TA407 Overview (Mabna Institute, Silent Librarian)

proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian

October 9, 2019

Blog

Threat Insight

Threat Actor Profile: TA407, the Silent Librarian

Threat Actor Profile: TA407, the Silent Librarian

October 14, 2019 The Proofpoint Threat Insight Team

Overview

In our September 5, 2019, Threat Insight post, "Seems Phishy: Back To School Lures Target University Students and Staff," we discussed the seasonal uptick of phishing campaigns that are directed at university students and staff, usually between June and October of every year. Since our blog post, colleagues at Secureworks have provided further details on one actor we highlighted, tracked by Proofpoint as TA407, also known as Silent Librarian, Cobalt Dickens, and Mabna Institute. In this blog, we provide additional insight into the actor and their evolving TTPs in ongoing, academia and university campaigns.

Like many educational phishing attacks, campaigns associated with TA407 are typically not geographically targeted, but rather tied to specific universities, with phishing landing pages developed for library and student or faculty access portals. While many of the attacks are directed at schools in the United States, Proofpoint researchers regularly observe campaigns affecting universities primarily in North America and Europe.

Silent Librarian is a prolific financially motivated actor operating out of Iran. In early 2018, the US Department of Justice indicted nine members of the cybercrime group for hacking, wire fraud, and identity theft. In particular, the group was cited for *"obtain[ing] unauthorized access to computer systems, steal[ing] proprietary data from those systems, and sell[ing] that stolen data to Iranian customers, including the Iranian government and Iranian universities."*

The indictment alleges that between 2013 and 2017, TA407's activities resulted in the following damages:

- Approximately $3.4 billion worth of intellectual property loss due to unauthorized access
- 31.5 terabytes of academic data and IP theft from compromised universities
- 7998 university accounts were successfully compromised worldwide
- 3768 accounts compromised that belonged to professors at US-based universities

Victims of the scheme included:

- Approximately 144 universities in the United States
- 176 foreign universities in 21 countries
- Five federal and state government agencies in the United States
- 36 private companies in the United States
- 11 foreign private companies
- Two international non-governmental organizations

The DOJ indictments, however, have had no appreciable effect on the group's activities and university email account compromises are ongoing, building on the success of previous campaigns.

Mabna Institute Tactics, Techniques, and Procedures

Mabna Institute (AKA TA407) primarily targets universities and higher education institutions worldwide with low-volume (tens or hundreds of messages), target-specific campaigns. These university phishing campaigns utilize well-crafted social engineering mechanisms including:

- Stolen university branding
- Fake email signatures/credentials/addresses
- University-specific email bodies/portal clones
- Themed subject lines (e.g., "Renewal of loaned items", "Renew your loaned items", "Renewal of materials", "Overdue notice on loaned items", and "Library Services")

Since the beginning of 2019, Proofpoint researchers observed several TA407 campaigns distributing phishing URLs leading to clones of university library login pages. Although TA407 has made minor updates to their social engineering techniques and infrastructure, their strategies have been overall rather consistent. Many of these campaigns use the same lures with minor variations in phrasing.

Historically, the group has employed the use of a series of phishing origin points, abusing access first at one university and then another. TA407 makes extensive use of Freenom domains to host credential phishing landing pages; the group then abuses compromised accounts at universities to phish users at other universities, compromising additional accounts and spreading from school to school.

Proofpoint researchers have observed changes in TA407's tactics, techniques, and procedures (TTPs), particularly in their use of URL shorteners, linking, and abuse of legitimate services and infrastructure. While the group does not always use URL shorteners, these frequently appear in their mix of linking and redirection techniques.

The following Freenom domains were observed in use by TA407 in September. A complete list of such domains used since January appears in the Appendix.

- atll[.]tk
- azll[.]tk
- cllt[.]cf
- cllt[.]tk
- fill[.]cf
- itll[.]tk
- llit[.]cf
- lliz[.]cf
- nlll[.]tk
- ntil[.]cf
- sitt[.]cf
- tlit[.]cf
- ttit[.]cf
- visc[.]cf
- xill[.]cf
- zlll[.]tk

Figure 1 illustrates the flow of a typical TA407 campaign. Note the abuse of university-controlled URL shortening services and compromised email accounts.

