

2015年09月24日星期四【萬年歷】

搜尋

[首頁](#) > [新聞](#) > [大陸新聞](#) > [大陸政治](#) > 正文

中共軍隊黑客再曝光 成都軍區78020部隊



【字號】大中小

更新: 2015-09-23 21:23:03 PM 標籤: [中共黑客](#), [成都軍區](#), [78020部隊](#)

【大紀元2015年09月24日訊】（大紀元記者海寧編譯報導）中共解放軍總參謀部第61所下屬的黑客部隊（全部以「61」開頭）已經廣為世界所知。但美國網絡安全公司ThreatConnect和諮詢公司DGI共同發表的一份報告稱，中共軍隊還存在其它的黑客部隊，如[成都軍區78020部隊](#)就是其中之一。



一個中共黑客的軌跡

《華爾街日報》報導說，明面上葛星是中共[成都軍區78020部隊](#)的一名泰國政治研究者，曾在中國雜誌上發表多篇有關泰國政治民主化議題的學術文章。

ThreatConnect和DGI通過對其社交網絡發言的分析表明，葛星居住在昆明，最近有了孩子，是一名山地車愛好者。他駕駛一輛白色大眾高爾夫轎車，偶爾批評一下中共政府。此人似乎不像是個黑客。

但是，葛星在互聯網上的其它活動卻將他和一個專門攻擊對美國具有戰略意義目標的中共軍隊黑客團體連在一起。ThreatConnect和DGI的報告指，葛星以

及他所在的78020部隊和一個名叫「Naikon」的黑客組織有直接關聯。安全專家表示，在南海爭端中許多反對中共的國家的政府網絡曾被這個黑客團體成功入侵。

葛星被發現，是因為他違反了Naikon的一貫模式。爲了盜竊情報而不被發現，Naikon使用了幾百個特殊的互聯網域名。大多數此類域名模仿目標國家的真實網址。但是「greensky27」的域名卻很特立獨行。

通過對「greensky27」域名5年的研究，研究者們發現，此域名頻繁並長時間的訪問中國城市昆明的網址。DGI裡講中文的分析師順藤摸瓜，發現了使用「greensky27」網名並取得了該賬號在昆明的社交網絡記錄。

通過對比Naikon網絡中「greensky27」域名和社交網絡的賬號，研究者們發現了一個固定模式。比如2012年2月，黑客「greensky27」域名多次訪問北京的互聯網服務器。同一天，騰訊微博上的用戶「greensky27」發微博說正在北京。同年11月，百度用戶「greensky27」在百度發帖說生了個男孩。此後黑客「greensky27」的域名沉寂了一個多星期，和休假照顧老婆孩子吻合。

2013年，騰訊用戶「greensky27」發布的照片稱，他去雲南玉溪縣參拜了葛氏祠堂。葛星的全名、電話號碼以及工作單位從此曝光。但是，他的軍職和階級仍不明。

葛星於2011年和2013年在工作時間拍攝的天際線證實他確實是在中共軍隊工作。這些照片顯示，其拍攝地點是昆明市中心的軍隊大院內部。另一系列照片中有積雪覆蓋的車輛、停車場和水塔，也被證實是在同一地點拍攝。《華爾街日報》記者最近的實地調查證明，該大院的確屬於中共解放軍78020部隊。但該部隊宣傳辦公室人員拒絕透露葛星是否在那裡工作。

網名為「greensky27」的用戶對自己的軍隊背景從不隱瞞。騰訊用戶「greensky27」稱，自己於1998年畢業於中國解放軍國際關係學院。2014年，同一用戶發布了一系列遊覽該大學南京校區的照片，並附言說「只貼不說，自己看」。幾週後，他又發布了解放軍火災演練以及慶祝中共建軍87週年活動的照片。自從葛星2012年有了兒子之後，他的社交媒體發言轉向家庭生活、天氣和旅行。但在《華爾街日報》記者和葛星通話後不到一天，騰訊賬戶「greensky27」即被刪除。

對黑客域名「greensky27」的分析發現，此人有正常的每週工作時間。這名黑客一般北京時間每天早上9點上線，然後在下午6點下線。在中國新年期間，此人一般不上線，但是也有例外。2012年中國新年（1月23日）期間，「greensky27」照例休假。但在一個菲律賓代表團同美國展開有關軍事合作的對話曝光之後，「greensky27」突然在一天之後的1月27日再度活躍。

ThreatConnect的數據表明，2012年起，黑客域名「greensky27」頻繁訪問泰國的域名和網址。2014年5月美國司法部起訴了5名中共61398部隊的黑客之後，其訪問量開始下降。

