Исследование атак на госорганы с применением коммерчески доступного ПО

Archived: 2026-04-10 02:47:35 UTC

Специалисты BI.ZONE по киберразведке обнаружили новую группировку, которая применяет свободно распространяемое ПО, чтобы вмешиваться в работу государственных организаций. Характерная особенность этого преступного сообщества, получившего название Sticky Werewolf, — в использовании достаточно популярных вредоносных программ, которые несложно обнаружить и заблокировать. Это не мешает Sticky Werewolf добиваться успеха: группировка активна как минимум с апреля 2023 года и к настоящему моменту провела не менее 30 атак.

Ключевые выводы

- Государственные организации в России и Беларуси остаются популярной целью атакующих, занимающихся шпионажем.
- При атаках на многие государственные организации злоумышленникам удается эффективно использовать даже популярное ВПО класса RAT для получения первоначального доступа.
- Чтобы повысить эффективность популярного ВПО, атакующие применяют протекторы, например Themida, — это затрудняет анализ их активности в виртуальной среде.

Описание кампании

Для получения первоначального доступа к целевым системам Sticky Werewolf использовала фишинговые электронные письма со ссылками на вредоносные файлы. Для генерации ссылок применялся сервис IP Logger. Сервис позволял злоумышленникам не только создавать фишинговые ссылки, но и собирать информацию о жертвах, которые по ним перешли. Так, например, они получали информацию о времени перехода, IP-адресе, стране, городе, версии браузера и операционной системы. Эта информация позволяла атакующим сразу провести базовое профилирование потенциально скомпрометированных систем и отобрать наиболее значимые, не обращая внимание на те, которые относятся, например, к песочницам, исследовательской деятельности и странам, не входящим в круг интересов группировки.

Кроме того, сервис позволял злоумышленникам использовать собственные доменные имена. Таким образом, фишинговая ссылка выглядела для жертвы максимально легитимно, например: `hXXps://diskonline[.]net/poryadok-deystviy-i-opoveshcheniya-grazhdanskoy-oborony.pdf`.

По фишинговым ссылкам располагались вредоносные файлы с расширением `.exe` или `.scr`, которые были замаскированы под документы Microsoft Word или PDF. За открытием такого файла следовала демонстрация легитимного документа соответствующего формата и инсталляция Ozone RAT или Darktrack RAT. В качестве документа, направленного на отвлечение внимания жертвы, использовалось, например, экстренное предупреждение МЧС России (рис. 1).

МИНИСТЕРСТВО ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ
ГЛАВНОЕ УПРАВЛЕНИЕ МЧС РОССИИ ПО КРАСНОДАРСКОМУ КРАЮ

Краснодарский край, г. Краснодар, ул. Уральская, 121

09.08.2023 № б/н
На № от

Администрациям городов и районов Краснодарского края
Начальникам подчиненных подразделений МЧС РФ
Руководителям предприятий
(согласно листу рассылки)

ЭКСТРЕННОЕ ПРЕДУПРЕЖДЕНИЕ

По данным Гидрометцентра МЧС РФ, в 9-10 часов утра 10 августа 2023 года в Краснодарском краю ожидается ливень, видимость 100-500 м. Сохранится утром. Уровень погодной опасности – желтый.

Прогнозируется вероятность возникновения чрезвычайных ситуаций, связанных с:

нарушением автотранспортного сообщения между населенными пунктами;

нарушением работы автотранспорта (из-за плохой видимости);

осложнением в работе экстренных и аварийных служб;

увеличением дорожно-транспортных происшествий с угрозой жизни и здоровью людей.

Источник возникновения чрезвычайных ситуаций – ливень, видимость 100-500 м.

Рекомендованные предупредительные мероприятия:

1. Органам исполнительной власти Краснодарского края (в рамках компетенции):

обеспечить готовность имеющихся сил и средств;

провести мероприятия, направленные на защиту населения, объектов жизнеобеспечения и социальной инфраструктуры, на снижение вероятности возникновения чрезвычайных ситуаций и смягчения ее последствий, а также обеспечение постоянной готовности органов управления;

реализовать меры, направленные на готовность диспетчерских (дежурных) служб.

