LUCKY ELEPHANT Campaign Masquerading

netscout.com/blog/asert/lucky-elephant-campaign-masquerading

Executive Summary

In early March 2019, ASERT Researchers uncovered a credential harvesting campaign targeting mostly South Asian governments. The actors behind this campaign we call LUCKY ELEPHANT use doppelganger webpages to mimic legitimate entities such as foreign governments, telecommunications, and military. Interestingly, at least one IP address used in the campaign was previously associated with a suspected Indian APT group, and one domain was previously attributed to Chinese APT activity. It is unclear the purpose of the overlap in the infrastructure, but it's possible the actors used it as a diversionary tactic.

NOTE: NETSCOUT AED/APS enterprise security products detect, and block activity related to the LUCKY ELEPHANT campaign using our ATLAS Intelligence Feed (AIF).

Key Findings

- ASERT uncovered a credential theft campaign we call LUCKY ELEPHANT where attackers masquerade as legitimate entities such as foreign government, telecommunications, and military.
- The doppelganger webpages primary purpose is to gather login credentials; we have not observed malware payloads associated with the campaign.
- One IP address used in the LUCKY ELEPHANT campaign was previously used by the suspected Indian APT DoNot Team; and at least one of the domains used for credential harvesting was previously attributed to a Chinese APT group.

Capabilities

From at least February 2019 to present, the actors in the LUCKY ELEPHANT campaign copied webpages to mimic South Asian government websites as well as Microsoft Outlook 365 login pages and hosted them on their own doppelganger domains, presumably to trick victims into providing login credentials. They registered their doppelgangers with various top-level domains (TLD), specifically those that afford the actors registrant anonymity. ASERT suspects that the Actors use phishing emails to lure victims to the doppelganger websites and entice users to enter their credentials. We have yet to uncover any malware associated with this campaign.

The Actors download legitimate websites and webmail portals, which copies the entirety of its contents and web components. This method saves time and prevents the introduction of errors that could arouse suspicion. **Figure 1** & **Figure 2** show two of the doppelganger webpages, clearly intending to pass as a legitimate place to input credentials.

Figure 1: Bangladesh Navy Fake Login Page

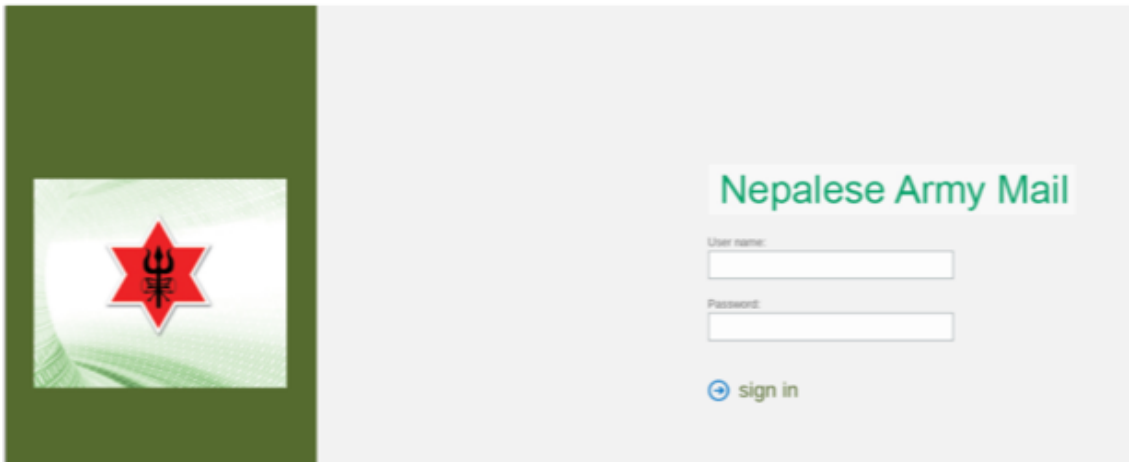

Figure 2: Nepalese Army Fake Login Page

Victims

Many of the targeted entities are easily identified based on the copied webpages or the doppelganger names of the fake domains. To date, ASERT has no knowledge of successful compromise. The following is a list of the organizations mimicked:

- Pakistan:
  - Pakistan Atomic Energy Commission
  - Pakistan Ministry of Foreign Affairs
  - Pakistan National Telecom Corporation
  - Pakistani Air Force
  - Pakistan Ministry of Law & Justice
  - Pakistan Prime Minister’s Office
  - Frontier Works Organization
  - Pakistan Ordnance Factories
  - Pakistani Nuclear Regulatory Authority
- Bangladesh:
  - Bangladesh Air Force
  - Bangladesh Navy
  - Bangladesh Armed Services

    - Rapid Action Battalion
- Sri Lankan Air Force
- Maldives National Defense Force
- Myanmar Ministry of Foreign Affairs
- Nepal:
    - Nepalese Army
    - Nepalese Ministry of Foreign Affairs
- Shanghai Cooperation Organization (a Eurasian political, economic, and security alliance)

Infrastructure

We discovered two active IP addresses: 128.127.105[.]13 and 179.43.169[.]20. Through the course of monitoring these IP addresses, we uncovered new doppelganger domains set up to facilitate the credential harvesting campaign. This activity started in February 2019 and appears to be ongoing. Though we don't have WHOIS data for the domains, we were able to track registration due to the small number of IP address utilized.

