Appendix A: Discovery Rules

The following Yara and Snort rules serve as examples of discovery rules for TRITON actor TTPs, turning the adversary methods into new haystacks for purposes of detection or hunting. Some of these discovery rules are narrow in aperture and build small haystacks, making them easy to review or applicable for high-fidelity detection. Some of these rules are broad in aperture and build large haystacks in which to hunt malicious activity. For all these TTP discovery rules, we recommend careful testing and tuning prior to implementation.

```
rule Methodology_PE_Bitvise_Wide
{
    meta:
        author = "@stvemillertime"
        date = "03/11/2019"
        description = "Looking for any Bitvise binary based on PDB path
strings, seen used heavily by TRITON actor"
    strings:
        $a1 = "d:\\repos\\main\\ssh2\\" ascii nocase wide
    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and $a1
}

rule Methodology_PE_Bitvise_But_Not
{
    meta:
        author = "@stvemillertime"
        date = "03/11/2019"
        description = "Looking for Bitvise binaries without Bitvise Limited
strings, seen used heavily by TRITON actor"
    strings:
        $a1 = "d:\\repos\\main\\ssh2\\" ascii nocase wide
        $z1 = "Bitvise Limited" ascii wide
    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and $a1
and not $z1
}

rule Methodology_PE_Bitvise_Microsoft
{
    meta:
        author = "@stvemillertime"
        date = "03/11/2019"
        description = "Looking for Bitvise binaries with PE metadata for
Microsoft Corporation, seen used heavily by TRITON actor"
    strings:
        $a1 = "d:\\repos\\main\\ssh2\\" ascii nocase wide
        $a2 = "Microsoft Corporation" ascii wide
    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and all of
them
}

rule Methodology_PE_OpenSSH_Strings
{
    meta:
```

```
        author = "@stvemillertime"
        date = "03/11/2019"
        description = "Looking for modified OpenSSH binaries with non-
standard PE metadata, seen used heavily by TRITON actor"
    strings:
        $a1 = "Microsoft openSSH client" ascii wide
        $z1 = "OpenSSH for Windows" ascii wide
    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and $a1
and not $z1
}

rule Methodology_PE_With_Hardcoded_OpenSSH_Private_Key
{
    meta:
        author = "@stvemillertime"
        date = "03/11/2019"
        description = "Looking for binaries with hard-coded OpenSSH private
key strings, seen used heavily by TRITON actor"
    strings:
        $a1 = "[-----BEGIN OPENSSH PRIVATE KEY-----" ascii nocase wide
        $a2 = { 0A 2D 2D 2D 2D 2D 45 4E 44 20 4F 50 45 4E 53 53 48 20 50 52
49 56 41 54 45 20 4B 45 59 2D 2D 2D 2D 2D 0A 25 73 73 68 2D }
    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and all of
them
}

rule Methodology_PE_CryptcatDefaultPw
{
    meta:
        author = "@Kapellmann"
        date = "03/24/2019"
        description = "Customized Cryptcat with default password, seen used
heavily by TRITON actor"
    strings:
        $z1 = "metallica"
        $s2 = "DNS fwd/rev mismatch: %s != %s"
        $s3 = "Hmalloc %d failed"
        $s4 = "Warning: forward host lookup failed for %s: h_errno %d"
    condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and $z1
and any of them and filesize < 3MB
}

rule Methodology_PE_Cryptcat
{
    meta:
        author = "@Kapellmann"
        date = "03/24/2019"
        description = "Customized Cryptcat with custom password, seen used
heavily by TRITON actor"
    strings:
        $s2 = "DNS fwd/rev mismatch: %s != %s"
        $s3 = "Hmalloc %d failed"
        $s4 = "Warning: forward host lookup failed for %s: h_errno %d"
    condition:
```

```
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and any
of them and filesize < 3MB
}

rule Methodology_PE_PDB_Path_Documents_VS20100
{
    meta:
        author = "@stvemillertime"
        date = "03/11/2019"
        description = "Warning, this is a big, broad haystack. Looking for
binaries with PDB paths containing a generic Documents\\Visual Studio 2010
folder structure, seen used by TRITON actor"
   strings:
        $anchor = "\\Documents\\Visual Studio 2010\\" nocase ascii wide
        $rsds = "RSDS"
        $pdb = {2E70646200}
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-
Z]:\\[\\\S|*\S]?.{0,250}\\Documents\\Visual Studio
2010\\[\\\S|*\S]?.{0,250}\.pdb\x00/ nocase
        $rsdspdbhex = {52 53 44 53 [21] 3A 5C [1-255] 2E 70 64 62 00}
   condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and
$anchor and $rsds and $pdb and $pcre and $rsdspdbhex and @rsds[1] < @anchor
[1] and @anchor [1] < @pdb [1] and filesize < 3MB
}

rule Methodology_PE_PDB_Path_Users_user
{
    meta:
        author = "@stvemillertime"
        date = "11/06/2018"
        description = "Warning, this is a big, broad haystack. Looking for
binaries with PDB paths containing a generic Users\\user folder, seen used by
TRITON actor"
   strings:
        $anchor = "C:\\Users\\user\\" nocase ascii wide
        $rsds = "RSDS"
        $pdb = {2E70646200}
        $pcre = /RSDS[\x00-\xFF]{20}[a-zA-
Z]:\\[\\\S|*\S]?.{0,250}C:\\Users\\user\\[\\\S|*\S]?.{0,250}\.pdb\x00/ nocase
        $rsdspdbhex = {52 53 44 53 [21] 3A 5C [1-255] 2E 70 64 62 00}
   condition:
        (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) == 0x00004550 and
$anchor and $rsds and $pdb and $pcre and $rsdspdbhex and @rsds[1] < @anchor
[1] and @anchor [1] < @pdb [1] and filesize < 3MB
}

alert tcp any !22 -> any any (msg:"Methodology - BITVISE SSH SERVER [!22]";
content:"SSH-2.0-"; depth:8; content:"FlowSsh\: Bitvise SSH Server";
within:33; metadata:author_name @reesepcres; sid:1; rev:1;)

alert tcp any 443 -> any any (msg:"Methodology - BITVISE SSH SERVER [443]";
content:"SSH-2.0-"; depth:8; content:"FlowSsh\: Bitvise SSH Server";
within:33; metadata:author_name @reesepcres; sid:2; rev:1;)

alert tcp any any -> any any (msg:"Methodology - RDP DEFAULT HOSTNAME [WIN-
*]"; content:"|c0 00|Duca"; depth:250; content:"W|00|I|00|N|00|-|00|";
```

```
distance:0; within:64; pcre:"/([A-Z0-9]\x00){11}[^A-Z0-9]/"; content:"rdpdr";
distance:0; metadata:author_name @itsreallynick sid:3; rev:1;)
```