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. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица ФГБОУ ВО «Юго-западный государственный университет». Во вложениях указанных писем прикреплен файл с наименованием «ЮЗГУ.docx.js», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Quasar RAT).

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:

196[.]251[.]69[.]23;

hxxp[:]//196[.]251[.]69[.]23[:]8080/f69ca4b4a559252eb0b613845807c9c6/.

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):
d8d1f24cb9a3d25511b5993891fe8edddb0fe711aaec1727e65f3cea8cd23751;
18d516d2827ebb094d2928dc42f509bc9b39c38391383f13153f2f6b1f01308c.

2. 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 «Расчет стоимости по договору №4850-54.scr». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для удаленного администрирования «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):
36541fad68e79cdedb965b1afcdc45385646611aa72903ddbe9d4d064d7bffb9;
dd5cebf0b4244af6d5bcb32a0079759b714df67c5c9beb988a7b0b76551fece2;
cc2c7915597cabed7a2e8b555fa5e4c6fb90556a8447e46b9adb480047c1b07c;
431ebadc524c3a4154887abb693bcd1f24b272425f7ab9a7b346e5bf9a4ba594.

3. Хакерской группировкой Core Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица УМВД России по г. Саранск. Во вложениях указанных писем прикреплен исполняемый файл с наименованием «Запрос на ПОВСК Расследования уголовного дела №1240 на территории Октябрьского района СУ УМВД через ВСО.exe», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для удаленного администрирования «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:

foundersinfluence[.]com;
dveri-kuban[.]ru;
195[.]2[.]70[.]182;
45[.]128[.]148[.]65.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
5cef676626962f9f140c5ecf187380aed16b166b44c9a58360494a8f4e8bf725;
77cc62e6a22c48931f85ec65ce09e61f19da8576dcb43da61551d8b6459c383f;
8859d16774cf3f24de05354667025fee205cefcc6bae90bf0aa49a1088d6be9a;
e53f9e5ceb2b03298ce01e7863ffe6ce8f618c2ca82a0df1c173bb93070e95a5;
7c0cce3e3f41974eb8e32bb43af7181967111695d45e018efcd40bbe7e532f6d;
530899fc0b2e0d0dacfbb171119845a07f0a0d23f9d75e64eedbaac81513d199;
8e4497c1f46f40ddd08dbe7bd4093082a41fad0708df4291529a756c8ca7d157;
bde868dbb6a5be921ff49c0a9d97773d72e729c93e658ef3c8dd2e0e2fd359c8;
a64bc48bccb814dfa1410e8ff7e7d990dfba9a456c594ff446985759f3c3e52d;
3cf6433bf5bbac26258c00d4cc38e2966237dba7fc3a9f59494dcbd9620600f7.

4. 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», содержащий файл-приманку с наименованием «Бланк.doc» и исполняемый файл с наименованием «Акт сверки взаиморасчетов предприятия № 185 от 13 октября 2025 года.exe», после запуска пользователем которого 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 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):
b5b8d144d2a7bb97636315294bbc496522f959de88560d2f7accb746495b761c;
a1bece6bdaa5d98b6b646ad4206515fae31622b6c7d8a9d01e22b1c4b4944124;
33a3fece5eecf6843309ead5534ff88e1e81f36219e28f273ed4c5af6a2ab22f;
c2787be035ada07a4b53d72df2776b1ec198cf4bed33ed5c5983d1ed17306f16.

5. 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 «1C_buh_doc_08102025_PDF.rar», содержащий исполняемый файл с наименованием «1C_buh_doc_08102025_PDF.com», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типов «троян удаленного доступа» (PureRAT) и «стилер» (PureLog Stealer).

