WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Tracking Down Sea Turtle IoCs in the DNS Ocean

Table of Contents

Executive Report

The Sea Turtle threat group recently made headlines when it expanded its operations to target ISPs and telecommunications and media companies in the Netherlands. In the past, Sea Turtle primarily targeted organizations in the Middle East and the U.S. using DNS hijacking and man-in-the-middle (MitM) attacks.

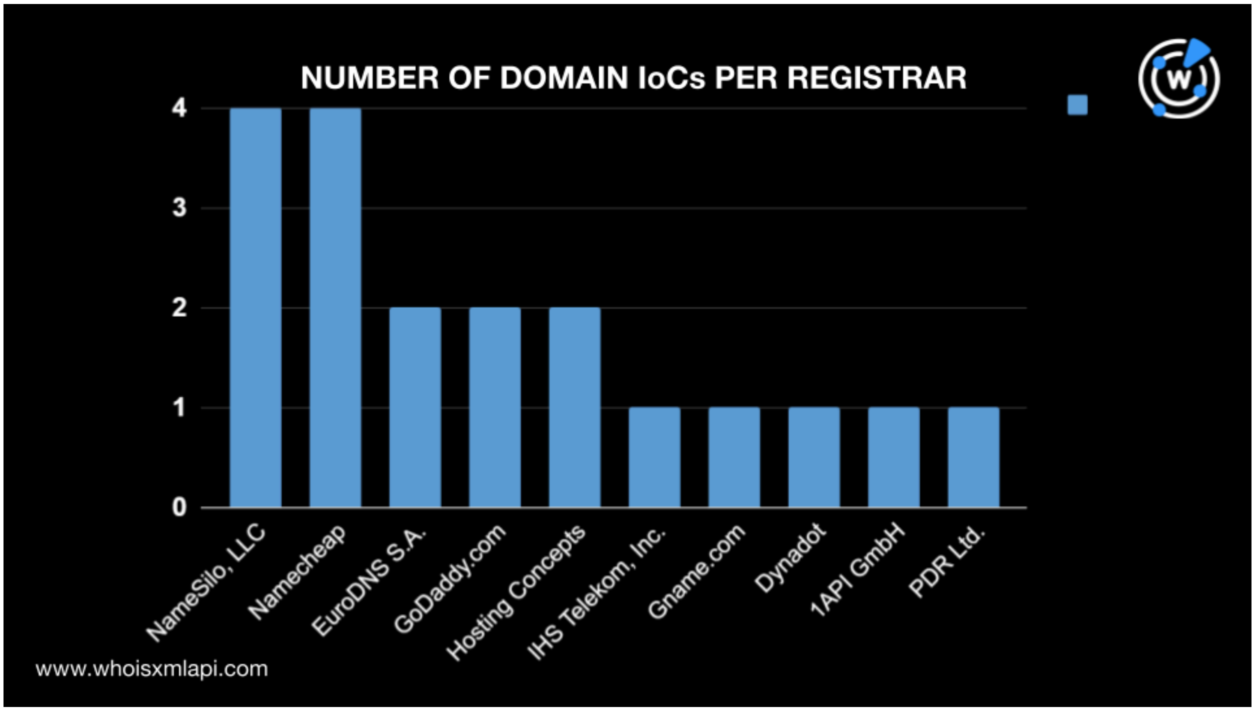
Before news about the threat group's attack on Dutch organizations, StrikeReady published a list of indicators of compromise (IoCs) comprising 14 IP addresses, eight subdomains, and 15 domains. To find more digital footprints and connected artifacts, the WhoisXML API research team expanded the IoC list that led to the discovery of:

- 81 email-connected domains
- 12 additional IP addresses
- 13 IP-connected domains
- 204 string-connected domains

