New research exposes Iranian threat group operations

By Allison Wikoff, Richard Emerson

Published: 2020-07-16 · Archived: 2026-04-05 21:55:40 UTC

Author

Allison Wikoff

Strategic Cyber Threat Analyst

IBM Security

Richard Emerson

Cyber Threat Intelligence Analyst

IBM X-Force Incident Response Intelligence Services (IRIS) has uncovered rare details on the operations of the suspected Iranian threat group ITG18, which overlaps with Charming Kitten and Phosphorus. In the past few weeks, ITG18 has been associated with targeting of pharmaceutical companies and the U.S. presidential campaigns. Now, due to operational errors—a basic misconfiguration—by suspected ITG18 associates, a server with more than 40 gigabytes of data on their operations has been analyzed by X-Force IRIS analysts.

Rarely are there opportunities to understand how the operator behaves behind the keyboard, and even rarer still are there recordings the operator self-produced showing their operations. But that is exactly what X-Force IRIS uncovered on an ITG18 operator whose OPSEC failures provide a unique behind-the-scenes look into their methods, and potentially, their legwork for a broader operation that is likely underway.

During a three-day period in May 2020, IBM X-Force IRIS discovered the 40 GBs of video and data files being uploaded to a server that hosted numerous ITG18 domains used in earlier 2020 activity. Some of the videos showed the operator managing adversary-created accounts while others showed the operator testing access and exfiltrating data from previously compromised accounts.

Among the information IBM X-Force IRIS uncovered were:

- In nearly five hours of videos, an ITG18 operator searching through and exfiltrating data from various compromised accounts of a member of U.S. Navy and a personnel officer with nearly two decades of service in Hellenic Navy. Using these accounts could allow the operator to obtain other data on military operations of potential interest to Iran.
- Failed phishing attempts targeting the personal accounts of an Iranian-American philanthropist and officials of the U.S. State Department.
- Personas and Iranian phone numbers associated to ITG18 operators.

IBM X-Force IRIS's longitudinal examination of this threat group's targeting indicates ITG18 has used its infrastructure for multiple, diverse strategic objectives that serve both short and long-term interests. ITG18 has been active since at least 2013. Hallmarks of this group's activity includes credential harvesting and email compromise operations through phishing attacks against numerous targets of strategic interest to the Iranian government.

The video files uncovered by IBM X-Force IRIS were desktop recordings using a tool called Bandicam, ranging from 2 minutes to 2 hours. The timestamps of the files indicated the videos were recorded approximately one day prior to being uploaded to the ITG18-operated server.

