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

Date: 29 Nov 2019

Cyber Security Advisory: Adwind Campaign

Our trusted partner has reported a new widespread ADWIND RAT campaign targeting the utility sector. It is a java based malware which uses Malware-as-a-Service (MaaS) platform. It has the following capabilities: Stealing system information, cryptographic keys, and credentials Keylogging, Evading detection by prominent anti-malware solutions, Targeting the utility sectors using URL redirection to malicious payloads Aliases: jRat, Unrecom, AlienSpy, JSocket, Sockrat.

Analyst's Notes:
The attack functionality uses the previous mechanisms such as persistence techniques, registry modifications to steal sensitive data but the latest references point out a significant change in the attack technique. The infected attack chain involves an email attachment of multi nested JAR files which involves multiple way of execution.

IoCs :

MD5
3bdfd33017806b85949b6faa7d4b98e4
a32c109297ed1ca155598cd295c26611
a9175094b275a0aaed30604f7dceeb14
781fb531354d6f291f1ccab48da6d39f
0b7b52302c8c5df59d960dd97e3abdaf

IP
185[.]205[.]210[.]48

Recommendations :

- Check attachment's file type and never open files that could be a script (BAT, CMD, and VBS files) or another executable (EXE files).
- Keep checking the web proxy logs for users downloading the file having MD5 from an external host using a non-standard or high TCP port.
- Monitor Connection attempts towards the listed domains /IPs. The list may include compromised domains /IP resources as well.
- 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.
- Enforce application whitelisting on all endpoint workstations. This will prevent droppers or unauthorized software from gaining execution on endpoints.

Reference: CERT-In

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.

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