Investigating and Mitigating Malicious Drivers

msrc-blog.microsoft.com/2021/06/25/investigating-and-mitigating-malicious-drivers/

The security landscape continues to rapidly evolve as threat actors find new and innovative methods to gain access to environments across a wide range of vectors. As the industry moves closer to the adoption of a Zero Trust security posture with broad and layered defenses, we remain committed to sharing threat intelligence with the community to shine a light on the latest techniques and exploits of attackers so the industry can better protect itself.

Microsoft is investigating a malicious actor distributing malicious drivers within gaming environments. The actor submitted drivers for certification through the Windows Hardware Compatibility Program. The drivers were built by a third party. We have suspended the account and reviewed their submissions for additional signs of malware.

No Evidence of Certificate Exposure

We have seen no evidence that the WHCP signing certificate was exposed. The infrastructure was not compromised. In alignment with our Zero Trust and layered defenses security posture, we have built-in detection and blocking of this driver and associated files through Microsoft Defender for Endpoint. We are also sharing these detections with other AV security vendors so they can proactively deploy detections.

The actor's activity is limited to the gaming sector specifically in China and does not appear to target enterprise environments. We are not attributing this to a nation-state actor at this time. The actor's goal is to use the driver to spoof their geo-location to cheat the system and play from anywhere. The malware enables them to gain an advantage in games and possibly exploit other players by compromising their accounts through common tools like keyloggers.

It's important to understand that the techniques used in this attack occur **post exploitation,** meaning an attacker must either have already gained administrative privileges in order to be able to run the installer to update the registry and install the malicious driver the next time the system boots or convince the user to do it on their behalf.

We will be sharing an update on how we are refining our partner access policies, validation and the signing process to further enhance our protections. There are no actions customers should take other than follow security best practices and deploy Antivirus software such as Windows Defender for Endpoint.

Just like our defenders, our adversaries are creative and determined. Because of this, Microsoft approaches security with an assume breach mentality and layered defenses. We work tirelessly alongside our industry partners to ensure the community as a whole is aware

of new attack tools, tactics and procedures that we have observed or that have been reported through responsible disclosure. By sharing the information we've learned with this report, we are raising awareness of these techniques so that more protections can be built in across the industry and to increase the degree of difficulty for attackers.

Additional Information on the Windows Hardware Compatibility Program

Microsoft Defender and Windows Security teams work diligently with driver publishers to detect security vulnerabilities before they can be exploited by malicious software. Microsoft Defender for Endpoint's UEFI scanner is able to scan below the operating system where these attacks occur to add further detection and protection from these kinds of low-level attacks. We also build automated mechanisms through Windows Update to block vulnerable versions of drivers and protect customers against vulnerability exploits based on ecosystem and partner engagement as this is an issue that challenges the industry at large.

Our security teams continue to work closely with the OEM and driver publishers to analyze and patch any known vulnerabilities and to update affected devices prior to shipment. Once the driver publisher patches the vulnerability, an update to all affected drivers is pushed out via the Windows Update (WU) platform. Once affected devices receive the latest security patches, drivers with confirmed security vulnerabilities are blocked on Windows 10 devices using Microsoft Defender for Endpoint Attack Surface Reduction (ASR) and Microsoft Windows Defender Application Control (WDAC) technologies to protect devices against exploits. More information is available via our Microsoft recommended driver block rules document.

Indicators of compromise

In addition to creating antimalware signatures for Microsoft Defender antivirus, sharing key detection guidance with our AV partners, we are also sharing these hashes and IP addresses for other defenders to leverage.

