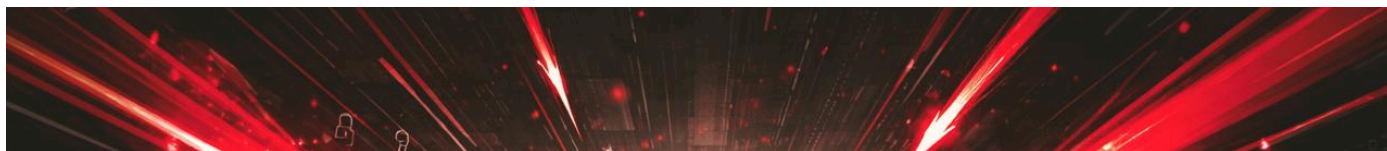


Проникнуть в офис через Office / Хабр

 habr.com/ru/companies/pt/articles/1004518

ptsecurity

February 27, 2026



В феврале российские компании столкнулись с целевой атакой хакеров из группировки BO Team (также известной как Black Owl, Lifting Zmiy и Hoody Hyena). Злоумышленники использовали уязвимость в системах с установленным пакетом Microsoft Office, распространяя фишинговые письма с RTF-файлами, оформленными под служебную переписку. При открытии вложений в программах Microsoft Office атакующие могли обходить встроенную защиту, получая возможность проникновения в ИТ-инфраструктуру организаций.

Подробности читайте в этом материале.

25 февраля группа киберразведки PT ESC зафиксировала первую фишинговую кампанию с использованием [CVE-2026-21509](#), направленную на российские организации. Злоумышленники распространяют RTF-документы, оформленные под служебную переписку.

АКТ проверки транспортного средства

Пример документа-приманки

Внутри RTF-документа встроен OLE-объект с CLSID EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B (Shell.Explorer.1). Данные объекта упакованы в OLE-хранилище; в стриме CONTENTS находится специально сформированный .lnk-ярлык, указывающий на удаленный ресурс:

`\rostransnazor.digital@SSL\svn\58\АКТ проверки транспортного средства.lnk`

Суффикс @SSL активирует WebDAV-редиректор Windows (службу WebClient), превращая обычное UNC-обращение в HTTPS-запрос к внешнему серверу.

CVE-2026-21509 здесь выступает механизмом обхода встроенных защит Microsoft Office при обработке OLE-компонентов. Уязвимость позволяет создать COM-объект и получить доступ к удаленному [.lnk](#) сразу после открытия документа, тем самым запуская следующую стадию атаки.

На момент исследования удаленный ярлык уже был недоступен, поэтому полностью воспроизвести вторую стадию не удалось.

При анализе домена rostransnadzor.digital выявлено, что в его SOA-записи (поле [RNAME](#)) указан контактный e-mail gjegoshcappaniesh@gmail.com — этот же e-mail ранее фигурировал у доменов, использовавшихся в атаках группировки BoTeam.

Дополнительно на возможную связь с группировкой указывает повторение характерных артефактов: одинаковое название вредоносных файлов «АКТ проверки транспортного средства», а также использование схожего доменного имени rostransnnadzor.ru.

Это позволяет нам предположить, что за кампанией с использованием CVE-2026-21509 может стоять **хакерская группировка BoTeam**.

 Для минимизации рисков рекомендуем **как можно скорее обновить Microsoft Office** до исправленной версии. Если оперативное обновление невозможно, в качестве временной меры следует заблокировать активацию уязвимого OLE-компонента Shell.Explorer.1 (CLSID EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B).

Необходимо найти либо создать ветку COM Compatibility (путь зависит от типа установки — MSI / Click-to-Run — и разрядности системы 32/64-bit):

MSI 64-bit или MSI 32-bit на 32-bit Windows:
HKLM\SOFTWARE\Microsoft\Office\16.0\Common\COM Compatibility\

MSI 32-bit на 64-bit Windows:
HKLM\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Common\COM Compatibility\

C2R 64-bit или C2R 32-bit на 32-bit Windows:
HKLM\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Microsoft\Office\16.0\Common\COM Compatibility\

C2R 32-bit на 64-bit Windows:
HKLM\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\WOW6432Node\Microsoft\Office\16.0\Common\COM Compatibility\

[Объяснить с](#)

Внутри [COM Compatibility](#) необходимо создать подраздел [{EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B}](#) и добавить параметр [DWORD Compatibility Flags = 0x00000400](#).

► Индикаторы компрометации

(Источник: <https://t.me/ptescalator>)

Группа киберразведки PT Expert Security Center