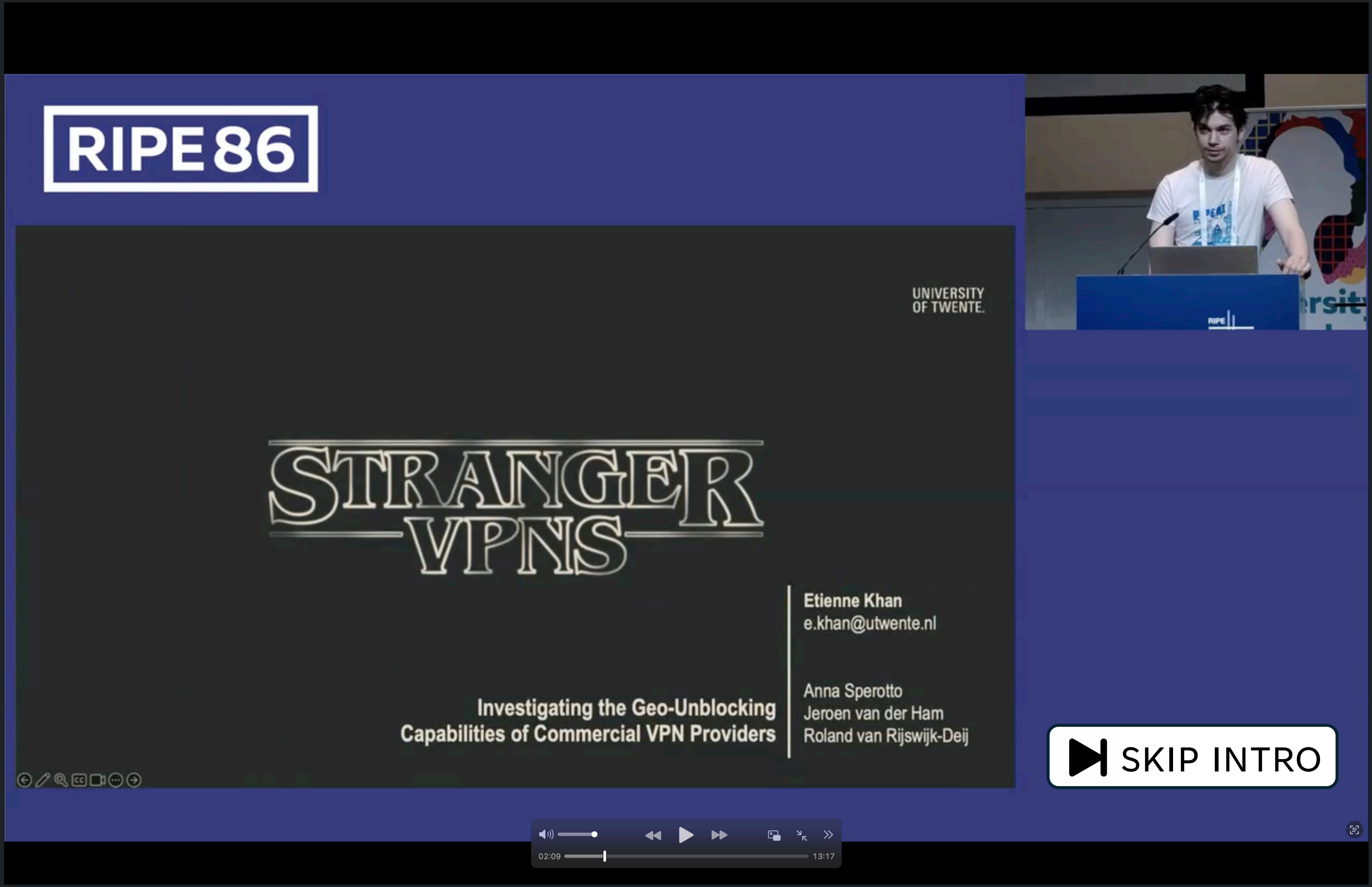
PREVIOUSLY ON…

Episode 1



RIPE86

UNIVERSITY OF TWENTE.

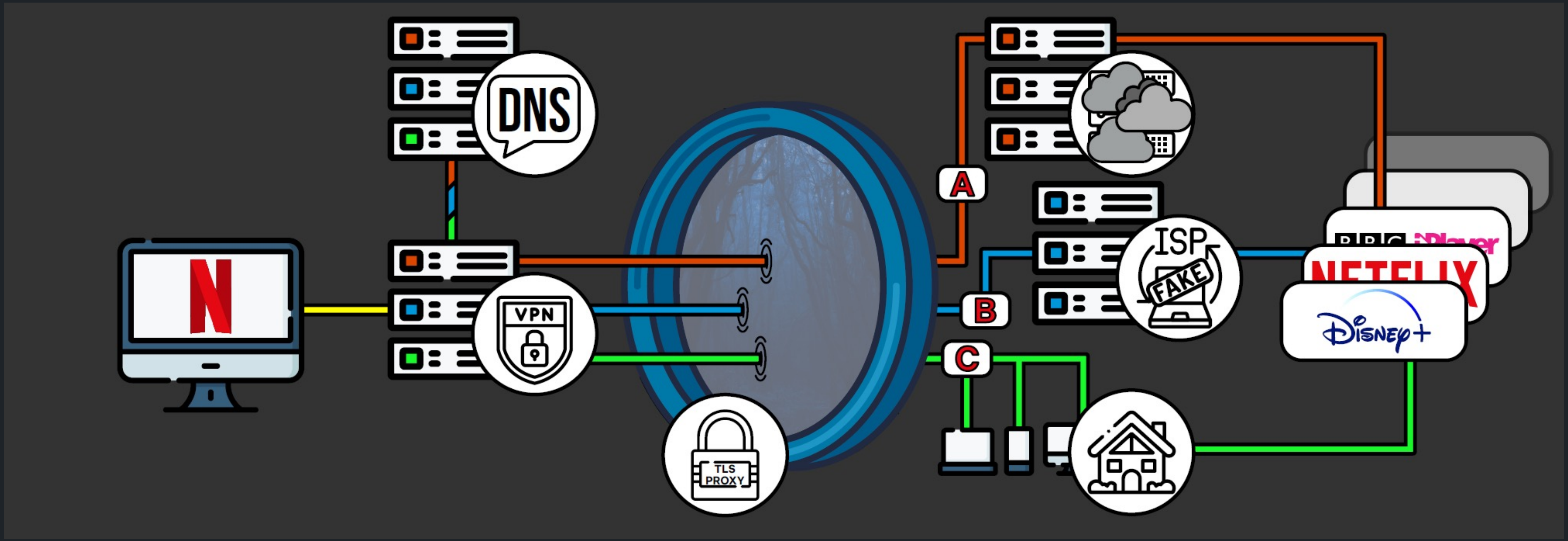
STRANGER VPNS

Investigating the Geo-Unblocking
Capabilities of Commercial VPN Providers

Etienne Khan
e.khan@utwente.nl

Anna Sperotto
Jeroen van der Ham
Roland van Rijswijk-Deij

Recap



Episode 2

UNIVERSITY
OF TWENTE.

