Trend Micro ServerProtect Compressed File Scanning Bypass

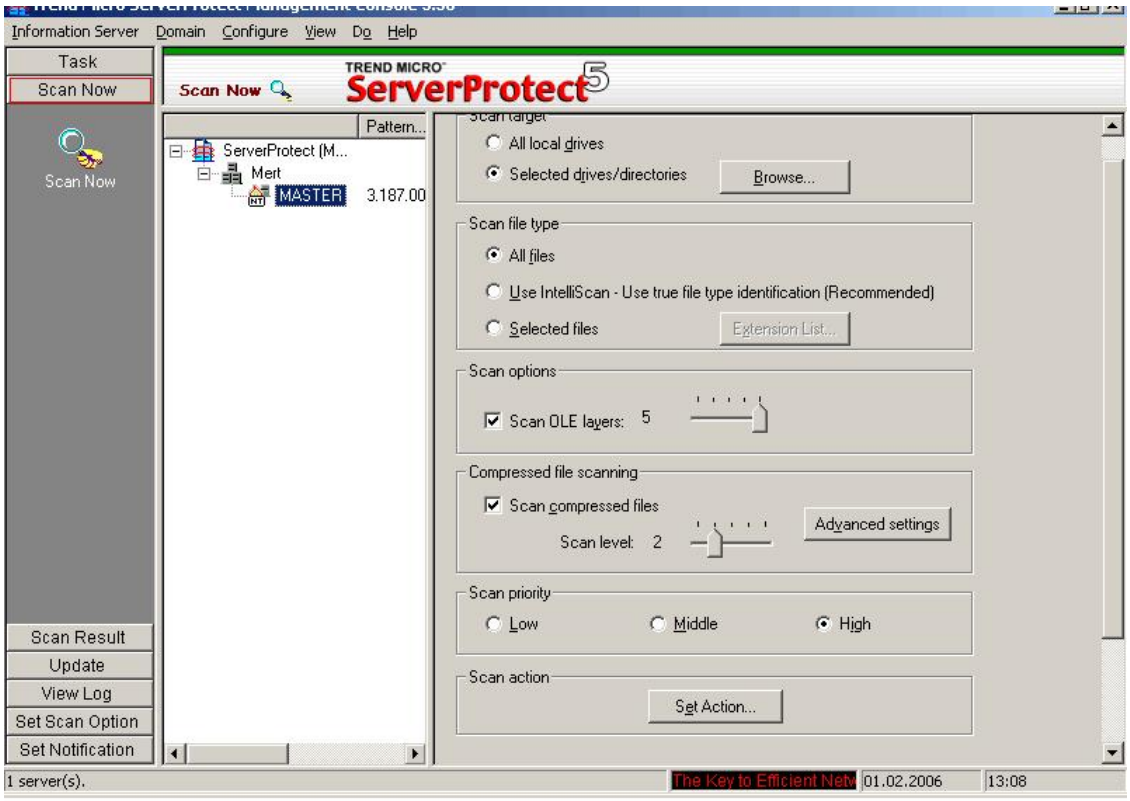
I. Background

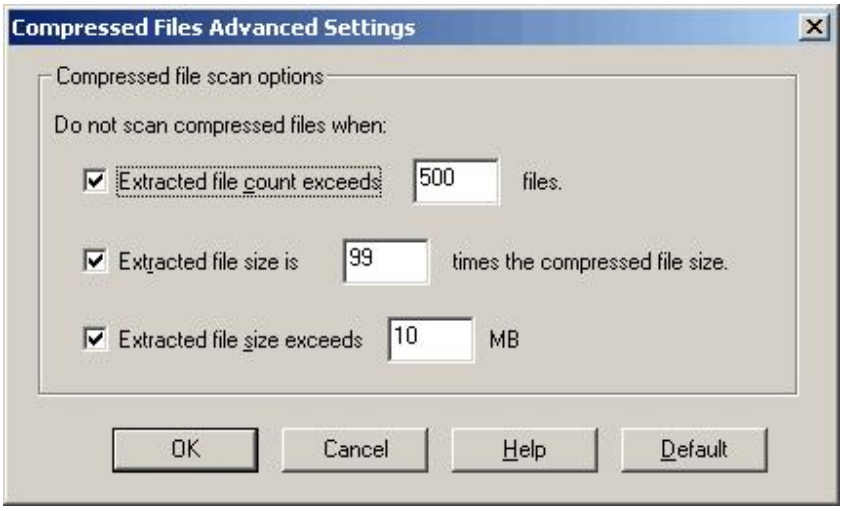
Trend Micro Incorporated is a global leader in network antivirus and Internet content security software and services. Founded in 1988 by Steve Chang, the company led the migration of virus protection from the desktop to the network server and the Internet gateway, gaining a reputation for vision and technological innovation along the way. Trend Micro focuses on outbreak prevention and providing customers with a comprehensive approach to managing the outbreak lifecycle and the impact of network worms and virus threats to productivity and information through initiatives such as Trend Micro™ Enterprise Protection Strategy.

