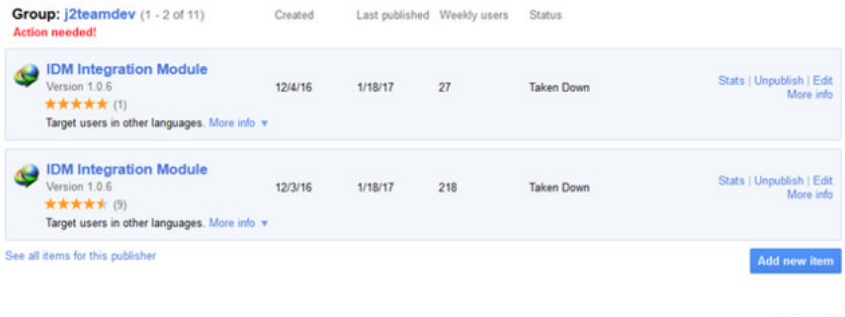
Security experts discovered that the line appropriated bank accounts, Facebook, Gmail ... very large in Vietnam, you can also be a victim

Many types of accounts, from bank accounts to website administration accounts.

Follow the crime track

Recently, in the process of strengthening the security of the company's system, a group of security experts from the Information Security department under VCCorp happened to find and trace the trail of an information-hijacking line. large scale in Vietnam. By taking advantage of the web browser, this group of hackers has a lot of account information in the system of many large organizations.

Specifically, on June 21, when an unusual sign was found in an admin account on a familiar website, the security team immediately went to the cause. After performing many business measures, they determined: account information was stolen from this employee's personal computer, by a malware in the form of extension (extension) on Chrome browser.



Malicious extension pretending to be Internet Download Manager has been around for a long time on the Chrome Web Store.
Note: the author's name for this extension has been confirmed as fake, the goal is currently being clarified.

The amount of stolen information is unprecedented

Notably, this is an extension to replicate IDM extension - Internet Download Manager is very popular in Vietnam, can be used on the top 2 browsers Google Chrome and Coc Coc. Although not strange with this form of fraud, but the sophistication and professionalism in the way of action as well as the victim is Vietnamese, the experts have continued to trace very small traces. The results really surprised the group of experts - even though they were used to the world of cyber security many events.

Row	username	password	url
1	08A43	1110	https://www.vietcombank.com.vn/IBanking2015/55c3c0a782b739e063efa9d5985e2ab4/Account/Login
2	9A30	2501	https://www.vietcombank.com.vn/IBanking2015/55c3c0a782b739e063efa9d5985e2ab4/Account/Login
3	07A19	1971	https://www.vietcombank.com.vn/IBanking2015/55c3c0a782b739e063efa9d5985e2ab4/Account/Login
4	a43	hctc	https://www.vietcombank.com.vn/IBanking2015/55c3c0a782b739e063efa9d5985e2ab4/Account/Login
5	7E56	4090	https://www.vietcombank.com.vn/IBanking2015/55c3c0a782b739e063efa9d5985e2ab4/Account/Login
6	6A36	2504	https://www.vietcombank.com.vn/IBanking2015/55c3c0a782b739e063efa9d5985e2ab4/Account/Login
7	60a27	thon	https://www.vietcombank.com.vn/IBanking2015/55c3c0a782b739e063efa9d5985e2ab4/Account/Login
8	60a27	thon	https://www.vietcombank.com.vn/ibanking2015/55c3c0a782b739e063efa9d5985e2ab4/account/login
9	9A55	!binh	https://www.vietcombank.com.vn/IBanking2015/55c3c0a782b739e063efa9d5985e2ab4/Account/Login
10	2e53	Sam	https://www.vietcombank.com.vn/IBanking2015/55c3c0a782b739e063efa9d5985e2ab4/Account/Login
11	32A35	Thao	https://www.vietcombank.com.vn/IBanking2015/55c3c0a782b739e063efa9d5985e2ab4/Account/Login
12	3A21	Dang	https://www.vietcombank.com.vn/IBanking2015/55c3c0a782b739e063efa9d5985e2ab4/Account/Login

Hackers have captured a large amount of electronic accounts, including Vietcombank accounts

According to preliminary statistics, this hacker group has stolen login information (Username / Password) of about 55,000 Facebook accounts, 6,000 Google accounts, 5,000 Yahoo accounts and the most frightening is over 5 million cookies of universal pages. variables like Facebook, Google Mail, Yahoo Mail, Hotmail or even PayPal. With the hacker group owning cookies, if you are careful to use the 2-layer security feature, please give condolences, they can still completely take over your rights.

