Приложение 1

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 и распространяемом ими вредоносном программном обеспечении.

1. Хакерской группировкой Cloud Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплены файлы с наименованиями «Счет_a19af3ed-a30a-45a0-b88d-6529f94398d4.pdf.lnk» и «Заявка_количество на поставку корпусов АО АМ3.pdf.lnk». После запуска пользователем указанных файлов осуществляется выполнение команд оболочки выполнения сценариев «PowerShell», демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (Goldbackdoor).

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:

istochnik[.]org;

hxxps[:]//istochnik[.]org/male-infertility/isoflor;

hxxps[:]//istochnik[.]org/spis[.]html/choanoflagellidae.

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):
81f26d8ad99ab743f97bfbaae0f260ef6d96b3b9eab2613622e6b0bd0032709e;
2ad7e07a86784f22bc0fa400f433fc905aa49506b1cb629192d3c0b718cae372;
2e7871b4cad8c77c1b7d7d430195470ee89ee15429ec3f32009d904e564595c6;
d2d77c457dffd42942098f57b80a1e557879d4706d5bb96fd69c5896edfb60ea.

2. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Заказной документ. N: 224/12028519303-1 от 05.08.25». Во вложениях указанных писем прикреплен архив, внутри которого содержится файл с расширением «.js». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (XWorm).

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:

146[.]70[.]100[.]227;

hxxp[:]//146[.]70[.]100[.]227[:]9779.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикатора компрометации (sha256): 2e8e9af8522ac591a6e322d726964f4012293de22f01e736d09691d2d2b531a1.

3. Хакерской группировкой Vengeful Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «1.zip». Архив содержит файл-приманку с наименованием «Бланк.doc» и исполняемый файл с наименованием «Акт сверки взаимных расчетов предприятия № 162 по состоянию на 1 августа 2025 года.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Revenge RAT и Xworm).

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 169[.]47[.]130[.]87, 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):
4370a609d9b7bd40ee5bb7c99976e0289d879a616511e99349cb4075bc21cb61;
f3d359ceb7bb4d81306627716f38ff01153f20dd6cc5b7ded46c7a69d1a222e2;
43be6e86aab9e52d927f673a6bc00666c025d5abf7c567c8d847f296dac572a6;
6327cdd9f0a6b327bc4e1a8a9af8fd357605825f9a09ee6f6dcf89c7834b9472;
f56f504b13aea4367902de74fd180060b26b0dc14a04d93e34fba4482be46cf1;
95ee443b26b571e3100ef711ea4d867bf14ba0d9c8d2078037a7552e751d29b9;
aab62dba65d15bb5d38ef9f9cb7e6bb348f510300924eee5dfcc083254b5b7b1;
1eefbb78811ef6960f68e9bc1338467e1fc89e39e082dbd839b24f89ef06ff84;
cca946d2e96bb2388630c84b05427fca9d0f0ceacd39ad3ec62d56c6b5bcc900;
a1247fae33a32ffe3ec82cc4b6e2a8d07cdf21c02b7ac50f5d6487f4c5fcf5bd;
c7ce2c41a2998856314466cd9b37aade995eceaa30559e35873a9109507be1fd;
4606eeae7910378fdfd25e210186f66b36cb12f5f177df9b5d2dbbcf4291e50f;
03b188d1b2c75cb8e7f849bf60dedf75d2d6021322ae34948e96632e83857e62;
ce5a054d1dd20dc425fcbd99220e878416a2489cf37230a84119ec9e91abb63d;
223abedecabf0d615b91259d5fa168da9c71b0efe564a4d9afc00dc0a1a1d4e7.

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

инфраструктуры Российской Федерации, с использованием системы электронного документооборота «Контур.Диадок» осуществляется распространение архива с наименованиями «DX2025.zip». Архив содержит вредоносный исполняемый файл, после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типов «червь» и «троян удаленного доступа» (Buhtrap), а также дальнейшее распространение вредоносного программного обеспечения в системах электронного документооборота.

