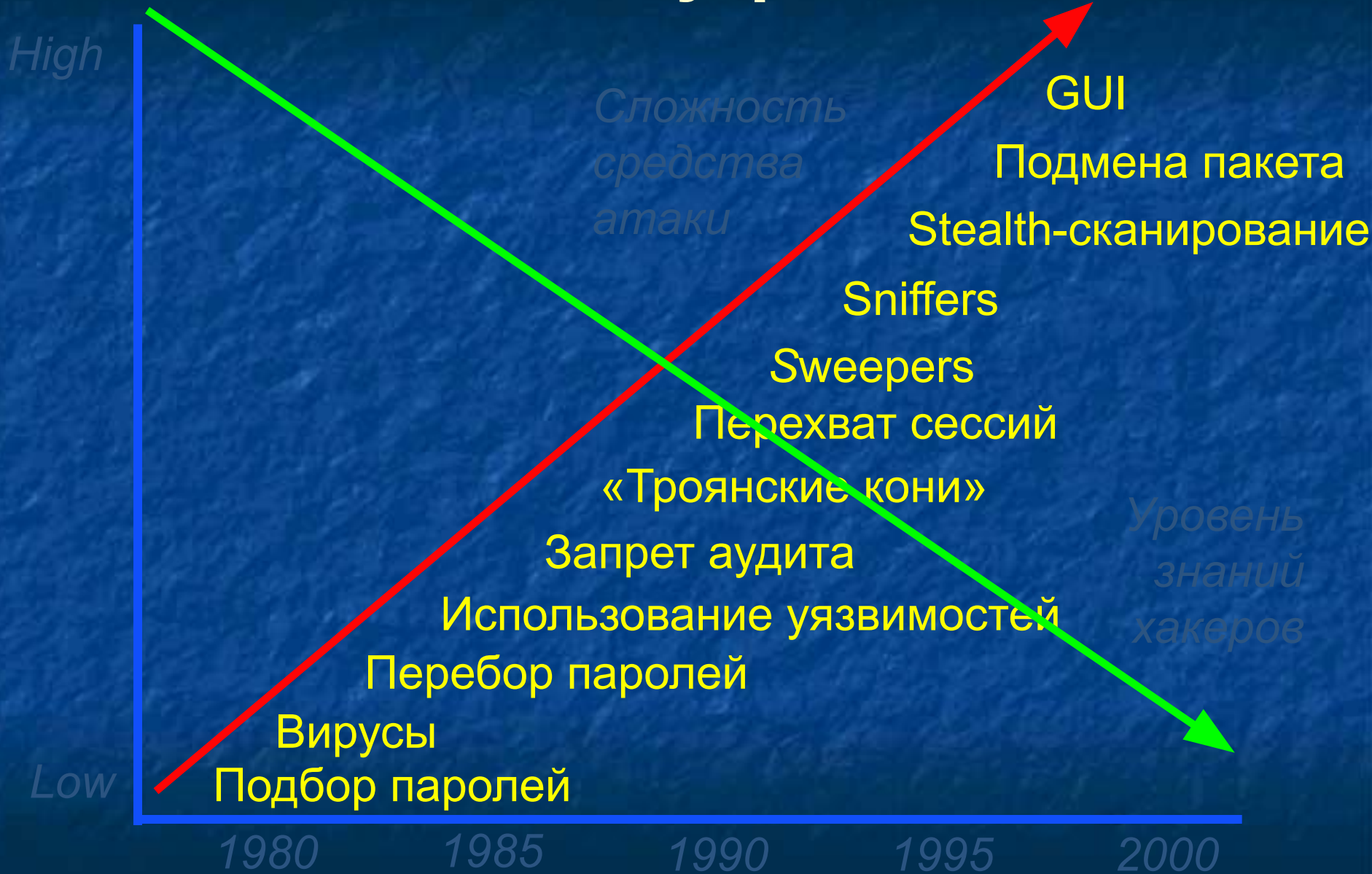


Рост угроз



Типовая схема сегмента корпоративной сети



Приложение масштаба предприятия

- Приложение масштаба предприятия

- различные платформы
- использование Internet
- разное ПО и аппаратура
- различные пользователи
- масштабность
- интеграция в технологию обработки информации



- Результат

- Данные и системы могут быть:
 - выведены из строя
 - украдены
 - несанкционированно изменены

Особенности приложений масштаба предприятия

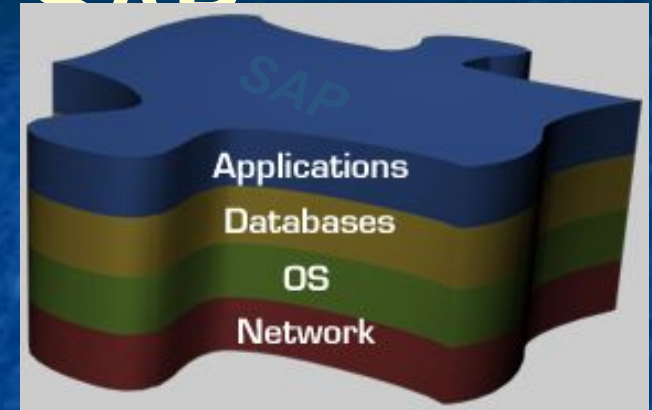
Внешние и внутренние злоумышленники

*Управление безопасностью сосредоточено
в разных руках:*

- администраторы безопасности*
- администраторы баз данных*
- системные и сетевые администраторы*
- Web-мастера*

*Ограниченные ресурсы на обеспечение
безопасности*

Пример приложений масштаба предприятия: SAP



Безопасность сети

- *Мониторинг всего трафика*
- *Обнаружение НСД*
- *Оповещение об атаках*
- *Завершение атаки*
- *Автоматическая реконфигурация сетевого оборудования*

Интервал безопасности

Желательный
уровень
защищенности

Реальный
уровень
защищенности

Если ничего не делать...

