Бюллетень информационной безопасности от 30.01.2025

I. Сведения об уязвимостях.

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

1. Уязвимость обработчика JavaScript-сценариев V8 браузера Google Chrome (BDU:2025-00111, уровень опасности по CVSS 3.0 – высокий), связанная с ошибками смешения типов данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код с помощью специально созданной HTML-страницы.

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 использовать альтернативные браузеры, а также осуществить настройки операционных систем на базе Linux в соответствии с Рекомендациями по безопасной настройке операционных систем Linux, утвержденными ФСТЭК России 25 декабря 2022 г.

2. 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.

3. Уязвимость функции VSP Elevation ядра системы аппаратной виртуализации Windows Hyper-V операционных систем Windows (BDU:2025-00282, BDU:2025-00288, 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.

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.

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;

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

произвести минимизацию пользовательских привилегий;

отключить (удалить) неиспользуемые учетные записи пользователей.

4. Уязвимость реализации протокола службы каталогов LDAP (Lightweight Directory Access Protocol) операционных систем Microsoft Windows (BDU:2024-11128, уровень опасности по CVSS 3.0 – высокий), связанная с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

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

5. Уязвимость функции «ole32.dll!UtOlePresStmToContentsStm» компонента Windows OLE операционных систем Windows (BDU:2025-00539, уровень опасности по CVSS 3.0 – критический), связанная с возможностью использования памяти после освобождения. 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 обеспечению;

использовать SIEM-системы для предотвращения попыток эксплуатации уязвимости;

использовать виртуальные частные сети для организации удаленного доступа;

ограничить доступ к устройствам из внешних сетей.

6. Уязвимость механизма защиты Mark-of-the-Web архиватора 7-Zip (BDU:2025-00670, уровень опасности по CVSS 3.0 – высокий), связанная с нарушением механизма защиты данных. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код в контексте текущего пользователя.

7. Уязвимость сервера приложений Apache Tomcat (BDU:2024-11586, уровень опасности по CVSS 3.0 – средний), связанная с ошибками синхронизации при использовании общего ресурса в результате отсутствия учета регистра в файловой системе при записи сервлетов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанных в пунктах 6-7 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. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Договор». К указанным письмам прикреплен вредоносный архив с наименованием «Contact_0103.bz», содержащий исполняемый файл с наименованием «Contact_0103.exe». После запуска пользователем указанного исполняемого файла осуществляется загрузка и внедрение вредоносного программного обеспечения типов «стилер» и «кейлоггер» (Matiex Keylogger).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок 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[:]//checkip[.]dyndns[.]org/;

104[.]21[.]48[.]1.

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):
2b33fef538dd14fcd3103ad57025963d5108e3cacc61cf393177ce84dbd2a5a0;
e4f2a7707dc8781db5279fef6f56adf628981b82c6b9640f82af0f7decce8626;
9341ed285a5e894095430766621508822d6973ef98bfc442336de526c8ad762e;
0d20e797680c68374a796f64bb313b4d5bec45edee49402259d59bae6d1ef1ec;
dfa55b036f0c9fadcd13e0080349bddc01f287fa01f4a99f8ccdc386bcd9cd7c;
55582499c891c1c68cda0425a90d5c141a8f238785eab9c80ef03d9d5e6d14e4;
bbf06ad2102036a68f0c7cbbf971a92f5f2c884cc38ad625fb3bdbc479acd265;
52e4748a3a601272a37d34fb40167c6168d35f457f2fa9c9e3676df246e0ac71.

2. 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 «Исх 3548 о формировании государственных заданий на проведение фундаментальных и поисковых исследований БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типа «загрузчик» (LazyOneLoader).

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 phpsymfony[.]com, 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):
fdf0ea5d761352791545b1af0223853b31592996600c4ee5f1122e546c6165d3;
420866ad15d5de2a6cdfab7ca317e5b20090098ad905d7cac784719f3e33360c;
ad80cbf12e5bee38a197f7bcafbe24983fdd3df6915e5a33a01f0311685e8b24;
14b1cd92b0a95ec76b31b0c2ec498b90d82054206f1056a58844513f89baeb55.

3. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный файл с наименованием «Соглашение о сотрудничестве.pdf.lnk». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типов «стилер» (LummaC2, CryptBot) и «загрузчик» (HijackLoader).

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:

hxxp[:]//download[.]wsconnect[.]org/Downloads/Instruction_1928_W9COI[.]pdf[.]lnk;

hxxp[:]//download[.]wsconnect[.]org/Downloads/Agreement%20for%20YouTube%20cooperation[.]pdf[.]lnk;

hxxps[:]//docu-sign[.]info/api/uz/0912545164/update[.]bin;

hxxps[:]//docu-sign[.]info/api/uz/0912545164/config[.]bin.

Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
8220a9b7b5a2ca3188278ea2e576df9b96d2d23ddfddc2fd5260851dcff9218a;
8ea35c2bfdf4cad1197abadd19f4f0e09579afcfdb32abc7e71bb5818c6d3ba6;
6a4ccd0f0bf4985af98f5e40da68cff98881c45b2f32dc03619f78bf43418575;
c18219bff85d2db88626e0f3b45a55558e5adbabea84f8a8132313338fea2383;
76cf24666515ee68ffa0a4756884e42783af499d6ba01c1aaa5d352900af349a;
164bccacc811b573c359f001fc433ca7e08cae806422a33981aa446f502d28e8;
480667dd13f7ac103847dd7f19c61e4b676210568fa0dfc3a4f354e688618cae.

4. Хакерской группировкой Red Wolf, нацеленной на органы государственной власти и субъекты критической информационной

инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержатся вредоносные файлы, замаскированные под корпоративные документы. После запуска пользователем указанных файлов на целевых системах, функционирующих на операционных системах Microsoft Windows, осуществляется выполнение вредоносного Python-скрипта, загрузка и внедрение вредоносного программного обеспечения типов «загрузчик» (RedLoader) и «стилер» (RedCurl).

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:

bora[.]teracloud[.]jp;
103[.]139[.]238[.]168;
alphastoned[.]pro;
172[.]67[.]214[.]172;
23[.]254[.]224[.]79;
104[.]21[.]37[.]229;
cdn[.]wgroadcdn[.]workers[.]dev;
172[.]64[.]80[.]1;
104[.]21[.]22[.]32;
172[.]67[.]202[.]51;
sup[.]wgsphere[.]workers[.]dev;
172[.]67[.]182[.]51;
104[.]21[.]83[.]219.

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

f574a55706697d7e0109cf920ae6e0047cd7a802c9ad457e3b68e7802f3f902ef;
6d85ad9e14a23ed6bf700f636273b30f53c54267d0f624c8ff7bc0008f7db4f7;
8117e40ee7f824f63373a4f5625bb62749f69159d0c449b3ce2f35aad3b83549;
c75048a4933c3061f6cd02c8ca96ed524166fce4cc4b9e0c7ea6ac8295dc3c47;
1935692d1c4492f99c969d11d81481aea736f3899b1f55af9c8f6cf6ca9b839c;
8117e40ee7f824f63373a4f5625bb62749f69159d0c449b3ce2f35aad3b83549;
904669bd897dbb99561ef080d9818ff4bc9c106aa476d25b992439cdea4d1b0b;
9bdf91507fb4f3772a6d66a78f0f1f44075eefba4af65094c374f9d72e25bade;
ff3706e94d9b769f78e4271928382426cb034b11c5a0f6a8ffea35726cc03692;
01d94de4d104f6df121f97bae9cbbfada5a9cd4c3af0e1c403271d8284815cad;
9d667de8a99e757176cea1aa0af0d81972005d4abf3b7aff942d8c30fb151e35;
5a8314cbdccc7362a100b9db92b05597dad37c13b4cbb7b0fd1ef58d625dd454;

ea308c76a2f927b160a143d94072b0dce232e04b751f0c6432a94e05164e716d;
4af2c0c6087f9410cf57af4cf7eb09b5a3038bb78f4e50625402e32ad9662e66.

5. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляется применение вредоносного программного обеспечения типов «троян удаленного доступа» и «шифровальщик» (NonEuclid RAT) для получения несанкционированного доступа к целевой системе.

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):
d32585b207fd3e2ce87dc2ea33890a445d68a4001ea923daa750d32b5de52bf0;
e1f19a2bc3ce5153e8dfe2f630cc43d6695fac73f5aaa59cd96dc214ca81c2b0.

6. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный архив с расширением «.zip». Внутри указанного архива содержится файл, замаскированный под официальный документ, с наименованием «EMO.doc.lnk». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки, загрузка 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 осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha1):

3ea711d020b52fb0490c359462451d4edd471e33;

0a6d07305028ee7c919eba624b37ccaa5db94e75.

7. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, замаскированных под платежные документы. Во вложениях указанных писем содержится вредоносный архив с наименованием «Swift.zip», внутри которого находится файл с наименованием «MTS Swift-TT819163 Report.svg». После запуска пользователем указанного файла осуществляется демонстрация документов-приманок, загрузка и внедрение 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 осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикатора компрометации (sha1) dd25dec0930328ab772142bcc2e358aad8a468f8.

8. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лиц отделов продаж российских компаний. Во вложениях указанных писем содержатся вредоносные архивы с наименованиями «Дополнительное соглашение.rar» и «Заказ-100124.rar». Внутри указанных архивов находится исполняемый файл, после запуска пользователем которого осуществляется внедрение вредоносного программного обеспечения типа «стилер» (MetaStealer).

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 87[.]120[.]120[.]22, 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):

6439c8e94bd2398ad15bd8cbf86a9ca9528cecf77506357e894a359880282724;
08dd0ab36a9415209b81be233b07d50b6a67188f6f55394211f92b685b9c70bc;
55d86ccb8abb8c1bb2a2e296bdad97802334d2282620d3c918600a94bca8b176;
7286e70a695a65f15f3120765f0aed13b6203e8ec4d9904ec54fe05b9522aa95.

9. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Прилагается обновленный счет-фактура за январь-апрель 2025 г.». Во вложениях указанных писем прикреплен вредоносный архив, содержащий исполняемый файл. После запуска пользователем указанного исполняемого файла осуществляется внедрение 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 осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
b62d5df37446de70b4e907c3bde03f6c25d0d7ac04356e1a59fdeecbc73891ee;
1b52e44c59760177a472ccaf6815844814db6628aed607bdf89b13723fcc4fa5.

10. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, замаскированных под техническую документацию. Во вложениях указанных писем содержится исполняемый файл с наименованием «Корпусные детали/00.000.003.com», после запуска пользователем которого на целевую систему осуществляется внедрение легитимного программного обеспечения для получения 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):
2e6c843254da86c328286cad7871963291bcaa6ed9942a482828ce4bc44c84a6;
780a6923705c0b57c2003dd917dcc05d95e7f2e030e63229d52faf05721f1b6b;
ad79bb5b155e55c0f91016edd39ba4809214b738c1ed9ca905fbd7cabd612e04;
ab05b12cf346bab8c80d168e4438b7d12f7eb654bc5b344aa42eba743158e2e2.

11. 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 файл-приманка с наименованием «Письмо_в_организации_по_привлечению_осужденных.docx» и вредоносный архив с наименованием «Форма заполнения.rar». Внутри указанного архива содержится файл-приманка «список рассылки.docx» и вредоносный исполняемый файл с наименованием «Форма заполнения.pdf.exe». После запуска пользователем указанного исполняемого файла на целевую систему осуществляется загрузка и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (Ozone 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 обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:
45[.]155[.]249[.]126;
84[.]22[.]195[.]72;
bitbucket[.]org/5w457/ed512/downloads/emnfpac[.]txt;
hxxps[:]//bitbucket[.]org/ghjkkkkkkkk/tdrdreest/downloads/img[.]jpg?537612;
hxxps[:]//raw[.]githubusercontent[.]com/gmedusa135/nano/refs/heads/main/new_img123[.]jpg.

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

969977a682bac07eb1f9196041077d3c332b2b37;
0919987e12e51e55824959323ed23a9d3387fbad;
74f6f78bd8f1cc30e911350b60fe9b4eaf69e21c;
4c92e612f006838f10b50a9aa102c4430f9b8495;
d558d8501286b0b322a06a2e2f21fc6c03d45316;
861118c8a32157349c1d3dc76e774c027c05433c.

12. Хакерской группировкой Sticky Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лиц федеральных органов исполнительной власти Российской Федерации. Во вложениях указанных писем содержится вредоносный исполняемый файл с наименованием «АО-*******-12904ДО.pdf.exe», после запуска пользователем которого осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (Darktrack 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 обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

31[.]214[.]157[.]167;
31[.]214[.]157[.]49.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
3172bf0dd76232fc633214f0ba92b25d27b136a2ed5d9e4e7d06b0686ef4d34c;
3eca76737c6aee34b4c38845fde13bceed23a31d39e958893a44f42380ff84d5;
fd50307b7f08d037c5d37f2505c8de6edc9c57e1843f4434309a135f4b43ff5c;
5061e83a380a9c3ebe91bd5de80fe8f11b666a182efbebe13a1b0dfbc2842487.

13. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, замаскированных под нормативные акты и официальные документы. Во вложениях указанных писем содержится вредоносный архив с расширением «.rar», внутри которого находится исполняемый файл с расширением «.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типов «троян удаленного доступа» и «стилер» (Zagrebator).

