Tracing Ivanti Zero-Day Exploitation IoCs in the DNS

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts

Executive Report

Among the latest to suffer from zero-day exploitation is Ivanti, a software company providing endpoint management and remote access solutions to various organizations, including U.S. federal agencies. High-impact zero-day vulnerabilities affecting Ivanti Connect Secure VPN and Policy Secure were recently reported, which could allow threat actors to execute arbitrary code with high-level access.

Mandiant already reported zero-day exploitations using these vulnerabilities by UNC5221, a suspected China-based espionage threat group. Other unknown threat groups may have also exploited the vulnerabilities. Mandiant published an in-depth investigation of the exploitation, including a list of indicators of compromise (IoCs) comprising 10 domains, two subdomains, and eight IP addresses.

In an effort to find more information and possibly connected artifacts, the WhoisXML API research team expanded the IoC list, leading to the discovery of:

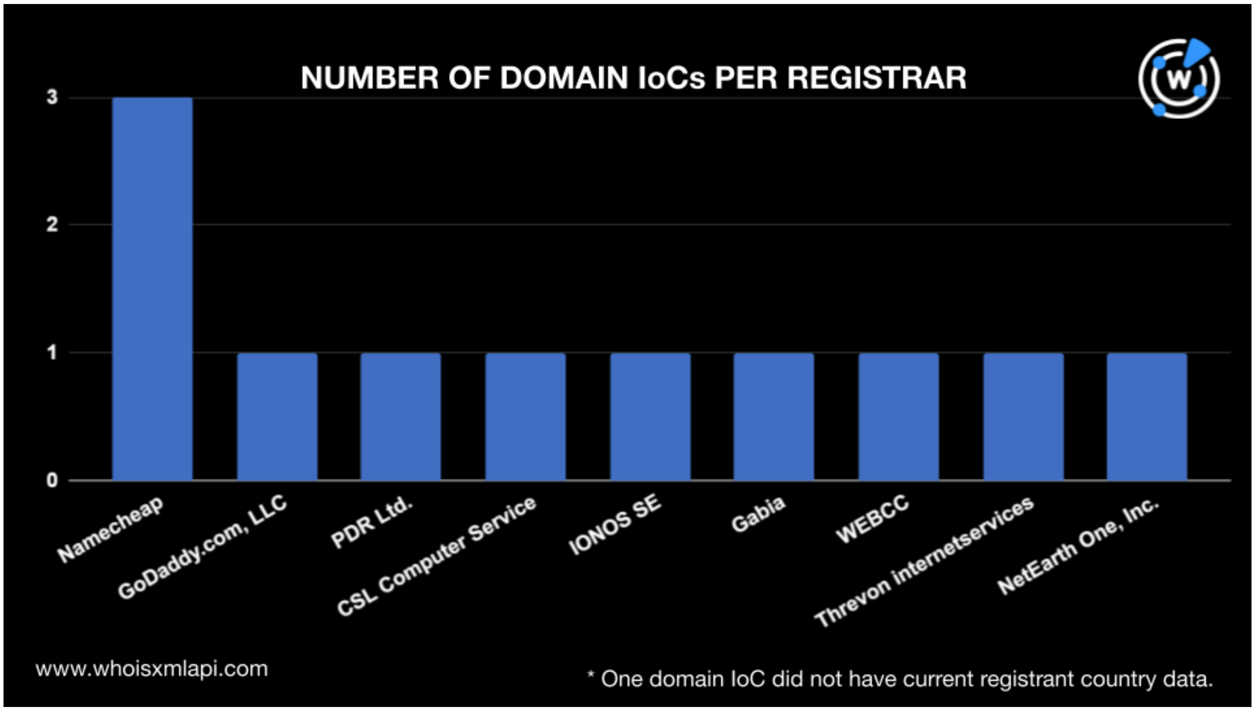
- Three public email addresses
- 33 email-connected domains
- 13 additional IP addresses
- 211 IP-connected domains
- 153 string-connected domains

A sample of the additional artifacts obtained from our analysis is available for download on our website.

