Introducing Cheng Feng

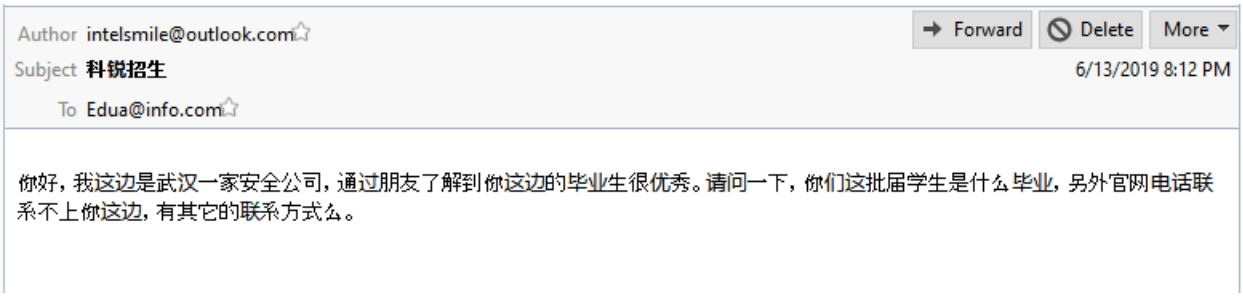
intrusiontruth ⋮⋮ 5/16/2023

You might be wondering why we have picked on Cheng Feng. Just a hard-working cyber security professional, right? Well, wrong, as it turns out. Cheng Feng helped us deduce what APT Wuhan Xiaoruizhi is a cover for.

As regular readers will know, Intrusion Truth is nothing without its global network of supporters. We had to reach out for support investigating Cheng Feng using the start points from his insurance certificate, and one of our collaborators came through with the goods. A cache of emails, documents, and photos from a cloud storage account belonging to Cheng.

Let's start here:

On 14th June 2019, Mr. Cheng sent an email to an address he believed to belong to the Kerui Cracking Academy. He described himself as a security company in Wuhan who had heard that Kerui's graduates were excellent, and asking when the next graduation date was. Well, well, well. It looks like our suspicions of Kerui were correct: not only have several Kerui graduates gone on to Wuhan Xiaoruizhi, we also now have Xiaoruizhi employees attempting to snap up their graduates. Looks like Kerui might be a pipeline into Xiaoruizhi after all.

