I Solemnly Swear My Driver Is Up to No Good: Hunting for Attestation Signed Malware | Mandiant

By Mandiant

Published: 2022-12-13 · Archived: 2026-04-05 22:08:23 UTC

The public key used for the attestation signing (Appendix C: POORTRY Certificate Details) contains two object identifiers (OIDs) of interest within the key usage value:

RFC 5280 Section 4.2.1.12 defines Extended Key Usage (EKU). The EKU values in this signature help identify which method was used to sign this file and what purposes this signing certificate may be used for. The values defined show that this certificate is used in the Windows Hardware Compatibility driver signing process and is used specifically for attestation signed drivers. Table 1 shows the OID descriptions.

The connection between the POORTRY sample, the attestation certificate, and the numerous legitimate samples signed with this certificate led Mandiant to assess with high confidence that this malware was verified via the Windows Hardware Compatibility process.

This field becomes an important artifact for identifying additional associated samples, and by pivoting on the Program Name, Mandiant identified eleven new suspicious files, including an additional POORTRY sample.

The `programName` field for attestation signed drivers appears to be populated by the X.509 Subject Organization Name (O) of the EV Code Signing certificate used to sign the initial CAB submission to the WHCP portal. This is corroborated by the high amount of malicious detections for samples associated with this Organization Name and other corresponding Program Name values on VirusTotal and within other Mandiant data sets. At time of writing, we have not been able to confirm with Microsoft that this is the exact mechanism for how the `programName` field is populated for attestation signed drivers.

All the observed corresponding EV code signing certificates were issued by Digicert. Over time certificate serial `01:15:3e:7a:3c:8d:c5:0b:3d:23:c8:ba:31:d3:70:52` was revoked, however several others appear to have not been revoked (bolded in Table 4). These corresponding Extended Validation certificates were used to sign launchers for SOGU malware utilized by Temp.Hex as well as signed distributions of the open source Fast Reverse Proxy tool, which has been used by suspected Iranian state-sponsored threat actors in intrusions observed by Mandiant.

Utilizing the OIDs and certificate data, YARA rules were developed to collect additional attestation signed drivers.

Examining these additional attestation signed drivers led to 57 suspicious samples that shared program names that were observed in malicious binaries (Appendix B: Indicators of Interest). These samples were spread across nine different program names.

The suspicious samples identified through this investigation have led to multiple development environment artifacts, specifically program database (PDB) paths, implying multiple different development environments and potentially multiple different malware authors.

Mandiant has previously observed scenarios when it is suspected that groups leverage a common criminal service for code signing. This is not a new phenomenon, and has been documented by the Certified Malware project at the University

of Maryland in 2017. This is what Mandiant believes is occurring with these suspicious attestation signed drivers and related EV signed samples.

The use of stolen or fraudulently obtained code signing certificates by threat actors has been a common tactic and providing these certificates or signing services has proven a lucrative niche in the underground economy. Mandiant has identified numerous threat actors and services advertising in a variety of languages, including English, Russian, and Chinese, that claim to provide code signing certificates or sign malware on behalf of threat actors. For example, while analyzing chat messages leaked by the Twitter user "@ContiLeaks," Mandiant identified several instances where threat actors involved in Trickbot operations purchased code signing certificates from multiple threat actors, with observed pricing ranging between approximately $1,000-$3,000 USD for a single certificate.

While most of these advertisements only mention EV code signing certificates, we have identified a small number of discussions focused on signing drivers through WHQL. While most of these discussions lamented to the challenges presented by WHQL restrictions, we observed at least one actor who mentioned experience signing drivers with WHQL, and we have also identified multiple websites on the open Internet advertising WHQL driver signing services to enterprise businesses. While we are unable to link the signed payloads observed in this activity to any of the identified services, it's plausible that actors are either enlisting services from underground forums or abusing commercial services to obtain signed driver malware.

A pattern emerges of suspected malicious attestation signed drivers that contain the `programName` corresponding to EV certificates that have also signed other suspected malicious samples. The Certificates appear to be issued primarily via Digicert and Globalsign to Chinese customers, indicating possible abuse of a Chinese market certificate reseller or signing service.

Given the different company names identified and the differing development environments Mandiant suspects there is a service provider getting these malware samples signed through the attestation process on behalf of the actors. Unfortunately, at this time, this assessment is stated with low confidence.

