Iranian Spies Accidentally Leaked Videos of Themselves Hacking

wired.com/story/iran-apt35-hacking-video/

Andy Greenberg   July 16, 2020
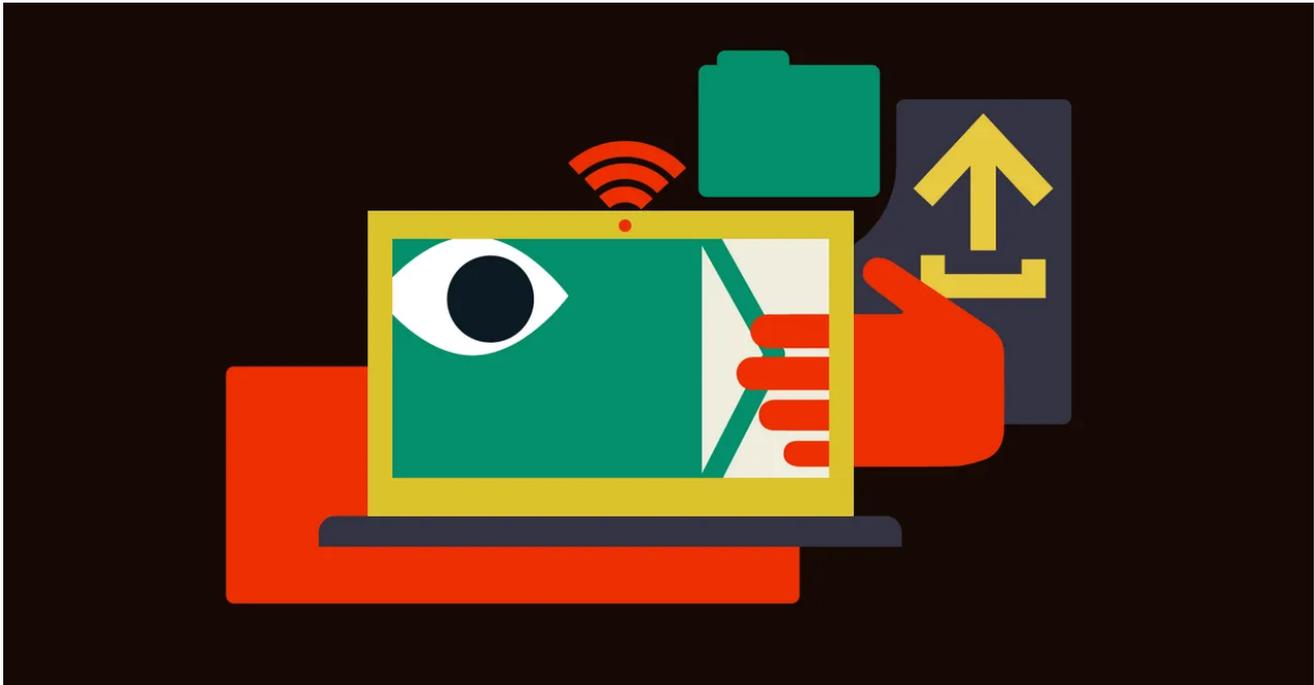
When security researchers piece together the blow-by-blow of a state-sponsored hacking operation, they're usually following a thin trail of malicious code samples, network logs, and connections to faraway servers. That detective work gets significantly easier when hackers record what they're doing and upload the video to an unprotected server on the open internet. Which is precisely what a group of Iranian hackers may have unwittingly done.

Researchers at IBM's X-Force security team revealed today that they've obtained roughly five hours of video footage that appears to have been recorded directly from the screens of hackers working for a group IBM calls ITG18, and which other security firms refer to as APT35 or Charming Kitten. It's one of the most active state-sponsored espionage teams linked to the government of Iran. The leaked videos were found among 40 gigabytes of data that the hackers had apparently stolen from victim accounts, including US and Greek military personnel. Other clues in the data suggest that the hackers targeted US State Department staff and an unnamed Iranian-American philanthropist.

The IBM researchers say they found the videos exposed due to a misconfiguration of security settings on a virtual private cloud server they'd observed in previous APT35 activity. The files were all uploaded to the exposed server over a few days in May, just as IBM was monitoring the machine. The videos appear to be training demonstrations the Iran-backed

hackers made to show junior team members how to handle hacked accounts. They show the hackers accessing compromised Gmail and Yahoo Mail accounts to download their contents, as well as exfiltrating other Google-hosted data from victims.

This sort of data exfiltration and management of hacked accounts is hardly sophisticated hacking. It's more the kind of labor-intensive but relatively simple work that's necessary in a large-scale phishing operation. But the videos nonetheless represent a rare artifact, showing a first-hand view of state-sponsored cyberspying that's almost never seen outside of an intelligence agency.

