The “EyePyramid” attacks

A homebrew cyberespionage operation that took Italy by storm

By GReAT on January 12, 2017. 2:54 pm

INCIDENTS

CYBERCRIME MALWARE DESCRIPTIONS SPEARPHISHING

GReAT
Kaspersky Lab's Global Research & Analysis Team
@e_kaspersky/great

On January 10, 2017, a court order was declassified by the Italian police, in regards to a chain of cyberattacks directed at top Italian government members and institutions.

The attacks leveraged a malware named “EyePyramid” to target a dozen politicians, bankers, prominent freemasons and law enforcement personalities in Italy. These included Fabrizio Saccomanni, the former deputy governor of the Bank of Italy, Piero Fassino, the former mayor of Turin, several members of a Masonic lodge, Matteo Renzi, former prime minister of Italy and Mario Draghi, another former prime minister of Italy and now president of the European Central Bank.

The malware was spread using spear-phishing emails and the level of sophistication is low. However, the malware is flexible enough to grant access to all the resources in the victim’s computer.

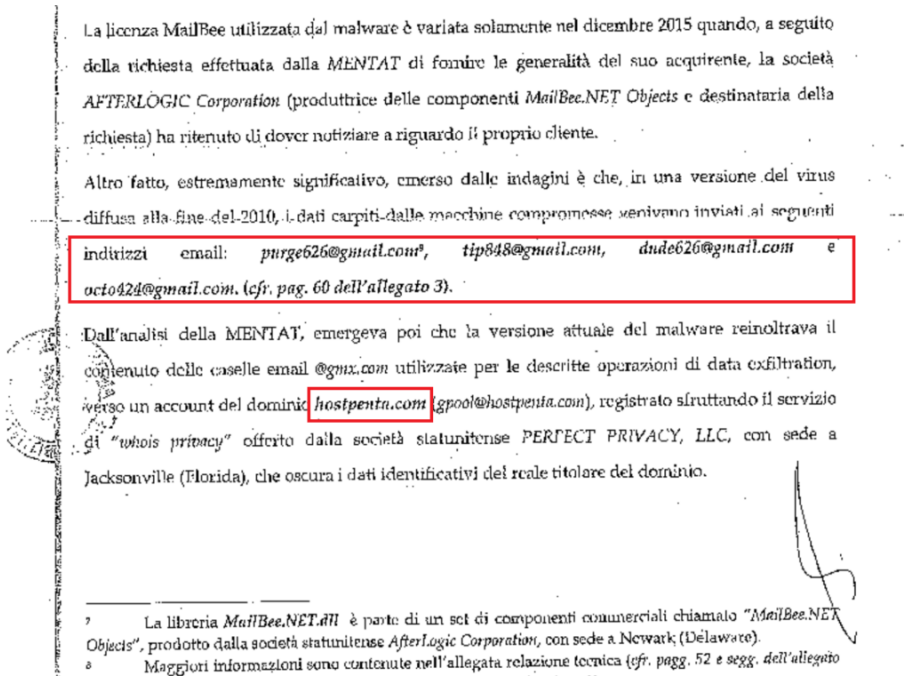
During the investigation, involved LEAs found more than 100 active victims in the server used to host the malware, as well as indications that during the last few years the attackers had targeted around 16,000 victims. All identified victims are in Italy, most of them being Law Firms, Consultancy services, Universities and even Vatican Cardinals.

Evidence found on the C&C servers suggests that the campaign was active since at least March 2014 and lasted until August 2016. However, it is suspected that the malware was developed and probably used years before, possibly as far back to 2008.

Two suspects were arrested on January 10th, 2017 and identified as 45-year-old nuclear engineer Giulio Occhionero and his 47-year-old sister Francesca Maria Occhionero.

Investigation

Although the Italian Police Report doesn’t include malware hashes, it identified a number of C&C servers and e-mails addresses used by the malware for exfiltration of stolen data.



La licenza MailBee utilizzata dal malware è variata solamente nel dicembre 2015 quando, a seguito della richiesta effettuata dalla *MENTAT* di fornire le generalità del suo acquirente, la società *AFTERLOGIC Corporation* (produttrice delle componenti *MailBee.NET Objects* e destinataria della richiesta) ha ritenuto di dover notiziare a riguardo il proprio cliente.

Altro fatto, estremamente significativo, emerso dalle indagini è che, in una versione del virus diffusa alla fine del 2010, i dati carpiti dalle macchine compromesse venivano inviati ai seguenti indirizzi email: *purge626@gmail.com*[8], *tip848@gmail.com*, *dude626@gmail.com* e *octo424@gmail.com*. (*cfr. pag. 60 dell'allegato 3*).

Dall'analisi della MENTAT, emergeva poi che la versione attuale del malware reinoltrava il contenuto delle caselle email *@gmx.com* utilizzate per le descritte operazioni di data exfiltration, verso un account del dominio *hostpenta.com* (*gpool@hostpenta.com*), registrato sfruttando il servizio di *"whois privacy"* offerto dalla società statunitense *PERFECT PRIVACY, LLC*, con sede a Jacksonville (Florida), che oscura i dati identificativi del reale titolare del dominio.

7 La libreria *MailBee.NET.dll* è parte di un set di componenti commerciali chiamato *"MailBee.NET Objects"*, prodotto dalla società statunitense *AfterLogic Corporation*, con sede a Newark (Delaware).

8 Maggiori informazioni sono contenute nell'allegata relazione tecnica (*cfr. pagg. 52 e segg. dell'allegato*

Excerpt from the Italian court order on #EyePyramid
(http://www.agi.it/pictures/pdf/agi/agi/2017/01/10/132733992-5cec4d88-49a1-4a00-8a01-dde65baa5a68.pdf)

Some of the e-mail addresses used for exfiltration and C&C domains outlined by the police report follow:

E-mail Addresses used for exfiltration
gpool@hostpenta[.]com
hanger@hostpenta[.]com
hostpenta@hostpenta[.]com
purge626@gmail[.]com
tip848@gmail[.]com
dude626@gmail[.]com
octo424@gmail[.]com
tim11235@gmail[.]com
plars575@gmail[.]com

Command-and-Control Servers
eyepyramid[.]com
hostpenta[.]com
ayexisfitness[.]com
enasrl[.]com
eurecoove[.]com
marashen[.]com
millertaylor[.]com
occhionero[.]com
occhionero[.]info
wallserv[.]com
westlands[.]com

Based on these indicators we've quickly written a YARA rule and ran it through our systems, in order to see if it matches any samples.