The Key to Efficient Network Antivirus Management ServerProtect for NT/Netware provides network-wide, comprehensive antivirus scanning for servers running the Microsoft™ Windows™ 2000, Microsoft Windows NT™, and Novell™ NetWare™ operating systems. Managed through an intuitive, portable console, ServerProtect provides virus outbreak management, centralized virus scanning, virus pattern file updates, event reporting, and antivirus configuration.

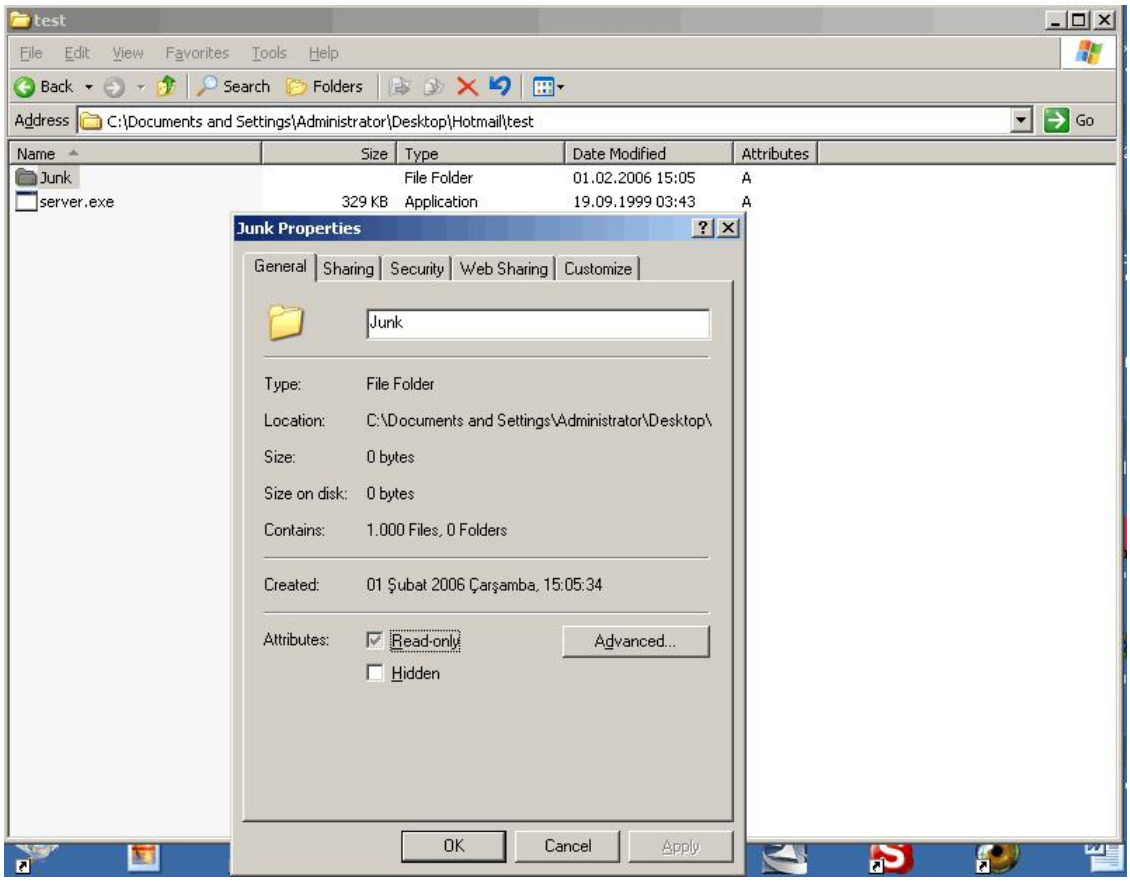
II. Description

Default Settings

