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 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 «Акт сверки.rar», содержащий исполняемый файл с наименованием «doc_1C_BUH_akt_f5er6g5sfew6fwegf_PDF.com». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типов «стилер» (Purelogs Stealer) и «троян удаленного доступа» (PureRAT).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо принять следующие меры защиты.

1.1. Производить на этапе приема письма почтовым сервером автоматическую проверку вложений с использованием публичных или имеющихся «песочниц» («sandbox») для выявления вредоносной активности.

1.2. 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.

1.3. Осуществлять автоматическую проверку указанных в письмах URL-адресов, содержащихся в электронных письмах, с использованием механизмов анализа ссылок.

1.4. 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.

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

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

1.7. 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 исключить работу под учетной записью root, при необходимости осуществить настройку необходимого перечня команд в файле конфигураций sudoers. Использовать для разграничения прав доступа к файлам и директориям как отдельных пользователей, так и групп пользователей команды chmod, chown, chgrp.

1.8. Обеспечить на уровне сетевых средств защиты информации ограничение обращений к IP-адресу 91[.]84[.]118[.]179, используя схему доступа по «черным» или «белым» спискам.

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.

1.9. Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации sha256:
8745d7a4939a4643d72ee3e9cb177bf6ee23600115bbc3b3e75b9338b64c006b;
2e1bd5aa28b63baea57be0ddf4eafaafef07dc59c3273d75513354a3f00aaeae;
7dc7c6d5cc65f48bc227e2d8d167c3a7d57d9c4f262bb3b61272958e14bff1e4.

2. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив, содержащий файл с расширением «.lnk» (например, Решение по СВОДУ.docx.lnk). После запуска пользователем указанного файла-ярлыка осуществляется демонстрация документа-приманки и внедрение на целевую систему инструмента для обмена файлами между локальным компьютером и облачным хранилищем «rclone», а также 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 1.1-1.7.

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.

3. Хакерской группировкой Hoody Hyena, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица Ространснадзора с тематикой «Уведомление о выявлении признаков административного правонарушения». Во вложениях указанных писем прикреплен архив с наименованием «АКТ проверки ТС_ФКП ГЛП Радуга.rar», содержащий исполняемые файлы с наименованиями «АКТ проверки ТС .exe» и «Форма письменных пояснений .exe». После запуска пользователем указанных файлов осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типов «дроппер» и «бэкдор» (BrockenDoor).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.7.

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

198514f5d9f457d3abdea6ff8b8a3f8d81304aa6c317ad5fc2bdec06cb3e67ef;
3b2664e5717121cf53ca39ceb49d2d5e93f447db8aac5a6eb06bd6e990e47338;
fba114a86a8b0f00fbebf3dd76064446aeff19e65db7577ef97b6e8f6c969531;
3a0d331fe9f760a1985eafcfafd8e074b654eb3a8cb34527ffeb2c2592e8fe91;
dde4e3b4f3fa08c2ec7dfa7dfff96d14520130836b5fa8a43d159e93571c2920;
61b3a09e233bebd6192694476e1439f93ed7fcd4a6201c9eac7991abb4d3a0c2;
87186684035454fc1e76828915711bf1038900a9c7d724fafdf548e37544d7d3;
1ca08f891e591a025a88bd4692ff0c80395950bf89d5ed19cc876be64d0bdf8f;
ff2098cd6506bec92300c39e481bba9e6a06a61523b5217887ed1880454ec094;
0101773fb051b17dcccad01fc8f79c1609dc12ea49ebc6400c35dd5b34baa02d;
2267c32da8f4a71a78c0dfab3223822fda3ac78fe45d804684e371469b764ada.

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

рассылки электронных писем с тематикой «акт сверки». Во вложениях указанных писем прикреплен архив с наименованием «Акт сверки.7z», содержащий исполняемый файл с наименованием «Акт сверки.exe». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (DarkWatchman).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.7.

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.

5. Хакерской группировкой Fairy Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Направляем Вам исходящее письмо №143/26 от 11.03.2026». Во вложениях указанных писем прикреплен архив с наименованием «ИСХ № 143_26 от 11.03.2026.zip», содержащий файл с наименованием «ИСХ № 143_26 от 11.03.2026.hta». После запуска пользователем указанного файла 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 1.1-1.7.

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

87809a6cdf4497f319959863f77ea17b8d6ad359145d304ed6f9b8b49333d83b;
e96eb34b531642130017e3798191d303bbeb2d647bc7be504cae60f67cf8995d;
bdfa346660e0bf46f5c795f26c0d94520aef3ad28f7f4b802e2ae17d926c4895;
9ac48c605acd5ff1d02e35a182f2c09163c40475c9477cb36d03767bbaf007b4;
1dbd4e476c60383b92ac3b94cc9001297bc81e46a7a99563ed8b05be76fd6491.

