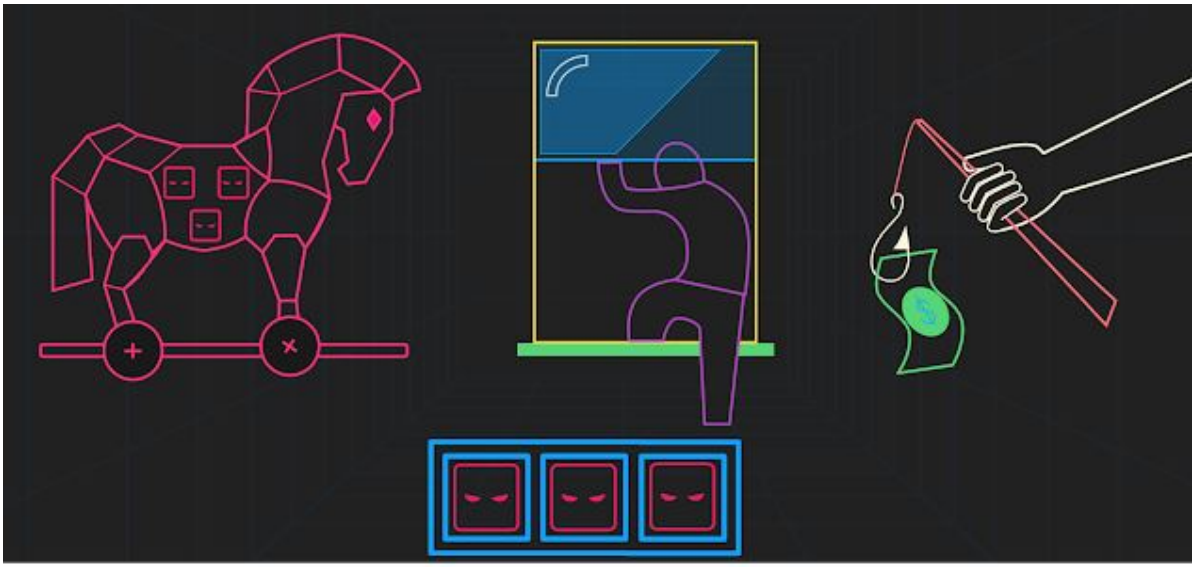
Tracing the Supply Chain Attack on Android

Published: 2019-06-25 · Archived: 2026-04-05 23:06:47 UTC

Earlier this month, **Google** disclosed that a supply chain attack by one of its vendors resulted in malicious software being pre-installed on millions of new budget Android devices. Google didn't exactly name those responsible, but said it believes the offending vendor uses the nicknames "**Yehuo**" or "**Blazefire**." What follows is a deep dive into the identity of that Chinese vendor, which appears to have a long and storied history of pushing the envelope on mobile malware.



"Yehuo" (野火) is Mandarin for "**wildfire**," so one might be forgiven for concluding that Google was perhaps using another dictionary than most Mandarin speakers. But Google was probably just being coy: The vendor in question appears to have used both "blazefire" and "wildfire" in two of many corporate names adopted for the same entity.

An online search for the term "yehuo" reveals an account on the **Chinese Software Developer Network** which uses that same nickname and references the domain **blazefire[.]com**. More searching points to a Yehuo user on **gamerbbs[.]cn** who advertises a mobile game called "Xiaojun Junji," and says the game is available at blazefire[.]com.

Research on blazefire[.]com via Domaintools.com shows the domain was assigned in 2015 to a company called "**Shanghai Blazefire Network Technology Co. Ltd.**" just a short time after it was registered by someone using the email address "**tosaka1027@gmail.com**".

The Shanghai Blazefire Network is part of a group of similarly-named Chinese entities in the "mobile phone pre-installation business and in marketing for advertisers' products to install services through mobile phone installed software."

“At present, pre-installed partners cover the entire mobile phone industry chain, including mobile phone chip manufacturers, mobile phone design companies, mobile phone brand manufacturers, mobile phone agents, mobile terminal stores and major e-commerce platforms,” reads a descriptive blurb about the company.

A historic records search at Domaintools on that tosaka1027@gmail.com address says it was used to register 24 Internet domain names, including at least seven that have been conclusively tied to the spread of powerful Android mobile malware.

Two of those domains registered to tosaka1027@gmail.com — elsyzsmc[.]com and rurimeter[.]com — were implicated in propagating the Triada malware. Triada is the very same malicious software Google said was found pre-installed on many of its devices and being used to install spam apps that display ads.

In July 2017, Russian antivirus vendor **Dr.Web** published research showing that Triada had been installed by default on at least four low-cost Android models. In 2018, Dr.Web expanded its research when it discovered the Triada malware installed on 40 different models of Android devices.

At least another five of the domains registered to tosaka1027@gmail.com — 99youx[.]com, buydudu[.]com, kelisrim[.]com, opnixi[.]com and sonyba[.]com — were seen as early as 2016 as distribution points for the Hummer Trojan, a potent strain of Android malware often bundled with games that completely compromises the infected device.

A records search at Domaintools for “Shanghai Blazefire Network Technology Co” returns 11 domains, including blazefire[.]net, which is registered to a **yehuo@blazefire.net**. For the remainder of this post, we’ll focus on the bolded domain names below:

Domain Name Create Date Registrar
2333youxi[.]com 2016-02-18 ALIBABA CLOUD COMPUTING (BEIJING) CO., LTD
52gzone[.]com 2012-11-26 ALIBABA CLOUD COMPUTING (BEIJING) CO., LTD
91gzonep[.]com 2012-11-26 ALIBABA CLOUD COMPUTING (BEIJING) CO., LTD
blazefire[.]com 2000-08-24 ALIBABA CLOUD COMPUTING (BEIJING) CO., LTD
blazefire[.]net 2010-11-22 ALIBABA CLOUD COMPUTING (BEIJING) CO., LTD
hsuheng[.]com 2015-03-09 GODADDY.COM, LLC
jyhxz.net 2013-07-02 —
longmen[.]com 1998-06-19 GODADDY.COM, LLC
longmenbiaoju[.]com 2012-12-09 ALIBABA CLOUD COMPUTING (BEIJING) CO., LTD
oppayment[.]com 2013-10-09 ALIBABA CLOUD COMPUTING (BEIJING) CO., LTD
tongjue[.]net 2014-01-20 ALIBABA CLOUD COMPUTING (BEIJING) CO., LTD

Following the breadcrumbs from some of the above domains we can see that “Blazefire” is a sprawling entity with multiple business units and names. For example, **2333youxi[.]com** is the domain name for **Shanghai Qianyou Network Technology Co., Ltd.**, a firm that says it is “dedicated to the development and operation of Internet mobile games.”

Like the domain blazefire[.]com, 2333youxi[.]com also was initially registered to tosaka1027@gmail.com and soon changed to Shanghai Blazefire as the owner.

The offices of Shanghai Quianyou Network — at Room 344, 6th Floor, Building 10, No. 196, Ouyang Rd, Shanghai, China — are just down the hall from **Shanghai Wildfire Network Technology Co., Ltd.,** reportedly at Room 35, 6th Floor, Building 10, No. 196, Ouyang Rd, Shanghai.

The domain tongjue[.]net is the Web site for **Shanghai Bronze Network Technology Co., Ltd.**, which appears to be either another name for or a sister company to **Shanghai Tongjue Network Technology Co., Ltd.** According to its marketing literature, Shanghai Tongjue is situated one door down from the above-mentioned Shanghai Quianyou Network — at Room 36, 6th Floor, Building 10, No. 196, Ouyang Road.

“It has developed into a large domestic wireless Internet network application,” reads a help wanted ad published by Tongjue in 2016. “The company is mainly engaged in mobile phone pre-installation business.”

That particular help wanted ad was for a “client software development” role at Tongjue. The ad said the ideal candidate for the position would have experience with “Windows Trojan, Virus or Game Plug-ins.” Among the responsibilities for this position were:

-Crack the restrictions imposed by the manufacturer on the mobile phone.
-Research and master the android [operating] system
-Reverse the root software to study the root of the android mobile phone
-Research the anti-brushing and provide anti-reverse brushing scheme