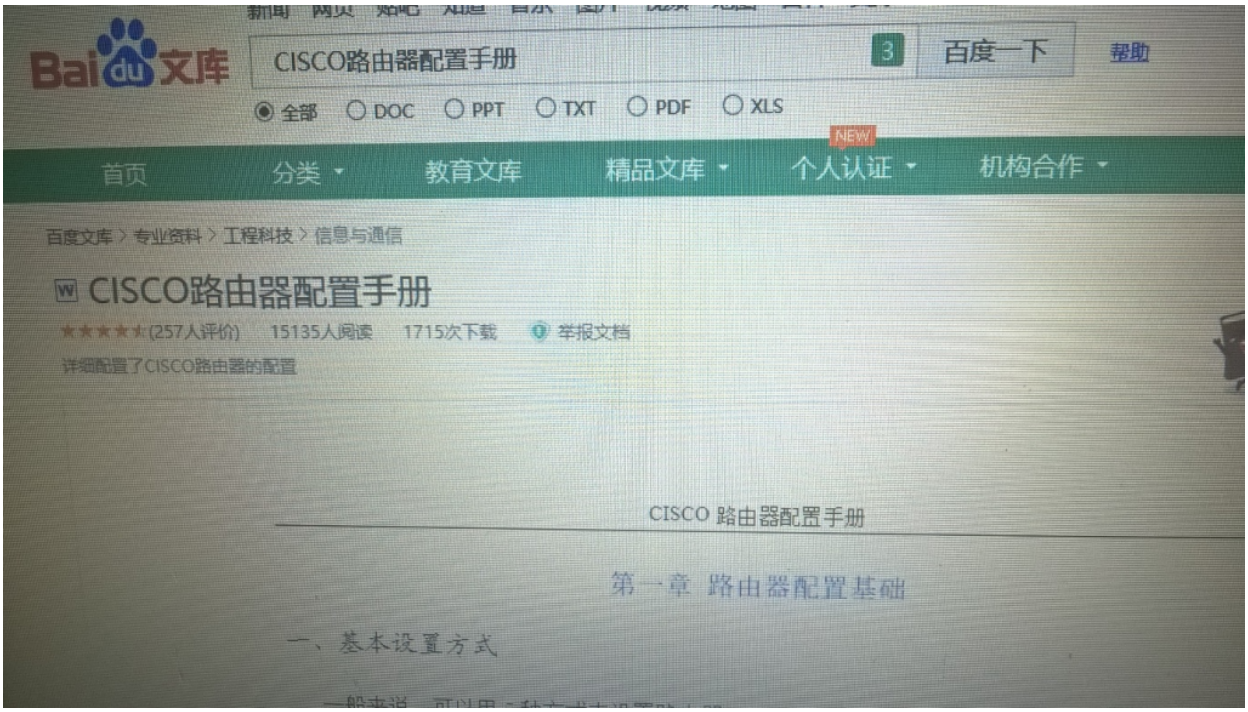


Let's continue.

A deeper dive into Cheng's documents revealed the beginnings of overlap between his apparent research interests and those of APT 31.

CISCO router exploitation:

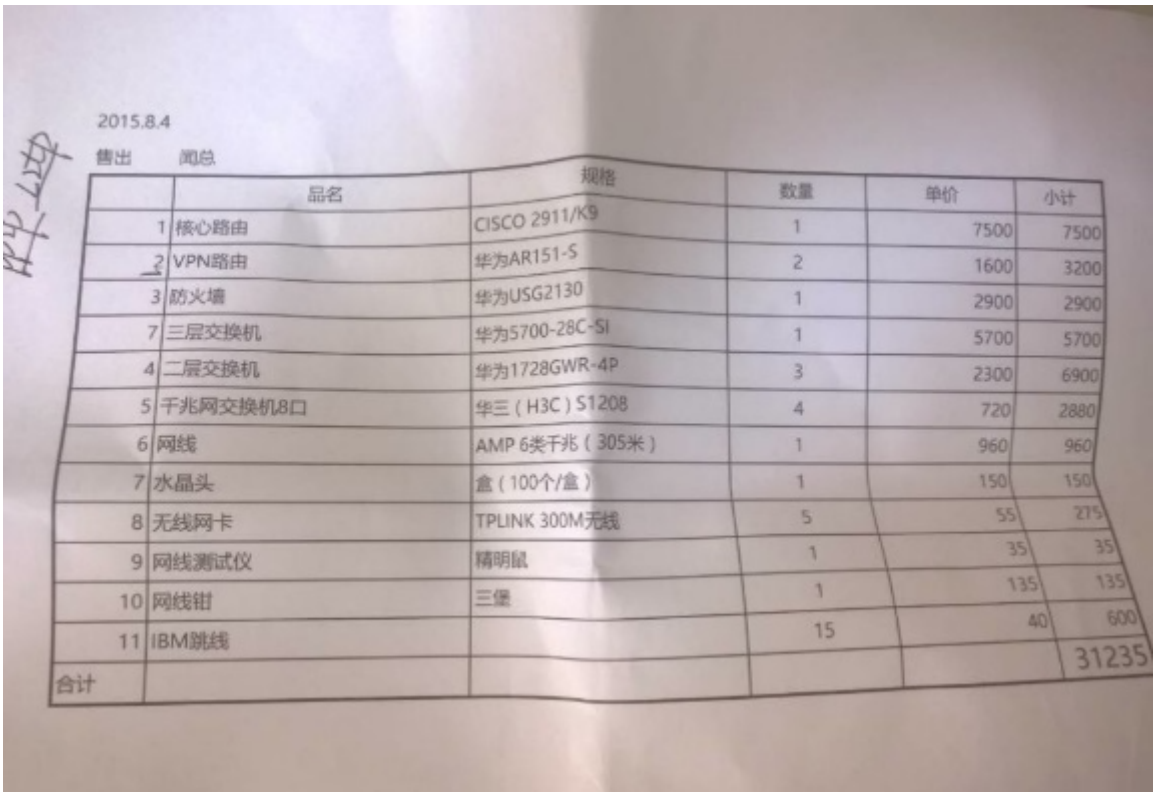
He we have Cheng, presumably in the course of his work duties, accessing the configuration manual for Cisco broadband routers.



Cheng Feng's document cache contains a number of indications of him being in possession of, or purchasing, or testing configurations of possible router exploitation on, varying different models of routers, including small office/home office (SOHO) routers, including Huawei Echolife, Huawei AR151-S, Cisco 2911/K9, and Cisco 1721 routers.


