



# Chinese Hacker Groups

Author: Sandra Watson Parcels (Research Assistant, ICT)

Supervisor: Ariel Levanon

June 2018

# Table of Content

<b>Table of Content</b>	2
<b>Executive Summary</b>	3
<b>Introduction</b>	5
<b>Main Research Questions</b>	7
<b>Chapter One</b>	8
<b>Chapter Two</b>	13
1. APT1 aka PLA Unit 61398, Comment Crew, Shanghai Group, Byzantine Candor, 61398 Budui.	13
2. APT3 aka UPS Team, Gothic Panda, Buckeye, TG-0110	17
3. NCPH (Network Crack Program Hacker)	18
4. Honker Union of China (HUC) aka Hongke (Red Guest), Red Hacker Alliance/Red League.	19
5. APT10 aka MenuPass Team, Stone Panda, Red Apollo	22
6. Bronze Butler aka Tick, REDBALDKNIGHT	25
7. KeyBoy	26
8. Elderwood Group aka Elderwood Platform, Elderwood Project, Elderwood Gang.	27
9. Hidden Lynx	30
10. APT12 aka Calc Team, DynCalc, DNSCALC, Numbered Panda.	32
11. DragonOK.	33
12. Moafee.	35
13. APT16	36
14. EvilPost	37
15. Danti	38
16. SVCMONDR	39
17. China Girl Security Team aka CN Girl Security Team.	40
18. APT27 aka Emissary Panda, Threat Group 3390, LuckyMouse, Bronze Union.	41
19. APT17 aka Deputy Dog, Tailgator Team, Voho, Group72, AuroraPanda.	43
20. APT18 aka Wekby, Dynamite Panda, TG-0416.	45
21. APT19 aka Codoso Team, Sunshop Group.	46
22. Shell Crew aka Deep Panda, Black Vine, WebMasters, KungFu Kittens, PinkPanther.	48
23. APT30	50
24. Winnti Group aka Winnti Umbrella, Wicked Panda, LEAD, Barium, GREF, PassCV.	52
<b>Bibliography</b>	54

## Executive Summary

Cyberspace is the newest theater of operations with China fighting for command. Chinese hacker groups have become professional, strategic, and operate with improved tactics. They once were considered very bold with little regard for operational security, but now they are strategically controlled. In general, hackers have various motivations, but the majority of Chinese hackers are nationalistic and are either working directly for, or on contract with, the Chinese government. Research findings strongly indicate the majority of Chinese hacker groups listed are connected to the Chinese Liberation Army (PLA), Strategic Support Force (SSF), Chinese intelligence, and/or on contract with the Chinese government. There is not one group on the list without ties or suspected ties to the Chinese government. As a researcher it was difficult to find details on many of the group's leaders, group structures and forum activity but the use of overlapping resources and consistent target countries reveals a common main actor profile. It is also important to recognize these groups are most likely not completely separate entities. They either work together or stop using one group when the group is identified and move to a new alias. This means when a group is not active, it does not mean the actors are no longer active. Rather, the actors have moved under a different group and/or name. Therefore, it may be most productive in searching and targeting Chinese hacker groups to focus on individual actors and their links to the Chinese government. Target countries are consistently Western and Asian countries that are perceived as a threat politically and industrially to the Chinese government. The United States by far is the largest targeted country, being targeted by almost every group. Other western countries, as well as Taiwan and Japan, are also highly targeted. Primary targets are political and industrial with the strongest focus on intellectual property. Within the intellectual property targeted, the primary target is defence technology and then other high-tech sectors.

In analysing the list of Chinese hacker groups, the list can be identified as *Priority 1 Groups*, *Priority 2 Groups*, and *Priority 3 Groups*.

*Priority 1 Groups* are groups one (APT1) and ten (APT12), which are connected, linked to the PLA and commit cyber-espionage. Its capabilities indicate a large group, focused primarily on targets of defence technology, including the Israeli Iron Dome system, United States, Taiwan, and Japan defence and high-tech sectors. Group two (APT3) is considered one of the most sophisticated Chinese hacker groups and is connected to China's tech giant, Huawei. Group five (APT10) targets

a broad range of countries and target industries, is suspected to be state funded, and conducts cyber-espionage. Groups eight (Elderwood Group) and nine (Hidden Lynx) are connected, target a broad range of industries including defence and multiple industrial sectors. It is known to be quiet in strategy and are suspected to be state funded. Groups eleven (DragonOK) and twelve (Moafee) are connected, suspected to be state funded, target a broad range of targets, especially the defence sector and politically on the South China Sea dispute. Group eighteen (APT27) is suspected to be state funded, highly sophisticated and targets USA, Asian defence, and European drone technology. Groups twenty (APT18), twenty-one (APT18), and twenty-two (Shell Crew) are connected, suspected to be state funded and perform cyber-espionage. It targets a broad range of countries and target industries including defence, high tech, and biotechnology. It are also suspected of targeting Daesh in Iraq in 2014 to protect oil interest in the region. Group twenty-four (Winnti Umbrella) has been identified as Chinese intelligence with high confidence. It has been active over a long period and it's main targets are political, including the USA, Tibet, Japan, and South Korea.

*Priority 2 Groups* are groups three (NCPH) which hacked the Pentagon several times in 2006, is known for its expertise in surveillance and is suspected to be PLA. However, there is no evidence of recent activity. Group thirteen (APT16) is suspected of being state funded, conducts cyber-espionage and targets Taiwan and Japan. Group fourteen (EvilPost), fifteen (Danti), and sixteen (SYCMONDR) are connected, are suspected of being state funded and targets are mainly industrial, with a focus on South and Central Asian countries. Group nineteen (APT17) targets the United States political and industrial targets including defence and technology.

*Priority 3 Groups* are group four (Honker Union of China) that has targets who are primarily political and focuses on the USA, Japan, Vietnam, and the Philippines. Group six (Bronze Butler) targets are Japan's industrial sector and some political targets. It is linked to the Chinese government and may hire out to steal technology. Group seven (KeyBoy) is known to have medium level expertise and targets are political and industrial, with a focus on Tibet, Taiwan, the Philippines, and the West. Group seventeen (China Girl Security Team) has targeted the USA and has targets that include the White House and Google. This group hasn't been linked to any recent activity. Group twenty three (APT30) is suspected of being state funded and has targeted SE Asian countries - members of ASEAN. Is not linked to recent activity.

The overall objective summarized from the data collected in this project is that Chinese hacker groups are mainly under the direction of the Chinese government. Their goals are to steal

intellectual property, focusing primarily in defence and other emerging technology, in order to further develop Chinese industry and advance Chinese military, political, and technological status.

## Introduction

Cyberspace is a rapidly increasing battlefield of conflict globally. Until recent years, Chinese cyber criminals, although very present on the dark net, lacked both structure and professionalism. Chinese hacker groups were known for sweeping up vast amounts of varying information, whereas Russian groups are known for being more specific and able to hide their tracks more efficiently. However, this is changing rapidly. Chinese hacker groups have become more strategic and operate with improved tactics. Where they once were considered very brash with little regard for operational security, now they are more strategically controlled. Hackers in general are nation-state actors, groups of hackers, lone hackers and criminal organizations. The majority of Chinese hackers are believed to be nationalistic and are either working directly for or on contract with the Chinese Government. Chinese nationals are culturally nationalistic and the Chinese government has controls on internet access, therefore Chinese hackers are less likely to hack solely for personal financial gain. In 2015, China and the United States signed a cyber agreement which was intended to reduce Chinese industrial espionage attacks on the United States. In 2016, the head of the Federal Bureau of Investigation (FBI) counterintelligence, Randall Coleman stated there was a 53% increase in the theft of United States trade secrets. In 2017, it was estimated, that intellectual-property theft costs United States alone, up to \$600 billion a year and that the Chinese are responsible for most of the loss. In March 2018, the Trump Administration revealed plans for import tariffs on Chinese products in what is said to be retaliation for decades of state-backed intellectual property theft.

The Chinese government, under President Xi is an increasingly dangerous force. President Xi is playing on rising nationalism in China and has the support of the People's Liberation Army (PLA). His recent policy changes in the industrial sector reveal his concern for control of privately-owned companies, and especially foreign-owned companies. These policy changes involve stopping or reducing production in private and state-owned factories. The reasoning given for stopping or reducing production is to implement environmental controls. However, some plants already have top-of-the-line environment controls. Sources at one factory with high-end equipment did not say what occurred or what was being installed during production reduction when there were no environmental controls to implement. The Chinese government did not target all state-owned

factories at first, even though environmental controls are poor to non-existent in many of them. However, by late 2017, production was being reduced by one-third to two-thirds in state-owned factories as well, with the same reason being environmental controls. Chinese strategy as understood through personal experience, would suggest the shutdowns were a threat to factories to cooperate with the new tightened control policies. As much as some controls could be solely environmental in nature, it is most likely connected to the control and power the government is attempting to regain in the industrial sector. Once the factory is sufficiently threatened, an offer to compromise will be made. This compromise, as of recently, entails putting a communist party member in each privately owned and state owned factory, including foreign-owned. This party member is given the title of Party Secretary, must be invited to every meeting and all major decisions of the corporation, must go through him/her. In essence, the Party Secretary has been given veto power. The Party Secretary also has access to all computers/networks in the corporation. Therefore, even if the corporation is private and foreign owned, the Chinese government has access to all its data, including intellectual property. Therefore, it would be advisable for corporations to not keep research and development data in Chinese offices or connected to Chinese offices, or the Chinese government will attain it. It is important to be aware, the Chinese government will always intervene physically or through cyber activity if it feels its' control, reputation or nationalist agenda is being threatened with little to no regard for ethics or morality.

A source recently advised of continued Chinese security services recruitment tactics to coerce Chinese nationals abroad. The source advised of accounts in Canada where the Chinese government approaches Chinese Canadians to perform one act of espionage with the approach of helping their homeland. The act usually entails doing something “small” like copying a set of blueprints or a thumb drive from their place of employment. If the individuals refuse, their families in China will receive a visit from Chinese security services. The first visit is always friendly but the family is aware of what is happening and the underlying threat (Chinese double-talk). The subsequent visits are not so friendly. This type of recruitment in diaspora communities has been occurring for many years. As long as an individual has ties in China, there is potential leverage for the Chinese government to exploit. With the vast population of China, and increasing number of Chinese nationals abroad, this risk will only increase exponentially and directly affect cyber security.

How does the world counter this increasing Chinese cyber threat? How do the political, industrial and academic sectors defend and protect intellectual property? How do security agencies combat these cyber criminals? The first step is to identify the threats, the main actors and their connections

to the Chinese government. Then, analysis their group structures, targets, strengths & weaknesses, and the forums they utilize.

## Main Research Questions

1. Identify the forums Chinese hackers use?
2. Identify the main Chinese hacker groups?
3. Identify the main actors/leaders and structure in each Chinese hacker group?
4. Identify if Chinese hackers groups are government entities, on contract with the government or civilians?
5. What are the Chinese groups main targets?
  - Political** - which governments? military espionage ie: weapons, aircrafts?
  - Industrial** - which businesses? ie: aerospace and armoments, medical equipment, pharmaceuticals?
  - Academic** - which universities? which fields of study ie: engineering, medicine?
6. What countries do Chinese hacker groups target?
7. What are the Chinese hacker groups tactics, techniques, procedures (TTP's), capabilities, limitations and vulnerabilities (how are they funded, software/hardware used, frequent specific forums, habits, weaknesses)?
8. What connections are there between forums, hacker groups, and actors?



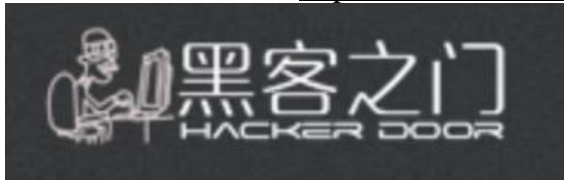
## Chapter One

### Identify Forums Chinese Hackers Use

Chinese hackers have, in the past, been less organized and professional than Russian hackers. Instead of building their own systems, many Chinese cyber-criminals started establishing themselves on forums and shops within the Russian underground. Chinese choose Russian systems because their markets have comparatively loose standards. They usually accept registration for users who don't speak Russian or English. Cyber criminals generally have full digital storefronts where they sell stolen credit cards and data. They stood in stark contrast to the high level Russian underground economy until 2015, when it became evident Chinese cybercrime underground was maturing and branching out internationally. Chinese cyber criminals often still use forums of direct communication for one-off data. They used Baidu Tieba and QQ Messenger to sell stolen goods. Sometimes Chinese cyber criminals would post ads for cyber crime on random forums. Chinese state hackers have primary allegiance to China and sell stolen information on the side part-time through secretive marketplaces they have created and/or are using.