A First Look at User-Installed Residential Proxies

From a Network Operator’s Perspective

Etienne Khan, Elisa Chiapponi, Martijn Verkleij,
Anna Sperotto, Roland van Rijswijk-Deij and Jeroen van der Ham-de Vos

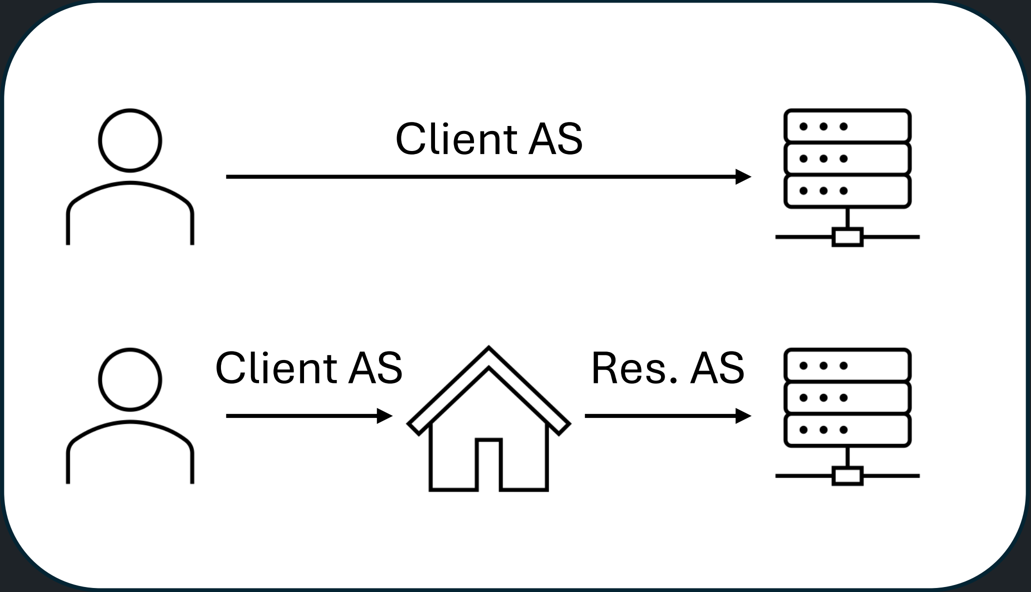
Episode 2

UNIVERSITY
OF TWENTE.

A First Look at User-Installed Residential Proxies

From a Network Operator’s Perspective

Residential Proxies



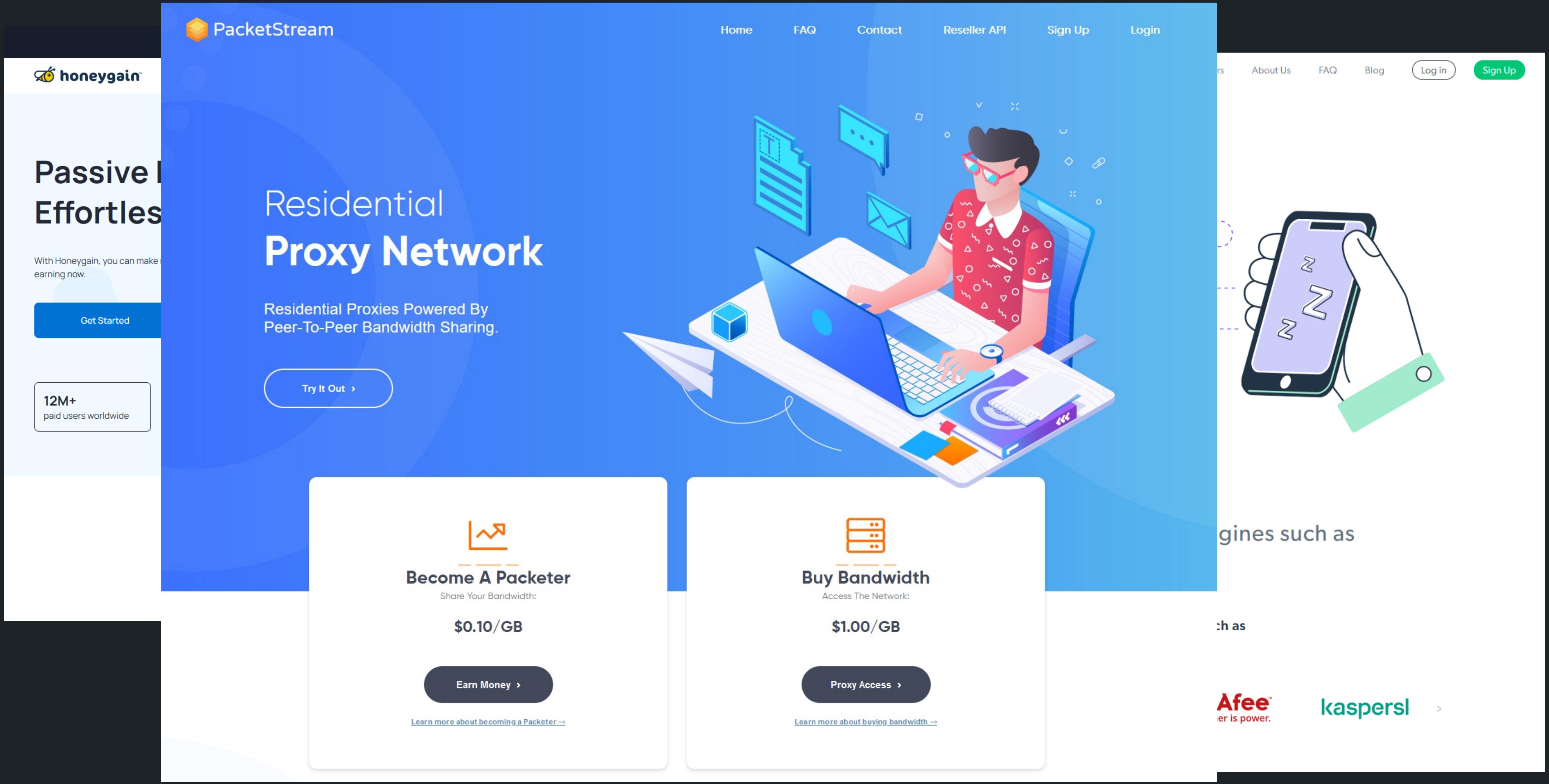
Episode 2

UNIVERSITY
OF TWENTE.

A First Look at User-Installed Residential Proxies

From a Network Operator’s Perspective

User-Installed



Passive I
Effortles

With Honeygain, you can make r
earning now.

12M+
paid users worldwide

Residential
Proxy Network

Residential Proxies Powered By
Peer-To-Peer Bandwidth Sharing.

