


BadBlood: TA453 Targets US and Israeli Medical Research Personnel in Credential Phishing Campaigns

 proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential

March 30, 2021



Blog

Threat Insight

BadBlood: TA453 Targets US and Israeli Medical Research Personnel in Credential Phishing Campaigns



March 30, 2021 Joshua Miller and the Proofpoint Threat Research Team

Overview

In late 2020, **TA453**, an Iranian-nexus threat actor, launched a credential phishing campaign targeting senior medical professionals who specialize in genetic, neurology, and oncology research in the United States and Israel. TA453 (aka CHARMING KITTEN and PHOSPHORUS) has historically aligned with Islamic Revolutionary Guard Corps (IRGC) collection priorities, targeting dissidents, academics, diplomats, and journalists. This latest campaign, dubbed BadBlood, is a deviation from the group's usual activity. [1,2,3] While this campaign may represent a shift in TA453 targeting overall, it is also possible it may be the result of a specific short term intelligence collection requirement. BadBlood is aligned with an escalating trend of medical research being increasingly targeted by threat actors.

Proofpoint researchers have named this campaign BadBlood based on the medical focus and continued geopolitical tensions between Iran and Israel.

Credential Phishing Campaign

In this December 2020 campaign, TA453 used an actor-controlled Gmail account that masqueraded as a prominent Israeli physicist. The account (zajfman.daniel[.]gmail.com) sent messages with the subject "Nuclear weapons at a glance: Israel" and contained social engineering lures relating to Israeli nuclear capabilities. These malicious emails contained a link to the TA453-controlled domain 1drv[.]casa. When clicked, the URL leads to a landing site spoofing Microsoft's OneDrive service along with an image of a PDF document logo titled CBP-9075.pdf.

