IMPORTANT CYBERSECURITY NEWS: EARTH KURMA TARGETS SOUTHEAST ASIA WITH ROOTKITS AND CLOUD-BASED DATA THEFT TOOLS

Vairav Cyber Security News Report

Date: April 28, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A recent cybersecurity campaign involving a new APT group called **Earth Kurma** has targeted government and telecommunications sectors across Southeast Asia, including the Philippines, Vietnam, Thailand, and Malaysia. Using custom malware, kernel-level rootkits, and trusted cloud services like Dropbox and OneDrive for data exfiltration, the attackers have established persistent footholds and engaged in widespread espionage. This operation highlights the evolving threat landscape where trusted platforms are leveraged for stealthy cyberattacks, significantly increasing business risk.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: Earth Kurma, an advanced persistent threat (APT) group active since at least June 2024, has executed a sophisticated cyber-espionage campaign. They used custom malware, rootkits (e.g., KRNRAT and Moriya), and cloud services to exfiltrate sensitive documents. The campaign relies on "living-off-the-land" (LotL) techniques, minimizing detection by using legitimate system tools like syssetup.dll. Attackers utilized tools such as TESDAT, SIMPOBOXSPY, and ODRIZ for stealing and uploading data.

Identification: Trend Micro researchers identified the campaign through their telemetry and threat hunting activities.

Threat Actor: Earth Kurma is an Advanced Persistent Threat (APT) group whose major motivation is Cyberespionage (intelligence gathering). Some overlaps with APT ToddyCat activities, but definitive attribution remains uncertain.

Affected Entities/Industries: Government agencies and Telecommunications providers in Southeast Asia in countries like Philippines, Vietnam, Thailand and Malaysia

Potential Impact:

- Espionage and sensitive data theft

- Credential harvesting via keyloggers
- Persistent system compromise with rootkits
- Reputational and operational damage for targeted entities

Exploitation Methods:

- Use of trusted cloud platforms (Dropbox, OneDrive) for data exfiltration
- Kernel-level rootkits for stealth persistence
- Open-source penetration tools (e.g., Ladon, FRPC, WMIHACKER)
- Keylogger KMLOG for credential harvesting
- Living-off-the-land techniques using legitimate system components

RELATED THREAT INTELLIGENCE & IOCs

Malicious IPs

- 103[.]238[.]214[.]88
- 149[.]28[.]147[.]63
- 166[.]88[.]194[.]53
- 185[.]239[.]225[.]106
- 38[.]147[.]191[.]103
- 38[.]60[.]199[.]225
- 45[.]77[.]250[.]21

Suspicious Domains

- dfsg3gfsga[.]space
- igtsadlb2ra[.]pw
- ihyvcs5t[.]pw
- vidsec[.]cc

Malware Hashes (SHA256)

- 004adec667373bdf6146e05b9a1c6e0c63941afd38e30c2461eaecb707352466
- 0a50587785bf821d224885cbfc65c5fd251b3e43cda90c3f49435bb3323d2a8b
- 10898b74b612b1e95826521c5ccf36f7a238f5d181993c3c78c2098fcfdc1f3f
- 131bacdddd51f0d5d869b63912606719cd8f7a8f5b5f4237cbdb5c2e22e2cba2

