Runs in the Family: Malware Family Variants Identification through API Sequence and Frequency Analysis

Aaron Walker*, Raj Mani Shukla†, Tapadhir Das* and Shamik Sengupta*
*Department of Computer Science and Engineering, University of Nevada, Reno, USA
†Department of Computer Science University of Bristol, UK
Email: awalker@unr.edu,raj.shukla@bristol.ac.uk tapadhird@nevada.unr.edu, ssengupta@unr.edu

***Abstract*—Malware may be classified into various families according to several factors, such as the method of delivery to an infected computing system, behaviors performed by the malware on an infected system, or through the presence of key characteristics which can be recognized through malware signatures. Additionally, a given malware family may be comprised of many variants which perform similarly on an infected system yet differ from each other in some discernible way. In this paper we show that understanding this difference in malware behavior among variants of the same malware family is possible through analysis of Windows API system call sequences and the related frequencies. This allows for the identification of changes in malware variant behavior and illustrates the relationships between malware families.**

***Index Terms*—Malware Analysis, Dynamic Analysis, Malware Signature, Behavior Analysis, Fingerprinting, Sequence Analysis**

I. Appendix

Malicious software, comes in many varieties such as a virus, trojan, or worm. These varieties represent the nature of how a given malware intends to infect a system, such as through hiding inside an otherwise benign software application or self-replication throughout a system of networked computing devices. Within these malware types there exist many diverse groups of malicious software which perform certain behaviors on an infected system, such as keyloggers and banking trojans which intend to steal sensitive information about a user such as passwords and financial information. These malware groups can be classified through similar behavior into families, similar to the taxonomy of animal and plant families as described through biology. Therefore many varieties or families of banking trojans can be identified according to similar behavior or unique characteristics which clearly differentiate one such banking trojan family from another.

The lack of distinction in the behaviors performed by variants of the same malware family frustrate efforts to fingerprint malware family variants. However, in this paper we show how the similarities between malware variants can be analyzed to verify the relationships in behavior to observe generational changes. Additionally, our methodology describes a process for verifying the derivation relationships between malware so as to promote a more complete malware phylogeny.

The following section illustrates the extensive results of our experiments in the form of tables and figures describing Windows API frequency analysis of related malware family variants and API sequence cosine similarity.

II. Tables and Figures

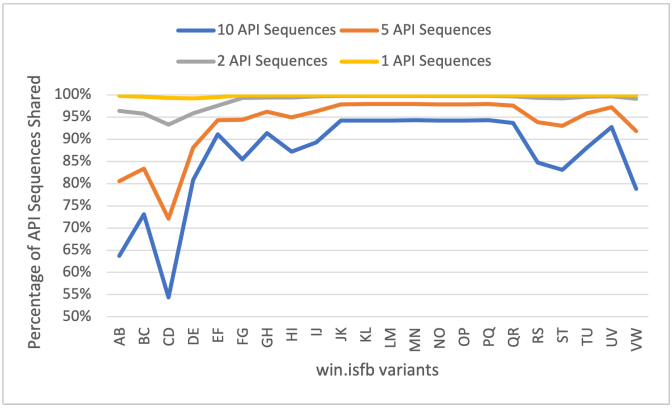

Fig. 1. Duplicate API Sequence Comparison for win.isfb Family

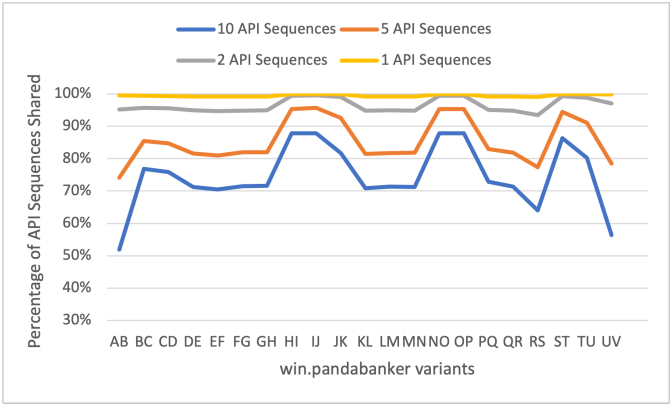

Fig. 2. Duplicate API Sequence Comparison for win.pandabanker Family

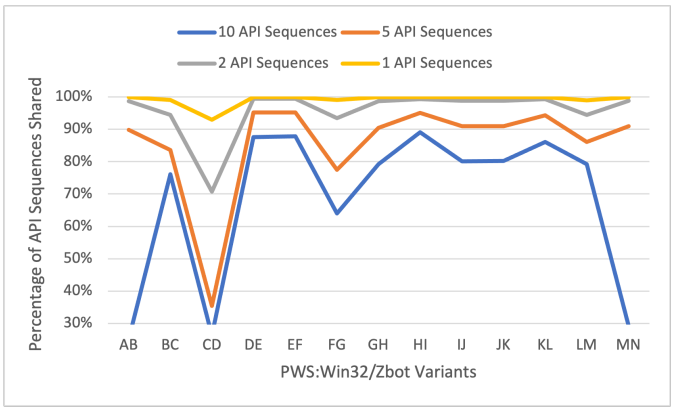

Fig. 3. Duplicate API Sequence Comparison for PWS:Win32/Zbot Family

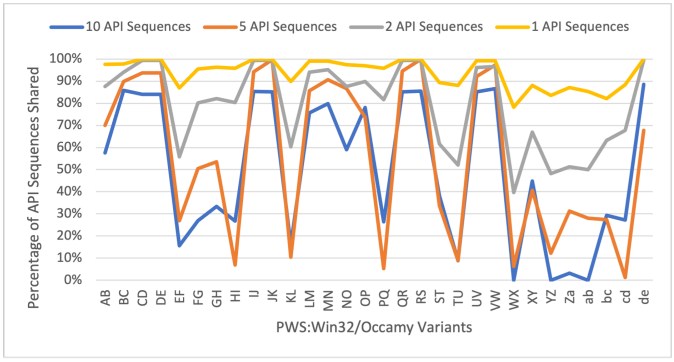

Fig. 4. Duplicate API Sequence Comparison for Trojan.Win32/Occamy Family

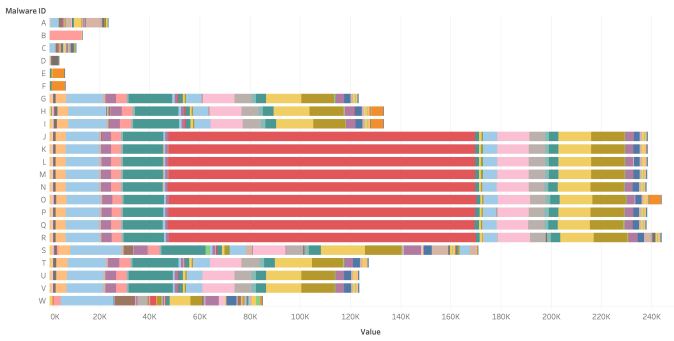

Fig. 5. API Frequencies for win.isfb

Fig. 6. API Legend for Frequency Graphs

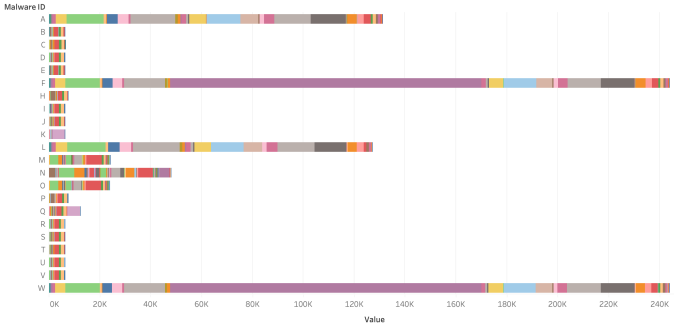

Fig. 7. API Frequencies for win.pandabanker

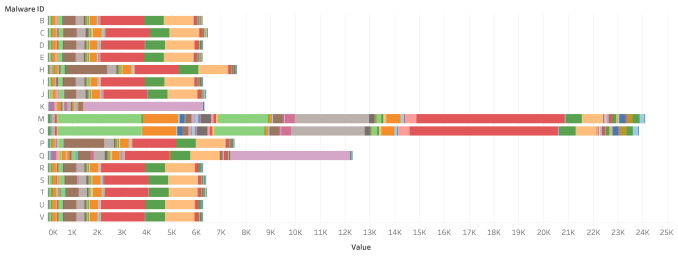

Fig. 8. API Frequencies for win.pandabanker with exclusions

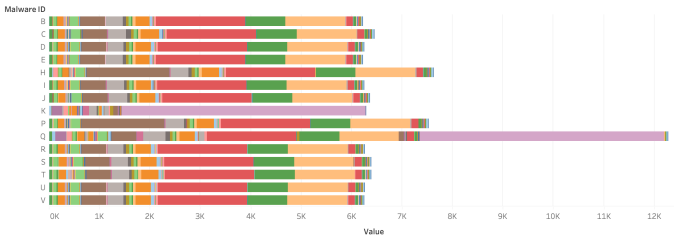

Fig. 9. API Frequencies for win.pandabanker with further exclusions

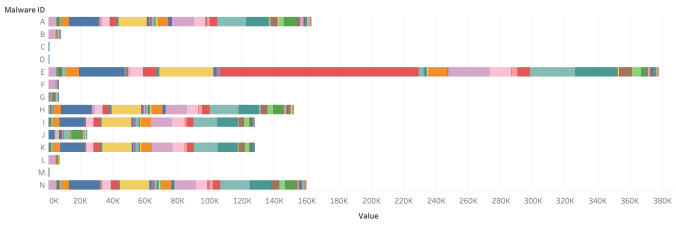

Fig. 10. API Frequencies for PWS:Win32/Zbot

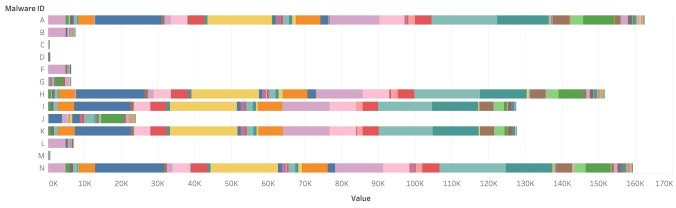

Fig. 11. API Frequencies for PWS:Win32/Zbot with exclusions

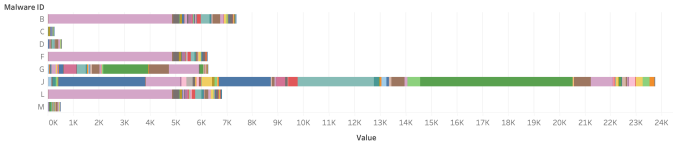

Fig. 12. API Frequencies for PWS:Win32/Zbot with further exclusions

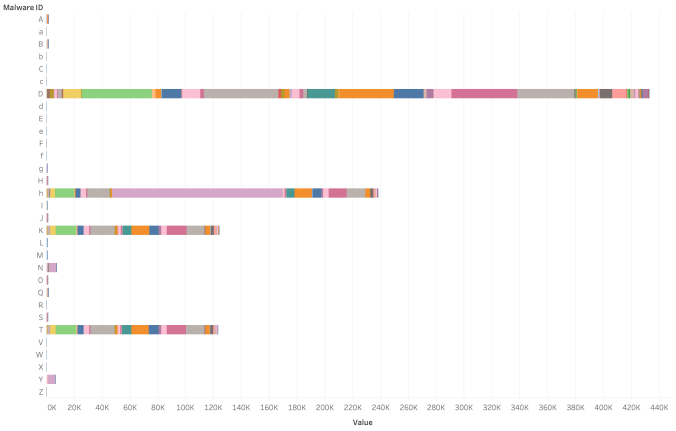

Fig. 13. API Frequencies for Trojan:Win32/Occamy

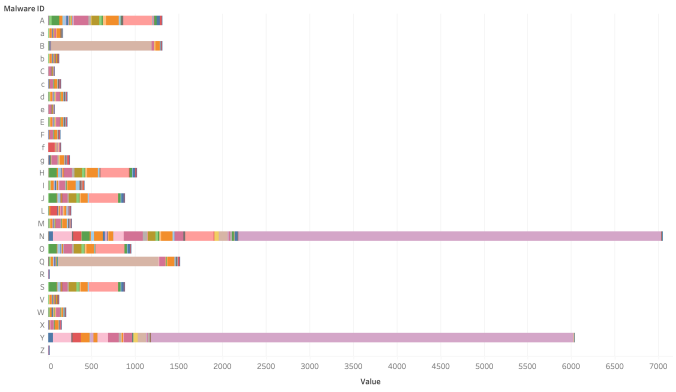

Fig. 14. API Frequencies for Trojan:Win32/Occamy with exclusions

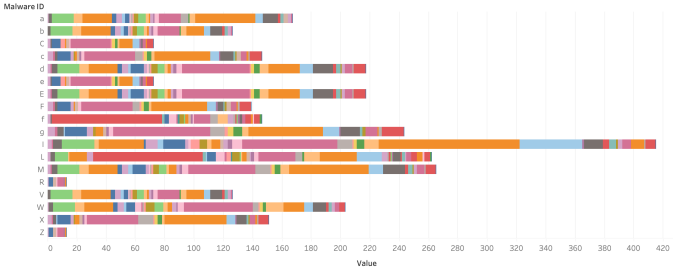

Fig. 15. API Frequencies for Trojan:Win32/Occamy with further exclusions

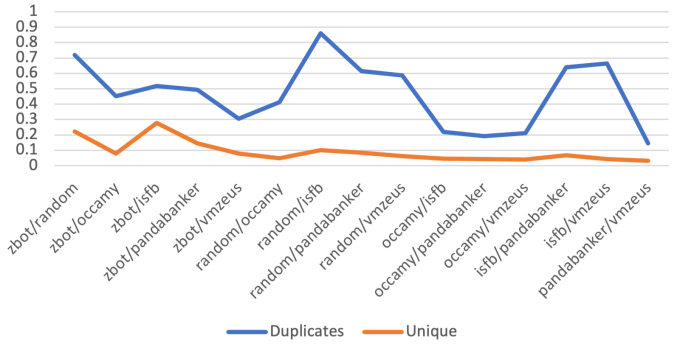

Fig. 16. Cosine Similarity for 10 API Sequences

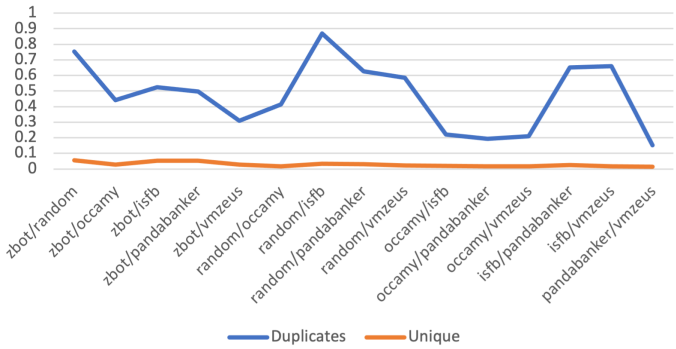

Fig. 17. Cosine Similarity for 5 API Sequences

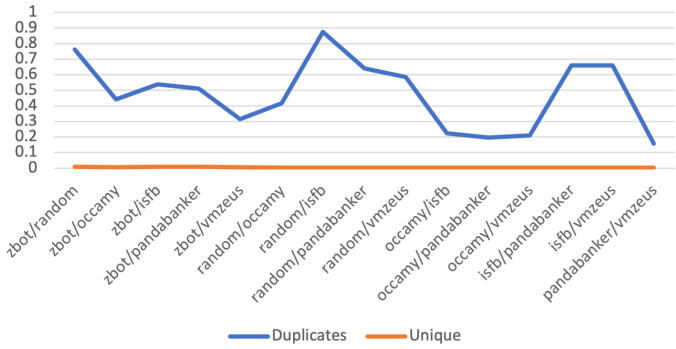

Fig. 18. Cosine Similarity for 2 API Sequences

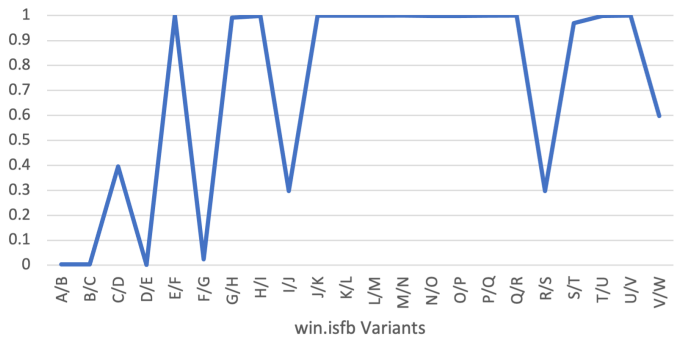

Fig. 19. API Frequency Cosine Similarity for win.isfb family

TABLE I
SAMPLE WIN.ISFB FAMILY COMPARISON FOR DUPLICATE AND UNIQUE API SEQUENCES

	10 APIs	
	Duplicates	Unique
(A) win.isfb.2014-07-23-v2.12.265	2730	1515
(B) win.isfb.2014-09-23-v2.12.308		36
(B) win.isfb.2014-09-23-v2.12.308	1901	34
(C) win.isfb.2015-04-13-v2.13.551		664
(C) win.isfb.2015-04-13-v2.13.551	902	658
(D) win.isfb.2015-05-06-v2.11.566		100

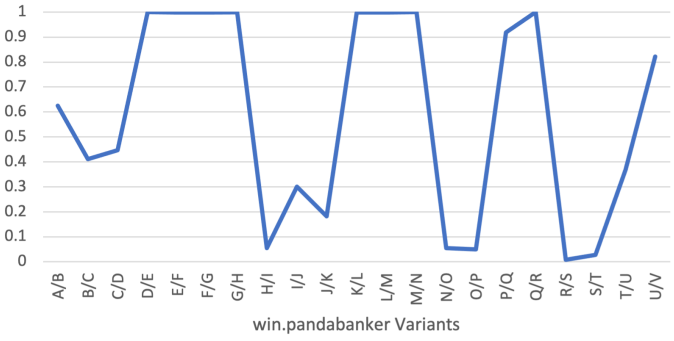

Fig. 20. API Frequency Cosine Similarity for win.pandabanker family

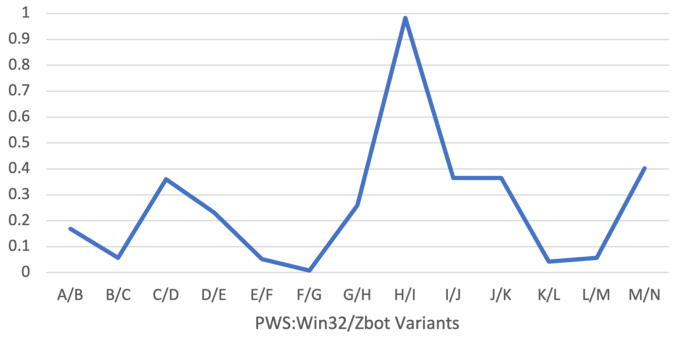

Fig. 21. API Frequency Cosine Similarity for PWS:Win32/Zbot family

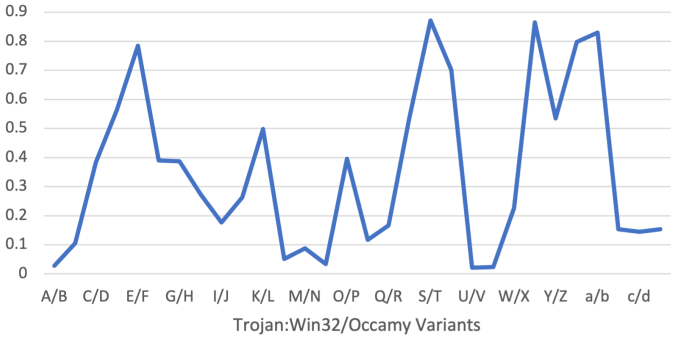

Fig. 22. API Frequency Cosine Similarity for Trojan:Win32/Occamy family

TABLE II
COMPARISON OF MALPEDIA LABELS AND MICROSOFT AV SIGNATURE

Malpedia Label	Microsoft Label
win.isfb	Program:Win32/Wacapew
	PUA:Win32/LoadMoney
	PUA:Win32/Papras
	PWS:Win32/Zbot!rfn
	Ransom:Win32/Enestaller
	Trojan:Script/Phonzy
	Trojan:Win32/Casdet!rfn
	Trojan:Win32/Casur
	Trojan:Win32/Dynamer!ac
	Trojan:Win32/Gozi
	Trojan:Win32/Occamy
	Trojan:Win32/Skeeyah
	Trojan:Win32/Tiggre!rfn
	Trojan:Win32/Ursnif
	Trojan:Win32/Wacatac
	TrojanDownloader:Win32/Beebone
	TrojanSpy:Win32/Skeeyah
	TrojanSpy:Win32/Ursnif
win.pandabanker	Trojan:Win32/Dynamer!ac
	Trojan:Win32/Matta
	PWS:Win32/Zbot
	Trojan:Win32/Skeeyah
	VirTool:Win32/VBInject
	VirTool:Win32/Injector
	Trojan:Win32/Casur
	DDoS:Win32/Nitol
	TrojanDownloader:Win32/Macapy
	Trojan:Win32/Chesir
	Trojan:Win32/Vagger
	Trojan:Win32/Zuepan
	Trojan:Win32/Sonoko.A!rfn
	Trojan:Win32/Tiggre!rfn
	Trojan:Win32/Occamy
	Ransom:Win32/GandCrab

TABLE III
COMPARISON OF MICROSOFT AV SIGNATURE AND MALPEDIA LABELS

Microsoft Label	Malpedia Label	
PWS:Win32/Zbot	win.citadel	win.pandabanker
	win.dispenserxfs	win.rerdom
	win.floki.bot	win.vmzeus
	win.gameover	win.zeus.action
	win.isfb	win.zitmo
	win.kins	
Trojan:Win32/Occamy	win.404keylogger	win.lookback
	win.8t.dropper	win.mbrlocker
	win.acridrain	win.nymaim2
	win.adkoob	win.oni
	win.afrodita	win.oski
	win.agent.tesla	win.ozh.rat
	win.anel	win.pandabanker
	win.artra	win.pekraut
	win.atmosphere	win.poulight.stealer
	win.aurora	win.psix
	win.ave.maria	win.psix.modules
	win.azorult	win.pslogger
	win.balkan.door	win.pss
	win.cloudeye	win.purplefox
	win.cryptic.convo	win.pylocky
	win.cursed.murderer	win.qulab
	win.dadjoke	win.raccoon
	win.dadstache	win.ramsay
	win.dispcashbr	win.rcs.scout
	win.doublefantasy	win.redpepper
	win.dridex	win.remexi
	win.dualtoy	win.retefe
	win.electricfish	win.sappycache
	win.evilnum	win.silence
	win.farseer	win.smanager
	win.fastloader	win.smokeloader
	win.fct	win.socelars
	win.fileice.ransom	win.sombrat
	win.galaxyloader	win.syscon
	win.grandoreiro	win.sysraw
	win.grandsteal	win.tflower
	win.himera.loader	win.tinynuke
	win.hotcroissant	win.tonedeaf
	win.http.troy	win.typehash
	win.hyperssl	win.valuevault
	win.immortal.stealer	win.vawtrak
	win.isfb	win.webmonitor
	win.kardonloader	win.wscspl
	win.kikothac	win.xagent
	win.kimsuky	win.xpertrat
	win.komprogo	win.yty
	win.kronos	win.zebrocy
	win.laturo	win.zloader

