НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: gov-cert@gov-cert.ru

Вредоносное программное обеспечение «EvilGnome»

ALRT-20190718.1 | 18 июля 2019 г.

Уровень угрозы: СРЕДНИЙ

TLP: WHITE

Целевые системы	Рабочие станции под управлением UNIX-подобных ОС
Актуальность	По настоящее время
Описание	17 июля компания Intezer опубликовала отчет, в котором говорится о новом шпионском ВПО «EvilGnome», которое нацелено на рабочие станции под управлением UNIX-подобных ОС. Данное ВПО распространяется с помощью самораспаковывающегося архива в виде shell-скрипта, созданного с помощью утилиты makeself, аналога утилиты WinZip Self-Extractor для Windows. ВПО устанавливается в папку ~/.cache/gnome-software/gnome-shell-extensions/ для маскировки под расширение среды рабочего стола Gnome и добавляет в планировщик задач запуск основного вредоносного скрипта gnome-shell-ext.sh каждую минуту. Каждый модуль ВПО запускается в отдельном процессе и имеет свой функционал: • ShooterSound – записывает звук с микрофона пользователя • ShooterImage – создает снимки экрана • ShooterFile – сканирует файловую систему на наличие недавно созданных файлов • ShooterPing – получает новые команды от центра управления • ShooterKey – не используется, возможно это незавершенный модуль-кейлоггер Все данные, собранные с помощью модулей, ВПО отправляет в центр управления. Если не удается установить связь с ним или от него поступает соответствующая команда, модули используют путь ~/.cache/gnome-software/gnome-shell-extensions/tmp/ для хранения собранных данных. Эксперты компании Intezer полагают, что данное ВПО является незавершенным тестовым прототипом, который впоследствии будет дорабатываться и изменяться. Также они отмечают, что IP-адреса и доменные имена центров управления продолжительное время контролируются группировкой Gamaredon. На текущий момент данное ВПО не определяется антивирусными средствами.
Рекомендации по нейтрализации угрозы	1. Применение актуальных политик безопасности 2. Блокирование средствами межсетевого экранирования соединений с серверами злоумышленников. 3. Добавление контрольных сумм файлов ВПО в черные списки AV/ATP-решений.

Контрольные суммы файлов и модулей ВПО	a21acbe7ee77c721f1adc76e7a7799c936e74348d32b4c38f3bf6357ed7e8032 82b69954410c83315dfe769eed4b6cfc7d11f0f62e26ff546542e35dcd7106b7 7ffab36b2fa68d0708c82f01a70c8d10614ca742d838b69007f5104337a4b869
Доменные имена, использующиеся злоумышленниками	clsass.ddns.net kotl.space
IP-адреса центров управления	195.62.52.101 185.158.115.44 185.158.115.154