# **Топ 5 угроз информационной безопасности**

## **Фишинговые атаки**

**Угрозой безопасности для любой информационной системы является её пользователь, поскольку, как минимум, представляет из себя наиболее уязвимое звено. Именно пользователь подвержен психологическому давлению (вымогательства, фишинг или целенаправленные действия), а также халатности (недостаточная защита аутентификационной информации – ключи, пароли).**

**Установлено, что для мелкого бизнеса, где сотрудники наименее осведомлены о базовых принципах ИБ, более половины атак являются фишинговыми [1]. Злоумышленники осознают, что в большинстве случаев проще воздействовать на пользователя, чем искать уязвимые места инфраструктуры. Видимо, в связи с этим фишинговые атаки продолжают активно распространяться (самый активный рост наблюдался в 2020 году, когда количество таких атак увеличилось вдвое по сравнению с 2019; в 2021 году число фишинговых атак остается стабильно высоким [2]). По статистике американского агентства ФБР в 2020 году [3]:**

* **было создано порядка 7 миллионов новых фишинговых сайтов;**
* **3 из 4 компаний подверглись фишингу;**
* **в 65% случаях в кибератаках применяются фишинговые письма.**

**По прогнозам специалистов популярность данной угрозы будет только возрастать [4]. Причем злоумышленники не отстают от современных «тенденций», в частности, в Великобритании была выявлена фишинговая атака, в которой предлагалось вводить банковские реквизиты для ПЦР теста на Omicron [5].**

**Источники:**

1. **Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats. 21 января 2022 г. URL:** <https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=4fe0d5d76b61>
2. Phishing statistics and facts for 2019–2022. 27 января 2022 г. URL: <https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/>
3. Top 50 Cybersecurity Statistics, Figures and Facts. 11 января 2022 г. URL: <https://connect.comptia.org/blog/cyber-security-stats-facts?sfredirect=/blog/all-the-cybersecurity-statistics-figures-and-facts-you-need-to-know-in-2022>
4. Security Brief: Seven 2021 Security Predictions and Trends to Watch. 9 декабря 2020 г. URL: <https://www.proofpoint.com/us/blog/security-briefs/seven-2021-security-predictions-and-trends-watch>
5. Weekly Threat Report 10th December 2021. URL: <https://www.ncsc.gov.uk/report/weekly-threat-report-10th-december-2021>

## Удаленная работа

В современных условия удаленная работа стала вынужденной мерой, но не все компании были готовы к ней и имели соответствующую инфраструктуру. Причем угрозой является не только непосредственно удаленный доступ (используемые для этого технологии), но и домашние ПК удаленных пользователей (вопросы актуальности обновления ОС и ПО, наличия антивируса и т.д.).

Ярким примером реализации подобной угрозы стал инцидент, произошедший 5 февраля 2021 г. в американском штате Флорида [1]. Злоумышленники через TeamViewer получили удаленный доступ к компьютеру сотрудника водоочистной станции, что в дальнейшем позволило им взломать внутренние компьютерные системы контроля станции. Таким образом хакеры хотели отравить воду для 15 000 жителей, попытавшись увеличить содержание гидроксида натрия в воде более чем в 100 раз [2]. Каким именно образом хакеры получили доступ к аккаунту TeamViewer: с применением известных уязвимостей ПО, подменой системных DLL или для входа в аккаунт использовались украденные данные [3] – не оглашается.

Источники:

1. 10 Крупнейших Кибератак В Первом Квартале 2021. 13 мая 2021 г. URL: <https://10guards.com/ru/uncategorized/10-major-cyber-attacks-in-q1-2021/>
2. Florida water treatment facility hack used a dormant remote access software, sheriff says. 10 февраля 2021 г. URL: <https://edition.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html>
3. Уязвимость в TeamViewer можно использовать для взлома пользовательского пароля. 6 августа 2020 г. URL: <https://cisoclub.ru/uyazvimost-v-teamviewer-mozhno-ispolzovat-dlya-vzloma-polzovatelskogo-parolya/>

## Вирусы-вымогатели

Стандартной схемой работы вируса-вымогателя является шифрование ОС, отдельных дисков или файлов с последующим требованием выкупа за получение ключей расшифрования. Хотя объектом воздействия таких вирусов могут быть и домашние компьютеры обычных пользователей, в настоящее время подобным атакам чаще подвергаются крупные корпорации, способные и готовые платить за свои данные.

Частным примером такой угрозы является ПО «Phoenix CryptoLocker», разработанное хакерской группировкой Evil Corp. 21 марта 2021 г. атака с применением этого ПО была успешно осуществлена на одну из крупнейших страховых компаний США (CNA Financial Corp.). Злоумышленники развернули в сети CNA программу-вымогатель, зашифровавшую 15 000 устройств и скомпрометировавшую данные более 75 000 сотрудников (номера социального страхования, информацию о медицинских пособиях, имена контрактных работников, сотрудников компании и членов их семей). Вирус затронул также компьютеры сотрудников, работающих удаленно, которые во время атаки были подключены к корпоративному VPN [1].