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

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

docbuh[.]ru;
buhgalteriya1c[.]website;
docbuh[.]online;
docbuh[.]fun;
hxxps[:]//docbuh[.]online/panel/uploads/Mxbljgkod[.]vdf;
hxxps[:]//docbuh[.]online/panel/uploads/Gndpbnfiwe[.]vdf;
hxxps[:]//docbuh[.]online/panel/uploads/Jfnsnf[.]vdf;
hxxps[:]//docbuh[.]fun/panel/uploads/Ylevwh[.]wav;
hxxps[:]//docbuh[.]online/panel/uploads/Yfapsyymcp[.]wav;
hxxps[:]//docbuh[.]fun/panel/uploads/Wlpvmd[.]pdf;
hxxps[:]//docbuh[.]fun/panel/uploads/Wqddwm[.]mp3;
hxxps[:]//docbuh[.]online/vncserver[.]exe;
hxxps[:]//docbuh[.]fun/panel/uploads/Toitc[.]dat;
hxxps[:]//docbuh[.]ru/1C_buh_doc_08102025_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):
459a421217d82f46b14b2d14c61d3a62841a71d8eb8e490cbeb343149af3d357;
e3b42b2a1a4dd58d49b577c51b4cb0f96cea6d349020c55993399175f1b320b8;
b1b0f79c51437a5f561f5a6b31d9df2e5cbd7555acdb070767684c59661dce2e;
9832871803111bcdaabcb11de6d6f4f928c93756dee7c5a25aa839cc64718abe;
3bb8dd29ecb9eb6f32c2ad9a0ab06bc8061a5f4e3c002a4e20c144aabba531ed;
2dcfca468cb2f6ba8dadd81ab88440a9d377eb3501594e56a5a461fccbb3cc82;
2b5737ebe552af49903bdf7e184270ae41de53fa380da7d28df9874973d9533b;
524144e2b0d551535db7bb1de9ddbe369e7f6e01dadde3c307c96704f8f7327d;
a5656a79a24c630a46773df83b8e494853f0aa018b825675dfdbdc1d583abafd;
fb07e48535048a2a679f2a500746edafca726ef31580af32baf59f7e628b1278;
06946517ad161f4eb497078c3b09379b76a393e378a5ca9279ab3d6f7e17d144;
e75fe75b0d1e5e30345d9259e207cd280bbed0239bcab9258b1b861b893e2e3f.

6. Хакерской группировкой Jewelbug (REF7707, CL-STA-0049, Earth Alux), нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются атаки на цепочку поставок применяемого программного обеспечения. Злоумышленники таким образом внедряют на целевую систему замаскированное под легитимное программное обеспечение вредоносное программное обеспечение типов «загрузчик» (Pathloader и Guidloader) и «троян удаленного доступа» (Finaldraft).

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:

app[.]blance[.]workers[.]dev;
cdn[.]kindylib[.]info;
95[.]164[.]5[.]209.

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.

7. 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 «стилер» (Lumma Stealer), функционирующего в операционных системах Windows.

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.

8. Хакерской группировкой Equation Group, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, при реализации целевых компьютерных атак возможно применение вредоносного программного обеспечения типов «троян удаленного доступа» (SecondDate) и «бэкдор» (Bvp47), предназначенного для функционирования в операционных системах Linux.

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки 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 следующим 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 следующих индикаторов компрометации (sha256):

d799ab9b616be179f24dbe8af6ff76ff9e56874f298dab9096854ea228fc0aeb;

7989032a5a2baece889100c4cfeca81f1da1241ab47365dad89107e417ce7bac.

9. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «Pereraschet_zarabotnoy_platy_01.10.2025.zip», содержащий файл с наименованием «Перерасчет заработной платы 01.10.2025.lnk», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (CAPI).

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[:]//carprlce[.]ru;

91[.]223[.]75[.]96.

10. 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 расширением «.scr» (например, «Платежное поручение № 194.scr», «комерческое предложение + договор 2025.scr»). После запуска пользователем указанного 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 следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hxxps[:]//identification[.]site/adriver[.]rar;

hxxps[:]//identification[.]site/adrivery[.]rar.

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

ec1518703ccce045caf74470c49a140f381b3c65be397971665c905d253297d7;
aab6d8c7e1db0441c487e81bf4246791e73d34f2848e9ea24f282f29f77b719c;
d997aa0f0c5388be5a00a9f5d17fe59d11d33b2d3bdde8c73c71cb1831924efa;
b56e31ce083dc54e0a31e9dfeab48c190c04513c5934ddc79e73c38c0224b550;
4b78beeed7e2d3cefeb9bd2a996625840b515425fad0fbc5a552169245753189;
dc99373ca1fa27d0bb907fc2a74fcc0e60145a1d7983e3812de5a20b8c851103;
fa417c2e377d847affaf9453443b6e38860060b984536e1ae6905cbe805a0e80.

11. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются атаки на доступные из сети «Интернет» серверы, функционирующие под управлением операционных систем Windows Server и имеющие неустраненные уязвимости. После получения несанкционированного доступа к указанным серверам злоумышленники внедряют вредоносное программное обеспечение типов «бэкдор» (Neursite), «загрузчик» (NeuralExecutor) и «фреймворк постэксплуатации» (Cobalt Strike).

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):
592a07800c1e52095b3b608e3756dbba4f33d40d5c2f6dfc44746597779cf29b;
415b2b861bca9872fc35c70930fa8d23d545e89e35b35f8526be419da691abd1;
25baeb86e76dbaafd6a81b4c9d1aa53bdc8d9ac5d0e09c4113532e4309b1e16b;
1e87d84fdd53a09f9466e85dec3d1c1d2d947fbd5d6672cdbc0a9650052e1b57;
6f6b1ee536e062c47c60d29064686d7b431466c93bfeccd4c573656e40948e59;
1d3fc66ba1f8707676feaf330e621b1a19f1938a6e51e6bf947bb03834dc8b33;
5277ad7cef03f580b3dc6d50f7c03c233434abaa99e0f2330ef6a573423f15df.

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 прикреплен файл с наименованием «ИСХ № 67ОП-98 от 20.10.2025.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 1.1-1.5.

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.

13. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Подтверждение банковского перевода». Во вложениях указанных писем прикреплен архив с наименованием «Подтверждение банковского перевода.zip», содержащий исполняемый файл с наименованием «Подтверждение банковского перевода.exe». После запуска пользователем указанного файла осуществляется выполнение команд оболочки сценариев «PowerShell», демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Phantom 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 осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
60994115258335b1e380002c7efcbb47682f644cb6a41585a1737b136e7544f9;
5bc908e71983c9ff8a5333c492bd6156331e2435852da83577bcdef9942da1b9;
78826700c53185405a0a3897848ca8474920804a01172f987a18bd3ef9a4fc77;
4b16604768565571f692d3fa84bda41ad8e244f95fbe6ab37b62291c5f9b3599;
448cd258dd36734b13c74ce38c277a10b596b17a72ba83ca35439d8e2141dabe;
fecc45443b786f09fc2502f5085de041ad24ac33bbfbc5ad96862d7b77b2ef68.

14. Хакерскими группировками, нацеленными 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 «2039847002.zip», содержащий файл с наименованием «rrk899c3.VBE». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Nova).

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

Кроме того, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
e57b3763e7509f1c84c8bdad69cdb4f4fa2a99113a9ce3ac1e3bdd41ec4426b8;
d1fd24e32d986ee702fb47ca00735731b0967150ff61eb12dad930c65e1b2c95;
8285d94bc15b8fdab803524e035c4774695c432876c9e2ff424937855a414e9d;
9406e468e006353e0bdde0ce143a367ced3bce1094b749976b88f1c3e750783f.

15. 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 «стилер» (BeaverTail, InvisibleFerret и OtterCookie), функционирующего в операционных системах Windows и Linux.

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 индикаторов компрометации, указанных в приложении к настоящим рекомендациям.

16. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются атаки на цепочку поставок применяемого в информационной инфраструктуре программного обеспечения. Злоумышленники таким образом внедряют на целевую систему замаскированное под легитимное программное обеспечение вредоносное программное обеспечение типа «фреймворк постэксплуатации» (AdaptixC2).

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:

cloudcenter[.]top/sys/update;
cloudcenter[.]top/macos_update_arm;
cloudcenter[.]top/macos_update_x64;
cloudcenter[.]top/macosUpdate[.]plist;
cloudcenter[.]top/linux_update_x64;
cloudcenter[.]top/linux_update_arm.

