Бюллетень информационной безопасности от 28.03.2025

I. Сведения об уязвимостях.

Обращаем внимание на зафиксированные специалистами ФСТЭК России уязвимости, отнесенные к категории «наиболее опасные уязвимости».

1. Уязвимость функции VSP Elevation ядра системы аппаратной виртуализации Windows Hyper-V операционных систем Windows (BDU:2025-00287, уровень опасности по CVSS 3.0 – высокий), связанная с переполнением буфера в динамической памяти. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии до уровня SYSTEM.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (далее – «Методика тестирования»), а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (далее – «Методика оценки») (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty).

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

использовать средства контроля целостности для отслеживания конфигураций, привилегированных операций и некорректного поведения виртуальных машин;

использовать средства обнаружения и предотвращения вторжений для отслеживания попыток эксплуатации уязвимости;

произвести минимизацию пользовательских привилегий;

отключить (удалить) неиспользуемые учётные записи пользователей.

2. Уязвимость гипервизоров VMware ESXi, и Vmware Workstation (BDU:2025-02354, уровень опасности по CVSS 3.0 – критический), связанная с ошибками синхронизации при использовании общего ресурса («Ситуация гонки»). Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

использовать средства обнаружения и предотвращения вторжений для отслеживания попыток эксплуатации уязвимости;

использовать средства контроля целостности для отслеживания изменений конфигурации системы;

производить мониторинг журналов безопасности с целью выявления нештатного поведения виртуальных машин;

произвести минимизацию пользовательских привилегий;

отключить (удалить) неиспользуемые учетные записи пользователей.

3. Уязвимость гипервизора VMware ESXi, VMware Workstation, VMware Fusion, платформы виртуализации VMware Cloud Foundation, телекоммуникационной облачной платформы VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure (BDU:2025-02375, уровень опасности по CVSS 3.0 – высокий), связанная с чтением за пределами допустимого диапазона в памяти. Эксплуатация уязвимости может позволить нарушителю получить несанкционированный доступ к защищаемой информации.

4. Уязвимость гипервизора VMware ESXi, платформы виртуализации VMware Cloud Foundation, телекоммуникационной облачной платформы VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure (BDU:2025-02379, уровень опасности по CVSS 3.0 – высокий), связанная с записью произвольного значения в любое произвольное место и переполнением буфера. Эксплуатация уязвимости может позволить нарушителю оказать влияние на конфиденциальность, целостность и доступность защищаемой информации.

5. Уязвимость подсистемы HID: Core ядра операционной системы Linux (BDU:2025-02383, уровень опасности по CVSS 3.0 – высокий), связанная с использованием неинициализированного ресурса. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

6. Уязвимость сервера приложений Apache Tomcat (BDU:2025-02511, уровень опасности по CVSS 3.0 – высокий), связанная с принятием входных данных пути в виде внутренней точки без проверки. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить несанкционированный доступ к защищаемой информации и выполнить произвольный код.

7. Уязвимость консоли управления операционных систем Windows (BDU:2025-02567, уровень опасности по CVSS 3.0 – высокий), связанная с ошибками при обработке входных данных. Эксплуатация уязвимости может позволить нарушителю обойти существующие ограничения безопасности.

8. Уязвимость файловой системы NTFS операционной системы Windows (BDU:2025-02622, уровень опасности по CVSS 3.0 – средний), связанная с раскрытием значения пароля в файле журнала. Эксплуатация уязвимости может позволить нарушителю раскрыть защищаемую информацию.

9. Уязвимость файловой системы NTFS операционной системы Windows (BDU:2025-02628, уровень опасности по CVSS 3.0 – средний), связанная с чтением за пределами допустимого диапазона в памяти. Эксплуатация уязвимости может позволить нарушителю раскрыть защищаемую информацию.

10. Уязвимость драйвера Fast FAT File System Driver операционной системы Windows (BDU:2025-02623, уровень опасности по CVSS 3.0 –

высокий), связанная с целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код.

11. Уязвимость подсистемы Windows Win32 Kernel Subsystem операционной системы Windows (BDU:2025-02629, уровень опасности по CVSS 3.0 – высокий), связанная с возможностью использования памяти после освобождения. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии до уровня system.

