ТАБЛИЦА ИЗ КОМАНДНОГО ЦЕНТРА LURK Т.Е. ВСЕМИ ЭТИМИ КОМПЬЮТЕРАМИ ХАКЕРЫ МОГУТ УПРАВЛЯТЬ А ПРИ НАЛИЧИИ ДОМЕН АДМИНА ВСЕМИ ПК В СЕТИ (АБСОЛЮТНЫЙ БОЛЬШИНС

80656	25.02.2016 13:48	02.03.2016 18:20	Moscow	194.190.23.67	Windows 7 6.1.7601 Service Pack 1	Связной банк, лицензия отозвана, на комп.ах шарится агенство по страхованию вкладов. [DC: SRVDCP15V-VRN] [Domain admins: alexsim; nicely; sof; spider;]	TM4322	WS-VRN-D2429	promtorgbank.local
80657	26.02.2016 8:31	29.02.2016 10:11	Moscow	178.215.85.85	Windows Server 2008 6.0.6002 Service Pack 2	29 польз в домене http://www.profimix.ru/ - Интернет магазин стройматериалов [DC: DC] [Domain admin] [Domain admins: root; Администратор;]	Администратор	PMSERVER	profimix.local
80658	26.02.2016 9:39	19.03.2016 19:10	Togliatti	31.28.50.141	Windows Server 2008 6.0.6002 Service Pack 2		a	SEVER1C	
80659	26.02.2016 12:52	26.02.2016 13:57	Bangalore	122.172.243.240	Windows 7 6.1.7601 Service Pack 1		udupir	UDUPIR3	auth.hpicorp.net
80660	26.02.2016 14:54	26.02.2016 15:01	XX	62.75.216.24	Windows XP 5.1.2600 Service Pack 3		John2	JOHN	
80661	26.02.2016 15:06	26.02.2016 15:07	XX	62.75.216.24	Windows 7 6.1.7601 Service Pack 1		john	JOHN-PC	
80662	26.02.2016 17:13	26.02.2016 17:13	XX	62.75.216.24	Windows XP 5.1.2600 Service Pack 3		John2	JOHN	
80663	26.02.2016 18:15	27.02.2016 1:31	Saint Petersburg	84.204.84.92	Windows Server 2003 5.2.3790 Service Pack 2		юзер power	SRV-KASPER-01 !	домен szb.sbrf.local
80664	26.02.2016 21:42	19.03.2016 9:07	Maykop	178.34.201.164	Windows 7 6.1.7601 Service Pack 1		777	777-TOSH	
80665	27.02.2016 1:46	27.02.2016 22:01	Saint Petersburg	84.204.84.92	Windows Server 2003 5.2.3790 Service Pack 2	ГЛАВНЫЙ АДМИН ВСЕГО СБЕРБАНКА →	mkadmin !!!	КАСПЕР? SRV-KASPER-01	szb.sbrf.local
80666	27.02.2016 2:40	27.02.2016 [illegible]	Saint Petersburg	84.204.84.91	Windows 7 6.1.7601 Service Pack 1		smolkovas	SMOLKOV-IK	szb.sbrf.local
80667	27.02.2016 18:56	27.02.2016 21:57	XX	62.75.216.24	Windows 7 6.1.7601 Service Pack 1	[T] Не трогать ни в коем случае! Бот для теста БК	test	WIN7-X64	workdomain.com

Выкачали в 16г все исходники с софтлаба по сбере...

