Университет ИТМО, факультет программной инженерии и компьютерной техники

Двухнедельная отчётная работа по «Информатике»: аннотация к статье

Дата сдачи :09/21/2021

Выполнил хатиб ватан № 291834 , № группы *p3113* , оценка

|  |  |  |
| --- | --- | --- |
| **Название статьи/главы книги/видеолекции** | | |
| **ФИО автора статьи (или e-mail)**  *Рави Лакшманан* | **Дата публикации**  **(не старше 2018 года)**   20 Сентябрь 2021 г. | **Размер статьи**  **(от 400 слов)**  550 |
| **Прямая полная ссылка на источник и сокращённая ссылка (bit.ly, goo.gl, tr.im и т.п.)**  *прямая ссылка* [*https://thehackernews.com/2021/09/a-new-wave-of-malware-attack-targeting.html*](https://thehackernews.com/2021/09/a-new-wave-of-malware-attack-targeting.html)  *сокращённая ссылка* bit.ly/3zA32ju | | |
| **Теги, ключевые слова или словосочетания** | | |
| **Перечень фактов, упомянутых в статье**   1. Кампания по рассылке спама, рассылающая целевые фишинговые письма, нацеленные на южноамериканские организации. 2. кампания методы, включив в нее широкий спектр обычных троянских программ удаленного доступа (RAT) и геолокационную фильтрацию, чтобы избежать обнаружения. 3. атака, приписываемая продвинутой постоянной угрозе (APT), отслеживаемая как APT-C-36, предполагаемая шпионская группа в Южной Америке. 4. В основном распространяется через мошеннические электронные письма, маскируясь под колумбийские правительственные учреждения, такие как Национальное налоговое . 5. Цепочка заражения начинается, когда получатели сообщения открывают ложный документ PDF или Word, который утверждает, что это приказ об изъятии, привязанный к их банковским счетам, и щелкают ссылку, созданную службой сокращения URL-адресов. 6. Сокращатели URL-адресов поддерживают географический таргетинг, поэтому, если пользователь из страны, не являющейся объектом атак злоумышленников, нажимает на ссылку, он будет перенаправлен на законный веб-сайт. 7. Сокращатели URL-адресов также могут обнаруживать основные службы VPN, и в этом случае сокращенная ссылка ведет пользователей на законный веб-сайт, а не перенаправляет их на вредоносную ссылку. 8. пользователь перенаправляется на сервер файлового хостинга, и автоматически загружается защищенный паролем архив, пароль для которого указывается в электронном письме или вложении, что в конечном итоге приводит к запуску трояна удаленного доступа на основе C ++ под названием BitRAT. 9. Множественные вертикали, включая правительство, финансы, здравоохранение 10. пострадали, при этом большинство целей последней кампании находилось в Колумбии. 11. APT-C-36 выбирает свои цели на основе местоположения и, скорее всего, финансового положения получателя электронной почты. 12. Конечная цель исполнителя угрозы - финансовая выгода. | | |
| **Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)**   1. rat хорош для получения полного удаленного доступа и контроля над целью. 2. Взлом хорош для военных целей. 3. Взлом может быть использован для поимки преступников | | |
| **Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)**   1. технология дает преступнику большую власть. 2. его можно было использовать для кражи денег (как в статье). 3. его можно было использовать, чтобы навредить другим людям. | | |
| **Ваши замечания, пожелания преподавателю *или* анекдот о программистах** | | |