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):
f77a9b72b2fd8063ecd15cccf1ce1181d6f1ef7df239f82236dc717cdfc5a0df;
671370919c8ebeac8c1552f2c306333c99049255d70eaabc3abd8ccfc0537b76;
bf9f246a6d5145da737720b43237f25111d50cd52caa0c950966820ca7bac1cf;
2dbea65f2cb2ec27d5bd1fca946f057626b52fbb8e07898a052205f1ff0eba28;
51399abc9d4fb92e47539bb5af658aa836abb6d32326a6b9cdad11dcaa3cbf14;
40e03e6f43a90534ba2da74488a754086d3ef925fbeabe45b672de592de87c63;
653a3805f81abed952bc98c32c1d079b79b7addd0e7da2831debbd26efeb66b8;
330d66815bb4cdbafc4c544d91d582b15ec4380c0f80707108b97d053a33ee22.

5. Хакерской группировкой Paper Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен исполняемый файл с наименованием «Резюме.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение вредоносного программного обеспечения типа «загрузчик».

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

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

hxxps[:]//circlewinds[.]org/interval/abdicating/breezy/phenomenal/debit?.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикатора компрометации (sha256):
86f40d64d8b1fed9589c82b7a9924924c00fba8b4ebe8994673e266f05c9b661.

6. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «технический акт № 173.2025.rar». Архив содержит исполняемый файл с наименованием «технический акт № 173.2025.scr », после запуска пользователем которого осуществляется внедрение на целевую систему 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 обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу hxxp[:]//bazalt-vpk[.]site/Chrom[.]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):
1e81c060728d131b12a848ca06a1573ad897fca80e421fb889fe1defe6385b0e;
608315bccea4a96868c020d9441b0b6e6aa2525116b2abb25f1275f8ae296ad1;
edb635b2ab3859d02cec06137fee964286dfcb87de7f04277ae78c09e528c9a2;
0aa9c137320c142b8edaf6374a285f2e14d6133bca410c60c2c8adabb9b5c23a;
638641be461a114208f1269a71034cfae04dcfef3ba06e37ad850dd1d3fb2a6a;
34e13de36b99cabf23fc95b59581ee7373b12325779aed86a0eb08f48ca48727;
9d71fa5455b2885825aa2be8832c771dd7cba9e633703d4ad24d9e2968b5ab59;
fcad1a8de33a347cc412a6c3825e83b4f5f0594aa0bc3279d1d3df62f684c0a6;
39e587fdba4060205e520a54fd498e5eb2d2945c0ded6217f28beb2e1410bdb5;
746475f67cd3456551c5cd9c6205c9754b2aef17472af1b40d41904df2337a2b.

7. Хакерской группировкой Core Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится исполняемый файл с наименованием «Отсканированные_документы_371_Выписка_по_противнику_на_доклад_по_08_08__командиру.pdf.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение на целевую систему 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:

areanc[.]info;

madebysbk[.]com;

45[.]128[.]148[.]24.

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

8. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложения которых содержится архив с наименованием «Demand_984175.zip». Архив содержит файл-приманку с наименованием «PASSWORD – 47692» и защищенный паролем архив с наименованием «Requirement.zip». Внутри указанного архива содержится файл с наименованием «Requirement.wsf», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Efimer).

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:

hxxps[:]//lovetahq[.]com/sinners-2025-torent-file/;

hxxps[:]//lovetahq[.]com/wp-content/uploads/2025/04/movie_39055_xmpg[.]zip;

hxxp[:]//cgky6bn6ux5wvlybtmm3z255igt52ljml2ngnc5qp3cnw5jlglamisad[.]onion;

hxxp[:]//he5vnov645txpcv57el2theky2elesn24ebvgwfoewlpftksxp4fnxad[.]onion.

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

39fa36b9bfcf6fd4388eb586e2798d1a;

5ba59f9e6431017277db39ed5994d363;

442ab067bf78067f5db5d515897db15c;

16057e720be5f29e5b02061520068101;

627dc31da795b9ab4b8de8ee58fbf952;

0f5404aa252f28c61b08390d52b7a054;

eb54c2ff2f62da5d2295ab96eb8d8843;

100620a913f0e0a538b115dbace78589;

b405a61195aa82a37dc1cca0b0e7d6c1.

9. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, внутри которых содержатся исполняемые файлы с расширением «.net», замаскированные под легитимные файлы программного обеспечения Microsoft Office. После запуска пользователем указанных файлов осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «загрузчик» (Steganography Loader).