6. Хакерской группировкой Vortex Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем по военной тематике, в тексте которых содержится ссылка на фишинговый сайт. Указанный сайт замаскирован под страницу авторизации в веб-версии мессенджера «Telegram», где для ознакомления с документами необходимо ввести номер телефона и код из СМС-сообщения. После выполнения указанных действий скачивается архив с наименованием «Proekt_prikaza_611_o_pooshchrenii.zip», содержащий файл с расширением «.lnk». После запуска пользователем указанного файла осуществляется внедрение на целевую систему программного обеспечения для туннелирования «Tor Hidden Service».

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.7.

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

103[.]83[.]86[.]235;
185[.]177[.]207[.]158;
185[.]85[.]87[.]222;
185[.]244[.]195[.]219;
45[.]12[.]139[.]49;
85[.]121[.]5[.]22;
198[.]98[.]62[.]82;
23[.]95[.]62[.]122;
94[.]142[.]246[.]132;
o472vqfrwgr6a3y5ckhf4safxmnwywnao2lyq2q7e7663y5yapchcwad[.]onion

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

cffe61e0c8dafd81b35f32d3b2f81332560c00593e7d502ea70afdbe11ad90bc;
ff883a6bb505c048df74094a01716431e3da4ee932b07290f985082a26b124c3;
28b32d6df3a30a4497f9dca91ef649abf5f35adc4104632e443fa1e0b2633085;
8b71d718237a139e399d83a716a406153d34fade9dc97c66b9a63ccd32e4e919;
6675fb335b8fd12f22fafdb66ccab7f2ea60597154a7159a4a503478a797597f;
9837bd74ae5a4a6c569c21fd529335e5e1369261ba9048b36bf711b2f4849b28;
dcd779c16cf27239ee2c9da74815cc066249232e8e6842fc2409f1b92b67e1b7;
3627c546f6af7ee790c24c3e1ba5d831dc4d0755e633786cb13772b8ec609e40;
433f44e2f3b090d00f99022e95a44c8be4935eba95654330fe45e802d8ee9666;
7be4a4652a97db8aed85824fb5ae414dc8a075ef83943e22fb66999100f7efba;
604a0e724618a03d5db5dc678c6c5942e696f0ffe0ad0b645c7b177bcbcf2ce3;

b410d3cb1d145260de53b025816664067d48251508c3866de9385e5ec3daf367;
e94d55cb981cef062bd35ed52b50c1033469523f8f93170034df3e0e7e290d9a;
02466803179c2520ed81ab7588c2955387f6e1232884e7af2fc10c5ed74f63c1.

7. Хакерской группировкой Fluffy Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Сверка на подпись!!!». Во вложениях указанных писем прикреплен архив с наименованием «doc_1C_11032026_fe5fwfeferfscd 6we6_PDF.rar», содержащий исполняемый файл с наименованием «doc_1C_11032026_fe5fwfeferfscd6we6_PDF.com». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типов «загрузчик» (PureCrypter, Donut Loader), «стилер» (Purelogs Stealer) и «троян удаленного доступа» (PureRAT).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.7.

Кроме того, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
d480e38883136f576b2f9a9d600bb85dd2d1bc5a9d44ca2eee2561daee883969;
f2f519009fbf68aed3b2011f10af1d85eddcd904bddbd9c9f5da079f125ba4af;
aa34fcbd1a948b25f16f44142289e12e411671f58ffed1ed723b1a92f56d9e09;
ea6dc73aeadb2b9938d1622995275c01e9f9d3770801c420a7b63731d6a48d82.

8. 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 «schet-no.-9564-39-i-garantiinoe-pismo-po-oplate-iskh.-no.-667.rar», содержащий исполняемый файл с наименованием «schet-no.-9564-39-i-garantiinoe-pismo-po-oplate-iskh.-no.-667.scr». После запуска пользователем указанного 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 1.1-1.7.

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

68[.]65[.]123[.]84;	depertament[.]sbs;
198[.]54[.]115[.]100;	woffice[.]online;

almaz-aero[.]site;
aviator-chek[.]online;
rostech[.]online;
sborsvo[.]space.
sbor-svo[.]online;

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.

9. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Запрос». Во вложениях указанных писем прикреплен архив с наименованием «sRFQ1002.docx.z», содержащий файл с расширением «.vbs». После запуска пользователем указанного файла осуществляется выполнение вредоносного VBS-скрипта и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Nova).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.7.

