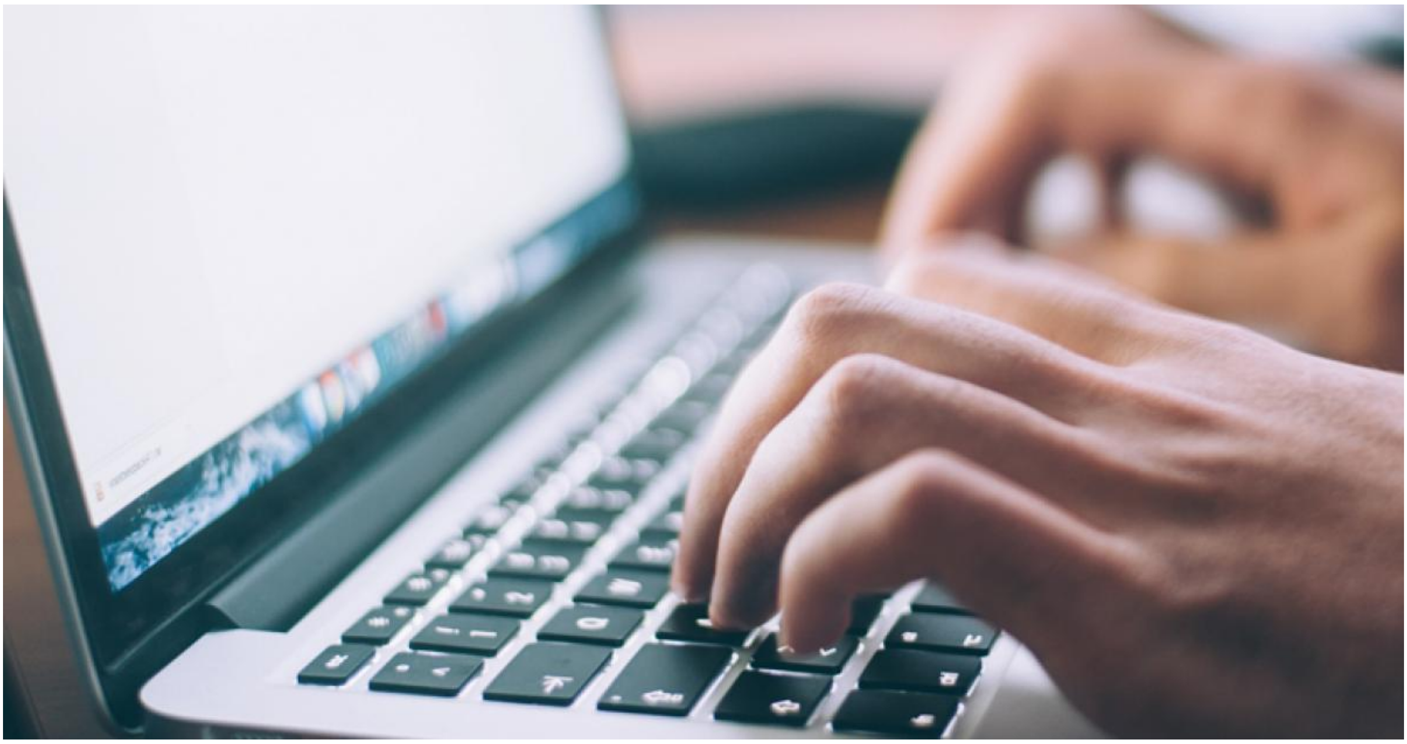
Would’ve, Could’ve, Should’ve…Did: TA453 Refuses to be Bound by Expectations

: 12/8/2022



December 14, 2022 Joshua Miller, Crista Giering and the Proofpoint Threat Research Team

Key Takeaways

- From at least late 2020 and through 2022, TA453 has engaged in campaigns that deviate from the group's expected phishing techniques and target victimology.
- In these campaigns, TA453 has employed the use of compromised accounts, malware, and confrontational lures to go after targets with a range of backgrounds from medical researchers to realtors to travel agencies.
- Proofpoint researchers assess with moderate confidence that this activity reflects a flexible mandate to the Islamic Revolutionary Guard Corps' (IRGC) intelligence requirements.
- Further, a sub-cluster of TA453 activity demonstrates a possible directive to support covert, and even kinetic, operations of the IRGC.

Overview

Since at least late 2020, Proofpoint researchers have observed aberrations in TA453 (which overlaps with groups publicly known as Charming Kitten, PHOSPHORUS, and APT42) phishing activity in which the threat actor has stepped away from its typical phishing techniques and target victimology. A hallmark of TA453’s email campaigns is that they almost always target academics, researchers, diplomats, dissidents, journalists, human rights workers, and use web beacons in the message bodies before eventually attempting to harvest a target's credentials. Such campaigns may kick off with weeks of benign conversations from actor-created accounts before attempted exploitation.

By comparison, TA453's outlier campaigns have targeted medical researchers, an aerospace engineer, a realtor, and travel agencies, among others. They have leveraged new-to-TA453 phishing techniques including compromised accounts, malware, and confrontational lures. Proofpoint judges with moderate confidence that this atypical activity reflects TA453's dynamic support to ad hoc Islamic Revolutionary Guard Corps' (IRGC) intelligence requirements. This activity also provides researchers with a better understanding of the IRGC's mandate and insight into TA453's potential support of IRGC surveillance and attempted kinetic operations.

Expected TA453 Activity

Proofpoint tracks approximately six subgroups of TA453—more details of which are shared in the Attribution section of this report—differentiated primarily by victimology, techniques, and infrastructure. Regardless of the subgroup, TA453 typically targets academics, policymakers, diplomats, journalists, human rights workers, dissidents, and researchers with expertise in the Middle East. Email accounts registered by TA453 generally match thematically with their targets and the threat actor favors including web beacons in its email campaigns. TA453 heavily relies on benign conversations to initiate contact with targets—of which Proofpoint has observed over 60 such campaigns in 2022. TA453 almost always delivers credential harvesting links with the intent of gaining access to a target's inbox for exfiltration of email content. Some subgroups will converse for weeks before delivering the malicious links, while others will immediately send the malicious link in the first email.

TA453 Branches Out with its Techniques and Targeting

Beginning in late 2020, Proofpoint researchers started to observe campaigns that deviated from TA453's expected phishing activity. These deviations have received little, if any, public attention, causing Proofpoint to decide to share our insights in this report. The campaigns notably leveraged techniques not previously associated with TA453's email activity, such as:

- Compromised accounts
    - At times, a subcluster of TA453 used compromised accounts to target individuals instead of using actor-controlled accounts.
    - This cluster of activity operated actor-controlled URL shorteners like bnt2[.]live and nco2[.]live that redirected to typical TA453 credential harvesting pages.
    - For example, in 2021, approximately five days after a US government official publicly commented on the Joint Comprehensive Plan of Action (JCPOA) negotiations, the official's press secretary was targeted via a compromised email account from a local reporter.
- Malware
    - In the fall of 2021, GhostEcho (CharmPower), a PowerShell backdoor, was sent to a variety of diplomatic missions across Tehran.
    - Throughout the Fall of 2021, GhostEcho was under development as demonstrated by changes in obfuscation and modifications to the kill chain, likely to evade detection.

    - GhostEcho is a lightweight first stage used to deliver follow-on espionage focused capabilities as documented by CheckPoint Research.
    - Based on similarities in delivery techniques, Proofpoint suspects that GhostEcho was also delivered to women's rights activists in late 2021 but the payload was not available at the time of our analysis.
- Confrontational lures
    - TA453 has leveraged one persona in particular, Samantha Wolf, for confrontational social engineering lures intended to use a target's sense of uncertainty and fear to get them to respond to the threat actor's emails.
    - Samantha, who we discuss in the next section, has sent these lures, including car accident and general complaint themes, to US and European politicians and government entities, a Middle Eastern energy company, and a US-based academic.

