**Cyber Security Advisories**

**Date: 30 October 2024**

1. **TA-APT-2024-10-17-007**

It has been discovered that state-sponsored groups or cybercriminal organizations are targeting various sectors, including government defence, external affairs, finance, technology, and critical infrastructure for espionage and data theft for sabotage and disruption.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Domain:

formainservercheap.com

IP:

188.208.141.218

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-10-18-011**

During analysis of Mirai samples over a week, following IOCs have been found. There are couple of things to be aware of while looking at this data:

Network IOCs may be associated with binary distribution or one of the "cnc" or "report" functions.

Network IOCs are identified from newly identified samples but may themselves not necessarily be new.

Because of nature of the static analysis, there is MODERATE confidence in accuracy of the network IOCs.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Domains:

drumev.eu

vpn.komaru.today

IPs:

93.123.85.135

103.238.235.110

Hashes:

026f74e7949f2803d79b733a33b53f8b1d7c65794cf1ef3a0ab841672ce5950a

1837837fd3e6dd85bd8980a530874fd66012ffca89c619849ff9abf86fd3f8a7

188bce5483a9bdc618e0ee9f3c961ff5356009572738ab703057857e8477a36b

1ca83df90274b61dc989daabfcbc01d9e03418ff303c51cc88458621ced820a3

1f4aae34ffc30b54cac44e2c5d42396e86d4b2cd05027be83c165a55d10fabd2

21e13bbe2df4004cedf4e5433ce416f6086ab94ab7f3dcefc93ec44dddef9899

3ec2220ac979688ea252f4bd6a8890593d4466055cc3dadebc0a02893a3dd6c4

4664e65d0f2c500ad8ff7b75c8a7567af5830cc2dc4ebfeeb7d209cddf033994

59e7d5768aa82742c8e2141151ce7b69d14a38fda945e83deef0827b840f96c7

640226b21ab618254e89e2ab714d27b113c5e5320c9ff03ce8d2332bbf43c571

65aa799f73ae9461173843390420a5cdbe3bcc1057cc786214f946cd4336b34c

67a8993bd9eb5892b12d5bb00363588935e71e8aec7591afa60cda5f5de66952

7251c3e03bc11c51d3b940577bd15c7ae9f3901bd404ad8600390b08d163e3f6

985d99722968cb49173b8c6cf81cd09983cb3fb8c08003b5338df2dcf2110b78

9a6b1db277b19234c80ec6fa48ab29ef3a8576b39b3155e09d4bcdb6f438e617

9cec900ec03ce1bcc1fe67841cfd232b3df6c998f0d58f4f56cfb30ee708548f

9da07ff4b9bdfdc46444fb49b398ae7d7a1ac9ad280458c03954d16d8aa3b456

a4ead190d24879d63034bc1f5b1c036d60072391fdc734f2fc65f02cc59d1d19

cd2ccacdee3df9a4658bbb2f9d89f5efdc6955e2566c3d341f83aae22ed1da99

cda634b082f19486ae35f4abbe5ae88f96946ab1319f72e6f5291217b48d454c

d2cdab0ef88e57347c3ea3db7d842edcd8a8d1d71847a8e66be391e5d0b9332d

d7564c7e6f606ec3a04be3ac63fdef2fde49d3014776c1fb527c3b2e3086ebab

d8458bf9845a6b4caf29b9910ed95a9521f34b159f3a763946f4f9a7167ded34

e08ba5f863c37697e9292aa6c387117327a17483d5bb72eba3b52d4c26492851

e708b2fc943bbb9782427435b3a39b7f80d9ef06946792119581c700b8c87d39

ec31feb0658ea418c2d0083f814942929ec3649c2b72a4f161a137d46c282214

f32da3a630777fd9da1cbf7587d1afdc612ba1dd5a8e38302d7cdb761f4e0c0a

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-10-18-008**

It has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Domains:

sebi-gov.info

mahagov.info

gov.in.nha.in

ail-gov.ink

email.gov.in.webiaf.link

gov.in.webiaf.link

in.webiaf.link

webiaf.link

www.washimpolice.gov.in.mengjihomedecor.com

indiapost-gov-in.help

indiapost-gov-in.sbs

hydrobharat.gov.in777.userhouse.com

mailgov.in.net

mail.mof-gov.info

www.irs-gov.info

ww25.cpcontacts.irs-gov.info

cpcontacts.irs-gov.info

ww25.cpcalendars.irs-gov.info

cpcalendars.irs-gov.info

ww25.autodiscover.irs-gov.info

autodiscover.irs-gov.info

ww25.webmail.irs-gov.info

webmail.irs-gov.info

ww25.mail.irs-gov.info

mail.irs-gov.info

ww25.cpanel.irs-gov.info

cpanel.irs-gov.info

ww25.webdisk.irs-gov.info

webdisk.irs-gov.info

ww25.irs-gov.info

www.dc.crsorgi.gov.in.auths.info

www.crsorgi.gov.in.web.inbex.info

www.dc.crsorgi.gov.in.dcindex.xyz

www.dc.crsorgi.gov.in.workfast.in

www.dc.crsorgi.gov.in.i.verifycertificatecrs.live

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-10-18-009**

It has been observed that threat actors hide malicious phishing pages behind legitimate CAPTCHAs, such as Google’s reCAPTCHA and Cloudflare’s Turnstile. The phishing emails contained a benign link that led to a legitimate page on either Publuu or ISSUU, digital document publishing sites. The page prompted the victim to click on a PDF document, which then displayed a CAPTCHA and ultimately resolved to a spoofed Microsoft 365 authentication page. This attack chain is likely to be challenging for automated email reputation systems to identify as malicious, as the phishing email did not contain any malicious content, and the phishing page was hidden behind a CAPTCHA.

The adversary is using a compromised email account to create a Cloudflare account. Then, the threat actor updated mailbox rules on the compromised account to hide email messages related to Cloudflare, possibly to prevent the account owner from noticing this activity. The threat actor may have intended to use the compromised account to expand their infrastructure, by leveraging it to send phishing messages that contain Cloudflare URLs that redirect the victim to a malicious phishing page that is protected by a Cloudflare CAPTCHA. The efficacy of CAPTCHAs in protecting malicious content used by threat actors.

