ПРИЛОЖЕНИЕ 1

Информация

о фишинговых угрозах,

мерах по предотвращению реализации угроз безопасности информации, связанных с деятельностью хакерских группировок по фишинговым рассылкам

1. Хакерскими группировками, нацеленными на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем, содержащих вредоносные архивы с наименованиями «ПРИЛОЖЕНИЕ № 1.10 К АКТУ № 4-0720240910-О.tbz» и «Форма приложения к контракту 001.tbz». В архивах находятся файлы с наименованиями «ПРИЛОЖЕНИЕ № 1.10 К АКТУ № 4-0720240910-О.com» и «Форма приложения к контракту 001.com», которые представляют собой вредоносное программное обеспечение типа «загрузчик» (GuLoader). После открытия указанных файлов осуществляется получение несанкционированного доступа к целевой системе.

2. Хакерской группировкой Sticky Werewolf, нацеленной на органы государственной власти Российской Федерации и организации сферы финансов, осуществляется распространение вредоносного программного обеспечения путем отправки фишинговых писем с тематикой «Заявление об актуализации персональных данных». Указанные письма содержат вредоносный архив с наименованием «Заявление об актуализации персональных данных.rar».В архиве находятся файл-приманка «Данные.pdf» и «Данные.pdf.exe» — вредоносное программное обеспечение типа «троян удаленного доступа» (Darktrack RAT). После открытия указанного файла осуществляется получение несанкционированного доступа к целевой системе.

3. Хакерской группировкой Core Werewolf, нацеленной на органы государственной власти Российской Федерации, организации сферы финансов и объекты оборонно-промышленного комплекса Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица Минобороны России. Указанные письма содержат замаскированный под легитимный документ файл с наименованием «Плановые цели авиации противника», который является самораспаковывающимся архивом. После загрузки указанного архива осуществляется инсталляция легитимного программного обеспечения «UltraVNC», используемого для удаленного доступа к целевой системе.

4. Хакерскими группировками, нацеленными на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем от сотрудника 6 отдела 7 управления ЦИБ ФСБ России. В тексте письма говорится о проведении проверки в отношении ряда организаций, подозреваемых в незаконном распространении персональных данных и сотрудничестве с иностранными спецслужбами. Указанные письма содержат ссылку на загрузку документа формата «HTML», замаскированного под список запрашиваемых документов. Данный документ содержит вредоносный JavaScript код, который запускается при открытии и осуществляет загрузку
и внедрение фреймворка постэксплуатации «Havoc», с помощью которого возможно получение несанкционированного доступа к целевой системе.

5. Хакерскими группировками, нацеленными на органы государственной власти Российской Федерации и организации в сфере энергетики, осуществляются фишинговые рассылки электронных писем, содержащих ссылку на облачный сервис «Яндекс Диск». По указанной ссылке доступен для скачивания вредоносный архив
с наименованием «Cписок наличия.rar», содержащий вредоносный файл
с наименованием «Список наличия.pdf.lnk». После открытия указанного файла осуществляется скачивание и запуск легитимного приложения «Microsoft HTML Application HOST», которое выполняет вредоносный VBS-скрипт, что позволяет получить несанкционированный доступ к целевой системе.

6. Хакерскими группировками, нацеленными на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем от лица Следственного комитета Российской Федерации с тематикой «СК РФ Вызов на допрос». Указанное письмо содержит документ с наименованием «Повестка о вызове на допрос.pdf». При открытии указанного документа предлагается скачать приложение «Adobe Font Package» по ссылке. После перехода по ссылке происходит скачивание вредоносного файла с наименованием «adobe\_PDF\_reader\_fonts\_update\_24.2.5\_Win\_x86-64.exe». После открытия указанного файла осуществляется загрузка и внедрение вредоносного программного обеспечения типа «стилер» (Medusa Stealer).

7. Хакерской группировкой MimiStick, нацеленной на органы государственной власти Российской Федерации, организации и объекты оборонно-промышленного комплекса, осуществляются фишинговые рассылки электронных писем от лица Минтруда России, содержащих вредоносный файл с наименованием «17\_09\_2024.msc». После открытия указанного файла осуществляется открытие файла-приманки и загрузка вредоносного программного обеспечения типа «стейджер» (Silver implant), а также получение доступа к целевой системе.

