```
// Rule appendix for the Definitive Dossier of Devilish Debug Details
// Blog link: https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html
// For more info, bother @stvemillertime or the #AdvancedPractices team on Twitter
// Updated on 2019-08-30, initial performance improvements by Florian Roth (@cyb3rops)

import "pe"
// used only in ConventionEngine_Anomaly_OutsideOfDebug

rule ConventionEngine_Keyword_Obfuscat
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "6724cef5a9a670d68e8ec00b6614997c"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}obfuscat[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Hook
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "92156ddfa4c1ec330ffd24ccef127a7a"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}hook[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Evil
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "9359b24a96df49972eda1750a35802de"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}evil[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Inject
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "081686496db01e44871f4e4a09e35fed"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}inject[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Trojan
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "060b2135d69fb33e8fc1c4d2bf7e2899"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}trojan[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Hide
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
```

```
        sample_md5 = "dd8af240a7a4a81b5f80250b44a778c4"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}hide[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Anti
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "d350ae5dc15bcc18fde382b84f4bb3d0"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}anti[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}

rule ConventionEngine_Keyword_Payload
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "10c534cacf65b604c1c2a30341bd2394"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}payload[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Keylog
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "1d7fd704fe4e41feff9e3a005ed868d6"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}keylog[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Bypass
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "00b8356235e510be95e367a25418b5cc"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}bypass[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Beacon
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "798afd5f648774c3133ea5e087efc2c1"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}beacon[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_UAC
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
```

```
        sample_md5 = "2e62974fbce2fc1bbde763b986ad7b77"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}uac[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Svchost
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "c1206ba56f7f0c2698adcb3280f345be"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}svchost[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Svhost
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "8edf49fd8421edc7f58997bb16961cf4"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}svhost[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Dropper
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "4847f692942358aff51b72ffcb3e40ac"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}dropper[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Attack
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "d6b1989d9c271b8575326e4fca159ae8"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}attack[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Encrypt
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "65746ec8d8488066a129821c27fcbfb3"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}encrypt[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Exploit
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "4215d029dd26c29ce3e0cab530979b19"
```

```
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}exploit[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Ransom
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "363bfef1781c107a08f46267f7676579"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}ransom[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Spy
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "15db41840f77723aa7e43460d9d3a5cc"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}spy[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Horse
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "1aa4a05fa321676b9934cd3aa54a5f95"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}horse[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_CVE
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "89dd326a64fdd77b467d2db1cc15e8ef"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}cve[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_shellcode
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "2cd7bc18377abb2464f55453e5bfab20"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}shellcode[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}

rule ConventionEngine_Keyword_Fake
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "124c475d67aa8391f5220efcc64ca5b3"
```

```
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}fake[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Backdoor
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "0017c2bfa513960f9ea4fee46382959b"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}backdoor[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_BDoor
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "ba08b593250c3ca5c13f56e2ca97d85e"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}(bkdoor|bckdoor|backdr)[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Zombie
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "05ce6c5b7e14c34d4e6189dc19675c98"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}zombie[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Rootkit
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "8d4c375e452c688b413882365437435b"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}rootkit[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Fuck
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "bce1069dd099f15170c5fd05bae921b5"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}fuck[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_LoadDLL
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "e03f94cf5e3b1df208967a87df13ccb5"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
```

```
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}loaddll[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Reflect
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "d4990a8d2ff6f2433acdad04521f85c6"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}reflect[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Sleep
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "0ce134d66531d2070b2c7db1ffb0dc6f"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}sleep[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Sploit
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "0637c45bdefaa93d26124c1f3899443a"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}sploit[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Reverse
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "fccb98a9a510cdcf7c730eba548729de"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}reverse[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Socket
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "9c836dcd5251c4c9272b408b486e65db"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}socket[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_PowerShell
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "337005359177441 7e3282f7b40ae8ad"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
```

```
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}PowerShell[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Infect
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "fdfea54231be21760b722d5cef32da2a"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}infect[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Worm
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "fdfea54231be21760b722d5cef32da2a"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}worm[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Katz
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "0512c5a8807e4fdeb662e61d81cd1645"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}katz[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Mimi
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "a2bcbcc1465be96fbb957b14f29d1ea4"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}mimi[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Droper
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "5410ab108cd251a2db724db762d6606c"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}droper[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_0day
{
    meta:
        author = "@a_tweeter_user"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "e8df15f480b7044cf44faff4273dba8f"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}0day[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
```

```
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Penetration
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "5f7796346d22ec5bd8c7b5a2e6caca3c"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}penetration[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Wiper
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "3b740cca401715985f3a0c28f851b60e"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}wiper[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Bootkit
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "b427a55b62d7f00c532d695c9b04b4d2"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}bootkit[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Bot
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "df1e54a3832aff3e714fa2c122aa7ea9"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}(bot_|_bot| bot|bot |bot\\|-bot|bot-|\\bot)[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Csrss
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "72e743f7752367b461c42561021eb30d"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}csrss[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Flood
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "17a8d4405458594444491f2feca7c129f"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}flood[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
```

```
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Overflow
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}overflow[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Kali
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "2cc23a6d971a8dc2093b73f72c2380b4"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}kali[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Malware
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "198ee041e8f3eb12a19bc321f86ccb88"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}malware[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Miner
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "0409644ae4d1afb21c53339e244b5cc8"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}miner[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Xmrig
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "433f936511c2302342f175ad020e34f1"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}xmrig[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_LOL
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "05486e8707ae94befde0bafd9bee5429"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}lol[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
```

```
rule ConventionEngine_Keyword_FUD
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "07c281acbe2eeb479a73580560cec0b8"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}fud[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Install
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "74494aff87dblef5843cbf8c4d40cab1"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}install[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Steal
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "f3f47f3986e9c55d36c49beefa627b54"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}steal[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Launch
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}launch[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Downloader
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "8c843aa6ded2f2cb4a78a8b4534ac063"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}downloader[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Hack
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "afe58fee2460947291e93bad9fb095ce"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}hack[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Kill
{
```

```
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "6d250a11f68b1fd4ed0505fb2965b6f7"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}kill[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Implant
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "40451f20371329b992fb1b85c754d062"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}implant[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre and filesize < 3MB
}
rule ConventionEngine_Keyword_RAT
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "18244062e6169b79f68d9b413cfd2c04"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}(\\rat|rat\\|\srat|\-rat|rat\.|rat\s)[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
        $this = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}administrator[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre and not $this
}
rule ConventionEngine_Keyword_Shell
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "32a16eff23f6c35e22b0b7d041728f62"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}shell[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
        $this = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}(shellcode|powershell)[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre and not $this
}
rule ConventionEngine_Keyword_Admin
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "67fff57bb44d3458b17f0c7a7a45f405"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}Admin[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
        $this = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}administrator[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre and not $this
}

rule ConventionEngine_Keyword_Proxy
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "7486404888b3223ef171a310426b2387"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}proxy[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
```

```
}
rule ConventionEngine_Keyword_Virus
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "5a537470e936dbb9611f95fb7f136a6e"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}virus[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Bind
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "0a2d51b0e58e41407f1a08744f1443b0"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}bind[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_1337
{
    meta:
        author = "@itsreallynick"
        description = "Searching for PE files with PDB path keywords, terms or anomalies. -YOUR BOY CARR"
        sample_md5 = "e9ecca14f19fe192fc48e714a649cadd"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]?:?\\[\\\s|*\s]?.{0,250}\\[ll]33[7t][\\\s|*\s]?.{0,250}\.pdb\x00/ nocase
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Thinstall
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "2ef545036c95aab395f3f2a3a0d38a9f"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}thinstall[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Keyword_Driver
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "24a6ec8ebf9c0867ed1c097f4a653b8d"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}driver[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre and filesize < 3MB
}
rule ConventionEngine_Keyword_Client
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "24a6ec8ebf9c0867ed1c097f4a653b8d"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}client[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre and filesize < 3MB
}
```

```
rule ConventionEngine_Keyword_Server
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "24a6ec8ebf9c0867ed1c097f4a653b8d"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}server[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre and filesize < 3MB
}
rule ConventionEngine_Term_GoogleDrive
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}(Google Drive|Google \xd0\xb4\xd0\xb8\xd1\x81\xd0\xba|Google \xe4\xba\x91\xe7\xab\xaf\xe7\xa1\xac\xe7\x9b\x98)[\x00-\xFF]
{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_Windows
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "25b965b0f56a7dc8a0e2aa7e72778497"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\Windows\\[\x00-\xFF]{0,200}\.pdb\x00/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_Documents
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "e766b979aecfc603b561b19e3880a7bc"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}\\Documents[\x00-\xFF]{0,200}\.pdb\x00/
        $this = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}\\Documents and Settings[\x00-\xFF]{0,200}\.pdb\x00/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre and not $this
}
rule ConventionEngine_Term_DocumentsAndSettings
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "e766b979aecfc603b561b19e3880a7bc"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}\\Documents and Settings[\x00-\xFF]{0,200}\.pdb\x00/
        $this = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}\\Documents\\[\x00-\xFF]{0,200}\.pdb\x00/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre and not $this
}
rule ConventionEngine_Term_Dropbox
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "5d6bfa1a1add10dbd6745ddf915812ed"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}dropbox[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
```

```
}
rule ConventionEngine_Term_OneDrive
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}OneDrive[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_ConsoleApplication
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "4840ee7971322e1a6da801643432b25f"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}overflow[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_WindowsApplication
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "f097c1b0c8fe178de14717a4fc8f2a91"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}WindowsApplication[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_WindowsFormsApplication
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "b51c35d5606c173961b2aa4e6867b40a"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}WindowsFormsApplication[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_NewFolder
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "fe23fa6df4d8fb500859f0f76e92552d"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}New Folder[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_Copy
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "6156214b767254d5282bc7feef950dca"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}- Copy[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_Desktop
```

```
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "71cdba3859ca8bd03c1e996a790c04f9"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}Desktop[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_Users
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "09e4e6fa85b802c46bc121fcaecc5666"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}Users[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_Users_X
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "09e4e6fa85b802c46bc121fcaecc5666"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}\/Users\/[\x00-\xFF]{0,500}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_VisualStudio
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}Visual Studio[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Term_VmwareHost
{
    meta:
        author = "@itsreallynick"
        description = "Searching for PE files with PDB path keywords, terms, or anomalies. -YOUR BOY CARR"
        sample_md5 = "2742750991eb6687440ef53a7a93df94"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}\\\\vmware-host\\[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Anomaly_Slash
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "09e4e6fa85b802c46bc121fcaecc5666"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}\/[\x00-\xFF]{0,500}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Anomaly_NonAscii
{
    meta:
```

```
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "07b62497e41898c22e5d5351607aac8e"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}[^\x00-\x7F]{1,}[\x00-\xFF]{0,200}\.pdb\x00/ nocase ascii
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre and filesize < 1MB
}
rule ConventionEngine_Anomaly_DriveShare
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "e7414d82d69b902b5bc1efd0f3e201d7"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}\\.{0,50}\\[a-zA-Z]\$\\[\x00-\xFF]{0,200}\.pdb\x00/ nocase
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Anomaly_MultiPDB_Double
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "013f3bde3f1022b6cf3f2e541d19353c"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}\.pdb\x00/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and #pcre == 2
}
rule ConventionEngine_Anomaly_MultiPDB_Triple
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "013f3bde3f1022b6cf3f2e541d19353c"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}\.pdb\x00/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and #pcre == 3
}
rule ConventionEngine_Anomaly_MultiPDB_Quadruple
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "063915c2ac8dcba0c283407ff91e48e1"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
         $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}\.pdb\x00/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and #pcre == 4
}
rule ConventionEngine_Anomaly_MultiPDB_Quintuple_Plus
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "08faf27c5738b34186613b4c98905690"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
         $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,200}\.pdb\x00/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and #pcre >= 5
}
rule ConventionEngine_Anomaly_Short_SingleChar
{
    meta:
        author = "@stvemillertime"
```

```
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "26f7394147f00ef7c3146ddcafb8f161"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[\x00-\xFF]{1}\.pdb\x00/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Anomaly_Short_DoubleChar
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[\x00-\xFF]{2}\.pdb\x00/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Anomaly_Short_TripleChar
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x00-\xFF]{20}[\x00-\xFF]{3}\.pdb\x00/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Anomaly_NulledOut
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "94218fba95e3f03796dd005a2851b5af"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x01-\xFF]{16}[\x01-\xFF]{1}\x00\x00\x00[\x00]{10,500}/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre
}
rule ConventionEngine_Anomaly_NulledOut_DoublePlus
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "bf0fea133818387cca7eaef5a52c0aed"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
    strings:
        $pcre = /RSDS[\x01-\xFF]{16}[\x01-\xFF]{1}\x00\x00\x00[\x00]{10,500}/
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and #pcre >= 2
}
rule ConventionEngine_Anomaly_OutsideOfDebug
{
    meta:
        author = "@stvemillertime"
        description = "Searching for PE files with PDB path keywords, terms or anomalies."
        sample_md5 = "bf0fea133818387cca7eaef5a52c0aed"
        ref_blog = "https://www.fireeye.com/blog/threat-research/2019/08/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware.html"
   strings:
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-Z]:\\[\x00-\xFF]{0,500}\.pdb\x00/
   condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $pcre and pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_DEBUG].virtual_address == 0
}
```