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

Date: 05 Dec 2019

Cyber Security Advisory: New Fileless Botnet Novter Distributed by KovCoreG Malvertising Campaign

Our trusted partner reported about a KovCoreG campaign distributing new modular fileless botnet malware named as "Novter," also known as "Nodersok" and "Divergent". KovCoreG's attacks are socially engineered malvertisements that lure users into downloading a software package to update Adobe Flash application. However, it instead drops a malicious HTML application (HTA) file named "Player{timestamp}.hta". When the victim executes the HTA file, it will load additional scripts from a remote server (communication is RC4-encrypted) and run a PowerShell script. Powershell script executes Novter malware which communicates with Command and Control (C2) servers and downloads multiple JavaScript modules for different purposes.

IOCs:

Domains:
hxxp://37[.]1[.]223[.]178/qmuw3fwdfw/tell2.dat (call_02 module URL)
hxxp://37[.]1[.]223[.]178/qmuwwedfw/block_av_01.dat (block_av_01 module URL)
hxxp://1065695240[.]rsc[.]cdn77[.]org/aefgwehh/05sall.dat
(all_socks_05/Nodster's module URL)
hxxp://1118069275[.]rsc[.]cdn77[.]org/aefgwehh/05sall.dat
(all_socks_05/Nodster's module URL)
bo0uiomeglecaptures[.]net (KovCoreG's malvertising domain)
uoibppop[.]tk (technical support scam's domain)

IPs:

Novter's C2 servers:
5[.]61[.]42[.]103
37[.]1[.]221[.]156
37[.]252[.]8[.]85
37[.]252[.]10[.]66
91[.]247[.]36[.]14
92[.]187[.]110[.]52
185[.]243[.]114[.]53

Nodster's C2 servers:
69[.]30[.]231[.]60
69[.]197[.]179[.]20
92[.]187[.]110[.]52
103[.]195[.]100[.]246
176[.]9[.]117[.]194
192[.]187[.]97[.]156

Hashes:
1692f3b6619a6aca2e41a473d146f7a33 3f54e86ce507146e626e2d0f82b7c0d
022106b4da6d0049f6d3f790b0a8c4692 3f24a09f10071d49f47388da9d1c298
b7c803fbdc13b22471339fcef6e9dfb4a8 18ed2857576e81d67887067a285442
a82dd93585094aeba4363c5aeedd1a85 ef72c60a03738b25d452a5d895313875
fc523f842e9b17b2706e489ffb537d1837 52e371d731fccda03deacad4f50c6b
4f600b1c0db498dcdb71e5c2750b8636f 66fc7a0712e565ffb28fe4bd214b3b1
90f6e2a250175da3ddf03064e65c49eb0 33d52059be538f89565f4bb915e0e60

b7f76bfeb39f3ab30210ca78465927854f 712b7d332091c476cd703095d27386
ba04eacaa80bb5da6b02e1e7fdf3775cf 5a44a6179b2c142605e089d78a2f5b6
2f4a9ef2071ee896674e3da1a870d4efa b4bb16e2e26ea3d7543d98b614ceab9
77498f0ef4087175aa85ce1388f9d02d1 4aaf280e52ce7c70f50d3b8405fea9f
b2d29bb9350a0df93d0918c0208af081f 917129ee46544508f2e1cf30aa4f4ce
bf2cdd1dc2e20c42d2451c83b82804908 79b3515aa6c15ab297419990e017142
a7656ccba0946d25a4efd96f4f4576494 d5f1e23e6ad2acc16d2e684656a2d4f

Recommendations :

- Monitor Connection attempts towards the listed domains. The list may include compromised domains /IP resources as well.
- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution. Maintain up-to-date antivirus signatures and engines.
- 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
https://blog.trendmicro.com/trendlabs-security-intelligence/new-fileless-botnet-novter-distributed-by-kovcoreg-malvertisingcampaign/

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