Finding WyrmSpy and DragonEgg Ties to APT41 in the DNS

Table of Contents

Executive Report

APT41, also known as “Winnti,” “BARIUM,” or “Double Dragon,” is an APT group said to originate from China. Having been active since 2012, APT41 rose to infamy by successfully launching targeted cyber espionage attacks on government agencies and private companies worldwide.

Lookout most recently discovered that the APT group employed at least two mobile spyware—WyrmSpy and DragonEgg—to siphon secrets off their chosen targets. The researchers believe the two spyware were linked to APT41 despite the fact that five cyberspies believed to be part of the threat group have already been caught. WhoisXML API thus sought to find DNS ties between them.

Using the five WyrmSpy IoCs Lookout identified as jump-off points, we uncovered eight domains containing the strings **win10 + microsoft** and **andropwn**, akin to two of the domains identified as IoCs.

Our expansion analysis of the list of seven DragonEgg IoCs, meanwhile, led to the discovery of:

- One additional IP address to which the domain identified as an IoC—alxc[.]tbtianyan[.]com—resolved, which turned out to be malicious based on a malware check
- 94 additional domains that shared some of the IoCs’ dedicated hosts
- 3,085 additional domains that contained the strings **alxc.**, **smiss.**, **imwork.**, **huaxin-**, and **bantian.**, akin to the IoCs, 14 of which were categorized as malicious based on a bulk malware check

The Ties That Bind WyrmSpy and DragonEgg to APT41

Taking a Closer Look at APT41

In an attempt to determine if WyrmSpy and DragonEgg were indeed related to APT41, we first sought to find DNS traces of the APT group's published IoCs. While these were publicized in 2022, we only need to determine their origins for comparison with the more recently publicized mobile spyware IoCs.

A bulk WHOIS lookup for the three domains identified as APT41 IoCs showed that:

- The threat actors employed two registrars—Netowl, Inc. and GoDaddy.com LLC—for two of the IoCs—ymvh8w5[.]xyz and vietsovspeedtest[.]com, respectively.
- They also indicated Japan and the U.S. as the registrant countries of the same two IoCs mentioned above.
- The remaining IoC—affice366[.]com—didn't have a retrievable current WHOIS record, though past records collected through WHOIS History indicated GoDaddy.com LLC as its registrar and Singapore as its registrant country.

A bulk IP geolocation lookup, meanwhile, for the two IP addresses identified as APT41 IoCs revealed that:

- The IP address 47[.]108[.]173[.]88 originated from China and was administered by Alibaba Cloud.
- The IP address 139[.]180[.]138[.]226, on the other hand, indicated Singapore as its geolocation country and Choopa as its ISP.

Examining Ties between APT41 and WyrmSpy

To identify commonalities between APT41 and WyrmSpy, we first subjected the three domains identified as WyrmSpy IoCs—win10micros0ft[.]com, andropwn[.]xyz, and umisen[.]com—to a bulk WHOIS lookup that led to these discoveries:

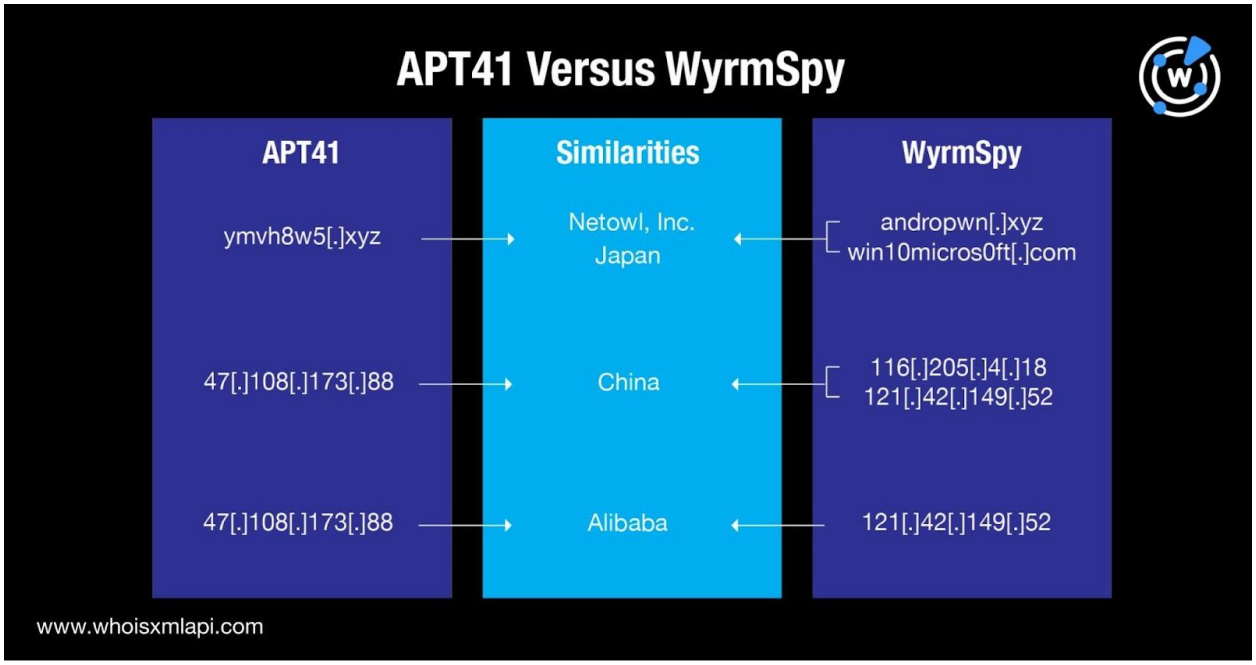
- Two of the IoCs—andropwn[.]xyz and win10micros0ft[.]com—were administered by Netowl, Inc., while umisen[.]com fell under the management of Xin Net Technology Corporation.
- The two Netowl-administered domains were registered in Japan while the Xin Net Technology-managed one was registered in China.

Even though andropwn[.]xyz and win10micros0ft[.]com were registered in Japan (not China where the group is believed to originate), they did share similarities with the APT41 IoC

ymvh8w5[.]xyz. Umisen[.]com, meanwhile, was registered in China, believed to be APT41's homebase.

Next, a bulk IP geolocation for the two IP addresses identified as WyrmSpy IoCs—116[.]205[.]4[.]18 and 121[.]42[.]149[.]52—also pointed to China. The IP address 121[.]42[.]149[.]52 was administered by Hangzhou Alibaba Advertising Co. similar to Alibaba Cloud-managed APT41 IoC 47[.]108[.]173[.]88.

The chart below sums up the APT41 and WyrmSpy commonalities that could point to close ties between them.



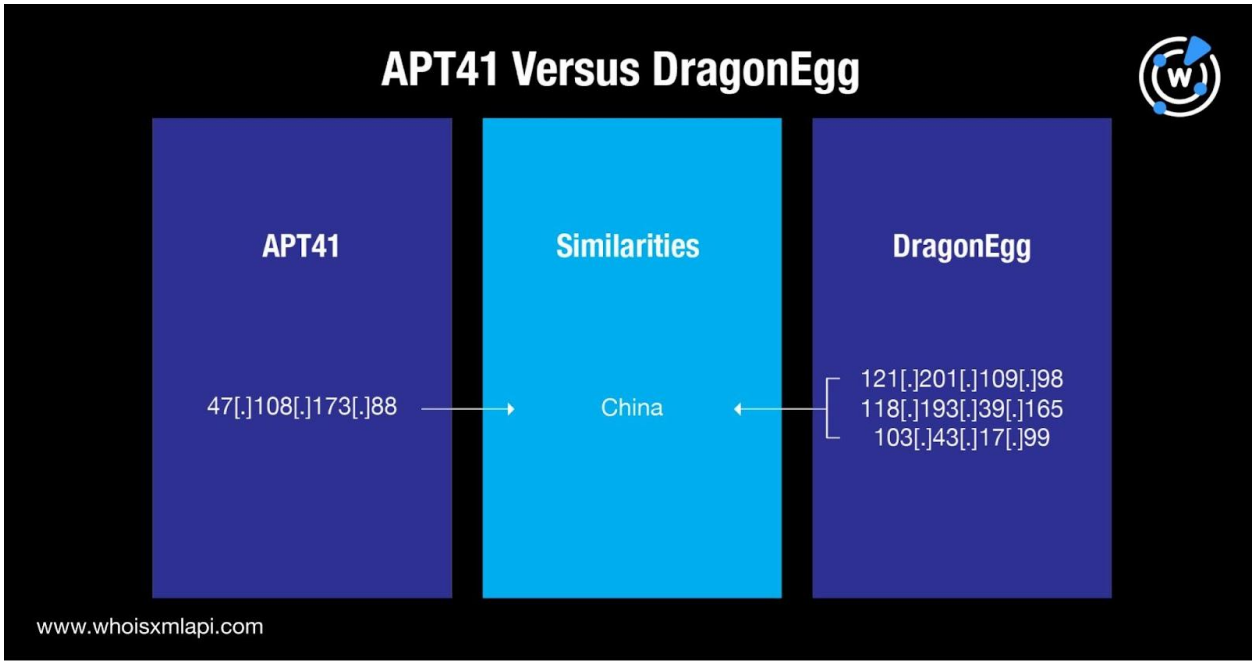
Determining Connections between APT41 and DragonEgg

To find similarities between APT41 and DragonEgg, meanwhile, we performed the same DNS searches we did with the WyrmSpy IoCs.

A bulk WHOIS lookup for the DragonEgg IoCs showed that while three of the four domains—tbtianyan[.]com, imwork[.]net, and yxwasec[.]com—didn't share any of the APT41 domain registrars, they were registered in China—the APT group's base of operations. The fourth IoC—huaxin-bantian[.]duckdns[.]org—was part of the Duck DNS infrastructure. As such, its WHOIS record details were excluded from our analysis.

Also, while a bulk IP geolocation lookup for the three IP addresses identified as IoCs—121[.]201[.]109[.]98, 118[.]193[.]39[.]165, and 103[.]43[.]17[.]99—didn't show ISP

similarities with APT41, all of them pointed to China as their origin, akin to the IoC 47[.]108[.]173[.]88. Take a look at the chart below.



WyrmSpy and DragonEgg IoC List Expansion Analysis Findings

Last but definitely not least, we sought to identify other WyrmSpy and DragonEgg connected artifacts that could put organizations at risk.

WyrmSpy IoCs

We noticed unique strings—**win10 + microsoft** and **andropwn**—in two of the WyrmSpy IoCs, alluding to Microsoft and Android ownership. Domains & Subdomains Discovery searches led to the discovery of eight additional domains—seven for **win10 + microsoft** and one for **andropwn**. None of them, however, have been classified as malicious as of this writing.

DragonEgg IoCs

We learned from DNS lookups for the domains identified as IoCs that alxc[.]tbtianyan[.]com resolved to the IP address 43[.]229[.]153[.]189, which wasn't part of Lookout's list and was malicious based on a malware check.

Reverse IP lookups for the four IP addresses (three IoCs and one additional IP resolution) revealed that three of them were dedicated hosts. Three out of the four IP addresses were shared by 94 domains, also yet unreported.

Finally, as with WyrmSpy, we also noticed unique strings among the domains identified as IoCs. We scoured the DNS for domains containing the strings **alxc.**, **smiss.**, **imwork.**, **huaxin-**, and **bantian.** and uncovered 3,085 such web properties, 14 of which turned out to be malicious based on a bulk malware check.

