ФСТЭК РОССИИ
УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПО ПРИВОЛЖСКОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ

Гагарина просп., д. 60, корп. 11,
г. Нижний Новгород, 603104
тел./факс (831) 439 – 68 – 79

«24» марта 2022 г.
№ 2-2/259

Заместителю Премьер-министра
Республики Татарстан -
руководителю Аппарата Кабинета
Министров Республики Татарстан
Ш.Х.ГАФАРОВУ

О дополнительных мерах по повышению защищенности информационной инфраструктуры

Уважаемый Шамиль Хамитович!

Согласно поступившей в ФСТЭК России информации от Национального координационного центра по компьютерным инцидентам одним из векторов проведения компьютерных атак в отношении информационной инфраструктуры Российской Федерации является внедрение вредоносного программного обеспечения. Злоумышленники используют методы социальной инженерии, отправляя жертвам фишинговые электронные письма с вредоносным вложением.

Указанные электронные письма с вредоносным вложением направляются со следующих зарегистрированных 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[.]ru, 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-rybinsk.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.minobrnauki.gov.ruoe[.]ru, postman.rosleshoz.ruoe[.]ru, mail.21.mchs.gov.ruoe[.]ru, email.mkrf.ruoe[.]ru, mail.knaaz[.]ruoe.org, mail.nicevt.ruoe[.]ru, mail.gardatech.ruoe[.]ru, mail.dtln.ruoe[.]ru, webmail.planar-elements.ruoe[.]ru, mx13.m13.ruoe[.]ru, mail.informseti.ruoe[.]ru, mail.cloud.mts.ruoe[.]ru, exchange.avito.ruoe[.]ru.

В целях недопущения нарушения функционирования информационной инфраструктуры Российской Федерации, а также компрометации размещаемой информации прошу Вас дать указания на принятие следующих дополнительных мер защиты информации:

обновить базы антивирусных средств защиты до актуальных версий;

проверить журналы DNS-серверов с целью выявления обращений к указанном почтовым серверам.

С уважением,

Руководитель Управления П.Максяков

Семенычев С.М.
8 (831) 439-68-75