РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО)

03.08.2020 г. г. Махачкала

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за июль 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) Комитет по 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 Комитет по информационной безопасности по номеру 8 (8722) 51-70-44.

Председатель Правления **К.А.Абдурахманов**

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за июль 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	**45.61.138.109** **157.245.243.44** **blockchain.info** **104.16.54.3** **104.16.55.3** **api.blockcypher.com** **104.20.21.251** **104.20.20.251** **milebgd.mycpanel.rs** **94.127.7.174** **167.172.200.71** **45.61.136.144** **fssspdocs.ru** **hxxp://www.fssspdocs.ru/Ispolnitelniy_List_218417004** **45.10.88.247** **51.77.235.233** **142.202.188.249** **142.202.188.251** **185.92.222.127** **172.105.59.15** **172.105.162.174** **172.105.59.15** **172.105.162.174** **51.38.94.172** **139.180.165.173** **139.180.128.156** **51.38.94.172** **137.74.153.125** **95.179.243.62** **45.76.18.240** **45.77.63.37** **149.28.50.148** **45.79.126.239** **45.79.121.184** **140.82.0.67** **91.200.102.242**

	45.79.126.239 45.79.121.184 172.105.48.152 172.105.63.133 45.61.136.126 45.61.139.113 45.61.139.50 45.61.138.66 139.180.214.192 45.61.136.140 91.200.102.113 45.61.136.140 45.61.139.4

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:

Vozvrashchenie tovara za proshlyj mesyac.exe
Запрос клиента 0013709.r00
Профт Групп Россия - Запрос клиента 0013709 - SKBMT-07-30-2020-115-img00251.exe
Dolg 29e iyulya.exe
Исполнительный лист №218417004.scr
Исполнительный лист №218417004.scr
Vse dokumenty konec iyunya.exe
Dlya sverki 27.07.exe
«Dokumenty 23.07.exe
Akty sverki za ves' iyun'.exe
Dokumenty 23e iyulya.exe
Dokumenty konec iyulya.exe
Dokumenty konec iyunya.exe
Sverka 23.07.exe
Sverka konec iyunya.exe
Dlya sverki konec proshlogo mesyaca.exe
Oplatit' 21.07.exe
Dlya oplaty 21.07.2020.exe
Paket dokumentov dlya oplaty 21.07.2020.exe
Na oplatu 21.07.exe
Na oplatu konec iyulya.exe
Oplatit' za iyun'.exe
Paket dokumentov dlya oplaty za iyun'.exe
Paket dokumentov dlya oplaty za etot mesyac.exe
Dokumenty na oplatu 21.07.2020.exe
Paket dokumentov dlya oplaty 21e iyulya.exe
Pasportnye dannye sotrudnikov ponedel'nik.exe
Paket dokumentov za proshlyj i za etot mesyac.exe
Vse dokumenty za proshlyj mesyac.exe
Dokumenty obshchee za 17.07.exe
Dokumenty za proshlyj i za etot mesyac.exe
Sluzhebn.zapiska za proshlyj i za etot mesyac.exe

Vse dok-ty na 17.07.exe
Dokumenty na obespechenie kontrakta iyun'-iyul'.exe
Sluzhebn.zapiska na 17.07.exe
Dokumenty na oplatu.exe
Paket 15.07.exe
Paket dokumentov vtornik.exe
Akt sverki 13.07.exe
Sluzhebn.zapiska za etot mesyac.exe
Zadolzhennost' konec iyunya.exe
Paket dokumentov za proshlyj mesyac.exe
Sverka za proshlyj mesyac.exe
Dokumenty za konec iyunya.exe
Perechen' dokumentov 30 iyunya.exe
Dokumenty zakryvayushchie za iyun'.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.	CentOS: 7	MITRE: CVE-2020-10757	Эксплуатация уязвимости позволяет локальному злоумышленнику повысить привилегии в целевой системе. Уязвимость обусловлена некорректной обработкой данных формата DAX Huge Pages компонентом mremap.	30 июля 2020 г.	https://lists.centos.org/pipermail/centos-announce/2020-July/035780.html	Есть
2.	Red Hat Process Automation Manager: 7.0.0, 7.1.0, 7.2.0, 7.3.0, 7.4.0, 7.5.0, 7.6.0, 7.7.0	MITRE: CVE-2020-9512	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании у целевой системы посредством отправки специально сформированных HTTP-пакетов. Уязвимость обусловлена некорректной обработкой HTTP/2-запросов.	29 июля 2020 г.	https://access.redhat.com/errata/RHSA-2020:3197	Есть
3.	Mozilla Thunderbird: 60.0, 60.2.1, 60.3, 60.3.0, 60.3.1, 60.3.2, 60.3.3, 60.4, 60.4.0, 60.5, 60.5.0, 60.5.1, 60.5.2, 60.5.3, 60.6.0, 60.6.1, 60.7.0, 60.7.1, 60.7.2, 60.8.0, 60.9.0, 60.9.1, 68.0, 68.1.0, 68.1.1, 68.1.2, 68.2.0, 68.2.1, 68.2.2, 68.3.0, 68.3.1, 68.4.1, 68.4.2, 68.5.0, 68.6.0, 68.7.0, 68.8.0, 68.8.1,	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

