UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00171

APT “LUMINOUSMOTH” DROPS FAKE ZOOM APP

DATE ISSUED: 19th July 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

A new campaign begun by LuminousMoth is not using spray-attack techniques, but is carefully selecting its victims with “almost surgical precision” targeting them A spear-phishing attack to create an Advanced Persistent Threat (APT) and spread via connected devices.

BREAKDOWN

LuminousMoth has also managed to fly under the radar by appearing to have low volume attack spread, making it harder for researchers to detect. Initially spread by a spear-phishing attack – a highly targeted, selective method of conducting a phishing attack, containing a Dropbox link that fetches an RAR archive, by downloading malicious DLLS disguised as a .docx file. The APT is then established by dropping a CobalStrike beacon and a fake Zoom application, sideloading two executables to spread. One method it is using is to propagate by copying itself on to connected USB drives. However, it has a high-infection rate which suggests that there may be a further, undetected propagation method. The network infrastructure of this group has been observed to overlap with other cybercrime groups Mustang Panda (a.k.a. HoneyMyte, TA416 or RedDelta). Currently notably targeting the Philippines, it is only a matter of time before other attack groups pick up these techniques and begin to deploy their own attacks.

REMEDIATION STEPS

- Educate users on the dangers of social engineering and phishing attacks and what to do with emails they deem to be suspicious.
- Remote the ability for user devices to run executable files.
- Run Next Generation Anti-Virus endpoint detection on all devices to detect anomalous behaviours and quarantine known malware.

REFERENCES & RESOURCES

SecureList by Kaspersky	https://securelist.com/apt-luminousmoth/103332/
Threatpost	https://threatpost.com/zoom-apt-luminous-moth/167822/