Silent Librarian APT right on schedule for 20/21 academic year

blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack

Threat Intelligence Team October 14, 2020

A threat actor known as Silent Librarian/TA407/COBALT DICKENS has been actively targeting universities via spear phishing campaigns since schools and universities went back.

In mid-September, we were tipped off by one of our customers about a new active campaign from this APT group. Based off a number of intended victims, we can tell that Silent Librarian does not limit itself to specific countries but tries to get wider coverage.

Even though many phishing sites have been identified and taken down, the threat actor has built enough of them to continue with a successful campaign against staff and students alike.

A persistent threat actor with a perfect attendance record

In March 2018, nine Iranians were indicted by the US Department of Justice for conducting attacks against universities and other organizations with the goal of stealing research and proprietary data.

Yet, both in August 2018 and 2019 Silent Librarian was lining up for the new academic years, once again targeting the same kind of victims in over a dozen countries.

IT administrators working at universities have a particularly tough job considering that their customers, namely students and teachers, are among the most difficult to protect due to their behaviors. Despite that, they also contribute to and access research that could be worth millions or billions of dollars.

Considering that Iran is dealing with constant sanctions, it strives to keep up with world developments in various fields, including that of technology. As such, these attacks represent a national interest and are well funded.

Same pattern in phishing domain registration

The new domain names follow the same pattern as previously reported, except that they swap the top level domain name for another. We know that the threat actor has used the ".me" TLD in their past campaigns against some academic intuitions and this is still the case, along side ".tk" and ".cf".

This new phishing campaign has been tracked by several security researchers on Twitter, notably Peter Kruse from the CSIS Security Group.

Phishing site	Legitimate site	Target
library.adelaide.crev.me	library.adelaide.edu.au	The University of Adelaide Library
signon.adelaide.edu.au.itlib.me	library.adelaide.edu.au	The University of Adelaide Library
blackboard.gcal.crev.me	blackboard.gcal.ac.uk	Glasgow Caledonian University
blackboard.stonybrook.ernn.me	blackboard.stonybrook.edu	Stony Brook University
blackboard.stonybrook.nrni.me	blackboard.stonybrook.edu	Stony Brook University
namidp.services.uu.nl.itlib.me	namidp.services.uu.nl	Universiteit Utrecht
uu.blackboard.rres.me	uu.blackboard.com	Universiteit Utrecht
librarysso.vu.cvrr.me	librarysso.vu.edu.au	Victoria University
ole.bris.crir.me	ole.bris.ac.uk	University of Bristol
idpz.utorauth.utoronto.ca.itlf.cf	idpz.utorauth.utoronto.ca	University of Toronto
raven.cam.ac.uk.iftl.tk	raven.cam.ac.uk	University of Cambridge
login.ki.se.iftl.tk	login.ki.se	Karolinska Medical Institutet
shib.york.ac.uk.iftl.tk	shib.york.ac.uk	University of York
sso.id.kent.ac.uk.iftl.tk	sso.id.kent.ac.uk	University of Kent
idp3.it.gu.se.itlf.cf	idp3.it.gu.se	Göteborg universitet
login.proxy1.lib.uwo.ca.sftt.cf	login.proxy1.lib.uwo.ca	Western University Canada
login.libproxy.kcl.ac.uk.itlt.tk	kcl.ac.uk	King’s College London
idcheck2.qmul.ac.uk.sftt.cf	qmul.ac.uk	Queen Mary University of London
lms.latrobe.aroe.me	lms.latrobe.edu.au	Melbourne Victoria Australia
ntulearn.ntu.ninu.me	ntulearn.ntu.edu.sg	Nanyang Technological University

adfs.lincoln.ac.uk.itlib.me	adfs.lincoln.ac.uk	University of Lincoln
cas.thm.de.itlib.me	cas.thm.de	TH Mittelhessen University of Applied Sciences
libproxy.library.unt.edu.itlib.me	library.unt.edu	University of North Texas
shibboleth.mcgill.ca.iftl.tk	shibboleth.mcgill.ca	McGill University
vle.cam.ac.uk.canm.me	vle.cam.ac.uk	University of Cambridge

Table 1: List of phishing sites and targets

Registering these subdomains to perform phishing attacks against universities is a known behavior for this APT group and therefore we can expect that they were registered by the same actor.

