

Limpeza do WORM_DOWNAD (Conficker)

Apelidos: Worm Downad (TrendMicro); W32.Downadup (Symantec); Mal/Conficker-A (Sophos); W32/Conficker.worm.gen.a (McAfee); Worm:Win32/Conficker.B (Microsoft); Net-Worm.Win32.Kido.cp (Kaspersky); W32/Conficker.C.worm (Panda); Virus identified I-Worm/Generic.CON (AVG)

Necessariamente todos estes procedimentos, precisam ser seguidos criteriosamente, para conter e limpar o WORM_Downad e suas possíveis variantes.

- 1- Habilitar o **Firewall** do OSCE, pois o mesmo contém listas de ataques contra vírus de rede. Isto verificará as conexões anormais existentes na rede/máquinas, bloqueando automaticamente e impedindo a proliferação do Worm através máquinas vulneráveis da rede.
- 2- Habilitar o **Web Reputation Services** do OSCE, impedindo que máquinas vulneráveis possam realizar a atualização (download) do próprio Worm através de sites maliciosos.
- 3- Todas as máquinas da rede precisam estar com **patch de segurança da Microsoft** (<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>) instalados e obrigatoriamente realizar o reinício após a instalação desse patch.

Observações:

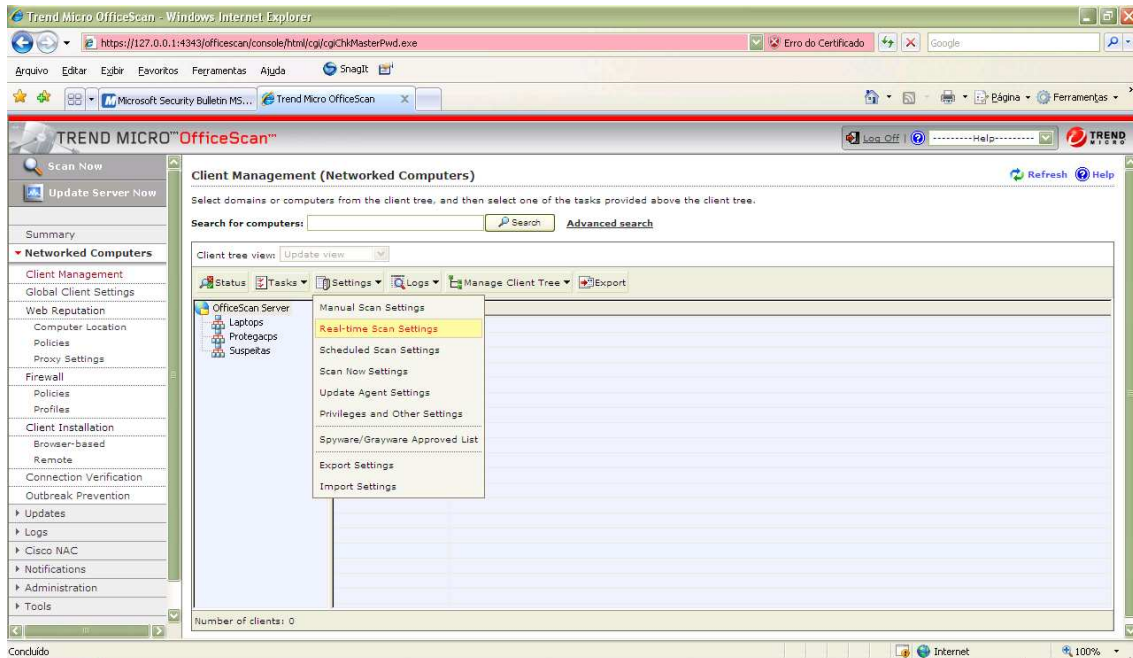
*O malware Worm_Downad “engana” o WSUS em alguns casos. Se a máquina já estiver infectada ela poderá informar que a mesma já está com o patch atualizado, por isso, verifiquem localmente nas estações (Add/Remove Programs > **KB958644**) se possui a instalação deste patch.*

Dependo da versão do sistema operacional, deverá realizar o download através de outro link específico.