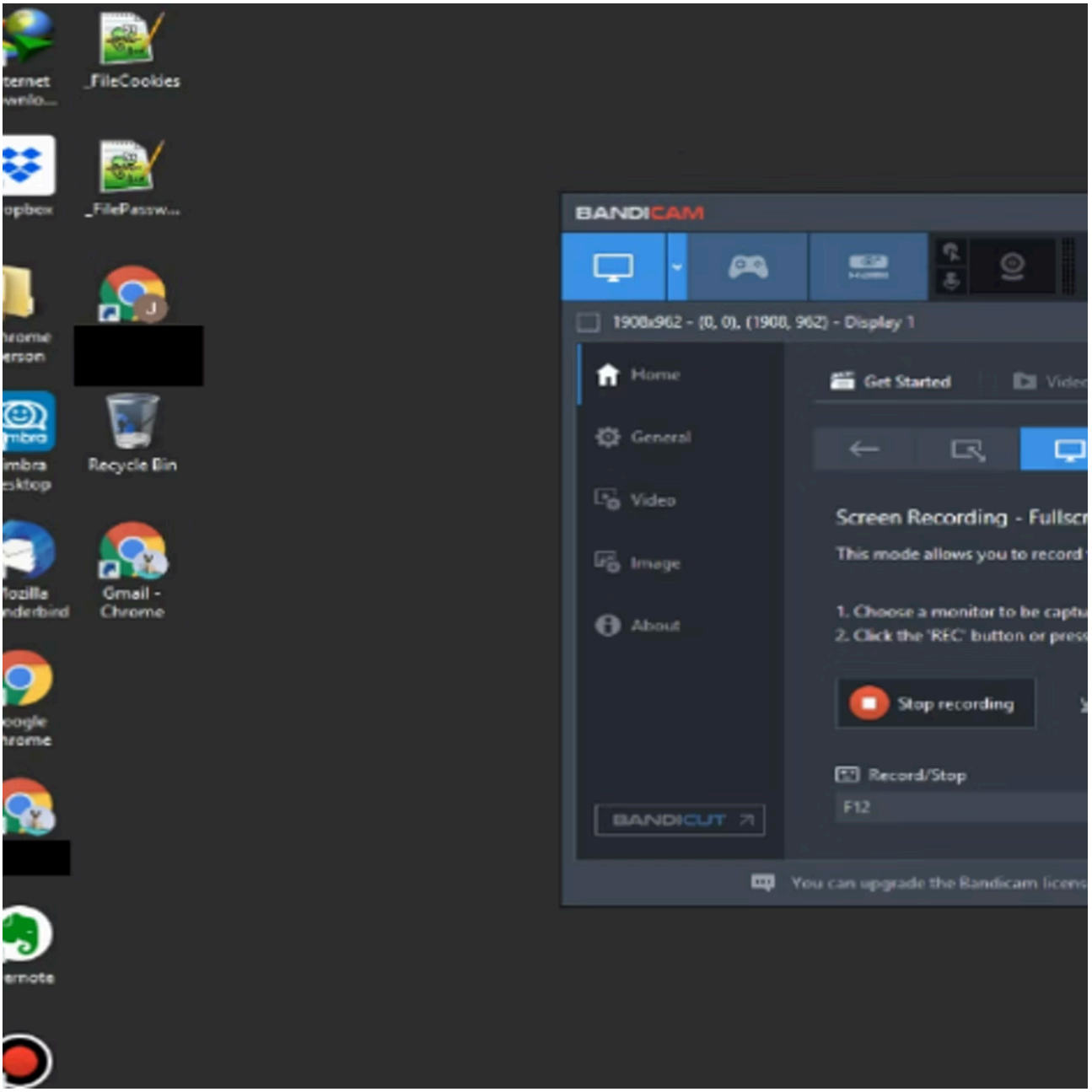

Figure 1: Image capture of ITG18 operator desktop from Bandicam recording (Source: IBM X-Force IRIS)

In five of the video files, named “AOL.avi”, “Aol Contact.avi”, “Gmail.avi”, “Yahoo.avi”, “Hotmail.avi”, the operator uses a Notepad file containing one credential for each platform, and video-by-video copied and pasted them into the associated website. The operator moved on to demonstrate how to exfiltrate various datasets associated with these platforms including contacts, photos, and associated cloud storage.

An additional action the operator took was to modify settings within the account security section of each account in order to add the account to Zimbra, a legitimate email collaboration platform that can aggregate numerous email accounts into one interface. Through the use of this platform, the operator was able to monitor and manage various compromised email accounts simultaneously.