#### Chinese Forums

- Hacker Door Forum - <http://www.hackerdoor.com>



- <http://www.hackercn.com/forum.php>



- Evil Octal Forum - <https://forum.eviloctal.com/>





- Roots Web Safe Team - <http://www.sh3llc0de.com/forum.php>



- 52Poie Forum (Love to Decipher/Reveal )(Wu Ai Po Jie) - <https://www.52pojie.cn/>



- Mersion Community - <http://www.vcccc.cn/>



- Network College Forum - <http://www.365cmd.com/forum.php>



- Safety Dragon - <http://www.anquanlong.com/>



- China Hacking Forum - <http://www.hackerbbs.cc/>



- 2cto - Red Black United (Hong Hei Lian Meng) - <https://bbs.2cto.com/>

**2cto** ★★★★★  
217,706 posts • Active since 1970 • Online

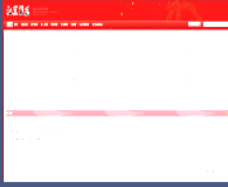
Site Details   Top 5 Actors

Description  
Chinese hacking forum

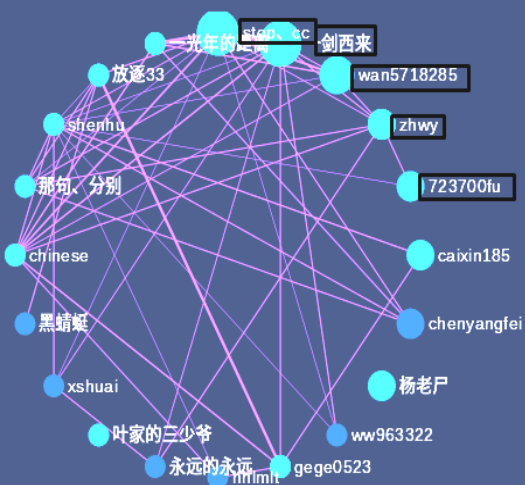
Language  
Chinese

Type  
Forum (closed)

Access  
Clear Web



**Social Network**



- Technology House of Enchantment - <https://www.0xaa55.com/>



- Zero Day Security Forum - <http://www.jmpoep.com/>



- Watch Snow Safety Forum - <https://bbs.pediy.com/>



- Dragon (Long Tian) Forum - <https://www.lthack.com/>



- Piaoyun Pavillion Safety Forum - <http://www.chinapyg.com/>



- 01 BinVul - Binary Vulnerability Research - <http://www.binvul.com/>



- CDlinux Forum - <http://cdlinux.net/>



- CYWL Team - Cheng Yin Network Forum - <http://www.chinacycc.com/portal.php>
- China Honker Army Forum - Top Five Actors boxed below. <http://www.cnhonkerarmy.com>

### cnhonkerarmy ★★★★★

510,314 posts • Active since 2010 • Online


Site Details [Top 5 Actors](#)

**Description**  
Chinese forum named "China Honker Army", sharing hacking and technical knowledge and tools.

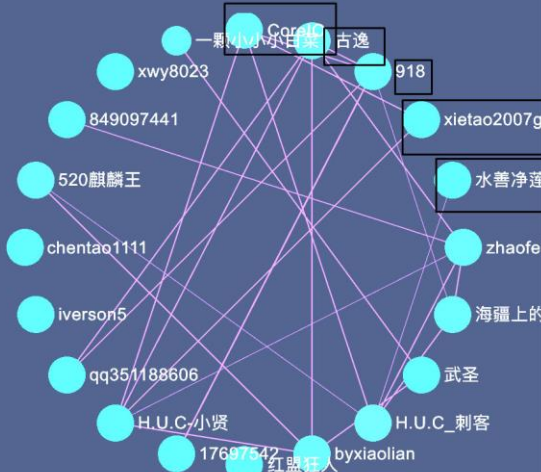
Language  
Chinese

Type  
Forum (closed)

Access  
Clear Web



### Social Network



- Deep Web Chinese Forum

### Deep Web Chinese ★★★★★

525,472 posts • Active since 2017 • Online


Site Details [Top 5 Actors](#)

**Description**  
General criminal forum with few different topics: hacking, carding, drugs, money laundering and fraud.


Language  
Chinese

Type  
Forum (closed)

Access  
Dark Web



### Social Network



- End of the World (Tianya) Club Forum - <http://www.tianya.cn/>



- HDHacker

- Black Hat Hacker Training Base
- cctry Forum - Top five actors boxed below.

**cctry** ★★★★★  
 666,027 posts • Active since 2009 • Offline


Site Details    Top 5 Actors

Description  
 Chinese forum with a vast coding section

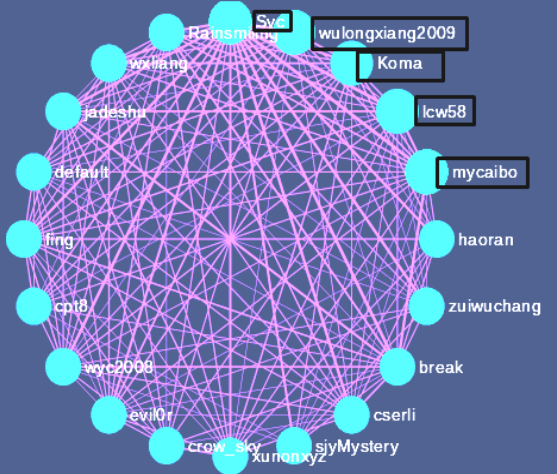
Language  
 Chinese

Type  
 Forum (locked)

Access  
 Clear Web



**Social Network**



- Chinese DarkNet Forum

**chinesedarknet** ★★★★★  
 12,758 posts • Active since 2014 • Offline

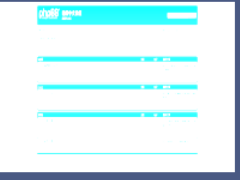
Site Details    Top 5 Actors

Description  
 Chinese darknet fraud forum

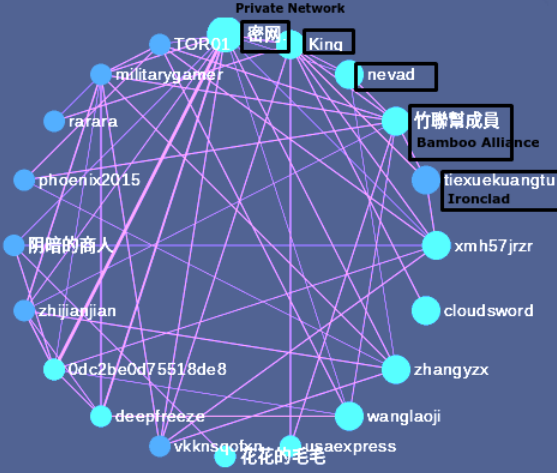
Language  
 Chinese

Type  
 Forum (locked)

Access  
 Dark Web



**Social Network**



- Freedom Kingdom

**freedomkingdom** ★★★★★

4,556 posts • Active since 2017 • Offline

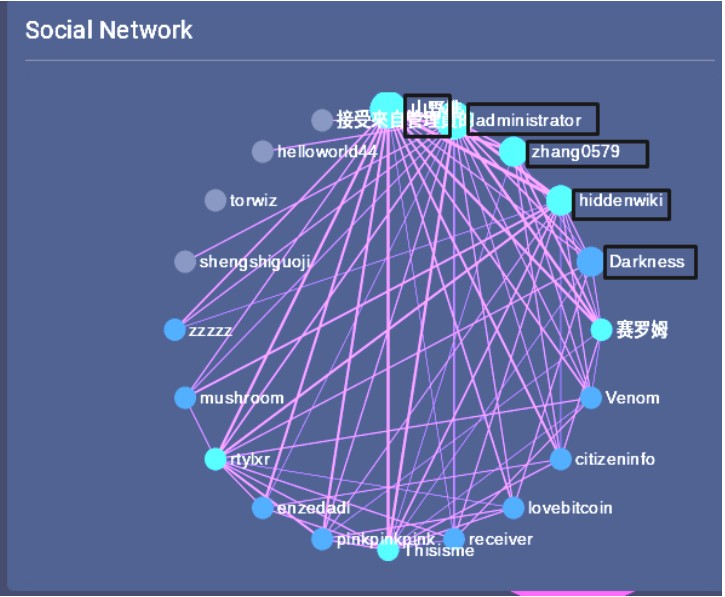
Site Details    Top 5 Actors

**Description**  
 A Chinese underground forum, contains hacking, carding, drugs, fraud and hitman sections.

**Language**  
 Chinese, Unknown

**Type**  
 Forum (closed)

**Access**  
 Dark Web

## Chapter Two

### List of Chinese Hacker Groups

#### 1. APT1 aka PLA Unit 61398, Comment Crew, Shanghai Group, Byzantine Candor, 61398 Budui.

Operating since: 2005.

Main actors/leaders and structure

# WANTED BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets



Huang Zhenyu    Wen Xinyu    Sun Kailiang    Gu Chunhui    Wang Dong

Huang Zhenyu (黄振宇)

Wen Xinyu (文新宇)

Sun Kailiang (孙凯亮)

Gu Chunhui (顾春晖)

Wang Dong (王东).

-The main actors/officers listed above have been indicted by the United States for theft of business property and intellectual property from American companies and for planting malware.

**Government entities, on contract with the government or civilians**

-Suspected to be members of the Second Bureau of the People's Liberation Army's General Staffs Departments (GSD) Third Department and work out of a 12 storey white building on Datong Road, Pudong, Shanghai.

-American intelligence agencies and private security firms are tracking over 20 hacker groups linked by unique digital signatures to PLA Unit 61398 and are suspected to be contractors for PLA Unit 61398. One of the largest of these groups is Comment Crew. Comment Crew received its name because it imbeds comments or hidden code into web pages.

**Chinese groups main targets: Political, Industrial, Academic, International Organizations.**

**Political** - Government databases including public administration.

Connected to 2011-2012 hack of Israeli Iron Dome System. Hacked documents pertaining to Arrow III missiles, drones and ballistic rockets.

# Chinese Hackers Stole Blueprints of Israel's Iron Dome Missile Defense System



VOLKOV | 7/29/2014, 12:00:00 AM post

Chinese Hackers Stole Blueprints of Israel's Iron Dome Missile Defense System

Category:  
Library  
> [Tutorials and Articles](#)

Site:  
[forum\\_opense](#)

Iron-dome.jpg

Chinese hackers infiltrated the databases of three Israeli defense contractors and stole plans for Israel's Iron Dome missile defense system, according to an investigation by a Maryland-based cyber security firm 'Cyber Engineering Services Inc. (CyberESI)'. Not just this, the hackers were also able to nab plans regarding other missile interceptors, including Unmanned Aerial Vehicles, ballistic rockets and the Arrow III missile interceptor which was designed by Boeing and other U.S.-based companies.

# Chinese Hackers Stole Blueprints of Israel's Iron Dome Missile Defense System



The intrusions were thought to be executed by Beijing's infamous "Comment Crew" hacking group – a group of cyber warriors linked to the Chinese People's Liberation Army (PLA) – into the corporate networks of top Israeli defense technology companies, including Elisra Group, Israel Aerospace Industries, and Rafael Advanced Defense Systems, between 10 October 2011 and 13 August 2012.

The three Israeli defense technology companies were responsible for the development of the "Iron Dome" missile shield. The attackers targeted the three companies through email phishing attacks.

Once the companies' security systems had been breached, they exfiltrated all types of documents, from the emails sent by a CEO to the PowerPoint presentations containing all the necessary information about Iron Dome and other sophisticated ballistic projects.

The Beijing-sponsored hacking group came into light earlier this year when the United States Justice Department in May charged five of its alleged members with various hacking and espionage offenses. The group allegedly infiltrated United States systems involved in the nuclear power, metals and solar products industries, in order to "steal information that would provide an economic advantage" for Chinese companies.

This serious allegations on the chinese group were detailed by Brian on its blog. CyberESI is not yet prepared to release the report publicly.

Although it is not exactly known that how much data the group was able to obtain, Cyber ESI identified more than 700 documents that were stolen from Israel Aerospace Industries (IAI) only, amounting to 763 Mbs including Word documents and spreadsheets, PDFs, emails, and executable binaries, Krebs reported. The actual number is believed to be much higher.

