Government of India
National Critical Information
Infrastructure Protection Centre
(A Unit of NTRO)

Date: 13 Feb 2020

Advisory No: Adv/2020/Feb/005

Cyber Security Advisory: Panda celebrates the year of the Gh0st RAT with new C2s

This data is to be considered as **TLP:AMBER**

Our trusted partner observed threat actor named "Panda" using Remote Access Tools (RATs) and illicit cryptocurrency-mining malware. The embedded malware payloads are dropped by the BuleHero botnet. The BuleHero botnet uses Umbrella domain regex patterns to find related infrastructure for dropping malware. The dropped malware creates services “aluuunb.exe” and “cwggqi.exe” with their respective path names “\Windows\vsgyfdil\aluuunb.exe” and “\Windows\SysWOW64\cwggqi.exe”. The malware uses registry key with name “MFIFVTTNU” for “C:\Windows\vsgyfdil\aluuunb.exes\\0” to maintain persistence on the host. The malware also uses defense evasion techniques like using the “netsh” command to halt and modify existing Windows Firewall rules. Threat Grid analysis also detected this sample using Nullsoft Scriptable Install System (NSIS), which was not detected in previous Panda samples analyzed recently. The use of NSIS bolsters defense evasion by allowing the malware operator to make the malware harder to collect and investigate.

Analyst Note:

Panda is a legitimate threat capable of spreading cryptocurrency miners that can use up valuable computing resources and slow down networks and systems. This thread actor continuously linked with widespread illicit mining campaign with a different set of Command and Control (C2) servers. This actor has updated its infrastructure, exploits and payloads.

