Appendix C: MITRE ATT&CK JSON Raw Data


```
{
	"name": "TRITON actor",
	"version": "2.1",
	"domain": "mitre-enterprise",
	"description": "FireEye TRITON actor TTPs",
	"filters": {
		"stages": [
			"act",
			"prepare"
		],
		"platforms": [
			"windows",
			"linux",
			"mac"
		]
	},
	"sorting": 0,
	"viewMode": 1,
	"hideDisabled": false,
	"techniques": [
		{
			"techniqueID": "T1043",
			"tactic": "command-and-control",
			"color": "#3182bd",
			"comment": "Look for outbound connections with port-
protocol mismatches on common and uncommon ports such as 443, 4444, 8531, and
50501.",
			"enabled": true,
			"metadata": []
		},
		{
			"techniqueID": "T1183",
			"tactic": "privilege-escalation",
			"color": "#3182bd",
			"comment": "Look for modifications and new entries
referencing .exe files under registry key
HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image
File Execution Options  ",
			"enabled": true,
			"metadata": []
		},
		{
			"techniqueID": "T1183",
			"tactic": "persistence",
			"color": "#3182bd",
			"comment": "Look for modifications and new entries
referencing .exe files under registry key
HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image
File Execution Options  ",
			"enabled": true,
			"metadata": []
		},
		{
			"techniqueID": "T1183",
			"tactic": "defense-evasion",
```

```
                "color": "#3182bd",
                "comment": "Look for modifications and new entries
referencing .exe files under registry key
HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image
File Execution Options  ",
                "enabled": true,
                "metadata": []
            },
            {
                "techniqueID": "T1076",
                "tactic": "lateral-movement",
                "color": "#3182bd",
                "comment": "Look for the presence of PLINK and non-standard
RDP usage with event logs, firewall logs and registry keys as described in
FireEye's blog on "Bypassing Network Restrictions Through RDP
Tunneling."\n\nFind internal RDP pivoting by looking for bitmap cache files
under user accounts that should not be accessing sensitive systems via RDP.
Look for bitmap cache files such as bcache22.bmc under default, service or
administrator accounts, or any account not expected to be conducting internal
RDP accesses to sensitive systems in a protected OT connected zone,
especially in the DMZ or DCS areas like HMIs or engineering workstations.\n",
                "enabled": true,
                "metadata": []
            },
            {
                "techniqueID": "T1053",
                "tactic": "execution",
                "color": "#3182bd",
                "comment": "Look for new and anomalous Scheduled Tasks XML
triggers referencing unsigned .exe files.",
                "enabled": true,
                "metadata": []
            },
            {
                "techniqueID": "T1053",
                "tactic": "persistence",
                "color": "#3182bd",
                "comment": "Look for new and anomalous Scheduled Tasks XML
triggers referencing unsigned .exe files.",
                "enabled": true,
                "metadata": []
            },
            {
                "techniqueID": "T1053",
                "tactic": "privilege-escalation",
                "color": "#3182bd",
                "comment": "Look for new and anomalous Scheduled Tasks XML
triggers referencing unsigned .exe files.",
                "enabled": true,
                "metadata": []
            },
            {
                "techniqueID": "T1099",
                "tactic": "defense-evasion",
                "color": "#3182bd",
```

```
                "comment": "Look for timestomping command strings such as
".CreationTime=" in PowerShell scripts or in PowerShell command line entries.
Look for PEs with NTFS creation time prior to PE compile time.",
                "enabled": true,
                "metadata": []
            },
            {
                "techniqueID": "T1065",
                "tactic": "command-and-control",
                "color": "#3182bd",
                "comment": "Look for outbound connections with port-
protocol mismatches on common and uncommon ports such as 443, 4444, 8531, and
50501.",
                "enabled": true,
                "metadata": []
            },
            {
                "techniqueID": "T1078",
                "tactic": "defense-evasion",
                "color": "#3182bd",
                "comment": "Look for timestomping command strings such as
".CreationTime=" in PowerShell scripts or in PowerShell command line entries.
Look for PEs with NTFS creation time prior to PE compile time.",
                "enabled": true,
                "metadata": []
            },
            {
                "techniqueID": "T1078",
                "tactic": "persistence",
                "color": "#3182bd",
                "comment": "Look for timestomping command strings such as
".CreationTime=" in PowerShell scripts or in PowerShell command line entries.
Look for PEs with NTFS creation time prior to PE compile time.",
                "enabled": true,
                "metadata": []
            },
            {
                "techniqueID": "T1078",
                "tactic": "privilege-escalation",
                "color": "#3182bd",
                "comment": "Look for timestomping command strings such as
".CreationTime=" in PowerShell scripts or in PowerShell command line entries.
Look for PEs with NTFS creation time prior to PE compile time.",
                "enabled": true,
                "metadata": []
            },
            {
                "techniqueID": "T1078",
                "tactic": "initial-access",
                "color": "#3182bd",
                "comment": "Look for timestomping command strings such as
".CreationTime=" in PowerShell scripts or in PowerShell command line entries.
Look for PEs with NTFS creation time prior to PE compile time.",
                "enabled": true,
                "metadata": []
            },
            {
```

```
                  "techniqueID": "T1329",
                  "tactic": "establish-&-maintain-infrastructure",
                  "color": "#3182bd",
                  "comment": "Look for inbound and outbound connections from
and to non-standard IP ranges, especially from international VPS providers
like OVH, and UK-2 Limited (uk2.net).",
                  "enabled": true,
                  "metadata": []
            },
            {
                  "techniqueID": "T1311",
                  "tactic": "adversary-opsec",
                  "color": "#3182bd",
                  "comment": "Look for timestomping command strings such as
“.CreationTime=” in PowerShell scripts or in PowerShell command line entries.
Look for PEs with NTFS creation time prior to PE compile time.",
                  "enabled": true,
                  "metadata": []
            }
      ],
      "gradient": {
            "colors": [
                  "#ff6666",
                  "#ffe766",
                  "#8ec843"
            ],
            "minValue": 0,
            "maxValue": 100
      },
      "legendItems": [],
      "metadata": [],
      "showTacticRowBackground": false,
      "tacticRowBackground": "#dddddd",
      "selectTechniquesAcrossTactics": true
}
```