

# Is Your Intranet Vulnerable to Attacks?

## Investigating Intranet Impersonation in the DNS

### Table of Contents

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

### Executive Report

On 10 February 2023, Reddit [announced](#) it suffered a security incident where a phishing campaign led an employee to a website that imitated the network's intranet gateway. The victim entered his credentials and a two-factor authentication (2FA) token, allowing the attacker to access codes, internal documents, and business systems. The attack was highly targeted. The threat actors knew what Reddit's intranet address was, how it behaves, and what it looks like.

In connection with this incident, WhoisXML API researchers looked into intranet-related domains that could be used as attack vectors. The report focused on web properties added between 1 January and 20 March 2023 to uncover possible phishing vehicles similar to those used in the Reddit security incident. Our key findings include:

- 800+ cybersquatting domains targeting 20 of the most popular intranet software
- 220+ domains containing the string ***intranet***
- Less than 1% of the cybersquatting domains that were publicly attributable to the imitated software providers
- 3.4% of the intranet-related domains that were flagged as malicious, some of which still hosted phishing sites as of 21 March 2023
- 60+ intranet domains that hosted publicly accessible login pages

### Cybersquatting Domains Targeting Popular Intranet Software

Using [Domains & Subdomains Discovery](#), we found 814 recently added domains containing the brand names of 20 popular intranet software. We also retrieved 277 domains containing the word ***intranet*** registered within the same period, bringing the total number of domains to 1,091.

## Domain Attribution

We retrieved the WHOIS records of the intranet brands' official domain and the possible cybersquatting properties using [Bulk WHOIS Lookup](#). Our analysis revealed that only five of the 814 cybersquatting domains shared the exact public registrant details as the software providers' official domains.

We also did [bulk IP geolocation lookups](#) on the official domains and cybersquatting resources to check their IPs. Only two of the cybersquatting domains resolved to the legitimate domains' IP addresses.

Overall, less than 1% of the cybersquatting properties could be publicly attributed to the imitated software providers, leaving most of the domains under unknown entities' control.

## WHOIS Infrastructures of the Intranet-Related Domains

With very few of the cybersquatting domains attributable to legitimate software providers, we sought to analyze their registration details. While most of them had redacted WHOIS records, 37 of the domains still had public registrant details. These led us to 32 registrant email addresses that were mostly Gmail addresses.

Running these email addresses on [Reverse WHOIS Search](#), we found they were associated with 10,611 domains. Dozens of these domains were cybersquatting properties targeting some of the intranet software featured in this study.

Furthermore, only one Gmail address accounted for 10,000 connected domains, suggesting they could be part of a domain investor's portfolio. Here's a screenshot of the connection established via Maltego.

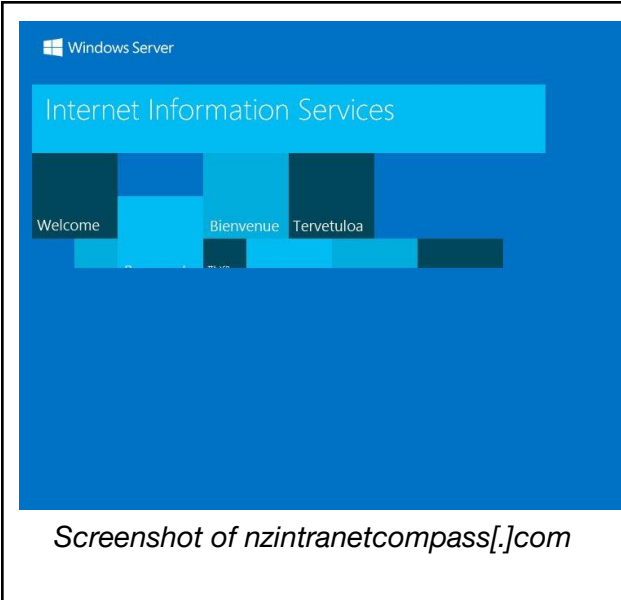
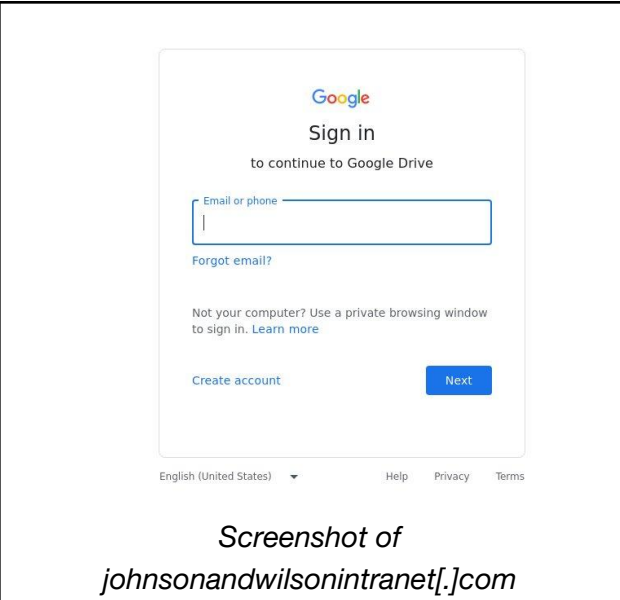


## Malicious and Suspicious Usage of the Cybersquatting Domains

While some domains could be legitimate intranet gateways of organizations, about 3.4% of the cybersquatting resources already figured in malicious campaigns as of 21 March 2023. Some continued to host phishing sites, like the domains below.

 <p><b>Warning: Suspected Phishing Site Ahead!</b> This link has been flagged as phishing. We suggest you avoid it.</p> <p><b>What is phishing?</b> This link has been flagged as phishing. Phishing is an attempt to acquire personal information such as passwords and credit card details by pretending to be a trustworthy source.</p> <p><b>What can I do?</b> <b>If you're a visitor of this website</b> The website owner has been notified and is in the process of resolving the issue. For now, it is recommended that you do not continue to the link that has been flagged. <b>If you're the owner of this website</b> Please log in to cloudflare.com to review your flagged website. If you have question about why this was flagged as phishing</p> <p><a href="#">Dismiss this warning and enter site</a></p> <p><i>Screenshot of <a href="#">www-basecamp-us[.]com</a></i></p>	 <p><b>Warning: Suspected Phishing Site Ahead!</b> This link has been flagged as phishing. We suggest you avoid it.</p> <p><b>What is phishing?</b> This link has been flagged as phishing. Phishing is an attempt to acquire personal information such as passwords and credit card details by pretending to be a trustworthy source.</p> <p><b>What can I do?</b> <b>If you're a visitor of this website</b> The website owner has been notified and is in the process of resolving the issue. For now, it is recommended that you do not continue to the link that has been flagged. <b>If you're the owner of this website</b> Please log in to cloudflare.com to review your flagged website. If you have question about why this was flagged as phishing</p> <p><a href="#">Dismiss this warning and enter site</a></p> <p><i>Screenshot of <a href="#">www-basecamp-us[.]com</a></i></p>
--	---

Some unflagged domains also hosted questionable content like [nzintranetcompass\[.\]com](#), which hosted a Windows Server page, and [johnsonandwilsonintranet\[.\]com](#), which redirected to a Google Drive. Their website screenshots appear below.

 <p><b>Windows Server</b> Internet Information Services Welcome Bienvenue Tervetuloa</p> <p><i>Screenshot of <a href="#">nzintranetcompass[.]com</a></i></p>	 <p><b>Google</b> Sign in to continue to Google Drive</p> <p>Email or phone [ ]</p> <p><a href="#">Forgot email?</a></p> <p>Not your computer? Use a private browsing window to sign in. <a href="#">Learn more</a></p> <p><a href="#">Create account</a> <a href="#">Next</a></p> <p>English (United States) Help Privacy Terms</p> <p><i>Screenshot of <a href="#">johnsonandwilsonintranet[.]com</a></i></p>
---	---

## Possible Vulnerabilities in Intranet Gateways

We mentioned that some of the intranet-related domains in this study could be legitimate intranet gateways. For example, our screenshot analysis showed that some of the domains resolved to 401, forbidden, or unauthorized access warning pages.

Several cybersquatting domains, however, hosted login pages. If these are legitimate, they could give threat actors a baseline for mimicking a target organization's intranet gateway. They could also be vulnerable to brute-force attacks. On the other hand, if these domains are not legitimate intranet gateways, it could take only one employee of the target organization to fall for the trap.

—

As the Reddit security incident illustrated, intranets can serve as an attack vector simply by mimicking a target's official gateway. With threat vectors piling up and organizations' attack surfaces getting wider than ever, proactive threat monitoring and vulnerability scanning can help.

***If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to [contact us](#).***

## Appendix: Sample Artifacts and IoCs

### Sample Intranet-Cybersquatting Domains

- aihcltech[.]com
- aunily[.]cf
- aunily[.]ga
- aunily[.]ml
- axero[.]me
- axero[.]work
- axeroc[.]net
- axeroc[.]org
- basecamp[.]ga
- basecamp[.]rest
- basecamp[.]sbs
- basecampbv[.]co
- basecampost[.]de
- basecamptw[.]co
- basecampv[.]ca
- bempulsa[.]shop
- circlinked[.]com
- clinked[.]ai
- clinked[.]com[.]au
- clinked-in[.]org
- cplworkvivo[.]com
- diejostle[.]com
- doclinked[.]nl
- elaxero[.]cn
- empuls[.]at
- empuls[.]cn
- empuls[.]com[.]cn
- empulsar[.]de
- empuls-ems[.]de
- flagstaffbasecamppt[.]com

