Dr.WEB

«Доктор Веб»: обзор вирусной активности в июне 2022 года

«Доктор Веб»: обзор вирусной активности в июне 2022 года

26 июля 2022 года

В июне анализ данных статистики Dr.Web показал уменьшение общего числа обнаруженных угроз на 14.62% по сравнению с маем. При этом количество уникальных угроз незначительно увеличилось — на 0.09%. В большинстве случаев пользователи продолжают сталкиваться с рекламными и нежелательными приложениями. В почтовом трафике преобладали вредоносные скрипты, приложения, использующие уязвимости документов Microsoft Office, а также всевозможные трояны-загрузчики.

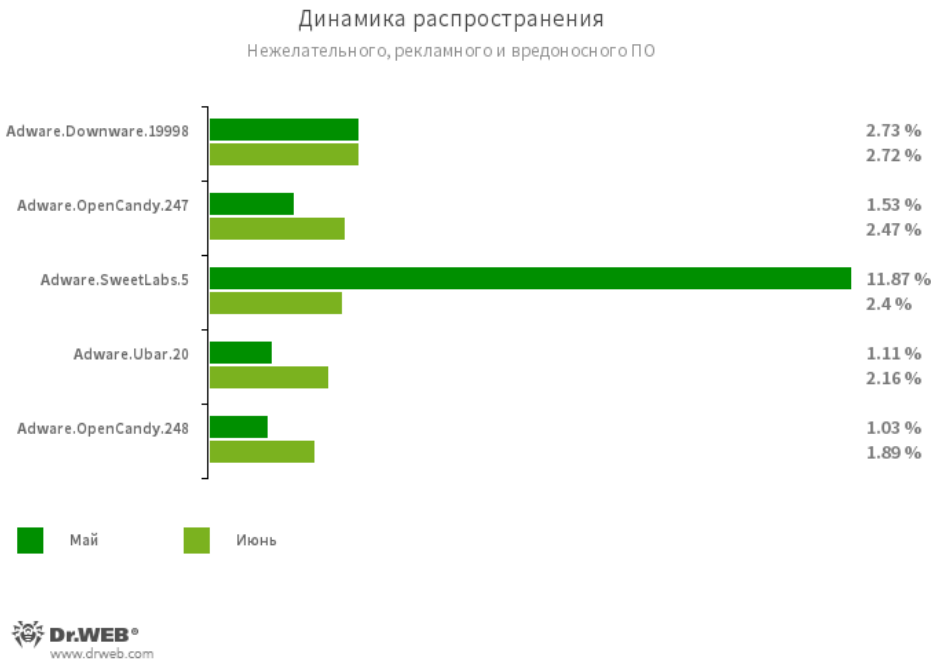
Число обращений пользователей за расшифровкой файлов выросло на 17.26% по сравнению с маем. Самым распространенным энкодером остается Trojan.Encoder.26996 — в прошлом месяце на его долю пришлось 33% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ ИЮНЯ

- Уменьшение общего числа обнаруженных угроз
- Рекламные приложения остаются одними из самых распространенных угроз
- Рост числа обращений пользователей за расшифровкой файлов, пострадавших от троянов-шифровальщиков.

«Доктор Веб»: обзор вирусной активности в июне 2022 года

По данным сервиса статистики «Доктор Веб»



Угрозы прошедшего месяца:

Adware.Downware.19998

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Adware.OpenCandy.247

Adware.OpenCandy.248

Семейство приложений, предназначенных для установки на компьютер различного дополнительного рекламного ПО.

Adware.SweetLabs.5

Альтернативный каталог приложений и надстройка к графическому интерфейсу Windows от создателей Adware.Opencandy.

Adware.Ubar.20

Торрент-клиент, устанавливающий нежелательное ПО на устройство.

«Доктор Веб»: обзор вирусной активности в июне 2022 года

Статистика вредоносных программ в почтовом трафике

W97M.DownLoader.2938

Семейство троянов-загрузчиков, использующих уязвимости документов Microsoft Office. Они предназначены для загрузки других вредоносных программ на атакуемый компьютер.

