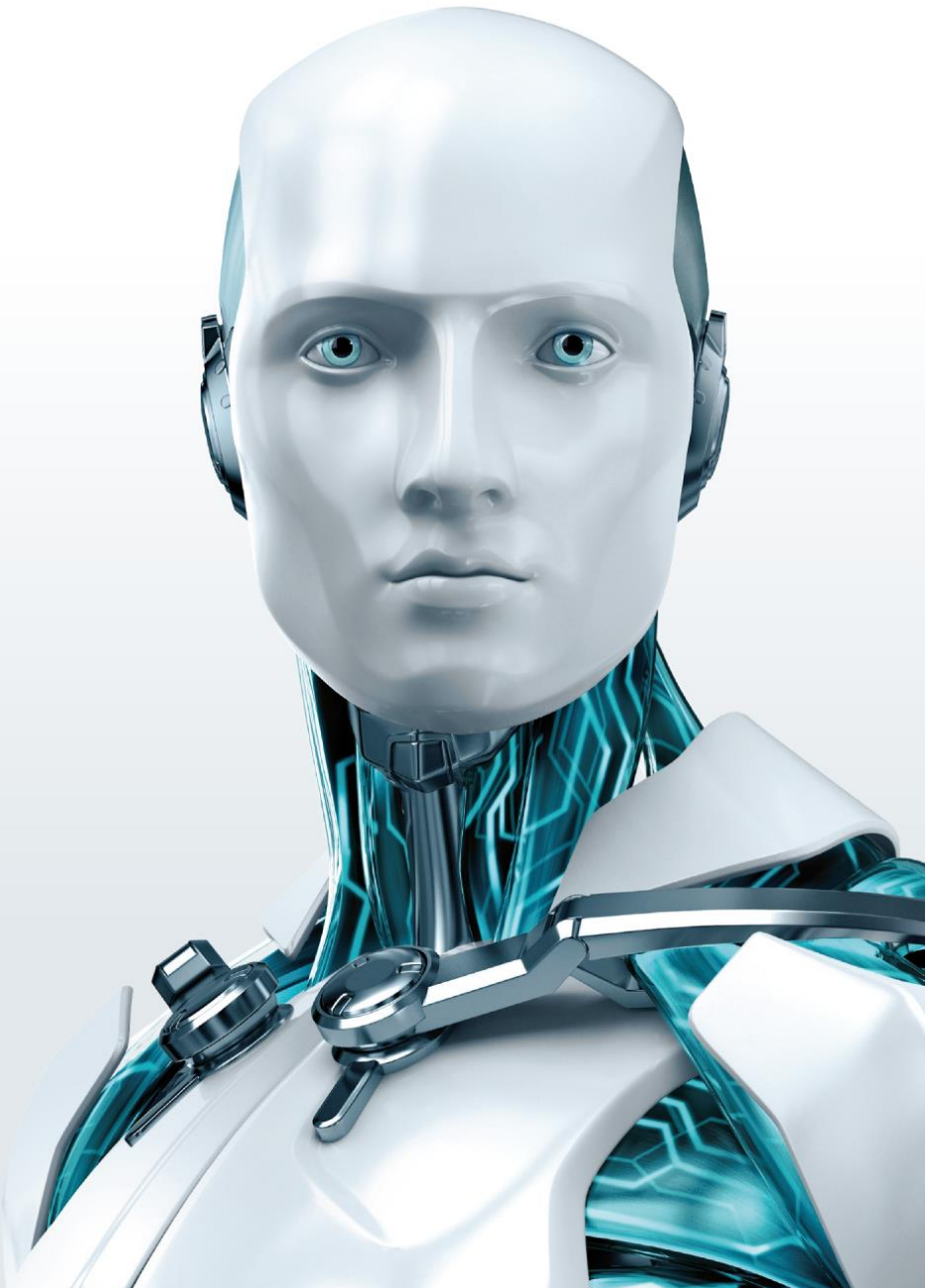
Рекомендації спеціалістів ESET для протидії атакам програми-шифратора Win32/Diskcoder.D (BadRabbit)

Версія 7.0
25.10.2017



НАСОЛОДЖУЙСЯ БЕЗПЕКОЮ

УВАГА! У разі виявлення ознак здійснення атаки, будь ласка, зверніться за допомогою до технічних спеціалістів ESET в Україні, надіславши запит на електронну адресу support@eset.ua.

Основні рекомендації для підвищення безпеки корпоративної мережі

1. Аудит облікових записів груп адміністраторів — **максимально скоротити кількість облікових записів з привілейованими правами** та змінити паролі до них.

2. **Захистити віддалене підключення до серверів за допомогою двофакторної аутентифікації**. Наприклад, рішення ESET Secure Authentication (доступна 30-денна безкоштовна версія*).

