WyrmSpy・DragonEggとAPT41の繋がりをDNSで発見

目次

要旨

「Winnti」、「BARIUM」、「Double Dragon」としても知られる「APT41」は、中国発の標的型攻撃グループです。2012年から活動しているAPT41は、世界中の政府機関や民間企業を標的としたサイバースパイ攻撃を成功させて一躍有名になりました。

Lookoutは、この攻撃グループが少なくとも2つのモバイルスパイウェア、すなわちWyrmSpyとDragonEggを使用して、選んだ標的から機密を吸い上げていたことを最近発見しました。グループの一員と思われる5人のサイバースパイは当時すでに逮捕されていましたが、Lookoutの研究者は、この2つのスパイウェアはAPT41に結びついていると考えています。そこで、WhoisXML APIでは、これらの間にある結びつきをDNSで調べることにしました。

当社では、Lookoutが特定した5個のWyrmSpyのIoCを出発点として調査を開始し、2個のIoCと同様に**win10 + microsoft**または**andropwn**という文字列を含む8個のドメイン名を新たに発見しました。

他方、DragonEggの7つのIoCを元に行った分析では、以下を検出することができました。

- IoCとして特定されたドメイン名alxc[.]tbtianyan[.]comが名前解決した1個のIPアドレス。マルウェアチェックの結果、悪意があることを確認
- 一部のIoCの専用ホストを共用していた94個のドメイン名
- IoCと同様に**alxc.**、**smiss.**、**imwork.**、**huaxin-** または**bantian.**という文字列を含む3,085個のドメイン名。そのうち14個は一括マルウェアチェックで悪意があると判明

WyrmSpyとDragonEggをAPT41と結びつけるもの

APT41の詳細

WyrmSpyとDragonEggが本当にAPT41に関連しているかどうかを判断するため、まず2022年に公表されたAPT41のIoCがDNSに残した痕跡を探しました。より最近になって公開されたWyrmSpy・DragonEggの各IoCと比較するために、その出所を特定しておく必要があったためです。

APT41のIoCとして特定された3個のドメイン名をBulk WHOIS Lookupで検索したところ、以下が判明しました。

- ymvh8w5[.]xyzとvietsovspeedtest[.]comのレジストラは、それぞれNetowl, Inc.とGoDaddy.com LLC
- 上記の2ドメインはそれぞれ日本と米国で登録
- もう1つのIoC、すなわちaffice366[.]comには現在WHOISレコードがない。ただし、当社のWHOIS Historyで収集した過去のレコードによれば、以前のレジストラはGoDaddy.com LLCで、登録国はシンガポール

他方、APT41のIoCとして特定されたIPアドレスをBulk IP Geolocation Lookupにかけた結果、以下のことがわかりました。

- 47[.]108[.]173[.]88は中国に位置しており、管理していたISPはAlibaba Cloud
- 139[.]180[.]138[.]226はシンガポールに位置し、ISPはChoopa

APT41とWyrmSpyの関連性

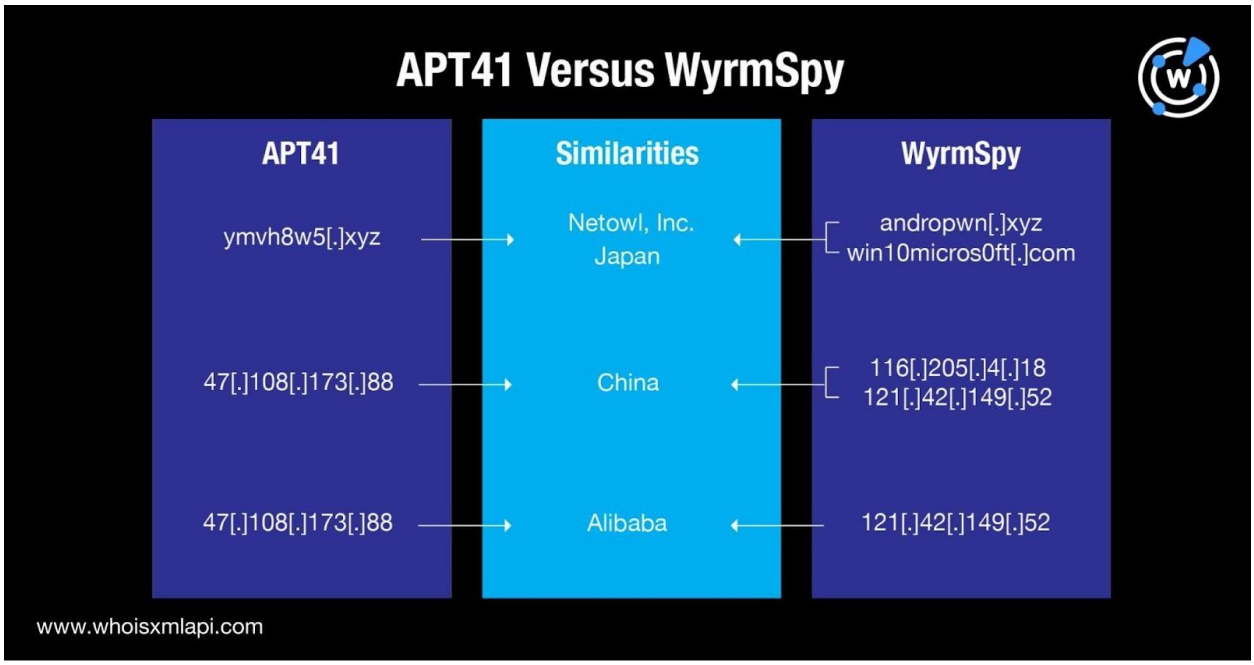
APT41とWyrmSpyの共通点を見つけるべく、WyrmSpyのIoCとして特定された3個のドメイン名（win10micros0ft[.]com、andropwn[.]xyz、umisen[.]com）をBulk WHOIS Lookupで検索しました。そして、以下を発見しました。

- andropwn[.]xyzとwin10micros0ft[.]comのレジストラはNetowl, Inc.で、umisen[.]comのレジストラはXin Net Technology Corporation
- Netowlが管理していた2個のドメイン名は日本で登録、XinNet Technologyが管理していた1個のドメイン名は中国で登録

andropwn[.]xyzとwin10micros0ft[.]comは、（APT41の起源とされる中国ではなく）日本で登録されたドメイン名ですが、APT41のIoCとの共通点がありました。その一方で、ymvh8w5[.]xyzとumisen[.]comは、APT41の本拠地と考えられている中国で登録されていました。

次に、WyrmSpyのIoCとして特定された116[.]205[.]4[.]18と121[.]42[.]149[.]52をBulk IP Geolocationで調べたところ、やはり中国を指しました。121[.]42[.]149[.]52 の管理ISPはHangzhou Alibaba Advertising Co.で、Alibaba Cloudが管理ISPだったAPT41のIoC（47[.]108[.]173[.]88）と似ています。