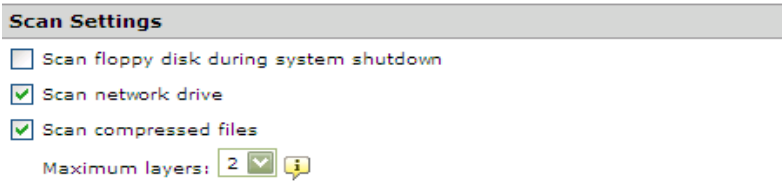
- 4- OBRIGATORIAMENTE, consultar se todas as estações possuem client do OfficeScan instalados e se estão atualizados com as últimas versões disponíveis para detecção e limpeza do malware:
 - OfficeScan Client versão 7.3 e 8.0: Versão superior da pattern **5.885.00**
 - OfficeScan Client versão 7.3: Versão de engine **8.913**
 - OfficeScan Client versão 8.0: Versão de engine **8.911**
 - OfficeScan Client versão 7.3 e 8.0: Versão superior do Damage Cleanup Engine (DCE) **6.0.1172**
 - OfficeScan Client versão 7.3 e 8.0: Versão superior do Damage Cleanup Template (DCT) **1002**
 - OfficeScan Client versão 8.0: Versão superior da pattern do firewall **10274**

5 - Configure o real-time scan, para quando houver acesso as pastas compartilhadas na rede, realize um scan dinâmico que removerá o Worm automaticamente desta pasta.

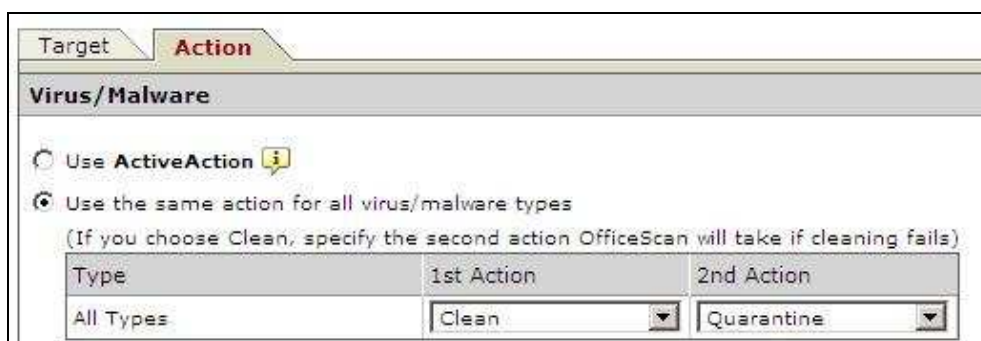
Acessando o console; **Networked Computers -> Client Management -> OfficeScan Server -> Settings -> Real-time Scan Settings.**



6 - Menu **Target** na opção **Scan Settings**, deixar marcada a opção **Scan network drive**, conforme figura abaixo.



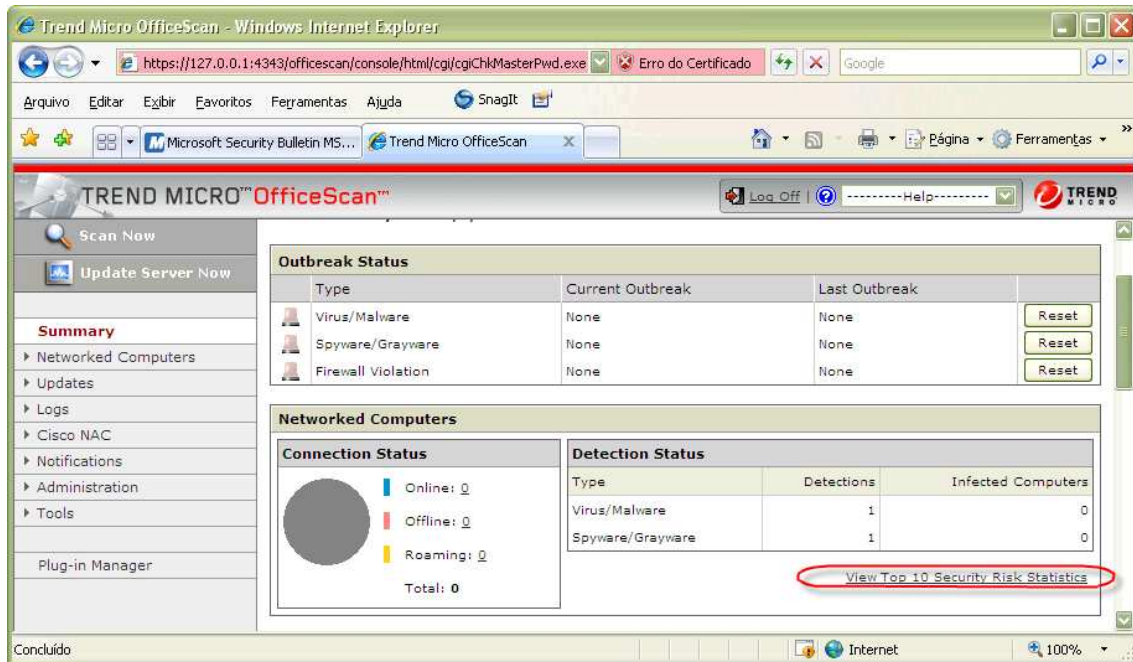
7 - No menu **Action**, opções de configuração **Vírus/Malware**, marcar a opção **Use the same action for all virus/malware types** e em 1st Action marcar a opção **Clean** e 2st Action marcar **Quarantine**, conforme figura abaixo.