WARRANTY VOID
IF SEAL IS BROKEN
请勿自行拆封
SN:2102310QWADMF6000314
AR161-S
HUAWEI
型号 Model: AR151-S
名称 Name: 接入路由器 Access Router
电源额定值 POWER RATING: 12 V; 2.0 A


HUAWEI
EchoLife HG8120C
PROD ID: 2150062654EGF6080758
(23S)MAC : 88A2D7C6B3A0-A8(9)
(30S)PON No: 48575443C6B3A042(HWTCC6B3A042)
DATE: 2015/06



2015.8.4

售出 闻总

	品名	规格	数量	单价	小计
1	核心路由	CISCO 2911/K9	1	7500	7500
2	VPN路由	华为AR151-S	2	1600	3200
3	防火墙	华为USG2130	1	2900	2900
7	三层交换机	华为5700-28C-SI	1	5700	5700
4	二层交换机	华为1728GWR-4P	3	2300	6900
5	千兆网交换机8口	华三（H3C）S1208	4	720	2880
6	网线	AMP 6类千兆（305米）	1	960	960
7	水晶头	盒（100个/盒）	1	150	150
8	无线网卡	TPLINK 300M无线	5	55	275
9	网线测试仪	精明鼠	1	35	35
10	网线钳	三堡	1	135	135
11	IBM跳线		15	40	600
合计					31235

Bottom image reads: sold by Chief Wen 2015.8.4

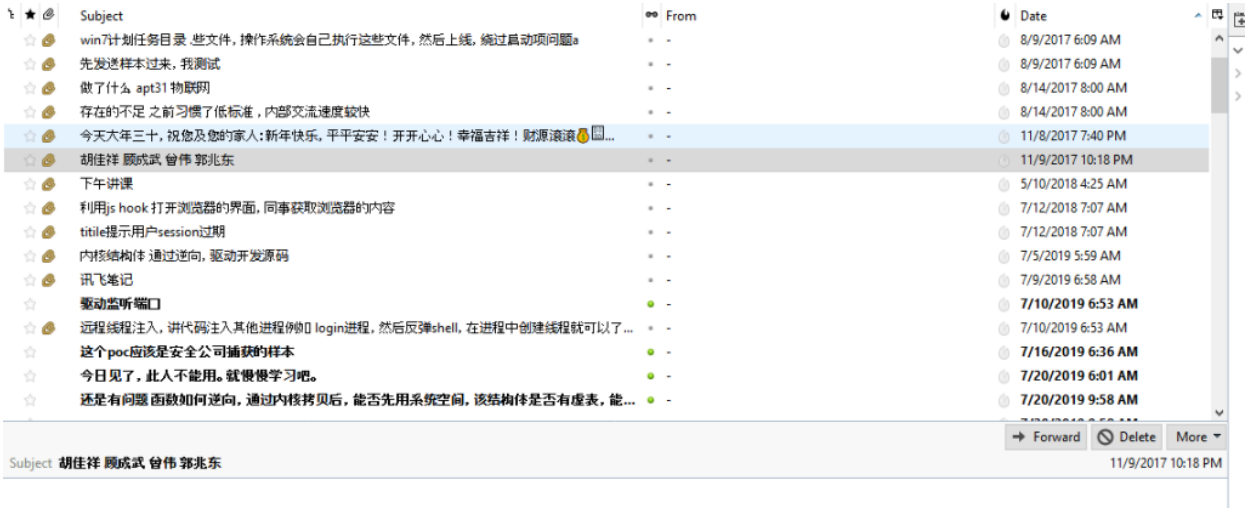
- 1 Service Router: CISCO 2911/K9
- 2 VPN Routers Huawei: AR151-5
- 1 Firewall: Huawei USG2130
- 1 Layer 3 Switch: Huawei 5700-28C-SI
- 3 Layer 2 Switches: Huawei 1728GWR-4P
- 4 Gigabit Network Switches: 8 Huasan (H3C) S1208
- 1 Network Cable: AMP Cat 6 GB (305M)
- 1 RJ Connector: Box (100 piece/box)
- 5 Wireless NICs: TPLINK 300M Wireless
- 1 Network Cable: Tester Wire Tracer
- 1 Network Plier: Sanbao Brand
- 15 IBM jumpers

APT31 is famous for router exploitation. APT31 hit the press in France over summer 2021, accused by the French cyber security agency of launching a major hack targeting French entities which utilized a network of more than 1000 compromised routers, including Pakedge, Sophos and Cisco routers. These routers were compromised and leveraged as anonymization relays, before APT31 carried out reconnaissance and attack activities. The listed devices in particular are SOHO routers, which APT31 have been exploiting since at least November 2019.

