

China: Cyber Activities Probably Prelude to Election Espionage

China is probing the presidential campaign for opportunities to tailor collection and gather insight on policy positions on US-Chinese issues. US policy on China is a longstanding high collection priority for Beijing, and Chinese cyber actors have conducted such activity in every US presidential election campaign since at least 2008, according to [REDACTED]

[REDACTED] open-source reporting.

- Since [REDACTED] 2018, Chinese cyber actors known in the private sector as APT31—[REDACTED]
[REDACTED]—have targeted the personal e-mail accounts of senior US leadership, including officials in the Executive Office of the President and high-ranking officials in multiple Executive Branch organizations, Congress, and the federal judiciary, [REDACTED]
- Since 2017, a separate [REDACTED] has worked with the [REDACTED] to enable more stealthy operations by identifying the e-mail addresses of high-level US officials, then requesting that [REDACTED] obtain or crack the passwords for targeted accounts, [REDACTED]



Chinese cyber actors are targeting US presidential campaign information, probably to gather intelligence that enables future operations.

As the 2020 election approaches, the IC has detected Chinese state-sponsored cyber actors targeting the former Vice President's presidential campaign, probably to gather intelligence that could enable future operations, the first instance this election cycle that we have seen them directly targeting a US presidential campaign China has also conducted cyber espionage against other US election-related entities, [REDACTED] The IC assesses that China does not currently intend to covertly interfere to try to sway the outcome of the election, although this activity could enable such operations, if Beijing made a decision to do so.

- As of 20 May, APT31 actors had sent spear-phishing e-mails containing tracking links to the G-mail accounts of staffers associated with a presidential campaign, [REDACTED] On 4 June, Google announced that APT31 was targeting the campaign.
- Google and the FBI both briefed campaign officials on the Chinese cyber operations shortly after discovering the activity. Google officials have publicly stated that the spear-phishing attempts were unsuccessful; [REDACTED]
- During the past year, Chinese cyber actors have collected US election-related information from US voter databases, a polling data company, political and nonprofit organizations, fundraisers, and advisory organizations for political campaigns, [REDACTED]

APT31's method of sending tracking links suggests that the Chinese operators are mapping out the target network for follow-on approaches, possibly including tasking campaign staffers' e-mail accounts in the Chinese military's signals intelligence system for collection. Tracking links collect metadata such as

Classified By: [REDACTED]

Derived From: [REDACTED]

Declassify On: [REDACTED]

Internet activity and system information that the operators can use to exploit the accounts and identify other targets of interest.

- [REDACTED] Knowledge of a campaign official's operating system and software would allow cyber actors to determine whether they could quickly exploit known vulnerabilities or if they needed to develop malware to gain undetected access to the victim's machine.
- [REDACTED] If a target opened a spear-phishing e-mail with a tracking link—even without clicking on any links—it would confirm an active account for the cyber actors, potentially narrowing the target set for future [REDACTED] operations.

(U) For additional information:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Produced jointly under the auspices of the Chief of Analysis, [REDACTED] the Federal Bureau of Investigation, and the National Security Agency.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

DOCUMENT DETAILS

CONTENTS

Produced By: CIA **Product Type:** World Intelligence Review **Document Number:** WIRe2020-05063

Publication Date: 01 Jul 2020

Contact: [REDACTED] (secure), [REDACTED] (open)

Material used in the WIRe may be subject to copyright laws. Further reproduction and dissemination by any means, for any purpose other than official business, may be subject to copyright restrictions and is generally prohibited without the permission of the copyright holder.