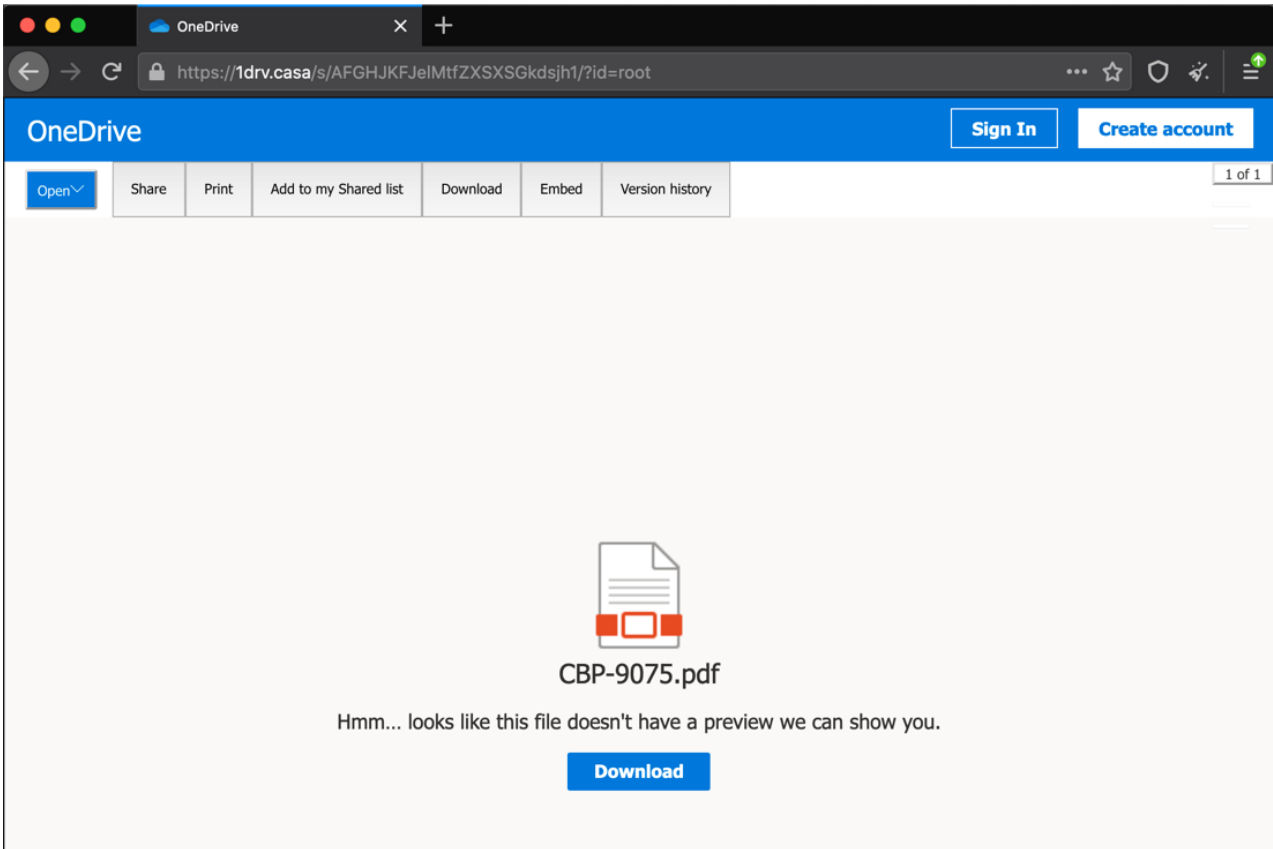


Figure 1: TA453 Landing Site with PDF Document Logo

When a user attempts to view and download the PDF document, 1drv[.]casa delivers a forged Microsoft login page which attempts to harvest user credentials. Attempting to use any other hyperlink in the webpage results in the same redirect to the same forged Microsoft login page, except for the "Create one!" link. This tab leads to the legitimate Microsoft Outlook "Sign Up" page at [https://signup.live\[.\]com](https://signup.live[.]com).

