IBM **X-Force Exchange** ALL

APT30

x-force (/search/%23x-force) threat-actor (/search/%23threat-actor)

(https://twitter.com/intent/tweet?text=APT30
%3A%2F
%2Fexchange.xforce.ibmcloud.com%2Fcollect
de76b1142bfc76ee62a5d82339c0ed18)
(https://www.linkedin.com/shareArticle?mini=tr
%3A%2F
%2Fexchange.xforce.ibmcloud.com%2Fcollect
de76b1142bfc76ee62a5d82339c0ed18&title=A
source=X-Force%20Exchange) (http://www
/sharer/sharer.php?u=https%3A%2F
%2Fexchange.xforce.ibmcloud.com%2Fcollect
de76b1142bfc76ee62a5d82339c0ed18&t=APT

▲ 1 ▼

Public Collection | 32 Followers | **TLP: (https://www.us-cert.gov/tlp) WHITE**

APT30

The APT30 threat actor, as dubbed by FireEye, has prosecuted a long running campaign of corporate and governmental espionage since at least 2005. They primarily target victims in Southeast Asia and India, possibly including classified government networks. Decoy documents on spear phishing emails tend toward topics related to India, Southeast Asia, border areas, and security and diplomatic issues in those areas. Of particular note, they have managed their operations well enough to continue using the same tools, tactics, and infrastructure over that period.

TTPs

- They generally target sensitive data for exfiltration, rather than pursuing direct financial reward.
- They have developed tools to attack air-gapped networks.
- They frequently register their own CnC domains. Some have been in use for years.
- Continuous automatic updating of the malware after infection.
- Spear phishing emails often appear to originate with governmental agencies, and target both personal and organizational email accounts of the intended victims.

Protocols Used

- HTTP (80/tcp)
- HTTPS (443/tcp)

- FTP (21/tcp)

Malware Used

The APT30 threat actor uses a variety of malware in its campaigns.

- Backdoor.Win32.Backspace.A (http://telussecuritylabs.com/threats/show/TSL20150414-18) (ZJ and ZR versions) (a/k/a Lecna) -- Backdoor
- NetEagle (Scout and Norton versions) -- Backdoor
- ShipShape -- Air-Gap Bridge
- SpaceShip -- Air-Gap Bridge
- FlashFlood -- Air-Gap Bridge
- Milkmaid
- Orangeade
- Creamsicle
- Backbend
- GemCutter

Additional Indicators

MD5

- MAL 15304d20221a26a0e413fba4c5729645 (/malware/15304d20221a26a0e413fba4c5729645)
- MAL 6ee35da59f92f71e757d4d5b964ecf00 (/malware/6ee35da59f92f71e757d4d5b964ecf00)

References

- APT30 and the Mechanics of a Long-Running Cyber Espionage Operation (https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf.) (PDF, FireEye)
- https://github.com/fireeye/iocs/tree/master/APT30 (https://github.com/fireeye/iocs/tree/master/APT30)
- Threat Description: Lecna (https://www.f-secure.com/v-descs/lecna_b.shtml) (HTML, F-Secure)

COLLECTION DETAILS **COMMENTS (0)**

Reports (202) +

VUL Virgin Media Hub denial of service
Report captured on Nov 7, 2018 12:30:01 AM by Zealous Williams

MAL d86df4f012398a9ea8742e62685415a1
Report captured on Mar 20, 2018 6:16:41 AM by 祎 刘

IP 145.14.144.200
Report captured on Nov 22, 2017 3:26:07 PM by Brian Roleston

URL http://tasconlin.com
Report captured on Nov 22, 2017 3:26:06 PM by Brian Roleston

IP 58.71.94.131
Report captured on Nov 22, 2017 3:26:04 PM by Brian Roleston

View all reports

Attachments (0) +

Linked Collections (0) +

Version History (21)

Doug Franklin
Last modified: Nov 7, 2018 12:30:02 AM

Doug Franklin
Last modified: Nov 22, 2017 3:26:08 PM

Doug Franklin
Last modified: May 17, 2017 9:34:32 PM

Doug Franklin
Last modified: Sep 11, 2015 4:53:18 PM