12. Уязвимость компонента MapUrlToZone операционной системы Windows (BDU:2025-02724, уровень опасности по CVSS 3.0 – средний), связанная с неправильным разрешением эквивалентности пути. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти существующие ограничения безопасности.

В целях предотвращения возможности эксплуатации указанных в пунктах 3-12 уязвимостей рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

13. Уязвимость файловой системы NTFS операционных систем Windows (BDU:2025-02569, уровень опасности по CVSS 3.0 – высокий), связанная с переполнением буфера в динамической памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код путем монтирования специально сформированного VHD-образа.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

использовать антивирусное программное обеспечение для предотвращения попыток эксплуатации уязвимости;

использовать SIEM-системы для обнаружения попыток эксплуатации уязвимости;

использовать изолированную рабочую станцию для подключения VHD-образов, полученных из недоверенных источников.

14. Уязвимость библиотеки Python JSON Logger языка программирования Python (BDU:2025-02469, уровень опасности по CVSS 3.0 – высокий), связанная с включением функций из недостоверной контролируемой области. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем размещения специально сформированного пакета.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

использовать средства межсетевого экранирования для ограничения возможности удаленного доступа к программному обеспечению;

ограничить возможность записи в директорию с установленными пакетами;

использовать SIEM-системы для обнаружения попыток эксплуатации уязвимости;

использовать средства обнаружения и предотвращения вторжений для выявления и реагирования на попытки эксплуатации уязвимости.

15. Уязвимость механизма обработки .LNK-файлов пользовательского интерфейса операционных систем Windows (BDU:2025-02936, уровень опасности по CVSS 3.0 – высокий), связанная с ошибками представления информации пользовательским интерфейсом. Эксплуатация уязвимости может позволить нарушителю скрытно выполнить произвольные команды операционной системы путем отправки специально сформированного .LNK-файла.

До выхода обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

использовать антивирусное программное обеспечение для предотвращения попыток эксплуатации уязвимости;

использовать SIEM-системы для отслеживания попыток эксплуатации уязвимости.

16. Уязвимость проводника Windows (Windows File Explorer) операционных систем Windows (BDU:2025-02757, уровень опасности по CVSS 3.0 – высокий), связанная с раскрытием информации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию.

17. Уязвимость службы удаленного рабочего стола Remote Desktop Services (RDS) операционных систем Windows (BDU:2025-02876, уровень опасности по CVSS 3.0 – высокий), связанная с использованием небезопасных механизмов обработки аутентификационных данных в памяти операционной системы. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанных в пунктах 2-3 уязвимостей рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

18. Уязвимость интерпретатора языка программирования PHP (BDU:2024-04432, уровень опасности по CVSS 3.0 – высокий), связанная с непринятием мер по нейтрализации специальных элементов, используемых в команде операционной системы. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированного HTTP-запроса.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

ограничить возможность запуска cgi-скриптов, полученных из недоверенных источников;

произвести переход с PHP CGI на более безопасную архитектуру (Mod-PHP, FastCGI или PHP-FPM);

использовать SIEM-системы для отслеживания попыток эксплуатации уязвимости;

использовать средства межсетевого экранирования уровня веб-приложений для ограничения возможности удаленного доступа.

II. Сведения о деятельности хакерских группировок.

По результатам анализа сведений об угрозах безопасности информации и деятельности хакерских группировок, проводимого специалистами ФСТЭК России в условиях сложившейся обстановки, выявлены сведения о деятельности хакерских группировок.

1. Хакерской группировкой Watch Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен вредоносный архив с наименованием, например, «Накладная №186-2114-0406.zip». Внутри указанного архива находится вредоносный исполняемый файл с наименованием «Накладная №186-2114-0406.exe», после запуска пользователем которого осуществляется внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (DarkWatchman).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо принять 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. Обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресам, указанным в приложении, используя схему доступа по «черным» или «белым» спискам и ограничить получение электронных писем с домена «ponyexpress[.]website».

Обращаем внимание, что редактирование в активное состояние ссылок на вредоносное программное обеспечение и серверы управления злоумышленников, приведенных в настоящем письме, а также переход по данным ссылкам не допускается, так как создает предпосылки к распространению вредоносного программного обеспечения.

