Федеральное государственное бюджетное образовательное учреждение высшего образования «САРАТОВСКАЯ ГОСУДАРСТВЕННАЯ ЮРИДИЧЕСКАЯ АКАДЕМИЯ»

Управление информационных технологий

Проректоры, руководители структурных подразделений, непосредственно подчиненных ректору

СЛУЖЕБНАЯ ЗАПИСКА

12.12.2024 № 25-10/154

О мерах по повышению защищенности информационной инфраструктуры Академии

Уважаемые коллеги!

Прошу отнестись к данной служебной записке с особым вниманием и ознакомиться с данным материалом.

Согласно поступившей новой информации одним из векторов проведения компьютерных атак является внедрение вредоносного программного обеспечения через почтовые вложения. Нарушители используют методы социальной инженерии, отправляя пользователям фишинговые[1] электронные письма с вредоносным вложением.

Указанные электронные письма содержат вложения в виде электронных документов, при открытии которых осуществляется попытка внедрения вредоносного программного обеспечения. В условиях сложившейся обстановки, выявлены сведения о рассылке фишинговых электронных писем с вредоносным вложением.

1. Рассылки электронных писем, содержащих вредоносный архив, защищенный паролем. Внутри указанного архива содержатся файл с расширением «.data» и файл-ярлык с расширением «.lnk». После открытия пользователем файла-ярлыка осуществляется запуск эмулированной среды Linux с предварительно настроенным клиентом «Chisel» для подключения к удаленному серверу управления злоумышленников, который выполняет функции вредоносного программного обеспечения типа «бэкдор»[2].

[1] Фишинг (phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логины и пароли к банковским картам, учетным записям).

[2] Бэкдор, тайный вход (от англ. back door — «чёрный ход», «лазейка», буквально «задняя дверь») — дефект алгоритма, который намеренно встраивается в него разработчиком/злоумышленником и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом.

2. Фишинговые рассылки электронных писем от лица несуществующих компаний, а также с похищенных почтовых аккаунтов. Указанные электронные письма замаскированы под запросы информации о заказах, во вложениях которых содержатся вредоносные архивы с расширениями (.iso, .7z, .gzip и .rar). Внутри указанных архивов содержится файл, после открытия которого осуществляется выполнение команд оболочки сценариев «PowerShell» и внедрение на целевую систему вредоносного программного обеспечения типа «загрузчик» (GuLoader – это продвинутый загрузчик вредоносных программ, который используется для распространения различных троянов для удалённого доступа (RAT-троянов)).

3. Фишинговые рассылки электронных писем осуществляющих заражение контроллеров доменов вредоносным программным обеспечением типа «стилер»[3] и «загрузчик»[4] (RustyStealer – это вредоносная программа, относящаяся к классу «кради». Вредоносные программы этого класса предназначены для кражи данных, например, названия устройства, сведений об оборудовании, версии и архитектуры операционной системы, имени пользователя, IP-адреса и так далее). Эти вредоносные программы извлекают и передают информацию). Через зараженные домены осуществляется дальнейшее распространение вредоносного программного обеспечения типа «шифровальщик» (Ymir – вымогательское вредоносное программное обеспечение, блокирует устройство или данные, шифруя их) путем выполнения команд оболочки сценариев «PowerShell».

4. Фишинговые рассылки электронных писем, во вложениях находятся вредоносные архивы, содержащие исполняемые файлы, которые являются вредоносным программным обеспечением типа «троян удаленного доступа» (например, Unicorn, Darktrack RAT, Sliver implant и Quasar RAT) или легитимным программным обеспечением для удаленного управления целевой системой (UltraVNC и MeshCentral). После открытия исполнительного файла запускается документ-приманка и выполняются вредоносные скрипты, позволяющие получить несанкционированный доступ к целевой системе.

5. Фишинговые рассылки электронных писем, содержащих документ с наименованием «Quotation.uue», замаскированный под легитимный платежный документ. После открытия указанного файла осуществляется выполнение вредоносного кода и внедрение вредоносного программного обеспечения типа «стилер» (FormBook).

6. Фишинговые рассылки электронных писем, содержащих вредоносный исполняемый файл с наименованием:

[3] Стилер – это вредоносное программное обеспечение, предназначенное для кражи сохранённых в системе паролей и отправки их злоумышленнику.

[4] Загрузчик – это вид вредоносного программного обеспечения, который записывается в первый сектор гибкого или жёсткого диска и выполняется при загрузке компьютера.