3. **Налаштувати резервне копіювання всієї важливої інформації, а також серверів.** Налаштувати реплікацію резервних копій в ізольоване місце. При чому, краще, якщо це буде односторонній зв'язок з боку додаткового сховища. Наприклад, резервне копіювання можна здійснити за допомогою рішення XOPERO.

4. **Поділ мережевої інфраструктури на сегменти:**
   - сервери повинні знаходиться в окремому, ізольованому VLAN-е;
   - доступ до серверів з інших підмереж повинен бути суворо обмежений (конкретні порти та з конкретних адрес);
   - в окремий обмежений сегмент мережі винести всіх адміністраторів, які обслуговують сервери;
   - також в окремий сегмент винести бухгалтерів, оскільки вони найчастіше стають жертвами фішингових атак.

5. **Змінити політики для Інтернет-трафіку (HTTP (s), FTP (s)):**
   - заблокувати доступ до Інтернет-мережі для всіх користувачів, для яких він не є необхідним;
   - ізолювати в окремий сегмент мережі користувачів, яким потрібен доступ в Інтернет;
   - провести додаткове інформування співробітників організації про базові правила безпеки під час роботи на ПК, звернувши особливу увагу на заборону відкривати вкладення та посилання, надіслані в листах від невідомих відправників, а також будь-які підозрілі вкладення та посилання від знайомих адресантів;
   - максимально обмежити доступ до серверів, яким необхідний доступ в Інтернет.

6. **Контроль доставки пошти від невідомих джерел**
   - заборонити використання безкоштовних поштових сервісів;
   - на поштовому сервері налаштувати блокування листів з підміненими адресами;
   - на поштовому сервері налаштувати фільтрацію листів від невідомих (недовірених) адресантів (тобто пошта від невідомих адресантів надсилається в окремий каталог і доставляється користувачеві тільки після перевірки адміністратором.

7. **Контроль актуальності оновлень операційної системи та програмного забезпечення (інвентаризація програмного забезпечення).** Наприклад, можна здійснити за допомогою рішення Flexera (доступна 21-денна безкоштовна версія*).

8. **Шифрування конфіденційної інформації з розмежуванням доступу.** Наприклад, можна здійснити за допомогою рішення ESET Endpoint Encryption (доступна 30-денна безкоштовна версія*).

9. **Контроль пристроїв / змінних носіїв інформації, які підключаються на робочих станціях** (функція реалізована в продуктах ESET Endpoint Security та ESET Endpoint Antivirus):
   - заборонити підключення будь-яких пристроїв;
   - створити білі списки дозволених пристроїв, що підключаються.

10. **Контроль та аналіз мережевого трафіку, як всередині мережі так і на зовні.** Наприклад, можна здійснити за допомогою рішення GREYCORTEX MENDEL (доступна 30-денна безкоштовна версія*).

Додаткові рекомендації для посилення захисту корпоративної IT-мережі від атак типу Not-Petya

1. **Усюди, де можливо, вимкніть SMB версії 1:**
   - Вимкніть SMBv1 через групові політики
   - Вимкніть SMBv1 на окремому сервері

2. **Вимкніть встановлені за замовчуванням облікові записи ADMIN$.**
3. Оскільки використовувались уразливості мережевих протоколів, то **потрібно перевірити системи на наявність уразливостей.** Для такої перевірки рекомендовано запустити інструмент EternalBlue Vulnerability Checker.
4. Оскільки розповсюдження також відбувалось з використанням `PsExec`, **необхідно ретельно контролювати використання портів 445,135,139. При можливості блокувати їх.**

   Якщо Ви використовуєте рішення ESET Endpoint Security, то можливо використовувати вбудований брандмауер для контролю портів. Також у ESET Endpoint Security є додатковий модуль, який контролює уразливості мережевих протоколів.

5. Також можна посилити захист робочих станцій шляхом **використання політик для антивірусних продуктів**, які дозволяють блокувати шкідливі програми-вимагачі:

   https://eset.ua/download_files/news/Anti-Ransomware-Techbrief_EN.pdf

   Звертаємо увагу! Перед використанням необхідно обов'язково протестувати!

*Для отримання безкоштовної пробної версії, будь ласка, надішліть запит на електронну адресу sales@eset.ua, вказавши необхідне рішення, кількість пристроїв, ім'я відповідальної особи та контактний номер телефону. У разі виникнення запитань, будь ласка, звертайтесь за телефоном +38044 545 77 26.

У разі виникнення запитань, будь ласка, зверніться до служби технічної підтримки ESET в Україні, надіславши запит на електронну адресу support@eset.ua або зателефонувавши за номером

+38044 545 77 26

(цілодобово, безкоштовно).