TrendLabs

CVE-2017-11882 Exploited to Deliver a Cracked Version of the Loki Infostealer

Appendix

TrendLabs Security Intelligence Blog
Rubio Wu, Anita Hsieh, and Marshall Chen
Threats Solution Team
December 2017

YARA Rule:

```
import "pe"

rule cracked_loki
{
  strings:
    $header = "MZ"
    $banner = "Fuckav.ru"
    $aPLib = "aPLib v1.01  -  the smaller the better :)"
    $dot_x_code_start = {60 90 90 90 90 90 90 FF 74 24 24 5F 90 90 90 90 90 90 90 90 90 90}
    $dot_x_code_xor = {BB FF FF DF DD BE 74 00 ?? ?? 90 90 90 90 30 1E 46 90 90 90 90 80 3E 00}
  condition:
    $header at 0 and $banner and $aPLib and
    pe.number_of_sections == 4 and
    pe.sections[3].name == ".x" and
    pe.sections[3].virtual_address == 0xA0000 and
    $dot_x_code_start and $dot_x_code_xor
}
```

Network-based Indicator:

The first message sent from Loki to C&C server will have the following HTTP header:

```
POST {C&C} HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: {IP}
Accept: */*
Content-Type application/octet-stream
Content-Encoding: binary
Content-Key: [0-9a-fA-F]{8}
Content-Length: \d+
Connection: close
```

Indicators of Compromise (IoCs)

Hashes related to the campaign by the Nigeria-based threat actor (SHA256):

Malicious DOCX attachment

Hash	Trend Micro Detection
00d1ed4049db2cd84b735813beaf785a3770f9e72bfe3684b5cea1ecf1b4be98	TROJ_CVE201711882.E
6018149449143aa2eb1a0248a9535c796fe9d319e96bdbb83a7c8abf0c145e2c	
a9e42dd2b74f90955494ebc33557e329850d1325db55ecbc1bcc6281c1b35990	
c1437395619147693b12be9f5d0f95e39d10862c641d8e94d7e169d6f44f81ef	TROJ_CVE201711882.E
df50d7d75bceb1cd995e955700c8ca8a0ef6efec5e25dde28b303313eb54405d	TROJ_RELSLODR.AN
50c5f427900dbda55661b57b30b6aaa66b458a9f34e50be0f9c5683a27873103	TROJ_DLOADR.TGN

CVE-2017-11882 (RTF)

Hash	Trend Micro Detection
8442611940c325a5e7d9f58b7a8fa333b4f0ef3fade263cc742ec135844c91b7	TROJ_CVE201711882.C
40b09df4e47bb14e19be9e2162bfd912b81df38c54922f3ca64e007a9778e2a2	
0a43de085bc0e4093fa965237f3673ac2a4404c219cf826aabf3ba998f29039e	
0e2385518be5d5ab4a3b55240debf15a34a184ca912ac598f009b34ad9f6902e	TROJ_CVE201711882.O
14ce9d17a63f2e4abd6f7c51e3a6c76e6ece24455dcdcf905dfd4df09b5fb74d	
8810506affca0ce17bfd22743c7a4f17f3f076f9cf6203d1464137f93841fb8f	
161953f59fe452c87461e0eaf4f292779ef190cc75ba46b3559bb628aaed3b00	TROJ_CVE201711882.SM
7cbc9bd3f2234872aeec5a2017790e98a227fcf7864156ab17f7421e17c3c7a9	
1c28178ae3b5749d7052ea8365f54337c9e55dbec6549e0a05a2e17e2d6fda92	

Malicious HTA Dropper

Hash	Trend Micro Detection
564ddae99617959c1f7a8f82e06d93d189ab075ab5ccc98841f452f4673e508d	HTML_POWLOAD.ASUSB
d61e36db60622a63b29733d9a6c8dc24f98e0e6d4e4e81a256904e22514bb0e6	
1b1c05cfb92775a361806f2683db1e8cd1582128488371d4286e7adb528ae74b	
a2cc58eee7021d61c189701c3b2b93d035647d439a86394a00ed2f473dd92601	
0f7b99d7d36b21a2d7b08dfd07e2377ab7326952986fb272f6190bf9b078d6d6	HTML_POWLOAD.ASUSF
a43f62ea3b268b5704b0415f110620f695590e073ede02afaa56e5b7a0505eba	
bc36d65b859871e1dba1f358e951a0bf78d0347777cbb5bba16c6a2a9aab7cdd	
a43f62ea3b268b5704b0415f110620f695590e073ede02afaa56e5b7a0505eba	
835473c44f5c613ac1ff7bed4517c28005c5edbc35059c1ba7fa2502c8ab5be9	
6c4ab8732d25510684839a466506f89c7aef133abf91f2ab30c12c94dd42c05a	
1c55d3dde7501259be934c188428ed4ab16ad245f742a0ec504c6ce168b9d174	
a43f62ea3b268b5704b0415f110620f695590e073ede02afaa56e5b7a0505eba	

Malicious URL Host

URL
hxxp://gamesarena[.]gdn
hxxp://gamestoredownload[.]download

Loki PE Sample detected as TSPY_LOKI.SMA

Hash
850e7a49e9d50a5195967b0cf68779b928030615b24161d86bcd8f4e63689785
71213c664ce0f013cd581a0e943945b1246f81bef43d606e312a961e5901601a
2bf5cfe7a5b6a81c4cfb5c45c1616f78bb36adfe89a6cfe21fe81f6f95220a2b
9006b9665fba06783fe32870fc0dfd9ba502e6cced5c7352d24d438ed83f2462
97cc28b6c03d62c0f768b7bce7ebf2e1ca0d12ae831f904ce3028a47ebea7d36
0eb633fae5cfd0ef55217e24cda47d75168c9af19c2e8077376a6dcb8b5a4b55
dd80431b9bd1dbd4f417d83b6b2859d760df0c292d02015b1abba6039faf13c9
ca612b0f95c6da850ac84c13f90a3094688ece98261695f0c0a1cf481cc3f68f
95ac59daf9cd7c69b35474188522286e2f6f2b23e94ad70aab744dd7f2dccaf6
bcce47980626fae2881fef38bff9edf1fae4c9d84c7c635153ba1bd3bd8e51bc

Hashes related to the campaign that uses Server Message Block Protocol (SMB)

CVE-2017-11882 RTF

SHA256	Trend Micro Detection
ff18b96950d524bf9aa0f377588663afa4a36ec1cf23002c2a894d688012416f	TROJ_EXPLOYT.JEJOUE
9cdbdc5b917a4e8be41b8ec3fee3a59d2aafd5303857f43a61cd36bcae874cd7	TSPY_LOKI.AUSIQY

Loki PE Sample detected as TSPY_LOKI.SMA (SHA256)

Hash	Trend Micro Detection
ff18b96950d524bf9aa0f377588663afa4a36ec1cf23002c2a894d688012416f	TROJ_EXPLOYT.JEJOUE
9cdbdc5b917a4e8be41b8ec3fee3a59d2aafd5303857f43a61cd36bcae874cd7	TSPY_LOKI.AUSIQY

Hashes related to Loki (SHA256):

Hashes	Trend Micro Detection
a921bbde5773619d7748ffd286853739748e78a287647e943507e2745b62db55	PE_VIRUX.O
f3fd17f9d8fad1160a90d881f8b9e1fb159a03f3960d1902ead740f8d5879f45	TROJ_GEN.R03EC0DHT17
4ff414a855b23a7a11a60aa1da89140aa70947371b0daaeb7baa7a70cc07d485	TROJ_GEN.R047C0DE917
28f129fd0c9d02be750dbcc7a6730d699223150af070917d55a284a9ab88952f	TROJ_GEN.R0EBC0DEB17
add2fa2c8f4065c393405885f0fc553e866ce4ad699a3f90b3707a04bb5df7f3	TSPY_DYRE.YYSQA
93dca3fc78bc266452402d83e184980b11e81e1e05b86d2b5abfbfe95504da39	TSPY_DYZAP.NJT
369638e06c737bce87c6eaa4f3fd6f5402af4d3aca2ace897f893714b59afb85	TSPY_DYZAP.NKA
a99aa73acc1944d0242fbf88089206b8bd44c7b37965bc459a20ceb81dade50d	TSPY_DYZAP_GE2300C8.UVPA
6ef6a9255f7448e0c37a51f19b9f97757b89b1fd6eebd63cedc2eeab9739cdcc	TSPY_FAREIT.VDS
1a53a0f445aca7b6b3aa6b87c4e08f2e649f47aab68c6aa0fc69aedd7f100bb4	TSPY_LOKI.GVI

Hashes related to Loki detected as TSPY_LOKI.SMA (SHA256):

Hash
0026b14f896934c621eccca48474353fff08f592ebc2949dde4b881f2353e3d2
01ab4ad758b3759fe16bba5262ad2d102d7081a56dcbe1103c6c409027a59b9d
03ad225eae702b381e4ebfb4025464d36d582c3fe2289369fac6c8339e69bfbc
06574c6cefac987b1988ed1397a86fdd5715742f78413d0a3a24ba0a7b751cdd
0a6dffa7e3fe94bef9865778816468cd9e6ca3065b592d93e33b3d9dc733a992
0a79089022601e04f2916f3ab52f6b5746c4938b3ae1488192af795f6d559825
0eb633fae5cfd0ef55217e24cda47d75168c9af19c2e8077376a6dcb8b5a4b55
0ecdd0c4b3a1eefa2b9aee2fa496f08d6a2a28777db849ad13c5a4b36211f19b
12979add67c70fa4d82fba7bd24632dc8dad2957c8b0d272a3644267bb32433d
13c42c75fb2a2eaa326efbc3afa543c78f08c11b75f3c666797b94551e01247b
1725a4902ac7f0727d68d6b745721a4ac1e56d7fcb221097bf9b2d2195237178
1ab1f44d9b860a211ae745eb44c87806a11a5b068ae91149b06e9639168d7f48
1bc9381f0e81f37f33513148867f918c937c78d4df3087039858fb8d058e7fc1
21c4155321a0aad0ebbd12db6e0f95003ae1853f3732112b37e1ccc114ae6e7b
220de568269d96b8eff47544567c07f255e50b88acc8dc653602ded575d93805
225cfc4cc0b9369d80e19f88ba69b65381c037f9cc2b74e2c3d6d34dc2fdc0a0