TABLE IV
WIN.ISFB FAMILY COMPARISON FOR DUPLICATE AND UNIQUE API SEQUENCES

	10 APIs		5 APIs		2 APIs		1 API	
	Duplicates	Unique	Duplicates	Unique	Duplicates	Unique	Duplicates	Unique
(A) win.isfb.2014-07-23-v2.12.265	2730	1515	6899	1599	20625	693	42659	69
(B) win.isfb.2014-09-23-v2.12.308		36		59		70		42
(B) win.isfb.2014-09-23-v2.12.308	1901	34	4330	46	12436	35	25852	3
(C) win.isfb.2015-04-13-v2.13.551		664		818		510		101
(C) win.isfb.2015-04-13-v2.13.551	902	658	2392	801	7731	460	16465	60
(D) win.isfb.2015-05-06-v2.11.566		100		124		97		47
(D) win.isfb.2015-05-06-v2.11.566	792	99	1726	122	4687	84	9700	23
(E) win.isfb.2015-05-14-v2.12.578		89		110		119		54
(E) win.isfb.2015-05-14-v2.12.578	1127	8	2331	11	6025	13	12277	7
(F) win.isfb.2015-09-02-v2.14.674		102		129		134		56
(F) win.isfb.2015-09-02-v2.14.674	13171	100	29063	123	76459	91	153882	24
(G) win.isfb.2015-09-17-v2.04.439		2130		1612		438		66
(G) win.isfb.2015-09-17-v2.04.439	28006	0	58950	0	152300	0	306130	0
(H) win.isfb.2015-09-17-v2.14.686		2624		2307		836		138
(H) win.isfb.2015-09-17-v2.14.686	27672	1908	60288	1474	157776	426	317240	56
(I) win.isfb.2016-04-18-v2.14.783		2162		1718		491		84
(I) win.isfb.2016-04-18-v2.14.783	37480	1489	80801	953	209051	141	419352	17
(J) win.isfb.2016-06-15-v2.16.831		2980		2140		537		83
(J) win.isfb.2016-06-15-v2.16.831	49112	31	102051	51	260024	25	521059	17
(K) win.isfb.2016-07-23-v2.16.843		2976		2130		526		81
(K) win.isfb.2016-07-23-v2.16.843	49132	7	102081	13	260027	9	521032	0
(L) win.isfb.2016-07-27-v2.16.843		2978		2132		525		82
(L) win.isfb.2016-07-27-v2.16.843	49111	30	102048	45	259978	21	520951	3
(M) win.isfb.2016-08-09-v2.16.849		249		205		114		46
(M) win.isfb.2016-08-09-v2.16.849	49091	21	102000	29	259802	35	520583	12
(N) win.isfb.2016-09-12-v2.16.861		2959		2107		499		73
(N) win.isfb.2016-09-12-v2.16.861	49597	15	103068	24	262651	16	526346	5
(O) win.isfb.2016-09-16-v2.14.721		3037		2199		554		85
(O) win.isfb.2016-09-16-v2.14.721	49602	92	103088	112	262712	62	526475	13
(P) win.isfb.2016-10-10-v2.16.881		2968		2116		511		75
(P) win.isfb.2016-10-10-v2.16.881	49077	24	101970	35	259707	32	520364	10
(Q) win.isfb.2016-11-01-v2.16.887		2948		2086		484		66
(Q) win.isfb.2016-11-01-v2.16.887	49375	4	102843	5	262725	7	526826	0
(R) win.isfb.2017-03-27-v2.16.935		3322		2547		746		125
(R) win.isfb.2017-03-27-v2.16.935	39870	2575	88258	1691	233581	248	470028	10
(S) win.isfb.2018-07-31-v2.17.016		4580		4095		1273		163
(S) win.isfb.2018-07-31-v2.17.016	29603	3940	66282	3347	176772	919	356073	97
(T) win.isfb.2018-10-04-v2.18.001		2083		1620		430		69
(T) win.isfb.2018-10-04-v2.18.001	26499	1441	57650	880	149832	85	300651	0
(U) win.isfb.2018-10-22-v2.17.038		2134		1615		445		70
(U) win.isfb.2018-10-22-v2.17.038	27423	6	57498	6	14734	11	295602	7
(V) win.isfb.2019-03-08-v2.17.xxx		2141		1633		454		68
(V) win.isfb.2019-03-08-v2.17.xxx	19323	2136	45024	1591	121508	320	244912	11
(W) win.isfb.2020-06-03-v3.0.898-rm3.loader		3046		2392		687		106

TABLE V
PWS:WIN32/ZBOT FAMILY COMPARISON FOR DUPLICATE AND UNIQUE API SEQUENCES

	10 APIs		5 APIs		2 APIs		1 API	
	Duplicates	Unique	Duplicates	Unique	Duplicates	Unique	Duplicates	Unique
(A) PWS:Win32/Zbot	15533	4436	36171	3849	99279	1106	200975	94
(B) PWS:Win32/Zbot!CI		163		221		193		67
(B) PWS:Win32/Zbot!CI	575	161	1255	215	3536	153	7409	29
(C) PWS:Win32/Zbot!MTB		19		31		53		39
(C) PWS:Win32/Zbot!MTB	20	18	52	28	256	25	7409	29
(D) PWS:Win32/Zbot!VM		19		31		53		39
(D) PWS:Win32/Zbot!VMn	37381	11	81161	15	211994	7	426218	0
(E) PWS:Win32/Zbot!rfn		5257		4108		1196		164
(E) PWS:Win32/Zbot!rfn	37954	5166	82307	3990	214846	1068	431918	112
(F) PWS:Win32/Zbot.ADW		98		126		133		52
(F) PWS:Win32/Zbot.ADW	835	86	2018	101	6084	86	12893	16
(G) PWS:Win32/Zbot.GOW!bit		384		486		338		104
(G) PWS:Win32/Zbot.GOW!bit	15108	294	34488	296	94045	113	190345	23
(H) PWS:Win32/Zbot.GOY!bit		3653		3319		1091		124
(H) PWS:Win32/Zbot.GOY!bit	30024	1551	64043	1657	167350	626	336765	49
(I) PWS:Win32/Zbot.gen!AJ		2120		1683		472		75
(I) PWS:Win32/Zbot.gen!AJ	14696	2114	33369	1651	90583	324	183201	10
(J) PWS:Win32/Zbot.gen!AO		1525		1647		755		111
(J) PWS:Win32/Zbot.gen!AO	14715	1517	33407	1611	90662	607	183362	48
(K) PWS:Win32/Zbot.gen!AP		2121		1683		477		79
(K) PWS:Win32/Zbot.gen!AP	13793	2084	30223	1617	79506	367	160004	27
(L) PWS:Win32/Zbot.gen!CI		140		185		178		65
(L) PWS:Win32/Zbot.gen!CI	572	121	1237	149	3379	131	7075	31
(M) PWS:Win32/Zbot.gen!VM		29		50		68		46
(M) PWS:Win32/Zbot.gen!VM	15409	7	34902	10	94713	10	191583	7
(N) PWS:Win32/Zbot.gen!Y		37367		3441		1143		133