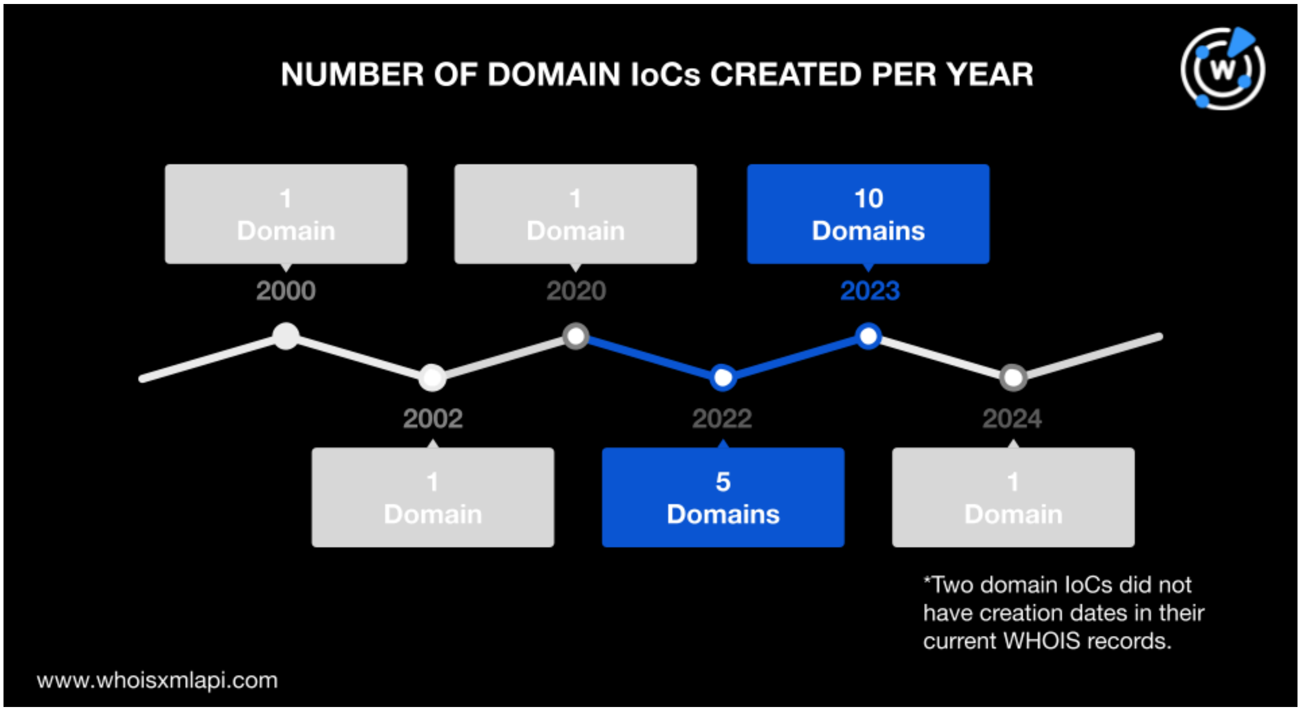
Infrastructure Analysis of the Sea Turtle IoCs

Following our usual first step, we analyzed the Sea Turtle IoCs to uncover more details. We began by performing a bulk WHOIS lookup for 21 domains (15 domains and six domains extracted from the subdomains tagged as IoCs) and found that:

- They were administered by 10 different registrars—NameSilo LLC and Namecheap, which accounted for four domains each; EuroDNS S.A., GoDaddy, and Hosting Concepts with two domains each; and IHS Telekom, Inc., Gname.com, Dynadot, 1API GmbH, and PDR Ltd. with one domain each. Two IoCs did not have current registrar data.

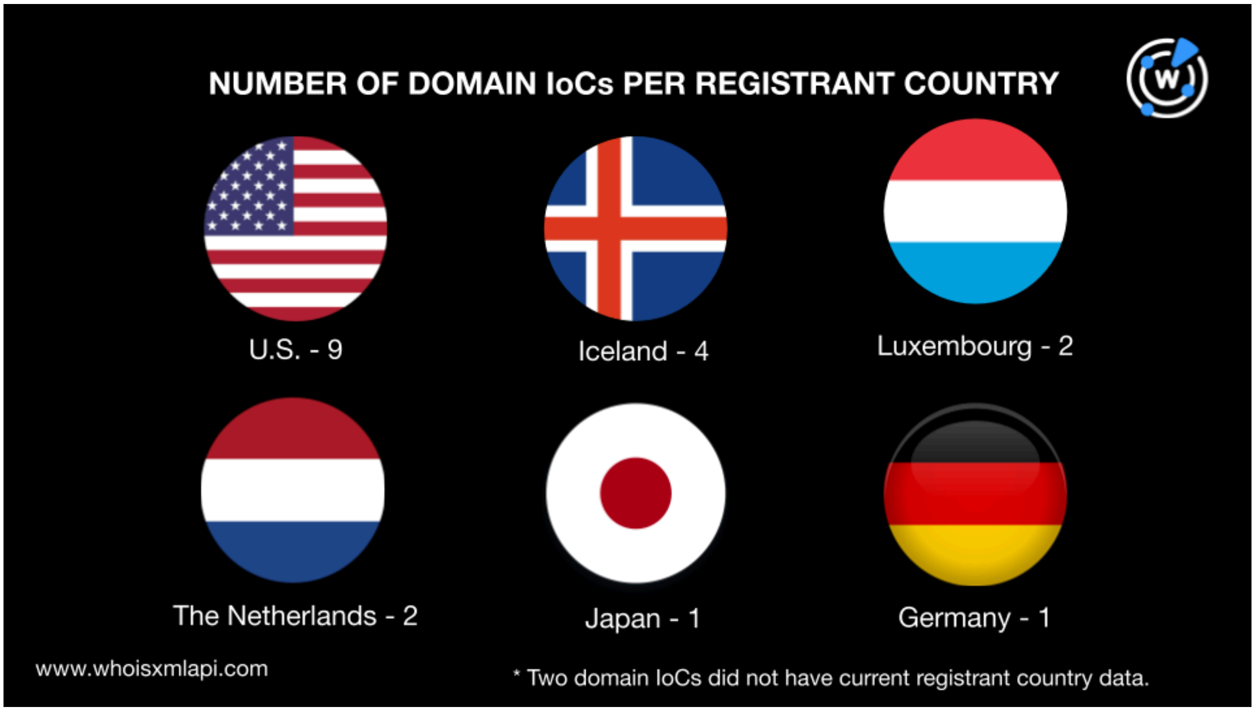


- One domain was created in 2024, 10 in 2023, five in 2022, one in 2020, one in 2002, and the oldest was created in 2000. The remaining two domains had no creation dates in their current WHOIS records.

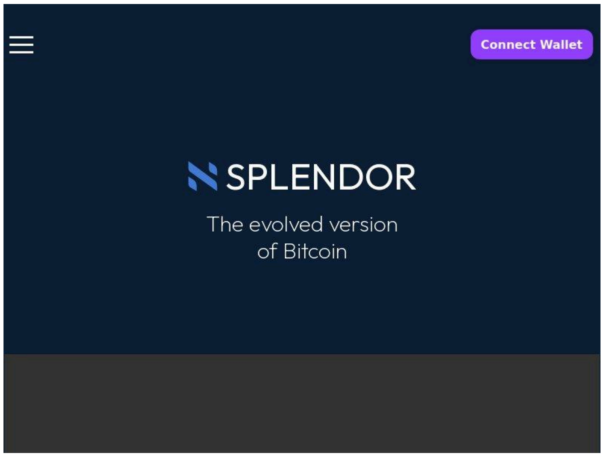


*Two domain IoCs did not have creation dates in their current WHOIS records.

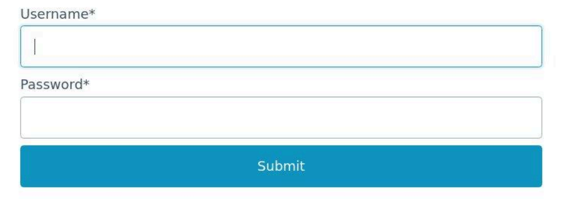
- They were spread across six registrant countries. Nine were registered in the U.S., four in Iceland, two each in Luxembourg and the Netherlands, and one each in Japan and Germany. Two domains did not have current registrant country data.



We also subjected the domain IoCs to a screenshot analysis, which revealed that some continued to host live content. They included the websites below.