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:

storages[.]supports-update[.]info;
fille[.]updates-drive[.]info;
dateo[.]drive-infos[.]homes;
updates[.]infosecur-date[.]homes;
mobis[.]my-android[.]homes;
fensesyste[.]defaces-homes[.]lol;
rk-simferopol-municipal[.]insurance-rus[.]shop.

Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
1c2ee5a5bc16ba130a51de02f1fe1e6560750e16e63e65f4f27c5ee2e74288d3;
09a0e99a1dcaafc901699c39a858d320b40e76d03566ee9f9a9ce6f772441c85;
f38ed3b1bc479248c09c3c69449ca6702aefc20a26074fb8e8e65442429e2591;
2d5ee1444a67c51194c6a9f01e23fd424c29b816b9cc0bd9d1d30ceba170f2d6;
59d7b48a2ed217609841472ff75b8c6db4568690d17563b2515eda4fba695aaf;
8d0cf230fd07a0e22c1937fd2b05e38bddb3bfb7cd6bd5fa27dd92dbe159876e;
95278a151be694e1fb2f7109ecfbea4442d83ff799962ee23c59a4208b0f6095;
878a94ead4c9deb3119993a0dcb9f35f38111d2d5840f529310fd6a24f6ebf0b;
84adf0841fc83f7220d330b59e5dc831d8975249c31aedace6ba7ae920a48b86;
1294a9c840603f2aeee1491d903f39fdbc6c3c77ca37db36769c048a889ab77a;
e36f92829bfaa7ba3e5c5ca769cc9a25b5a4cf8922e46ee4818fd0595621df4d;
0d41414c3eedaa62f4c8733204432fe93c66fec7320843ffcc66fb04497864e6;
29976fef84d04b1a3e95bdc1b0d7a5f8d7cd2dabba8e335796c368c2e6a1052d;
57b6e5c52ef3c15852602e86bb33339208195180e5407d941f6075254e511ff5;
00793b6f15ba77e7560f50c4506de1697ec3ae8868f5f3fe9a26a2bcceb78263;
194f719f9aff798fa02798b145ff473cde8c6886189c6c0849e1b17edd0ebd21;
90432fdc7cc151b99954deface5ce9c3520a158f5284ec5b5d7115c3bdb03d13;
585635b37f30c4e6e3a5a5d05642c1c7b32fd83fd842390d7ed58342e0105ee4;

eba4193e2008006eedacb18a45b5cd6d32ae6bbf53996f9b113c438a894f5076;
3b5ecd89ae691e1bfcbe20d9a31f38cb98c63cea076336982f9d04d74d80231c;
d5c6af702f225c218bda9f4ef2d2c2dbd64b7f834b939d66e75c47b94df46b6b.

14. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лиц промышленных компаний из Республики Казахстан. Во вложениях указанных писем содержится вредоносный архив, внутри которого находится исполняемый файл с наименованием «909302902920092.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типа «стилер» (FormBook).

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:

www[.]ok33r[.]shop;

hxxp[:]//www[.]ok33r[.]shop/3nop.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
4ad091fa8c8282a901e49a9e1ae14b26259292446bee75d73f76833e77091bee;
be3c139f71a35dd103525f6c3556baf0892289585c8d4051caf00d908f9da508.

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 файл с наименованием «doklad.xls.bin», замаскированный под документ Microsoft Excel. После запуска пользователем указанного файла осуществляется демонстрация документа-приманки, загрузка и внедрение 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 (sha1):

0181b6751c8c6225a4bebf3c663e7d72c2580eb5;
2bc7425ec98b7b0890aefb73dcfa4a8eab96acf7;
44177b6e5ef8095d059475a86172f5a9a609a241;
43743a7521757df583ab342755422587b8fd31a3.

16. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Коммерческое предложение и чертеж к нему». Во вложениях указанных писем содержится вредоносный архив с паролем с наименованием «КП и чертежи.rar», внутри которого находится исполняемый файл с наименованием «2_эт_ФЭО_затрат_внебюджета_на_дораб_пробукта_1.docx.scr». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки, загрузка 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):
a71e3e0cade4a9cf4848a17094e11436893e0d470f67c96699d6a8eef4e37554;
321b7473425dc9ae8ed0a1fb7e501a956df4ca3a91e310ca9523895328ddf72f;
0d39b1cea03cebe7014f91a36408616ae2ffd28b0c274123290fdb403cd42454.

17. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный архив с наименованием «Contract.bz», внутри которого находится исполняемый файл с наименованием «Contract.exe». После запуска пользователем указанного исполняемого файла осуществляется загрузка и внедрение вредоносного программного обеспечения типов «кейлоггер» и «стилер» (SnakeKeylogger).