1.7. Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
1fa0161210fd02fdad616bd3c1f140f58b018963e141056e09d70b2b334e1c53;
fd341be26730b0fb9202852ffa0ea8c25b26b7a1aab8950d8bd0c09c8600322a;
a454fdc612637e229ce1138b7a599ea2936e6ea84b1391adc38b9a5abdb6c805;
03846249abbc6fac612493843a39c55c8e45cbd795d85cf954d1cafc7602864b;
66ee7011fdf4052fb960afdba3f30661b4cf29b99142ace75a8896a88d27183e.

2. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица Минобороны России. Во вложениях указанных писем содержится архив с наименованием «Заявка_ГУВ_5_03Д.zip», внутри которого находится исполняемый файл с наименованием «Заявка_ГУВ_5_03Д.pdf.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного

обеспечения типа «стилер».

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо ограничить получение электронной почты с адреса secretary@spbtv[.]com и обеспечить на уровне сетевых средств защиты информации ограничение обращений к IP-адресу 109[.]107[.]182[.]11, используя схему доступа по «черным» или «белым» спискам.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

c190435790d365d8884645e76e5fe1ec21e4042ff65c65aae714527fb9111fcd;
b013c08926f021e27566572b102cd7df2390a1c5144a9435b677c85007a4c6bb;
3a4f3c495dc1fa5a4159a705a7cf5f13bfd071edc6578ad6fc66456b4c601390;
afc5d66e183ef670c74fdeeb2e9ceaced3fbf2c32d8b51d84faaae940b7f697f;
6cf6696db18d46c5e21cc90d9eb98dd2b3329b8aa1e6ca6712a479205dfc630e;
7bc98fe9b7559a2dbbf86f8269160df83112a35e2ffddd0f0ff33aa705137293.

3. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица АО «Росэлектроника». Во вложениях указанных писем прикреплен архив с наименованием «РЭ-Исх-ПО-8564.rar», внутри которого содержится вредоносный исполняемый файл с наименованием «РЭ-Исх-ПО-8564.scr». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение легитимного программного обеспечения для удаленного доступа «AnyDesk».

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha1):

edf1ee7018233f8414af40978525043b809edf0f;
836f94f2a94db48059b08a8a2dd0cb87a1cec48d;
c538c30985f270e59001939519699117 8c253b49;
a0019aabf10181bd77d7726ccf6fc6b554ab9abd.

4. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые

рассылки электронных писем, во вложениях которых содержится вредоносный исполняемый файл с наименованием «п.2.13.exe». После запуска пользователем указанного исполняемого файла осуществляется внедрение вредоносного программного обеспечения типа «троян удаленного доступа».

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу wxanalytics[.]ru, используя схему доступа по «черным» или «белым» спискам.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha1):

7bab670e1e85bde396e3bd0dc78ac19a1d8ff639;
b2872ad6a7ef4cc4e93942f683e51b621a2c55d6;
7d6f2967eca332b086e635f43f606f77641af4ac;
80fefd46dbdafaa6ceeeab0b321f91ff6d0c99b7;
ac186a7002963b1d0ccdc541f0ed05d59bdc44c6;
56a003f2c52b0e9be860ad4eb1b624be11416c23;
f4cc1f2435e4e7e3d6fe4b1c8a9c27dbeee9646d;
92299f121d4cfca18e3ac04af675b8d64752ba71;
8b38995d86f61befc5179ad50ca09f28d0bae6fe;
0d9a4ed1b0e6d59dbdf96074528757be291c4383;
10a8c42cbf39589e802ae33a7263d8d2aa966c7c;
9c789cd5f814b5670c47bc97e8425a5c557c5e15.

5. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, внутри которых содержится вредоносный архив с наименованием «ПЕРЕЧЕНЬ 314.zip». Внутри указанного архива находятся файлы приманки с наименованием «ПЕРЕЧЕНЬ 314.lnk», «ПЕРЕЧЕНЬ 314.docx» и вредоносный файл с наименованием «ПЕРЕЧЕНЬ 314.jpg». После запуска пользователем указанного вредоносного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор».

