Chasing Shadows: A deep dive into the latest obfuscation methods being used by ShadowPad

By PricewaterhouseCoopers

Archived: 2026-04-02 11:49:43 UTC

Appendix A – Indicators of compromise

Indicator	Type	
9cbfa03a65e6cd4b62b2aa60a4cc4785b824378f735de2596a1195b75f71ecf3	SHA-256	
dbb02aaea56a1f0200b76f3f5b2d3596622503633285c7798b4248e0a558f01c	SHA-256	
d29113e3417dcba9d0e2d540fc53f702869dc7dc018a6b053bc3f70b4e55e436	SHA-256	
5f1a21940be9f78a5782879ad54600bd67bfcd4d32085db7a3e8a88292db26cc	SHA-256	
0371fc2a7cc73665971335fc23f38df2c82558961ad9fc2e984648c9415d8c4e	SHA-256	
fb17b3886685887aeb8f7c3496c6f7ef06702ec1232567278286c2f8ec4351bb	SHA-256	
26de542f77da51071389463fad1a50c687b70d902bbd0800db6c959e40dff755	SHA-256	
8065da4300e12e95b45e64ff8493d9401db1ea61be85e74f74a73b366283f27e	SHA-256	
c0fbb71af4863db0cd829429749570889O8f815ef7f02b197834e22d02d4a460	SHA-256	
c0aae2d5e77acb8b35037f3cd3b76e92eebdb1c53cf3775921bd6f64d94e9a99	SHA-256	
991511785a05f4dfbf1212e3fb69ff3b666659ecba5f3e5e9c8fbe9804afd23c	SHA-256	
943778353ce3af1043ec161ef18c9ba3e1ad6a9915dfe1783dff7aac8b53df16	SHA-256	
7579e864d47898f1322bb189bdd21b537b40e549149318ce8409f1d57233fa48	SHA-256	
c951a1d1294c46c995189dce4a70da0460dd19c0b7136a4905f41212cdead0c7	SHA-256	
7c8b6dfcdbcb6e0d87513eec841302a202e7371cdff16101d1594ea34a8dd1af	SHA-256	
c602456fae02510ff182b45d4ffb69ee6aae1166746000l241685807db2e29c3	SHA-256	
5e7e336bc7b489c3d4c59af861580ed73a5731d26560488bce03befdef9faadf	SHA-256	
c72436969d708905901ac294d835abb1c4513f8f26cb16c060d2fd902e1d5760	SHA-256	
dbb32cb933b6bb25e499185d6db71386a4b5709500d2da92d377171b7ff43294	SHA-256	