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

29523252648a607825afe9122708e655b56efe7cec1aaf5f9f41d24534583111;
fd0eab4671a7e626c597a7f5de930af1dc66c1014622649a4e94b7c3d086e097;
de8a99f4b1b0a7cc86ef5d28fb9c6fb2f9842c4795a974bb74354658cda63d68;
2ed4ef708e42036e295e65567d25ba03b2b7ecdad9d939632d45ab48a931d616;
c81b5c1d135fd6bd9cca75fe9ede727abd84b9a0b50cb98c8c3ecc2a33813ed5;
d988fb61d3b3370fc9fa8bf013be8fc24a8f5dd63cfdfefee52c77ab1dc94458.

17. Хакерскими группировками GOFFEE и «Киберпартизаны», нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляется распространение вредоносного программного обеспечения типов «бэкдор» (Vasilek) и «фреймворк постэксплуатации» (Cobalt Strike), предназначенного для получения несанкционированного доступа к целевой системе и удаленного администрирования через API-запросы мессенджера «Telegram».

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:

easylink[.]lol;
git[.]npovsdev[.]com;
chck[.]yastats[.]com;
81[.]200[.]208[.]62;

77[.]232[.]37[.]179;
mwdns[.]ru;
linuxpedia[.]ru;
ttl-service[.]ru;
kotlinapps[.]ru;
feedback[.]ignorelist[.]com;
static-content[.]strangled[.]net;
194[.]36[.]150[.]227;
213[.]183[.]54[.]189;
91[.]210[.]107[.]252;
103[.]136[.]43[.]40;
hxxps[:]//requestbin[.]kanbanbox[.]com/1bgrbdm1;
146[.]70[.]52[.]221.

18. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Запрос цен и условий поставки». Во вложениях указанных писем прикреплен архив с наименованием «Scan_61115872.7z», содержащий исполняемый файл с наименованием «Scan.scr». После запуска пользователем указанного файла осуществляется выполнение команд оболочки сценариев «PowerShell», демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для осуществления удаленного администрирования «AnyDesk».

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:

198[.]54[.]114[.]214;
titan-barykady[.]site;
hxxps[:]//titan-barykady[.]site/Libe/nkgobfvdryujytfr[.]rar;
hxxp[:]//www[.]4t-niagara[.]com/checkupdate[.]php.

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

0ebe79abbfc9091bdc6f7fcf863020e5b005886592e72dc9f5c3c69560176aee;
be567874f5161979ffefe75f4e2be1db9224cfc1670f8b6fb8a67a32db623ff8;
5afbb7dfa6a8269e1e95cf72999b8d1d72fecf63054d7fd3243c85dd8210963c;
3689afd3b78f7818cdfbc7805f67772c11e0b480b990cd5a54246c9bb0c1da9d;
c43438dda5c749e3d22834432c36ec74e109bdc705813d49dd6404117a6f8e5a;
e613d07619b28f896b4adf24d888cf52814fa2eb89f261f2e4715485954251b7;
431ebadc524c3a4154887abb693bcd1f24b272425f7ab9a7b346e5bf9a4ba594;
36541fad68e79cdedb965b1afcdc45385646611aa72903ddbe9d4d064d7bffb9.

19. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Новый контракт». Во вложениях

указанных писем прикреплен архив с наименованием «Контракт Кит Питер.7z», содержащий исполняемый файл с наименованием «Swift payment advice-4567688978676564.cmd». После запуска пользователем указанного файла осуществляется выполнение вредоносного Batch-сценария, демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (RemcosRAT).

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:

192[.]145[.]124[.]4;

westy[.]karslioglu-tr[.]com;

hxxps[:]//files[.]catbox[.]moe/3lyygr[.]afm.

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

0b3df1b7b218d03bff0e447148a47430906571a3d4addd8f7d7c804aad9f8362;
a087dfc9ba318c28051f4405ca146a71a1f4018d5600c3fe89a999a61690cd6b;
0764d8bca072090e53966419e3c34553d1c09fb859aab96e5db90a6634c62dbd;
66832a905fd412dbef52aafe547c6c1c53e879a73e1fc4b38d580d69eb6976e3;
54bac2856701e27534709111dda8489ff7b49f1fc45209620722292c00ded183.