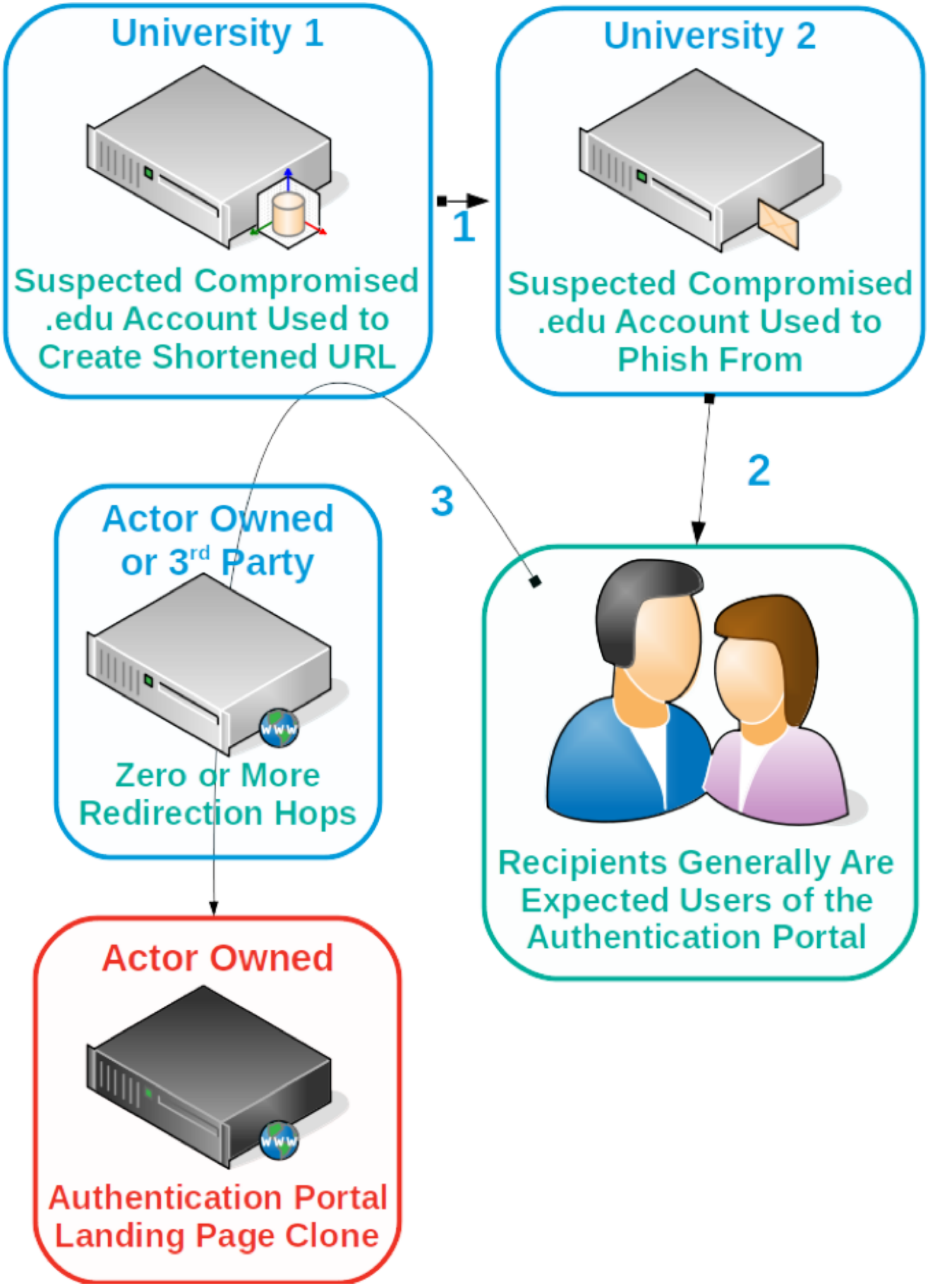
University 1
Suspected Compromised .edu Account Used to Create Shortened URL
1
University 2
Suspected Compromised .edu Account Used to Phish From
2
3
Actor Owned or 3rd Party
Zero or More Redirection Hops
Recipients Generally Are Expected Users of the Authentication Portal
Actor Owned
Authentication Portal Landing Page Clone

Figure 1: Typical attack flow of TA407/Silent Librarian

Proofpoint researchers frequently observe Silent Librarian's phishing attempts originating from a university unrelated to their current target using a separate, unrelated university's URL shortening service. This short URL links to a phishing landing page either directly or via one or more third-party sites that eventually lands the user on a clone of a login portal hosted on an actor-controlled server.

The following illustration depicts the attack flow of the actor's use of phishing links starting at any of the redirection phases. Variation between university-based URL shorteners and free shorteners represents one of the shifting TTPs observed in Silent Librarian's recent activity.

