The Pod People Campaign: Driving User Traffic via Social Networks

podpeople@infimach.com

Executive Summary

Users of social networks are having their accounts subverted. Threat actors are gaining unauthorized access to large numbers of accounts and inserting links to suspicious websites. Shared command-and-control infrastructure is used across 70+ different social networks, suggesting a coordinated campaign to drive user traffic. The actors behind this campaign, and the end goal for driving user traffic, remains uncertain. The campaign remains active with changing indicators. The fact that this campaign spans so many different social networks makes determining the scope of the overall problem difficult. Using Goodreads as an example, we detail how the attack is constructed.

THIS REPORT DOES NOT IDENTIFY VICTIM ACCOUNTS.

Key Findings

- Over 70 social networks are experiencing user account subversion.
- The most likely method for subverting these accounts is credential stuffing.
- User accounts are modified to insert a link that redirects to another site.
- The way the links are presented vary across the affected social networks.
- Some social networks are aware of the problem and are actively remediating it.
- Second party networks that include data from other social networks may be indirectly affected.

Introduction

This report describes a campaign by threat actors, which we are calling “Pod People.” The “Pod People” name is meant to invoke the two *Invasion of the Body Snatchers* science-fiction movies [1] [2] where alien invaders replace human victims with emotionally stunted duplicates.

The purpose of this report is to share cyber threat indicators that document the threat actors’ infrastructure. Along with those indicators, this report also provides analyses on the likely intrusion methods.

The Pod People campaign utilizes social network accounts that once belonged to human users which are turned into empty shells for sharing suspicious URLs. These URLs are meant to passively entice other users and redirect them to a potentially malicious domain. Depending on the social network, there is limited threat actor activity to draw attention to the inserted URLs.

The importance of this report is in sharing indicators and tools, techniques, and procedures (TTP) related to these yet-unknown threat actors. These threat actors have thousands of social media accounts at their command. What this report establishes is that the current utilization of the subverted accounts is focused on driving user traffic to questionable web sites. These accounts could be repurposed at a later date.

Users of the DeviantArt social network assembled a coherent picture of Pod People activity on their site in January of 2019 [3]. The user known as "Colonel-Knight-Rider" correctly outlined a large amount of the Pod People activity. A later response in September of 2020 by user "River-Ratto" corrects the original blog post by suggesting credential stuffing as the attacker vector. Another useful data point from this blog is that threat actor activity was witnessed as early as the fall of 2018.

The way these subverted accounts present themselves differs in degrees. The presentation is consistent within a particular website, but various slightly across different affected sites. On some sites, the suspicious URLs are prepended with "www.". But these are not Latin 'w' characters, they are Cyrillic "we" (U+051C) characters that are visually similar to the Latin 'w'. This appears to be a homoglyph attack [3]. In addition to the homoglyph URLs, some of the affected social networks also have pseudo-gibberish sex appeals as lures alongside the suspicious URL. See Appendix B at the end of this report for a comprehensive comparison of these characteristics.

Account Subversion

How did the threat actors acquire the accounts they are using to spread their URLs? There are four possible scenarios, and the conclusion may involve one or more of them:

1. Data breach – A hack of the target social network resulted in the leak of user login credentials.
2. Created – These are wholly artificial accounts created specifically for this campaign by the threat actor.
3. Sold – A third-party created and curated these accounts before selling them to the threat actors.
4. Credential stuffing – Threat actors assembled a list of user credentials from multiple breaches and gained access to victim accounts where those users reused their passwords [4].

A data breach would be the most direct source of credentials that threat actors could use to subvert accounts. However, this appears inconsistent with the activity we see. Despite widespread victimization of Goodreads user accounts, **there is no evidence that Goodreads has fallen victim to such a data breach**. Infinite Machines team members entered their own email addresses into Have I Been Pwned [5] without finding any hits for Goodreads. Similarly, some Goodreads users embedded their email addresses into their user names. These email addresses also did not generate any hits that would suggest a Goodreads breach. There exist a number of large-scale breaches in the recent past that could provide ammunition to a credential stuffing attack such as the over two billion sets of user credentials released as "Collection #1." [6]

These accounts could be artificially created from scratch. The tools to create personas are freely available, but artificial accounts are often superficial and rarely lack depth and diversity of their attributes and history. What researchers found when examining select victim accounts were users too in-depth, and too diverse to be artifacts. These means that **at least some portion of the accounts being used at one time**

belonged to human users. **It also does not rule out the possibility that some portion of the accounts are artificial**.

Curating social media accounts is not a new phenomenon. Users will spend time creating a “lived in” account with a history and pattern of behavior that makes them seem more trustworthy to other users. These curated accounts are then sold to end users such as viral marketing agencies. Reddit is one such social network to see this pattern of behavior. But this begs the question of the value of a Goodreads account to a second party. **Purchasing curated accounts would be most useful in applications such as trolling and influence peddling**.

The fourth and most likely account subversion scenario is credential stuffing. Credential stuffing attacks succeed based on scale. There are two things required for credential stuffing attacks to succeed. First, users have to reuse their passwords across multiple web sites. Second, enough of these sites have to suffer breaches for threat actors to accumulate enough of a user credential database to find matches. The number of affected accounts found during the course of this investigation is low relative to the overall number of Goodreads users. These numbers are consistent with a small proportion of users having their reused passwords stolen in the breaches of other web sites. Shape Security estimates the success rate of credential stuffing attacks at 0.5% [7], which suggests that the attacker have a user credential database of at least 680,000 entries.

Figure 1 below shows the user profile page of a lived-in account. The evidence suggests that it belonged at one time to a legitimate user. The user has rated several books, has a series of conceptually related bookshelves, and is connected to a large number of friends whose profile summaries suggest additional books and friends. To develop this coherent of a phony user profile would demand an amount of time and resources that is inconsistent with the other levels of effort that the threat actor has demonstrated; a low amount of effort to control a large number of accounts as simply as possible.

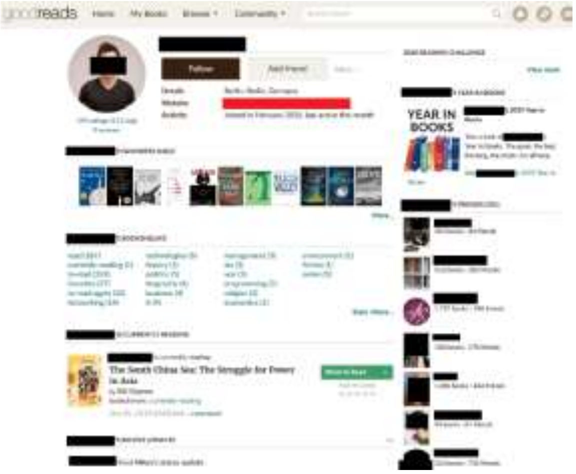
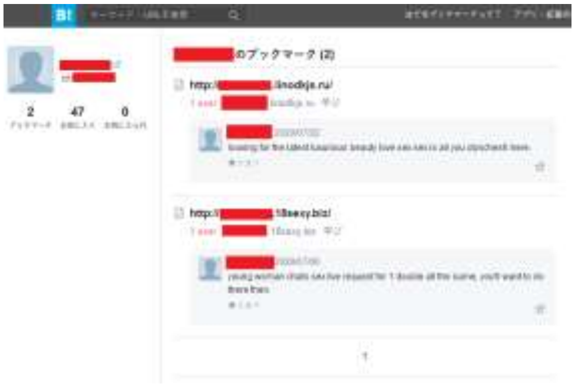


Figure 1: Example of a lived-in account that was subverted by Pod People.

An Active Campaign

The threat actors behind the Pod People campaign are actively making changes to their infrastructure. First, they are changing the redirection URL seen in user profiles. Figure 2 below is a screenshot that illustrates just such an occurrence. The red bars censor the user’s account name. But both the initial `18sexy[.]biz` redirection URL and the later `linodkjs[.]ru` URL use the user’s account name as a subdomain.



[redacted]のブックマーク (2)

[redacted]

2 47 0

http://[redacted].inodkje.ru/

[redacted]

http://[redacted].18sexy.biz/

[redacted]

Figure 2: A subverted account from Hatena where the threat actors returned after two weeks with a new domain.

These suspicious domains date back over ten years in some cases. Figure 3 below plots the number of suspicious domains registered over time. The graph paints a picture of a slow accumulation of domains over time. Then, beginning at the end of 2018, there is a surge in registrations. It is shortly after this time that the Pod People campaign starts to take shape.

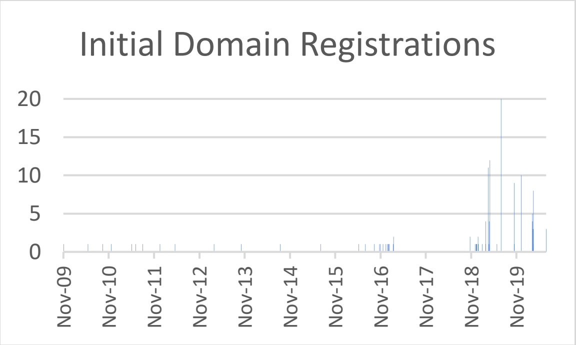


Figure 3: The initial registration dates of the suspicious redirection domain names.

The second type of infrastructure change that the threat actors are making is to the landing page. As of August 13, 2020, the original landing domain of `your-dating-space2[.]com` had its DNS records updated to point it to the loopback IP address, effectively ending its use. The redirector domains now point to a new domain, `adultdating-space[.]com`, which was first seen on August 11, 2020. The new domain hosts the same pornographic/dating web page that the previous domain did. Other landing domains are now seen across the Pod People links (see Appendix A: Landing Domains for a more comprehensive list).

Case Study: Goodreads

Goodreads is a social network targeted at book readers. The site offers features that let users organize, review, and share books. Goodreads is also a subsidiary of Amazon. This investigation began as a result of Goodreads users reporting strange patterns of behavior. When a user performs certain actions such as reviewing a book, or flagging a book to be read in the future, it creates an event that by default is shared with the entire user base. The strange behavior that users report is that other, unfamiliar users “like” the user status updates [8] [9]. Some of the accounts that like stranger’s status updates contain suspicious-looking URLs in the profile.

This behavior of liking statuses of random other users is a way of appearing in front of as many users as possible. Because the bots do not perform activity that normal users do, such as posting reviews, they don’t inadvertently like another bot’s status. However, as we will see next, there is enough bot “liking” activity that multiple bots end up liking the same status update.

The attackers implemented this “liking” campaign using an automated system. Figure 4 plots the status like activity of 42 subverted accounts. These 42 accounts each liked four different status updates, and did so in exactly the same order, exactly two hours apart every time. None of these 42 accounts has liked another status update since July 14, 2020.

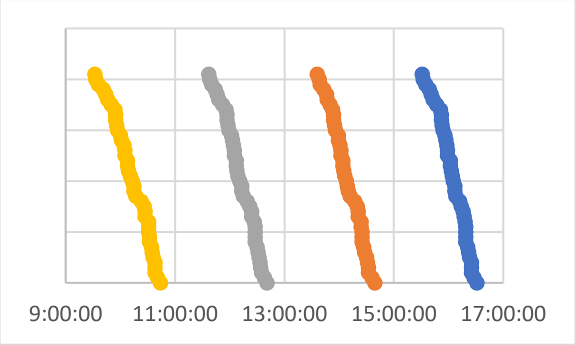


Figure 4: Subverted Goodreads user accounts "liking" status updates on July 14, 2020. (Vertical separation is for visibility purposes only.)

Analysts at Infinite Machines took some of these accounts and automated a web scraper to identify similar accounts. The scraper adopted an iterative approach. Each run of the scraper would start with a set of known suspicious accounts (those with the user ID as the URL subdomain), look at every status update that was liked by at least one other user, and then check those other users for suspicious domains. Figure 5 below shows a network of users and likes collected by the scraper. This network shows three users who are not known to have suspicious URLs, but have liked two different status updates the same way that known subverted accounts have.

Over 3000 suspicious accounts were identified by using the scraper. If the estimates of 90 million active Goodreads users are correct, then these 3000 suspicious accounts form just small proportion of the overall user base. However, these accounts are being actively used to reach out and snare a larger number of active, legitimate users. **The volume of activity is difficult to estimate from externally available information**. Goodreads limits status updates in a user profile to just the four most recent events.

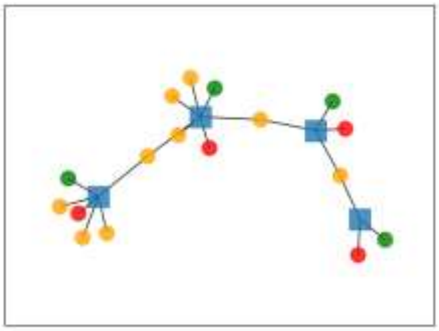


Figure 5: A series of status updates (blue squares) liked by a subverted account (red circle) with the original poster in green and other likers in yellow.

Affected accounts exhibit a very specific pattern. Every Goodreads account has a unique string associated with the user. This string begins with a numerical sequence then an optional sequence of letters and hyphens. With this string, a user can browse to any Goodreads profile page via the URL: `https://www.goodreads.com/user/show/<user_string>` It is important to note that only the numerical prefix is required to resolve a user's profile and the following alphanumeric string derived from the user profile's name is optional. This means that browsing to "`0-snoopy`" would resolve to the same profile as browsing to just "`0`".

Affected accounts also include a URL in the Website line of the user profile (see Figure 7). By default, user profiles do not include a Website URL. What is the reliable indicator is that these suspicious **URLs feature the exact Goodreads user string as a subdomain**. A hypothetical example would be a Goodreads user, "`0-snoopy`", with a Website URL of "`0-snoopy.badsite.xyz`". The threat actors potentially use these Goodreads-generated user strings to avoid namespace collisions when creating the subdomains. Figure 6 below shows the distribution of top-level domains (TLDs) used in these URLs. The Russian `.ru` TLD is the far away leader with `.xyz` in second place, which is a TLD that shows up in F-Secure's reporting on suspect TLDs [11].

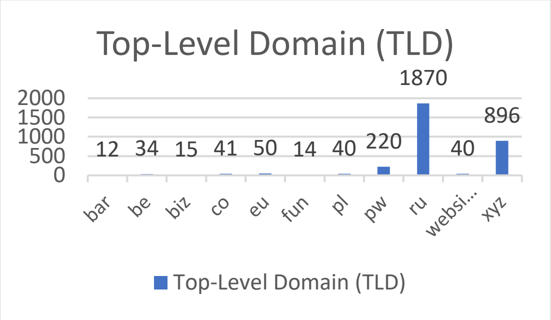
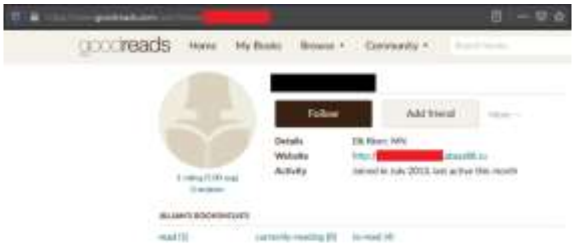


Figure 6: Occurrences of top-level domains in the 3232 suspicious URLs.

Figure 7 below shows one such subverted account. The user's name is censored in black. The red blocks censor the same, Goodreads-generated string, which is used as a subdomain to `ataxa88[.]ru` in this example.



[redacted]

Details Elk River, MN
Website http://[redacted].ataxa88.ru
Activity Joined in July 2013, last active this month

Figure 7: Subverted Goodreads user page.

There are other patterns in the suspicious URLs as well. Several domains begin with the same substring, differing only with a final two-letter sequence where these final two letters appear to be randomly generated. "`cloob`", "`ok`", "`linod`", and "`love`" appear frequently. **Some of these randomized domains may be an attempt to appear superficially similar to the domains of legitimate sites**. For instance, "`okzj[.]ru`" could look the same as "`ok.ru`" to a user who is quickly skimming a text. The website, "`ok.ru`", is the Russian social network, Odnoklassniki (Одноклассники). Figure 8 below is the distribution of domains from the suspicious URLs that Infinite Machines collected from Goodreads profiles. **Over 3000 suspicious accounts used 135 different domains**. The distribution shows what may be two different phases of registering domains for this campaign. Domains beginning with "ok" and "`linod`" appear almost exclusively in the most frequently used (and therefore oldest) domains on the left, and domains that start with "`cloob`" appear on the right after a significant drop in count.

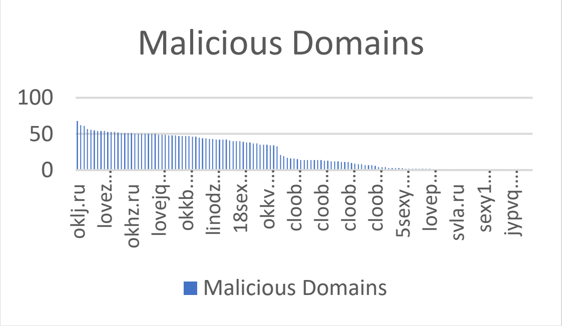


Figure 8: Distribution of domains used in suspicious URLs.

When a user browses to one of the suspicious URLs they received an HTTP 302 response that redirects them to `your-dating-space2[.]com/u=63fkp0n&o=uhcpmz8`. See Figure 9 below for a visual depiction of the sequence of events. Notice the two GET parameters at the end of the redirected URL. Searches for these GET parameters yields previous threat intelligence research [12] [13] dating back to December of 2019 which reference a similar-looking domain, `your-dating-space[.]com` (no "2" in the URL).

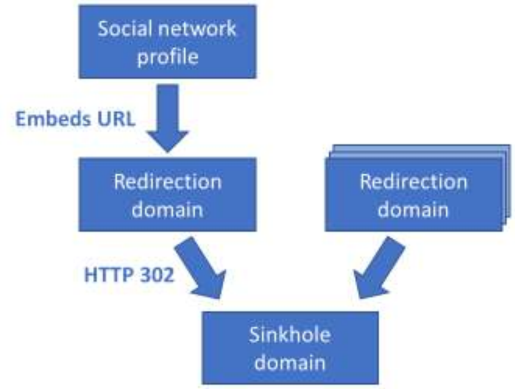


Figure 9: The URL embedded in the user profile redirects to a second website.

Redirection is accomplished using two redundant methods. First, there is JavaScript code that sets the `window.location` to the `your-dating-space2` site. Second, there is a meta refresh in the HTML head section that specifies the exact same URL as the JavaScript code.

The website at the your-dating-space2[.]com domain demonstrates some inconsistencies. The domain name itself suggests a dating website, but the text on the landing page declares that it is *not* a dating site but rather a pornography host. Scantily clad cartoon women adorn this page, as shown below in Figure 10. There are no ads presented either. The page has some internationalization with translated strings for 14 languages stored in a JSON file and selected based on the browser's source IP address.

Figure 10: Screen shot of the sinkhole server's landing page as rendered in German.

An initial HTTP request to the landing server takes over 20 seconds to resolve. Subsequent requests resolve in under 2 seconds. One hypothesis for this behavior is an initial fingerprinting of the user's browser which is cached, causing additional requests to resolve more quickly. This could be consistent with the behavior of an exploit kit. However, **Infinite Machines researchers have yet to definitively observe an exploit attempt or a subsequent malware installation**.