81144	10.03.2016 19:01	16.03.2016 10:17	XX	91.196.95.207	Windows XP 5.1.2600 Service Pack 3		USERS	ГКА20	
81145	11.03.2016 10:25	16.03.2016 18:52	Dolgoprudn yy	217.174.99.209	Windows 7 6.1.7601 Service Pack 1	https://hbs.prod-srv.local/bot/view/id/81093	lobanov	LOBANOV	softlab.ru
81146	11.03.2016 10:26	18.03.2016 9:51	Dolgoprudn yy	217.174.99.209	Windows 7 6.1.7601 Service Pack 1	https://hbs.prod-srv.local/bot/view/id/81093	Kobalkina	SALES7	softlab.ru
81147	11.03.2016 10:26	21.03.2016 5:56	Dolgoprudn yy	217.174.99.209	Windows Server 2008 R2 6.1.7601 Service Pack 1	https://hbs.prod-srv.local/bot/view/id/81093	Domain	CORE	softlab.ru
81148	11.03.2016 15:56	11.03.2016 15:56	XX	62.75.216.24	Windows XP 5.1.2600 Service Pack 3		John2	JOHN	
81149	11.03.2016 17:51	21.03.2016 5:58	Novotorssy sk	46.173.5.54	Windows 7 6.1.7600		Home	HOME-ПК	
81150	11.03.2016 18:16	21.03.2016 5:53	Dolgoprudn yy	217.174.99.194	Windows Server 2008 R2 6.1.7601 Service Pack 1		Solovyova	MIMAS	softlab.ru
81151	11.03.2016 21:55	17.03.2016 23:23	Moscow	109.252.44.76	Windows 7 6.1.7601 Service Pack 1		Елена	ЕЛЕНА-ПК	
81152	12.03.2016 15:40	12.03.2016 15:40	Moscow	213.193.20.135	Windows XP 5.1.2600 Service Pack 3		Дима	HOME-219D16174D	
81153	12.03.2016 15:59	12.03.2016 17:33	Moscow	213.193.20.135	Windows XP 5.1.2600 Service Pack 3		Дима	HOME-219D16174D	
81154	12.03.2016 16:59	21.03.2016 5:55	Togliatti	195.144.219.153	Windows Server 2008 R2 6.1.7601 Service Pack 1	tolcn.ru является поддоменом kuzrol.ru адрес: https://hbs.prod-srv.local/default/bot/view/id/76484 tolcn/habibrahimovmn h(}t81i(e ig	habibrahimovmn	DC1	tolcn.ru
81155	12.03.2016 17:39	21.03.2016 18:05	Moscow	213.193.20.135	Windows XP 5.1.2600 Service Pack 3		Дима	HOME-219D16174D	
81156	13.03.2016 1:13	16.03.2016 15:23	Krasnodar	178.34.182.46	Windows 7 6.1.7601 Service Pack 1	Не трогать Кеш	term	TERMINAL_UPDATE	

SoftLAB подрядчик сбера по разработке клиент банка для физ лиц

Domain Admin

SERVER

Приложение № 8

79460	19.02.2016 15:43	20.02.2016 16:57	Krasnodar	37.78.131.108	Windows XP 5.1.2600 Service Pack 3		Admin	MICROSOF-3B4803	
79461	19.02.2016 15:44	19.02.2016 15:44	XX	93.189.251.68	Windows XP 5.1.2600 Service Pack 3		Кузнецов	DIRECTOR	velent
79462	19.02.2016 15:44	27.02.2016 10:41	Saint Petersburg	84.204.84.94	Windows 7 6.1.7601 Service Pack 1	!!! Username : krutikova_adm * Domain : SZB.SBRF.LOCAL * Password : Atdhfkm2016 Primary user : mkadmin wdigest : Swort4fish5 Primary user : smolkov_adm wdigest : 224cHoobAb4	sbs-fedorovia	IK-VSP-01112-07	szb.sbrf.local
79463	19.02.2016 15:44	18.03.2016 23:28	Kaluga	62.148.154.208	Windows 7 6.1.7601 Service Pack 1		User	USER-ПК1	
79464	19.02.2016 15:44	20.02.2016 1:17	Izberbash	78.156.229.18	Windows 7 6.1.7601 Service Pack 1		1	1-ПК	
79465	19.02.2016 15:44	19.02.2016 16:17	XX	62.81.229.130	Windows 7 6.1.7601 Service Pack 1		mcrufor	E1003009	gruposervinform.es
79466	19.02.2016 15:44	05.03.2016 14:19	Antwerp	79.132.230.114	Windows Server 2008 R2 6.1.7601 Service Pack 1		271	WIN-9J9ITMN98BO	
79467	19.02.2016 15:44	19.02.2016 15:44	Málaga	92.58.218.68	Windows 7 6.1.7601 Service Pack 1		Lorena	LORENA-PC	
79468	19.02.2016 15:45	22.02.2016 10:36	London	195.12.23.58	Windows 7 6.1.7601 Service Pack 1		michaell	LT-JRDCN12	gondolagroup.local
79469	19.02.2016 15:45	26.02.2016 14:24	Moscow	81.200.5.169	Windows 7 6.1.7601 Service Pack 1		yluzin	SERVICE8	scgmedia.ru
79470	19.02.2016 15:45	24.02.2016 9:24	Naryan-mar	5.142.113.250	Windows XP 5.1.2600 Service Pack 3		Admin	MICROSOF-A48830	
79471	19.02.2016 15:45	01.03.2016 9:37	XX	80.79.251.2	Windows 7 6.1.7601 Service Pack 1	не смог зайти в дбо	Татьяна	ТАТЬЯНА-МХР	