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[:]//checkip[.]dyndns[.]org;
reallyfreegeoip[.]org;

104[.]21[.]48[.]1.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
08e2c1d9318e0a9e099aa995873d728cc4e36f7cce8325c2ad36cb191b89e24b;
a09257e46e2cc1434c890bcadfc725e41330227ffbf728059d9c8f4ebdaa4fba;
8004a9c84332b68b0a613a5de9dcf639e415feb14b3da926e164375f3c5a3609;
3a1f0f0c85df1ef9a91daa659ee261f8560136e39b9f86d6fd8b1a0f632eed69.

18. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный файл с наименованием «Наименование работ и затрат.xlsm». После запуска пользователем указанного файла осуществляется выполнение вредоносного VBA-макроса, который загружает и внедряет вредоносное программное обеспечение типа «бэкдор» (Xred).

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 hxxps[:]//www[.]dropbox[.]com/s/zhp1b06imehwylq/Synaptics.rar, 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):
af103ba44e86522db245d3f02779d58b404f7ce223a0d06fa8944f8a03ae0689;
e3a1f5c793d8cd45a09374af674821e6be8dbe77a6e2f6558ad5635cc0b14de2.

19. Хакерской группировкой Cloud Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с различными тематиками (например, «По антикоррупционной работе», «О кадровой системе ВС РФ»). Во вложениях указанных писем содержится вредоносный файл, замаскированный под легитимный документ Microsoft Office. После запуска пользователем указанного файла осуществляется загрузка и внедрение 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 обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hxxp[:]//cyberservice24[.]com/?tag_high-torque-12v-gear;

hxxps[:]//cyberservice24[.]com/?tag_high-torque-12v-gear/aplysia;

hxxps[:]//cyberservice24[.]com/?informatica/teucri.

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

f4730051838e9d95280406cd1c24a584597879468e4e7ba6001b29d5fa61db88;

98faf6bbea66f07eba832748059a9d466745ab1d4ab16542a91d610dc2b43829.

20. Хакерской группировкой Kimsuky, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный архив с расширением «.zip». Внутри указанного архива содержится файл, замаскированный под легитимный файл Wordpad. После запуска пользователем указанного файла осуществляется выполнение команд оболочки сценариев PowerShell, загрузка и внедрение фреймворка постэксплуатации (Cobalt Strike).

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):

c2faf67cab95cba996e6b705e9579ffbc53fec55b09064308c2c38dbf6018077;

ce13fdeb751805770de676f0b387623e590ac17c569c5bc9e81323bdd6213521.

21. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный архив с расширением «.zip». Внутри указанного архива находится вредоносный файл, после запуска которого осуществляется загрузка и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (GhostRAT).

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):
b86af545e9a2f86c05538eb7fcb85cf63085a0730925a9587253d46590a4e4e9;
b35314c2c3b1aab777d621c6fd8516a877b27efbde4dd4addd6843c411e96aa3;
c4d1454ad9740c5f0945650a250dbefa7fcdb516214e3242dd66ab4ea35ced67;
c1eb83993c85e01ee6ae84eb6e05744ff8c3ccc02c41d09c22286e3012ef46fc;
9c6e9543c8bd435e3e02ef1a312c502eeb9fb42d11add8e45a063b6ed9cd9cf6;
176d4dc9403dc70824912ea81379fa8c3c0bb8b555c672a648e1cb4ae9cd0805.

22. Хакерской группировкой Core Werewolf, нацеленной 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 вредоносный файл с наименованием «Отсканированные_документы_29283544_scanned_PDF_План_работы.pdf», после запуска пользователем которого осуществляется демонстрация документа-приманки, загрузка и внедрение легитимного программного обеспечения для удаленного доступа «UltraVNC».

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 138kasko[.]ru[:]443, 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):
19a993795d9ee0afbfbb185cfa1614f22c9eb1b044bba01b1cdc8aacf2058cb6;
9a413e1f94ffd4329719eeae28d0f6452cc84ee67160b0e93f47f6f15f4d2059;
1814f5f3fa55eb0d4e9cafa2f89569b91750ac7834a0fff8c7c70fe92c09cf97;
f528ce5fb8a45829f90af69dd95dfe15784311aff18fe72145254a10940a8ec6;
b9a2d83447d704f35f38e6366fbdfb8807ba08d16c1c6a5a95a886c0ff309811;
fb89ed88ca0d7fc7602984dc844dad00c731213d04921664c58b203af6288725;
a8801dc60dde71b8184686c2dded65071443e9bfc36b544ad80c03d219ee0f91.

