того, чтобы наверняка избежать обнаружения вредоносной ссылки, злоумышленники могут приложить к письму QR-код, который поможет скрыть вредоносные URL-адреса от получателей и систем защиты. Эти средства используют не только для загрузки вредоносного ПО на устройство жертвы, но и для получения учетных данных.

Самые популярные типы файловых вложений, используемых для доставки вредоносной полезной нагрузки:

- **Архивы** (форматы .zip, .rar, .7z и подобные). Это самый популярный тип вложений
- **Статические веб-страницы** (файлы с расширениями .html, .htm и другие)
- **Файлы с расширениями офисных таблиц и документов** (.doc, .pdf, .xls, .pptx и другие)

4

5

ЧТО ПОМОЖЕТ ЗАЩИТИТЬСЯ ОТ ВПО

1. Проверка файлов в виртуальной среде

Обязательным уровнем защиты от вредоносных программ являются решения класса «песочница». Они не только проверяют файлы и ссылки статическими методами на основе сигнатур, но и используют поведенческий анализ в изолированной среде для запуска файлов и исследования их поведения.

6

Песочница PT Sandbox[6] позволяет выявлять вредоносные действия в файлах, которые на первый взгляд кажутся безопасными, и обнаруживает угрозы нулевого дня (zero-day). Она детектирует ВПО, поступающее в организацию из разных источников (почтовые вложения, общие файлы, веб-трафик при интеграции с периметровыми решениями и другие), и блокирует его распространение.

2. Регулярное тестирование самого популярного канала распространения ВПО

7

Сервис PT Knockin[7] позволяет регулярно проверять корректность работы средств защиты электронной почты. Он имитирует атаки на почту с помощью отправки файлов с вредоносной нагрузкой. На основании результатов проверки оценивается защищенность почты и предоставляются рекомендации по устранению выявленных недостатков. PT Knockin не требует интеграции в ИТ-инфраструктуру компании: для запуска нужно зайти в веб-консоль, ввести адрес электронной почты и начать проверку.

PT KNOCKIN PT
KNOCKIN PT KN
PT KNOCKIN PT
KNOCKIN PT KN
PT KNOCKIN PT
KNOCKIN PT KN
PT KNOCKIN PT
KNOCKIN PT KN