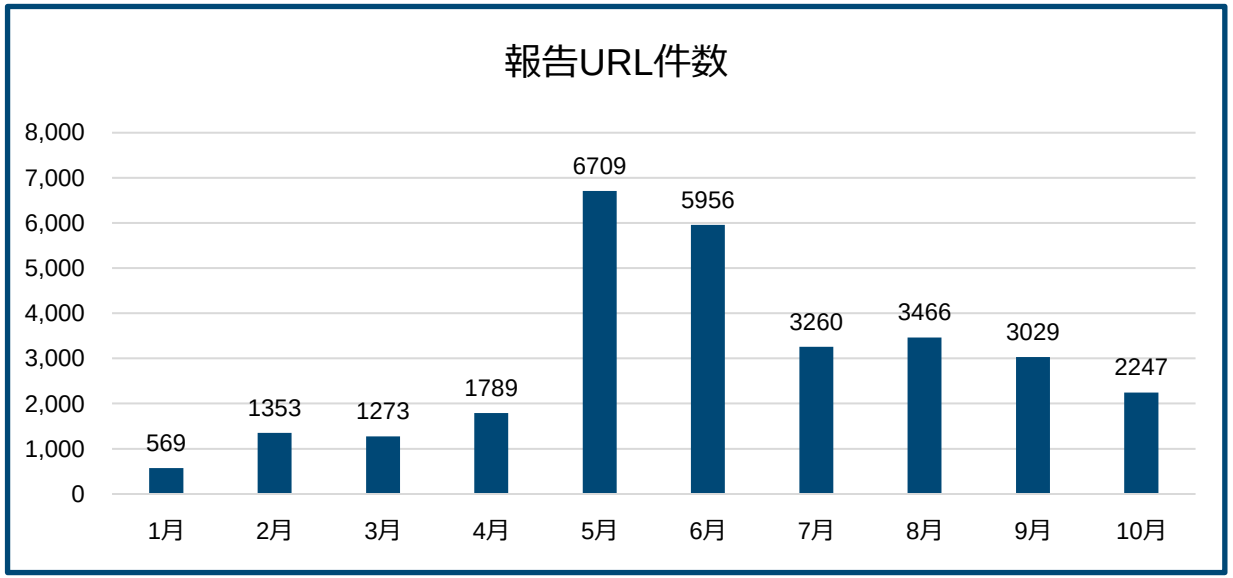
従来の攻撃プラットフォームがモバイルに変わりつつある現状と要因について

JPCERTコーディネーションセンター
インシデントハンドリンググループ
中井 尚子

インシデント報告数から見える現状

- JPCERT/CCに届いた報告数から現状を把握
  - マルウェアによってSMS経由で配布されたと思われるURL数を集計（2021年1月から2021年10月まで）



攻撃が拡大した要因の一つである、攻撃インフラについて調べてみました

- 攻撃者が用意したインフラ
- 悪意あるサイトへの誘導方法
- その他

攻撃者が用意したインフラ（1）

- 攻撃者はDuck DNSサービスを主に利用
  - Duck DNSとは
    - Free Dynamic DNSサービスを提供
    - サブドメインを生成し利用
    - 利用規約があり、違反した不正サブドメインに関してはサスペンドされる

