Коварный трюк хакеров с Microsoft Word искренне удивил ИБ-специалистов.

Исследователи в области кибербезопасности обнаружили новый вредоносный загрузчик SquidLoader, распространяющийся через фишинговые кампании, нацеленные на китайские организации.

По данным специалистов LevelBlue Labs – это подразделение компании AT&T, занимающееся исследованиями в области кибербезопасности. Оно специализируется на выявлении и анализе новых угроз и вредоносного ПО. Основная цель LevelBlue Labs – защита организаций от киберугроз путем предоставления актуальной информации о методах и инструментах, используемых злоумышленниками. Лаборатория активно сотрудничает с другими подразделениями AT&T и внешними партнерами для разработки передовых решений в области кибербезопасности." data-html="true" data-original-title="LevelBlue Labs" >LevelBlue Labs, впервые зафиксировавших этот вредоносный код в конце апреля 2024 года, SquidLoader использует методы, позволяющие избежать статического и динамического анализа и, в конечном счёте, обнаружения.

Цепочки атак используют фишинговые электронные письма с вложениями, которые маскируются под документы Microsoft Word, но на самом деле являются бинарными файлами, запускающими выполнение вредоносного кода. Этот код используется для загрузки второго этапа вредоносного ПО с удалённого сервера, включая Cobalt Strike представляет собой законный фреймворк для проведения тестов на проникновение, позволяющий доставить на компьютер жертвы полезную нагрузку и управлять ею. Злоумышленники же могут использовать Cobalt Strike в реальных атаках на целевые системы, эффективно совмещая фреймворк с другими инструментами." data-html="true" data-original-title="Cobalt Strike" >Cobalt Strike.

Исследователь безопасности Фернандо Домингес отмечает, что загрузчики обладают сложными механизмами уклонения и создания ложных целей, что помогает им оставаться незамеченными и затрудняет анализ. Поставляемый шелл-код загружается в тот же процесс, чтобы избежать записи вредоносного ПО на диск и тем самым не попасть под обнаружение.

SquidLoader применяет различные техники уклонения, такие как использование зашифрованных сегментов кода, ненужного кода, который остаётся неиспользованным, обфускация графа управления потоком (CFG), обнаружение отладчиков и выполнение прямых системных вызовов вместо вызовов API Windows NT.

Загрузчики вредоносного ПО стали популярными среди злоумышленников, стремящихся доставить и запустить дополнительные полезные нагрузки на скомпрометированных устройствах, обходя антивирусные защиты и другие меры безопасности.

Эволюция киберугроз требует постоянной бдительности и адаптации. Организациям следует не только укреплять технические аспекты защиты, но и обучать сотрудников распознавать фишинговые атаки, ведь даже самые продвинутые системы безопасности можно обойти благодаря человеческому фактору.