SolarWinds/SunBurst FNV-1a-XOR hash founds analysis

docs.google.com/spreadsheets/d/1u0_Df5OMsdzZcTkBDiaAtObbIOkMa5xbeXdKk_k0vWs

00-Hash	00-Cracked	00-Type	00-Product	00-Purpose	00-Reference
1475579823244607677	100-continue		n/a	HTTP status	https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/100
2734787258623754862	accept		n/a	HTTP header	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Accept
1368907909245890092	afwserv	assembly	Avast	Antivirus	
16858955978146406642	apac.lab	domain	n/a	dev/test zone	SolarWinds Asia/Pacific lab AD domain
2597124982561782591	apimonitor-x64	assembly	Rohitab	RE/Malware analysis	http://www.rohitab.com/apimonitor
2600364143812063535	apimonitor-x86	assembly	Rohitab	RE/Malware analysis	http://www.rohitab.com/apimonitor
6195833633417633900	aswengsrv	assembly	Avast/AVG	Antivirus	
2934149816356927366	aswidsagent	assembly	Avast/AVG	Antivirus	
13029357933491444455	aswidsagenta	assembly	Avast/AVG	Antivirus	
15194901817027173566	atrsdfw.sys	driver	Altiris / Symantec	EDR	
4821863173800309721	autopsy	assembly	Autopsy	Forensics	
13464308873961738403	autopsy64	assembly	Autopsy	Forensics	
3320026265773918739	autoruns	assembly	Autoruns	RE/Malware analysis	Sysinternals
12969190449276002545	autoruns64	assembly	Autoruns	RE/Malware analysis	Sysinternals
10657751674541025650	autorunsc	assembly	Autoruns	RE/Malware analysis	Sysinternals
12094027092655598256	autorunsc64	assembly	Autoruns	RE/Malware analysis	Sysinternals
27606633535502801 47	avastavwrapper	assembly	Avast	Antivirus	
8146185202538899243	avastsvc	assembly	Avast	Antivirus	
11818825521849580123	avastui	assembly	Avast	Antivirus	
11109294216876344399	avgadminclientservice	assembly	AVG	Antivirus	
27971291088837494 91	avgidsagent	assembly	AVG	Antivirus	
3660705254426876796	avgsvc	assembly	AVG	Antivirus	
3890794756780010537	avgsvca	assembly	AVG	Antivirus	
3890769468012566366	avgsvcx	assembly	AVG	Antivirus	
12709986806548166638	avgui	assembly	AVG	Antivirus	
14095938998438966337	avgwdsvcx	assembly	AVG	Antivirus	
13611051401579634621	avp	assembly	Kaspersky	Antivirus	
18147627057830191163	avpui	assembly	Kaspersky	Antivirus	
16423314183614230717	bccavsvc	assembly	Avast	Antivirus	
11913842725949116895	binaryninja	assembly	Binary Ninja	RE/Malware analysis	https://binary.ninja/
54497306916575726 3	blacklight	assembly	Blacklight	Forensics	https://www.blackbagtech.com/products/blacklight/
12679195163651834776	brcow_x_x_x_x.sys	driver	Bromium	App allowlisting	
1614465773938842903	brfilter.sys	driver	Bromium	App allowlisting	
11385275378891906608	carbonblack	service	Carbon Black	App allowlisting	
13693525876560827283	carbonblackk	service	Carbon Black	App allowlisting	
17204844226884380288	cavp		Carbon Black?	App allowlisting?	MS ref says security-related
59849631053896767 59	cb		Carbon Black	App allowlisting	
17849680105131524334	cbcomms	service	Carbon Black	App allowlisting	
18246404330670877335	cbstream	service	Carbon Black	App allowlisting	
292198192373389586	cff explorer	assembly	NTCore Explorer Suite	RE/Malware analysis	https://ntcore.com/?page_id=388
14226582801651130532	close		n/a	HTTP header	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Connection - 'Close' token
11266044540366291518	connection		n/a	HTTP header	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Connection
6116246686670134098	content-type		n/a	HTTP header	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Type