Attestation signing is a legitimate Microsoft program, and the resulting drivers are signed with legitimate Microsoft certificates. This makes execution-time detection difficult as Microsoft and most EDR tools will allow Microsoft signed binaries to load. Organizations must instead depend on behavioral detections to overcome the implicit trust granted to Microsoft-signed binaries and alert on suspicious or rootkit-like activities. For proactive hunts, however, there are numerous ways to search for these files.

The OLEs allow detection to be implemented to identify any binary that is signed via the attestation process. This rule matches on the presence of the OLEs and the Microsoft Windows Hardware Compatibility Publisher certificate subject.

The identified company names that were in the certificate program name can be used to home in on potentially suspicious samples. However, know that due to the nature of these certificates it is not true that all samples with the certificate are malicious, but simply have been abused in the past and warrant further investigation.

The VirusTotal dataset has additional data available for access via LiveHunt rules. This includes various tags and other metadata from the related sandbox execution. This information can be used to identify suspected malicious attestation signed binaries by combining the M_Hunting_Signed_Driver_Attestation_1 rule with the malicious count metadata.

As documented in the Definitive Dossier of Devilish Debug Details, PDB paths can be used to identify strings that are present within the malware.However, it's important to remember that this is a consequence of the malware and malware developers, and not the certificate or signing process.

See Appendix A: YARA for the full list of detections.

The attestation signing process offloads the responsibility of verifying the identity of the requesting hardware or software vendor to the Certificate Authorities. In theory this is a valid process as the CAs must follow agreed upon procedures to verify the identity of the requesting entity and the authority of the individual making the request to represent the software vendor. However, this process is being abused to obtain malware signed by Microsoft.

While this blog post has focused on POORTRY and the attestation signing process, Mandiant has observed other malware being signed via attestation. TEMPLESHOT is a malware family consisting of dropper, backdoor, a filter driver, and a protection driver. The TEMPLESHOT driver with MD5 `48bf11dd6c22e241b745d3bb1d562ca1` has been observed in the wild and is signed via attestation.

Use of the Signify python library made automated analysis of Authenticode data extremely efficient. This content would not have been possible without the assistance of analysts across the Mandiant Intelligence and FLARE organizations.

One sample (`688c138fffbb4e7297289433c79d62f5`) does not have a Signature Date, and this is likely due to binary tampering including the use of VMProtect after signing and other modifications.

The following table includes signed POORTRY samples.

The following table includes samples signed by EV certificates where the Organization Name is 大连纵梦网络科技有限公司.

The following list of MD5s are attestation signed binaries that have been identified as suspicious by numerous security solutions. While each one may not be directly malicious, they warrant an investigation should they be present in an environment.

`0080fde587d6aedccb08db1317360d32`	`ff985a86bfa60576a8e86b05603ac5fa`	`b00c95692923b8c1e2d45c4a64a5ff05`
`00a7538086c266e8bcf8a0b1c2b6a2e4`	`62f289f3b55b0886c419a5077d11eb3c`	`b0fea98c70e510f88b57f45a3f516326`
`00dd476fa04da76fc2ed37cfdde59875`	`63960dbc7d63767edb6e1e2dc6f0707b`	`b164daf106566f444dfb280d743bc2f7`
`024e92733def0b1180f0ee54b81e5836`	`63d877650a3219f5991fd66bafc46bc5`	`b3440350249974176291 2c7bfc9ff21f`
`03710450e5bebd207bbe471c4685dc49`	`64a81238d20dcbd4b21abb609040f698`	`b44dfd8c5e7b0c8652d7a647dfe252e4`
`07bac50f875f09ad644827c8918e6837`	`66c1452335767660136880 88b03103e3`	`b500ee8d8cb045936d2996a1747bcded`
`07c4309678ce891fdd868e10c6e7aad4`	`66d2860a078fb11832ceef28b23481c2`	`b5c73db8e70d6f46ad9b693f3ce060d2`