**“Интервал”
увеличивается**

Время



Интервал безопасности



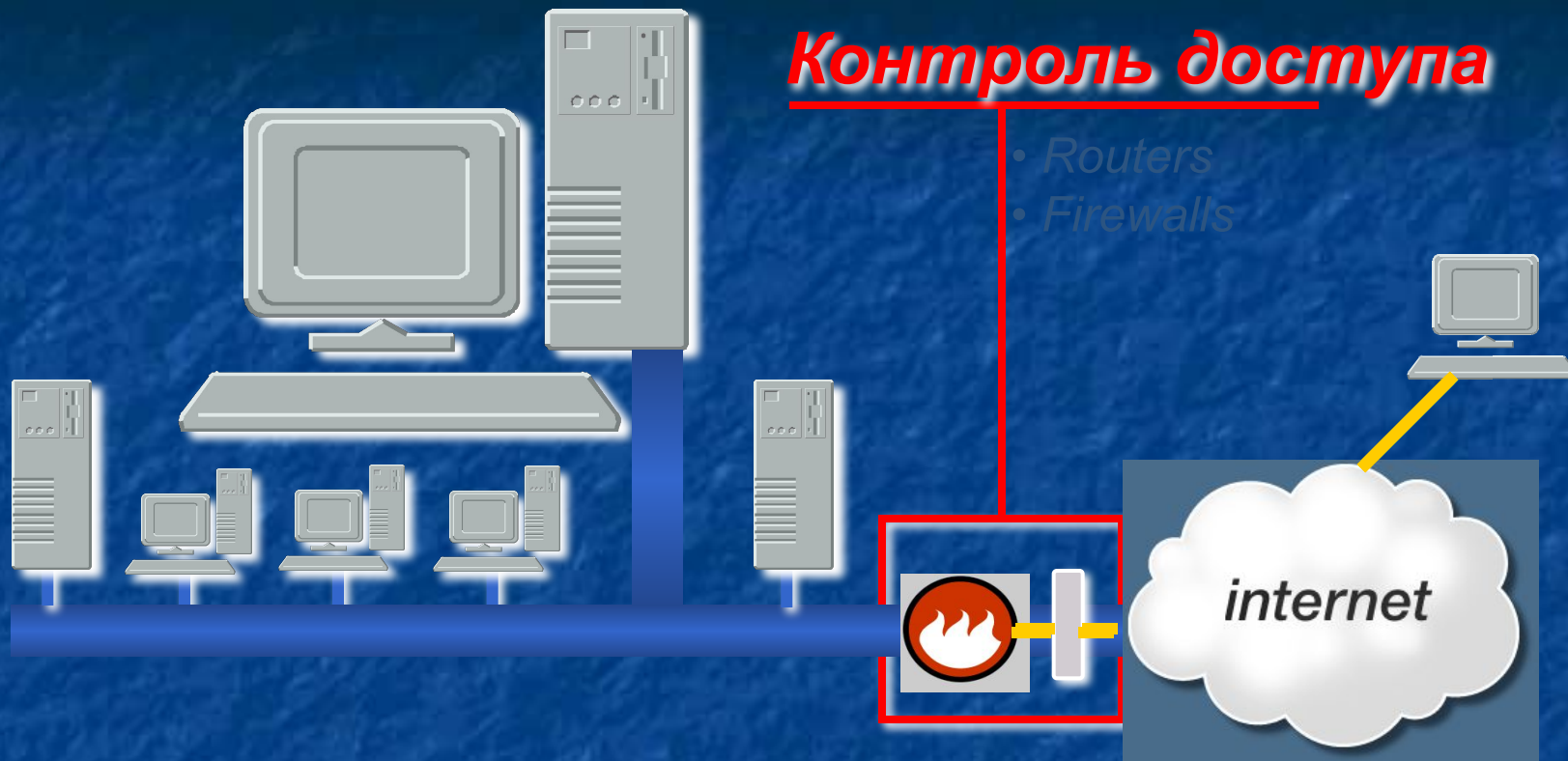
Традиционные средства защиты

Компоненты системы безопасности

- Access Control
- Encryption
- Authentication
- Virus/Content Security

ИНФРАСТРУКТУРА БЕЗОПАСНОСТИ

Инфраструктура безопасности

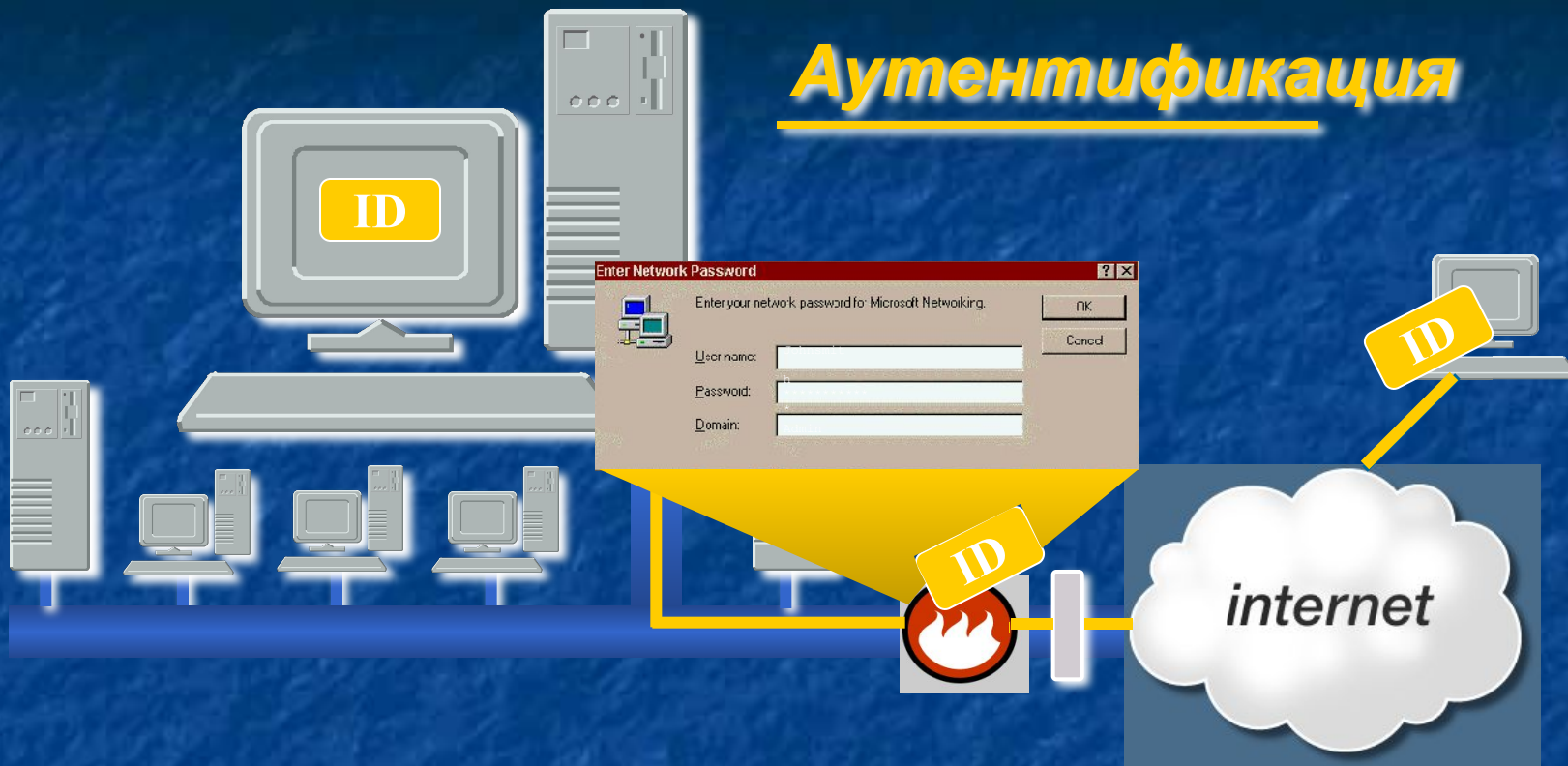


- **Access Control**
- Encryption
- Authentication
- Virus/Content Security

ИНФРАСТРУКТУРА БЕЗОПАСНОСТИ

Инфраструктура безопасности

Аутентификация



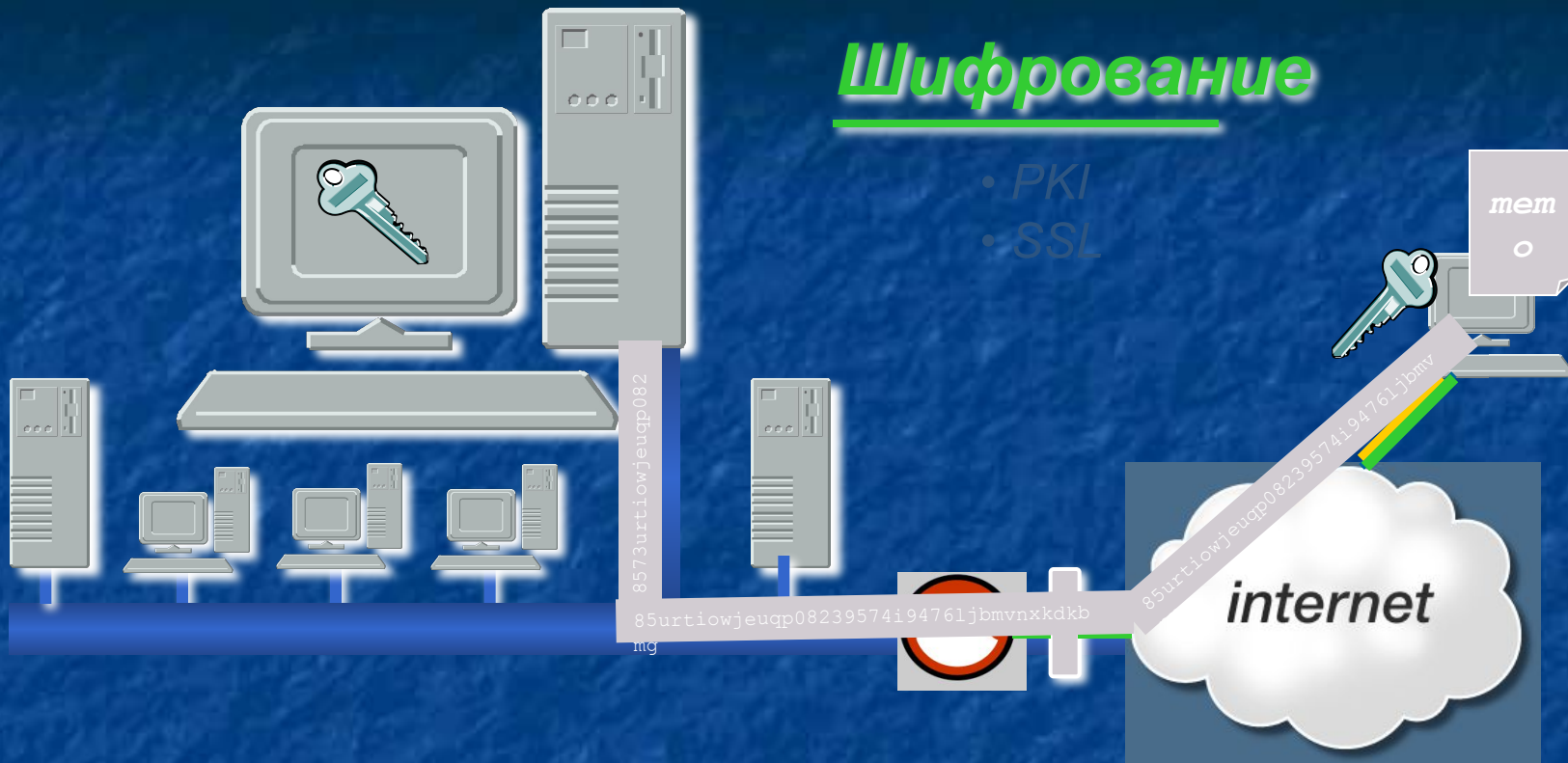
- Access Control
- Encryption
- **Authentication**
- Virus/Content Security

ИНФРАСТРУКТУРА БЕЗОПАСНОСТИ

Инфраструктура безопасности

Шифрование

- PKI
- SSL



- Access Control
- Encryption
- Authentication
- Virus/Content Security

ИНФРАСТРУКТУРА БЕЗОПАСНОСТИ

Уязвимости

Любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

- ошибки в программах;
- человеческие ошибки и неправильная конфигурация
- разрешенный, но неиспользуемый сервис
- восприимчивость к атакам типа «отказ в обслуживании»
- ошибки при проектировании



Угрозы и атаки

Атака - любое действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей информационной системы.