Exploit.CVE-2018-0798.4

Эксплойт, предназначенный для эксплуатации уязвимости в ПО Microsoft Office и позволяющий выполнить произвольный код.

JS.Redirector.435

Вредоносный сценарий на языке JavaScript, размещаемый в коде веб-страниц. Предназначен для перенаправления пользователей на фишинговые или рекламные сайты.

HTML.FishForm.311

Веб-страница, распространяющаяся посредством фишинговых рассылок. Представляет собой фиктивную форму ввода учетных данных, которая имитирует авторизацию на известных сайтах. Введенные пользователем данные отправляются злоумышленникам.

Trojan.DownLoader44.63714

Троянская программа, загружающая полезную нагрузку с облачного хранилища OneDrive. После скачивания файл расшифровывается и запускается на исполнение.

«Доктор Веб»: обзор вирусной активности в июне 2022 года

Шифровальщики

По сравнению с маем, в июне число запросов на расшифровку файлов, затронутых трояна-ми-шифровальщиками, увеличилось на 17.26%.

- Trojan.Encoder.26996 — 32.99%
- Trojan.Encoder.25069 — 11.34%
- Trojan.Encoder.3953 — 8.06%
- Trojan.Encoder.567 — 7.30%
- Trojan.Encoder.11539 — 0.76%

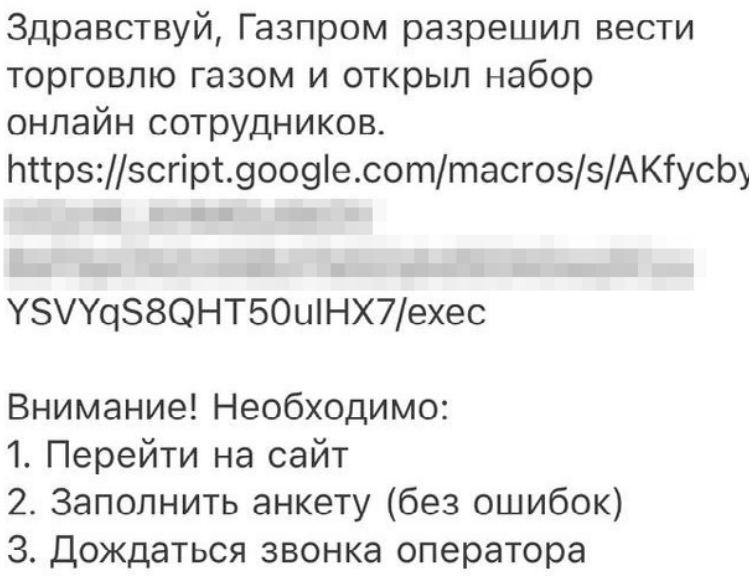
Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

Настрой-ка Dr.Web от шифровальщиков
Обучающий курс
О бесплатном восстановлении
Dr.Web Rescue Pack

Опасные сайты

В прошлом месяце специалисты «Доктор Веб» продолжили фиксировать массовое распространение спам-писем со ссылками на мошеннические сайты. В частности, популярными среди злоумышленников остаются поддельные сайты известных нефтегазовых компаний. На них потенциальным жертвам предлагается стать инвесторами, получить бесплатные активы или принять участие в розыгрыше призов. Для этого пользователям необходимо «зарегистрироваться», указав имя, номер телефона и другую персональную информацию. В других случаях от них требуется оплата якобы необходимой услуги — пошлины, комиссии за перевод «выигрыша» или конвертации валюты. Ничего из обещанного они, конечно же, не получают и лишь передают мошенникам конфиденциальные данные, а также теряют деньги.