Here's how our initial "blind"-written YARA rule looked like:

```
rule crime_ZZ_EyePyramid {

meta:
```

```
copyright = ” Kaspersky Lab”
author = ” Kaspersky Lab”
maltype = “crimeware”
filetype = “Win32 EXE”
date = “2016-01-11”
version = “1.0”

strings:

$a0=”eyepyramid.com” ascii wide nocase fullword
$a1=”hostpenta.com” ascii wide nocase fullword
$a2=”ayexisfitness.com” ascii wide nocase fullword
$a3=”enasrl.com” ascii wide nocase fullword
$a4=”eurecoove.com” ascii wide nocase fullword
$a5=”marashen.com” ascii wide nocase fullword
$a6=”millertaylor.com” ascii wide nocase fullword
$a7=”occhionero.com” ascii wide nocase fullword
$a8=”occhionero.info” ascii wide nocase fullword
$a9=”wallserv.com” ascii wide nocase fullword
$a10=”westlands.com” ascii wide nocase fullword
$a11=”217.115.113.181″ ascii wide nocase fullword
$a12=”216.176.180.188″ ascii wide nocase fullword
$a13=”65.98.88.29″ ascii wide nocase fullword
$a14=”199.15.251.75″ ascii wide nocase fullword
$a15=”216.176.180.181″ ascii wide nocase fullword
$a16=”MN600-849590C695DFD9BF69481597241E-668C” ascii wide nocase
fullword
$a17=”MN600-841597241E8D9BF6949590C695DF-774D” ascii wide nocase
fullword
$a18=”MN600-3E3A3C593AD5BAF50F55A4ED60F0-385D” ascii wide nocase
fullword
$a19=”MN600-AD58AF50F55A60E043E3A3C593ED-874A” ascii wide nocase
fullword
$a20=”gpool@hostpenta.com” ascii wide nocase fullword
$a21=”hanger@hostpenta.com” ascii wide nocase fullword
$a22=”hostpenta@hostpenta.com” ascii wide nocase fullword
$a23=”ulpi715@gmx.com” ascii wide nocase fullword
$b0=”purge626@gmail.com” ascii wide fullword
$b1=”tip848@gmail.com” ascii wide fullword
$b2=”dude626@gmail.com” ascii wide fullword
$b3=”octo424@gmail.com” ascii wide fullword
$b4=”antoniaf@poste.it” ascii wide fullword
$b5=”mmarcucci@virgilio.it” ascii wide fullword
$b6=”i.julia@blu.it” ascii wide fullword
$b7=”g.simeoni@inwind.it” ascii wide fullword
$b8=”g.latagliata@live.com” ascii wide fullword
$b9=”rita.p@blu.it” ascii wide fullword
$b10=”b.gaetani@live.com” ascii wide fullword
$b11=”gpierpaolo@tin.it” ascii wide fullword
$b12=”e.barbara@poste.it” ascii wide fullword
$b13=”stoccod@libero.it” ascii wide fullword
$b14=”g.capezzone@virgilio.it” ascii wide fullword
$b15=”baldarim@blu.it” ascii wide fullword
$b16=”elsajuliette@blu.it” ascii wide fullword
$b17=”dipriamoj@alice.it” ascii wide fullword
$b18=”izabelle.d@blu.it” ascii wide fullword
$b19=”lu_1974@hotmail.com” ascii wide fullword
$b20=”tim11235@gmail.com” ascii wide fullword
$b21=”plars575@gmail.com” ascii wide fullword
$b22=”guess515@fastmail.fm” ascii wide fullword

condition:

((uint16(0) == 0x5A4D)) and (filesize < 10MB) and
((any of ($a*)) or (any of ($b*)) )
}
```

To build the YARA rule above we’ve used every bit of existing information, such as custom e-mail addresses used for exfiltration, C&C servers, licenses for the custom mailing library used by the attackers and specific IP addresses used in the attacks.

Once the YARA rule was ready, we’ve ran it on our malware collections. Two of the initial hits were:

MD5	778d103face6ad7186596fb0ba2399f2
File size	1396224 bytes
Type	Win32 PE file
Compilation Timestamp	Fri Nov 19 12:25:00 2010

MD5	47bea4236184c21e89bd1c1af3e52c86
File size	1307648 bytes
Type	Win32 PE file
Compilation timestamp	Fri Sep 17 11:48:59 2010

These two samples allowed us to write a more specific and more effective YARA rule which identified 42 other samples in our summary collections.

At the end of this blogpost we include a full list of all related samples identified.

Although very thorough, the Police Report does not include any technical details about how the malware was spread other than the use of spear phishing messages with malicious attachments using spoofed email addresses.

Nevertheless, once we were able to identify the samples shown above we used our telemetry to find additional ones used by the attackers for spreading the malware in spear-phishing emails. For example:

From: **Di Marco Gianmaria**
Subject: **ricezione e attivazione**
Time:**2014/01/29 13:57:42**
Attachment: **contatto.zip//Primarie.accdb (…) .exe**

From**: Michelangelo Giorgianni**
Subject**: R: Re: CONVOCAZIONE]**
Time**: 2014/01/28 17:28:56]**
Attachment**: Note.zip//sistemi.pdf (…) .exe**

Other attachment filenames observed in attacks include:

