Бюллетень информационной безопасности от 11.03.2025

I. Сведения об уязвимостях.

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

1. Уязвимость пакетов программ Microsoft Office, Excel и 365 Apps for Enterprise (BDU:2025-01553, уровень опасности по CVSS 3.0 – высокий), связанная с разыменованием недоверенного указателя. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код.
2. Уязвимость пакетов программ Microsoft Office, Excel и 365 Apps for Enterprise (BDU:2025-01550, уровень опасности по CVSS 3.0 – высокий), связанная с возможностью использования памяти после освобождения. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код.
3. Уязвимость компонента NTLM Hash операционной системы Windows (BDU:2025-01633, уровень опасности по CVSS 3.0 – средний), связанная с раскрытием хешей в результате некорректного внешнего управления именем или путем файла. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, проводить спуфинг-атаки и получить несанкционированный доступ к защищаемой информации.
4. Уязвимость пакета офисных программ LibreOffice (BDU:2025-00554, уровень опасности по CVSS 3.0 – средний), связанная с недостаточной защитой служебных данных. Эксплуатация уязвимости может позволить нарушителю раскрыть конфиденциальную информацию.
5. Уязвимость функции psi_write компонента psi.c ядра операционной системы Linux (BDU:2025-00843, уровень опасности по CVSS 3.0 – высокий), связанная с записью за границами буфера. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.
6. Уязвимость ядра операционных систем Windows (BDU:2025-00382, уровень опасности по CVSS 3.0 – средний), связанная с недостаточной защитой регистрационных данных. Эксплуатация уязвимости может позволить нарушителю раскрыть защищаемую информацию.
7. Уязвимость DHCP-клиента операционных систем Windows (BDU:2025-01532, уровень опасности по CVSS 3.0 – высокий), связанная с возможностью использования памяти после освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.
8. Уязвимость службы Core Messaging операционных систем Windows (BDU:2025-01548, уровень опасности по CVSS 3.0 – высокий), связанная с переполнением буфера в динамической памяти. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

В целях предотвращения возможности эксплуатации указанных в пунктах 1-8 уязвимостей 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).

9. Уязвимость функций PQescapeLiteral(), PQescapeIdentifier(), PQescapeString() и PQescapeStringConn() библиотеки libpq системы управления базами данных PostgreSQL (BDU:2025-01601, уровень опасности по CVSS 3.0 – критический), связанная с непринятием мер по защите структуры запроса SQL. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, 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 межсетевого экранирования для ограничения удаленного доступа к уязвимому программному средству;

использовать «белый» список IP-адресов для ограничения доступа к веб-интерфейсу управления уязвимого программного средства;

использовать SIEM-системы для отслеживания попыток эксплуатации уязвимости программного средства;

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

10. Уязвимость функции addRelatedObjects универсальной системы мониторинга Zabbix (BDU:2024-10543, уровень опасности по CVSS 3.0 – критический), связанная с непринятием мер по защите структуры запроса SQL. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии путем отправки специально сформированного SQL-запроса через прикладной программный интерфейс (API).

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 доступ пользователей к прикладному программному интерфейсу уязвимого программного обеспечения;

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

отключить (удалить) неиспользуемые учетные записи пользователей уязвимого программного обеспечения;

произвести минимизацию пользовательских привилегий.

11. Уязвимость драйвера вспомогательных функций (реализации) прикладного программного интерфейса Winsock операционных систем Windows (BDU:2025-01475, 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 путем отправки специально сформированных запросов.

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 SIEM-системы для отслеживания попыток эксплуатации уязвимости;

использовать системы обнаружения и предотвращения вторжений для отслеживания индикаторов компрометации;

произвести минимизацию пользовательских привилегий;

отключить (удалить) неиспользуемые учетные записи пользователей.

12. Уязвимость функции move_page_tables() ядра операционной системы Linux (BDU:2025-00297, уровень опасности по CVSS 3.0 – высокий), связанная с ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии и выполнить произвольный код.

13. Уязвимость функции tcp_twsk_unique() в модуле net/ipv4/tcp_ipv4.c реализации протокола IPv4 ядра операционной системы Linux (BDU:2024-04557, уровень опасности по CVSS 3.0 – средний), связанная с повторным использованием ранее освобожденной памяти из-за конкурентного доступа к ресурсу (состояние гонки). Эксплуатация уязвимости может позволить нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации.

В целях предотвращения возможности эксплуатации указанных в пунктах 12-13 уязвимостей рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

14. Уязвимость функции pam_sm_authenticate() модуля аутентификации PAM-PKCS#11 операционных систем Linux (BDU:2025-01619, уровень опасности по CVSS 3.0 – критический), связанная с ошибками аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти процедуру аутентификации и получить несанкционированный доступ к защищаемой информации.