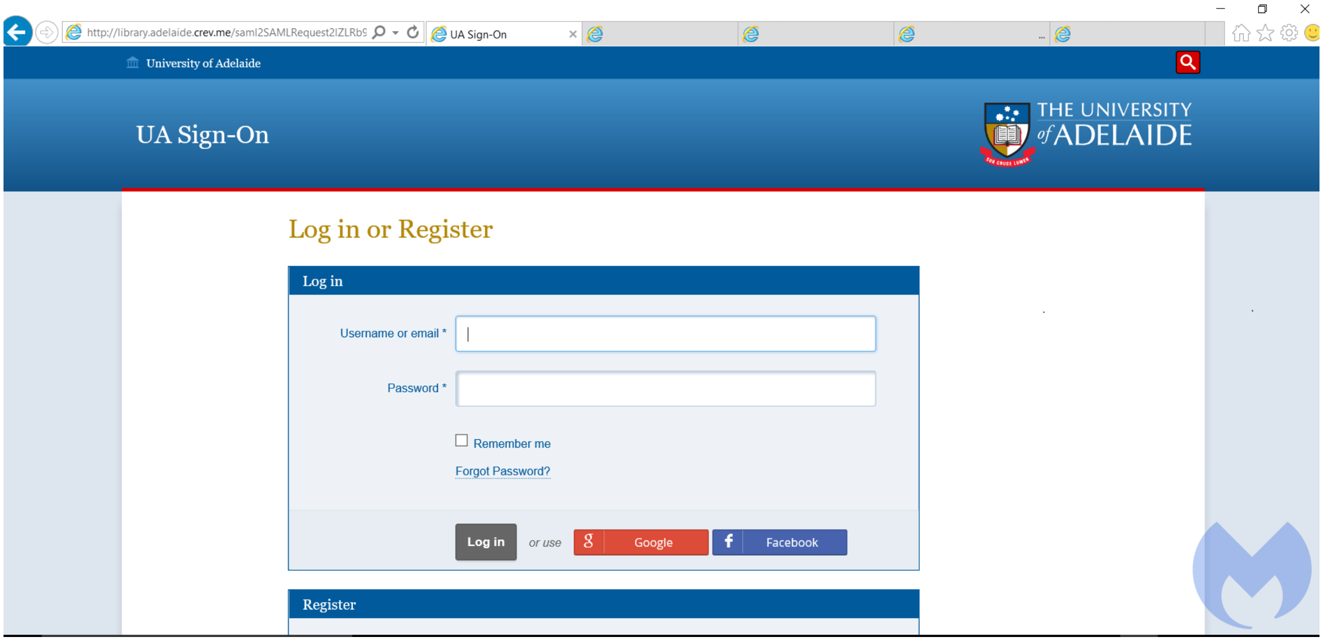
http://library.adelaide.crev.me/saml2SAMLRequest2lZLRb9

Figure 1: Phishing site for the University of Adelaide

Phishing sites hosted in Iran

The threat actor uses Cloudflare for most of their phishing hostnames in order to hide the real hosting origin. However, with some external help we were able to identify some of their infrastructure located on Iran-based hosts.

It may seem odd for an attacker to use infrastructure in their own country, possibly pointing a finger at them. However, here it simply becomes another bulletproof hosting option based on the lack of cooperation between US or European law enforcement and local police in Iran.

