Приложение 1

Деятельность хакерских группировок

1. Хакерской группировкой Rare Werewolf осуществляются:

фишинговые рассылки электронных писем с тематикой «Запрос цен и условий поставки». Во вложениях указанных писем прикреплен архив с наименованием «Scan_61115872.7z», содержащий исполняемый файл с наименованием «Scan.scr». После запуска пользователем указанного файла осуществляется выполнение команд оболочки сценариев «Powershell», демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для осуществления удаленного администрирования «AnyDesk»;

фишинговые рассылки электронных писем с тематиками «Схема оповещения!» и «Пневмокатапульта с самолетом». Во вложениях указанных писем прикреплен архив с наименованием, например «документы_закупки.rar» и «Пневмокатапульта с самолетом.rar», содержащие исполняемые файлы с аналогичными наименованиями и расширениями «.com» и «.exe». После запуска пользователем указанного файла осуществляется выполнение команд оболочки сценариев «PowerShell», демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для осуществления удаленного администрирования «AnyDesk».

2. Хакерской группировкой Core Werewolf осуществляются:

фишинговые рассылки электронных писем электронных писем, во вложениях которых прикреплен исполняемый файл с наименованием «Уведомление №221 о начале комплексной проверки согласно плану утечек-копия-7.exe». После запуска пользователем указанного файла осуществляется выполнение вредоносного скрипта, демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для осуществления удаленного администрирования «UltraVNC»;

фишинговые рассылки электронных писем, во вложениях которых прикреплен исполняемый файл с наименованием «Часть 1 Проект ДРОНОБОЙ видеопрезентация Дмитрия Чулкова для нужд СВО и ВПК России.exe». После запуска пользователем указанного файла осуществляется демонстрация видеозаписи-приманки, выполнение вредоносного скрипта и внедрение на целевую систему программного обеспечения для осуществления удаленного доступа «UltraVNC».

3. Хакерской группировкой Fluffy Wolf осуществляются:

фишинговые рассылки электронных писем с тематикой «Акт и УПД» от лица ООО «АльтаСтрой». Во вложениях указанных писем прикреплен архив с наименованием «УПД и акт сверки.rar», содержащий файл с наименованием «УПД акт сверки 1C buh Doc 27102025 PDF.scr» или «scrin shot 1C buh Doc 27102025 PDF.exe». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типов «стилер» (PureLog Stealer) и «троян удаленного доступа» (PureRAT).

4. Хакерской группировкой Cloud Werewolf осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен файл с расширением «.doc». После запуска пользователем уазанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (VBShower, VBCloud и PowerShower).

5. Хакерской группировкой Head Mare осуществляется эксплуатация уязвимостей программного обеспечения TrueConf Server (BDU:2025-10114, уровень опасности по CVSS 3.1 – высокий) и (BDU:2025-10116, уровень опасности по CVSS 3.1 – критический). Эксплуатация уязвимостей позволяет злоумышленникам получить несанкционированный доступ к системам с установленным указанным программным обеспечением. Для предотвращения реализации угроз безопасности, связанных с деятельностью указанной хакерской группировки необходимо своевременного обновлять программное обеспечение, а также на уровне сетевых средств защиты информации обеспечить ограничение обращений к следующим адресам, используя схему доступа по «черным» и «белым» спискам:

5[.]178[.]96[.]82; 5[.]252[.]178[.]171; 31[.]57[.]108[.232; 31[.]58[.]134[.]251;

31[.]57[.]109[.]151; 185[.]90[.]60[.]227; xbox-updater[.]online

6. Хакерской группировкой Fairy Wolf осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен файл с наименованием «ИСХ № 951ОП-13 от 28.10.2025.hta». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Unicorn Stealer).

7. Хакерской группировкой Erudite Mogwai осуществляются:

фишинговые рассылки электронных писем с тематикой «УВЕДОМЛЕНИЕ о необходимости внутренней проверки на предмет угроз информационной безопасности». В тексте указанных писем содержится ссылка, после открытия пользователем которой загружается архив с наименованием «Приложения.7z», содержащий файлы-приманки с расширениями «.doc» и «.pdf» и файл с наименованием «УВЕДОМЛЕНИЕ о необходимости внутренней проверки на предмет угроз информационной безопасности.pdf.lnk». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типов «загрузчик» (TADS) и «фреймворк» (Hermes).

8. Хакерской группировкой BO Team осуществляются:

фишинговые рассылки электронных писем с тематикой «FW:Страховая компания «Капитал МС» Клиентское обращение по ОМС. Запрос на разбор претензии застрахованного лица по качеству медуслуг». Во вложениях указанных писем прикреплен исполняемый файл с наименованием «Результаты медицинского обследования.exe», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (BrockenDoor).

9. Хакерской группировкой Silent Lynx осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «План развитие стратегического сотрудничества.pdf.rar», содержащий файл с аналогичным наименованием и расширением «.lnk», после открытия пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения (SilentLoader, Laplas и SilentSweeper). Для предотвращения реализации угроз безопасности информации необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» и «белым» спискам:

62[.]113[.]66[.]137; 62[.]113[.]66[.]7; 37[.]18[.]27[.]27; 206[.]189[.]11[.]142;

updates-check-microsoft[.]ddns[.]net;

catalog-update-update-microsoft[.]serverftp[.]com.

10. Хакерской группировкой Lone Wolf осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с расширением «.zip», содержащий файл-приманку с наименованием «досудебное дело.png» и файл-ярлык с наименованием «сверка.lnk». После запуска

пользователем указанного файла-ярлыка осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «фреймворк постэксплуатации» (Cobalt Strike).