0ae78b90151ec2b0457bb0c2675048f5	67ff9de8e72c4dfdf4b4404abf253e7e	b7239e06bcbe6e2c7bb2f7a859cbf4f7
0b4a0fe7db8400ef65ce7618177351cf	688c138fffbb4e7297289433c79d62f5	b83d8761748abb032ab5ae75519eaf71
0d0ffa28823276732a9e4dea5c25cc34	688ca3c12b63fec9f921334d24cf6f78	b849deae20052d72c3c623660fa97e64
14a1d3e07520df607635a3356877f5b9	6916b29893f618ba76b36bd8c297b7ac	b8783155d6be5bb3a6d75edaa7ae7f71
14e6507566a404e3158b3e36314bb3a1	6a066d2be83cf83f343d0550b0b8f206	b9d40581ae936662c37f2edc979d7e99
1548b70d8581cbde703b1fb50b48a6a8	6a23d752fbc30e603bbb050a83a580eb	ba9907be3a0752369082199ed126f8d8
163118c947aacd0978ad3e019c7d121f	6a893aab7b79b73da7a049c2707aabf1	bb46eb379caae3b05e32d3089c0dd6d0
179ca82f2e523be47df0dcebe808408d	6b0a733568d80be653fc9a568cdd88c5	bd25be845c151370ff177509d95d5add
198877a8ce99289f7281b1475c13ba9f	6c3180163e4a5371647e734c7c817de5	bf13a2f4e2deb62b7dee98a012e94d61
19d14bf80b3dc4e5b774b362f079a102	6c7479b5bb27f250fa32331b6457883a	c0471f786486439502176 20f6e7e24cc
19d99758b1f33b418cb008530b61a1e7	6d32d2d7a44584c92115ac2a2c3ba3af	c0debd2cfb62fc2c56bfd4104b1ff760
1e63ec5b89edb805956f347b5b5cfaae	6e1bb443369973923c8eced16fcbd5cf	c12d465743b9c167fc819b7872cd014c
1f2888e57fdd6aee466962c25ba7d62d	6e3516775e7e009777dcdb7a314f1482	c35e6a0e1aef31ed9855499df4317acd
1f46065ac9479253e4babc42b72bc4a8	6e730cf4ebcd166d26414378cab3a6d8	c5120095bf08655407c2f0215d10ac1d
1f929fd617471c4977b522c71b4c91ed	6fcf56f6ca3210ec397e55f727353c4a	c77e931a6388b2040cc7c5a1a0f56d93
207cfc647647419adcfcc44c6059a1d1	7182ed3da406ba19bb9ffd8e4948d858	c7850060cfe574a2ef278ba46a136a5e

20f94c9cfc3cf012bf90546985f9f3c4	721b40a0c2a0257443f7dcc2c697e28a	c812fa7c628c3e19a3da5910acf6206e
22519936cd9e8c7d524b0590826c3e6e	72dbbd1dd61c6b0c2571e83f2c3d1825	c8495649615bf1b9f839d7f357d6d02f
228f9f0a0466fba21ac085626020a8e1	734b3a6e6cbd1f53fbb693140d2c3049	cadc3e4090aed708526f0d6016aba7fd
22949977ce5cd96ba674b403a9c81285	761939b0e442821985ab3281f97e6ceb	cb68b7979bbb55bbde0a8c60fe3e5184
232b0156173a9f8f5db6b65aa91e923b	76c6ae0157ea7f41f55ed7e7d241f910	cb6a416204b57470fab0b944d7b59756
23cebc6b0eb76262d796577895f418d2	7737e5e40a439899f326279b7face22c	cbc3d1c88a5d0491b7b50bb77ada93fe
24eb9eef69475e4980a555898b25f0c1	77392be5eae901ae371c37861aa88589	cc29cf2294175315acbf33054151f3cd
262c92f2437c80adf232ef147ca2d734	787782e0395b3d5e32cda6fdea2faba0	cd4b6d8bb762c2281c9b1142588ede4c
267c30e484322ad31fa9e1374d6653f0	79ebae9ab3f3b59c754ab1cc82bf7e95	ce455358bf71c88b45fcb5789100969a
26caf3361ec353593f51ebbd3fe5bbde	7a5896673b81beb5589b512c6d781a85	ce4d3a69331ff87920c903a4e4091904
26d6833b1875b138ea34d6ab430cafcd	7a9df5c46c7c65b807f78c6c0bb2c38c	ce658935ef6e223893121dce22908655
2739311a6bb1a7b0b88ff24bf603a54d	7b6e3fe75c5ae68d7d5a3ae7b00097e0	ce6ef4dc1dd54baddaa51eaf594a496a
27bb03f2659cd95bf9e7af899ee32728	7ba744b584e28190eb03b9ecd1bb9374	d11b9a4664ea03dfe3e8e1d737cd15f8
286b10451fe364310f4a7baeb0e94a3f	7c6c1b7e6378b4c0bcceee84e0e26fde	d22a56e31b4e1fd5b06d46fa56f59151
2a12b959c55f4a2d34f96e45e2417a71	7cb012393114dfb35d60e70166a97986	d27fac80339ad1f2ee86374884996c52
2aa8dc7a5dff7817ce0a9c7cf30847bf	7d78b5773845c5189ca09227d27a9d5a	d2ed678542a5d1db494dc47359861467