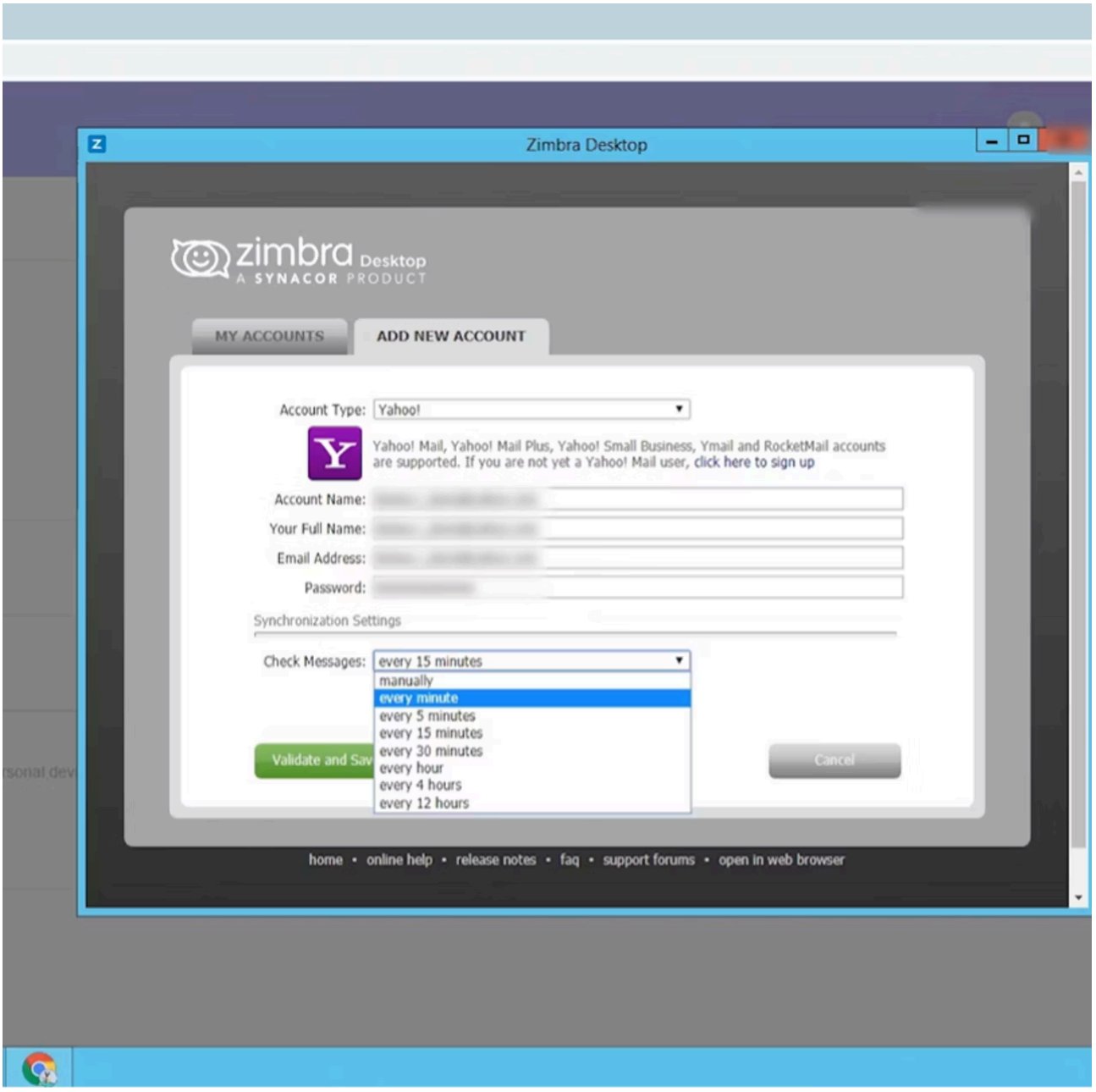

Figure 2: Image capture of ITG18 operator syncing their persona account to Zimbra (Source: IBM X-Force IRIS)

Some of the accounts were likely threat actor personas—designed to appear as real people to victims.

Some of the operator-owned accounts observed in the training videos provided additional insight into personas associated to ITG18, such as phone numbers with Iranian country codes. IBM X-Force IRIS observed the "Yahoo.avi" video displayed profile details for a fake persona, which we will reference as "Persona A" including a phone number with a +98 country code, the international country code for Iran. (See Figure 3)