Угроза - потенциально возможное событие, действие или процесс, которое посредством воздействия на компоненты информационной системы может привести к нанесению ущерба.

Информационная инфраструктура



Анатомия атаки



BigWidget



The Part That Fits™

[Company](#) [Products](#) [Services](#) [Support](#)



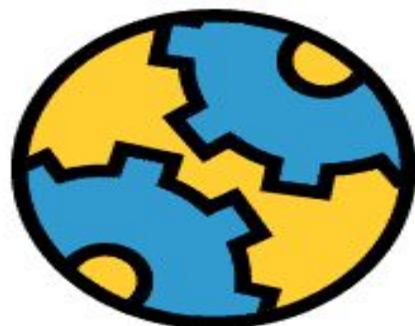
[BigWidget Announces Titanium Machining Capabilities](#)

BigWidget Incorporated announced today the purchase of a Consolidated Conglomerate abrasive waterjet cutter. This new machine will allow BigWidget to offer advanced machining services for titanium cogs and widgets.

[More News...](#)

- [BigWidget acquires Spacely Sprockets for \\$17.3 million](#)
- [BigWidget announces record third quarter earnings](#)

Welcome to Network Solutions' 
InterNIC Registration Services



NETWORK SOLUTIONS®
REGISTRATION SERVICES

Domain name registration services

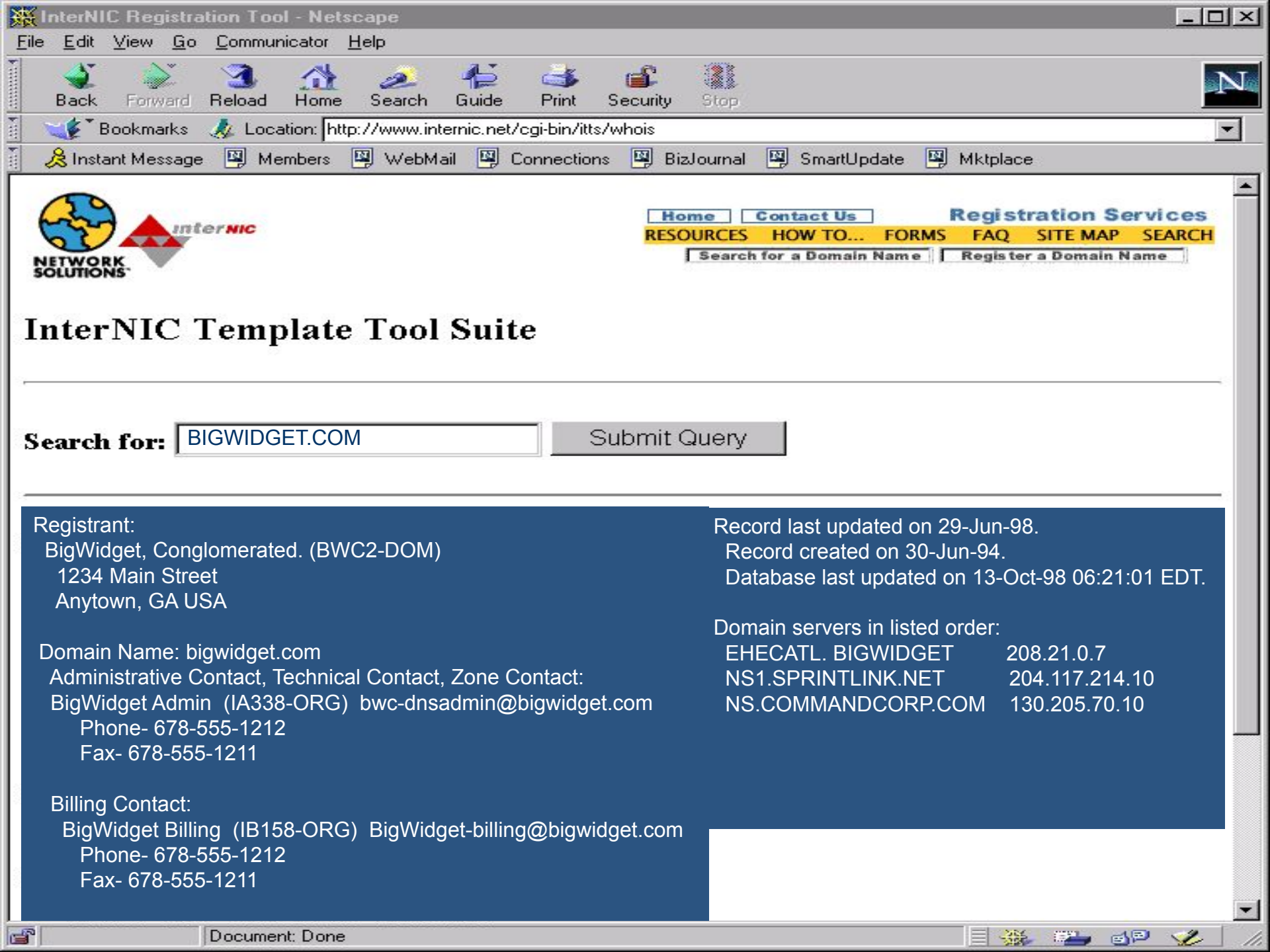
The InterNIC provides [domain name registration services](#) for the top level domains *.com*, *.net*, *.org*, and *.edu*. Please visit the [What's New?](#) page to see a listing of recently added features or changes to the site.