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):

7300535ef26158bdb916366b717390fc36eb570473ed7805c18b101367c68af5;
abb1291f05e30b2c0ede259914a1e8d389e78109e83d0cc1573b3a2dba5f6778;
0e60ec28b9f93bff7e94142f6ffeae605303c0e49d262f98ed9291f56c1d6d9c;
8c7b8e90bef30d07480ef31e6ec3ff8c4ae660912429466b634c74057d7943dd;
ce744d26c1adb79f1d7a2d51db1838f33ddab7d165fdfb1727c2ec4917161857;
ee16b728f9349c098dc5fc0ecfa5b57af898560c1570e53366101809492662ab;
8c02bf4930c4e52c75a617366a12d7374a7f02e5e97c40dc57e4ab7ebbda661a;
694ba08164ceacda976ace02b328050d8f01eceea82b852b05dbe0e7be286b44;
c2647bf49224666dc10191c758ed59eb9af813b0a6d9ac1f64dbf94557d4995e;
f2392e04e5ffb9bcee95ce763a7686322a9abd7210af28ef3f653402515a6013;
976336ef319fb3eedc60f19703a4bff9d3c6c798c83b0fd80a2e3e4c1e86680a;
6bb21551577d98edc3a3c4db8d941258f86c89db185fa2095f54ad4944a62b87;
6bfaef5dc204e1b5a1da28f9e6ca73c3c0ad9724abb42412c755a4d9c03d0285;
8e0af283e7c58a6308a4b5d1b62ecf1eb4bf6e2c9566228c6b44e642bc954bcf.

10. Хакерскими группировками Team46 и TaxOff, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, в тексте которых содержится вредоносная ссылка. После открытия пользователем указанной ссылки осуществляется загрузка и внедрение на целевую систему вредоносного программного обеспечения типов «загрузчик» (TaxOff Loader и Team46 Loader) и «бэкдор» (TaxOff Trinper).

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

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 primakovreadings[.]info, используя схему доступа по «черным» или «белым» спискам.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
81f26d8ad99ab743f97bfbaae0f260ef6d96b3b9eab2613622e6b0bd0032709e;
2ad7e07a86784f22bc0fa400f433fc905aa49506b1cb629192d3c0b718cae372;
2e7871b4cad8c77c1b7d7d430195470ee89ee15429ec3f32009d904e564595c6;
d2d77c457dffd42942098f57b80a1e557879d4706d5bb96fd69c5896edfb60ea.

11. 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 с наименованием «Спецификация 13_ Гидравлика.pdf.exe». После запуска пользователем указанного исполняемого файла осуществляется выполнение вредоносного Batch-скрипта и внедрение на целевую систему 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:

94[.]142[.]140[.]52;
80[.]85[.]155[.]40;
103[.]71[.]20[.]195;
185[.]117[.]153[.]140;
185[.]221[.]152[.]17;
siloneq[.]ru.

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

fc3650cfbbbf3d5a03482df1deb4d6f35a9ff3d294aaa583948597a527106b8d.

12. 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 с наименованием «Исх 14-0554-4 от 09 06 2025 (уведомление о невыполнении

соглашения).zip». Внутри указанного архива находится файл с наименованием «Исх 14-0554-4 от 09 06 2025 (уведомление о невыполнении соглашения).lnk», замаскированный под официальный документ. После запуска пользователем указанного файла осуществляется выполнение вредоносного VBS-скрипта и внедрение 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 следующим адресам, используя схему доступа по «черным» или «белым» спискам:

188[.]114[.]97[.]3;

188[.]114[.]96[.]3.

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

4986426b95bfb311425e0e3f685eb40f130e93ff87009e0e21fbace520b47093;

5206ed4803efd7b24fc575b772a163ab06300820c84744670af2b29b0c94f9c3.

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

f64636bd145ba58c25cd510c6eceee2d7cee5843f6b80bafd17e78054de152ec.

14. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Приказ МО РФ №811 29.05.2025». Во вложениях указанных писем прикреплен архив с наименованием «Приказ МО РФ №811.rar», внутри которого содержится исполняемый файл с наименованием «Приказ МО РФ №811.scr». После запуска пользователем

указанного исполняемого файла осуществляется внедрение на целевую систему 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 обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

autotificate[.]com;
92[.]63[.]173[.]61;
92[.]63[.]173[.]57;
31[.]172[.]74[.]174.

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

fb9271d55e4b3449fe68557d9567cb49e2fc143d1d5cdc07de268dda41a7e6ca;
06d16b4fda038727da6a65e6d4acb0e5337d47324ee898e7f20d280751300677;
b863ff33b0e7772452600f582fd005204f4afce69f670f901426e32057b6442d.

15. Хакерской группировкой Lone Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Досудебная претензия». Во вложениях указанных писем прикреплен архив с наименованием «рекламация.rar», внутри которого содержатся вредоносные файлы с наименованиями «рекламация.pdf.lnk» и «рекламация.doc». После запуска пользователем указанных файлов осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «фреймворк 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 обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

armstroy42[.]ru;
toolhaus[.]ru;
clack[.]su;
45[.]141[.]233[.]44;
83[.]220[.]168[.]36.

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

внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
2d00a237594ba9998c8f3ad07b3921bafa53ef7402a6da6988b343c6120ccb56;
1750548c9021915f3b66e5a853eaa556487e375390267c174d9148dc3d5d0121;
453bb4b2fe1c71c2e1319e5ee621d2da2d60476e35a0853960bc8d25fbb96677;
4640c58e3c658d8178f4e9d9570566040ad162e25b61a46b0be989aeb69db679.

16. Хакерской группировкой PhantomCore, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Транспортная накладная ТТН № 39144 от 26.06.2025». Во вложениях указанных писем прикреплен архив с наименованием «Транспортная накладная ТТН № 39144 от 26.06.2025.zip», внутри которого содержится файл с наименованием «Транспортная_накладная_ТТН_№391-44_от_26.06.2025.xls.lnk». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (PhantomRemote).

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 адресам, указанным в приложении к настоящим рекомендациям, 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 индикаторов компрометации, указанных в приложении к настоящим рекомендациям.

17. Хакерской группировкой Vengeful Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «1.zip». Архив содержит файл-приманку с наименованием «Бланк.doc» и исполняемый файл с наименованием «Акт сверки взаимных расчетов предприятия № 196 от 11 августа 2025 года..exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (XWorm).

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 maketppk[.]ru, используя схему доступапо «черным» или «белым» спискам.

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

18. Хакерской группировкой Fluffy Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «akt_sverka04082025_1C_PDF.rar». Архив содержит исполняемый файл с наименованием «akt_sverka04082025_1C_PDF.com», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типов «стилер» (PureLogStealer) и «троян удаленного доступа» (PureHVNC).

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:

195[.]26[.]227[.]209;

jump-finance[.]tech;

hxxps[:]//jump-finance[.]tech/akt_sverka04082025_1C_PDF[.]rar.

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

fce715985f0f3c08d2fdf90a7c1f3cca7726ccc6dc5fcb39afb69acf248a90ef;
1659e11532c50daf1e44f5b6013c15892151117d6b0e77ed4bb56b698eefc043;
744e11de7cda0b4ea66c3926efffc52b83428b2d689de82fa3aac31dbe3d6b66;
2db0e734359874247d51485268444e79271d35e601dbf094ac91a1bcd3659fce;
e9fd849646bb153bb051c48b2b11a8b40a4d236744ac7eeca083469a60f3deef;
41da72d3570c2ff0fc3dcca24be6590908370a8c44d69256d5fb8844ac1177f2;
710470303d1a26bc891ba28890f41a8e3606c4b906dbf751356b3d928569a1ae;
5bb4e43c90c51a536fe387221737a900c1de97b6137c40ba520a9a6b7a3e8ac9;
d64b38bd275f9bd83f2be728d4760ba3097aaf939ad4d46f0477b8625f2d5b49;
19cd804f65452e2ae1000bdf15e4b84cb4e8745e158cc1a84e12a37c7820edba;
ce2ed2fb9f7cd5cf06caaa530f48d2e5cb59147d6a35a934318b49aa2e06dce8;
cfceb7cc20dda7d3057c57e33ed610c64c62130b199fb4798bde177a11be48c5.