—

DNS deep dives, like the ones featured in this post, could aid organizations looking for commonalities that threats and threat groups share. We have, for instance, found ties that somewhat bound WyrmSpy and DragonEgg to APT41 in support of what Lookout initially believed. They can also help identify other yet-unreported threat artifacts that may enhance cybersecurity processes and solutions.

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

Sample WyrmSpy IP-Connected Domains

- microsoftwin10[.]tk
- microsoft-win10[.]in
- microsoftwin10[.]com
- andropwn[.]com

Sample DragonEgg IP-Connected Domains

- 0vo4y[.]cn
- 80ll[.]cn
- 82jz[.]cn
- aem[.]net[.]cn
- allgasan[.]cn
- arousi[.]cn
- b8075[.]cn
- bedrock[.]net[.]cn
- bets8888[.]in
- bets8888[.]org
- biosin[.]cn
- bktjc[.]cn
- cddzw[.]cn
- cegyy[.]cn
- china-cds[.]com
- cl444444[.]cn
- cookb[.]cn
- csmpi[.]cn

- daxinfang[.]com
- dious-bj[.]com

Sample DragonEgg String-Connected Domains

- alxc[.]cn
- alxc[.]dk
- alxc[.]eu
- alxc[.]tw
- alxc[.]jp
- alxc[.]tk
- alxc[.]ml
- alxc[.]la
- alxc[.]de
- zalxc[.]tk
- walxc[.]tk
- galxc[.]co
- alxc[.]art
- galxc[.]nl
- qalxc[.]tk
- qalxc[.]cn
- halxc[.]tk
- walxc[.]cn
- zalxc[.]cn
- falxc[.]tk
- smiss[.]kr
- smiss[.]nl
- smiss[.]ch
- smiss[.]pw
- smiss[.]co
- smiss[.]vg
- smiss[.]ua
- smiss[.]us
- smiss[.]fr
- smiss[.]se
- smiss[.]nu
- smiss[.]jp
- smiss[.]de
- smiss[.]hu
- smiss[.]it
- smiss[.]cn
- smiss[.]cz
- smiss[.]ca
- smiss[.]ai
- smiss[.]ru
- imwork[.]se
- imwork[.]ru
- imwork[.]in
- imwork[.]eu
- imwork[.]id
- imwork[.]ch
- imwork[.]ml
- imwork[.]cf
- imwork[.]tk
- imwork[.]cn
- imwork[.]mx
- imwork[.]de
- imwork[.]nl
- imwork[.]pl
- timwork[.]uk
- timwork[.]it
- bimwork[.]no
- imwork[.]xin
- timwork[.]mk
- simwork[.]jp
- huaxin-hk[.]cn
- huaxin-co[.]cn
- huaxin-sd[.]cn
- huaxin-js[.]cn
- huaxin-cp[.]cn
- huaxin-e[.]com
- huaxin-1[.]com
- huaxin-gz[.]com
- huaxin-v8[.]top
- huaxin-cp[.]com
- huaxin-gd[.]com
- huaxin-im[.]com

- huaxin-co[.]com
- huaxin-at[.]com
- huaxin-ic[.]com
- huaxin-yl[.]com
- huaxin-ct[.]com
- huaxin-id[.]com
- huaxin-xs[.]com
- huaxin-mc[.]com
- bantian[.]cn
- bantian[.]me
- bantian[.]red
- bantian[.]com
- bantian[.]ren
- bantian[.]bid
- bantian[.]xyz
- bantian[.]top
- bantian[.]fit
- bantian[.]pro
- bantian[.]net
- bantian[.]mom
- bantian[.]ltd
- bantian[.]win
- tbantian[.]cn
- bantian[.]org
- bantian[.]vip
- abantian[.]eu
- bantian[.]biz
- hbantian[.]cn

Sample Malicious DragonEgg String-Connected Domains

- goldismiss[.]xyz
- empiredismiss[.]live
- kdsrty-dismiss[.]xyz
- thoroughdismiss[.]xyz
- inflatedismiss[.]shop
- meaningdismiss[.]shop
- sjcnyfdismiss[.]click