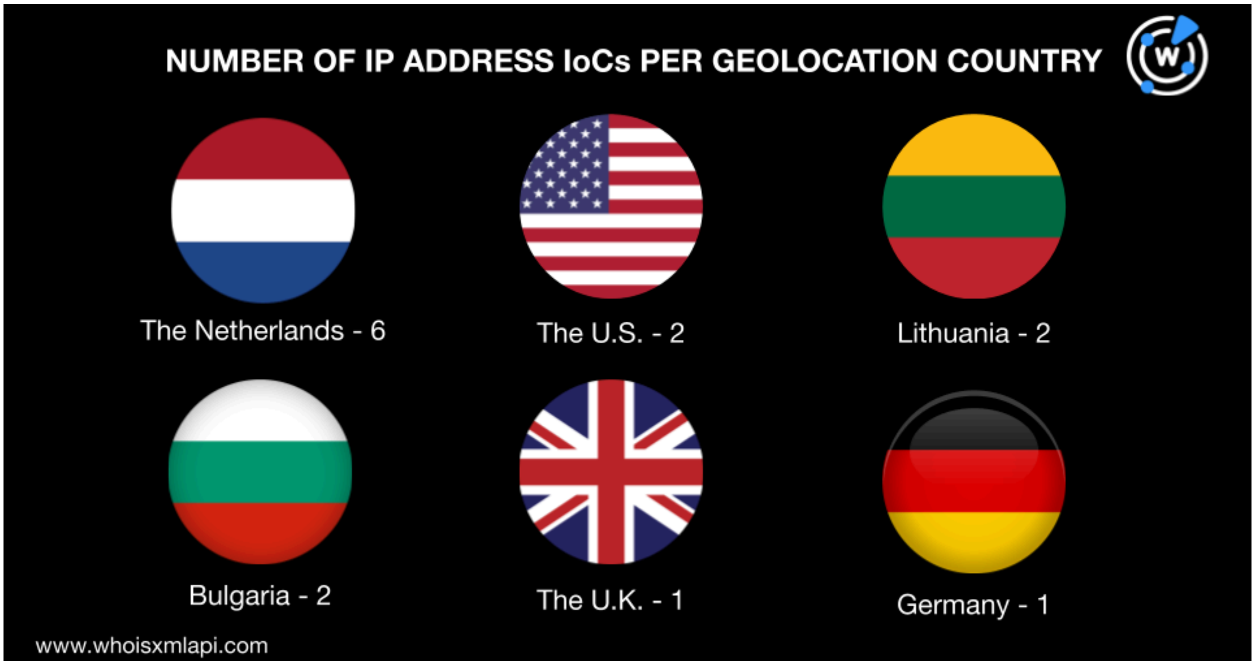
Screenshot of domain IoC splendor[.]org



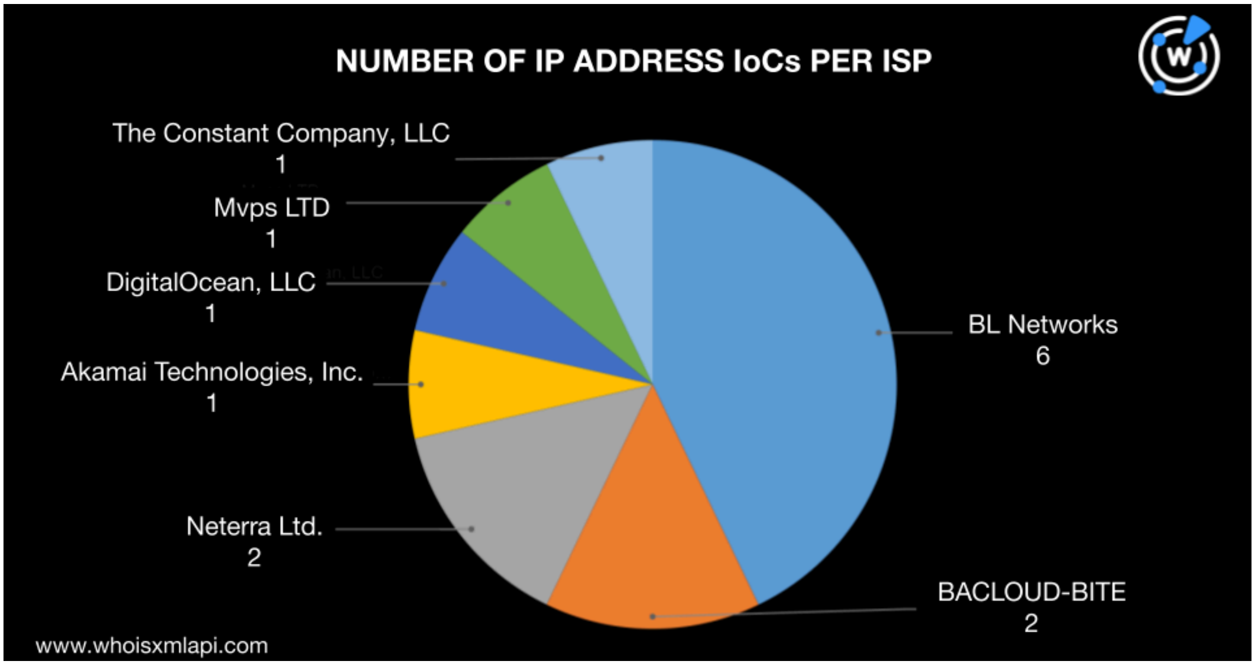
Screenshot of domain IoC splendos[.]org

Next, we did a bulk IP geolocation lookup on the 14 IP addresses listed as IoCs, which revealed that:

- They were spread across six geolocation countries—six in the Netherlands; two each in the U.S., Lithuania, and Bulgaria; and one each in Germany and the U.K.



