An Investigative Analysis of the Silent Librarian IoCs

By **Jonathan Zhang** Founder and CEO of WhoisXMLAPI & ThreatIntelligencePlatform.com

- November 13, 2020
- Views: 8,851
- Add Comment

The Silent Librarian advanced persistent threat (APT) actors have been detected once again, as the academic year started in September. With online classes increasingly becoming the norm, the group's phishing campaigns that aim to steal research data and intellectual property could have a high success rate.

Dozens of phishing domain names have been reported, although some may have already been taken down. Still, the Silent Librarian APT group could have more weaponized domains in their arsenal, so we tried to uncover some connections throughout this investigative analysis using domain and IP intelligence.

The IoCs: Commonalities and Characteristics

Malwarebytes has identified 25 phishing subdomains and three IP addresses that targeted 21 universities and colleges worldwide.

IP Geolocation

Using IP geolocation, we identified that two malicious IP addresses were assigned to Iran, and another one to India.

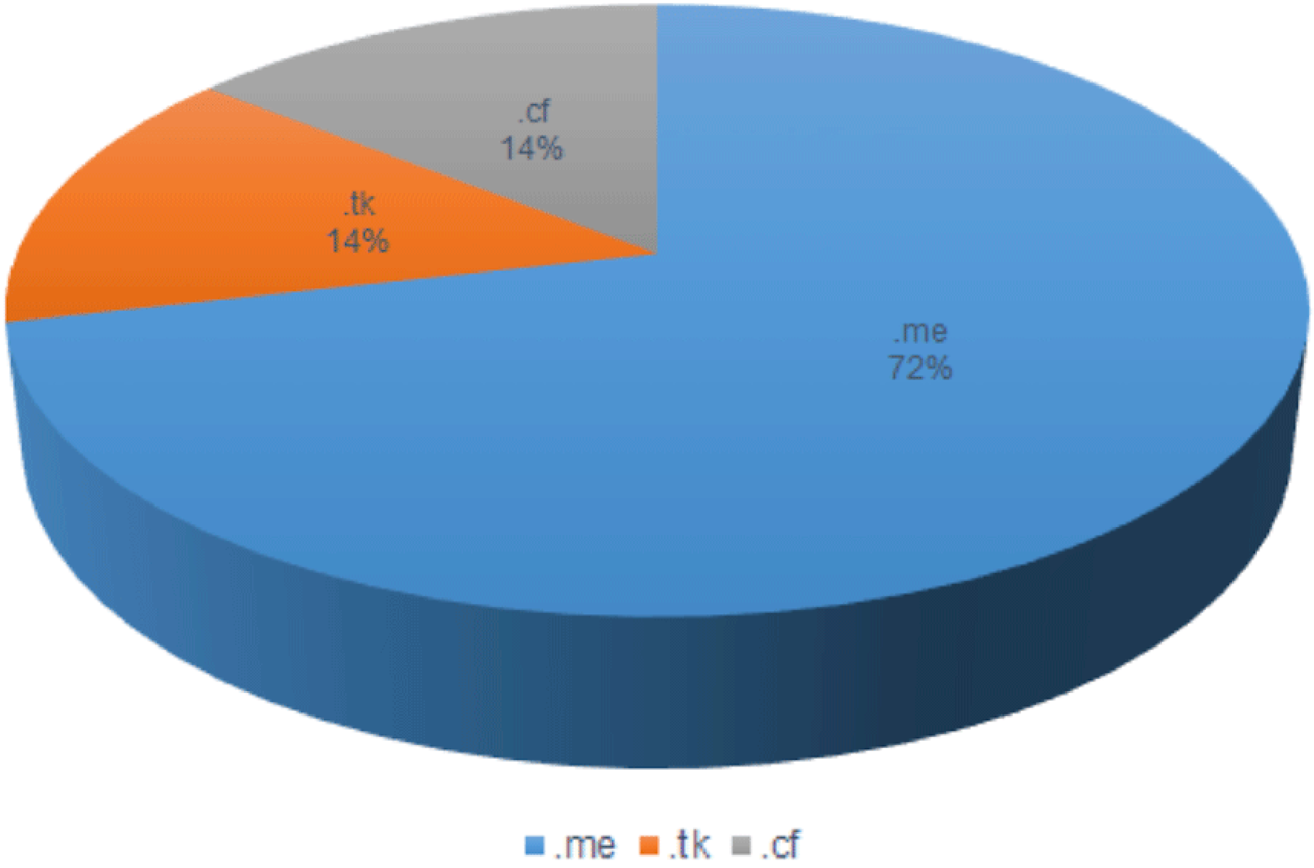
The Use of Subdomains

The phishing subdomains used the same strings found in the universities' legitimate domains but at the third-level domain under a different root domain. The phishing domain library[.]adelaide[.]crev[.]me, for example, looks much like the University of Adelaide Library's legitimate domain library[.]adelaide[.]edu[.]au.

Instances when the threat actors used the full legitimate domain, such as idpz[.]utorauth[.]utoronto[.]ca[.]itlf[.]cf, which targets the University of Toronto (legitimate domain: idpz[.]utorauth[.]utoronto[.]ca), were also found.

TLD and Registrar Distribution of Root Domains

Out of the 25 phishing subdomains, 14 root domains were identified. Ten of them are in the .me generic top-level domain (gTLD) space, two used .tk, while another two used .cf.



TLD Distribution of Phishing Root Domains (%)

WHOIS data showed that as of 5 November 2020, the two .cf domains (itlf[.]cf and sftt[.]cf) have already been dropped. All of the other domains remain active and have the following details:

- Their registrar is NameCheap, Inc.
- The .me domains use WhoisGuard, Inc. protection, while the .tk domains use Freedom Registry, Inc.
- The registrant countries reflect that of the domains' privacy protection services—Panama for WhoisGuard and the U.S. for Freedom Registry.

- All of the domains were recently registered with dates within 14 August and 2 October.

Uncovering More Digital Footprints

Noting the number of times the root domains were used as Silent Library indicators of compromise (IoCs), we discovered many possibly suspicious subdomains. The numbers are reflected in the table below.

Root Domain	Number of Times Used as a Silent Library IoC	Number of Subdomains Found through Subdomains Lookup
itlf[.]cf	2	17
itlt[.]tk	1	13
itlib[.]me	5	8
iftl[.]tk	5	8
aroe[.]me	1	4
crir[.]me	1	4
canm[.]me	1	3
crev[.]me	2	3
rres[.]me	1	3
cvrr[.]me	1	2
ernn[.]me	1	2
nrni[.]me	1	2
sftt[.]cf	2	2
ninu[.]me	1	1

We focused on investigating the second to fourth root domains in the list above:

- itlt[.]tk
- itlib[.]me
- iftl[.]tk

These domains had way more subdomains that were not used as IoCs. The first on the list, itlf[.]cf, is no longer active.

Looking up subdomain and DNS data, we found 11 more subdomains that could be used to target universities, along with two IP addresses. The chart below shows the subdomains of the three root domains. The subdomains in red have already been reported as Silent Library IoCs, while the rest could still figure in future attacks.

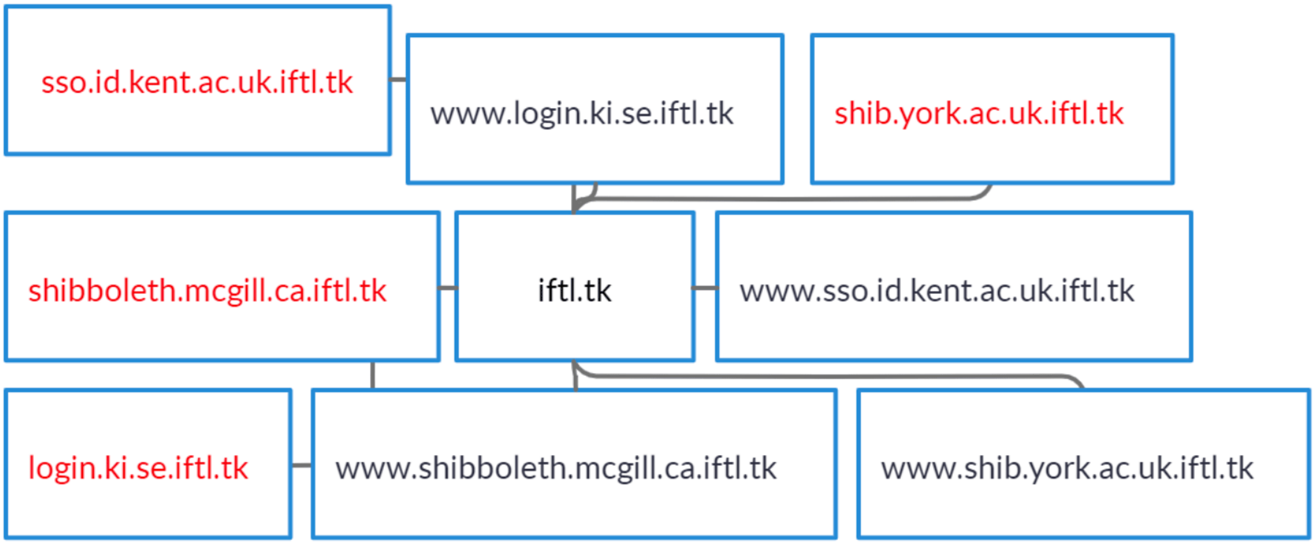

sso.id.kent.ac.uk.iftl.tk
www.login.ki.se.iftl.tk
shib.york.ac.uk.iftl.tk
shibboleth.mcgill.ca.iftl.tk
iftl.tk
www.sso.id.kent.ac.uk.iftl.tk
login.ki.se.iftl.tk
www.shibboleth.mcgill.ca.iftl.tk
www.shib.york.ac.uk.iftl.tk

Chart 1: Root domain “iftl[.]tk”