The phishing kit named FishXProxy, is highly sophisticated with automated features that allow even minimally skilled cybercriminals to conduct attacks. The kit’s features allow criminals to opt to leverage Cloudflare’s CAPTCHA to protect malicious content from automated scanners and will even automatically present CAPTCHA if automated security crawlers are detected. Phishing kit developers often offer a tiered pricing structure with inexpensive options that make these tools easy to acquire.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Domains:

buyubaby.com

getcompright.com

dubaicompanieslist.com

ceremophies.com

Koffestore.co.uk

Preparadonn.credit

Budged.net

ynjac.com

alpinemetalteck.com

Morrisconsulting.eu

jankoors.com

Catholicentury.net

clickandflirt.com

happyworking.com.pe

campairing.com

lfdocatin.com

cpcseguro.com

filternus.com

khobregankghaz.com

patriotmindful.com

Creditron.org

attacklaced.com

cpaberg.com

Silkroadvmt.ae

spesbonaconstruction.com

4kmedia-market.com

theexpertkingdom.com

becoquin.com

Financestackle.one

itatrckrone.com

tructions.com

red2be.com

amburghley.directory

Gwshop.ru

Expreserted.net

Newsletterbroadcast.net

sspgtravel.com

archerite.com

keywoodenum.com

fadrcaiuwjaaw.click

glgibson.com.au

globaldiasporanews.com

gafm.com

Fastlog.org

insightsofa.com

songwrait.com

YARA rule to detect captcha gated redirects:

rule logging\_sig\_Captcha

{

meta:

author="mmolyett"

date="2024/06/06"

brand="captcha"

strings:

$recaptcha\_a = "g-recaptcha-bubble-arrow"

$recaptcha\_b = "recaptcha/api2/bframe"

$recaptcha\_c = "pointer-events: none;"

$recaptcha\_d = "allow-forms allow-popups allow-same-origin allow-scripts allow-top-navigation allow-modals allow-popups-to-escape-sandbox"

$human\_check\_a = "Are you human?"

$response\_class\_a = /"g-recaptcha-response"/

condition:

(any of ($response\_class\_\*)) and (

all of ($recaptcha\_\*) or

all of ($human\_check\_\*)

)

}

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-10-18-010**

It has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Domains:

fcsupgovin.in

postngov.ink

indiapiost.top

postn.ink

postigov.top

postgovi.top

dhli.ink

dhlc.ink

indiaposttgovin.top

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-APT-2024-10-21-008**

It has been observed that threat actors are primarily targeting Indian defence establishments and government agencies to perform cyber espionage operations with the intention of collecting sensitive information.

Please find below malicious IPs which are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IPs:

APT 36 aka Transparent Tribe

206.189.134.185

State Sponsored Threat Actors:

116.204.211.139

139.84.165.29

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **VA-2024-10-21-010**

Vulnerability in Ai3 QbiBot

A lack of proper access control vulnerability has been discovered in the password reset feature of Ai3 QbiBot.

CVE ID: CVE-2024-3777 (Critical)

Moxa Security Updates

Moxa has released security updates to address missing authentication and OS command injection vulnerabilities in Moxa's Cellular Routers, Secure Routers, and Network Security Appliances.

CVE ID: CVE-2024-9137 (Critical), CVE-2024-9139 (High)

GitLab Security Updates

GitLab has released updated versions 17.4.2, 17.3.5, and 17.2.9 for GitLab Community Edition (CE) and Enterprise Edition (EE) to resolve multiple vulnerabilities.

CVE ID: CVE-2024-9164 (Critical), CVE-2024-8970 (High), CVE-2024-8977 (High), CVE-2024-9631 (High), CVE-2024-6530 (High), CVE-2024-9623 (Medium), CVE-2024-5005 (Medium), CVE-2024-9596 (Low)

Vulnerability in Mecha CMS

A directory traversal vulnerability has been discovered in Mecha CMS. The affected version is Mecha CMS 3.0.0.

CVE ID: CVE-2024-46446 (Critical)

Security Update for Wordpress Plugin

WordPress has released security update to resolve Remote Code Execution vulnerability in the Hunk Companion plugin for WordPress. The affected versions are Hunk Companion plugin for WordPress up to and including, 1.8.4.

CVE ID: CVE-2024-9707 (Critical)

Vulnerability in Zimbra Collaboration

A vulnerability has been discovered in postjournal service of Zimbra Collaboration that allows unauthenticated users to execute commands. The affected versions are Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9 and 10.1 before 10.1.1.

CVE ID: CVE-2024-45519 (Critical)

Mozilla Released Security Updates

Mozilla has released security updates to address multiple vulnerabilities in Firefox 131.0.2, Firefox ESR 115.16.1 and Firefox ESR 128.3.1. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-9680 (Critical)

Adobe Security Updates

Adobe has released security updates to address multiple vulnerabilities in Adobe software products. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-45115 (Critical)

Vulnerability in SECOM WRTR-304GN-304TW-UPSC

An OS command injection vulnerability has been discovered in SECOM WRTR-304GN-304TW-UPSC. The affected product is WRTR-304GN-304TW-UPSC V02.

CVE ID: CVE-2024-10118

Vulnerability in Wireless Router WRTM326 from SECOM

An OS command injection vulnerability has been discovered in wireless router WRTM326 from SECOM. The affected products are WRTM326 before version 2.3.20.

CVE ID: CVE-2024-10119

Security Update for Wordpress Plugin

WordPress has released a security update to resolve a privilege escalation vulnerability in the UserPro plugin for WordPress. The affected versions are UserPro plugin for WordPress up to and including, 3.6.0.

CVE ID: CVE-2024-9863 (Critical)

Security Update for Wordpress Plugin

WordPress has released a security update to resolve an authentication bypass vulnerability in the Nextend Social Login Pro plugin for WordPress. The affected versions are Nextend Social Login Pro plugin for WordPress up to and including, 3.1.14.

CVE ID: CVE-2024-9893 (Critical)

Oracle Released October 2024 Critical Patch Update

Oracle has released its critical patch update for October 2024 to address 334 vulnerabilities across multiple products. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-45492 (Critical), CVE-2023-38408 (Critical), CVE-2024-4577 (Critical), CVE-2023-6816 (Critical), CVE-2022-2068 (Critical), CVE-2024-37371 (Critical), CVE-2022-36760 (Critical), CVE-2022-34381 (Critical), CVE-2024-5535 (Critical), CVE-2024-21216 (Critical), CVE-2024-28752 (Critical), CVE-2022-23305 (Critical), CVE-2023-38545 (Critical), CVE-2024-29736 (Critical), CVE-2024-21172 (Critical), CVE-2022-46337 (Critical)

Vulnerability in ChanGate

A SQL Injection vulnerability has been discovered in the Property Management System of ChanGate that allows to inject arbitrary SQL commands to read, modify, and delete database content.

CVE ID: CVE-2024-9972 (Critical)

Security Update for Wordpress Plugin

WordPress has released a security update to resolve a path traversal vulnerability in the WordPress File Upload plugin for WordPress. The affected versions are WordPress File Upload plugin for WordPress up to and including, 4.24.11.