- They were administered by seven ISPs led by BL Networks, which accounted for six IP addresses. BACLOUD-BITE and Neterra Ltd. managed two IP addresses each while DigitalOcean, LLC, Akamai Technologies, Inc., Mvps LTD, and The Constant Company, LLC handled one IP address each.



Uncovering Sea Turtle DNS Connections

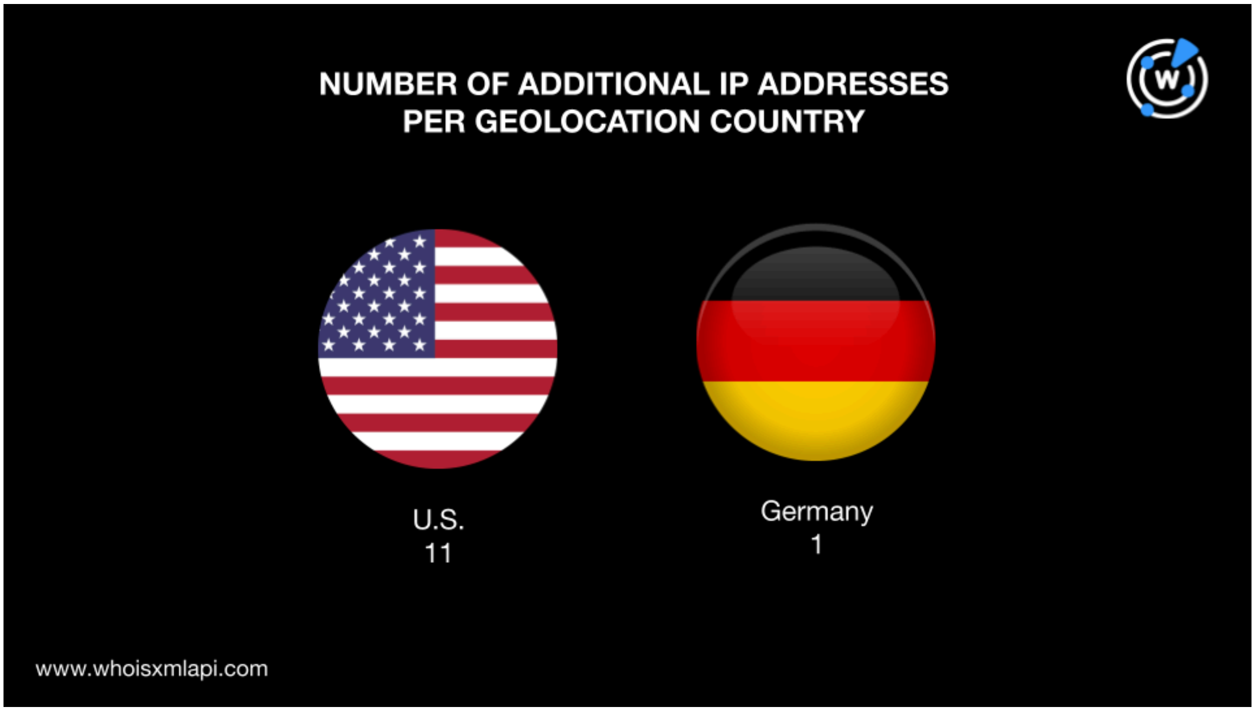
We then searched the DNS for more traces of Sea Turtle resources.

WHOIS History API searches for the domain IoCs led to the discovery of 33 email addresses in their historical WHOIS records. Although only one of the email addresses was public, Reverse WHOIS API searches showed that it appeared in the current WHOIS records of 81 domains after duplicates and IoCs were filtered out.