Пример нежелательного письма со ссылкой на мошеннический ресурс и пошаговой инструкцией для пользователей:

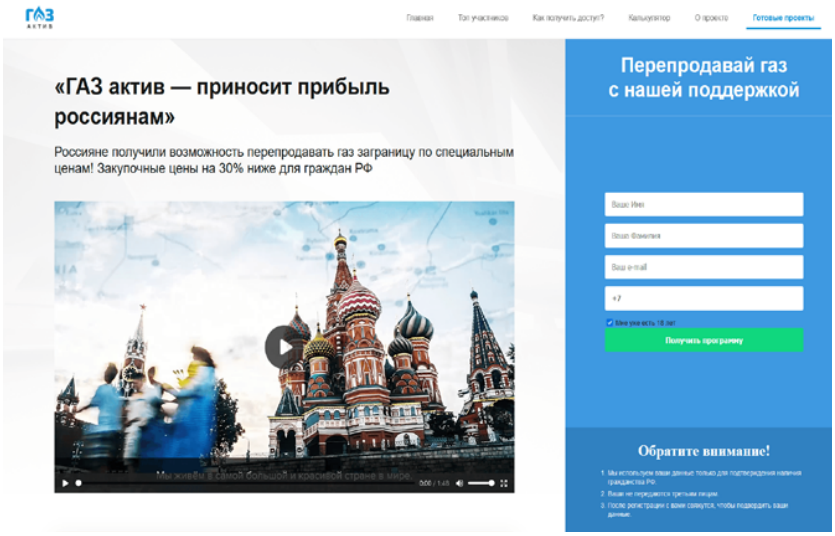

Здравствуй, Газпром разрешил вести
торговлю газом и открыл набор
онлайн сотрудников.
https://script.google.com/macros/s/AKfycby
[redacted]
YSVYqS8QHT50uIHX7/exec

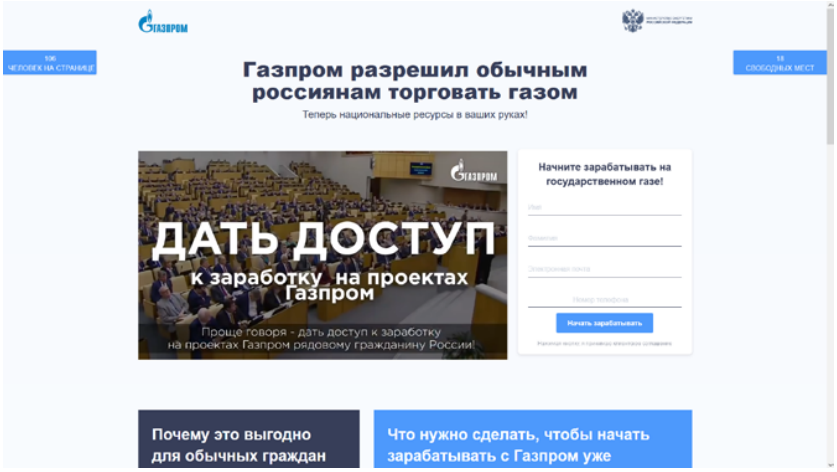
Внимание! Необходимо:
1. Перейти на сайт
2. Заполнить анкету (без ошибок)
3. Дождаться звонка оператора

«Доктор Веб»: обзор вирусной активности в июне 2022 года

Опасные сайты

Примеры мошеннических сайтов с предложением регистрации, после которой у пользователей якобы появится возможность выгодной торговли природным газом:





Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В июне продолжилось снижение активности троянской программы Android.Spy.4498, которая крадет информацию из уведомлений от других приложений. Несмотря на это, она все еще остается самой распространенной Android-угрозой. По сравнению с маем активность рекламных троянов также снизилась.

В течение месяца наши специалисты выявили в каталоге Google Play множество вредоносных программ. Среди них были рекламные трояны семейства Android.HiddenAds, мошеннические приложения Android.FakeApp, а также трояны семейства Android.PWS.Facebook, похищающие логины и пароли от учетных записей Facebook. Кроме того, вирусные аналитики компании «Доктор Веб» обнаружили очередных троянов семейства Android.Joker, которые подписывают пользователей на платные услуги.

Наиболее заметные события, связанные с «мобильной» безопасностью в июне:

- снижение активности трояна-шпиона Android.Spy.4498;
- снижение активности рекламных троянов;
- обнаружение множества вредоносных приложений в каталоге Google Play.

Более подробно о вирусной обстановке для мобильных устройств в июне читайте в нашем обзоре.

«Доктор Веб»: обзор вирусной активности в июне 2022 года

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.
Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

Полезные ресурсы
Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125124 Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах

Узнайте больше
Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека