РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО)

01.09.2020 г. г. Махачкала

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

В связи с необходимостью снижения рисков воздействия вредоносного кода, рисков использования уязвимостей программного обеспечения и повышения уровня безопасности 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 **К.А.Абдурахманов**

Согласовано:

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за август 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	**45.61.139.16** **161.35.104.138** **blockchain.info** **104.16.54.3** **104.16.55.3** **api.blockcypher.com** **104.20.21.251** **104.20.20.251** **67.205.148.45** **45.61.136.26** **blockchain.info** **104.16.54.3** **104.16.55.3** **api.blockcypher.com** **104.20.21.251** **104.20.20.251** **142.93.0.206** **blockchain.info** **104.16.54.3** **104.16.55.3** **api.blockcypher.com** **104.20.21.251** **104.20.20.251**

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 dokumentov dlya oplaty za etot mesyac.exe
Dokumenty dlya sverki konec iyulya.exe
Sverka 13.07.2020.exe
Sverka za ves' iyul'.exe
Dok-ty sverka za ves' iyul'.exe
Dokumenty nachalo avgusta.exe

Dlya sverki chetverg.exe
Akty sverki za iyul'.exe
SDFSSvc.exe
Sverka konec proshlogo mesyaca.exe
Zakryvayushchie dokumenty za iyul'.exe
Akt sverki za ves' iyul'.exe
Paket dok-ov 31.08.exe
Kopii dok-ov na proverku.exe
Paket avgust.exe
Paket dok-ov avgust.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.	Internet Explorer 9, 11	MITRE: CVE-2020-1380	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код с привилегиями текущего пользователя в целевой системе посредством открытия пользователем специально созданных вредоносных веб-страницы или документа Microsoft Office. Уязвимость обусловлена некорректным способом обработки сценариев объектов памяти в Internet Explorer.	11 августа 2020 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1380 https://www.cybersecurity-help.cz/vdb/SB2020081114 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1567 https://www.cybersecurity-help.cz/vdb/SB2020081230	Есть
2.	Повышение привилегий в Microsoft Netlogon	MITRE: CVE-2020-1472	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально созданных сетевых пакетов и последующего подключения через удаленный протокол Netlogon (MS-NRPC) к контроллеру домена. Уязвимость обусловлена некорректной политикой безопасности в службе Netlogon.	11 августа 2020 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472 https://www.cybersecurity-help.cz/vdb/SB2020081242	Есть
3.	Множественные уязвимости в Adobe Acrobat и Adobe Reader	MITRE: CVE-2020-9722 CVE-2020-9715	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена некорректным управлением памятью при обработке PDF-файлов.	11 августа 2020 г.	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	Есть
4.	Удаленное выполнение кода в WiFi D-Link DAP-1860	MITRE: CVE-2020-15631	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированной	23 июля 2020 г.	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10185 https://nvd.nist.gov/vuln/detail/CVE-2020-15631	Есть

			команды в заголовке SOAPAction сетевого пакета. Уязвимость обусловлена некорректной обработкой сетевых пакетов службой HNAP.			
5.	Множественные уязвимости в Microsoft Windows Codecs Library	MITRE: CVE-2020-1585	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла изображения. Уязвимость обусловлена ошибкой границ памяти в библиотеке кодеков Microsoft Windows.	11 августа 2020 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1585 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1574 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1560 https://www.cybersecurity-help.cz/vdb/SB2020081209	Есть
6.	Выполнение произвольного кода в Microsoft .NET Framework	MITRE: CVE-2020-1046	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных в Microsoft .NET Framework.	11 августа 2020 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1046 https://www.cybersecurity-help.cz/vdb/SB2020081231	Есть
7.	Выполнение произвольного кода в Microsoft Outlook	MITRE: CVE-2020-1483	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти при обработке файлов в электронном письме.	11 августа 2020 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1483 https://www.cybersecurity-help.cz/vdb/SB2020081123	Есть
8.	Получение аутентификационных данных в TeamViewer Desktop для Windows	MITRE: CVE-2020-13699	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить NTLM-хэш текущего пользователя Windows и НСД к данным в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректными ограничениями пользовательских обработчиков URI в TeamViewer Desktop для Windows.	29 июля 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020081024 https://www.helpnetsecurity.com/2020/08/06/cve-2020-13699/ https://nvd.nist.gov/vuln/detail/CVE-2020-13699	Есть
9.	НСД к данным в SQLite	MITRE: CVE-2020-13630	Эксплуатация уязвимости позволяет удаленному злоумышленнику осуществить НСД к целевой системе посредством отправки специально сформированных данных приложению. Уязвимость обусловлена некорректным функционированием модуля FTS3.	6 августа 2020 г.	https://sqlite.org/src/info/0d69f76f0865f962 https://www.cybersecurity-help.cz/vdb/SB2020080601	Есть
10	Множественные уязвимости в Mozilla Thunderbird	MITRE: CVE-2020-15656	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных приложению. Уязвимость обусловлена некорректным функционированием компонента IonMonkey.	28 июля 2020 г.	https://www.mozilla.org/en-US/security/advisories/mfsa2020-33/ https://www.mozilla.org/en-US/security/advisories/mfsa2020-35/	Есть
11	Множественные уязвимости в продуктах компании Intel	MITRE: CVE-2020-8708	Эксплуатация уязвимости позволяет злоумышленнику, который находится в смежной сети, повысить свои привилегии и получить доступ к BMC-контроллеру, управляющему целевой системой, посредством отправки специально созданного	13 августа 2020 г.	https://threatpost.com/critical-intel-flaw-motherboards-server-compute-modules/158270/ https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00384.html https://vuldb.com/?id.159804 https://vuldb.com/?id.159821 https://vuldb.com/?id.159822	Есть

			вредоносного запроса. Уязвимость обусловлена некорректным механизмом аутентификации.			