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

Date: 30 Nov 2019

Cyber Security Advisory: Threat Actor TA505 Group Activity

Our trusted partner reported about threat actor TA505 group activities, distributing a new Remote Access Trojan (RAT) named ‘SDBbot’ via the Get2 downloader. TA505 is using Get2 as their initial downloader and it was noticed that the downloader eventually downloads FlawedGrace, FlawedAmmyy RAT, and Snatch as secondary payloads along with new SDBbot RAT. It uses new Microsoft Office macros along with Get2 downloader, which works in conjunction with a new Microsoft Excel macros, with downloader being embedded into the Microsoft Excel file as an image. A separate loader DLL is used to execute the SDBbot RAT payload.

Analyst's Note:

It is reported that TA505 cyber espionage group which is known for spy campaigns targeting financial institutions. This group uses phishing and social engineering techniques to compromise systems. It distributes malspam emails containing URL shortened links for redirecting victims to a landing page that in turn links to an excel sheet or may distributing Microsoft Excel and .ISO attachments in the mail itself. It is also reported that threat actor is behind the distribution of a backdoor “ServHelper” [CMTX-P09082019] and downloader malware, AndroMut and Gelup downloader [CMTX-P08072019]. The same group is also behind Neutrino bot, Dridex banking Trojan[CMTX-P03072019], Necurs Botnet, Locky ransomware [CMTX-P011022018].

IOCs:

Domain/IPs/URLs:

212[.]80[.]216[.]172
37[.]59[.]52[.]229[:]53
95[.]169[.]190[.]29
102[.]130[.]114[.]246
5[.]149[.]252[.]171
167[.]114[.]194[.]56
170[.]75[.]175[.]209
147[.]135[.]204[.]64
103[.]75[.]118[.]231
192[.]99[.]211[.]205
94[.]44[.]166[.]189
185[.]176[.]221[.]64
185[.]86[.]148[.]144
195[.]123[.]228[.]14
95[.]217[.]16[.]248
45[.]8[.]126[.]7
185[.]238[.]3[.]76
195[.]123[.]242[.]250
hXXps[:]//update365-office-ens[.]com/rb8
hXXps[:]//windows-update-sdfw[.]com/trase
hXXps[:]//office365-update-en[.]com/frey
hXXps[:]//office365-update-eu[.]com/frey
hXXps[:]//en-gb-facebook[.]com
hXXps[:]//news-server-drm-google[.]com
hXXps[:]//static-google-analtyic[.]com
hXXps[:]//windows-wsus-en[.]com/version
hXXps[:]//windows-wsus-en[.]com
hXXps[:]//windows-msd-update[.]com/2019
hXXps[:]//windows-cnd-update.com
hXXps[:]//windows-fsd-update[.]com/2020
hXXps[:]//windows-sys-update[.]com/2021
hXXps[:]//windows-me-update[.]com/2021
hXXps[:]//windows-se-update[.]com/2022
hXXps[:]//office365-eu-update[.]com/2023
drm-server13-login-microsoftonline[.]com

Hashes(SHA512):

```
8916a09f205910759edb082175bf2808d2acae00c7ded5bb8c9c174f60ebe152
c2f99a2bba225fe3ab49cb952e418b2ab29ba7f2e34db6cf9bc51b0349d0acd8
84f7c3fcf3a53f37ecbb21d0b9368d332901fe8c3f06b3d1a92123479c567c95
f4fed12625e2b983b918f239bf74623746cfc6b874717e6d8dd502a45e073d32
f4fed12625e2b983b918f239bf74623746cfc6b874717e6d8dd502a45e073d32
99c76d377e1e37f04f749034f2c2a6f33cb785adee76ac44edb4156b5cbbaa9a
6b3aa7a7a9771f7464263993b974c7ba233ec9bd445ea635e14a0764523cbef
133121ea82269ec943847e04cb070109ca94612aed23a471868937f119ae8175
edb838be33fde5878010ca84fc7765c8ff964af9e8387393f3fa7860c95fc70b
9eaad594dd8038fc8d608e0c4826244069a7a016ffd8881d8f42f643c972630f
4efcc22da094e876346cff9500e7894718c8b6402ff3735ea81a9e057d488849
e3ec2aa04afecc6f43492bfe2e0d271045ab693abfa332a2c89a5115ffe77653
34f3733177bbe3d7a8d793fe3c4fd82759519ddc6545b608613c81af9019a52d
f27c5375046c734dfe62d2efe936b92cd519da091d04f22db713514caafece2a
0683d9f225d54d48081f53abd7d569b32bc153d98157a5a6b763bc3cf57a6ad6
cfce53335bbe61de612353cdd83ce17953b1f230c576ed6de1463626aff9088e
```

Recommendations:

- Enable code signing feature for all types of users in Power script so that only signed script will execute in Power shell.
- Monitor suspicious network activities and all outbound traffic especially the traffic that is destined to newly-registered domains or belongs to the category: “Uncategorized” should be inspected closely or blocked.
- Disable macros in Microsoft Office products.
- Block the attachments of file types: exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf.
- Enforce application whitelisting on all endpoint workstations.
- Maintain up-to-date antivirus signatures and engines and keep operating system patches up-to-date.
- Users must keep their device firmware device up-to-date with the latest releases to prevent any potential attacks.

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