Hash
26af5209c0536daa6ca3b190cc37f1fa85eb7362f57dbcf34594bdb616da8b33
26e61a3ace86d1b5d3f9b1e7142e3219445467ac653f49d90f4aa4d5cc164830
27826bd0951e02bbe17b86560808b876e90805ace44f3d664eea41d96441ab4a
2a01d210d341987abe066998bf00a2773e1ece297102e72c7599722bf0f27444
2a8f8218bef8755edcb9b6c1f1c30d678645f6e1d7fa967311b027678516fe43
2bb3b199e484cf70b03550853da021416cb801178c5bd6063bca50ed4b579375
2bf5cfe7a5b6a81c4cfb5c45c1616f78bb36adfe89a6cfe21fe81f6f95220a2b
2d01bbe9bf65d249e47601ed5de95c04054f0032cc541d2e00897bbd79fe7cfb
30854636603f3a8b1b7f8426eaa2ff4afdb06281f0207f1b2c5dbb981679bb4b
31cc0f50bdd9a91281dba7df979b3bfa9428b09878b9ab2a9dd31cfeef5cd3df
326c05270666f33c76d0405ea5fec943c4cea64c5acb5cd0a72f0d3c29f67c0f
33c7891f8d57d1f0a932cf8d5827865c033f5be075d0c30e902c83bc1bd27a8c
35dbdc8374c26cc26e078bd1bd2f51c1651291c2ad1dfcb4b90f9d4da1530917
36905de277ff2a2d8c20baaef8b1905cbd4d10007c152984c34344018b480fbe
3b54d1a177ea34a7c581ea1a3c7b1a2f4b14dd1fbb07d141f1544a4105588cba
3c1d73942f00af5359e999074d82c6947daa7cbe4eb4b91faa694b095929cbbd
3dfb11c5ee8c8f8f8021abde03ab64a3d03fdc1d7529bf81666361aaf6b2c9d7
3e781bf4593008df056e187c494912ce7283e18697961968fd86771ec29c1421
404cab99464058f0722bc3238b209755963b232e5a81d8748ad6ee0de82ca35c
4619eed02a96dd100dac96da7a50abb0ddf6c9bc8dce27d3b4f4531efb12cca6
467c63a8b829902b3b7321b1bfd603a70614473db58c468c5f5d40982913d610
470f62d54626f1342b745a9a7e6d128f8442dfc023e2f5ceddc6ca73b5054c8
48b5e024d397299626ae8cb48ccb566012a004cb3c0d182a382f51d466020e7f
49e2ddc6a8de9e34f1fbcd63aed340d84016c58be13b1b0dd6e985b663680f56
4caa711f7c98f5fa3bc88e98699378e7e6082a7baf8aba596d3f5882497813fc
503f3caed43219494659f6b06e169d14f809df07897e39d5e835930856648944
571bd8985f9297ea39f688ffbbaa14a765e89a0db8bcc161b05c5046fa921aa0
58e531e58db5602de9de0bebe5c7e26579394ec8f30f468fbd41e41868e0742d
5995a599feb35b4dbdea133cc3b9121c37f78a8011f06250c64322307c960969
59bb26ff7cc47591501c1389a263c93aa3493aa9c0a909c421e62eccfb4afd4f
5bd97158059a46026770efc687b238cf0baf41880e01f125f55ae54b6f501984
5c090801cd3b554b3f2409bc52e95ddd491540ae618500f907b677902ba3f818

Hash
5d656d7182517d0e09f1fc7544457bfefdddbc317de15fdfb4850886b695f6d7
611b20c5535bf53f88b5cc7c7af61bf76cb62a10bb6b4b53090ad10998c7b060
6351fd8c3a125dd0c2060540961477e56efb5c5fb8fad930c2929aaa666dd9a2
68ed422ffaa75740d4ca899aa152b8263d9189fb8579345399cdd99f8c88a243
69bde8f8a0f2a23956eb9c0fa8782dc1e89f534eb8e01e0c8e193e07e72ac76c
70871088793bf3ad866e39250fcfa306b964406e7e54034c8e8304ea0fbea21f
71213c664ce0f013cd581a0e943945b1246f81bef43d606e312a961e5901601a
7619f2a6c8db65df0b27c9af4fb1bf062e255c357f52fb93e4b41efe151dfd49
7744f7b3c707e4b5d1f8e0f5e4f1db3398194857af50798ac13c7f3c55ce8f9d
7a64ee76948dcc792da710a9e737490ec700b68b89149804237bba23f45409eb
7f638f6206be06396d60b883572c43f606e99ea9f437f17fd5c9c1e190367357
850e7a49e9d50a5195967b0cf68779b928030615b24161d86bcd8f4e63689785
8559aa90340a97631b039ad3cb9e0498a5d78b87e3d71d3a6728c46a6d50edc3
86ee72ba631a13f7ad6047c43ee5499f2f32a9643695e5afe4bbf0d97b14e8f7
8a42b676f5998f2c9c155a018ad788ec6e603ddfa900c70e413af094584d5679
8eb1be5c6b2ab5e97488abe1fa9af945a6d99880e413ecb139648498336b166a
9006b9665fba06783fe32870fc0dfd9ba502e6cced5c7352d24d438ed83f2462
901cee065f549a98a990ec30f8099c9b3457d39e89ce648aaea16a0cd3240e16
92f1219f1dd31f00412579b846e77b61f1a6e3e1f039e7f08409985930b9143b
95ac59daf9cd7c69b35474188522286e2f6f2b23e94ad70aab744dd7f2dccaf6
97894235124b1b4027278dd80f152bd9c977f31ffcb9f6c3cfe4bbb7847e7407
97a58c2760ec7a1a47f132e0df5f6d76761e6e58cee6846eca1ffbed001aad40
97cc28b6c03d62c0f768b7bce7ebf2e1ca0d12ae831f904ce3028a47ebea7d36
9921fcab60058b3591c5f412422e260aa056fb1dcedd1278c31b52006eb640b5
9b69ffa0990d178d087d83b9f9e393d0b96b8c6c2da2f58996c1889730c8f765
9d4c4838366d3a84516a820a9faf56e3fa6249baa2225a9fd14e38aa235bd57a
9d6ce921878e549e8a09826cb1c1b7944280c1b606f9fb1e9b4454916a5d0c26
9e7b90185bfa8b596af7dd53851eed0eae29d2b7ae82aef6fee0ce619f340413
a1856e1cd568458e74011e7cbc7ca7db16d9dfe6f9d2d59490c810436a34dd8c
a3e2ab5bd6f9c3f6568333cbafd0789314b8dc66144af20deed72195d37a5382
a440df4c2569bfa68a00b74815c8062b6da63791c4fb99d59a75cbc92b2f486b
a5b9f7dca4918414a2226dce459e606b2974eb865ebd3af18e668a5ecea8fe45

Hash
a6814014b4390e2498bf7ec23c34c1fdb6ed06490ef23320232591ff5d0b1354
a987c746715952542b746c09cb3d50342c168085620fbddd5c82a72ff1052af8
ab6e1b20e7bddc16df72b7a6fd7ec0ef003cfb2944acc5f4f889913994ed49b0
abbb1bbf0a38d69db27dc448b3dc093b63dfaadcf84af5ff9d84eef3f29825f6
ac87b9ba5619fbf64a0cae490e268f0cf41e2da113cbda1a3b72d2dd6a3274c5
b0454ffa73fcc3025fda06a52cce1a27a51cf796729ee3734fb7b5d89cd13d10
b1336bed53a86c24385ee478f1cdbffad6430dc31bdc72bfcd64f420911de4cf
b27e6130e023d289d8e1c8c43e2bde714b4f3ccb445392d868a97e8c8f466cd6
b4494cd7f55e105b6010d969968d8034dc83fbcfe773ef83c70f2311848c10a1
b50ba791f516bbef4cf16a876f40bc9d65cbd184bf25de41da726ef4b8a7e224
bb16e622533031379c44eaa58cb1b7ffa3a983e2662dc3ad769f4415305c76a0
bcce47980626fae2881fef38bff9edf1fae4c9d84c7c635153ba1bd3bd8e51bc
bd69f0e6f0aa10b9dcf70382709a1956e6a50e7be3e709d9bb2b1753405e6e03
c2e0b3d6933b86991de47f40cb19e275dd2af0df98c54567058701df986e3e0d
c41de290657158d61f50ad32ae802eff77c70e491fcaeae5bffeb0b1c964f334
c6a360518ffc7d1b7638070b7a21fdc138f1c887aee38f1294d3741dfed88fa5
ca612b0f95c6da850ac84c13f90a3094688ece98261695f0c0a1cf481cc3f68f
cc9060fa93461114bdf8bdba44f8e3c1a78be5e891eca3bc850d0d273456ddfe
cda5f709a738fa29e53e918e3573289c201f84d1472adcade624dad65343d8d9
d0567b928dc0a7180c4596486abadd7b8fd7d49621fe8ced84b7d6f9382a65ba
d0a69965781b3c4c53c62e2ee74fc73a672da7efe571404bea249371534ad090
d428a5f52d0daf3c2780375bc9f0dd6d9e8cc0a292df7ca4dea05f222ca24a5e
d7ae1c11678e54d25218a116694ca0db2b01033ee291da6a3471571007b5dcc3
dd06b2e2164e0d0a8f1f76678e2d96117b290f16bb3a97834ef0684bd379291e
dd80431b9bd1dbd4f417d83b6b2859d760df0c292d02015b1abba6039faf13c9
e20438bd29158030c8d9dcf47b7ca332cdfc657a577407b543d17df6fed1d415
f5cc0b0ae5d2339c5ec6480669e745a443292d49f666f2bec8d7725f51d7765a
f7a9cf61b4ce80bb9feab56f3ba288cecf6f4459e8c176a0e58cf17a50517051
f813cf02237da59747c8ee5947cc7a6cffbd6403e54734a3bf5fe4b6e98daa3c
f82276a4d36d019ac5dc37d114c864881b36d4fc59ad5364656c6ce810bdce6b
f961d8a4a9c168d553910bea89a4760d1ad06ec6ac3032d23872e0378aee512c
faa709570e833845c747bc7fa88c599c0b28be5d7adaad5b58913346ca2d344f

