WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

APT29 Goes from Targeted Attacks to Phishing via NOBELIUM: A DNS Deep Dive

Table of Contents

Executive Report

APT29, believed to be an espionage group from Russia, became known for launching targeted attacks against organizations in Ukraine. But over the course of investigating the threat group, Mandiant discovered that it may have a hand in cybercriminal operations, specifically phishing, as well.

As far as security researchers could tell, APT29's cybercriminal arm went by the moniker "NOBELIUM," which has been trailing its sights on Microsoft's cloud-based products. An in-depth investigation on the threat identified 48 indicators of compromise (IoCs)—41 domains and seven IP addresses to date.

The WhoisXML API research team expanded this list of IoCs in search of more artifacts potentially connected to APT29's phishing operation arm NOBELIUM and uncovered:

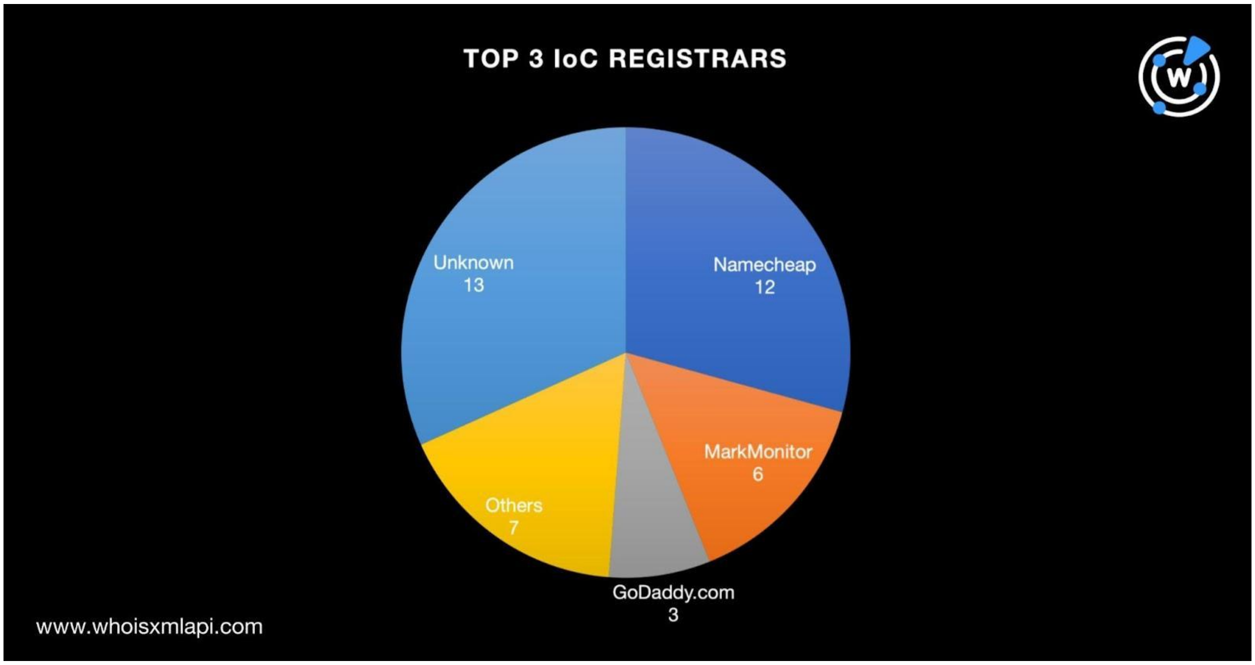
- 13 unreported IP addresses to which some of the domains identified as IoCs resolved, 10 of which turned out to be malicious based on malware checks
- 422 unreported domains that shared the IP addresses of some of the IoCs and additional resolutions as hosts
- 577 domains and subdomains containing strings related to five of Microsoft's cloud services, 10 of which turned out to be malware hosts based on bulk malware checks

Facts about the IoCs

We started our DNS deep dive into APT29's phishing operation by looking for more information on the NOBELIUM IoCs.