Become A Packeter
Share Your Bandwidth:
$0.10/GB
Learn more about becoming a Packeter →

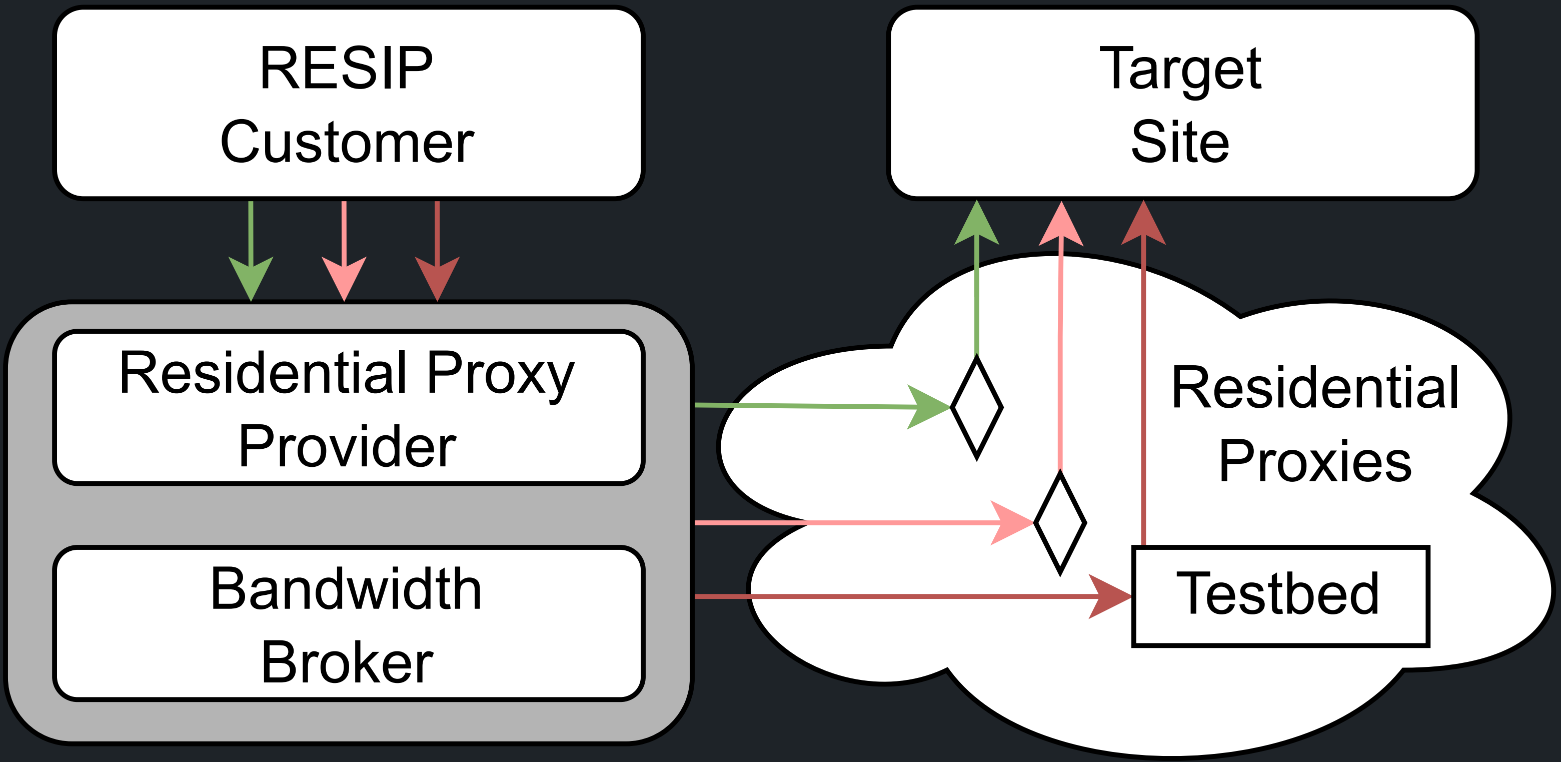
Buy Bandwidth
Access The Network:
$1.00/GB
Learn more about buying bandwidth →

gines such as

ch as

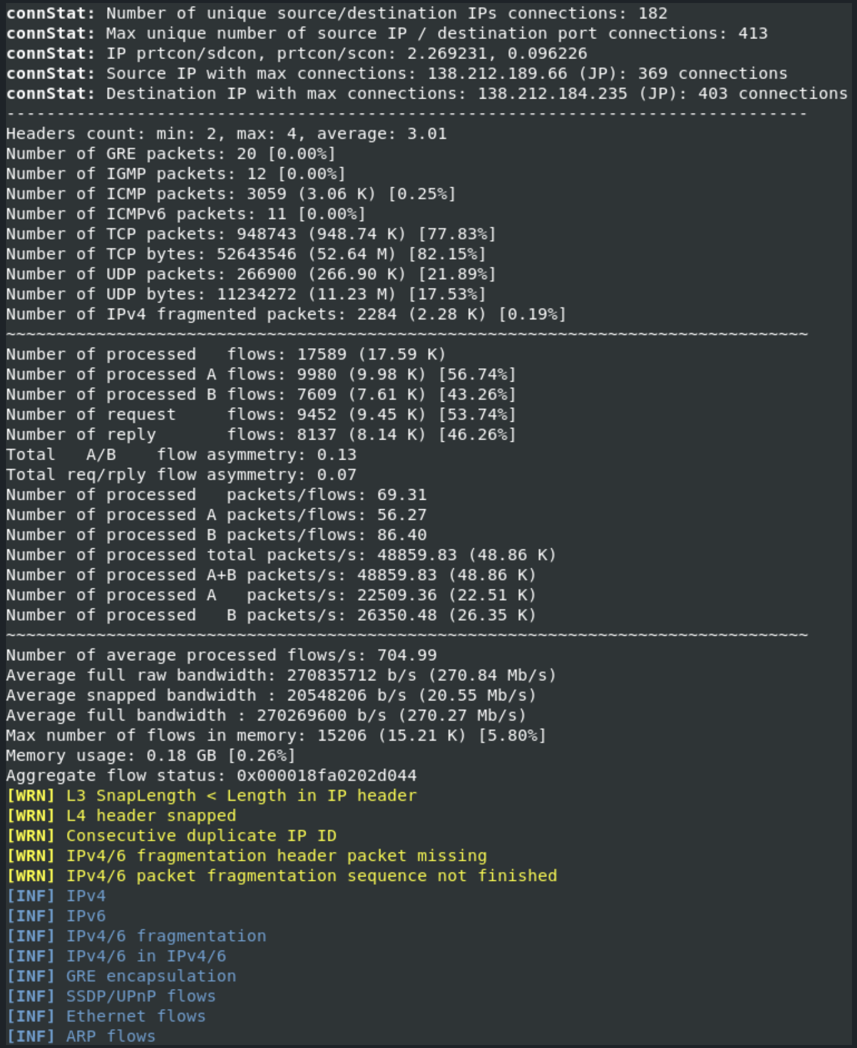
User-Installed

UNIVERSITY
OF TWENTE.