20. 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 «Уведомление №221 о начале комплексной проверки согласно плану утечек-копия-7.exe». После запуска пользователем указанного файла осуществляется выполнение вредоносного Batch-скрипта, демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для осуществления удаленного администрирования «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 ilyaforexperts[.]ru, используя схему доступа по «черным» или «белым» спискам.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
773e2806b20a0897f7b7af74d15435cdd459965af8d01e2470738bfa1c6349b0;
91c16c64a572a2231e3c387cc48ddbe1b7c1ac84ee66ffa99b2d88e99d564afb;
6f1f91c967aafd9f878fcf06ef97c9ec654f47cd5fd418ecbee83dd4fbbe5f56;
9d39eb2650783f4931a4640280f59dc1c7a0b1e1ca57ddd6cc6c4f7da456b0a2;
0e461fa2ec0bd361f7c03fde81d1313485fc1c1a21a03fd06ff12e7970891a48;
0c61d0d6e8453681da7088b0fc269e7e7c81dcbbbb05f3db62b12570db6b5208.

21. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «авр акт сверки срочно» от лица АО «Казпочта». Во вложениях указанных писем прикреплен архив с наименованием «SKMACPATCHTECH116456437673474344377.7z», содержащий файл с наименованием «SKMACPATCHTECH116456437673474344377.vbs». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типов «загрузчик» (Guloader) и «троян удаленного доступа» (RemcosRAT).

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:
138[.]199[.]59[.]4;
adigo[.]ydns[.]eu;
wormoni[.]lms-austria[.]com;
hxxps[:]//files[.]catbox[.]moe/3kacg4[.]ttf;
bafybeihcr7wnyfhbzcr4cibteqb5frfny3bjzavywphousve5ddfah6bry[.]ipfs[.]w3s[.]link;
bafybeie52e6zbmarzitwsiggtg4qpmrbek2wovzs2tsxv7brqysbbl62gm[.]ipfs[.]w3s[.]link;
hxxps[:]//bafybeihcr7wnyfhbzcr4cibteqb5frfny3bjzavywphousve5ddfah6bry[.]ipfs[.]w3s[.]link/sporadial[.]ttf;
hxxps[:]//bafybeie52e6zbmarzitwsiggtg4qpmrbek2wovzs2tsxv7brqysbbl62gm[.]ipfs[.]w3s[.]link/oiJTzNDvxryVBDPmcTyClnV76[.]bin.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
c7b32275fad875299025fe19ea7c455bdd2555b542197e7a8bb0f1518d304dbd;

9a9c53a7d5a059f5b40b4aab7837aa4f08948919c6dd8e2d7cc53efe6ebe15fb;
3aa368339720e867c6853c6157828e58a2ad5d19281e9f09786aeb0f3918366b.

22. Хакерской группировкой Fluffy Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Акт и УПД» от лица ООО «АльтаСтрой». Во вложениях указанных писем прикреплен архив с наименованием «УПД и акт сверки.rar», содержащий файл с наименованием «УПД_акт_сверки_1C_buh_Doc_27102025_PDF.scr» или «scrin_shot_1C_buh_Doc_27102025_PDF.exe». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типов «стилер» (PureLog 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 1.1-1.5.

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

hxxps[:]//1c-buh-akt[.]ru/Vckrip[.]exe;

hxxps[:]//1c-buh-akt[.]ru/panel/uploads/Vdmbydnup[.]pdf;

hxxps[:]//1c-buh-akt[.]ru/panel/uploads/Xhsvqgfwn[.]vdf.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
29f5b9d8f1f120a20d870a9b8c9e7c7b57243d68eaecae196f1865c53feb73bd;
dcc7a76ae19a68cfc9655ab3fdde661ac098bd352dcdbc41d0e9d113abe31085;
5b1cfeb90e33b144d17f2912f795867bbee3028f2c21db11facdd7a3bb7b8921.

23. Хакерской группировкой Cloud Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен файл с расширением «.doc». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (VBShower, VBCloud и PowerShower).

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

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

kommando[.]live;

atelierdebondy[.]fr;

hxxps[:]//kommando[.]live/us/?idmt[.]html/dementedly;

hxxps[:]//kommando[.]live/usa-online-casinos-zealand-the-pokies-king/?idmt_html/dementedly.