The GET parameters previously mentioned appear significant to the server. Omitting the parameters causes the server to return an empty page with an "Under construction" message. This begs the question: **why are the GET parameters static and universal across the landing URLs**?

Conclusions

A threat actor or group of threat actors controls a large number of user accounts spread across several social networks. To date, they seem content with using the subverted user accounts to drive user traffic to websites of dubious trustworthiness. There is no guarantee that this will remain the case because, as shown earlier in the report, the threat actors are actively involved with changing their infrastructure.

Courses of Action

When discussing the actions of threat actors, it is useful to examine possible future courses of action. There are the most dangerous courses of action; the changes that create the worst possible outcomes for the victims. And there are the most likely courses of action, which contrast with the most dangerous courses of action to provide a more nuanced assessment.

Most Dangerous Course of Action

The most dangerous course of action that the Pod People threat actors could pursue is to weaponize their social network accesses. 2020 is a year of a presidential election in the United States. Already, information operations are attempting to sway the American electorate. It may require a software upgrade on the part of the threat actors, but the victim accounts commandeered in the Pod People campaign provide an avenue for sharing arbitrary posts.

Another weaponization of the Pod People accesses would be to drive traffic to exploit kits. This could be done in conjunction with other weaponization steps such as the disinformation campaign hypothesized above.

Most Likely Course of Action

There is a lack of intelligence currently about the Pod People campaign. As such, the most likely course of action is the null hypothesis; the threat actors will continue to expand their access based on targets of opportunity, and will continue to use their accesses to drive user traffic.

Unanswered Questions

- Why the limited bot behavior (only liking)?
- Is there an exploit kit at the landing web page?
- Is this prepositioning of assets within social networks for later activation?
- Why are some subdomains that map to existing Goodreads user accounts not being actively used?
- Are some of the accounts that like the same posts as the bots also subverted, but without the telltale suspicious URL?
- Why are the threat actors exhibiting inconsistent levels of operational security?

Recommendations

There are several actions that can be taken by both social networks and users in order to stem these kinds of attacks.

User Recommendations

- Don’t reuse passwords across multiple websites. Reuse enables credential stuffing attacks.
- Use a password manager to create and store strong passwords.
- Report suspicious behavior to the social network.
- Minimize the amount of personal information shared on social networks.
- Use social network access controls to limit who has access to your user profile.

Social Network Recommendations

- Perform a mandatory password reset for all affected accounts.
- Require email account validation as a step for creating a user account.
- Use a CAPTCHA to prevent automated account creation.
- Consider the use of multi-factor authentication.
- Accounts should be deactivated or deleted after a period of inactivity.
- Don’t render URLs in user-provided fields as anchor tags that are clickable in a web browser.

Credits

Author: Courtney Falk

Special thanks to Josiah Dykstra and Aamil Karimi for their proofreading work and valuable feedback.

Thanks also goes to Selenium (selenium.dev), RiskIQ (riskiq.com), and ANY.RUN (any.run) for making their tools available to the community.

Appendix A: Indicators

These indicator lists should be treated as incomplete. For the most up-to-date and comprehensive list of indicators, refer to this report's GitHub page at: https://github.com/podpeople/podpeople

Redirector Domains

12sexy[.]ru
18sexy[.]be
18sexy[.]biz
18sexy[.]co
18sexy[.]eu
18sexy[.]pl
18sexy[.]pw
18sexy[.]website
18sexy[.]xyz
19sexy[.]pw
1sexy[.]ru
20sexy[.]pw
21sexy[.]pw
3sexy[.]ru
5sexy[.]ru
6sexy[.]ru
aajgo[.]ru
ataxa88[.]ru
cloobagfod[.]ru
cloobczcp[.]ru
cloobdewjtxzr[.]ru
cloobdkpb[.]ru
cloobejobeuya[.]ru
cloobjs[.]ru
cloobodqxb[.]ru
cloobolosbrqb[.]ru
cloobpkgb[.]ru
cloobpon[.]ru
cloobrbn[.]ru
cloobrgbul[.]ru
cloobrsrdv[.]ru
cloobrwt[.]ru
cloobtareje[.]ru
cloobvklxw[.]ru
cloobxb[.]ru
cloobxk[.]ru
cloobxx[.]pw
cloobxxx[.]bar
cloobxxx[.]fun
cloobxxx[.]pw
cloobxxx[.]ru
cloobxxx[.]website
cloobxxx[.]xyz
cloobykwlthh[.]ru
cloobzfye[.]ru
csvut[.]ru
ctze[.]ru
cwaz[.]ru
czdbs[.]ru
dcue[.]ru
ddab[.]ru
djwr[.]ru
eeyp[.]ru
ewfjt[.]ru
jver[.]ru
jypvq[.]ru
linodix[.]ru
linodkjs[.]ru
linodnk[.]ru
linodps[.]ru
linodrvs[.]ru
linoduba[.]ru
linodwi[.]ru
linodxz[.]ru
linodyq[.]ru
linodzn[.]ru
loveal[.]ru
lovefc[.]ru
lovejj[.]ru
lovejq[.]ru
lovekc[.]ru
lovemyrlove[.]ru
loveor[.]ru
lovepatifac[.]ru
loveqn[.]ru
loveret[.]ru
lovestes[.]ru
lovevv[.]ru
lovewc[.]ru
lovezg[.]ru
lovorutootoo[.]ru
lyow[.]ru
nakgz[.]ru
nvyk[.]ru
ocxcs[.]ru
oegr[.]ru
oesb[.]pw
okao[.]xyz
okbl[.]xyz
okcs[.]ru
okcx[.]ru
okdr[.]xyz
okec[.]xyz
okgr[.]xyz
okgx[.]xyz
okhu[.]xyz
okhz[.]ru
okje[.]xyz
okkb[.]xyz
okkc[.]xyz
okkf[.]ru
okkh[.]xyz
okkl[.]ru
okkv[.]xyz
okkw[.]xyz
oklj[.]ru
okln[.]xyz
okoe[.]xyz
okpg[.]xyz
okwb[.]ru
okwh[.]xyz
okxp[.]ru
okyx[.]xyz
okzj[.]ru
okzu[.]xyz
okzv[.]ru
okzx[.]xyz
qwhkl[.]ru
rrdtj[.]ru
sexy13[.]ru
sexy17[.]ru
sexy22[.]ru
sexy6[.]ru
sexy7[.]ru
svla[.]ru
tudjt[.]ru
tujej[.]ru
tyyx[.]ru
ulsiv[.]ru
wilu[.]ru
wlwrb[.]ru
xvwqg[.]ru
xwxl[.]ru
xxld[.]ru
ycwr[.]ru