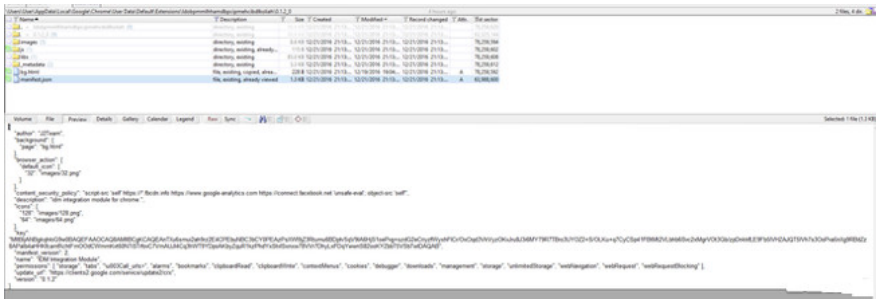
Row	username	password	url
2	trungnn3		https://mail.bidv.com.vn/owa/auth/logon.aspx?replaceCurrent=1&reason=2&url=https%3a%2f%2fmail.bidv.com.vn%2fowa%2f
3	040451		https://onepay.vn/onecomm-pay/bidvauth_submit.op
4	lantn		https://mail.bidv.com.vn/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.bidv.com.vn%2fowa%2f
5	Vietnt3		https://mail.bidv.com.vn/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.bidv.com.vn%2fowa%2f
6	Vietnt3		https://mail.bidv.com.vn/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.bidv.com.vn%2fowa%2f
7	trungnn3		https://mail.bidv.com.vn/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.bidv.com.vn%2fowa%2f
8	ngocn		https://mail.bidv.com.vn/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.bidv.com.vn%2fowa%2f
9	ngocnd		https://mail.bidv.com.vn/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.bidv.com.vn%2fowa%2f
10	113720		https://onepay.vn/onecomm-pay/bidvauth_submit.op
11	545764		https://onepay.vn/onecomm-pay/bidvauth_submit.op
12	586743		https://onepay.vn/onecomm-pay/bidvauth_submit.op
1	sonnx1		https://mail.bidv.com.vn/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.bidv.com.vn%2fowa%2f

Many banking customers are also victims of hackers

Experts also note that this type of malware has existed for a long time but has not been captured by antivirus software and prevented because of mischief in the mode of infection. Users can "accidentally" infect this malware via two main routes:

1. Infection through the release of pirated software (crack):

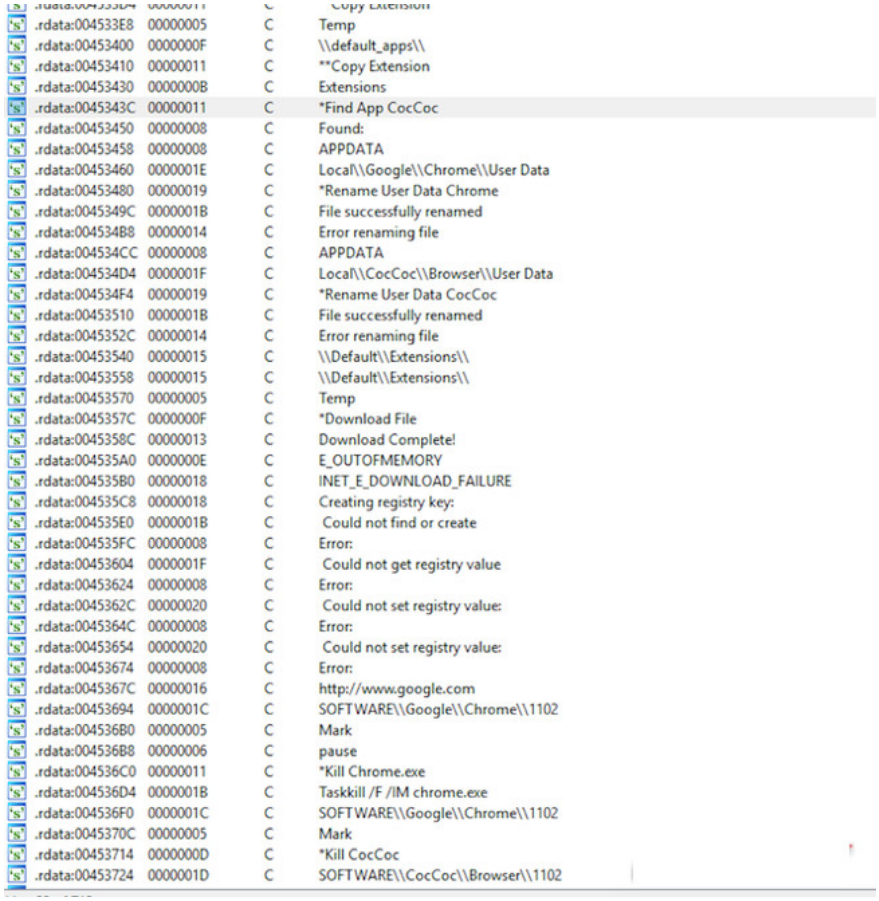
When users download pirated software from any website (uploaded by hackers), in the crack file will attach a task execution file in the following order: turn off the browser (Chrome / Coc Coc) if running , create a connection to the extension page and finally download the extension and install it in the victim's computer.



