Virustotal analysiert verdächtige **Dateien und erleichtert die schnelle Erkennung** von Viren, Würmern, Trojanern und jeglicher Art von Malware, welche von den Antivirus-Engines festgestellt werden.

Datei **Test.exe** empfangen **2008.05.03 06:43:54 (CET)**
Status: **Beendet**
Ergebnis: **1/30 (3.34%)**

Antivirus	Version	letzte aktualisierung	Ergebnis
AhnLab-V3	2008.5.3.0	2008.05.02	-
AntiVir	7.8.0.11	2008.05.02	-
Authentium	4.93.8	2008.05.02	-
Avast	4.8.1169.0	2008.05.03	-
AVG	7.5.0.516	2008.05.03	-
BitDefender	7.2	2008.05.03	-
CAT-QuickHeal	9.50	2008.05.02	-
ClamAV	None	2008.05.02	-
DrWeb	4.44.0.09170	2008.05.03	-
eTrust-Vet	31.3.5755	2008.05.03	-
Ewido	4.0	2008.05.02	-
F-Prot	4.4.2.54	2008.05.02	-
F-Secure	6.70.13260.0	2008.05.02	-
Fortinet	3.14.0.0	2008.05.02	-
Ikarus	T3.1.1.26	2008.05.03	-
Kaspersky	7.0.0.125	2008.05.03	-
McAfee	5287	2008.05.02	-
Microsoft	None	2008.04.22	-

NOD32v2	3072	2008.05.03	-
Norman	5.80.02	2008.05.02	-
Panda	9.0.0.4	2008.05.03	-
Prevx1	V2	2008.05.03	-
Rising	20.42.22.00	2008.04.30	-
Sophos	4.29.0	2008.05.03	-
Sunbelt	3.0.1097.0	2008.05.01	-
Symantec	10	2008.05.03	-
TheHacker	6.2.92.299	2008.05.03	-
VBA32	3.12.6.5	2008.05.02	-
VirusBuster	4.3.26:9	2008.05.02	-
Webwasher-Gateway	6.6.2	2008.05.03	Virus.Win32.FileInfector.gen!80 (suspicious)

weitere Informationen

File size: 5120 bytes

MD5...: 3eff59e55776bfb55d4e988c1f9b27d5

SHA1..: 0f102637d4092bfdaa8f1656e2a3481544969271

SHA256: 3da3cdc3be690803cccd10f9851c9bb30c031fdebcd482596fdd29296343d334

SHA512: 0de4e16c5ebb27fa2ef1bac908c658d019660cb45814fe5c89eb9d471f3b061e
0a316f7baf53a628279f146f23099c8db1af0fce74a49cfec20d8da0056c6fe4

PEiD..: PureBasic 4.x -> Neil Hodgson

PEInfo: PE Structure information

```
( base data )
entrypointaddress.: 0x401000
timedatestamp.....: 0x481bea7d (Sat May 03 04:30:53 2008)
machinetype.......: 0x14c (I386)

( 4 sections )
name viradd virsiz rawdsiz ntrpy md5
.code 0x1000 0x96 0x200 1.35 2872bd475091ee779f1a64f71b3f4ea0
.text 0x2000 0x2be 0x400 4.23 3da35ce9b6019c322d1b3be29d9d6fff
.data 0x3000 0x4d4 0x600 3.96 db14fe40816cb90d9be387d36cdfc1ea
.rsrc 0x4000 0x2b8 0x400 4.08 f743910c204cb4352b6252932588bf7e

( 5 imports )
> CRTDLL.dll: memset
> KERNEL32.dll: GetModuleHandleA, HeapCreate, HeapDestroy, ExitProcess,
GetCurrentThreadId, GetCurrentProcessId, HeapAlloc, HeapFree
> USER32.dll: MessageBoxA, GetWindowThreadProcessId, IsWindowVisible,
```

```
IsWindowEnabled, GetForegroundWindow, EnableWindow, EnumWindows
> COMCTL32.dll: InitCommonControls
> OLE32.dll: CoInitialize

( 0 exports )
```

❕ **ACHTUNG:** VirusTotal ist ein kostenloser Dienst bereitgestellt von Hispasec Sistemas. Es gibt keine Garantie zur Verfügbarkeit sowie Fortbestehen der Dienstleistung. Obwohl die Erkennungsrate meherer Antivirus-Engines besser ist als nur durch ein Produkt, **garantieren die Ergebnisse des Scans nicht die Harmlosigkeit einer Datei**. Gegenwärtig gibt es keine Lösung, welche eine Erkennungsrate aller Viren und *Malware* zu 100% bietet.

Virustotal analysiert verdächtige **Dateien und erleichtert die schnelle Erkennung** von Viren, Würmern, Trojanern und jeglicher Art von Malware, welche von den Antivirus-Engines festgestellt werden.