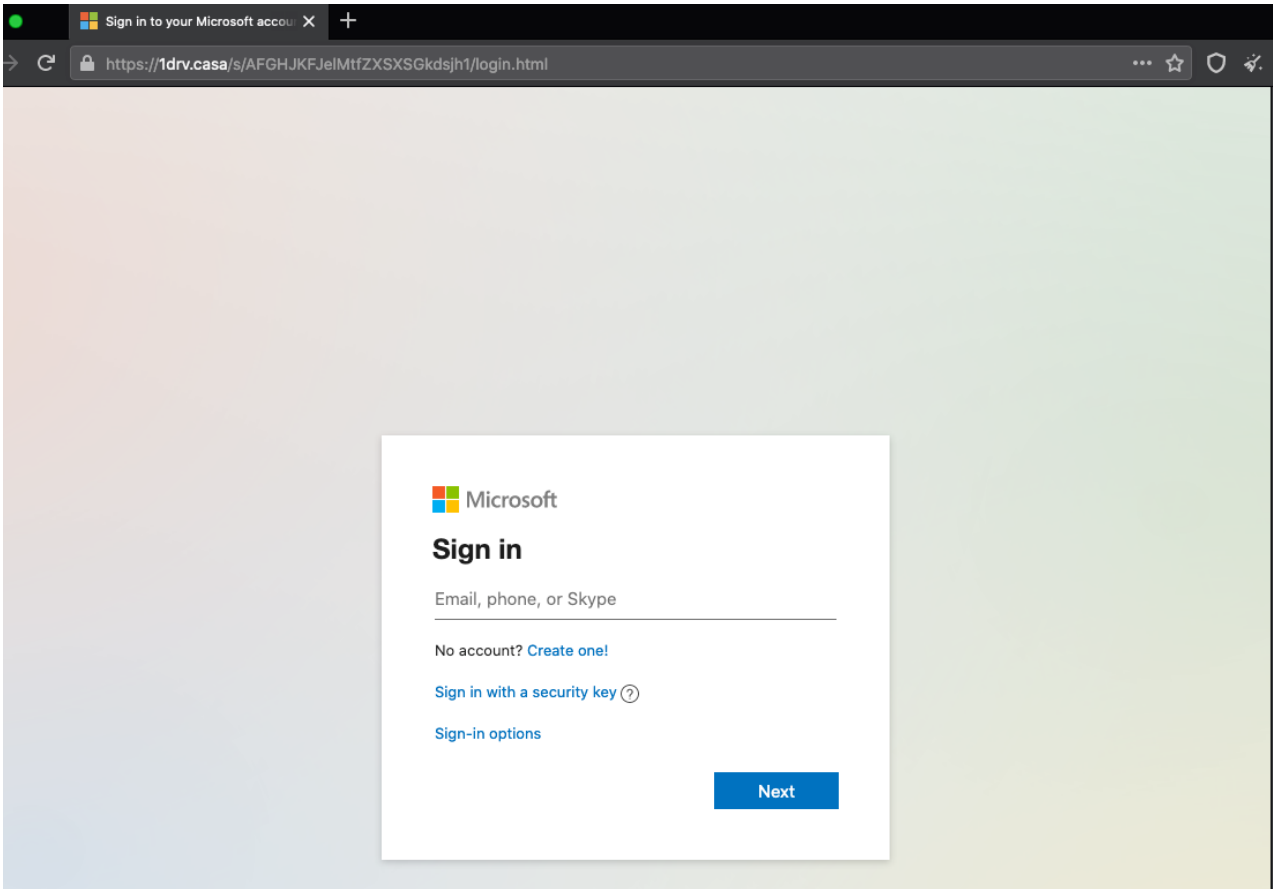


Figure 2: TA453 Credential Harvesting Page at 1drv[.] casa

Once an email is entered by the user and “Next” is clicked, the page prompts for a password.

Once a user enters their credentials, they are then redirected to Microsoft’s OneDrive where the benign "Nuclear weapons at a glance: Israel" document is hosted.

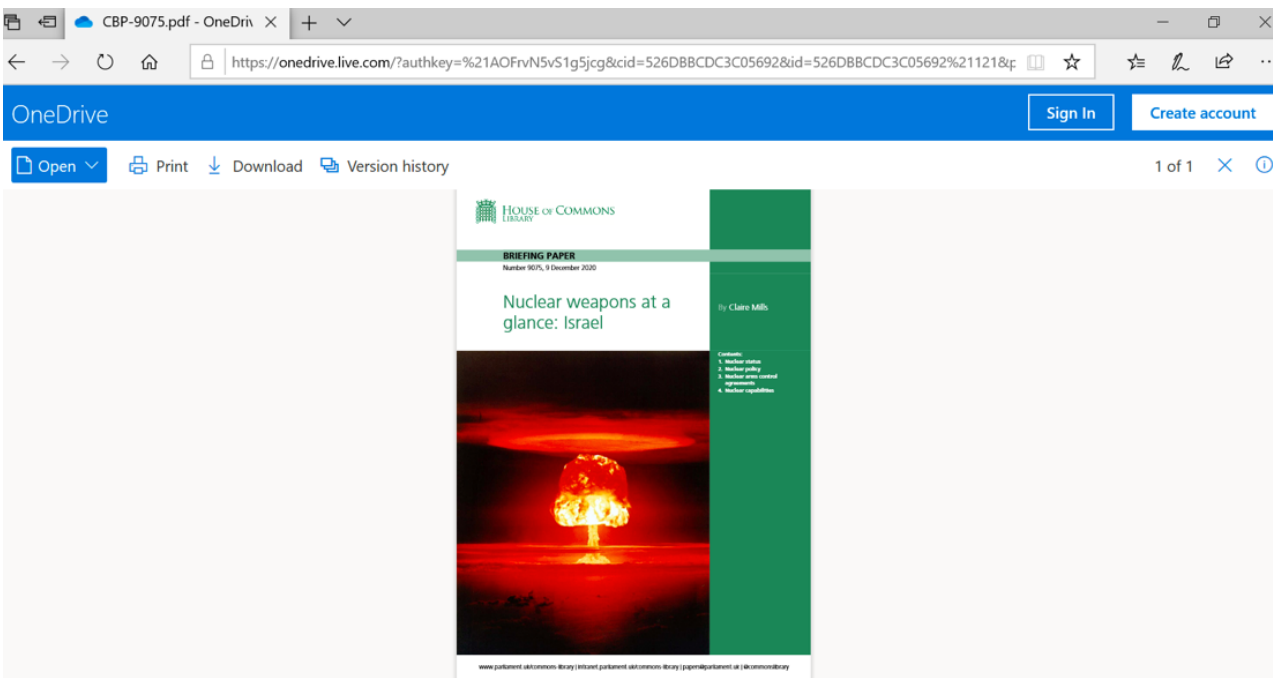


Figure 3: Microsoft OneDrive TA453 Benign Document

At this time, it does not appear 1drv[.]casa conducts any sort of multi-factor authentication bypass. Although Proofpoint does not currently have further visibility into how TA453 used any credentials obtained from this specific campaign, public reporting from CERTFA indicates TA453 has previously used harvested credentials to exfiltrate email inbox contents.[4] In select prior campaigns, Iranian-aligned actors, including TA453, have used compromised accounts for further phishing.[5]