- **Search** the database of registered domain names using WHOIS:

- **[Register a domain name:](#)** If you are registering a domain name for the first time, please see [How to Register a new domain name](#) for guidance.
- **[Forms:](#)** Registration Services maintains a variety of forms to assist you in registering or transferring your domain name and modifying your domain name and associated records.
- **[Resources:](#)** Links to everything from [policies](#) to [payment options](#).

The InterNIC is a cooperative activity between the U.S. Government and [Network Solutions, Inc.](#)

Please read our [disclaimer](#).



Bookmarks Location:

Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace



[Home](#) [Contact Us](#) **Registration Services**
RESOURCES HOW TO... FORMS FAQ SITE MAP SEARCH

InterNIC Template Tool Suite

Search for:

Registrant:
BigWidget, Conglomerated. (BWC2-DOM)
1234 Main Street
Anytown, GA USA

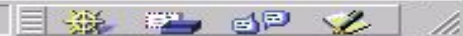
Record last updated on 29-Jun-98.
Record created on 30-Jun-94.
Database last updated on 13-Oct-98 06:21:01 EDT.

Domain Name: bigwidget.com

Administrative Contact, Technical Contact, Zone Contact:
BigWidget Admin (IA338-ORG) bwc-dnsadmin@bigwidget.com
Phone- 678-555-1212
Fax- 678-555-1211

Domain servers in listed order:
EHECATL.BIGWIDGET 208.21.0.7
NS1.SPRINTLINK.NET 204.117.214.10
NS.COMMANDCORP.COM 130.205.70.10

Billing Contact:
BigWidget Billing (IB158-ORG) BigWidget-billing@bigwidget.com
Phone- 678-555-1212
Fax- 678-555-1211





- exploits
- news
- search
- documentation
- imap

Do you have security related news? Please e-mail it to news@rootshell.com.

OpenSite Web Auctions truly open
9/24/98 8:22AM PDT

[OpenSite Technologies, Inc.](#) has a product allowing sites to offer Web Auctions. Apparently most sites using this software have it misconfigured and anyone browsing their site has access to users credit cards and personal information. If you are a user of this software please contact OpenSite for information on securing your website.

- [news.com - Auctions close major security hole](#)

Fraud alleged in the transfer of ownership of Thailand.com site
9/23/98 1:40PM PDT

Do you rely on DNS for authentication. If you do then this is another reason to think twice. Under current InterNIC policy it is quite easy to steal someones domain and make the courts figure it out later.

- [bangkokpost.net - Fraud alleged in the transfer of ownership of Thailand.com site](#)
- www.thailand.com

Rootshell t-shirts coming soon!
9/22/98 11:28AM PDT

Rootshell t-shirts are coming soon! In order to anticipate demand if you think you might be interested in purchasing a t-shirt please [click on this link](#). It is looking like t-shirts will be priced somewhere around \$15-\$18 US. If you have any design


 Bookmarks Location: <http://www.rootshell.com/search.fcgi>

Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace



exploits

news

search

documentation

Connect from dhcp174-180.iss.net [208.27.174.180] (Mozilla/4.05 [en] (WinNT; D))logged.

Rootshell search results

7/17/98	imapd4.txt	New remote root exploit in University of Washington imapd 4. (that came with Pine 4.0)
4/13/98	impack103.tar.gz	Luke_Skyw'w Imap Pack 1.03 - exploit imapd attack vunerable hosts. (Warning: contains untested binaries)
2/19/98	imapd_core.txt	When imapd core dumps, the core will have encrypted shadowed passwords.
11/21/97	imaps.tar.gz	Serveral different versions of the remote imapd buffer overflow exploit.
10/30/97	imapd_4.1b.txt	It's possible to crash imapd, thus leaving shadow and password files in core file.
9/26/97	imapd_scan.sh	This script will scan (and exploit) an entire subnet for imap2 vulnerabilites.
6/24/97	imapd_exploit.c	Get remote root access on Redhat systems by overwriting a buffer in imapd.



rootshell

To: neighbor@home.org
From: neighbor@home.org
Subject: Hope you had a nice vacation

[exploits](#)[news](#)[search](#)[documentation](#)

[Download NON-HTML Version](#) | [Add Comment](#) | [View Comments \(1 comment\(s\)\)](#)

/*

This is the remote exploit of the hole in the imap daemon, for Linux. The instruction code is doing open(), write(), and close() system calls, and it adds a line root::0:0.. at the beggining of /etc/passwd (change to /etc/shadow if needed). The code needs to be self modifying since imapd turns everything to lowercase before it pushes it on the stack. The problem is that it rewrites the first line of passwd/shadow, therefore loosing the root password.

I'm sorry, but I don't have time to add in the seek syscall.

- Akylonius (aky@galeb.etf.bg.ac.yu) [1997]

Modifications made on 5.1.97 to accept command line hostname, with 'h_to_ip' function that resolves it to an ip. - p1 (p1@el8.org)



<http://www.theargon.com>
Encryption, Security, Remailers, **CLICK HERE** PGP, Privacy on the Net, And Much More!

Search For Files

Articles

- [Bugtrac](#)
- [Faq](#)
- [Rootshell](#)

Crew

- [Members](#)
- [Programs](#)
- [Projects](#)

News & Info

- [Contact](#)
- [Links](#)
- [Mirrors](#)
- [Sponsors](#)
- [Thanks](#)
- [WarBoard](#)

Software

- [Denial Of Service](#)
- [Hacking](#)



Top Stories

New mirror opens - 8/20/98

I'm pleased to announce that a new mirror site has opened. If you are having trouble downloading files here, I suggest that you try the mirror site or buy [The WarForge CD](#). The mirror is: <http://www.paran0id.com/warforge/>