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 альтернативные средства многофакторной аутентификаци;

использовать системы мониторинга событий для отслеживания попыток аутентификации.

15. Уязвимость библиотеки SPID.AspNetCore.Authentication программной платформы ASP.NET Core (BDU:2025-01829, уровень опасности по CVSS 3.0 – критический), связанная с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить несанкционированный доступ к защищаемой информации путем отправки специально сформированного SAML-ответа.

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 уровня веб-приложений;

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

16. Уязвимость компонента Disk Cleanup Tool операционной системы Windows (BDU:2025-01894, уровень опасности по CVSS 3.0 – высокий), связанная с ошибками обработки символических ссылок. Эксплуатация указанной уязвимости может позволить нарушителю повысить свои привилегии.

17. Уязвимость модуля net/vmw_vsock/vsock_bpf.c ядра операционных систем Linux (BDU:2025-01465, уровень опасности по CVSS 3.0 – средний), связанная с разыменованием указателей. Эксплуатация указанной уязвимости может позволить нарушителю вызвать отказ в обслуживании.

18. Уязвимость модуля net/vmw_vsock/virtio_transport_common.c ядра операционных систем Linux (BDU:2025-01393, уровень опасности по CVSS 3.0 – средний), связанная с разыменованием указателей. Эксплуатация указанной уязвимости может позволить нарушителю вызвать отказ в обслуживании.

19. Уязвимость сервера средства криптографической защиты OpenSSH (BDU:2025-01893, уровень опасности по CVSS 3.0 – средний), связанная с неконтролируемым расходом ресурсов. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

20. Уязвимость компонента VerifyHostKeyDNS средства криптографической защиты OpenSSH (BDU:2025-01959, уровень опасности по CVSS 3.0 – средний), связанная с недостатками обработки ошибок при проверке ключа хоста. Эксплуатация указанной уязвимости может позволить

нарушителю, действующему удаленно, провести атаку межсайтового скриптинга (XSS).

В целях предотвращения возможности эксплуатации указанных в пунктах 16-20 уязвимостей рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

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 Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица российских телекоммуникационных компаний. Во вложениях указанных писем содержится вредоносный исполняемый файл с наименованием «22897 04.02.2025.pdf.exe», после открытия пользователем которого 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 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 следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hxxp[:]//vniir[.]nl/file/pas[.]rar;

hxxp[:]//vniir[.]nl/file/driver[.]exe;

hxxp[:]//vniir[.]nl/file/bk[.]rar.

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):
bb243113d236f823abd1839025190e763fe34c40da4949b77558995cc1a07625;
016adffeddba27bb29a225d86684bd9b7346bcf92d5c82134193264aa484208b;
1fbdad264ad5104c116263e391b408af22892111bcdfb825b4af28b633de4be5.

2. Хакерской группировкой Stone Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица представителей российских энергетических и промышленных компаний (например, ООО «Башкирэнерго», ПАО «Т Плюс» и ООО «Альянс-Автоматика»). Во вложениях указанных писем содержится вредоносный исполняемый файл с наименованиями, например:

«Скан_Башкирэнерго_ТЗ_44-01_29.01.2025_annexe.pdf»,

«Скан_Т-Плюс_ТЗ_№2679_30.01.2025_annexe.pdf»,

«Скан_А-Автоматика_ТЗ_57_29.01.2025_annexe.pdf».

После открытия пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки, загрузка и внедрение 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:

wmiadap[.]cdf;
wmiadap[.]sbs;
wmiadap[.]cfd;
hxxp[:]//wmiadap[.]cfd[:]6180/x.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
9d77a413c201860740e56a9838b1aa1956e4325c64ba03da9d25a13675b0f7440;
64a9ab3133816aeca13e3c462412d253c536638d378f04c025659cd497a51506;
8519cdce7d8b3b39bdcaaf808e4d90db18d7343937b2bc82f4fe856da00686f4;
ddd69518d5eda3d9be7376ea7d58c333f5ce1d2a96ee0d63150edfb6dff882db;
84cccdadde94763591bb6ae4173c4e8db54902a1a29ceb6ad42d9958bc7fba3d;
9d18e2c752672ac055f99f353b200cd09a3102b5a68222998aca88857f226b9d;
527363530ca1f822108681b26b74dd131f1d48b5b12f494a8193d877e2359062.

3. Хакерской группировкой Stone Wolf, нацеленной 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 «win_x64_update_20250130.exe», замаскированный под установочный файл легитимного программного обеспечения «1С:Предприятие». После запуска пользователем указанного исполняемого файла осуществляется установка указанного легитимного программного обеспечения, загрузка и внедрение 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:

77[.]239[.]124[.]207;
195[.]14[.]123[.]49;
wmiadap[.]xyz;
mofcomp[.]space;
hxxp[:]//mofcomp[.]space[:]7180/t.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем

внесения в правила корреляции событий следующего индикатора компрометации (sha256) 44b0c764da5f1981f719904d8f7ac5cbc3dab2141bbf3f71a9f0e3842e71bc1f.