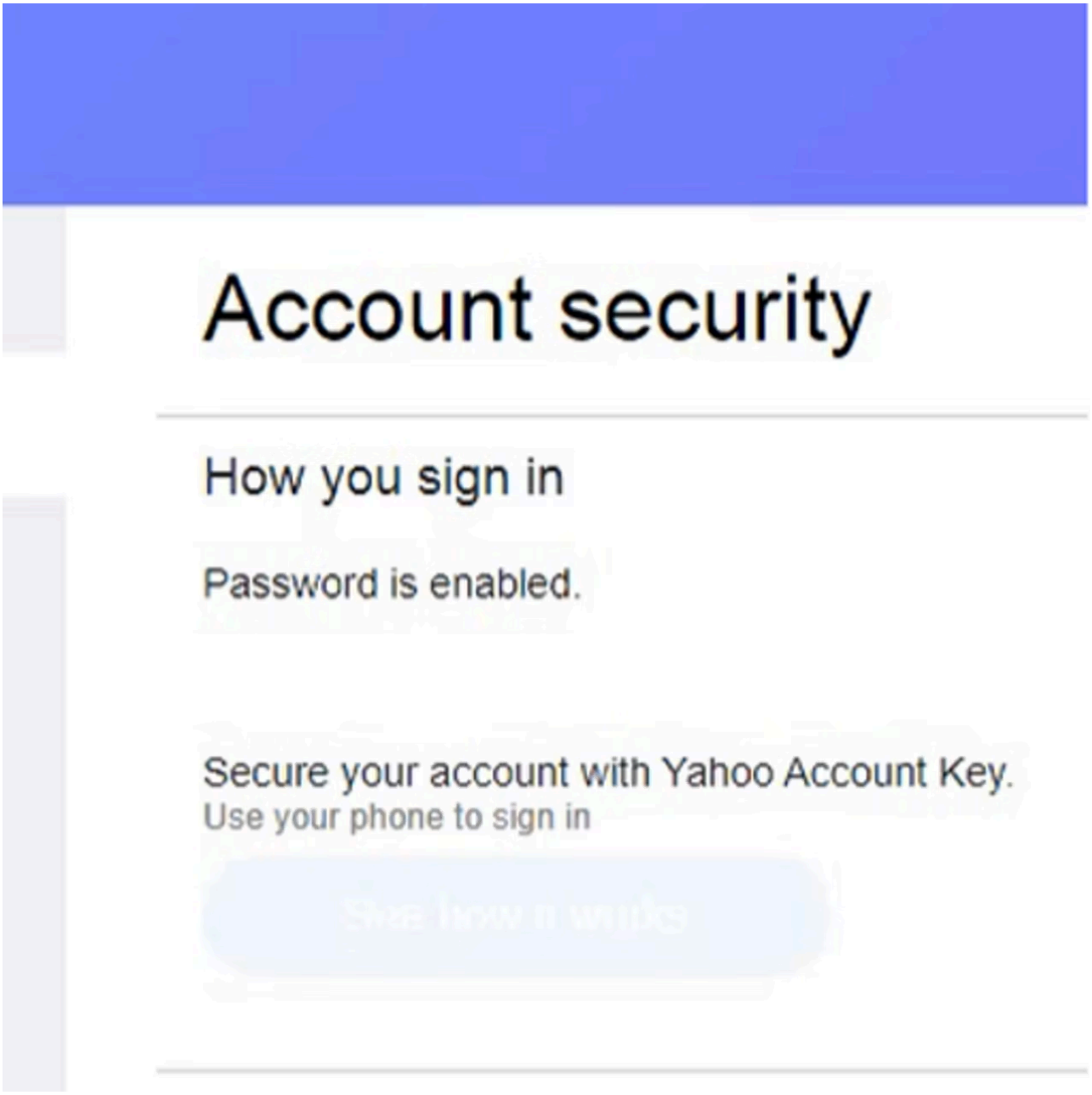

Figure 3: Persona A has an Iranian phone number (+98) associated with the account (Source: IBM X-Force IRIS)

Other suggestions of an Iranian operator behind Persona A included unsuccessful attempts to send emails to an Iranian American philanthropist, and potentially two personal email accounts for U.S. State Department officials in April 2020, including one account that was associated with the U.S. Virtual Embassy to Iran. The recording appeared to show bounce-back emails in the operator's inbox, notifying them that these possible spear phishing emails did not go through, though we do not know the theme. The targeting of these individuals is in line with prior ITG18 operations.

Three of the video files discovered reveal that ITG18 had successfully compromised several accounts associated with an enlisted member of the United States Navy as well as an officer in the Hellenic Navy. Specifically, ITG18 had credentials for a number of what appear to be their personal email and social media accounts – a common characteristic of ITG18, as observed in previous operations.

The videos show the operator following a similar playbook to the training videos involving the persona accounts. Once successful access to victims' accounts was gained, the ITG18 operator actively deleted notifications sent to the compromised accounts suggesting suspicious logins, presumably as to not alert the victims.

The operator exported all account contacts, photos, documents from associated cloud storage sites, such as Google Drive, before adding the webmail account credentials to Zimbra, presumably for monitoring. The operator was also able to sign into victims' Google Takeout (takeout.google.com), which allows a user to export content from their Google Account, to include location history, information from Chrome, and associated Android devices.