- gaxero[.]net
- gclinked[.]com[.]au
- gempulsa[.]xyz
- happeon[.]fr
- happeon[.]shop
- happeon[.]store
- haystack[.]fi
- haystacka7a[.]shop
- haystackex[.]com
- haystacks[.]capital
- hcltech[.]co[.]kr
- hcltech[.]com[.]pl
- hcltechsw[.]cz
- hcltechsw[.]de
- hcltechsw[.]eu
- hirayammer[.]com
- iclinked[.]com[.]cn
- igloosoftware[.]ws
- it-hcltech[.]com
- jesterjostler[.]com
- jostle[.]app
- jostled[.]jio
- jostle-presidency[.]com
- jostlesuccess[.]me
- mangoappsfun[.]com
- maryammerlin[.]com
- maxero[.]pl
- metaworkplace[.]de
- metaworkplace[.]ml
- metaworkplace[.]mp
- metaworkplace[.]pa
- metaworkplace[.]ph
- metaworkplace[.]pk
- metaworkplace[.]tk
- networkvivor[.]com
- networkvivor[.]xyz
- onthesamepage[.]club
- ryunilyan[.]ml
- samepage[.]cafe
- samepage[.]church
- samepage[.]fyi
- samepageacademy[.]com
- samepagemeeting[.]net
- samepagesports[.]org
- sharepointaa[.]com
- sharepointlab[.]jir
- sharepointsf[.]ga
- sharepointxs[.]nl
- sharepointxz[.]ml
- staffbase[.]cn
- staffbase[.]com[.]cn
- staffbase[.]me
- staffbase[.]online
- staffbase[.]studio
- sunily[.]co[.]in
- syammerijaya[.]com
- thoughtfarmerdev[.]vg
- unilya[.]com
- usehaystack[.]fyi
- usehaystack[.]us
- usehaystack[.]xyz
- workvivo[.]de
- workvivome[.]com
- wssharepoint[.]de
- wwwmangoapps[.]com
- wwwstaffbase[.]com
- wwwunily[.]com
- yammer-blog[.]com
- yammergram[.]jio
- yammerindia[.]vg
- yammers[.]lol
- ysharepoint[.]net
- zoho[.]hair
- zohobraincenter[.]com
- zohogermany[.]de
- zohohoist[.]vg
- zohomailbox[.]eu
- zohoz[.]com[.]pe
- zohoz[.]de

## Sample Domains Containing the String *intranet*

- aicintranet[.]ht
- aocintranet[.]org
- ascintranet[.]ws
- azintranet[.]vg
- bcintranet[.]com
- bintranet[.]de
- btintranet[.]ga
- cintranet[.]net
- dd-intranet[.]de
- ecintranet[.]ph
- escintranet[.]ws
- faintranet[.]co
- hdintranet[.]org
- hhdintranet[.]vg
- ids-intranet[.]de
- intranet[.]arab
- intranet[.]cfd
- intranet[.]mba
- intranet[.]nyc
- intranet3[.]fr
- intranet365[.]vg
- intranetapp[.]it
- intranet-bs[.]ch
- intranetey[.]com
- intranetgun[.]vg
- intranet-gw[.]ws
- intranet-ivt[.]de
- intranet-old[.]ws
- intranetpsw[.]vg
- intranetrd[.]vg
- intranets[.]shop
- intranetsa[.]net
- intranetsma[.]com
- jul-intranet[.]de
- lbg-intranet[.]nl
- mtgintranet[.]vg
- nvcintranet[.]xn--node
- oelcintranet[.]ca
- oi-intranet[.]fr
- pintranet[.]pl
- qmcintranet[.]ws
- skintranet[.]be
- smuintranet[.]vg
- spcintranet[.]ws
- spintranet[.]ws
- tcaintranet[.]org
- tccintranet[.]gq
- wb-intranet[.]de
- wbuintranet[.]vg
- ww-intranet[.]nl

## Sample Malicious Cybersquatting Domains as of 21 March 2023

- 1sharepointprofile[.]com
- apagcosyst-sharepoint[.]com
- astridenterprise-sharepoint[.]net
- basecampadventurepakistan[.]com
- basecampuscom[.]top
- basecampus-com[.]top
- findauthorizationsharepoint[.]com
- info-sharepoint[.]top
- info-sharepoints[.]top
- intranetey[.]com
- irisintranet[.]dev
- mysharepoint-onedrive[.]com
- sharepointnote[.]cfd
- sharepoint-payment-invoice[.]ml
- websharepoint[.]sbs
- wv-basecamp-us[.]com
- wv-basecamp-us[.]top
- www-basecamp-us[.]com
- zohoc[.]net
- zoho-hero[.]com

