



Examining the Mirai.TBOT IoCs under the DNS Microscope

Table of Contents

1. [Executive Report](#)
2. [Appendix: Sample Artifacts](#)

Executive Report

The Mirai botnet, first discovered way back in 2016, made headlines and gained infamy as the biggest botnet to hit networks the world over. It has resurfaced with multiple ways of infecting Internet of Things (IoT) devices and the ability to launch zero-day exploits.

XLab researchers performed a [thorough analysis](#) of what they've dubbed "Mirai.TBOT" and identified 112 domains and 22 IP addresses as indicators of compromise (IoCs) in the process. We expanded the published list of IoCs to determine other potential infection avenues and found:

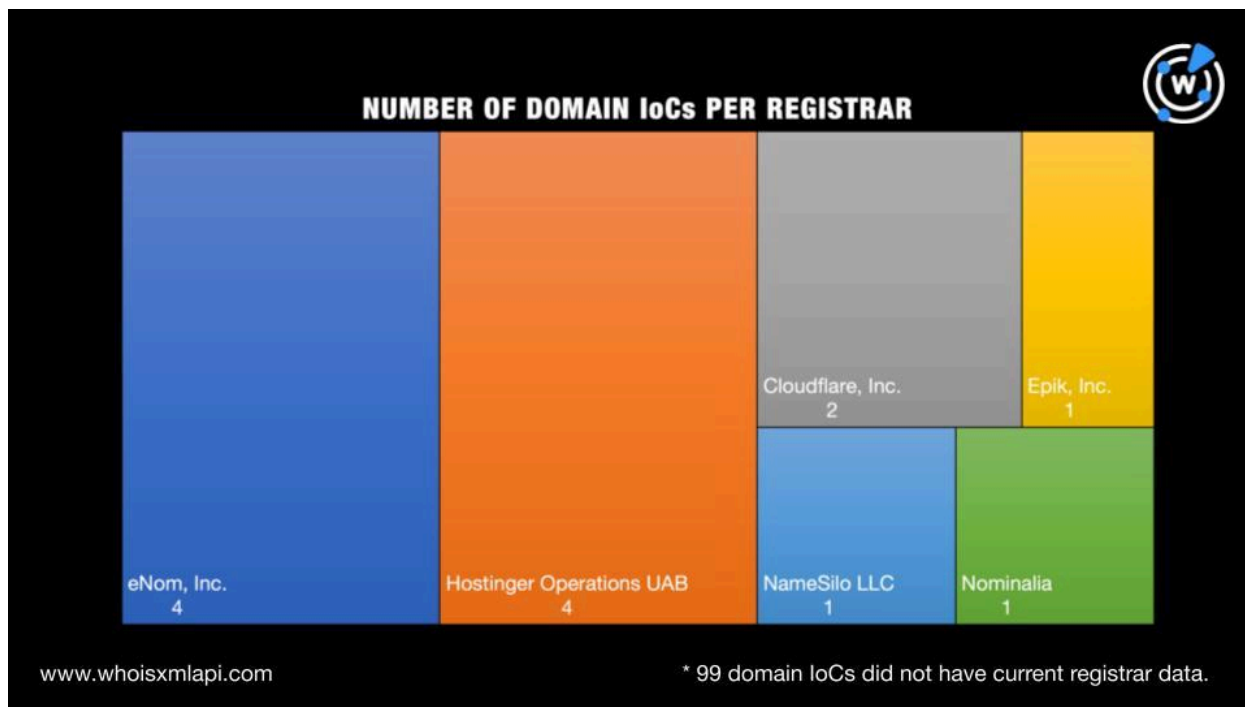
- One email-connected domain
- Six IP-connected domains, all of which turned out to be malicious
- 6,863 string-connected domains