Hash
ff8c4b15e7a7836402e3c4b9b5edff3e89c92d239d3f034902bf730822bca604
ffc20098f0cdf113ab5632d1390342d4763037b74301bf000e8822efe0e8fc3e
ffcd475da57f057ab63d3219f088007eae2a746a7a8b87ae24b4e0db7afb8d3f
17efdd8db9c65225ddc30aa099d026bba0489cd9eb5b21f0079d7fc9e8a745f3
c528934b17a1577d3be5d7feb74ca69a0f39a35bac1414b529efc21c915332f9

Command-and-control (C&C) domains related to Loki:

Domain
hxxp://amazoncc[.]ru/lokey/fre[.]php
hxxp://subsindia[.]com/new2/fre[.]php
hxxp://247bags[.]website/bobokay/wp-content/Panel/five/fre[.]php
hxxp://jahisable[.]com/divver/Panel/five/fre[.]php
hxxp://185[.]165[.]29[.]182/alexben1/1/fred[.]php
hxxp://bitxz[.]online/five/fre[.]php
hxxp://shipboot[.]com/dev/wp-admin/images/Panel/five/fre[.]php
hxxp://156[.]67[.]106[.]239/cronic/loki/fre[.]php
hxxp://185[.]207[.]207[.]20/slim/five/fre[.]php
hxxp://alhadin[.]nl/Earl2/five/fre[.]php
hxxp://mobizwiz[.]xyz/rox/rox[.]php
hxxp://185[.]165[.]29[.]24/cgi-binn/five/fre[.]php
hxxp://citricpule[.]xyz/jacku/jack[.]php
hxxp://94[.]23[.]148[.]41/fre[.]php
hxxp://amazoncc[.]ru/lokey/fre[.]php
hxxp://gamestoredownload[.]download/autoconfig/level3sp/fre[.]php
hxxp://epco[.]nut[.]cc/ml/vrs/peta/2/lok/panel/fre[.]php
hxxp://tokimecltd[.]ru/test/five/fre[.]php
hxxp://u0431828[.]cp[.]regruhosting[.]ru/ADMIN/Charles/fre[.]php
hxxp://198[.]54[.]120[.]205/scroll/NW/fre[.]php
hxxp://ajexceptapps[.]club/five/fre[.]php
hxxp://jahisable[.]com/baggins/Panel/five/fre[.]php
hxxp://247bags[.]website/bobokay/wp-content/Panel/five/fre[.]php