37417f300e1382b5b1b93e0be675ba8ab2d418747ea3fa015329f7ca405ae603	SHA-256	
c738af04c5b531abdb303a68cfb8994bb8db6e088bf99b45f85bdb863d3fb3e5	SHA-256	
ffc5bc143ab2320ae6989ccdf8c37a3d7c3c51c09eabf5a94ada86ab7c3abebd	SHA-256	
a8e5a1b15d42c4da97e23f5eb4a0adfd29674844ce906a86fa3554fc7e58d553	SHA-256	
1e06fd5b9aa0e5260369e52ec2d9f87060941de835234afd198b1d4c0b161678	SHA-256	
7cbd4339c33af40c70d27256cf3ec473bea588ac33ddfa64a8771344c82d9e6c	SHA-256	
cb5f8759831829614b82ed4a3bf1ac3f27f1640faf2a1f15ba728751e2fa44fa	SHA-256	
04089c1f71d62d50cbd8009dfd557aa1e6db1492a9fa2b35902182c07a0ed1c1	SHA-256	
531e54c055838f281d19fed674dbc339c13e21c71b6641c23d8333f6277f28c0	SHA-256	
042541cc39bafdcb0565ee468359ef575256f5adfda0e53c915ecdbbedd91316	SHA-256	
5a151aa75fbfc144cb48595a86e7b0ae0ad18d2630192773ff688ae1f42989b7	SHA-256	
f768bd36e88ffa496e7b6c538f2259cbdab0317e88432a99050f550b4c9f2f12	SHA-256	
8d1a5381492fe175c3c8263b6b81fd99aace9e2506881903d502336a55352fef	SHA-256	
a41348407e01886e76baf7cb8bb0efcf790b213cab87924b8a4f6bf8a9502350	SHA-256	
f8c5e93d6114f5a69d1544504d9d7f6a1d7397e3e5e0cce8e24e6d7b884c109e	SHA-256	
2a3cf204dcc977df6347a039428ae863066700cecfac965dcaeb7b9bd61bc1b6	SHA-256	
15371908d89caef3f4487298a452e58732d9f671f2c6a1f07036d123ce3c840d	SHA-256	
96dc16bbc0f3e6e80fba447e3a3e1085fddf8e97edf286ee8b3fd82954f565bb	SHA-256	
39f92aed5dfa2cd20ae7df11e16acce9bb2e80c7e6539bc81f352d42ab578eb6	SHA-256	
8396e35b19f906f9c6e342e6cd90ab8bbbecc90f9090b0afe68f4fa53530bc33	SHA-256	
ebe4347e993c81d145b68a788522d5c554edfa74c35e9e61ededd6c510e80c75	SHA-256	
02a18df00e241f82cecb7477f661ebe3f26012cdfc5b8172d634c07af4468130	SHA-256	
f7ef194f2dcc341ba03f76872cb7c0dfbae8f79118f99cf73dfccfb146c4e966	SHA-256	
f4effcf4d7321be824fd637b27f404250d0b1f03205bbc0682022d61aba5801e	SHA-256	
06539163f71f8bd496db75ccb41db820	MD5	
493698b1d7acfbf57848b964b4b0ae97	MD5	
69be59f365f74b406e505a8c0e128047	MD5	

bf98b795957d40ed8e0c52403af659d2	MD5	
8b9436c358a1d7f0ca61eca81b5025f7	MD5	
4ad23aae3409c31d3d72e1d10e9d957d	MD5	
ffbadead054d1eac270f1a24d02e8a1f	MD5	
3520e591065d3174999cc254e6f3dbf5	MD5	
a22fce6e7c1b2d129602ff938a2ac039	MD5	
ad82d23accb10b4c0fc7f8c9782ae6ad	MD5	
2a4976a82a07016bd1b5de1a372d8e15	MD5	
3e372906248b215ea0ee853cb4e29dd8	MD5	
ab8b13f3a93baaa36b730cb42434620a	MD5	
67329d4239551b51c481062b5d38a687	MD5	
18b391d91883979fc2df9e13c8aee075	MD5	
529e9edc37b668e13be6b077a399f195	MD5	
42988a0bd2bbdf4454d5d15a2733aa31	MD5	
ea6be331b5fa349a2fa464b062043b0e	MD5	
d50b9ca68a3a650016e64ab4c3ff8e4c	MD5	
409b27c8eab8b043cfe8854ca22799b3	MD5	
70477683ea5a7e193bb80c6cf01da8dd	MD5	
373eacf3ffd1b5722f9d3c1595092b4c	MD5	
d7e153c2957a519a1ee6734820e5efbd	MD5	
9563df80a0f9709baa909c25bdd64214	MD5	
64cc83ba22f67c6c8c82c162f64a7c92	MD5	
25f3713b9ff40b7fb1293213916c1dbc	MD5	
c486da41dda4f55f5bafa4f22d877495	MD5	
af10f874ee9a24d4a8d5e515af9c24a2	MD5	
9d3aaaf04c684bf6c90ada2030ceaea3	MD5	
21779cdfbe7ce838d3adc11f42b64191	MD5	