Mirai.TBOT IoC Facts

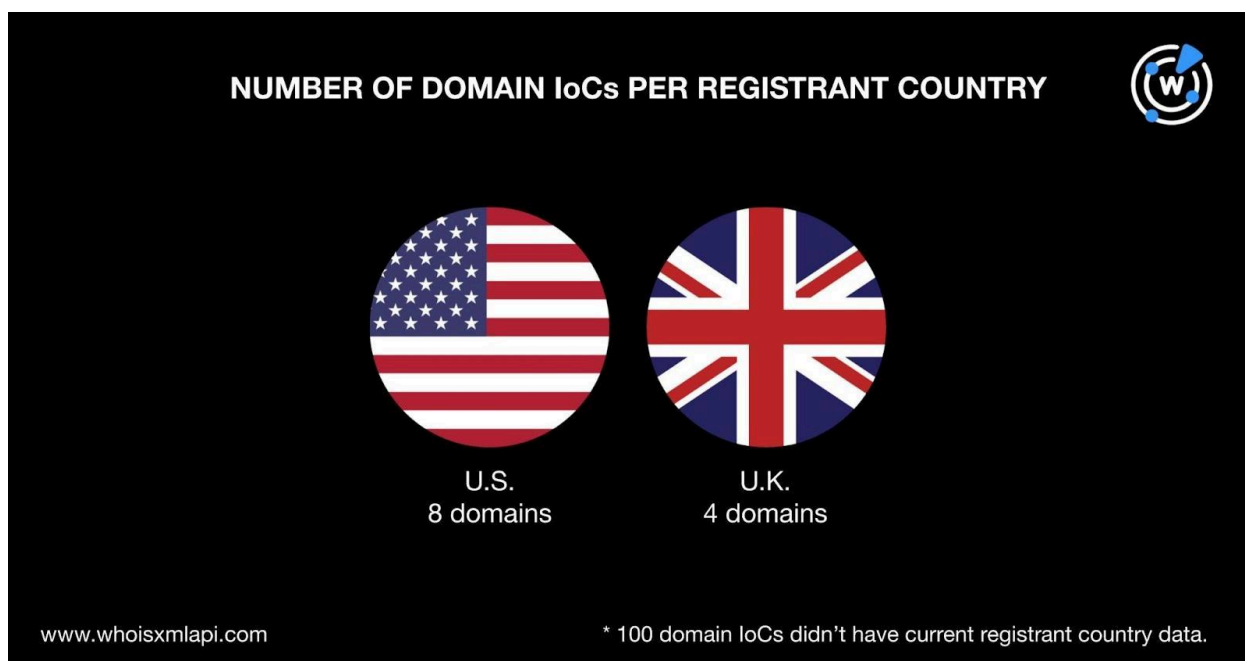
We began our investigation by taking a closer look at the 134 IoCs.

A [bulk WHOIS lookup](#) for the 112 domains identified as IoCs revealed that:

- They were distributed among six registrars led by eNom, Inc. and Hostinger Operations UAB, which accounted for four domains each. Cloudflare, Inc. took the second spot with two domains. Epik, Inc.; NameSilo LLC; and Nominalia shared the third place with one domain each. A total of 99 domains, however, didn't have current registrar data.



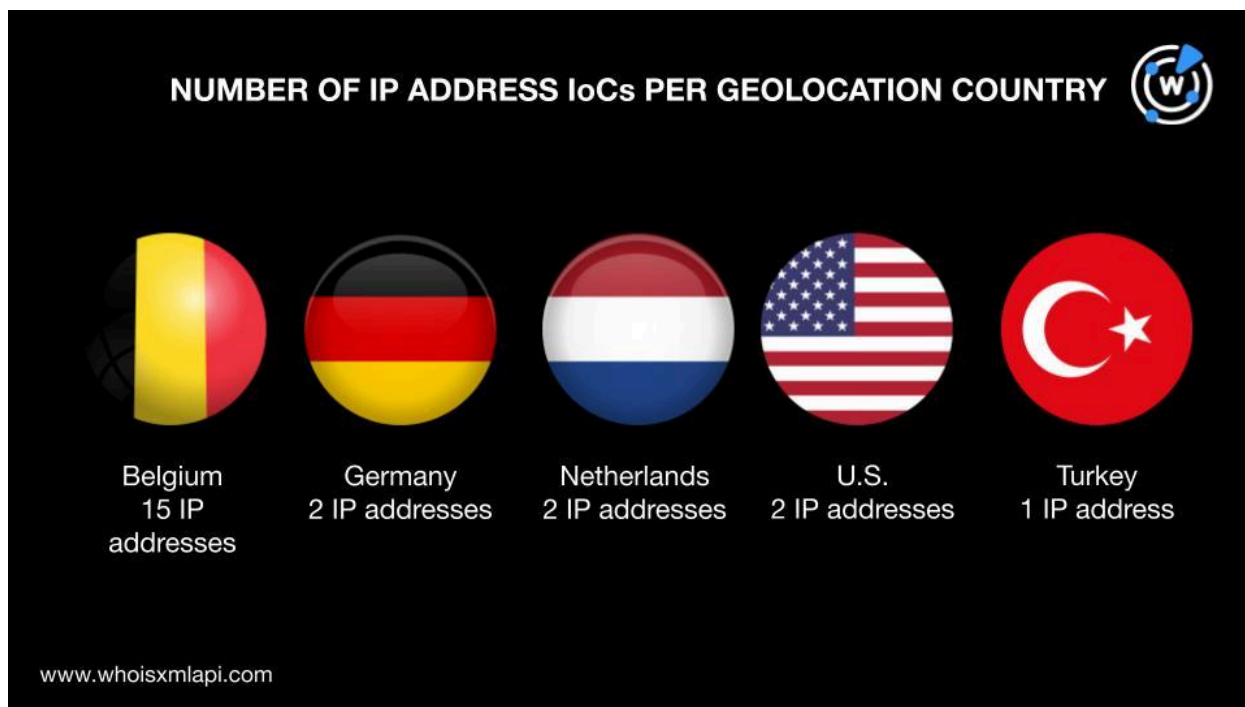
- Thirteen domains were created in 2022 and 2023. The remaining 99 didn't have creation dates in their current WHOIS records, though.
- The U.S. was the top registrant country, accounting for eight domains. Four domains were registered in the U.K. while the remaining 100 didn't have registrant country information in their current WHOIS records.