TABLE VI
WIN.PANDABANKER FAMILY COMPARISON FOR DUPLICATE AND UNIQUE API SEQUENCES

	10 APIs		5 APIs		2 APIs		1 API	
	Duplicates	Unique	Duplicates	Unique	Duplicates	Unique	Duplicates	Unique
(A) win.pandabanker.2016-09-21-v2.2.8	1989	1449	5670	1492	18223	549	38114	30
(B) win.pandabanker.2017-01-25-v2.2.13		392		491		356		108
(B) win.pandabanker.2017-01-25-v2.2.13	1612	19	3578	23	10011	18	20780	4
(C) win.pandabanker.2017-02-15-v2.2.14		465		584		427		122
(C) win.pandabanker.2017-02-15-v2.2.14	1495	92	3338	113	9408	91	19548	18
(D) win.pandabanker.2017-03-09-v2.3.1		384		4186		338		104
(D) win.pandabanker.2017-03-09-v2.3.1	984	0	2252	0	6540	0	13676	0
(E) win.pandabanker.2017-03-15-v2.3.2		397		506		351		106
(E) win.pandabanker.2017-03-15-v2.3.2	984	23	2259	38	6603	19	13834	1
(F) win.pandabanker.2017-04-20-v2.3.3		390		494		351		107
(F) win.pandabanker.2017-04-20-v2.3.3	989	16	2266	25	6555	20	13705	3
(G) win.pandabanker.2017-05-04-v2.3.4		379		474		333		104
(G) win.pandabanker.2017-05-04-v2.3.4	979	5	2239	7	6483	0	13538	0
(H) win.pandabanker.2017-06-06-v2.4.1		384		485		340		104
(H) win.pandabanker.2017-06-06-v2.4.1	24049	0	52185	0	136102	0	273574	0
(I) win.pandabanker.2017-06-16-v2.4.2		3326		2558		749		123
(I) win.pandabanker.2017-06-16-v2.4.2	37200	1806	81008	1092	210796	94	423149	0
(J) win.pandabanker.2017-07-19-v2.4.3		3326		2558		749		123
(J) win.pandabanker.2017-07-19-v2.4.3	13341	2599	30236	1923	80854	397	163046	18
(K) win.pandabanker.2017-08-29-v2.5.0		381		478		336		105
(K) win.pandabanker.2017-08-29-v2.5.0	979	7	2247	7	6535	5	13665	1
(L) win.pandabanker.2017-08-30-v2.5.1		396		504		348		105
(L) win.pandabanker.2017-08-30-v2.5.1	990	12	2262	19	6561	8	13708	1
(M) win.pandabanker.2017-09-07-v2.5.2		384		485		340		104
(M) win.pandabanker.2017-09-07-v2.5.2	972	11	2227	17	6450	13	13489	0
(N) win.pandabanker.2017-09-29-v2.5.5		381		478		336		105
(N) win.pandabanker.2017-09-29-v2.5.5	24050	8	52197	10	136137	9	273656	1
(O) win.pandabanker.2017-10-16-v2.5.6		3327		2555		751		130
(O) win.pandabanker.2017-10-16-v2.5.6	24179	2948	52460	2082	136814	410	275021	18
(P) win.pandabanker.2017-10-25-v2.5.7		396		494		358		115
(P) win.pandabanker.2017-10-25-v2.5.7	1094	24	2484	29	7111	29	14837	10
(Q) win.pandabanker.2017-12-04-v2.6.0		383		482		341		108
(Q) win.pandabanker.2017-12-04-v2.6.0	984	0	2252	0	6517	0	13630	0
(R) win.pandabanker.2017-12-07-v2.6.1		394		499		354		108
(R) win.pandabanker.2017-12-07-v2.6.1	847	380	2045	472	6166	306	13067	72
(S) win.pandabanker.2018-02-14-v2.6.4		97		125		126		52
(S) win.pandabanker.2018-02-14-v2.6.4	13749	83	30107	99	79126	57	159163	16
(T) win.pandabanker.2018-04-18-v2.6.7		2097		1647		444		69
(T) win.pandabanker.2018-04-18-v2.6.7	14721	2078	33413	1597	90662	303	183350	11
(U) win.pandabanker.2018-04-20-v2.6.8		1552		1688		774		112
(U) win.pandabanker.2018-04-20-v2.6.8	4879	1287	13581	1160	41961	300	86302	11
(V) win.pandabanker.2018-05-31-2.6.10		2486		2557		978		160

