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

Date: 29 Nov 2019

Cyber Security Advisory: **WiryJMper Dropper**

Our trusted partner observed a new malware dropper “WiryJMper” that infects computers with Netwire malicious Payload which is prevalent in cyber threat landscape and poses as wallet application. Attack mechanism involves uncommon obfuscation that helps in evading antivirus engines. The threat drops a RAT named NETWIRE which has capabilities: Keylogging, Collecting information such as login credentials, chat messages, search keywords. Upon getting dropped on the targeted system it maintains persistence, creates registry entries, processes and involves activity of the anti-malware engine and virtual system software.

IOCs :

IP
46[.]166[.]160[.]158

MD5
1f634dfa20f0131b2e3d0d82d1447baf
e22c87f2d004148388691e4e4bcd380c
3532a62342d5ab07ed0e49b1f5c86636
50e8c7229c849eaa19281e4f1843aa59
6543cb84602eb8d0d2c6c90d74bcdc0b
07312d3d24628252e20547b7b63c1f2e
31b7eb84f5a557ed45931036e52d5a23
ec8eeb820ae59f0a81a9291d19659f0a
fe05f04facfd004bf207761f69d3bc7f
0e830752a5037b99e1c64577431e59e2
4bbb88cc61eafb92150f0b75597d123a
03bbab88f32d0b0aa9bae0b30f6bb883
74c45cb272eaed319efb004cbf255a92

Recommendations :

- Monitor Connection attempts towards the listed domains /IPs as a potential indicator of infection. The list may include compromised domains /IP resources as well.
- Disable macros in Microsoft Office products. For Windows, specific settings can block macros originating from the Internet from running.
- Deploy web and email filters on the network. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled script block logging and transcription enabled. Ensure that only signed script will execute in Power shell and practice “least privilege” of access.
- Enforce application whitelisting on all endpoint workstations. This will prevent droppers or unauthorized software from gaining execution on endpoints.

Reference: CERT-In

Disclaimer:

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