Want to see if you have BO? - 8/19/98

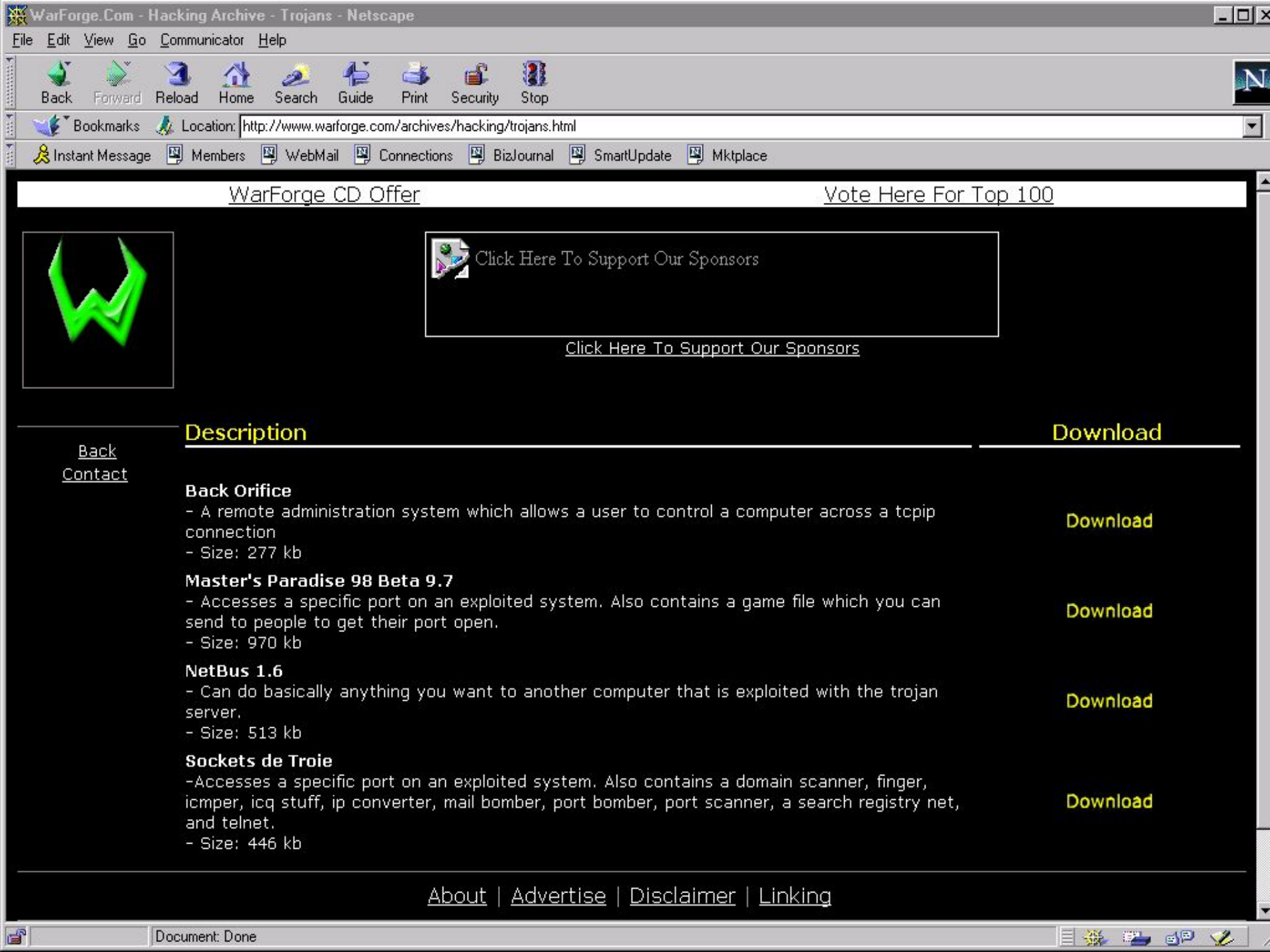
As the trojan Back Orifice is becoming more and more popular, many more people will become infected with the trojan. Information has been provided on how to remove the trojan, information about the program, and many other interesting features about Back Orifice.

- [AntiGen - Back Orifice Cleaner](#)
- [More information at Wired News](#)

New ICQ Number - 8/5/98

Please make sure that you add my new number to your ICQ list. My new number is 16709918. **Thank you.**

WarForge CD Now Available - 7/29/98



[WarForge CD Offer](#)

[Vote Here For Top 100](#)



[Click Here To Support Our Sponsors](#)

[Back](#)
[Contact](#)

Description

Download

Back Orifice

- A remote administration system which allows a user to control a computer across a tcpip connection
- Size: 277 kb

[Download](#)

Master's Paradise 98 Beta 9.7

- Accesses a specific port on an exploited system. Also contains a game file which you can send to people to get their port open.
- Size: 970 kb

[Download](#)

NetBus 1.6

- Can do basically anything you want to another computer that is exploited with the trojan server.
- Size: 513 kb

