

ПРОМСВЯЗЬИНВЕСТ

расчетная небанковская кредитная организация

367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»

ОКПО 43340114 БИК № 048209395 корсчет 301038109820900000395

тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«06» октября 2020г.

г. Махачкала

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за сентябрь 2020 г.»

В связи с необходимостью снижения рисков воздействия вредоносного кода, рисков использования уязвимостей программного обеспечения и повышения уровня защиты информации при работе с системой дистанционного банковского обслуживания «iBank2» (Интернет-банком) служба информационной безопасности РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО) рекомендует it-специалистам наших клиентов (организаций и индивидуальных предпринимателей) применять в своей работе рекомендации по защите информации, указанные в Приложении 1 к данному письму. В случае возникновения вопросов по применению рекомендаций просим Вас позвонить в службу информационной безопасности по номеру 8 (8722) 51-70-44.

Председатель Правления



подпись

Абдурахманов К.А.

М.П.

Исп. Ирганов Ю.Г.
Руководитель СИБ
8 (8722) 62-62-39

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за сентябрь 2020 г.»

По информации **ФИНЦЕРТ** (центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, специального структурного подразделения Банка России) участились случаи распространения вредоносного программного обеспечения семейства «RTM», ориентированного на клиентов кредитно-финансовых организаций, являющихся юридическими лицами и индивидуальными предпринимателями.

URL-адреса и IP-адреса, рекомендуемые к блокировке it-специалистами организаций и индивидуальных предпринимателей через сетевые экраны, брандмауэры, сетевое оборудование	45.61.138.66 142.93.123.101 blockchain.info 104.16.54.3 104.16.55.3 api.blockcypher.com 104.20.21.251 104.20.20.251 45.61.138.66 188.166.55.131 165.232.57.172 45.61.139.207 134.209.85.152 172.86.75.52 134.122.54.113 45.61.138.210 45.61.138.91 188.166.223.168 206.166.251.226 206.189.140.215 blockchain.coinmarketcap.com 206.166.251.223 188.166.2.222
---	---

При работе с электронной почтой организациям и индивидуальным предпринимателям следует учитывать, что участились случаи отправки по электронной почте ложных писем от мошенников. Целью данных писем является распространение вредоносного кода с целью кражи денежных средств. Подобные письма содержат файлы со следующими именами:

Paket na podpis'.exe
Ves' paket na podpis'.exe
Raschet vtornik.exe
Platzhi za proshlyj mesyac.exe
Akt sverki 02.09.exe
Akt sverki za etot mesyac.exe

Dogovora sreda.exe
 Dok-ty na vozvrat konec avgusta.exe
 Dok-ty na vozvrat nachalo sentyabrya.exe
 Dokumenty na vozvrat nachalo sentyabrya.exe
 Dokumenty sreda.exe
 Pogashenie zadolzhennosti konec proshlogo mesyaca.exe
 Spisok dokumentov avgust-sentyabr'.exe
 Sverka 02.09.2020.exe
 UPD za etot mesyac.exe
 Vozvrashchenie tovara 2e sentyabrya.exe
 Vozvrat dokumentov nachalo sentyabrya.exe
 Vse dokumenty za proshlyj mesyac.exe
 Zayavka na vozvrat za avgust.exe
 Dok-ty na vozvrat avgust-sentyabr'.exe
 Akt 2e sentyabrya.exe
 Vozvrashchenie tovara za proshlyj mesyac.exe
 Zayavka za proshlyj mesyac.exe
 Zayavka 2e sentyabrya.exe
 Zayavka sreda.exe
 Doplata na proverku.exe
 Kopii dok-ov proverit'.exe
 Skany podpisat'.exe
 Sluzhebnyaya zapiska za proshlyj mesyac.exe
 Oplata po kontraktu ponedel'nik.exe
 Dokumenty na obespechenie kontrakta za 07.09.exe
 «Dok-ty za proshlyj i za etot mesyac.exe
 Vse dokumenty za sentyabr'.exe
 Dokumenty konec mesyaca 10e sentyabrya.exe
 Akt 11.09.2020.exe
 Dok-y vtornik.exe
 Dok-ty sverka 23e sentyabrya.exe

При обнаружении во входящих письмах своей электронной почты писем с файлами с подобными имени не рекомендуется открывать такие файлы и такие письма.

На компьютере, с использованием которого осуществляется работа в системе ДБО «iBank2», не рекомендуется устанавливать программное обеспечение, имеющее уязвимости с критичным уровнем опасности. К такому программному обеспечению относится программное обеспечение, указанное в таблице ниже.