The log logs that the executable file automatically downloads and installs the extension.

2. Using curious links (links):

Previously, by circumventing the law, hackers have posted 11 different versions of this fake extension on the Chrome Web Store. Hackers will spread many curious links, the victim after clicking will get invited to install a "plugin" (to see the content, to use the web faster, etc.). Because the extension exists on Chrome Web Store properly, most users will accept the installation.



.rdata:004533E8	00000005	C	Temp
.rdata:00453400	0000000F	C	\\default_apps\\
.rdata:00453410	00000011	C	**Copy Extension
.rdata:00453430	0000000B	C	Extensions
.rdata:0045343C	00000011	C	*Find App CocCoc
.rdata:00453450	00000008	C	Found:
.rdata:00453458	00000008	C	APPDATA
.rdata:00453460	0000001E	C	Local\\Google\\Chrome\\User Data
.rdata:00453480	00000019	C	*Rename User Data Chrome
.rdata:0045349C	0000001B	C	File successfully renamed
.rdata:004534B8	00000014	C	Error renaming file
.rdata:004534CC	00000008	C	APPDATA
.rdata:004534D4	0000001F	C	Local\\CocCoc\\Browser\\User Data
.rdata:004534F4	00000019	C	*Rename User Data CocCoc
.rdata:00453510	0000001B	C	File successfully renamed
.rdata:0045352C	00000014	C	Error renaming file
.rdata:00453540	00000015	C	\\Default\\Extensions\\
.rdata:00453558	00000015	C	\\Default\\Extensions\\
.rdata:00453570	00000005	C	Temp
.rdata:0045357C	0000000F	C	*Download File
.rdata:0045358C	00000013	C	Download Complete!
.rdata:004535A0	0000000E	C	E_OUTOFMEMORY
.rdata:004535B0	00000018	C	INET_E_DOWNLOAD_FAILURE
.rdata:004535C8	00000018	C	Creating registry key:
.rdata:004535E0	0000001B	C	Could not find or create
.rdata:004535FC	00000008	C	Error:
.rdata:00453604	0000001F	C	Could not get registry value
.rdata:00453624	00000008	C	Error:
.rdata:0045362C	00000020	C	Could not set registry value:
.rdata:0045364C	00000008	C	Error:
.rdata:00453654	00000020	C	Could not set registry value:
.rdata:00453674	00000008	C	Error:
.rdata:0045367C	00000016	C	http://www.google.com
.rdata:00453694	0000001C	C	SOFTWARE\\Google\\Chrome\\1102
.rdata:004536B0	00000005	C	Mark
.rdata:004536B8	00000006	C	pause
.rdata:004536C0	00000011	C	*Kill Chrome.exe
.rdata:004536D4	0000001B	C	Taskkill /F /IM chrome.exe
.rdata:004536F0	0000001C	C	SOFTWARE\\Google\\Chrome\\1102
.rdata:0045370C	00000005	C	Mark
.rdata:00453714	0000000D	C	*Kill CocCoc
.rdata:00453724	0000001D	C	SOFTWARE\\CocCoc\\Browser\\1102

This extension has many rights that can be abused on bad and unnecessary.
Here the hacker continues to take another name in the author section.

How hackers can upload up to 11 different versions of this malicious extension and overcome many security tools, due to the framework of a limited article, we will provide details for you. read on the next lesson. Going back to the incident, this extension after being installed will steal the victim's login information when accessing all websites, as well as recover all user cookies sent to the hacker server.

So when you read this article, readers should immediately take the following steps, especially when you find yourself having the same behavior as what is mentioned in the 2 ways of infection above:

1. Check the extensions in your computer browser, you can use the same tools as in this article.
2. If there are suspicious signs such as using unnecessary permissions at any extension, erase it.You can refer to the meaning of extension permissions at this address .
3. Change all passwords in all your electronic accounts.

At the same time as checking your computer, readers should actively share this information to those around you, especially those with little knowledge of technology. Don't let bad guys take over people's information, or use them to serve more dangerous purposes.

We will give detailed information on how security experts find out the culprit group in the next articles. Looking forward to your attention.

Follow genk