‘Shadow Academy’ Targets 20 Universities Worldwide

riskiq.com/blog/external-threat-management/shadow-academy/

December 2, 2020

External Threat Management Labs

December 02, 2020

By Team RiskIQ

In early July 2020, RiskIQ began tracking a phishing campaign identified through our internet intelligence graph targeting colleges and universities worldwide. From July 2020 into October 2020, RiskIQ systems uncovered 20 unique targets in Australia, Afghanistan, the UK, and the USA.

All these attacks used similar tactics, techniques, and procedures (TTPs) as Mabna Institute, an Iranian company that, according to the FBI, was created for illegally gaining access "to non-Iranian scientific resources through computer intrusions." Mabna Institute earned the moniker "Silent Librarian" due to its focused efforts to compromise university students and faculty by impersonating university library resources using domain shadowing to harvest credentials.

However, while RiskIQ's findings are consistent with TTPs in use by Silent Librarian, they alone are not sufficient to attribute the threat activity we've detected against these 20 universities directly to Mabna Institute. Therefore, RiskIQ has named actors identified during this research as "Shadow Academy."

- **37%** of the universities were targeted with Library themed attacks.
- **63%** of the universities were targeted with general access or student portal attacks.

- **11%** of the universities were targeted with financial aid-themed attacks.

An Orientation to Shadow Academy

The first target identified from RiskIQ crawl data was a Louisiana State University (LSU)-themed student portal login page. While using PassiveTotal to analyze this resource, it became clear that threat actors were leveraging domain Shadowing, a technique known to be used by Silent Librarian.

Domain shadowing intercepts account traffic flowing to existing, registered, and otherwise trustworthy web domains. First, threat actors steal domain account credentials. They then register unauthorized subdomains to point traffic to malicious servers or, in this case, create phishing pages. These subdomains are challenging to detect because they are associated with well-known domains, often don't follow any discernible pattern, and don't affect the parent domain or anything hosted on that domain.

A Far-reaching Campaign

Expanding on our identification of the initial LSU-imposter domain, we saw that Shadow Academy used this same resource to host similar malicious infrastructure to target three other universities, all using certificates that share a distinct pattern.

RiskIQ's internet intelligence graph helped unearth a new batch of compromised domains by keying in on the URL structure and date range of registration. Subdomains created from these domains spanned multiple campaign themes, which focused primarily on credential harvesting and financial theft. The credential-harvesting URLs focused mainly on popular services like Amazon, Instagram, and online banking.

'Murrez' is a Possible Shadow Academy Competitor

During this investigation, RiskIQ researchers discovered through RiskIQ crawl data that the vocational-technical school **azma.edu[.]af**, located in Ehsan Azizi, Herat, Afghanistan, had been defaced by the actor "Murrez."

Many of the tools in Murrez's GitHub account have code comments with references or file names(**priv8bruter.pl)** connected to a well known Russian cybercrime forum named "Priv-8". The account contains repositories of compromised database and domain credentials and hacking tools related to objectives similar to but not directly attributed to Silent Librarian.

Murrez's "private-tool" repository has a Perl-based tool that automates brute force attacks and would enable an attacker to gain unauthorized access to these resources and facilitate the creation of certificates and shadow domains. Priv-8 facilitates the sharing and selling of compromised datasets, tools, and resources for attackers. Searching for" .edu" in one of Murrez's dumped databases reveals hundreds of compromised ".edu" accounts.

Murrez appears to be a member of W4coders, a relatively small hacking collective, possibly comprised of four other actors. According to a site the group uses to rank its successes, W4coders has 81 successful compromises ranging from defacement to domain takeover dating back to May 2020, many of which are related to education, news media, and, in some cases, law enforcement.

Protect Your Attack Surface

Many college campuses began releasing timelines for on-campus operations in July 2020. Research suggests that Shadow Academy actors timed the development of malicious infrastructure to take advantage of the first few days of class, which can be a chaotic time that overwhelms IT staff.

However, having access to the infrastructure that comprises the web helps analysts note similarities between threat campaigns are observable behavior by threat actors to track them to identify and investigate threats during heightened periods of attacker activity.

Starting with the unique data sets in RiskIQ PassiveTotal built upon RiskIQ's Internet Intelligence Graph, analysts can quickly enumerate infrastructure related to even seemingly disparate campaigns to paint a vivid picture of the threat landscape targeting their institution.

RiskIQ will continue research efforts to enumerate Shadow Academy infrastructure and share findings. To read the full report and explore the comprehensive list of IOCs, visit the Threat Intelligence Portal in RiskIQ PassiveTotal. Sign up with a corporate email address for a free month of enterprise access.

Subscribe to Our Newsletter

Subscribe to the RiskIQ newsletter to stay up-to-date on our latest content, headlines, research, events, and more.

Base Editor