CVE ID: CVE-2024-9047 (Critical)

Vulnerability in Pedalo Connector Plugin for WordPress

An authentication bypass vulnerability has been discovered in Pedalo Connector plugin for WordPress. The affected versions are Pedalo Connector plugin for WordPress up to and including, 2.0.5.

CVE ID: CVE-2024-9822 (Critical)

1. **TA-MAW-2024-10-23-13**

It has been found that an unknown malware is targeting Critical Sector Entities. Please find below IOCs in this regard.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Hashes:-

MD5:-

f02c8340b23bcd6d38159f09af4d88e2

3587409a3bbf53be5808dd5fccdbabe1

d7a3fa6a6c738b4a3c40d5602af20b08

SHA1:-

d33d3a124ac365496f8d8e501c5afbd7dac58fc2

SHA256:-

0ee6a849224b400822f4d1247e6fed4f2013b6160095bdbd44ab87690b692145

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-10-23-011**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The phishing email with the theme of "Credential-for indiancoastguard.nic.in Password Expiration Notice" and contains a URL "http://Indiancoastguard.aramempire.com/password/expiration/rutvR/icgs-sajag@indiancoastguard.nic.in". On clicking, it redirects to a malicious URL "https://0nline1.avacharms.xyz/?username=icgs-sajag@indiancoastguard.nic.in".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

URL:-

http://Indiancoastguard.aramempire.com/password/expiration/rutvR/icgs-sajag@indiancoastguard.nic.in

https://0nline1.avacharms.xyz/?username=icgs-sajag@indiancoastguard.nic.in

Domains:-

aramemPire.com

avacharms.xyz

IPs:-

192.185.167.23

64.226.125.218

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-10-24-13**

It has been observed that several threat actors are using Adversary in The Middle (AiTM) phishing attack techniques to compromise targets. AiTM phishing allows a threat actor to circumvent Multi Factor Authentication (MFA) by inserting a proxy between the victim and a legitimate login portal to steal credentials and session tokens. This technique is indicative of cyber actors’ focus on identity-based attacks where actors compromise personal identifiers like credentials or valid tokens.

The attacks are initiated via a phishing email containing a malicious link that led to an adversary-controlled website for credential harvesting. To appear legitimate, the emails are crafted to appear as though the victim had received an encrypted email or document from a trusted third party. When the victim clicked on the link, it leads to either being brought to a spoofed login page for Microsoft O365 or a blurred document that could only be viewed by inputting O365 credentials. When the victim entered their credentials, the adversary proxied those credentials to the legitimate M365 authentication service, starting a login attempt. Then, the adversary presented the user with an MFA code input prompt in their browser, designed to collect the legitimate code sent to the user via SMS. That code, again proxied by the adversary to the legitimate M365 service, allowed the adversary to complete the login and, in most cases, gain a session token. In some cases, the threat actors also opted to link their own device to the compromised account for MFA, likely as a precaution to ensure they retained access to the account.

AiTM phishing attacks target the authentication process, allowing attackers to steal data such as passwords and Personally Identifiable Information (PII) to gain unauthorized access to sensitive systems and data. These attacks rely on social engineering to incentivize the victim into opening the email or text message and interacting with the malicious link, which redirects to a malicious website that often looks like a legitimate login portal. Attackers can also use this technique to bypass MFA with techniques such as token hijacking. Users can also be tricked into entering MFA One Time Passwords (OTP), which the adversary can forward to the application to complete the authentication process, which would result in successful authentication and the attacker being granted session tokens.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IPs

24.123.192.166

72.43.174.83

47.45.234.127

74.143.2.14

20.190.151.0/24

20.190.181.0/24

185.220.101.102

188.213.202.0/24

193.37.33.0/24

172.183.249.139

45.143.82.229

69.5.53.144

179.41.183.40

141.136.92.76

180.247.187.17

203.109.207.210

179.68.204.121

Domains/URLs

https[:]//susgdoxu3o8p.larksuite.com/wiki/I4H9wTK4piqxTvk7mfIuLi8usjg?from=from\_copylink

https[:]//pub-d75bb1be9d414347a8fca3ada45e0c35.r2.dev/link.html

https[:]//rccgnet.org/protect.php

loancalculatorforrealtors.com

savio.com

Hashes

5259e3c268399650190597840f2b26301b1ce7cf06aa331ff4be5e732eebb1c4

618c564c8ffd0f3a87cb749da711e0b16184fd68edbed215fc540b0c71076766

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-10-24-12**

It has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Domains:-

www.email.gov.in.indianarmy.pl

email.gov.in.indianarmy.ml

\*.indianarmy.pl

\*.indianarmy.ml

meagov.org

scigov.xyz

govscicourt.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-10-24-14**

t has been observed that threat actor UAC-0050's phishing campaign targets government and critical infrastructure entities. Adversary is using a multi-stage infection chain leveraging malicious Visual Basic Scripts (VBS) and image steganography, resulting in a final payload detected as the Remcos Remote Access Trojan (RAT). Adversary uses state-sponsored based hosting provider “Shinjiru” for Command and Control (C2).  Remcos RAT provides full control over infected systems and allows adversaries to execute remote commands, keylogging, screen capturing, process and file manipulation and network surveillance. Remcos uses anti-debugging and obfuscation techniques to evade detection and is commonly spread via malicious email attachments, exploiting vulnerabilities or social engineering.

Multiple additional commodity malware payloads obtained from Bitbucket or other similar file hosting sites, consistent with the Remcos RAT activity targeting Ukraine, including AsyncRAT, XenoRAT, DarkTrackRAT, Lumma Stealer, Redline Stealer, Agentb and Neshta.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**URLs**

https[://]bitbucket.org/sdgw/sdge/downloads/one.txt

https[://]bitbucket.org/sharedua/ua/downloads/scan\_documet\_027839.rar

https[://]bitbucket.org/shieldadas/gsdghjj/downloads/img\_test.jpg?11811735

https[://]raw.githubusercontent.com/santomalo/audit/main/img\_test.jpg?14441723

http[://]geoplugin.net/json.gp

https[://]bitbucket.org/sdgw/sdge/downloads/ash.txt

https[://]bitbucket.org/sdgw/sdge/downloads/pngmrdb.txt

https[://]bitbucket.org/sdgw/sdge/downloads/5652.txt

https[://]bitbucket.org/rulmerurk/ertertqw/downloads/wil25.txt

https[://]bitbucket.org/rulmerurk/ertertqw/downloads/mca.txt

https[://]bitbucket.org/rulmerurk/ertertqw/downloads/mca5.txt

https[://]bitbucket.org/fasf24124/fdgfytrj/downloads/mca2.txt

http[://]bitbucket.org/miryp/gasgqw/downloads/mca5.txt

https[://]bitbucket.org/rulmerurk/ertertqw/downloads/mca2.txt

https[://]bitbucket.org/miryp/gasgqw/downloads/mca10.txt

https[://]bitbucket.org/rulmerurk/ertertqw/downloads/se16.txt

https[://]raw.githubusercontent.com/santomalo/audit/main/R1CO.txt

**IPs**

101.99.93.144 – Remcos RAT C2

111.90.147.146 – Remcos RAT C2

94.228.169.30 – Address of originating mail server “gmail.com” from message headers