A bulk WHOIS lookup for the 41 domains identified as IoCs led to these discoveries:

- The top 3 registrars were Namecheap (12 domains), MarkMonitor (six domains), and GoDaddy.com (three domains). Thirteen of the IoCs didn't have publicly viewable registrars. The remaining seven domains were spread across six other registrars.



- The IoCs were created between 1999 and 2023, which could mean the threat actors didn't discriminate when it came to domain age.
- A majority of the IoCs were registered in the U.S. (15 domains) and Iceland (11 domains).

A bulk IP geolocation lookup, meanwhile, for the seven IP addresses identified as IoCs led to these findings:

- The IP addresses were geolocated in five countries led by the U.K. (three IoCs). The remaining four originated from Australia, France, Romania, and Ukraine.
- None of the IP addresses shared an Internet service provider (ISP).

IoC List Expansion Findings

In a bid to find other potential NOBELIUM artifacts, we ran historical WHOIS searches on the 41 domains identified as IoCs and found that the registrants of 22 of them registered 22 other domains that aren't part of the current IoC list.

We then subjected them to DNS lookups that uncovered 13 unreported IP addresses to which some of the domains identified as IoCs resolved. Three of them hosted several domains as shown in the table below.

199[.]36[.]158[.]100	34[.]120[.]160[.]131	3[.]64[.]163[.]50
● cdnappservice[.]web[.]app ● logicworkservice[.]web[.]app ● humanitarian-forum[.]web[.]app ● security-updater[.]web[.]app ● supportcdn[.]web[.]app	● eventbrite-com-default-rtdb[.]firebaseio[.]com ● cdnappservice[.]firebaseio[.]com ● humanitarian-forum-default-rtdb[.]firebaseio[.]com ● security-updater-default-rtdb[.]firebaseio[.]com ● supportcdn-default-rtdb[.]firebaseio[.]com	● aimsecurity[.]net ● stsnews[.]com

Ten of the 13 IP resolutions also turned out to be malicious based on malware checks. In fact, nine of them were reported to AbuseIPDB several times as shown below.

IP RESOLUTION	NUMBER OF TIMES REPORTED ON ABUSEIPDB
199[.]36[.]158[.]100	204
3[.]64[.]163[.]50	72
64[.]91[.]249[.]20	3
35[.]205[.]61[.]67	20
162[.]55[.]100[.]32	68
208[.]91[.]197[.]46	5
13[.]248[.]169[.]48	19
23[.]227[.]38[.]32	52
76[.]223[.]54[.]146	13

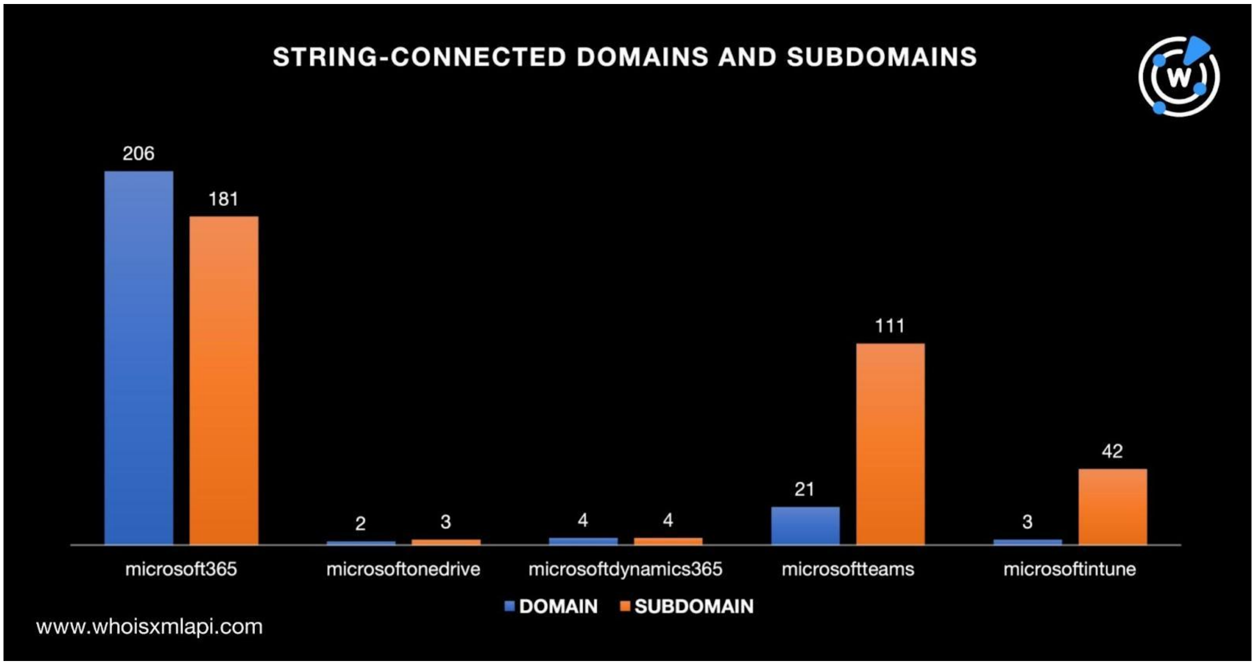
Reverse IP lookups for the seven IoCs and additional IP addresses showed that:

- None of the IP addresses identified as IoCs were currently in use.
- Four of the unreported IP resolutions were possibly dedicated, playing host to 422 domains in total.

NOBELIUM also reportedly targeted Microsoft's cloud-based products. We sought to find if potential threat vectors, particularly domains and subdomains created this year, already exist in the DNS. We used these strings as Domains & Subdomains Discovery search terms based on a list of five of the company's cloud services.

MICROSOFT CLOUD SERVICE	SEARCH TERM
Microsoft 365	**microsoft365**
Microsoft OneDrive	**microsoftonedrive**
Microsoft Dynamics 365	**microsoftdynamics365**
Microsoft Teams	**microsoftteams**
Microsoft Intune	**microsoftintune**

We found 236 domains and 341 subdomains containing the five strings listed above. Take a look at their volume breakdown below.



A bulk WHOIS lookup for the 236 string-connected domains showed that only three were Microsoft-owned. They had the same registrant organization as the company's official domain microsoft[.]com. A bulk malware check, meanwhile, revealed that five of them have already been categorized as malicious and, as expected, none of them belong to Microsoft despite bearing its name. And one of the malicious domains was currently up for sale.

A bulk WHOIS lookup, meanwhile, for the 341 string-connected subdomains showed that only three belonged to Microsoft based on their registrant organization. A bulk malware check showed that five of them were already classified as malicious and none were owned by the company. Four of them remained accessible—two led to index pages while the other two led to error pages.

—

Our expansion analysis of the APT 29-NOBELIUM IoCs led to the discovery of 1,034 potentially connected artifacts that could figure in future attacks. At least 20 of them may have or are already being used as threat entry points to date. Preventing access to them would be a good idea.

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 and IoCs

APT29-NOBELIUM IoCs

- cdnappservice[.]web[.]app
- logicworkservice[.]web[.]app
- humanitarian-forum[.]web[.]app
- security-updater[.]web[.]app
- eventbrite-com-default-rtdb[.]firebaseio[.]com
- supportcdn[.]web[.]app
- r20[.]rs6[.]net
- 74d6b7b2[.]app[.]giftbox4u[.]com
- aimsecurity[.]net
- cdn[.]theyardservice[.]com
- cdnappservice[.]firebaseio[.]com
- cityloss[.]com
- content[.]pcmsar[.]net
- cross-checking[.]com
- dailydews[.]com

- dataplane[.]theyardservice[.]com
- doggroomingnews[.]com
- email[.]theyardservice[.]com
- emergencystreet[.]com
- enpport[.]com
- financialmarket[.]org
- giftbox4u[.]com
- hanproud[.]com
- holescontracting[.]com
- humanitarian-forum-default-rtdb[.]firebaseio[.]com
- newsplacec[.]com
- newstepsco[.]com
- pcmsar[.]net
- security-updater-default-rtdb[.]firebaseio[.]com
- smtp2[.]theyardservice[.]com
- static[.]theyardservice[.]com
- stockmarketon[.]com
- stsnews[.]com
- supportcdn-default-rtdb[.]firebaseio[.]com
- tacomanewspaper[.]com
- techiefly[.]com
- theadminforum[.]com
- theyardservice[.]com
- trendignews[.]com
- usaid[.]theyardservice[.]com
- worldhomeoutlet[.]com
- 139[.]99[.]167[.]177
- 185[.]158[.]250[.]239
- 195[.]206[.]181[.]169
- 37[.]120[.]247[.]135
- 45[.]135[.]167[.]27
- 51[.]254[.]241[.]158
- 51[.]38[.]85[.]225

Sample IP Resolutions

- 199[.]36[.]158[.]100
- 34[.]120[.]160[.]131
- 208[.]75[.]122[.]11
- 3[.]64[.]163[.]50
- 64[.]91[.]249[.]20
- 35[.]205[.]61[.]67
- 162[.]55[.]100[.]32

Sample Malicious IP Resolutions

- 199[.]36[.]158[.]100
- 3[.]64[.]163[.]50
- 64[.]91[.]249[.]20
- 35[.]205[.]61[.]67
- 162[.]55[.]100[.]32
- 208[.]91[.]197[.]46

Sample IP-Connected Domains

- aceconsulting[.]gm
- activedgetechnologies[.]com
- ad-al-prod-and-pre-prod[.]firebaseio[.]com
- admob-app-id-5702209339[.]firebaseio[.]com
- agencyjobs[.]com
- alamanecerboxing[.]org
- alertemsllc[.]org
- alihunterclient-default-rtdb[.]firebaseio[.]com
- aljazeeragold[.]com
- amshalem[.]com

- api-project-652995075284[.]firebaseio[.]com
- ar-viewer-f6c68[.]firebaseio[.]com
- arcdevelopmentglobal[.]com
- astressedoutmom[.]com
- ateeqkhan[.]com
- autentia-movil[.]firebaseio[.]com
- autospect[.]com[.]sl
- awesome-table[.]firebaseio[.]com
- balthazarllc[.]com
- banco-ripley-sp-2-0-dev[.]firebaseio[.]com
- banco-ripley-sp-2-0[.]firebaseio[.]com
- barbdietz[.]com
- baseec-message[.]firebaseio[.]com
- baseec-remote-config[.]firebaseio[.]com
- basictwowayradio[.]com
- battle-vs-viewers[.]firebaseio[.]com
- bci-cl[.]firebaseio[.]com
- beardydad[.]com
- bellajosiedesigns[.]com
- bintimanipvd[.]com
- blazing-inferno-8771[.]firebaseio[.]com
- bloomingtonbikes[.]com
- bluespringscpasolutions[.]com
- bluespringsmarketingsolutions[.]com
- bluespringssolutions[.]com
- buddiesrestaurant[.]com
- buildaclass[.]org
- cakechemistry[.]com[.]au
- caleacare[.]com[.]sl
- caleacare[.]com
- caleacare[.]sl
- californiangrills[.]com
- cam4-10[.]firebaseio[.]com
- cam4-9[.]firebaseio[.]com
- cam4[.]firebaseio[.]com
- camaralatina[.]com
- camerliga-bb[.]com
- carear-v0[.]firebaseio[.]com
- carlsongraciesouthlakeland[.]com
- carpetbuying[.]com

Sample String-Connected Domains

- microsoft365[.]ir
- microsoft365[.]ar
- microsoft365[.]ai
- microsoft365[.]lv
- microsoft365[.]nz
- microsoft365[.]do
- microsoft365[.]ms
- microsoft365[.]zip
- microsoft365[.]lat
- xn--microsof365-pjc[.]com
- microsoft365[.]cyou
- microsoft365[.]wiki
- microsoft365[.]name
- microsoft365i[.]com
- onmicrosoft365[.]ch
- imicrosoft365[.]com
- microsoft365lab[.]cz
- aimicrosoft365[.]com
- microsoft365ai[.]com
- microsoft365vip[.]cn
- microsoft365[.]my[.]id
- microsoft365[.]org[.]nz
- microsoft365ppe[.]com
- microsoft365demo[.]ga
- microsoft365plus[.]nl
- microsoft365[.]web[.]tr
- csp-microsoft365[.]fr
- microsoft365[.]net[.]au

