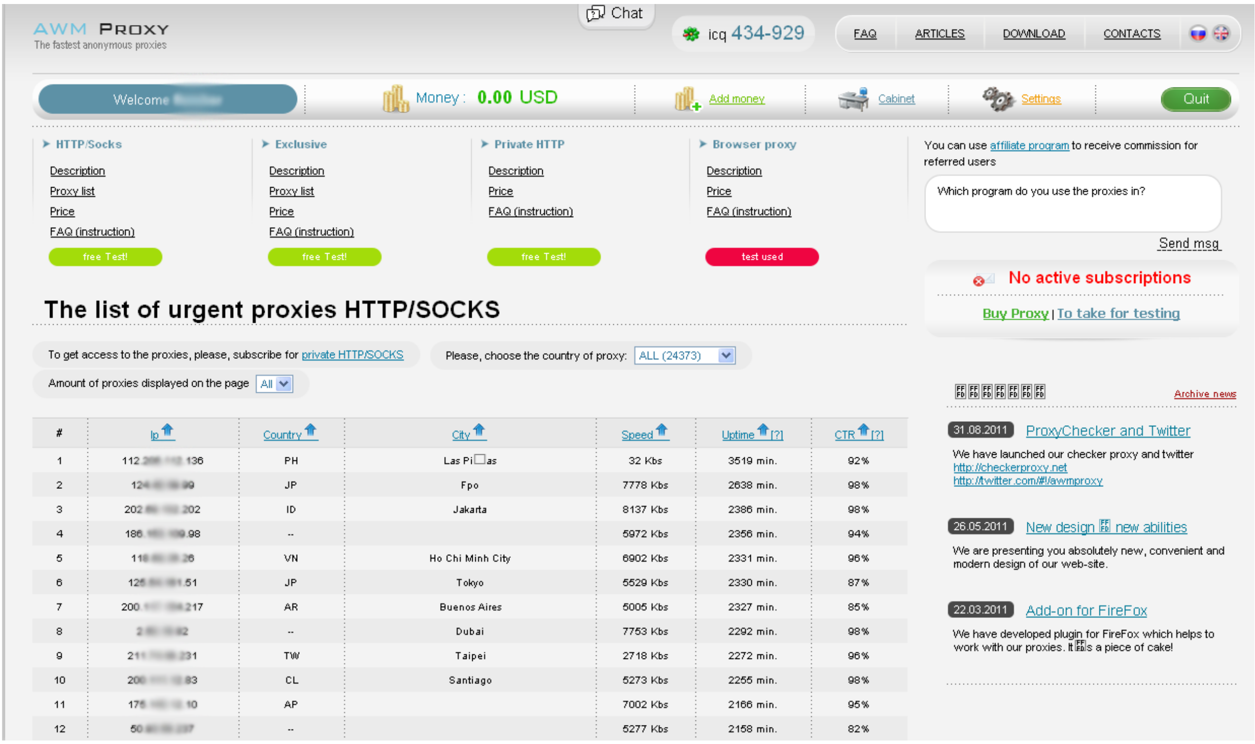
The Link Between AWM Proxy & the Glupteba Botnet

krebsonsecurity.com/2022/06/the-link-between-awm-proxy-the-glupteba-botnet/

On December 7, 2021, **Google** announced it was suing two Russian men allegedly responsible for operating the **Glupteba** botnet, a global malware menace that has infected millions of computers over the past decade. That same day, **AWM Proxy** — a 14-year-old anonymity service that rents hacked PCs to cybercriminals — suddenly went offline. Security experts had long seen a link between Glupteba and AWM Proxy, but new research shows AWM Proxy's founder is one of the men being sued by Google.



HTTP/Socks
Description
Proxy list
Price
FAQ (instruction)
free Test!

Exclusive
Description
Proxy list
Price
FAQ (instruction)
free Test!

Private HTTP
Description
Price
FAQ (instruction)
free Test!