Known C2 IP addresses

110.42.4[.]180
45.113.202[.]180

Known malicious files

These are the list of SHA256 file hashes known to Microsoft as malicious:

04a269dd0a03e32e5b2a1c8ab0768791962e040d080d44dc44dab01dd7954f2b
0856a1da15b2b3e8999bf9fc51bbdedd4051e21fab1302e2ce766180b4931d86
0c42fe45ffa9a9c36c87a7f01510a077da6340ffd86bf8509f02c6939da133c5

0eace788e09c8d3f793a1fad94d35bcfd233f0777873412cd0c8172865562eec
115034373fc0ec8f75fb075b7a7011b603259ecc0aca271445e559b5404a1406
12656fc113b178fa3e6bfffc6473897766c44120082483eb8059ebff29b5d2df
12c0002af719c6abbc1e726b409fce099fffb90f758477f5295c152bde504caa
16b6be03495a4f4cf394194566bb02061fba2256cc04dcbde5aa6a17e41b7650
18b923b169b2c3c7db5cbfda0db0999f04adb2cf6c917e5b1fb2ff04714ecac1
1aa8ba45f9524847e2a36c0dc6fd80162923e88dc1be217dde2fb5894c65ff43
1cd75de5f54b799b60789696587b56a4a793cf60775b81f236f0e65189d863af
1d1f7e26109e6cb28c6b369c937b407d7b0cce3c4800ce9852eda94742b12259
1d60819f0ab8547dcd4eb18d39a0c317ec826332afa19c0a6af94bc681a21f14
1f05f74ebae7e65d389703d423445ffb269e657d8278b0523417e1f72b0228eb
1f90d9c4d259c1fde4c7bb66a95d71ea0122e4dfb75883a6cb17b5c80ce6d18a
22da5a055b7b17c69def9f5af54e257c751507e7b6b9a835fcf6245ab90ae750
22f6fe6bd62fb03f7aee489cccbc918999f49596052ac0153c02cd7a3320de13
23c061933d471c1f959c77806098ec0528d9b1d0130689bb3f417dd843138468
24ea733bae1b8722841fb4c6cead93c4c4f0b1248ca9a21601b1ce6b95b06864
26d67d479dafe6b33c980bd1eed0b6d749f43d05d001c5dcaaf5fcddb9b899fe
26f2b9cf6e0fb50bad49a367bee63e808f1d53c476b38642d13c7db6e50687f4
2fa78c2988f9580b0c18822b117d065fb419f9c476f4cfa43925ba6cd2dffac3
314affdc86f62c8f8069ccd50a2cdf73bcd319773a031be700ba97a1ea4129a8
34c890fa43ca0e5165a4960549828ba43d7f48a216a22fc46204548ebfc34f72
3700b38d63d426ff0a985226b45eca6e24d052f4262d12aff529e62c2cb889c3
40c45c9b1c764777096b59f99ae524cbd25b88c805187e615c3ed6840f3d4c15
45ee083e28fbb33afa41b1b8cd00d94c29dea8cb7cee70bae4079e6c3dfb5501
4ce61ad21f186cf10dbcc253feee31262203cb5c12c5a140d2dda5447c57aba1
516159871730b18c2bddedb1a9da110577112d4835606ee79bb80e7a58784a13
5cb1dc26159c6700d6cadece63f6defda642ec1a6d324daefb0965b4e3746f70
5d0d5373c5e52c4405f4bd963413e6ef3490b7c4c919ec2d4e3fb92e91f397a0
62d7c5465852cdb7b59a86c20b4de5991c8f4820ce11a7c01cf0dde6032e500d
630d7bdc20f33e6f822f52533a324865694886b7b74dfaad1dc30c9aee4260a2
635273eaa4c2e20c4ec320c6c8447ce2e881984e97c9ed6aeec4fad16b934e81
63d61549030fcf46ff1dc138122580b4364f0fe99e6b068bc6a3d6903656aff0
640eeb3128ae5c353034ee29cb656d38c41353743396c1c936afd4d04a782087
6703400b490b35bcde6e41ce1640920251855e6d94171170ae7ea22cdd0938c0
6a234a2b8eb3844f7b5831ee048f88e8a76e9d38e753cc82f61b234c79fe1660
6a6db5febdaf3f1577bf97c6e1e24913e6c78b134062c02fd1f9875099c03a3f
6c7f24d8ed000bc7ce842e4875b467f9de1626436e051bd351adf1f6f8bbacf8
70b63dfc3ed2b89a4eb8a0aa6c26885f460e5686d21c9d32413df0cdc5f962c7
79e7165e626c7bde546cd1bea4b9ec206de8bed7821479856bdb0a2adc3e3617
7ff8fe4c220cf6416984b70a7e272006a018e5662da3cedc2a88efeb6411b4a4
8249e9c0ac0840a36d9a5b9ff3e217198a2f533159acd4bf3d9b0132cc079870
8e0b330a8df3076153638f5b76afc24d1083ebccc60e4d63ee0df5c11c45d58a

93d99a5fbfc888c0a40a18946933121ae110229dcf206b4d17116a57e7cf4dc9
97030f3c81906334429afebbf365a89b66804ed890cd74038815ca18823d626c
9b55b35284346bbcdc2754e60517e1702f0286770a080ee6ff3e7eed1cab812a
9f9315790d0b0cc5213ac9a8eff0968cccc0a6c469b50d6598ce759748fe74bf
9f9ebd6cd9b5b33ab2780122ee9c5feec84927f362890a062d13ef9816c7b85f
a0050c33c8263da02618872d642617959b3564fe173985e078bfedb89df93724
aa97f4f98ff842b1bfd78e920fcb1dedaec3f882dd19311bba6037430868e7a7
ad2dd8a68ce22d0959f341e9269e8033b34362b34bdea50b8ee2390907f1a610
b2cd9cca011064d03ddd8fe3521ce0e9f9d8b16f63e4ecaf03eacfef47d22dbf
b7516dca419d087ef844c42e061a834908f34e7363577ab128094973896222c8
b847e717215e0198cb4e863bd96390613f83eb92693171be50ca14255c5fb088
bbc58fd69ce5fed6691dd8d2084e9b728add808ffd5ea8b42ac284b686f77d9a
bfb4603902c6c9ff32bc36113280ee8b5687cc3ef4c0ff9fc56f2925c7f342f0
c0e74f565237c32989cb81234f4b5ad85f9dd731c112847c0a143d771021cb99
c2f23ad4e2f12c490cfd589764464e293d5d56c31b6b3f5081e2d677384cb2fe
c95af9eb52111b72563875d85d593d96d7e54e19690827a052377c77cc80e06f
caa0d9bb7ed2d21a76b71dfc22ffaef80371de8af2a03b8103cbcec332897a88
d0e1639e6386ef3c063bfae334fcc35cdfa85068ac1a65bb58f2463276c31ac9
d1ac4d07ba6fe1dd988c471975e49e35b83d03a9b9d626fa524fd8300b80b14a
d4335f4189240a3bcafa05fab01f0707cc8e3dd7a2998af734c24916d9e37ca8
d60fdabaf5a0ab375361d2ed1a9b39832bdb8bd33466d6c43d42a48ba2ffd274
e0afb8b937a5907fbe55a1d1cc7574e9304007ef33fa80ff3896e997a1beaf37
e2449ccc74e745c0339850064313bdd8dc0eff17b3a4e0882184c9576ac93a89
e8e7f2f889948fd977b5941e6897921da28c8898a9ca1379816d9f3fa9bc40ff
edc6e32e3545f859e5b49ece1cabd13623122c1f03a2f7454a61034b3ff577ed
ee6d0d0ea24be622521ee1a4defa5d5729b99ee2217ac65701d38d05dbc0d4e6
f1718a005232d1261894b798a60c73d971416359b70d0e545d7e7a40ed742b71
f83c357106a7d1d055b5cb75c8414aa3219354deb16ae9ee7efe8ee4c8c670ca
fd8a5313bf63f5013dc126620276fb4f0ef26416db48ee88cbaaca4029df1d73