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов

компрометации (sha256):
21d34a02ec28e9bd6f7b2f96ac7921f5ef08d291416b38a3fc8cf651f11fc820;
d4207c990986bc670b4192004ffb8450e84141517dae38b818cc6703dfde54df;
7c2c32560ed74771f9cad55e96209090b122ac1ba1e888298ff5bfc9f6895179.

6. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Оплата». Во вложениях указанных писем содержится вредоносный исполняемый файл с наименованием «12937000.exe» и вредоносный файл с наименованием «Contract.bz». После запуска пользователем указанных файлов осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Nova).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо ограничить получение электронных писем с адреса buh3@arslift[.]ru и осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
fe9c2882eb9abb3d248c9c35430898ca7abd93b9b674256bb51c259ab8a96c41;
ada9ca84e907cda335a6de2ffdaf3b2ce9e72198c128278f0e65427fc8d69ded;
8043f7bb52917a51cb9c8f9f0d6881415d48df0c0ae34f6a1e465efb3f683fbe;
d5a60d148df8534b1d3d585abaecc2edb979d3f69ae8975c7d9c7e77153aa645.

7. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится архив с наименованием «TOR_S-K_PMC_24-02-2025.7z». Внутри указанного архива находится вредоносный файл с наименованием «TOR_S-K_PMC_24-02-2025.bat», после запуска пользователем которого осуществляется выполнение команд оболочки сценариев PowerShell и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Remcos RAT).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hftook7lmoutsg1[.]duckdns[.]org;

hftook7lmoutsg2[.]duckdns[.]org;
hftook7lmoutsg3[.]duckdns[.]org;
hftook7lmoutsg4[.]duckdns[.]org;
hftook7lmoutsg5[.]duckdns[.]org.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
8e60eeff39a1ddd3c5db7b273ee2dd7b57fa7f33b7910ae6bc5c51218f777378;
6a01172e97a462132b54b031da655990915b6ca57337efdbc5aadb957876276f;
5b9affaa1c7e1ffc704a789921caf886aca3d6d4d731b27ac24775ff517b1fd1;
3907766313937c029abc537001e5f86543804a5f1c65f76a827b1a7f4490589b;
2da38e43a05294d110f189f7a2a723410976cda5895a2243af64f6222a9ea62c;
f8cff184fd969fcb0fce3e81f2afbebfd59ff1ab660a3fd20a8e82df0da410bf.

8. Хакерской группировкой Sticky Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица Минпромторга России. Во вложениях указанных писем содержится архив с наименованием «Исходяший.7z». Внутри указанного архива находится вредоносный исполняемый файл с наименованием «ДОЛГОВАЯ НАГРУЗКА.pdf.exe», замаскированный под легитимный документ. После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки, выполнение вредоносного Batch-скрипта и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (QuasarRAT).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу thelightpower[.]info, используя схему доступа по «черным» или «белым» спискам.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
b4b94fbdb809adb39841febe61c73715c29dbd61b7ed7124dc0be69badb52c12;
a411e845cc2fb3c20a41478fd67ff4e9641d227d72d044e747e4fda29651b85a.

9. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Список товаров». Во вложениях указанных писем содержится вредоносный файл с наименованием

«KYNIX24255.jar», замаскированный под легитимный документ. После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (STRRAT).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

176[.]65[.]139[.]53;

www[.]kposlifestyle[.]design;

jbfrost[.]live;

hxxp[:]//jbfrost[.]live/strigoi/server/?hwid=1&lid=m&ht=5.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

f6c3a9cbb44a6bbed4889e7e79c0d8a5c6797d91da76067c053ffb2cd6b4c25d;
7058923f62ef66b9a9d589dae9d1d581f5c692c4a38511e1820587a730576f65;
9b06f513705fd1f58888d74326cfb7c37daa41855e977ceb103e929398dab233;
aad091ecab7d3b2b89ef5e5eee93aecdf12573aad66e6c84b6def900d40a3f97;
eabec9a614aa3ec6a0d7f660089bc544613b27aaebf3b8667258b85a765684c9.

10. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются атаки на целевые системы через эксплуатацию служб удаленного доступа (например, RDP). После получения несанкционированного доступа к инфраструктуре злоумышленники осуществляют внедрение вредоносного программного обеспечения типа «шифровальщик» (PE32).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

339eeca831924662bd8d9b5de150777a1170d70c5b951624af2cf183c474722b;
7aa93332867bad267b0546dd35391304d38eee276f57f03f7345b764cace51b8;
a6f1a892293805c56db91d21d4df0240de706e7f35f1f447a4e917edee62ff9b;
f81fcabbd0949505f7bca07af97713f43114e102bb2d38c7d5a9a90568d34ef5;
3c53016fa88d25c356a25efa09d8f3332ff88cb3d4348df5d268361ea4fe73ea;
e09af611db950b072716fe9c9a496ee8cc9e5037527db2e5822e402f22176f6a;
f852d769d3919b10ef85c4ba1ee34ef9d930a42553384570faa455901cc0aaf6;
c6ddc9c2852eddf30f945a50183e28d38f6b9b1bbad01aac52e9d9539482a433;

5d19cbc6ca77c0a88a68f863d08c4cafbe775aa6a077d77ff98cfe91d989ba6a;
8b2f0d263c06bceb32d6d1e00d97021cc86bc4645d7eccaad95c2549df78d6d5;
9dc216c359d2ca20541011d87202399d20af222d2511990e55736ff9af1eeaff;
e63f9a5b7d0b12c2b58fd9e9c40cb01c8d7cb7f4d70026c6eed871aa060a8c72;
efe6eb562807af48667b23e0081bc52e7f79e6a07d6cf8e647fd2bcd33544a9e;
52284b3e28216267b78e96950885dd0584b39d39a1d7fba5413097f9ce53b540.

11. Хакерской группировкой APT37, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Торговые соглашения». Во вложениях указанных писем прикреплен вредоносный архив с расширением «.zip», внутри которого содержится вредоносный файл с расширением «.lnk», замаскированный под легитимный документ. После запуска пользователем указанного файла осуществляется выполнение команд оболочки сценариев PowerShell и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (RokRat).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
94159655fa0bfb1eff092835d8922d3e18ca5c73884fd0d8b78f42c8511047b6;
09a4adef9a7374616851e5e2a7d9539e1b9808e153538af94ad1d6d73a3a1232;
cfc814a16547dd4e92607bd42d2722cc567492e88d2830d7d28a0cc20bf3950c;
7df7ad7b88887a06b559cd453e7b65230d0cccff1a403328a521d8753000c6c9;
9d96e4816a59475768d461a71cecf20fd99215ce289ecae8c865cf45feeb8802;
5306582c8a24508b594fed478d5abaa5544389c86ba507d8ebf98c5c7edde451;
2b6928101efa6ededc7da18e7894866710c10794b8cbaf43b48c721e9731c41a;
6d790df4a2c81e104db10f5e47eb663ca520a456b1305e74f18b2f20758ea4e1;
1c4cd06ebece62c796ea517bf26cc869fa71213d17e30feb0f91c8a4cfa7ef1b;
09a4adef9a7374616851e5e2a7d9539e1b9808e153538af94ad1d6d73a3a1232.

12. В дополнение к пункту 11 Бюллетеня от 11.03.2025 (письмо от 12.03.2025 № 31/ПА/513) сообщаем об обнаружении дополнительной информации о деятельности указанных хакерских группировок.

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

185[.]80[.]91[.]107;
94[.]131[.]113[.]79;

94[.]131[.]113[.]80;
45[.]156[.]21[.]178;
api[.]wilbderreis[.]ru;
api[.]yandex-disk[.]info;
dev[.]sauselid[.]ru.