	A	B	C	D	E	F
1	00-Hash	00-Cracked	00-Type	00-Product	00-Purpose	00-Reference
2	1475579823244607677	100-continue		n/a	HTTP status	https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/100
3	2734787258623754862	accept		n/a	HTTP header	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Accept
4	1368907909245890092	afwserv	assembly	Avast	Antivirus	
5	16858955978146406642	apac.lab	domain	n/a	dev/test zone	SolarWinds Asia/Pacific lab AD domain
6	2597124982561782591	apimonitor-x64	assembly	Rohitab	RE/Malware analysis	http://www.rohitab.com/apimonitor
7	2600364143812063535	apimonitor-x86	assembly	Rohitab	RE/Malware analysis	http://www.rohitab.com/apimonitor
8	6195833633417633900	aswengsrv	assembly	Avast/AVG	Antivirus	
9	2934149816356927366	aswidsagent	assembly	Avast/AVG	Antivirus	
10	13029357933491444455	aswidsagenta	assembly	Avast/AVG	Antivirus	
11	15194901817027173566	atrsdfw.sys	driver	Altiris / Symantec	EDR	
12	4821863173800309721	autopsy	assembly	Autopsy	Forensics	
13	13464308873961738403	autopsy64	assembly	Autopsy	Forensics	

	A	B	C	D	E	F
14	3320026265773918739	autoruns	assembly	Autoruns	RE/Malware analysis	Sysinternals
15	12969190449276002545	autoruns64	assembly	Autoruns	RE/Malware analysis	Sysinternals
16	10657751674541025650	autorunsc	assembly	Autoruns	RE/Malware analysis	Sysinternals
17	12094027092655598256	autorunsc64	assembly	Autoruns	RE/Malware analysis	Sysinternals
18	2760663353550280147	avastavwrapper	assembly	Avast	Antivirus	
19	8146185202538899243	avastsvc	assembly	Avast	Antivirus	
20	11818825521849580123	avastui	assembly	Avast	Antivirus	
21	11109294216876344399	avgadminclientservice	assembly	AVG	Antivirus	
22	2797129108883749491	avgidsagent	assembly	AVG	Antivirus	
23	3660705254426876796	avgsvc	assembly	AVG	Antivirus	
24	3890794756780010537	avgsvca	assembly	AVG	Antivirus	
25	3890769468012566366	avgsvcx	assembly	AVG	Antivirus	
26	12709986806548166638	avgui	assembly	AVG	Antivirus	
27	14095938998438966337	avgwdsvcx	assembly	AVG	Antivirus	
28	13611051401579634621	avp	assembly	Kaspersky	Antivirus	
29	18147627057830191163	avpui	assembly	Kaspersky	Antivirus	
30	16423314183614230717	bccavsvc	assembly	Avast	Antivirus	
31	11913842725949116895	binaryninja	assembly	Binary Ninja	RE/Malware analysis	https://binary.ninja/
32	5449730069165757263	blacklight	assembly	Blacklight	Forensics	https://www.blackbagtech.com/products/black
33	12679195163651834776	brcow_x_x_x_x.sys	driver	Bromium	App allowlisting	
34	1614465773938842903	brfilter.sys	driver	Bromium	App allowlisting	
35	11385275378891906608	carbonblack	service	Carbon Black	App allowlisting	
36	13693525876560827283	carbonblackk	service	Carbon Black	App allowlisting	
37	17204844226884380288	cavp		Carbon Black?	App allowlisting?	MS ref says security-related
38	5984963105389676759	cb		Carbon Black	App allowlisting	
39	17849680105131524334	cbcomms	service	Carbon Black	App allowlisting	

	A	B	C	D	E	F
40	18246404330670877335	cbstream	service	Carbon Black	App allowlisting	
41	292198192373389586	cff explorer	assembly	NTCore Explorer Suite	RE/Malware analysis	https://ntcore.com/?page_id=388
42	14226582801651130532	close		n/a	HTTP header	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Connection - 'C token
43	11266044540366291518	connection		n/a	HTTP header	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Connection
44	6116246686670134098	content-type		n/a	HTTP header	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Type
45	10734127004244879770	cork.lab	domain	n/a	dev/test zone	SolarWinds Cork (Ireland) AD domain
46	18159703063075866524	crexecprev.sys	driver	Cybereason	EDR	
47	11771945869106552231	csagent	service	Crowdstrike	EDR	
48	9234894663364701749	csdevicecontrol	service	Crowdstrike	EDR	
49	9061219083560670602	csfalconcontainer		Crowdstrike Falcon	EDR	
50	8698326794961817906	csfalconservice	service	Crowdstrike Falcon	EDR	
51	12790084614253405985	cutter	assembly	Rizin / Cutter	RE/Malware analysis	https://cutter.re/ (by @megabeets_)
52	16570804352575357627	cve.sys	driver	Absolute Software Corp.	EDR	https://www.absolute.com/platform/editions/ (which? Visibility / Control / Resilience?)
53	17097380490166623672	cybkerneltracker.sys	driver	CyberArk	EDR	
54	16066522799090129502	date		n/a	HTTP header	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Date
55	5219431737322569038	de4dot	assembly	de4dot	Forensics	https://github.com/de4dot/de4dot
56	15535773470978271326	debugview	assembly	DebugView	RE/Malware analysis	Sysinternals
57	11073283311104541690	dev.local	domain	n/a	dev/test zone	SolarWinds Local dev AD domain
58	3626142665768487764	dgdmk.sys	driver	Verdasys	EDR	
59	7810436520414958497	diskmon	assembly	DiskMon	RE/Malware analysis	Sysinternals
60	40302364139751996 54	dmz.local	domain	n/a	dev/test zone	SolarWinds local DMZ AD domain
61	13316211011159594063	dnsd	assembly	n/a	?	perhaps DNS proxy?
62	13825071784440082496	dnspy	assembly	dnSpy	RE/Malware analysis	https://github.com/dnSpy/dnSpy
63	14480775929210717493	dotpeek32	assembly	dotPeek	RE/Malware analysis	https://www.jetbrains.com/decompiler/
64	14482658293117931546	dotpeek64	assembly	dotPeek	RE/Malware analysis	https://www.jetbrains.com/decompiler/