Category:  
Library  
> [Tutorials and Articles](#)

Site:  
[forum\\_opense](#)

**Industrial** - Information technology sector, aerospace, satellites and telecommunications, energy, transportation, construction, manufacturing, engineering services, legal services, media, advertising, entertainment, navigation, chemicals, financial services, food, agriculture, healthcare, metals, mining. Targets include electrical grids, gas lines and waterworks in the United States. Attacks also include a company that controls 60% of all oil and gas pipelines in North America and the RSA, the



computer security company that protects corporate and government databases. Industrial targets include Coca cola.

-Comment Crew attacked Coca cola at the time it was negotiating the acquisition of China Huiyuan Juice Group for 2.4 Billion US\$. If Coca cola was successful in purchasing China Huiyuan, it would have been the largest foreign purchase of a Chinese company. Comment Crew attack on Coca cola started as a spear phishing attack and lead to the group stealing terabytes of data regarding negotiation strategy. The negotiations failed.

- The same technique was used on RSA, the computer security company. As a result of successfully attacking RSA, Comment Crew was able to attack Lockheed Martin, the United States largest defence contractor.

-In 2011, Project 2049 Institute out of Virginia said Comment Crew was the premiere entity attacking Canadian and American political, economic and military intelligence.

-In 2011, 70 organizations over a five year period, including the UN, and government agencies in Canada, United States, South Korea, Taiwan and Vietnam were targeted by an attack later called Shady RAT. Dell SecureWorks reverse engineered the masked location tool used in operation Shady RAT and found the IP address located in Shanghai. From there, it was identified to IP addresses linked to Comment Crew.

-Connected to the 2017 hack on Mandiant Senior Analyst, Adi Peretz.

**Academic** - Scientific research, education.

**International Organizations** - United Nations.

### **Countries Chinese hacker groups target**

-United States

-Canada

-South Korea

-Taiwan

-Vietnam

- Israel

### **TTP's etc.**

-State Funded, specifically PLA.

-APT1 has stolen hundreds of terabytes of data from over 141 organizations.

-The size of APT1's infrastructure implies hundreds of human operators.

-Most common initial compromise is spear-phishing.

-Malware - TROJAN, ECLYTS, BACKDOOR.BARKIOFORK, BACKDOOR.WAKEMINAP, TROJAN.DOWNBOT, BACKDOOR.DALBOT, BACKDOOR.REVIRD, TROJAN.BADNAME, BACKDOOR.WUALESS.

### **Connections to forums and other Hacker Groups**

---

## 2. APT3 aka UPS Team, Gothic Panda, Buckeye, TG-0110

Operating since: 2009.

### Main actors/leaders and structure

Wu Yingzhou

Dong Hao

-The above individuals have registered domains used by APT3. They are both listed as shareholders for China based security firm called **Guangzhou Boyu Information Technology Company (Boyusec)**.

-Boyusec is working with Chinese telecom giant **Huawei** to develop spyware-laden security products loaded onto computers and phones.

### Government entities, on contract with the government or civilians

-Suspected to have ties to the Chinese government.

-Connected to **Boyusec**, which is closely connected to Chinese Ministry of State Security.

### Chinese groups main targets: Political , Industrial.

**Political** - Aerospace, defence.

**Industrial** - Aerospace, defence, construction, engineering, high tech sector, telecommunications, transportation.

### Countries Chinese hacker groups target

-United States.

-United Kingdom

-Hong Kong

### TTP's etc.

-Suspected to be State Funded.

**-Considered one of the most sophisticated hacker groups.**

-Uses browser-based exploits as zero-days, such as Internet explorer, Firefox and Adobe Flash Player.

-APT3's CnC is difficult to track. There is little overlap across attacks.

-Malware - SHOTPUT, COOKIECUTTER, SOGU.

## Connections to forums and other Hacker Groups

### APT3 Hackers Linked to Chinese Ministry of State Security

**RD** radikal | 5/18/2017, 12:59:00 AM post

Independent researchers and experts from threat intelligence firm Recorded Future are confident that the cyber espionage group tracked as APT3 is directly linked to the Chinese Ministry of State Security (MSS).

While much of the security community typically tries to avoid making attribution statements, arguing that false flags make this task difficult, there are some individuals and companies that don't shy away from accusing governments of conducting sophisticated cyberattacks.

A mysterious group called "intrusiontruth," which claims to focus on investigating some of the most important advanced persistent threat (APT) actors, has recently published a series of blog posts on APT3, a group that is also known as UPS Team, Gothic Panda, Buckeye and TG-0110.

Category:  
[Russian-speaking Me...](#)  
[> English-speaking Me...](#)

Site:  
[forum\\_skyfraud](#)

Tags:  
hacking (1)

### **3.NCPH (Network Crack Program Hacker)**

**Operating since:**1994

#### Main actors/leaders and structure

-Approx 10 members and 4 leaders.

Top leader: **Tan Dailin** (Mei Gui)(Wicked Rose) - believed to be in the Chinese Military.

KuNgBim

Charles

Rodag.

-Current membership numbers unknown.

#### Government entities, on contract with the government or civilians

-Suspected to be the People's Liberation Army and based out of Zigong, Sichuan Province.

#### Chinese groups main targets **Political.**

**Political** - Hacked the US. Department of Defence/Pentagon multiple times in 2006.

#### Countries Chinese hacker groups target

-United States.

#### TTP's etc.

-Suspected to be State Funded, specifically PLA.

-Gained respect and recognition after hacking about 40% of other hacker associations websites in China.

-Gin Wui Rootkit

**-This group known for its expertise in surveillance and intrusion control programs.**

## أكثر عشرة فرق هكرز قدرت تغيير العالم الافتراضي و الواقعي



Network Crack Program Hacker Group"-5

Formed in 1994 to 2006 from Zigong, China.

10 members and 4 leaders, headed by "Tan Dailin"- in the Chinese Military. Current size of group is unknown. Successfully attacked competing groups. Attacked the Pentagon multiple times in 2006 using "Gin Wui".

Suspected to be funded by the PLA.

تدعى شبكة القرصنة تلك باسم مختصر "NCPH" وقد تم تشكيلها في تسي كونغ الصينية عام 1994 وحتى عام 2006 كان يعتقد أن أعضاء المجموعة مؤلفون من عشرة أفراد فقط بالإضافة لأربعة أعضاء في سدة القيادة على رأسهم "Tan Dailin" الملقب بالوردة الشريفة والذي عرف عنه العمل في الجيش الصيني لكن إلى الآن لم يتم تقدير الحجم الحالي لأفراد تلك المنظمة.

تمكنت المنظمة في بداياتها من تسديد ركلات مباشرة لعدد كبير من مواقع فُرَق الاختراق المنافسة، وسرعان ما لوحظ التطور الرهيب لدى المنظمة تلك بعد هجماتها المتكررة، والعمل على اختراقات في عمق وزارة الدفاع الأمريكية خلال فترات عديدة من 2006 باستخدام "Gin Wui"، أما في وقت لاحق من ذلك العام ربطت مؤسسة "Defense" المعنية بأمن الانترنت العديد من الهجمات المختلفة بذلك الفريق السري وأدائه.

تعرف المنظمة بخبرتها في برامج التحكم بشبكات المراقبة وبرامج التسلل أيضاً وكلها متوفرة للتحميل على موقعهم الرسمي، وفقاً لأحد أعضائها فإن المنظمة مدعومة مادياً من قِبَل رعاة غامضين، ومن المتوقع أن جيش التحرير الصيني من يقف وراء كل هذا الدعم.

Category:

الأقسام العامة

الحوار العام >

Site:

forum\_locker\_it

### Connections to forums and other Hacker Groups

**Hacker Group:** Honker Union of China.

## 4. Honker Union of China (HUC) aka Hongke (Red Guest), merged with Red Hacker Alliance/Red League.



**Operating since:** 1999.

### Main actors/leaders and structure

**Founder alias:** Lion

**Possible Actors:** Fish, Mooku, Purple Enchantress, Soy and Fifth element in dialogue on China Honker Army Forum:

Fish: Posts announcement of Happy New Year from China Honker Forum

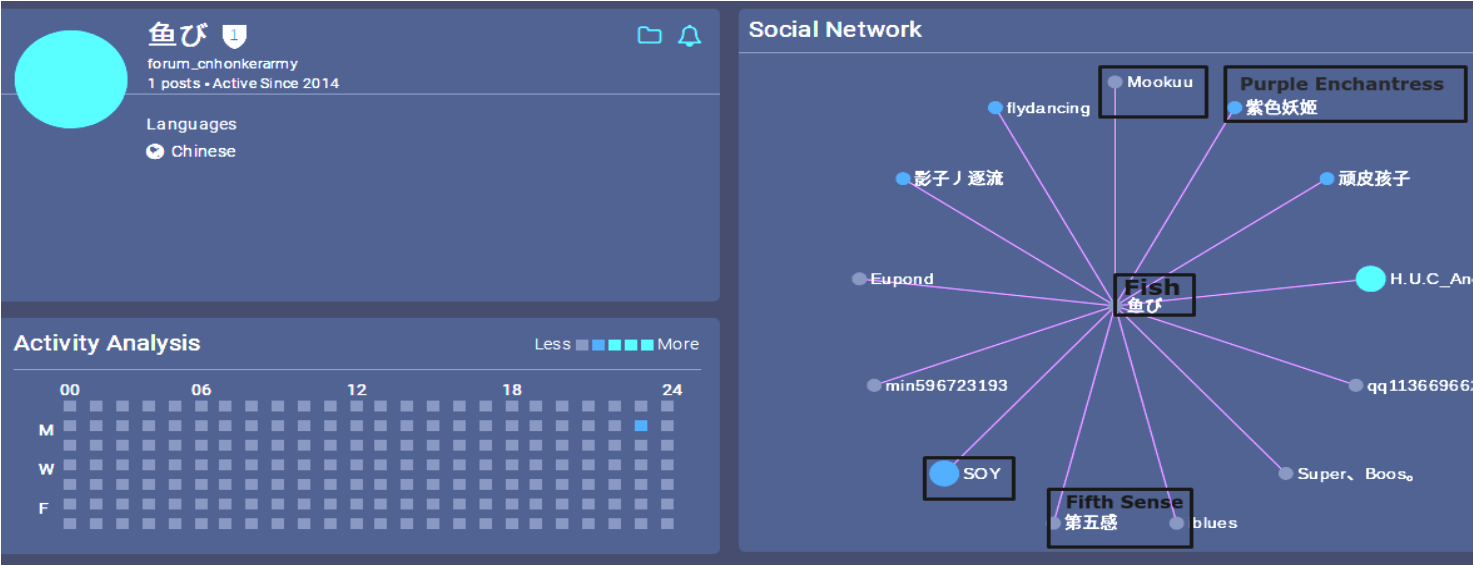
Mooku: Posts, "I believe Red League (Red Alliance) will become more powerful"

Purple Enchantress: Posts, "Wishing Red Alliance will flourish in the new year"

Soy: Posts, "thanks for your wishing of Honker Union of China, best wishes."

Fifth Element: Posts, "I wish we Red Alliance, will get better and better".

It is worth noting when the term ‘red’ is used in Chinese culture it is attached to patriotism/nationalism, which indicates connection to the Chinese government.



**中国红客联盟祝福各位新年快乐! Happy New Year from China Honker Union.**

📁 🔔

顶啊啊@@!!!

^ Back to Original Post ^

22 **HA** H.U.C\_Anonym、 | 2/17/2014, 5:34:48 PM  
、嗯，同乐。

23 **MK** Mookuu | 2/18/2014, 10:32:44 PM  
红盟一定会更加强大起来的! 我相信  
I believe Red League (Red Alliance) will become more powerful

24 **MK** Mookuu | 2/18/2014, 10:32:44 PM  
红盟一定会更加强大起来的! 我相信

25 **紫色妖姬** | 2/20/2014, 12:55:04 PM  
祝红盟在新的一年里蒸蒸日上，团结共进  
Wishing Red Alliance will flourish in the new year.

Actor:  
**Fish**  
鱼び

Category:  
官方公告区 > 行动规划  
Official Announcements

Site:  
forum\_cnhonkerarmy

---

10 **Fifth Element**  
第五感 | 2/9/2014, 4:54:13 PM  
祝咱们的红盟越办越好!  
I wish we Red Alliance, will get better and better.