Datei **TestUPX.exe** empfangen **2008.05.03 06:48:55 (CET)**
Status: **Beendet**
Ergebnis: **3/31 (9.68%)**

Antivirus	Version	letzte aktualisierung	Ergebnis
AhnLab-V3	2008.5.3.0	2008.05.02	-
AntiVir	7.8.0.11	2008.05.02	-
Authentium	4.93.8	2008.05.02	-
Avast	4.8.1169.0	2008.05.03	-
AVG	7.5.0.516	2008.05.03	-
BitDefender	7.2	2008.05.03	-
CAT-QuickHeal	9.50	2008.05.02	(Suspicious) - DNAScan
ClamAV	0.92.1	2008.05.02	-
DrWeb	4.44.0.09170	2008.05.03	-
eSafe	7.0.15.0	2008.04.28	suspicious Trojan/Worm
eTrust-Vet	31.3.5755	2008.05.03	-
Ewido	4.0	2008.05.02	-
F-Prot	4.4.2.54	2008.05.02	-
F-Secure	6.70.13260.0	2008.05.02	-
Fortinet	3.14.0.0	2008.05.02	-
Ikarus	T3.1.1.26	2008.05.03	-
Kaspersky	7.0.0.125	2008.05.03	-
McAfee	5287	2008.05.02	-
Microsoft	1.3408	2008.04.22	-

NOD32v2	3072	2008.05.03	-
Norman	5.80.02	2008.05.02	-
Panda	9.0.0.4	2008.05.03	-
Prevx1	V2	2008.05.03	-
Rising	20.42.22.00	2008.04.30	-
Sophos	4.29.0	2008.05.03	-
Sunbelt	3.0.1097.0	2008.05.01	VIPRE.Suspicious
Symantec	10	2008.05.03	-
TheHacker	6.2.92.299	2008.05.03	-
VBA32	3.12.6.5	2008.05.02	-
VirusBuster	4.3.26:9	2008.05.02	-
Webwasher-Gateway	6.6.2	2008.05.03	-

weitere Informationen

File size: 4096 bytes

MD5...: 57e04557b577293a14e4848157b9a0bd

SHA1..: 111c20e2a2c736cc9200901d417b74407d11dad4

SHA256: 0eb58ac537b28d8b8ca9786c26e369582a1db081ec2cab2b2aced838b44b7c23

SHA512: 34d3e7c3b091338c70aa0623819d28a19b1015b8898e5d3680f25dc559cc3cfe
b53d80271adec5bb258a51b2076673cdab0305e315f839ca52534836d2890af8

PEiD..: UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser

PEInfo: PE Structure information

```
( base data )
entrypointaddress.: 0x406530
timedatestamp.....: 0x481bea2a (Sat May 03 04:29:30 2008)
machinetype.......: 0x14c (I386)

( 3 sections )
name viradd virsiz rawdsiz ntrpy md5
0x1000 0x5000 0x0 0.00 d41d8cd98f00b204e9800998ecf8427e
0x6000 0x1000 0x800 6.69 4b1113881393aaffe4ba0df69a5c0e11
.rsrc 0x7000 0x1000 0x600 3.95 f909bbe84bbeb88aa21d0a3b1d9b1d09

( 5 imports )
> KERNEL32.DLL: LoadLibraryA, GetProcAddress, VirtualProtect, VirtualAlloc,
VirtualFree, ExitProcess
> COMCTL32.dll: InitCommonControls
> CRTDLL.dll: memset
> OLE32.dll: CoInitialize
> USER32.dll: MessageBoxA
```

```
( 0 exports )
packers: UPX
packers: UPX
packers: PE_Patch.UPX, UPX
```

❗ **ACHTUNG:** VirusTotal ist ein kostenloser Dienst bereitgestellt von Hispasec Sistemas. Es gibt keine Garantie zur Verfügbarkeit sowie Fortbestehen der Dienstleistung. Obwohl die Erkennungsrate meherer Antivirus-Engines besser ist als nur durch ein Produkt, **garantieren die Ergebnisse des Scans nicht die Harmlosigkeit einer Datei**. Gegenwärtig gibt es keine Lösung, welche eine Erkennungsrate aller Viren und *Malware* zu 100% bietet.

Virustotal analysiert verdächtige **Dateien und erleichtert die schnelle Erkennung** von Viren, Würmern, Trojanern und jeglicher Art von Malware, welche von den Antivirus-Engines festgestellt werden.

Datei **Test.exe.Molebox.exe** empfangen **2008.05.03 16:09:03 (CET)**
Status: **Beendet**
Ergebnis: **6/30 (20%)**

Antivirus	Version	letzte aktualisierung	Ergebnis
AhnLab-V3	2008.5.3.0	2008.05.02	-
AntiVir	7.8.0.11	2008.05.02	HEUR/Crypted
Authentium	4.93.8	2008.05.02	-
Avast	4.8.1169.0	2008.05.03	-
AVG	7.5.0.516	2008.05.03	-
BitDefender	7.2	2008.05.03	-
CAT-QuickHeal	9.50	2008.05.02	(Suspicious) - DNAScan
ClamAV	0.92.1	2008.05.03	-
DrWeb	4.44.0.09170	2008.05.03	-
eSafe	7.0.15.0	2008.04.28	Suspicious File
eTrust-Vet	31.3.5755	2008.05.03	-
Ewido	4.0	2008.05.03	-
F-Prot	4.4.2.54	2008.05.02	-
F-Secure	6.70.13260.0	2008.05.03	Suspicious:W32/Malware! Gemini
Fortinet	3.14.0.0	2008.05.03	-
Ikarus	T3.1.1.26	2008.05.03	Virus.Win32.DCom.F
Kaspersky	7.0.0.125	2008.05.03	-
McAfee	5287	2008.05.02	-

Microsoft	1.3408	2008.04.22	-
NOD32v2	3072	2008.05.03	-
Norman	5.80.02	2008.05.02	-
Panda	9.0.0.4	2008.05.03	-
Prevx1	V2	2008.05.03	-
Rising	20.42.22.00	2008.04.30	-
Sophos	4.29.0	2008.05.03	-
Sunbelt	3.0.1097.0	2008.05.03	-
TheHacker	6.2.92.299	2008.05.03	-
VBA32	3.12.6.5	2008.05.03	-
VirusBuster	4.3.26:9	2008.05.02	-
Webwasher-Gateway	6.6.2	2008.05.03	Heuristic.Crypted

weitere Informationen

File size: 61440 bytes

MD5...: 9d79b7b7ab3a9ec0a33004ea32c57ef8

SHA1..: e5b213bf00f76e23daf506b69bf0a4dfbc2cf637

SHA256: 579266af998e12e84d50d3eb0e0f3abfd709c64dacc5b7e1d2057d989972f18a

SHA512: b702c326ad3d2c3779c37462b3a9f2cb9535b9fc87d5f9dbad784558b69d5ea4
05adab56bd6b3954731702f9a356f49cbe11e79b491c578d70930b72b8b76b70

PEiD..: MoleBox V2.3X -> MoleStudio.com

PEInfo: PE Structure information

```
( base data )
entrypointaddress.: 0x407253
timedatestamp.....: 0x481c6eda (Sat May 03 13:55:38 2008)
machinetype.......: 0x14c (I386)

( 7 sections )
name viradd virsiz rawdsiz ntrpy md5
0ode 0x1000 0x96 0x200 4.77 395590a80beb32fbc50d02cf6c1eb3c3
1ext 0x2000 0x2be 0x200 7.60 2f4b1026b057307ef85ed0ed9ecbe84b
2ata 0x3000 0x4d4 0x400 6.68 246d5dbb6e5b200782b46a2875ed5a13
3src 0x4000 0x2b8 0x400 4.07 79ef87e1e37740ec71b947d5920acba7
4ext 0x5000 0xf170 0xb200 7.87 6fc803fc44474ef75d2c839aa553e24d
5data 0x15000 0x1038 0x1200 4.43 a0f60a0933952b37f65cf165f1d3023b
6ata 0x17000 0x7a14 0x1c00 7.97 f13d77e095302d1ede5e3d0c69eafe42

( 4 imports )
> KERNEL32.dll: LocalAlloc, GetModuleHandleA, LeaveCriticalSection,
```

```
EnterCriticalSection, GetCurrentDirectoryA, GetShortPathNameA,
FindResourceExA, EnumResourceLanguagesA, ResumeThread, WriteProcessMemory,
RaiseException, SetFileAttributesA, CreateDirectoryA, GetCurrentThreadId,
GetPrivateProfileSectionA, GetStringTypeA, LCMapStringW, LCMapStringA,
MultiByteToWideChar, LocalFree, GetProcAddress, InitializeCriticalSection,
WideCharToMultiByte, RtlUnwind, GetStringTypeW
> USER32.dll: SetFocus, AdjustWindowRectEx, DefWindowProcA
> ADVAPI32.dll: RegCreateKeyA, RegSetValueA, RegCloseKey
> ole32.dll: CoRegisterClassObject, ReadClassStm

( 0 exports )
```

Virustotal analysiert verdächtige **Dateien und erleichtert die schnelle Erkennung** von Viren, Würmern, Trojanern und jeglicher Art von Malware, welche von den Antivirus-Engines festgestellt werden. Weitere Informationen...