Domain
hxxps://impoexpoboton[.]com/images/Panel/five2/fre[.]php
hxxp://krets[.]square7[.]ch/wrk/fre[.]php
hxxps://mnbvcxz[.]biz/oj/five/fre[.]php
hxxp://example[.]com/fre[.]php
hxxp://palapala[.]square7[.]ch/job/fre[.]php
hxxp://etc[.]ashcarsales[.]co[.]za/fre[.]php
hxxp://amberwater[.]com[.]my/plugins/panel/fre[.]php
hxxp://nelz[.]shiponka[.]com[.]de/panel/fre[.]php
hxxp://etc[.]ashcarsales[.]co[.]za/fre[.]php
hxxps://mnbvcxz[.]biz/pc/five/fre[.]php
hxxps://burkino51[.]000webhostapp[.]com/Panel/five/fre[.]php
hxxp://heyofnices[.]com/trice/five/fre[.]php
hxxp://henqipec[.]com/kentex/Panel/five/fre[.]php
hxxp://topytop[.]xyz/ch/Panel/five/fre[.]php
hxxp://kingu[.]xyz/cool/Panel/five/fre[.]php
hxxp://rythm[.]globalmekrim[.]com/love/five/fre[.]php
hxxp://195[.]181[.]245[.]196/v1/fre[.]php
hxxp://gamesarena[.]gdn/animationsetup2/animation2kc/fre[.]php
hxxp://gamestoredownload[.]download/donjykes/fre[.]php
hxxp://gortyllc[.]website/images/Panel/five/fre[.]php
hxxp://elalamia2000[.]xyz/chikarica/5/fre[.]php
hxxps:// logzbox[.]info/admin1/Panel/five/fre[.]php
hxxp://ramesa[.]com[.]au/pro/Panel/fre[.]php
hxxp://randomheadshots[.]tk/fre[.]php
hxxp://gamestoredownload[.]download/animationsetup3/animation3kc/fre[.]php
hxxp://wellmaxlimiteds[.]com/en/max/fre[.]php
hxxp://justloki[.]info/marley/five/fre[.]php
hxxp://rbxl[.]services/smad/five/fre[.]php
hxxp://accountsofsc[.]com/west/five/fre[.]php
hxxp://gamesarena[.]gdn/donjykes/fre[.]php
hxxp://u0437697[.]cp[.]regruhosting[.]ru/Admin/iyke/fre[.]php
hxxp://zeroci[.]club/boss/fre[.]php
hxxp://gamesarena[.]gdn/startsetup/startup5ed/fre[.]php
hxxp://u0431828[.]cp[.]regruhosting[.]ru/ADMIN/Bobokay/fre[.]php

Domain
hxxps://satriafbs[.]com/eby/wp-admin/Panel/five2/fre[.]php
hxxp://loramyra.smrtp[.]ru/lok/five3/fre[.]php
hxxp://eualube[.]com/throwan/bhoka[.]php
hxxp://gamestoredownload[.]download/flexysettings/settings4flexy/fre[.]php
hxxp://weneedcheese898[.]com/wp/wp1/pr/j/fre[.]php
hxxp://btlworldwides[.]com/grim/zax/fre[.]php
hxxp://gamestoredownload[.]download/animationsetup1/animation1kc/fre[.]php
hxxp://pviewfile[.]ru/2695217/original/fre[.]php
hxxp://108[.]61[.]196[.]228/five/fre[.]php
hxxp://gamestoredownload[.]download/animationsetup2/animation2kc/fre[.]php
hxxp://gamestoredownload[.]download/startsetup/startup5ed/fre[.]php
hxxps://tacro[.]eu/wp/wpmf/fre[.]php
hxxp://egobiawa[.]com/Panel/five3/fre[.]php
hxxp://gamestoredownload[.]download/animationsetup4/animation4kc/fre[.]php
hxxp://henqipec[.]com/kentex/Panel/five/fre[.]php
hxxp://ddbb[.]eu/five/fre[.]php
hxxp://198[.]46[.]238[.]120/ochus/Panel/index/five/fre[.]php
hxxp://clargee[.]us/jon/fre[.]php
hxxp://101[.]99[.]84[.]24/sms/52-1/fred[.]php
hxxp://gamestoredownload[.]download/wp-contents/settingspa/fre[.]php
hxxp://gamesarena[.]gdn/settings/settingsdu/fre[.]php
hxxp://gamestoredownload[.]download/settingsdu/wp-contentsdu/fre[.]php
hxxp://gistsstack[.]com/panel/fre[.]php
hxxp://gamesarena[.]gdn/configsettings/winning4cj/fre[.]php
hxxp://u0432678[.]cp[.]regruhosting[.]ru/DECEMBER/iyke//fre[.]php
hxxp://176[.]31[.]222[.]117/kros/fre[.]php
hxxp://gamesarena[.]gdn/donjykes/fre[.]php
hxxp://u0424064[.]cp[.]regruhosting[.]ru/ADMIN/IK/fre[.]php
hxxp://p-hub[.]net/cane/dony/fre[.]php
hxxp://185[.]141[.]26[.]69/~hastic/muller/fre[.]php
hxxp://gamesarena[.]gdn/setup-bin/settingspascal/fre[.]php
hxxp://fbcom[.]review/lo/five6/fre[.]php
hxxp://gamesarena[.]gdn/animationsetup1/animation1kc/fre[.]php
hxxp://knowkeren[.]xyz/adi/Panel/five/fre[.]php