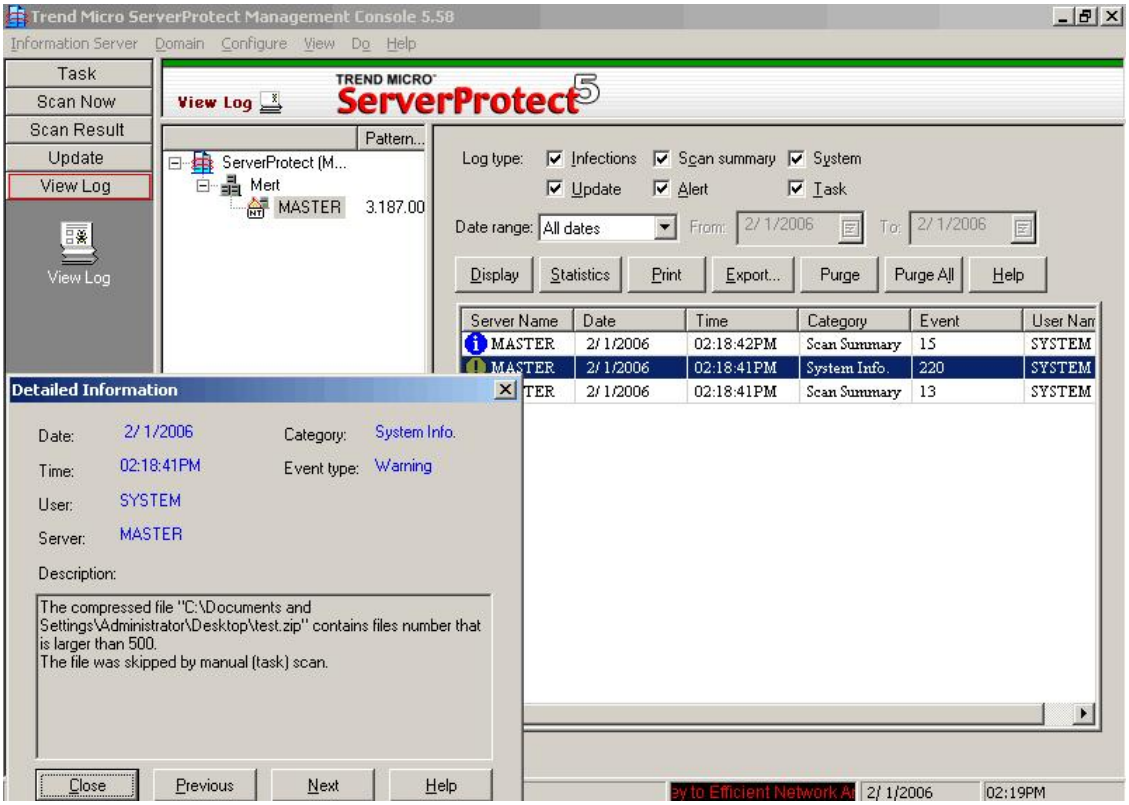


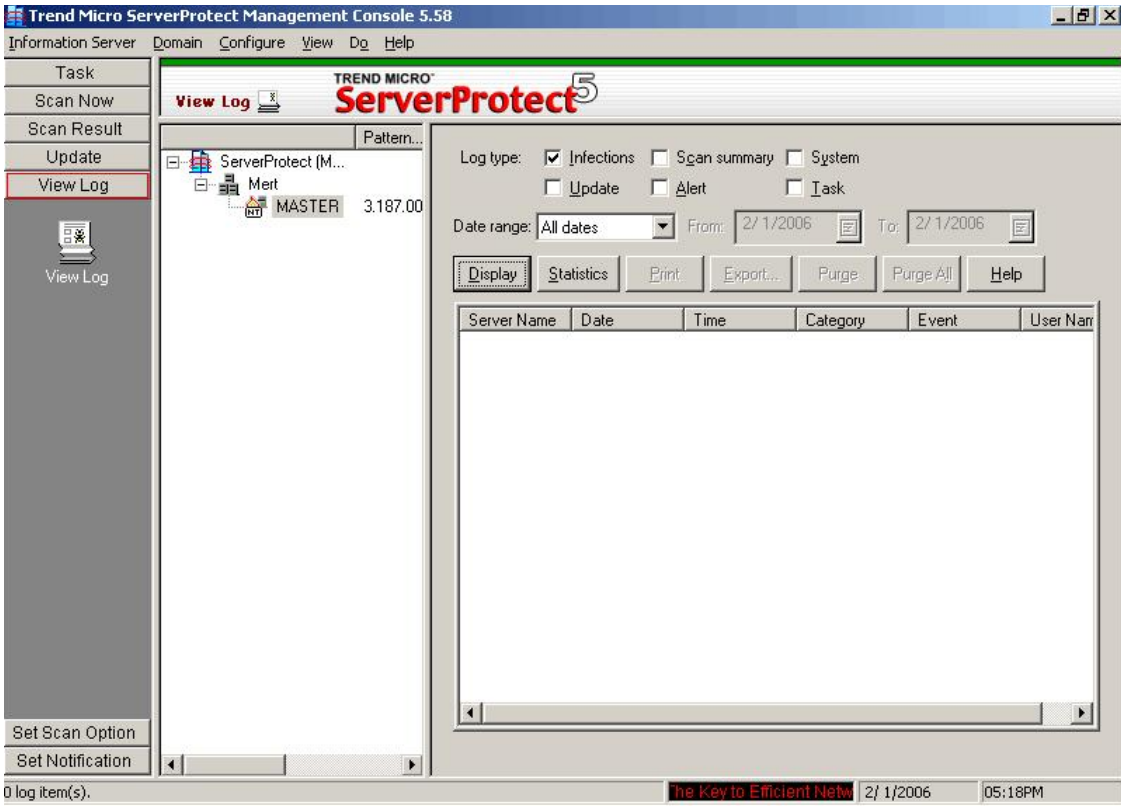


As you see default value for **extracted file count exceeds** is **500** files. What happens if an attacker creates a folder like "**Test**" then creates a folder in it like "**Junk**" then make that folder hidden and then puts **500+** empty text files in it and finally puts a virus or trojan in "**Test**" folder and then zips it? The answer is harmful file can easily be bypassed by the antivirus real-time and manual scan.