Datei **TestUPX.exe.Molebox.exe** empfangen **2008.05.03 16:22:16 (CET)**
Status: **Beendet**
Ergebnis: **8/31 (25.81%)**

Antivirus	Version	letzte aktualisierung	Ergebnis
AhnLab-V3	2008.5.3.0	2008.05.02	-
AntiVir	7.8.0.11	2008.05.02	HEUR/Crypted
Authentium	4.93.8	2008.05.02	-
Avast	4.8.1169.0	2008.05.03	-
AVG	7.5.0.516	2008.05.03	-
BitDefender	7.2	2008.05.03	-
CAT-QuickHeal	9.50	2008.05.02	(Suspicious) - DNAScan
ClamAV	0.92.1	2008.05.03	-
DrWeb	4.44.0.09170	2008.05.03	-
eSafe	7.0.15.0	2008.04.28	Suspicious File
eTrust-Vet	31.3.5755	2008.05.03	-
Ewido	4.0	2008.05.03	-
F-Prot	4.4.2.54	2008.05.02	-
F-Secure	6.70.13260.0	2008.05.03	Suspicious:W32/Malware!Gemini
Fortinet	3.14.0.0	2008.05.03	-
Ikarus	T3.1.1.26	2008.05.03	Virus.Win32.DCom.F
Kaspersky	7.0.0.125	2008.05.03	-
McAfee	5287	2008.05.02	-

Microsoft	1.3408	2008.04.22	-
NOD32v2	3072	2008.05.03	-
Norman	5.80.02	2008.05.02	-
Panda	9.0.0.4	2008.05.03	Suspicious file
Prevx1	V2	2008.05.03	-
Rising	20.42.22.00	2008.04.30	-
Sophos	4.29.0	2008.05.03	Sus/ComPack
Sunbelt	3.0.1097.0	2008.05.03	-
Symantec	10	2008.05.03	-
TheHacker	6.2.92.300	2008.05.03	-
VBA32	3.12.6.5	2008.05.03	-
VirusBuster	4.3.26:9	2008.05.02	-
Webwasher-Gateway	6.6.2	2008.05.03	Heuristic.Crypted

weitere Informationen

File size: 65024 bytes

MD5...: f5b423a83f2a1f092b12ec7149c818f3

SHA1..: 75d4690be9218425ad4919a473477f8beb4a0ae4

SHA256: e4719654ae100dd368939ec9160fb691528d64b516c223972c867fb344cd49c8

SHA512: 3ee7bd8e53c0314c207ee9dc489a2ad7e58dc06497d4b08e2be5d72ea19dd17f
d19058b040ad6ad80ef45835e98be13d00ce2df17263304e62d6465a3b69f9aa

PEiD..: MoleBox V2.3X -> MoleStudio.com

PEInfo: PE Structure information

(base data)
entrypointaddress.: 0x40a253
timedatestamp.....: 0x481c6eda (Sat May 03 13:55:38 2008)
machinetype.......: 0x14c (I386)

(6 sections)
name viradd virsiz rawdsiz ntrpy md5
0X0 0x1000 0x5000 0x0 0.00 d41d8cd98f00b204e9800998ecf8427e
1X1 0x6000 0x1000 0x800 7.57 a6819c0f2aedc526a6f905fed2f83884
2src 0x7000 0x1000 0x600 3.94 ef4e1be40d8e8fe1248c2e586098b5c8
3ext 0x8000 0xf170 0xb200 7.87 4fa85dc620ec4a32586b29dffc8e9f19
4data 0x18000 0x1038 0x1200 4.43 21cfd9812d6202474df093deaf2815b7
5ata 0x1a000 0x7a14 0x1c00 7.97 b95109d76d0876760a06b73172b5438c

(4 imports)

```
> KERNEL32.dll: LocalAlloc, GetModuleHandleA, LeaveCriticalSection,
EnterCriticalSection, GetCurrentDirectoryA, GetShortPathNameA,
FindResourceExA, EnumResourceLanguagesA, ResumeThread, WriteProcessMemory,
RaiseException, SetFileAttributesA, CreateDirectoryA, GetCurrentThreadId,
GetPrivateProfileSectionA, GetStringTypeA, LCMapStringW, LCMapStringA,
MultiByteToWideChar, LocalFree, GetProcAddress, InitializeCriticalSection,
WideCharToMultiByte, RtlUnwind, GetStringTypeW
> USER32.dll: SetFocus, AdjustWindowRectEx, DefWindowProcA
> ADVAPI32.dll: RegCreateKeyA, RegSetValueA, RegCloseKey
> ole32.dll: CoRegisterClassObject, ReadClassStm

( 0 exports )
```