- Nuoveassunzioni.7z
- Assunzione.7z
- Segnalazioni.doc (…) 7z.exe
- Regione.7z
- Energy.7z
- Risparmio.7z
- Pagati.7z
- Final Eight 2012 Suggerimenti Uso Auricolari.exe
- Fwd Re olio di colza aggiornamento prezzo.exe
- Approfondimento.7z
- Allegato.zip
- Eventi.bmp (…) .exe
- Quotidiano.mdb (…) _7z.exe
- Notifica operazioni in sospeso.exe

As can be seen the spreading relied on spearphishing e-mails with attachments, which relied on social engineering to get the victim to open and execute the attachment. The attachments were ZIP and 7zip archives, which contained the EyePyramid malware.

Also the attackers relied on executable files masking the extension of the file with multiple spaces. This technique is significant in terms of the low sophistication level of this attack.

High profile victims

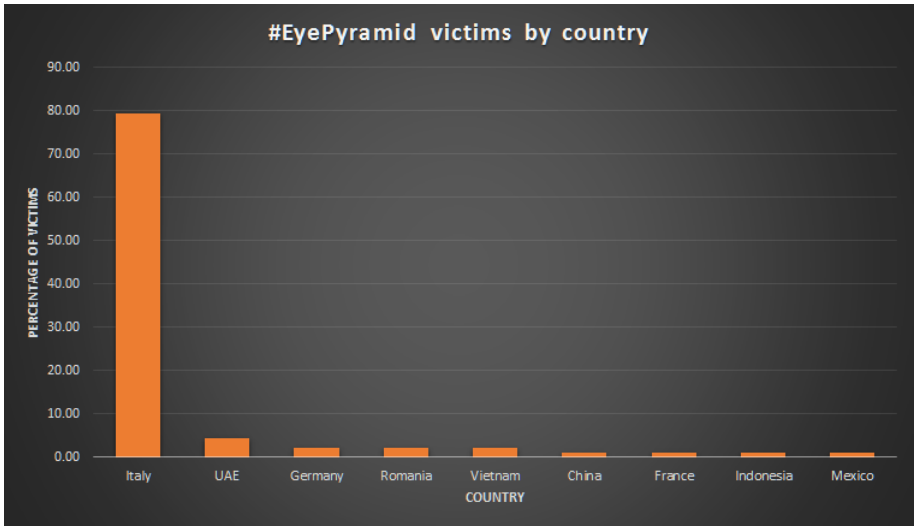
Potential high-profile Italian victims (found as recipients of spear-phishing emails according to the police report) include very relevant Italian politicians such as Matteo Renzi or Mario Draghi.

It should be noted however there is no proof than any of them got successfully infected by EyePyramid – only that they were targeted.

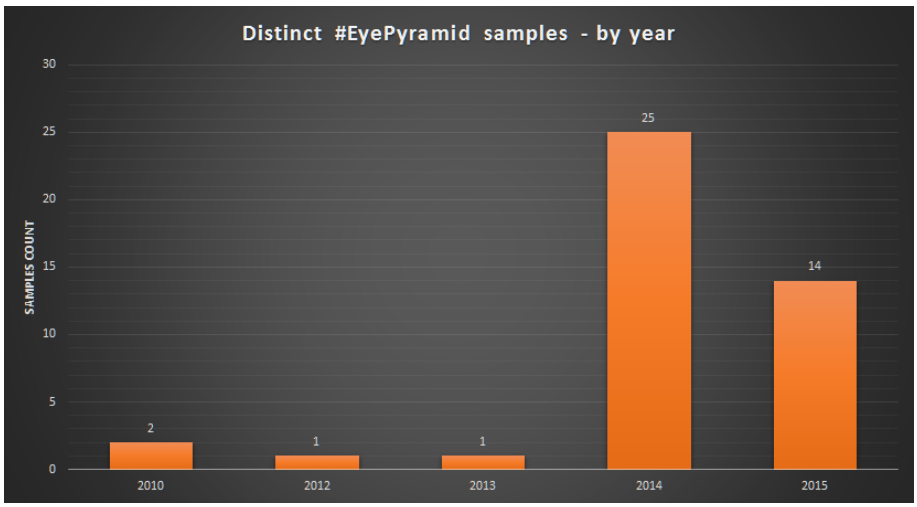
Of the more than 100 active victims found in the server, there’s a heavy interest in Italian law firms and lawyers. Further standout victims, organizations, and verticals include:

Professional firms, Consultants	Universities	Vaticano
Construction firms	Healthcare	

Based on the KSN data for the EyePyramid malware, we observed 92 cases in which the malware was blocked, of which the vast majority (80%) of them were in Italy. Other countries where EyePyramid has been detected includes France, Indonesia, Monaco, Mexico, China, Taiwan, Germany and Poland.



Assuming their compilation timestamp are legit – and they do appear correct, most of the samples used in the attacks have been compiled in 2014 and 2015.



Conclusions

Although the “EyePyramid” malware used by the two suspects is neither sophisticated nor very hard to detect, their operation successfully compromised a large number of victims, including high-profile individuals, resulting in the theft of tens of gigabytes of data.

In general, the operation had very poor OPSEC (operational security); the suspects used IP addresses associated with their company in the attacks, discussed the victims using regular phone calls and through WhatsApp and, when caught, attempted to delete all the evidence.

This indicates they weren’t experts in the field but merely amateurs, who nevertheless succeeded in stealing considerably large amounts of data from their victims.

As seen from other known cyberespionage operations, it’s not necessary for the attackers to use high profile malware, rootkits, or zero-days to run long-standing cyberespionage operations.

Perhaps the most surprising element of this story is that Giulio Occhionero and Francesca Maria Occhionero ran this cyber espionage operation for many years before getting caught.

Kaspersky Lab products successfully detect and remove EyePyramid samples with these verdicts:

- HEUR:Trojan.Win32.Generic
- Trojan.Win32.AntiAV.choz
- Trojan.Win32.AntiAV.ciok
- Trojan.Win32.AntiAV.cisb
- Trojan.Win32.AntiAV.ciyk
- not-a-virus:HEUR:PSWTool.Win32.Generic
- not-a-virus:PSWTool.Win32.NetPass.aku

A full report #EyePyramid, including technical details of the malware, is available to customers of Kaspersky APT Intelligence Services. Contact: intelreports (at) kaspersky [dot] com.

To learn how to write YARA rules like a GReAT Ninja, consider taking a master class at Security Analyst Summit. – https://sas.kaspersky.com/#trainings

References and Third-Party Articles

- http://www.agi.it/pictures/pdf/agi/agi/2017/01/10/132733992-5cec4d88-49a1-4a00-8a01-dde65baa5a68.pdf
- https://ftalphaville.ft.com/2017/01/10/2182125/the-arrested-pair-are-residents-of-london-but-are-domiciled-in-rome-and-are-well-known-in-the-world-of-high-finance/
- http://www.politico.eu/article/mario-draghi-matteo-renzi-mario-monti-victims-of-cyberattacks/
- https://github.com/eyepyramid/eyepyramid
- http://cybersecurity.startupitalia.eu/53903-20170111-eye-pyramid-the-italian-job-storia-malware-spionaggio-massoneria
- http://www.affaritaliani.it/cronache/cyberspionaggio-massoneria-p4-mire-segreti-ecco-chi-sono-gli-spioni-458076.html

Indicators of Compromise

Hashes:

09ff13b020de3629b0547e0312a6c135
102bccd95e5d8a56c4f7e8b902f5fb71
12f3635ab1de63fbcb5e1c492424c605
1391d37c6b809f48be7f09aa0dab7657
1498b8d6e946b5d6b529abea13592381
14db577a9b0bfc62f3a25a9a51765bc5
17af7e00936dcc8af376ad899501ad8b
192d5866cbfafae36d5ba321c817bc14
325f5d379c4d091743ca8581f15d3295
36bd8feed1b17c59f3c653e6427661a4
380b0f1921fed82e1b68b4e442b04f05
3c30f0114c600510fdb2573cc48d5c06
3fed695e2a6e63d971c16fd9e825fec5
47bea4236184c21e89bd1c1af3e52c86
47dd1e017aae694abd2b7bc0b12cf1da
47f1f9b1339147fe2d13772b4cb81030
53b41dc0b8fd9663047f71bc91a317df
5bc1b8c07c0f83d438a3e891dc389954
5eb17f400f38c1b65990a8d60c298d95
6de1e478301d59ac14b8e9636b53815d
75621de46a12234af0bec15620be6763
778d103face6ad7186596fb0ba2399f2
859f60cd5d0f0fbd91bde3c3914cbb18
8afb6488655cbea2737d2423843ea077
9173aefe64b7704510c873e2ce7305e0
92c32eb72f5713ca1f2a8dc918f1f770

932bd2ad79cbca4341d853a4b5ea1da5
94eff87eca2f054aa5fbc1877a6cf919
98825a1ce35f46d004c0839e87cc2778
9b8571b5281f3751750d3099049098e0
9c57839b3f8462bd6c2d36db80cd5ecc
9d3ce3246975ae6d545ee9e8ba12d164
9d4b46d3c389e0144238c821670f8537
a41c5374a14a2c7cbe093ff6b075e8ac
b39a673a5d2ceaa1fb5571769097ca77
b533b082ed1458c482c3663ee12dc3a4
bcfd544df7d8e9a2efe9d2ed32e74cad
c0243741bfece772f02d1657dc057229
c38e9edc0e4b18ff1fc5b61b771f7946
ce76b690dc98844c721e6337cd5e7f4b
cf391937d79ed6650893b1d5fbed0604
d8432ddec880800bfa060af1f8c2e405
eb604e7e27727a410fc226196c13afe9
fafd293065daf126a9ad9562fc0b00b2

Related hashes identified by @GaborSzappanos:

014f69777d2e0c87f2954ad252d52810
02965c8a593989ff7051ec24736da6bd
04b3c63907c20d9be255e167de89a398
04e949f64e962e757f5bb8566c07800b
06e47736256c54d9dd3c3c533c73923e
09ff13b020de3629b0547e0312a6c135
0a80fd5abf270ddd8080f93505854684
0b3c1ff3b3b445f46594227ca2babdcd
0c33c00a5f0f5bde8c426c3ce376eb11
0ded0389cbddeeb673836794269ffb3b
0e19913ce9799a05ba97ac172ec5f0bc
11062b36893c4ba278708ec3da07b1dd
12b4d543ae1b98df15c8712d888c54f0
1334a7df1e59380206841d05d8400778
14cb305de2476365ef02d2226532dd34
1748c33cb5ac6f26d55cd1a58b68df8a
18e24ef2791030693a4588bfcae1dec0
192d5866cbfafae36d5ba321c817bc14
1b4d423350cd1159057dd7dbef479328
1deb28ae7b64fb44358e69e5afd1f600
2222a947ebccc8da16badeacca05df4b
23beed8aaac883a5902039e6fd84ee5f
2485e7ae3e0705898b7787ed0961878d
2642990a46c434e7787a599f04742a32
268698314c854bc483d05ffe459dc540
2866ced99b46b39838f56fbe704d387b
2896ae0489451d32f57c68b919b3fa72
28ba7d1a4c5d64a65f2f2bf5f6ced123
28e65b9577abaabf3f8c94d9fda50fc5
2a809644e6d07dc9fc111804a62b8089
30215197622f5c747fc869992768d9c6
325f5d379c4d091743ca8581f15d3295
33890f9268023cd70c762ad2054078c7
3673c155eb6a0bd8a94bea265ebb8b76
369cd42dfabea188fa57f802a83b55d9
380b0f1921fed82e1b68b4e442b04f05
3a0af8bba61734b043edc0f6c61cd189
3c30f0114c600510fdb2573cc48d5c06
3db711afc09c0a403a8ccff6a8a958df
3e4365b079239b0a2451f48f33761332
3ebbae038d7bf19baa1bcfbc438bb5e7
3fed695e2a6e63d971c16fd9e825fec5
3ffcd0eedd79a9cc79c2c4a0f7e04b21
4025834a88dcfba3ed1774068c64c546
417593eaf61d45e88adbad259d5585d0
422fe9c78c71fb30d376e28ad1c41884
44d91f49f261da6b1f183ea131d12a7f
45dde4082c0407b9904c5f284080337f
47bea4236184c21e89bd1c1af3e52c86