This included gaining access to associated other accounts owned by the victims, illustrating the breadth of information that ITG18 was able to collect on the two military members. Amongst the personal files exfiltrated on the U.S. Navy enlisted member were details on the military unit they were associated with including the Naval base they were affiliated with. The operator collected a significant amount of personal information about this victim including presumed residence, personal photos including numerous selfies and a video of a home being staged, tax records and the contents of a personal cloud storage site (See Figure 4). Similar information was exfiltrated for the Hellenic Navy officer, including information from a Gmail account, an account associated with a Greek university and a Hellenic Navy payroll site.

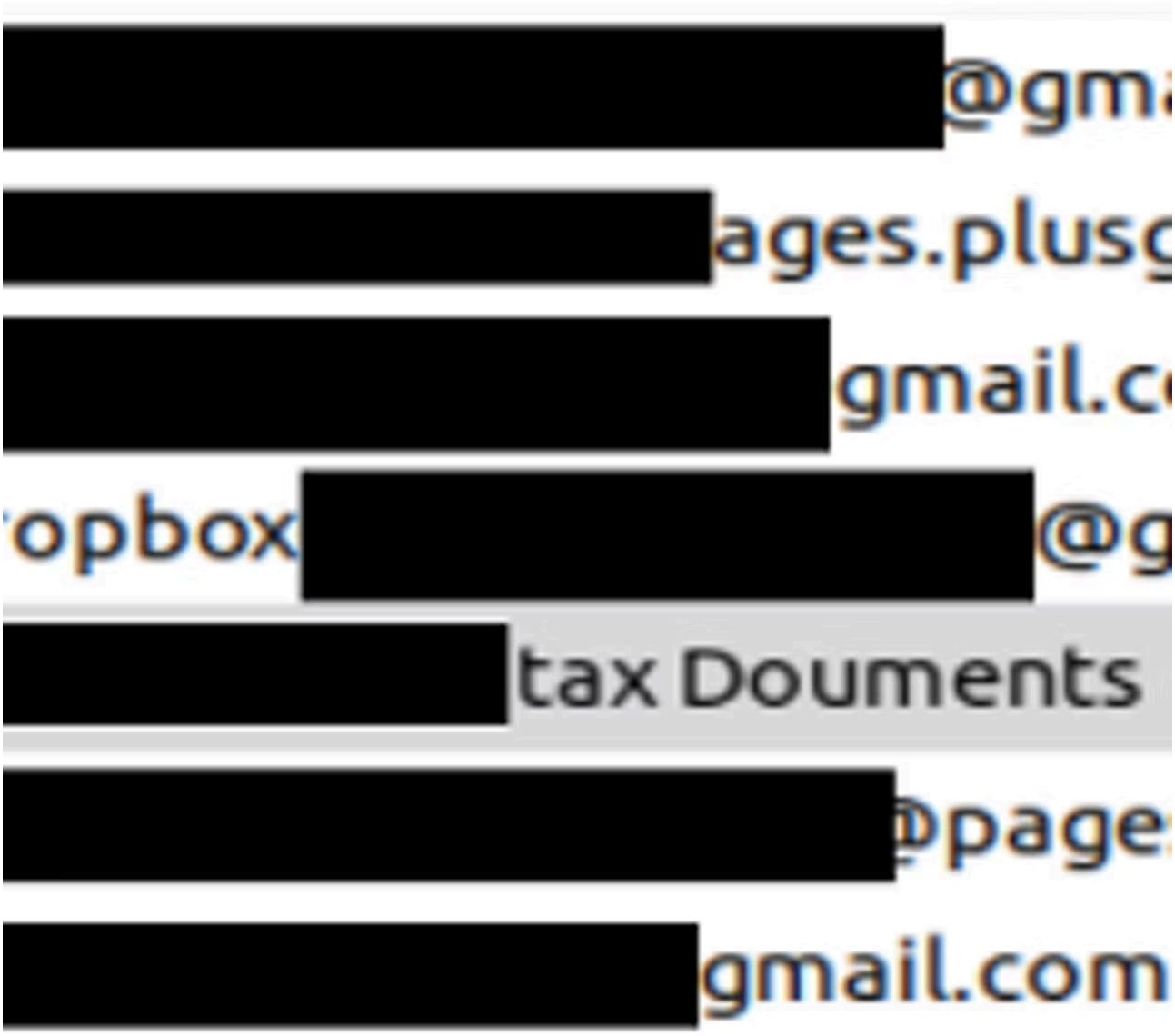

Figure 4: Screenshot of some of the folders on the ITG18 server. These folders contained exfiltrated data from the accounts of a victim (Source: IBM X-Force IRIS)