8 - Após configurar, clicar em **Apply to All Clients**

9 - Executar um SCAN COMPLETO em toda rede (estações e servidores).

10 - Verifique em **Summary** e **TOP 10 Security Risk Statistics** se as máquinas listadas em **Infection Source**, receberam todos os procedimentos executado acima.

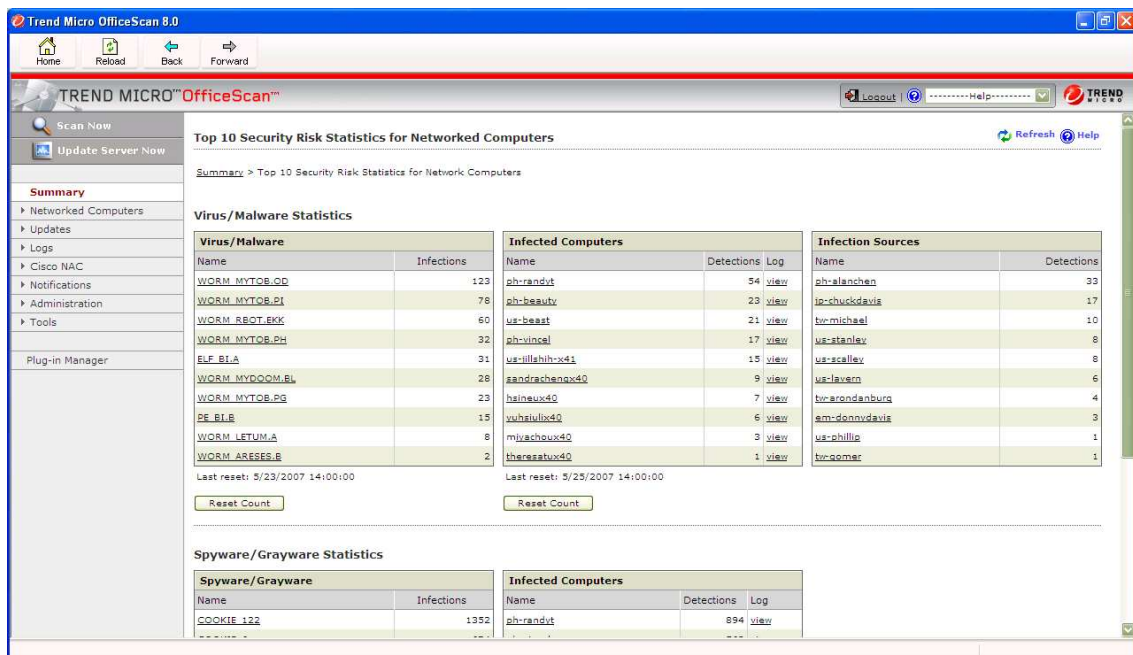


The screenshot shows the Trend Micro OfficeScan console interface. The 'Outbreak Status' section displays a table with columns for Type, Current Outbreak, and Last Outbreak. The 'Networked Computers' section includes a 'Connection Status' pie chart and a 'Detection Status' table. A red circle highlights the 'View Top 10 Security Risk Statistics' link.

Type	Current Outbreak	Last Outbreak
Virus/Malware	None	None
Spyware/Grayware	None	None
Firewall Violation	None	None

Type	Detections	Infected Computers
Virus/Malware	1	0
Spyware/Grayware	1	0

11 – Caso haja dúvidas da limpeza do Worm_Downad, envie ao Suporte Protega e um screenshot das máquinas listadas em **Infection Source** e o Log Completo do Virus/Malware atual de toda a rede.



The screenshot shows the 'Top 10 Security Risk Statistics for Networked Computers' page. It includes sections for Virus/Malware Statistics and Spyware/Grayware Statistics, each with a table of detected items and infected computers.

Name	Infections
WORM_MYTOB_OD	123
WORM_MYTOB_PI	78
WORM_RBOT_EKK	60
WORM_MYTOB_PH	32
ELF_BLA	31
WORM_MYDOOM_BL	28
WORM_MYTOB_PG	23
PE_BLB	15
WORM_LETUM_A	8
WORM_ARESESE_L	2

Name	Detections
ph-randy	54
ph-beauty	23
us-beast	21
ph-inceal	17
us-illshih-w4i	15
sandrashepaq40	9
haineux40	7
yuhaiubx40	6
mjaychoux40	3
theresatux40	1

Name	Detections
ph-alanshen	33
ip-chuckdavis	17
tw-michael	10
us-stanley	8
us-calley	8
us-lavern	6
tw-arondanbura	4
em-donnodavis	3
us-philip	1
tw-gomac	1