Рис. 1. Пример документа, использованного атакующими

Еще один пример — исковое заявление (рис. 2).

Савёловский районный суд города Москвы, Российская Федерация
(наименование суда)

125196, Москва, ул. Бутырский вал, д.7, стр.1
(почтовый адрес)

ИСТЕЦ: [redacted]

(Ф.И.О., адрес, телефон)

ОТВЕТЧИК: [redacted]

(Ф.И.О., адрес, телефон)

ТРЕТЬИ ЛИЦА:

*(При наличии.
Указать адрес, телефон)*

ЦЕНА ИСКА: 37 780
(сумма, рублей)

Исковое заявление
о взыскании заработной платы, иных выплат, причитающихся работнику, а также процентов за нарушение срока их выплаты при увольнении

С "11"сентября 2019 года по "07"марта 2023 года истец работал в (у) [redacted] на должности главного специалиста транспортной безопасности, что подтверждается приказом о приеме на работу от "11" сентября 2019 г. N 1245/41, записью в трудовой книжке от "13" 09 2019 г.

N 3, трудовым договором от "11" 09 2019 г. N 2040.

В соответствии с п. 6 трудового договора N 20 от "11" 09 2019 г. размер заработной платы за выполняемые истцом должностные обязанности составлял 32 000 рублей в месяц.

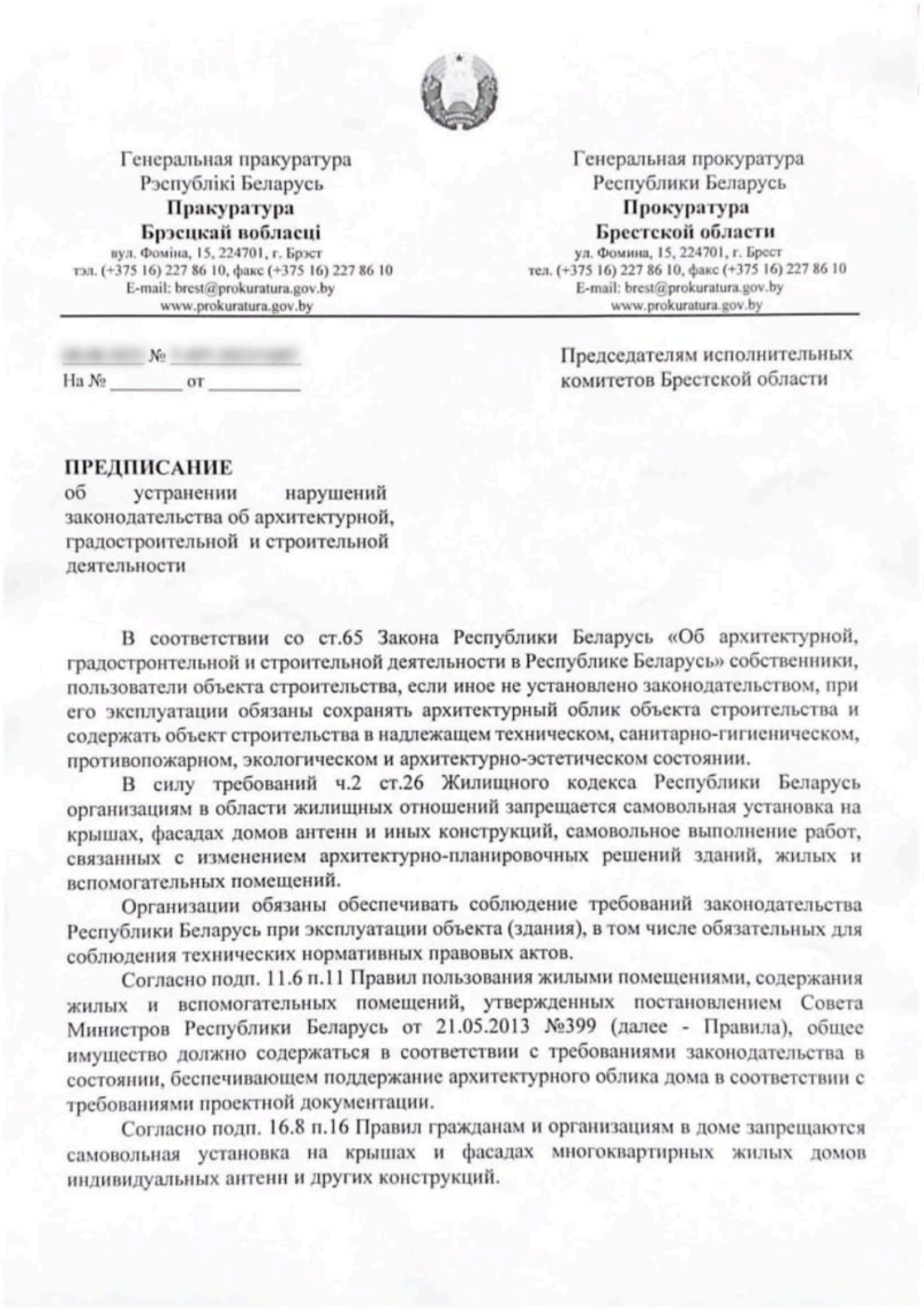
Приказом от "07" марта 2023 года N 277 истец был уволен с должности главного специалиста транспортной безопасности [redacted] по собственному желанию (иному основанию) в соответствии с ч. 1 ст. 80 Трудового кодекса Российской Федерации. В день увольнения истцу была выдана справка о причитающихся ему суммах и трудовая книжка, однако расчет в день увольнения произведен не был по причине отсутствия денежных средств на балансе в предприятия (не зависящей от истца).

