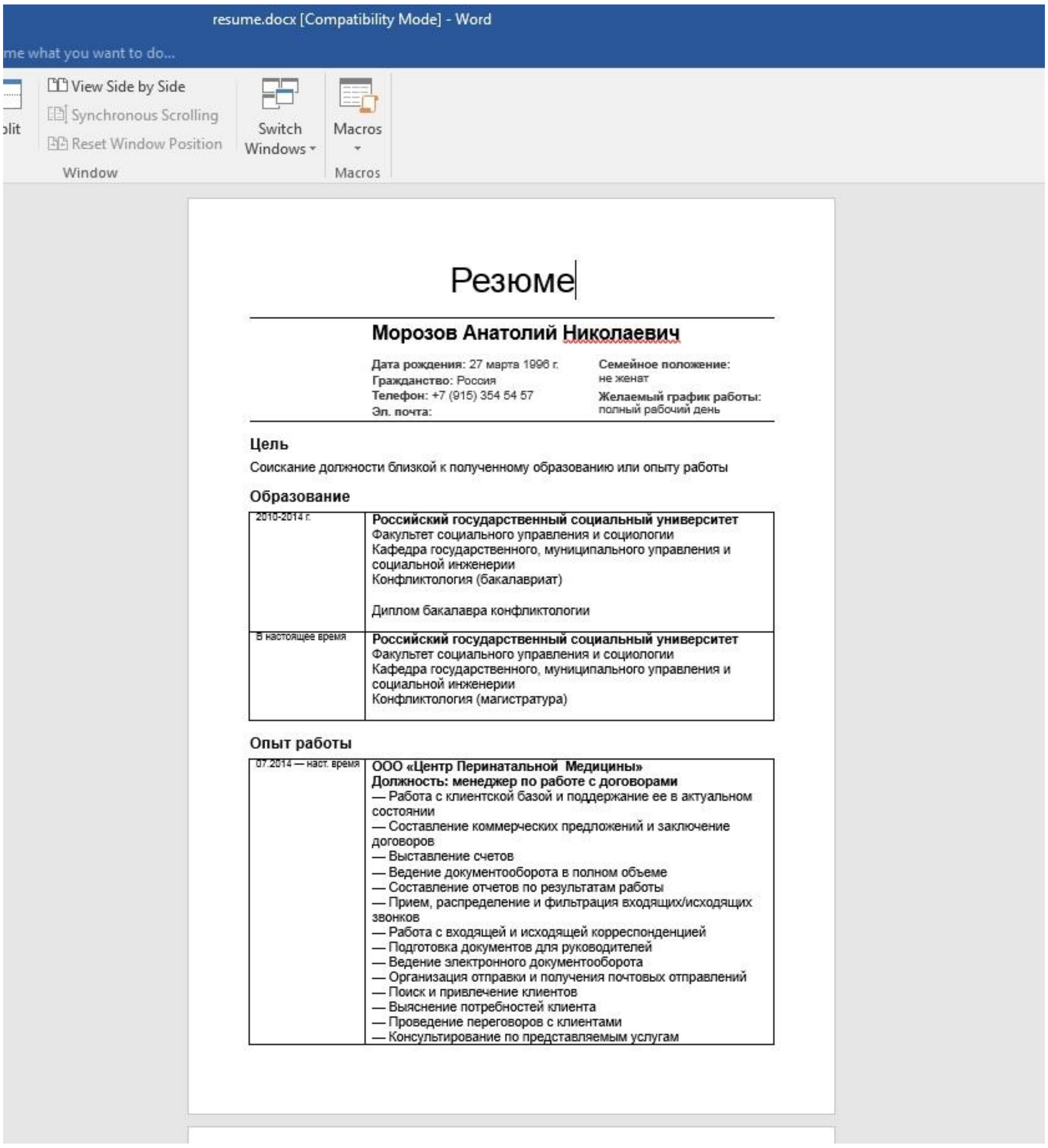
Severity

High

Analysis Summary

Gamaredon is a Russia-backed advanced persistent threat (APT) that has been operating since at least 2013. The main goal of this APT is to use the malicious document to gain control of the target machine. The exploit document uses the template injection technique to infect the victim's computer with further malware. When the document is opened, it connects to the hacker's server and downloads the payload file. Gamaredon's tools are simple and designed to collect sensitive information from hacked systems and propagate it further. Its information-gathering efforts are nearly comparable to those of a second-tier APT, whose primary purpose is to collect and disseminate information with their units.



Резюме

Морозов Анатолий Николаевич

Дата рождения: 27 марта 1996 г.
Гражданство: Россия
Телефон: +7 (915) 354 54 57
Эл. почта:

Семейное положение:
не женат
Желаемый график работы:
полный рабочий день

Цель

Соискание должности близкой к полученному образованию или опыту работы

Образование

2010-2014 г.	**Российский государственный социальный университет** Факультет социального управления и социологии Кафедра государственного, муниципального управления и социальной инженерии Конфликтология (бакалавриат) Диплом бакалавра конфликтологии
В настоящее время	**Российский государственный социальный университет** Факультет социального управления и социологии Кафедра государственного, муниципального управления и социальной инженерии Конфликтология (магистратура)

Опыт работы

07.2014 — наст. время	**ООО «Центр Перинатальной Медицины»** **Должность: менеджер по работе с договорами** — Работа с клиентской базой и поддержание ее в актуальном состоянии — Составление коммерческих предложений и заключение договоров — Выставление счетов — Ведение документооборота в полном объеме — Составление отчетов по результатам работы — Прием, распределение и фильтрация входящих/исходящих звонков — Работа с входящей и исходящей корреспонденцией — Подготовка документов для руководителей — Ведение электронного документооборота — Организация отправки и получения почтовых отправлений — Поиск и привлечение клиентов — Выяснение потребностей клиента — Проведение переговоров с клиентами — Консультирование по представляемым услугам

Impact

- Template Injection
- Exposure of Sensitive Data

Indicators of Compromise

Domain Name

- linux-techworld[.]com

Filename

- 7ZSfxMod_x86[.]exe

MD5

- 49749ee8fb2a2dab83494ab0e6cf5e7b

SHA-256

- 31f565d936ec5457b2b6b57e3e3027c15859034ecdd0887f3505a31d26ffd453

SHA-1

- 4b52a6d255ebd1ba54b2d19d3e542d697f58b07b

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.