4a494c20bcfb77afd06908eb5a9718cb
53b41dc0b8fd9663047f71bc91a317df
5523aa1d4ee5f19522299be6f1111b89
5627cb8752c4c0774f822ccf8f1363eb
56499e0b590857f73bb54f500008c656
568895c8340a88316fdc0d77a7f2a91d
5847072fd4db9e83d02d8b40a1d67850
5accd89d6483dec54acc7b1484dfbace
5b5f3f65b372f9e24dbc50b21fe31f81
5bc1b8c07c0f83d438a3e891dc389954
622fb530276a639892398410de03d051
63d9e7cca593360411b5d05a555d52f3
6648a255610c5f60f580098bbc1d387c
690cdf20faf470f828fe468a635da34e
6c25a0974a907d368372ac460d8261d6
6c5693df933924e8a633ccfd7ef2635d
6ff7876db06d9102786ae0e425aeaf37
70882709d86e2a7396779f4111cd02e3
70f094e347d4088573c9af34430a3cd6
72ffb3418d3cde6fdef16b5b5db01127
734cfa84d68506fe6e74eb1b038d9c70
7633748203b705109ededadfbe08dcfa
778d103face6ad7186596fb0ba2399f2
77c2a369d0850c7a75487e8eee54b69e
78b7d1caa4185f02b1c5ef493bf79529
7971c90d7533f2c69e33f2461434096a
7aad90ce44e355f95b820fb59c9f5d56
7bf348005958658ba3fcf5ccb3e2ae22
7cddc3b26bb8f98e9b14d9c988f36f8f
81624dc108e2d3dc712f3e6dd138736a
820ca39f331f068cca71e7a7c281e4ac
84c14a1327ae7c0e5a07a67a57451cc4
860f607dbd0d6a2dc69cbc4f3b0eeeaf
889c86aaf22876516964eafa475a2acd
88c31f3b589d64a275608f471163989c
89368652dc98b13f644ec2e356c7707c
89696dbead484bf948c1dd86364672eb
898150dea4d7275f996e7341463db21f
8b27bcfa38205754c8e5fdf6a509d60e
8f419bca20b767b03f128a19b82611ab
915cc3c9c8cb8e200dbe04e425e7018b
92c32eb72f5713ca1f2a8dc918f1f770
932bd2ad79cbca4341d853a4b5ea1da5
98825a1ce35f46d004c0839e87cc2778
98b1157b9f3f3ec183bf322615f1ce41
9b19729531bf15afc38dd73bcc0596f8
9c99ecf33301e4cafdd848a7d3d77ef9
9cf08b15724e0eaf69a63e47690cdee2
a16d8cf9a7a52e5c2ad6519766ae6b92
a35312a5c0b06ee89ddadaea9ca6bad2
a4c551ec6d3b5ab08a252231439e099f
a615a4f5e93a63682a8f25b331f62882
a6c29f9680fe5ae10a9250e5431754d4
ab71ca072d4b526e258c21bd84ec0632
ac6fa4005e587ac4b3456a14bd741ff0
afab0fcbf8bc6595f9f2c0051b975a4e
b1ddec2f71727dcf747e1d385272e24d
b2a756f557d273d81a61edc9fbfc9daf
b2e1663647addc92bf253f389ac98027
b39a673a5d2ceaa1fb5571769097ca77
b533b082ed1458c482c3663ee12dc3a4
b6e86ac7d3bbedf18b98437df49c1b60
b70ddb9f6e4e2c85e80cf2079b10e762
b89a8d3442d96161cef07552116407c3
bb2a0aee38980aeb39cac06677936c96
bc333001d3f458ff8fde9d989b53e16d
bd7a2b795419c0b842fd041eaac36d7f
bf850dcb074e0cf2e30fbee6bfaa4cd9
c0d4e5ba26ef3c08dc1a29ac7496f015
c38832f484645b516b57f6813c42d554
c4abb3210f26d4a15a0d4fd41b47ee0e

