Приложение 1

**Деятельность хакерских группировок.**

1. Хакерской группировкой Rare Werewolf:

осуществляются фишинговые рассылки электронных писем с тематикой «FWD: RE: Добрый день. Отправляем вам договор, регулирующий производство и поставку продукции.». Во вложениях указанных писем прикреплен архив с наименованием «Платежный документ и приложение к контракту на поставку Исх. N 4691 - 21.rar», содержащий исполняемый файл с наименованием «Платежный документ и приложение к контракту на поставку Исх. N 4691 - 21.com». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для получения удаленного доступа «AnyDesk». Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

172[.]67[.]132[.]183;

goffice[.]digital; smtp[.]qqoffice[.]ru;

smtp[.]goffice[.]click;

www[.]qqoffice[.]ru;

mail[.]qqoffice[.]ru;

qqoffice[.]ru;

pop[.]goffice[.]click;

mail[.]goffice[.]click;

ftp[.]qqoffice[.]ru;

pop[.]qqoffice[.]ru.

2. Хакерской группировкой Vengeful Wolf:

осуществляются фишинговые рассылки электронных писем с тематикой «Акт сверки взаиморасчетов».Во вложениях указанных писем прикреплен архив с наименованием «Сверка.cab», содержащий документ-приманку с наименованием «Бланк.doc» и исполняемый файл с наименованием «Акт сверки взаимных расчетов предприятия № 397 от 16 июня 2026 года.scr». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-

приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (XWorm RAT).

3. Хакерской группировкой Clubfoot Wolf:

осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «Заявка АО ЮЕ КСР 61.zip», содержащий файлы-приманки с наименованиями «ИНН ОГРН Свидетельство о рег. в налог. Органе от 16.04.2019.pdf» и «Карточка организации АО ЮЕ КСР.doc», а также файл-ярлык с наименованием «Заявка на закупку от компании АО ЮЕ КСР на июнь 2026г.lnk». После запуска пользователем указанного файла-ярлыка осуществляется демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для получения удаленного доступа «Net Support». Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу fleepsterones[.]fun, используя схему доступа по «черным» или «белым» спискам.

4. Хакерской группировкой Core Werewolf:

при реализации целевых компьютерных атак осуществляется применение вредоносного программного обеспечения типа «бэкдор» (TokenBuoy, TokenBuoySH) и инструмента для обмена файлами между локальным компьютером и облачным хранилищем «rclone»

5. Хакерской группировкой Fluffy Wolf, осуществляются фишинговые рассылки электронных писем с тематикой «Акты сверок на 19.06.2026».В тексте указанных писем пользователю предлагается ознакомиться с документом, нажав кнопку «Скачать», после нажатия которой осуществляется загрузка архива с наименованием «document_buh.rar», содержащего файл с наименованием «document_1C_sverka_buh.bat». После запуска пользователем указанного файла осуществляется выполнение команд оболочки сценариев «PowerShell», демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типов «стилер» (PureLogs Stealer) и «троян удаленного доступа» (PureRAT). Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо обеспечить на уровне сетевых средств защиты

информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

5[.]230[.]201[.]201;

hxxps[:]//github[.]com/Nataly2696/;

hxxp[:]//66[.]63[.]170[.]33/img/1[.]jpg;

hxxp[:]//kickstrean[.]art/1[.]jpg.

6. Хакерской группировкой Eagle Werewolf, осуществляются фишинговые рассылки электронных писем с тематикой гуманитарной помощи от благотворительного фонда (например, «ЗаЩИТа», «Братское сердце», «Защитники Отечества»). Во вложениях указанных писем прикреплен файл с расширением «.exe» (например, «полный список бф 23.04.2026.exe»), после запуска пользователем которого осуществляется запуск программного обеспечения, замаскированного под онлайн-магазин «Военторг», и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Still Sync, Still Audio). Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

145[.]223[.]70[.]69, service8date[.]com,screenserv[.]com, 23[.]27[.]25[.]251
xyzserve[.]net , defendercloud[.]net, 23[.]27[.]124[.]133
windowserv[.]net, liteservice[.]net, 93[.]115[.]19[.]231
plantlabelstore[.]com, orderapiserver[.]info, 45[.]59[.]114[.]86
updatee-msf[.]comtg4service[.]com,23[.]26[.]237[.]70
configurationserv[.]com, srwinservice[.]com, 23[.]26[.]237[.]99
portalsupdates[.]com, winservsrv[.]com, 91[.]227[.]77[.]218
astracloud[.]cc, servrwindow[.]com, 104[.]194[.]134[.]27
whatsservice[.]site managementapiservice[.]com, 213[.]252[.]246[.]23
cloudanalitics[.]net, updateser[.]com, 51[.]15[.]110[.]186, apibroker[.]xyz
updateservs[.]com, 103[.]253[.]43[.]49, toolsserv[.]com, drivercloud[.]net
45[.]59[.]124[.]84, edgesnet[.]cc, newagebrain[.]net, 146[.]103[.]45[.]131
sync-rtk-api[.]com best4service[.]net, 2[.]59[.]218[.]195, driverupdate[.]store
srv5backupdb[.]org, 45[.]83[.]131[.]103, winservup[.]com, 5microservices[.]com
upd-link6[.]com, linkservice-backup[.]com.

7. Хакерской группировкой Fairy Wolf, осуществляются фишинговые рассылки электронных писем с тематикой «Исходящее 189». Во вложениях указанных писем прикреплен архив с наименованием «ИСХ 189_26 от 25.06.2026.zip», содержащий файл с наименованием «ИСХ 189_26от 25.06.2026.hta». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Unicorn Stealer).

8. Хакерской группировкой Vengeful Wolf, осуществляются фишинговые рассылки электронных писем с тематикой «Акт сверки взаиморасчетов». Во вложениях указанных писем прикреплен архив с наименованием «Документы.cab», содержащий документ-приманку с наименованием «Бланк.doc» и исполняемый файл с наименованием «Акт сверки взаимных расчетов предприятия № 427 от 24 июня 2026 года.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (XWorm RAT).

9. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации:

осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен файл-образ с наименованием «РОЗЫСКНОЕ_ДЕЛО_64-233-16_Скоропупов.iso». Внутри указанного файла-образа содержится файл с наименованием «a6.txt» и файлы-ярлыки с расширением «.lnk» (например, «Требование_о_предоставлении_информации.pdf.lnk»), после запуска пользователем которых осуществляется выполнение команд оболочки сценариев «PowerShell», демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «фреймворк постэксплуатации» (Mythic). Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступапо «черным» или «белым» спискам:

178[.]17[.]58[.]177;

twinky[.]vip;

hxxps[:]//twinky[.]vip/logs;

hxxps[:]//twinky[.]vip/doc;

hxxps[:]//twinky[.]vip/api/test;

hxxps[:]//twinky[.]vip/login;

hxxps[:]//twinky[.]vip/auth;

hxxps[:]//twinky[.]vip/visit/history;

hxxps[:]//twinky[.]vip/api/ujsmE;

hxxps[:]//twinky[.]vip/visit.

осуществляются фишинговые рассылки электронных писем с тематикой «Приказ на отпуск». Во вложениях указанных писем прикреплен архив с наименованием «25_ОТ_16.05.zip», содержащий файл с наименованием «ПРИКАЗ 25-ОТ 16.06.2026.lnk». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «стилер». Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к IP-адресу 81[.]90[.]31[.]87, используя схему доступа по «черным» или «белым» спискам.

осуществляются фишинговые рассылки электронных писем с тематикой «Contract_234_17_06_26». Во вложениях указанных писем прикреплен архив с наименованием «Contract_234_17_06_26.r13», содержащий исполняемый файл с наименованием «Contract_234_17_06_26.exe». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (XWorm RAT). Для предотвращения реализации угроз безопасности информации, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к IP-адресу 109[.]248[.]150[.]234, используя схему доступа по «черным» или «белым» спискам.

осуществляются фишинговые рассылки электронных писем с тематикой «8481687336». Во вложениях указанных писем прикреплен архив с наименованием «Уведомление 8481687336.7Z», содержащий образ виртуального жесткого диска с наименованием «Уведомление 8481687336.vhdx». Внутри образа содержится файл с наименованием «JS.js», после запуска пользователем которого осуществляется

внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Remcos RAT).