**Domains**

server1.kamon.la – Remcos RAT C2

**Hashes (SHA256)**

57bad5db5dc112223b53e7b5ea6ce3101900206e6b8763c22fcf9c58a17fe257 – Remcos RAT (MZ)

E52e0b9a0a5d83cf808af70a1891d19f7a2f31886d251a065b7088cb7141d003 – Remcos RAT (MZ)

1a1776acfbc3d21e48b87e7035f3f1180fbd94a5944c5346e447490cbcf474e9 – one.txt

03fc22f699ba6ce9fa37f68c96fc35b6b6f8bdc7c55944977653fe2de6e1adad – one.txt

96a30bb4a3b4a1287cc044cbbe36dc8e6987286369138a6a65fc071656472bc4 – one.txt

A195b64eaae8353c3de14d8e02849a0f30593859bdc2fb443ad5f9db9a803168 – testpowershell.exe

700a9a6eb11bbae7ef16e727c44913861a12510c5a4b8450ce6c33f616cf1df5 – img\_test.jpg

02be347bd34ba0a7ad2c5e50d1f74e88e0222eaa96ae3255c2eaa7e162c48d88 – img\_test\_2.jpg

Fe82b14fd6a7516accefb582aa96754dc569ffd28b007ace5791860b5906c7c5 - scan\_documet\_027839.vbs

Cb6c92921e3bc58250684d6bd5dda9b92d22917f2d5e7b137c9694907309e986 - scan\_documet\_027839.vbs

Ff1cfb2ff5cec597bd7163ab40e8e33b4729eddd1a76e13b8f759a9b0ff35afc - Платіжне доручення.vbs

84dab25530ba75d9610b9b7e7f8665ba066679cb1e433d7657f9b0577e37717d - scan\_documet\_027839.rar

F8cc03d9209b7a16cbc17eff0dcbd5c5ff6e346fc941feef2896673697d43007 – ash.txt

91e9ce1a314f7aded71c18144b069c5a86c8f9424a8cf72fb02d2acc440d5992 – AsyncRAT

0fc8c85b71ef2ecadfa43c7515947277e264138d468a968c4792355f3c6d1b33 – pngmrdb.txt

Da23b67cd3b28994245a374a5eb00acfa39611b7f81e5215ff6fc573974b2d50 – Redline Stealer

F20c466371b9a1447ffd85284b95d8ec4959373f824bf0363b82eaa4ac18b4cf – 5652.txt

50a246ec446e216d053e15b13f6d78dacc747a3c0aa399c1fee61c485a5b95ef – XenoRAT

Ac20c30454ae387bf63a41ad5786dd7f86684af8e133283efe734018a22c9780 – wil25.txt

Bb6dc8e819f6feea6608204c9dd5a9b132551f53e8fe6ba359d36601eec25418 – Redline Stealer

Ac5e75993ee0d837e3ec1810d006a6b2ec66d861984d59b6b18186f97a50759f – mca.txt

2881a2a79b9dde2a036648df3f04996cac0401505af3d67156ceb1a4d9011b7c – Neshta

C6ab3f142b6c70146102748002eaad2b5b8279588f61a19c153cb48a5266769d – se16.txt

45b33888ddb2748434643e4811f156f1fc2a5d339d3577945d8c9e9d88c5ff57 – DarkTrackRAT

6d5bc5a71bced605238e8f4e5d5fe29da4cb1d156104fe729d3b01cece68c417 – R1CO.txt

Fc062bea1baea6f433145458742ef3c7427bbf105879a892c2a3b8e1166995a6 – Remcos RAT (MZ)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-APT-2024-10-24-007**

It has been observed that an Advanced Persistent Threat (APT) group, IcePeony attack, began with SQL injection techniques, targeting vulnerable public-facing web servers. After successfully exploiting, the adversary deploys webshells and a custom backdoor IceCach. The backdoor IceCache, is an ELF64 binary developed in Go taken from open-source software called reGeorge. The IceCache's command set is extensive, allowing it to function as a proxy and facilitate file uploads and downloads. The group also employs StaX, an enhanced version of the open-source tool Stowaway, which features encryption and high-performance proxy functionalities. Another malware, IceEvent, is a passive-mode backdoor that shares similarities with IceCache in terms of its encoding and command execution. IceEvent was used in cases where the adversary required minimal functionality to maintain persistence on compromised systems.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:-**