"We don't get this kind of insight into how threat actors operate really ever," says Allison Wikoff, a senior analyst at IBM X-Force whose team discovered the videos. "When we talk about observing hands-on activity, it's usually from incident-response engagements or endpoint monitoring tools. Very rarely do we actually see the adversary on their own desktop. It's a whole other level of 'hands-on-keyboard' observation."

"Nothing was off-limits."

Allison Wikoff, IBM X-Force

In two videos IBM showed to WIRED on the condition that they not be published, the hackers demonstrate the workflow for siphoning data out of a hacked account. In one video, the hacker logs into a compromised Gmail account—a dummy account for the demonstration— by plugging in credentials from a text document, and links it to the email software Zimbra, designed to manage multiple accounts from a single interface, using Zimbra to download the account's entire inbox to the hacker's machine. Then the hacker quickly deletes the alert in the victim's Gmail that says their account permissions have been changed. Next the hacker downloads the victim's contacts and photos from their Google account too. A second video shows a similar workflow for a Yahoo account.

A screenshot from a leaked video of Iranian hackers demonstrating how to exfiltrate emails from a Yahoo account using the email management tool Zimbra.Screenshot: IBM

The most telling element of the video, Wikoff says, is the speed the hacker demonstrates in exfiltrating the accounts' information in real time. The Google account's data is stolen in around four minutes. The Yahoo account takes less than three minutes. In both cases, of course, a real account populated with tens or hundreds of gigabytes of data would take far longer to download. But the clips demonstrate how quickly that download process is set up, Wikoff says, and suggest that the hackers are likely carrying out this sort of personal data theft on a mass scale. "To see how adept they are at going in and out of all these different webmail accounts and setting them up to exfiltrate, it is just amazing," says Wikoff. "It's a well-oiled machine."

In some cases, IBM's researchers could see in the video that the same dummy accounts were also themselves being used to send phishing emails, with bounced emails to invalid addresses appearing in the accounts' inboxes. The researchers say those bounced emails revealed some of the APT35 hackers' targeting, including American State Department staff as well as an Iranian-American philanthropist. It's not clear if either target was successfully phished. The dummy Yahoo account also briefly shows the phone number linked with it, which begins with Iran's +98 country code.

In other videos the IBM researchers declined to show to WIRED, the researchers say the hackers appeared to be combing through and exfiltrating data from real victims' accounts, rather than ones they created for training purposes. One victim was a member of the US Navy, and another was a two-decade veteran of the Greek Navy. The researchers say the APT35 hackers appear to have stolen photos, emails, tax records, and other personal information from both targeted individuals.

A file directory on an unsecured server used by the APT35 hackers, listing accounts whose data they had stolen.Screenshot: IBM

In some clips, the researchers say they observed the hackers working through a text document full of usernames and passwords for a long list of non-email accounts, from phone carriers to bank accounts, as well as some as trivial as pizza delivery and music-streaming services. "Nothing was off-limits," Wikoff says. The researchers note that they didn't see any evidence that the hackers were able to bypass two-factor authentication, however. When an account was secured with any second form of authentication, the hackers simply moved on to the next one on their list.

The sort of targeting that IBM's findings reveal fits with previous known operations tied to APT35, which has carried out espionage on behalf of Iran for years, most often with phishing attacks as its first point of intrusion. The group has focused on government and military targets that represent a direct challenge to Iran, such as nuclear regulators and sanctions bodies. More recently it has aimed its phishing emails at pharmaceutical companies involved in Covid-19 research and President Donald Trump's reelection campaign.

It's hardly unprecedented for hackers to accidentally leave behind revealing tools or documents on an unsecured server, points out former NSA staffer Emily Crose, who now works as a researcher for the security firm Dragos. But Crose says she's not aware of any public instance of actual videos of state-sponsored hackers' own operations being left for investigators, as in this case. And given that the hacked accounts likely also contain evidence of how they were compromised, she says the leaked videos may well force the Iranian hackers to change some of their tactics. "This kind of thing is a rare win for the defenders," Crose says. "It's like playing poker and having your opponents lay their entire hand out flat on the table in the middle of the last flop."

Even so, IBM says it doesn't expect its discovery of the APT35 videos to slow down the pace of the hacking group's operations. After all, it had <u>nearly a hundred of its domains seized by Microsoft last year</u>. "They simply rebuilt and kept going," says Wikoff. If that sort of infrastructure purge didn't slow down the Iranians, she says, don't expect a bit of video-leaked exposure to, either.

More Great WIRED Stories

- Behind bars, but <u>still posting on TikTok</u>
- My friend was struck by ALS. To fight back, <u>he built a movement</u>
- Deepfakes are becoming the <u>hot new corporate training tool</u>
- America has a sick obsession <u>with Covid-19 polls</u>
- Who discovered <u>the first vaccine</u>?
- 👁 If done right, AI could <u>make policing fairer</u>. Plus: <u>Get the latest AI news</u>
- 📱 Torn between the latest phones? Never fear—check out our <u>iPhone buying guide</u> and <u>favorite Android phones</u>