Кроме того, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
b20f57db3282010cfa0208d6b07b115db8ae73d7f822493fb810218b0a0c62db;
011b31d7e12a2403507a71deb33335d0e81f626d08ff68575a298edac45df4cb;
7fb9de5299b2d60b14c2af44e1890b9fb289edfe7f96d8716e1f3285aa9d7aa3;
ed9615d6506e46b1a0fcc7006eda8aed9f974f4a8b3e97402742dfec0f5b3677;
9daab82289f2889f122fc8bdd58beb003fce8f634ea212b63fab225fe0d2795f;
51203a25d81b12a60c190369bc7f8367156f7f46685caa31d0e5fbfe2f81e73b;
917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2;
fd10120afcad7ce9f20aed34679bbeef3173009f7b78caee40aae285512503d0;
1e85f98c39c3a1931e95bf732df5e2d8a470f1323c60cb2f95e328a9c404003f;
f4ba92f3280a21833f6ab6cdf67a956e96c1299df23b62d0ca3eb7c4b68429d1;
edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef;
a98576591e0e03e13239e35f8e02e30b71b6e4109f568a3d245af6ac67591699;
786feaef202a37a8d693c57b1aeb7c8995313e358b901015c4e60033776929c3;
7dc0e13a5f1a70c4e41f4b92372259b050a395104650d57385ecaa148481ae5c.

13. Хакерской группировкой Lone Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Актуальная задолженность(просроченная)». Во вложениях указанных писем прикреплен архив под паролем с наименованием «выписка.zip», внутри которого содержится вредоносный файл с наименованием «Выписка.lnk». После запуска пользователем указанного файла осуществляется выполнение команд оболочки сценариев PowerShell и внедрение вредоносного программного обеспечения типа «фреймворк постэксплуатации» (Cobalt Strike).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5. Обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hxxps[:]//remarket[.]ru[:]8443/jquery-3[.]3[.]1[.]min[.]js;
hxxp[:]//zetag[.]ru/z[.]hta;
hxxp[:]//remarket[.]ru[:]8443;
hxxp[:]//45[.]145[.]91[.]164[:]64830;
hxxp[:]//zetag[.]ru/tramp[.]rtf;

hxxp[:]//mcnn[.]ru[:]8443/;
hxxp[:]//moscable77[.]ru[:]8443/;
hxxps[:]//iplogger[.]cn/forensicsas[.]png;
hxxps[:]//iplis[.]ru/tramp[.]jpg;
hxxp[:]//ecols[.]ru/ecols[.]hta.

Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации:

(sha256):
584c51f79538eef3cc4f7def3f77c070ba5740e927c8f3e544d2f3f49473ac81;
5e68b88253e4f8bb83fc86b610390d28057d4656ec37e1ce3de5100129998df3;
2e31d86d18d4ed04f73fd472e6d2a180f4488e50bd7b052fe84e56787202b052;
91d75784137b5b5fd99fa9b2d7688a99212a30ef36f58c941930bb998d4f46b0;
a2459ae74aaa37edc24e89188b2091c26ab27e07c2fb5a16bd99fadb8827e999;
2aff7d6cd63663ac3ba79af5cfd64c32b10b89c0919bec95bc840ade098d2264;

(md5):
ce5e30bf0c6c5c8bcbe3448737f630e2;
360a0d98cfce72e1f1b52f43bcd8897d.

14. Хакерской группировкой Silent Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, содержащих архив с наименованием «dokazatelstva.zip». Внутри него находится вредоносный архив, замаскированный под файл с расширением «.ini», и файл-ярлык, после запуска пользователем которого осуществляется выполнение вредоносного Batch-скрипта, осуществляющего распаковку указанного вредоносного архива. После распаковки осуществляется демонстрация документа-приманки (презентация Microsoft Office PowerPoint) и внедрение вредоносного программного обеспечения типа «загрузчик».

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:
pdfdepozit[.]com;
pdf-bazaar[.]com;
hxxps[:]//pdfdepozit[.]com/newfiles/?pti=ybutpdk&yay=JhWWZstFbM9D09Q;
hxxps[:]//pdf-bazaar[.]com/files2025/?pti=npu&yay=3oKPkD33tx5Tuzz;
hxxps[:]//pdfdepozit[.]com/newfiles/?pti=ftp&yay=adJZAITbB1bBwNd;
hxxps[:]//huggingface[.]co/TheBloke/Llama-2-70B-GGUF/resolve/main/llama-2-70b[.]Q5_K_M[.]gguf;
hxxps[:]//pdfdepozit[.]com/newfiles/?pti=ioxcq&yay=WwvgFkR70Acasl8;

hxxps[:]//pdfdepozit[.]com/newfiles/?pti=kskwue&yay=fCsIU5YQR5Gr1hL;
hxxps[:]//pdfdepozit[.]com/newfiles/?pti=oja&yay=zb2su1ewva8K7HI.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикаторов компрометации, указанных в приложении к настоящим рекомендациям.