	68.9.0, 68.10.0, 78.0					
4.	TYPO3: 6.2.16, 6.2.17, 6.2.18, 6.2.19, 6.2.20, 6.2.21, 6.2.22, 6.2.23, 6.2.24, 6.2.25, 6.2.26, 6.2.27, 6.2.28, 6.2.29, 6.2.30, 6.2.31, 6.2.32, 6.2.33, 6.2.34, 6.2.35, 6.2.36, 6.2.37, 6.2.38, 6.2.38 ELTS, 6.2.39, 6.2.51 ELTS	MITRE: CVE-2020-15086 CVE-2020-15099	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить привилегии в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректным применением ограничений безопасности внутренним механизмом проверки и субкомпонентом eID API.	28 июля 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020072812 https://typo3.org/security/advisory/typo3-psa-2020-001/	Есть
5.	Google Chrome до v84.0.4147.104	MITRE: N/A N/A	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой данных формата HTML.	27 июля 2020 г.	https://chromereleases.googleblog.com/2020/07/stable-channel-update-for-desktop_27.html https://crbug.com/1105318 https://crbug.com/1102408 https://crbug.com/1102054 https://crbug.com/1096677 https://crbug.com/1104061 https://crbug.com/1105635 https://crbug.com/1106773	Есть
6.	RV110W Wireless-N VPN Firewall: 1.2.2.5 Cisco Small Business RV130 Series VPN Routers: 1.0.0.21, 1.0.1.3, 1.0.2.7, 1.0.3.14, 1.0.3.16, 1.0.3.22, 1.0.3.28, 1.0.3.44, 1.0.3.45, 1.0.3.51, 1.0.3.52, 1.2.2.5, 1.2.2.8 RV130W	MITRE: CVE-2020-3323 CVE-2020-3331	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных в веб-интерфейсе управления.	15 июля 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-AQKREqp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-code-exec-wH3BNFb https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv110w-static-cred-BMTWBWTy	Есть
7.	GLPI до v 9.5.1	MITRE: CVE-2020-15108	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный SQL-запрос к базе данных уязвимого приложения посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой предоставленных пользователем данных.	21 июля 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020072220 https://github.com/glpi-project/glpi/releases/tag/9.5.1	Есть
8.	RV110W Wireless-N VPN Firewall: 1.2.2.5 Cisco Small Business RV130 Series VPN Routers	MITRE: CVE-2020-3145 CVE-2020-3146	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе управления.	15 июля 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-m4FEEGWX https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-auth-bypass-cGv9EruZ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmd-shell-injection-9jOQn9Dy	Есть
9.	Adobe Photoshop: 20.0, 20.0.1, 20.0.2, 20.0.3, 20.0.4, 20.0.5, 20.0.6, 20.0.7, 20.0.8, 20.0.8.5,	MITRE: CVE-2020-9684 CVE-2020-9685 CVE-2020-9687	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена	21 июля 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020072118 https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	Есть