Приложение № 8

	#64151, Просмотр лога keylogger-а #609930, Просмотр карточки бота #74680, Просмотр карточки бота #76484, Просмотр карточки бота #80778, Просмотр карточки бота #74881, Просмотр карточки бота #10747, Просмотр карточки бота #29857, Просмотр лога keylogger-а #1098589, Просмотр карточки бота #59345, Просмотр карточки бота #76899, Просмотр лога keylogger-а #1183489, Просмотр дампа #411313165, Боту #72470 был установлен шаблон(-ы), Просмотр карточки бота #64892, Просмотр карточки бота #80709, Просмотр карточки бота #80233, Просмотр карточки бота #59359, Просмотр карточки бота #73523, Просмотр карточки бота #77473, Просмотр дампа #409508355, Просмотр лога keylogger-а #1184729, Просмотр карточки бота #58446, Просмотр карточки бота #64222, Скачивание архива с видеозаписями бота #64750, Просмотр карточки бота #68090, Просмотр карточки бота #81016, Просмотр лога keylogger-а #1009329, Просмотр карточки видеозаписи #95764, Просмотр карточки бота #58925, Просмотр карточки бота #58463, Просмотр лога keylogger-а #1078747, Боту #63110 установлен комментарий "Buhgalter MTT - SVYAZ"', Просмотр карточки бота #64209, Просмотр карточки бота #70806, Просмотр карточки бота #13442, Просмотр карточки бота #60660, Просмотр карточки бота #59958, Просмотр лога keylogger-а #1050145, Просмотр карточки бота #81071, Просмотр карточки бота #58466, Просмотр карточки бота #58935, Просмотр лога keylogger-а #1230448, Просмотр карточки бота #52950, Боту #79462 установлен комментарий " Username : krutikova_adm * Domain : SZB.SBRF.LOCAL * Password : Atdhfkm2016 Primary user : smolkov_adm wdigest : 224cHoobAb4", Просмотр лога keylogger-а #1098588, Просмотр дампа #409508011, Просмотр карточки бота #69000, Просмотр карточки бота #60682, Просмотр карточки бота #62421, Просмотр карточки бота #63313, Просмотр дампа #373431026, Просмотр карточки бота #80665, Просмотр карточки бота #58523, Просмотр карточки бота #81164, Просмотр карточки бота #77749, Просмотр лога keylogger-а #1050268,		

МЕС корректирует комментарии

МЕС

Следователь

КОПИЯ ВЕРНА

Следственный департамент Министерство внутренних дел Российской Федерации

реверс, Просмотр карточки бота #61127, Просмотр карточки бота #62209, Просмотр карточки бота #64942, Просмотр карточки бота #80762, Удаление бота #81072, причина - реверс, Просмотр карточки бота #81280, Просмотр карточки бота #73828, Просмотр карточки бота #58841, Удаление бота #81071, причина - реверс, Просмотр карточки бота #70877, Просмотр карточки бота #80420, Удалена команда на подъем БК для бота #58345, Просмотр дампа #378379114, Просмотр карточки сервисной команды #55846, Просмотр карточки бота #58831, Просмотр карточки бота #81082, Удаление бота #81070, причина - реверс, Просмотр карточки бота #64186, Боту #64892 установлен комментарий "tovarisch.ru", Просмотр карточки бота #80726, Просмотр лога keylogger-a #1435976, Удалена команда на подъем БК для бота #59011, Просмотр карточки бота #69149, Просмотр дампа #390637350, Просмотр лога keylogger-a #1233547, Просмотр карточки бота #75177, Просмотр правила keylogger-a #392, Просмотр карточки бота #80671, Просмотр карточки бота #72047, Просмотр карточки бота #76746, Просмотр карточки бота #71006, Просмотр лога keylogger-a #1097834, Просмотр карточки бота #81018, Просмотр карточки сервисной команды #56396, Просмотр карточки бота #58910, Просмотр карточки бота #60678, Просмотр дампа #405617107, Просмотр карточки бота #60167, Просмотр карточки бота #58881, Боту #58655 был установлен шаблон(-ы), Просмотр лога keylogger-a #1233546, Просмотр дампа #395190379, Просмотр карточки бота #60244, Просмотр карточки сервисной команды #46992, Просмотр лога keylogger-a #1133562, Просмотр карточки бота #58906, Просмотр лога keylogger-a #1238167, Просмотр карточки бота #71355, Просмотр карточки бота #65601, Боту #79462 установлен комментарий " Username : krutikova_adm * Domain : SZB.SBRF.LOCAL * Password : Atdhfkm2016", Удаление бота #81094, причина - , Просмотр лога keylogger-a #1097832, Просмотр лога keylogger-a #1185350, Просмотр карточки бота #58846, Просмотр карточки бота #60846,