Targeting

TA453 targeted less than 25 senior professionals at a variety of medical research organizations located in the US and Israel. Proofpoint analysis of the targets' publicly available research efforts and resumes indicate TA453 targeted individuals with a background in either genetics, oncology, or neurology. These medical professionals appear to be extremely senior personnel at a variety of medical research organizations. Additionally, TA453 targeting Israeli organizations and individuals is consistent with increased geopolitical tensions between Israel and Iran during 2020. [6]

At this time, Proofpoint cannot conclusively determine the motivation of actors conducting these campaigns. As collaboration for medical research is often conducted informally over email, this campaign may demonstrate that a subset of TA453 operators have an intelligence requirement to collect specific medical information related to genetic, oncology, or neurology research. Alternatively, this campaign may demonstrate an interest in the patient information of the targeted medical personnel or an aim to use the recipients' accounts in further phishing campaigns. While this campaign may represent a shift in TA453 targeting overall, it is also possible it may be an outlier, reflective of a specific priority intelligence tasking given to TA453.

Attribution

While Proofpoint cannot independently attribute TA453 to the IRGC, the tactics and techniques observed in BadBlood continue to mirror those used in historic TA453 campaigns and the overall targeting of TA453 campaigns detected by Proofpoint appear to support IRGC intelligence collection priorities.[7]

In 2019, the US Department of Justice indicted four Iranian individuals for using social media and credential phishing emails to conduct malicious computer intrusions on behalf of the IRGC.[8] Private industry reporting identified this activity as part of CHARMING KITTEN in both 2017 and 2019.[9,10] In early 2019, Microsoft reported TA453 was abusing well known email brands to conduct spearphishing operations against government agencies, political targets, and journalists on behalf of the Iranian government.[11]

Related Infrastructure

While investigating this campaign, Proofpoint Threat Research identified other domains attributed to TA453 with high confidence based on network infrastructure components, campaign timing, and similarity in lure documents. Both Proofpoint and VirusTotal telemetry indicated additional actor-controlled domains were used in TA453 campaigns attempted to compromise more traditional TA453 targets with a similar attack-chain in late December 2020. Finally, the provided lure documents at the end of the attack chain share similar, national security themes, including Congressional Research Reports, think tank publications, and other policy minded documents. While researchers were not able to directly correlate all of these domains with phishing campaigns, we judge this activity to be consistent with the BadBlood campaign.

