Hackers attacked hundreds of universities to gain access to library data

Cobalt Dickens is one of the world's most sought after hacker groups.

Cobalt Dickens, one of the most sought after FBI hackers in the world and thought to be closely connected to the Iranian government, recently ran a series of large-scale fraud attacks. took place last July and August, targeting more than 60 major universities worldwide.

In reality, however, the report of international security researchers said that the malicious activities of Cobalt Dickens group had affected at least 380 universities in more than 30 countries and territories. 6 times more than the original target set by this hacker group.

1. The Toyota subsidiary lost $ 37 million just after an online fraud campaign

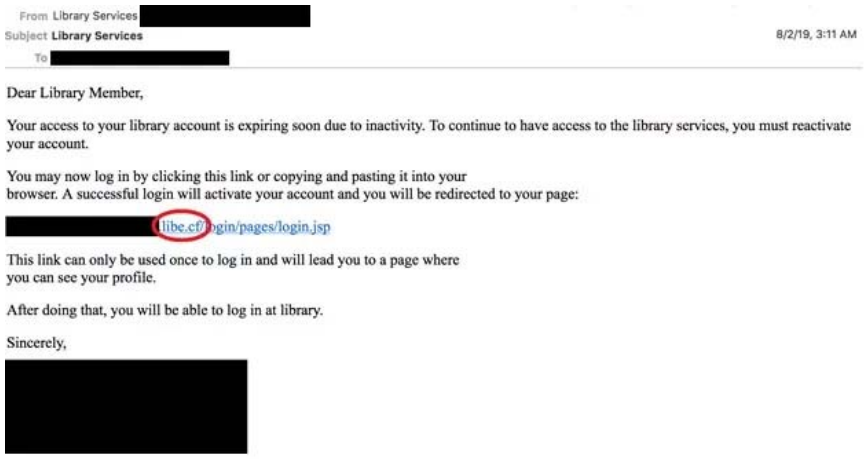
Cobalt Dickens is one of the most wanted Iranian hacker groups in the world.

Free domain name and TLS certs

This large-scale scam campaign mainly targets institutions and educational institutions in Australia, Hong Kong, the United States, Canada, the United Kingdom and Switzerland. The Cobalt Dickens team has used at least 20 new domain names registered with Freenom, one of the leading free premium domain name services (.ml, .ga, .cf, .gq, .tk)).

The method of fraud is not new. The Cobalt Dickens team will first send to the administrators, who have access to the university's library data archives on the targeted list a malicious email. This email displays a message to remind you to reactivate your account by clicking on the fake link as shown in the image below.

1. French police successfully cracked down on a botnet that exploits 850,000 computers from more than 100 countries.


From Library Services [redacted]
Subject Library Services 8/2/19, 3:11 AM
To [redacted]

Dear Library Member,

Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account.

You may now log in by clicking this link or copying and pasting it into your browser. A successful login will activate your account and you will be redirected to your page:

[redacted]libe.cf/login/pages/login.jsp

This link can only be used once to log in and will lead you to a page where you can see your profile.

After doing that, you will be able to log in at library.

Sincerely,

[redacted]