Кроме того, при увольнении истцу не были выплачены: компенсация за неиспользованный отпуск. в размере 10 4550 рублей, что подтверждается справкой отдела кадров от 17.03.2023 года.

В соответствии со ст. 140 Трудового кодекса Российской Федерации при прекращении трудового договора выплата всех сумм, причитающихся работнику от работодателя, производится в день

Рис. 2. Пример документа, использованного атакующими

Что касается атак на белорусские организации, в качестве документа использовалось, например, предписание об устранении нарушений законодательства (рис. 3).



Генеральная пракуратура
Рэспублікі Беларусь
Пракуратура
Брэсцкай вобласці
вул. Фоміна, 15, 224701, г. Брэст
тэл. (+375 16) 227 86 10, факс (+375 16) 227 86 10
E-mail: brest@prokuratura.gov.by
www.prokuratura.gov.by

Генеральная прокуратура
Республики Беларусь
Прокуратура
Брестской области
ул. Фомина, 15, 224701, г. Брест
тел. (+375 16) 227 86 10, факс (+375 16) 227 86 10
E-mail: brest@prokuratura.gov.by
www.prokuratura.gov.by

[redacted] № [redacted]
На № _____ от _____

Председателям исполнительных комитетов Брестской области

ПРЕДПИСАНИЕ
об устранении нарушений законодательства об архитектурной, градостроительной и строительной деятельности

В соответствии со ст.65 Закона Республики Беларусь «Об архитектурной, градостронтельной и строительной деятельности в Республике Беларусь» собственники, пользователи объекта строительства, если иное не установлено законодательством, при его эксплуатации обязаны сохранять архитектурный облик объекта строительства и содержать объект строительства в надлежащем техническом, санитарно-гигиеническом, противопожарном, экологическом и архитектурно-эстетическом состоянии.

В силу требований ч.2 ст.26 Жилищного кодекса Республики Беларусь организациям в области жилищных отношений запрещается самовольная установка на крышах, фасадах домов антенн и иных конструкций, самовольное выполнение работ, связанных с изменением архитектурно-планировочных решений зданий, жилых и вспомогательных помещений.

Организации обязаны обеспечивать соблюдение требований законодательства Республики Беларусь при эксплуатации объекта (здания), в том числе обязательных для соблюдения технических нормативных правовых актов.

Согласно подп. 11.6 п.11 Правил пользования жилыми помещениями, содержания жилых и вспомогательных помещений, утвержденных постановлением Совета Министров Республики Беларусь от 21.05.2013 №399 (далее - Правила), общее имущество должно содержаться в соответствии с требованиями законодательства в состоянии, беспечивающем поддержание архитектурного облика дома в соответствии с требованиями проектной документации.