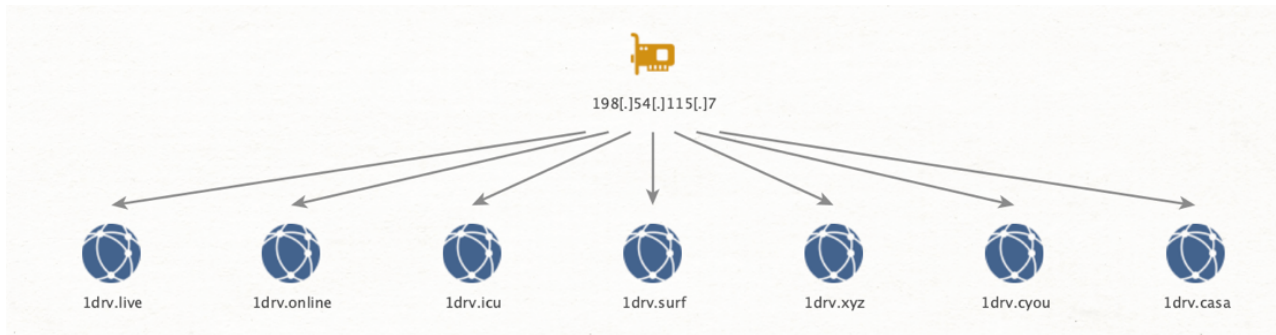


Figure 4: Diagram of Related Infrastructure

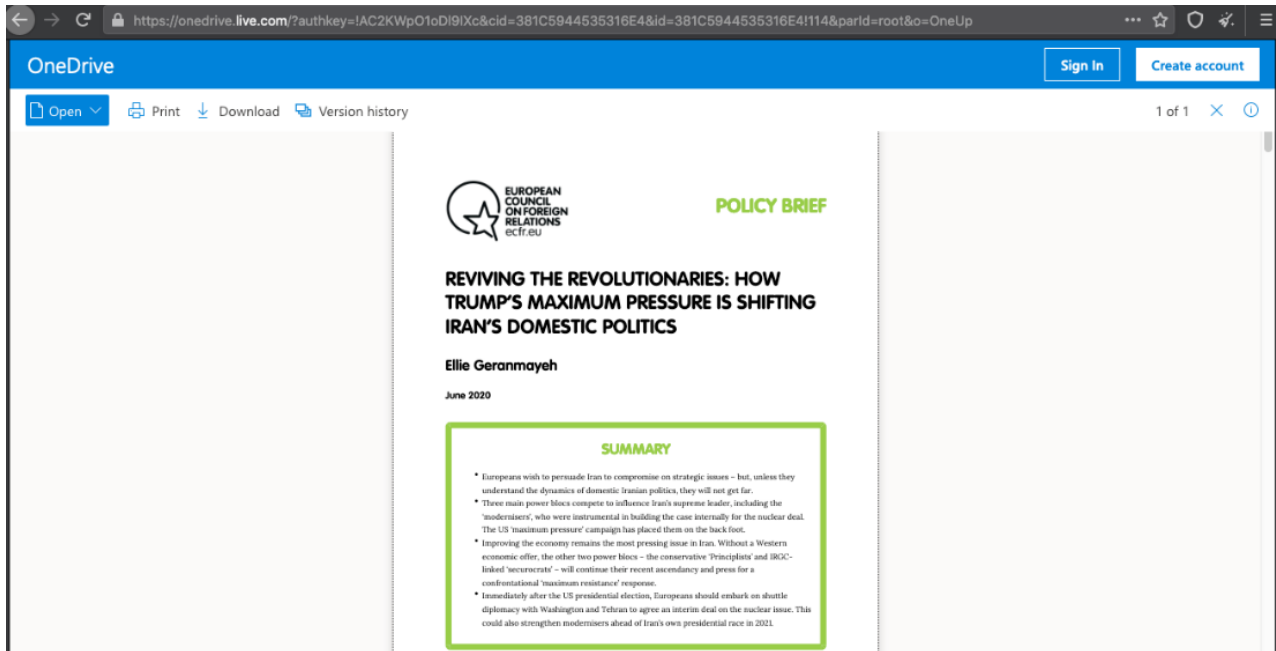


Figure 5: Final 1drv[.]xyz Lure “Reviving The Revolutionaries Document”