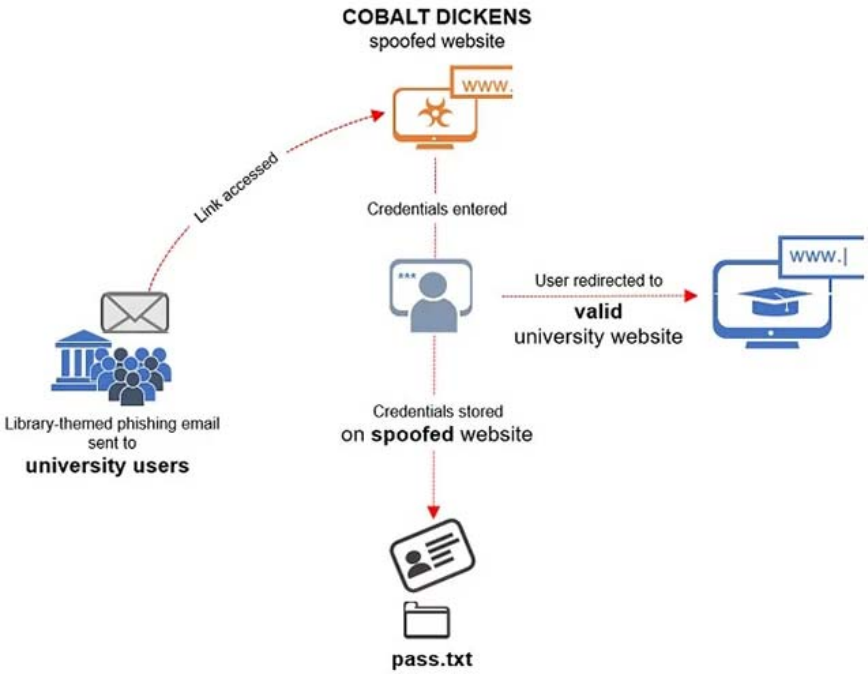
The fake URL uses a free domain name

The use of fake links can be considered a small change in the way this hacker group works because in previous campaigns, members of Cobalt Dickens relied heavily on shortened URLs to Directly redirect the victim to the fake login page.

This malicious link will lead the victim to "a fake website that looks identical or similar to the official library resource management page", researchers from Secureworks Counter Threat Unit (CTU), The first people who discovered this phishing attack campaign said.

When the victim enters his / her login information into the fake website, this data will be stored in a file named 'pass.txt' and the browser will immediately redirect to the 'owner' website. The university lets the victim think that he / she has logged into the official website.

1. Detecting many serious vulnerabilities that allow an attacker complete control of 4G router



Schematic illustration of Cobalt Dickens' phishing attack

To further bolster the trust and eliminate any traces of fraud, the Cobalt Dickens team often uses valid TLS certificates for their websites. Most of the certificates found in this campaign are free, issued by the non-profit authentication agency Let Encrypt.

1. More than 1 million payment card information from South Korea are sold on the Dark Web

No public data leakage cases have been recorded

In general, the main objective of Cobalt Dickens members in this campaign focused primarily on fraud, gaining access to or even controlling library databases of educational institutions in any country. In addition, there have been a few exceptions for private sector companies. The purpose of this group seems to be to steal library account information, access and steal the necessary data, then sell these academic resources to organizations and individuals in need (mainly in Iran).

Earlier, nine individuals believed to have played an important role in the operation of the Cobalt Dickens group were ordered to prosecute in March 2018 with a series of accusations of intrusion. unauthorized network. U.S. law enforcement believe this group of hackers has been a partner specializing in a company called Mabna Institut, and has carried out hundreds of large and small hacking campaigns on a global scale since at least 2013.

1. Alarming statistics on the situation of cyber security in our country in the first half of 2019

Nine members of Cobalt Dickens are wanted by the FBI around the globe

Many of the illegal intrusion campaigns by the Cobalt Dickens group are thought to be in close association with the Islamic Revolutionary Guards (IRGC). There are even many opinions that this group is an entity under the management of the Iranian government and the main task is to collect intelligence via cyberspace.

The objective of the group in the campaign is to be "computer systems belonging to 144 US universities, 176 universities in 21 foreign countries, 47 domestic and foreign private sector companies".

In particular, the Cobalt Dickens target list also includes a number of important U.S. government agencies, including the U.S. Department of Labor, the Federal Energy Regulatory Commission, and the state's public computer system. Hawaii, Indiana There are also both the United Nations and the United Nations Children's Fund.

According to cybersecurity experts, this group of hackers stole more than 31 terabytes of documents and data from victims worldwide. But despite the ongoing indictments, prosecution and wanted warrants issued by the US government and many other countries, the Cobalt Dickens group did not seem to care and was still comfortable deploying new campaigns on a large scale. and the level of danger is even greater.

1. The most dangerous hackers on the planet: Anonymous, Equation Group, Bureau 121 . What do you know about them?

The fight against government-sponsored cyber-criminal activities is still very arduous

The fight against cybercrime activities in general and especially cybercrimes sponsored by the government and state organizations in particular is still very difficult and no appointment of ending date.