19. Хакерской группировкой Fairy Wolf, нацеленной на органы государственной власти и субъекты критической информационной

инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «Исх С-41251-25 от 11 08 2025 Соглашение о конфиденциальной информации.zip». Архив содержит файл с наименованием «Исх С-41251-25 от 11 08 2025 Соглашение о конфиденциальной информации.hta», после запуска пользователем которого осуществляется выполнение вредоносного VBS-скрипта, демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Unicorn 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 следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hxxps[:]//discord[.]com/api/webhooks/1404358532228452434/sdd1Tow8F6smdGq2pHb6QawUqkRi5NAebWnbbdGT6wfY-C6qXWQJsCwa9dgb9SOYY5Qn;

hxxps[:]//discord[.]com/api/webhooks/1400380055603122238/YjImNhISQx-OW93lmh4lHHYoxetp4QFs6WPKyuAEnYueGgcGN9bPI88OxVcXKXVG7FD3;

hxxps[:]//discord[.]com/api/webhooks/1402964109904974037/RuGnEMuIafQm1_8fqH8nuRCvTCNepDJ9lBzQuf-vV49KHkSv03HuGOiPEaQiA6bYy_-r;

hxxps[:]//discord[.]com/api/webhooks/1402572617491415151/lLbB_sypSYypODjxGzwGvYgzztBKQ_b-JO_1XPtK_Xbyj8X_HtnV8U9gQfRDMHGFkmro;

hxxps[:]//discord[.]com/api/webhooks/1400774611792298004/BjhspobaqPDZ4vClV7aAMlnrpe5uW9JzcyNuCdx4E-8fgjpbh2fh_A3sKl9jrjzwCn58.

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

20. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен исполняемый файл с наименованием «технический акт № 173.2025.scr». После запуска пользователем указанного исполняемого файла осуществляется внедрение на целевую систему 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 обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

66[.]29[.]132[.]150;

zakypky-ru-info[.]website;

hxxps[:]//zakypky-ru-info[.]website/fdbnjgcergf[.]rar.

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

b3b6f660bc37e1ece5e638dfdaf87b97899df972f6cebe5062fd964142b1fcce;
0aa5b62cdf23f5ab74eff183646e866ae2775bf9318c90344489d169360e91ea;
c7ff03e049a8f70b66a9779d049f193a83211f7032dbb8eeb8c9bd8e4a6087a5;
dfd5b5d44f17ed18a93f3839635911ec3b75da34c395c41e6005cbb5257e04ae;
1030ec0675e603684941aff16d5f6f33c5bc9976cca293afa156a7bcacbc6b9d;
d4c5657e267a7788b034326a4576e54a66ea8be335725652548f50a06c5b07b5;
1c542f09a5aa23aa8b48843a2910745cc4f61c3657f0fbcd06e45e82cc82d935;
84ce5141d16e5935ac043971f5285ff19fa427c4bc2305a2aeee32178a5249cb;
36f974b35a75f75e51860c8d28eeacebde6ed9b5422365883f972c48769bae0a;
7d77e9605d392c5989c0a12ea3a8c3909266f11f8dcea877af6a25ef938f9635.

21. Хакерской группировкой Scaly Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен исполняемый файл с наименованием «Акт Сверки.pdf.exe». После запуска пользователем указанного исполняемого файла осуществляется внедрение вредоносного программного обеспечения типов «троян удаленного доступа» (Trojan.Updatar.1) и «бэкдор» (Trojan.Updatar.2 и Trojan.Updatar.3).

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[.]105[.]161[.]30;
roscosmosmeet[.]online;
roscosmosmeet[.]ru;
doc-mil[.]ru;
updating-services[.]com;
etti-deti[.]ru;
etti-deti[.]online;
e97861mi[.]beget[.]tech.

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

22. Хакерской группировкой Kinsing, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, при реализации целевых компьютерных атак осуществляется эксплуатация уязвимостей серверов и сервисов (например, Docker API), доступных из сети «Интернет», под управлением операционных систем Linux. После получения несанкционированного доступа к целевой системе злоумышленники осуществляют внедрение вредоносного программного обеспечения типа «майнер» (XMRing).