For non-email accounts, the operator validated credentials no matter how trivial seeming the website may have been. Some of the categories of the websites the operator validated credentials for included video and music streaming, pizza delivery, credit reporting, student financial aid, municipal utility, banks, baby products, video games, and mobile carriers, to name a few. The operators appear to have been meticulously gathering trivial social information about the individuals. In total, the operator attempted to validate credentials for at least 75 different websites across the two individuals.

If the credentials were successful, the operator frequently visited the account details page first, presumably to review sensitive information available there. Also of note, the operator, who only used the Chrome browser to

validate credentials, frequently used the built-in translation feature to translate websites in the Greek language to English when checking the credentials associated with the Hellenic Navy member.

IBM X-Force IRIS did not find evidence of the two military members' professional network credentials being compromised, and no professional information appears to have been included. However, it's possible that the threat actor was searching for specific information within the military members' personal files that would allow ITG18 to extend their cyber espionage operation further into the U.S. and Greek Navy.

During the videos where the operator was validating victim credentials, if the operator successfully authenticated against a site that was set up with multifactor authentication (MFA) they paused and moved on to another set of credentials without gaining access.

The compromise of personal files of members of the Greek and U.S. Navy could be in support of espionage operations related to numerous proceedings occurring in the Gulf of Oman and Arabian Gulf. It is also worth noting that the U.S. and Greece are strategic allies, with a nearly eight-decade mutual defense cooperation agreement. Greece hosts a U.S. naval base in Crete in the Eastern Mediterranean.

Some target types of ITG18 have remained consistent over the past three years while others appear associated with specific geopolitical events. For instance, while ITG18 has consistently targeted individuals with an Iranian connection over the past three years, in 2018 the group targeted individuals associated with the U.S. Office of Foreign Assets Control, a group that implements economic sanctions. This timing aligned with new sanctions the U.S. was developing as global concessions to extend sanctions on Iran expired. More recently, ITG18's April 2020 targeting of a pharmaceutical executive aligns with Iran's COVID-19 outbreak, which spiked at the end of March 2020.