Tranalyzer

UNIVERSITY
OF TWENTE.



```
connStat: Number of unique source/destination IPs connections: 182
connStat: Max unique number of source IP / destination port connections: 413
connStat: IP prtcon/sdcon, prtcon/scon: 2.269231, 0.096226
connStat: Source IP with max connections: 138.212.189.66 (JP): 369 connections
connStat: Destination IP with max connections: 138.212.184.235 (JP): 403 connections
--------------------------------------------------------------------------------
Headers count: min: 2, max: 4, average: 3.01
Number of GRE packets: 20 [0.00%]
Number of IGMP packets: 12 [0.00%]
Number of ICMP packets: 3059 (3.06 K) [0.25%]
Number of ICMPv6 packets: 11 [0.00%]
Number of TCP packets: 948743 (948.74 K) [77.83%]
Number of TCP bytes: 52643546 (52.64 M) [82.15%]
Number of UDP packets: 266900 (266.90 K) [21.89%]
Number of UDP bytes: 11234272 (11.23 M) [17.53%]
Number of IPv4 fragmented packets: 2284 (2.28 K) [0.19%]
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Number of processed   flows: 17589 (17.59 K)
Number of processed A flows: 9980 (9.98 K) [56.74%]
Number of processed B flows: 7609 (7.61 K) [43.26%]
Number of request     flows: 9452 (9.45 K) [53.74%]
Number of reply       flows: 8137 (8.14 K) [46.26%]
Total   A/B    flow asymmetry: 0.13
Total req/rply flow asymmetry: 0.07
Number of processed   packets/flows: 69.31
Number of processed A packets/flows: 56.27
Number of processed B packets/flows: 86.40
Number of processed total packets/s: 48859.83 (48.86 K)
Number of processed A+B packets/s: 48859.83 (48.86 K)
Number of processed A   packets/s: 22509.36 (22.51 K)
Number of processed   B packets/s: 26350.48 (26.35 K)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Number of average processed flows/s: 704.99
Average full raw bandwidth: 270835712 b/s (270.84 Mb/s)
Average snapped bandwidth : 20548206 b/s (20.55 Mb/s)
Average full bandwidth : 270269600 b/s (270.27 Mb/s)
Max number of flows in memory: 15206 (15.21 K) [5.80%]
Memory usage: 0.18 GB [0.26%]
Aggregate flow status: 0x000018fa0202d044
[WRN] L3 SnapLength < Length in IP header
[WRN] L4 header snapped
[WRN] Consecutive duplicate IP ID
[WRN] IPv4/6 fragmentation header packet missing
[WRN] IPv4/6 packet fragmentation sequence not finished
[INF] IPv4
[INF] IPv6
[INF] IPv4/6 fragmentation
[INF] IPv4/6 in IPv4/6
[INF] GRE encapsulation
[INF] SSDP/UPnP flows
[INF] Ethernet flows
[INF] ARP flows
```

User-Installed

Episode 2

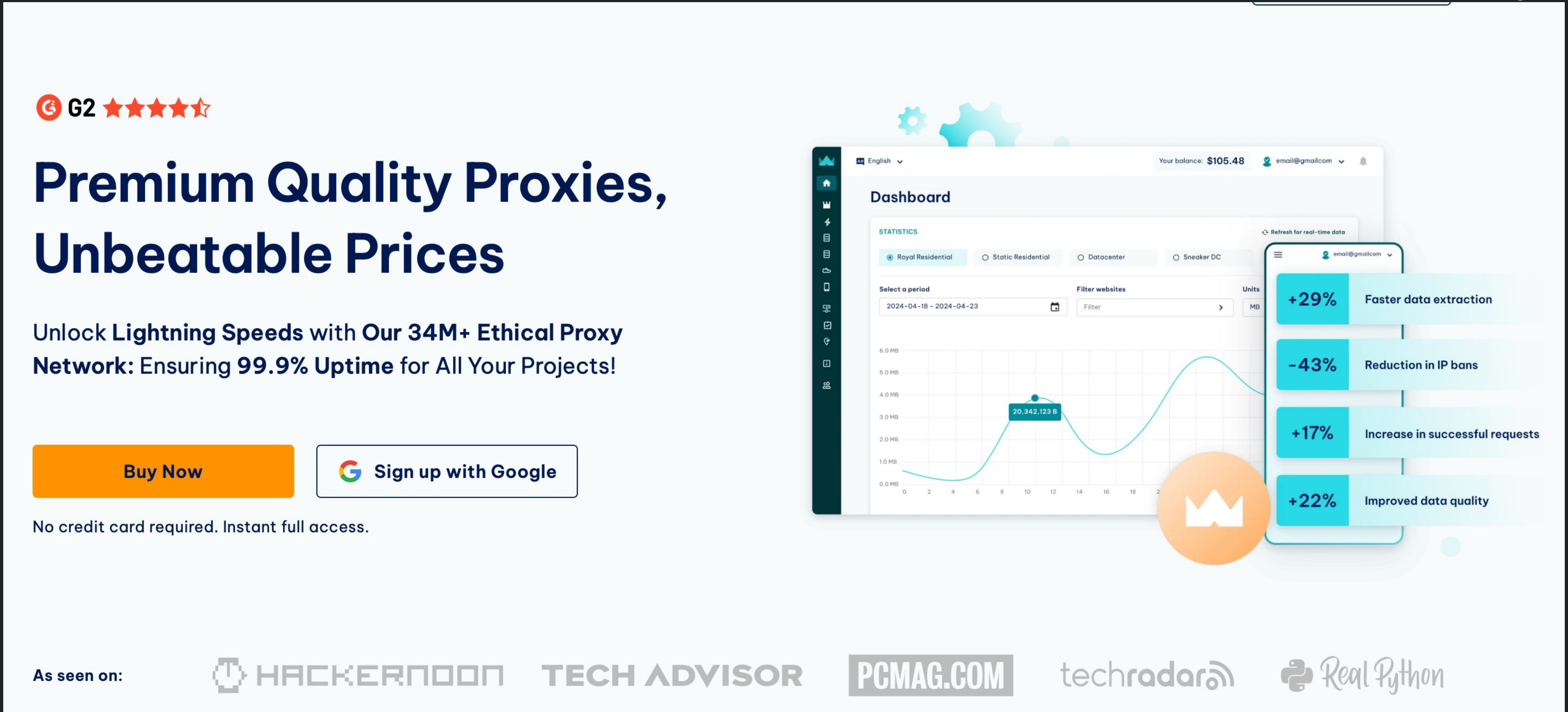
UNIVERSITY
OF TWENTE.

A First Look at User-Installed Residential Proxies

From a Network Operator’s Perspective

First Look

UNIVERSITY OF TWENTE.



G2 ★★★★☆

Premium Quality Proxies, Unbeatable Prices

Unlock **Lightning Speeds** with **Our 34M+ Ethical Proxy Network:** Ensuring **99.9% Uptime** for All Your Projects!