Redirector IP Addresses

These are the IP addresses that the suspicious domains currently resolve to. It is not a comprehensive list of all the IP addresses that the suspicious domains have ever resolved to. It is also possible that there are unrelated domains that resolve to the same addresses.

185[.]189[.]13[.]16
194[.]58[.]56[.]100
194[.]58[.]56[.]112
194[.]58[.]56[.]113
194[.]58[.]56[.]117
194[.]58[.]56[.]119
194[.]58[.]56[.]120
194[.]58[.]56[.]121
194[.]58[.]56[.]131
194[.]58[.]56[.]133
194[.]58[.]56[.]134
194[.]58[.]56[.]135
194[.]58[.]56[.]142
194[.]58[.]56[.]146
194[.]58[.]56[.]190
194[.]58[.]56[.]198
194[.]58[.]56[.]217
194[.]58[.]56[.]218
194[.]58[.]56[.]228
194[.]58[.]56[.]229
194[.]58[.]56[.]233
194[.]58[.]56[.]234
194[.]58[.]56[.]235
194[.]58[.]56[.]238
194[.]58[.]56[.]244
194[.]58[.]56[.]251
194[.]58[.]56[.]26
194[.]58[.]56[.]33
194[.]58[.]56[.]34
194[.]58[.]56[.]36
194[.]58[.]56[.]43
194[.]58[.]56[.]52
194[.]67[.]71[.]110
194[.]67[.]71[.]145
194[.]67[.]71[.]150
194[.]67[.]71[.]157
194[.]67[.]71[.]161
194[.]67[.]71[.]165
194[.]67[.]71[.]170
194[.]67[.]71[.]195
194[.]67[.]71[.]23
194[.]67[.]71[.]26
194[.]67[.]71[.]39
194[.]67[.]71[.]42
194[.]67[.]71[.]43
194[.]67[.]71[.]50
194[.]67[.]71[.]6
194[.]67[.]71[.]70
194[.]67[.]71[.]71
194[.]67[.]71[.]85
194[.]67[.]71[.]93
194[.]67[.]71[.]95
31[.]31[.]205[.]163
46[.]17[.]107[.]154

Redirector Page Hashes

your-dating-space2[.]com:

MD5:	5A678E64F21D0573AC17BE01535C0A96
SHA1:	AC9F2BE0512613B65252C1B3615CD86E3B8A1CF3
SHA256:	734474393570D91F6B3DA9C49770493842D7D53CFE8F989AA61BF45FEBE91FDF

adultdating-space[.]com:

MD5:	137D721B060288923A9B7BBFA282AFFD
SHA1:	83573C99DF9A024C0A2AF1952B5D103C0D159A74
SHA256:	1EBFDDCE61CE7EB84FE942A214C98BC0FF89F0ED68F08D2CFB73BA16C10A2A70

Landing Domains

aditms[.]me
adultdating-space[.]com
bongacams[.]com
e-active[.]ru
eatcells[.]com
expialidosius[.]com
findher2date[.]com
go-2-date[.]us
onclickmega[.]com
stripchat[.]com
takespecial-prizenow2[.]life
the-best-bonus-here[.]life
tosuicunea[.]com
your-dating-space2[.]com

Appendix B: Affected Social Networks

This table is the result of attempting to grasp the breadth of the Pod People problem. Each suspicious domain was run through the DuckDuckGo search engine. In cases where three or more matching domains were found, that social network was documented. This is not a scientific approach for two reasons. First, the DuckDuckGo search results were cached. Not all affected accounts were cached in the first place so the results are not exhaustive. Second, some of the social networks have proactively taken measures to remediate the links that the Pod People inserted.