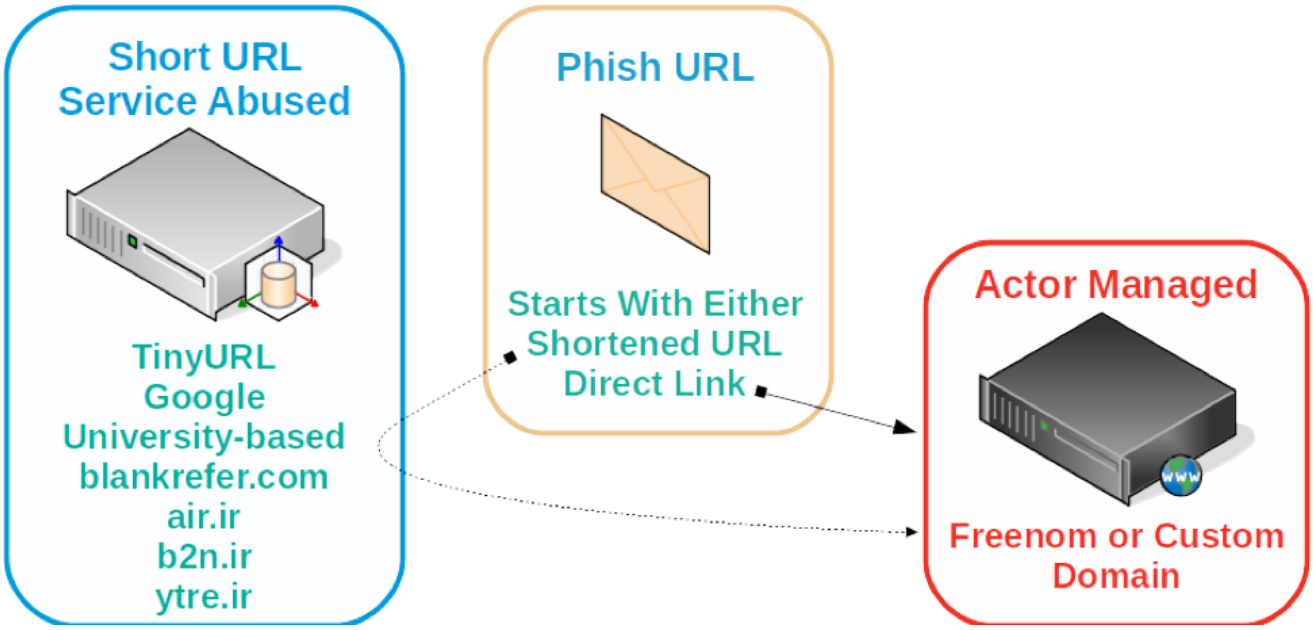

Figure 2: How TA407 utilizes short URL services in its phishing attack redirections.

Over time, Proofpoint researchers have observed TA407 abuse several short URL services for initial redirection to phishing landing pages. These have included the now discontinued Google URL shortening service, .ir-based short URL services, and .edu URL shorteners. We observed apparent experimentation with university-based URL shorteners prior to the discontinuation of Google's goo.gl services. Earlier in 2019, after goo.gl was discontinued, abuse of university URL shortening services appeared to increase and has been observed as recently as September of 2019.

Campaign Lure Examples

Very little has changed with TA407's phishing lures in 2019. Most phish lures are themed around library access.