Domain
hxxp://lokpanels[.]info/ext/donemy/fre[.]php
hxxp://gamestoredownload[.]download/configsettings/winning4cj/fre[.]php
hxxp://u0431828[.]cp[.]regruhosting[.]ru/WP-Content/Ben/fre[.]php
hxxp://80[.]209[.]224[.]203/v2/fre[.]php
hxxp://fourrese[.]net/colonel/Panel/five/fre[.]php
hxxp://toch[.]hgigardenpatio[.]com/Panel/five/fre[.]php
hxxps://master-patent[.]ru/filesthrogh/Panel/five/fre[.]php
hxxp://mulyadi[.]co[.]id/wp-content/uploads/2017/01//Panel/five/fre[.]php
hxxp://109[.]235[.]70[.]223/lifetn/fre[.]php
hxxp://koprio[.]ml/atlantics/panel/fre[.]php
hxxps://jibnd[.]com/wp/wp-ups/wp_config/wp-files/fre[.]php
hxxp://maunowhg[.]com/wp-content/themes/twentytwelve/css/Panel/five/fre[.]php
hxxp://80[.]208[.]226[.]44/v2/fre[.]php
hxxp://icaropccint[.]club/sev7n/fre[.]php
hxxps://salesxpert[.]biz/marley/five/fre[.]php
hxxp://yupservice[.]ru/five/fre[.]php
hxxp://gamesarena[.]gdn/autoconfig/level3sp/fre[.]php
hxxp://mairi-g[.]com/Work0space/IK/fre[.]php
hxxp://185[.]62[.]188[.]11/marieg/010/fred[.]php
hxxp://gamesarena[.]gdn/animationsetup4/animation4kc/fre[.]php
hxxps://supertroit.xyz/dbwork/fre[.]php
hxxp://belarustravelsview[.]ml/voke/Panel/five/fre[.]php
hxxp://216[.]170[.]123[.]111/price/five/fre[.]php
hxxp://194[.]135[.]82[.]113/v1/fre[.]php
hxxp://constructorasinmuros[.]com/css/images/admin/modules/five/fre[.]php
hxxp://luxloki[.]info/lux/five/fre[.]php
hxxp://gamesarena[.]gdn/animationsetup3/animation3kc/fre[.]php
hxxp://youthwinger[.]com/let/Panel/five/fre[.]php
hxxp://156[.]67[.]106[.]239/hustle/loki/fre[.]php
hxxp://globalmekrim[.]com/love/fre[.]php
hxxp://u0418693[.]cp[.]regruhosting[.]ru/name/Masky/fre[.]php
hxxp://loramyra[.]smrtp[.]ru/lok/five9/fre[.]php

Securing Your Journey to the Cloud

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO