دانستنیها

راه‌هایی برای مقابله با بدافزارها

اشاره :

چند راهکار ساده می‌تواند شما را از صدمات ناشی از حمله بدافزارها دور نگه دارد . در این مقاله با تعدادی از آنها آشنا میشود .

۱ - آمادگی در برابر حملات

همواره از بروزترین نرم‌افزارهای دارای مجوز به همراه آخرین نسخه‌های Patchهای آنان استفاده کنید .

همه سیستم‌های موجود در شبکه را اسکن کنید تا از عدم وجود هر نوع ویروس ، تروجان یا جاسوس‌افزار مطمئن شوید . مطمئن شوید نرم‌افزار امنیتی شما کلیه راه‌های ورود و خروج شبکه را حفاظت می‌کند . همچنین همیشه مطمئن باشید که نرم‌افزار امنیتی شما از آخرین فایل‌های شناسایی کدهای مخرب ، بهره‌مند است .

با استفاده از یک زمانبندی مناسب ، همواره از اطلاعات سیستم خود (هفتگی ، روزانه و . . .) پشتیبان‌گیری کنید .

در سایت‌های مربوط به فروشندگان نرم‌افزارهای امنیتی عضو شوید تا بولتن‌های مربوط به آخرین پچ‌ها و سایر امور و موارد لازم برای شما ارسال شود .

یک تیم ۲۴ ساعته آماده ، شامل افراد فعال در زمینه مسائل مدیریتی - فنی برای مقابله با مسائل امنیتی و بدافزارها تشکیل دهید .

فهرستی از شماره تلفن یا وسیله تماس افرادی که در مواقع بروز مشکل به آنان نیاز دارید ، جمع‌آوری نمایید .

از تمام اطلاعات و سیستم‌های مهم خود کپی‌برداری کنید تا در مواقع ضروری و مورد نیاز بتوانید به عنوان پشتیبان از آن‌ها استفاده کنید و آن‌ها را در محیط اصلی بازیابی نمایید . برای این کار باید مطمئن‌شوید که به اندازه کافی فضای مورد نیاز برای نگهداری اطلاعات کامپیوترهای آلوده را در دسترس دارید . در این صورت باید کل هارددیسک را به صورت Image کپی بگیرید .

بیشتر بدافزارها به دلیل عدم آگاهی کاربران داخلی و از طریق آن‌ها به سیستم راه می‌یابند . بنابراین تا می‌توانید کاربرانتان را با این مسائل آشنا نمایید .

۲ - شناسایی حمله

به برخی علایم شایع و غیرعادی در زمان حمله بدافزارها توجه کنید :

خاموش یا خاموش و روشن شدن سیستم
ترافیک زیاد شبکه
کند شدن سیستم‌های ورود و خروج شبکه
فعالیت بی‌دلیل هارددیسک ، درایوها یا برخی فایل‌ها

غیرقابل دسترس شدن ناگهانی برخی سایت‌ها یا کامپیوترهای راه دور (البته ممکن است آن سایت‌ها موردحمله قرار گرفته باشند) .

۳ - پاسخ به حمله

سیستم‌های آلوده را از شبکه جدا کنید . البته این کار را باید با دقت بیشتری انجام دهید ؛ چرا که برخی بدافزارها متوجه جدا شدن یک کامپیوتر آلوده شده از شبکه می‌شوند و آن گاه فعالیت اصلی خود را آغاز می‌کنند .

سیستم‌های آلوده را با استفاده از نرم‌افزارهای امنیتی ضد بدافزارها پاکسازی نمایید . مطمئن باشید که فایل‌های شناسایی نرم‌افزار مورد استفاده شما بروز است ؛ چرا که ممکن است خطرناک‌ترین نوع بدافزارها همین چند ساعت پیش بروز شده باشند . هدف نهایی مورد نظر بدافزار را شناسایی نمایید و از صحت آن اطمینان حاصل کنید .

اگر آلوده نیست ، از آن نسخه پشتیبان تهیه کنید . کدهای مخرب درون بدافزار ممکن است هنوز فعال نشده باشند . بنابراین قبل از فعال شدن ، آن‌ها را پاک کنید .

محل ورود بدافزار را شناسایی کنید . این مسئله به شما کمک می‌کند از شبکه ، سرورها و سایر سیستم‌هایی که می‌توانند راه ورود بدافزار باشند ، حفاظت بیشتری کنید . فرض کنید بدافزار ، بیش از صرفا چند فایل معمولی را هدف قرار داده است .

حتی تصور کنید شاید در حین پاکسازی ، برخی اطلاعات کاری خود را از دست بدهید .

بنابراین قبل از اسکن کردن مطمئن شوید که سیستم از روی یک سی‌دی سالم یا فلاپی دیسک غیر قابل نوشتن بوت شده است تا عمل اسکن با اطمینان بیشتری انجام شود .

این که سیستم به بدافزار آلوده شده ، مسئله‌ای شایع است .

بنابراین از بروز چنین مسئله‌ای ناامید و سرگشته نشوید و سعی کنید مشکل را با کمک افراد خبره تیم خود حل نمایید . افراد متخصص درمسائل امنیتی می‌توانند در پاره‌ای موارد به ویروس ، کرم یا هر بدافزار دیگری عمدا اجازه دهند در سیستم پراکنده شود و خود را بیشتر آشکار کند تا عملکرد و شیوه مقابله با آن سریع‌تر کشف شود .

۴ - بازیابی سرویس‌ها و سیستم‌ها

رمز عبورهای کلیه سیستم‌ها و سرورها را عوض کنید .

مطمئن شوید برای عمل بازیابی ، فایل‌های پشتیبان را از سیستم‌های غیرآلوده برداشته‌اید .

اگر سیستم شما مورد حملات مستمری قرار می‌گیرد ، لاگ فایلتان را چک کنید تا شاید آدرس IP حمله کننده را پیدا کنید .

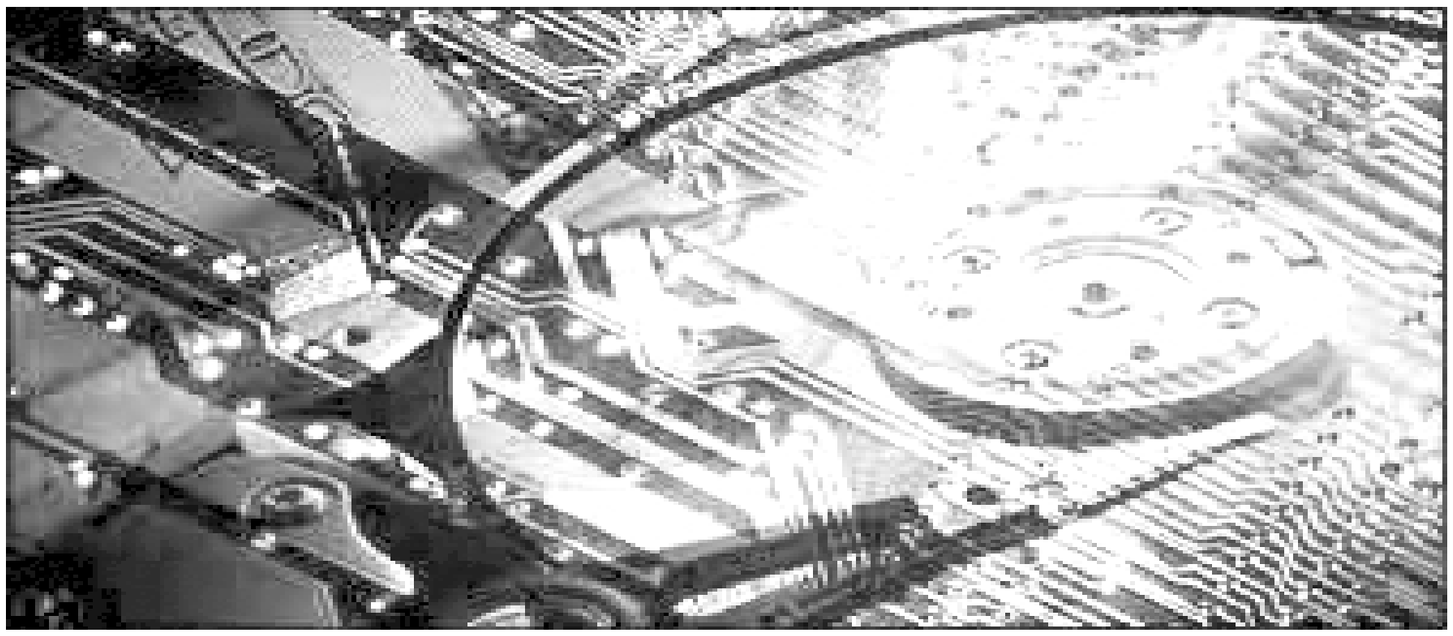
فعالیت شبکه را به‌طور منظم و با دقت کنترل کنید تا مطمئن شوید هیچ بدافزاری در سیستم پنهان نشده یا هیچ کد مخرب جدیدی در سیستم ایجاد نشده است .