- 1ab42121bb45028a17a3438b65a3634adb7d673a4e1291efeabf227a4e016cfb
- 1c350d09c1cd545d54c38cd03aba3fd4eb0e8d97a3ba6c3744cc33ed92cb9a48
- 1e48967e24d4ae2ac2697ef09c0f2702285825831bd516cb3be8859496fd296f
- 1f3f384e29eab247ec99d97dfe6a4b67110888e4ad313b75fa9d0beceef87e93
- 1f5f6cc1cbf578412ea5279dbdb432eda251309695513a74de66063ab02789f1
- 2c9b8e4852181d51ff72dc6dec78bef014db8af83d30c05c3e9c5eb060278730
- 2e87615142170a7510e26f94790bfb81df4d499a9f530d0bd8fe0fb1575b17f8
- 34366323262346e10d8780bad9d30c6d4d747e4ec543243be76f33b7c028ea36
- 37a397a2482b37d19d58588c0a897a08111b74d122c21542f1bf852ae83e1db0
- 383aa73fe72caf268ce0874ebbcd13fc4c9e1e5c6200cdd66862de7257942cea
- 398234b692a80a424939e98a2d96a705ce3fd9d61950420b5f2af45890abc48e
- 4198b4ec5bb0c72112e9cf835686c33b9a97037acfb7727e494046a73106e938
- 45e1138f2b8e822cbd4573cb53104b402ae26dcddb42c70534cf024a8bc6db66
- 49ab6e2b5e378c74d196aecac4e84c969c800051167c1e33d204531fabd17990
- 4ae186ee19d0d3e246dc37ac722a27d5297d2577de59b8583c97897480290bc1
- 54e14b7742801970c578fad2ec2a193334ca8a17b60ee18dd6ec0fbfc8ce900b
- 612a5fcb7620deef45a021140b6c06ab9c0473dce5b7e4a54960e330a00c90f3
- 6190b13df521306bfa7ee973b864ba304ee0971865a66afbe0b4661c986099f4
- 66edb72f6f7c8cad23c6659a81fa023f57c1a86c7d7b7022f1453b177f2b3670
- 6bbbb227d679ea00f0663c2e261d5649417d08285f9acc1fd80e806ddea08403
- 6ef3a27fdca386fe093c12146cd854d9ae6b42ca637950ca46bfd364ceab5b53
- 73afc6af6fdfcaf9832aa2975489271bad7c8ea58679f1a2ddd8f60b44cc4a13
- 75cc8474abb1d9a06cd8086fede98958653d013fb7ff89bbc32458b022a8fc94
- 823a0862d10f41524362ba8e8976ddfd4524c74075bd7f3beffa794afb54f196
- 8414136128f73fa7e29032df7b8115bc89832c57e2602d81de1e520cc2d7958d
- 85e78a1b0a78e5d921c89241aaadd505d66dc4df29ca7d8a81098f42487ba350
- 876c822f333e812041af24ae80935a830ca5016f9aaf2e8319ebb6cab1f9d7d0
- 8c703148567cb66fe27bc07d18de58aa36aa84a49f1ce7545e9ec56378857d3d
- 8ca1ffbd3cd22b9bead766ebd2a0f7b2d195b03d533bacf0cb8e1b1887af5636
- 8e6583cca6dd4a78bdc0387c7f30334ab038e5c77848f708fe578e60dd8d9e00

- 96b407856889c920a49f921d925118a130b904e99f9fe43a87342c680ffb9f27
- a359a06fbc6b5cf5adf7f53c35145b28f3c8a70f6998631090021825aea08e22
- aa925a5a8a7d5b36a66431f4968bd1003d1bbb6cb3ff6d03d9e3e0143c48382b
- aef3407310de48e13575c3d98b660ab7ddafb7efe3f4909682907ac286062392
- b26e8e0be066ee0b86f8fb2b0a703717ebbf34c8a33ef9a6f8f164ad012f1746
- c0326a0cd6137514ee14b6ac3be7461e8cf6c6adec74d087fd30cb06b91ecda2
- c6f73268eba553c7991f876a166440f5b4d519dea6b13bc90583fde1e89e81ed
- d3d2355b1ffb3f6f4ba493000e135dfd1b28156672e17f0b34dfc90cc3add352
- e143c15eaa0b3faccc93ce3693960323dbaa683ac9ce30382e876690278dfefa
- ec9220cf8208a3105022b47861d4e200672846ef484c1ea481c5cfd617cb18dc
- f3916c414db0f660d488c9d3aaa8355f3eb036ca27a9c606fe7e5e1a9bd42b38
- f52d9355b9efb6a1fcb32b890c5c373274df21ce38050d49416f469be95dc783
- f9892636093266a01ed6f0486c00189d2eeb532a3086660490f4efeb6d026487

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Monitor Dropbox and OneDrive traffic for anomalous activity.
- Review systems for signs of KRNRAT, Moriya, or TESDAT malware.
- Check for unauthorized syssetup.dll activity.

Security Best Practices

- Implement strict access controls for cloud services.
- Enhance monitoring and alerting for lateral movement tools (e.g., NBTSCAN, FRPC).
- Apply behavioral-based detection mechanisms for LotL activities.

For Advanced Security Teams

- Conduct memory forensics to detect stealthy in-memory loaders.
- Deploy kernel-level defenses and EDR solutions capable of detecting rootkit behavior.
- Establish honeytokens to detect credential harvesting attempts.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/04/earth-kurma-targets-southeast-asia-with.html
- https://www.trendmicro.com/en_us/research/25/d/earth-kurma-apt-campaign.html

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com