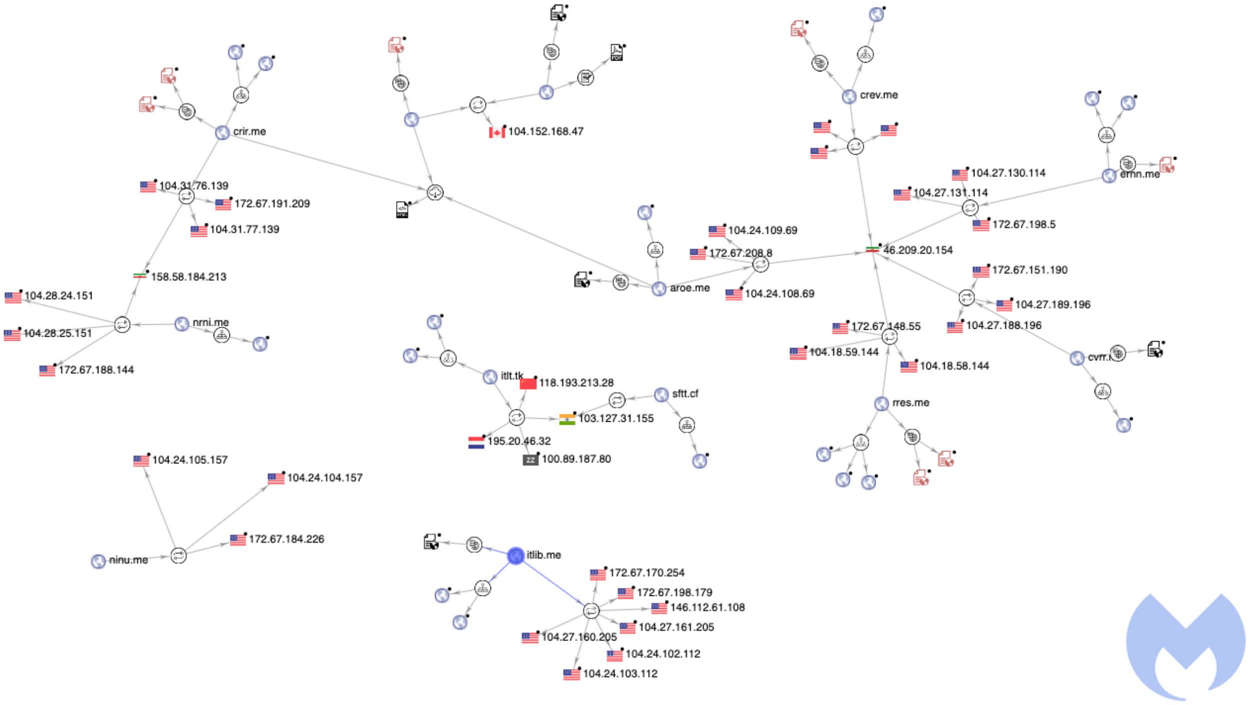

Figure 2: Part of the phishing infrastructure showing connections with Iran

Clearly we only uncovered a small portion of this phishing operation. Although for the most part the sites are taken down quickly, the attacker has the advantage of being one step ahead and is going for many possible targets at once.

We are continuing to monitor this campaign and are keeping our customers safe by blocking the phishing sites.

Indicators of Compromise (IOCs)

library[.]adelaide[.]crev[.]me
signon[.]adelaide[.]edu[.]au[.]itlib[.]me
blackboard[.]gcal[.]crev[.]me
blackboard[.]stonybrook[.]ernn[.]me
blackboard[.]stonybrook[.]nrni[.]me
namidp[.]services[.]uu[.]nl[.]itlib[.]me
uu[.]blackboard[.]rres[.]me
librarysso[.]vu[.]cvrr[.]me
ole[.]bris[.]crir[.]me
idpz[.]utorauth[.]utoronto[.]ca[.]itlf[.]cf
raven[.]cam[.]ac[.]uk[.]iftl[.]tk

login[.]ki[.]se[.]iftl[.]tk
shib[.]york[.]ac[.]uk[.]iftl[.]tk
sso[.]id[.]kent[.]ac[.]uk[.]iftl[.]tk
idp3[.]it[.]gu[.]se[.]itlf[.]cf
login[.]proxy1[.]lib[.]uwo[.]ca[.]sftt[.]cf
login[.]libproxy[.]kcl[.]ac[.]uk[.]itlt[.]tk
idcheck2[.]qmul[.]ac[.]uk[.]sftt[.]cf
lms[.]latrobe[.]aroe[.]me
ntulearn[.]ntu[.]ninu[.]me
adfs[.]lincoln[.]ac[.]uk[.]itlib[.]me
cas[.]thm[.]de[.]itlib[.]me
libproxy[.]library[.]unt[.]edu[.]itlib[.]me
shibboleth[.]mcgill[.]ca[.]iftl[.]tk
vle[.]cam[.]ac[.]uk[.]canm[.]me

158[.]58[.]184[.]213
46[.]209[.]20[.]154
103[.]127[.]31[.]155