Browser proxy
Description
Price
FAQ (instruction)
test used

The list of urgent proxies HTTP/SOCKS

To get access to the proxies, please, subscribe for private HTTP/SOCKS

Please, choose the country of proxy: ALL (24373)

Amount of proxies displayed on the page All

#	Ip	Country	City	Speed	Uptime [?]	CTR [?]
1	112[redacted]136	PH	Las Pi□as	32 Kbs	3519 min.	92%
2	12[redacted]99	JP	Fpo	7778 Kbs	2638 min.	98%
3	202[redacted]202	ID	Jakarta	8137 Kbs	2386 min.	98%
4	186.[redacted].98	--		5972 Kbs	2356 min.	94%
5	11[redacted]26	VN	Ho Chi Minh City	6902 Kbs	2331 min.	96%
6	12[redacted]51	JP	Tokyo	5529 Kbs	2330 min.	87%
7	200.[redacted]217	AR	Buenos Aires	5005 Kbs	2327 min.	85%
8	2[redacted]82	--	Dubai	7753 Kbs	2292 min.	98%
9	21[redacted]231	TW	Taipei	2718 Kbs	2272 min.	96%
10	20[redacted]83	CL	Santiago	5273 Kbs	2255 min.	98%
11	17[redacted]10	AP		7002 Kbs	2166 min.	95%
12	50[redacted]	--		5277 Kbs	2158 min.	82%

You can use affiliate program to receive commission for referred users

Which program do you use the proxies in?

Send msg

No active subscriptions

Buy Proxy | To take for testing

□□□□□□□ Archive news

31.08.2011 ProxyChecker and Twitter

We have launched our checker proxy and twitter
http://checkerproxy.net
http://twitter.com/#!/awmproxy

26.05.2011 New design □ new abilities

We are presenting you absolutely new, convenient and modern design of our web-site.

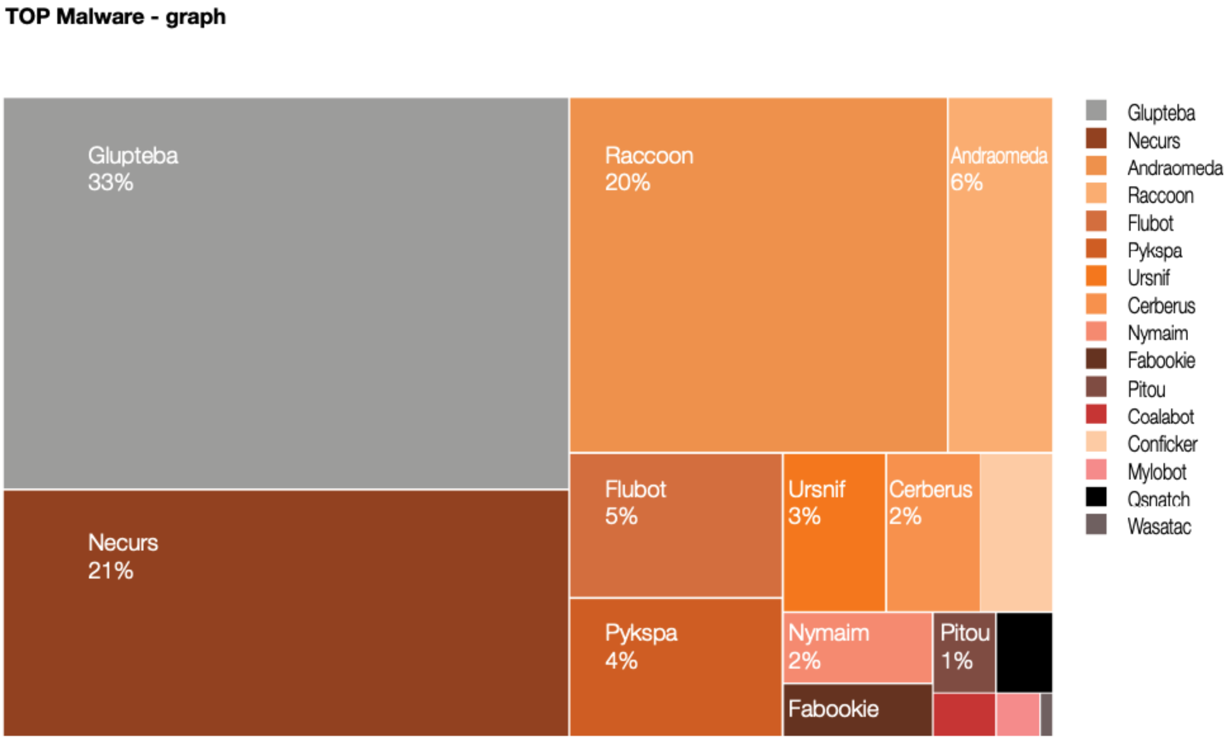
22.03.2011 Add-on for FireFox

We have developed plugin for FireFox which helps to work with our proxies. It□s a piece of cake!