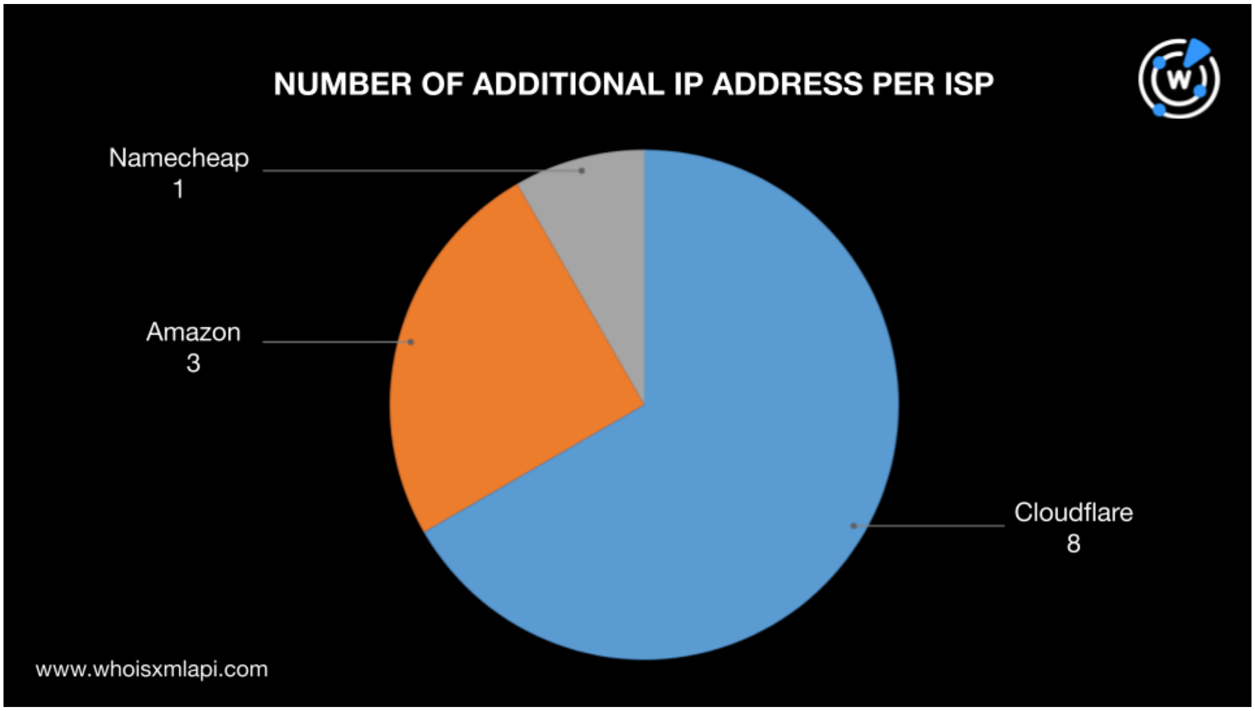
Next, we performed DNS lookups on the 21 domain IoCs, which led us to 12 unique IP addresses, excluding those already tagged as IoCs.

IP geolocation lookups for the 12 additional IP addresses showed that:

- They were spread across two countries that were also the origin of three IoCs. Eleven of the IP addresses were geolocated in the U.S. while one pointed to Germany as its origin.


NUMBER OF ADDITIONAL IP ADDRESSES PER GEOLOCATION COUNTRY

- They were managed by three ISPs—Cloudflare with eight IP addresses, Amazon with three, and Namecheap with one.

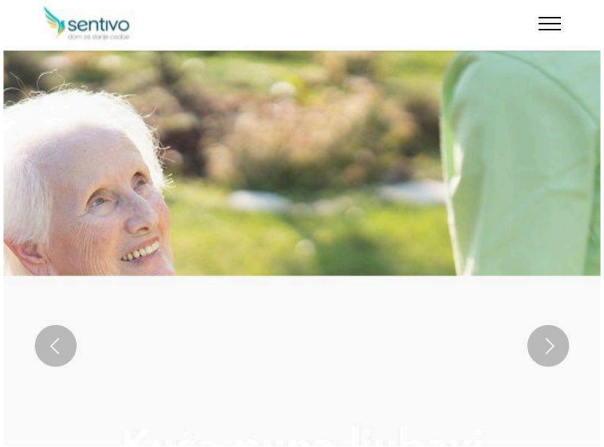
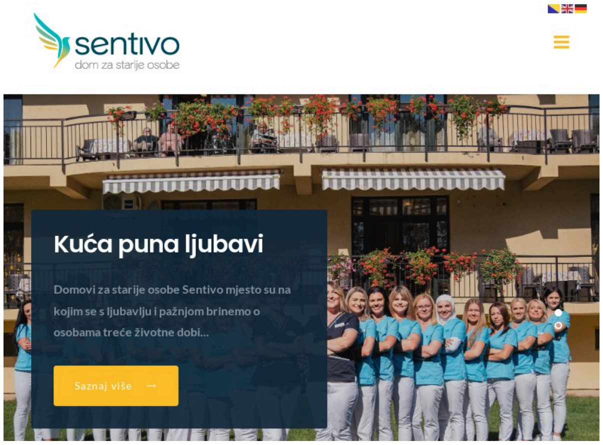