Экспертами установлено, что Phoenix CryptoLocker похож на другой вирус-вымогатель «Indrik Spider» от этой же группировки, который получает первоначальный доступ к сетям с использованием RDP или путем доступа к VPN с использованием скомпрометированных учетных данных. Группа также распространяла вредоносное ПО с помощью поддельных обновлений программного обеспечения [2].

Согласно же отчету CNA, злоумышленники получили доступ к системе 5 марта и находились в ней вплоть до 21 марта и ещё до запуска Phoenix CryptoLocker смогли скопировать часть данных [3]. В качестве выкупа было выплачено 40 миллионов долларов.

Источники:

1. 15 Biggest Cybersecurity Attacks in 2021. 19 февраля 2022 г. URL: <https://www.privacyaffairs.com/cybersecurity-attacks-in-2021/>
2. Phoenix Cryptolocker Ransomware. URL: <https://digital.nhs.uk/cyber-alerts/2021/cc-3813>
3. FORMAL NOTICE OF CYBERSECURITY INCIDENT. 9 июля 2021 г. URL: <https://www.cna.com/web/wcm/connect/1077e9ef-e397-47f1-ad3c-27470e1b3fbc/privileged-confidential-grey-capybara-legal-notice-070921.pdf?MOD=AJPERES>

## Проблемы администрирования

Неправильные настройки могут стать для злоумышленника удобными инструментами для использования недекларированных возможностей, причем проблемы с настройками могут встречаться как в программных, так и в аппаратных составляющих.

Так, например, некорректная конфигурация сервера позволила злоумышленнику совершить взлом стриминговой платформы Twitch (Amazon). В общем доступе оказались 125 Гб данных: исходные коды сервиса (в том числе, механизмы аутентификации пользователей), подробности работы внутренних служб, инструменты безопасности (анализ возможных угроз и способов борьбы с ними) [1, 2]. Хотя представители компании и утверждают, что часть опубликованных данных была похищена ранее.

Как сообщается, целью данной атаки была попытка пошатнуть доминирующую позицию платформы.

Источники:

1. The Biggest Cyber Attacks of 2021 (So Far). URL: <https://geeks.lk/biggest-cyber-attacks-2021/>
2. Масштабная утечка данных Twitch: что стало известно из-за взлома платформы. 7 октября 2021 г. URL: <https://www.forbes.ru/tekhnologii/442259-masstabnaa-utecka-dannyh-twitch-cto-stalo-izvestno-iz-za-vzloma-platformy>

## Уязвимости в стороннем ПО

Как было описано в предыдущем пункте, некорректная конфигурация является неприятной брешью в безопасности. Особенно много неудобств причиняет такая ситуация, если исправление подобных уязвимостей может быть выполнено только третьей стороной: обновления и патчи ОС, серверного ПО и оборудования.

Весной 2021 года уязвимости были выявлены сразу у двух крупных корпораций.

Производитель графических карт NVIDIA вынужден был выпустить экстренный патч и рекомендовать пользователям обновить драйвера устройств. Компания обнаружила сразу несколько уязвимостей [1, 2]:

* CVE-2021-1074 (важность исправления которой оценивается в 7,5 из 10 баллов) – возможность замены ресурсов приложения вредоносными файлами для кражи пользовательской информации или перехвата управления;
* CVE-2021-1075 (7,3 балла) – возможность подмены данных определённым образом для получения повышенных привилегии в системе;
* CVE-2021-1076 – возможность запуска сетевых атак с целью кражи или повреждения конфиденциальной информации.

Второй компанией, обнаружившей у себя 0-day уязвимости, стала Microsoft [3]. Критических проблем выявлено 6, из которых 2 уже активно использовались злоумышленниками:

* CVE-2021-42292 – обход механизмов безопасности Microsoft Excel;
* CVE-2021-42321 – уязвимость в Microsoft Exchange Server, связанная с удаленным выполнением кода.

Причем Microsoft заявила, что уже известно о нескольких целенаправленных атаках с использованием уязвимости в Microsoft Exchange Server, но подробности не раскрываются.

Источники:

1. Security Bulletin: NVIDIA GPU Display Driver - April 2021. 10 мая 2021 г. URL: <https://nvidia.custhelp.com/app/answers/detail/a_id/5172>
2. В драйверах NVIDIA найдена опасная уязвимость. 29 апреля 2021 г. URL: <https://4pda.to/2021/04/29/384910/v_drajverakh_nvidia_najdena_opasnaya_uyazvimost/>
3. Microsoft исправила 55 уязвимостей, две из которых использовали хакеры. 10 ноября 2021 г. URL: <https://xakep.ru/2021/11/10/exchange-and-excel-0days/>