4. Хакерской группировкой Fluffy Wolf, нацеленной 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 «Doc_1_buh_1C_akt.pdf.exe», замаскированный под финансовый документ. После запуска указанного файла осуществляется внедрение вредоносного программного обеспечения типа «стилер» (PureLog Stealer).

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 IP-адресу 195[.]26[.]227[.]209, 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):
159425f2830cb43e5cbff862456ee37a25fe31bd2ba0f58d7361c60aea79de3f;
82ec5adfa3ba3fe0dd0b2f287528bb54812d61171534e804677d30f952f4b40b;
27edcc980888f34e958b8de88d76e693ac0cc55d26bad3ce11146ba5118a6d1b.

5. Хакерской группировкой Fairy Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится архив. Внутри указанного архива содержится вредоносный исполняемый файл с наименованием «Условия.pdf.hta», после запуска пользователем которого осуществляется демонстрация документа-приманки с наименованием «Список гум помощь.pdf» и выполнение вредоносного VBS-скрипта. Указанный скрипт выполняет загрузку и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Unicorn).

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 vm-tiktok[.]org, 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):
207ed2a3882b6f66e26a5a31a48414fa9c3f4167ba28412fcffecce6f9ed66a4;
35380d08e09618beef490af405a777a729802bbaa81366e49a66bb1720cd9c4b;
4e96f10a6c67aec709c53bf36983af561993b3b95d70c7abfa3cbfe9344177a3;
b6e0c2af4398154ed528e370c5fe2435acdee9f75f3c8459df37436ef8f251af.

6. Хакерской группировкой Red Wolf (RedCurl), нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится файл-приманка с расширением «.pdf». В тексте указанного файла-приманки пользователю предлагается перейти по ссылке для связи с отправителем. После перехода по фишинговой ссылке осуществляется загрузка на целевую систему архива, внутри которого содержится файл с расширением «.img». После запуска пользователем указанного файла осуществляется открытие образа диска, в котором содержится файл с расширением «.scr». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение вредоносного программного обеспечения типа «загрузчик» (EarthKapre).

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:

cvsend[.]resumeexpert[.]cloud;
live[.]itsmartuniverse[.]workers[.]dev;
datascience[.]iotconnectivity[.]workers[.]dev;
sm[.]vbigdatasolutions[.]workers[.]dev;
community[.]rmobileappdevelopment[.]workers[.]dev;
mia[.]nl[.]tab[.]digital;
hxxps[:]//cvsend[.]resumeexpert[.]cloud/id/45bc4c3c-e212-43ab-a5d3-1a668c2df00e/kAal108.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
c6ef0416f7008882317696e66b93885170f5999968bc36d9165d313fa57ef041;
868d382f98a4465b239f9e5b6dc91a46ada7f334df26af9e780dd7fa74dc4e3c;
e6715e140ecab861235ae01c84345f7453847a9ba330512a37137bdf9e908edb;
bd5099e03d81613802d6ef4c2743195cb6e31d37b35a71011c924e66c40e6635;
ff3706e94d9b769f78e4271928382426cb034b11c5a0f6a8ffea35726cc03692;
e451287843b3927c6046eaabd3e22b929bc1f445eec23a73b1398b115d02e4fb.

7. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляется распространение через фишинговые сайты вредоносного программного обеспечения типа «троян удаленного доступа» (SocGholish), замаскированного под обновления популярных браузеров (например, Google Chrome, Mozilla Firefox, Yandex Browser и др.).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок, необходимо осуществлять обновление программного обеспечения (браузеров) из доверенных источников.

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

djdi6tukqamtyym[.]top;
bmadfjbhnijhckh[.]top;
miutubzxe[.]top;
rosettahome[.]top;
r3vgxgl24fywid4[.]top;
query-dns-cdn[.]com;
cdns-clfr-dns[.]com;
akami-cdns[.]com;
64[.]52[.]80[.]211/1[.]php?s=boicn;
web3-authframe[.]top/st1?s=exodus_24;
web3-authframe[.]top/st1h?s=exodus_24.

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

c7aa85c0b97c8f1f6f119109df02e0f33aa7cd495dd7399a39927c9f1fbc258b;
5051f0aa11da67e16797daa51992467ad45c5bf18dcd2e252e8aa63d3fce31bc;
91e405e8a527023fb8696624e70498ae83660fe6757cef4871ce9bcc659264d3;
f39319312a567fa771921d11ece66f3ce8996ba45f90d6fc89031b621535eb7e;
40ebd719aa66a88e261633887ed4e2c144bd11fbcc6f7793f9b32652cc5bf2d3;
33ea72b46af7bb2ecc0775f7536d3259f34bd7a13e298cac66649ee694097c2e;
44dc2777ee8dd6d5cd8ebb10e71caf73b330940131417b5fca2b174a264e19e3;
f2a1488df1036549da2da37bd9cbc2b411c3bb2c3d4d431bc2e86a744578ad37.

8. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится файл-приманка с расширением «.lnk», замаскированный под официальный документ. В тексте указанного файла-приманки пользователю предлагается установить легитимное программное приложение для проектирования

«Компас», перейдя по ссылке. После перехода пользователем по указанной ссылке осуществляется установка указанного легитимного программного обеспечения и внедрение вредоносного программного обеспечения типа «стилер» (Lumma 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 следующим адресам, используя схему доступа по «черным» или «белым» спискам:

tripeggyun[.]fun;
processhol[.]sbs;
librari-night[.]sbs;
befall-sm0ker[.]sbs;
p10tgrace[.]sbs;
peepburry828[.]sbs;
owner-vacat10n[.]sbs;
3xp3cts1aim[.]sbs;
p3ar11fter[.]sbs;
smiteattacker[.]org;
yuriy-gagarin[.]com;
vladimir-ulyanov[.]com;
nikolay-romanov[.]su;
aleksandr-block[.]com;
misha-lomonosov[.]com;
sputnik-1985[.]com;
lev-tolstoi[.]com;
hxxps[:]//80[.]76[.]51[.]231/Kompass-4[.]1[.]2[.]exe;
hxxps[:]//80[.]76[.]51[.]231/Samarik;
hxxp[:]//87[.]120[.]115[.]240/Downloads/254-zebar-school-for-children-that-tej-pro-order-abad-rural[.]pdf[.]lnk;
87[.]120[.]115[.]240;
80[.]76[.]51[.]231.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
bb2e14bb962873722f1fd132ff66c4afd2f7dc9b6891c746d697443c0007426a;
e15c6ecb32402f981c06f3d8c48f7e3a5a36d0810aa8c2fb8da0be053b95a8e2;
40b80287ba2af16daaf8e74a9465a0b876ab39f68c7ba6405cfcb41601eeec15.

9. Хакерской группировкой Fluffy Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые

рассылки электронных писем от лица «ООО ЗАВОД ВОЛГА ПОЛИМЕР» с тематикой «заказ на покупку». Во вложениях указанных писем прикреплен архив с наименованием «заказ на покупку.arj», содержащий вредоносный исполняемый файл. После открытия пользователем указанного исполняемого файла осуществляется загрузка и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (QuasarRAT).

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:

196[.]251[.]71[.]142;

hxxp[:]//196[.]251[.]71[.]142/win32/panel/uploads/Fmcqcdce[.]vdf.

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

2bef42440781af7998c27fd76b5baf7649852e995e73abcf039053bf49f179a6;

21ff5ebd865aee71a6713d5888639db0c93e17d7affbe83877ac4b6ffbbbae52.

10. 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 «Информационное письмо. Гранты, премии Распоряжени_PDF_.exe». После открытия пользователем указанного исполняемого файла внедрение вредоносного программного обеспечения типа «кейлоггер» (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 осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

07861e9666c68b4f15f766da755e76b02fef579e0ba97dd533e31d7efc1d13a6;

37c6e4ce9eee9bdaafa55b644aa53671cc6a204ae262ab8f37106c1d7349ccf6;

f82d5a6ceb18a206bee9700dee7fa3aa3049ac7cbe0d8368591ea1ea6de6f27c.

11. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляется внедрение вредоносного программного обеспечения типа «шифровальщик» (LockBit) на целевые системы при успешной реализации компьютерных атак через подрядные организации. Кроме того, для осуществления удаленного доступа,

закрепления в целевой системе и дальнейшего распространения вредоносного программного обеспечения внутри инфраструктуры злоумышленники используют различные инструменты, например, Mimikatz, NetExec, NBTscan.

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

213[.]165[.]84[.]7;
198[.]167[.]193[.]92;
194[.]226[.]49[.]147.

