Пентестеры, разработчики ВПО, операторы… кто стоит за группировкой?

Специалисты центра исследования киберугроз Solar 4RAYS обнаружили и изучили деятельность высокопрофессиональной хакерской группировки Shedding Zmiy. Эксперты рассказали , что злоумышленники использовали скомпрометированные данные российских компаний не только для последующих атак, но и публиковали их в открытом доступе. При этом основной целью группы, по словам исследователей, была не финансовая выгода, а кража конфиденциальной информации.

В Solar 4RAYS не смогли точно атрибутировать происхождение группы, но отметили несколько характерных этой группировке признаков. Во-первых, похищенные данные публиковались в проукраинских Telegram-каналах. Во-вторых, в части используемого инструментария Shedding Zmiy связана с другими группировками (Cobalt, exCobalt, Shadow, Comet, Twelve, «о происхождении которых в сообществе исследователей киберугроз сложилось определенное мнение»). В-третьих, в логах атак встречались команды на украинском и русском языках. Наконец, целями Shedding Zmiy становились преимущественно российские организации.

По словам экспертов, группировка представляет серьезную угрозу для РФ. Она применяет как общедоступное, так и собственное уникальное вредоносное ПО. Для внедрения вредоносов на системы жертв хакеры порой использовали скомпрометированные легитимные серверы. Shedding Zmiy умеет запутывать следы: группировка владеет «обширной сетью командных серверов на территории России, арендует ресурсы у различных хостинг-провайдеров и на облачных платформах; это помогает хакерам обходить блокировки атак по территориальному признаку (по GeoIP)».

На первый взгляд разрозненные инциденты со схожими признаками использования ВПО, уязвимостей, инфраструктуры были объединены экспертами в один кластер. Всего специалисты Solar 4RAYS обнаружили следы применения 35 различных инструментов на этапах разведки, доставки вредоносов, распространения по сети и кражи данных. Для проникновения в сеть, эскалации привилегий и закрепления хакеры задействовали как минимум 20 известных уязвимостей в популярном корпоративном ПО.

Кроме технических средств, Shedding Zmiy охотно прибегала к социальной инженерии. Так, в одном случае злоумышленники создали фейковый Telegram-аккаунт, выдав себя за сотрудника ИБ-службы компании-жертвы, чтобы выпросить у реального работника пароль для входа в систему. Используя скомпрометированную учетку,

Все права защищены

save pdf date >>> 24.11.2024

злоумышленники успели побывать еще на нескольких хостах, где разместили ВПО.

С начала 2022 года группа успела атаковать несколько десятков российских компаний из государственного, промышленного, телекоммуникационного и других ключевых секторов. В Solar 4RAYS не раскрыли имен конкретных жертв.

По оценке экспертов, в состав Shedding Zmiy входят отдельные команды разных специализаций: пентестеры, разработчики ВПО, операторы и администраторы. Минимально для подготовки таких атак требуется 5-6 высококвалифицированных сотрудников разного профиля и серьезный бюджет, включая средства на покупку коммерческого вредоносного ПО вроде SystemBC, EkipaRAT и DarkGate.

На подпольных форумах предложения о продаже DarkGate достигают примерно $100 000 за годовую лицензию. Сама разработка арсенала стоит на порядок больше, чем стоимость экземпляра ПО — то есть уже не $100 000, а $1 млн., отмечают эксперты. В свою очередь, стоимость атаки уже на порядок выше стоимости разработки — туда входит как несколько утилит, так и немалый ресурс самих атакующих.

Сами хакеры демонстрируют высочайший уровень разработки. В частности, ими был создан целый фреймворк для автоматизированной эксплуатации одной из уязвимостей. Это говорит об инвестициях значительных временных и финансовых ресурсов в развитие вредоносного арсенала группы.

Все права защищены

save pdf date >>> 24.11.2024