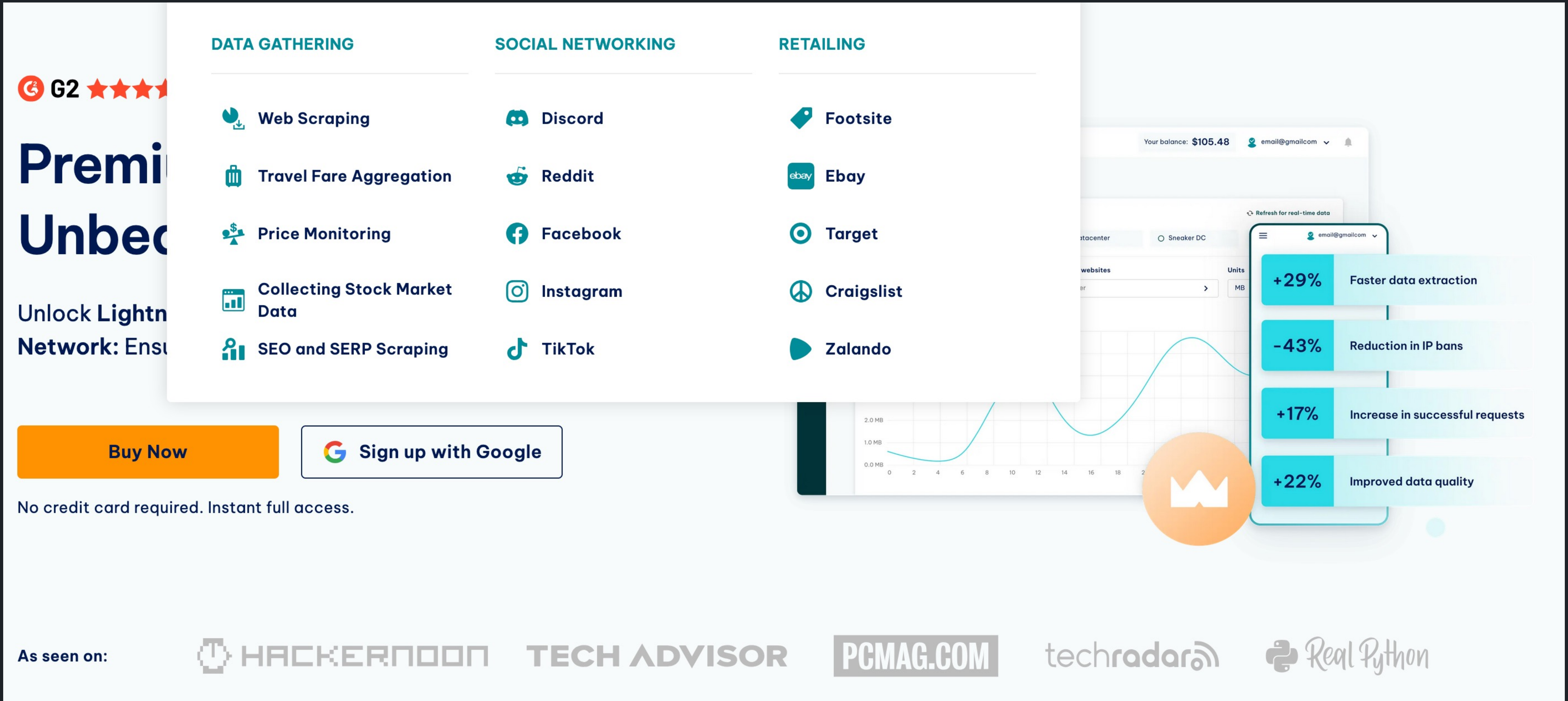
Buy Now

Sign up with Google

No credit card required. Instant full access.

As seen on: HACKERNOON TECH ADVISOR PCMAG.COM techradar Real Python

First Look



G2 ★★★★

Premi

Unbec

Unlock **Lightn**

Network: Ensu

DATA GATHERING

- Web Scraping
- Travel Fare Aggregation
- Price Monitoring
- Collecting Stock Market Data
- SEO and SERP Scraping

SOCIAL NETWORKING

- Discord
- Reddit
- Facebook
- Instagram
- TikTok

RETAILING

- Footsite
- Ebay
- Target
- Craigslist
- Zalando

Buy Now

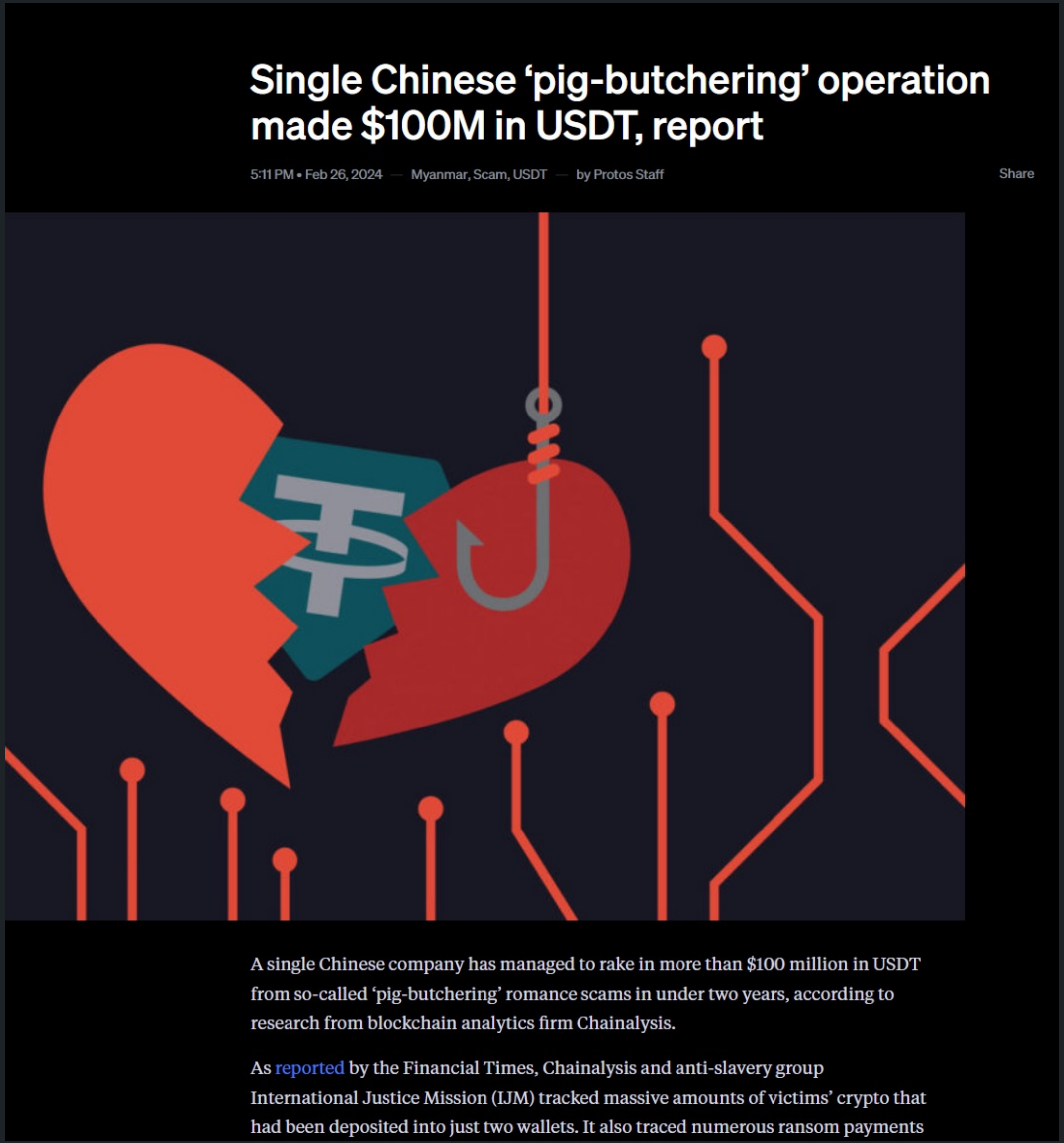
Sign up with Google

No credit card required. Instant full access.