۵ - بازسازی صحنه حادثه

تیم مقابله با بدافزار را دور هم جمع کنید تا معلوم شود همگی از این مقابله ، چه تجربیاتی کسب نموده‌اند .

مشخص کنید شیوه مقابله این تیم با بدافزار تا چه اندازه مطثر بوده است و آیا می‌توان این مقابله را در آینده موثرتر نمود؟ در واقع مدیر تیم باید بتواند تغییر و تحولات لازم در این زمینه را انجام دهد .

کلیه وقایع پیش آمده را برای مدیران رده بالاتر توضیح دهید تا آن‌ها را برای اتفاقات آینده آماده نمایید .



SCANNER

EPSON

مدل	قیمت
PERFECTION 4990	۵۲۵۰۰۰۰
PERFECTION 4490	۲۸۵۰۰۰۰
PERFECTION 3950	۱۶۵۰۰۰۰
PERFECTION 3490	۱۰۹۸۰۰۰
OPTIC PRO ST-48	۷۸۰۰۰۰
OPTIC PRO ST-28	۶۹۰۰۰۰
OPTIC SLIM-2400	۵۱۰۰۰۰

HP

SCANjET-4370	۹۵۰۰۰۰
SCANjET-4850	۱۳۵۰۰۰۰
SCANjET-4890	۱۸۵۰۰۰۰
SCANjET-5590	۴۱۰۰۰۰۰
SCANjET-8300	۴۴۵۰۰۰۰
SCANjET-7650	۶۸۰۰۰۰۰
SCANjET-8200	۴۲۵۰۰۰۰
SCANjET-5530	۲۴۰۰۰۰۰

CASE

4350	320000
Acer	130000
HP	580000

MOUSE

OPTICAL VAIO	60000
microlab	30000
delco	58000
Microsoft	230000

HDD

MAXTOR

ظرفیت	نوع رابط	قیمت (ریال)
GB160	IDE	۵۵۰۰۰۰
GB200	IDE	۷۲۵۰۰۰
GB80	SATA 2	۴۴۰۰۰۰
GB160	SATA 2	۵۷۰۰۰۰
GB200	SATA 2	۶۸۰۰۰۰
GB250	SATA 2	۷۲۰۰۰۰
GB400	SATA 2	۱۷۰۰۰۰۰
GB500	SATA 2	۲۲۵۰۰۰۰

WESTERN DIGITAL

ظرفیت	نوع رابط	قیمت (ریال)
GB160	SATA 2	۶۲۵۰۰۰
GB200	SATA 2	۷۱۰۰۰۰
GB250	SATA 2	۷۷۰۰۰۰
GB320	SATA 2	۱۰۱۰۰۰۰
GB400	SATA	۱۸۵۰۰۰۰
GB500	SATA	۲۴۵۰۰۰۰