11. Хакерской группировкой Sticky Werewolf осуществляются:

фишинговые рассылки электронных писем с тематикой «Субъектам ТЭК_О проведении мероприятий». Во вложениях указанных писем прикреплен архив с аналогичным наименованием и расширением «.7z», содержащий файлы с расширениями «.dll» и «.exe». После запуска файла с расширением «.exe» осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Pulsar RAT). Для предотвращения реализации угроз безопасности информации, связанных с указанной группировкой необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» и «белым» спискам:

194[.]226[.]121[.]225; 5[.]8[.]11[.]105; 194[.]226[.]121[.]225.

12. Хакерской группировкой Cavalry Werewolf осуществляются:

фишинговые рассылки электронных писем, во вложения которых прикреплен исполняемый файл с наименованием «О предоставлении информации для подготовки совещания.exe». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (BrockenDoor).

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

осуществляются фишинговые рассылки электронных писем с тематикой «Новый контакт». Во вложениях указанных писем прикреплен архив с наименованием «Контракт Кит Питер.7z», содержащий исполняемый файл с наименованием «Swift payment advice-4567688978676564.cmd». После запуска пользователем указанного файла осуществляется выполнение вредоносного сценария, демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (RemcostRAT);

осуществляются фишинговые рассылки электронных писем с тематикой «авр акт сверки срочно» от лица АО «Казпочта». Во вложениях указанных писем

прикреплен архив с наименованием «SKMACPATCHTECH 11645643767347434437.7z», содержащий файл с аналогичным наименованием и расширением «.vbs». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типов «загрузчик» (GuLoader) и «троян удаленного доступа» (RemcosRAT);

осуществляются фишинговые рассылки электронных писем, в тексте которых содержится вредоносная ссылка. После открытия пользователем указанной ссылки злоумышленники эксплуатируют уязвимость компонента Mojo браузера Google Chrome для операционных систем Windows (BDU:2025-03258, уровень опасности по CVSS 3.1 – высокий) для получения несанкционированного доступа к целевой системе и внедрения вредоносного программного обеспечения типа «стилер» (LeetAgent и Dante). В целях предотвращения возможности эксплуатации указанной уязвимости необходимо своевременно обновлять программное обеспечения до последних версий либо исключить использование браузера Google Chrome;

осуществляются фишинговые рассылки от имени ФСТЭК России с тематикой «Важное обновление системы», содержащие вредоносные вложения (архив с расширением «.rar»), с помощью которых осуществляется распространение вредоносного программного обеспечения типа «троян удаленного доступа» (AsyncRAT). Рассылки осуществляются с подменного почтового адреса postin@fsteck[.]ru. С целью предотвращения реализации угроз безопасности информации, связанных с фишингом, необходимо: проверять имя домена отправителя электронного письма в целях идентификации отправителя; при получении подозрительных писем от имени ФСТЭК России связаться с работником ФСТЭК России и удостовериться в его легитимности; обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам – 176[.]46[.]152[.]62, 78[.]137[.]2[.]165; 212[.]15[.]49[.]30; 176[.]46[.]152[.]62[:]5858/pipanos[.]exe;

осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «Исх №6626 Представление на назначение на воинскую должность.pdf.zip», содержащий файл с аналогичным наименованием и расширением «.lnk», после запуска пользователем которого осуществляется выполнение команд оболочки сценариев «PowerShell», демонстрация документа-приманки и внедрение на целевую систему вредоносного

программного обеспечения типа «фреймворк постэксплуатации» (PowerShell Stager);

при реализации целевых компьютерных атак осуществляет применение вредоносного программного обеспечения типа «фреймворк постэксплуатации» (Cobalt Strike). Для предотвращения реализации подобных угроз безопасности информации необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу 146[.]56[.]251[.]111/api/websessionindex/open/Lists[.]jsp, используя схему доступа по «черным» и «белым» спискам;

осуществляются фишинговые рассылки электронных писем с тематикой «Декларация». Во вложениях указанных писем прикреплен архив с наименованием «Список спецификаций продукта MT245353575746 Sympatetiskes.7z», содержащий файл с аналогичным наименованием и расширением «.wsf». После запуска пользователем указанного файла осуществляется выполнение команд оболочки сценариев «PowerShell» и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Remcos RAT). Для предотвращения угроз безопасности, связанных с указанной рассылкой, необходимо на уровне сетевых средств защиты информации ограничить обращение к следующим адресам, используя схему доступа по «черным» и «белым» спискам:

files[.]catbox[.]moe; metavasipar[.]hu; wormoni[.]lms-austria[.]com;

adigo[.]ydns[.]eu; 108[.]181[.]20[.]35;

осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен файл с наименованием «PurchaseOrder_25005092.js». После запуска пользователем указанного файла осуществляется выполнение вредоносного JS-скрипта и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (XWorm). Для предотвращения реализации указанной угрозы необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» и «белым» спискам:

196[.]251[.]115[.]62; 103[.]83[.]86[.]27;

осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с расширением «.zip», содержащий файлы-приманки и файл с расширением «.js». После запуска пользователем указанного файла

осуществляется выполнение вредоносного JS-скрипта и внедрение на целевую систему вредоносного программного обеспечения типа «загрузчик» (Gootloader);

при реализации целевых компьютерных атак осуществляется применение вредоносного программного обеспечения типа «стилер» (Vidar Stealer), предназначенного для кражи пользовательских данных программного обеспечения Microsoft. Для предотвращения реализации указанных атак необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» и «белым» спискам:

telegram[.]me/ahnadar; steamcommunity[.]com/profiles/76561198780411257;

xp[.]lorenabulei[.]com;