It is important to note that one domain, yahoomail[.]cf is only associated with this group/campaign from February 2019 onward. In late 2018, the domain was associated with a different APT group/campaign of Chinese origin. The subdomains security[.]yahoomail[.]cf and cc[.]yahoomail[.]cf are related to the ExileRAT campaign Cisco Talos reported (link). It is unclear if the domain ownership change was coincidental or intended to confuse researchers.

IOC List:

103.243.173.253	mail-nepalarmymil-np.gq	paec-gov-pk.ga
128.127.105.13	mail-ntc-net-pk.tk	paec-gov-pk-taskmail.tk
179.43.169.20	mail-outlook-support-team.tk	paecweb-gov.gq
77.244.211.55	mail-paf-gov.cf	paecwebmail.gq
account-sign-in-security.ga	mail-sign-alert-notification.cf	paf-gov-pk.cf
account-update-com.tk	mail-updates-systems.ga	paf-gov-pk.ga
account-updates-team.ga	mail-update-task.ga	paf-gov-pk.tk
afd-gov-bd.gq	mail-update-team.ga	paknavy-pk.gq
baf-mil-bd.tk	mail-yahoo-com.tk	pmo-gov-pk.tk
checkbox.gq	mail-yahoo-task.tk	pnra-org.gq
cyber-net-pk.cf	micorsoft-outlook-update.ml	pof-gov-pk.tk
fwo-com.tk	mofa-gov-mm.ml	rab-gov-bd.gq
g00gle-com.cf	mofagov-np.cf	sco-gov-pk.tk
googlemail-com.gq	mofa-gov-np.cf	sharepoint-google.ml
live-com.gq	mofa-gov-pk.tk	slaf-gov-lk.ml
live-com.ml	molaw-gov-pk.cf	super-net-pk.cf

live-service.cf	outlook-com.cf	super-net-pk.tk
login-live-com.cf	outlook-livecom.cf	test-updates.ga
login-yah00-com.tk	outlook-live-com.cf	userscontent.com
login-yahoo-com.ga	outlook-live-com.ga	yahoo-com.ga
live-com-owa .gq	outlooklive-com.ml	**yahoomail.cf**
mail-account-security-com.cf	outlook-live-com.tk	yahoomail-com.cf
mail-accounts-verify-com.cf	outlookmail-com.tk	yahoo-mail-com.ml
mail-intl-ja-mail-about.gq	paecgov-pk.cf	

Adversary

Based on our analysis into the activity, ASERT deems with moderate confidence that an Indian APT group is behind the LUCKY ELEPHANT campaign. The targets are typical of known Indian APT activity and the infrastructure was previously used by an Indian APT group. Phishing and credential theft are commonly observed with Indian targeting in-region.

One of the IP addresses, 128.127.105[.]13, was previously used by the DoNot Team (aka APT-C-35), a suspected Indian APT group. DoNot Team has a history of heavily targeting Pakistan, in addition to other neighboring countries. The 360 Intelligence Center observed four distinct campaigns against Pakistan since 2017 (link), recently targeting Pakistani businessmen working in China. They also note that DoNot has targeted other South Asian countries for cyber espionage purposes. DoNot Team's confirmed use of this IP dates back to September 2018, with a six-month gap until it was used to host doppelganger domains for the LUCKY ELEPHANT campaign in early February.

The targeting of Pakistan, Bangladesh, Sri Lanka, Maldives, Myanmar, Nepal, and the Shanghai Cooperation Organization are all historical espionage targets by India. The Indian government is particularly concerned with its neighboring countries, specifically regarding contested land; the targeting aligns with these concerns. The heavier targeting in Pakistan adheres to historical targeting and the ongoing tension between the two countries, which has escalated since a terrorist attack in Kashmir on 14 February 2019.

Figure 3: South Asia Map (generated by Google Maps)

Conclusion

Social engineering continues to be a key tool for adversaries to trick users into yielding valuable information. The actors behind LUCKY ELEPHANT recognize the effectiveness and use doppelganger webpages nearly identical to legitimate sites, enticing users to input their credentials. It is unclear exactly how effective and widespread this campaign is at gathering credentials, as well as how any compromised credentials are being used. However, it is clear is that the actors are actively establishing infrastructure and are targeting governments in South Asia.

ASERT Researchers are interested in collaborating with others to further the collective knowledge of this campaign and we will tweet any additional IOCs under the Twitter handle @ASERTResearch.

Recommendations

- Organizations with a presence in South Asia should be on the lookout for these IOCs and examine any “password” or “account”-themed emails

- Users should always be wary when an email directs them to enter credentials of any kind
- Users should be cognizant of websites with TLDs such as .tk, .ml, .ga, .gq, and .cf, as they are highly unlikely to be a legitimate government or corporate domain
- Multi-factor authentication would likely prevent access from the compromised credentials
- If compromise of credentials is suspected, administrators should:
    - Perform an immediate password reset
    - Look for abnormal login activity that is outside the typical pattern of life for the legitimate user
    - Host infosec training for users and remind them they are a target--at work and home