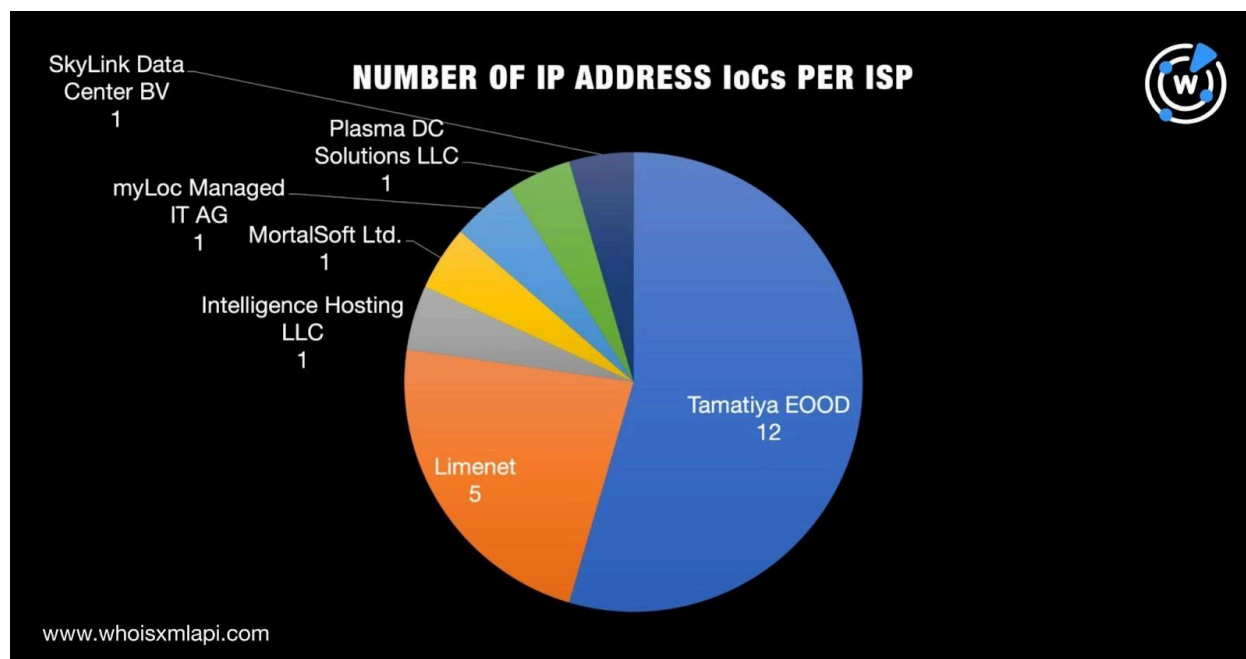


Next, we subjected the 22 IP addresses to a [bulk IP geolocation lookup](#) and found that:

- A majority of them, 15 to be exact, were geolocated in Belgium. Two each pointed to Germany, the Netherlands, and the U.S. while the last one was geolocated in Turkey.