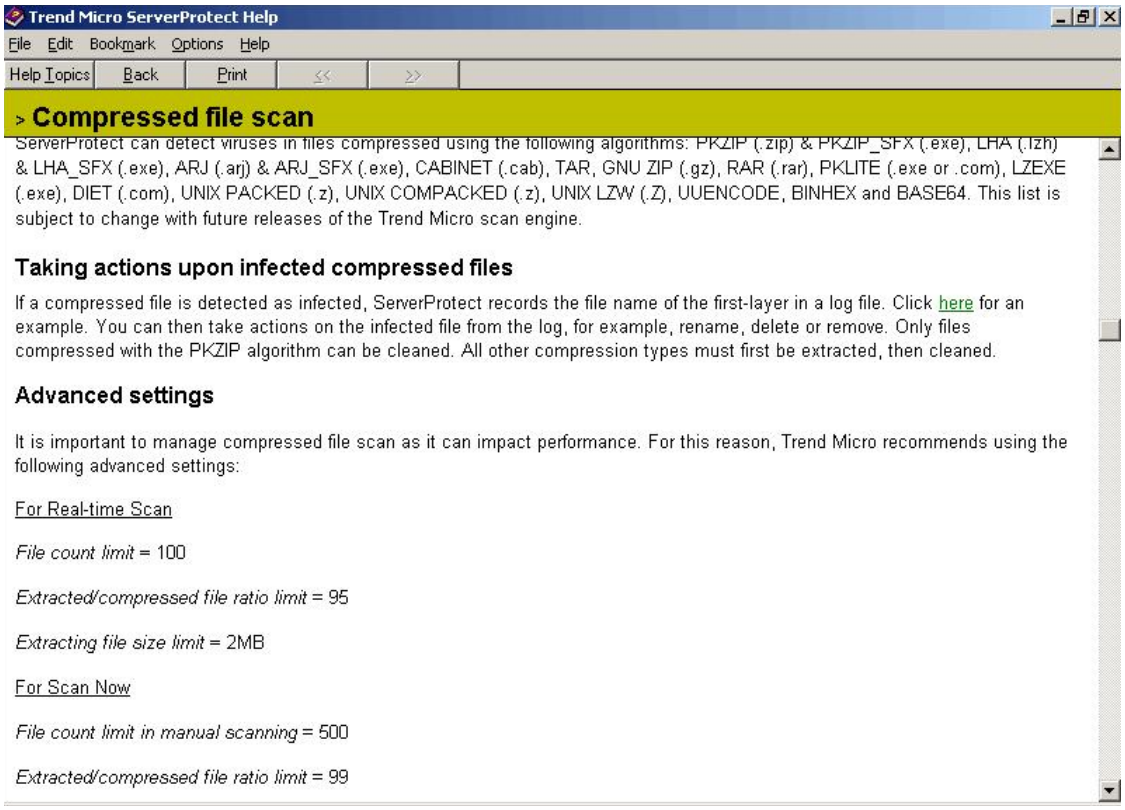


I used Subseven 2.0 server.exe (**332 KB**) as a harmful file in my test. Here is the result of manual scan on **Trend Micro ServerProtect v5.58**

