Related Insights

info.phishlabs.com/blog/silent-librarian-university-attacks-continue-unabated-in-days-following-indictment

April 5, 2018

Get The Latest Insights

By The PhishLabs Team | April 5, 2018

On Friday, March 23, nine Iranian threat actors were indicted for stealing massive quantities of data from universities, businesses, and governments all over the world.

If you've been following our blog (or the news), you already know the actors are associated with an organization called the Mabna Institute, and are responsible for stealing more than 31 terabytes of data over the past four and a half years. To put that number in context, you'd need to cut down more than 1.5 million trees to make enough paper to print out all of the stolen data.

The group, which we have called "Silent Librarian," has targeted universities and other organizations with strong research departments, particularly those focused on medicine and technology.

But the scale of the attacks, while alarming, isn't the most concerning thing right now. Here's the real headline:

Silent Librarian phishing attacks have continued unabated in the days since the indictment.

Since the indictment less than 14 days ago, PhishLabs analysts have observed 18 new phishing attacks targeting 14 different universities from five countries: United States, United Kingdom, Canada, Australia, and France.

What Does This Mean for Potential Targets?

Over the past two weeks, the indicted Iranian threat actors have continued their attacks despite being formally charged. Including the most recent attacks, PhishLabs has attributed more than 780 phishing attacks to Silent Librarian, which includes attacks against more than 300 universities in 22 countries.

While extradition or real sanctions were likely never in the cards, it was probably hoped that publicly “naming and shaming” the actors would at least put the attacks on hold. Since that hasn’t happened, it’s doubly important that potential targets do everything they can to protect themselves from further attacks.

To reiterate, the attackers have explicitly gone after universities and other organizations with strong research departments, particularly in the fields of technology and medicine.

Below is a list of high-level indicators of compromise (IOCs) that we have previously associated with Silent Librarian phishing attacks, which includes domains hosting university phishing sites and IP addresses linked to those domains. It should be noted that all of the domains used by Silent Librarian are maliciously registered and no legitimate content has been observed on any of the domains. For IP addresses referenced below, other non-Silent Librarian domains have historically resolved to many of them and the maliciousness of those domains has not been determined.

While stringent anti-phishing measures should be taken to minimize the threat posed by Silent Librarian (or any threat, for that matter), the first order of business for any potential target organization should be to blacklist the domains and monitor and/or set flags for outbound traffic for the IP addresses listed below. It should also be noted that because this group is still deploying new attacks, new domains are being actively created, so this should be viewed as a historical list, not a real-time list.

DOMAINS:
1edu.in
acll.cf
aill.cf
atna.cf
atti.cf
authn.in
authn.website
aztt.tk
cavc.tk
cave.gq
ccli.cf
cill.cf
citt.cf
cntt.cf
crll.tk

csll.cf
csna.cf
ctll.tk
cvnc.ga
cvre.tk
czll.tk
cztt.tk
ditt.cf
edlu.info
edu-lib.cf
edu-lib.ml
edue.in
edun.cf
eill.cf
eslog.in
euca.cf
euce.in
ezauth.xyz
ezll.tk
ezplog.in
ezproxy.in
ezproxy.tk
ezproxy.top
ezprx.xyz
eztt.tk
flll.cf
iell.tk
iull.tk
izll.tk
lett.cf
lib1.bid
lib1.ga
lib1.ml
lib2.xyz
libb.ga
libc.cf
libe.ml
libg.cf
libg.ga
libg.gq
libk.gq
libk.ml