15. Хакерской группировкой Vengeful Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «1.zip». Архив содержит файл-приманку с наименованием «Образец.rtf» и вредоносный файл с наименованием «Акт сверки взаиморасчетов по состоянию на 10.03.2025 года.xslx.scr», замаскированный под легитимный документ. После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Revenge RAT).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо ограничить получение электронных писем с адреса «mv[.]andrianov@cdek[.]ru» и обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

myhost[.]misecure[.]com;

myhost[.]servepics[.]com.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
a3be4274ba2f9b7e4de7f5552c114b450befeb3a4061df02e19c167c1bd45bc3;
e76098ca704cb4a61558907e9d3ca9382aad6256b230aafead4f11f5675ef109.

16. Хакерской группировкой Cloud Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен вредоносный файл с наименованием «Инструкция.doc». После запуска пользователем указанного файла осуществляется загрузка и внедрение вредоносного программного обеспечения типа «бэкдор» (VBShower, VBCloud, PowerShower).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу hxxps[:]//1c-update[.]com/search/q=etf/nonproficience, используя схему доступа по «черным» или «белым» спискам.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикатора компрометации (sha256):

7c86f545064491bb31af3b1e5f5285ea811333563f888e1faa2a6df9e692feac.

17. Хакерскими группировками Head Mare и Twelve, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются компьютерные атаки через скомпрометированные учетные записи подрядных организаций путем подключения к информационной инфраструктуре по протоколу удаленного доступа (RDP). Для закрепления в целевой системе злоумышленники внедряют вредоносное программное обеспечение типа «бэкдор» (CobInt).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок, необходимо:

провести анализ учетных записей администраторов и пользователей информационных систем на предмет наличия незаблокированных учетных записей уволенных работников и неизвестных учетных записей;

проинформировать подрядные организации, осуществляющие сопровождение информационной инфраструктуры органа (организации), о необходимости реализации базовых мер по информационной безопасности в собственной инфраструктуре;

определить перечень учетных записей подрядных организаций, для которых предполагается удаленный доступ к информационной инфраструктуре;

определить перечень информации и информационных ресурсов, к которым будет предоставляться удаленный доступ работникам подрядных организаций;

предоставлять учетные записи работникам подрядных организаций для доступа в информационную систему с минимально необходимыми правами доступа;

реализовать в инфраструктуре для привилегированных пользователей подрядных организаций двухфакторную аутентификацию;

обеспечить сбор, запись, хранение событий информационной безопасности связанных с деятельностью подрядных организаций при осуществлении удаленного подключения и осуществлять постоянный мониторинг (просмотр, анализ) указанных событий;

ограничить использование подрядными организациями программного обеспечения для удаленного управления автоматизированным рабочим местом (например, TeamViewer, AnyDesk, AmmyAdmin, AeroAdmin, Radmin,

LiteManager, Удаленный рабочий стол Chrome, Microsoft Remote Assistance, Microsoft Remote Desktop);

реализовать мониторинг (просмотр, анализ) сетевого трафика на предмет необычной активности (например, многократного увеличения исходящего трафика, обращения к иностранным IP-адресам), а также пользовательской активности (например, многократные попытки входа, множественные единообразные действия) при подключении и осуществлении работ сотрудников подрядной организации в информационной инфраструктуре органа (организации);

регламентировать доступ подрядных организаций к инфраструктуре органа (организации) путем введения согласования каждого удаленного подключения и ограничения времени сессии, в течение которой будут выполняться работы;

произвести проверку работоспособности систем мониторинга информационной безопасности в том числе на предмет работоспособности уведомлений администратора информационной безопасности о событиях информационной безопасности.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

360nvidia[.]com;
web-telegram[.]uk;
45[.]156[.]27[.]115;
45[.]156[.]21[.]148;
185[.]229[.]9[.]27;
45[.]87[.]246[.]34;
185[.]158[.]248[.]107;
64[.]7[.]198[.]109.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (md5):

6008e6c3deaa08fb420d5efd469590c6;
09bcfe1ccf2e199a92281aade0f01caf;
70c964b9aeac25bc97055030a1cfb58a;
87eecdcf34466a5945b475342ed6bcf2;
e930b05efe23891d19bc354a4209be3e;
c21c5dd2c7ff2e4badbed32d35c891e6;
96ec8798bba011d5be952e0e6398795d;
d6b07e541563354df9e57fc78014a1dc.

18. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с

наименованием «act verificare.zip». Внутри указанного архива содержится вредоносный исполняемый файл с наименованием «USD 830,100.exe». После запуска пользователем указанного исполняемого файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (PureLogs Stealer).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к IP-адресу 198[.]46[.]178[.]137, используя схему доступа по «черным» или «белым» спискам.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

ebd8b60eabc7cd536ed7a7dad00a1d3c76351aeb1927196d73046b86763a67c3;

d183843d99bef40af0d7bb99273ac658d403fb7330e6c42a4a2f4f39ba42e8b7.

19. Хакерской группировкой Stone Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплены вредоносные исполняемые файлы, замаскированные под легитимные документы с расширением «.pdf», с наименованиями, например:

«Scan_ARMAN_TZ_138-03_11.03.2025fdp.exe»;

«Scan_Kartochka_ARMANfdp.exe».

После запуска пользователем указанных исполняемых файлов осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (BrockenDoor).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

194[.]226[.]121[.]37;

hxxp[:]//194[.]226[.]121[.]37[:]7182.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

368641d8d2243e1d9d7d1b2917448878c673ceb138b08ee74f4ff310fcc0f779;

418cc2172ed58b525752aada2b74db73ca55e181cc0d112367e03bf5c8e897d0;

d200a8bd73925f5680ed0e08cc5d02a95767f03825bf4aee8c8f56e21e522953.

20. Хакерской группировкой Watch Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Заказ оборонки». Во вложениях указанных писем прикреплен архив с наименованиями «Док-ты на рассчет ФЕВРАЛЬ-МАРТ.rar» («Заявка на март.rar»). Внутри указанного архива содержится вредоносный исполняемый файл, после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (DarkWatchman).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу fb0bf2b1[.]shop, используя схему доступа по «черным» или «белым» спискам.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

a30078d2abdd0268cf1e6fe52d0da68173cb3af85836d81344b2d6aae9ed3d5d;
9cd8618ddb42413360c77180002aa9f1fd4854d2c645e61a7b9bf2e620415094;
19ee97f3cec9092b2cdb1066073ea668b2c4520531c3191e366b882f1b42cad6;
facb92f554788780f221d984870eee2998155e334d83025f710ec2e77a31d811;
93750ec3291dd11b4b8c1c48e842d44a0abfb1d8ab5ffa366a20dce14f11073d.

21. Хакерской группировкой Telemancon (Herald Werewolf), нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «РБШ 2С35-1 (Коалиция- СВ) БВЭ.zip». Внутри указанного архива содержится вредоносный файл с расширением «.scr». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типов «дроппер» (TMCDropper) и «бэкдор» (TMCShell).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hxxps[:]//telegra[.]ph/1821344345856-02-26;

hxxps[:]//telegra[.]ph/791645547103-01-13;
hxxps[:]//telegra[.]ph/973163812793-02-06-2;
hxxps[:]//telegra[.]ph/166019571712-02-25;
hxxps[:]//telegra[.]ph/428609015723-12-15;
hxxps[:]//telegra[.]ph/791645547103-01-14;
hxxps[:]//telegra[.]ph/427509323253-02-02-2;
hxxps[:]//telegra[.]ph/904200825856-03-03;
hxxps[:]//telegra[.]ph/135239756800-03-02;
hxxps[:]//telegra[.]ph/1366278687744-03-01;
hxxps[:]//telegra[.]ph/1359266484096-02-28;
hxxps[:]//telegra[.]ph/590305414912-02-27;
45[.]93[.]95[.]91;
83[.]229[.]70[.]5;
212[.]80[.]205[.]9;
178[.]208[.]78[.]11;
212[.]80[.]205[.]31;
83[.]229[.]70[.]226.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикаторов компрометации, указанных в приложении к настоящим рекомендациям.