SAMSUNG

ظرفیت	نوع رابط	قیمت (ریال)
GB160	IDE	۵۷۰۰۰۰
GB200	IDE	۷۰۰۰۰۰
GB200	SATA2	۷۱۶۰۰۰
GB250	IDE	۷۵۲۰۰۰
GB250	SATA2	۷۶۳۰۰۰
GB300	SATA	۹۲۲۰۰۰

ASUS

CD DRIVE 40X	۱۲۵۰۰۰
CD RW 52X32X52X	۲۲۰۰۰۰
DVD ROM 16X 48X	۲۸۰۰۰۰
COMBO 52X32X52X16X	۳۵۰۰۰۰

MP3 PLAYER

CREATIVE

مدل	ظرفیت	قیمت
MUVO S200	1GB	۹۵۰۰۰۰
MUVO S200	512MB	۷۳۰۰۰۰
MUVO SLIM	1GB	۹۵۰۰۰۰
MUVO SLIM	512MB	۷۲۰۰۰۰
MUVOTXFM	256MB	۵۰۰۰۰۰
MUVO TXFM	512MB	۷۳۰۰۰۰

IPOD

مدل	ظرفیت	قیمت
NANO	1GB	۱۴۵۰۰۰۰
NANO	2GB	۲۰۰۰۰۰۰
NANO	4GB	۲۴۰۰۰۰۰
PHOTO	20GB	۲۸۰۰۰۰۰
PHOTO	30GB	۳۳۰۰۰۰۰
PHOTO	60GB	۴۰۰۰۰۰۰

LEONO

مدل	ظرفیت	قیمت
۲۰۲-G	128MB	۲۶۰۰۰۰
۲۱۰-G	512MB	۴۳۵۰۰۰
۲۱۰C-G	256MB	۳۱۵۰۰۰
۲۱۰A-G	512MB	۴۹۵۰۰۰
۲۱۵-G	256MB	۳۱۰۰۰۰
۲۲۵-G	1GB	۸۷۵۰۰۰

CPU

INTEL

PENTIUM 4 519j	3.06 GHz	۸۵۰۰۰۰
PENTIUM 4 520j	2.8 GHz	۸۷۰۰۰۰
PENTIUM 4 520j	2.93 GHz	۹۸۰۰۰۰
PENTIUM 4 520j	3.0 GHz	۱۷۰۰۰۰۰
PENTIUM 4 630	3.0 GHz	۱۹۵۰۰۰۰
PENTIUM 4 640	3.2 GHz	۹۵۰۰۰۰
PENTIUM 4 D	2.6 GHz	۲۰۰۰۰۰۰
PENTIUM 4 D	3.4 GHz	۹۷۰۰۰۰

AMD

ATHLON 64BiT X2	+۳۶۰۰	۱۲۰۰۰۰۰
ATHLON 64BiT X2	+۳۸۰۰	۱۵۸۰۰۰۰
ATHLON 64BiT X2	+۴۲۰۰	۱۹۰۰۰۰۰
ATHLON 64BiT X2	+۴۶۰۰	۲۴۰۰۰۰۰
ATHLON 64BiT X2	+۴۸۰۰	۲۸۵۰۰۰۰
ATHLON 64BiT X2	+۵۰۰۰	۲۹۹۰۰۰۰

P4VTG	385000
P4TGV	495000
P4TSP-D2	445000
P4VMA-M	

VGA

AKN

RADEON

X600	1300000
X300	900000
9600PRO	820000
9600XT	780000
9550	670000
7500	290000

ASUS

Geforce 6600	۶۳۰۰۰۰
Geforce 7300	۶۹۰۰۰۰
Geforce 6200	۵۷۰۰۰۰
Geforce 6200	۴۵۰۰۰۰
Geforce 6200	۴۴۰۰۰۰
Geforce 6200	۵۹۰۰۰۰
Geforce FX 5200	۳۸۰۰۰۰
RADEON 1600	۱۲۴۰۰۰۰
RADEON X700 XT	۹۹۰۰۰۰
RADEON X300 XT	۴۹۰۰۰۰