11 **SO** SOY | 2/11/2014, 12:03:33 PM  
thanks for your wishing of Honker Union of China.best wishes

Site:  
forum\_cnhonkerarmy

**Government entities, on contract with the government or civilians**

-There is no direct evidence they are working for the Chinese government but is suspected to be a freelance group working on contract with the Chinese government.

**Chinese groups main targets: Political.**

**Political** - The word “Honker” emerged in 1999, when the United States bombed the Chinese Embassy in Belgrade, Yugoslavia. The Honkers formed a Honkers Union whose members combine hacking skills with nationalism. Active in hacktivism supporting the Chinese government against “US Imperialism” and “Japanese Militarism” and has launches attacks on websites mainly in the United States and mostly government websites. Main attacks deface websites and leave certain messages by attacking their appearance.

**Countries Chinese hacker groups target**

- United States,
- Japan
- Vietnam
- Philippines

**TTP’s etc.**

-Suspected to be State Funded.

**Connections to forums and other Hacker Groups**

**Forum:** China Honker Army Forum.

## 5. APT10 aka MenuPass Team, Stone Panda, Red Apollo

**Operating since:**2009.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

#### **-Chinese espionage group.**

-Targets are consistent with Chinese government goals, including military, intelligence and business sector data.

### Operation Cloud Hopper - PwC/BAE

APT10, a name originally coined by FireEye, is also referred to as Red Apollo by PwC UK, CVNX by BAE Systems, Stone Panda by CrowdStrike, and menuPass Team more broadly in the public domain. The threat actor has previously been the subject of a range of open source reporting, including most notably a report by FireEye comprehensively detailing the threat actor's use of the Poison Ivy malware family2

Category:

Site:  
[paste\\_pastebin](#)

### Chinese groups main targets: Political, Industrial, Academic.

**Political** - Governments of the United States, France, Japan and other European countries, sensitive military data and intelligence in hopes of strengthening China's own security and shielding China from attacks. Suspected to be responsible for a South Korean missile defence system hack. Also targets Islamic group in Western China known as the Uyghurs - Turkic Ethnic Group.

**Industrial** - Construction, Engineering, aerospace, telecom sectors. Theft of confidential business data to support Chinese corporations, targeting manufacturing companies in India, Japan and Northern Europe. A mining company in South America has also been targeted.

**Academic** - Japanese Universities.

-Hacks are cyber-espionage.

### Operation Cloud Hopper - PwC/BAE

The threat actor's targeting of diplomatic and political organisations in response to geopolitical tensions, as well as the targeting of specific commercial enterprises, is closely aligned with strategic Chinese interests.

Operation Cloud Hopper 5  
 APT10 as a China-based threat actor  
 APT10 as a China-based threat actor  
 1 The defence industrial base comprises the US Department of Defense and a plethora of companies that support the design, development and maintenance of defence assets and enable US military requirements to be met.  
<https://www.dhs.gov/defense-industrial-base-sector>  
 2 <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf>  
 3 <http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/>  
 PwC UK and BAE Systems assess it is highly likely that APT10 is a China-based threat actor with a focus on espionage and wide ranging information collection. It has been in operation since at least 2009, and has evolved its targeting from an early focus on the US defence industrial base (DIB)1 and the technology and telecommunications sector, to a widespread compromise of multiple industries and sectors across the globe, most recently with a focus on MSPs.

Category:

Site:  
[paste\\_pastebin](#)



**Countries Chinese hacker groups target**

- United States
- Canada
- France
- Switzerland
- Norway
- Finland
- Japan
- South Korea
- India
- Brazil
- South Africa
- Australia
- China - Islamic group in Western China known as the Uyghurs - Turkic Ethnic Group.

## China-Linked Hackers Target U.S. Trade Group

Fidelis Cybersecurity published a report detailing the campaign on Thursday, just hours before a meeting between U.S. President Donald Trump and his Chinese counterpart, Xi Jinping.

The company noticed in late February that the website of the National Foreign Trade Council (NFTC) had been hacked and set up to serve malware in what is known as a watering hole attack, or a strategic web compromise. Experts believe the attack ended by March 2, when links injected into the NFTC website had been removed.

Evidence uncovered by investigators led them to believe that the attack was conducted by a China-linked cyber espionage group known as APT10, MenuPass and Stone Panda. Fidelis has dubbed the campaign Operation TradeSecret.

According to researchers, the hackers set up certain web pages of the NFTC website to serve a reconnaissance framework known as Scanbox. The tool has been used for several years, including in attacks aimed at U.S. organizations and the Uyghur population in China.

Category:  
[Russian-speaking Me...](#)  
[English-speaking Me...](#)

Site:  
[forum\\_skyfraud](#)

Tags:  
hacking (1)

**TTP's etc.**

- Suspected to be State Funded.
- Target multiple IT service providers worldwide.
- in 2016 APT10 identified as cyber-espionage. Attack dubbed Cloud Hopper, the campaign targeted companies through managed IT service providers. Targeted countries were Canada, Brazil, France, Norway, Finland, Switzerland, South Africa, Australia, Japan, and India for intellectual property and other information.
- In 2014-2016, APT10 primarily used PlugX malware.
- In 2016-2017 in addition to using SOGU, intrusions involved a series a tools believed to be unique to APT10. These tools are first stage backdoors such as HAYMAKER and SNUGRIDE. They have

also used customized versions of the open source QUASARRAT, as well as BUGJUICE, both as second stage backdoors.

-Malware - HAYMAKER, SNUGRIDE, BUGJUICE, QUASARRAT.

### Connections to forums and other Hacker Groups

The screenshot shows a forum post on a dark blue background. The title is "China-Linked Hackers Target U.S. Trade Group". The user "radikal" posted it on 4/7/2017 at 1:41:00 AM. The post text describes a threat actor hijacking the website of the National Foreign Trade Council (NFTC) to deliver malware. It mentions a report by Fidelis Cybersecurity and identifies the attack as being conducted by a group known as APT10, MenuPass, and Stone Panda. The post is categorized under "English-speaking Me..." and has a tag for "hacking (1)".

## China-Linked Hackers Target U.S. Trade Group

**RD** radikal | 4/7/2017, 1:41:00 AM **post**

A threat actor linked to China hijacked the website of a prominent U.S. trade association in an effort to deliver reconnaissance malware to individuals who accessed certain web pages.

Fidelis Cybersecurity published a report detailing the campaign on Thursday, just hours before a meeting between U.S. President Donald Trump and his Chinese counterpart, Xi Jinping.

The company noticed in late February that the website of the National Foreign Trade Council (NFTC) had been hacked and set up to serve malware in what is known as a watering hole attack, or a strategic web compromise. Experts believe the attack ended by March 2, when links injected into the NFTC website had been removed.

Evidence uncovered by investigators led them to believe that the attack was conducted by a China-linked cyber espionage group known as APT10, **MenuPass** and Stone Panda. Fidelis has dubbed the campaign Operation TradeSecret.

Category:  
Russian-speaking Me...  
> English-speaking Me...

Site:  
forum\_skyfraud

Tags:  
**hacking (1)**

---

## 6. Bronze Butler aka Tick, REDBALDKNIGHT

**Operating since:**2012.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

- Linked to the People's Republic of China
- Some researchers believe the group may be hired by multiple teams or organizations seeking competitor information.

### Chinese groups main targets: Political, Industrial.

**Political:** Japanese international relations.

**Industrial:** Japanese heavy industry, manufacturing.

- Focused was on exfiltrating confidential data.

### Countries Chinese hacker groups target

- Japan

### TTP's etc.

- Suspected to be State Funded.
- Use spearphishing, strategic web compromises in targeted attacks and leverages zero-day exploit to compromise targeted systems. Uses phishing emails with Flash animation attachments to download malware.
- Periodically revisits compromised sites to exfiltrate more data.
- Experts highlighted the groups ability to discover a zero-day flaw in software used in a certain region.
- One documented malware, the Daserf backdoor allowed full control over the compromised system. Two versions of the tool were developed. In 2016, the hackers replaced Daserf with two remote access trojans (RATS) called xxmm and Datper.
- Malware: DASERF, XXMM, DATPER.

### Connections to forums and other Hacker Groups

## 7. KeyBoy

**Operating since:** 2013

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-Operates out of China

### Chinese groups main targets: Political, Industrial.

**Political:** Tibetan Parliament in 2016.

**Industrial:** Western and SE Asian organizations



### Countries Chinese hacker groups target

- Tibet
- Taiwan
- Philippines
- Western Countries

### TTP's etc.

-Uses malware attacks on western organizations and SE Asia that infects computers with certain type of malware than can secretly download info, take screenshots, browse logs.

-Malware downloaded and installed as fake Microsoft word DLL file needed to open infected file a user has already downloaded.

-Malware capabilities include screenshots, keylogging features, and also stroll through and download files of victims, gather extended system information about the machine and shutting down infected systems.

- Keyboys latest hacking tool gains access by sending infected word document “Q4 Work Plan.docx”
- Disables Windows File Protection, their bait uses a Dynamic Data Exchange protocol to locate and download remote payload, instead of downloading malicious macros or exploit.
- Medium level of technical and operational expertise.

### Connections to forums and other Hacker Groups

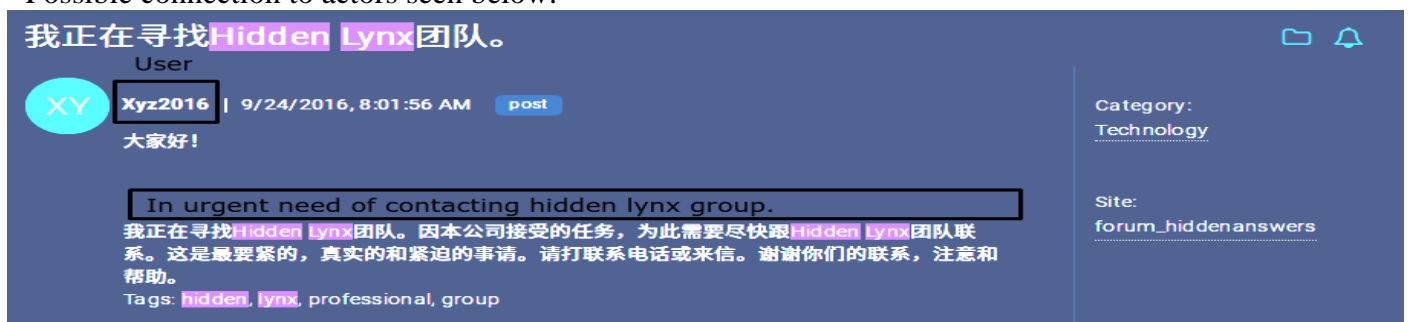
## 8. Elderwood Group aka Elderwood Platform, Elderwood Project, Elderwood Gang.

### Subgroups: Hidden Lynx, Vidgrab, Icefog, Sakurel, Blue Termite

Operating since: 2005

#### Main actors/leaders and structure

- Unknown actors.
- Elderwood platform being used by subgroups - assuming Elderwood hackers are developing exploits for its own teams “subgroups.” It’s also possible the developer of Elderwood platform is actively selling the platform.
- Possible connection to actors seen below.



#### Government entities, on contract with the government or civilians

- Rumoured to be Chinese government sponsored because of resources needed for attacks and ability to analysis the resources.

#### Chinese groups main targets: Political, Industrial.

**Political** - Defence, including shipping, aeronautics, arms, energy, manufacturing, engineering and electronic. Also companies fighting human rights. Countries that have detected elderwood activity are Canada, United States, China, Hong Kong, Australia, Taiwan, United Kingdom, Switzerland, India and Denmark.

**Industrial** - NGO’s, finance and software firms.

- Hidden Lynx specifically targets Japanese users and the defence industry.
- Vidgrab specifically targets Uyghur dissidents in Western China.
- Icefrog specifically targets the manufacturing industry.
- Sakurel specifically targets aerospace industry.
- Blue Termite - targets Japanese organizations. Believed to be responsible for the CloudyOmega operation, which is linked with subgroup Hidden Lynx. Also connected to the unknown actors responsible for the LadyBoyle attacks.

#### Countries Chinese hacker groups target

- United States

- Canada
- Hong Kong
- China
- Taiwan
- Japan
- Australia
- United Kingdom
- Switzerland
- Denmark
- India

**TTP's etc.**

-Suspected to be State Funded.