Some of the table fields warrant an explanation:

- **Lang** – The ISO 639-3 language code for the default/dominant language on that particular network.
- **Field(s)** – The one or more fields in which the suspicious links were inserted.
- **Text** – Whether or not the suspicious link was accompanied by some kind of text lure.
- **Punycode** – Whether or not the suspicious link uses a homoglyph attack [3].

Network	Genre	URL	Lang	Field(s)	Text	Punycode
2gis	Mapping	2gis.ru	rus	Name	FALSE	TRUE
500px	Photos	500px.com	eng	Profile	TRUE	TRUE
8tracks	Music	8tracks.com	eng	Website	TRUE	FALSE
Academia	Research	academia.edu	eng	Profile	TRUE	TRUE
Advisor.Travel	Travel	advisor.travel	eng	Name	FALSE	TRUE
Airtripp	Travel	airtripp.com	eng	Name	FALSE	TRUE
Ameba	Blog	ameba.jp	jpn	Profile	TRUE	TRUE
Amino	Community	aminoapps.com	eng	Post	TRUE	TRUE
BDFF	Dating	blackdatingforfree.com	eng	Profile,Website	FALSE	TRUE
Blogg.se	Blog	blogg.se	swe	Post	TRUE	TRUE
Bored Panda	News	boredpanda.com	eng	Profile	TRUE	TRUE
Carousell	Store	carousell.com	eng	Profile	FALSE	TRUE
Cloob	General	cloob.com	fas	Post	TRUE	FALSE
ComicNewbies	Comicbooks	comicnewbies.com	eng	Name	TRUE	FALSE
Coub	Video	coub.com	eng	Website	FALSE	FALSE
Couchsurfing	Travel	couchsurfing.com	eng	About	TRUE	TRUE

CROSS.TV	Religious	cross.tv	eng	Profile	FALSE	FALSE
Crunchyroll	Anime	crunchyroll.com	eng	Sig Block	TRUE	TRUE
Dark Moe (暗萌)	Anime	dmoe.org	cmn	Name	FALSE	TRUE
Delectable	Wine	delectable.com	eng	Post	TRUE	TRUE
DeviantArt	Art	deviantart.com	eng	Website,Bio	FALSE	TRUE
Disqus	Comment Hosting	disqus.com	eng	Website	FALSE	FALSE
Dribbble	Work for Hire	dribbble.com	eng	Website	FALSE	FALSE
Drive2	Cars	drive2.ru	rus	Profile	FALSE	FALSE
Dukascopy	Bank	dukascopy.com	eng	Name	FALSE	TRUE
Duolingo	Language Learning	duolingo.com	eng	Name	TRUE	TRUE
Ello	General	ello.co	eng	Website,Profile	TRUE	TRUE
Facebook	General	facebook.com	eng	Website	FALSE	FALSE
Filmow	Movies	filmow.com	por	Post	FALSE	FALSE
Fishki	General	fishki.net	rus	Post	TRUE	TRUE
Flamp	Review	flamp.ru	rus	User	FALSE	TRUE
Flipboard	News	flipboard.com	eng	Profile	FALSE	TRUE
Foursquare	Review	foursquare.com	eng	Name	FALSE	TRUE
Goodreads	Books	goodreads.com	eng	Website	FALSE	FALSE
Gravatar	Avatars	gravatar.com	eng	Profile	FALSE	TRUE
Hatena	Bookmarking	hatena.ne.jp	jpn	Post	TRUE	FALSE
Houzz	Design	houzz.co.uk	eng	Ideabook	TRUE	TRUE
imgur	Photos	imgur.com	eng	Post	TRUE	TRUE
Instagram	Photos	instagram.com	eng	Website	FALSE	FALSE
JDN	News	journaldunet.com	fra	Profile	FALSE	TRUE
Jugl.net	Streaming	jugl.net	eng	About	FALSE	TRUE
KickStarter	Crowdfunding	kickstarter.com	eng	Name	FALSE	TRUE
last.fm	Music	last.fm	eng	About	FALSE	TRUE
LiveInternet	Blog	liveinternet.ru	rus	Post	TRUE	TRUE
Lovelama	Dating	lovelama.ru	rus	Profile	FALSE	TRUE