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

144[.]172[.]105[.]88;

hxxps[:]//res[.]cloudinary[.]com/dzptvoj1b/image/upload/v1773339102/MSI_PRO_with_b64_wavpuj[.]jpg;

hxxp[:]//144[.]172[.]105[.]88/img_090304[.]png.

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

2a76996372ef555e3f44cf6bff216afa3d7ac4024ee424dea1ce0a06ff190721;

6e923c3abeee19ec74dfa98f304811bad45112fda0d7d6ced0230fe42a031f52.

10. Хакерской группировкой Vengeful Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Акт сверки взаимных расчетов». Во вложениях указанных писем прикреплен архив с наименованием «Документы.rar», содержащий исполняемый файл с наименованием «Акт сверки взаимных расчетов № 198 от 12 марта 2026 года.exe». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (XWorm RAT).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.7.

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

95[.]211[.]67[.]193;

red[.]redirectme[.]net.

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

f4c5ff5415129ec3c78f3b058d3940af4b6263968feb21a3cdc8897ba68d2877;
e350407e3250a8aa84a53b79e1c65200d31fba7d8e64663c29e24367e0c20723;
4a7422531271d3a9f67ae73472dde947350f8487a4e6265cd7726a454cb26946;
3ad75c868b657a78c26405090fbabe1230d964c3adb94a000c404fdf780a2550;
78d9171e4c62b268f452522b382d29497d6994f27e373ce17a2ba13bf5f8014f;
dc939d69b4912782fb5f45960d4a7643b81a0a24b701e58dd02d4b0d28e66061;
e61bead9a297951760107292b0dd7a15be8902ef868f7a338957cc89b9cae2c1;
5b23344bb837e03355eafa2bd452143ca8f40db04709cffc2a74ca6839847033;
2760e71f4773ddd273791255271e6b796eefda51352ffbe831176040c06a465b;
373cad7008a6ed3d5bb12d406bea0d062ed03a9d96b458f48b701afb21840d40;
d2f5689b5e08823b8deb15d44b6c8370bb527e257e5eeade37c36d098ee227e5;
699c0b5fd515964a1c667fc89aec9c12bda5d5ea2dffc0b9bf52b4ed059d17d1;
445ad24a35ec3432fb90cb98a1330f78021a02d94acf2553951c82575887a2d3.

11. Хакерской группировкой Toy Ghouls, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, при реализации целевых компьютерных атак осуществляется получение несанкционированного доступа к серверам, доступным из сети «Интернет», путем компрометации учетных записей, а также продвижение в инфраструктуре с использованием протоколов удаленного доступа (RDP-протокол). После получения такого доступа злоумышленники осуществляют внедрение вредоносного программного обеспечения типа «шифровальщик» (LockBit, RedAlert, Babuk).

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:

31[.]56[.]27[.]60;

217[.]154[.]172[.]41.

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.

12. Хакерской группировкой Warlock, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, при реализации целевых компьютерных атак осуществляется применение вредоносного программного обеспечения типа «шифровальщик» (Warlock).

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

auth[.]qgtxtebl[.]workers[.]dev;
hxxps[:]//litter[.]catbox[.]moe/zqqxb3[.]txt;
hxxps[:]//litter[.]catbox[.]moe/uaw2gm[.]txt;
hxxps[:]//files[.]catbox[.]moe/wzsjlw[.]dll;
hxxps[:]//github[.]com/cloudflare/cloudflared/releases/latest/download/cloudflared-windows-amd64[.]msi.

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

ef1b604bf2e2d598437d97af38cbed4e6dbdb3fde771eaaf8389b46c86391a0d;
129eec0c999653e30a659f6a336c76d3b6ce810d459a7f860bacbc06fd556277;
34b2a6c334813adb2cc70f5bd666c4afbdc4a6d8a58cc1c7a902b13bbd2381f4;
9a3b6cf6aec6df3e5b43dc024d288d06ae03d2a909f188f38ba275a5ac6d3bf0;
206f27ae820783b7755bca89f83a0fe096dbb510018dd65b63fc80bd20c03261.

13. 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 «стилер» (MicroStealer).