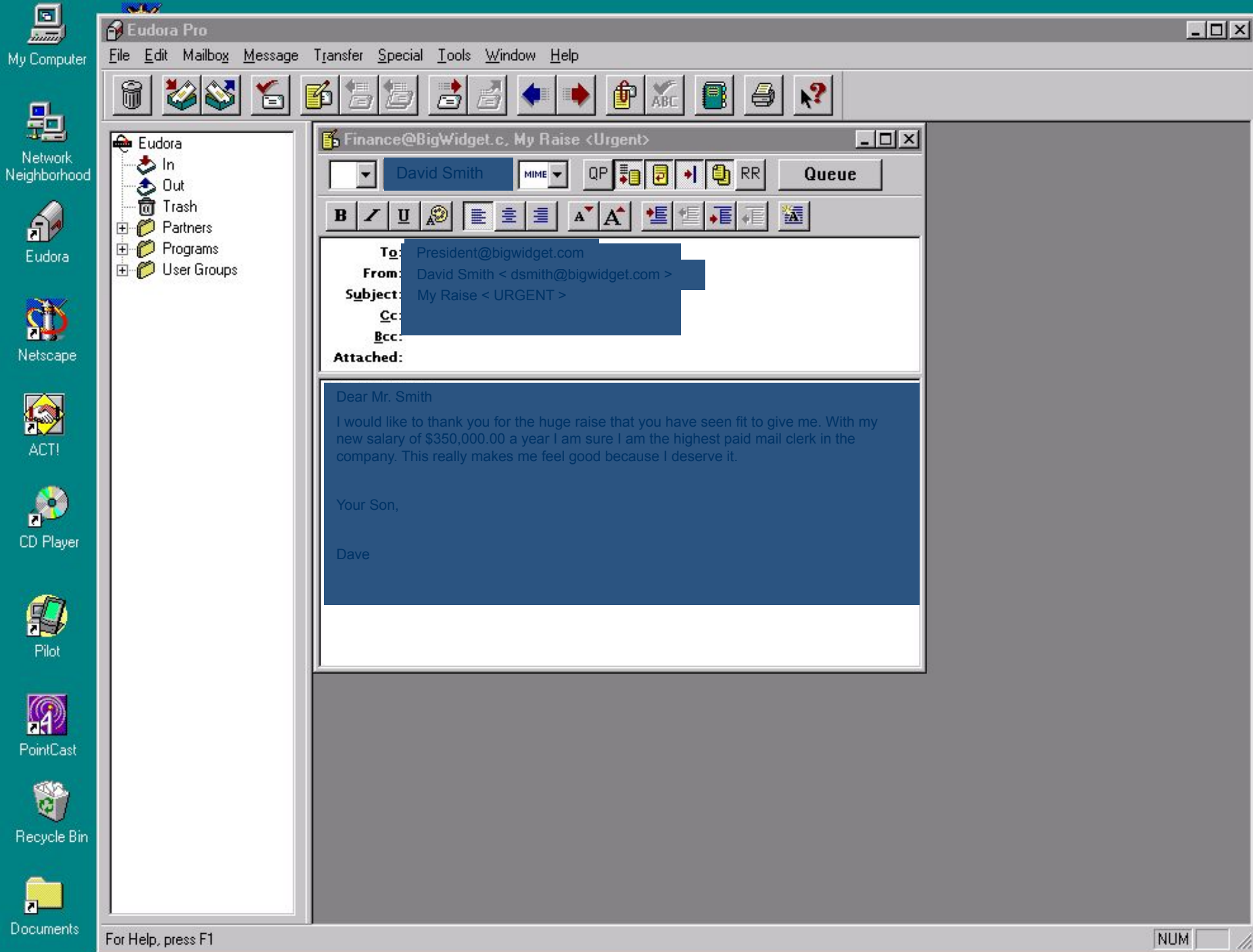
[Download](#)

Sockets de Troie

-Accesses a specific port on an exploited system. Also contains a domain scanner, finger, icmper, icq stuff, ip converter, mail bomber, port bomber, port scanner, a search registry net, and telnet.
- Size: 446 kb

[Download](#)

[About](#) | [Advertise](#) | [Disclaimer](#) | [Linking](#)



Eudora Pro

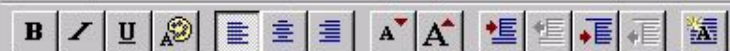
File Edit Mailbox Message Transfer Special Tools Window Help



- Eudora
 - In
 - Out
 - Trash
 - Partners
 - Programs
 - User Groups

Finance@BigWidget.c. My Raise <Urgent>

David Smith MIME QP RR Queue



To: President@bigwidget.com
From: David Smith <dsmith@bigwidget.com >
Subject: My Raise <URGENT >
Cc:
Bcc:
Attached:

Dear Mr. Smith
I would like to thank you for the huge raise that you have seen fit to give me. With my new salary of \$350,000.00 a year I am sure I am the highest paid mail clerk in the company. This really makes me feel good because I deserve it.

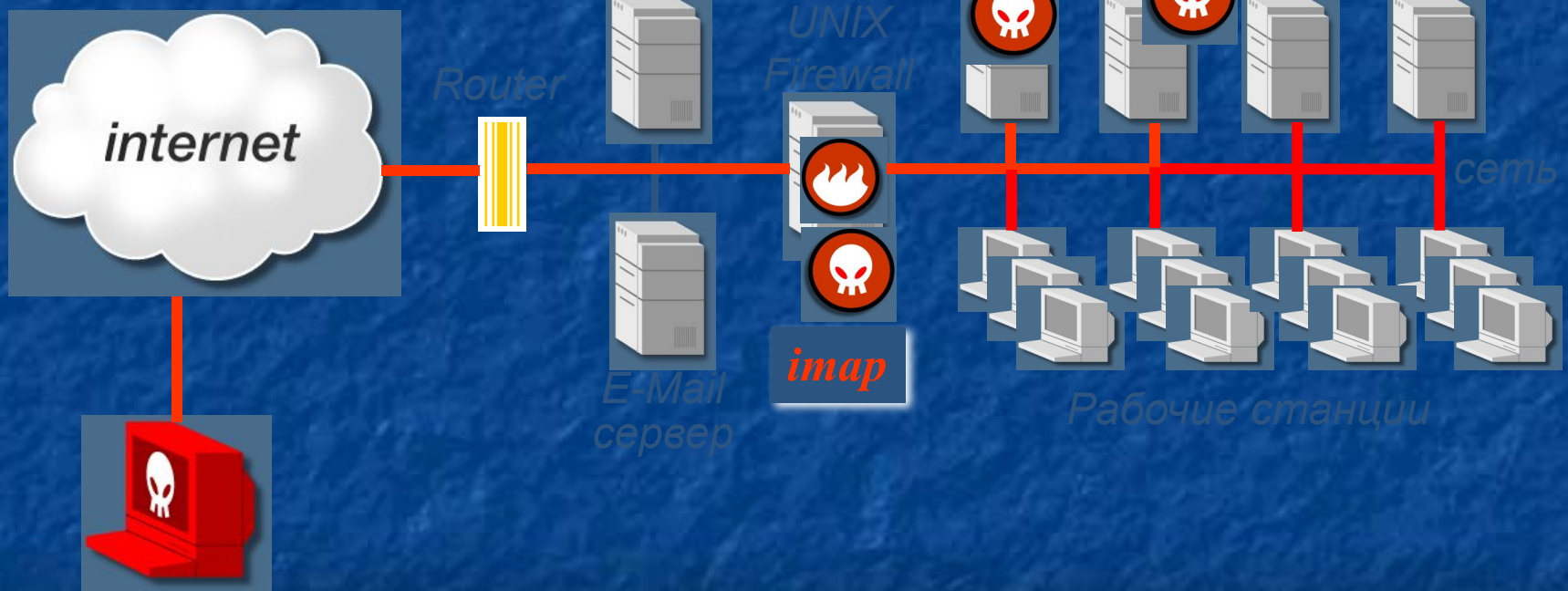
Your Son,

Dave

For Help, press F1

NUM

Сеть BigWidget



Web сервер

Router

UNIX Firewall

Crack

NetBus

UNIX

NT

UNIX

NT

сеть

E-Mail сервер

imap

Рабочие станции





BigWidget



The Part That Fits™

[Company](#) [Products](#) [Services](#) [Support](#)