Согласно подп. 16.8 п.16 Правил гражданам и организациям в доме запрещаются самовольная установка на крышах и фасадах многоквартирных жилых домов индивидуальных антенн и других конструкций.

Рис. 3. Пример документа, использованного атакующими

Вместе с документом в папку `%TEMP%` под именем легитимного приложения, например `utorrent.exe` (µTorrent), копировался загрузчик Ozone RAT. Для закрепления в скомпрометированной системе в папке автозагрузки создавался ярлык, который указывает на образец ВПО, например: `%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\uTorrent.lnk`. При этом для обфускации Ozone RAT Sticky Werewolf использовала протектор Themida, что затрудняло обнаружение и анализ.

Ozone RAT построен на модульной архитектуре и включает два ключевых компонента: загрузчик и основной модуль, отвечающий за функции трояна удаленного доступа. В данном случае группировка Sticky Werewolf использовала загрузчик Ozone RAT.

На момент анализа основной модуль был недоступен. Однако известно, что загрузчик скачивает с командного сервера (C2) зашифрованный основной модуль в виде DLL, который сохраняется на диске под именем `data.dbf` в том же каталоге, где находится загрузчик. Далее основной модуль расшифровывается и загружается непосредственно в оперативную память с использованием рефлексивной загрузки DLL через функцию BTMemoryModule из API Delphi. После этого управление передается основному модулю, который выполняет вредоносные действия.

Основной модуль Ozone RAT предоставляет атакующим широкий набор функциональных возможностей для управления скомпрометированной системой и выполнения различных вредоносных действий, включая:

- Управление файлами, процессами и службами.
- Изменение записей в реестре Windows.
- Запись нажатий клавиш с помощью модуля кейлоггера.
- Захват видео с экрана, доступ к веб-камере и запись звука с микрофона в режиме реального времени.
- Удаленное выполнение команд через командную строку Windows.
- Загрузку и запуск файлов с командного сервера (C2).
- Удаление себя из системы для сокрытия следов.
- Использование модуля HVNC для скрытого управления компьютером жертвы.
- Восстановление паролей из веб-браузеров и почтовых клиентов, таких как Outlook и Thunderbird.
- Работу в режиме обратного прокси для обхода сетевых ограничений.

Выводы

Свободно распространяемое и коммерческое ВПО пользуется большим спросом как среди киберпреступников, так и проправительственных группировок, так как позволяет получить широкие функциональные возможности за несколько десятков долларов. Более того, зачастую такие программы активно используются злоумышленниками даже после ареста их разработчиков.

Как обнаружить следы Sticky Werewolf

1. Обращайте внимание на запуск подозрительных исполняемых файлов из временных папок.
2. Отслеживайте появление исполняемых файлов, замаскированных под легитимные приложения, в нестандартных расположениях.

3. Осуществляйте мониторинг доступа подозрительных процессов к файлам, содержащим аутентификационные данные, например, относящиеся к веб-браузерам или электронной почте.

MITRE ATT&CK

Тактика	**Техника**	**Процедура**
Initial Access	Phishing: Spearphishing Link	Sticky Werewolf использует вредоносные ссылки в электронных письмах для получения первоначального доступа
Execution	User Execution: Malicious File	Жертве необходимо открыть загруженный вредоносный файл для инициализации цепочки компрометации системы
	Command and Scripting Interpreter: Windows Command Shell	Sticky Werewolf использует командную строку Windows для выполнения команд и сценариев
	Native API	Sticky Werewolf использует Windows API в своих вредоносных программах для взаимодействия со скомпрометированной системой
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Sticky Werewolf использует каталог автозагрузки для создания ярлыка с целью закрепления в скомпрометированной системе
Defense Evasion	Obfuscated Files or Information: Software Packing	Sticky Werewolf использует протектор Themida для обеспечения противодействия анализу
	Masquerading: Double File Extension	Sticky Werewolf использует двойное расширение для маскировки вредоносных файлов
	Process Injection: Process Hollowing	Sticky Werewolf может внедрять вредоносный код в легитимные процессы