2bec13be352db14fc9665ddf128deb8c	7dd800f100a049a72983dd75f5286d70	d47494b717c82eca8278dea610e1265d
2cc14f20cf6847a2084f2c9cc0622015	7e0a6a234a64350e684544e272c7fc41	d60d8f3f12550dca4ba07ff61263b67f
2d84c734d813af49cec3c3aa4aa4e6e3	7e2e29707e7a601e8ea7f3e2f4d672a2	d60e235b769cadbc7e83090b79b73ed3
2e323c67a8781531a294684f7d2761ec	7e7002dc10c62fb674a3184f4ad6688a	d617c9a86328921a8caf924575faf2a2
2f6daca66d2f64c7b1b6f8693ea09cb7	7ee0b286003dc9e8006c22dcd70663f0	d66fc4e2f537566bb4d91cdea0ac64e5
309f16f50e9074ce797eb38eda279298	7f9309f5e4defec132b622fadbcad511	d6b2947d8ff985fa84d697cc6cfdb7ff
331113d1d54a3610f9c9bd72fc783721	811f8d76ff00c9eda27b51a0fb2b0d39	d6e506a1e0417c4507a5314529d84e34
33b5485b35b33fd8ead5a38899522cce	822bbdec4e5630c3170ee05119dcfb5c	d77209a21352486435d85e339596eeae
3452586b669e12c1c4ee9db3c1006018	8264b3bdf46c0ece4f66151a613baed5	d87f08d1e50f2a3423813bf161b40859
35c95b6b5f4a6a0bda56276846dae17b	832fe73a91993b387f9a49fafb9d4ea7	dc170d9bba14b0421c2514465055a93f
35deaa9d004714dc6ef9661b91889148	84ce2a917e3d4aefcfc7d17e4a840a99	dc564bac7258e16627b9de0ce39fae25
3608b3a24736dea4bf24a8ac5ae00e30	85063d67203b91bef9772446a1723021	dd1a5bd34f8cfa56e439c6fb275356d6
37d4ba16136986bfded2b6fc698abf02	860f5812d65dc157a59c14e57bc0eaaf	ddee86b84dcb72835b57b1d049e9e0cd
395ea8b7d0f257850a3a04a1484bac4d	8986b5b6013cfb2bd3e6c8d22c453390	de4b5043c82ab3b36b4ae73a2e96d969
398384a6cf2b7e26947d2e0acbfeeda5	8ac6ef2475ec89d3709fc124573cb380	e051141b1dcb9e7f889fea7c8b1d6ba5
39ee31f03fe1bb93d47f560f73deffa9	8af6a129902a594ddaceafba38b7c060	e0e0c46ba4f969919e2879717c60ef2a