JPCERT/CCで確認した悪用されたサブドメインの特徴

- ランダムで英字5桁～10桁と桁数は増加
- [A-Z]{n}.duckdns.org

[A-Z]{n}.duckdns.org

- JPCERT/CCに報告されたduckdns.orgを以下に一部掲載
  - ホスト数：21487ホスト

aaannnmmed.duckdns.org	baarrrdqqd.duckdns.org	caazmvvjku.duckdns.org	zzqyxmghcq.duckdns.org
aaauujvepi.duckdns.org	baaskswizb.duckdns.org	cabhudoysu.duckdns.org	zzrtlajdyc.duckdns.org
aaazuuskgz.duckdns.org	bactumkhcq.duckdns.org	cabowxztui.duckdns.org	zzsfsucpzb.duckdns.org
aabagpyiio.duckdns.org	bacxrakjmw.duckdns.org	cabxmnlcme.duckdns.org	zzskswnsde.duckdns.org
aabccpqdqd.duckdns.org	baefssttgt.duckdns.org	cacydvzexy.duckdns.org	zzsthvviww.duckdns.org
aaboyevyak.duckdns.org	bafavtzfim.duckdns.org	cacyjaubys.duckdns.org	zztrehruaj.duckdns.org
aabsgxibfk.duckdns.org	baftduzfpz.duckdns.org	caeqmtycjd.duckdns.org	zzucytuqyw.duckdns.org
aacaltupqy.duckdns.org	bagffredqp.duckdns.org	caidytvmln.duckdns.org	zzuwgilnqn.duckdns.org
aadbzljdvw.duckdns.org	bagmunayxc.duckdns.org	caizhuhopt.duckdns.org	zzwwqbcvrn.duckdns.org
aadgwbwykk.duckdns.org	bagmwgagya.duckdns.org	cakinkswbg.duckdns.org	zzyyqdccoa.duckdns.org
aaemfkrtnf.duckdns.org	bahyxrpwve.duckdns.org	camanzzlll.duckdns.org	zzzodncgav.duckdns.org
aafunzccrm.duckdns.org	bajlnlzmaf.duckdns.org	cammmbfftg.duckdns.org	zzzzylcdcb.duckdns.org

攻撃者が用意したインフラ（2）

- ホスティング業者が提供するDNSサービスを利用
  - 確認できたトップTLD：com, xyz, top
  - 129ドメイン数

TLD	レジストラー	ドメイン数（※1）
com	GoDaddy.com, LLC	26
	NICENIC INTERNATIONAL GROUP CO., LIMITED	14
	DYNADOT, LLC	6
	Sav.com, LLC	3
xyz	NameSilo, LLC	16
	Xin Net Technology Corp.	1
top	JIANGSU BANGNING SCIENCE & TECHNOLOGY CO. LTD	11

（※1）2021年11月時点でwhois情報が存在したドメイン対象

com, xyz, top

- JPCERT/CCに報告されたドメイン名を以下に一部掲載

adwnh.com	chickenkiller.com	kijjh.com	sdfwx.com	aweer.xyz	kuroneko-yamato-dv.top
aeoio.com	cioaq.com	mdwyw.com	shsxa.com	feraes.xyz	kuroneko-yamato-jc.top
aeoir.com	civrr.com	mlper.com	tdden.com	jsjp.xyz	kuronekoyamato-a.top
aeozk.com	cwqer.com	msnbee.com	tpliv.com	jvjp.xyz	kuronekoyamato-ag.top
aqgry.com	cwsqy.com	msnebs.com	trtbs.com	lajp.xyz	kuronekoyamato-aj.top
asswh.com	cxwrg.com	msnettv.com	tskgn.com	lxjp.xyz	kuronekoyamato-f.top
aswrd.com	czwrw.com	msswz.com	tsnea.com	lzjp.xyz	sagawa-exp-ff.top
aswsx.com	docomoa.com	mttyu.com	uydmk.com	soiwgaw-pri.xyz	sagawa-exp-ft.top
baqre.com	dqwes.com	muvdp.com	vaqop.com	tejp.xyz	sagawa-exp-oz.top
bcawe.com	duckdns.com	ngfrt.com	vcdew.com	tfjp.xyz	ukrtd.top
bfopf.com	efvwe.com	nheggs.com	vdert.com	thjp.xyz	yamato-xb.top
bgqry.com	eioocc.com	nuerw.com	vderw.com	tnjp.xyz	yamato-xe.top

悪意あるサイトへの誘導パターン

- 悪意あるサイトへの誘導パターンを２つ紹介します
  - Duckdnsドメインサイトから Duckdnsドメインサイトへ遷移
  - Duckdns以外のドメインサイトから Duckdnsドメインサイトへ遷移

パターン（1）

- Duckdnsドメインサイトから Duckdnsドメインサイトへ遷移するパターン
  - 遷移条件にUserAgentを参照
    - iPhoneの場合は他のDuckdnsドメインサイトへ遷移
    - Androidの場合は同じホストのk.htmlに遷移

http://nktrmroklr.duckdns.org/

```
<script>
    if(navigator.userAgent.match(/(iPhone)/i)){
                            document.location.href = "http://poyvtyfcfm.duckdns.org/";
    } else if (navigator.userAgent.match(/(Android)/i)) {

        document.location.href = "k.html";
    }
</script>
```