TABLE VII
TROJAN.WIN32/OCCAMY FAMILY COMPARISON FOR DUPLICATE AND UNIQUE API SEQUENCES

	10 APIs		5 APIs		2 APIs		1 API	
	Duplicates	Unique	Duplicates	Unique	Duplicates	Unique	Duplicates	Unique
(A) Trojan:Win32/Occamy.AA	151	97	364	136	1134	129	2523	34
(B) Trojan:Win32/Occamy.B		14		20		31		29
(B) Trojan:Win32/Occamy.B	115	14	239	19	624	29	1296	18
(C) Trojan:Win32/Occamy.B!bit		5		8		10		11
(C) Trojan:Win32/Occamy.B!bit	43420	4	96871	3	256729	2	516477	181
(D) Trojan:Win32/Occamy.C		8257		6469		1607		181
(D) Trojan:Win32/Occamy.C	43440	8236	96907	6432	256813	1548	516641	144
(E) Trojan:Win32/Occamy.C!ctv		21		37		59		37
(E) Trojan:Win32/Occamy.C!ctv	5	16	17	28	86	44	268	19
(F) Trojan:Win32/Occamy.C02		11		18		24		21
(F) Trojan:Win32/Occamy.C02	31	8	115	10	454	9	1080	3
(G) Trojan:Win32/Occamy.C15		76		103		103		48
(G) Trojan:Win32/Occamy.C15	48	64	153	83	584	62	1366	17
(H) Trojan:Win32/Occamy.C26		32		50		65		36
(H) Trojan:Win32/Occamy.C26	35	29	127	46	520	44	1239	16
(I) Trojan:Win32/Occamy.C28		67		87		83		37
(I) Trojan:Win32/Occamy.C28	12761	0	28215	0	74276	0	149453	0
(J) Trojan:Win32/Occamy.C2D		2194		1692		489		77
(J) Trojan:Win32/Occamy.C2D	12676	2194	28051	1690	73909	463	148765	49
(K) Trojan:Win32/Occamy.C383		18		31		55		39
(K) Trojan:Win32/Occamy.C38	8	17	26	28	146	31	433	12
(L) Trojan:Win32/Occamy.C53		25		44		65		37
(L) Trojan:Win32/Occamy.C53	554	22	1237	29	3431	34	7218	6
(M) Trojan:Win32/Occamy.C75		156		195		182		68
(M) Trojan:Win32/Occamy.C75	643	88	1398	107	3813	98	7942	27
(N) Trojan:Win32/Occamy.C7E		74		100		96		43
(N) Trojan:Win32/Occamy.C7E	147	69	350	91	1080	77	2401	17
(O) Trojan:Win32/Occamy.C8D		33		54		76		46
(O) Trojan:Win32/Occamy.C8D	117	33	245	54	669	76	1443	46
(P) Trojan:Win32/Occamy.C95		0		0		0		0
(P) Trojan:Win32/Occamy.C95	24	0	94	0	369	0	867	0
(Q) Trojan:Win32/Occamy.C9C		67		87		83		37
(Q) Trojan:Win32/Occamy.C9C	12670	66	28034	83	73824	55	148549	14
(R) Trojan:Win32/Occamy.CA1		2128		1609		434		63
(R) Trojan:Win32/Occamy.CA1	12645	2128	27938	1608	73471	413	147782	38
(S) Trojan:Win32/Occamy.CA9		13		25		41		30
(S) Trojan:Win32/Occamy.CA9	13	0	28	0	101	0	292	0
(T) Trojan:Win32/Occamy.CB5		21		39		63		35
(T) Trojan:Win32/Occamy.CB5	3	20	11	37	84	50	283	17
(U) Trojan:Win32/Occamy.CB8		11		18		27		21
(U) Trojan:Win32/Occamy.CB8	524	11	1116	16	2951	17	6083	7
(V) Trojan:Win32/Occamy.CC8		80		96		99		43
(V) Trojan:Win32/Occamy.CC8	522	80	1107	96	2907	99	5968	43
(W) Trojan:Win32/Occamy.CCB		0		0		0		0
(W) Trojan:Win32/Occamy.CCB	0	0	2	0	31	0	122	0
(X) Trojan:Win32/Occamy.CD6		16		30		47		34
(X) Trojan:Win32/Occamy.CD6	13	3	28	5	95	6	250	4
(Y) Trojan:Win32/Occamy.CD9		13		25		41		30
(Y) Trojan:Win32/Occamy.CD9	0	13	6	24	56	32	193	16
(Z) Trojan:Win32/Occamy.CE5		11		17		28		22
(Z) Trojan:Win32/Occamy.CE5	1	10	20	6	80	17	271	3
(a) Trojan:Win32/Occamy.CEB		21		37		59		37
(a) Trojan:Win32/Occamy.CEB	0	21	7	36	63	53	215	26
(b) Trojan:Win32/Occamy.CEF		5		8		10		11
(b) Trojan:Win32/Occamy.CEF	5	5	14	8	50	9	129	9
(c) Trojan:Win32/Occamy.CF1		7		10		20		19
(c) Trojan:Win32/Occamy.CF1	9	7	28	10	109	17	283	13
(d) Trojan:Win32/Occamy.CFB		17		27		35		24
(d) Trojan:Win32/Occamy.CFB	23069	16	49953	24	129685	19	260323	4
(e) Trojan:Win32/Occamy.CFC		2956		2104		495		69