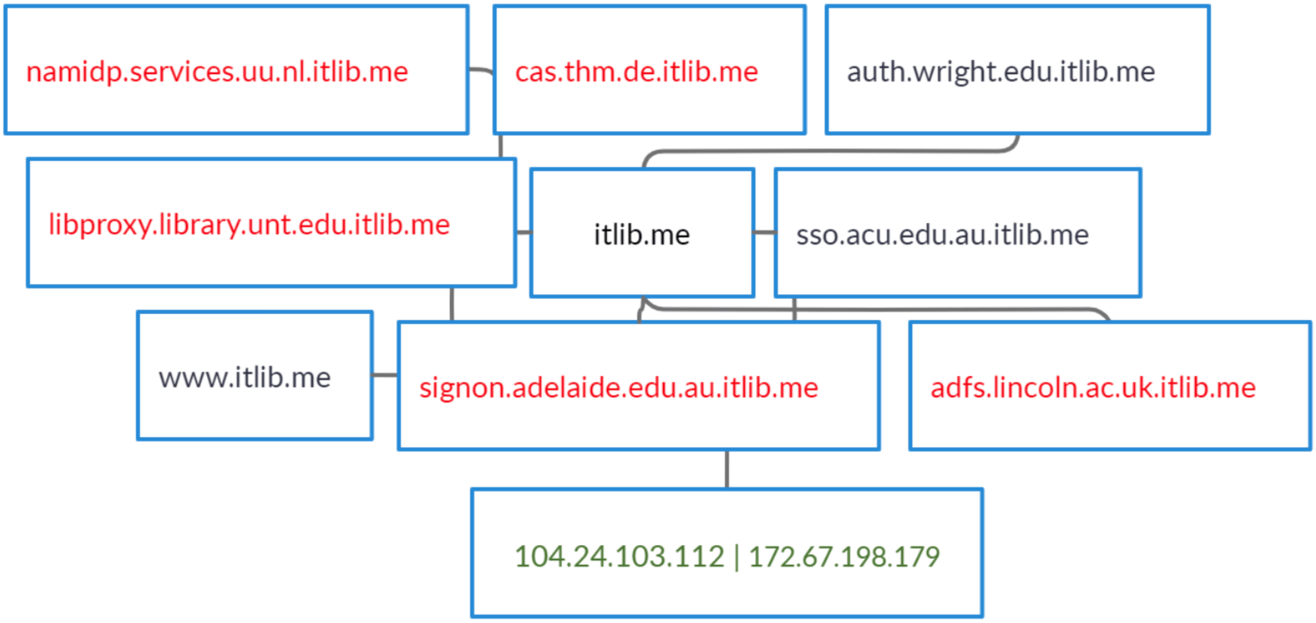

namidp.services.uu.nl.itlib.me
cas.thm.de.itlib.me
auth.wright.edu.itlib.me
libproxy.library.unt.edu.itlib.me
itlib.me
sso.acu.edu.au.itlib.me
www.itlib.me
signon.adelaide.edu.au.itlib.me
adfs.lincoln.ac.uk.itlib.me
104.24.103.112 | 172.67.198.179

Chart 2: Root domain “itlib[.]me”