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

vrcpluginhub[.]com;
buradakimvar[.]com;
kittenscraft[.]com;
dashlune[.]xyz;
buradabmwking[.]com;
crushfall[.]com;
slumpcute[.]com;
banterplugins[.]com;
velyonar[.]com;
churilend[.]com;
zarvethion[.]com;
kittiesmc[.]com;
kittycraftmc[.]com;
welarith[.]com;

eldrynworld[.]com; hxxps[:]//78smp[.]com/m/.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
9cf1d4f87d9f2edf53ce681b59c209f57a805e6157693e784d9d946fc3b17a04;
05f0c8e89248d3477115d9f62b20ca8a95d925140c727e975ab9f3025a5ad01d;
df5e2b824c0fd40323a46019bfbc325f89b5b68697ed3c94b52189cf90e1bec4.

14. Хакерской группировкой Vortex Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем по военной тематике, в тексте которых содержится ссылка на фишинговый сайт. Указанный сайт замаскирован под страницу авторизации в веб-версии мессенджера «Telegram», где для ознакомления с документами необходимо ввести номер телефона и код из СМС-сообщения. После выполнения указанных действий скачивается архив с наименованием «Spisok_na_perepodgotovky_mart.zip», содержащий файл с расширением «.lnk». После запуска пользователем указанного файла осуществляется внедрение на целевую систему программного обеспечения для туннелирования «Tor Hidden Service».

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.7.

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

5[.]78[.]114[.]1;
185[.]177[.]207[.]158;
158[.]69[.]55[.]8;
89[.]167[.]12[.]157;
91[.]208[.]206[.]67;
148[.]113[.]173[.]182;
23[.]94[.]169[.]122;
217[.]154[.]153[.]110;
94[.]142[.]246[.]132;
jgwlqantwdpfjb7xoifv4pke5ichmvk3taidaa3gt7254r5xfrehg5qd[.]onion.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
a2306445f6a9a9313ec3709c84bc3e932f75240fcaf2543bb1cdc3c362b64552;
0c6c020a92517dcd757939c4f907550dbff08f133311d74928f27cf4133db7e9;
27f8714fdd2cef76beb5aeb8e9973604a77ba2197532002f4d8d30a1249dcaba;

42b64728b2a758e0e0c0dce181bc757cbe1245b927dda2a7d492aab3dd35e402;
a7a6feef6c85474bbd09d49225f84d1ada56e609386d7617aa05e9f613f6b594;
d5b5c7e7ef10680f208dd887f53ab95256e0aa7b22610bb774a5e382efbae3cf;
68389d6eeccc87499e4e31d92f63f3a0ce995638990a29984dc5aae41568baa2;
d0fb64fe998c332a1f99cadbe41d3ade4759301a0d891bc472023054973c1a8c;
f0845fdf742e64769bf2814f4416172023f5cda9e6c714e3a84d797b3ca8e419;
a4f3ca2dfb499d67a47af889e27ed8cc6924be43b1032bd6fa2db6c220682634;
c7459289fe8fc5dc7b073bc22626ad3a7e40c206ab81b08f9ee000eb8d752d0f;
f5f9f66d0fbc1ab7ad0efe82e0aa29e1665047e945c7b821bb4189901c57ef13;
ad1045181268be6c0c05ac5c57471fecbaeef2de6cdcc2619d989c490ae4dd50;
599b21b953c4091710062e753b50b419a182690cae376a5d6c3fbe60cd8e250e;
ea6c8182092241d19b9cf25e20aa9455bb02ef8418e74e3916412a5a228520fe;
d999b540bcfb7b09f8fc42497f509cfcd26ac2d168a5dedfec0557a77af696c5.

15. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Отправка: Исх. 9, ТКП Эко-Фильтр». Во вложениях указанных писем прикреплен документ с наименованием «189808.xls», после запуска пользователем которого осуществляется эксплуатация уязвимости пакета программ Microsoft Office (BDU:2018-00096, уровень опасности по CVSS 3.0 – высокий) и дальнейшее внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Remcos RAT).

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28.10.2022, а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 30.06.2025 (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.7.

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

192[.]3[.]176[.]237;
172[.]94[.]100[.]226;
shuiqianyeting[.]com;
gsxshpltd[.]com;
alphaheat[.]pl;
192[.]3[.]176[.]237[:]80/500000000000000000000000000[.]php.

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.

16. Хакерской группировкой Watch Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Счет на оплату». Во вложениях указанных писем прикреплен архив с наименованием «Счет на оплату НК-24.7z», содержащий исполняемый файл с наименованием «Счет на оплату НК-24.exe». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (DarkWatchman).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.7.

Кроме того, 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 Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Добрый день! Отправляю финальную редакцию технического задания на разработку изделия.». Во вложениях указанных писем прикреплен архив с наименованием «Проект технического задания на разработку изделия № 6073 Исх. N 274.rar», содержащий исполняемый файл с наименованием «Проект технического задания на разработку изделия № 6073 Исх. N 274.com». После запуска пользователем указанного 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 1.1-1.7.