Infrastructure Analysis of the Ivanti Zero-Day Exploitation IoCs

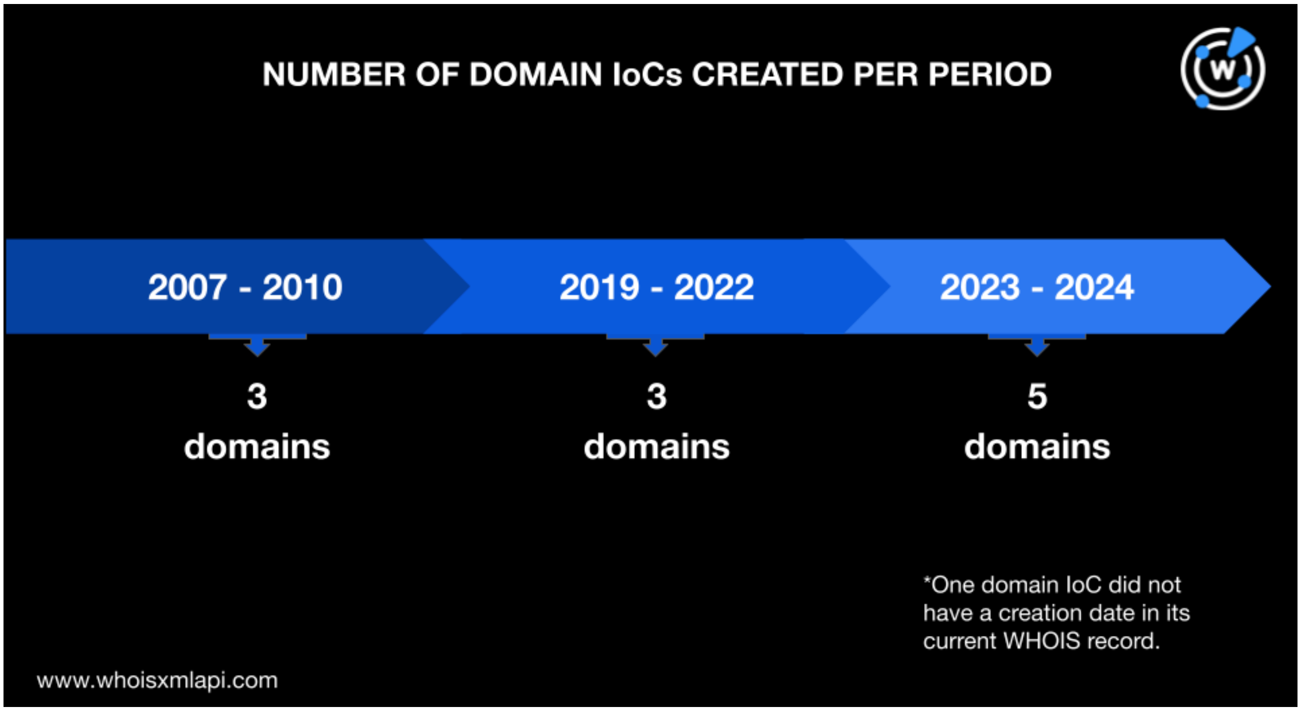
As our usual first step in analyzing IoCs, we performed a bulk WHOIS lookup for 12 domains (10 domain IoCs and two domains extracted from the subdomains tagged as IoCs) and found that:

- They were administered by nine different registrars—Namecheap, which accounted for three domains, and GoDaddy.com LLC; PDR Ltd.; CSL Computer Service Langenbach GmbH; IONOS SE; Gabia; WEBCC; Threvon Internet Services; and NetEarth One, Inc. with one domain each. One IoC did not have current registrar data.



* One domain IoC did not have current registrant country data.

- Three domains were created in 2024, two in 2023, one in 2022, one in 2021, one in 2019, two in 2010, and the oldest in 2007. The remaining domain had no creation date in its current WHOIS record.