5f3093473ae4167fd51d4282fce73741	MD5	
42794ad1300ed3edb1ed2d1a473b77ad	MD5	
52c28bdb6b1fc4d77b1ea58dc8c1c810	MD5	
73790e781a0b3c7f1e1e8f9fa8f9d239	MD5	
5fe99a8f8cbfe46832478aa9c9634ed6	MD5	
263b7fb02bb4c05c789d2c1de92e0007	MD5	
24f73d5f67bc6cf0bccaade97e04fbca	MD5	
d2b97a3391c91d1577fb46963b8ef18a	MD5	
af78467a6cdbb4efa3894a30edef608b	MD5	
9d3a9edec791cb3eb7225be225337c1e	MD5	
7c8c3700757ddb5c6d423d88dd944065	MD5	
4d6705979b4ba29e44d3178ac979e1c6	MD5	
5fcdb89a3b2eb7ff31c5122e8f145277	MD5	
ff46982c58cf9cd0371e187a6c0dd6f7712c084c	SHA-1	
880fa69a6efd8de68771d3df2f9683107fb484c0	SHA-1	
0cfba69898627c620575cadfff92130429dcd019	SHA-1	
ea43dbef69af12404549bc45fda756bfefcb3d88	SHA-1	
cad05dec778a6dbdeb170a63bbbd18271b56d719	SHA-1	
addf67b8bcb8074927431bdfe3e3c867b07f5333	SHA-1	
7db78548aae9e4872b06ee9e79c29553947db3d6	SHA-1	
c73329dfbe99de4abb93b4fda6310a0c5eedd8f9	SHA-1	
47cdaf6c5c3fffeeff1f2c9e6c7649f99ab54932	SHA-1	
3342ad3a686be7a873409ae01cfab2eb0b621840	SHA-1	
215404d27c6a63a47561d6ab5258af26843b1769	SHA-1	
34ce0df62814e3a2430784836914c629d49f22b1	SHA-1	
c62b977c93979effb48a1614956c2a788abb22fe	SHA-1	
fa397effbb1d2d9b276d9d109e79ef89790729bc	SHA-1	

6512750a9da8c81c6b7c5b5301a60d4962c0c41b	SHA-1	
b885b9c4a9cd7872cd995198834471e52219ae41	SHA-1	
f8e4b7bd1cc973be7540f731028953073430759a	SHA-1	
6966687463365f08cfb25fd2c47c6e9a27af22b0	SHA-1	
9605ad1bf0432ffb148d422099e23eaa26bed4c8	SHA-1	
30c63b1e252ea0dc72b97785c1874ab7b6ddef43	SHA-1	
48daf01f86cfc9f22c446d602f0cdbd4b763dfc8	SHA-1	
b73134449329fd640a6de94a36cbcbebb4d5f541	SHA-1	
363e32fafd2732b3cfb53dfd39bef56da1affd7f	SHA-1	
e96759fcb766744a7aae9692947b4ed4ba77ce37	SHA-1	
55811e2fade5fa4412bd5ff7f17eca79887d6aff	SHA-1	
a36e63f41ee3fdfaf2a826c0b6e7728af546981e	SHA-1	
44fc5b13ac3947a3be3fff7808d5d664d7258cb9	SHA-1	
03a47494b76aa6feed68053e44c0a2fde6172ea5	SHA-1	
494d8239650f3acb0b946f0d00f6dbc9c2c05be0	SHA-1	
1c997ddb204bc597f937a07665511ae7d9d98661	SHA-1	
c227d3cdcb39b56eddb7ab62d0da62f006207764	SHA-1	
d4086a747566d5a7b0e80f0c977e1e6db3410d26	SHA-1	
e2898e362dd19a0fb6f317d559cbdb78eac6488c	SHA-1	
9853fe35e1b6e06b53ad2234d4fa2156fa5ccf97	SHA-1	
f6f6f352fa58d587c644953e4fd1552278827e14	SHA-1	
b224ae9ffd8119d773dedb1863d46725c29143f8	SHA-1	
7cd459821ef2daea764df2f52c896e6ab00ed263	SHA-1	
3f2ec5d5ae8be0394baff82bd5c08fcf8df0e754	SHA-1	
fd492b013d52e061f101b6086c5c4902abb4b0e0	SHA-1	
ba985d268bca9ff3bf0b09ab63085b57f52d3574	SHA-1	
1bbc81db4d2d98a1cf29d4f84d065c6556f7caed	SHA-1	

