Приложение № 1

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 «Расчёт 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.