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

37ddeef565d9679f2d7cd5f75aa6d3f39e5086f03bd3d3a0f7fe478d25bc1c8b;
6d5bd06f09aad4f55379567af48458d63d59098e6e7f51116f5c815af8568038;
dc12cb7101c0e0582d013b6b60fbbfbdf8a16a4f00d8ac44e8a7849169bb1367;
2cf3248c08fe13385c41047a67b9e3134bfbfd94a6e7861a024be7a8a420a7ce;
74e987ef2596732cb3cc338270e96ce19412231305e3376aed2e49ebc364d885;
a6acbb9a00ac9a978109ae972bbe5e5a739417cb0f0a967cd95ca9b3255832ad;
e79d57168593a3d8b71a8c07ae8c8d2e9041e025d991d3a2cfbc4f836e85bf37;
5938bcdc325b100e3d2e3b20ae25b78deb15d50e81462580b925c7b3ed1bda1f;
42b8ecfd3a093131f52688304a99cac4f643247ef04cb5bb32dad7e4e2323f25;
47c75f77e5d6799a3ce1ec33f7be851bea93bd00566d6865bc0ba5821cbba4d8;
f4ba92f3280a21833f6ab6cdf67a956e96c1299df23b62d0ca3eb7c4b68429d1;
186f8bb178e03408890874cd134951279a4e73565e6c82f3c09d2eccc6694e23;
336eb14672abe2a43c609d20be7deacc837e3da71864c21eb488a47869785f95;
ee4fbe88f0f02018cc659bf95368ffda5db5e7749d07afe3d7250a20e9390b1a;
1cb4a643cb7dad2cae127e6b8e1e80ee30445f9514ae7775590844f95d739fea;
b4b903762f196595731bfbabcd96fb004a052f0a8a778bf3047d5419fb423dfb;
35247745562c939bbf2dca7b9283e8693101e8c865c5a49bad1b8ef8fa8a879c.

12. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Срочно: Просьба проверить и подтвердить сверку». Во вложениях указанных писем содержится вредоносный файл с наименованием «21.02.2025.xlsm», после запуска пользователем которого осуществляется демонстрация документа-приманки, выполнение вредоносного JS-скрипта и внедрение вредоносного программного обеспечения типа «загрузчик».

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:

103[.]152[.]255[.]227;
181[.]49[.]105[.]59;
acusense[.]ae;
hxxp[:]//181[.]49[.]105[.]59/649566714;
www[.]befiler[.]com.

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

7dc74a89d6d5745218c395d064df54df39d1ab4cbfc388bed234f35333901780;
f16578fdsffc8b4934557025599647b8540a39bd299a9ssfbs6fczed7se11c97;
854bc205d704d75ace0c730c434da11f311d6ee15cf6668897db3e740d0fcde5;
2f045bdd1d60e37d98ee8d660208b77b839770fe6fbefb4001a694a24ba04632;
6a98b438b67da7316e9251eb1a92cd5384a8349d239a77903f7282fa076a77c3.

13. Хакерской группировкой Sticky Werewolf (Angry Likho), нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится защищенный паролем архив с расширением «.rar» (напрмер, «Приглашение на ВКС.rar»). Внутри указанного архива содержатся два вредоносных файла с расширением «.lnk» и файл-приманка. После запуска пользователем указанных файлов осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (LummaStealer).

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:

testdomain123123[.]shop;
averageorganicfallfaw[.]shop;
distincttangyflippan[.]shop;
macabrecondfucews[.]shop;
greentastellesqwm[.]shop;
stickyyummyskiwffe[.]shop;
sturdyregularrmsnhw[.]shop;
lamentablegapingkwaq[.]shop;

innerverdanytiresw[.]shop;
standingcomperewhitwo[.]shop;
uniedpureevenywjk[.]shop;
spotlessimminentys[.]shop;
specialadventurousw[.]shop;
stronggemateraislw[.]shop;
willingyhollowsk[.]shop;
handsomelydicrwop[.]shop;
softcallousdmykw[.]shop.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикаторов компрометации (md5), указанных в приложении.

14. Хакерской группировкой Stately Taurus, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится архив с расширением «.zip». Внутри указанного архива содержится вредоносный файл, после запуска пользователем которого осуществляется внедрение вредоносного программного обеспечения типов «загрузчик» (PubLoad), «бэкдор» (ToneShell) и «троян удаленного доступа» (Bookworm).

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:

123[.]253[.]32[.]15;
123[.]253[.]35[.]231;
www[.]fjke5oe[.]com;
update[.]fjke5oe[.]com;
www[.]i5y3dl[.]com;
www[.]hbsanews[.]com;
www[.]b8pjmgd6[.]com;
www[.]zimbra[.]page;
www[.]ggrdl4[.]com;
www[.]gm4rys[.]com.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикаторов компрометации (sha256), указанных в приложении.

15. 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 расширением «.exe», замаскированный под легитимный документ. После запуска пользователем указанного файла осуществляется демонстрация файла-приманки, выполнение вредоносного VBS-скрипта и внедрение вредоносного программного обеспечения типа «кейлоггер» (Snake Keylogger) и легитимного программного обеспечения для удаленного доступа «AutoIt».

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 hxxp[:]//51[.]38[.]247[.]67[:]8081/_send_php?L, 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 (md5):

f8410bcd14256d6d355d7076a78c074f;

77f8db41b320c0ba463c1b9b259cfd1b.