STIX2 attachment : **"Adv2020Feb005.json".**

```
{
        "type": "bundle",
        "spec_version": "2.0",
        "id": "bundle--5e344af4-a8c8-4923-a8d9-2a25ac110004",
        "objects": [{
                "type": "identity",
                "id": "identity--5df15c12-89fc-45a7-9620-0044ac110004",
                "name": "Talos",
                "identity_class": "organization",
                "created": "2020-01-31T15:42:45.490Z",
			"modified": "2020-01-31T15:42:45.490Z"
		}, {
			"type": "report",
			"id": "report--5e31d395-4798-4dbf-9ab3-145fac110004",
			"name": "[AEGIS] Panda celebrates the year of the Gh0st RAT with new C2",
			"created_by_ref": "identity--5df15c12-89fc-45a7-9620-0044ac110004",
			"created": "2020-01-29T00:00:00.000Z",
			"published": "1970-01-01T00:00:00Z",
			"object_marking_refs": ["marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"],
			"labels": ["Threat-Report", "misp:tool=\"misp2stix2\"", "Threat Type:RAT", "\tmalware_classification:malware-category=\"Botnet\"", "AEGIS", "Panda", "dnc:malware-type=\"CoinMiner\""],
			"object_refs": ["indicator--5e31d8eb-a35c-4bda-a986-2a53ac110004", "indicator--5e31d8eb-8410-4859-8aff-2a53ac110004", "indicator--5e31d8eb-3e38-4161-bec7-2a53ac110004", "indicator--5e31d8eb-b8fc-42a3-a232-2a53ac110004", "indicator--5e31d8eb-c7f0-4d23-8baa-2a53ac110004", "indicator--5e31d8eb-282c-4eb4-b51c-2a53ac110004", "indicator--5e31d8eb-11b4-4942-a5a4-2a53ac110004", "indicator--5e31d8eb-07e8-442e-adcc-2a53ac110004", "indicator--5e31d8eb-1a60-441a-96f3-2a53ac110004", "indicator--5e31d8eb-e088-4bde-af11-2a53ac110004", "indicator--5e31d8eb-d028-4a3b-8437-2a53ac110004", "indicator--5e31d8eb-03f0-4508-acce-2a53ac110004", "indicator--5e31d8eb-c104-4a77-b601-2a53ac110004", "indicator--5e31d8eb-88b4-4010-b35c-2a53ac110004"],
			"modified": "2020-01-31T15:42:45.519Z"
		}, {
			"id": "indicator--5e31d8eb-a35c-4bda-a986-2a53ac110004",
			"type": "indicator",
			"labels": ["misp:type=\"domain\"", "misp:category=\"Network activity\"", "misp:to_ids=\"True\""],
			"kill_chain_phases": [{
					"kill_chain_name": "misp-category",
					"phase_name": "Network activity"
				}
			],
			"valid_from": "2020-01-29T00:00:00Z",
			"created_by_ref": "identity--5df15c12-89fc-45a7-9620-0044ac110004",
			"pattern": "[domain-name:value = 'ae86.decode0x.online.com.cn']",
			"created": "2020-01-31T15:42:45.490Z",
			"modified": "2020-01-31T15:42:45.490Z"
		}, {
			"id": "indicator--5e31d8eb-8410-4859-8aff-2a53ac110004",
			"type": "indicator",
			"labels": ["misp:type=\"domain\"", "misp:category=\"Network activity\"", "misp:to_ids=\"True\""],
			"kill_chain_phases": [{
```

```
                    "kill_chain_name": "misp-category",
                    "phase_name": "Network activity"
                }
            ],
            "valid_from": "2020-01-29T00:00:00Z",
            "created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
            "pattern": "[domain-name:value =
'xdx.s4f5er4t5g1df23saadse.club']",
            "created": "2020-01-31T15:42:45.498Z",
            "modified": "2020-01-31T15:42:45.498Z"
        }, {
            "id": "indicator--5e31d8eb-3e38-4161-bec7-2a53ac110004",
            "type": "indicator",
            "labels": ["misp:type=\"domain\"", "misp:category=\"Network
activity\"", "misp:to_ids=\"True\""],
            "kill_chain_phases": [{
                    "kill_chain_name": "misp-category",
                    "phase_name": "Network activity"
                }
            ],
            "valid_from": "2020-01-29T00:00:00Z",
            "created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
            "pattern": "[domain-name:value = 'xor.0xbdairolkoie.host']",
            "created": "2020-01-31T15:42:45.500Z",
            "modified": "2020-01-31T15:42:45.500Z"
        }, {
            "id": "indicator--5e31d8eb-b8fc-42a3-a232-2a53ac110004",
            "type": "indicator",
            "labels": ["misp:type=\"ip-dst\"", "misp:category=\"Network
activity\"", "misp:to_ids=\"True\""],
            "kill_chain_phases": [{
                    "kill_chain_name": "misp-category",
                    "phase_name": "Network activity"
                }
            ],
            "valid_from": "2020-01-29T00:00:00Z",
            "created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
            "pattern": "[network-traffic:dst_ref.type = 'ipv4-addr' AND
network-traffic:dst_ref.value = '218.240.43.70']",
            "created": "2020-01-31T15:42:45.501Z",
            "modified": "2020-01-31T15:42:45.501Z"
        }, {
            "id": "indicator--5e31d8eb-c7f0-4d23-8baa-2a53ac110004",
            "type": "indicator",
            "labels": ["misp:type=\"ip-dst\"", "misp:category=\"Network
activity\"", "misp:to_ids=\"True\""],
            "kill_chain_phases": [{
                    "kill_chain_name": "misp-category",
                    "phase_name": "Network activity"
                }
            ],
            "valid_from": "2020-01-29T00:00:00Z",
            "created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
            "pattern": "[network-traffic:dst_ref.type = 'ipv4-addr' AND
network-traffic:dst_ref.value = '185.147.34.139']",
            "created": "2020-01-31T15:42:45.506Z",
            "modified": "2020-01-31T15:42:45.506Z"
        }, {
            "id": "indicator--5e31d8eb-282c-4eb4-b51c-2a53ac110004",
            "type": "indicator",
            "labels": ["misp:type=\"ip-dst\"", "misp:category=\"Network
activity\"", "misp:to_ids=\"True\""],
            "kill_chain_phases": [{
                    "kill_chain_name": "misp-category",
                    "phase_name": "Network activity"
                }
            ],
            "valid_from": "2020-01-29T00:00:00Z",
            "created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
            "pattern": "[network-traffic:dst_ref.type = 'ipv4-addr' AND
network-traffic:dst_ref.value = '185.147.34.106']",
            "created": "2020-01-31T15:42:45.507Z",
            "modified": "2020-01-31T15:42:45.507Z"
        }, {
            "id": "indicator--5e31d8eb-11b4-4942-a5a4-2a53ac110004",
            "type": "indicator",
            "labels": ["misp:type=\"ip-dst\"", "misp:category=\"Network
activity\"", "misp:to_ids=\"True\""],
            "kill_chain_phases": [{