- They were spread across seven Internet service providers (ISPs) topped by Tamatiya EOOD, which accounted for 12 IP addresses. Limenet placed second with five. The five remaining IP addresses were split among the same number of ISPs, namely, Intelligence Hosting LLC, MortalSoft Ltd., myLoc Managed IT AG, Plasma DC Solutions LLC, and SkyLink Data Center BV.



Mirai.TBOT IoC List Expansion Results

Now, on to finding more Mirai.TBOT traces in the DNS.

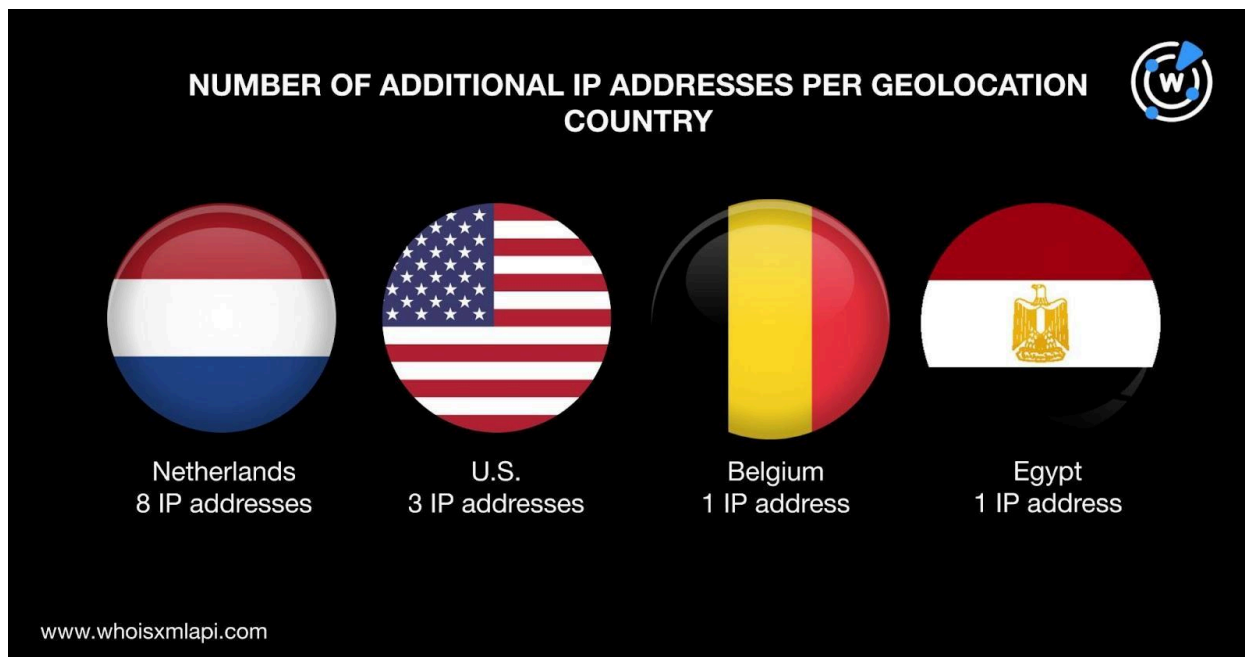
Our search for email-connected domains started with [WHOIS History API](#) searches that led to the discovery of nine email addresses in the domain IoCs' historical WHOIS records, three of which were public.

[Reverse WHOIS API](#) searches showed that one public email address appeared in the current WHOIS record of one domain—qqmmqqw[.]cn—after duplicates and those already tagged as IoCs were removed.

Next, we performed [DNS lookups](#) on the 112 domain IoCs that enabled us to collate 13 IP addresses after duplicates and those that were already part of the original IoC list were filtered out.

