Beneath the Belly of the Latest BlueNoroff Attack: A DNS Investigation

Table of Contents

Executive Report

Huntress was alerted to the recent BlueNorroff attack when an end-user reported potentially downloading a malicious Zoom extension on 11 June 2025. As it turned out, the malware came disguised as a Calendly meeting invite from a supposed contact sent via Telegram. Ironically, instead of a Google Meet page as the link hinted, the user ended up on a threat actor-controlled fake Zoom domain when clicked. That triggered the download of a malicious AppleScript whose final payload was the malware.

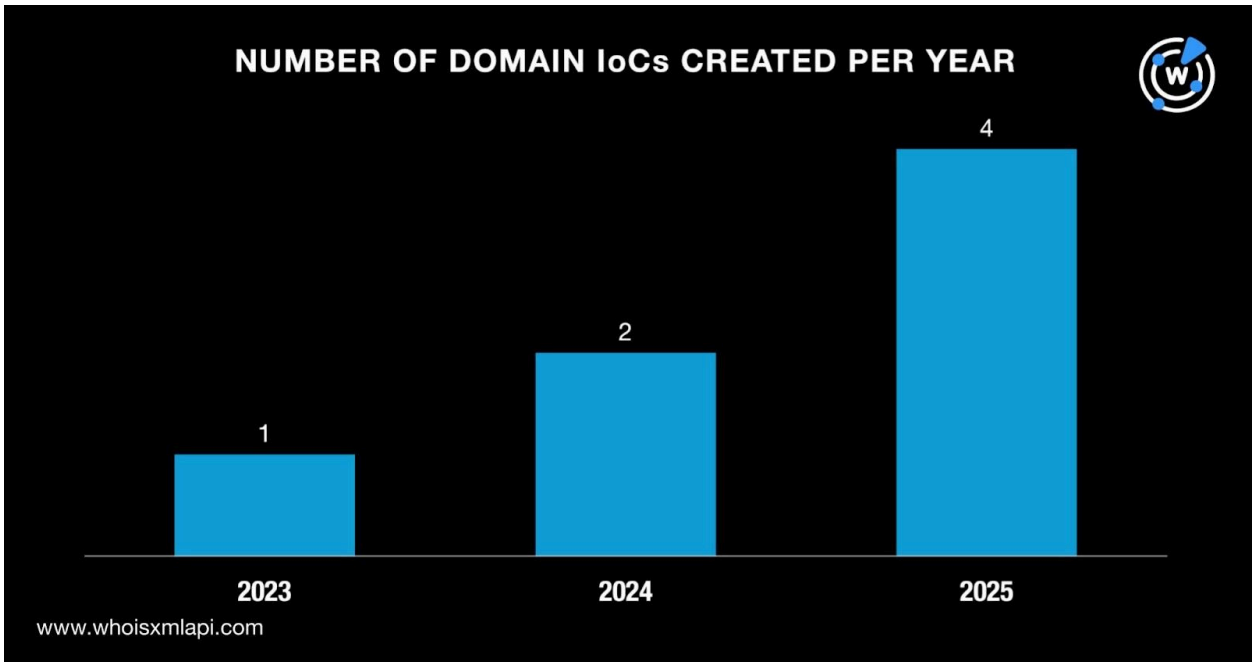
The researchers identified four domains and three URLs as indicators of compromise (IoCs) from which we derived seven domains for further analysis. Our bid to uncover more potentially connected artifacts notably led to the discovery of:

- Three domains tagged likely to turn malicious by First Watch Malicious Domains Data Feed 72–281 days prior to the attack's discovery
- 16 email-connected domains
- Six IP addresses, all turned out to be malicious
- 13 IP-connected domains, one turned out to be malicious
- 21,617 string-connected domains, 95 turned out to be malicious

A Closer Look at the IoCs

We began our investigation by querying the seven domains identified as IoCs on Bulk WHOIS API. We discovered that all of them had current WHOIS records that allowed us to determine that:

- They were created between 2 August 2023 and 31 March 2025, leading us to infer that BlueNoroff did not discriminate in terms of domain age given that the attack was discovered on 11 June 2025.



- All of them were administered by Namecheap and registered in Iceland.

Next, we queried the seven domains identified as IoCs on DNS Chronicle API and found that all of them had historical domain-to-IP resolutions. All in all, they resolved to 45 IP addresses over time with the oldest resolution for awaitingfor[.]site to 162[.]255[.]119[.]131 recorded on 3 August 2023. Take a look at more details below.

DOMAIN IoC	TOTAL NUMBER OF DOMAIN-TO-IP RESOLUTIONS	FIRST DOMAIN-TO-IP RESOLUTION DATE
firstfromsep[.]online	15	4 September 2024
readysafe[.]xyz	7	11 January 2025
safeupload[.]online	7	12 January 2025

We then sought to find out if any of the seven domains identified as IoCs have been dubbed “likely to turn malicious” as soon as they were created by querying them on First Watch. We discovered that three of them were found as such before they were reported as malicious to Huntress on 11 June 2025. Here are the details.

