ГАРДА

Гарда Лабиринт

Функциональная спецификация. Модуль Приманки

gardatech.ru

2023

Тип документа:	Функциональная спецификация. Модуль Приманки
Дата выпуска:	03.11.2023
Статус документа:	Released
Версия:	1.8.0

Содержание

1 Введение

1.1 Аннотация

Данный документ представляет собой Функциональную спецификацию к модулю Примаки, входящего в состав Программного Комплекса "Гарда Лабиринт" (далее – «Гарда Лабиринт», Программный Комплекс, Комплекс).

1.2 Использование имен, номеров телефонов, сетевых адресов

Приведенные в настоящем документе сведения о юридических и физических лицах, включая любые их данные, являются вымышленными, а IP-адреса и номера телефонов не соответствуют их действительным владельцам. Любые совпадения случайны.

1.3 О компании

Гарда Технологии (входит в ГК Гарда) – разработчик семейства продуктов в области защиты данных и сетевой безопасности. Решения Гарда защищают данные крупнейших государственных организаций и корпораций, защищают 50% всего российского интернета от DDoS-атак, обеспечивают защиту цифровых сервисов и мероприятий федерального масштаба. Продуктовый портфель холдинга построен на основе технологий собственной разработки, которые не требуют сторонних лицензий, включены в Единый реестр российского ПО и сертифицированы ФСТЭК.

1.4 Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании "Гарда Технологии":

- Тел. +7 (831) 422-12-20 (с 9-00 до 18-00 по московскому времени).
- Email: glb.support@gardatech.ru.

2 Модуль Приманки

2.1 Назначение модуля Приманки

Модуль Приманки предназначен для постоянной доставки самораспаковывающегося архива, распространяющего приманки на АРМ предприятия. Приманки используются для увеличения вероятности взаимодействия злоумышленника с ловушкой. Приманка предлагает обратиться по адресу ловушки и провзаимодействовать с ней, таким образом злоумышленник выявлен на ранней стадии атаки и администратор ИБ или ИТ службы предприятия имеет возможность заранее реагировать на возникающие угрозы.

2.2 Принцип работы модуля

Комплекс предлагает скачать сконфигурированный самораспаковывающийся архив и разместить его на общедоступном в сети ресурсе для того чтобы групповой политикой домена или каким-то другим образом произошло обращение реального устройства к данному файлу. Далее в соответствии с заранее определенными правилами для определенных доменных групп или конкретных узлов происходит доставка Приманки на узел сети с которого произошло обращение с помощью самораспаковывающегося архива. Приманки представляют из себя различные артефакты, содержащие путь до ловушки и уникальную для каждого узла учетную запись.

2.3 Функциональные свойства приманок

- Имеется возможность распространять приманки типа SSH, RDP, FTP, HTML, SMB, MSSQL, MySQL
- Приманки распространяются в виде:
  - куки данных,
  - учетных данных в хранилище операционной системы,
  - в хранилище учетных данных браузера,
  - текстовый файл,
  - настроенное соединение putty.

- При распространении приманок не устанавливаются никакие программы, выполняющие роль агента на конечные узлы сети.
- В приманках уникальные учетные данные для каждого отдельного узла сети.
- Процесс доставки приманок на конечный узел не эксплуатирует протоколы и службы: PsExec, PaExec, WMI/RPC, WinRM, SSH, sh – скрипты.
- Доставка приманок должна происходить по защищенному шифрованием каналу связи.