Back to School: COBALT DICKENS Targets Universities

secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities

Counter Threat Unit Research Team

Despite indictments in March 2018, the Iranian threat group is likely responsible for a large-scale campaign that targeted university credentials using the same spoofing tactics as previous attacks. Friday, August 24, 2018 *By: Counter Threat Unit Research Team*

In August 2018, members of university communities worldwide may have been providing access to more than just homework assignments.

Secureworks® Counter Threat Unit™ (CTU) researchers discovered a URL spoofing a login page for a university. Further research into the IP address hosting the spoofed page revealed a broader campaign to steal credentials. Sixteen domains contained over 300 spoofed websites and login pages for 76 universities located in 14 countries, including Australia, Canada, China, Israel, Japan, Switzerland, Turkey, the United Kingdom, and the United States (see Figure 1).

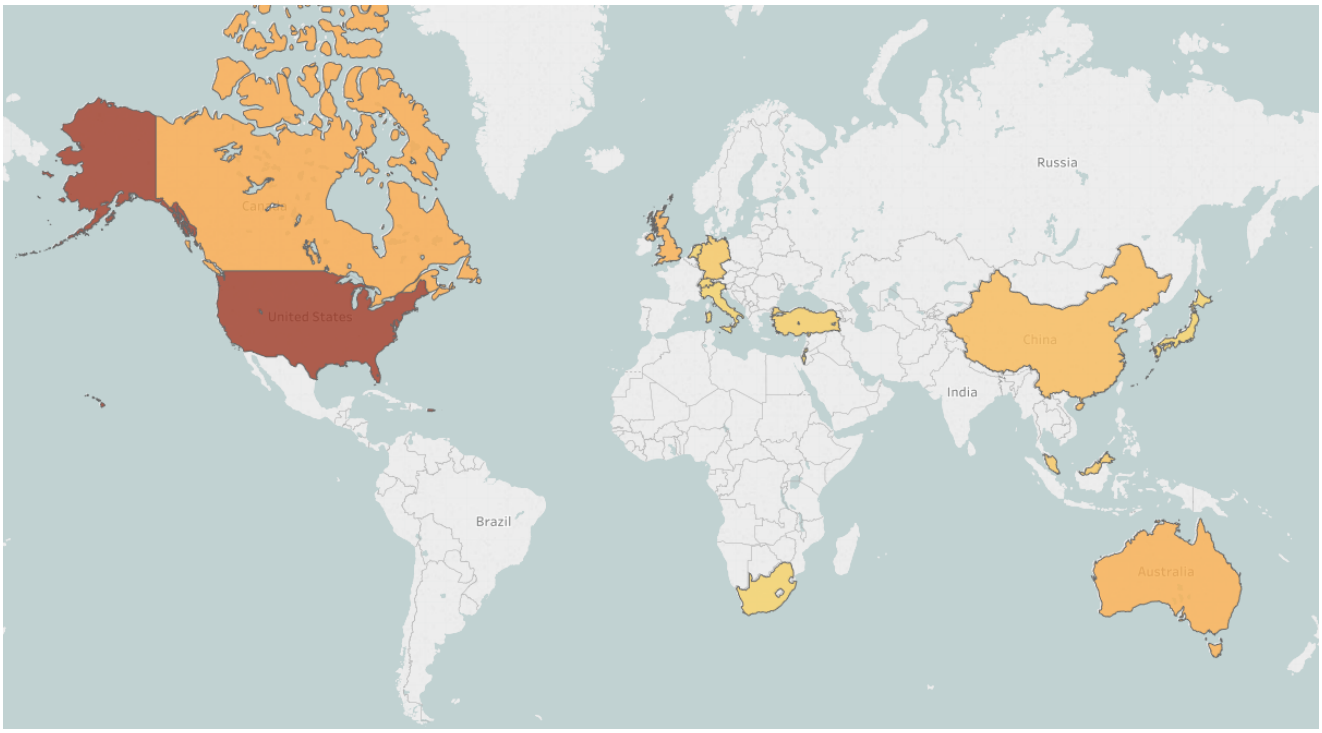

Figure 1. Countries with targeted universities. The darker the color, the higher the number of affected universities. (Source: Secureworks)

After entering their credentials into the fake login page, victims were redirected to the legitimate website where they were automatically logged into a valid session or were prompted to enter their credentials again. Numerous spoofed domains referenced the targeted universities' online library systems, indicating the threat actors' intent to gain access to these resources.