LovePlanet	Dating	loveplanet.ru	rus	About	FALSE	TRUE
Luulla	Shopping	luulla.com	eng	Name	FALSE	TRUE
Mail.ru	General	mail.ru	rus	Name,Post	FALSE	FALSE
Mastodon	School	mastodon.social	eng	Website	FALSE	FALSE
Meeting.lv	Tourism	meeting.lv	rus	Profile	TRUE	TRUE
Menéame	News	meneaame.net	spa	Profile	FALSE	TRUE
Mi Community	Technology	c.mi.com	cmn	Interests	FALSE	TRUE
Minds	General	minds.com	eng	Website	FALSE	FALSE
Mosaic Tiles	Shopping	mosaictilesonline.com	eng	Profile,Post	TRUE	FALSE
MUBI	Video	mubi.com	eng	Profile	FALSE	TRUE
MySpace	General	myspace.com	eng	Profile	TRUE	FALSE
N4G	Video Games	n4g.com	eng	PM	TRUE	TRUE
NK	Alumni	nk.pl	pol	Name	FALSE	TRUE
Odnoklassniki	Alumni	ok.ru	rus	Status	FALSE	TRUE
Photobucket	Photos	photobucket.com	eng	Profile	TRUE	TRUE
PicsArt	Art	picsart.com	eng	Name	FALSE	TRUE
Pinterest	Photos	pinterest.com	eng	Website	FALSE	FALSE
Plurk	Blog	plurk.com	eng	Website	FALSE	TRUE
Rediff	General	rediff.com	eng	Company	FALSE	TRUE
Skyrock	Blog	skyrock.com	eng	Profile,Post	FALSE	TRUE
SlideServe	Document Sharing	slideserve.com	eng	Website	FALSE	FALSE
StyleShare	Fashion	styleshare.kr	kor	Profile	FALSE	TRUE
Topface	Dating	topface.com	kor	Profile	TRUE	TRUE
tumblr	Blog	tumblr.com	eng	Post	TRUE	FALSE
Twitter	Blog	twitter.com	eng	Website	FALSE	FALSE
Typepad	Blog	typepad.com	eng	Website	FALSE	FALSE
Unsplash	Photos	unsplash.com	eng	Website,Profile	TRUE	TRUE

References

[1] D. Siegel, Director, *Invasion of the Body Snatchers.* [Film]. USA: Walter Wanger Productions, 1956.

[2] P. Kaufman, Director, *Invasion of the Body Snatchers.* [Film]. USA: Solofilm, 1978.

[3] Colonel-Knight-Rider, "URGENT: Invasion of the Old Account Hijackers," DeviantArt, 9 January 2019. [Online]. Available: https://www.deviantart.com/colonel-knight-rider/journal/URGENT-Invasion-of-the-Old-Account-Hijackers-780368793. [Accessed 24 October 2020].

[4] Wildfire Labs, "What you see is not what you get: when homographs attack," 1 April 2019. [Online]. Available: https://blog.blazeinfosec.com/what-you-see-is-not-what-you-get-when-homographs-attack/. [Accessed 18 August 2020].

[5] M. Coates, "How Third Party Password Breaches Put Your Website at Risk," 18 November 2013. [Online]. Available: https://michael-coates.blogspot.com/2013/11/how-third-party-password-breaches-put.html. [Accessed 2 August 2020].

[6] T. Hunt, "Have I Been Pwned," [Online]. Available: https://haveibeenpwned.com/. [Accessed 2 August 2020].

[7] T. Hunt, "The 773 Million Record "Collection #1" Data Breach," 17 January 2019. [Online]. Available: https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/. [Accessed 18 August 2020].

[8] Shape Security, "2018 Credential Spill Report," 2018. [Online]. Available: http://info.shapesecurity.com/rs/935-ZAM-778/images/Shape_Credential_Spill_Report_2018.pdf. [Accessed 1 August 2020].

[9] markovian-parallax, "Goodreads filling up with bot accounts?," 29 December 2019. [Online]. Available: https://www.reddit.com/r/goodreads/comments/eh77w1/site_issues_goodreads_filling_up_with_bot_accounts/. [Accessed 28 July 2020].

[10] LunaTherapy, "Weird random likes on Goodreads?," 10 October 2019. [Online]. Available: https://www.reddit.com/r/goodreads/comments/dg70qi/weird_random_likes_on_goodreads/. [Accessed 28 July 2019].

[11] S. Proske, "Why is there's so much spam coming from .xyz and other new top-level domains?," 5 June 2019. [Online]. Available: https://blog.f-secure.com/why-is-theres-so-much-spam-coming-from-xyz-and-other-new-top-level-domains/. [Accessed 27 July 2020].

[12] urlscan.io, "x3x3x.lovepatifac.ru," 15 December 2019. [Online]. Available: https://urlscan.io/result/f23f1445-bcf3-4453-9b2a-8bb4ed358277. [Accessed 2 August 2020].

[13] Joe Security, "Automated Malware Analysis Report for http://www.Bhsala.cloobxxx.ru," 24 July 2020. [Online]. Available: https://www.joesandbox.com/analysis/250879/0/html. [Accessed 2 August 2020].

Change Log

Version	Date	Changes
1.0.0	2020-08-28	• Initial release.
1.1.0	2020-10-24	• Included a contact email address. • Inserted a useful citation to a DeviantArt blog post. • Added 27 redirector domains. • Added 8 affected sites.