осуществляются фишинговые рассылки электронных писем с тематикой «8481687336». Во вложениях указанных писем прикреплен архив с наименованием «Уведомление 8481687336.7Z», содержащий образ виртуального жесткого диска с наименованием «Уведомление 8481687336.vhdx». Внутри образа содержится файл с наименованием «JS.js», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Remcos RAT). Для предотвращения реализации угроз безопасности информации, необходимо реализовать меры защиты,необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hxxps[:]//vestashop[.]ge/img_234155[.]png;

hxxps[:]//nickart[.]ro/wqaccess/optimized_MSI[.]png.

осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «OFFZONE_2026_Информация_и_гостевые_приглашения.zip», содержащий исполняемые файлы с наименованием «OFFZONE_2026_Гостевое_приглашение_для_представителей_компаний.exe» и «OFFZONE_2026_О_мероприятии_и_возможностях_для_компаний.exe». После запуска пользователем указанных файлов осуществляется демонстрация документа-приманки и внедрениена целевую систему программного обеспечения для получения удаленного доступа «OpenSSH». Для предотвращения реализации угроз безопасности информации необходимо реализовать меры защиты на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

46[.]17[.]40[.]11;

microservices[.]casacam[.]net;

hxxp[:]//46[.]17[.]40[.]11/root/OpenSSH[.]zip;

hxxp[:]//kazansky[.]camdvr[.]org/1-2026-06-22-9320045808[.]pdf;

hxxp[:]//kazansky[.]camdvr[.]org/2-2026-06-22-9320045808[.]pdf;

hxxp[:]//kazansky[.]camdvr[.]org/1-2026-05-22-7552205386[.]pdf;

hxxp[:]//productiondetails[.]webredirect[.]org/2-2025-07-01-94393hf934h[.]pdf.

осуществляются фишинговые рассылки электронных писем с тематикой «Учетная запись готова к деактивации» от лицаООО «ГЛОНАССсофт». В тексте указанных писем пользователю предлагается нажать на кнопку «Повторная проверка», в результате чего отображается форма для ввода аутентификационных данных учетной записи. После ввода пользователем данных осуществляется демонстрация изображения-приманки и компрометация пользовательской учетной записи. Для предотвращения реализации угроз безопасности информации необходимо ограничить получение электронных писем с адреса tretyakov[.]ev@glonasssoft[.]ru и обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

www[.]scientamicron[.]com;

pronew-webmail-signin-page-free-3994005985894[.]mos[.]ap-southeast-2[.]sufybkt[.]com;

visevisa-3049940309494994030[.]mos[.]ap-southeast-2[.]sufybkt[.]com;

neotes[.]space;

hxxps[:]//fullcheck[.]com[.]mx/uploads/pronew/Redirection[.]html;

hxxps[:]//www[.]scientamicron[.]com/phpfolder/eL0gin[.]php;

hxxps[:]//pronew-webmail-signin-page-free-3994005985894[.]mos[.]ap-southeast-2[.]sufybkt[.]com/ProNew-login-script-differentt[.]html?eta=;

hxxps[:]//fullcheck[.]com[.]mx/uploads/obfuscate/Redirection[.]html;

hxxps[:]//visevisa-3049940309494994030[.]mos[.]ap-southeast-2[.]sufybkt[.]com/Science-New-login-script-differentt[.]html?eta;

hxxps[:]//neotes[.]space/page/eL0gin[.]php.

осуществляются фишинговые рассылки электронных писем с тематикой «Candidate Representation Notice». Во вложениях указанных писем прикреплен архив с наименованием «resume.zip», содержащий файлы с наименованием «resume.desktop» (предназначен для функционирования в операционных системах Linux)и «resume.pdf.lnk» (предназначен для функционирования в операционных системах Windows). После запуска пользователем указанных файлов осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типов «шифровальщик» (Doge Big Balls) и «майнер» (XmRig). Для предотвращения реализации угроз безопасности информации, необходимо реализовать меры защиты, 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:

trackerjacker-proxy[.]goodfeathers[.]workers[.]dev
session-worker[.]stephen-miller7892[.]workers[.]dev
3d3894f0[.]whatdoumeanfunny[.]pages[.]dev
hxxps[:]//3d3894f0[.]whatdoumeanfunny[.]pages[.]dev/resume[.]zip
hxxps[:]//pystatemachine[.]goodfeathers[.]workers[.]dev/statemachine[.]sh[.]txt
hxxps[:]//trackerjacker-proxy[.]goodfeathers[.]workers[.]dev
hxxps[:]//session-worker[.]stephen-miller7892[.]workers[.]dev
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/amsibypass[.]ps
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/slurm[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/muchexcite[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/register[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/trackerjacker[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/attempt-elevation[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/fileless-ransomware[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/dcstage1[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/powerstealer[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/regpersist[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/patcher[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/stealerium-reflected[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/rubeuspivot[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/pivot[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/worm[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/webdelivery[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/ztinstall[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/filelessbombtrack[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/addadmins[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/grwrapper[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/trufflehog[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/rootkit[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/xmrigstart[.]ps1
hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/edgedump[.]ps1

hxxps[:]//bomberman[.]c2[.]workers[.]dev/statemachine[.]ps1

hxxps[:]//8548c8ca[.]whatdoumeanfunny[.]pages[.]dev/fileless-kernelexploit[.]ps1

при реализации целевых компьютерных атак возможно применение вредоносного программного обеспечения через скомпрометированные репозитории Arch Linux (Arch User Repository). Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу olrh4mibs62l6kkuvvjyc5lrercqg5tz543r4lsw3o6mh5qb7g7sneid[.]onion, используя схему доступа по «черным» или «белым» спискам.

при реализации целевых компьютерных атак возможно применение вредоносного программного типа «стилер» (Vidar Stealer).

при реализации целевых компьютерных атак возможно применение вредоносного программного типа «троян удаленного доступа», предназначенного для функционирования 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 адресу hxxp[:]//95[.]216[.]92[.]207[:]8080/, используя схему доступа по «черным» или «белым» спискам.

осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с расширением «.zip», содержащий документ-приманку с наименованием «Информация о среднемесячной заработной плате....pdf» и файл-ярлык с наименованием «Информация о среднемесячной заработной плате....lnk». После запуска пользователем указанного файла-ярлыка осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор». Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

ru-dns[.]net;

dns-ntp[.]com;

hxxp[:]//dns-ntp[.]com[:]80/api;

hxxp[:]//ru-dns[.]net[:]80/api;

hxxp[:]//ru-dns[.]net[:]8080/hlpcenter[.]zip;

hxxp[:]//ru-dns[.]net[:]8080/hlpmanager[.]zip.

осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен файл-ярлык с расширением «.lnk». После запуска пользователем указанного файла-ярлыка осуществляется выполнение вредоносного VBS-скрипта, демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Millenium RAT). Для предотвращения реализации угроз безопасности информации, обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hxxp[:]//158[.]94[.]208[.]168/files/8514679081/DRTjyu7[.]exe;

hxxps[:]//www[.]thesnapchatmodapk[.]com/update1[.]exe;

hxxps[:]//modedapk[.]net/update1[.]exe;

hxxps[:]//75877[.]mcdir[.]me/files/doc1[.]exe;

hxxp[:]//kuttabilla[.]top/mr[.]exe;

hxxp[:]//62[.]60[.]226[.]97[:]5553/voshod[.]exe;

hxxp[:]//130[.]12[.]180[.]43/files/7924412375/upOSLDn[.]exe;

hxxps[:]//blackhatusa[.]com/setup[.]exe;

hxxps[:]//blackhatusa[.]com/clip[.]exe;

hxxp[:]//blackhatusa[.]com/mr[.]exe;

hxxps[:]//blackhatusa[.]com/update[.]exe.

осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен файл с расширением «.js». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (LokiBot). Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

158[.]94[.]211[.]95;

kbfvzoboss[.]bid;

alphastand[.]trade;

alphastand[.]win;

alphastand[.]top;

hxxp[:]//158[.]94[.]211[.]95/kelly/five/fre[.]php;
hxxp[:]//kbfvzoboss[.]bid/alien/fre[.]php;
hxxp[:]//alphastand[.]trade/alien/fre[.]php;
hxxp[:]//alphastand[.]win/alien/fre[.]php;
hxxp[:]//alphastand[.]top/alien/fre[.]php.