**-Quiet group - does not advertise attacks or motivation behind attacks.**

-Reusing components of an infrastructure called the Elderwood Project to deploy zero-day exploits through spear phishing emails. Also increased attacks through Web injections in watering hole attacks. Have gained access to source code for some widely used applications, or have reverse engineered the applications to discover vulnerabilities.

-Target web based applications. Have attacked Adobe Flash Player, Microsoft internet explorer, Microsoft xml, Google infrastructure. Attacks referred to as Operation Aurora because an Aurora type trojan horse used.

**Hidden Lynx** – Professional Hackers for Hire
📁 🔔

VR

Versus71 | 9/19/2013, 3:04:00 PM post

For the past few years, reports have continued to emerge detailing the activities of actors behind various targeted attacks or Advanced Persistent Threats (APTs). Here at Symantec Security Response, we've been keeping our eyes on a group that we believe are among the best of breed. We've given them the name of **Hidden Lynx**—after a string that was found in the command and control server communications. This group has a hunger and drive that surpass other well-known groups such as APT1/Comment Crew. Key characteristics of this group are:

technical prowess agility organized sheer resourcefulness patience

Infographic:

Category:

[Hacking | Administraci...](#)

> [Hacking](#)

Site:

[forum\\_level23hackert...](#)

## Chinese APT Espionage campaign, dubbed 'Icefog' targeted Military contractors and Gov



**DB** DarkBot | 9/27/2013, 10:15:00 PM post

Kaspersky Lab has identified a nother Chinese APT campaign. Dubbed 'Icefog', the largely Japanese, Taiwanese and South Korean targets included a well-publicised attack on Japan's House of Representatives in 2011.

Kaspersky Lab and others have released a steady stream of research on what is starting to look like a thriving mostly Chinese industry selling hacking expertise and espionage to governments.

In recent weeks, Symantec published a paper on a major hacking-for-hire group it called **Hidden Lynx** responsible for a large number of attacks while Kaspersky itself has uncovered evidence that North Korea was trying its hand at the same chicanery with its 'Kimsuky' Trojan.

Judging from Kaspersky's latest research, Icefog looks like a smaller player than **Hidden Lynx** or the notorious Comment Crew/APT1 convincingly blamed for a hugely successful raid on defence contractor QinetiQ.

Category: [Community](#) > [News](#)

Site: [forum\\_bitshacking](#)

## RSS\_BOT Latest Internet Explorer zero-day linked to **Elderwood** Project



**1L** Illusion | 1/6/2013, 4:05:00 PM post

Latest Internet Explorer zero-day linked to **Elderwood** Project

Last week we have seen ongoing attacks was exploiting a vulnerability in Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8 that came to light after the Council on Foreign Relations website was hacked and was hosting the code. Symantec has linked exploits to the group responsible for a spate of recent espionage attacks Dubbed the **'Elderwood** Project'.

Category: [General](#) > [World News](#)

Site: [forum\\_sinisterly](#)

Tags: [exploit \(1\)](#) [hacking \(1\)](#)

### Connections to forums and other Hacker Groups

**Hacker Subgroups:** Hidden Lynx, Vidgrab, Icefog, Sakurel, Blue Termite

## Хакеры из Black Vine делят 0day-уязвимости с конкурентами

0-day Vulnerability

Данная сеть распространения впервые попала на экраны радаров три года назад и тогда получила имя Elderwood platform. Сеть постоянно пополняется новыми 0day, с ней точно были соотнесены эксплоиты для уязвимостей Hidden Lynx, Vidgrab, Icefog и **Sakurel**.

Elderwood Platform 0day connected to Hidden Lynx, Vidgrab, Icefog and Sakurel.

Корни Elderwood platform, по данным экспертов, уходят в Китай, и этот конгломерат используется для направленных фишинговых и watering-hole атак против крупных представителей оборонной и IT индустрии, а также против компаний борющихся за права человека.

Category: [Проект NETSKY](#)

Site: [forum\\_skyfraud](#)

Tags: [hacking \(1\)](#)



## 9. Hidden Lynx

**Operating since:** 2009.

### Main actors/leaders and structure

- Unknown actors.
- 50-100 members based on hacking behavior.

### Government entities, on contract with the government or civilians

#### **-Highly professional group - Hackers for hire.**

-Suspected ties to Chinese government - attack infrastructure and tools used originate from network infrastructure in China.

### Chinese groups main targets: Political, Industrial Academic, Non-Profit.

**Political:** All levels of government. Military/Defence sector.

**Industrial:** Defence industry in western countries, non-profit sector, media sector, legal, engineering, healthcare, financial sector.

**Academic:** Education sector.

### Countries Chinese hacker groups target

United States

Taiwan

China

Hong Kong

Japan

South Korea

Canada

Russia

Germany

Ukraine

Australia

United Kingdom

France

Singapore

India

### TTP's etc.

-Suspected to be State Funded.

-The variety of targets implies the group does not focused on one task but is likely tasked with obtaining very specific information to gain competitive advantages in the industrial sector and Chinese state level.

#### **-Members are experts at breaching systems.**

-Strategy of mass exploitation and pay-to-order targeted attacks for intellectual property using two Trojans. -Backdoor.Moudoor, a customized version of "Gh0st RAT", for large-scale campaigns across several industries. Distribution of Moudoor requires a significant number of people.

- Trojan.Naid, the Trojan found during the Bit9 attack, appears to be reserved for attacks against high value targets. This Trojan was leveraged for a special operation during the VOHO campaign and is probably used by a specific team of highly skilled attackers within the group. This Trojan was also found as part of "Operation Aurora" in 2009.

-The group is methodical and display a skillset far in advance of other attack groups also operating in that region, such as APT1.

-Malware: Backdoor.Moudoor, Trojan.Naid,

### Connections to forums and other Hacker Groups

**Hacker Groups:** Elderwood Group and its subgroups.

## Хакеры из Black Vine делят 0day-уязвимости с конкурентами

### 0-day Vulnerability

Данная сеть распространения впервые попала на экраны радаров три года назад и тогда получила имя Elderwood platform. Сеть постоянно пополняется новыми 0day, с ней точно были соотнесены эксплоиты для уязвимостей Hidden Lynx, Vidgrab, Icefog и **Sakurel**.

Elderwood Platform 0day connected to Hidden Lynx, Vidgrab, Icefrog and Sakurel.

Корни Elderwood platform, по данным экспертов, уходят в Китай, и этот конгломерат используется для направленных фишинговых и watering-hole атак против крупных представителей оборонной и IT индустрии, а также против компаний борющихся за права человека.

Category:

[Проект NETSKY](#)

Site:

[forum\\_skyfraud](#)

Tags:

[hacking \(1\)](#)

## 10. APT12 aka Calc Team, DynCalc, DNSCALC, Numbered Panda.

Operating since: 2013.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

- Operating out of China with major links to the PLA.
- Targets are consistent with Chinese government goals, keen interest in Taiwan.

### Chinese groups main targets: Political, Industrial

**Political** - Taiwanese government organizations, defence.

**Industrial** - Japanese Technology sector, defence industry sector, Journalists. Media - NY Times.



The screenshot shows a forum post with the following content:

**Apt Groups Return - Chinese Hackers Resume Cyber Espionage Operations**

It's also been monitoring the second Chinese hackers group, **APT12** that apparently hacked the New York Times in January 2013 compromising its networks over the course of past four months.

Last year Mandiant provided the evidence linked APT1 group to UNIT 61398 of China's 2nd Bureau of the People's Liberation Army (PLA), but Beijing has always denied the accusations, remarking the report as "full of loopholes" and stated, "Chinese laws prohibit any action including hacking that damages Internet security," and added, "to accuse the Chinese military of launching cyber attacks without solid proof is unprofessional and baseless."

But the American computer security firm, Mandiant keep on following the groups' activities. The report reads, "Mandiant's continued observations of APT1 and **APT12** activity, measured by command and control (C2) sessions, revealed a different response behind the scenes, suggesting a possible acknowledgement that both groups had been exposed."

Category: International > General Discussion  
Site: forum\_lampeduza

### Countries Chinese hacker groups target

- Taiwan
- Japan
- United States

### TTP's etc.

- Suspected to be State Funded, mostly likely PLA.
- Hacks are cyber-espionage.
- Attacks utilize spear phishing email with a Microsoft word document.
- Known especially for its ability to evolve and adapt in order to stay on mission.
- Malware - RIPTIDE, HIGHTIDE, THREBYTE, WATERSPOUT, IXESHE.

### Connections to forums and other Hacker Groups

Hacker Groups: APT1

## 11. DragonOK.

**Operating since:** 2014.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-Linked to China, possibly operating out of Guangdong Province.

### Chinese groups main targets: Political, Industrial, Academic.

**Political** - Defence entities in the United States, espionage operations in Japan and Taiwan.

**Industrial** - Defence entities in the United States. In 2017, targeted Japanese manufacturing, technology, energy, and semiconductors. Conducted corporate espionage operations on high-tech and manufacturing companies in Japan and Taiwan. The KHRAT RAT campaign targets citizens in Cambodia.

**Academic** - Targeted Japanese higher education sector.

### Countries Chinese hacker groups target

-United States

-Cambodia

-Taiwan

-Japan

-Russia

-India

-Tibet

### TTP's etc.

-Suspected to be State Funded.

-Campaign in 2017 leveraged the KHRAT remote access Trojan (RAT).

-Has updated spearphishing techniques and themes used in the campaign.

-Use many methods to download and execute additional payloads using built-in Windows applications and also started mimicking Dropbox.

-Used a JavaScript code that allowed it to monitor who visited the site. The code gathered data such as user-agent, domain, cookie, referrer and Flash version, and appears almost identical to that found on a blog hosted on the Chinese Software Developer Network (CSDN) website.

-DragonOKhas updated both its malware and tactics, techniques and procedures (TTPs) during 2017. **It is suspected they plan to intensify its activity.**

-Connected to the 2017 hack on Mandiant Senior Analyst, Adi Peretz.

-Malware - SYSGET, IsSpace, TIDEPOOL, NetTraveler (TravNet), PlugX, Saker, Netbot, DarkStRat, ZeroT.

-Sysget - malware - used to target Taiwan.

-IsSpace - malware - used to target Taiwan.

-TidePool - malware - used to target Indian Embassies, Russia and Tibet.

### Connections to forums and other Hacker Groups

**Hacker Group:** Moafee. First noticed as two hacking campaigns conducted by two groups operating in separate regions of China but worked in parallel.

The first team, Moafee, targeted military and government organizations involved in South China sea dispute. The second team, DragonOK, conducted corporate espionage operations on high-tech and manufacturing companies in Japan and Taiwan.

## China-linked KHRAT Operators Adopt New Delivery Techniques



radikal | 9/4/2017, 11:23:00 PM post

A recently observed KHRAT remote access Trojan (RAT) infection campaign uses updated spear phishing, download and execution techniques, Palo Alto Networks security researchers warn.

KHRAT is a backdoor associated with the China-linked cyber espionage group known as **DragonOK**, which has been previously known to use malware such as NetTraveler (aka TravNet), PlugX, Saker, Netbot, DarkStRat, and ZeroT in attacks against organizations in Russia and other surrounding countries. The recent campaign featuring the RAT targets victims located in Cambodia.

The malware was designed to register victims using their machine's username, system language and local IP address, while also providing attackers with the typical set of RAT features, including remote access to the victim system, keylogging, screenshot taking capabilities, remote shell access, and the like.

Category:  
[Russian-speaking Me...](#)

Site:  
[forum\\_skyfraud](#)

Tags:  
hacking (1)

## 12. Moafee.

**Operating since:** 2014.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

Linked to China, possibly operating out of Guangdong Province.

### Chinese groups main targets: Political.

**Political** - Targeted military and government organizations involved in South China sea dispute, U.S. defence sector.

### Countries Chinese hacker groups target

- United States
- Taiwan

### TTP's etc.

- Suspected to be State Funded.
- Malware: IsSpace - used to target Taiwan.

### Connections to forums and other Hacker Groups

**Hacker Group:** DragonOk. First noticed as two hacking campaigns conducted by two groups operating in separate regions of China but worked in parallel.

The first team, Moafee, targeted military and government organizations involved in South China sea dispute. The second team, DragonOK, conducted corporate espionage operations on high-tech and manufacturing companies in Japan and Taiwan.

## China-Linked "DragonOK" Group Expands Operations

The group also targeted Taiwan with a piece of malware named "IsSpace." This Trojan is believed to be an evolution of the NFlog backdoor, which has been used by both DragonOK and a different China-based threat group tracked as **Moafee**. IsSpace was previously seen in a watering hole attack targeting an aerospace company, but the samples spotted recently appear to have been updated.

