МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ АЛТАЙСКОГО КРАЯ
(МИНОБРНАУКИ АЛТАЙСКОГО КРАЯ)

ул. Ползунова, 36, г. Барнаул, 656043
телефон: 29-86-00, факс: 29-86-59
E-mail: info@22edu.ru

14.01.2025 № 23-05/18/10

На № _____

О направлении информации по информационной безопасности

Краевые государственные организации, подведомственные Министерству образования и науки Алтайского края

Муниципальные органы управления образованием

В целях повышения уровня информационной безопасности и устойчивости информационных систем и ресурсов направляем для использования в работе разработанный Министерством цифрового развития и связи Алтайского края бюллетень по повышению защищенности информационной инфраструктуры.

Приложение: в электронном виде.

Заместитель министра

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 62B59E9C2B270538AD02D0A0FACC02C3
Владелец Исакова Лариса Васильевна
Действителен с 02.07.2024 по 25.09.2025

Л.В. Исакова

Ларьков Егор Сергеевич
(3852) 29 86 63

Бюллетень информационной безопасности от 13.01.2025

I. Сведения об уязвимостях.

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

1. Уязвимость драйвера Windows Common Log File System (CLFS) операционных систем Windows (BDU:2024-11011, уровень опасности по CVSS 3.0 – высокий), связанная с переполнением буфера в динамической памяти. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии до уровня SYSTEM.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (далее – «Методика тестирования»), а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (далее – «Методика оценки») (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty).

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

использовать SIEM-системы для отслеживания индикаторов компрометации (IOC), указывающих на попытки эксплуатации уязвимости;

использовать программные средства контроля действий пользователей для обнаружения попыток эксплуатации уязвимости;

использовать средства антивирусной защиты информации;

произвести минимизацию пользовательских привилегий;

отключить (удалить) неиспользуемые учетные записи пользователей.

2. Уязвимость реализации протокола службы каталогов LDAP операционной системы Microsoft Windows (BDU:2024-11018, уровень опасности по CVSS 3.0 – критический), связанная с целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

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

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

ограничить для контроллера домена получение входящего RPC-трафика из недоверенных сетей;

ограничить возможность внешних подключений по протоколам RPC и LDAP с использованием SSL.

3. Уязвимость программного средства резервного копирования и восстановления данных для удаленных и облачных клиентов Veeam Service

Provider Console (VSPC) (BDU:2024-10848, уровень опасности по CVSS 3.0 – высокий), связанная с ошибками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, удалять произвольные файлы на сервере VSPC.

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

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

организовать доступ к уязвимому программному средству с использованием «белого» списка IP-адресов;

отключить (удалить) неиспользуемые учетные записи пользователей;

произвести минимизацию пользовательских привилегий.

4. Уязвимость сервера приложений Apache Tomcat Framework (BDU:2024-11286, уровень опасности по CVSS 3.0 – критический), связанная с ошибками синхронизации при использовании общего ресурса («Ситуация гонки»). Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем загрузки специально сформированных JSP-файлов.

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

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

ограничить возможности загрузки JSP-файлов в каталоги сервера приложений с помощью сервлетов;

использовать средства межсетевого экранирования уровня веб-приложений для ограничения возможности удаленного доступа к серверу приложений;

использовать средства обнаружения и предотвращения вторжений для отслеживания подключений к серверу приложений и загрузки файлов;

использовать виртуальные частные сети для организации удаленного доступа.

5. Уязвимость функции nft_verdict_init() в модуле net/netfilter/nf_tables_api.c ядра операционной системы Linux (BDU:2024-01187, уровень опасности по CVSS 3.0 – высокий), связанная с повторным использованием ранее освобожденной памяти. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации и повысить свои привилегии.

6. Уязвимость компонента clk-mt2701 ядра операционной системы Linux (BDU:2024-10523, уровень опасности по CVSS 3.0 – средний), связанная с разыменованием указателя NULL. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

7. Уязвимость реализации протокола аутентификации NTLMv2 операционных систем Windows (BDU:2024-09487, уровень опасности по CVSS 3.0 – средний), связанная с раскрытием хешей в результате некорректного внешнего управления именем или путем файла. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, реализовать атаку Pass-the-hash.

В целях предотвращения возможности эксплуатации указанных в пунктах 5-7 уязвимостей рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

II. Сведения о деятельности хакерских группировок.

По результатам анализа сведений об угрозах безопасности информации и деятельности хакерских группировок, проводимого специалистами ФСТЭК России в условиях сложившейся обстановки, выявлены сведения о деятельности хакерских группировок.

1. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от имени Федеральной антимонопольной службы. Во вложениях указанных писем содержится вредоносный файл с наименованием «2024_Определение о возбуждении дела.docx.lnk», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение вредоносного программного обеспечения на целевую систему.

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:

185[.]22[.]152[.]199;
ftp[.]media-storage[.]myftp[.]info;
hxxps[:]//mivz[.]ru/api/files2[.]php?fileid=PLMN;
hxxps[:]//mivz[.]ru/api/files2[.]php;
hxxp[:]//185[.]22[.]152[.]199[:]443/api/send_to_client;
hxxps[:]//mivz[.]ru/api/files2[.]php?get=1PLMN1731912032;
hxxp[:]//185[.]22[.]152[.]199[:]443/api/register.

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):
231cf0075fd311223539743906a974b37354c45e3a792b30f410bd307f32712e;
0ed459cf2682b12d95613ca8f1f1b9d71bcc529c681f8a2a0ec347bba7d8f4b6;
d3aaf9a04437859b513efabfdd2d57ef6eb1e66c46645a09c1b8d80328997e28;
88aa1bd65a6ff5d92ac7041e9685c20e08286709971881660df9c0f4a04c06db;
46c0fd35e4699265db0223cee00b3da48ec157e2d7a51590c87b077918f76d5b;
601f00162583c82d933ad27ec6b3f900d2efde81a1f4cf3724e5cfc4875305cb.

2. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематиками «Срочно нужен новый заказ» и «Дополнительное соглашение к договору». Во вложениях указанных писем содержится вредоносный архив с наименованием «*.pdf.rar» или «*.xls.rar»,

замаскированный под финансовый документ. Внутри указанного архива содержится исполняемый файл, после запуска пользователем которого осуществляется загрузка и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (MetaStealer).

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

Заблокировать возможность получения электронных писем с адресов oqnap@ingehim[.]ru и lazunina@b-technology[.]ru.

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

87[.]120[.]120[.]86; hxxp[:]//87[.]120[.]120[.]86[:]1912/.

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

c4a993a439395763eaa84f6f2cdcd20c2b8d3a9bafe795ce1874f7d510d34293;
cbffa6a62ef883d9379f5da7bd8c3d4b0fe95c40db2a8a85d5af9c9fb8a04d7f;
bcd51ae21d90b326dfc29c3b7f5e7d16144683ce2916f83a0597119291e2d88c;
2d38fac7d02a4d32b8579c25ec1ce2d6bb14bc27d846874ad6f1897ca21889cd;
425dd1eb40b5c657dd605c672d62d6bc413e79985aee2719a39a4e48c49ac7af;
15ccd076972fcd606c2f0dbc12357ed7bbc40793aaa8080afeb2666a74c4449f.

3. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержатся вредоносные исполняемые файлы с наименованиями «Мои контакты в морпехе.doc» и «Контакты в морпехе.doc», замаскированные под легитимные документы. После запуска пользователем указанных файлов осуществляется загрузка и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (NjRat).

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:

4[.]tcp[.]eu[.]ngrok[.]io; hxxp[:]//4[.]tcp[.]eu[.]ngrok[.]io[:]13267.

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

f5b2d5cdeef399f6c963dce42c1be443343d8a24fb93ded8149c519097e1f9d7;
2478f66866bf5cd2ea5c5714d01220addc336e1b6fec6867362b0f866e76c739;
c01c307e77ad6133b04b21d46905c277cf64d4e3a9c138375d60645075ad1981;
6bdb8f7a7ae0f20fc4888a48e9bbd9471dbfb795ea43066f09919b6adc17e779;
85e360dd772da192ac56b18d2a6f04ea6c01fd4064c6c7ba9efb334c705cba2a;
77c9d51ff369b73922696c4a1a32fd54758b2b634ceb2419100c764b283887e0.

4. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Запрос цены». Во вложениях указанных писем содержится вредоносный архив с наименованием «Список запросов - NTLDT 000009142188.pdf (82KB).lzh». Архив содержит исполняемый файл с наименованием «Список запросов - NTLDT 000009142188.pdf (82KB).com». После запуска указанного исполняемого файла осуществляется загрузка и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (QuasarRAT).

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:

wqo9[.]firewall-gateway[.]de;
rency[.]ydns[.]eu;
hxxp[:]//rency[.]ydns[.]eu[:]5287;
hxxp[:]//wqo9[.]firewall-gateway[.]de[:]8841.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
27a8774ed1c127b540cbac62ceb139096fc7162962a57c02798341268cb78d11;
3970b6a03ba24a7f6062bb6695b49e272d049fae120107d121c569d839bdecf1;
173a6408366a409c2c77e43eaac1bbb0e43c51e8e70b7af0c3b0edcf98e0291e;
5182c93d80ab847541599124d388613c23bfb193b7879f5395b421bba5c568f6;
5fbc9dfb2e50425e3bac71421f660a66ca7a2e538798e7631eacfca44918c3c4;
9c9974c0ebbfa38c978b834f205e255775c51e28fbb4ff4bd61eb98db08a7df9.

5. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный исполняемый файл с наименованием «отчет по СТП 12 (Декабрь).pdf.exe», замаскированный под финансовый документ. После запуска указанного файла осуществляется загрузка и внедрение вредоносного программного обеспечения типа «стилер» (Meduza).

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:

93[.]123[.]85[.]46;

hxxp[:]//93[.]123[.]85[.]46[:]15666;

hxxp[:]//93[.]123[.]85[.]46[:]80.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикатора компрометации (sha256) 4eab1725873c1475060db3de60742052145a86997d34088fc6ab5b9089b71701.

6. Хакерской группировкой Head Mare (Rainbow Hyena), нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный архив с наименованием «Doc.zip». Внутри указанного архива содержатся документ-приманка с наименованием «Контактные данные для оплаты.pdf» и вредоносные файлы с наименованиями «Список товаров и услуг.pdf.lnk» и «Счет-фактура.pdf.lnk». После запуска пользователем указанных вредоносных файлов осуществляется загрузка и внедрение вредоносного программного обеспечения типа «бэкдор» (PhantomCore).

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[:]//city-tuning[.]ru/collection/srvhost[.]exe;	hxxps[:]//filetransfer[.]io/data-package/AiveGg6u/download;
hxxp[:]//45[.]10[.]247[.]152/init;	hxxp[:]//45[.]10[.]247[.]152/check;
hxxp[:]//45[.]10[.]247[.]152/connect;	hxxp[:]//45[.]10[.]247[.]152/command;
hxxp[:]//185[.]80[.]91[.]84/command;	hxxp[:]//185[.]80[.]91[.]84/connect;
hxxp[:]//185[.]80[.]91[.]84/check;	hxxp[:]//185[.]80[.]91[.]84/init;
hxxp[:]//45[.]87[.]245[.]53/init;	hxxp[:]//45[.]87[.]245[.]53/check;
hxxp[:]//45[.]87[.]245[.]53/connect;	hxxp[:]//45[.]87[.]245[.]53/command.

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

6ac2d57d066ef791b906c3b4c6b5e5c54081d6657af459115eb6abb1a9d1085d;

0f578e437f5c09fb81059f4b5e6ee0b93cfc0cdf8b31a29abc8396b6137d10c3;

dd49fd0e614ac3f6f89bae7b7a6aa9cdab3b338d2a8d11a11a774ecc9d287d6f;
57848d222cfbf05309d7684123128f9a2bffd173f48aa3217590f79612f4c773;
4b62da75898d1f685b675e7cbaec24472eb7162474d2fd66f3678fb86322ef0a;
44b1f97e1bbdd56afeb1efd477aa4e0ecaa79645032e44c7783f997f377d749f;
2dccb526de9a17a07e39bdedc54fbd66288277f05fb45c7cba56f88df00e86a7;
1a2d1654d8ff10f200c47015d96d2fcb1d4d40ee027beb55bb46199c11b810cc;
8aad7f80f0120d1455320489ff1f807222c02c8703bd46250dd7c3868164ab70;
9df6afb2afbd903289f3b4794be4768214c223a3024a90f954ae6d2bb093bea3.

7. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица Министерства промышленности и торговли Российской Федерации. Во вложениях указанных писем содержится вредоносный исполняемый файл с наименованием «Письмо в МНТЦ и ЦРП_(файл отображения)», после запуска которого осуществляется демонстрация документа-приманки, загрузка и внедрение легитимного программного обеспечения «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):
dca379399328aa76daa9afe1109eb393e1353e83f756811b26d6508ef23a34fd;
6d0ee86f30393751eea9df49c307f9c91f4b0b72862a9f09ff9a6b5f91441e8a.

8. Хакерской группировкой Cloud Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица организаций, ведущих деятельность в сфере связи и информационных технологий. Во вложениях указанных писем содержится вредоносный файл, замаскированный под официальный документ. После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение вредоносного программного обеспечения типа «бэкдор» (PowerShower) в целевую систему.

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5. Обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

mehafon[.]com;
mirconnect[.]info;
jhsdshdkajdhgfyhsfhjshh[.]cfd;

web-whatapp[.]net;
79[.]143[.]87[.]233;
188[.]127[.]235[.]216;
185[.]99[.]2[.]168;
176[.]124[.]33[.]86;
80[.]85[.]153[.]195;
hxxps[:]//officeconfirm[.]technoguides[.]org/icm-string-studio-in-recital/;
hxxps[:]//officeconfirm[.]technoguides[.]org/icm-string-studio-in-recital/asecretory;
hxxp[:]//officeconfirm[.]technoguides[.]org/icm-string-studio-in-recital/;
hxxps[:]//officeconfirm[.]technoguides[.]org/pl/;
hxxps[:]//officeconfirm[.]technoguides[.]org/pl/5-glutamina/;
hxxps[:]//officeconfirm[.]technoguides[.]org/pl/5-glutamina/pluricarinate.

Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
e09f90563be00fc947a80bb1902a1b05c9e9aa8c86d01a34204717d68eb1684f;
c985309140500090ad457c4e380b461b7548cf837ddd45415edd4653e2ef50b2;
e91df17051b16bde97e7dec66a67025d2905612cc0bc5e3bc6b93493edf43d70;
9e838d7ad444130873a8c171d204283eb23ce9c2c5e3eb9d604848ef4401d71d;
89d56295bc8571334aa6916587d3ca6be01934b97f5fdf1cf895d1beda1d73bf;
650409dc7ba6e4565e7ba598d9a21fa422cdc0404ab188d368faced929d634cf;
8521d257295396a487dc0d7ccbeed25c05dcc12944e7f1addb06b57412676bf6;
bf6cfd89f09e0a28ec76ba1e2610c7fed149c4b94fa59f0a5a07f989fc7faa91;
27f77e73e1b1ce12b098362019266f5acb64f4bc34752ca0e3a16229880d300d;
b52233e2f3e885928834aaf1a8df86ec8e741fba2de5fedb31d1ed86768aeb4b;
b8f06954357e6ad1524d13d3c9ee6b495bcd7e3b04acac8694d2f2408c201278;
11b3ca9969c8eb06b28048972706863606ddf73b408df26fd1e226c2ad9f9fdf.

9. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляется распространение вредоносного программного обеспечения типа «руткит» (PUMAKIT). Указанное вредоносное программное обеспечение предназначено для систем, функционирующих под управлением операционных систем Linux, и позволяет злоумышленникам повысить свои привилегии для получения несанкционированного доступа к целевой системе.

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

sec[.]opsecurity1[.]art;
rhel[.]opsecurity1[.]art;
89[.]23[.]113[.]204.

Необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
30b26707d5fb407ef39ebee37ded7edeea2890fb5ec1ebfa09a3b3edfc80db1f;
cb070cc9223445113c3217f05ef85a930f626d3feaaea54d8585aaed3c2b3cfe;
934955f0411538eebb24694982f546907f3c6df8534d6019b7ff165c4d104136;
8ef63f9333104ab293eef5f34701669322f1c07c0e44973d688be39c94986e27;
8ad422f5f3d0409747ab1ac6a0919b1fa8d83c3da43564a685ae4044d0a0ea03;
bbf0fd636195d51fb5f21596d406b92f9e3d05cd85f7cd663221d7d3da8af804;
bc9193c2a8ee47801f5f44beae51ab37a652fda02cd32d01f8e88bb793172491;
1aab475fb8ad4a7f94a7aa2b17c769d6ae04b977d984c4e842a61fb12ea99f58.

Кроме того, в целях обнаружения вредоносной активности провести сканирование с использованием сертифицированных антивирусных средств защиты.

10. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляется распространение вредоносного программного обеспечения типа «бэкдор» (PowerStalin). После запуска указанного вредоносного программного обеспечения происходит выполнение команд оболочки сценариев «PowerShell» для получения злоумышленниками несанкционированного доступа к целевой системе.

Для предотвращения реализации угроз безопасности информации, связанных с указанной деятельностью хакерских группировок, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

b86d4dcce63e118c328f32ece114fb0afa5b5517f18541bea47c390adb4dc828;
1c0e40e79017dcc7e576451ceffa70a7ef2cf654a4cf411b2a450a0f2ac95be8;
4c36999ff4e8f813f490967dfc500ac449a11752c8890d29d26d6165d1fecc9c.

11. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляется распространение вредоносного программного обеспечения типа «стилер» (Lumma Stealer) и его координация с использованием инфраструктуры управления (LummaC2).

Для предотвращения реализации угроз безопасности информации, связанных с указанной деятельностью хакерских группировок, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресам, указанным в приложении, 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.

12. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный файл, замаскированный под официальный документ. После запуска указанного файла осуществляется загрузка и внедрение вредоносного программного обеспечения типа «кейлоггер» (Nova), которое является усовершенствованным вариантом «кейлоггера» Snake Keylogger, упоминавшимся ранее в бюллетенях.

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 следующему адресу, используя схему доступа по «черным» или «белым» спискам:

hxxps[:]//api[.]telegram[.]org/bot7479124552[:]AAELHYVLYxHEQdxzK-H17KRix-YKXifzKCI/sendDocument.

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

afb1dae7a6f2396c3d136e60144b02dd03c59ab10704918185d12ef8c6d7ec93;
66dbb9c8deadea9f848b1b55405738d8a65a733c804f1444533607c20584643e.

13. Хакерской группировкой Stone Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный файл, замаскированный под документ с наименованием «Scan_Kartochka_A-Automation.pdf». После запуска пользователем указанного вредоносного файла осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типа «бэкдор» (BrockenDoor).

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

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

193[.]124[.]33[.]184;

hxxp[:]//193[.]124[.]33[.]184[:]443/x.

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

внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
6d903f8b7abb2c19d972b9b5bb6543b247ea811889cf2d8c1ff16dd0685248e4;
f970c663143eb0e4a29a90e56fa800528ffcd5f6b97e3eef2a04a9cd1f835ddf;
cf5d1120ab7e7db31ac4432b5c9a91083df7881b91faa47950db4430e97cd2f0;
bec4938eee3664c66a5b1e05f8398c439360fb66d1f72b4c5a7cd2633d8cef3e.

14. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный файл с наименованием «2024.06.13. № МИР-53-24. Генеральному директору. 27 школа. По списку ОПК.pdf». После запуска указанного файла осуществляется демонстрация документа-приманки, загрузка и внедрение легитимного программного обеспечения для удаленного управления системой «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 индикатора компрометации (sha256) 773d9c788c11d6181d5fda031cde49dafb6441c8a9bef43fd670c56eeaaa08aa.

15. Хакерской группировкой Sticky Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица МВД России. Во вложениях указанных писем содержится документ-приманка с наименованием «Запрос провайдер.docx» и вредоносный архив с наименованием «Список IP адресов, дата и время захода в интернет.pdf.rar». Внутри указанного архива содержится исполняемый файл с расширением «.exe», после запуска пользователем которого осуществляется демонстрация документа-приманки и выполнение команд оболочки сценариев «PowerShell», загружающих и внедряющих в целевую систему вредоносное программное обеспечение типа «троян удаленного доступа» (Ozone RAT).

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

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

45[.]155[.]249[.]126;
84[.]22[.]195[.]72;
hxxps[:]//bitbucket[.]org/fgdfgre/fwqfqw/downloads/kfmFhra[.]txt;

hxxps[:]//bitbucket[.]org/adssgfdsg/testing/downloads/img_test[.]jpg?144417.

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

3e08efa825c583d91eae43da6b8a599b1a9238ff47a184a94946a982c5d724f3;
f50a9ddf3d452687b10734c96aac362ad4ddeaf3fa52408628b59a87d9b67850;
9318e4d6a93e0a9b3f4d9d6311eab3d24be30ea9f1c968c4c0d4d966d3f8a390;
f6108824b1fe0c2f1483611db89ed968a3f339475ffd20eeda87e978c796e955;
3eca76737c6aee34b4c38845fde13bceed23a31d39e958893a44f42380ff84d5;
5bfd261ad68a4c0ac564ebc787598d98403481e709ea80a824097ea7c0b430f7;
1fb6670d1f96d83c02eb08fdd3a5683d302513cf3982878a92a12acd63540f30;
6851c7a0db960f5c3d81cb20b261256377f819a24897a1f8e55282cbd0a5499b;
6a45a3330843c11ce549c55b393fdc28cc0072b24cc74f322f5932291094db16.

16. Хакерской группировкой Sticky Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица Министерства промышленности и торговли Российской Федерации. Во вложениях указанных писем содержится вредоносный исполняемый файл с наименованием «Долговая нагрузка.exe», замаскированный под легитимный документ. После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (QuasarRAT).

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:

crostech[.]ru;

5[.]8[.]11[.]91;

hxxp[:]//5[.]8[.]11[.]91[:]4782.

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

258976daa25d6ca2675764e995d4ca48ccf262a7cb9520cccc5c4c4c698ff163;
d444ec105e426dba19db51164d2912b33b8f7c0ff5cb6c6f6318331505dec7d5;
54d0fd3d916875c85327066b22bb0dcfb86fa77e0971cf5db2b701eba1a9ec32.

17. Хакерской группировкой Rainbow Hyena, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые

рассылки электронных писем, во вложениях которых содержится вредоносный архив с наименованием «Doc.zip». Внутри указанного архива содержатся файлы, замаскированные под финансовые и юридические документы, после запуска пользователем которых осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типа «загрузчик» (PhantomDL).

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[.]87[.]246[.]157;
hxxp[:]//45[.]87[.]246[.]157/command;
hxxp[:]//45[.]87[.]246[.]157/check;
hxxp[:]//45[.]87[.]246[.]157/init;
hxxp[:]//45[.]87[.]246[.]157/connect.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
0f578e437f5c09fb81059f4b5e6ee0b93cfc0cdf8b31a29abc8396b6137d10c3;
46ba5110a447746cf7fe2c2d62c0c20fb7cdf66930f630c8dfb8eac97fbb5bf1;
6ac2d57d066ef791b906c3b4c6b5e5c54081d6657af459115eb6abb1a9d1085d;
a728fa92ed923cd65833228664a7e8402f0bbbb29942da70f87cc7cf1ac9c71a;
6ad06573fff4fcc7cd16c2ac3e1c4635b567a89b2d6c07cf98930133d3f90683;
dd49fd0e614ac3f6f89bae7b7a6aa9cdab3b338d2a8d11a11a774ecc9d287d6f;
25a308fd1d37d7af4bd0c47aa5368228ddd3e1dd682c030a9e3c958d32c15c0d;
70a3a64911c9ddc01562d1b39a359e5800ac9a59b7d9e94d1a54d5ca12809b09.

18. Хакерской группировкой Cloud Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится замаскированный под официальный документ вредоносный файл. После запуска указанного файла осуществляется эксплуатация уязвимости редактора математических формул и уравнений текстового редактора Microsoft Word, пакета программ Microsoft Office и пакета обеспечения совместимости Microsoft Office Compatibility Pack (BDU:2018-00246, уровень опасности по CVSS 3.0 – высокий), а также внедрение вредоносного программного обеспечения типа «бэкдор» (VBShower, VBCloud, PowerShower).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5. Обеспечить на уровне сетевых средств защиты информации ограничение

обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам, указанных в приложении к настоящему письму.

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

Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации, указанных в приложении к настоящему письму.

19. Хакерской группировкой Cyber Anarchy Squad, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются атаки на сетевые ресурсы через эксплуатацию уязвимых сервисов (например, Jira, Confluence и Microsoft SQL), доступных из сети «Интернет». Для закрепления в целевых системах злоумышленники внедряют вредоносное программное обеспечение типа «троян удаленного доступа» (Revenge RAT и Spark RAT).

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:

194[.]36[.]188[.]94; 185[.]117[.]75[.]3.

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

fc3a8eabd07a221b478a4ddd77ddce43;
48210ca2408dc76815ad1b7c01c1a21a;
8c70377554b291d4a231cf113398c00d;
23b873bb66dc09e91127e20825b6cbc7;
bcec17275114c6a87d8b7110aecec5cc;
6cbc93b041165d59ea5ded0c5f377171;
1fcd4f83bf6414d79d5f29ad1e795b3d.

20. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются атаки путем эксплуатации уязвимости сервера для управления программами Fortinet FortiClient Enterprise Management Server (EMS), связанная с непринятием мер по защите структуры запроса SQL (BDU:2024-02008, уровень опасности по CVSS 3.0 – критический). После получения доступа к инфраструктуре злоумышленники осуществляют установку легитимного программного обеспечения для удаленного доступа (например, AnyDesk, ScreenConnect).

Для предотвращения реализации угроз безопасности информации, связанных с указанной деятельностью хакерских группировок, необходимо обеспечить на уровне сетевых средств защиты информации ограничение

обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам, указанных в приложении к настоящему письму.

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

746710470586076bb0757e0b3875de9c90202be2;
bc29888042d03fe0ffb57fc116585e992a4fdb9b;
73f8e5c17b49b9f2703fed59cc2be77239e904f7;
841fff3a36d82c14b044da26967eb2a8f61175a8;
cf1ca6c7f818e72454c923fea7824a8f6930cb08;
e3b6ea8c46fa831cec6f235a5cf48b38a4ae8d69;
75ebd5bab5e2707d4533579a34d983b65af5ec7f;
44b83dd83d189f19e54700a288035be8aa7c8672;
8834f7ab3d4aa5fb14d851c7790e1a6812ea4ca8.

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

21. Хакерской группировкой Masque, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются атаки на публично доступные сервисы через эксплуатацию уязвимости компонента JNDI библиотеки журналирования Java-программ Apache Log4j2 (BDU:2021-05969, уровень опасности по CVSS 3.0 – критический). Злоумышленники устанавливают легитимное программное обеспечение для удаленного доступа (AnyDesk), загружают и внедряют вредоносное программное обеспечение типов «загрузчик» (MystiqueLoader) и «шифровальщик» (LockBit 3 и Babuk).

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

consultant-info[.]ru;
local-system[.]online;
infobuhgalter[.]ru;
b-buhgalteria[.]ru;
ms-update-cdn[.]info;
45[.]151[.]62[.]110;
62[.]60[.]187[.]254;
89[.]23[.]113[.]172;
193[.]233[.]48[.]31;
212[.]192[.]14[.]54.

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

компрометации (sha256):
7aecb02611f5f6ba2f180cc86df7c8e9636d7eb34b9256a69e799ba341899208;
b63d536dfeb6a869aed0f174e0299eee07e61acdc63a6e5ded3b694ffba89f68;
d474a9030cd04002de1dd676d44e6962bc5c3d54a72d4c305d87174495972a58;
d7d15d9de93438bba8ea79ebe54f03d5594f338cf9be2e122f2ba0456746fdf8;
44797383aa1969cee3fd09f0e53ed50ac6c7afbb83bbac1b825e41d1ba0bb544;
da2191203b39fda0823520a85a9ca0bb8c42c4ef5b341a929d69dfd99e971d7d;
3bfdacd5ecf70c53beeaefbd85c90eaceca5ca4787a8b61407e4bcb6ee3aef1a;
ff282c788a380bb68de2e8c9d8d2e1a7dd3b07d49fd4a965e279bbf4dd965b88;
8eddc062b68f0511dc2b28908630ae2381cfd66b78a9270f5d8e1729b30ca3b2;
763b65a4c7cf55aba8913378892cb0716585f502bc2695e839b493a46c372b5e;
996e68f2fe1c8bb091f34e9bf39fd34d95c3e21508def1f54098a1874bfb825e;
d8090f5058db31956d0503d0e4c9e16504d58623ba481715609a8ff1303d6e72;
9491075bdb1bca34dab092a357914b6e14a825c37c268327e1f67a7a602308ab;
92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50.

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

22. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица «ООО Master Steel» с тематикой «емкости и автоматика». Во вложениях указанных писем содержится вредоносный архив с наименованием «Add_05.12.2024.rar». Архив содержит файл, после запуска пользователем которого осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типа «стилер» (MetaStealer).

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

Кроме того, необходимо заблокировать получение электронных писем с адреса component@smetal[.]ru и обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

87[.]120[.]120[.]86;

hxxp[:]//87[.]120[.]120[.]86[:]1912/.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикатора компрометации (sha256) c0af8dd2f78b56279e52ebccbce086e0c9821678fb00659e6ad6abff923aa7dc.

23. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится

вредоносный архив с наименованием «Aviasales Partnership.rar». Архив содержит исполняемый файл, после запуска пользователем которого осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типа «стилер» (Rhadamanthys).

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:

45[.]150[.]32[.]106;

hxxps[:]//45[.]150[.]32[.]106[:]8680/eba20e054a2b3/enbpm0ob[.]o3duh.

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

8da3d3e5861c700155466ff4cc8fc6be38113c94186c5302ad6894691c55cd4d;
38c8f07e4f2e8a662ca9a2910af1b9cd8875056589f95c9338116c72bc795159.

24. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный исполняемый файл. После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки «Приказ о допуске к государственной тайне», загрузка и внедрение в целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (DCRat).

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:

cj46586[.]tw1[.]ru;

hxxp[:]//cj46586[.]tw1[.]ru/L1nc0In[.]php.

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

16ef9df3533d911bc0d414251e9def3c8d1335de3c31fea4e3b8fccf9599600c;
02d7945313b059e6aa528c66647c59141ca62ca8ac52a8c3a960f5dc328be666;
28dffaabf6f685cdbad4b814ebd280006919f8311f2ffb2b6a153799eeb315bb;
e4861621bd49b3ff92b6094ceae288f4d52ff70aa60d730e790f010bace17bba.

25. Хакерской группировкой Watch Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица оператора логистики «PonyExpress» с тематикой «Уведомление об окончании срока бесплатного хранения». Во вложениях указанных писем содержится вредоносный архив с наименованием «Накладная №*.zip», внутри которого находится исполняемый файл с наименованием «Накладная №*.exe». После запуска пользователем указанного исполняемого файла осуществляется выполнение вредоносного скрипта «JavaScript», загрузка и внедрение вредоносного программного обеспечения типа «бэкдор» (DarkWatchman).

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

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

ponyexpress[.]website;
bd0baba4[.]store;
bd0baba4[.]online;
bd0baba4[.]site;
hxxps[:]//bd0baba4[.]store/index[.]php_CURRENT_USER;
hxxp[:]//bd0baba4[.]store/index[.]php;
hxxps[:]//bd0baba4[.]store/index[.]php/.

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

8f0796dc1847c8e1cf00c505c5ff855942b1d182e356e4733b4be480a5569ac3;
f5f7f1bbc71fb6da221049d1fc7a31d1312b07da46accdcd76588e989488297b;
5654faf2d7d2bf6e8fcca0ff5bf12d10c284503632cbc964466cc810ded31571;
43c2da7c3c85c7658701c01e2fe8bda40c8efd701f0f89c2681313b15b206b20;
f81f5880ff69a0030b8578bd38e4c6350f95ae1c506e9372a2c57461a9bb375f;
947d88de855c44d6a04c26a4fca45f67d54fc1bbd3f3bb76e3de6c7103fc4651;
c16a7751df8b8c3af4b8aa769816cfc7ecfa378d42ce238c3d7616f36f46dd28;
1be2db951e3df606fa9717fbc179652d76c7bd67393426af73b369ad3a490a93;
21b0e575c3366e4958296b9c2f1e05ace038f3f4c653fb7c5bc5ab816e5c609c;
ae63a886c36cf4b9bb53837595b2b5c9fe0b52e78edc6c6569d41ce0f1a047c6;
889f6feb0f804a391fc75482d0e5a18ff67a52d655ced8078862a347a1947517;
d1348d73eafbcd78a584ce7c57542331061bbd44d2b425644e92d01368ad6862;
71c03b36162312b61f7f531c295fe23fe3a52539a59a26c3f3f2d351c2ad2b95;
407afe8f6e6cb696c72209aa952e4f415514196d7605c305517118743ad1ae27;
33d5ca7ec51b5f3a16e9bcc0b16db7c22fffc5afb1d03b68a83ae54455210de2;
3f99c6b90b7488d59d17adcd1b6fde61752ab3709533f34a5d9eaafcb0fe412e;

889f6feb0f804a391fc75482d0e5a18ff67a52d655ced8078862a347a1947517.

26. Хакерской группировкой Core Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица Минобороны России. Во вложениях указанных писем содержится вредоносный исполняемый файл с наименованием «Выписка из осведомленности ВСУ о состоянии и положении объектов ВС РФ по состоянию на 20.12.2024 г.». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и выполнение вредоносного VBS-скрипта, который загружает и внедряет легитимное программное обеспечение 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:

ipcor[.]ru;

hxxp[:]//ipcor[.]ru[:]443.

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

7d05951fb05b770d14b42637fd15770d70749ec1968e0628dc078b17e2dde679;

55849509dd7199426381dc425de04f2676ae2e4acb60ed37fe543555a22bbf9d;

57cb78d44501b417b8e95e6d31b46e9b4dd19456c3c3163f1e0537c93562edef;

bbf4965798aed26726a4dc9bb4c0aeaba8ebb1764627cc8ce68839396112a972.

27. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный архив с наименованием «загрузка.zip». Внутри указанного архива содержится вредоносный файл с расширением «.doc». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (Cryp RAT).

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):
1ce80b2bb2a5f56573ca786f662accea56f4b9e0e3052ddec14fe03364c14dfe;
ead58c483c8208cd57464f8a49290795390634f4698213054bf7370227c026dc;
2a0aa0763fdef9c38c5dd4d50703f0c7e27f4903c139804ec75e55f8388139ae;
e17cd94cd8fc0e001a49f43a0801cea4625fb9aee211b6dfebebec446c21f460;
593e60cc30ae0789448547195af77f550387f6648045847ea244dd0dd7abf03d;
f6c55900318781681edf34838e74b6bf3a7106ca34881d7f5c63b8e0d7ac3694;
f00b21185f93e23409e9383930c7999094983671b1c1e0dc00208bb1c8f1e10d;
44887df9f68f5a3084c7d80c1c7492ca5209e816a4e83fdbd6e2fcb6f1ff936f;
f6c559c031b7b16b1edf34b38e74b6bf3a7106ca34881d7f5c63b8e0d7ac36944;
027d0f9d3b924d76cfa043e7b0b51facb401f2b8bceb1e9778d8bbe87cdc8717;
070b710671c05da85d005cfb16a924bae030c74bf1ed3fdd0b649befde2baa1a;
0081b7bc078c1e2dd6413cdb47a0e02dbd4e3d3c647a14c6dfc48d137647cdd3b;
097bf0f5b07c4834e4c65be0ad645362ce641e8cb72dfb46711ca254da70511d;
oc5bef12a9a37a8166d1cf10150b7bd4668bcd706221d08b1d11297761e09956.

28. Хакерской группировкой Paper Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный файл, замаскированный под легитимный документ. После запуска указанного файла осуществляется демонстрация зашифрованного документа Microsoft Word. Пользователю предлагается подтвердить выполнение процедуры расшифровки, в таком случае будет осуществлены команды оболочки сценариев «PowerShell» для загрузки и внедрения вредоносного программного обеспечения типа «троян удаленного доступа» (PowerRAT).

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:

lobbyluxuries[.]com;
94[.]103[.]85[.]47;
185[.]244[.]182[.]87;
5[.]252[.]176[.]55;
85[.]198[.]110[.]216.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
fa8853aaa156485855b77a16a2f613d9f58d82ef63505be8b19563827089bf52;
13252199b18d5257a60f57de95d8c6be7d7973df7f957bca8c2f31e15fcc947b;
8ba4cd7ea29f990cb86291003f82239bfafe28910d080b5b7d3db78e83c1b6f3;

37b3fa8a3a05e4aedb25eb38d9e4524722f28c21fac9f788f87113c5b9184ef5;
804cd68f40d0bb93b6676447af719388e95cafd5a2b017a0386eb7de590ebf17.

29. Хакерской группировкой Lazarus Group, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица, выдающего себя за представителя отдела кадров сторонней организации. Во вложениях указанных писем содержатся исполняемые файлы с расширением «.exe» и файлы-приманки с расширением «.txt». После запуска указанных исполняемых файлов осуществляется открытие окна, в котором пользователю предлагается ввести свой IP-адрес. После ввода IP-адреса в систему осуществляется загрузка и внедрение вредоносного программного обеспечения типа «загрузчик» и легитимного программного обеспечения для удаленного доступа «UltraVNC».

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

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

c6323a40d1aa5b7fe95951609fb2b524;
cf8c0999c148d764667b1a269c28bdcb;
37973e29576db8a438250a156977ccdf;
d966af7764dfeb8bf2a0feea503be0fd;
778942b891c4e2f3866c6a3c09bf74f4;
1315027e1c536d488fe63ea0a528b52d;
b0e795853b655682483105e353b9cd54;
e0dd4afb965771f8347549fd93423985;
739875852198ecf4d734d41ef1576774;
bf5a3505273391c5380b3ab545e400eb;
0ee8246de53c20a424fb08096922db08;
80ab98c10c23b7281a2bf1489fc98c0d;
4c4abe85a1c68ba8385d2cb928ac5646;
e6a1977ecce2ced5a471baa52492d9f3;
fdc5505d7277e0bf7b299957eadfd931;
2b2cbc8de3bdefcd7054f56b70ef58b4;
57453d6d918235adb66b896e5ab252b6;
00a2952a279f9c84ae71367d5b8990c1;
5eac943e23429a77d9766078e760fc0b.

Приложение

Перечни идентификаторов компрометации

II раздел, пункт № 11.

Перечень индикаторов компрометации инфраструктуры управления LummaC2	
Сетевые индикаторы компрометации	
hxxps[:]//intelinsights[.]substack[.]com/p/a-multi-actor-infrastructure-investigation	
154[.]216[.]20[.]204	193[.]124[.]205[.]63
61[.]149[.]4[.]214	198[.]251[.]84[.]107
172[.]67[.]75[.]172	43[.]143[.]130[.]50
192[.]169[.]69[.]26	58[.]56[.]172[.]234
192[.]169[.]69[.]28	60[.]222[.]237[.]158
208[.]95[.]112[.]1	61[.]157[.]153[.]24
45[.]125[.]247[.]123	101[.]207[.]142[.]35
129[.]6[.]15[.]28	112[.]216[.]232[.]82
239[.]255[.]255[.]250	113[.]240[.]239[.]242
81[.]19[.]131[.]103	115[.]239[.]173[.]226
83[.]217[.]208[.]134	117[.]141[.]0[.]134
107[.]189[.]28[.]160	118[.]112[.]188[.]39
154[.]216[.]17[.]46	123[.]52[.]136[.]150
154[.]216[.]17[.]167	123[.]135[.]104[.]58
154[.]216[.]20[.]89	183[.]215[.]11[.]163
154[.]216[.]20[.]133	183[.]230[.]82[.]22
154[.]216[.]20[.]204	183[.]237[.]57[.]250
154[.]216[.]20[.]224	191[.]97[.]7[.]106
162[.]254[.]34[.]46	218[.]59[.]172[.]213
185[.]196[.]8[.]56	218[.]66[.]5[.]17
185[.]196[.]8[.]68	222[.]87[.]204[.]236
185[.]196[.]8[.]76	222[.]249[.]226[.]134
185[.]196[.]10[.]135	223[.]95[.]119[.]193
185[.]196[.]11[.]18	
Файловые индикаторы компрометации (sha256)	
34a265197110995c087e43edde1d1425b1c4c809443491b480cdef4d89a1d302	
39a2a0e55cd35c5f61c80e3de3335e529778f9602a3aa281d08e38df8df4071c	
3cb18e4d9f70b897cf1bba44ceb965522b31da34ace530d8a1fb9f481a9cae3d	
642a7f341146d4b2a5381186ec636a8e0ce7ccc16bb730be331e51d6e65f4db3	

68d54b631ec36072fe2a833a0a4aa6c131b7f464383cab338a83aff7827ccc06
7d3ff6ad74c57a4df53ada02881d2da8243ba098c6b65bddefd405829729b40b
81e362d1aae7ca2398219edc502323062fbd06845a42a044668ac808362d58e6
9adfca702feeb585a9bb2e370cb27746a9f7bcecce8c4f182cffc411b829226f
c041e7547fc7f9dbbcde766a199fb6226309c60f76795ddfe46da698664f9311
e53e552a44c7746c9b2916b83d5d9c7d5f0f19305b313bde698841509efccdff
ea2db0b533eacf73d3b23f4da806e87be41925251a69108d9eb699b895f4cf80
ef54db47ae752d795e0734e3ea73c4607490cec58e2570818b65681d94a35f4c
fae4297f765a1c93fef48d7bddd8c88e6361dcb7eb9efc7cb10ff050e2157d80
12ca4ad8cd613c8d086cd39a5c6e787c12209f2271ba850817b72eae3cd559da
0909cf95903c9f07651f4361b8e929c53a62162f6eaaeb11b0dd70eaef2c2784
083f0f217bff41523e9faa49bb13e9e5d691a3c51341b12d0c4829d8cfc33292
a9f22319f417a9c78eb4c96257c847f1c08e9381ad05ebc05889d8b140ebf5d2

II раздел, пункт № 18.

Индикаторы компрометации хакерской группировки Cloud Werewolf	
Сетевые индикаторы компрометации	
content-protect[.]net	yandesks[.]net
control-issue[.]net	yandisk[.]info
office-confirm[.]com	mirconnect[.]info
onesoftware[.]info	sber-cloud[.]info
serverop-parametrs[.]com	gosportal[.]net
web-privacy[.]net	riamir[.]net
net-plugin[.]org	yandesktop[.]com
triger-working[.]com	web-wathapp[.]com
Файловые индикаторы компрометации (MD5)	
9d3557cc5c444fe5d73e4c7fe1872414	242e86e658fe6ab6e4c81b68162b3001
cba05e11cb9d1d71f0fa70ecd1af2480	2fe7e75bc599b1c68b87cf2a3e7aa51f
cbfb691e95ee34a324f94ed1ff91bc23	36dd0fbd19899f0b23ade5a1de3c2fec
2d24044c0a5b9ebe4e01ded2bfc2b3a4	389f6e6fd9dcc84c6e944dc387087a56
88be01f8c4a9f335d33fa7c384ca4666	3a54acd967dd104522ba7d66f4d86544
a30319545fda9e2da0532746c09130eb	3f12bf4a8d82654861b5b5993c012bfa
15fd46ac775a30b1963281a037a771b1	49f8ed13a8a13799a34cc999b195bf16
31b01387ca60a1771349653a3c6ad8ca	4b96dc735b622a94d3c74c0be9858853
389bc3b9417d893f3324221141edea00	f45008bf1889a8655d32a0eb93b8acdd
aa8da99d5623fafed356a14e59acbb90	0139f32a523d453bc338a67ca45c224d
016b6a035b44c1ad10d070abcdfe2f66	01db58a1d0ec85adc13290a6290ad9d6
160a65e830eb97aae6e1305019213558	0f37e1298e4c82098dc9318c7e65f9d2
184cf8660af7538cd1cd2559a10b6622	6fcee9878216019c8dfa887075c5e68e
1af1f9434e4623b7046cf6360e0a520e	d445d443ace329fb244edc3e5146313b
1bfb9cba8aa23a401925d356b2f6e7ed	f3f28018fb5108b516d802a038f90bde
21585d5881cc11ed1f615fdb2d7acc11	

II раздел, пункт № 20.

Сетевые индикаторы компрометации, связанные с деятельность хакерских группировок пункта 20
45[.]141[.]84[.]45
185[.]216[.]70[.]170[:]1337
hxxps[:]//solarnyx2410150445[.]screenconnect[.]com/Bin/ScreenConnect[.]ClientSetup[.]exe?e=Access&y=Guest
hxxps[:]//allwebemails1[.]screenconnect[.]com/Bin/ScreenConnect[.]ClientSetup[.]exe?e=Access&y=Guest
hxxps[:]//webr6hl0n[.]screenconnect[.]com/Bin/ScreenConnect[.]ClientSetup[.]exe?e=Access&y=Guest
hxxp[:]//185[.]196[.]9[.]31[:]8080/bd7OZy3uMQL-YabI8FHeRw
HXXP[:]//148[.]251[.]53[.]222[:]14443/SETUP[.]MSI
HXXP[:]//185[.]216[.]70[.]170/OO[.]BAT
HXXP[:]//185[.]216[.]70[.]170/HELLO
HXXP[:]//185[.]216[.]70[.]170/A
hxxp[:]//185[.]216[.]70[.]170
hxxp[:]//185[.]216[.]70[.]170/oo[.]bat
hxxp[:]//185[.]216[.]70[.]170/hello
hxxp[:]//185[.]216[.]70[.]170/sos[.]txt
hxxp[:]//185[.]216[.]70[.]170/72[.]bat
hxxp[:]//206[.]206[.]77[.]33[:]8080/xeY_J7tYzjajqYj4MbtB0w
hxxp[:]//5[.]61[.]59[.]201[:]8080/FlNOfGPkOL4qc_gYuWeEYQ%TEMP%\gfLQPbNLYYYh[.]exe
hxxp[:]//5[.]61[.]59[.]201[:]8080/7k9XBvjahnQK09abSc8SpA%TEMP%\FaLNkAQGOe[.]exe
hxxp[:]//5[.]61[.]59[.]201[:]8080/7k9XBvjahnQK09abSc8SpA%TEMP%\QgCNsJRB[.]exe
hxxps[:]//www[.]lidahtoto2[.]com/assets/im[.]ps1
hxxp[:]//87[.]120[.]125[.]55[:]8080/BW_qY1OFZRv7iNiY_nOTFQ%TEMP%\EdgouRkWzLsK[.]exe