パターン（1）続き

- 別のDuckdnsドメインサイトでも同じスクリプトを確認
  - http://aegtxvpkwk.duckdns.org/
  - http://nbuapgpmkh.duckdns.org/

```
<script>
    if(navigator.userAgent.match(/(iPhone)/i)){
                                document.location.href = "http://poyvtyfcfm.duckdns.org/";
    } else if (navigator.userAgent.match(/(Android)/i)) {

        document.location.href = "k.html";
    }
</script>
```

複数のDuckdnsドメインサイトで同じスクリプトが使われている

遷移元サイトの確認

- document.location.href = が参照するサイト

” http://poyvtyfcfm.duckdns.org”をもとに調べた結果、複数の遷移元サイトを確認

http://roswqnfssk.duckdns.org/
http://qlhtcaztcx.duckdns.org/
http://nktrmroklr.duckdns.org/
http://terchdwyro.duckdns.org/
http://rwzxtjppaf.duckdns.org/
http://vdheiwcwfg.duckdns.org/
http://mjyoodflkv.duckdns.org/
http://trxnxicipt.duckdns.org/
http://nvykfpqtgd.duckdns.org/
http://bntxfelksr.duckdns.org/
http://zujvdytkdg.duckdns.org/
http://xtbhxwvlzy.duckdns.org/
http://mzvjqutnji.duckdns.org/
http://aegtxvpkwk.duckdns.org/
http://nbuapgpmkh.duckdns.org/

http://poyvtyfcfm.duckdns.org

パターン（2）～ホスティング業者のDNSサービス～

- Duckdns以外のドメインサイトから Duckdnsドメインサイトへ遷移するパターン
  - ホスティング業者のDNSサービスを利用

http://sjcuf.xswry.com/

<script> タグで遷移
http://fqcycobeff.duckdns.org/

パターン（2）~短縮URL~

- Duckdns以外のドメインサイトから Duckdnsドメインサイトへ遷移するパターン
  - 短縮URLからDuckdnsドメインサイトに遷移

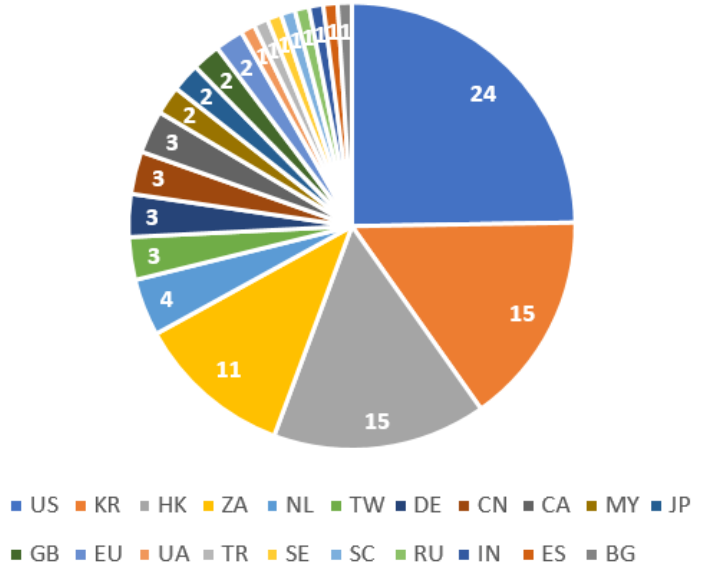
短縮URL
https://bit.ly/3q1rg4V

location：レスポンスヘッダーで遷移
http://roswqnfssk.duckdns.org/

<script> タグで遷移
http://poyvtyfcfm.duckdns.org/

サイトの分散状況

- 攻撃のために準備されたサイトに紐づくIPアドレスから、サイトが世界中に分散されている状況が確認できます
  - 21各国、97個のIPアドレスで稼働確認



一部のサイトで稼働していたネットワーク機器

- 悪意あるサイトを調査中に、ネットワーク機器のログイン画面を確認
  - D-LINK SYSTEMS, INC.　WIRELESS ROUTER HOME

まとめ

- 攻撃者は大規模に準備したサーバーやその他DNSサービスを利用し、新しい攻撃環境や不正ファイルを容易に生成できるため、セキュリティ製品で全てを検知することが難しい

【関連情報】

モバイル端末のマルウェア感染対策および、感染後の対応方法についてよくある質問をまとめてます

➢ モバイル端末を狙うマルウェアへの対応FAQ-JPCERT/CC

https://blogs.jpcert.or.jp/ja/2021/12/mobile-malwarefaq.html

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html

脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/

ご清聴ありがとうございました