12118603b97e6b3d3a8cb6e48ec7351e160da445	SHA-1	
93fec58769f40285b5a76106377644924d0c1dd0	SHA-1	
5zsi53pi6uu[.]livehost[.]live	Domain	
coivo2xo[.]livehost[.]live	Domain	
ui79zm8o9b[.]livehost[.]live	Domain	
qrvc7pdnbf[.]symantecupd[.]com	Domain	
pow2u24h7[.]wikimedia[.]vip	Domain	
vt[.]livehost[.]live	Domain	
c5t7dvucq[.]symantecupd[.]com	Domain	
1dfpi2d8kx[.]wikimedia[.]vip	Domain	
dns[.]dnslookup[.]services	Domain	
bsyu[.]dnslookup[.]services	Domain	
2og8qfrkrk[.]symantecupd[.]com	Domain	
test[.]wikimedia[.]vip	Domain	
dust[.]dnslookup[.]services	Domain	
dntc[.]livehost[.]live	Domain	
fljhcqwe[.]com	Domain	
5q4qp9trwi[.]dnslookup[.]services	Domain	
www[.]livehost[.]live	Domain	
bj0wyck5v5[.]livehost[.]live	Domain	
7ec8txihoa[.]dnslookup[.]services	Domain	
wikimedia[.]vip	Domain	
4yti11wlo5[.]livehost[.]live	Domain	
cigy2jft92[.]kasprsky[.]info	Domain	
6q4qp9trwi[.]dnslookup[.]services	Domain	
sci[.]livehost[.]live	Domain	
524ce3dm8h[.]symantecupd[.]com	Domain	

lmogv[.]dnslookup[.]services	Domain	
dlbo92v2ef[.]livehost[.]live	Domain	
bctu[.]dnslookup[.]services	Domain	
wcuhk[.]livehost[.]live	Domain	
hccadkml89[.]dnslookup[.]services	Domain	
r1d3wg7xofs[.]livehost[.]live	Domain	
jn3thp2wl6[.]symantecupd[.]com	Domain	
d89o0gm34t[.]livehost[.]live	Domain	
coivotek[.]livehost[.]live	Domain	
a[.]fljhcqwe[.]com	Domain	
evbyo7jj0v[.]livehost[.]live	Domain	
www[.]wikimedia[.]vip	Domain	
bm2l41risv[.]livehost[.]live	Domain	
wntc[.]livehost[.]live	Domain	
69gy9k6wc2[.]symantecupd[.]com	Domain	
wvt[.]livehost[.]live	Domain	
m2[.]livehost[.]live	Domain	
dns[.]livehost[.]live	Domain	
8hh3aktk2[.]kasprsky[.]info	Domain	
1160idswz5[.]kasprsky[.]info	Domain	
files[.]windowshostnamehost[.]club	Domain	
8hh3aktk[.]kasprsky[.]info	Domain	
wiki[.]windowshostnamehost[.]club	Domain	
windowshostnamehost[.]club	Domain	
6lh9bgi4n[.]symantecupd[.]com	Domain	
v2ray[.]windowshostnamehost[.]club	Domain	
5s2zm07ao[.]wikimedia[.]vip	Domain	