AWMproxy, the storefront for renting access to infected PCs, circa 2011.

Launched in March 2008, AWM Proxy quickly became the largest service for crooks seeking to route their malicious Web traffic through compromised devices. In 2011, researchers at **Kaspersky Lab** showed that virtually all of the hacked systems for rent at AWM Proxy had been compromised by **TDSS** (a.k.a TDL-4 and Alureon), a stealthy "rootkit" that installs deep within infected PCs and loads even before the underlying Windows operating system boots up.

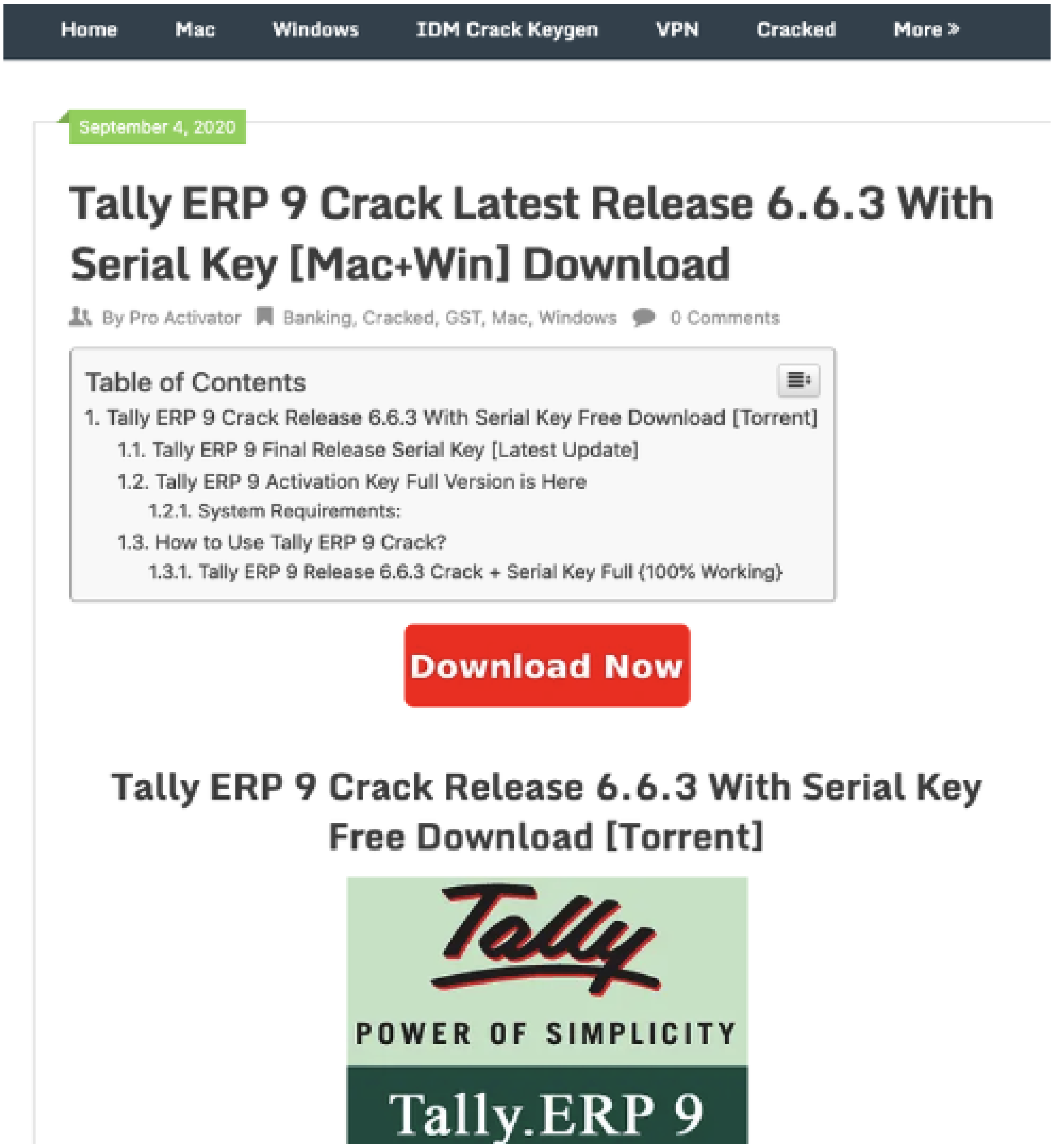
In March 2011, security researchers at **ESET** found TDSS was being used to deploy Glupteba, another rootkit that steals passwords and other access credentials, disables security software, and tries to compromise other devices on the victim's network — such as Internet routers and media storage servers — for use in relaying spam or other malicious traffic.