16. Хакерской группировкой Erudite Mogwai, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются компьютерные атаки путем компрометации публично доступных сервисов. В случае успешной реализации атаки злоумышленники осуществляют распространение вредоносного программного обеспечения типов «бэкдор» (LuckyStrike Agent) и «троян удаленного доступа» (Shadowpad Light) для дальнейшего закрепленияв инфраструктуре.

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки, необходимо:

провести инвентаризацию сервисов (служб), функционирующих в информационной инфраструктуре органа (организации), которые в перечне публичных (внешних) IP-адресов доступны из сети Интернет;

определить легитимность доступных по открытым портам сервисов, IP-адресов, сетевых служб, доступ к которым возможен за периметром информационной инфраструктуры органа (организации). В случае невозможности отнесения их к легитимным осуществить их блокировку;

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

wiod[.]mynetav[.]net[:]443;

46[.]17[.]43[.]99[:]443.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
ce5045a20bcbc0e8386485dcf66ca58d02b026c47de649720d13cad71d564e90;
661f88afb7fbe1c6b83596f4e42a91fd3e8fc0a2e7fb9632536b9a6006f5f898;
b0784c92bbb372062bc1d805316913b50b0f8cfb8696e33af26b61b8abc307ad;
4e0b608982cc37dc08d3f099c1783290fcc959421cb0d7703ca1210990d02c93.

17. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица представителей федеральных органов исполнительной власти. Во вложениях указанных писем содержится файл-приманка, после запуска которого пользователю предлагается перейти по ссылке для обновления программного обеспечения для просмотра указанного файла. После перехода пользователем по указанной ссылке осуществляется загрузка и внедрение на целевую систему вредоносного программного обеспечения типов «стилер» (Meduza Stealer) и «бэкдор» (ReaverDoor).

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:

hxxp[:]//62[.]197[.]48[.]140/res[.]js?id=1;
hxxp[:]//62[.]197[.]48[.]140/res[.]js?id=2;
5[.]42[.]73[.]251[:]15666;
hxxps[:]//openmailertrack[.]com/;
hxxps[:]//alarti[.]ru/mobile_app/;
hxxp[:]//62[.]197[.]48[.]140/v2/build/4/lib/examplep3msw;
hxxp[:]//62[.]197[.]48[.]140/tlog/logr[.]php;
45[.]136[.]196[.]76[:]15666;
hxxp[:]//62[.]197[.]48[.]140/v2/?a4f0aacc192c599841878e243792ee067fe994e0881a42b842331150e524098839e5f8e95308933e2da4e78128ff9f40;
hxxp[:]//62[.]197[.]48[.]140/v2/build/6/lib/examplep3mswMSm/;
hxxp[:]//62[.]197[.]48[.]140/tlog/;
hxxp[:]//62[.]197[.]48[.]140/connect/.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (md5):
dd9fa916c5f14c66b2e83243808072d2b084828167f9f2029366c91023c49532;
11e036461b9dfa27fda024e77cd993a2052211c87a01ef4957515fc4ae71dac2;

1c0916151fecb515237bb36bc533db16449990cdcc37c3c5e801b76977d1df8e;
c8a9b64552498453d15fddfa92f550b178ebb4db14d7335052c1b95e681810a8;
d40224818c5740d0dbf5990d7d457ba64f32e5fe573da74ce6c970210f4eacca;
850a577ac47759faabdda4bcf39876cfcfd2ec4ec549402e1cb22b3c2f47e4b3;
a6cdfba0c7cdeb09ec0cb07907a1d85040938df924b3f937f4d5e8c503b4d77d;
87e958acaff20e8cbcbf7febbf216f327ac5a8d816eafdc0f16ceee39bc2a0a4;
7bef68a99e3396721ed90e5d7257da53c33aa7a2c9ea8c376922b922ee05ae89;
d0253d173616a7e2dc12fdd10682ca2581da0ac8d4f7af6e7365a571e353398d;
850a577ac47759faabdda4bcf39876cfcfd2ec4ec549402e1cb22b3c2f47e4b3;
e9568cd742af5d6f2facbd789cfe349b13518524eab518e6d3bb99ac3809b6dd;
a9c94fc0d0538736647fcb49891b273ed3d6166692dbe2f56a94f6a9ffacf12b;
c2c873a1b504913d15d78683d138d066c22860ded6ffef15d4704b0798062090;
fd97409a782b56886ee0afa33c556d943a8408c053c925d3aa4af979a4c7515d.

18. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица ТОО «КЕН-САРЫ». Во вложениях указанных писем содержится архив с наименованием «РО-МТ-25-018-01.7z», внутри которого находится вредоносный файл с наименованием «РО-МТ-25-018-01.vbs». После запуска пользователем указанного файла осуществляется загрузка и внедрение вредоносного программного обеспечения типов «кейлоггер» и «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 ограничить получение электронной почты с адреса csa[.]taf@yakhroma[.]com и обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

yakhroma[.]com;

78[.]132[.]141[.]85;

hftook7lmoutsg1[.]duckdns[.]org.