23. Хакерской группировкой GamaCopy, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «О состоянии объектов вооруженных сил Российской Федерации». Во вложениях указанных писем содержится вредоносный архив с расширением «.zip», внутри которого находится исполняемый файл с наименованием «*.pdf.exe». После запуска

пользователем указанного исполняемого файла осуществляется выполнение вредоносных VBS-скриптов, 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:

nefteparkstroy[.]ru[:]443;

fmsru[.]ru[:]443.

Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
c9ffc90487ddcb4bb0540ea4e2a1ce040740371bb0f3ad70e36824d486058349;
a9799ed289b967be92f920616015e58ae6e27defaa48f377d3cd701d0915fe53;
afcbaae700e1779d3e0abe52bf0f085945fc9b6935f7105706b1ab4a823f565f;
2da473d1f510d0ddbae074a6c13953863c25be479acedc899c5529ec55bd2a65;
2b2da38b62916c448235038f09c51f226d96087df531b9a508e272b9e87c909d;
f583523bba0a3c27e08ebb4404d74924b99537b01af5f35f43c44416f600079e.

24. Хакерской группировкой DarkGaboon, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица представителей российских компаний. Во вложениях указанных писем содержится вредоносный архив с наименованием «Акт сверки.zip», внутри которого находятся файлы-приманки с расширениями «.txt» и «.xls» и исполняемый файл с расширением «.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки, загрузка и внедрение 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 обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

kilimanjaro[.]dns[.]army;

kilimanjaro[.]hopto[.]org.

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

25. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица представителей ликвидированных российских компаний, во вложениях которых содержится вредоносный файл с расширением «.rdp». После запуска пользователем указанного файла осуществляется получение злоумышленниками удаленного доступа к целевой системе по протоколу RDP.

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, а также заблокировать получение электронной корреспонденции с вложениями, имеющими расширение «.rdp».

Обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу platforma-zakupki[.]ru, используя схему доступа по «черным» или «белым» спискам, а также ограничить исходящие RDP-подключения к серверам за пределами внутренней сети.

Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикатора компрометации (sha256): C7DB6B2A340DDF1A5567BC55BDCA1C3D3F14473B1A29F5C34C559FA7F5BED660.

26. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой предложений по трудоустройству. В тексте указанных писем предлагается осуществить видеозвонок для проведения собеседования, запустив файл, замаскированный под приложение для связи, содержащийся во вложениях письма. После запуска пользователем указанного файла осуществляется загрузка и внедрение вредоносного программного обеспечения типов «загрузчик» (BeaverTail) и «троян удаленного доступа» (InvisibleFerret).

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:

147[.]124[.]214[.]129;
173[.]211[.]106[.]101;
hxxp[:]//147[.]124[.]214[.]129[:]1244;
hxxp[:]//147[.]124[.]214[.]129[:]1244/keys;
hxxp[:]//147[.]124[.]214[.]129[:]1244/pdown;

hxxp[:]//173[.]211[.]106[.]101[:]1245;
hxxp[:]//173[.]211[.]106[.]101[:]1245/brow;
hxxp[:]//173[.]211[.]106[.]101[:]1245/bow;
hxxp[:]//173[.]211[.]106[.]101[:]1245/adc.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
a9dfab4915a1318643cdfea9ba9e5b22752be8058564513b60a37721e1f84342;
48ef099f3eccc4eaabe0128bb5e6f81b8e6ffdf09a047ae350c9dc5faf5cfabc;
47830f7007b4317dc8ce1b16f3ae79f9f7e964db456c34e00473fba94bb713eb;
6a104f07ab6c5711b6bc8bf6ff956ab8cd597a388002a966e980c5ec9678b5b0.

27. Хакерской группировкой Cloud Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный файл с расширением «.rtf», замаскированный под легитимный документ Microsoft Office. После запуска пользователем указанного файла осуществляется загрузка вредоносного rtf-шаблона, содержащего эксплоит уязвимости пакета программ Microsoft Office, вызванной выходом операции за границы буфера в памяти (BDU:2018-00096, уровень опасности по CVSS 3.0 – высокий). Эксплуатация уязвимости позволяет злоумышленникам выполнить вредоносный код для загрузки вредоносного программного обеспечения на целевую систему.