8. Хакерскими группировками, нацеленными на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем, во вложении которых находится архив с наименованием «Оплата.zip». Указанный архив содержит исполняемый файл с наименованием «USD 720,100.com», который представляет собой скомпилированный обфусцированный Autoit-скрипт. После запуска указанного исполняемого файла осуществляется загрузка вредоносного программного обеспечения типа «стилер» (MetaStealer)
и получение несанкционированного доступа.

9. Хакерскими группировками, нацеленными на органы государственной власти и организации сферы здравоохранения, через фишинговые рассылки осуществляется распространение загрузчика фреймворка постэксплуатации «Havoc» под видом амбулаторной карты. Электронные письма содержат во вложении архив с наименованием «Выписка амбулаторная Камильская.zip», в котором находится файл образа диска «Документы Камильская.iso». После запуска указанного файла осуществляется открытие файла-ссылки «Камильская А. Г.lnk», после чего осуществляется загрузка вредоносного программного обеспечения.

10. Хакерской группировкой Rare Wolf, нацеленной на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем, содержащих вредоносные вложения, замаскированные под легитимные документы. К письмам прикреплены файлы с наименованиями «О ведении Каталога Российской ЭКБ (6-3223 от 25.09.2024).scr», «Список рассылки ПРОМ.pdf.scr», «Приложение\_по\_загрузке\_мощностей.xlsx.scr», при запуске которых осуществляется загрузка и внедрение программного обеспечения для удаленного доступа «МИПКО Employee Monitor».

11. Хакерской группировкой Core Werewolf, нацеленной на органы государственной власти Российской Федерации и организации оборонно-промышленного комплекса, осуществляются фишинговые рассылки электронных писем, содержащих вредоносные вложения. Прилагаемый архив содержит в себе исполняемые файлы с наименованиями «План\_работы\_по\_вопросам\_эффективности\_применения\_огневого\_поражения\_РВиА\_\_.exe» или «Временный порядок получения ключей\_ЭП\_.exe», замаскированные под документы формата «.pdf». После запуска указанного файла осуществляется сбор сведений о целевой системе и отправка их на управляющие сервера злоумышленников.

12. Хакерскими группировками, нацеленными на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем с тематикой «Contract / Договор» от имени компании, производящей строительные материалы. Во вложениях находится архив, содержащий исполняемый файл, который представляет собой вредоносное программное обеспечение типа «стилер» (SnakeLogger).

13. Хакерскими группировками, нацеленными на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем от лица сотрудника отдела закупок кабельного завода с предложением уточнить ассортимент предлагаемой продукции.

Во вложении находится архив с наименованием «Сканированный список товаров № 11756.7z», содержащий закодированный исполняемый файл с наименованием «Сканированный список товаров № 11756.vbs». Указанный файл представляет собой вредоносное программное обеспечение типа «загрузчик» (GuLoader).

14. Физическое лицо (хакер) под псевдонимом «dragonforce» осуществляет продвижение партнерской программы по эксплуатации программы-вымогателя «DragonForce» (по схеме «Ransomware-as-a-Service»). В функции указанной программы входит: отслеживание жертв, автоматическая доставка файлов, контроль доступа, установка драйверов для отключения и обхода систем обнаружения и реагирования (XDR) и обнаружения и реагирования на конечных устройствах (EDR), шифрование и работа в системе с привилегиями «SYSTEM».

Злоумышленники используют инструмент сетевого сканирования «SoftPerfect Network Scanner» для получения списка доступных хостов, которые используются для первоначального доступа через сервер удаленного рабочего стола по протоколам RDP, WMI, SMB. После чего злоумышленники осуществляют внедрение вредоносного программного обеспечения (например, фреймворк постэксплуатации «Cobalt Strike»).

15. Физическим лицом (хакером) Narketing163, нацеленным на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем, содержащих вредоносные вложения (например, RedLine Stealer, Agent Tesla, FormBook (FormBookFormgrabber), Snake Keylogger), которые разработаны для внедрения и функционирования в операционных системах под управлением Windows.

16. Хакерской группировкой Sticky Werewolf, нацеленной на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем, во вложении которых находится архив с наименованием «отчет об авиаинциденте.rar». Указанный архив содержит документ приманку и исполняемый файл с наименованием «отчет об авиаинциденте.pdf.exe», который представляет собой вредоносное программное обеспечение типа «троян удаленного доступа» (Darktrack RAT). После запуска указанного исполняемого файла осуществляется получение несанкционированного доступа к целевой системе.

