Threat Category: APT / Malware, Backdoor

Threat Description: The YARA rule is designed to detect unpacked variants of a network backdoor associated with the Lazarus Group. This rule identifies executables that utilize specific network and command execution functionalities, indicative of the Lazarus Group's tools.

The detection focuses on identifying the use of 'netsh' commands for firewall rule manipulation, command execution via 'cmd.exe', and specific file paths and function calls commonly associated with this backdoor.

Indicators of Compromise (IoCs)

Network manipulation strings: "netsh firewall add portopening TCP %d", "netsh firewall delete portopening TCP %d"

Command execution strings:

```
$str_netsh_1 = "netsh firewall add portopening TCP %d" ascii wide nocase
$str_netsh_2 = "netsh firewall delete portopening TCP %d" ascii wide nocase
$str_mask_1 = "cmd.exe /c \"%s >> %s 2>&1\"" ascii wide
$str_mask_2 = "cmd.exe /c \"%s 2>> %s\"" ascii wide
$str_mask_3 = "%s\\%s\\%s" ascii wide
$str_other_1 = "perflog.dat" ascii wide nocase
$str_other_2 = "perflog.evt" ascii wide nocase
$str_other_3 = "cbstc.log" ascii wide nocase
$str_other_4 = "LdrGetProcedureAddress" ascii
$str_other_5 = "NtProtectVirtualMemory" ascii
```

File paths and function calls: "perflog.dat", "perflog.evt", "cbstc.log", "LdrGetProcedureAddress", "NtProtectVirtualMemory"

Detection Mechanism:

his rule identifies suspicious executables using the following conditions:

The file must be a valid Windows Portable Executable (PE) file, checked by verifying the MZ header (0x5A4D) at the beginning of the file.

The file size must be less than 3000KB.

The file must contain at least one of the network manipulation strings.

The file must contain at least one of the command execution strings.

The file must contain at least one of the specified file paths or function calls.

Possible Attribution & Use Cases: The presence of these strings and characteristics suggests the file is an unpacked variant of a Lazarus Group network backdoor.

Lazarus Group is known for cyber espionage and financial crime.

This detection can be used to identify and block malicious activity associated with this group.

Recommended Actions: Monitor and Investigate: Analyze any file triggering this rule to confirm malicious activity and determine the scope of the compromise.

Containment & Mitigation: Isolate affected systems and remove the malicious executable. Implement network security measures to prevent further intrusion.

Threat Hunting & Intelligence Sharing: Use this rule to proactively hunt for this backdoor. Share information with the security community.

Author & Attribution:

Rule Author: f-secure

Rule Date: 2020-06-10

Reference: https://labs.f-secure.com/publications/ti-report-lazarus-group-cryptocurrency-vertical

Rule ID: 8eda9e74-1a19-5510-82d8-cd2eb324629c