МЕС

МЕС корректирует коммент

КОПИЯ ВЕРНА

Следователь

Следственный департамент Министерства внутренних дел Российской Федерации

Отчет действий в командном центре LURK по нику

МЕС

#70455, Просмотр карточки бота #61995, Просмотр карточки сервисной команды #39793, Просмотр карточки бота #80783, Просмотр дампа #425671882, Просмотр карточки бота #63396, Боту #59775 был установлен шаблон(-ы), Просмотр карточки бота #81069, Просмотр карточки бота #63370, Просмотр карточки сервисной команды #39797, Просмотр лога keylogger-a #1133339, Просмотр карточки бота #61737, Удалена команда на подъем БК для бота #62616, Просмотр карточки бота #62773, Просмотр карточки бота #67760, Просмотр карточки бота #74887, Просмотр карточки бота #63970, Просмотр карточки бота #65356, Просмотр карточки бота #65450, Просмотр лога keylogger-a #1253355, Просмотр карточки бота #62698, Просмотр карточки бота #77798, Просмотр карточки бота #60197, Просмотр карточки бота #62684, Просмотр карточки бота #56384, Просмотр дампа #407231265, Просмотр дампа #400509053, Просмотр карточки бота #61990, Просмотр карточки бота #69204, Просмотр карточки бота #59517, Просмотр карточки бота #65638, Бот#75177 добавлен в список важных, Просмотр карточки бота #63051, Бот#77730 добавлен в список важных, Просмотр карточки бота #57714, Удалена команда на подъем БК для бота #64142, Бот#80734 добавлен в список важных, Просмотр карточки бота #67776, Просмотр карточки бота #81216, Просмотр карточки бота #74971, Просмотр карточки бота #67765, Просмотр карточки бота #81556, Просмотр карточки бота #63284, Просмотр карточки бота #62679, Просмотр карточки бота #77713, Добавлена сервисная команда 'back_connect' для бота #55351. Параметры:, Просмотр дампа #401737257, Боту #55984 был установлен шаблон(-ы), Просмотр карточки бота #66060, Боту #79462 установлен комментарий " Username : krutikova_adm * Domain : SZB.SBRF.LOCAL * Password : Atdhfkm2016 Primary user : mkadmin wdigest : Swort4fish5 Primary user : smolkov_adm wdigest : 224cHoobAb4", Удаление бота #80619, причина - реверс, Просмотр карточки бота #66758, Удалена команда на подъем БК для бота #80874, Просмотр

МЕС внес в командный центр Lurk комментарии содержащий Domain Admin сборы

Приложение № 7

Копия верна

#16330, Просмотр карточки холдера #16395, Боту #58593 был установлен шаблон(-ы), Просмотр карточки бота #60239, Просмотр лога keylogger-а #1199742, Просмотр карточки бота #69513, Просмотр карточки бота #69402, Просмотр карточки бота #71055, Просмотр карточки холдера #18490, Просмотр карточки лога демона #72110514, Просмотр дампа #382656482, Просмотр карточки бота #70716, Боту #81649 установлен комментарий "SKYLAB\ZeleninNA Kjkinj15Hfvbym", Просмотр карточки бота #57105, Боту #48899 установлен комментарий "АО "СберБанк лизинг" [DC: SRV-DC04] [Domain admins: adm.bushnev.sa; adm.dzyubenko.vs; adm.orlov.ag; adm.sapunov.ia; dzyubenko.vs; swLDAP; swscan;] RDleas\adm.orlov.ag S0nsh1ne1", Боту #60589 был установлен шаблон(-ы), Добавлена сервисная команда 'back_connect' для бота #43915. Параметры:, Просмотр карточки бота #81551, Просмотр карточки бота #59183, Добавлена сервисная команда 'back_connect' для бота #46300. Параметры:, Просмотр карточки бота #73125, Боту #60464 установлен комментарий "IP: 192.168.24.133 [Отдел информационной безопасности] Ведущий специалист Чубик Евгений Викторович password: aw3ngrSP password: Zsd5yi9L -> 79.175.45.39:52302 WebCam (root/Sbvideo_Depo) Ведущий специалист отдела информационной безопасности 172.16.0.12 sa WlwKFmby1YFnHgBRI7n7", Просмотр карточки бота #62112, Боту #77691 был установлен шаблон(-ы), Просмотр дампа #372526118, Боту #55415 установлен комментарий "dgolub Project013 27 psexec 34 - zip Монетка Департамент IT", Просмотр карточки бота #77770, Просмотр дампа #375598120, Просмотр карточки бота #74304, Добавлена сервисная команда 'back_connect' для бота #62169. Параметры:, Удален пользователь с логином - Oper3, Просмотр карточки холдера #19028, Просмотр карточки холдера #19959, Бот #53362 был отправлен обратно на сортировку, Боту #65814 установлен комментарий " RDP Пашет Zero0Night", Добавлена сервисная команда 'set_video_capture' для бота #60095. Параметры:,

Домен Админ
на
СберБанк лизинг

Приложение № 7

КОПИЯ ВЕРНА