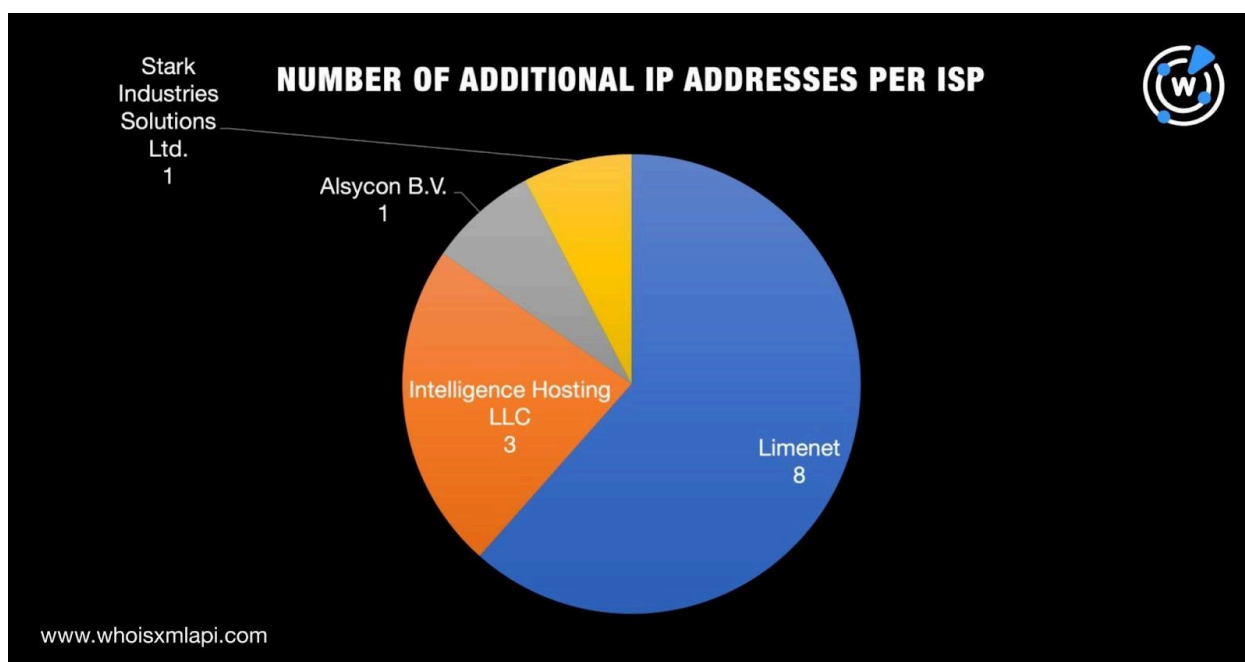
[IP geolocation lookups](#) for the 13 additional IP addresses showed that:

- They were spread across four geolocation countries topped by the Netherlands, which accounted for eight IP addresses. The U.S. took the second spot with three IP addresses while the remaining two pointed to Belgium and Egypt as their origins.



Twelve of the additional IP addresses shared three of the IoCs' geolocation countries—the Netherlands, the U.S., and Belgium.

- They were administered by four ISPs—Limenet (8 IP addresses), Intelligence Hosting LLC (3 IP addresses), and Alsycon B.V. and Stark Industries Solutions Ltd. (1 IP address each).





- The built-in Threat Intelligence API engine results also revealed that 11 of them were associated with various threats. Take a look at five examples below.

IP ADDRESSES	ASSOCIATED THREAT TYPES
185[.]194[.]176[.]137	Attack
45[.]95[.]146[.]126	Attack Generic Malware
85[.]209[.]134[.]96	Attack Malware
91[.]92[.]241[.]184	Attack Malware Spam
91[.]92[.]244[.]7	Attack Malware Spam

[Reverse IP lookups](#) for the 35 IP addresses—22 loCs and 13 additional—showed that 26 of them could be dedicated. They accounted for six IP-connected domains after duplicates, the loCs, and email-connected domains were removed.

All the six IP-connected domains turned out to be malicious based on [threat intelligence lookups](#). One—hailnet[.]online—proved interesting in that it seemingly hosted or led to a satirical Federal Bureau of Investigation (FBI) website according to a [screenshot lookup](#).



I Want To



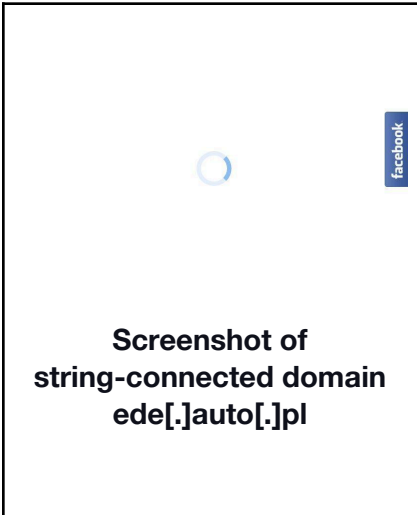
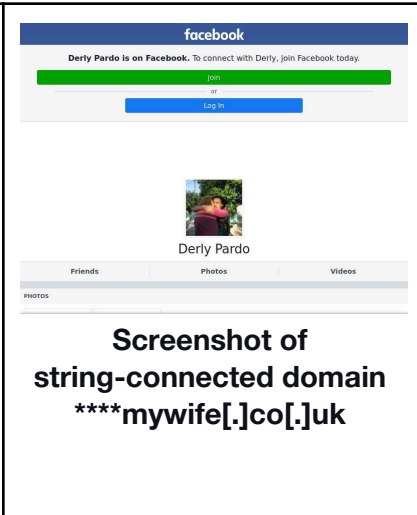
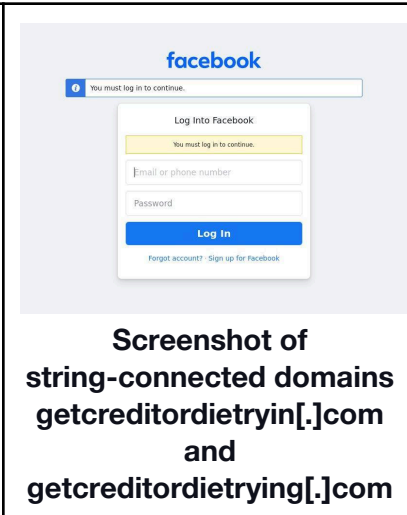
Screenshot of the IP-connected domain hailnet[.]online

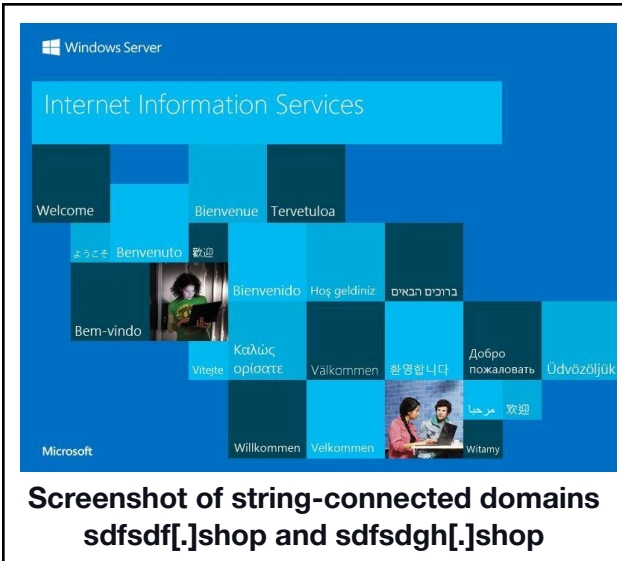
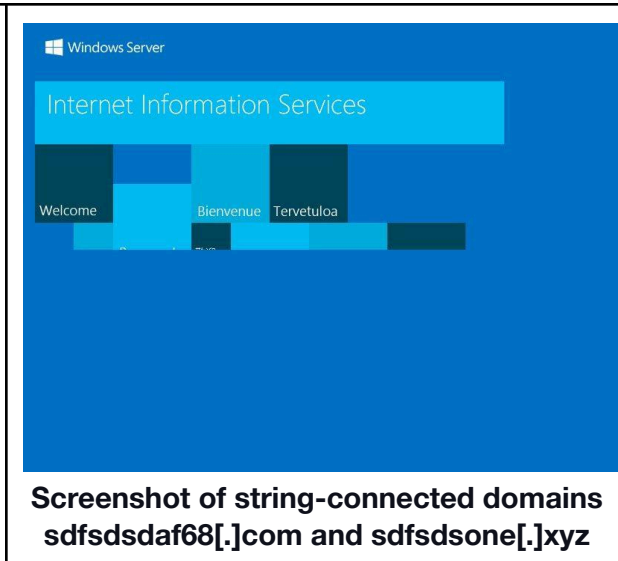
As our final step, we looked for string-connected domains via [Domains & Subdomains Discovery](#) using the **Starts with** parameter. We found 6,863 such domains containing these 34 text strings that appeared in the domain IoCs:

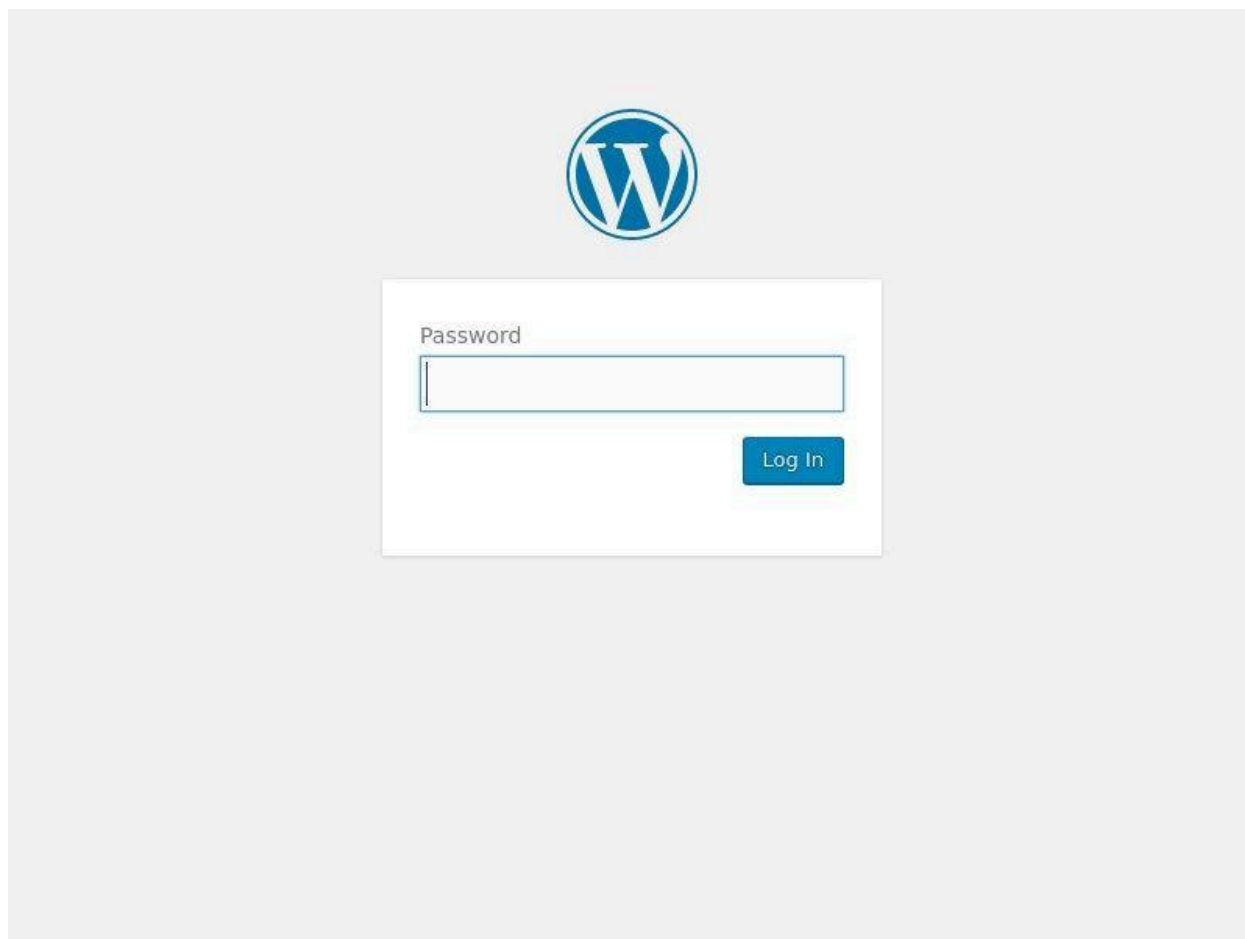
- asdjjasdhioasdia
- cjfop
- czbrwa
- ede.
- etbez
- fawzpp
- fszki
- fuckmy
- getcred
- gottalovethe
- gropethe
- hiakamai
- hinetlab
- homehitter
- iarrfd
- icansinga
- iliveona
- infectedchink
- jxhfn
- ksarpo
- metbez
- oke.
- qcgbs
- rdtqq
- sdfsd
- shetoldmeshewas12
- skid.
- suckmytoe
- ulkvb
- ulkvmb
- vrodpw
- wnisyi
- yellowskin
- youra.



While none of them turned out to be malicious, some could be considered suspicious in that they seemed to be mimicking three often impersonated companies—Facebook, Microsoft, and WordPress—based on their screenshots.

