Как международная сеть прокси использовалась для кражи социальных выплат.

Министерство финансов США ввело санкции против сети киберпреступников, включающей трех граждан Китая и три компании из Таиланда. Субъекты связаны с крупным ботнетом, который контролировал сервис резидентных прокси под названием «911 S5».

Обнаружение и деятельность 911 S5

В июне 2022 года исследователи из канадского университета Шербрука выявили, что 911 S5 заманивал жертв, предлагая бесплатный VPN. VPN использовался для установки вредоносного ПО, которое добавляло IP-адреса жертв в 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 911 S5. На тот момент ботнет контролировал около 120 000 резидентных прокси-узлов по всему миру, каждый из которых взаимодействовал с несколькими C2-серверами, расположенными за рубежом или размещенными на облачном сервере.

Приостановка и возрождение ботнета

Месяц спустя журналист-расследователь Брайан Кребс сообщил, что 911 S5 прекратил работу после уничтожения ключевых компонентов его бизнес-операций вследствие нарушения безопасности. Тем не менее, ботнет был возрожден спустя несколько месяцев под названием CloudRouter, согласно отчету компании Spur Intelligence в феврале.

Интерфейс CloudRouter

Меры OFAC и ущерб

Управление по контролю за иностранными активами при Министерстве финансов США (OFAC) заявило, что ботнет 911 S5 представлял собой вредоносную службу, компрометировавшую компьютеры жертв и позволявшую киберпреступникам проксировать свои интернет-соединения через зараженные компьютеры.

Зараженные устройства позволяли преступникам замаскировать свои действия, перекладывая ответственность на компьютеры жертв. Ботнет скомпрометировал около

19 миллионов IP-адресов, что позволило киберпреступникам подать десятки тысяч мошеннических заявок на программы, связанные с законом Закон о помощи, поддержке и экономической безопасности в связи с коронавирусом (CARES Act) — комплексный пакет мер, принятый в США в марте 2020 года для смягчения экономических последствий пандемии COVID-19.

 Основные положения включают: прямые выплаты гражданам, увеличение пособий по безработице, поддержку малого бизнеса через программу защиты зарплат, финансовую помощь крупным компаниям, помощь медицинским учреждениям и поддержку образовательных учреждений.

 Закон направлен на быструю и широкую поддержку различных секторов экономики и общества, пострадавших от кризиса, вызванного пандемией." data-html="true" data-original-title="CARES Act" >CARES Act, что привело к убыткам в миллиарды долларов.

Тарифы 911 S5

Санкции против участников

OFAC ввело санкции против следующих лиц и компаний:

По документам OFAC, «перечисленные физические и юридические лица использовали ботнет для компрометации личных устройств, что позволило киберпреступникам обманным путем получать экономическую помощь, предназначенную для нуждающихся».

В результате санкций все операции, затрагивающие интересы США и собственность внесенных в перечень физических и юридических лиц, запрещены. Любые сделки с этими лицами и компаниями также подвергаются санкциям или принудительным действиям.