以下に、APT41とWyrmSpyの密接な繋がりを示す共通点をまとめました。

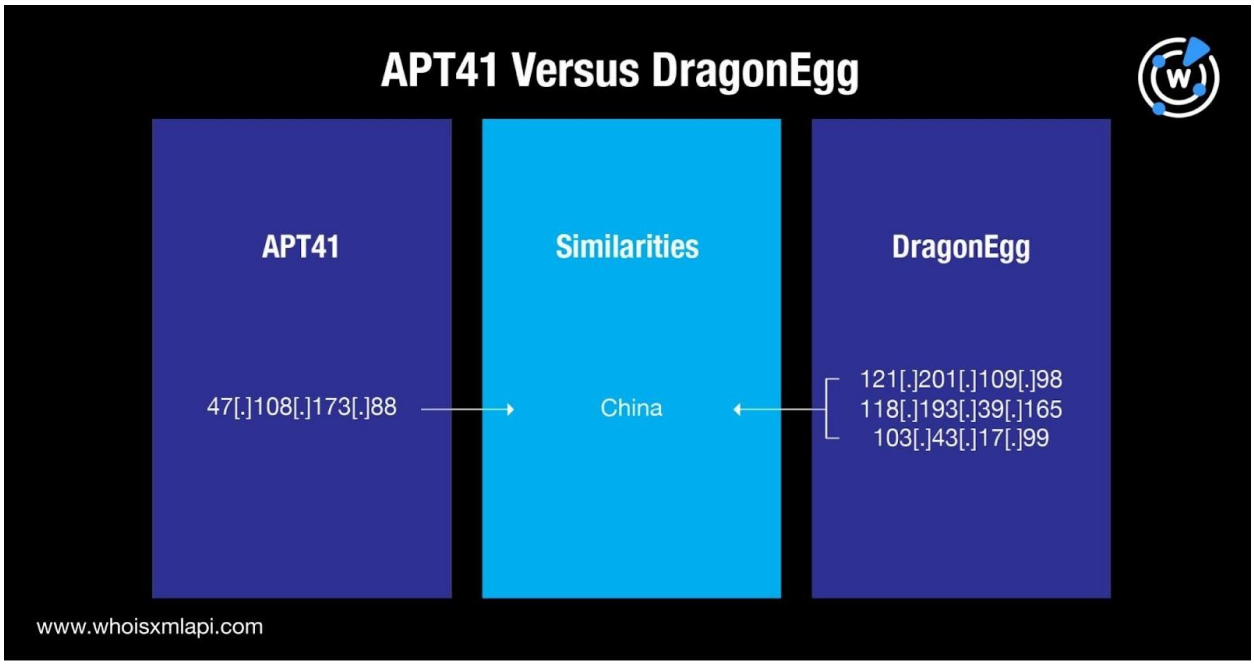


APT41とDragonEggの関連性

APT41とDragonEggの類似点を見つけるため、WyrmSpyのIoCに対して行ったのと同様のDNS調査を実施しました。

DragonEggのIoCをBulk WHOIS Lookupで検索したところ、tbtianyan[.]com、imwork[.]net、yxwasec[.]comはAPT41のIoCとされたドメイン名のレジストラと合致しませんでしたが、登録国はAPT41の本拠とされる中国でした。なお、あと1つのIoC（huaxin-bantian[.]duckdns[.]org）はDuck DNSのインフラの一部であったため、そのWHOISレコードは今回の分析対象から除外しました。

また、IoCとして特定された121[.]201[.]109[.]98、118[.]193[.]39[.]165、103[.]43[.]17[.]99をBulk IP Geolocation Lookupで検索した結果、ISPに関してAPT41のIoCとの共通点はありませんでしたが、3つともAPT41のIoCである47[.]108[.]173[.]88と同様に中国に位置していました。以下は、APT41のIoCとDragonEggのIoCの共通点をまとめたものです。



WyrmSpyとDragonEggのIoCリスト拡張でわかること

最後に、組織を危険にさらす可能性のある、WyrmSpyとDragonEggの関連アーティファクトを特定しました。

WyrmSpyのIoC

WyrmSpyのIoCのうち2個のドメイン名には、MicrosoftとAndroidの所有であるかのように見える**win10 + microsoft**および**andropwn**という文字列がそれぞれ含まれていました。そこで、この2つの文字列を検索語としてDomains & Subdomains Discoveryで検索したところ、さらに8個のドメイン名が新たに見つかりました。そのうち7個は**win10 + microsoft**を、1個は**andropwn**を含んでいました。ただし、本稿執筆時点でそれらのいずれも悪意あるドメイン名とは判定されていません。

DragonEggのIoC

DragonEggのIoCとして特定されたドメイン名をDNS Lookupで検索したところ、alxc[.]tbtianyan[.]comは43[.]229[.]153[.]189というIPアドレスに名前解決しました。このアドレスはLookoutのリストに含まれていませんでしたが、マルウェアチェックの結果、悪意があると確認されました。

3個のIoCと上記の名前解決した1個のIPアドレスをReverse IP Lookupで検索した結果、3個は専用ホストと判明しました。また、3個のアドレスはLookoutが特定していなかった94個のドメイン名によって共用されていました。

WyrmSpyと同様に、IoCとして識別されたドメインの中にユニークな文字列があることにも気づきました。 **alxc.**、**smiss.**、 **imwork.**、 **huaxin-**および**bantian.**という文字列を含むドメイン名をDNSで検索したところ、いずれかを含むドメイン名が3,085個見つかりました。一括マルウェアチェックの結果、そのうち14個は悪意あるドメイン名と判明しました。

—

このように、DNSデータの分析から脅威や脅威グループの間にある共通点を特定することができます。今回は、WyrmSpy、DragonEggとAPT41とのつながりを明らかにすることで、Lookoutの見解を裏付けることができました。こうした調査によって未報告のアーティファクトを発見できれば、組織におけるサイバーセキュリティのプロセスやソリューションを強化することができます。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトとIoCの例

IPアドレスを共用していたWyrmSpy関連ドメイン名の例

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

IPアドレスを共用していたDragonEgg関連ドメイン名の例

- 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

共通の文字列を含むDragonEgg関連ドメイン名の例

- 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

共通の文字列を含む悪意あるDragonEgg関連ドメイン名の例

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