Part 3: Analysing MedusaLocker ransomware

By By Theta

Archived: 2026-04-05 18:04:41 UTC

We have mapped the TTPs of this adversary to the MITRE ATT&CK framework as a heatmap of activity. We can see that this adversary used a limited, but powerful, selection of TTPs.

Unfortunately, we're seeing the same TTPs being used over and over again for ransomware attacks, even if the initial access or lateral movement exploits vary.

We keep getting asked by customers to "tell us what we don't know about our vulnerabilities". While the use of traditional defensive frameworks like ISO 27001, NIST or PCI serve a compliance function, thinking like an attacker can rapidly highlight blind spots in your environment.

Phishing attacks are a nuisance but largely a means to an end for adversaries and won't put you out of business on their own. A ransomware attack will lose reputation, money and customers.

Never mind encrypting user workstations or file shares - destroying ERP and EDI systems (as happened here) will leave an organisation completely unable to trade and haemorrhaging money. That's not counting the cost of restoring business systems, which is incredibly labour-intensive, let alone the underlying IT infrastructure and the other parts of the Incident Response process, or the intangibles like the reputational damage.

Without enough cash reserves or insurance coverage, there's a real chance of even medium-sized business ending up underwater depending on time-to-recovery and the bill at the end. You might be tempted to just pay the ransom – but this isn't a great option either as there's no guarantee you'll get what you paid for. You still need to run through the IR (Incident Response) process to find the intruders and kick them out of your network.

We should also pause and take note of the human cost of these operations – they are brutal. The toll they take on those who suffer them is worse than intelligence motivated intrusions where "damage" is a more abstract concept. There is often a massive time crunch to restore systems at the expense of well-planned incident response process.

Several additional folders and files were deployed by the actor.

The following 4 deleted files were able to be recovered from the filesystem of the server with timestamps and other metadata suggesting they are associated with the actor. The purpose of these is not immediately clear and thus are not placed into this timeline.

EXPORT.EXE (35K) SHA256: c945efb7f7c77cda9e54962b707268da57532ccd89253f0ccc98911cae7b3d77

PCC.EXE (512K) SHA256: ef05323d278d60b3573c8d5b3bffd3a356eb4b8490c759ad71706e3e2eb9e470

PUZZLE.EXE (17K) SHA256: aa49a4459cfd27cf4be40f8fa3bdabc198b93cb57f215aa61b28838af4b59005

Despite the naming convention they are not directly executable and appear to be obscured with high entropy values (> 7.99)

_backup.bat (SHA256: 465A1ACD9BE9B7BA027F34DFDF07C7A0ACEA6723F9D38A4E4CB920DC05425878)

NetworkShare_pre2.exe (SHA256: 47E3555461472F23AB4766E4D5B6F6FD260E335A6ABC31B860E569A720A5446)


```
{
	"name": "Medusa Locker TTPs - June 2020 ",
	"version": "2.2",
	"domain": "mitre-enterprise",
	"description": "",
	"filters": {
		"stages": [
			"act"
		],
		"platforms": [
			"Windows"
		]
	},
	"sorting": 0,
	"viewMode": 0,
	"hideDisabled": false,
	"techniques": [
		{
			"techniqueID": "T1110",
			"tactic": "credential-access",
			"color": "#e60d0d",
			"comment": "",
			"enabled": true,
			"metadata": []
		},
		{
			"techniqueID": "T1059",
			"tactic": "execution",
			"color": "#fce93b",
			"comment": "",
			"enabled": true,
			"metadata": []
		},
		{
			"techniqueID": "T1003",
			"tactic": "credential-access",
```

```
            "color": "#e6550d",
            "comment": "",
            "enabled": true,
            "metadata": []
        },
        {
            "techniqueID": "T1002",
            "tactic": "exfiltration",
            "color": "#fce93b",
            "comment": "",
            "enabled": true,
            "metadata": []
        },
        {
            "techniqueID": "T1486",
            "tactic": "impact",
            "color": "#e60d0d",
            "comment": "",
            "enabled": true,
            "metadata": []
        },
        {
            "techniqueID": "T1074",
            "tactic": "collection",
            "color": "#e6550d",
            "comment": "",
            "enabled": true,
            "metadata": []
        },
        {
            "techniqueID": "T1089",
            "tactic": "defense-evasion",
            "color": "#e60d0d",
            "comment": "",
            "enabled": true,
            "metadata": []
        },
        {
            "techniqueID": "T1487",
            "tactic": "impact",
            "color": "#e60d0d",
            "comment": "",
            "enabled": true,
            "metadata": []
        },
        {
            "techniqueID": "T1041",
```

```
                "tactic": "exfiltration",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1133",
                "tactic": "persistence",
                "color": "#e60d0d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1133",
                "tactic": "initial-access",
                "color": "#e60d0d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1061",
                "tactic": "execution",
                "color": "#e60d0d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1490",
                "tactic": "impact",
                "color": "#e60d0d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1046",
                "tactic": "discovery",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
```

```
                "techniqueID": "T1135",
                "tactic": "discovery",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1040",
                "tactic": "credential-access",
                "color": "#fce93b",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1040",
                "tactic": "discovery",
                "color": "#fce93b",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1086",
                "tactic": "execution",
                "color": "#e60d0d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1219",
                "tactic": "command-and-control",
                "color": "#e60d0d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1076",
                "tactic": "lateral-movement",
                "color": "#e60d0d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
```

```
        {
                "techniqueID": "T1018",
                "tactic": "discovery",
                "color": "#e60d0d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1053",
                "tactic": "execution",
                "color": "#e60d0d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1053",
                "tactic": "persistence",
                "color": "#e60d0d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1053",
                "tactic": "privilege-escalation",
                "color": "#e60d0d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1064",
                "tactic": "defense-evasion",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1064",
                "tactic": "execution",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
```

```
        },
        {
                "techniqueID": "T1035",
                "tactic": "execution",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1016",
                "tactic": "discovery",
                "color": "#fce93b",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1049",
                "tactic": "discovery",
                "color": "#fce93b",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1529",
                "tactic": "impact",
                "color": "#fce93b",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1078",
                "tactic": "defense-evasion",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1078",
                "tactic": "persistence",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
```

```
                "metadata": []
        },
        {
                "techniqueID": "T1078",
                "tactic": "privilege-escalation",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1078",
                "tactic": "initial-access",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1077",
                "tactic": "lateral-movement",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1047",
                "tactic": "execution",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1028",
                "tactic": "execution",
                "color": "#e6550d",
                "comment": "",
                "enabled": true,
                "metadata": []
        },
        {
                "techniqueID": "T1028",
                "tactic": "lateral-movement",
                "color": "#e6550d",
                "comment": "",
```

```
                        "enabled": true,
                        "metadata": []
                }
        ],
        "gradient": {
                "colors": [
                        "#ff6666",
                        "#ffe766",
                        "#8ec843"
                ],
                "minValue": 0,
                "maxValue": 100
        },
        "legendItems": [
                {
                        "color": "#e60d0d",
                        "label": "Observed TTPs"
                },
                {
                        "color": "#e6550d",
                        "label": "Med/High Confidence TTPs"
                },
                {
                        "color": "#fce93b",
                        "label": "Low/Med Confidence TTPs"
                }
        ],
        "metadata": [],
        "showTacticRowBackground": false,
        "tacticRowBackground": "#dddddd",
        "selectTechniquesAcrossTactics": true
}
```