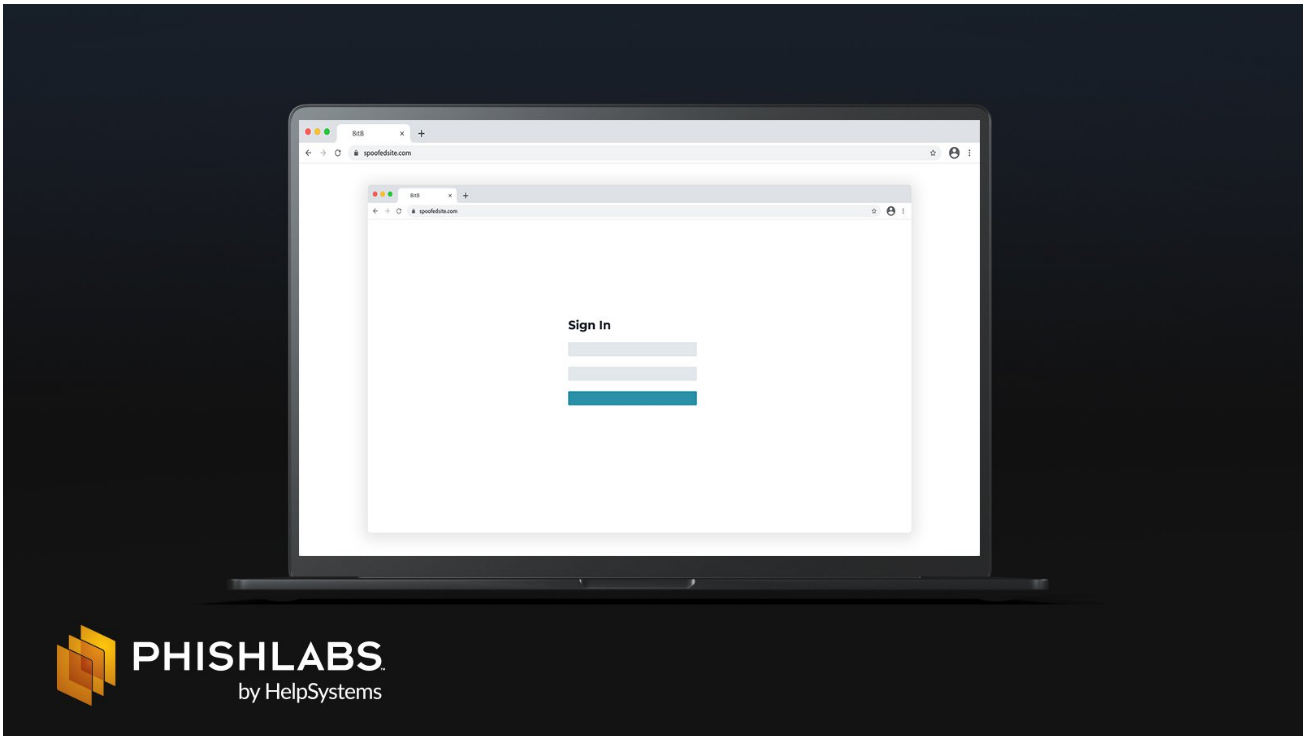
libloan.xyz
libn.gq
libnicinfo.xyz
libr.gq
library1.online
librarylog.in
libraryme.ir
libt.cf
libt.ml
libu.gq
libv.ga
libv.gq
libw.cf
libw.ml
lill.gq
llbt.tk
llib.cf
llib.ga
llic.cf
llic.tk
llil.cf
llit.cf
lliv.tk
llse.cf
medpoint.ir
mncr.tk
ncll.tk
ncnc.cf
nctt.tk
necr.ga
nelib.top
nika.ga
nikc.cf
nsae.ml
nuec.ml
nuvo.cf
nvre.tk
reactivation.in
rill.cf
rtll.cf
rtll.tk
saea.ga

sctt.cf
seae.tk
shibboleth.link
sitl.tk
slli.cf
tilc.tk
till.cf
titt.cf
uill.cf
uitt.tk
ulibe.ml
ulibi.ml
ulibl.ga
ulibr.cf
ulibr.ga
ulibt.ml
umlib.ml
umll.tk
uni-lb.com
univ-database.cf
univ-library.ga
unll.tk
unsw.ga
utll.tk
vsre.cf
web2lib.info
webauth.in
webauth.xyz
weblogin.site
weblogon.xyz
xill.tk
zedviros.ir
zill.cf

IP ADDRESSES:
103.241.3.91
104.152.168.23
107.180.57.7
107.180.58.47
136.243.145.233
136.243.198.45
138.201.17.56
141.8.224.221

144.217.120.73
144.76.189.80
148.251.116.93
148.251.12.172
162.218.237.3
167.114.103.215
167.114.13.164
172.246.144.34
173.254.239.2
176.31.33.115
176.31.33.116
176.9.188.235
178.33.115.10
184.95.37.90
185.105.185.22
185.28.21.83
185.28.21.95
185.55.227.104
185.86.180.250
188.40.34.186
192.169.82.134
193.70.117.250
195.154.102.75
198.252.106.149
198.27.68.142
198.91.81.5
199.204.187.164
31.220.20.111
45.35.33.126
46.4.91.26
5.135.123.163
5.196.194.234
51.254.198.131
51.254.21.142
66.70.197.208
78.46.77.105
79.175.181.11
82.102.15.215
87.98.249.207
88.99.128.229
88.99.139.8
88.99.160.209

88.99.40.240
88.99.69.4
93.174.95.64
94.76.204.201



Why BitB Attacks are Concerning

PhishLabs has identified a Browser-in-the-Browser (BitB) campaign targeting financial institutions with a fake Office 365 (O365) authorization protocol.

What is the HelpSystems Value Proposition for Cybersecurity?

In this guest blog, Dr Ed Amoroso, CEO, Tag Cyber, provides a high-level overview of the HelpSystems cybersecurity portfolio value proposition based on a mapping of its component solution offerings to the NIST Cybersecurity Framework (CSF) phases.

Cybercrime Cost U.S. $6.9 Billion in 2021

The FBI's annual look at phishing, scam, and personal data breach statistics is out.