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

Date: 19 Nov 2019

Cyber Security Advisory: Dark Universe APT framework

This data is to be considered as **TLP:AMBER**

Our trusted partner has reported that a surge in malicious activity by threat actor gang name as Dark Universe is seen. The initial infection vector used by this gang is via Spear phishing which carry malicious document as attachment. As victim opens an attached malicious Microsoft Office document, the executable file embedded in the documents extracts two malicious files from it updater.mod and glue30.dll, and saves them in the working directory of the malware. After that, it copies the legitimate rundll32.exe executable into the same directory and uses it to run the updater.mod library.

Analyst's Notes:

- The malware contains all the necessary modules (keylogging, executing commands from the command and control, and maintaining persistence) for collecting all kinds of information about the infected system.
- Finally malware start build communication with command and control server controlled by attacker. Attacker used cloud storage and for every victim, attacker create a new account within that storage and uploaded additional malware modules and a configuration file with commands to execute upon that victim machine. A list of Indicators of compromise is provided below for action.

IOCs :

Hashes
C2EDDA7E766553A04B87F2816A83F563
D716917BEFE0767021DE7B2BA9E17039
C692B36632038A6ABFF64E2DE284924E
4033E595B8C06109F83A46C6523538FA
27D0FB0874182939DBDB6323E435ADC8
755B555BC21AB602D2404BE5B612C3BE
639F510C475159E78071E9E2A30AD5C7
1ADDEE050504BA999EB9F9B1EE5B9F04
1FFD19C73B0DEDB1ED55A48066346C21
F7927D471947F3AEE283AB367FAC7E2B
497FB564DFBC57C5DD3C0AB999746F64
4B71EC0B2D23204E560481F138833371
764A4582A02CC54EB1D5460D723AE3A5
6637ECC7B8AD355CB3027A0CB1AC56C3
8835FE4383E10D211C4177B8C1C79D5B
4E24B26D76A37E493BB35B1A8C8BE0F6
8E5F8C722314E528C01AFB9A291FA1BB
08223170F9E9D7C4B824DF63E403E843
BBBD8BDD2A478BBDC72B5C1B591BC5E2
73B0813525D9316D5AF6D754776E463A
71D36436FE26FE570B876AD3441EA73C
E50FDE6F225A58D06122FE4BB9DE3A2F
405EF35506DC864301FADA6F5F1D0711
A07564DE35BD83D26744984AE9809843
DA0B55A486EFEA230DA9ACF3054EC7AD
FC2B996A8FD9CC6EED5F53576283F7A5
5291830985944C80C4BF2FE1FAFDE9E3
D5B28F82B5CBC5A1725716342520A94C

Domain/IPs
webdav.mydrive[.]ch
adrive[.]com
katejackson.no-ip[.]biz

File Structure
%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Reorder

Recommendations :

- Monitor Connection attempts towards the listed domains.
- Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled script block logging and transcription enabled.

- 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.
- Enforce application white listing on all endpoint workstations.
- Both ingress and egress traffic of the listed Domains and all hash values should be kept under an active watch-list in the respective / supported endpoints and security solutions.
- Disable macros in Microsoft Office products. Some Office products allow for the disabling of macros that originate from outside of an organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can block macros originating from the Internet from running.
- 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.

- Add appropriate Host firewall rules, Active Directory structuring, and/or Group Policy settings, to stop communications between systems and increase the survivability and defensibility of a network under attack and deter Lateral Movements.
- Monitoring 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.
- Keep operating system patches up-to-date.

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.

This document is distributed as TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

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