Threat Name: Hunting_GadgetToJScript

Threat Category: Exploit Toolkit, Scripting Engine Abuse

Threat Description: The YARA rule Hunting_GadgetToJScript_1 detects Base64-encoded artifacts of the LazyNetToJscriptLoader, a component of GadgetToJScript, which is used for executing .NET payloads via JavaScript engines.

Indicators of Compromise (IoCs):

Base64-encoded payload strings:

"GF6eU5ldFRvSnNjcmlwdExvYWRl"

"henlOZXRUb0pzY3JpcHRMb2Fk"

"YXp5TmV0VG9Kc2NyaXB0TG9hZGV"

MD5 Hash: 7af24305a409a2b8f83ece27bb0f7900

Detection Mechanism: Matches Base64-encoded scripting payloads commonly used in GadgetToJScript exploits.

Possible Attribution & Use Cases: Used in bypassing application whitelisting through JavaScript execution.

Recommended Actions:

Monitor execution of JavaScript-based process injections.

Investigate scripting engines loading unexpected .NET payloads.

Author & Attribution:

Rule Author: FireEye