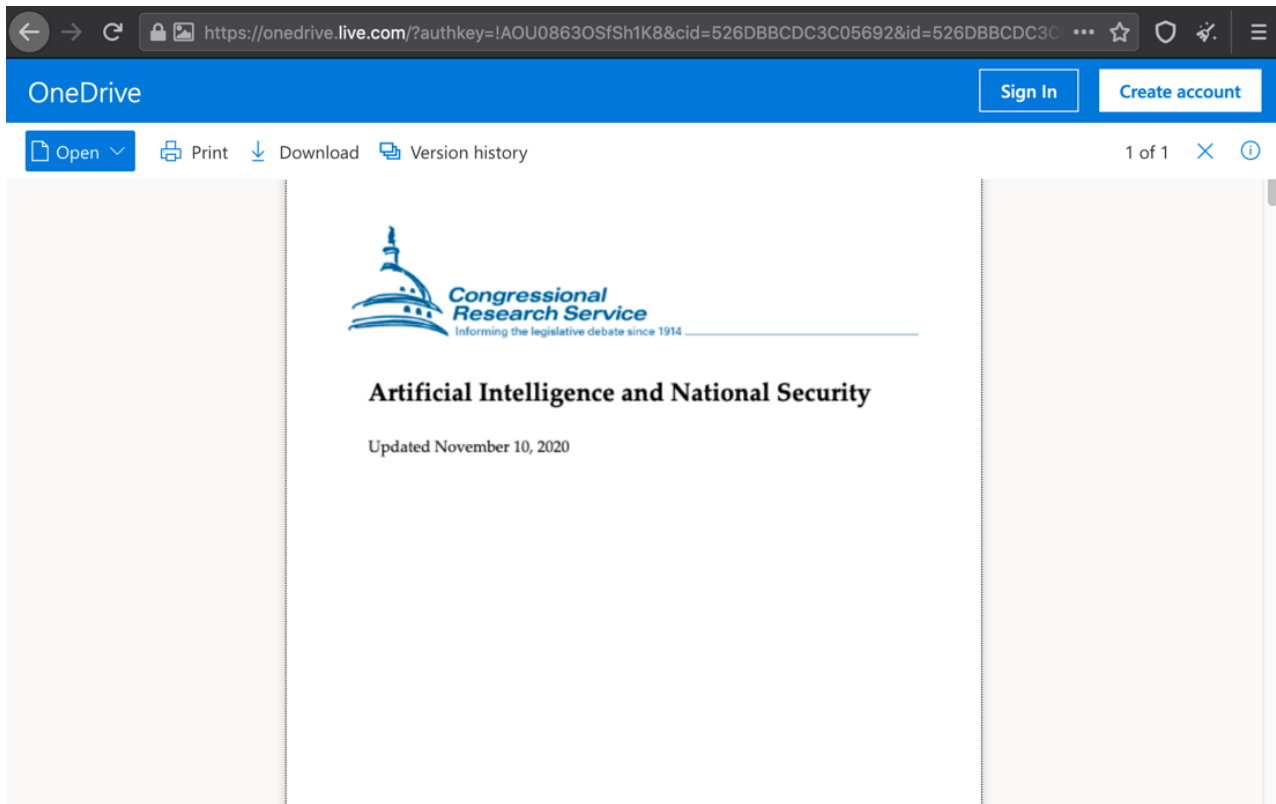


Figure 6: Final 1drv[.]surf Lure Congressional Research Service Document

Outlook

While TA453 has consistently demonstrated a desire to collect and exfiltrate the email mailbox contents belonging to typical intelligence targets of the Iranian government like the Iranian diaspora, policy analysts, and educators, this TA453 campaign demonstrated a desire to target medical researchers and providers. Further detection and analysis of TA453 campaigns will likely determine whether this targeting is an outlier or if targeting has evolved to support the medical sector becoming a consistent intelligence requirement and target for TA453.

While targeting medical experts in genetics, neurology and oncology may not be a lasting shift in TA453 targeting, it does indicate at least a temporary change in TA453 collection priorities. BadBlood is aligned with an escalating trend globally of medical research being increasingly targeted by espionage motivated focused threat actors. [12]

References

- [1] <https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/>
- [2] <https://blogs.microsoft.com/on-the-issues/2020/10/28/cyberattacks-phosphorus-t20-munich-security-conference/>
- [3] <https://www.clearskysec.com/wp-content/uploads/2020/08/The-Kittens-are-Back-in-Town-3.pdf>
- [4] <https://blog.certfa.com/posts/charming-kitten-christmas-gift/>

[5] https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

[6] <https://www.cpomagazine.com/cyber-security/hidden-cyber-war-between-israel-and-iran-spills-into-public-view-with-attacks-on-physical-infrastructure/>

[7] <https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-in-intelligence-operations>

[8] <https://www.justice.gov/opa/press-release/file/1131726/download>

[9] https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf

[10] <https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant>

[11] <https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking>

[12] <https://us-cert.cisa.gov/ncas/alerts/AA20126A>

Indicators of Compromise

IOC	IOC Type	Description
1drv[.]live	Domain	
1drv[.]online	Domain	Educational Credential Phishing Domain
1drv[.]jicu	Domain	
1drv[.]surf	Domain	
1drv[.]xyz	Domain	
1drv[.]cyou	Domain	
1drv[.]casa	Domain	Medical Credential Phishing Domain