NUMBER OF DOMAIN IoCs CREATED PER PERIOD

2007 - 2010

3 domains

2019 - 2022

3 domains

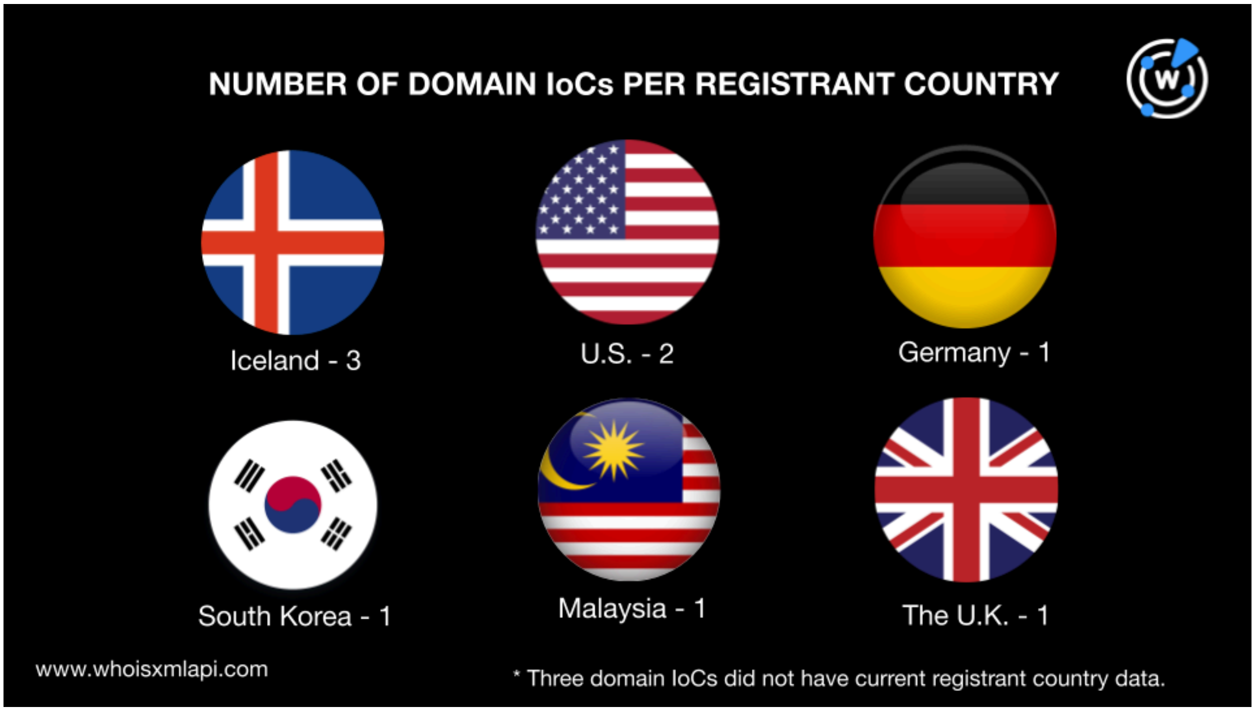
2023 - 2024

5 domains

*One domain IoC did not have a creation date in its current WHOIS record.

www.whoisxmlapi.com

- They were spread across six registrant countries. Three were registered in Iceland, two in the U.S., and one each in Germany, South Korea, Malaysia, and the U.K. Three domains did not have a current registrant country data.



NUMBER OF DOMAIN IoCs PER REGISTRANT COUNTRY

Iceland - 3

U.S. - 2

Germany - 1

South Korea - 1

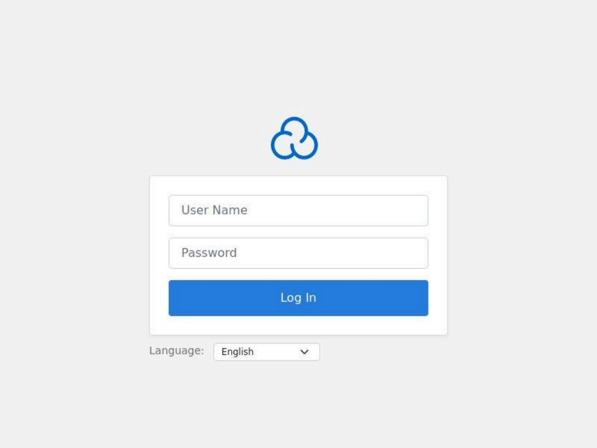
Malaysia - 1

The U.K. - 1

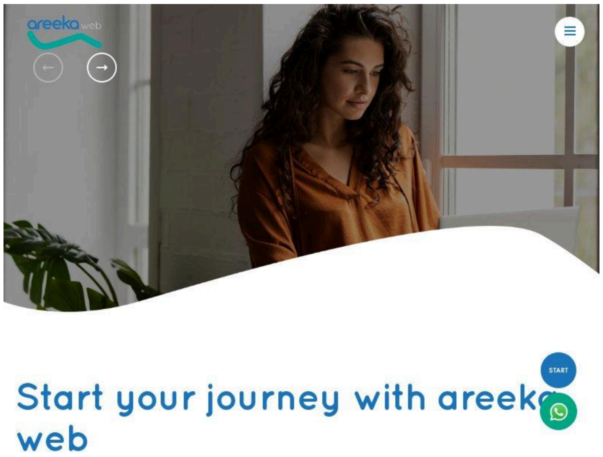
www.whoisxmlapi.com

* Three domain IoCs did not have current registrant country data.

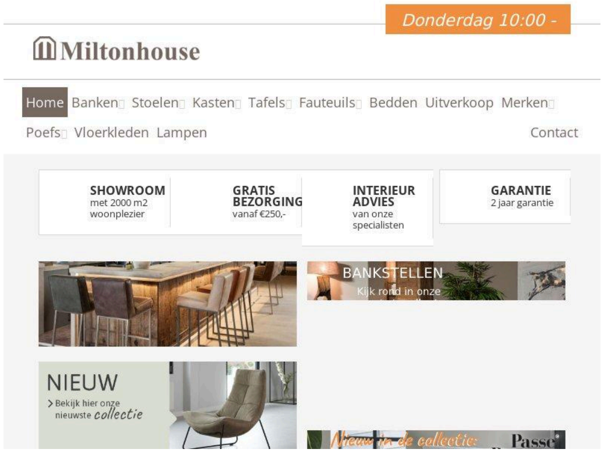
We also subjected the domain IoCs to a screenshot analysis, which revealed that some continued to host live content, including the websites below.



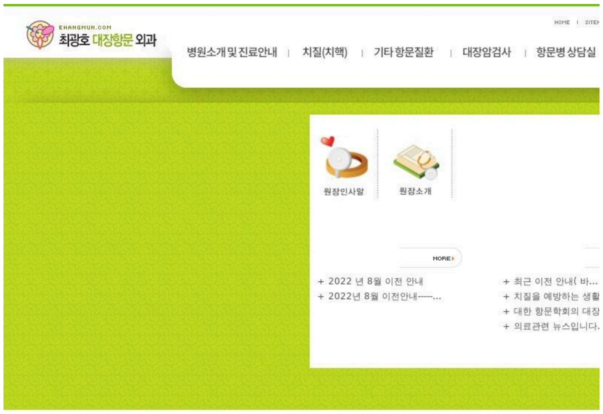
Screenshot of domain IoC cpanel[.]netbar[.]org



Screenshot of domain IoC areekaweb[.]com



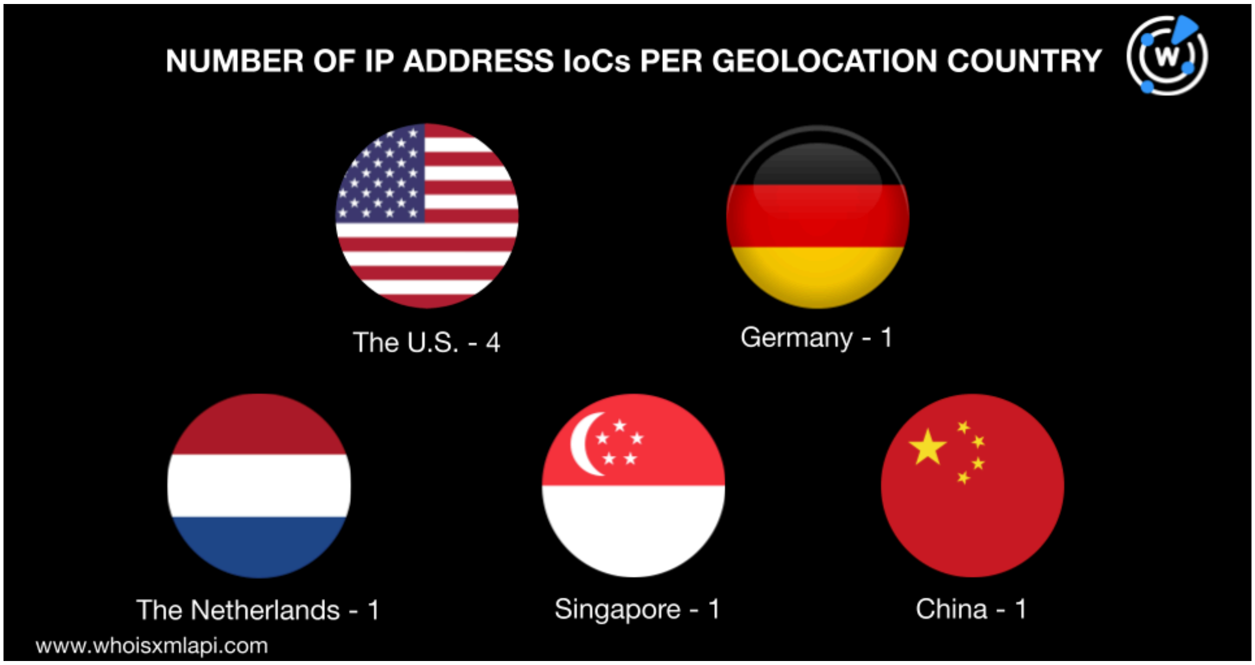
Screenshot of domain IoC miltonhous[.]enl



Screenshot of domain IoC ehangmun[.]com

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

- They were spread across five geolocation countries—four in the U.S. and one each in Germany, the Netherlands, Singapore, and China.



- Each was administered by a different ISP, namely, Host Europe GmbH, DigitalOcean LLC, Hangzhou Alibaba Advertising Co. Ltd., Limenet, Corporación Dana S.A., Comcast Cable Communications LLC, BL Networks, and Cablevision Systems Corp.