NUMBER OF ADDITIONAL IP ADDRESS PER ISP

- Threat Intelligence API also revealed that all 12 IP addresses were involved in various threats. A few examples are shown in the table below.

IP ADDRESSES	ASSOCIATED THREAT TYPES
3[.]33[.]130[.]190	Phishing Malware Command-and-control (C2) Generic Suspicious
15[.]197[.]148[.]33	Phishing Malware C2 Generic Suspicious
104[.]21[.]67[.]252	Phishing Malware Generic
172[.]67[.]183[.]141	Phishing Malware Generic
2606:4700:3034::6815:43fc	Phishing Malware Generic

Reverse IP lookups for the 12 additional IP addresses and 14 IP address IoCs revealed that eight were potentially dedicated. They led to 13 IP-connected domains after duplicates, the IoCs, and email-connected domains were removed.

Screenshot analyses for the IP-connected domains revealed that one domain—rocosmetic[.]club—hosted content similar to Dom Sentivo, a nursing home in Ilidža, Bosnia and Herzegovina.

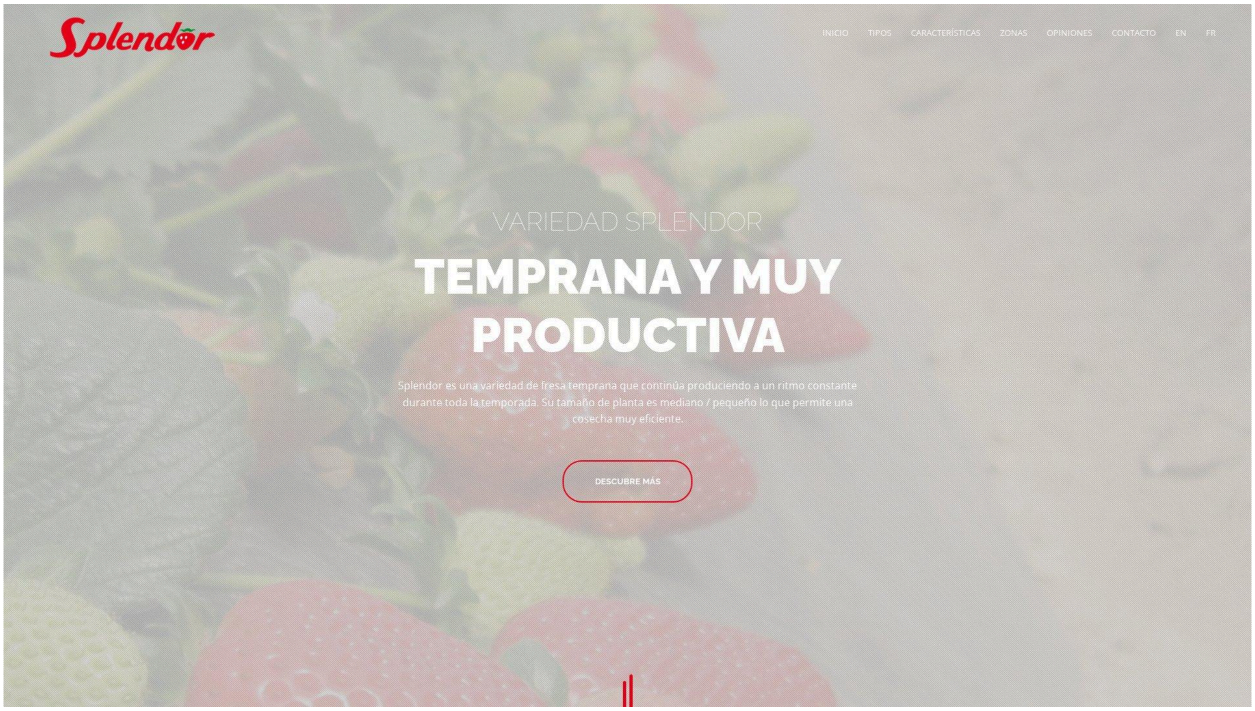
 Screenshot of IP-connected domain rocosmetic[.]club	 Kuća puna ljubavi Domovi za starije osobe Sentivo mjesto su na kojim se s ljubavlju i pažnjom brinemo o osobama treće životne dobi... Screenshot of domsentivo[.]com