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

b51671564147c1fe7b29b542a49cf2bcf7d7e9316fe46babbceefc6aad3b0c42;
246f9bf383ddbd9ba648a07eb53947ce28cb245531274f503a1642a7f388b2e8;
c9714db43da197c08d0c53f697d857cfcbda18163a5fc758fd57fd16fd6a563f;
0dc1074384598dd74620d35066e7e84c9e845cc1dfecd475c1ca8cb054167201.

19. Хакерской группировкой Core Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые

рассылки электронных писем, во вложениях которых прикреплен исполняемый файл, замаскированный под легитимный документ с наименованием «Отсканированные _документы _План_работы_робочих_ групп_МО_и_ПУ_по_изучению». Указанный исполняемый файл является вредоносным программным обеспечением типа «дроппер», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение легитимного программного обеспечения для удаленного доступа «UltraVNC».

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:

emoneyrabota[.]ru;

hxxps[:]//emoneyrabota[.]ru.

Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
22effd31ca77182685166915bc1b2883ce2c08350011ab90b3fc2e62ad1b61f8;
ff9ada05ba255ee71529a3e4d9177c9d562beb2f700de21ffdff37d88032ce2d;
2ab7240d99a813a4bfbf420a19cbf0a40f31b7ae681afc86f95fa136ee29a1a5;
33056acc92789add4fd0ae280eb2c27d3108fc17587f91091d132072a8440526;
9160e464f172425539f108458435265729e15040f03b0e8b9efee27d49787b53;
87b570e1b299bb9d57b5b3a1df0073fdda1177b9def3d153fc2a155b51b9bcac;
c62605046955b0a05cb600d77045001ff7352d4d4546b52b4f3d3136211e898c.

20. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с просьбой подписать юридические документы. Во вложениях указанных писем содержится архив с наименованием «ScanDocuments6524667698pdf56478898087946765.rar», внутри которого находится исполняемый файл с наименованием «fac876545678900098.exe» и файлы с наименованиями «tier0_s64.dll» и «vstdlib_s64.dll». После запуска пользователем указанного исполняемого файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (SnakeLogger).

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 akimjanova[.]g@asia[.]kg и осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем

внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
d7f11bcde1d4ee9229317c7cfee071ea73a53683a6293d3cd10d082e736729f1;
e55b48206c8d124140a64f2897f027e4e438cbcf35af2c7b94dc4a632f32556c;
d25b201fa604edb2856c68e2d44a66d899d860602c001cf4619a9fac77f81e3c;
494e0cd842d9ca80f678dff69043299e530b1e6e29142e0427b0da7b18bef58f;
6296888dd4e50eb21f4ec72f2d9beb9c04285dc8130260ffc2b5de73fa168a54;
027be8638e1e309810aad09a6feb5fadb658cca15c611e28a84324f7ddc83326.

21. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный исполняемый файл, замаскированный под договор поставки. 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 (sha256):
3bc29c85ee83110aa086df587624da35dfa350d5157f409cda83fcda5a70606c;
916920bfaa2b7bf0c1183372a264bc7d9f709c62b8419850dc5dda1d99df299d.

22. Хакерской группировкой Sapphire Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Служебная записка». Во вложениях указанных писем содержится вредоносный исполняемый файл с наименованием «служебная записка.exe», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение вредоносного программного обеспечения типа «стилер» (AmethystStealer).

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[:]//civet-lucky-bug[.]ngrok-free[.]app;

hxxps[:]//wondrous-bluejay-lively-ngrok-free[.]app;

hxxp[:]//canarytokens[.]com/traffic/tags/static/xjemqlqirwqru9pkrh3j4ztmf/payments[.]js.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
4149b07d9fdcd04b34efa0a64e47a1b9581ff9d1f670ea552b7c93fb66199b5f;
29548fb375288b25a163b83932ac330f5154d3246fe310461f40f32b02bdfa61.

23. Хакерской группировкой Squid Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Предложение о работе». Во вложениях указанных писем содержится защищенный паролем архив с наименованием «Предложение о работе.zip», внутри которого находится вредоносный файл с наименованием «Предложение о работе.pdf.lnk». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения.

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 электронной почты с адреса info@industrial-complex[.]ru и обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hwsrv-1253398[.]hostwindsdns[.]com;

hxxps[:]//hwsrv-1253398[.]hostwindsdns[.]com/307c77ab-f41f-4dd4-a478-2a71b9625f64/c/discountcode[.]php;

hxxps[:]//hwsrv-1253398[.]hostwindsdns[.]com/307c77ab-f41f-4dd4-a478-2a71b9625f64/c/shoppingcart[.]php.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
49a2ed08930ed20cbf859ca2fe3113e64f7a305c7a03cbda284fcceb781d053b;
20dd93441c5e78b7adc7764c92719bed70ddb0676f707df7ea9f37d7969f4776;
0601426a6da40ec9b47bab54e4ec149ba69ee58f787eea0e32d1001cab1abd04.