+29%	Faster data extraction
-43%	Reduction in IP bans
+17%	Increase in successful requests
+22%	Improved data quality

As seen on: HACKERNOON TECH ADVISOR PCMAG.COM techradar Real Python

First Look



Single Chinese ‘pig-butchering’ operation made $100M in USDT, report

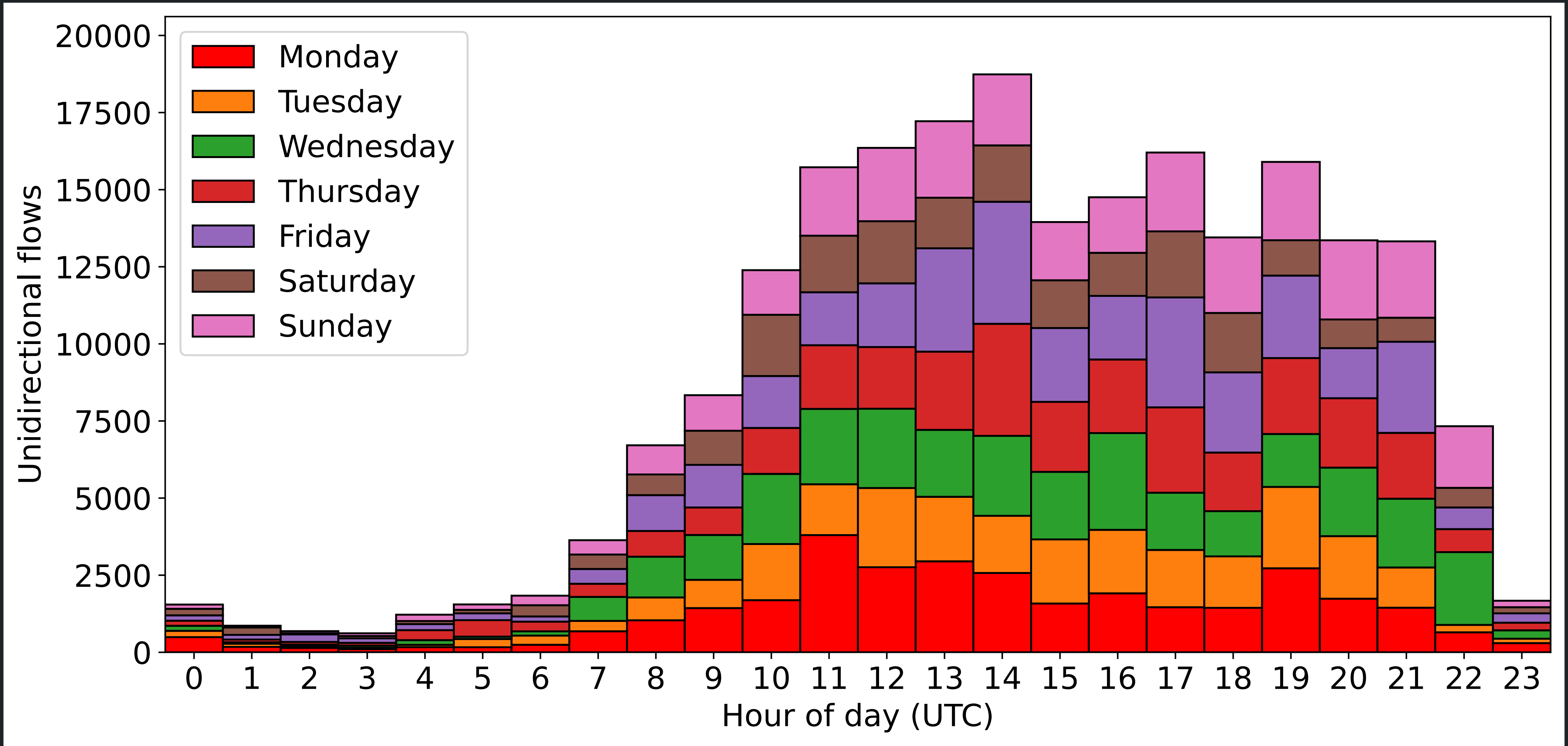
5:11 PM • Feb 26, 2024 — Myanmar, Scam, USDT — by Protos Staff

A single Chinese company has managed to rake in more than $100 million in USDT from so-called ‘pig-butchering’ romance scams in under two years, according to research from blockchain analytics firm Chainalysis.

As reported by the Financial Times, Chainalysis and anti-slavery group International Justice Mission (IJM) tracked massive amounts of victims’ crypto that had been deposited into just two wallets. It also traced numerous ransom payments

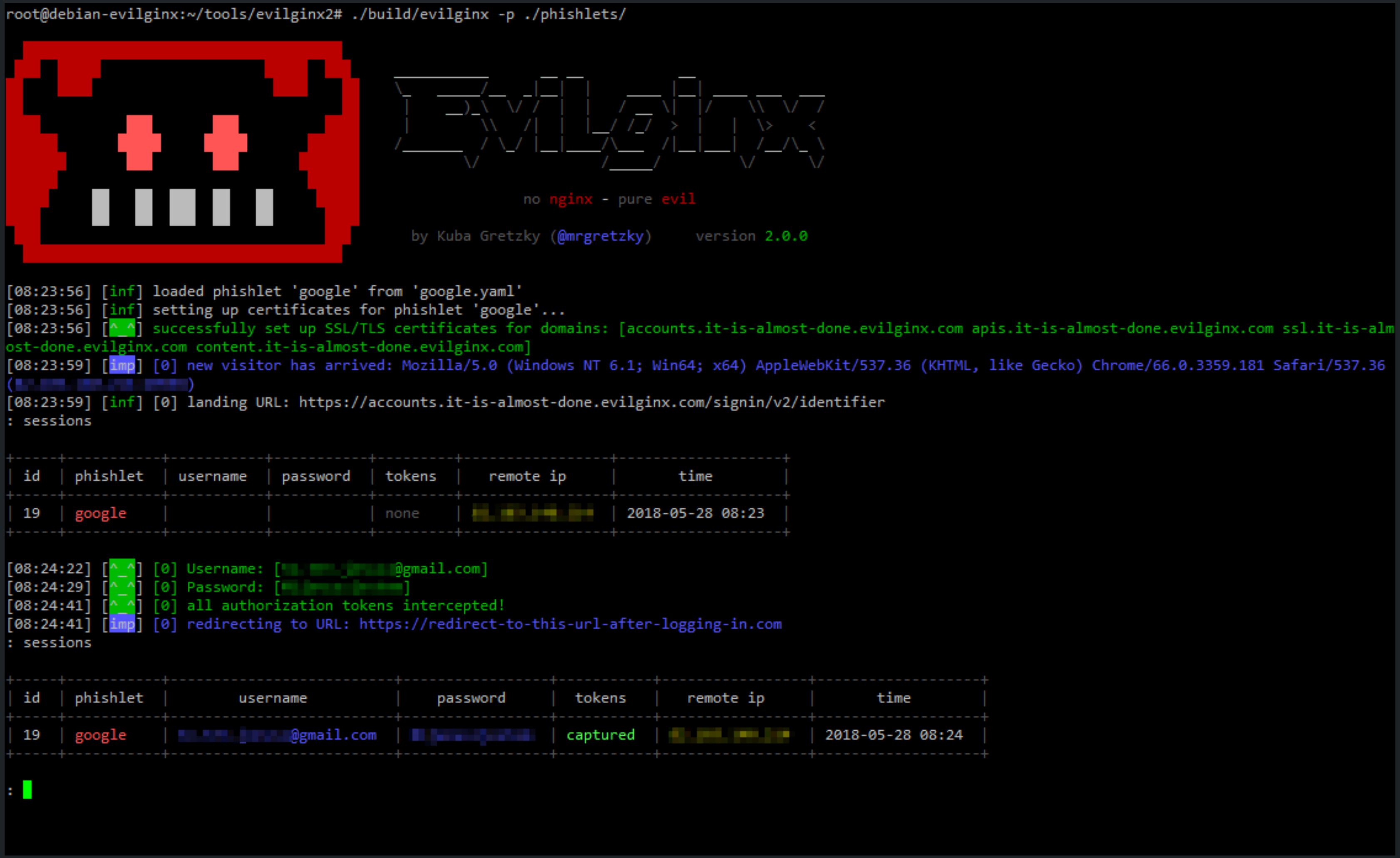
First Look - Tinder

UNIVERSITY OF TWENTE.



First Look - Phishing

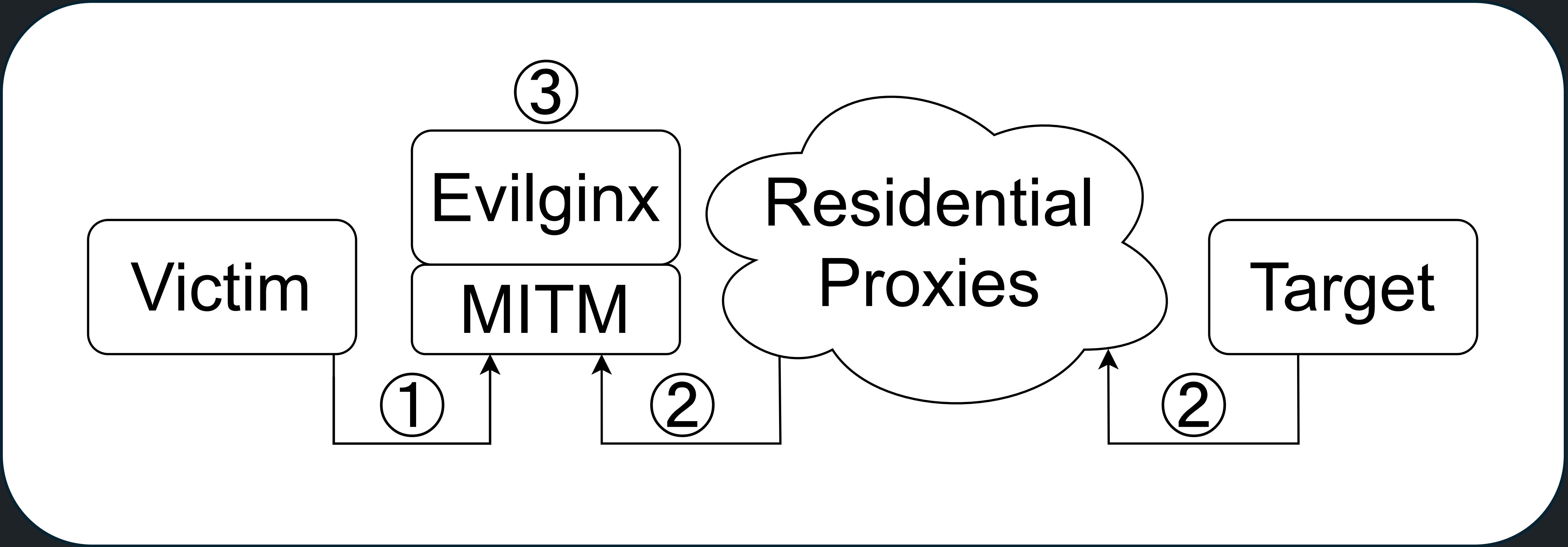
UNIVERSITY
OF TWENTE.



```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

                        no nginx - pure evil

            by Kuba Gretzky (@mrgretzky)     version 2.0.0

[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-alm
ost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

+-----+----------+----------+----------+--------+------------------+------------------+
| id  | phishlet | username | password | tokens |    remote ip     |       time       |
+-----+----------+----------+----------+--------+------------------+------------------+
| 19  | google   |          |          | none   | [redacted]       | 2018-05-28 08:23 |
+-----+----------+----------+----------+--------+------------------+------------------+

[08:24:22] [^_^] [0] Username: [[redacted]@gmail.com]
[08:24:29] [^_^] [0] Password: [[redacted]]
[08:24:41] [^_^] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions

+-----+----------+--------------------------+------------------+----------+------------------+------------------+
| id  | phishlet |         username         |     password     |  tokens  |    remote ip     |       time       |
+-----+----------+--------------------------+------------------+----------+------------------+------------------+
| 19  | google   | [redacted]@gmail.com     | [redacted]       | captured | [redacted]       | 2018-05-28 08:24 |
+-----+----------+--------------------------+------------------+----------+------------------+------------------+

: 
```

First Look - Phishing

UNIVERSITY OF TWENTE.



First Look - Phishing: TLS Fingerprinting

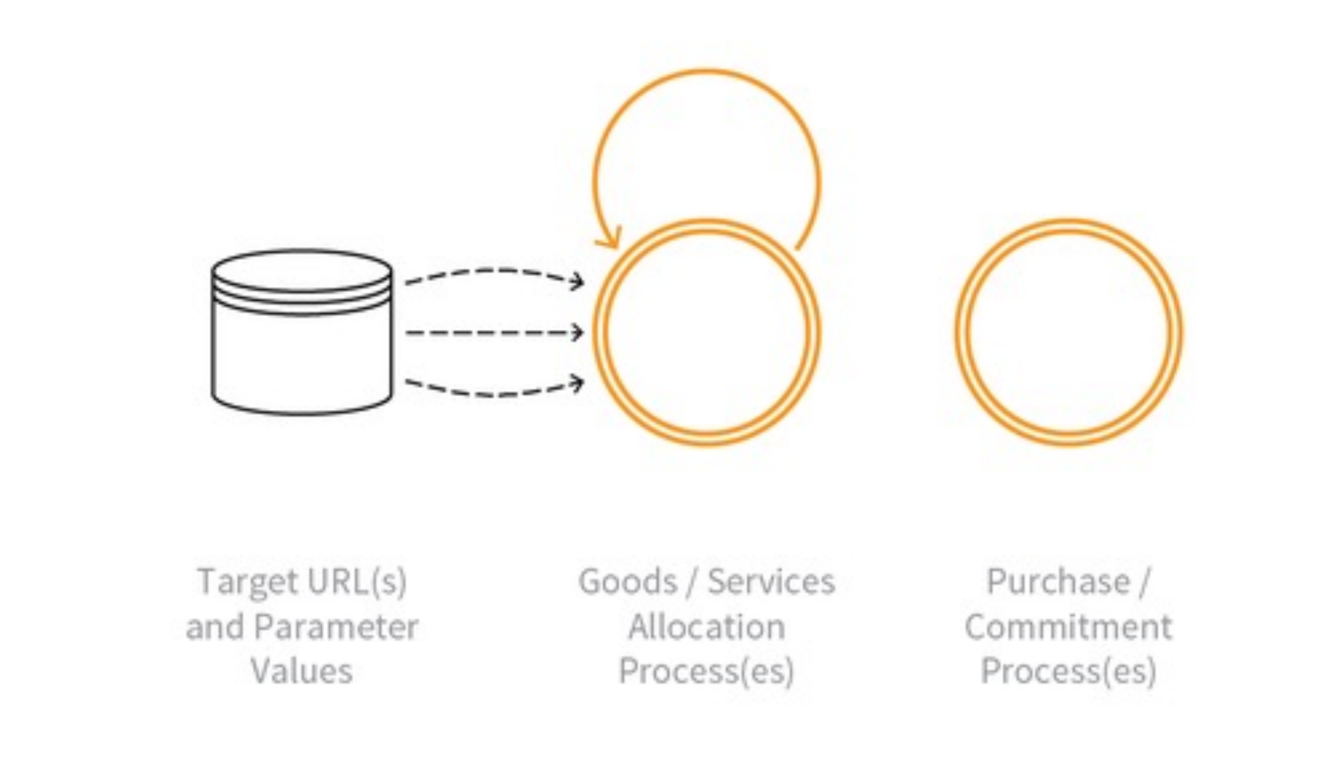
JA4 + SNI =

First Look - Phishing: TLS Fingerprinting

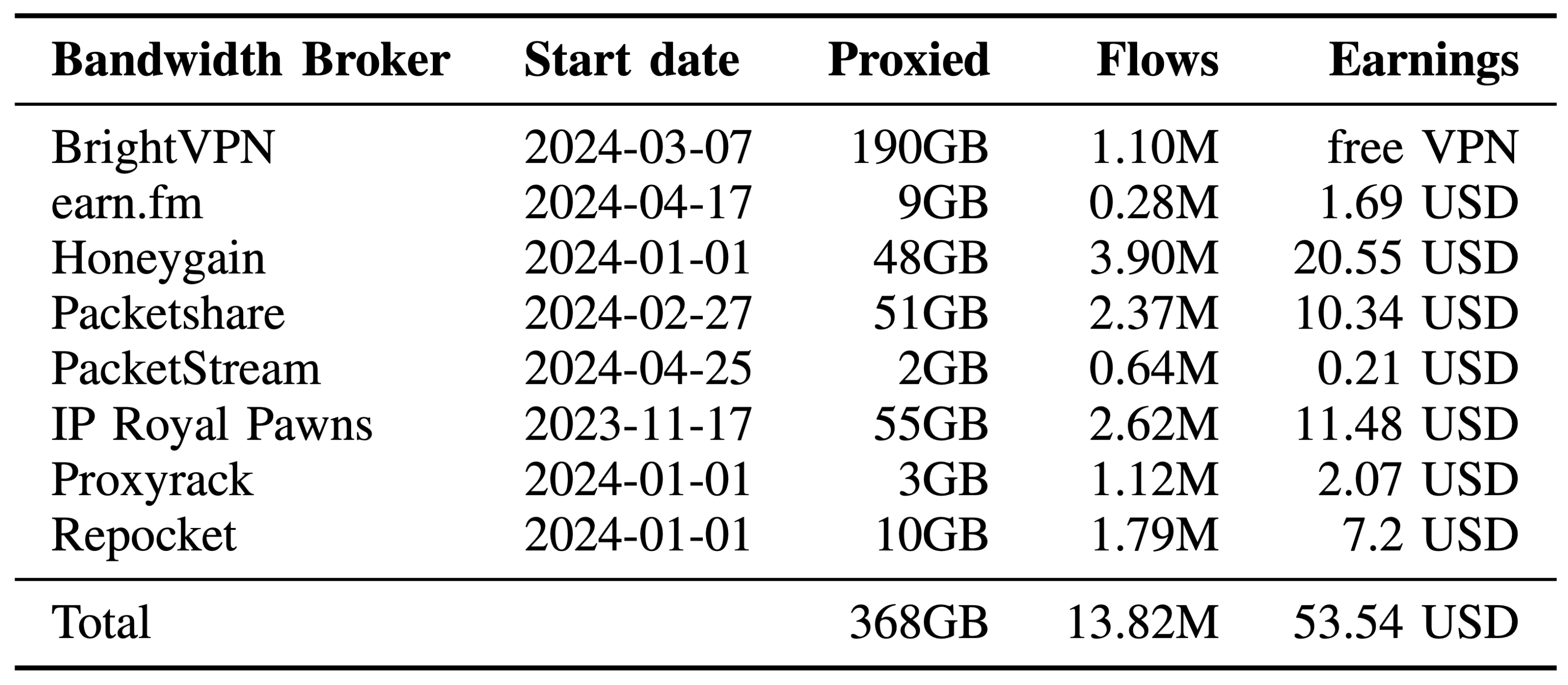
account.booking.com
outlook.office365.com
discord.com
paypal.com
And more

First Look - Sophisticated Bots

UNIVERSITY OF TWENTE.


Target URL(s) and Parameter Values
Goods / Services Allocation Process(es)
Purchase / Commitment Process(es)

First Look - Riches Beyond Imagination



Bandwidth Broker	Start date	Proxied	Flows	Earnings
BrightVPN	2024-03-07	190GB	1.10M	free VPN
earn.fm	2024-04-17	9GB	0.28M	1.69 USD
Honeygain	2024-01-01	48GB	3.90M	20.55 USD
Packetshare	2024-02-27	51GB	2.37M	10.34 USD
PacketStream	2024-04-25	2GB	0.64M	0.21 USD
IP Royal Pawns	2023-11-17	55GB	2.62M	11.48 USD
Proxyrack	2024-01-01	3GB	1.12M	2.07 USD
Repocket	2024-01-01	10GB	1.79M	7.2 USD
Total		368GB	13.82M	53.54 USD

Episode 2

UNIVERSITY
OF TWENTE.

A First Look at User-Installed Residential Proxies

From a Network Operator’s Perspective

From a Network Operator’s Perspective

UNIVERSITY
OF TWENTE.

My testbed consisted only of one network operator…

Call to Action

We can deepen our understanding of this phenomenon by sampling for proxy indicators in end-user networks or at IXPs

Takeaways

UNIVERSITY
OF TWENTE.

- Don’t share your Internet connection for money
- Vehicle for serious crime
- Looking for traces in end-user networks might reveal the true extent of these residential proxies

Contact, Questions, Discussions

Etienne Khan
e.khan@utwente.nl

Or here, in person