DOMAIN IoC	DATED ADDED TO FIRST WATCH	NUMBER OF DAYS DUBBED “LIKELY TO TURN MALICIOUS” PRIOR TO 11 JUNE 2025
firstfromsep[.]online	3 September 2024	281
safeupload[.]online	11 January 2025	151
us05web-zoom[.]biz	31 March 2025	72

It is also worth noting these characteristics about the seven domains identified as IoCs:

- Three of them had the text string **safe** and sported either the gTLD .xyz or .online.
- One of them had the string **zoom** (the actual application target) and sported the gTLD .biz.

The Hunt for Connected Artifacts

After learning more about the IoCs, we moved on toward finding more connected artifacts. We began by querying the seven domains identified as IoCs on WHOIS History API. We learned that only one of them had email addresses in its historical WHOIS records. Specifically, the domain had two email addresses although only one was a public email address.

A Reverse WHOIS API query for the public email address from current WHOIS records did not turn up results. As such, we queried historical WHOIS records and obtained 16 email-connected domains after filtering out those already identified as IoCs.

Next, we queried the seven domains identified as IoCs on DNS Lookup API and discovered that six of them had current domain-to-IP resolutions. In particular, they resolved to six unique IP addresses.

A Threat Intelligence API query for the six IP addresses showed that they were all malicious. Take a look at three examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT
104[.]168[.]136[.]231	Malware distribution
142[.]11[.]196[.]220	Malware distribution
192[.]119[.]116[.]231	Malware distribution

We then queried the six IP addresses on Bulk IP Geolocation Lookup and found that they were all geolocated in the U.S. under the administration of Hostwinds.

After that, we queried the six IP addresses on Reverse IP API and discovered that all of them could be dedicated hosts. Altogether, they hosted 13 IP-connected domains after those already identified as IoCs and the email-connected domains were filtered out.

A Threat Intelligence API query for the 13 IP-connected domains revealed that one—signsafe[.]site—has already been weaponized to distribute malware. Interestingly, it contained the text string **safe** akin to three of the domains identified as IoCs.

As our final step, we looked for domains that shared text strings with the seven identified as IoCs using Domains & Subdomains Discovery. We specifically used these parameters and strings:

- Starts with **awaitingfor.**
- Starts with **firstfromsep.**
- Starts with **productnews.**
- Starts with **readysafe.**
- Starts with **safefor.**
- Starts with **safeupload.**
- Starts with **us05web-zoom.**
- Contains **safe.** and ends with **xyz**
- Contains **safe*.** and ends with **xyz**
- Contains **safe*.** and ends with **online**
- Contains **zoom.** and ends with **biz**

We uncovered 21,617 string-connected domains after those already identified as IoCs and the email- and IP-connected domains were filtered out. Note that this dataset comprises domains with the characteristics shown in the table below.

CHARACTERISTIC	PARAMETER	NUMBER OF DOMAINS
Exact strings found in domains identified as IoCs; different TLD extension only	**Starts with**	124
Shared two general string characteristics (i.e., contained **safe** and ended with **xyz** or **online**; contained **zoom** and ended with **biz**)	**Contains** and **ends with**	21,493

A Threat Intelligence API query for the 21,617 string-connected domains showed that 95 have already figured in various attacks. Take a look at five examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT
360safety[.]xyz	Malware distribution
acersafe[.]online	Phishing
binaxsafe[.]online	Phishing
capitalsafetyplatform[.]online	Phishing
dex-safebridge[.]xyz	Attack

—

Our in-depth analysis of the most recent BlueNoroff attack led to the discovery of 21,652 connected artifacts comprising 16 email-connected domains, six IP addresses, 13 IP-connected domains, and 21,617 string-connected domains. To date, 102 of these web properties have already been dubbed “malicious.”

If you wish to 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

- areasaludable[.]info
- darkca[.]com
- henry-hernandez[.]com
- luisalbertobarrios[.]com
- mmorpggames[.]online
- niyafashionstore[.]com
- siemprevital[.]com
- theafrincanmangoextract[.]com
- wikimediamarketing[.]com
- yobajedepeso[.]com

Sample IP Addresses

- 104[.]168[.]136[.]231
- 142[.]11[.]196[.]220
- 192[.]119[.]116[.]231

Sample IP-Connected Domains

- 866dcae7-a392-4525-87c2-752ed84a67b9[.]random[.]larfdsabh[.]pro
- cpanel[.]larfdsabh[.]pro
- ftp[.]larfdsabh[.]pro
- larfdsabh[.]pro
- mail[.]larfdsabh[.]pro
- pop[.]larfdsabh[.]pro
- signsafe[.]site
- webdisk[.]larfdsabh[.]pro