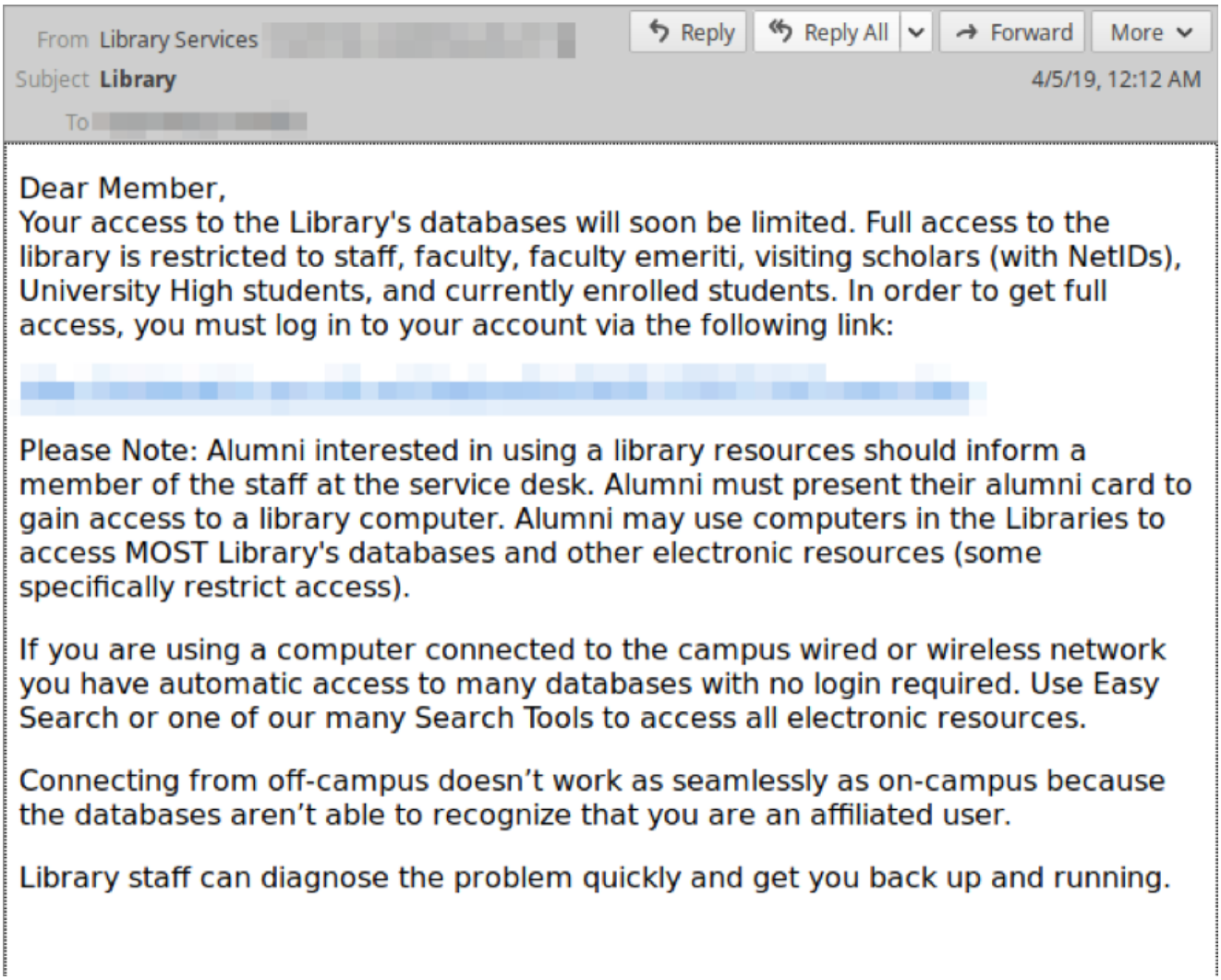

Figure 3: Example of a library access phish lure from TA407

Over time, Proofpoint researchers have observed slight adjustments in lure verbiage, but most continue to emphasize loss of library access privileges:

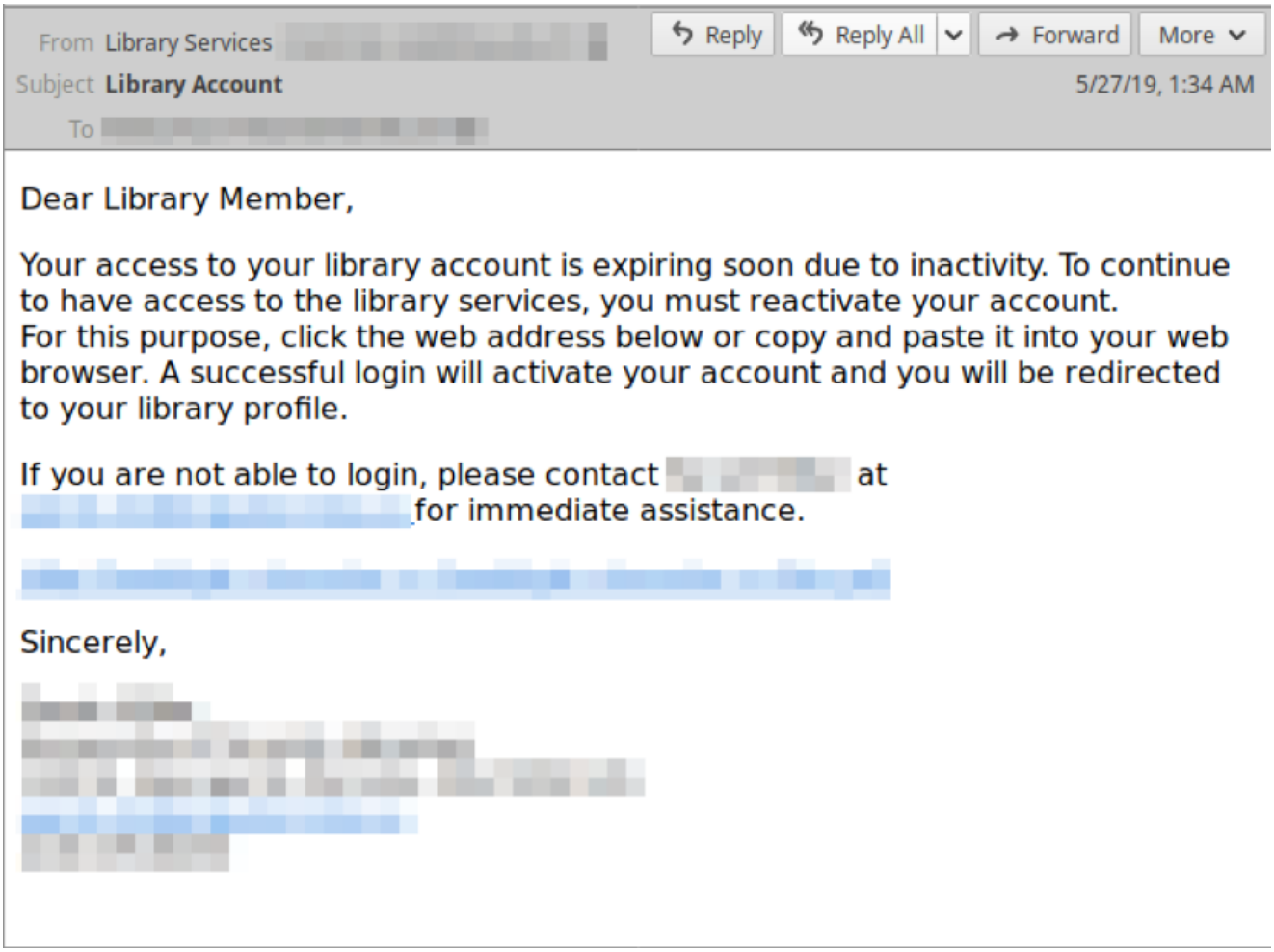

Figure 4: Example of how TA407's lure verbiage has evolved over time

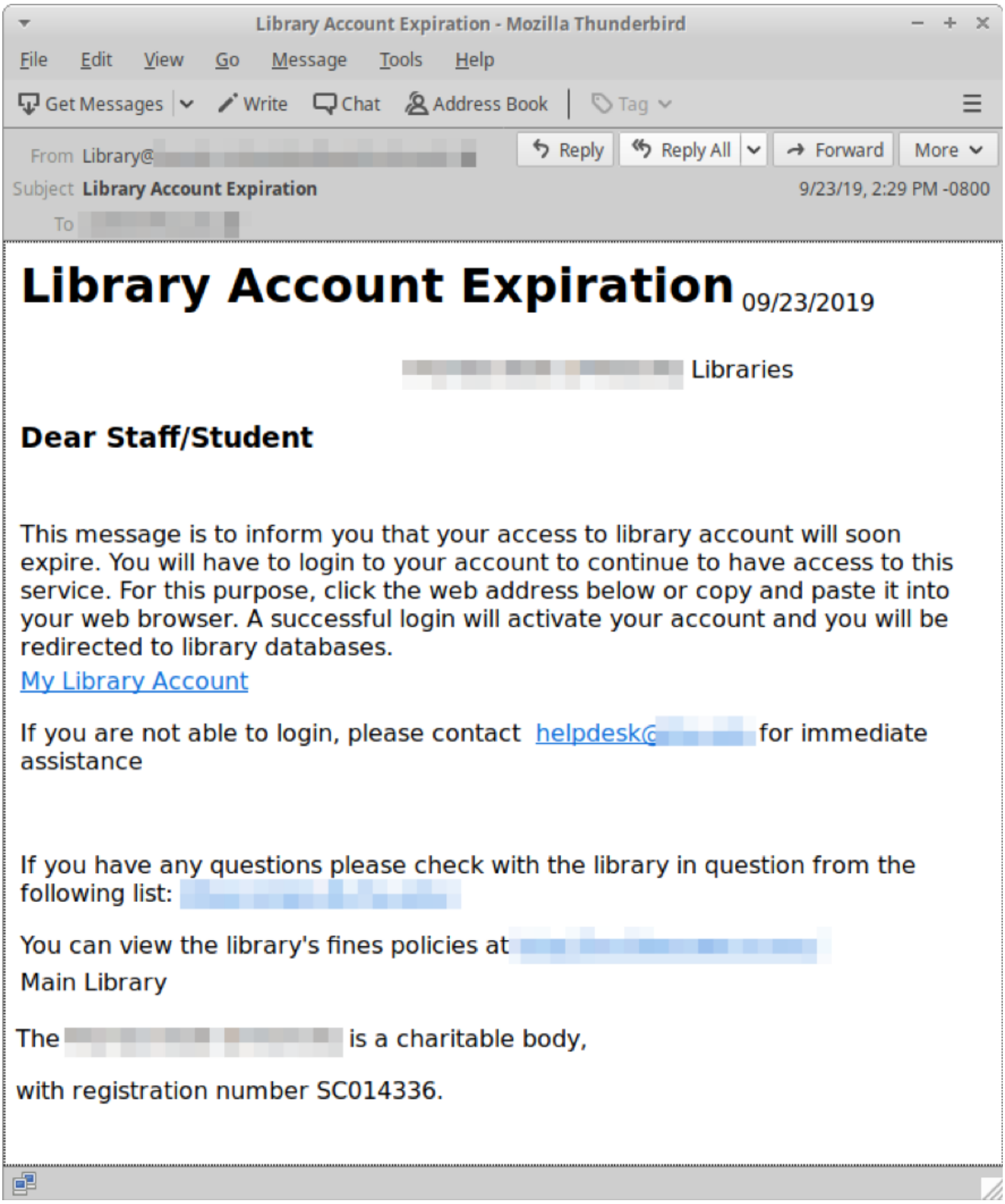

Figure 5: Basic lure verbiage by TA407. This style has been used for years.

In many examples, TA407 uses stolen branding from the university being targeted. In the following example, we have redacted the image of the signature block using the school logo that was used in the message body.