24. Хакерской группировкой Stone Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержатся вредоносные исполняемые файлы, замаскированные под легитимные документы, например, «Scan_Kartochka_2D_Group_ind_fdp.exe»,«Scan_2D_Group_TZ_№3482_21.02.

2025_ind_fdp.exe» и «Scan_A9-Studio_TZ_67-02_19.02.2025_ind_fdp.exe». После запуска пользователем указанных исполняемых файлов осуществляется демонстрация документа-приманки и 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:

picyc[.]space;

hxxp[:]//picyc[.]space[:]7180/.

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

9eb007b3f2e744c0e669cf70831d5b66851921b2eb40500571b11f8505f2b553;
fbcfc9baf5b7b5c7d63ff4b8bf9cdc8ce2ee1b2670ec1504673ca57026568b7e;
3392aed3617be84e3550a68ec20bd4dc97ec4ea33867cb2fd63c3bd3236f42f9;
907a044172bb4841c02689c8a8f92bdb4b346f6a15a86fddbdf54360a30b618c;
90a17f37f9fdf9d87825da5a93c9864df47c508b963ab6fc5a79cb052a8de1b6.

25. 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 «Накладная №171-8314-0617.zip». Внутри указанного архива находится вредоносный исполняемый файл с наименованием «Накладная №171-8314-0617.exe», после запуска пользователем которого 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 следующим адресам, используя схему доступа по «черным» или «белым» спискам:

49[.]13[.]77[.]253;

195[.]149[.]114[.]21;

4ad74aab[.]store;

4ad74aab[.]site;

4ad74aab[.]space;

4ad74aab[.]fun;

791688a4[.]site;
942a8b18[.]store;
4ad74aab[.]biz[.]ua;
6e93d646[.]store;
f62a2474[.]space;
f55445cb[.]fun.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
a454fdc612637e229ce1138b7a599ea2936e6ea84b1391adc38b9a5abdb6c805;
66ee7011fdf4052fb960afdba3f30661b4cf29b99142ace75a8896a88d27183e.

III. Другие угрозы информационной безопасности.

По имеющейся в ФСТЭК России информации злоумышленниками осуществлен несанкционированный доступ к информационным системам ООО «ЛАНТЕР» и ООО «ЛАН АТМсервис», входящих в группу компаний «ЛАНИТ».

Отмечаем, что группа компаний «ЛАНИТ», осуществляет разработку программного обеспечения, в том числе специализированного, обслуживание информационной инфраструктуры, а также предоставляет вычислительные услуги и производит системные интеграции программного обеспечения и оборудования.

В случае, если организации, входящие в группу компаний «ЛАНИТ», оказывают услуги или осуществляют свою деятельность на объектах информатизации органа (организации), в целях нейтрализации угроз безопасности информации, связанных с несанкционированным доступом к информационным системам через подрядные организации, необходимо принять следующие дополнительные меры защиты информации:

сменить пароли учетных записей пользователей информационной инфраструктуры организации, учетных записей пользователей и сервисных учетных записей для программного обеспечения и оборудования, поставщиками которых являются организации, входящие в группу компаний «ЛАНИТ»;

ограничить удаленный доступ работников организаций, входящих в группу компаний «ЛАНИТ», которые осуществляют техническое сопровождение поставляемого ими программного обеспечения и оборудования. В случае невозможности ограничения удаленного доступа работников организаций, входящих в группу компаний «ЛАНИТ», необходимо обеспечить мониторинг их действий;

провести внеплановое сканирование на наличие уязвимостей в инфраструктуре организации. Принять исчерпывающие меры по устранению критических уязвимостей, выявленных в ходе сканирования;

обеспечить резервирование информации, обрабатываемой в сегментах информационных систем, где применяется программное обеспечение, поставляемое организациями, входящими в группу компаний «ЛАНИТ»;

временно (на 1 месяц) ограничить возможность получения электронной почты с адресов со следующими доменными именами:

lanit[.]ru;

cloud[.]lanit[.]ru;

fit-out[.]itlanit[.]ru;

itlanit[.]ru;

lanatm[.]ru;

lanit[.]tech;

oazis[.]lanit[.]ru.

Кроме того, осуществить проверку средствами антивирусной защиты всех входящих электронных писем, ранее полученных с адресов, относящихся к указанным доменным именам.

В случае необходимости осуществления взаимодействия с организациями, входящими в группу компаний «ЛАНИТ», использовать альтернативные каналы связи.