葛星於2008年發表的兩篇論文中，作者單位均為78020部隊。該部隊是成都軍區的技術偵查部隊，駐地在昆明。美國2049計劃研究所執行主任斯托克斯（Mark Stokes）是中國軍隊在情報收集和網絡間

諜中角色的權威。他表示，中共解放軍一共有20多個類似78020部隊的建制，其功能為情報收集與分析以及計算機網絡防禦和攻擊。

成都軍區的職責之一是負責維護西藏安全，此外還有維護中共和越南、緬甸以及印度的邊界。斯托克斯說，成都軍區還有另一支類似78020部隊的黑客組織，專門針對流亡西藏精神領袖達賴喇嘛身邊的網絡系統。他說，因此78020部隊去收集有關南海的情報理所當然。

ThreatConnect和DGI發現，葛星在社交媒體上的用戶名為「greensky27」。而黑客組織Naikon裡，也有一個「greensky27」。在此報告發表前，ThreatConnect和DGI將其草稿交給了《華爾街日報》。今年8月，《華爾街日報》記者在和葛星的短暫通話中，證實「greensky27」確為葛星在社交媒體上的用戶名，但葛星拒絕談論他是否是ThreatConnect和DGI報告中的主人公。他在電話中威脅《華爾街日報》記者說，如果見報，他就報告警察。從此以後，葛星再沒有接電話，也沒有回復短信。ThreatConnect公司說，《華爾街日報》記者在和葛星通話後大約一小時，黑客組織Naikon中的用戶「greensky27」就停用了，近來一直處於離線狀態。

葛星的社交媒體發言表明他是一個山地車愛好者。昆明一個自行車俱樂部的創建人認出了葛星的照片，說他有時會加入該俱樂部在昆明地區的騎行活動。

像許多中國的戶外運動愛好者一樣，葛星在想到污染的天空時就流露出期盼的念頭。在一張於78020部隊大院內拍攝的天空照片中，葛星評論道：「今天空氣質量一般。祝願大家和平，世界安寧」。

中共黑客組織Naikon

Naikon這個名字來自該組織使用的一款惡意軟件中的一段代碼。該組織慣於使用精心打造的釣魚電子郵件，誘使收件人打開其帶有惡意軟件的附件。俄國反病毒軟件公司卡巴斯基實驗室表示，Naikon過去使用的附件中，有老撾選美大賽佳麗拍攝的日曆、有關戰略話題的英文或本地語言新聞以及看上去像機密的備忘錄等。卡巴斯基實驗室稱，Naikon使用這種被稱之為「釣魚」的技術，成功的打入越南、菲律賓以及其它南亞國家的政府、軍隊、媒體和能源公司網絡。

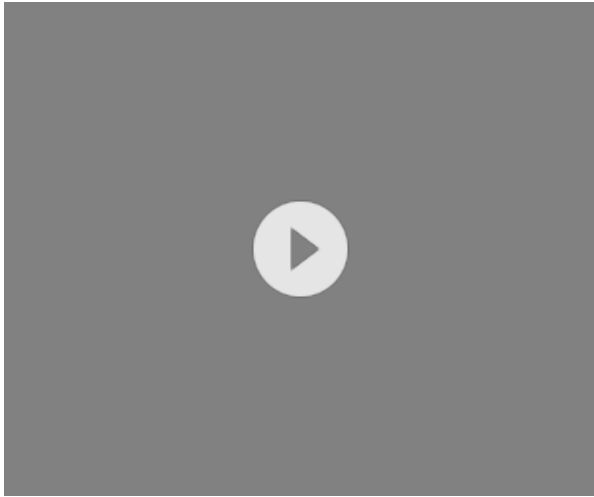
供職於ThreatConnect公司的巴格爾（Richard Barger）說，和俄國黑客使用的惡意軟件相比，Naikon的病毒還處於「石器時代」。但因為Naikon的對手不夠老道，因此Naikon的成功率很高。

責任編輯：黃小渝

相關文章

- [【禁聞】法廣：中共開兩條件交換令完成](#) 9/21/15
- [美網絡專家：習訪美前 中共黑客攻擊收斂](#) 9/20/15
- [習訪美前 奧巴馬暗示將制裁中共黑客](#) 9/18/15
- [習近平訪美前夕白宮或制裁黑客 北京緊張](#) 9/15/15

