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

Date: 30 Nov 2019

Cyber Security Advisory: Calypso APT Campaign

Our trusted partner reported a surge in malicious activity from threat actor Calypso. The initial mode of spreading the infection is via exploiting a vulnerability or guessing default credentials for remote access of victim's machine. When attacker successfully gains the access to victim's machine, they upload their web shell through which attacker upload utilities, execute commands and distribute malware inside the network. Attack spreads within the network either by exploiting vulnerability MS17-010 or by using stolen credentials. It drops malware (including well-known tools like Mimikatz, and tools like EternalBlue and EternalRomance) to steal confidential data.

Analyst's Note:
In order to evade detection it uses a variety of legitimate administrative tools like SysInternals, TCP Port Scanner, WMIExec etc in its attack campaign. Attacker group is reportedly also using trojans like PlugX RAT, Byeby trojan apart from using Calypso RAT for performing their malicious activity.

IOCs:

Hashes(SHA512):
C9C39045FA14E94618DD631044053824
F0F5DA1A4490326AA0FC8B54C2D3912D
CB914FC73C67B325F948DD1BF97F5733
0171E3C76345FEE31B90C44570C75BAD
17E05041730DCD0732E5B296DB16D757
22953384F3D15625D36583C524F3480A
1E765FED294A7AD082169819C95D2C85
ACAAB4AA4E1EA7CE2F5D044F198F0095
85CE60B365EDF4BEEBBDD85CC971E84D
1ED72C14C4AAB3B66E830E16EF90B37B
CB914FC73C67B325F948DD1BF97F5733
974298EB7E2ADFA019CAE4D1A927AB07
05F472A9D926F4C8A0A372E1A7193998
E1A578A069B1910A25C95E2D9450C710
847B5A145330229CE149788F5E221805
CCE8C8EE42FEAED68E9623185C3F7FE4
43B7D48D4B2AFD7CF8D4BD0804D62E8B
617D588ECCD942F243FFA8CB13679D9C
5199EF9D086C97732D97EDDEF56591EC
06C1D7BF234CE99BB14639C194B3B318
Domains/IPs:
23[.]227[.]207[.]137
45[.]63[.]96[.]120
45[.]63[.]114[.]127
r01[.]etheraval[.]com
tc[.]streleases[.]com
tv[.]teldcomtv[.]com
krgod[.]qqm8[.]com
Recommendations:

- Keep your operating system, application servers, SQL servers, browsers, browser plugins & Antivirus Software up-to-date with the latest patches.
- Maintain and actively monitor centralized host and network logging solutions after ensuring that all devices have logging enabled and their logs are being aggregated to those centralized solutions.
- Create / Configure SRP's / APPLOCKER based on SHA/MD5 hashes to prevent malware running them on the client machines.

- Add appropriate Host firewall rules, Active Directory structuring, and/or Group Policy settings, to stop communication between systems and increase the survivability and defensibility of a network under attack and deter lateral movements.
- Disable the execution of MACROS in office docs, Remote Desktop Connections and employ least-privileged accounts. If not required, consider disabling Powershell, windows script hosting.
- Establish a Sender Policy Framework (SPF) for your domain.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type".
- Strict External Device (USB drive) usage policy. Exercise caution when using removable media (e.g. USB thumb drives, external drives, CDs, etc.).
- Users are advised to patch their window SMB server with latest patch to avoid its exploitation.
- Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths.
- Block the attachments of file type: exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|

Reference: CERT-In

Link: https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/

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