c547a30fa39f22e2093b51ed254bb1c2
c69c370fcb7b645aaac086b2a3b18286
c7ef4c7b12b5ad8198dafc58c4bea2a3
c97ef1f13bf3d74c78f50fa7abe7766b
ca010bcdfe3c4965df0c6bc12b40db76
ca243796e79c87c55f67a61bc3ee8ddc
ca9a7c6b231fadfae3466da890b434c5
cf391937d79ed6650893b1d5fbed0604
cf3b3c796114f6908a35542d4fd02b0e
d034810ddab55c17dcddd2c2990b3ef3
d1273537add3f2282391726489c65e38
d20487e2d2f674bfd849cb8730225dde
d8432ddec880800bfa060af1f8c2e405
d864ad5030d354c1e40a873a335b2611
dac10dcede69eb9b4ccce8e6798f332c
db95221ebed1793bf5b5527ecb52eb0c
dc64307ef67177449b31c6bb829edbf2
dd734c07b94c8685bb809f83876c7193
e0e862dbf001eb4a169d3340c200b501
e727b444a6a9fa9d40a34a9508b1079f
e7539ed9616b61c12028a663c298f6be
e78ed9fac4f3e9b443abd02bfa9f3db2
e85ff9e3a27899b0d1de8b958af5ad90
eb604e7e27727a410fc226196c13afe9
eba8aa2572cf0d6ccdf99c34cc26b6f3
ec21252421f26072e9fe75586eb6b58a
ee9435593494f17f3efc3a795c45482e
eeca6409dcf0e46d0182d53d230c701d
eff2d3f9f56e9aabcf970c4c09fe7ef8
f0b61a531a72f0cc02d06d2ebfb935ab
f1a037e2edc5ddf4db4e1e7fcd33d5fb
f3802442727c0b614482455d6ad9edc2
f41be516fa8da87a269845c9ea688749
f7d4742d2e746962440bf517b261f126
f96335bf0512c6e65ea374a844ab7ceb
f9b4459f18ca9d2974cf5a58495c5879
fa4266c305aa75a133ebae2a4dcc9b75
fafd293065daf126a9ad9562fc0b00b2

Backdoor Filenames:

pnbwz.exe
pxcfx.exe
qislg.exe
rqklt.exe
runwt.exe
ruzvs.exe
rvhct.exe
vidhdw.exe
winlng.exe
wxrun.exe
xddrv.exe
xdwdrv.exe

Malicious attachments filenames (weak indicators):

contatto.zip//Primarie.accdb (…) .exe
Note.zip//sistemi.pdf (…) .exe
Nuoveassunzioni.7z
Assunzione.7z
Segnalazioni.doc (…) 7z.exe
Regione.7z
Energy.7z
Risparmio.7z
Pagati.7z
Final Eight 2012 Suggerimenti Uso Auricolari.exe
Fwd Re olio di colza aggiornamento prezzo.exe
Approfondimento.7z
Allegato.zip

Eventi.bmp (…) .exe
Quotidiano.mdb (…) _7z.exe

Related Posts

INPAGE ZERO-DAY EXPLOIT USED TO ATTACK FINANCIAL INSTITUTIONS IN ASIA

KASPERSKY SECURITY BULLETIN. PREDICTIONS FOR 2017

KASPERSKY LAB BLACK FRIDAY THREAT OVERVIEW 2016