Sample String-Connected Domains

- 0451safe[.]xyz
- 0591safe[.]xyz
- 0631safe[.]xyz
- 0nesafe[.]xyz
- 0xsafe[.]xyz
- a-safer[.]xyz
- a-saferanti-virus[.]xyz
- a1safety[.]online
- a1safetychimney[.]online
- a1safetynpackaging[.]online
- b-safe-at[.]online
- b-safe-gloves[.]online
- b-safe[.]online
- b-safe[.]xyz
- b-safeinfo[.]online
- c-hikari-safety-speedy-com[.]xyz
- c-safe[.]online
- c-safe[.]xyz
- c-safelog[.]xyz
- c2cpublicsafety[.]online
- d-safe[.]online
- d33safe[.]xyz
- dadesafe[.]online
- dadofsafemoon[.]online
- daggersafeknife[.]xyz
- e-foodsafety[.]online
- e-safe[.]xyz
- e-safepay[.]online
- e-safetech[.]xyz
- e-safety[.]online

- f-safer[.]online
- fabsafehub[.]xyz
- face-safepace[.]online
- facebooksafe[.]online
- facesafe[.]xyz
- g-nosissafe[.]xyz
- g-safelog[.]xyz
- g-up-safetywear[.]online
- gaaqn-safe[.]xyz
- gaaqnsafe[.]xyz
- ha-safe-keeping[.]xyz
- habit-safety[.]xyz
- haccpfoodsafety[.]online
- haccpsafetytraining[.]online
- hackersafe[.]xyz
- i-am-safe[.]online
- i-biosafe[.]online
- i-safe[.]online
- i-safeness[.]online
- i-zoom[.]biz
- j34securesafety[.]xyz
- jabberzoom[.]biz
- jackdupsafety[.]online
- jaesafenby[.]xyz
- jahkimsfireandsafety[.]online
- k7transjakartasafetytravel[.]xyz
- kaaraasafeed[.]xyz
- kabosafe[.]xyz
- kahzoom[.]biz
- kaiasafelite[.]xyz
- la-safe-keeping[.]xyz
- la1safety[.]online
- laborious-safe[.]xyz
- laborsafe[.]xyz
- laborsafety[.]online
- m-bank-safe[.]online
- m-safe[.]xyz
- m-safepayer[.]online
- m26-personal-safety-device[.]xyz
- m9safe[.]online
- n-safe[.]online
- nacxg-safe[.]xyz
- naiaeksafety[.]xyz
- nailcleansafe[.]xyz
- nairobisafetywear[.]xyz
- oaksafetytools[.]xyz
- oarsafe[.]xyz
- oasafety[.]online
- oasiscomsafetymistakes[.]xyz
- oasissafe[.]xyz
- p1-item-24safepay[.]xyz
- p1-item-safepay24[.]xyz
- p2p-safe[.]online
- p2psafespace[.]online
- p3safetygear[.]online
- q-safe[.]online
- qafbh-safe[.]xyz
- qayasafetysolutions[.]online
- qazksafe[.]xyz
- qcsafety[.]xyz
- r3projectsafe[.]xyz
- ra-zoom[.]biz
- rabbosafety[.]xyz
- rabo-safe[.]xyz
- rabosafe[.]online
- s3safetyservices[.]xyz
- sa-safe-keeping[.]xyz
- saare-safes[.]xyz
- sabinassafetyitems[.]xyz
- sadsafeo[.]xyz
- t-safe[.]xyz
- ta-safe-keeping[.]xyz
- taalresafe[.]xyz
- tacho4safe[.]online
- tacomasafe[.]online
- u-safe[.]online
- u-safe[.]xyz
- u-safety[.]online
- ua-olx-safe[.]xyz
- ua-safe[.]online

- v2safemoonconsolidation[.]online
- vac-safe[.]online
- vadnymsafe[.]xyz
- vahansafety[.]online
- vainhlsafe[.]xyz
- w3safe[.]xyz
- wa-safe-keeping[.]xyz
- wab-site-safe[.]online
- wabashsafety[.]online
- wabdomainsafe[.]online
- x2000safety[.]online
- xajatuposafe[.]xyz
- xbcvxnsafe[.]xyz
- xbvcnvsafe[.]xyz
- xdarm-safe[.]xyz
- ya-safe-keeping[.]xyz
- yandex-resafe[.]online
- yandex-safe-delivery[.]online
- yandex-safe[.]online
- yandex-safedeal[.]online
- z3safety[.]online
- zachisafeguard[.]xyz
- zaful-safety[.]xyz
- zainitsafe[.]xyz
- zanzoom[.]biz