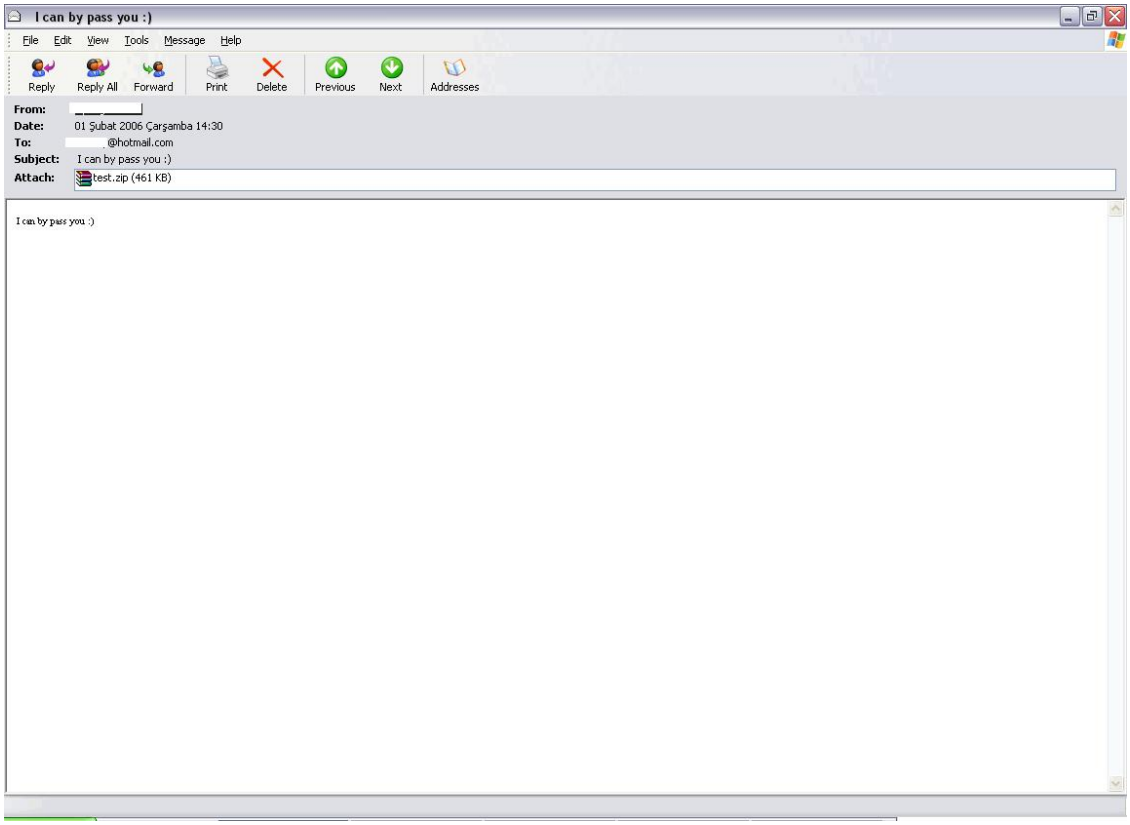

Trend Micro ServerProtect Management Console 5.58
Information Server Domain Configure View Do Help
Task
Scan Now
Scan Result
Update
View Log
View Log
TREND MICRO
ServerProtect 5
Pattern...
ServerProtect (M...
Mert
MASTER 3.187.00
Log type: Infections Scan summary System
Update Alert Task
Date range: All dates From: 2/ 1/2006 To: 2/ 1/2006
Display Statistics Print Export... Purge Purge All Help
Server Name Date Time Category Event User Nam
MASTER 2/ 1/2006 02:18:42PM Scan Summary 15 SYSTEM
MASTER 2/ 1/2006 02:18:41PM System Info. 220 SYSTEM
TER 2/ 1/2006 02:18:41PM Scan Summary 13 SYSTEM
Detailed Information
Date: 2/ 1/2006
Category: System Info.
Time: 02:18:41PM
Event type: Warning
User: SYSTEM
Server: MASTER
Description:
The compressed file "C:\Documents and Settings\Administrator\Desktop\test.zip" contains files number that is larger than 500.
The file was skipped by manual (task) scan.
Close Previous Next Help
ey to Efficient Network Ar 2/ 1/2006 02:19PM


Trend Micro ServerProtect Management Console 5.58
Information Server Domain Configure View Do Help
Task
Scan Now
Scan Result
Update
View Log
View Log
TREND MICRO
ServerProtect 5
Pattern...
ServerProtect (M...
Mert
MASTER 3.187.00
Log type: Infections Scan summary System
Update Alert Task
Date range: All dates From: 2/ 1/2006 To: 2/ 1/2006
Display Statistics Print Export... Purge Purge All Help
Server Name Date Time Category Event User Nam
Set Scan Option
Set Notification
0 log item(s).
The Key to Efficient Netw 2/ 1/2006 05:18PM

Let's see what **Trend Micro** recommends...



After all, I remembered that **Hotmail** uses **Trend Micro**. So did some tests and verified that Hotmail users who use **Outlook** and **Outlook Express** for receving mails are afftected. Hotmail web users are not affected.




