Jeremy Kirby

DropperSpark | Attacks Evade Detection with SparkNSF and Solving Source Code Interpretation

By Jeremy Kirby, Rhett Adams, Jon Rios, and Blake Berry-Morton

Executive Summary

- We analyze Ember Bear's Ukraine-focused cyber operations, which target organizations in Ukraine and Poland.
- Ember Bear's operations have evolved from using commodity malware families to using custom malware families.
- Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.
- Ember Bear's custom malware families have been observed being used in conjunction with commodity malware families.
- Ember Bear's custom malware families have been observed being used in conjunction with "living-the-land" techniques.
- Ember Bear's custom malware families have been observed being used in conjunction with "living-the-cloud" techniques.

Overview

Ember Bear's custom malware families have been observed being used in conjunction with "living-the-land" techniques, "living-the-cloud" techniques, and commodity malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Initiator Vector

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

SparkNSF

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Downloaded from raw.githubusercontent.com ]
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 1: SparkNSF stager

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 2: SparkNSF stager

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 3: SparkNSF stager

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Solving Source Code Interpretation For Evading Detection

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

- Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.
- Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.
- Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.
- Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.
- Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.
- Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.
- Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.
- Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 4: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 5: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 6: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 7: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 8: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 9: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 10: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 11: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 12: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 13: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 14: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 15: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 16: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 17: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 18: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 19: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 20: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 21: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 22: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 23: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 24: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 25: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 26: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 27: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 28: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 29: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 30: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 31: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 32: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 33: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 34: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 35: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 36: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 37: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 38: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 39: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 40: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 41: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 42: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 43: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 44: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 45: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 46: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 47: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 48: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 49: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 50: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 51: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 52: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 53: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 54: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 55: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 56: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 57: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 58: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 59: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 60: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 61: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 62: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 63: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 64: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 65: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 66: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 67: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 68: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 69: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 70: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 71: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 72: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 73: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

```
[ Decrypt AES-256-CBC ]
[ Write to %TEMP% ]
[ Execute via cmd.exe /c ]
[ Self-delete ]
```

Listing 74: Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families.

Ember Bear's custom malware families have been observed being used in conjunction with other custom malware families. Ember