- 美情報總監：加強網絡安全對抗中共黑客 9/12/15
- 華府制裁中共黑客 北京以非正統方式回應圖 9/10/15
- 美國最快下週制裁中共黑客圖 9/5/15
- 克里：中共和俄羅斯很可能偷看了我的電郵圖 8/12/15
- NBC：中共竊取奧巴馬政府高官私人電郵圖 8/11/15
- 英手機零售商被黑客攻擊 240萬信息洩漏圖 8/10/15



👍 4.8 萬

0

0

0

in



f 讚

f 分享

Tweet

G+1

in 分享

Recommended



中共治下女警察們駭人聽聞的暴行



蘇軾驚夢回文詩 茶禪一味



馬桶不通 5招教你快速疏通



我該送14歲的兒子去餐館打工嗎？



9月28日——罕見連環四血月 天文學家驚嘆

如果您有新聞線索或資料給大紀元，請進入[安全投稿爆料平台](#)。

前列腺

男人不得不關心的事

BAYER



前列腺癌通常沒有任何徵狀...
美國第二大癌症死因...

詳情請見

最熱新聞



共青團重提共產主義接班人 任志強撰文炮轟
人氣 26023

f 讚

分享

0



罪惡必遭清算 德國91歲女性納粹成員受審

人氣 14099

f 讚 分享 0



江迫害法輪功成沉重包袱 習抓江可解困局

人氣 11722

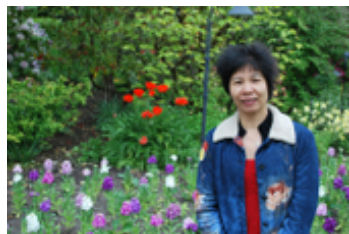
f 讚 分享 0



習近平車隊司機：法輪功學員給人類希望

人氣 11060

f 讚 分享 0



中國學生加國殺母 臥底探員還原謀殺情節

人氣 8698

f 讚 分享 0

獨家視角

»

- 習近平訪美令人關注的議題（完整版） 圖
- 谷俊山大案背後的較量（完整版） 圖
- 夏小強：陸媒透露江澤民閱兵露面真相 圖
- 江露面與否不重要 習閱兵前釋信號 圖
- 天津大爆炸真相探秘（完整版） 圖
- 不見血的謀殺 上百精神病院的政治任務 圖

娛樂追星

»

EXO陸團員解約模式 專家憂：韓國成跳板

人氣 968

 讚

分享

0

新片《實習生》紐約首映 海瑟薇盛裝亮相

人氣 666

 讚

分享

0

宋承憲被安排秀甜蜜 劉亦菲羞拒男友抱起

人氣 366

 讚

分享

0

常楓周遊獲金鐘「特別貢獻獎」聚餐同樂

人氣 348

 讚

分享

0

貝克漢姆對小七難說不 貝嫂更嚴肅

人氣 339

讚 分享 0

評論: [我要發言](#) [看留言](#) [聯係編輯](#) [推薦好友](#)

「大紀元將選取精彩讀者評論在全球報紙版面上刊登，請您與我們一起記錄歷史」
「大紀元保留刪除髒話貼、下流話貼、攻擊個人信仰貼等惡意留言的權利」


發表留言

大紀元網友

發表時間:12小時41分鐘以前


不過是小挫人用錢奴役的狗奴才。社會蛀蟲一條。

[【舉報】](#) | [【推薦】](#) | [【跟評】](#)



**Save your own PC.
Now at BEST BUY**

[LEARN MORE](#)



**FIX ME
STICK**
VIRUS REMOVAL DEVICE

【禁聞】法廣：中共開兩條件交換令完成



【大紀元2015年09月21日訊】(新唐人周玉林編輯報道)中共黑客攻擊美國政府和公司，竊取人事和商業機密的事件，一直受到美國方面的譴責。在中共國家主席習近平訪美前夕，美國網路安全專家說，最近幾個月，中共黑客的網路襲擊行動明顯減緩。[下載觀看](#)

習訪美前 中共黑客攻擊收斂

習近平將於9月22號至28號，對美國進行國事訪問。據英國「路透社」報導，在中共和美國就習近平訪美一事開始磋商之後，中共黑客似乎有所收斂。專門調查複雜網路攻擊事件的曼迪安公司創始人曼迪亞說，近來美國公司因網路攻擊而洩密的新增事件正在減少。美國網路安全公司賽蘭斯（Cylance）和Trend Micro也注意到了中共網路攻擊有所下降的趨勢。

今年7月，美國聯邦調查局FBI說，過去12個月的經濟間諜案猛增了53%，其中中共是最大的攻擊來源國。

法廣：中共開兩條件交換令完成

而隨著習近平訪美日期的臨近，有關中共前中央辦公廳主任令計劃的弟弟令完成的傳言，也再次被海外媒體熱炒。有觀點認為，令完成遣返事件也將成為美中兩國之間協商的議題之一。

9月20號，《法國國際廣播電台》引述消息說，北京當局急於追回潛藏在美國的令完成，在與美方的秘密談判中，向美方開出了兩個條件，聲稱如果美國能把令完成交給中方，第一，中共將放棄追回令完成在美國全部資產的權利，涉及金額大約6億美元。第二，中共願意接收美國遣返的2萬5千名非法中國移民。

早前《紐約時報》曾報導說，藏匿在美國的令完成，赴美時帶走了大量令人難以置信的中共高層機密，這些機密是他的兄長令計劃交給他的。

這些機密的具體內容外界一直不得而知。9月19號，《法廣》還報導說，有消息透露，令完成手中的核心機密，首先是中共在海外的間諜名單，其中包括中高層以上的間諜網路負責人名單。

其次是中共高層官員的人事關係資料，其中包括江澤民時代和胡錦濤時代的領導人詳情，這些資料連最高領導人本人可能都不全部知情。

報導說，如果這些資料交給美國，美國對中國將有針對性的制定政策，造成的損失遠超犧牲一些間諜人員。

責任編輯：安妮

相關文章

- 習訪美「解決」令完成？四消息被密集釋放 9/21/15
- 令完成疑掌握涉高層機密及海外間諜名單 9/21/15
- 周曉輝：或涉令家 青島報業總經理被查 9/20/15
- 美首遣返「紅通人員」當局意在令完成 9/20/15
- 習近平要訪美 令計劃又「瘋」了圖 9/20/15
- 傳孟建柱要求美方遣返令完成和郭文貴圖 9/18/15

- 圍繞令完成 中美想法不一圖 9/17/15
- 習近平訪美前 令完成等中方追捕名單再惹關注圖 9/17/15
- 落馬中信總經理被曝攜令完成玩轉百元股 9/17/15
- 令計劃姐夫被免職 中美或合作抓令完成圖 9/16/15



A Bayer advertisement for prostate health. The background is a close-up photograph of a large green leaf with prominent veins. In the center, the Chinese characters "前列腺" (Prostate) are written in large, bold, white font. Below this, the phrase "男人不得不關心的事" (Something men can't ignore) is written in a smaller, bold, white font. Underneath that, in a smaller, regular, white font, is "多關心 多健康" (Care more, be healthier). In the lower-left quadrant, the Bayer logo is displayed, which is a circular emblem with the word "BAYER" written vertically inside. At the bottom of the advertisement, two lines of white text are present: "前列腺癌通常沒有任何徵狀..." (Prostate cancer usually has no symptoms...) and "美國第二大癌症死因..." (Second leading cause of cancer death in the US...). At the very bottom, there is a dark green rectangular button with the white text "詳情請見" (See details).

即時	評論	社區新聞	副刊	體育	娛樂
北美新聞	財經評論	紐約	文化新聞	國際足球	明星--內地
台灣新聞	外電評論	舊金山	神傳文化	中國足球	明星--港台
大陸新聞	環球好評	洛杉磯	生命探索	籃球	明星--日韓
國際新聞	時政評論	華府	人生感悟	網球	明星--歐美
港澳新聞	九評三退	波士頓	文學世界	棋牌	影視--華語
科技新聞	諷刺幽默	新澤西	史海鉤沉	棒球	影視--環球
財經消息	紀元社論	美南	人物春秋	其他	樂壇風景線
台灣地方	專欄文集	美東南	教育園地	網聞	電子報
社會新聞	以史為鑒	美中	奇聞異事	論壇新聞	關於我們

文化學術	費城	典故傳奇	網上真情	投稿中心
文藝娛樂	聖地亞哥	房產天地	悲情中國	廣告服務
編讀往來	西雅圖	留學移民	壇笑風生	萬年曆
紀元特稿	歐洲	醫療保健	讀者投書	
新穎視角	亞洲	生活時尚	犀利網評	
爭鳴商榷	澳洲	縱橫職場	網友親歷	
自由廣場	南美	美食天地	民謠/順口溜	
感悟隨筆	加拿大東	旅遊休閒	奇聞趣事	
一吐為快	加拿大西	藝術長河	談古論今	
	康州		網上文學	
	美國其它			

Copyright© 2000 - 2015 大紀元 授權與許可 服務條款