	A	B	C	D	E	F
65	8473756179280619170	dumpcap	assembly	Wireshark	RE/Malware analysis	
66	15587050164583443069	eamonm	service	ESET	EDR	
67	12718416789200275332	eaw.sys	driver	Raytheon Cyber Solutions	EDR	
68	9559632696372799208	eelam	service	ESET	EDR	
69	607197993339007484	egui		ESET	EDR	
70	14513577387099045298	eguiproxy		ESET	EDR	
71	4931721628717906635	ehdrv	service	ESET	EDR	
72	14079676299181301772	ekbdflt	service	ESET	EDR	
73	3200333496547938354	ekrn	service	ESET	EDR	
74	2589926981877829912	ekrnepfw	service	ESET	EDR	
75	8727477769544302060	emea.sales	domain	n/a	dev/test zone	SolarWinds Europe / Middle East / Africa sale domain
76	17939405613729073960	epfw	service	ESET	EDR	
77	17997967489723066537	epfwwfp	service	ESET	EDR	
78	3778500091710709090	evidence center	assembly	Belkasoft Evidence Center	Forensics	https://belkasoft.com/x
79	8799118153397725683	exeinfope	assembly	Exeinfo PE	RE/Malware analysis	no longer maintained?
80	8873858923435176895	expect		n/a	HTTP header (client)	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Expect
81	13783346438774742614	f-secure filter	service	F-Secure	EDR	
82	16112751343173365533	f-secure gatekeeper	service	F-Secure	EDR	
83	17624147599670377042	f-secure gatekeeper handler starter	service	F-Secure	EDR	
84	3425260965299690882	f-secure hips	service	F-Secure	EDR	
85	16066651430762394116	f-secure network request broker	service	F-Secure	EDR	
86	2380224015317016190	f-secure recognizer	service	F-Secure	EDR	
87	13655261125244647696	f-secure webui daemon	service	F-Secure	EDR	
88	12027963942392743532	fakedns	assembly	fakedns	RE/Malware analysis	Verisign iDefense group?

	A	B	C	D	E	F
89	576626207276463000	fakenet	assembly	fakenet	RE/Malware analysis	may be ancestor of https://www.fireeye.com/services/freeware/fakng.html
90	9384605490088500348	fe_avk	service	FireEye	EDR	
91	15092207615430402812	feelam	service	ESET	EDR	
92	6274014997237900919	fekern	service	FireEye	Forensics	
93	3320767229281015341	fewscservice	service	FireEye	Forensics	
94	7412338704062093516	ffdec	assembly	Free Flash Decompiler	RE/Malware analysis	https://github.com/jindrapetrik/jpexs-decompile
95	682250828679635420	fiddler	assembly	Fiddler	RE/Malware analysis	https://www.telerik.com/fiddler
96	13014156621614176974	fileinsight	assembly	McAfee	RE/Malware analysis	https://www.mcafee.com/enterprise/en-us/downloads/free-tools/fileInsight.html
97	18150909006539876521	floss	assembly	FireEye	RE/Malware analysis	https://github.com/fireeye/flare-floss
98	5587557070429522647	fnrb32		F-Secure	EDR	
99	12445177985737237804	fsaua		F-Secure	EDR	
100	12445232961318634374	fsaus	service	F-Secure	EDR	