DRIVES

SONY

FLOPPY DRIVE 1.44	50000
CD DRIVE 52X	150000
CD.R/RW 52X32X52X	260000
DVD ROM 16X48X	300000

MONITOR

SAMSUNG

LCD

970 P-17"	6270.000
940 B-19"	5220.000
M 1740-17"	2700.000
B 1750-17"	2900.000
BF 1750-17"	2900.000

HANSOL

CRT

722ED COLOR 17"	1380000
730ED+COLOR 17"	1590000
740DPRO COLOR 17"	1680000
730DCOLOR 17"	1650000
922 P 19"	1850000

LCD

H550 15"	2650000
H750 17"	3150000

BENQ

LCD

FP-51G-15"	2110.000
FP-567S-V2-15"	2360.000
FP-71G-17"	2630.000
FP-72E-17"	2980.000
FP-71W-17"	3390.000
FP-91G-19"	3580.000
FP-202W-20	420.000

MB

ASUS

P5WDG2-WS	۲۷۰۰۰۰
P5N32-SLI Deluxe	۲۴۵۰۰۰۰
P5WD2 E Premium	۲۱۲۰۰۰۰
P5WD2 Premium	۱۹۲۰۰۰۰
P5LD2 Deluxe	۱۵۰۰۰۰۰
P5LD2 SE	۱۰۵۰۰۰۰
P5LD2 VM	۱۰۴۰۰۰۰
P5LD2 VW DH	۱۱۳۰۰۰۰
P5PL2	۸۹۰۰۰۰
P5AD2 E	۸۱۰۰۰۰
P5GD2 X	۷۹۰۰۰۰
P5RD1-VM	۶۶۰۰۰۰
P5VDC X	۶۸۵۰۰۰
P5VD2 M X	۶۹۰۰۰۰

NOTE BOOK

مدل	سی پی یو(CPU)	هارد(HDD)	رم(RAM)	ال سی دی (LCD)	درایو (DRIVE)	قیمت	
DGW3J	1.66 GHZ/NAPA	60 GB	512 MB DDR2	۱۴ WXGA	DVD-RW SUPER	۱۷۵۴۰۰۰	ASUS
DGA3FC	1.66 GHZ/NAPA	60 GB	512 MB DDR2	۱۵ XGA	DVD-RW SUPER	۱۲۷۹۰۰۰	ASUS
DGW6F	1.83 GHZ/NAPA	100 GB4	768 MB DDR2	۳/۱۳ WXGA	DVD-RW SUPER	۱۹۷۹۰۰۰	SONY
VAIOSZ230 P/B	1.83 GHZ/CORE DUO	120 GB SATA	1024 MB DDR2	۳/۱۳ WXGA	DVD/RW	۱۸۵۰۰۰۰	SONY
VAIOSZ250 P/C	1.83 GHZ/CORE DUO	100 GB SATA	512 MB DDR2	۳/۱۳ WXGA	DVD/RW	۲۱۰۰۰۰۰	SONY

HYUNDAI

NO.	MODEL		CPU	RAM	HDD	LCD	DRIVE	VGA	Price (toman)
1	HYUNDAI	M 540 S	1.6 Celeron	512 MB	40 GB	14" WXGA TFT(Ultra Bright)	DVD/RW DUAL	128 MB	850.000
2	HYUNDAI	M 123 W	1.7 Centrino	512 MB	80 GB	12.1" WXGA (Ultra Bright)	DVD/RW DUAL	64 MB	1.300.00
3	HYUNDAI	M 540 N	1.66 Core Duo	1024 MB	80 GB SATA	14" WXGA (Ultra Bright)	DVD/RW DUAL	128 MB	1.480.000
4	HYUNDAI	T 210 C	1.7 Centrino	1024 MB	80 GB	14.1" XGA TFT Rotate	Ext.USB DVD/RW DUAL	64 MB	1.500.000
5	HYUNDAI	M 560 A	2.0 SONOMA	1024 MB	80 GB	15.4" WUXGA	DVD/RW DUAL	128 MB ATI	1.900.000