```
X-Message-Info: JGTYoYF78jEHjJx360i8+Z3TmmkSEdPt4iogl2abg+M=
Received: from omc1-s18.bay6.hotmail.com ([65.54.248.220]) by bay0-mc4-f17.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.211);
       Wed, 1 Feb 2006 04:31:05 -0800
Received: from hotmail.com ([64.4.19.76]) by omc1-s18.bay6.hotmail.com with Microsoft SMTPSVC(6.0.3790.211);
       Wed, 1 Feb 2006 04:30:52 -0800
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
       Wed, 1 Feb 2006 04:30:52 -0800
Message-ID: <BAY109-DAV4D2E07BF3F3489DC2B65BDB0B0@phx.gbl>
Received: from  by BAY109-DAV4.phx.gbl with DAV;
      Wed, 01 Feb 2006 12:30:52 +0000
X-Originating-IP: [ ]
X-Originating-Email: [ @hotmail.com]
X-Sender: @hotmail.com
From: =?iso-8859-9?Q? _ ?= < @hotmail.com>
To: < @hotmail.com>
Subject:  I can by pass you :)
Date: Wed, 1 Feb 2006 14:30:32 +0200
MIME-Version: 1.0
Content-Type: multipart/mixed;
      boundary="----=_NextPart_000_00A2_01C6273C.0EBD8420"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180
X-OriginalArrivalTime: 01 Feb 2006 12:30:52.0951 (UTC) FILETIME=[575E4270:01C6272B]
Return-Path: @hotmail.com

This is a multi-part message in MIME format.

------=_NextPart_000_00A2_01C6273C.0EBD8420
Content-Type: multipart/alternative;
      boundary="----=_NextPart_001_00A3_01C6273C.0EBD8420"


------=_NextPart_001_00A3_01C6273C.0EBD8420
Content-Type: text/plain;
      charset="iso-8859-9"
Content-Transfer-Encoding: quoted-printable

I can by pass you :)

------=_NextPart_001_00A3_01C6273C.0EBD8420
Content-Type: text/html;
      charset="iso-8859-9"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =
charset=3Diso-8859-9">
```

III. Version

Only tested on **Trend Micro ServerProtect v5.58**.

IV. Author

Mert SARICA < mert.sarica@gmail.com >