Кроме того, 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 Rainbow Hyena, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляется эксплуатация

уязвимостей программного обеспечения TrueConf Server (BDU:2025-10114, уровень опасности по CVSS 3.1 – высокий) и (BDU:2025-10116, уровень опасности по CVSS 3.1 – критический). Эксплуатация указанных уязвимостей позволяет злоумышленникам получить несанкционированный доступ к системам и осуществить внедрение вредоносного программного обеспечения типа «бэкдор» (PhantomPxPigeon).

В целях предотвращения возможности эксплуатации указанных уязвимостей рекомендуется установить обновление программного обеспечения в соответствии с рекомендациями разработчика указанного программного обеспечения (https://trueconf.ru/blog/update/security-updates).

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

19. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, при реализации целевых компьютерных атак осуществляется применение вредоносного программного обеспечения типов «загрузчик» (CastleLoader) и «троян удаленного доступа» (CastleRAT).

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

172[.]86[.]123[.]222;
23[.]94[.]145[.]120;
sennbuappec[.]zhivachkapro[.]com;
serialmenot[.]com.

Кроме того, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
bd8203ab88983bc081545ff325f39e9c5cd5eb6a99d04ae2a6cf862535c9829a;
a4787a42070994b7f1222025828faf9b153710bb730e58da710728e148282e28;
8b7c1657f4d5cf0cc82d68c1f1a385adf0de27d46fc544bba249698e6b427856;
fddc186f3e5e14b2b8e68ddbd18b2bda41d38a70417a38e67281eb7995e24bac;
dfaf277d54c1b1cf5a3af80783ed878cac152ff2c52dbf17fb05a7795fe29e79.

20. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, при реализации целевых

компьютерных атак осуществляется применение вредоносного программного обеспечения типа «вайпер» (consumerWiper).

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):
7a00f5219f61850b5999bde9669094ac8932971e15978d11962e42af964c096c;
89e0f599afa7705df55bf345c41236e70efa813c7e82caee4171dce678010b66;
e4dfcf17aab37f01b0d24010cab1875f28ee545a9d330c85de1a21ec682e840f;
8554f4062d3fc3dd8efeda65b8620ce74d98b125627d5be72bca7b0930edf737;
5cfce12d2c8687eba1529ec82f93b85ff2b503959d19d82e9873c0c473caebe1;
ba2d428d5b4e0ee1cc4a952fec254de453d8514e546f64919abd13c0bbc59473.

21. Хакерской группировкой Toy Ghouls, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, при реализации целевых компьютерных атак осуществляется получение несанкционированного доступа к серверам, доступным из сети «Интернет», путем компрометации учетных записей, а также продвижение в инфраструктуре с использованием протоколов удаленного доступа (RDP-протокол). После получения такого доступа злоумышленники осуществляют внедрение вредоносного программного обеспечения типа «шифровальщик» (GenieLocker,Vice Society, LockBit, Babuk).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки, 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. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, при реализации целевых компьютерных атак осуществляется применение вредоносного программного обеспечения типов «бэкдор» (Gafgyt), «ботнет» (Mirai, Moobot) и «троян удаленного доступа» (Remcos RAT, AsyncRAT, njRAT, DarkComet RAT).

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

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

9f13b2aa5804719b318a0cdd0a98b6aa26e03da947a739a95a3419206a06681a;
7f94c2c694a9cfe1d0438acf5e05dedb2f03612c3596abb2ed729f35da33e462;
bc933b5ecca8b3864741c92fe0682f41a36bf809862ec9a61b09c83ad7b3d6ce.

23. 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 «загрузчик» (ICE Cloud Client), предназначенного для функционирования на серверах с программным обеспечением «Microsoft SQL Server».

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

hostroids[.]com;

hxxp[:]//109[.]205[.]211[.]13/api[.]exe.

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

6130a96f19ab4e3af5dfaf16fef8d8c176d9cc508b0422032ef4c18a4b65ef19;
0c16e8b6232ecc2f3e1ed09b21ecda6bd27f098fb662dc253963219a26a72661;
006193f1b6125ce5b14a68dd0944e089c6575a8a772749f751e55c6d934b40d5;
393b731eeb04e8aa8844028d046cdea653598a7258b7a25e4efa6ebcaba68916;
7ac9ea9f9d9a25c73d3267e7466cb0643f4e981bda36013ee9264feebe38b51c;
9084885412af5ae242082869ebb204bcc855db4216bda0b399d06097d193aab9.