	20.0.9, 21.0.1, 21.0.2, 21.1, 21.1.1, 21.2		некорректным определением границ буфера памяти.			
10	Cisco RV340 Dual WAN Gigabit VPN Router: -, 1.0.3.17 Cisco RV340W Dual WAN Gigabit Wireless-AC VPN Router: 1.0.01.16, 1.0.01.17, 1.0.01.18, 1.0.01.20, 1.0.02.16, 1.0.03.15, 1.0.03.16, 1.0.03.17 Cisco RV345 Dual WAN Gigabit VPN Router: -, 1.0.3.17 Cisco RV345P Dual WAN Gigabit POE VPN Router: -, 1.0.3.17	MITRE: CVE-2020-3357	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных компонентом SSL VPN.	15 июля 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-dos-ZN5GvNH7 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rce-dos-9ZAjkx4	Есть
11	Cisco SD-WAN Solution до v17.2.7, 18.3.0	MITRE: CVE-2020-3351	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного вредоносного UDP-сообщения. Уязвимость обусловлена некорректной проверкой входных данных.	15 июля 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-dos-KWOdyHnB	Есть
12	Windows Server: 2008 SP2, 2008 R2 SP 1, 2012, 2012 R2, 2016, 2019, версии 1909, версии 1903, версии 2004	MITRE: CVE-2020-1350	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного DNS-запроса. Уязвимость обусловлена некорректной работой функции выделения памяти DNS-сервера.	14 июля 2020 г.	https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350 https://github.com/tinkersec/cve-2020-1350	Есть
13	Oracle WebLogic Server версий 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0.	MITRE: CVE-2020-2967	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в целевой системе посредством отправки специально сформированного запроса про протоколу IIOP. Уязвимость обусловлена некорректной проверкой входных данных в компоненте веб-службы.	15 июля 2020 г.	https://www.oracle.com/security-alerts/cpujul2020.html https://www.cybersecurity-help.cz/vdb/SB2020071683	Есть
14	Mozilla Firefox ESR до v68.10, Firefox до v78 и Thunderbird до v68.10.0.	MITRE: CVE-2020-12419	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректным обнулением указателей на ячейки буфера памяти при обработке обратных вызовов.	9 июля 2020 г.	https://nvd.nist.gov/vuln/detail/CVE-2020-12419 https://www.cybersecurity-help.cz/vdb/SB20200716124	Есть
15	Windows: 10, 10 1709, 10 1803, 10 1809, 10 1903, 10 1909, 10 2004 Windows Server: 2019, 2019 1709,	MITRE: CVE-2020-1457 CVE-2020-1425	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносной файла изображения. Уязвимость	30 июня 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020063027 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1457 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1425	Есть

	2019 1903, 2019 2004		обусловлена некорректной обработкой объектов в библиотеке Microsoft Windows Codecs.			
16	Cisco IOS XE включая v16.12.1 для Cisco Catalyst серии 9800	MITRE: CVE-2020-3221 BDU:2020-02744	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного вредоносного сетевого пакета. Уязвимость обусловлена некорректной проверкой входных данных в компоненте Flexible NetFlow v9.	3 июня 2020 г.	https://nvd.nist.gov/vuln/detail/CVE-2020-3221 https://tools.cisco.com/security/center/content /CiscoSecurityAdvisory/cisco-sa-iosxe-fnfv9-dos-HND6Fc9u	Есть
17	Mozilla Thunderbird: 60.0, 60.2.1, 60.3, 60.3.0, 60.3.1, 60.3.2, 60.3.3, 60.4, 60.4.0, 60.5, 60.5.0, 60.5.1, 60.5.2, 60.5.3, 60.6.0, 60.6.1, 60.7.0, 60.7.1, 60.7.2, 60.8.0, 60.9.0, 60.9.1, 68.0, 68.1.0, 68.1.1, 68.1.2, 68.2.0, 68.2.1, 68.2.2, 68.3.0, 68.3.1, 68.4.1, 68.4.2, 68.5.0, 68.6.0, 68.7.0, 68.8.0, 68.8.1, 68.9.0	MITRE: CVE-2020-12419 CVE-2020-12420	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректным функционированием компонента nsGlobalWindowInner.	30 июня 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020070301 https://www.mozilla.org/en-US/security/advisories/mfsa2020-26/	Есть