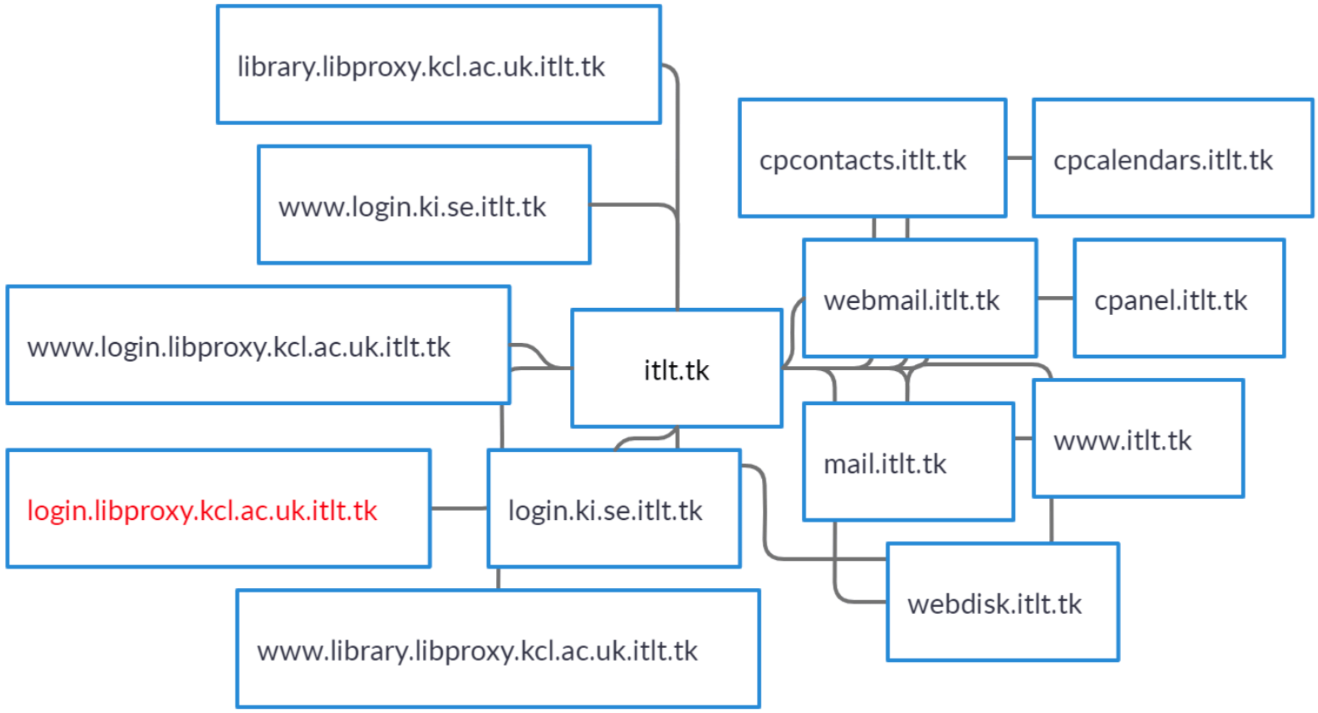


Chart 3: Root domain “itit[.]tk”

The table below lists the potential subdomains that may be used to target the corresponding academic institutions in the future. Some may currently be undetected.

Possible Phishing Subdomains	Target
library[.]libproxy[.]kcl[.]ac[.]uk[.]itlt[.]tk	King’s College London
www[.]login[.]libproxy[.]kcl[.]ac[.]uk[.]itlt[.]tk	King’s College London
www[.]library[.]libproxy[.]kcl[.]ac[.]uk[.]itlt[.]tk	King’s College London
www[.]login.ki[.]se[.]itlt[.]tk	Karolinska Institutet
login[.]ki[.]se[.]itlt[.]tk	Karolinska Institutet
www[.]login[.]ki[.]se[.]iftl[.]tk	Karolinska Institutet
www.sso[.]id[.]kent[.]ac[.]uk[.]iftl[.]tk	University of Kent
www[.]shibboleth[.]mcgill[.]ca[.]iftl[.]tk	McGill University
www[.]shib[.]york[.]ac[.]uk[.]iftl[.]tk	University of York
auth[.]wright[.]edu[.]itlib[.]me	Wright State University
sso[.]acu[.]edu[.]au[.]itlib[.]me	Australian Catholic University

Some of the Silent Library APT members have already been indicted in 2018, yet what remains of the group seem to continue targeting different universities across several continents. Constant investigation and monitoring are required to keep up.

By **Jonathan Zhang, Founder and CEO of WhoisXMLAPI & ThreatIntelligencePlatform.com**

Filed Under

- Brand Protection
- Cybercrime
- Cybersecurity
- DNS
- Domain Management
- Domain Names
- Threat Intelligence
- Whois

Comments

Comment Title:

Notify me of follow-up comments

Related

These DeFi Domains Might Be Risky to Investors

- WhoisXML API

- May 27, 2022 11:18 AM PDT
- Views: 1,267

Branded Domains Are the Focal Point of Many Phishing Attacks

- David Barnett
- May 26, 2022 8:40 PM PDT
- Views: 1,196

Website Defacement: Age-Old but Still Works as Ongoing Campaigns Show

- WhoisXML API
- May 24, 2022 12:07 PM PDT
- Views: 3,280

Don’t Hit That Update Button Just Yet, It Could Lead to Malware Infection

- Threat Intelligence Platform (TIP)
- May 23, 2022 3:23 PM PDT
- Views: 4,066

Webcast May 23: Finnish Internet Forum – ‘Internet and War’ Panel

- Joly MacFie
- May 21, 2022 10:52 AM PDT
- Views: 3,928

NIS2: A New Cyber Jurisdiction Paradigm

- Anthony Rutkowski
- May 19, 2022 2:22 PM PDT
- Views: 8,875

Behind the Bylines of Fake News and Disinformation Pages

- WhoisXML API
- May 18, 2022 3:15 PM PDT
- Views: 5,309

Threat Actors Might Be Interested in Elon Musk’s Twitter Purchase, Too

- WhoisXML API
- May 16, 2022 2:24 PM PDT
- Views: 6,037

Securing Weak Links in Supply Chain Attacks

- Vic DeBari
- May 13, 2022 11:16 AM PDT
- Views: 7,797

Monumental Cybersecurity Blunders

- Anthony Rutkowski
- May 13, 2022 10:42 AM PDT
- Views: 7,877

More