Министерство жилищно-коммунального хозяйства, энергетики, цифровизации и связи Забайкальского края
Чкалова ул., д. 136, г. Чита, 672002
а/я 523
тел.: (302-2) 23 32 75
e-mail: pochta@minenergo.e-zab.ru
ОГРН 1197536003972
ИНН 7536176880, КПП 753601001

Руководителям органов местного самоуправления Забайкальского края

на № _____ от _____ г.

Уважаемые коллеги!

Согласно поступающей информации от Национального координационного центра по компьютерным инцидентам, а также от Управления ФСТЭК России по ДФО Министерство жилищно-коммунального хозяйства, энергетики, цифровизации и связи Забайкальского края (далее - Министерство) доводит до вас информацию о компьютерных атаках в отношении информационной инфраструктуры Российской Федерации путем применения методов социальной инженерии и внедрения вредоносного программного обеспечения.

Основным вектором компьютерных атак на информационную инфраструктуру Российской Федерации является электронная почта. Злоумышленники составляют убедительные адресные письма и используя техники социальной инженерии и актуальные информационные поводы, обманом заставляют пользователей загружать вредоносное программное обеспечение или вводить на фишинговых страницах (вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей) принадлежащие пользователю учётные и персональные данные, номер банковской карты и т.д.

В целях недопущения нарушения функционирования информационной инфраструктуры Российской Федерации необходимо принять следующие дополнительные меры защиты информации:

1. организовать выделенный почтовый ящик, на который работники смогут пересылать подозрительные письма для оценки риска заражения или компрометации данных, назначить ответственных из числа наиболее квалифицированных работников за анализ подозрительных писем;

2. провести обучение работников базовым мерам защиты от фишинга и социальной инженерии, а также проинформировать их о необходимости пересылки подозрительных сообщений на выделенный почтовый ящик;

3. не переходить по ссылкам и не скачивать файлы, содержащиеся в письмах электронной почты от неизвестных адресантов;

4. уточнять у известных адресантов с помощью других доступных каналов связи (телефонного звонка, сообщения в мессенджере) действительно ли они отправляли электронное письмо;

5. проверять реальные адреса гиперссылок, содержащихся в письме, особое внимание обратить на длинные ссылки, ссылки, созданные с помощью сервисов сокращения (например, bit.ly, tinyurl.com), либо на гиперссылки, привязанные к тексту;

6. считать подозрительными письма, у которых в поле «Тема» содержится призыв к действиям (например «открой», «прочитай», «ознакомься»), а также упоминаются финансы, банки, геополитическая обстановка или содержатся угрозы;

7. считать подозрительными письма, содержащие документы с макросами, архивы с паролями, а также файлы с расширениями .rtf, .lnk, .chm, .vhd;

8. считать подозрительными письма, в тексте которых содержатся орфографические ошибки, письма на иностранном языке, письма с большим количеством получателей;

9. подвергать обязательной антивирусной проверке все приходящие вложенные материалы перед открытием;

10. удостовериться, что учётная запись администратора домена защищена надёжным паролем и двухфакторной аутентификацией.

11. заблокировать техническими средствами доставку вложенных файлов со следующими расширениями: «.ade», «.adp», «.apk», «.appx», «.appxbundle», «.bat», «.cab», «.chm», «.cmd», «.com», «.cpl», «.dll», «.dmg», «.ex», «.exe», «.hta», «.ins», «.isp», «.iso», «.jar», «.js», «.jse», «.lib», «.lnk», «.mde», «.msc», «.msi», «.msix», «.msixbundle», «.msp», «.mst», «.nsh», «.pif», «.ps1», «.scr», «.sct», «.shb», «.sys», «.vb», «.vbe», «.vbs», «.vhd», «.vxd», «.wsc», «.wsf», «.wsh».

12. считать вредоносными электронные письма направленные со следующих почтовых серверов: «mx.roztec.ru», «mx.nacimibio.ru», «mail.kazkad.ru», «mlrmailer.com», «mail.mlrmailer.com», «sender-gosuslugi.ru», «mail.sender-gosuslugi.ru», «mail.gazpromlpg.ruoe.ru», «mail.npoem.ruoe.ru», «email.tpprf.ruoe.ru», «dionis.r31.rosreestr.ruoe.ru», «mx.vertical.ruoe.ru», «mail.muctr.ruoe.ru», «mail.tcm-u.ruoe.ru», «mail.it-vbc.ruoe.ru», «mail.ktrv.ruoe.ru», «mail.hi-tech.ruoe.org», «mail.acti.ruoe.ru», «mail.am-tec.ruoe.ru», «mail.sevastopolteplo.ruoe.ru», «olymp.deloports.ruoe.ru», «outlook.ekassir.uercus.com», «post.sberbank-tele.uercus.com», «mail-kras.bbr.ruoe.ru», «email.okb-nouator.ru», «mail.kronshadt.ru», «mail.tscrimea.ruoe.ru», «mail.gazpromviet.uercus.com», «mail.volnamobile.ruoe.ru», «mail.5-tv.ruoe.ra», «exchange-log.rzdlog.ruoe.ru», «mail.rossiya-airlines.uercus.com», «mail.dynasystems.ruoe.ru», «mail.ventocloud.ruoe.ru», «mail.omg.transneft.ruoe.ru»,

«mail.digital.gov.ruoe.ru», «mail.tass.ruoe.ru», «post2.interfax.ruoe.ru», «mail.iz.ruoe.ru», «app.aif.ruoe.ru», «mail.tvrain.ruoe.ru», «mail.life.ruoe.ru», «mail.vniiem.ruoe.ru», «mail.aviaremont.ruoe.ru», «smtp.mikron.ruoe.ru», «mail.kmz.ruoe.ru», «mail.vympel-ybinsk.ruoe.ru», «mail.goz.ruoe.ru», «mail.ach.gov.ruoe.ru», «mail.fadm.gov.ruoe.ru», «mail.rst.gov.ruoe.ru», «mail.minstroyrf.ruoe.ru», «mail.minobmauki.gov.ruoe.ru», «postman.rosleshoz.ruoe.ru», «mail.21.mchs.gov.ruoe.ru», «email.mkrf.ruoe.ru», «mail.knaaz.Jruoe.org», «mail.nicevt.ruoe.ru», «mail.gardatech.ruoe.ru», «mail.dtln.ruoe.ru», «webmail.planar-elements.ruoe.ru», «mxl3.ml3.ruoe.ru», «mail.informseti.ruoe.ru», «mail.cloud.mts.ruoe.ru», «exchange.avito.ruoe.ru».

Министерство просит довести данную информацию до всех подведомственных учреждений.

Министр И.В.Золотухин

Исп.: Ларионов Иван Александрович
8 (3022) 23 32 21