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:

cyberservice24[.]com;
hxxp[:]//cyberservice24[.]com/?products_hair-straightners/untreated;
hxxps[:]//cyberservice[.]24[.]com/?mac-eddy-today-journal-76-released/besiegement;
hxxps[:]//cyberservice24[.]com/?news_2022_07/2[.]php/phanar;
hxxps[:]//cyberservice24[.]com/?products_hair-straightners/untreated.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
505e1531d8902de5d198327e238d4694e2eb28fc4f8c239b0db31f09136dce3d;
0806e4661777f2b30b7abc96cdbca56ecde5c5703ee52fe5013d30a41ad5508f;
46a4389c8bd8f1bf3a39706f62026adaf9792edcf4e5630f3f69bef69ba97ea3.

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

28. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Редакционный совет журнала «Военная техника». Во вложениях указанных писем содержится файл-приманка с наименованием «Пневмокатапульта с самолетом.docx» и исполняемый файл. После запуска пользователем указанного исполняемого файла осуществляется загрузка 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):

e40a1a00e81f65638363417b582091a4330f3cf0895f4349489cf413366816e1;

c79413ef4088b3a39fe8c7d68d2639cc69f88b10429e59dd0b4177f6b2a92351;

b7dd715888a372a9c32e09e0d7755db63c948560e002848bc24c3832f146e85e.

29. Хакерской группировкой Core Werewolf, нацеленной 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 вредоносный файл с наименованием «Отсканированные_документы_29283544_scanned_PDF_План_работы.pdf», 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 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:

argusscan[.]ru;

hxxps[:]//argusscan[.]ru[:]443.

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

внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
f34f75cf23e80d7b19dee5aaffb66a6b573bd5da9718d025fd0aaf1ad0006f3c;
4097bfa2db506a5fbc622f7936d75db9de7c56918c6a7fb021c735b847ee988f;
519865c848b26ef4abfd33fcf5cd1ab8751a96e7589b53edbeb43ba0c4255939;
f13459c680fc7bf35f8979deba9f087b65a2c4fec0cec8620abb0ee69975f427;
7f6b48e1a70c91cb181546863b2904fed74a3161b9ec9c244b12c7d0099443cd;
73ca9fdd96c4cd7ff95d0fb6986b2f993dcd3b2b5d2210a870388c262eec0e42.

III. Другие угрозы информационной безопасности.

Анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что зарубежными хакерскими группировками осуществляются целевые компьютерные и фишинговые атаки с использованием сервисов обратной связи и обращений граждан посредством электронной почты и форм обратной связи официальных сайтов органов (организаций).

В соответствии с подпунктом «е» пункта 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» направляем дополнительные организационные и технические меры по повышению защищенности информационной инфраструктуры органа (организации), подлежащие реализации.

В целях предотвращения реализации угроз безопасности информации, связанных с указанной деятельностью хакерских группировок, необходимо:

1. Исключить возможность получения органом (организацией) электронных писем с почтовых сервисов, доменное имя которых принадлежит недружественным Российской Федерации государствам (Перечень иностранных государств и территорий, совершающих в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия утвержден распоряжением Правительства Российской Федерации от 5 марта 2022 г. № 430-р).

При реализации указанной блокировки необходимо учитывать служебную необходимость органа (организации) взаимодействия с организациями и гражданами, использующими почтовые сервисы, доменное имя которых может принадлежать недружественным Российской Федерации государствам. В этой связи необходимо реализовать указанное взаимодействие с использованием «белых списков» разрешенных доменных имен или отдельно заданных адресов электронной почты.

2. Исключить возможность получения органом (организацией) обращений по формам обратной связи (сервисы «Прием обращений граждан и организаций»), размещенным на официальном сайте органа (организации), с IP-адресов (доменов), страной происхождения которых являются недружественные Российской Федерации государства.

С целью информирования граждан и организаций рекомендуется разместить на официальном сайте информацию об установленных ограничениях по приему обращений с иностранных IP-адресов (доменов).

С перечнем IP-адресов иностранных государств для настройки блокировки можно ознакомиться на сайте IPdeny (https://www.ipdeny.com/ipblocks/), а также на сайте MaxMind (https://www.maxmind.com/).

Реализация указанной блокировки возможна с использованием имеющихся средств межсетевого экранирования уровня веб-приложений и (или) уровня периметра сети (в соответствии с инструкциями по эксплуатации соответствующих средств защиты информации).

Ограничение доступа по IP-адресам к таким разделам сайта, как форма обратной связи (сервисы «Прием обращений граждан и организаций») возможно осуществить путем настройки политик доступа, содержащихся в файле .htaccess. Например:

Order Allow,Deny
Allow from all
Deny from 123.123.123.123
Deny from 122.122.122.122

где 123.123.123.123, 122.122.122.122 — пример IP-адресов, для которых необходимо запретить доступ.