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

45[.]15[.]158[.]124;
45[.]137[.]155[.]55;
78[.]153[.]140[.]66;
78[.]153[.]140[.]96;
92[.]242[.]40[.]21;
178[.]20[.]40[.]200;
185[.]14[.]30[.]35;
193[.]178[.]170[.]47;
194[.]38[.]20[.]2;
194[.]38[.]20[.]32;
194[.]38[.]20[.]199;
194[.]38[.]20[.]242;
194[.]38[.]21[.]25;
194[.]38[.]22[.]53;
213[.]209[.]143[.]44.

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

23. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с расширением «.zip». Архив содержит исполняемый файл с расширением «.exe», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (KiwiStealer).

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 ebeninstallsvc[.]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):
4b62fc86273cdc424125a34d6142162000ab8b97190bf6af428d3599e4f4c175;
13d128038c341e850b55bc900ecee93496521c74bd9f3f8ea63e86042c5b6a9b;
5057690b451456890a34931d11d16a111f7adbd6ef966bd20d420c72afcd6f6d.

24. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляется распространение вредоносного программного обеспечения типа «бэкдор» (PipeMagic), замаскированного под обновление программного обеспечения (например, Google Chrome), предназначенного для работы в системах под управлением операционных систем Windows.

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу aaaaabbbbbbb[.]eastus[.]cloudapp[.]azure[.]com, используя схему доступа по «черным» или «белым» спискам.

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

5df8ee118c7253c3e27b1e427b56212c;
60988c99fb58d346c9a6492b9f3a67f7;
7e6bf818519be0a20dbc9bcb9e5728c6;
e3c8480749404a45a61c39d9c3152251;
1a119c23e8a71bf70c1e8edf948d5181;
bddaf7fae2a7dac37f5120257c7c11ba.

25. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Служебная записка». Во вложениях указанных писем прикреплен архив с наименованием «Служебная записка от 12.08.2025.rar». Архив содержит исполняемый файл с наименованием «Служебная записка от 12.08.2025.exe», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа».

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

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к IP-адресу 62[.]113[.]114[.]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):
04769b75d7fb42fbbce39d4c4b0e9f83b60cc330efa477927e68b9bdba279bb8;
ab0ad77a341b12cfc719d10e0fc45a6613f41b2b3f6ea963ee6572cf02b41f4d.

26. 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 с наименованием «Отсканированые_документы_по_ВСО_заключение_по_запросу_на_начальника.exe». После запуска пользователем указанного исполняемого файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа».

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[.]128[.]148[.]246; 193[.]238[.]152[.]128.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
f7d4080ad8259b0aac2504f8b5d8fab18e5124321c442c8bcb577598059d0b24;
b49e9759e529158aff7d81081f0f5242bc741873fb0fe414b475c4b6c83360ee;
5f225c7f9f81d78b2ee45ec1eeb305d009631748bb2537b3376d7cd3390ad811;
9448d1a7eac7112ec68964eabc71134b14727bec3c13882d8b1c869c5dc3a8f7.

27. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа». Во вложениях указанных писем прикреплен архив с наименованием «Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа проектов к проектам.rar», внутри которого содержится исполняемый файл с наименованием «Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа проектов к проектам.exe». После запуска пользователем указанного исполняемого файла осуществляется внедрение на целевую

систему вредоносного программного обеспечения типа «троян удаленного доступа».

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

Кроме того, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
8722d5b97208398b93d7b2db8v65818vd43d93a68e11e220a889e8270e628bd1;
6b290953441b1c53f63f98863aae75bd8ea32996ab07976e498bad111d535252.