Mapping the DNS Connections of the Ivanti Zero-Day Exploitation IoCs

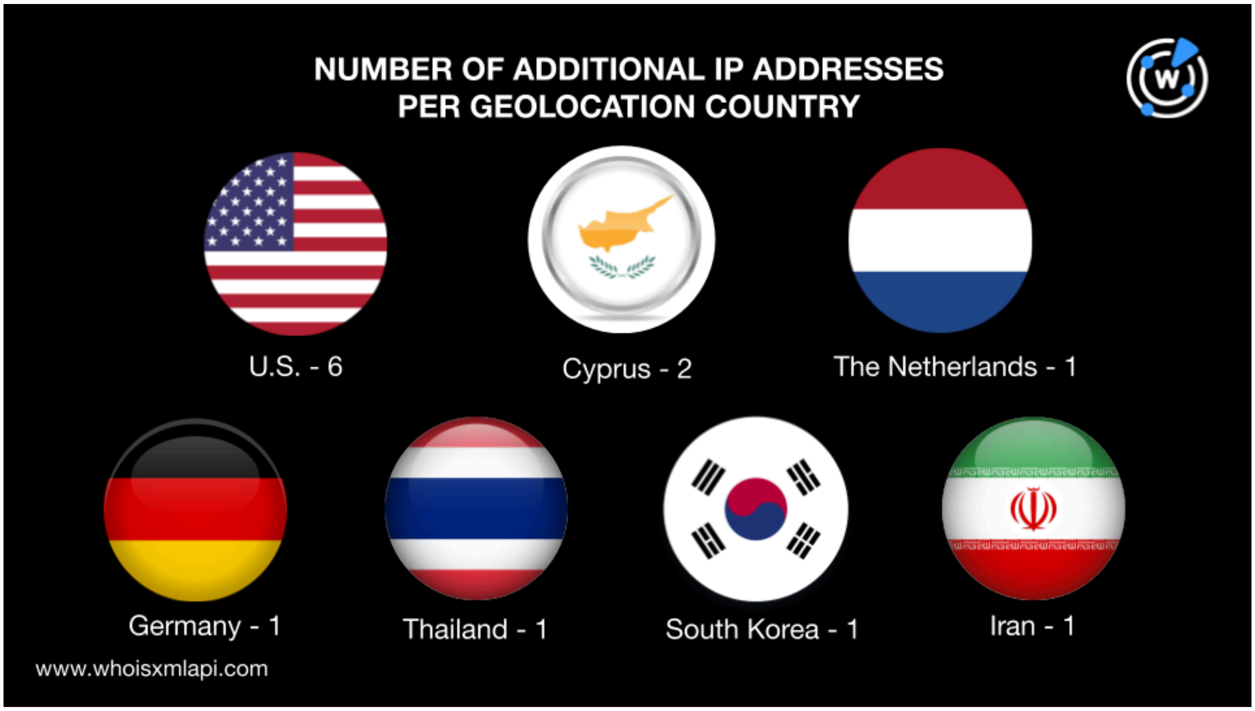
Our next step was to scour the DNS for more traces of the malicious resources used in the vulnerability exploitation.

WHOIS History API searches for the domain IoCs enabled us to discover 14 email addresses in their historical WHOIS records, three of which were public. Subjecting the three unredacted email addresses to Reverse WHOIS API searches revealed that they appeared in the current WHOIS records of 33 domains after duplicates and IoCs were removed.

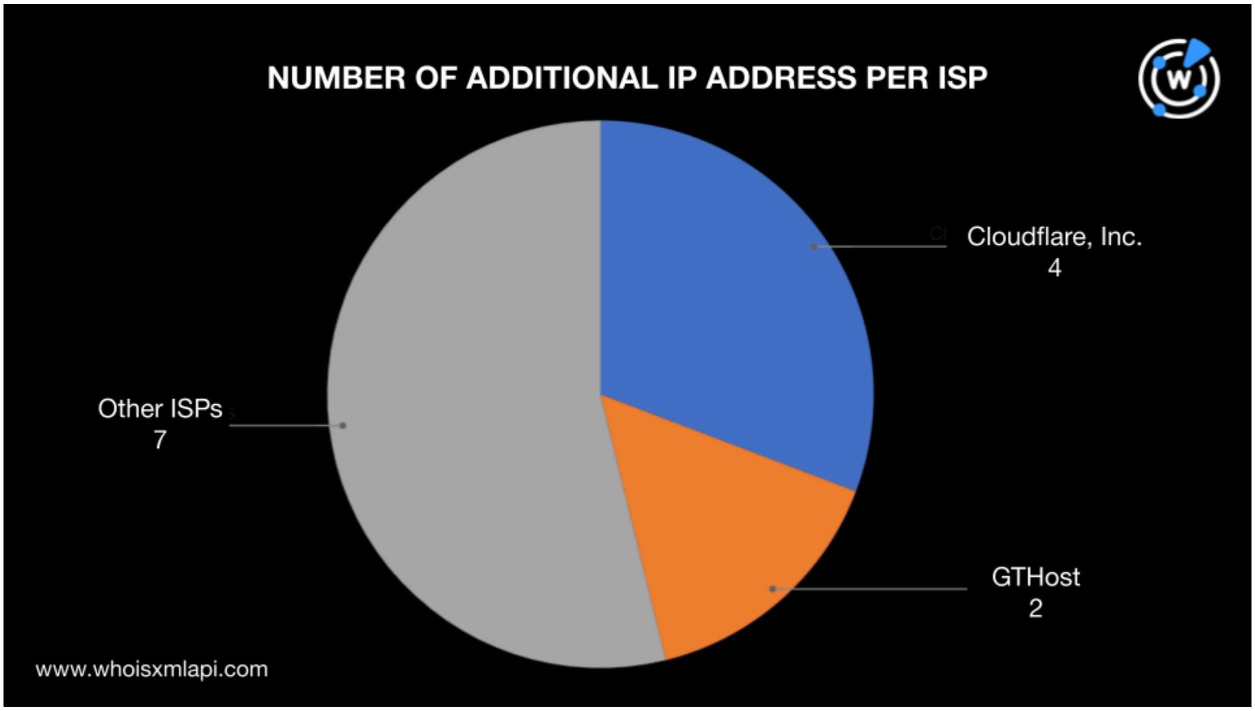
Next, we performed DNS lookups for the 12 domain IoCs (including two from the subdomains tagged as IoCs), which led us to 13 unique IP addresses, excluding those already tagged as IoCs.