165.22.211.62

64.227.133.248

173.208.156.19

173.208.156.144

154.213.17.225

103.150.186.219

63.141.255.16

204.12.205.10

107.148.37.63

103.99.60.119

154.213.17.237

45.195.205.88

154.213.17.244

103.99.60.93

149.115.231.17

149.115.231.39

103.99.60.108

**Domains**

d45qomwkl.online

k9ccin.com

k8ccyn.com

88k8cc.com

googlesvn.com

**Hashes:**

484e274077ab6f9354bf71164a8edee4dc4672fcfbf05355958785824fe0468f

5b16d1533754c9e625340c4fc2c1f76b11f37eb801166ccfb96d2aa02875a811

ceb47274f4b6293df8904c917f423c2f07f1f31416b79f3b42b6d64e65dcfe1b

e5f520d95cbad6ac38eb6badbe0ad225f133e0e410af4e6df5a36b06813e451b

d1955169cd8195ecedfb85a3234e4e6b191f596e493904ebca5f44e176f3f950

11e90e2458a97957064a3d3f508fa6dadae19f632b45ff9523b7def50ebacb63

de8f58f008ddaa60b5cf1b729ca03f276d2267e0a80b584f2f0723e0fac9f76c

b8d030ed55bfb6bc4fdc9fe34349ef502561519a79166344194052f165d69681

535586af127e85c5561199a9a1a3254d554a6cb97200ee139c5ce23e68a932bd

0b8b10a2ff68cb2aa3451eedac4a8af4bd147ef9ddc6eb84fc5b01a65fca68fd

5fd5e99fc503831b71f4072a335f662d1188d7bc8ca2340706344fb974c7fe46

3eb56218a80582a79f8f4959b8360ada1b5e471d723812423e9d68354b6e008c

a66627cc13f827064b7fcea643ab31b34a7cea444d85acc4e146d9f2b2851cf6

0eb60e4c5dc7b06b719e9dbd880eb5b7514272dc0d11e4760354f8bb44841f77

80e831180237b819e14c36e4af70304bc66744d26726310e3c0dd95f1740ee58

9a0b0439e6fd2403f764acf0527f2365a4b9a98e9643cd5d03ccccf3825a732e

9aba997bbf2f38f68ad8cc3474ef68eedd0b99e8f7ce39045f1d770e2af24fea

bc94da1a066cbb9bdee7a03145609d0f9202b426a52aca19cc8d145b4175603b

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-010-24-014**

It has been observed that Redline stealer malware, written in C#, has been designed to steal passwords, credit card information, and other sensitive data stored in web browsers. Adversary can also collect details about the infected system’s environment in order to facilitate secondary attacks such as privilege escalation and maintaining persistence. Redline Stealer is typically distributed through phishing campaigns, malicious advertisements, and bundled with cracked software, highlighting the risks of downloading unverified software from the internet.

**Impacts:**

* Information Stealer: Redline focuses on harvesting a wide range of sensitive information, including login credentials, browser data, cryptocurrency wallets, and system information.
* Credential Theft: It can steal passwords stored in web browsers, email clients, and FTP clients, leading to potential data breaches and identity theft.
* Dark Web Activity: Stolen data is often sold on dark web forums, making it a lucrative tool for cybercriminals.
* Remote Access and Surveillance: Redline may allow attackers to remotely control infected systems, exfiltrating more data.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Address:**

185.196.9.26

185.215.113.67

88.99.151.68

45.132.1.33

185.159.129.54

193.37.71.131

147.45.67.15

45.137.22.171

80.66.89.228

136.244.88.135

5.254.73.99

188.114.96.3

188.114.97.3

45.9.73.169

45.137.22.252

93.115.91.27

185.222.58.236

108.61.177.169

65.21.18.51

185.215.113.22

185.222.58.250

163.172.24.191

185.222.58.245

193.26.115.118

89.105.223.196

212.233.122.234

185.222.58.233

185.222.58.80

147.45.47.192

185.222.58.248

5.206.227.2

45.137.22.123

176.111.174.140

213.248.43.53

212.233.122.248

154.216.20.204

45.137.22.91

185.215.113.25

213.248.43.54

185.222.58.247

185.222.58.48

95.179.250.45

91.211.248.215

95.216.232.170

31.42.189.18

45.89.247.82

185.222.58.74

91.92.242.38

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **VA-2024-10-24-011**

It has been discovered that the threat actors are exploiting a critical deserialization vulnerability (CVE-2024-40711) in Veeam Backup & Replication (VBR) servers to deploy Akira & Fog ransomware to gain Remote Code Execution (RCE) and also leveraging compromised VPN credentials. For successful exploitation of the vulnerability, the attackers managed to create a local account “point” with administrative privileges to compromise VPN gateways without multifactor authentication and are running outdated software versions. In the Fog ransomware incident, the attacker deployed it to an unprotected Hyper-V server, then used the utility rclone to exfiltrate data.

Fog ransomware is targeting both Windows and Linux systems, affecting various sectors. The malware exploits compromised VPN credentials and critical vulnerabilities to gain initial access by creating local accounts with administrative privileges. Once inside a network, attackers utilize pass-the-hash techniques for lateral movement, often deploying the ransomware on unprotected Hyper-V servers.

The Akira ransomware gang has links to the defunct Conti ransomware gang. Adversary, operating under a Ransomware as a Service (RaaS) model, collaborates with other cybercriminals to carry out attacks. Adversary utilizes double extortion tactics by first stealing sensitive data, then encrypting it, and demanding two separate ransoms, one for decryption & another to prevent the public release of the stolen data. Initial access is frequently gained through compromised credentials.

1. **TA-PHI-2024-10-25-015**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The phishing email contains an attached PDF file with the subject of "24 September Letter Reply.pdf" which contains a hyperlink "https://email.gov.in.indianarmy.pl/service/home/?auth=co&id=29238&filename=INDIAN%20Armed%20Forces%20And%20Agencies%20Report&charset=UTF-8") with the title "View Documents". Upon clicking the hyperlink, it opens the phishing page of NIC login page and seeks for username and password.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**URL:**

https://email.gov.in.indianarmy.pl/service/home/?auth=co&id=29238&filename=INDIAN%20Armed%20Forces%20And%20Agencies%20Report&charset=UTF-8

**Domain:**

indianarmy.pl

**IPs:**

45.141.59.178

93.157.106.19

146.70.142.89

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-010-25-015**

Credential and information stealing malware named Trickbot primarily spreads through spam emails containing malicious URLs or weaponized attachments. Once downloaded, it connects to a Command and Control (C2) server to upload victim's data and receive instructions for various follow-on activities. The malware spreads across network by brute-forcing usernames and passwords, sending malspam that originate from the infected user’s account, and leveraging the EternalBlue exploit to attack unpatched systems.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**IP Address:**

175.184.232.234

27.109.116.144

41.77.134.250

177.190.76.82

196.41.57.46

103.201.142.30

96.9.77.142

194.87.94.14

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

1. **TA-MAW-2024-10-25-016**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IP Addresses:

165.231.253.216

61.152.154.52

45.133.172.204

198.12.64.41

154.8.141.46

67.21.32.154

38.95.13.138

217.138.192.220

24.152.49.139

185.224.128.67

84.17.59.85

192.30.83.185

113.134.156.54

209.38.4.240

183.240.139.6

23.228.72.18

50.3.182.152

107.175.31.202

176.97.210.238

154.216.17.31

172.120.11.62

120.86.252.59

107.167.122.109

185.224.128.67

168.205.75.24

8.140.234.207

50.3.182.152

107.175.31.202

23.228.72.18

154.216.17.31

64.235.37.140

URLs:-

http://59.183.111.142:53592/

http://103.197.115.17:56909/

http://220.112.108.64:50476/

http://bins.rootwho.su/sshdbot

http://119.185.174.37:45396/

http://117.222.197.178:49978/

http://59.95.92.208:39564/

http://59.92.198.138:45154/

http://117.195.92.194:41391/

http://58.208.93.232:48853/

http://45.230.66.25:10347/

http://183.240.139.142:58474/

http://103.197.115.107:34197/

http://45.115.89.74:39283/

http://223.8.31.130:55759/

http://117.222.197.178:49978/

http://42.232.211.227:60398/

http://124.131.134.29:58247/

http://117.248.23.176:43500/

http://59.89.225.48:56200/

http://113.24.133.2:37029/

http://115.55.185.238:59658/

http://117.235.112.131:55250/

http://223.10.49.125:44164/

http://120.60.232.87:38544/

http://115.54.163.30:48075/

http://117.253.6.77:35645/

http://117.253.2.150:41450/

http://58.47.107.197:45017/

http://123.13.229.93:42324/

http://113.231.206.214:50954/

http://113.235.117.215:53413/

http://110.182.40.168:52274/

http://117.206.29.47:34217/

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **VA-2024-10-25-017**

It has been observed that threat actors are exploiting a missing authentication for critical function vulnerability (CVE-2024-47575 (CVSS score: 9.8)) in FortiManager fgfmd daemon that may allow to execute arbitrary code or commands via specially crafted requests.