The following is a comprehensive chart of Proofpoint-observed outlier activity followed by deeper dives into campaigns that exemplify TA453's irregular activity.

Highlights of Proofpoint-Observed Abnormal TA453 Targeting Between 2020 and 2022

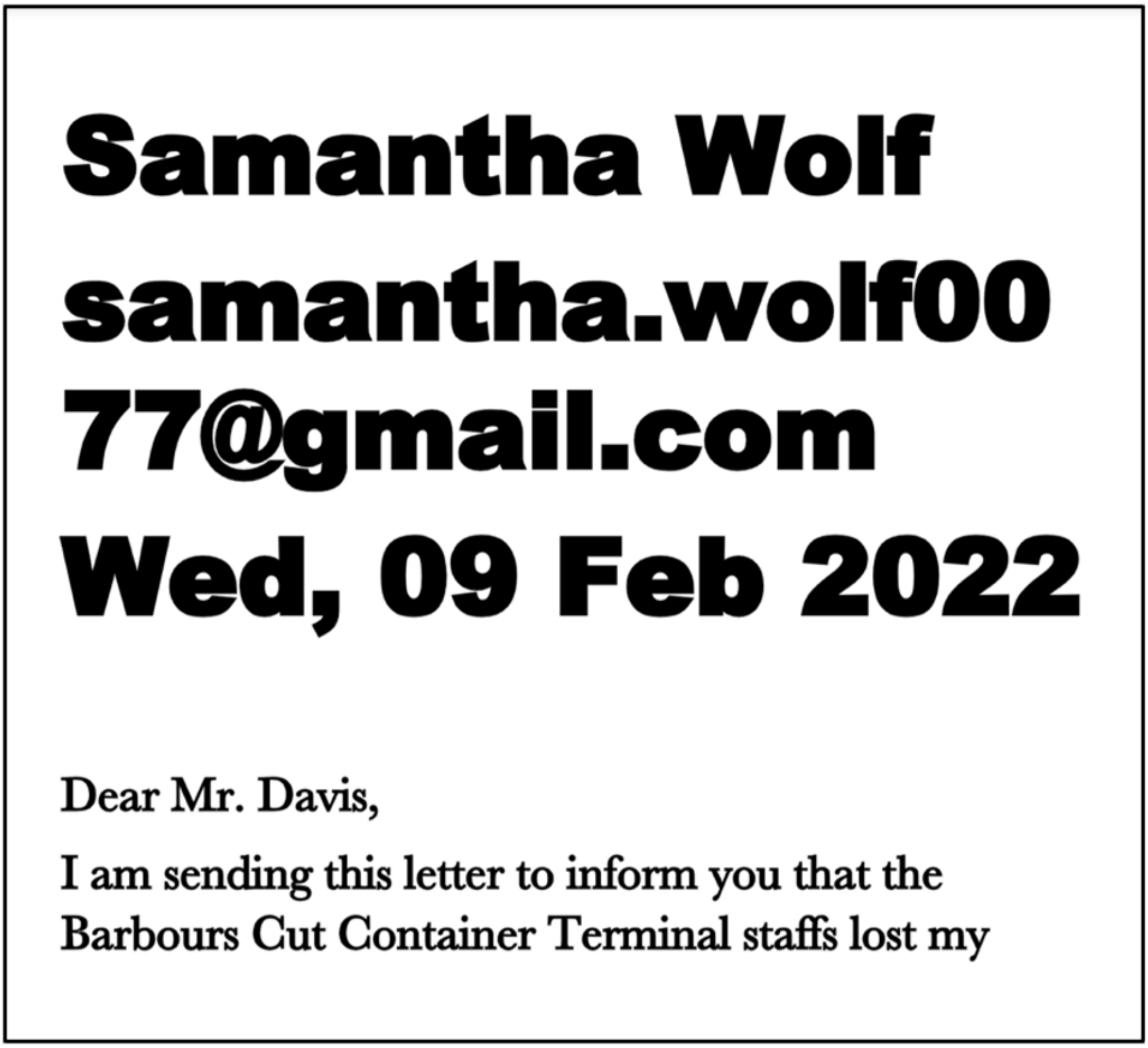
Time of Activity	**Activity Description**
December 2020: Medical Targeting	In TA453's BadBlood campaign they targeted senior medical professionals who specialize in genetic, neurology, and oncology research in the United States and Israel with credential phishing.
2021: Aerospace Company	According to some open-source reporting, the Islamic Revolutionary Guard Corps (IRGC) has increasingly inserted themselves into Iran's fledgling space program, so it is not surprising that TA453 targeted the email accounts of an engineer involved in space research in 2021.
July & August 2021: Women's and Gender Studies	Proofpoint identified a cluster of spear phishing targeting scholars with backgrounds in women's and gender studies at a variety of North American universities. These campaigns started with generic password change lures, but the targets eventually received separate benign conversation emails that TA453 is known for. Proofpoint also observed an email address associated with this cluster of activity targeting an international sporting organization.
August 2021: Iranian Travel Agencies	Proofpoint identified multiple Iranian travel agencies operating out of Tehran that were targeted with TA453 credential harvesting links. The targeting of travel agencies is consistent with intelligence agency collection requirements of both the movement of Iranians outside of Iran along with domestic travel.
June 2022: Medical Research	As noted in our recent blog on Multi-Persona Impersonation, TA453 occasionally targets medical researchers. Most recently they focused their attentions on researchers working on organ replacement.
February 2022: Realtor in Florida	Proofpoint observed a Gmail address targeting a Florida-based realtor with a benign conversation and TA453 affiliated web beacon. Open-source research of the realtor identified they were involved in the sale of multiple homes located near the headquarters of US Central Command (CENTCOM) during the phishing campaign.