A report from the Polish computer emergency response team (CERT Orange Polksa) found Glupteba was by far the biggest malware threat in 2021.

Like its predecessor TDSS, Glupteba is primarily distributed through “pay-per-install” or PPI networks, and via traffic purchased from traffic distribution systems (TDS). Pay-per-install networks try to match cybercriminals who already have access to large numbers of hacked PCs with other crooks seeking broader distribution of their malware.

In a typical PPI network, clients will submit their malware—a spambot or password-stealing Trojan, for example —to the service, which in turn charges per thousand successful installations, with the price depending on the requested geographic location of the desired victims. One of the most common ways PPI affiliates generate revenue is by secretly bundling the PPI network’s installer with pirated software titles that are widely available for download via the web or from file-sharing networks.



September 4, 2020

Tally ERP 9 Crack Latest Release 6.6.3 With Serial Key [Mac+Win] Download

By Pro Activator Banking, Cracked, GST, Mac, Windows 0 Comments

Table of Contents

Tally ERP 9 Crack Release 6.6.3 With Serial Key Free Download [Torrent]

An example of a cracked software download site distributing Glupteba. Image: Google.com.

Over the past decade, both Glupteba and AWM Proxy have grown substantially. When KrebsOnSecurity first covered AWM Proxy in 2011, the service was selling access to roughly 24,000 infected PCs scattered across dozens of countries. Ten years later, AWM Proxy was offering 10 times that number of hacked systems on any given day, and Glupteba had grown to more than one million infected devices worldwide.

There is also ample evidence to suggest that Glupteba may have spawned **Meris**, a massive botnet of hacked Internet of Things (IoT) devices that surfaced in September 2021 and was responsible for some of the largest and most disruptive distributed denial-of-service (DDoS) attacks the Internet has ever seen.

But on Dec. 7, 2021, Google announced it had taken technical measures to dismantle the Glupteba botnet, and filed a civil lawsuit (PDF) against two Russian men thought to be responsible for operating the vast crime machine. AWM Proxy's online storefront disappeared that same day.

AWM Proxy quickly alerted its customers that the service had moved to a new domain, with all customer balances, passwords and purchase histories seamlessly ported over to the new home. However, subsequent takedowns targeting AWM Proxy's domains and other infrastructure have conspired to keep the service on the ropes and frequently switching domains ever since.

Earlier this month, the United States, Germany, the Netherlands and the U.K. dismantled the "**RSOCKS**" botnet, a competing proxy service that had been in operation since 2014. KrebsOnSecurity has identified the owner of RSOCKS as a 35-year-old from Omsk, Russia who runs the world's largest forum catering to spammers.

The employees who kept things running for RSOCKS, circa 2016.

Shortly after last week's story on the RSOCKS founder, I heard from **Riley Kilmer**, co-founder of Spur.us, a startup that tracks criminal proxy services. Kilmer said RSOCKS was similarly disabled after Google's combined legal sneak attack and technical takedown targeting Glupteba.

"The RSOCKS website gave you the estimated number of proxies in each of their subscription packages, and that number went down to zero on Dec. 7," Kilmer said. "It's not clear if that means the services were operated by the same people, or if they were just using the same sources (i.e., PPI programs) to generate new installations of their malware."

Kilmer said each time his company tried to determine how many systems RSOCKS had for sale, they found each Internet address being sold by RSOCKS was also present in AWM Proxy's network. In addition, Kilmer said, the application programming interfaces (APIs) used by both services to keep track of infected systems were virtually identical, once again suggesting strong collaboration.

“One hundred percent of the IPs we got back from RSOCKS we’d already identified in AWM,” Kilmer said. “And the IP port combinations they give you when you access an individual IP were the same as from AWM.”

In 2011, KrebsOnSecurity published an investigation that identified one of the founders of AWM Proxy, but Kilmer’s revelation prompted me to take a fresh look at the origins of this sprawling cybercriminal enterprise to determine if there were additional clues showing more concrete links between RSOCKS, AWM Proxy and Glupteba.

IF YOUR PLAN IS TO RIP OFF GOOGLE…

Supporting Kilmer’s theory that AWM Proxy and RSOCKS may simply be using the same PPI networks to spread, further research shows the RSOCKS owner also had an ownership stake in **AD1[.]ru**, an extremely popular Russian-language pay-per-install network that has been in operation for at least a decade.

Google took aim at Glupteba in part because its owners were using the botnet to divert and steal vast sums in online advertising revenue. So it’s more than a little ironic that the critical piece of evidence linking all of these operations begins with a Google Analytics code included in the HTML code for the original AWM Proxy back in 2008 (**UA-3816536**).

That analytics code also was present on a handful of other sites over the years, including the now-defunct Russian domain name registrar **Domenadom[.]ru**, and the website **web-site[.]ru**, which curiously was a Russian company operating a global real estate appraisal business called American Appraisal.

Two other domains connected to that Google Analytics code — Russian plastics manufacturers **techplast[.]ru** and **tekhplast.ru** — also shared a different Google Analytics code (**UA-1838317**) with web-site[.]ru and with the domain “**starovikov[.]ru**.”

The name on the WHOIS registration records for the plastics domains is an “**Alexander I. Ukraincki**,” whose personal information also is included in the domains tpos[.]ru and alphadisplay[.]ru, both apparently manufacturers of point-of-sale payment terminals in Russia.

Constella Intelligence, a security firm that indexes passwords and other personal information exposed in past data breaches, revealed dozens of variations on email addresses used by Alexander I. Ukraincki over the years. Most of those email addresses start with some variation of “**uai@**” followed by a domain from one of the many Russian email providers (e.g., yandex.ru, mail.ru). [Full disclosure: Constella is currently an advertiser on this website].

But Constella also shows those different email addresses all relied on a handful of passwords — most commonly “**2222den**” and “**2222DEN**.” Both of those passwords have been used almost exclusively in the past decade by the person who registered more than a dozen email addresses with the username “**dennstr**.”

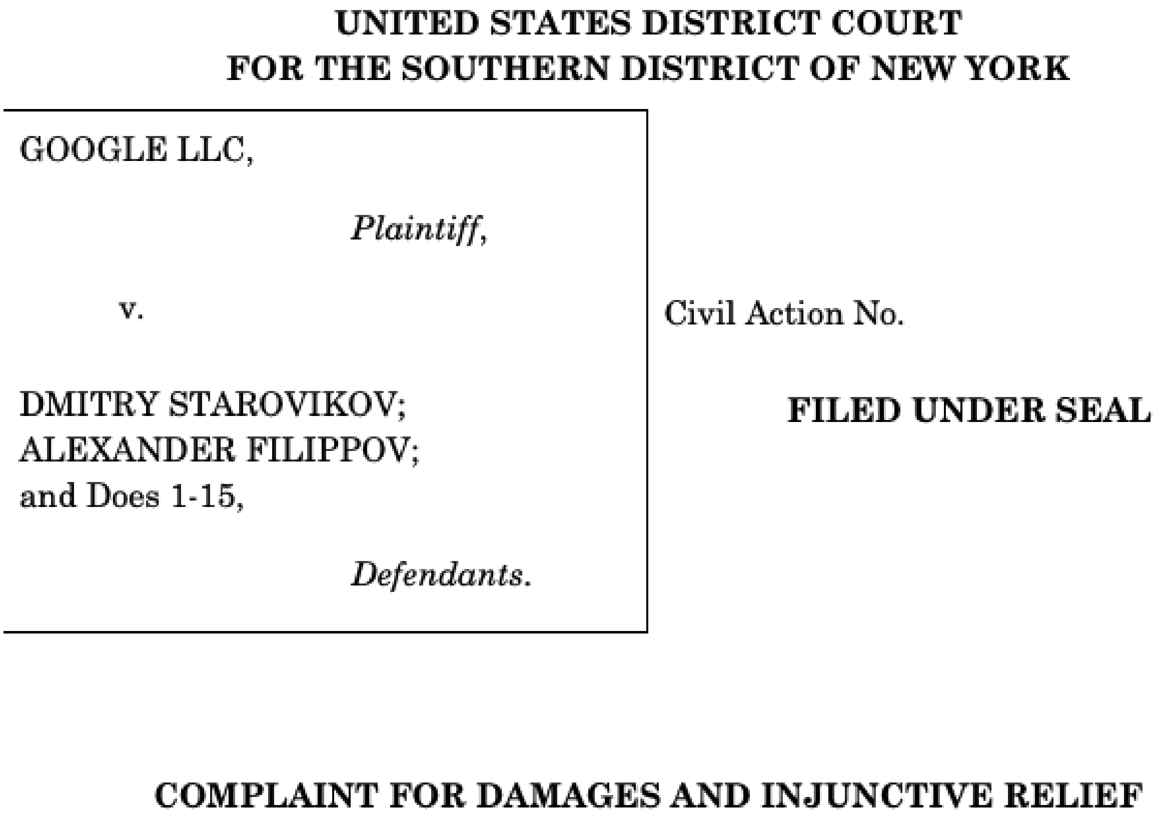
The dennstr identity leads to several variations on the same name — Denis Strelinikov, or Denis Stranatka, from Ukraine, but those clues ultimately led nowhere promising. And maybe that was the point.

Things began looking brighter after I ran a search in DomainTools for web-site[.]ru’s original WHOIS records, which shows it was assigned in 2005 to a “private person” who used the email address **lycefer@gmail.com**. A search in Constella on that email address says it was used to register nearly two dozen domains, including starovikov.ru and **starovikov[.]com**.

A cached copy of the contact page for Starovikov[.]com shows that in 2008 it displayed the personal information for a **Dmitry Starovikov**, who listed his Skype username as “lycefer.”

Finally, Russian incorporation documents show the company LLC Website (web-site[.]ru)was registered in 2005 to two men, one of whom was named **Dmitry Sergeevich Starovikov**.

Bringing this full circle, Google says Starovikov is one of the two operators of the Glupteba botnet:



UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC,

Plaintiff,

v.

DMITRY STAROVIKOV;
ALEXANDER FILIPPOV;
and Does 1-15,

Defendants.

Civil Action No.

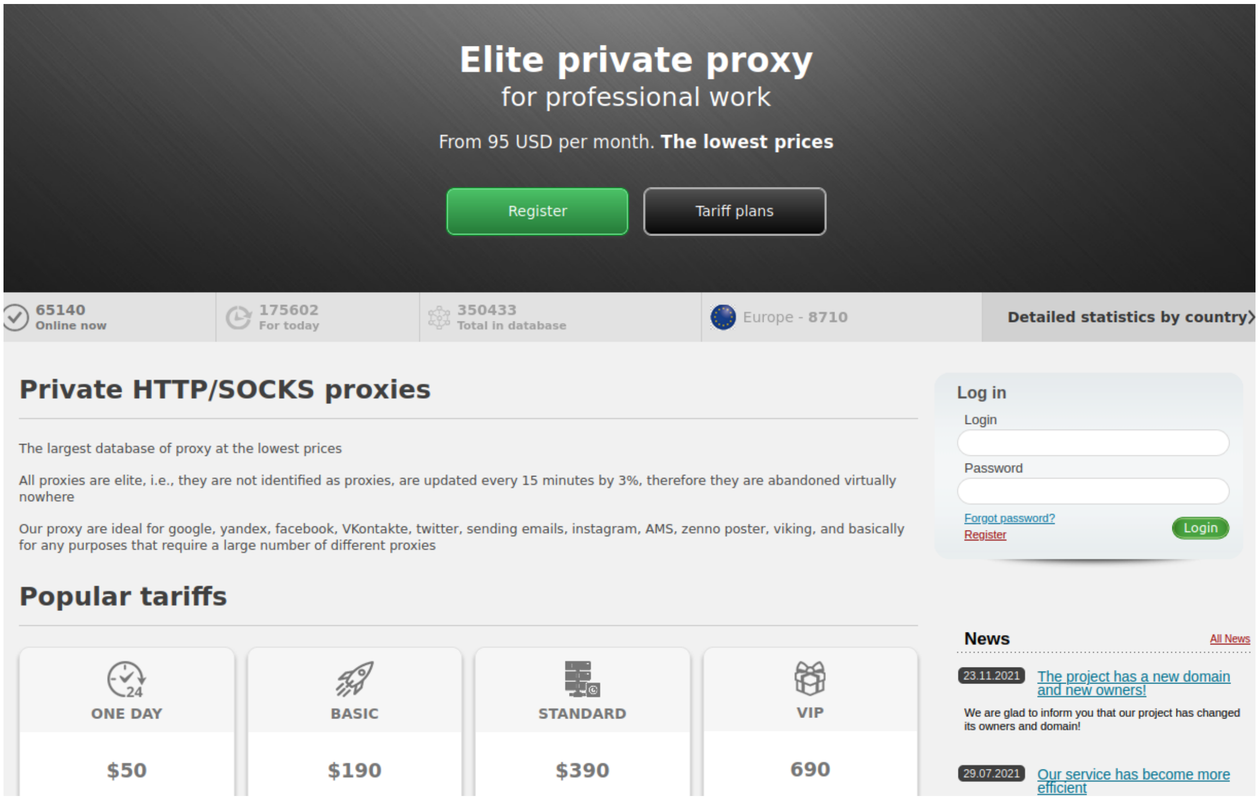
FILED UNDER SEAL

COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

The cover page for Google’s lawsuit against the alleged Glupteba botnet operators.

Mr. Starovikov did not respond to requests for comment. But attorneys for Starovikov and his co-defendant last month filed a response to Google's complaint in the Southern District of New York, denying (PDF) their clients had any knowledge of the scheme.

Despite all of the disruption caused by Google's legal and technical meddling, AWM is still around and nearly as healthy as ever, although the service has been branded with a new name and there are dubious claims of new owners. Advertising customer plans ranging from $50 a day to nearly $700 for "VIP access," AWM Proxy says its malware has been running on approximately 175,000 systems worldwide over the last 24 hours, and that roughly 65,000 of these systems are currently online.



Private HTTP/SOCKS proxies

The largest database of proxy at the lowest prices

All proxies are elite, i.e., they are not identified as proxies, are updated every 15 minutes by 3%, therefore they are abandoned virtually nowhere

Our proxy are ideal for google, yandex, facebook, VKontakte, twitter, sending emails, instagram, AMS, zenno poster, viking, and basically for any purposes that require a large number of different proxies

Popular tariffs

23.11.2021 The project has a new domain and new owners!

We are glad to inform you that our project has changed its owners and domain!

29.07.2021 Our service has become more efficient

AWM Proxy, as it exists today.

Meanwhile, the administrators of RSOCKS recently alerted customers that the service and any unspent balances will soon be migrated over to a new location.

Many people seem to equate spending time, money and effort to investigate and prosecute cybercriminals with the largely failed war on drugs, meaning there is an endless supply of up-and-coming crooks who will always fill in any gaps in the workforce whenever cybercriminals face justice.

While that may be true for many low-level cyber thieves today, investigations like these show once again how small the cybercriminal underground really is. It also shows how it makes a great deal of sense to focus efforts on targeting and disrupting the relatively small number of established hackers who remain the real force multipliers of cybercrime.