Palo Alto Networks said recent DragonOK attacks also involved a piece of malware known as TidePool. Researchers observed this Trojan earlier this year in attacks launched by a different China-linked group against Indian embassies, but it had not been used by DragonOK in earlier campaigns. DragonOK appears to have leveraged TidePool in attacks aimed at entities in Russia and Tibet.

The Russian-language decoy document used by the attackers referenced GOST, a block cipher developed by the Russian government in the 1970s. The malicious document believed to be aimed at Tibet, or individuals interested in Tibetan affairs, contained an internal newsletter from the Central Tibetan Ministry.

Category:  
[Russian-speaking Me...](#)  
[> English-speaking Me...](#)

Site:  
[forum\\_skyfraud](#)

Tags:  
[hacking \(1\)](#)

## 13. APT16

Operating since: 2015.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-Located in China and suspected to be the Chinese government.

### Chinese groups main targets: Political, Industrial.

**Political** - Government Services.

**Industrial** - High tech sector, media, financial services sector.

### Countries Chinese hacker groups target

-Taiwan

-Japan

### TTP's etc.

-Suspected to be State Funded.

### **-Hacks are cyber-espionage.**

-Used an exploit from Microsoft Office vulnerability CVE-2015-2545 to target media and government agencies in Taiwan.

-Spear-phishing emails and webmail addresses used.

-Malware: IRONHALO, ELMER.

### Connections to forums and other Hacker Groups

**Hacker groups:** EvilPost, Danti, DragonOK.

## Microsoft Office Flaw Exploited by Several APT Actors 📁 🔔

One of the first APT groups to start leveraging CVE-2015-2545 after it was fixed by Microsoft's **EvilPost**, a China-linked gang that used weaponized Word documents to attack a Japanese defense contractor in December 2015.

At around the same time, a different Chinese attacker dubbed **APT16** used an exploit for this Office vulnerability to target media and government agencies in Taiwan. Organizations in Taiwan were also targeted in December 2015 by a threat actor dubbed by Kaspersky "SVCMONDR."

The **SVCMONDR** attacks share similarities with operations carried out by a group called **Danti**. However, researchers have not been able to precisely determine if SVCMONDR and Danti are the same group or if they simply used the same malicious code.

Category:

- Russian-speaking Me...
- > English-speaking Me...

Site:

forum\_skyfraud

Tags:

exploit (1)
hacking (1)

## 14. EvilPost

Operating since: 2015.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-China linked gang.

### Chinese groups main targets: Political ,Industrial.

**Political** - Japanese defence.

**Industrial** - Japanese defence contractors - 2015.

### Countries Chinese hacker groups target

-Japan

### TTP's etc.

-Leveraged Microsoft Office remote code execution flaw, tracked as CVE-2015-2545. Used weaponized word documents to attack the Japanese defence contractor.

-Malware:

### Connections to forums and other Hacker Groups

**Hacker groups:** Danti, DragonOK.

## Microsoft Office Flaw Exploited by Several APT Actors

One of the first APT groups to start leveraging CVE-2015-2545 after it was fixed by Microsoft is **EvilPost**, a China-linked gang that used weaponized Word documents to attack a Japanese defense contractor in December 2015.

At around the same time, a different Chinese attacker dubbed **APT16** used an exploit for this Office vulnerability to target media and government agencies in Taiwan. Organizations in Taiwan were also targeted in December 2015 by a threat actor dubbed by Kaspersky "SVCMONDR."

The **SVCMONDR** attacks share similarities with operations carried out by a group called **Danti**. However, researchers have not been able to precisely determine if SVCMONDR and Danti are the same group or if they simply used the same malicious code.

Category:

[Russian-speaking Me...](#)  
[English-speaking Me...](#)

Site:

[forum\\_skyfraud](#)

Tags:

[exploit \(1\)](#)

[hacking \(1\)](#)



## 15. Danti

**Operating since:** 2013.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-Suspected to be the Chinese government.

### Chinese groups main targets Political, Industrial.

**Political** - Indian diplomatic organizations, including embassies.

**Industrial** - Various corporate entities in Kazakhstan, Kyrgyzstan, Uzbekistan, Myanmar, Nepal and the Philippines.

### Countries Chinese hacker groups target

India

Kazakhstan

Kyrgyzstan

Uzbekistan

Myanmar

Nepal

Philippines

### TTP's etc.

-Suspected to be State Funded.

-Malware used to attack Indian diplomatic organizations similar to that used in 2013 Operation Ke3chang, out of China.

### Connections to forums and other Hacker Groups:

**Hacker groups:**DragonOK, SVCMONDR.

## Microsoft Office Flaw Exploited by Several APT Actors

**Danti** is an actor that has been observed targeting entities in Kazakhstan, Kyrgyzstan, Uzbekistan, Myanmar, Nepal and the Philippines. It's believed to be a new group that is related to the NetTraveler and DragonOK cyberspies, whose activities were analyzed in 2013 and 2014.

Danti used CVE-2015-2545 in February and March to launch attacks against Indian diplomatic organizations, including many embassies. The group's activities were also analyzed recently by Palo Alto Networks, which found connections between the malware used in the attacks aimed at Indian embassies and malware used in 2013 in a campaign called Operation Ke3chang. Evidence suggests that the attackers are located in China.

Palo Alto Networks recently also analyzed a campaign where an APT group leveraged the Office flaw to deliver a Poison Ivy variant named "SPIVY" to organizations in Hong Kong.

Exploitation of cve-2015-2545 by APT actors

Category:  
[Russian-speaking Me...](#)  
[> English-speaking Me...](#)

Site:  
[forum\\_skyfraud](#)

Tags:  
exploit (1)
hacking (1)

## 16. SVCMONDR

**Operating since:** 2013.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-Suspected to be the Chinese government.

### Chinese groups main targets: Industrial.

**Industrial** - Organizations in Taiwan.

### Countries Chinese hacker groups target

-Taiwan

### TTP's etc.

-Suspected to be State Funded.

-Used an exploit from Microsoft Office vulnerability CVE-2015-2545 to organizations in Taiwan.

### Connections to forums and other Hacker Groups

**Hacker groups:** Danti. It is suspected to be the same group as Danti or sharing same code.

## Microsoft Office Flaw Exploited by Several APT Actors 📁 🔔

One of the first APT groups to start leveraging CVE-2015-2545 after it was fixed by Microsoft's **EvilPost**, a China-linked gang that used weaponized Word documents to attack a Japanese defense contractor in December 2015.

At around the same time, a different Chinese attacker dubbed **APT16** used an exploit for this Office vulnerability to target media and government agencies in Taiwan. Organizations in Taiwan were also targeted in December 2015 by a threat actor dubbed by Kaspersky "SVCMONDR."

The **SVCMONDR** attacks share similarities with operations carried out by a group called **Danti**. However, researchers have not been able to precisely determine if SVCMONDR and Danti are the same group or if they simply used the same malicious code.

Category:

- [Russian-speaking Me...](#)
- > [English-speaking Me...](#)

Site:

[forum\\_skyfraud](#)

Tags:

exploit (1)
hacking (1)

## 17. China Girl Security Team aka CN Girl Security Team.



**Operating since:** 2007.

### Main actors/leaders and structure

-Main actor: Xiao Tian - A Chinese national, started this female only hacking group at 19 years old, now has over 2200 members and is tied to some of the biggest hacking groups in the world. A celebrity in China that sells tee-shirts and other memorabilia.

-Originated from the Six Golden Flowers Hacker Group, the first all female group in the world. Xiao Tian split up from the group, created China Girl Security Team and became its leader.

### Government entities, on contract with the government or civilians

-Located in China

### Chinese groups main targets: Political, Industrial.

**Political** - Linked to denial-of-service attacks on the U.S. White House website and have links to attacks of cyber warfare. Also, known to deface U.S. government websites.

**Industrial** - Linked to attacks on Google and contributed to google's withdraw from China but this is not confirmed.

<p>ia juga tertarik sekali dengan dunia fashion, khususnya sepatu. Dalam blog nya dia sering berbagi cerita tentang tempat-tempat yang pernah dia datangi. Itulah alasan mengapa Xiao memiliki banyak fans dan followers di dunia, khususnya para pria.</p> <p><b>Xiao Tian</b> mulai dikenal sejak umur 19 tahun. Setelah membentuk <b>China Girl Security Team</b> salah satu kelompok hacker khusus wanita terbesar di china. Kiprahnya dalam dunia hacking juga tidak diragukan lagi. Raksasa search engine nomor satu di dunia, Google pun pernah merasakan serangan hebat dari Tian beserta timnya. Xiao Tian melakukan serangan canggih terhadap sistem infrastruktur google china. Bahkan, google akhirnya tidak tahan dan memilih untuk menarik semua layanan operasionalnya di China akibat hantaman hacker yang bertubi-tubi tersebut.</p> <p>Xiao Tian is leader of the China Girl Security Team. She has high level hacking skills as proven in her attack against Google.</p>	<p>Category:  <a href="#">The Lounge</a> &gt; <a href="#">Bebas</a></p> <p>Site:  <a href="#">forum_devilzcode</a></p>
---	--

### Countries Chinese hacker groups target

-United States

### TTP's etc.

### Connections to forums and other Hacker Groups

## 18. APT27 aka Emissary Panda, Threat Group 3390, LuckyMouse, Bronze Union.

Operating since: 2013.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-Located in China and suspected to be linked to the Chinese government.

### Chinese groups main targets: Political, Industrial.

**Political** - U.S. government defence. European drone manufacturer.

**Industrial** - In 2013, launched a campaign called Iron Tiger. Iron Tiger targeted multiple U.S. government contractors working in intelligence, aerospace, energy, telecoms and nuclear industries. European manufacturer of drone technology.

-Investigated by the CIA as revealed by Wikileaks.

-In 2017, targeted National Data Center in Central Asia.

### The CIA has learned hacking techniques in cybercrime 📁 🔔

According to leaked documents from November 2014 to September 2015 the company Raytheon Blackbird Technologies provided the CIA at least five reports on the work done within the project UMBRAGE Component Library (UCL). The reports are summarized designed by cybercriminals and researchers disclosed methods and attack vectors. Probably, the CIA specialists have used this information to develop their own malware. In the first Raytheon Blackbird Technologies report describes a tool for remote access HTTPBrowser developed around 2015. The malware is designed to intercept keystrokes on the keyboard and use the Chinese cybercrime gang **Emissary Panda**.

Category:  
[Library](#)  
> [Tutorials and Articles](#)

Site:  
[forum\\_openc](#)

YA

**YourAnonRiot** | 6/14/2018, 6:40:17 AM post

Detected In March 2018 an ongoing campaign targeting a national data center in the Central Asia (active since autumn 2017) The websites were compromised to redirect visitors to instances of both ScanBox and BEeF.

Via @securityaffairs cc: @binitamshah

<https://securityaffairs.co/wordpress/73498/apt/emissary-panda-campaign.html>

[https://twitter.com/\\_odisseus/status/1007149253188349952/photo/1](https://twitter.com/_odisseus/status/1007149253188349952/photo/1)

Category:

Site:  
[twitter](#)

WS

**WarTech Support** | 6/15/2018, 1:46:00 PM post

Category:  
[Основной раздел](#)  
[> Другие новости](#)

Site:  
[forum\\_rutor](#)

Хакерская группировка LuckyMouse, предположительно связанная с китайским правительством, атаковала государственный центр обработки данных в Центральной Азии. Как полагают исследователи из «Лаборатории Касперского», основной целью хакеров является подготовка плацдарма для кибератак на правительственные web-сайты страны.

Working since 2010. Attacked hundreds of organizations around the world. American defence contractors, financial firms, European drone manufacturers, and American energy sector. In 2018, this group competed an attack on the data center in central asia.

Группировка, известная под названиями LuckyMouse, Emissary Panda, APT27 и Threat Group 3390, работает по меньшей мере с 2010 года и была замечена в атаках на сотни организаций по всему миру, включая американских оборонных подрядчиков, финансовые фирмы, европейского производителя дронов, а также американскую компанию по управлению энергопотреблением.

Исследователи «Лаборатории Касперского» зафиксировали новую атаку, совершенную группировкой в марте 2018 года. Целью атаки был государственный центр обработки данных в неназванной стране в Центральной Азии.

**Countries Chinese hacker groups target**

- United States
- Asia
- Europe

**TTP's etc.**

- suspected to be State Funded.
- Many techniques used to attack include input capture, remote file copy, and external remote services. Use software including PlugX and China Chopper.
- Since the PZChao campaign attacking targets in the United States and Asia, there is some suspicion this hacker group has returned since its attack tactics are similar to that of Iron Tiger.
- 2017 attack targeting the National Data Center in Central Asia website redirected visitors to instances of ScanBox and BEeF.
- **Known to be highly competent and sophisticated.**

**Connections to forums and other Hacker Groups**

## 19. APT17 aka Deputy Dog, Tailgator Team, Voho, Group72, AuroraPanda.

Operating since: 2010.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-Suspected to be linked to the Chinese government.

### Chinese groups main targets: Political, Industrial.

**Political** - U.S government organizations including the military/defence sector.

**Industrial** - International law firms, information technology sector - including Google (loss of intellectual property), financial sector, the mining industry and NGO's.

### Operation Cloud Hopper - PwC/BAE

📁 🔔

2010: Technology, financial and defence sectors were targeted by Operation Aurora, a campaign attributed to **APT17**/Aurora Panda. The list of targets included Google, who suffered the loss of intellectual property and attempted access to the Gmail accounts of human rights activists.

Category:

Site:  
[paste\\_pastebin](#)

---

### Chinese Threat Group Uses Microsoft's TechNet Portal to Host C&C IPs

📁 🔔

HC

**hackerjon** | 8/7/2015, 8:44:15 AM post

The Chinese threat actor known as **APT17** and DeputyDog has been using profile pages and forum threads on Microsoft's TechNet web portal to host IP addresses for command and control (C&C) servers.

Researchers at FireEye Threat Intelligence and the Microsoft Threat Intelligence Center have prepared a brief report on the advanced persistent threat (APT) actor's C&C obfuscation techniques.

Experts have determined that the attackers haven't actually compromised Microsoft's website. Instead, they are using the portal's legitimate functionality to host encoded strings that hide C&C IP addresses.

**APT17** is a Chinese threat group that has been targeting United States government organizations, the military, law firms, defense contractors, IT firms, mining companies, and NGOs. One of the tools leveraged by the group is BLACKCOFFEE, a backdoor that can be used to upload and download files, create a reverse shell on the infected system, enumerate files and processes, manipulate files, and terminate processes.

The malware, which has been used by **APT17** since at least 2013, now gets the IP address of the C&C server it's supposed to communicate with from an encoded string embedded on the TechNet portal.

The new version of BLACKCOFFEE contains URLs that point to TechNet forum threads or biography sections in profiles created by the attacker. The encoded string that hides the IP address in plain sight is found in profiles and posts between the "@MICROSOFT" and "CORPORATION" tags.

Category:  
[wut it do?](#) > [ayo](#)

Site:  
[forum\\_hell](#)

Tags:  
hacking (1)
security (1)

---

### **Countries Chinese hacker groups target**

-United States.

### **TTP's etc.**

-Suspected to be State Funded.

-Created profiles and posts in forums to embed encoded CnC for use with malware.

-Axiom

-Malware: BLACKCOFFEE

### **Connections to forums and other Hacker Groups**

## 20. APT18 aka Wekby, Dynamite Panda, TG-0416.

**Operating since:** 2014.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-Suspected ties to Chinese government.

### Chinese groups main targets: Political, Industrial, Academic.

**Political:** Aerospace and defence.

**Industrial:** Aerospace, construction, engineering, health & biotechnology, high tech sector, telecommunications, transportation.

**Academic:** Education.

### Countries Chinese hacker groups target

-United States.

### TTP's etc.

-Suspected to be State Funded.

-Exploited Community Health Systems (USA hospital operator), OpenSSL vulnerability (dubbed Heartbleed).

-Have added Flash Player exploit.

-Data from Hacking Team leak used (CVE-2015-5119) - developed or adapted for operations.

-Malware: Gh0st RAT.

### "Wekby" Group Uses DNS Requests for C&C Communications

RD

**radikal** | 5/27/2016, 3:26:00 PM post

Category:

Russian-speaking Me...

> English-speaking Me...

Site:

forum\_skyfraud

Tags:

hacking (1)

Palo Alto Networks researchers noticed that a China-linked advanced persistent threat (APT) actor has been using a piece of malware that leverages DNS requests for command and control (C) communications.

The group, known as Wekby, APT 18, Dynamite Panda and TG-0416, is believed to be responsible for the 2014 attack on Community Health Systems, one of the largest hospital operators in the United States. In that operation, the attackers reportedly stole 4.5 million patient records by exploiting the OpenSSL vulnerability dubbed Heartbleed.

The group is known to quickly add new exploits to its arsenal. One example is a Flash Player exploit that the actor started using shortly after it was leaked last year from Italian spyware maker Hacking Team.

In a more recent attack aimed at a US-based organization, Wekby leveraged a piece of malware dubbed by Palo Alto Networks "pisloader." Based on metadata and the

### Connections to forums and other Hacker Groups



## 21. APT19 aka Codoso Team, Sunshop Group.

Operating since: 2017.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-Suspected to be Chinese government.

### Chinese groups main targets: Industrial.

**Industrial** - Legal, Investment sectors, Forbes.

### Countries Chinese hacker groups target:

-United States.

-Canada.

### TTP's etc.

-Suspected to be State Funded.

### **-Hacks are cyber-espionage.**

-Believed to have worked in part with Shell Crew (aka. Deep Panda) to target an IT Service Provider through a Canadian tech company called Altair Technologies Ltd.(now called FireGen Analytics).



**Serious Breach Linked to Chinese APTs Comes to Light**

The malicious version of the software was delivered between April 9 and April 25, 2015, and it was downloaded by at least one Windows system administrator working for a defense contractor.

While it's unclear exactly how many organizations downloaded the backdoored software in the April 9-25 timeframe, RSA said the portal that hosted it had numerous subscribers, including four major telecoms providers, over ten western military organizations, more than two dozen Fortune 500 companies, five major defense contractors, and tens of IT solutions providers, government organizations, banks and universities.

While RSA has not named the company whose systems were compromised, investigative journalist Brian Krebs determined that it was Canada-based Altair Technologies Ltd. The company offers firewall log analyzers, a Windows event monitoring product, and a repository of troubleshooting information related to Windows event log messages (EventID.Net).

Category: Russian-speaking Me...  
 > English-speaking Me...

Site: forum\_skyfraud

Tags: hacking (1)

-Suspect of hacking Forbes through Adobe Flash Player widget that delivers the Thought of the day page on the Forbes website.

- Malware used was written in simplified Chinese and similar to malicious software derusbi (which is unique to Chinese cyber espionage operators).

-May 2017 - Exploited Microsoft Windows vulnerability CVE 2017-0199. Leveraged RTF

attachments.

-May 2017 - End of May. Started using Microsoft Excel (XLSM) documents.

-Most recently - Added an application whitelisting bypass to the Microsoft Excel documents.

-Malware - BEACON, COBALTSTRIKE.

## News alert:Chinese Cyber Spies Infected Forbes.com

The firms said that they only identified a few organizations in financial and defense services which were targeted and declined to identify them. They also said that they were not sure if the hackers had succeeded in stealing any data but they believed that other visitors to Forbes.com were affected.

Partners of iSight are very much sure that the attacking group behind these attacks is a team of Chinese cyber espionage dubbed Codoso team (also publicly known as **Sunshop Group**) because the malware used in the campaign is similar to variants of Derusbi which is unique to operators of Chinese cyber espionage. CC domain is connected with a domain used in many campaigns related to Codoso Team and minimum three more sites hosted the same exploit before its public disclosure. These sites are related to Chinese unorthodox issues and the team of Codoso is frequently exploiting zero-day vulnerabilities in their attacks and has shown favoritism for watering hole attacks.

Category: Educational, Tech & Pr...  
> Tech, Gadgets & Scien...

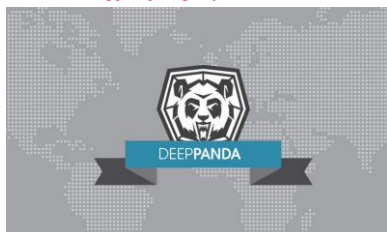
Site: forum\_jamiiforums

Tags: hacking (1) security (1)

### Connections to forums and other Hacker Groups

**Hacker Groups:** Shell Crew aka Deep Panda, Black Vine, WebMasters, KungFu Kittens, PinkPanther.

## 22. Shell Crew aka Deep Panda, Black Vine, WebMasters, KungFu Kittens, PinkPanther.



**Operating since:** 2014.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-Suspected ties to Chinese government.

### Chinese groups main targets: Political, Industrial, Terrorist Organization.

**Political** - National Security think tanks, government defence.

**Industrial** - Financial, legal, telecommunications, Anthem Health Group

**Terrorist Organizations** - June 18th, 2014 targeting began - **Possibly Daesh in Iraq to protect**

**Chinese oil interest in the region.**

### Countries Chinese hacker groups target

Western Countries

Asia Pacific region.

Iraq & Middle East - target change since 2014.

### TTP's etc.

-Suspected to be State Funded.

-Western countries targeted through Terracotta VPN nodes to exploit sensitive targets. Use Terracotta VPN node Internet addresses that are used to send phishing emails targeting users in targeted organizations.

-Script planted in victims windows computers, that once executed, it downloads and executes from memory a .NET executable (aka Wafer), which then downloads and runs MadHatter.NET Remote Access Tool (RAT). -This is a favourite of Deep Panda. By running from memory, no disk artifacts or host based IOCs that can be ID in forensic analysis.

- Used Windows PowerShell to infiltrate think tanks.

- **Considered highly stealthy.**

### Connections to forums and other Hacker Groups

**Hacker Groups:** APT19 aka Codoso Team, Sunshop Group.

## Serious Breach Linked to Chinese APTs Comes to Light



While Altair representatives said they don't expect large organizations to use the EvLog tool, the company's main website claims the EventID.Net portal has helped millions of users worldwide. SecurityWeek has reached out to Altair Technologies for clarifications.

RSA pointed out that the defense contractor targeted by Kingslayer was attacked only 11 weeks after the breach of Altair's systems, which suggests that the attackers may have focused on other targets in those 11 weeks.

Evidence uncovered by RSA suggests that the attack was linked to **Shell Crew**, aka **Deep Panda**, and **Codosi**, aka **Sunshop Group**. Both **Shell Crew** and **Codosi** are advanced persistent threat (APT) groups believed to be operating out of China.

RSA also pointed to similarities with another supply chain attack known as the 2014 Monju incident, which targeted a nuclear facility in Japan. That attack was also linked to China.

Category:

[Russian-speaking Me...](#)

> [English-speaking Me...](#)

Site:

[forum\\_skyfraud](#)

Tags:

[hacking \(1\)](#)

## 23. APT30

**Operating since:** 2005.

### Main actors/leaders and structure

Unknown.

### Government entities, on contract with the government or civilians

-Suspected ties to Chinese government.

### Chinese groups main targets: Political.

**Political** - Members of the Association of Southeast Asian Nations (ASEAN).

### Countries Chinese hacker groups target

- Brunei Darussalam
- Cambodia
- Indonesia
- Lao PDR
- Malaysia
- Myanmar
- Philippines
- Singapore
- Thailand
- Vietnam
- India

## Russian-based Hackers Use Two Zero-day Exploits In One Attack

VS

visa | 4/21/2015, 9:11:00 PM post

Category:  
PrvtZone > Home

Site:  
forum\_prvtzone

Tags:  
hacking (1)

Security firm FireEye issued a report on April 18 alleging that Operation RussianDoll made use of two zero-day flaws—one in Adobe Flash and the other in Microsoft Windows—in a targeted attack. FireEye has labeled the hacker group behind the attack as APT28, which is operating out of Russia and may have ties to the Russian government. "The target firm is a foreign government entity in an industry vertical that aligns with known APT28 targeting," Darien Kindlund, director of threat intelligence at FireEye, told eWEEK. "We cannot be any more specific than that. We detected this attack in real time, reporting the attack to the victim accordingly." FireEye's APT28 RussianDoll attack report comes barely a week after the security firm released a report on a Chinese hacker group identified as APT30 that has been exploiting governments across Southeast Asia since 2005.

more info: <http://www.eweek.com/security/russian-based-attackers-use-two-zero-days-in-one-attack.html>

### TTP's etc.

-Suspected to be State Funded.

**-Active over long periods.**

-Modifies and adapts source code to continue using the same tools, tactics and infrastructure.

