Threat Category: Malware

Threat Description: The YARA rule is designed to detect a specific sample mentioned in the Dubnium Report. This rule identifies files that contain specific cryptographic keys and match certain file characteristics.

The detection mechanism focuses on identifying files that meet the following criteria:
The file must be a valid Portable Executable (PE) file, indicated by the MZ header (0x5A4D).
The file size must be less than 2000KB.
The file must contain both of the following ASCII strings:
"3b840e20e9555e9fb031c4ba1f1747ce25cc1d0ff664be676b9b4a90641ff194" (fullword ascii)
"90631f686a8c3dbc0703ffa353bc1fdf35774568ac62406f98a13ed8f47595fd" (fullword ascii)

Indicators of Compromise (IoCs):
MZ Header: 0x5A4D
File size: < 2000KB
Specific cryptographic keys (strings): (See Threat Description)
MD5 Hash: 839baf85de657b6d6503b6f94054efa8841f667987a9c805eab94a85a859e1ba

Possible Attribution & Use Cases:
The rule is designed to detect a sample associated with the Dubnium threat actor or campaign.
Dubnium is known for conducting cyber espionage activities.
Detection of this sample can indicate potential targeting by the Dubnium group.

Recommended Actions:
Investigation: If this rule is triggered, investigate the affected system for signs of compromise and further Dubnium activity.

Containment: Isolate affected systems to prevent lateral movement.

Remediation: Remove the identified sample and any related malicious artifacts.

Enhanced Monitoring: Implement enhanced monitoring and logging to detect potential follow-on activity.

Intelligence Sharing: Share information about the Dubnium activity with relevant security communities.

Author & Attribution:

Rule Author: Florian Roth (Nextron Systems)

Rule Reference: https://goo.gl/AW9Cuu

Rule Date: 2016-06-10

Rule Identifier: 377ecbaa-9324-562e-a973-0276d44f3feb