The final step of our investigation entailed looking for string-connected domains using Domains & Subdomains Discovery with the **Starts with** search parameter. We found 202 domains containing these four text strings that appeared in the domain IoCs:

- **splendor.**
- **splendos.**
- **solhaber.**
- **xtechsupport.**

We also found two additional subdomains that began with the text string **ai-connector**, which also appeared in two subdomains tagged as IoCs. The total number of string-connected domains we discovered was 204, after removing duplicates, the IoCs, and email- and IP-connected domains.

Threat intelligence lookups revealed that one of the string-connected domains—splendor[.]es—was associated with malicious command and control and malware attacks. It hosted the following content based on a screenshot lookup:



VARIEDAD SPLENDOR

TEMPRANA Y MUY PRODUCTIVA

Splendor es una variedad de fresa temprana que continúa produciendo a un ritmo constante durante toda la temporada. Su tamaño de planta es mediano / pequeño lo que permite una cosecha muy eficiente.

—

Our expansion of the Sea Turtle IoCs led to the discovery of 311 potentially connected artifacts comprising one personal email address, 81 email-connected domains, 12 additional IP addresses, 13 IP-connected domains, and 204 string-connected domains. We also found several suspicious and malicious web properties, including 12 IP addresses, one IP-connected domain, and one string-connected domain.

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 Email-Connected Domains

- sporcu[.]co
- turuncsenizapart[.]com

- rs11outlet[.]com
- marmarisoutlet[.]com
- orhansaglam[.]com[.]tr
- mavisel[.]com[.]tr
- zimbba[.]com
- nuremlakmarmaris[.]com
- creaberg[.]com
- sohomarmaris[.]com
- hkyapi[.]com
- ysemlak[.]com
- tatiloskop[.]com
- kalorimatik[.]com
- policem41[.]com
- policem54[.]com
- tatilekac[.]com
- kesfetti[.]com
- policem16[.]com
- herturburada[.]com

Sample Additional IP Addresses

Note that all of the additional IP addresses were already being tagged as malicious.

- 3[.]33[.]130[.]190
- 15[.]197[.]148[.]33
- 104[.]21[.]67[.]252
- 172[.]67[.]183[.]141
- 2606:4700:3034::6815:43fc
- 2606:4700:3031::ac43:b78

Sample IP-Connected Domains

- greenblu[.]club
- statemntcorrection-mybeii[.]com
- rocosmetic[.]xyz
- rocosmetic[.]top
- rocosmetic[.]info
- rocosmetic[.]club
- pageforyou[.]top

Sample String-Connected Domains

- xtechsupport[.]com
- splendor[.]world
- splendor[.]dev
- splendor[.]kz
- splendor[.]technology
- splendor[.]tk
- splendor[.]africa
- splendor[.]hu
- splendor[.]ch
- splendor[.]ga
- splendor[.]top
- splendor[.]tn
- splendor[.]luxury
- splendor[.]hk
- splendor[.]by
- splendor[.]rocks
- splendor[.]cz
- splendor[.]us
- splendor[.]pl
- splendor[.]cl
- splendor[.]city
- splendor[.]ind[.]br
- splendor[.]amsterdam
- splendor[.]tokyo
- splendor[.]team
- splendor[.]plus
- splendor[.]info
- splendor[.]nz

- splendor[.]co[.]th
- splendor[.]house
- splendor[.]tv
- splendor[.]ir
- splendor[.]pt
- splendor[.]net[.]pl
- splendor[.]site
- splendor[.]name
- splendor[.]blog
- splendor[.]com[.]cn
- splendor[.]ro
- splendor[.]xyz
- solhaber[.]com
- solhaber[.]org
- solhaber[.]ml
- solhaber[.]xyz
- solhaber[.]tk
- solhaber[.]com[.]tr
- solhaber[.]org[.]tr
- splendos[.]com
- solhaber[.]net
- solhaber[.]site
- solhaber[.]org[.]tr
- splendos[.]com
- solhaber[.]net
- solhaber[.]site