                    "kill_chain_name": "misp-category",
                    "phase_name": "Network activity"
                }
            ],
            "valid_from": "2020-01-29T00:00:00Z",
            "created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
            "pattern": "[network-traffic:dst_ref.type = 'ipv4-addr' AND
network-traffic:dst_ref.value = '185.158.249.90']",
            "created": "2020-01-31T15:42:45.508Z",
            "modified": "2020-01-31T15:42:45.508Z"
        }, {
            "id": "indicator--5e31d8eb-07e8-442e-adcc-2a53ac110004",
            "type": "indicator",
            "labels": ["misp:type=\"ip-dst\"", "misp:category=\"Network
activity\"", "misp:to_ids=\"True\""],
                        "kill_chain_phases": [{
                                        "kill_chain_name": "misp-category",
                                        "phase_name": "Network activity"
                                }
                        ],
                        "valid_from": "2020-01-29T00:00:00Z",
                        "created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
                        "pattern": "[network-traffic:dst_ref.type = 'ipv4-addr' AND
network-traffic:dst_ref.value = '185.158.249.176']",
                        "created": "2020-01-31T15:42:45.510Z",
                        "modified": "2020-01-31T15:42:45.510Z"
                }, {
                        "id": "indicator--5e31d8eb-1a60-441a-96f3-2a53ac110004",
                        "type": "indicator",
                        "labels": ["misp:type=\"url\"", "misp:category=\"Payload
delivery\"", "misp:to_ids=\"True\""],
                        "kill_chain_phases": [{
                                        "kill_chain_name": "misp-category",
                                        "phase_name": "Payload delivery"
                                }
                        ],
                        "valid_from": "2020-01-29T00:00:00Z",
                        "created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
                        "pattern": "[url:value =
'http://fk.openyourass.club:80/goupdboke.exe']",
                        "created": "2020-01-31T15:42:45.511Z",
                        "modified": "2020-01-31T15:42:45.511Z"
                }, {
                        "id": "indicator--5e31d8eb-e088-4bde-af11-2a53ac110004",
                        "type": "indicator",
                        "labels": ["misp:type=\"url\"", "misp:category=\"Payload
delivery\"", "misp:to_ids=\"True\""],
                        "kill_chain_phases": [{
                                        "kill_chain_name": "misp-category",
                                        "phase_name": "Payload delivery"
                                }
                        ],
                        "valid_from": "2020-01-29T00:00:00Z",
                        "created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
                        "pattern": "[url:value =
'http://ae86.decode0x.fun:63145/cfg.ini']",
                        "created": "2020-01-31T15:42:45.512Z",
                        "modified": "2020-01-31T15:42:45.512Z"
                }, {
                        "id": "indicator--5e31d8eb-d028-4a3b-8437-2a53ac110004",
                        "type": "indicator",
			"labels": ["misp:type=\"sha256\"", "misp:category=\"Payload
delivery\"", "misp:to_ids=\"True\""],
			"kill_chain_phases": [{
					"kill_chain_name": "misp-category",
					"phase_name": "Payload delivery"
				}
			],
			"valid_from": "2020-01-29T00:00:00Z",
			"created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
			"pattern": "[file:hashes.'sha256' =
'a88ea84e7e13d770b7ad0d51ac7d836dc206a51bc7db2566d191a6d981c25dc2']",
			"description": "Samples communicating with
xdx[.]s4f5er4t5g1df23saadse[.]club",
			"created": "2020-01-31T15:42:45.513Z",
			"modified": "2020-01-31T15:42:45.513Z"
		}, {
			"id": "indicator--5e31d8eb-03f0-4508-acce-2a53ac110004",
			"type": "indicator",
			"labels": ["misp:type=\"sha256\"", "misp:category=\"Payload
delivery\"", "misp:to_ids=\"True\""],
			"kill_chain_phases": [{
					"kill_chain_name": "misp-category",
					"phase_name": "Payload delivery"
				}
			],
			"valid_from": "2020-01-29T00:00:00Z",
			"created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
			"pattern": "[file:hashes.'sha256' =
'31dcda7af03c4d887cc77e1ccc8162e459c7e4127cdf9c39964e55f86988d6f7']",
			"description": "Samples communicating with
xdx[.]s4f5er4t5g1df23saadse[.]club",
			"created": "2020-01-31T15:42:45.515Z",
			"modified": "2020-01-31T15:42:45.515Z"
		}, {
			"id": "indicator--5e31d8eb-c104-4a77-b601-2a53ac110004",
			"type": "indicator",
			"labels": ["misp:type=\"sha256\"", "misp:category=\"Payload
delivery\"", "misp:to_ids=\"True\""],
			"kill_chain_phases": [{
					"kill_chain_name": "misp-category",
					"phase_name": "Payload delivery"
				}
			],
			"valid_from": "2020-01-29T00:00:00Z",
			"created_by_ref": "identity--5df15c12-89fc-45a7-9620-
0044ac110004",
			"pattern": "[file:hashes.'sha256' =
'5b02416c689c30923961c52ff50605474b742918751a51c9bdbe6566ee36ca37']",
			"description": "Samples communicating with xdx[.]s4f5er4t5g1df23saadse[.]club",
			"created": "2020-01-31T15:42:45.516Z",
			"modified": "2020-01-31T15:42:45.516Z"
		}, {
			"id": "indicator--5e31d8eb-88b4-4010-b35c-2a53ac110004",
			"type": "indicator",
			"labels": ["misp:type=\"sha256\"", "misp:category=\"Payload delivery\"", "misp:to_ids=\"True\""],
			"kill_chain_phases": [{
					"kill_chain_name": "misp-category",
					"phase_name": "Payload delivery"
				}
			],
			"valid_from": "2020-01-29T00:00:00Z",
			"created_by_ref": "identity--5df15c12-89fc-45a7-9620-0044ac110004",
			"pattern": "[file:hashes.'sha256' = 'd2034b0d58bb1dc10da4aba27c8b55f84a91d474e6041eae45a7acb200da42a0']",
			"created": "2020-01-31T15:42:45.517Z",
			"modified": "2020-01-31T15:42:45.517Z"
		}
	]
}
```

References:

https://blog.talosintelligence.com/2019/09/panda-evolution.html
https://www.zscaler.com/blogs/research/recent-bulehero-botnet-payload
https://www.oasis-open.org/events/sites/oasis-open.org.events/files/Borderless_Cyber_2017%20final_Dec7_2017.pdf

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

This document is distributed as TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430