CENTCOM is the US Combatant Command responsible for military operations in the Middle East.

The tracking pixel was hosted on profilepic[.]site, which Proofpoint attributes to TA453 partially based on registration similarities to other known TA453 domains.

Samantha? I don’t even know a Samantha…Do I?

Proofpoint researchers first identified the Samantha Wolf persona when the associated email, samantha.wolf0077[@]gmail.com, was included in the lure content of a malicious document (SHA256: a8c062846411d3fb8ceb0b2fe34389c4910a4887cd39552d30e6a03a02f4cc78). This document, which was uploaded to VirusTotal, used remote template injection to download multiple .dotm files from office-updates[.]info and is attributed to TA453. The attack chain for this cluster of activity typically resulted in a PowerShell backdoor Proofpoint calls GhostEcho (publicly tracked as CharmPower). As detailed by PwC, the downloaded template establishes persistence by replacing the user’s previous default Microsoft Word template.



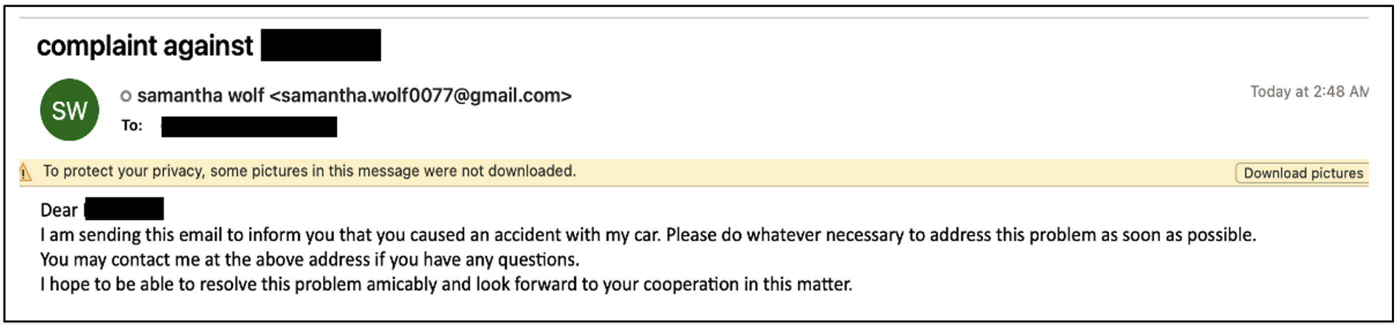
Samantha Wolf
samantha.wolf0077@gmail.com
Wed, 09 Feb 2022

Dear Mr. Davis,

I am sending this letter to inform you that the Barbours Cut Container Terminal staffs lost my

Figure 1. Screenshot of the lure document containing the Samantha Wolf email persona.

In mid-March 2022 and early April 2022, Proofpoint researchers first observed TA453 using Samantha as the actor-controlled sender to target a Middle Eastern energy company with benign conversation emails. In late April 2022, Samantha pivoted to target a US-based academic Proofpoint previously observed targeted by multiple Iranian intrusion sets, including traditional approaches by TA453. This lure broke the typical TA453 mold and used confrontational tactics to increase the urgency behind the lure.



complaint against [redacted]

samantha wolf <samantha.wolf0077@gmail.com>

To: [redacted]

Today at 2:48 AM

To protect your privacy, some pictures in this message were not downloaded.

Dear [redacted]
I am sending this email to inform you that you caused an accident with my car. Please do whatever necessary to address this problem as soon as possible.
You may contact me at the above address if you have any questions.
I hope to be able to resolve this problem amicably and look forward to your cooperation in this matter.

Figure 2. The Samantha persona reaches out to a US-based academic claiming a car accident.

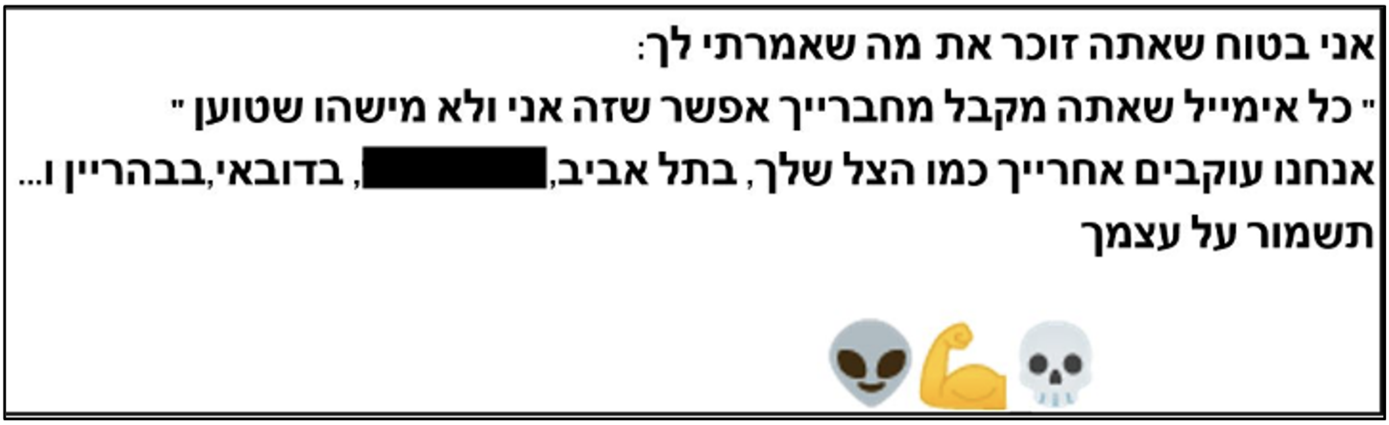
In late 2022, Samantha encountered even more people with whom she has taken umbrage, sending additional complaint-themed benign conversation emails to senior US and European government officials. Samantha's confrontational lures demonstrate an interesting attempt to generate engagement with targets not seen from other TA453 accounts.

Not So Charming: A Look at TA453's Aggressive Side

While most of TA453's operations have appeared to focus on collecting intelligence, a subset of late 2021 and mid-2022 activity showed a more aggressive side to TA453 that indicates possible support to the IRGC's kinetic operations.

In May 2022, Israeli media reported Israeli intelligence agency Shin Bet identified Iranian intelligence services' phishing activity designed to lure targets in order to kidnap them. Based on the indicators provided, Proofpoint correlated this activity with TA453 campaigns from December 2021 in which campaigns attributed to TA453 used a spoofed email address of a reputable academic from the domain (css-ethz[.]ch) to give a researcher an "Invitation to Zurich Strategic Dialogue Jan-2022."

In early May 2022, Proofpoint identified a disturbing TA453 attributed campaign targeting a single individual. In this campaign, TA453 utilized multiple compromised email accounts, including those of a high-ranking military official, to deliver a link to the target—a former member of the Israeli military. The use of multiple compromised email accounts to target a single target is unusual for TA453. While each of the URLs observed were unique to each compromised email account, each linked to the domain gettogether[.]quest and pointed to the same threatening message in Hebrew. The message displayed on the web page (Figure 3 below) was an image with the target's first name in the file name.



אני בטוח שאתה זוכר את מה שאמרתי לך:
"כל אימייל שאתה מקבל מחברייך אפשר שזה אני ולא מישהו שטוען"
אנחנו עוקבים אחרייך כמו הצל שלך , בתל אביב,[redacted] , בדובאי,בבהריין ו...
תשמור על עצמך

👽💪💀

Figure 3. Redacted screenshot of TA453's aggressive messaging in Hebrew.

Machine translation of the Hebrew text in the image:

I'm sure you remember what I told you

"Every email you get from your friends may be me and not someone who it claims"

We follow you like your shadow, in Tel Aviv, in [redacted], in Dubai, in Bahrain.

Take care of yourself

👽💪💀

After Proofpoint blocked the initial email attempts, TA453 included a commercial web beacon from mailtrack[.]io likely to verify the delivery of its threatening emails.

It is this method of using multiple compromised accounts belonging to established connections of the target to send a message of intimidation rather than a phishing link that indicates a possible collaboration between TA453 and hostile Iranian state-aligned operations. This assessment is further supported by the content of the email itself and overlapping infrastructure. The gettogether[.]quest domain has resolved to 66.29.153[.]90 since mid-April 2022. Co-located on that infrastructure since December 2021 is css-ethz[.]ch, the domain similar to the one spoofing The Center for Security Studies (CSS) at ETH Zurich in support of kidnapping operations discussed previously.

Additionally, Proofpoint in mid-2022 identified that a close affiliate of a former US official targeted in the IRGC murder-for-hire plot was targeted and successfully compromised by the Korg malware, a family exclusive to TA453. TA453 previously targeted this same individual with phishing links in April 2021 and July 2021. This further corroborates Proofpoint's assessment that a subcluster of TA453 supports kinetic IRGC operations.

Attribution

Proofpoint continues to assess that TA453 generally operates in support of the IRGC, specifically the IRGC Intelligence Organization (IRGC-IO). This assessment is based on a variety of evidence, including overlaps in unit numbering between Charming Kitten reports and IRGC units as identified by PWC, the US Department of Justice indictment of Monica Witt, and IRGC-affiliated actors, and analysis of TA453 targeting compared to reported IRGC-IO priorities. Proofpoint judges with moderate confidence that the more aggressive activity could represent collaboration with another branch of the Iranian state, including the IRGC Quds Force.

Clustering cyber espionage activity is often difficult when looking from different telemetry. Proofpoint currently views TA453 as overlapping with PHOSPHORUS and roughly equivalent to APT42 and Yellow Garuda, all of which can be considered Charming Kitten.

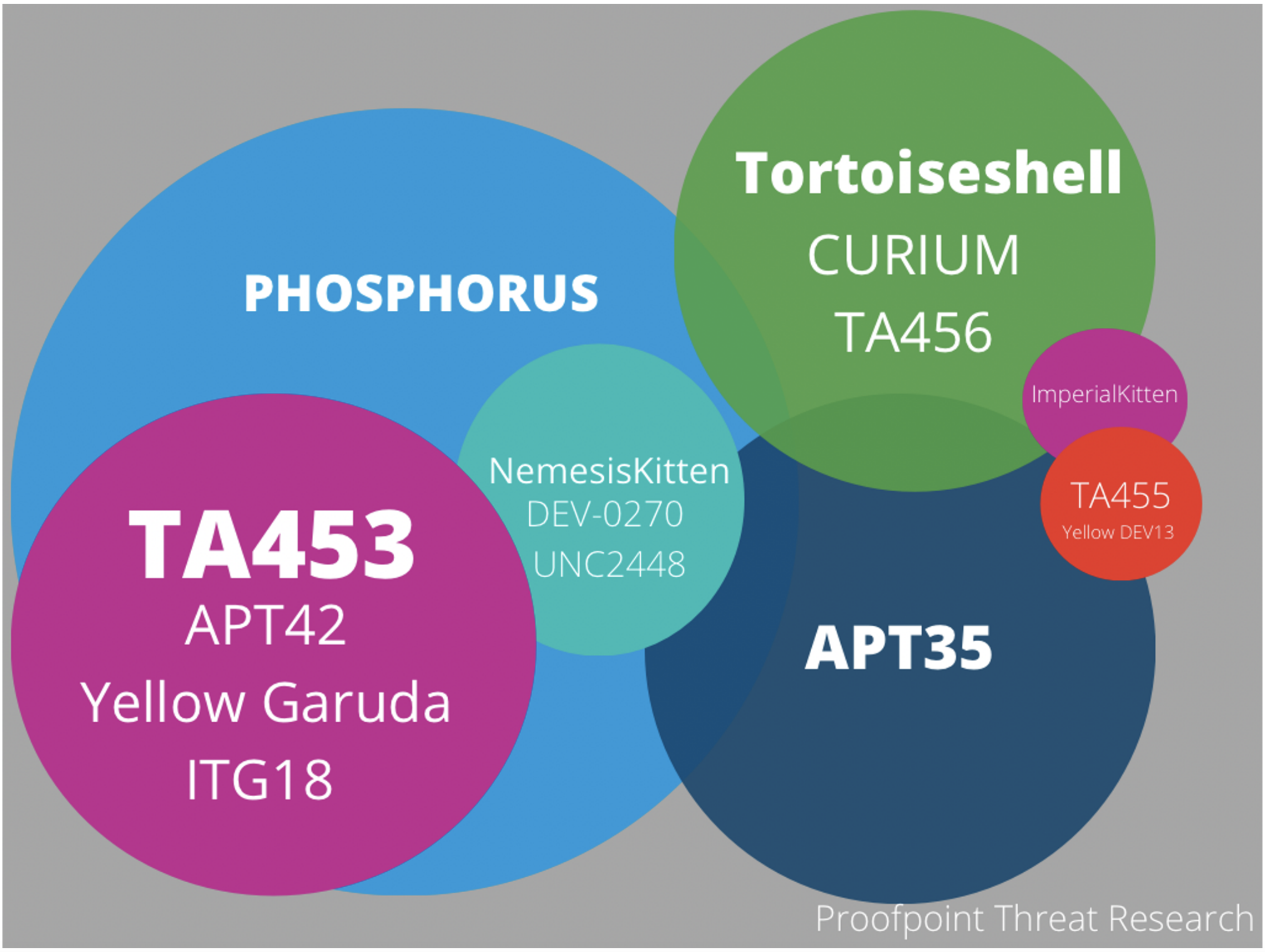


Figure 4. Charming Kitten activity clusters.

Conclusion

TA453, like its fellow advanced persistent threat actors engaged in espionage, is in a constant state of flux regarding its tools, tactics, techniques, and targeting. Adjusting its approaches likely in response to ever changing and expanding priorities, the Proofpoint-observed outlier campaigns are likely to continue and reflect IRGC intelligence collection requirements, including possible support for hostile, and even kinetic, operations.