28. Хакерской группировкой Fairy Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Исходящий № 2150П-19 от 25.08.2025» Во вложениях указанных писем прикреплен архив с наименованием «ИСХ № 215ОП-19 от 25.08.2025.zip», внутри которого содержится файл с наименованием «ИСХ № 215ОП-19 от 25.08.2025.hta». После запуска пользователем указанного файла осуществляется выполнение вредоносного VBS-скрипта и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Unicorn 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 адресу van-darkholm[.]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):
d32f5aace4668f7282b20202e5e2d28220b93fdbbf0a00f17043c46e58cd89c6;
5352fbb053f7c14966b1a711144085dcc615763c7cc6be858c1f8b3090290e4e;
6a2a7f7c03384aa6c0f4c667835ce3ec947dd025160df0109bff7150e6069a2f;
62bf6f7858997702b951e883b0b3faff67a9d639c1661a291fff0f7012d86b2d;
b26e5cd757ad44b2853efc0e29f522a91001a92f2fb0fccde1c7f05b959649e1;
7e0a28569fd87ce81e296fdc28bc86ffe75ebda9441733d28e90e7eeaea22572.

29. Хакерской группировкой Fluffy Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «akt_sverki_1C_9856665_PDF.rar». Архив содержит

исполняемый файл с наименованием «akt_sverki_1C_9856665_PDF.com», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (PureLogStealer).

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 возможность получения электронной почты с адреса prostor-plast@mail[.]ru и 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):
ebdef6c402cbd2a7424a5a6dd30c08f67719c656bc28a1c8aa0edaf7823c5547;
3f8ede55b8fbc733b47e0a61c1def8fbd59aafdf86572ce57300b819d4ef8f79;
e438142b8341d18ee983538e58bfbe37e59d29c0b3dd32e1d220b64c825ea520.

30. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица органов государственной власти Донецкой Народной Республики. Во вложениях указанных писем прикреплен исполняемый файл, замаскированный под PDF-документ, после запуска пользователем которого осуществляется внедрение на целевую систему программного обеспечения для удаленного доступа «AnyDesk» и вредоносного программного обеспечения типа «майнер» (XMRig).

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 mail[.]center-mail[.]ru, используя схему доступа по «черным» или «белым» спискам.

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

31. Хакерской группировкой Rainbow Hyena, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с

наименованием «Задание_на_оценку_N_2046_от_05_августа_2025_года.zip». Архив содержит файл с наименованием «Задание_на_оценку_N_2046_от_05_августа_2025_года.pdf.lnk». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типов «загрузчик» (PhantomRShell) и «бэкдор» (PhantomTaskShell и PhantomRemote).

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 адресам, указанным в приложении к настоящим рекомендациям, 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 индикаторов компрометации, указанных в приложении к настоящим рекомендациям.

32. Хакерской группировкой Paper Werewolf (Goffee), нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица Главного управления МВД России по г. Москве с тематикой «По вопросам миграции». Во вложениях указанных писем прикреплен файл с наименованием «187-2325.pdf», в тексте которого пользователю предлагается перейти по ссылке, указанной в документе. По ссылке доступна веб-страница, замаскированная под сайт системы электронного документооборота МВД России, на которой пользователю предлагается скачать архив документов. Архив содержит файлы-приманки (например, «Памятка работодателю.docx» и «Уведомление о прибытии иностранного гражданина или лица без гражданства в место пребывания.xls») и исполняемый файл с наименованием «182-1672143-01(исполнитель Васнецовский М.Д).exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «загрузчик».

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

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресам, указанным в приложении к настоящим рекомендациям, 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 индикаторов компрометации, указанных в приложении к настоящим рекомендациям.

33. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, при реализации целевых компьютерных атак возможно применение вредоносного программного обеспечения типа «бэкдор» (Vshell), предназначенного для получения несанкционированного доступа к целевой системе под управлением операционных систем Linux.

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к IP-адресу 47[.]98[.]194[.]60, 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):

5bde055523d3b5b10f002c5d881bed882e60fa47393dff41d155cab8b72fc5f4;
8ef56b48ac164482dddf6a80f7367298d7b4d21be3aadf0ee1d82d63e3ac0c0a;
72702d6ddb671dc75e2ee6caf15f98b752df6125a43dae71cda35d305d989cf4;
5712d8a629d607c86a9d094dd24b4747b212d5a37b68ad7f10a84dd601fac751;
dd1b1e6d548b32a3cde72418f1fb77353e42142676266641a9bb12447303e871;
69e9eabfd18445352ece9383be55077cdb5bfb790a30a86758bc5249ff6b45bb;
73000ab2f68ecf2764af133d1b7b9f0312d5885a75bf4b7e51cd7b906b36e2d4.