Another, use of externally-controlled format string vulnerability (CVE-2024-23113 (CVSS score: 9.8)) has been discovered in FortiOS fgfmd daemon that may allow a remote unauthenticated attacker to execute arbitrary code or commands via specially crafted requests.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IPs:-

45.32.41.202

104.238.141.143

158.247.199.37

45.32.63.2

195.85.114.78

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-10-28-017**

It has been observed that Agent Tesla usually spreads through phishing however, the malware has a function which allows it to run automatically from a USB stick/ pen drive. At present, Agent Tesla is able to operate exclusively on Windows machines.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Address:**

46.175.148.58

110.4.45.197

213.189.52.181

217.116.201.44

193.141.65.39

37.27.98.198

93.216.70.207

148.66.136.151

195.252.110.253

92.37.142.45

47.76.82.23

37.247.119.59

5.2.84.236

85.26.241.192

93.89.225.40

144.217.198.22

103.6.196.236

148.251.209.169

92.205.7.112

167.235.180.68

78.128.81.95

185.191.171.10

185.191.171.16

49.36.188.172

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-10-28-018**

Amadey is a simple Trojan bot. It is primarily used for collecting information on a victim's environment, though it can also deliver other malware.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**IP Address:**

77.91.78.17

185.196.10.188

45.9.74.182

78.46.242.112

193.233.20.14

62.204.41.252

193.3.19.154

193.106.191.201

62.204.41.89

79.137.203.59

188.40.187.155

176.113.115.201

207.154.243.184

89.163.249.231

78.47.9.120

193.42.33.74

45.9.74.164

31.41.244.146

31.41.154.129

185.215.113.35

77.73.134.66

195.2.70.68

194.190.152.209

45.202.35.101

45.9.74.166

185.11.61.121

185.215.113.204

185.215.113.101

45.9.74.141

49.12.117.51

185.196.8.176

77.91.124.1

77.91.124.207

31.41.244.237

46.8.231.42

80.66.75.214

31.177.76.32

31.177.80.32

62.204.41.79

35.187.168.7

92.43.25.99

34.163.37.95

80.66.89.124

194.163.35.54

62.204.41.87

188.40.141.211

62.182.156.153

185.174.136.244

77.105.160.21

89.163.210.240

34.88.137.133

158.196.149.66

81.30.189.18

185.232.14.89

37.247.10.18

185.196.8.126

213.202.223.111

89.163.152.111

91.228.238.70

85.209.135.11

85.209.11.155

34.77.123.245

5.75.139.35

185.215.113.16

194.163.38.5

5.104.108.23

35.198.88.107

81.17.29.162

119.18.58.248

77.72.17.124

185.231.220.10

80.66.75.114

212.204.112.234

5.181.86.244

92.204.58.67

34.89.169.66

193.167.100.88

89.163.220.66

92.60.224.35

129.132.80.25

45.15.156.208

89.163.155.199

185.215.113.26

213.202.223.115

31.41.244.10

91.192.226.152

35.187.35.15

23.215.121.14

176.126.172.243

156.67.212.207

34.90.10.178

35.228.19.145

212.204.112.241

77.91.124.20

129.132.18.8

35.204.250.43

79.110.62.15

35.233.77.94

35.234.76.210

31.41.244.158

213.202.229.103

34.76.205.124

213.202.223.113

92.205.111.226

77.73.133.72

138.201.203.107

62.204.41.182

192.121.16.27

77.91.124.242

91.189.114.25

31.41.244.15

62.122.170.171

195.251.3.214

147.32.80.105

95.211.227.207

104.155.66.110

87.62.82.197

213.246.57.71

129.241.56.201

185.37.231.211

46.16.234.119

94.247.170.66

3.126.57.221

35.205.156.75

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

1. **TA-MAW-2024-10-28-019**

SocGholish is a malware downloader that spreads through drive-by downloads on compromised websites. Drive-by compromise can occur when users can unknowingly download malware from a malicious website or advertisement masquerading as a legitimate one. When users visit these sites, malicious JavaScript executes, often tricking them into believing they need to perform a fake browser update. This script collects information about their browser and system before prompting a download. If users fall for the use and execute the download, Socgholish installs itself on their computer, potentially leading to data theft or further malware infections.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**IP Address:**

77.245.56.14

93.190.41.79

45.130.201.24

164.52.214.211

92.205.49.95

217.160.0.220

31.220.15.143

5.101.115.147

217.160.0.215

92.204.68.47

185.216.114.10

217.160.0.246

195.24.68.25

94.130.138.216

35.215.148.34

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

1. **TA-PHI-2024-10-28-016**

It has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

loginmygov.info

ww25.indian.airforce.life

serviceonline.gov.in.viewcerts.org

ww38.iwww.joinindiannavy.com

viewcert.life

tpplus.top

\*.indian.airforce.life

\*.in.viewcerts.org

\*.joinindiannavy.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **VA-2024-10-28-012**

Microsoft released updates to address multiple vulnerabilities in its products for the month of Oct 2024. However, Microsoft provides patch information in the form of Knowledge Base (KB) Articles that are associated with one or more CVEs.

Please find below link for the monthly CVE - KB Correlation list of Oct 2024 for your perusal and necessary action.

https://nciipc.gov.in/advisories/CVE/CVE-KB/2024/Oct.html

The list consists of 121 CVEs and their corresponding KBs for the month of Oct 2024.