CTU™ researchers were unable to confirm functionality of all identified spoofed pages because some of the domains were not accessible at the time of analysis. Many of the domains were registered between May and August 2018, with the most recent being registered on August 19. Domain registrations indicate the infrastructure to support this campaign was still being created when CTU researchers discovered the activity.

Most of the domains observed in this campaign resolved to the same IP address and DNS name server. A domain registered in May 2018 also contained subdomains spoofing university targets. These subdomains redirected visitors to spoofed login pages on other attacker-controlled domains.

> "The pain of parting is nothing to the joy of meeting again."
>
> — Nicholas Nickleby by Charles Dickens

The targeting of online academic resources is similar to previous cyber operations by COBALT DICKENS, a threat group associated with the Iranian government. In those operations, which also shared infrastructure with the August attacks, the threat group created lookalike domains to phish targets and used credentials to steal intellectual property from specific resources, including library systems. In March 2018, the U.S. Department of Justice indicted the Mabna Institute and nine Iranian nationals in connection with COBALT DICKENS activity occurring between 2013 and 2017. Many threat groups do not change their tactics despite public disclosures, and CTU analysis suggests that COBALT DICKENS may be responsible for the university targeting despite the indictments of some members.

Universities are attractive targets for threat actors interested in obtaining intellectual property. In addition to being more difficult to secure than heavily regulated finance or healthcare organizations, universities are known to develop cutting-edge research and can attract global researchers and students. CTU researchers have contacted various global partners to address this threat.

This widespread spoofing of login pages to steal credentials reinforces the need for organizations to incorporate multifactor authentication using secure protocols and implement complex password requirements on publicly accessible systems. CTU researchers recommend that clients implement training programs to educate users about security threats, including guidance for recognizing and reporting suspicious emails.

CTU researchers have identified indicators for this threat (see Table 1). Note that IP addresses can be reallocated. The domains and IP address may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
anvc.me	Domain name	Hosting phishing website used by COBALT DICKENS
eduv.icu	Domain name	Hosting phishing website used by COBALT DICKENS
jhbn.me	Domain name	Hosting phishing website used by COBALT DICKENS

nimc.cf	Domain name	Hosting phishing website used by COBALT DICKENS
uncr.me	Domain name	Hosting phishing website used by COBALT DICKENS
unie.ga	Domain name	Hosting phishing website used by COBALT DICKENS
unie.ml	Domain name	Hosting phishing website used by COBALT DICKENS
unin.icu	Domain name	Hosting phishing website used by COBALT DICKENS
unip.cf	Domain name	Hosting phishing website used by COBALT DICKENS
unip.gq	Domain name	Hosting phishing website used by COBALT DICKENS
unir.cf	Domain name	Hosting phishing website used by COBALT DICKENS
unir.gq	Domain name	Hosting phishing website used by COBALT DICKENS
unir.ml	Domain name	Hosting phishing website used by COBALT DICKENS
unisv.xyz	Domain name	Hosting phishing website used by COBALT DICKENS
univ.red	Domain name	Hosting phishing website used by COBALT DICKENS
untc.me	Domain name	Hosting phishing website used by COBALT DICKENS

untf.me	Domain name	Hosting phishing website used by COBALT DICKENS
unts.me	Domain name	Hosting phishing website used by COBALT DICKENS
unvc.me	Domain name	Hosting phishing website used by COBALT DICKENS
ebookfafa.com	Domain name	Hosting subdomains associated with COBALT DICKENS phishing targets
lib-service.com	Domain name	Hosting subdomains associated with COBALT DICKENS phishing targets
208.115.226.68	IP address	Hosting suspicious and phishing domains used by COBALT DICKENS

Table 1. Indicators for this threat.