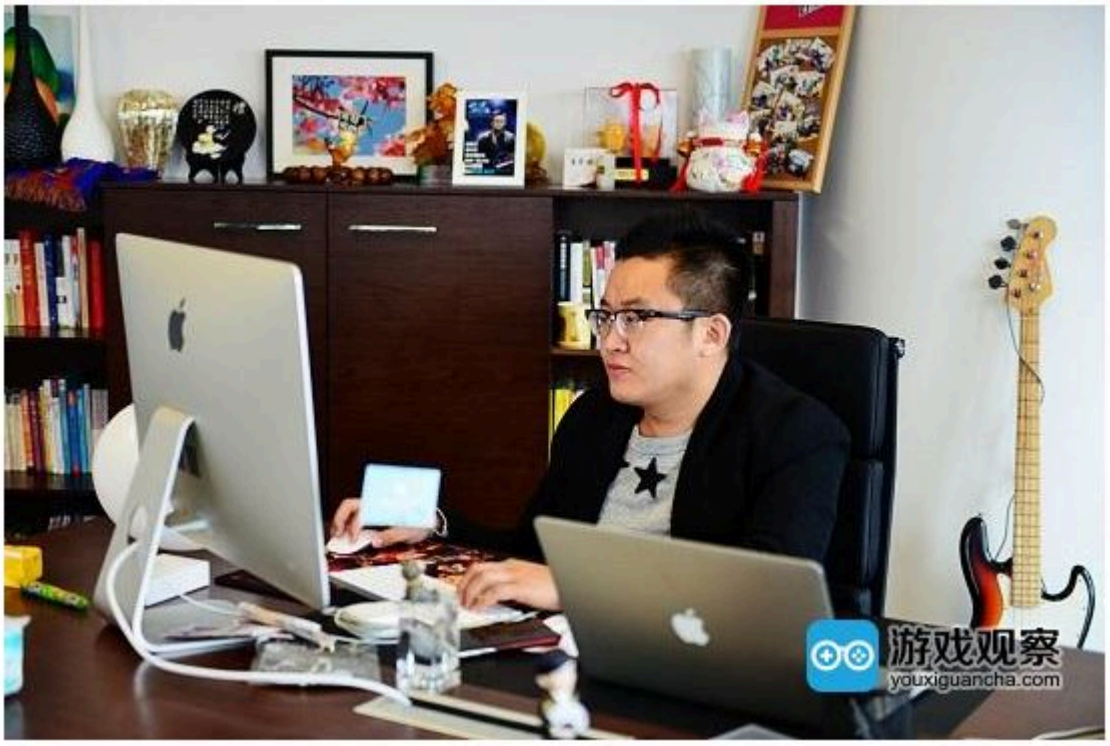
WHO IS BLAZEFIRE/YEHUO?

Many of the domains mentioned above have somewhere in their registration history the name “Hsu Heng” and the email address yehuo@blazefire.net. Based on an analysis via cyber intelligence firm 4iq.com of passwords and email addresses exposed in multiple data breaches in years past, the head of Blazefire goes by the nickname “Hagen” or “Haagen” and uses the email “**chuda@blazefire.net**“.

Searching on the phrase “chuda” in Mandarin turns up a 2016 story at the Chinese gaming industry news site Youxiguancha.com that features numerous photos of Blazefire employees and their offices. That story also refers to the co-founder and CEO of Blazefire variously as “Chuda” and “Chu da”.

“Wildfire CEO Chuda is a tear-resistant boss with both sports (Barcelona hardcore fans) and literary genre (playing a good guitar),” the story gushes. “With the performance of leading the wildfire team and the wildfire product line in 2015, Chu has won the top ten new CEO awards from the first Black Rock Award of the Hardcore Alliance.”

Interestingly, the registrant name “Chu Da” shows up in the historical domain name records for longmen[.]com, perhaps Shanghai Wildfire’s oldest and most successful mobile game ever. That record, from April 2015, lists Chu Da’s email address as yehuo@blazefire.com.



The CEO of Wildfire/Blazefire, referred to only as “Chuda” or “Hagen.”

It’s not clear if Chuda is all or part of the CEO’s real name, or just a nickname; the vice president of the company lists their name simply as “Hua Wei,” which could be a real name or a pseudonymous nod to the embattled Chinese telecom giant by the same name.

According to this cached document from Chinese business lookup service TianYanCha.com, Chuda also is a senior executive at six other companies.

Google declined to elaborate on its blog post. Shanghai Wildfire did not respond to multiple requests for comment.

It's perhaps worth noting that while Google may be wise to what's cooking over at Shanghai Blazefire/Wildfire Network Technology Co., Apple still has several of the company's apps available for download from the iTunes store, as well as others from Shanghai Qianyou Network Technology.
