ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА

Старая Басманная, д. 17, Москва, 105066
Тел., факс (495) 696-49-04
E-mail: postin@fstec.ru

9.04. 2024 № 240/ 91/1692

На №_____

О мерах по повышению защищенности информационной инфраструктуры Российской Федерации

Федеральным органам исполнительной власти и организациям по указателю рассылки

Анализ сведений об угрозах безопасности информации и деятельности хакерских группировок, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что хакерской группировкой Werewolves, нацеленной на российские производственные, энергетические и геологоразведочные российские компании, осуществляются фишинговые рассылки электронных писем, содержащих вредоносные .doc- и .xls-файлы, при открытии которых осуществляется внедрение вредоносного программного обеспечения Cobalt Strike Beacon. Указанные рассылки осуществляются от имени военных комиссариатов, транспортных компаний, ресторанов.

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки, необходимо принять следующие меры защиты:

производить проверку почтовых вложений с использованием средств антивирусной защиты;

проверять имя домена отправителя электронного письма в целях идентификации отправителя;

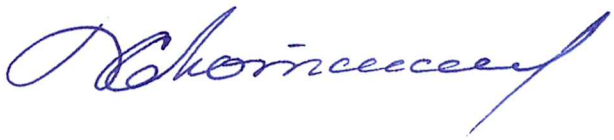
организовать получение почтовых вложений только от известных отправителей;

не открывать и не загружать почтовые вложения писем с тематикой, не относящейся к рабочей деятельности;

осуществлять работы с электронной почтой с учетных записей пользователей операционной системы с минимальными возможными привилегиями;

обеспечить на уровне периметровых средств защиты информации, ограничение обращений к следующим адресам: phod[.]ru, gays.egorvlasov[.]ru.

использовать системы обнаружения вторжений при организации доступа к сети Интернет.



В.Лютиков

Исп. и отп. Зиновьев С.И.
тел. (495) 693-68-70