b3d3fn9n[.]kasprsky[.]info	Domain	
6czumi0fbg[.]symantecupd[.]com	Domain	
ns2[.]windowshostnamehost[.]club	Domain	
dbtwcse10sd[.]kasprsky[.]info	Domain	
mx[.]windowshostnamehost[.]club	Domain	
wfftm5kcj[.]kasprsky[.]info	Domain	
wlamazcsrv1[.]windowshostnamehost[.]club	Domain	
cde858l2yf[.]kasprsky[.]info	Domain	
bnmyphvq[.]wikimedia[.]vip	Domain	
local[.]windowshostnamehost[.]club	Domain	
juv0cumdo3[.]kasprsky[.]info	Domain	
felzeaxrs8hd[.]kasprsky[.]info	Domain	
c2[.]windowshostnamehost[.]club	Domain	
687eb876e047[.]kasprsky[.]info	Domain	
a6olaxgd[.]kasprsky[.]info	Domain	
ur1lwzh2qp[.]kasprsky[.]info	Domain	
hostmaster[.]wikimedia[.]vip	Domain	
bc[.]windowshostnamehost[.]club	Domain	
db311secsd[.]kasprsky[.]info	Domain	
arress[.]windowshostnamehost[.]club	Domain	
www[.]kasprsky[.]info	Domain	
7hln9yr3y6[.]symantecupd[.]com	Domain	
vwlamazcsrv1[.]windowshostnamehost[.]club	Domain	
v3hagesrj[.]symantecupd[.]com	Domain	
z16sxt822s[.]symantecupd[.]com	Domain	
dnslookup[.]services	Domain	
ybk47i6z8q[.]wikimedia[.]vip	Domain	

d89o0gm35t[.]livehost[.]live	Domain	
zk4c9u55[.]wikimedia[.]vip	Domain	
dsyu[.]livehost[.]live	Domain	
wsyu[.]livehost[.]live	Domain	
sc[.]livehost[.]live	Domain	
w0eew6nkmb[.]livehost[.]live	Domain	
r315imowtg[.]symantecupd[.]com	Domain	
o56n1tosy[.]livehost[.]live	Domain	
ti0wddsnv[.]wikimedia[.]vip	Domain	
symantecupd[.]com	Domain	
wctu[.]livehost[.]live	Domain	
4iiiessb[.]wikimedia[.]vip	Domain	
tei1sw0d98[.]symantecupd[.]com	Domain	
livehost[.]live	Domain	
nslookup[.]club	Domain	
kasprsky[.]info	Domain	
60.250.18[.]188	IPv4	
141.164.35[.]117	IPv4	
139.180.135[.]175	IPv4	
66.42.44[.]130	IPv4	
182.162.136[.]235	IPv4	
128.199.232[.]13	IPv4	
182.16.112[.]226	IPv4	
149.28.145[.]214	IPv4	

207.148.78[.]244	IPv4	
207.148.99[.]56	IPv4	
149.28.152[.]196	IPv4	
139.180.135[.]200	IPv4	
158.247.219[.]236	IPv4	
207.148.98[.]61	IPv4	
45.76.100[.]224	IPv4	
139.180.187[.]35	IPv4	
158.247.217[.]102	IPv4	
45.76.148[.]41	IPv4	
141.164.61[.]70	IPv4	
141.164.63[.]174	IPv4	
202.182.96[.]238	IPv4	
139.180.141[.]227	IPv4	
158.247.206[.]194	IPv4	
139.180.156[.]26	IPv4	
112.121.168[.]2	IPv4	
141.164.62[.]81	IPv4	
108.160.134[.]80	IPv4	
5bcd1346428b6d7f1f19c0f175d96800c5a0951d	SSL SHA-1 fingerprint	
743f1ef860a1cad5c046cb0099c479acf6815b97	SSL SHA-1 fingerprint	
61c39c6c60f7a45ff18806ed855985ef48d954ef	SSL SHA-1 fingerprint	
f1f5fe0dd96e165e049b8a7d508ccd951c7cca0b	SSL SHA-1 fingerprint	
9575b444beeed7a16d639223b08e18e29b5eb5a4	SSL SHA-1 fingerprint	
c9b276bd2166c95726fbe33f126fa0a014f84a36	SSL SHA-1 fingerprint	
5aa19bfcbc980d65df184e644053bf4732929d8e	SSL SHA-1 fingerprint	
log.dll.dat	Filename	

secur32.dll.dat	Filename	
mscoree.dll.dat	Filename	