Order Allow,Deny
Order Deny, Allow
Deny from all
Allow from 111.111.111.111

где 111.111.111.111 - пример IP-адреса, для которого разрешен доступ.

3. Обеспечить получение органом (организацией) обращений граждан и организаций по формам обратной связи (сервисы «Прием обращений граждан и организаций»), размещенным на официальном сайте органа (организации), только после прохождения отправителем обращения предварительной идентификации.

Организация указанной идентификации возможна несколькими способами:

подтверждение личности с использованием Единой системы идентификации и аутентификации;

подтверждение владения номером телефона путем отправки смс-кода на указанный при обращении номер телефона российского оператора связи;

подтверждение владения почтовым адресом путем отправки цифрового или буквенного кода на указанный в обращении адрес электронной почты.

4. Реализовать следующие настройки параметров безопасности почтовых серверов органа (организации) в целях исключения подмены адресов электронной почты.

4.1. Осуществить настройку параметра безопасности Sender Policy Framework (SPF) путем редактирования записей DNS-зоны сервера необходимого домена следующим образом:

добавить новую TXT-запись, которая описывает перечень DNS и IP-адресов, являющихся источниками отправки электронных сообщений. Например, следующего содержания:

example.org IN TXT "v=spf1 mx ip4:133.133.133.133 +a:smtp.mail.ru include:yandex.ru ~all"

из которой следует, что отправлять сообщения от имени домена example.org могут только сервера, указанные в mx-записях, а также IP адрес 133.133.133.133.

Расшифровка параметров:

v=spf1 является версией, всегда принимает значение spf1;

a – разрешает прием писем с адреса, который указан в A и\или AAAA записи домена отправителя;

mx – разрешает принимать письма с адреса, который указан в mx записи домена;

all – определяет, что будет происходить с письмами, которые не соответствуют установленной политике: "-" – отклонять, "+" – пропускать, "~" – дополнительные проверки, "?" – нейтрально;

include – разрешает принимать письма с серверов, разрешенных SPF-записями домена;

ip4 и ip6 – уточняющие параметры для указания конкретных адресов.

4.2. Осуществить настройку функции безопасности Domain Keys Indentfied Mail (DKIM) подписи и DNS записей путем создания пары ключей шифрования (открытый и закрытый):

openssl genrsa -out private.pem 1024 (сгенерировать закрытый ключ длинной 1024, ключи с длинной менее 1024 применять не рекомендуется);

openssl rsa -pubout -in private.pem -out public.pem (получить публичный ключ из закрытого).

Далее необходимо указать путь к закрытому ключу в файле конфигурации почтового сервера и указать публичный ключ в конфигурации DNS путем добавление записи следующего содержания:

mail._domainkey.your.tld TXT "v=DKIM1; k=rsa; t=s; p=<публичный ключ>".

Если требуется заполнить поле TTL, то необходимо указать параметр 21600.

Расшифровка параметров:

mail – селектор. Можно указать несколько записей с разными селекторами, где в каждой записи будет свой ключ. Применяется тогда, когда задействовано несколько серверов (на каждый сервер свой ключ);

v – версия DKIM, всегда принимает значение v=DKIM1 (обязательный аргумент);

k – тип ключа, всегда принимает значение k=rsa (по крайней мере, на текущий момент);

p – публичный ключ, кодированный в base64 (обязательный аргумент);

t – флаги:

t=y – режим тестирования. Такие ключи отличаются от неподписанных и нужны лишь для отслеживания результатов;

t=s – означает, что запись будет использована только для домена, к которому относится запись. Использование указанного флага не рекомендуется, если используются субдомены.

4.3. Осуществить настройку функции безопасности Domain-based Message Authentication, Reporting and Conformance (DMARC) путем добавления TXT-записи с указанием действий сервера в случае, когда проверка подлинности DKIM и SPF не пройдена, например:

_dmarc IN TXT “v=DMARC1; p=reject; rua=mailto:dmarc@example.org; sp=reject; aspf=s; adkim=s; ri=604800“.

Расшифровка параметров:

v - версия протокола DMARC, принимает значение v=DMARC1 (обязательный параметр);

p – правило для домена. (обязательный параметр), принимает значения none, quarantine и reject, где:

none – не делает ничего, кроме подготовки отчетов;

quarantine – добавляет письмо в СПАМ;

reject – отклоняет письмо;

rua=mailto:dmarc@example.org - адрес электронной почты на который присылать уведомления о результатах проверки;

aspf - определяет тип проверки “strict“ для SPF-записей;

adkim - определяет тип проверки “strict“ для DKIM-подписей;

ri - интервал в секундах, определяющий как часто получать агрегировать XML-отчеты.