Октябрьский районный комитет информирует

№ 24/2023

Хакерские атаки

30 мая РИА Новости сообщили, что в очередной раз хакеры начали рассылать российским компаниям письма с вирусами.

Мы с вами уже пережили подобное несколько лет тому назад. Особенно пострадавшим среди нас на тот момент была школа – интернат № 15, в которой хакеры заблокировали все компьютеры и программы, в том числе бухгалтерские. Можете представить масштаб этой катастрофы.

В связи с последними событиями хакеры вновь «оживились» и начали рассылать российским компаниям фишинговые письма с вредоносным программным обеспечением, исходные коды которого размещены в открытом доступе и доступны всем желающим, рассказали РИА Новости в компании Bi.Zone

Источник: Reuters

«Эксперты обнаружили кампанию, направленную против российских организаций из разных отраслей. Ее цель — распространение вредоносного программного обеспечения Umbral, которое собирает с зараженных компьютеров учетные данные пользователей. Примечательно, что исходные коды размещены в открытом доступе на веб-сервисе для хранения IT-проектов GitHub и доступны всем желающим», — выяснили специалисты.

Отмечается, что для доставки вредоносного программного обеспечения в корпоративные сети злоумышленники выбрали простой, но эффективный метод — фишинговые письма с приложенными файлами с опасными ярлыками. Их замаскировали под документы с названием «План Рейдеров», а открытие такого файла запускало процесс компрометации устройства.

Вредоносный Umbral позволяет злоумышленникам обходить средства защиты, повышать привилегии, собирать информацию о скомпрометированной системе и извлекать аутентификационные данные из широкого ряда приложений, включая браузеры Chrome, Opera и «Яндекс Браузер», мессенджера Discord и игры Minecraft.

Эксперты обратили внимание, что многие из этих приложений могут содержать не только пароли для личных учетных записей, но и для корпоративных. Это может позволить атакующим получить доступ к целевой сети, а потом использовать ее для рассылки фишинговых писем внутри организации.

В связи с этим прошу предупредить руководство, сотрудников, специалистов и детей ни в коем случае не открывать письма с неизвестных источников, не посещать подозрительные сайты. Лозунг «Будьте бдительны» как никогда актуален в наше время. Берегите себя и свои данные.

Председатель РК Профсоюза Н.И. Могилева