

Jan 17 Trojan Darkmoon.B EXE Haiti relief from santi_nidas@yahoo.com 17 Jan 2010 13:15:02 -0800 PST

contagiodump.blogspot.com/2010/01/jan-17-trojan-darkmoonb-exe-haiti.html



This message contains a zip attachment with ârâfâl.exe (Darkmoon.B) and a 20100118.pdf (containing pictures).



[Download the A4754BE7B34ED55FAFF832EDADAC61F6 -Darkmoonb.zip \(password protected< please contact me if you need it\)](#)

The message is in Japanese



From: santi_nidas@yahoo.com [mailto:santi_nidas@yahoo.com]
Sent: Sunday, January 17, 2010 4:15 PM
To: xxxxxxxxxxxx
Subject: ハイチの救援活動が難航 7千人埋葬、時間との勝負

ハイチの救援活動が難航 7千人埋葬、時間との勝負

【ポルトープランス共同】大地震発生から2日が経過したハイチでは14日、現地入りした欧米の救援チームが倒壊家屋の下敷きになった被災者の捜索活動を始めるなど、国際的な救援活動が本格化した。しかし、人員や医薬品が不足し活動は難航している。

ロイター通信によると、プレバル・ハイチ大統領は同日、地震による死者約7千人が既に墓地に埋葬されたと述べた。国連の潘基文事務総長は「発生後、72時間が鍵だ」と述べ、時間との勝負になっていることを強調した。

国連や米CNNテレビによると、米の救援チームが14日朝、首都ポルトープランスで倒壊した平和維持活動(PKO)部隊の本部ビルに下敷きになっていたエストニアの警備要員の男性(38)を救助。現地には災害救助犬を連れたフランス隊のほか、スペイン、ドミニカ共和国などの救援チームが続々と到着、活動を始めた。事務総長は「今後、各国からさらに派遣される」と語った。

被災地では医師、医療品不足が深刻化。国連や各国は救援物資の運搬、配布に全力を挙げる方針だ。ただ、ロイター通信によると、甚大な被害を受けたポルトープランスの空港は人員や物資を運ぶ航空機で満杯状態となり、米連邦航空局(FAA)は米国から同空港への飛行を当面見合わせるよう指示した。

Subject: Haiti relief deadlock seven people buried in 1000, race against time

Haiti's troubled rescue seven people buried in 1000, race against time [Co] from a large earthquake in Port au Prince in Haiti two days after the 14th, and now he will begin his search for victims buried under collapsed houses in the West entered the local rescue team, the international relief activities in earnest. However, a lack of activity and medical personnel are faced with difficulties.



According to Reuters, the president said pre-Barbera Haiti, said seven were killed by the earthquake that buried thousands of people already.

UN Secretary General Ban Ki-moon "after a failure, but 72 hours is key," and emphasized that it is a race against time.

CNN television said the United Nations and the United States, North Korea has 14 rescue teams in the U.S., collapsed in the capital Port peacekeeping operations (PKO) security personnel in Estonia men had been buried in the headquarters of the troops (38) rescued the . In addition to the local disaster relief team with a dog on France, Spain, Dominican Republic, such as rescue teams continued to arrive and we started to work.

Secretary-General "We will also be dispatched from the country," he said.

Doctors in disaster areas, a shortage of medical supplies. The United Nations and international transportation of relief supplies, we will make a concerted effort to distribute. However, according to Reuters, the airport of Port-au-affecté state and became filled with enormous aircraft carrying personnel and supplies, Federal Aviation Administration (FAA) has asked to postpone the airport's flight from the U.S. did.

Headers

Received: from (santi_nidas@218.67.131.82 with login)
by smtp113.plus.mail.sp1.yahoo.com with SMTP; 17 Jan 2010 13:15:02 -0800 PST
X-Yahoo-SMTP: APkRSTKswBAItjtRmEcOWOvp0HAuXtE8
X-YMail-OSG:
6TNaz1oVM1nFg57xH0ABi34Uqp874reW9HI.vvjrQ6E1lzS13PFJujNh3DivLqjPCewT1TINsHkCsU8adegb_w2ZTtwgc0YPhZmye5uDpETKWVa_R
X-Yahoo-Newman-Property: ymail-5
Message-ID:

Hostname: 218.67.131.82
ISP: China Unicom Tianjin province network
Organization: China Unicom Tianjin province network
Country: China
City: Tianjin
Latitude: 39.1422
Longitude: 117.1767

âĖĖfâĖĖ.exe

<http://www.virustotal.com/analysis/81d634888b069313492b30f737ed07085f335d1cc29964050514412bf5d4b7d1-1263879006>

File_r_f_l.exe received on 2010.01.19 05:30:06 (UTC)

Result: 14/41 (34.15%)

Antivirus	Version	Last Update	Result
AhnLab-V3	5.0.0.2	2010.01.18	Win-Trojan/Agent.45056.AMQ
Antiy-AVL	2.0.3.7	2010.01.18	Trojan/Win32.Agent.gen
Avast	4.8.1351.0	2010.01.18	Win32:Malware-gen
CAT-QuickHeal	10.00	2010.01.19	Trojan.Agent.cvpr
Comodo	3632	2010.01.19	TrojWare.Win32.Trojan.Agent.~IAZ
DrWeb	5.0.1.12222	2010.01.19	Trojan.Siggen.27190
F-Secure	9.0.15370.0	2010.01.19	Trojan:W32/Agent.LGJ
GData	19	2010.01.19	Win32:Malware-gen
Jiangmin	13.0.900	2010.01.18	Trojan/Agent.cule
Kaspersky	7.0.0.125	2010.01.19	Trojan.Win32.Agent.dbzx
nProtect	2009.1.8.0	2010.01.18	Trojan/W32.Agent.45056.TM
Sophos	4.49.0	2010.01.19	Troj/DarkMoon-B
TrendMicro	9.120.0.1004	2010.01.19	BKDR_POISON.SME
ViRobot	2010.1.19.2143	2010.01.19	Trojan.Win32.Agent.45056.HO

Additional information

File size: 45056 bytes

MD5...: a4754be7b34ed55faff832edadac61f6

PDF inside zip

File **20100118.pdf** received on 2010.01.19 05:30:36 (UTC)

<http://www.virustotal.com/analysis>

/27f63881ec53b66e863cc91bef587ab52d51a04f9771a4c0a5215f41d38d60d3-1263879036

Current status: finished



Result: 0/41 (0%)