The 13 additional IP addresses were then subjected to IP geolocation lookups, which revealed that:

- They were geolocated in seven countries, three of which were also the origin of three IoCs. Six IP addresses pointed to the U.S. as their origin, two were geolocated in Cyprus, and one each in the Netherlands, Germany, Thailand, South Korea, and Iran.



- They were managed by nine ISPs—Cloudflare with four IP addresses, GTHost with two, and Signet BV, IONOS SE, Siamdata Communication Co. Ltd., Korea Telecom, QuadraNet Enterprises LLC, SoftLayer, and Pars Parva System LLC with one IP address each.

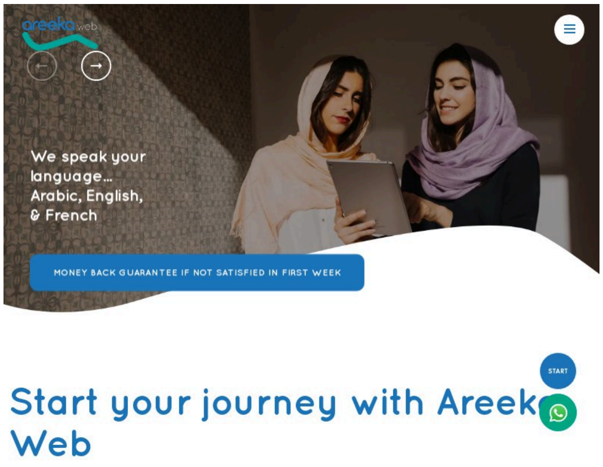


- Threat Intelligence API also revealed that all 13 IP addresses were associated with various threats. A few examples are shown in the table below.

IP ADDRESSES	ASSOCIATED THREAT TYPES
104[.]21[.]61[.]132	Phishing Malware Generic
217[.]160[.]0[.]177	Phishing Malware
5[.]8[.]18[.]6	Malware Generic
172[.]67[.]209[.]167	Phishing Malware Generic
104[.]21[.]69[.]158	Phishing Malware Generic

To find more connected domains, we subjected the 13 additional IP addresses and eight IP address IoCs to reverse IP lookups, which showed that nine were potentially dedicated. They led to 211 IP-connected domains after filtering out duplicates, the IoCs, and email-connected domains.

Screenshot analyses for the IP-connected domains revealed that one domain—tedtankal[.]xyz—hosted content similar to one of the domain IoCs, areekaweb[.]com. While the two domains had redacted WHOIS records, they were both registered with GoDaddy.