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

8ff9b4b1dcc3b759e31cc249dfb15e9d0f3705cd;

4ab950002e2e1968b1915ec95b62a91740b10cb8;

e3d62ba9609851719080f4d62d22ff8e8584731d;

ff30ebff67258f067021556338195b0e02ba9a40;

af989433c920346e9f74bb27ccde0c3c14f7f578;

c8028a2656f0cc0a1c44450b8270634bd3f88617;

da381c853f1544ebe1c8aba4ac565255dbb438ee;

b45607c5114852cb07c191719cceea9c2e2316ea;

9c34b77bc68fb9b8f440d8f0ed4b0cbacd1ae2c7;

f305ebaacbeb7746147f651d15bfb5da5dfe6ecc;

63e07982afbfe0154d5894c314379af11c84a5af;

c00926833b195eabf1281da51ea566db7025c15b;

2441ddb88b998915de991e76c915dca591f01245;

57db839a5060ea25423a19ae9bf0c0c32a2bbf8d;

405237bd1231d3b1a47ff17930b11b6992491a2f;

5ff4f47ba79a0a0649a25910e6df5c09f4b83f11;

a08343ace9a8891f0e54d4e7efd219800c52bb0c;

b80561b2d0725ed2125567e8b3976403a041e485;

4dc916b2537071a0f73f2600b008a8571c30488d;

a17543a66b8035a0816b6c50beef9fd725914f7d.

24. Хакерскими группировками, 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 злоумышленники эксплуатируют уязвимость компонента Mojo браузера Google Chrome для операционных систем Windows (BDU:2025-03258, уровень опасности по CVSS 3.1 – высокий) для получения несанкционированного доступа к целевой системе и внедрения вредоносного программного обеспечения типа «стилер» (LeetAgent и Dante).

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).

Кроме того, рекомендуется принять следующие компенсирующие меры:

ограничить возможность пользователей перехода по ссылкам, полученным из недоверенных источников;

использовать средства изолированной программной среды для открытия ссылок, полученных из недоверенных источников;

использовать средства обнаружения и предотвращения вторжений (IDS/IPS) для выявления и реагирования на попытки эксплуатации уязвимости.

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.

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

2e39800df1cafbebfa22b437744d80f1b38111b471fa3eb42f2214a5ac7e1f13;
388a8af43039f5f16a0673a6e342fa6ae2402e63ba7569d20d9ba4894dc0ba59;
07d272b607f082305ce7b1987bfa17dc967ab45c8cd89699bcdced34ea94e126.

25. 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 «шифровальщик» (Warlock).

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):

9d52af33c05ea80f9bc47404b02ace4e16203dd81aef9021924885a6bff1d3c1;
15649e4d246fe6d03dc75ecb4cabe5d1f8723519ed8dd3176e1a97325e827daf;
24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf;
f6ee01303cf1d68015eee49f7dc7f26151a04ae642a47e49c70806931ce652d3;
edcf76600cd11ef7d6a5c319087041abc604e571239fe2dae4bca83688821a3a;
e23d5cb32a2d62314a8b26a205b634ee968f5a0500c190bc6edb55ec70285eb5;
9f2434d5f8d042323cc7964520d99bda661bb23ce505cb03c8a07758bc9397a6;
8ca7304846c69300237a8577fbeec2720ea9a4bd09cb7fe484a8d5efc79ad073;
bba75dc056ef7f9c4ade39b32174c5980233fc1551c41aca9487019191764bac;

ca2c02f592d72cafc218f4edd1ea771f8d1458cb95c2c76c3e384e63cefd1fb6;
6feb5361fd3abd3a7a733c30bfcc2b58fc774ac6aa91a468ce2e31dcffc9d4de;
2c9f0f324e9cca0481162cdc21ee9b60a7541941a33af99113d08bbd859d7473.

26. Хакерской группировкой Head Mare, 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 с установленным указанным программным обеспечением.

Необходимо обновить программное обеспечение TrueConf Server согласно рекомендациям разработчика.

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:

5[.]178[.]96[.]82;
5[.]252[.]178[.]171;
31[.]57[.]108[.]232;
31[.]58[.]134[.]251;
31[.]57[.]109[.]151;
185[.]90[.]60[.]227;
xbox-updater[.]online.