Хитрый ботнет выжимает все соки с каждого заражённого устройства.

Исследователи из команды безопасности Команда безопасности XLab является подразделением китайской компании QiAnXin, одной из крупнейших компаний по кибербезопасности в Китае. Основное направление деятельности XLab – исследование кибербезопасности, анализ угроз и создание масштабных многомерных платформ безопасности данных. Команда известна своими успехами в мониторинге крупных ботнетов и выявлении более 30 глобально значимых ботнетов, таких как Mirai и Bigpanzi." data-html="true" data-original-title="XLab" >XLab недавно обнаружили в киберпространстве новый Ботнет — это совокупность подключенных к Интернету устройств, которые могут включать персональные компьютеры (ПК), серверы, мобильные устройства и устройства Интернета вещей (IoT), которые заражены и контролируются вредоносным ПО без ведома их владельца." data-html="true" data-original-title="Ботнет" >ботнет Zergeca, отличающийся своими передовыми возможностями и представляющий серьёзную угрозу для миллионов цифровых устройств. Zergeca способен не только проводить DDoS-атака – распределенная атака типа отказ в обслуживании, которая являет собой одну из самых распространенных и опасных сетевых атак. В результате атаки нарушается или полностью блокируется обслуживание законных пользователей, сетей, систем и иных ресурсов.

 DDoS-атака заключается в непрерывном обращении к сайту со многих компьютеров, которые расположены в разных частях мира. В большинстве случаев эти компьютеры заражены вирусами, которые управляются мошенниками централизовано и объедены в одну ботсеть (ботнет). Компьютеры, которые входят в ботсеть, рассылают спам, участвуя, таким образом, в DDoS-атаках." data-html="true" data-original-title="DDoS" >DDoS-атаки, но и выполнять множество других вредоносных функций.

20 мая 2024 года XLab зафиксировала подозрительный ELF-файл в каталоге «/usr/bin/geomi» на платформе Linux — это свободная и открытая операционная система, разработанная Линусом Торвальдсом в 1991 году. С тех пор Linux стал одной из наиболее популярных альтернатив коммерческим операционным системам.

 Основное преимущество Linux заключается в его открытом исходном коде, что позволяет пользователям свободно изменять и распространять систему в соответствии с лицензией GNU GPL.

 Linux предоставляет стабильную, надежную и гибкую платформу для работы с компьютером или сервером. Большинство дистрибутивов Linux (например, Ubuntu, Fedora, Debian) поставляются с разнообразными программами и инструментами для работы, включая офисные приложения, интернет-браузеры, мультимедийные инструменты и многое другое.

 Linux также широко используется в серверной сфере и встроенных системах,

таких как маршрутизаторы и мобильные устройства." data-html="true" data-original-title="Linux" >Linux одного из своих клиентов. Этот файл, упакованный с помощью модифицированного UPX, долгое время оставался незамеченным антивирусными программами.

После анализа исследователи выяснили, что это ботнет, реализованный на Go (часто также «Golang») – компилируемый многопоточный язык программирования, разработанный внутри компании Google. Официально язык был представлен в ноябре 2009 года. На данный момент поддержка официального компилятора, разрабатываемого создателями языка, осуществляется для операционных систем FreeBSD, OpenBSD, Linux, macOS, Windows, DragonFly BSD, Plan 9, Solaris, Android, AIX." data-html="true" data-original-title="Golang" >Golang. А учитывая то, что в его Инфраструктура управления и контроля, также известная как C2, или C&C (сокр. от англ. «command-and-control»), представляет собой набор инструментов и методов, которые злоумышленники используют для обмена данными со скомпрометированными устройствами после первоначального вторжения (постэксплуатации). Конкретные механизмы атак сильно отличаются друг от друга, но обычно C2 включает один или несколько скрытых каналов связи между устройствами в атакуемой организации и контролируемой злоумышленником платформой. Эти каналы связи используются для передачи инструкций взломанным устройствам, загрузки дополнительных вредоносных данных и передачи украденных данных злоумышленнику." data-html="true" data-original-title="C2" >C2-инфраструктуре использовалась строка «ootheca», напоминающая о зергах из StarCraft, специалисты XLab назвали ботнет Zergeca, подчёркивая его агрессивный и стремительный характер распространения.

Zergeca поддерживает шесть методов DDoS-атак, а также функции проксирования, сканирования, самообновления, сохранения постоянства, передачи файлов, обратной оболочки и сбора конфиденциальной информации.

Zergeca использует несколько методов DNS-разрешения, включая DNS over HTTPS (DOH). Также применяется библиотека Smux для C2-протокола, обеспечивающая шифрование с помощью XOR. Это позволяет ботнету эффективно скрывать свою деятельность и усложняет его обнаружение.

Анализ показал, что IP-адрес 84.54.51.82, используемый для C2, с сентября 2023 года обслуживал два ботнета Mirai, что говорит о накопленном опыте его создателей. Основные методы распространения Zergeca включают эксплуатацию слабых паролей Telnet и уязвимостей CVE-2022-35733 и CVE-2018-10562.

С начала июня 2024 года Zergeca нацелился на Канаду, США и Германию. Основным типом атаки был ackFlood (atk_4), а жертвами становились различные автономные системы (ASN). Zergeca работает на архитектуре x86-64 и нацелена на платформу Linux, однако в коде ботнета исследователи также обнаружили упоминания Android и Windows, что намекает на будущие сценарии развития вредоноса.

Zergeca достигает постоянства на скомпрометированных устройствах, добавляя системную службу «geomi.service», что обеспечивает автоматический запуск процесса при перезагрузке устройства. Для шифрования строк используется XOR с жёстко закодированным ключом.

Ботнет включает модуль Silivaccine, который устраняет конкурентные угрозы, такие как майнеры и трояны, обеспечивая монополию на заражённом устройстве и использование максимальной производительности.

Открытие Zergeca демонстрирует непрерывную эволюцию и усложнение ботнетов. Благодаря своим передовым функциям, обеспечению постоянства и гибкости, Zergeca представляет серьёзную угрозу. Специалисты в области кибербезопасности должны оставаться бдительными и принимать проактивные меры для выявления и смягчения таких угроз.