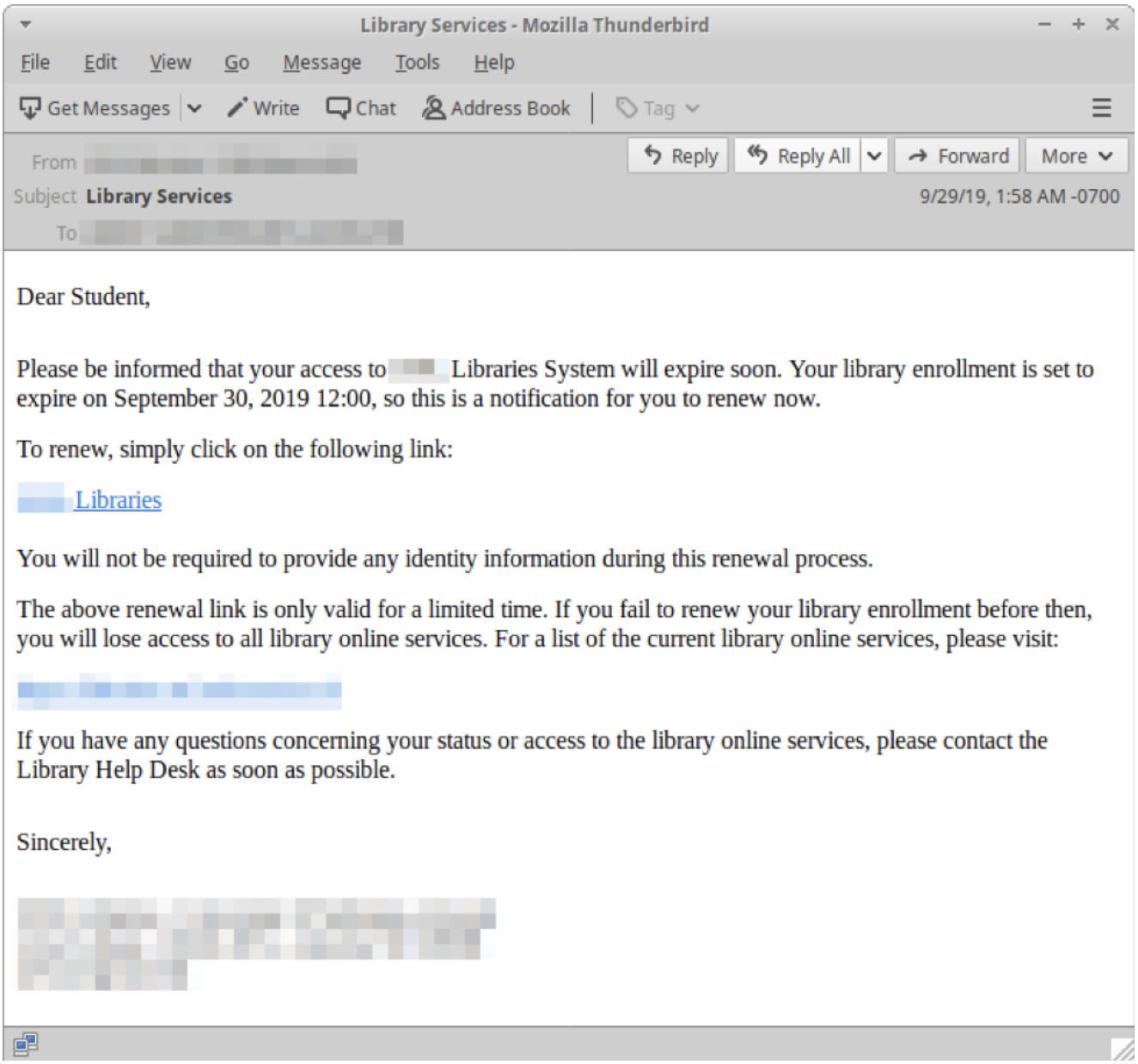

Figure 6: More evolution in attack verbiage from TA407

TA407 has demonstrated awareness of close to real-time changes in authentication portal traits, such as weather notification banners, that are sometimes reflected on the landing page clones used in their campaigns. The awareness manifests in both the lure wording and/or landing page appearance. However, Proofpoint researchers do occasionally observe what appears to be an outdated clone of a previous version of their target's portal, suggesting either inconsistent updates or coincidental timing of clone updates.