№	Наименование уязвимого программного обеспечения	Идентификатор уязвимостей	Описание уязвимости	Дата выявления	Ссылка на источники	Наличие обновлений
1.	Повышение привилегий в продуктах в Cisco ENCS серии 5400-W и CSP серии 5000-W	MITRE: CVE-2020-3446	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к интерфейсу командной строки уязвимого устройства с правами администратора посредством отправки специально созданных вредоносных сетевых пакетов. Уязвимость обусловлена наличием учетных записей пользователей со статическими паролями по умолчанию.	19 августа 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-waas-encsw-cspw-cred-hZzL29A7	Есть
2.	Выполнение	MITRE: CVE-	Эксплуатация уязвимости	29 июля	https://tools.cisco.com/security/center/content/Ci	Есть

	произвольного кода в Cisco Data Center Network Manager	2020-3382	позволяет удаленному злоумышленнику выполнять произвольные действия с административными привилегиями на уязвимом устройстве посредством отправки специально созданных вредоносных сетевых пакетов. Уязвимость обусловлена использованием в разных установках статического ключа шифрования.	2020 г.	scoSecurityAdvisory/cisco-sa-dcnm-bypass-dyEejUMs	
3.	Повышение привилегий в Cisco SD-WAN	MITRE: CVE-2020-3374 CVE-2020-3375	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии, получить НСД к данным, внести изменения в систему и выполнить команды с привилегиями пользователя root в уязвимой системе посредством отправки специально созданных вредоносных сетевых пакетов. Уязвимость обусловлена некорректной проверкой входных данных.	29 июля 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uabvman-SYGzt8Bv https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdbufof-h5f5VSeL	Есть
4.	Несанкционированный доступ в Trend Micro Vulnerability Protection	MITRE: CVE-2020-15601 CVE-2020-15605	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к уязвимому приложению посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной обработкой запросов аутентификации, если включена LDAP-аутентификация.	29 июля 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020083112 https://success.trendmicro.com/solution/000252039 https://www.zerodayinitiative.com/advisories/ZDI-20-1077/ https://www.zerodayinitiative.com/advisories/ZDI-20-1083/	Есть
5.	Повышение привилегий в Windows Defender	MITRE: CVE-2020-0951	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику обойти ограничения безопасности и выполнить произвольный код в целевой системе посредством отправки PowerShell команд. Уязвимость обусловлена некорректной работой функции безопасности в Windows Defender Application Control.	8 сентября 2020 г.	https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0951 https://www.cybersecurity-help.cz/vdb/SB2020090874	Есть
6.	Множественные уязвимости в Microsoft Windows Codecs Library	MITRE: CVE-2020-1319	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного изображения. Уязвимость обусловлена некорректной обработкой изображений в Microsoft Windows Codecs Library.	8 сентября 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020090856 https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1129 https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1319	Есть
7.	Выполнение произвольного кода на сервере Microsoft Exchange	MITRE: CVE-2020-16875	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного электронного письма на сервер Exchange. Уязвимость обусловлена ошибкой граници памяти при обработке сообщений электронной почты.	8 сентября 2020 г.	https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16875 https://www.cybersecurity-help.cz/vdb/SB2020090811 https://www.thezdi.com/blog/2020/9/8/the-september-2020-security-update-review	Есть
8.	Множественные уязвимости в технологическом стандарте Microsoft COM для Windows	MITRE: CVE-2020-1507	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректным способом	8 сентября 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020090832 https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0922 https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1507	Есть

			обработки объектов в памяти в Microsoft COM.			
9.	Множественные уязвимости в Apple Safari	MITRE: CVE-2020-9948	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой данных в компоненте WebKit в браузере Apple Safari.	16 сентября 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020091802 https://support.apple.com/en-us/HT211845	Есть
10	Множественные уязвимости в Google Chrome	MITRE: CVE-2020-15965	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена смешением типов компонентом V8.	21 сентября 2020 г.	https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop_21.html	Есть
11	Множественные уязвимости в Mozilla Firefox и Firefox ESR	MITRE: CVE-2020-15678	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной работой функции APZCTreeManager::ComputeClippedCompositionBounds при обработке HTML-содержимого.	22 сентября 2020 г.	https://www.mozilla.org/en-US/security/advisories/mfsa2020-42/ https://www.mozilla.org/en-US/security/advisories/mfsa2020-43/	Есть