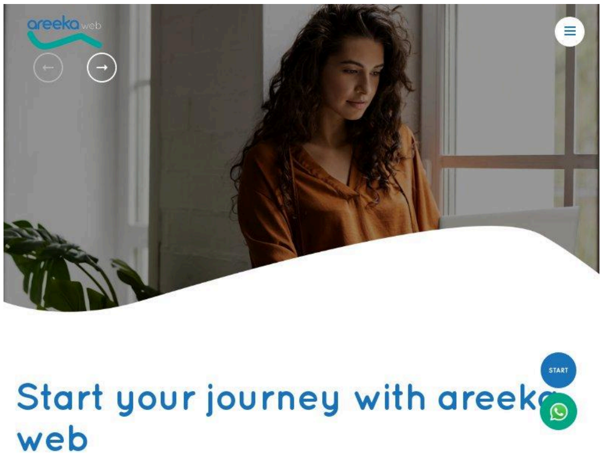


We speak your language… Arabic, English, & French

MONEY BACK GUARANTEE IF NOT SATISFIED IN FIRST WEEK

Start your journey with Areeka Web

Screenshot of IP-connected domain tedtankal[.]xyz



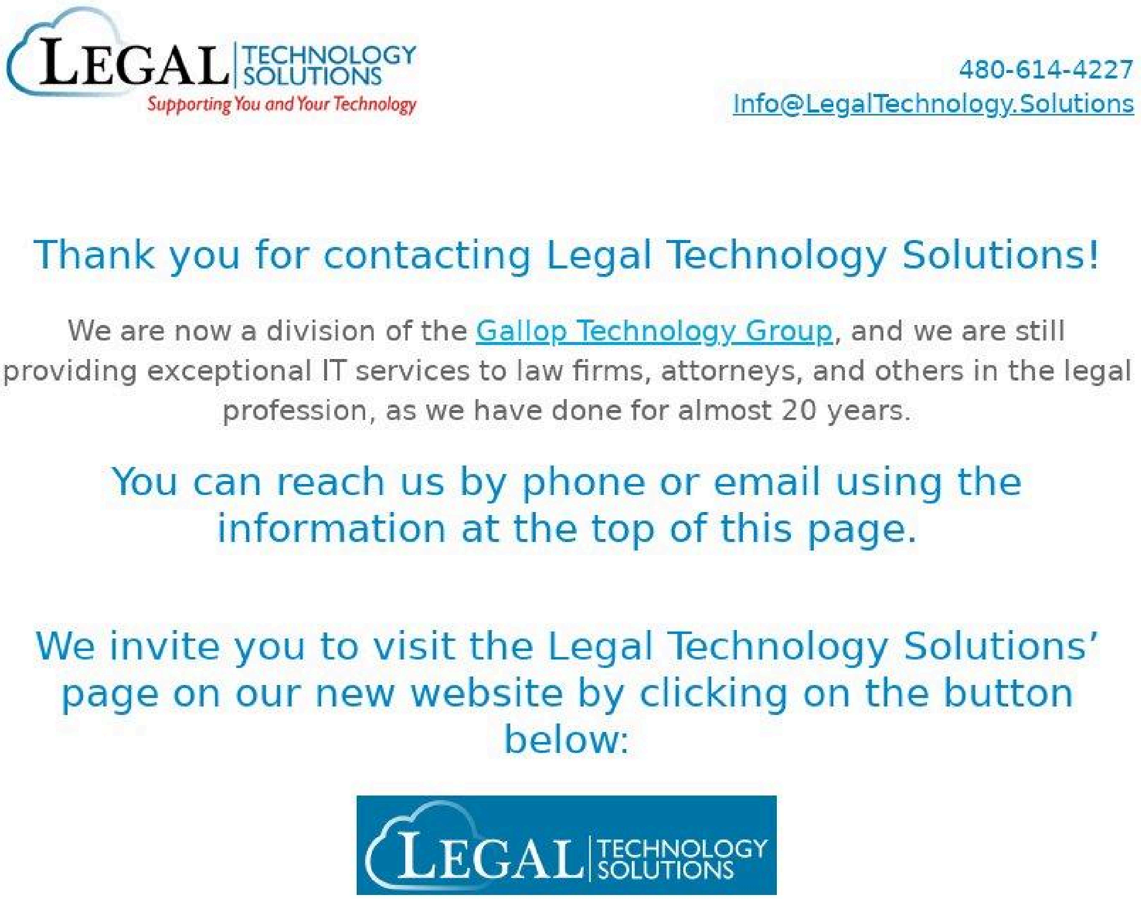
Start your journey with areeka web

Screenshot of domain IoC areekaweb[.]com

As a final step, we looked for string-connected domains using Domains & Subdomains Discovery using the **Starts with** search parameter. They led to the discovery of 145 domains that began with these strings that appeared among the domain IoCs:

- **symantke**
- **miltonhouse.**
- **entraide-internationale**
- **clickcom.**
- **clicko.**
- **duorhytm**
- **line-api**
- **areekaweb**
- **ehangmun**
- **secure-cama**

Meanwhile, a wildcard search on Threat Intelligence API using the string **clicko** (i.e., **clicko***) revealed eight domains associated with phishing, malware, and other threats. One of the malicious domains continued to host live content.


LEGAL TECHNOLOGY SOLUTIONS
Supporting You and Your Technology

480-614-4227
Info@LegalTechnology.Solutions

Thank you for contacting Legal Technology Solutions!

We are now a division of the Gallop Technology Group, and we are still providing exceptional IT services to law firms, attorneys, and others in the legal profession, as we have done for almost 20 years.

You can reach us by phone or email using the information at the top of this page.