Тактика	**Техника**	**Процедура**
	Indicator Removal: File Deletion	Sticky Werewolf может удалять файлы вредоносных программ после их выполнения
	Virtualization/Sandbox Evasion: System Checks	Sticky Werewolf использует протектор Themida с функцией проверки запуска вредоносной программы в виртуальной среде
	Debugger Evasion	Sticky Werewolf использует протектор Themida для проверки наличия инструментов отладки
Credential Access	Input Capture: Keylogging	Sticky Werewolf может использовать модуль кейлоггера вредоносной программы Ozone RAT для осуществления записи нажатий клавиш
	Unsecured Credentials: Credentials In Files	Sticky Werewolf может использовать Ozone RAT для получения аутентификационных данных почтовых приложений Outlook и Thunderbird
	Credentials from Password Stores: Credentials from Web Browsers	Sticky Werewolf может использовать Ozone RAT для получения аутентификационных данных, сохраненных в веб-браузерах
Discovery	File and Directory Discovery	Sticky Werewolf использует Ozone RAT для получения информации о файлах и папках
	Process Discovery	Sticky Werewolf использует Ozone RAT для получения информации об активных процессах
	Query Registry	Sticky Werewolf использует Ozone RAT для удаленной работы с реестром ОС Windows

Тактика	**Техника**	**Процедура**
	System Information Discovery	Sticky Werewolf использует Ozone RAT для получения информации о скомпрометированной системе
Lateral Movement	Remote Services: VNC	Sticky Werewolf может использовать модуль HVNC вредоносной программы Ozone RAT для скрытого управления скомпрометированными хостами
Collection	Data from Local System	Sticky Werewolf собирает данные со скомпрометированной системы
	Screen Capture	Sticky Werewolf может осуществлять запись с экрана с помощью Ozone RAT
	Video Capture	Sticky Werewolf может осуществлять запись с веб-камеры с помощью Ozone RAT
	Audio Capture	Sticky Werewolf может осуществлять запись с микрофона с помощью Ozone RAT
Command and Control	Non-Application Layer Protocol	Sticky Werewolf использует протокол TCP для взаимодействия с C2-сервером
	Ingress Tool Transfer	Sticky Werewolf использует модуль загрузки Ozone RAT для получения основного модуля вредоносной программы
	Non-Standard Port	Sticky Werewolf использует нестандартный порт для коммуникаций с C2-сервером

Тактика	Техника	Процедура
Exfiltration	Exfiltration Over C2 Channel	Sticky Werewolf использует C2-сервер для выгрузки собранных данных

Индикаторы компрометации

- `185.12.14[.]32:666`;
- `yandeksdisk[.]org`;
- `diskonline[.]net`;
- `078859c7dee046b193786027d5267be7724758810bdbc2ac5dd6da0ebb4e26bb`;
- `9162ccb4816d889787a7e25ba680684afca1d7f3679c856ceedaf6bf8991e486`.

Больше индикаторов компрометации доступно на платформе BI.ZONE Threat Intelligence.

Как защитить компанию от таких угроз

Фишинговые рассылки — популярный вектор атаки на организации. Для защиты почты можно применять специализированные сервисы, помогающие фильтровать нежелательные письма. Одно из таких решений — BI.ZONE Mail Security. Оно избавляет компании от проблемы нелегитимных писем, инспектируя каждое электронное сообщение. При этом используется более 600 механизмов фильтрации, реализованных на основе машинного обучения, статистического, сигнатурного и эвристического анализа. Такая проверка не задерживает доставку безопасных писем.

Для того чтобы лучше знать актуальный ландшафт киберугроз и понимать, как именно атакуют инфраструктуры, похожие на вашу, мы рекомендуем использовать данные с платформы BI.ZONE Threat Intelligence. Решение помогает проактивно защищать бизнес благодаря аналитическим данным с исчерпывающей информацией об атакующих и ежедневно обновляемым индикаторам компрометации для повышения эффективности работы ваших средств защиты информации.