3d4b685dcaebc5bba5f9421572a4ab91	8b423e0395ba6419fcedc0701327c97c	e2465ea5c2d5dac4ae1b8d50da1d7cce
3db8146544ee26866a8e99bacb11188c	8d38a092ae5a3511bedadb7243a84409	e2c146a2522e4f40e5036c3fe12c3560
3ecaf3ba4e93916714cc43320f6f2c58	8e4d0f679b092296a2f74cf812907d05	e30830c05ed3d2a3178a3678f3169bec
3fd815ebb7d2ab2b62cff3c777b51e30	8fc8c6e1b2a1047752f60549878fb55f	e5f62ef06b0dd656e1e47913f01f9f8a
4070a8b16f318d108be0984e628421ad	909f3fc221acbe999483c87d9ead024a	e6960ae657786979493da1786191bcf4
40fda9a3c1be41be414f3795b25647f5	90affc996a2932cb0fec4e31cd673ae9	e777e5a8d2ba97c82128f04272e7841c
415240633837ebcbd80e080ba99c03a9	90b9a4328c4f712815760f9da49bcb6a	e7ff38a94ad765eb305fc7f0837f5913
42200c8422347f63b3edb45ea5aa9c45	913d50851abf337abc3c73f2d4e7fb34	ea033ee6df904d863448ffef6386b6ae
42a417e54639c69f033f72bbafe6e09a	929b293090bcc7900c1e8f9ba519e219	ea45419d992c15002c93067840568121
4349378822e2316f18784c10c7ca08a1	934d0cda4cba428e9b75ff16d5f4b0b1	ea5f6ab5666193f805d13a49009f0699
45991757d4ca2dab9e81f2fcbbc1ae23	93c5faf90bc889963f10c608cbde5a14	ee3bad1f5508e2129e0b423b009383e3
45be5c0e7dfe37f88f1fa6c2fbb462c5	947ebc3f481a7b9ee3cf3a34d9830159	ee6b1a79cb6641aa44c762ee90786fe0
467e60b9a0d1153057e0cfd0e721e198	95a04866e6afb8e9b0426f5890681f9a	f07506c30237c96e49eecafa0e5a4ed4
48190fd615dcea5c6679b8e30a8bfec0	9885d56d64ac2391a43f02abb2202181	f111bd9b8e55f60f909649820e116430
486b1afce3484a784a1662513ca1272a	9a8323bc7187441a0d85b9a2e8f580e3	f35a8a8f36c13769b9e9fff05fa4f720
48bf11dd6c22e241b745d3bb1d562ca1	9c4034691f6508e2361b6fca890671f9	f4ee6bee04b2ed18024e3a64a0d58385

48fc05c42549d0b3ec9e73bbb5be40dc	9d1424c87d89095e3cd6785adb54d2ec	f59a1409ce773658e72ad73424841890
4a0f22286134a58d9d20f911a608f636	9dabf30a780794200cd068b145730317	f783277840bbd2023879a87d0788f36e
4b2e59a821589ab091a63770f4a658ed	9e91e55c89f9c17c0a2acaf4376cd72b	f78915cbf89d8749a0a4ab18a2b182bd
4d4c17d8b52cd89da0b17cc9653b2010	9f1d60d3cddea7f7558fad0217759094	f8ccabcbe08bbd2c8420f4d1cffcefd8
4d947e4163e8aeafbfc626eb033bc665	a0fdc4543687a1b341b365d6dd16551c	f9844524fb0009e5b784c21c7bad4220
4e1f656001af3677856f664e96282a6f	a2ee1cc9e80390ca248863004adbde60	f9aad310a5d5c80bbc61d10cc797e4f0
4e8d5c44bfdeffd0168f8a05f6a04e8b	a2f3bce86beef23aede69396dcf7e184	fa00cc96c5bea2979a59d0da0d22c83d
4f5c7367f2ebae0097b6f2f1bebd19b6	a55cb8be2887e99b4f662fc1ae08d265	fa914061f5a40b324454d3fb9fc85ca5
508d42f26f8bd562728e6fca866e05eb	a7251aad1e81c6194b34dabf6edd6b4a	faa5806826ff1ba749b70de0e14835c3
50d13758b811c794bc13769ee3b42e85	a9541530619a3ac2615b92603b705fe6	fbd9ba2b8b2d677d41c30a01c02cfd01
52494f624378ef6ee298f0fc73082d0e	aba1be25da0691761f593725e9c067e5	fd3b7234419fafc9bdd533f48896ed73
52fc9ec7a5c177fe27fb00b6c2c5ff09	ac2a1f2ae6b547619bef93dfadb48937	fd4cee1c7b8167f25a8b4b864ede3c5d
548d48b658305ffb77cc814ea080b542	ac7f0fcb6040eb47ea9855d418c32510	fdb6dae1e8c182089fdb86996436330c
561bc6902367d9e43e27c5543e7a5818	acac842a46f3501fe407b1db1b247a0b	fe2f8e46ae540d7299c61ba083d52399
5800a88d39fdf63e5a43bfcc6700d907	adab615712eac2719691d01b69254f29	fe7ecd399eec7036a63f0b7eb5ebcfb1
5b281df4aaa915f660e075dc944a02c2	add02792cfff7b19b8e526a247acb0ba	ff43f91f2465504e5e67d0b37d92ef18

`5e5d9971c90287a6aa905e54b2a21b1c`	`ae2f3e2412925a767e372c9c0ccf7ced`	

The following certificate details are extracted from the certificate signing to the POORTRY sample. However, note that this is a legitimate attestation signing Microsoft certificate. Note that some details were removed for brevity.

Source: https://www.mandiant.com/resources/blog/hunting-attestation-signed-malware