Threat Name: APT_Backdoor_Win_GORAT

Threat Category: Remote Access Trojan (RAT), Espionage Malware

Threat Description:

The YARA rule APT_Backdoor_Win_GORAT_3 detects the GORAT backdoor, an advanced RAT used for covert access and data exfiltration.

Indicators of Compromise (IoCs):

Strings referencing:

```
$dirty1 = "fireeye" ascii nocase wide
$dirty2 = "kulinacs" ascii nocase wide
$dirty3 = "RedFlare" ascii nocase wide
$dirty4 = "gorat" ascii nocase wide
$dirty5 = "flare" ascii nocase wide
$go1 = "go.buildid" ascii wide
$go2 = "Go build ID:" ascii wide
$json1 = "json:\"pid\"" ascii wide
$json2 = "json:\"key\"" ascii wide
$json3 = "json:\"agent_time\"" ascii wide
$json4 = "json:\"rid\"" ascii wide
$json5 = "json:\"ports\"" ascii wide
$json6 = "json:\"agent_platform\"" ascii wide
$rat = "rat" ascii wide
$str1 = "handleCommand" ascii wide
$str2 = "sendBeacon" ascii wide
$str3 = "rat.AgentVersion" ascii wide
```

```
$str4 = "rat.Core" ascii wide
$str5 = "rat/log" ascii wide
$str6 = "rat/comms" ascii wide
$str7 = "rat/modules" ascii wide
$str8 = "murica" ascii wide
$str9 = "master secret" ascii wide
$str10 = "TaskID" ascii wide
$str11 = "rat.New" ascii wide
```

MD5 Hash: 995120b35db9d2f36d7d0ae0bfc9c10d

Detection Mechanism:

Detects malicious RAT behavior in Windows PE executables.

Possible Attribution & Use Cases:

Used in nation-state espionage campaigns.

Recommended Actions:

Block RAT communication channels.

Conduct endpoint forensics to locate persistent backdoors.

Author:

Rule Author: FireEye