-Appears to work in groups and in shifts.

- Capable of infecting air-gapped networks.
- Uses a suite of tools - downloaders, backdoors, central controllers.
- Malware - SHIPSHAPE, SPACESHIP, FLASHFLOOD.

### **Connections to forums and other Hacker Groups**

## **24. Winnti Group aka Winnti Umbrella, Wicked Panda, LEAD, Barium, GREF, PassCV.**

Operating since: 2007.

### **Main actors/leaders and structure**

Unknown actors.

**-Structure - Chinese state intelligence.**

### **Government entities, on contract with the government or civilians**

-High confidence of connection to Chinese state intelligence - some elements located in Xicheng district of Beijing.

### **Chinese groups main targets: Political, Industrial.**

**Political** - High profile political targets include Tibetan journalists, Uyghur and Tibetan activists. Primary long-term mission appears political.

**Industrial** - Software and gaming organizations, high value technology organizations.

### **Countries Chinese hacker groups target**

-United States

-Japan

-South Korea

-Tibet

### **TTP's etc.**

-Suspected to be State Funded.

**-Active from 2007 until 2018 - continue to be very successful.**

-TTP's are consistent.

-Experiment with new tooling and attack methodologies often.

**-Operational mistakes during attacks have provided attacker locations with high confidence.**

-Primary attacks focus on theft of code signing certificates.

-Secondary attacks focus on financial gain.

-Malware - Winnti.

## Microsoft targets state-sponsored hackers in latest 'Patch



GS

guest | 5/10/2018, 3:30:19 PM

paste

Microsoft Corp. has focused on addressing vulnerabilities being used by suspected state-sponsored hackers as part of its monthly "Patch Tuesday" release, issuing patches for two actively targeted new attacks used to steal data.

In one case, an advanced persistent threat group, which is nearly always used as a term to describe state-sponsored hacking groups, has been targeting a Windows VBScript Engine Remote Code Execution Vulnerability first discovered in April.

"In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website," Microsoft said in a security advisory.

The second vulnerability, a privilege-escalation flaw in the Win32k component of Windows that is also being actively exploited, allows an attacker to run arbitrary code in kernel mod. "An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights," Microsoft explained.

Exactly which APTs are targeting the vulnerabilities is not clear, although at least one of the attacks was first detected by Chinese antivirus maker Qihoo 360 Core, suggesting that the attacks may be coming from China as opposed to Russia. The link to China comes a day after ProtectWise Inc. released a report claiming that many previous hacks thought to have come from APT groups, dubbed the **Winnti Umbrella**, were coordinated by "Chinese state intelligence apparatus."

Category:

Site:

[paste\\_pastebin](#)

Tags:

exploit (1)

hacking (1)

### Connections to forums and other Hacker Groups



## Bibliography

- "Advanced Persistent Threat Groups." FireEye. 2018. Accessed March 28, 2018.  
<https://www.fireeye.com/current-threats/apt-groups.html>.
- "ASEAN Member States." ASEAN | ONE VISION ONE IDENTITY ONE COMMUNITY. Accessed March 28, 2018. <http://asean.org/asean/asean-member-states/>.
- Ashok. "China Hacking South Korea Organisations to Block Missile Defence Efforts Claim Researchers." International Business Times UK. April 22, 2017. Accessed April 18, 2018.  
<http://www.ibtimes.co.uk/china-hacks-south-korea-attempt-block-missile-defence-efforts-claim-researchers-1618099>.
- "APT 10's Cloud Hopper Campaign Exposed." SC Media US. April 07, 2017. Accessed April 18, 2018.  
<https://www.scmagazine.com/report-exposes-apt-10s-cloud-hopper-campaign/article/648775/>.
- "APT Groups." Fireeye.com. Accessed April 18, 2018.  
<https://www.fireeye.com/current-threats/apt-groups.html>.
- Azani, Eitan. *Cyber-Terrorism Activities*. Report no. Report No.,3. International Institute of Counter-Terrorism, IDC Herzliya. 2012.
- Azani, Eitan. *Cyber-Terrorism Activities Report*. Report no. Report No.,13. International Institute for Counter-Terrorism, IDC Herzliya. 2015.
- Blair, Dennis C., and Keith Alexander. "China's Intellectual Property Theft Must Stop." The New York Times. August 15, 2017. Accessed April 18, 2018.  
<https://www.nytimes.com/2017/08/15/opinion/china-us-intellectual-property-trump.html>.
- "Blue Termite APT Group Focuses on Japanese Organizations." Security Affairs. November 28, 2016. Accessed April 18, 2018. <http://securityaffairs.co/wordpress/39472/cyber-crime/blue-termite-apt.html>.
- Breene, Keith. "Who Are the Cyberwar Superpowers?" World Economic Forum. Accessed April 18, 2018.  
<https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/>.
- Brown, Peter J. "How Russian and Chinese Hackers Are Different." Asia Times. February 21, 2017. Accessed April 18, 2018. <http://www.atimes.com/article/russian-chinese-hackers-different/>.
- "Chinese Hackers, Businesses and Government Coordinate Cyber Efforts." SIGNAL Magazine. July 01, 2016. Accessed April 18, 2018. <https://www.afcea.org/content/?q=Article-chinese-hackers-businesses-and-government-coordinate-cyber-efforts>.

"China-based Hacker Groups to Target India, Hong Kong in 2018: FireEye." Business Standard. December 07, 2017. Accessed April 18, 2018. [http://www.business-standard.com/article/current-affairs/china-based-hacker-groups-to-target-india-hong-kong-in-2018-fireeye-117120701204\\_1.html](http://www.business-standard.com/article/current-affairs/china-based-hacker-groups-to-target-india-hong-kong-in-2018-fireeye-117120701204_1.html).

"Connect the Dots on State-Sponsored Cyber Incidents." Council on Foreign Relations. Accessed April 18, 2018. <https://www.cfr.org/interactive/cyber-operations/apt-16>.

"CVE-2015-2545: Overview of Current Threats." Securelist - Kaspersky Lab's Cyberthreat Research and Reports. May 25, 2016. Accessed April 18, 2018. <https://securelist.com/cve-2015-2545-overview-of-current-threats/74828/>.

"Cyber Desk." International Institute for Counter-Terrorism. Accessed April 18, 2018. <https://www.ict.org.il/Articles.aspx?WordID=99#gsc.tab=0&gsc.sort=>.

"Deep in Thought: Chinese Targeting of National Security Think Tanks »." CrowdStrike. May 12, 2017. Accessed April 18, 2018. <https://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/>.

"DragonOK APT Is Adopting New Tactics, Techniques and Procedures." Security Affairs. September 02, 2017. Accessed April 18, 2018. <http://securityaffairs.co/wordpress/62615/apt/dragonok-apt-changes-ttps.html>.

"Donald Trump Threatens Tariffs on Chinese Industrial Goods." Financial Times. Accessed April 04, 2018. <https://www.ft.com/content/42fb1100-378f-11e8-8eee-e06bde01c544>.

"Elderwood Platform Is Still Providing Zero-Day Exploits." Security Affairs. May 17, 2014. Accessed April 18, 2018. <http://securityaffairs.co/wordpress/25002/hacking/elderwood-platform-still-active.html>.

Fox-Brewster, Thomas. "Forbes.com Hacked In November, Possibly By Chinese Cyber Spies." Forbes. February 25, 2015. Accessed April 18, 2018. <https://www.forbes.com/sites/thomasbrewster/2015/02/10/forbes-com-hacked-in-november-possibly-by-chinese-cyber-spies/#1e2eddbb26b9>.

Franceschi-Bicchierai, Lorenzo. "How the Chinese Government Became the World's Hacking Superpower." Motherboard. July 26, 2016. Accessed April 18, 2018. [https://motherboard.vice.com/en\\_us/article/pgkq49/how-the-chinese-government-became-the-worlds-hacking-superpower](https://motherboard.vice.com/en_us/article/pgkq49/how-the-chinese-government-became-the-worlds-hacking-superpower).

Graham. "Iron Tiger: How Hackers Have Stolen Terabytes of Confidential Data from US High-tech Firms."

The State of Security. September 17, 2015. Accessed April 18, 2018.

<https://www.tripwire.com/state-of-security/security-data-protection/iron-tiger-data-us-firms/>.

Groll, Elias. "Feds Quietly Reveal Chinese State-Backed Hacking Operation." *Foreign Policy*. November 30,

2017. Accessed April 18, 2018. <http://foreignpolicy.com/2017/11/30/feds-quietly-reveal-chinese-state-backed-hacking-operation/>.

"Hidden Lynx - Professional Hackers for Hire." *Symantec - Security Response*. 2013, no. 1 (2013): 1-28.

doi:10.1016/s1353-4858(10)70039-8.

Hsu, Philip. "Chinese Hacking Against Taiwan: A Blessing for the United States?" *The Diplomat*. January 23,

2018. Accessed April 18, 2018. <https://thediplomat.com/2018/01/chinese-hacking-against-taiwan-a-blessing-for-the-united-states/>.

Intelligence, FireEye ISIGHT. "APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat « APT10 (MenuPass Group): New Tools, Global Campaign

Latest Manifestation of Longstanding Threat." *FireEye*. April 06, 2017. Accessed April 18, 2018.

[https://www.fireeye.com/blog/threat-research/2017/04/apt10\\_menupass\\_grou.html](https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html).

McReynolds, Joe. "In a Fortnight." *China Brief* 14, no. 8 (April 24, 2014): 1-3. *International Security & Counter Terrorism Reference Center*, EBSCOhost (accessed March 21, 2018).

Nash-Hoff, Michele. "What Could Be Done about China's Theft of Intellectual Property?" *IndustryWeek*.

June 28, 2017. Accessed April 18, 2018. <http://www.industryweek.com/intellectual-property/what-could-be-done-about-chinas-theft-intellectual-property>.

"Operation CloudyOmega: Ichitaro Zero-day and Ongoing Cyberespionage Campaign Targeting Japan."

Symantec Security Response. Accessed April 18, 2018.

<https://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan>.

Palmer, Danny. "Chinese Hacking Group Returns with New Tactics for Espionage Campaign." *ZDNet*.

November 03, 2017. Accessed April 18, 2018. <http://www.zdnet.com/article/chinese-hacking-group-returns-with-new-tactics-for-espionage-campaign>.

"REDBALDKNIGHT/BRONZE BUTLER's Daserf Backdoor Now Using Steganography." *TrendLabs*

Security Intelligence Blog. November 09, 2017. Accessed April 18, 2018.  
<https://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/>.

Richard. "China's State Hackers Operate On The Darknet." AlphaBay Market. June 15, 2016. Accessed April 18, 2018. <https://alphabaymarket.com/chinas-state-hackers-operate-on-the-darknet/>.

"SecureWorks Shed Light on BRONZE BUTLER Group That Targets Japanese Enterprises." Security Affairs. October 14, 2017. Accessed April 18, 2018.  
<http://securityaffairs.co/wordpress/64311/apt/bronze-butler-ttps.html>.

Solomon, Shoshanna. "'Winter' of Cyber-threats Is Coming, Experts Warn." The Times of Israel. Accessed April 18, 2018. <https://www.timesofisrael.com/winter-of-cyber-threats-is-coming-experts-warn/>.

"Taiwan Opposition Hacked as China's Cyberspies Step up Attacks." The Business Times. Accessed April 18, 2018. <http://www.businesstimes.com.sg/government-economy/taiwan-opposition-hacked-as-chinas-cyberspies-step-up-attacks>.

Tom, and Hegel. "Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers." *ProtectWise 401TRG*, ProtectWise 401TRG, 3 May 2018, [401trg.pw/burning-umbrella/](http://401trg.pw/burning-umbrella/).



## ABOUT THE ICT

Founded in 1996, the International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world, facilitating international cooperation in the global struggle against terrorism. ICT is an independent think tank providing expertise in terrorism, counter-terrorism, homeland security, threat vulnerability and risk assessment, intelligence analysis and national security and defense policy.

ICT is a non-profit organization located at the Interdisciplinary Center (IDC), Herzliya, Israel which relies exclusively on private donations and revenue from events, projects and programs.

## ABOUT ICT CYBER-DESK

The Cyber Desk Review is a periodic report and analysis that addresses two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse) and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack).

The Cyber Desk Review addresses the growing significance that cyberspace plays as a battlefield in current and future conflicts, as shown in the recent increase in cyber-attacks on political targets, crucial infrastructure, and the Web sites of commercial corporations