«Исх_10_09_2024_№6_223_Организациям_по_списку_Визуализация.scr». После открытия указанного файла происходит загрузка программного обеспечения для удаленного доступа «МИПКО Employee Monitor», которое позволяет злоумышленникам взаимодействовать с целевой системой.

7. Фишинговые рассылки электронных писем, содержащих вредоносные архивы с наименованиями «RusAutomation.rar» или «RusAutomation.rar». Архивы содержат исполняемые вредоносные файлы с наименованиями:

«RusAutomation/Scan_A-Automation_TZ_827_02.09.2024.lnk»,
«RusAutomation/Scan_Kartochka_RusAutomation.pdf»,
«RusAutomation/Scan_RusAutomation_TZ_298_21.08.2024.lnk»,
«Scan_Kartochka_Promavtomatika.pdf»,
«Scan_Promavtomatika_TZ_633_23.08.2024.lnk»,
«Scan_Promavtomatika_TZ _633_23.08.2024.pdf».

После открытия указанных файлов осуществляется загрузка и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (RemcosRAT).

8. Фишинговые рассылки электронных писем, содержащих вредоносный файл с расширением «.url». После открытия указанного файла осуществляется загрузка вредоносного программного обеспечения типа «стилер» (Atlantida – крадёт широкий спектр данных для входа в такие программы, как Telegram, Steam, несколько офлайн-кошельков с криптовалютой, данные, хранящиеся в браузере, а также данные расширений для криптовалютных кошельков. Она также записывает экран жертвы и собирает данные об оборудовании).

9. Осуществляется распространение вредоносного программного обеспечения типа «троян»[5] (Buhtrap RAT) путем использования фишинговых сайтов, замаскированных под профильные бухгалтерские сайты. Упомянутые сайты содержат вредоносные архивы с образцами договоров, содержащими вредоносное программное обеспечение Buhtrap RAT. После загрузки и открытия указанных файлов осуществляется получение несанкционированного доступа к целевой системе.

10. Фишинговые рассылки электронных писем от лица работника Министерства связи и информатизации Республики Беларусь. Во вложениях указанных писем находится вредоносный файл с наименованием «O predstavlenii informatsii.doc», после открытия которого осуществляется внедрение вредоносного программного обеспечения и получение несанкционированного доступа к целевой системе.

[5] Троян – разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения. В отличие от вирусов и червей, трояны не распространяются самопроизвольно.

11. Фишинговые рассылки электронных писем, замаскированных под финансовые документы. Во вложениях указанных писем содержится вредоносный архив, внутри которого находятся документ-приманка с расширением «.xls» и исполняемый файл с расширением «.exe». После открытия пользователем исполняемого файла осуществляется внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (Revenge RAT).

12. Фишинговые рассылки электронных писем, во вложениях которых содержатся вредоносные архивы. В указанных архивах содержатся документы-приманки и исполняемый файл с расширениями «.com» и «.exe», после их открытия пользователем осуществляется демонстрация файла-приманки и внедрение вредоносного программного обеспечения типа «стилер» (MetaStealer – шпионское ПО, которое нацелено на кражу конфиденциальной информации с компьютера жертвы. Чаще всего распространяется через рассылку фишинговых писем. Имеет версии для атак как на Windows, так и на MacOS).

В целях предотвращения реализации указанных угроз информационной безопасности просим сотрудников Академии о необходимости безопасной работы с электронной почтой, а именно:

- производить проверку почтовых вложений с использованием средств антивирусной защиты;
- внимательно 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;
- не открывать и не загружать почтовые вложения писем с тематикой, неотносящейся к деятельности организации;
- не открывать письма от неизвестных адресатов;
- не открывать вложения, особенно если в них содержатся документы с макросами, архивы с паролями, исполняемые файлы (exe, iso и др.);
- не переходить по ссылкам, которые содержаться в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т.д.);
- проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься», «вниманию» и пр.);
- проверять ссылки, даже если письмо получено от другого пользователя информационной системы.

Соблюдение вышеперечисленных мер позволит повысить уровень защищенности информационной инфраструктуры Академии, стабильность функционирования работы и исключит возможность внедрения вредоносного программного обеспечения по средствам электронной почты.

И.о. начальника

СГЮА
ДОКУМЕНТ ПОДПИСАН
Лазоренко Павел Николаевич
Дата: 12.12.2024

П.Н. Лазоренко

Давыдов Денис Владимирович
вн. 11-13