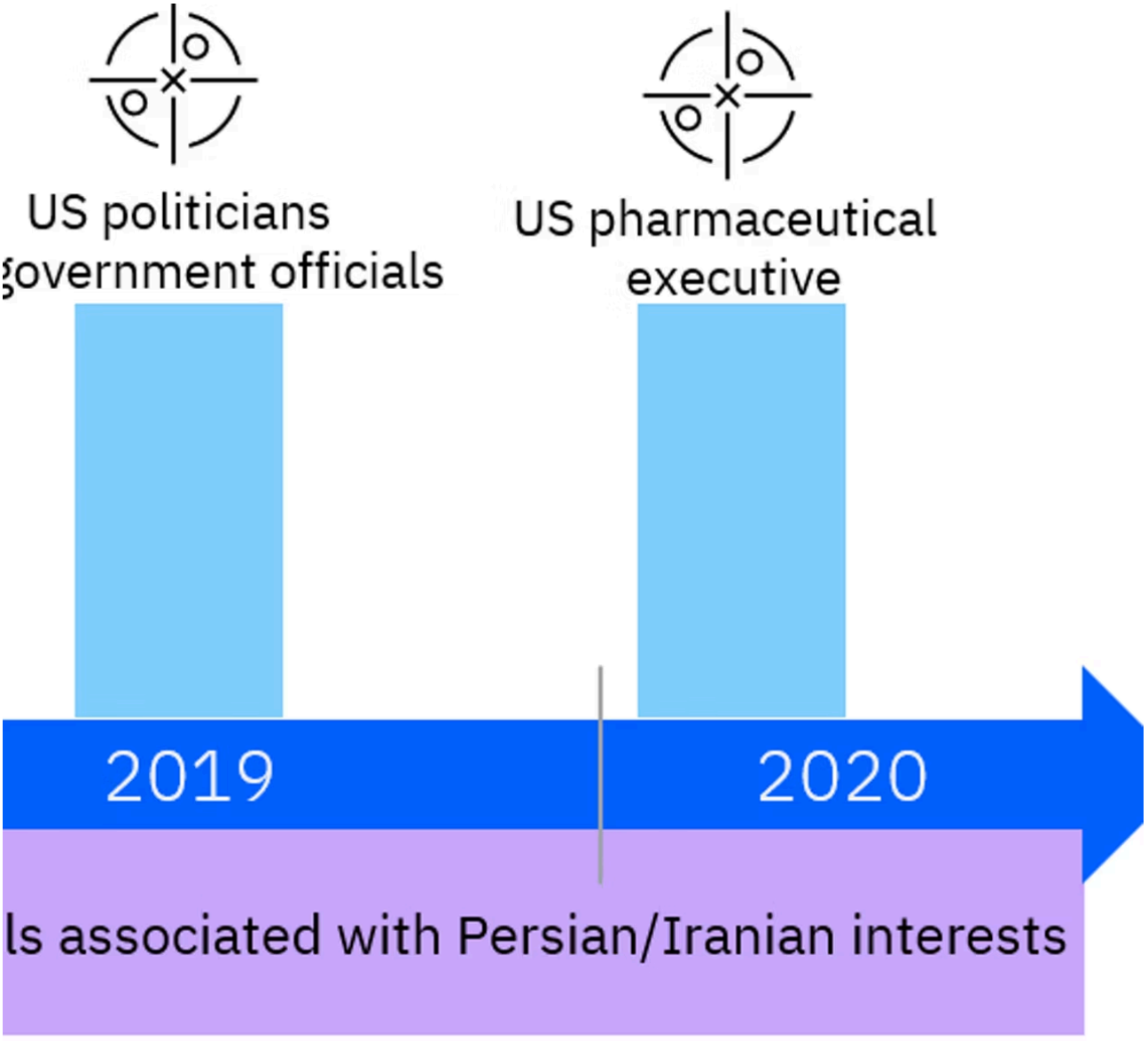

Figure 5: Timeline of ITG18 targeting demonstrating its blended objectives (Source: IBM X-Force IRIS)

Regardless of motivation, mistakes by the ITG18 operator allowed IBM X-Force IRIS to gain valuable insights into how this group might accomplish action on its objectives and otherwise train its operators. IBM X-Force IRIS considers ITG18 a determined threat group with a significant investment in its operations. The group has shown persistence in its operations and consistent creation of new infrastructure despite multiple public disclosures and broad reporting on its activity.

ITG18 has demonstrated it performs operations to serve multiple, distinct long-term objectives that align to Iranian strategic interests. It is highly likely the group has been successful in these efforts as its operational cadence for harvesting credentials has not significantly changed over several years.

The discovery also emphasizes the need to follow certain important security hygiene practices, including:

Use multifactor authentication (MFA) – Multifactor authentication works as a fail-safe if a malicious actor has gained access to your credentials. As a last line of defense, MFA offers a second form of verification requirement in order to access an account.

Reset your passwords periodically – Don't use the same password across various accounts and regularly update passwords. If you use the same password for all your accounts, it can leave you open to multiple attacks if one account is compromised. Consider using unique passphrases and more than 14 characters for stronger passwords.

Use a password manager – Password managers can generate stronger passwords for you, and they do not require you to memorize them.

Review settings and limit access to third-party apps from your email – In a few instances, the operators had to change account preferences to permit third-party apps to connect with compromised accounts. These settings allowed the threat actor to extend the access they had to other victims.

Additional analysis of ITG18's tactics, techniques and procedures (TTP) and is available on our Enterprise Intelligence Management platform via TruSTAR, which was originally published June 2, 2020.

Responsible disclosure

During the course of the investigation and where possible, IBM X-Force IRIS notified the appropriate parties about the activity and compromised accounts.
