NOTICES

Notice No.	20221119-2	Notice Date	19 Nov 2022
Category	Others	Segment	General
Subject	Malware Advisory for Stockbrokers | Trading members | Clearing Members		

Content

Scope and Applicability: Stockbroker | Trading Members | Clearing Members.

With reference to our circular no 20221118-60 dated November 18,2018, regarding delay in settlements, noticed due to malware in CDSL. In regard to the malware detection at CDSL, members are hereby notified and requested to undertake appropriate actions as applicable to their environment. A brief description and immediate steps to be taken are mentioned below.

1) Following are the IOC's which should be validated and update in your anti-virus / anti-malware / firewall and other security devices.

Malicious Hash Value

MD5	SHA
cfcc2ec7f91c125b10d2eccd5f69db65	9fd79779d8d8644e901997f864bf8d95fdd6bdb138c61829d6bdb80a2b27abd6
951dce6731c5f3d2dae570597bc19d59	eee8150ba918a7ed099074a1b87a97b3c7f6648a763eedd7096acf16f40e0a73
ae59e82ddd8d9840b79bfddbe4034462	b02d57f1c4f7f233044a56fdc57c89b6cc3661479dc cc3b4cfa1f6f9d20cd893
bf4d4f36c34461c6605b42c456fa4492	8b26b750d84c2b825e31b1150751ec7e76fb3ec7270 431bc3cf15e61276ec0eb
56c9c8f181803ece490087ebe053ef72	12eb4ca3ec5b7c650123c9053ea513260d802aa524 86b7512b53fb7e86ec876b
f9ab1c6ad6e788686509d5abedfd1001	a56b41a6023f828cccaaef470874571d169fdb8f683a 75edd430fbd31a2c3f6e
5e54923e6dc9508ae25fb6148d5b2e55	f582e67056ca8c8ffb5d080c82c7aa587c3101cc7a87959fc7e8738fa1c61a87
bf331800dbb46bb32a8ac89e4543cafa	
ad444dcdadfe5ba7901ec58be714cf57	
1690f558aa93267b8bcd14c1d5b9ce34	
13b12238e3a44bcdf89a7686e7179e16	
3ee21dbaa37d0048e2e174cb41a664d6	
98991e46004f13a4cfe8adbbebab473d	

2) Malicious Command and Control (C&C) IP Subnet –

5[.]44[.]42[.]0[/]24

188[.]34[.]187[.]110

v5sqpe[.]dotm

Below are some precautionary measures for adherence.

a) In order to prevent infection, users and organizations are advised to apply patches to Windows operating systems and Microsoft Office products

b) Update firmware/patches for all network components and network products

c) Ensure anti-virus signatures are updated on all assets.

d) Block any suspicious IP addresses on firewall

e) Block USB usage

f) Ensure IPS/IDS signatures are updated.

g) Ensure Email Gateway solutions has all relevant updates for detecting possible mails that may bring Trojans/malicious content in the environment. Also block sensitive file extensions such as ".exe", ".rtf", ".vbs", and ".js" etc. , including macros - at the perimeter level

h) Make the users aware about this threat and ensure that users do not download any suspicious attachments and/or browse suspicious/malicious links

i) Maintain a backup of critical data and store it offline and/or at a different location

j) 24X7 SOC Monitoring.

Disclaimer:

a) The information contained in this notice has been extracted from trusted sources (Internal / External) and has been published as a guidance/awareness to members. As the future course of events with regards to this threat are not known, members are advised to keep a close watch on their systems to identify, timely detection and remediation of such threat.
b) Members shall act upon this notice at their own discretion after conducting appropriate impact/risk analysis to their specific environment.
c) Please note that the other exploit kits are also widely in circulation and available for download for free on the Internet and there are possibilities of attack vectors other than this threat which may exist/emanate. It is critical to perform a self-assessment against such zero-days/ exploit kits released in the wild.

Members are requested to take note of the above and take precautionary measures.

For and on behalf

Shri. Shivkumar Pandey
Group Chief Information Security Officer