- microsoft365mail[.]co
- microsoft365-csp[.]fr
- microsoft365edu[.]top
- microsoft365[.]agency
- microsoft365fax[.]com
- microsoft365chat[.]com
- microsoft365labo[.]com
- microsoft365-int[.]com
- microsoft365[.]courses
- microsoft365admin[.]hu
- csp-microsoft365[.]com
- microsoft365-csp[.]com
- microsoft365test1[.]xyz
- microsoft365office[.]nl
- microsoft365cloud[.]net
- microsoft365expert[.]nl
- microsoft365awards[.]xn--kprw13d
- azure-microsoft365[.]fr
- microsoft365office[.]it
- microsoft365ltd[.]co[.]de
- microsoft365logon[.]com
- auth-microsoft365[.]com

Sample Malicious String-Connected Domains

- teams-microsoft365[.]com
- update-microsoft365[.]com
- product-microsoft365[.]com

Sample String-Connected Subdomains

- microsoft365[.]senetic[.]pe
- microsoft365[.]7host[.]vn
- microsoft365[.]lancaster[.]ac[.]uk
- microsoft365[.]atmoss[.]fit
- microsoft365[.]starlit[.]kr
- microsoft365[.]sogesi[.]it
- microsoft365[.]ragoids[.]com
- microsoft365[.]heysummit[.]com
- microsoft365[.]lancs[.]ac[.]uk
- microsoft365[.]avans[.]nl
- microsoft365[.]mesnicabasic[.]ba
- microsoft365[.]springintveldbellingen[.]be
- microsoft365[.]mcri[.]edu[.]au
- microsoft365[.]photonag[.]com[.]de
- microsoft365[.]jawnet[.]com[.]pl
- microsoft365[.]claracloud[.]com[.]br
- microsoft365[.]schools[.]ac[.]cy
- microsoft365[.]wieza[.]pl
- microsoft365[.]mso[.]vn
- microsoft365[.]northeastern[.]edu
- microsoft365[.]solucionesmks[.]com
- microsoft365[.]aquaorange[.]co[.]th
- microsoft365[.]greenstaretpplant[.]com
- microsoft365[.]eafc-sudlux[.]be
- microsoft365[.]zentarle-autoglas[.]de
- microsoft365[.]tier16[.]com
- microsoft365[.]formcc[.]com
- microsoft365[.]blog[.]info
- microsoft365[.]jachwang[.]co[.]uk
- microsoft365[.]ndscognitivelabs[.]com
- microsoft365[.]abarco[.]com[.]mx
- microsoft365[.]landpage[.]co[.]il
- microsoft365[.]microsoftonline[.]cn
- microsoft365[.]gofatech[.]edu[.]vn
- microsoft365[.]blog[.]us
- microsoft3654[.]zendesk[.]com
- microsoft365[.]nl[.]admin-mcas[.]ms
- microsoft365wed[.]repl[.]co
- microsoft365ltd[.]co[.]xyz
- microsoft365ltd[.]co[.]com[.]au

- www[.]microsoft365[.]landpage[.]co[.]il
- www[.]microsoft365[.]secure-authentication[.]cloud
- www[.]microsoft365[.]jawnet[.]com[.]pl
- www[.]microsoft365[.]tier16[.]com
- microsoft365[.]com[.]admin-mcas-df[.]ms
- www[.]microsoft365[.]abarco[.]com[.]mx
- www[.]microsoft365[.]setup2[.]com
- www[.]microsoft365[.]gwsdeployment[.]com
- microsoft365[.]com[.]mcas-df-gov[.]us
- www[.]microsoft365[.]mesnicabasic[.]ba

Sample Malicious String-Connected Subdomains

- microsoft365[.]ragoids[.]com
- microsoft365[.]mesnicabasic[.]ba
- www[.]microsoft365[.]mesnicabasic[.]ba