17. Хакерской группировкой Sticky Werewolf, нацеленной на органы государственной власти и организации, от лица Минтруда России через фишинговые рассылки осуществляется распространение загрузчика фреймворка постэксплуатации «Sliver» под видом амбулаторной карты и вредоносного программного обеспечения типа «троян удаленного доступа» (Quasar RAT). Электронные письма содержат во вложении архив, в котором находится файл, замаскированный под легитимный документ с расширением «.pdf» (наименование файлов - «17\_09\_2024.msc», «19\_09\_2024.msc» или «25-09-2024.msc»). После запуска указанного документа осуществляется загрузка вредоносного программного обеспечения.

18. Хакерскими группировками, нацеленными на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем, содержащих вредоносное программное обеспечение «Mythic». При запуске указанного вредоносного программного обеспечения осуществляется сбор информации о целевой системе.

19. Хакерскими группировками, нацеленными на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем, содержащих вредоносное программного обеспечения типа «бэкдор» (ShadowPad). Указанное вредоносное программное обеспечение позволяет злоумышленникам получить полный доступ к целевой системе.

20. Хакерской группировкой Buhtrap, нацеленной на органы государственной власти Российской Федерации и организации сферы финансов, осуществляются фишинговые рассылки электронных писем, во вложении которых находится архив
с наименованием «док\_архив\_54408.zip». Внутри архива находится исполняемый файл с наименованием «Документ № [0-9].exe», который представляет собой вредоносное программное обеспечение типа «троян удаленного доступа» (Buhtrap RAT). Указанное вредоносное программное обеспечение позволяет злоумышленникам получить полный доступ к целевой системе.

21. Хакерской группировкой Core Werewolf, нацеленной на органы государственной власти Российской Федерации и организации, осуществляются фишинговые рассылки электронных писем, в которых, предположительно, содержится самораспаковывающийся архив, после открытия которого в целевой системе осуществляется установка программного обеспечения MeshAgent, позволяющего удаленно управлять устройствами.

22. Хакерской группировкой Core Werewolf, нацеленной на объекты оборонно-промышленного комплекса Российской Федерации, осуществляются фишинговые рассылки электронных писем от имени ФСТЭК России с тематикой «Субъектам критической информационной инфраструктуры в Южном и Северо-Кавказском федеральных округах». Во вложениях находится исполняемый файл, который является самораспаковывающимся архивом. При запуске указанного файла пользователем осуществляется показ документа-приманки и загрузка программного обеспечения для удаленного доступа к целевой системе «UltraVNC».

Меры по предотвращению реализации угроз безопасности информации, связанных с деятельностью хакерских группировок по фишинговым рассылкам

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью хакерских группировок по фишинговым рассылкам, необходимо принимать следующие меры защиты.

1.1 Производить проверку почтовых вложений с использованием средств антивирусной защиты:

для антивирусного средства Kaspersky Endpoint Security необходимо использовать функцию «Защита от почтовых угроз». Для того, чтобы включить указанную функцию, необходимо перейти в настройки приложения и в разделе «Базовая защита» активировать функцию «Защита от почтовых угроз»;

для антивирусного средства Dr.Web Security Space необходимо использовать утилиту SpIDer Mail. Для того, чтобы задействовать указанную утилиту необходимо перейти в настройки приложения и в разделе «Компоненты защиты» выбрать и активировать утилиту SpIDer Mail.

1.2 Проверять имя домена отправителя электронного письма в целях идентификации отправителя. Для этого необходимо обращать внимание
на наименование почтового адреса (домена), указанного после символа «@»,
и сопоставлять его с адресами (доменами) органов (организаций), с которыми осуществляется служебная переписка.

1.3 Организовать получение почтовых вложений только от известных отправителей. Для этого необходимо организовать ведение списков адресов электронной почты органов (организаций), с которыми осуществляется взаимодействие.

1.4 Не открывать и не загружать почтовые вложения писем с тематикой,не относящейся к деятельности органа (организации).

1.5 Осуществлять работу с электронной почтой под учетными записями пользователей операционной системы с минимальными возможными привилегиями:

для операционных систем семейства Microsoft Windows ограничение привилегий можно осуществить через «Панель управления» - «Учетные записи пользователей» - «Управление учетными записями»;

для операционных систем семейства Linux возможно использование команд chmod, chown, chgrp для разграничения прав доступа к файлам и директориям как отдельных пользователей, так и групп пользователей.

1.6 Обеспечивать на уровне сетевых средств защиты информации ограничение обращений к адресам (Приложение 2), используя схему доступа
по «черным» или «белым» спискам.