We invite you to visit the Legal Technology Solutions' page on our new website by clicking on the button below:

Screenshot of the malicious string-connected domain clickcomputerservices[.]com

—

Our investigation started out with 10 domains, two subdomains, and eight IP addresses tagged as IoCs in the zero-day exploitation of Ivanti vulnerabilities. It then led to the discovery of three public email addresses, 33 email-connected domains, 13 additional IP addresses, 211 IP-connected domains, and 153 string-connected domains. We also found that all 13 additional IP addresses and eight string-connected domains already figured in various cyber threats.

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

- ohs[.]com[.]cn
- hw-tech[.]net
- hitcn[.]net
- istarwild[.]com
- xn--fiqa70wb2hn4c03sb4smo9d[.]xn--55qx5d
- xn--fhq199gu2f40o[.]xn--55qx5d
- xn--fiqa70wb2h5jo5h0y4cuib[.]xn--55qx5d
- xn----kq6ab834ak7i4rdzq2c[.]xn--55qx5d
- vf-transformerasia[.]com
- glodon[.]us
- chenxiango2o[.]com
- xn--p5tq45e76a[.]com
- viewrankshare[.]com
- videohover[.]com
- videohilarity[.]com
- affluencenetwork[.]marketing
- videostore[.]click
- afflinkit[.]com
- creativebranding[.]club
- viralvideoclass[.]com

Sample Additional IP Addresses

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

- 104[.]21[.]61[.]132
- 188[.]240[.]53[.]22
- 217[.]160[.]0[.]177
- 5[.]8[.]18[.]6
- 5[.]8[.]18[.]4
- 172[.]67[.]209[.]167

Sample IP-Connected Domains

- 2sky[.]co[.]kr
- 33in[.]or[.]kr
- affmewin888[.]com
- anyink[.]ink
- anyink[.]kr
- anyink[.]net
- app[.]ezyinn-panel[.]com
- arche1[.]co[.]kr
- arh[.]co[.]kr
- arika[.]live
- atlantic21c[.]com
- babycap[.]co[.]kr
- bangkokdesignandprint[.]com
- barweb[.]ir
- beerlaokorea[.]co[.]kr
- belfarm[.]net
- biz-apps[.]com
- btenc[.]com
- bydforkliftth[.]com
- cenit[.]kr
- cenwha[.]com
- changdaegagu[.]com

- charish[.]co[.]th
- chongsolcoop[.]com
- cimaro[.]co[.]kr
- cnkmachine[.]com
- coolclinic[.]co[.]kr
- depia[.]co[.]kr
- dhammanava[.]net
- dhmtech[.]com
- digitaxs[.]com
- diode[.]kr
- dkpile[.]co[.]kr
- domyeong[.]co[.]kr
- dooripension[.]co[.]kr
- dumbwaiter[.]co[.]kr
- e-goldenbridge[.]co[.]kr
- e-goldenbridge[.]com
- egundrill[.]co[.]kr
- epostbanner[.]co[.]kr
- eraguardian[.]com
- eunsungpoly[.]co[.]kr
- eventhappy[.]co[.]kr
- eyang-wa[.]com
- ezyinn-panel[.]com
- faceoff1[.]com
- faceoffbaby[.]com
- faceprove[.]com
- fariwealth[.]com
- favolosovillasapanca[.]com

Sample String-Connected Domains

- symantkec[.]ga
- symantkec[.]tk
- miltonhouse[.]eu
- miltonhouse[.]pl
- miltonhouse[.]irish
- miltonhouse[.]co[.]uk
- miltonhouse[.]de
- miltonhouse[.]com[.]ua
- miltonhouse[.]gallery
- miltonhouse[.]cc
- miltonhouse[.]net
- miltonhouse[.]be
- miltonhouse[.]biz
- miltonhouse[.]com[.]pl
- miltonhouse[.]ca
- miltonhouse[.]co[.]za
- miltonhouse[.]uk
- miltonhouse[.]org
- miltonhouse[.]com
- clickcom[.]nl
- clickcom[.]info
- clickcom[.]app
- clickcom[.]co[.]uk
- clickcom[.]us
- clickcom[.]kr
- clickcom[.]pro
- clickcom[.]work
- clickcom[.]md
- clickcom[.]online
- clickcom[.]ru
- clickcom[.]store
- clickcom[.]org
- clickcom[.]net[.]br
- clickcom[.]tk
- clickcom[.]com
- clickcom[.]com[.]br
- clickcom[.]shop
- clickcom[.]at
- clickcom[.]biz
- clickcom[.]co[.]th
- clickcom[.]cl
- clickcom[.]it
- clickcom[.]es
- clickcom[.]vn
- clickcom[.]eu
- clickcom[.]xyz

- clickcom[.]co
- clickcom[.]net
- clickcom[.]io
- clickcom[.]guru

Sample Malicious String-Connected Domains

- clickcomputerstz[.]com
- clickcomfort[.]co
- clickco[.]net
- clickcounter1[.]com