 <p>Screenshot of string-connected domain <code>ede[.]auto[.]pl</code></p>	 <p>Screenshot of string-connected domain <code>****mywife[.]co[.]uk</code></p>	 <p>Screenshot of string-connected domains <code>getcreditorietryin[.]com</code> and <code>getcreditorietrying[.]com</code></p>
--	--	---

 <p>Screenshot of string-connected domains <code>sdfsdf[.]shop</code> and <code>sdfsdfgh[.]shop</code></p>	 <p>Screenshot of string-connected domains <code>sdfsdsdaf68[.]com</code> and <code>sdfsdsone[.]xyz</code></p>
---	--



Screenshot of string-connected domain getcredentialing[.]com

—

Our Mirai.TBOT IoC expansion allowed us to obtain 6,870 unreported potentially connected threat artifacts. We also uncovered several malicious web properties, including 11 IP addresses to which some of the domain IoCs resolved and six IP-connected domains.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to [contact us](#).

Disclaimer: We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as “threats” or “malicious” may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.



Appendix: Sample Artifacts

Sample Additional IP Addresses

- 185[.]194[.]176[.]137
- 185[.]194[.]176[.]249
- 185[.]194[.]176[.]252
- 45[.]95[.]146[.]126
- 85[.]209[.]134[.]96
- 91[.]92[.]241[.]184
- 91[.]92[.]244[.]7

Sample Malicious Additional IP Addresses

- 185[.]194[.]176[.]137
- 45[.]95[.]146[.]126
- 85[.]209[.]134[.]96
- 91[.]92[.]241[.]184
- 91[.]92[.]244[.]7
- 91[.]92[.]251[.]113

Sample IP-Connected Domains

Note that all the IP-connected domains we found were already being tagged as malicious.

- akamaicute[.]online
- dsfasdfasdfasd[.]online
- hailnet[.]online
- oosdfewugsd[.]online

Sample String-Connected Domains

- cjfop[.]loan
- cjfop[.]nom[.]za
- cjfopa9[.]top
- cjfopz[.]top
- czbrwanuk[.]xyz
- ede[.]ac
- ede[.]accountant
- ede[.]adm[.]br
- ede[.]ae
- ede[.]aero
- ede[.]africa
- ede[.]agency
- ede[.]ai
- ede[.]airport[.]aero
- ede[.]app
- ede[.]asia
- ede[.]at
- ede[.]au
- ede[.]auto[.]pl
- ede[.]ba
- ede[.]be
- ede[.]bid
- ede[.]biz
- ede[.]bj[.]cn
- ede[.]blue
- ede[.]bz
- ede[.]ca
- ede[.]care
- ede[.]cat
- ede[.]catering
- ede[.]cc
- ede[.]center
- ede[.]city
- ede[.]cl



- ede[.]clothing
- ede[.]cloud
- ede[.]club
- ede[.]cm
- ede[.]cn
- ede[.]co
- ede[.]co[.]at
- ede[.]co[.]il
- ede[.]co[.]in
- ede[.]co[.]kr
- ede[.]co[.]nz
- ede[.]co[.]th
- ede[.]co[.]uk
- ede[.]co[.]za
- ede[.]coffee
- ede[.]com
- ede[.]com[.]au
- ede[.]com[.]br
- ede[.]com[.]cn
- ede[.]com[.]co
- ede[.]com[.]ec
- ede[.]com[.]es
- ede[.]com[.]hk
- ede[.]com[.]mx
- ede[.]com[.]my
- ede[.]com[.]ng
- ede[.]com[.]pk
- ede[.]com[.]pl
- ede[.]com[.]sa
- ede[.]com[.]tr
- ede[.]com[.]tw
- ede[.]com[.]ua
- ede[.]com[.]vn
- ede[.]cool
- ede[.]country
- ede[.]cz
- ede[.]dance
- ede[.]date
- ede[.]dating
- ede[.]de
- ede[.]design
- ede[.]digital
- ede[.]directory
- ede[.]dk
- ede[.]download
- ede[.]durban
- ede[.]earth
- ede[.]ec
- ede[.]education
- ede[.]ee
- ede[.]email
- ede[.]es
- ede[.]eu
- ede[.]events
- ede[.]exchange
- ede[.]faith
- ede[.]family
- ede[.]fi
- ede[.]finance
- ede[.]fitness
- ede[.]fj[.]cn
- ede[.]fm
- ede[.]fr
- ede[.]fun
- ede[.]gdh
- ede[.]gg