So – here we have Cheng in possession of a manual for Cisco routers and in possession of a number of different SOHO router devices. Could have been his process to begin learning to exploit them?

APT IoT

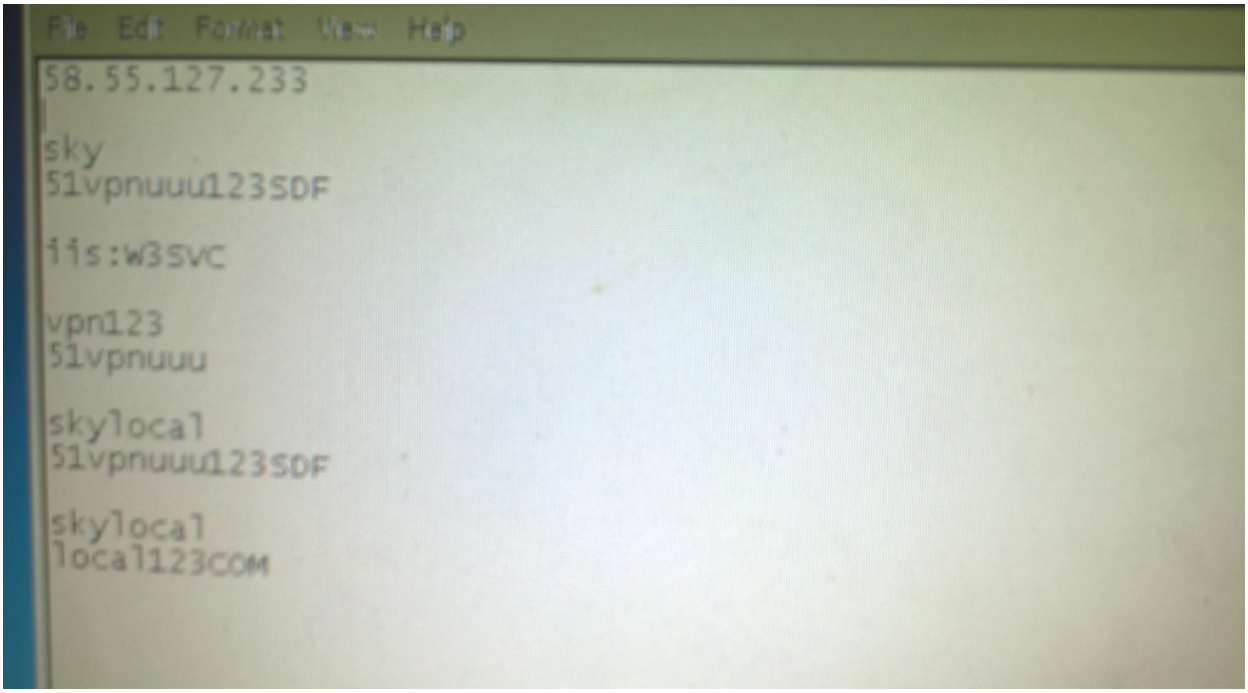
Next. In August 2017, Cheng created a task intriguingly labelled “做了什么 apt31 物联网”, or ‘what did APT31 IoT do’/’what did APT 31 do with regards to IoT’.



We know from our previous discussion that APT31 is known to exploit IoT devices, in particular SOHO routers, to form part of their operational infrastructure. And APT31 is clearly on Cheng’s mind. In addition, the timing of the task in August 2017 was prior to public exposure of APT31’s involvement in IoT/router exploitation, indicating that Cheng had insider knowledge of APT31’s TTPs. Perhaps because he is APT31?

Clibcom

We’ll leave you with one more clue which we think rounds things out nicely. Mr. Cheng also had in his possession a 2015 photo of a computer screen showing usernames and passwords for 58.55.127.233.



On investigating this domain, we discovered that it’s hosted in Wuhan. From March 2015, it hosted webmail.dnsapple.com, and later hosted Clibcom.com from 2017. An industry source told us that clibcom.com was previously attributed to APT31. Can anyone help us verify this?

We are pretty confident that Cheng is affiliated with APT31. He has material indicating his interest in Cisco and SOHO router exploitation, known TTPs of APT31. Notes on his phone indicate he is thinking about APT31 and, presumably, their exploitation of IoT devices, *and* he has the log in credentials for an IP which a source has attributed to APT31.

Overall, things are heating up. We've linked the hacking school to the MSS via its owner. We've linked the hacking school to Xiaoruizhi via its employees and its poaching of graduates. And we have enough information to tentatively link Xiaoruizhi in turn to APT31. But, there's one missing link. The MSS.