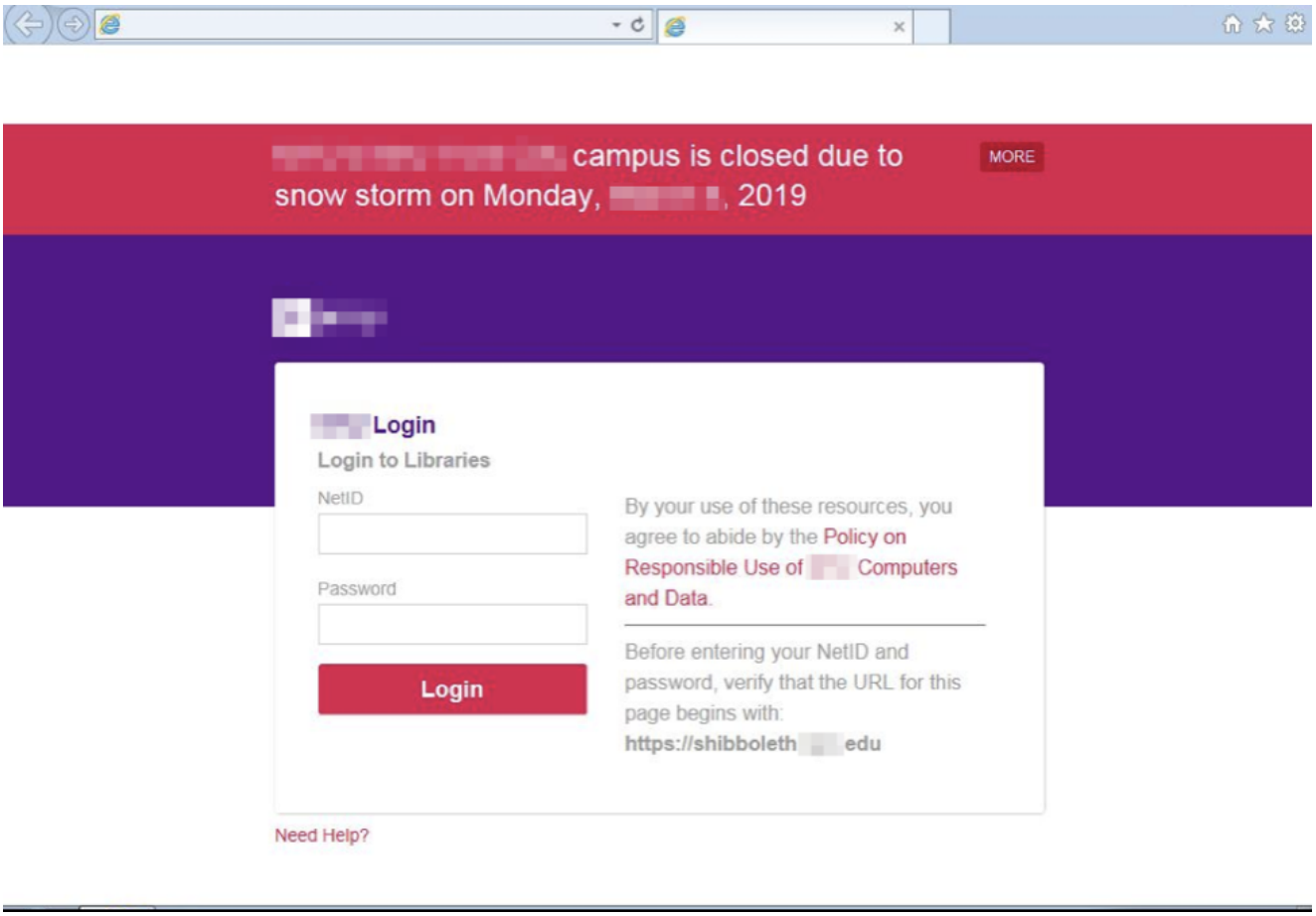

Figure 7: Fake university login portal with spoofed display name, stolen branding, and accurate weather forecast warning

Conclusion

Last year's DOJ indictments had no appreciable effect on curtailing the activities of TA407. Campaigns with the apparent intent to compromise user accounts at universities are ongoing with new Freenom domains appearing in September to host phishing pages. Most notably,

- TA407 takes advantage of publicized downtime and weather alerts, among other events, to add credibility to the phish, increasing the risk for universities and their constituents.
- In its attacks, TA407 uses a series of phishing origin points, abusing access first at one university and then another for use against new targets. The group then appears to continue the cycle with a chosen subset of freshly compromised accounts.
- The changes in URL shorteners, linking and hosting practices described here make detection of TA407's activities increasingly difficult for defenders and demonstrate the adaptability and innovation that have enabled this threat actor to drive billions of dollars in losses in terms of intellectual property theft and resale of stolen journal subscriptions.

Proofpoint recommends that universities remain vigilant against these threats to prevent losses and protect valuable IP and personal information. Implementing two-factor authentication within publicly exposed systems can help mitigate overall attack risk and substantially increase the level of effort needed by threat actors to compromise university accounts.

Appendix: List of OpenTLD and Freenom domains used by TA407 since January 2019

Month observed in campaigns	Domain
January	aill[.]nl
	cnen[.]cf
	eill[.]nl
	libt[.]ga
February	aill[.]nl
	cnen[.]cf
	eill[.]nl
	libt[.]ga
March	aill[.]nl
	cnen[.]cf
	flil[.]cf
	libt[.]ga
	llif[.]cf
	llit[.]cf
	llli[.]cf
	lllt[.]cf

April	cill[.]ml
	cnen[.]cf
	cvve[.]cf
	eill[.]cf
	eill[.]ga
	flil[.]cf
	illl[.]cf
	libdo[.]cf
	libt[.]ga
	lllt[.]cf
	ncce[.]cf
	nlib[.]ml
	nlll[.]cf
	nuec[.]cf
	rvna[.]cf
May	azll[.]cf
	clll[.]cf
	cvve[.]cf
	flll[.]cf
	libn[.]gq
	libt[.]ga
	ssll[.]cf

June	blibo[.]ga
	cvve[.]cf
	elll[.]cf
	euve[.]tk
	flll[.]cf
	jlll[.]cf
	libk[.]ga
	libm[.]ga
	libt[.]ga
	libw[.]gq
	lllib[.]cf
	mlibo[.]ml
	nlll[.]cf
	nlll[.]tk
	tlll[.]cf
July	cvve[.]cf
	elll[.]cf
	libb[.]ga
	libf[.]ga
	libk[.]ga
	libt[.]ga
	lIii[.]xyz
	lzll[.]cf
	ntll[.]cf
	ntll[.]tk
	venc[.]cf

August	clll[.]tk
	cllt[.]tk
	ills[.]cf
	itll[.]tk
	liba[.]gq
	libe[.]cf
	libe[.]ga
	libf[.]ga
	librt[.]ml
	libver[.]ml
	llit[.]cf
	llli[.]nl
	ntll[.]tk
	stll[.]tk
	tlll[.]tk
	ttll[.]cf
	ulll[.]tk
	visc[.]cf
	vtll[.]cf

September	atll[.]tk
	azll[.]tk
	cllt[.]cf
	cllt[.]tk
	fill[.]cf
	itll[.]tk
	llit[.]cf
	lliz[.]cf
	nlll[.]tk
	ntil[.]cf
	sitt[.]cf
	tlit[.]cf
	ttit[.]cf
	visc[.]cf
	xill[.]cf
	zlll[.]tk