1. **TA-MAW-2024-10-28-020**

It has been observed that threat actors are deplying Supershell backdoor on inadequately managed Linux SSH servers. Supershell, developed in the Go language, supports various platforms including Windows, Linux, and Android. It provides a reverse secure shell (SSH) tunnel to obtain a fully interactive shell, remote system management, execute interactive scripts, and perform various remote operations using its fully interactive shell.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**IP Address:**

107.189.8.15

179.61.253.67

2.58.84.90

209.141.60.249

45.15.143.197

**URLs:**

http[:]//45.15.143.197/sensi.sh

http[:]//45.15.143.197/ssh1

http[:]//45.15.143.197/x64.bin

http[:]//45.15.143.197[:]10086/supershell/compile/download/ssh

http[:]//45.15.143.197[:]44581/ssh1

**Hashes:**

4ee4f1e7456bb2b3d13e93797b9efbd3

5ab6e938028e6e9766aa7574928eb062

e06a1ba2f45ba46b892bef017113af09

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

1. **VA-2024-10-29-013**

Two critical vulnerabilities affecting Ivanti Endpoint Manager and Ivanti Cloud Services Application (CSA) are as follows:-

1) CVE-2024-29824 (CVSS score:9.6) - An Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability tracked as CVE-2024-29824 exists in the Core server of Ivanti Endpoint Manager (EPM) which is exploited in the wild. On successful exploitation, it allows an unauthenticated attacker to execute arbitrary code . Its non-weaponized code is publicly available.

2).CVE-2024-9379 (CVSS score: 6.5) - SQL injection in the admin web console of Ivanti Cloud Services Application (CSA) before version 5.0.2 allows a remote authenticated attacker with admin privileges to run arbitrary SQL statements.

1. **TA-MAW-2024-10-29-021**

During analysis of Mirai samples over a week, following IOCs have been found. There are couple of things to be aware of while looking at this data:

Network IOCs may be associated with binary distribution or one of the "cnc" or "report" functions.

Network IOCs are identified from newly identified samples but may themselves not necessarily be new.

Because of nature of the static analysis, there is MODERATE confidence in accuracy of the network IOCs.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IPs:

154.216.19.155

194.37.80.211

80.76.51.218

Hashes:

0193ced7be5bc5a7f16f50bfdfdf22a5dbcf518356ecb7af97d0fcfad2e50df2

07a7bd8688f31ddbed29202d1add59d191ae727cf3a5064904e091c7cb5ba35e

07c2afb7002ba2d4f72bea9ea784c7c12dedaa271b3d40207ff745b13768fa52

093c17cbd61476443a69dd71850f75abc324128010a3f682956b0846da69b3c3

09876fa69e52eeeb2f52af37f77abab7eb9fad0d1821048f6c62c180c8f1661b

0c00399240709e29abe6e6367b6d01d60451606d90bc9d44291435618a98a211

0e7c8ae049e75286073460dc2383430e218e37057a5795bece3dccb24fd9c8d2

0fa548e33cfff110ae452d5511a3e728251fc06cad0601e21da577a6b448a94d

10bf6cdc2b3b371666555a4c3b9a538e2da87609b9fb54b336ac301bfb2e0f37

1694b278d30dd7f73f00381d8f597ac59f85c6aa8187ba9227693699ce638fb9

16b5a97c987c546aa3064266dbaf07d7b7544800ed1c8ac3a42865c62521cb33

1842e7506726c23aaf47e5fb647a324cf4fc133cee2bda5786f091a8bb30c06d

1afba84cdbc99e303306f2df6d1b1cbcff8ba3283373c40504a184182bf5c412

1b8a5cbe5ee784739e11dc0d498afd608ccdb67c39e0ab394e23aa9ac1cf9619

1cd37035c9e226da4d7e2d4f22df3ae851560a537e7a7648f97d69011c908467

1d39f6e0fae845f57ba0bd9b6e5ecce3a596eb16b5adc8a2ce75b650f1031890

209bba81fd743b93052003c6ef8fcd808d8fc8b86f039606875606681ba924a8

2190fd1904c3ce1f10966e84b97bff30e7366d16f4e0566729804967991f577d

29bac78b54342a6924c3d591178e933a255b5780e14e6033636467509041c62c

2f2ad2bd12bdcb9fc81c7ac1a94ef7175a73607e339a0e59bc3f6b6c6a6bc08c

32412894ef3995cb8c361963c013db5699056fb2c0d1571d69e17bfd9477cf26

336d7115c40816ce91aa8a58b89d0d8cb467121e3cf0db0f823a3d41d9ffe7e9

350e5c8f59b34503b6a0a8e287ebc154a315f90c8ba5bfe0702155249cd7ceab

3906d9e3e0d9a7ec8ed4bfcc2268fe394f5d0d21c96fb22d6caae63d957ad04c

3987e0b04bc53bcc7694b42bed9e5e62360297e179cbe5a11dec859908c7ae48

3b82a31e8c22d9731a754fe0a2d225102ceb37fe220dee95183fd0f31f715ae2

40c4bc40b610a46d8f034055c098b32543292963f08f2d05964f204b5112bf9a

426490e410087312be2804d345fe1ad2bb5814f1b1e2378bd58d52723e7bcee9

430ea1000e5e9d0d779ff1e1d7eb86ade9886230b270bf4e295de634418b7f4e

4726df0fb04bed954d7bcc46626cbc4d89274eb28cc04192e762446cd68d9b9f

48a5eb4f6485db3dd0b87a43e0dc1d5b3c47a00f1afc77394ee174eeb0f9daf7

4bddd3a10853d7fa0c2bc253cbf1b540ebc609899fa8989ff46f8ade3ace7de7

4c76c89f84e156877efe8db83748a11d73a8d024c731b89b2c1e0caf710fbb1e

4cc1a0aab914fc58a08899022d961005611910d03ba687befe00c9e8deae5b87

4f3cbc12aee647b7b568876a6d66cc7a21eeba9116ead1ec1baf4b9fa8d2fb9d

54c3ad58398aa0f6ec9bf3837b23453cd51173ddc154e776d2258beccf0c5c64

55369cc33155052a2dc2dd710bfbc200a563ea5ef178a55e38048c8c7b34a6c1

55fd66573bfc18489b71fcfac108aff790ff44ef556f68c635a2fdb2160e2046

60bd70c042c2f3364dbfa1dfccd7e01f458646e5082b62df452a6f45285b9746

62858a9fad83b60493add4f59e2f92299a087507b4e87d01a45229bb651f57b2

65e3ae2f67ed5762f07a3c18cfeff9da4f9feb09df6f27e67ca1595fd2b1b799

665c8368c0338ff16b9a2b80347e0b0c15289103f4c541ca315230a1010de88a

66d2624db5ba5ac10343e3d34455172e371c45ec23a0c700dc6e27106253b920

6ba2d4d07384e95818f146e494492e320035a949c8baaf81ce4537e4686d9c45

6c18bd6fec14f6929d211c35ee1e1074472881b26421bd1e03991121748ab075

72f65520aa3ffac125f387e65360a5d83ed361d52ad8d3062a444aab71bfc6da

75d6bc2bbec8d0cb1bc2257d5aa63c1394c1b5d6206031f665f60efbf862d914

76e719ff42f4b6cd19709e5df425851e0ccf2c64625de11301409f451da6a1f5

76f31b9180a0fa7400118a8f24936af72fe8e10b837675e9eb59a05cd20c5e8a

777990ee8f8b50e6552b4e6f5ac438985f819f25b4fff29d5f47137cb6a28bc3

78fe21bc07d728abab167c5ff112cd4b235418ebe958cab99db46d1ce6bdb18c

79d3b450be507d5871e4d7021c8bbcd38bc328e3a579a05aeaf58c84f3fa7a24

7c9de3b2bf6df921d93d26e89ea2c170c8baa9f09d83a4b5ab677bb36fef2534

80773867479756b0c6babb82bed63d3b4a0a0009a1f99159b1c20d2395ec4393

81c51d0532da7ef96b787578e9346dfc6eb5ea9cd19279ec71d030d6b65ff693

8a52c58330ff27df84ea888e69b25e88824e2a224109b4527963cc8b5090c8dc

8bc3c63a5388b9fbe7f2e476b0c201f6fca5c122867b1f60dfaace11710d8150

8c3b5b72684bf186da4ac28f6f22b9b0f41ed80d2619a6d711c53bfde146229f

91d920d0b5a70491e1c5621e6e4106e1860b8cc7ba9945c7a8308b461b4d4b75

946e3cf44f4bdd74755c239bbcc0dd1df472adc79e5da4709918d46e0613f8fa

94c495ffc72f3c5b67ad580090c8292d4d2867e720e6ba58e50039dff7da24dd

95d2db991085ba3d3e123b3fc5a871e2cc02a45420560cb3431a4a52e273e574

9a7f87c3bb00617e0a17a6f799931596741c3f731d022329a26e107494759317

9e25488eb9fb920069e9f8066eaeb16b16ba9b999e1d1d45d727758f49fb43c5

9ffbe69f016f5477a8df47888811a30296654d2472d87b6cdc73714916744e58

a0421cfba0db60030decba6a12051c1a50ff1f23cd830bfdb1eec2bd4ccb249c

a3d133e76ec0ff5bbf4fd28dce0bbff243bdede6398c8baa99b41754d62c8bb2

a6b358beb8b18d35d87b983c4e18986e3ea0b8677bbf4c00917a3bbd4541c491

a76a6da8483740648dfa0c2085d26bd9a65c2c38bbea8075336e391ed0b3dae0

a8f53b7cd22640fa1b94fc2547489ef53975e49e38cd6e685adac40ef16e34a1

ae1c4bfce3fac0b218b9d72a12bf6177505110edbe080a266e199bd207f4f1f2

b150199f20695547a23cd449170293cc0e7b32095f9bf346d4ddce9e4630d3a0

b78b2bafd00e2b98368c59791a1c6589a19a25959c6bd5ca6e6d47c5caad39cf

b7cf5e4e2efafb2dbd9e8e1c372aeba11e5a5e8feff62e24499e7454d43ea14b

c2059520cd0efb8f54525a1d8c571245611be218781b1055ab8a68db056fcbe9

c4b109360dbe4f7c8204debc89c010e56edb042a9400171366a43c5c38d85675

c79986589c830fd8dfe0f446ed4ff4ccf9d4e560f4fd0f00b079174f22537033

c8864cf97889d0a40d8b87c6936246e1c9c3cd6134663cb6590d8accc67740e5

c98be032dd7b1ecf2de87ef80f1e556e63eacd26f18c7febfe7162f1e68fe191

cba823fdb10dd85b677b7c1df63f59818bc625d743a7517c2fd3478d07bf623a

cca4a2d29cedd49289d589052d302f65a40274e71552cbce767b700a11c056bb

ccc267aff58fa4e02a7a822c9ac6989d72c63f3e33534f96fbb705f66f6f2fc5

cd1052176ea71053669dc85222c92f78a8309358d6b1e923c8df89be02397e59

cde69f287ea9a2bc6ced4647a7e5271def816f10cca4d0bb6d7b581146eb01c3

d30922e18b7cc3a1c251624537bc95d592117db287d2b3e34e1c356b30f3fbc3

d5a61b95a3b6ba4b2babbc12c03ece769b4cf4f3c940664799932401c327737f

d73be84649dcf47f0b3159512c2d7bdc1b88a8d7be4350d1b843cb9038b9ee82

d8e7e65c338bd95fa30d23f467984d16b857d3f3ca5e9b129f07c589e935ffec

d9b6b7418c587f67c47575ebbbefc9781ed5b567b62d6ee5442e673fc852d6db

e19eb9d5c86d2fc5b2f482ccb4217b2a2c75ecc6836da41439915ded0bd49f23

e1f10c16d3b13ee6d2211ad553ea3a8cf3055f167e4de87149b3e86e8b512488

e258d773a3037b9ac4f8a4086ec617201871ea42ee2f9efdb5b2b711dca04f88

e3006bc13b6baf3aebf14ea3d2c79d38a42ed995ed72069683ffe5f619764530

e5902a268e2886f359adb6939217e90244451a5ccc9cc4263bf1340abe171666

ea2b6b705bfa57215dddde26441ecd08d4a9334c5a1c13f1c5d4fbc5db40a3ee

ee8d44ec2250c8a0012b7387612c6c84398e4ca01672c465230b62e75499a31b

ef20459c31faafdbc779ce159f01d06f0e1be88a325c616134ea4a197cababeb

f05ce1bfd3ab947bac548c35297b719e950d00f52f49f4ec99677c7ae687a732

f16cb4420951397ee81e4ec3c3a50a9ad1eeaacddf3494c303300193cafcd35e

f49aa7c0d516c07a1b376866b784e9bd93b7694d2d12fb0dc808ba87dcdce34a

f68eb843ff307f06c16c5e31004e1368f1989ca0dd46d5a7cc4cbf80462dcabd

f979976fece1697c5af00fade98f5edc9ecab180a87ee3f972bdee8f5c4c50e5

fc949675a149f8c5b08df6e027b7b3264f65ef3369a3a12b21392823ee3ab343

ffd027255c5a00c4e2fcb2641b0f3cc586d4c0d96a5537799c78091592fea92f

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-10-29-022**

It has been found that an unknown malware is targeting Critical Sector Entities. Please find below IOCs in this regard.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Domains:-**

kumar123.evils.in

objector.ns01.info

offine.dsmtp.com

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***