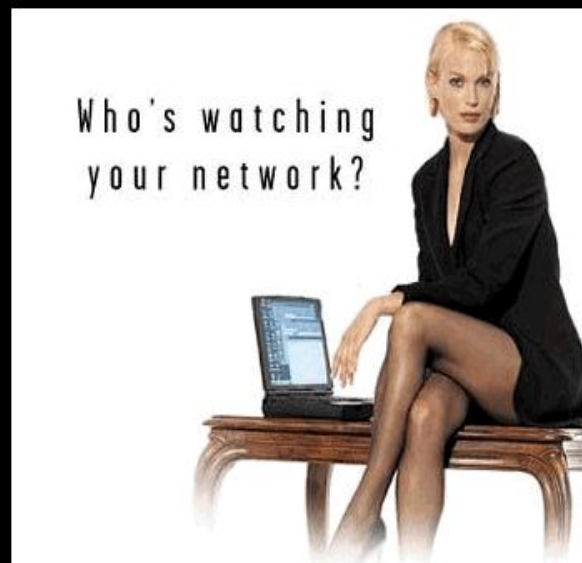


[BigWidget Announces Titanium Machining Capabilities](#)

BigWidget Incorporated announced today the purchase of a Consolidated Conglomerate abrasive waterjet cutter. This new machine will allow BigWidget to offer advanced machining services for titanium cogs and widgets.

[More News...](#)

- [BigWidget acquires Spacely Sprockets for \\$17.3 million](#)
- [BigWidget announces record third quarter earnings](#)








-  My Computer
-  ACDsee
-  Network Neighborhood
-  Microsoft Visual C++ 5.0
-  Internet Explorer
-  Outlook Express
-  Recycle Bin
-  w32Dasm
-  Winamp
-  Shortcut to prioritize...
-  Netscape Communicator
-  SMS Network Monitor
-  Yahoo Pager
-  UltraEdit-32 Text Editor
-  CD Player
-  Windows NT Explorer
-  CuteFTP
-  WinZip 6.3 32-bit
-  F-Secure SSH
-  Shortcut to Services
-  Shortcut to Server


Network Monitor


File Capture Tools Options Window Help









\Ethernet\NET1 Capture Window (Station Stats)

Time Elapsed: 00:00:00.000

% Network Utilization:

0 0 100

Frames Per Second:

0 0 100

Bytes Per Second:

0 0 1000

Network Address 1 1->2 1<-2 Network Address 2

Network Statistics

- # Frames: 0
- # Broadcasts: 0
- # Multicasts: 0
- # Bytes: 0
- # Frames Dropped: 0
- Network Status:

Captured Statistics

- # Frames: 0
- # Frames in Buffer: 0
- # Bytes: 0
- # Bytes in Buffer: 0
- % Buffer Utilized: 0
- # Frames Dropped: 0

Network Address	Frames Sent	Frames Rcvd	Bytes Sent	Bytes Rcvd	Directed Frames Sent	Multicasts Sent	Broadcasts Sent

Network Monitor V4.00.350



\Ethernet\NET1 Capture Window (Station Stats)

C:\temp.cap (Hex)

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
52	5.159	0060975946D8	00104B281213	TCP	.AP..., len: 20, seq: 979155133-979155152, ack:
53	5.305	00104B281213	0060975946D8	TCP	.A..., len: 0, seq: 69034-69034, ack: 97915
54	5.515	00104B281213	0060975946D8	TCP	.AP..., len: 20, seq: 69034-69053, ack: 97915
55	5.515	0060975946D8	00104B281213	TCP	.AP..., len: 15, seq: 4189009641-4189009655, ack:
56	5.529	0060975946D8	00104B281213	TCP	.A..., len: 0, seq: 979155153-979155153, ack:

IP: ID = 0x250D; Proto = TCP; Len: 55
 TCP: .AP..., len: 15, seq: 4189009641-4189009655, ack: 50405, win: 32120, src: 6109 dst: 110

TCP: Source Port = 0x17DD
 TCP: Destination Port = Post Office Protocol - Version 3
 TCP: Sequence Number = 4189009641 (0xF9AF36E9)
 TCP: Acknowledgement Number = 50405 (0xC4E5)
 TCP: Data Offset = 20 (0x14)
 TCP: Reserved = 0 (0x0000)

TCP: Flags = 0x18 : .AP...
 TCP: Window = 32120 (0x7D78)
 TCP: Checksum = 0xBC10
 TCP: Urgent Pointer = 0 (0x0)
 TCP: Data: Number of data bytes remaining = 15 (0x000F)

```

00000000  00 10 4B 28 12 13 00 60 97 59 46 D8 08 00 45 00  .K(...`ÿYF+..E.
00000010  00 37 25 0D 40 00 40 06 70 D7 D0 15 02 12 D0 15  .7%.@.@.p+-$..-$
00000020  02 A0 17 DD 00 6E F9 AF 36 E9 00 00 C4 E5 50 18  .á.|.n.»6T...sP.
00000030  7D 78 BC 10 00 00 75 73 65 72 20 6A 69 6D 73 6D  }x+...user jimsm
00000040  69 74 68 0D 0A                                     ith..
  
```



\Ethernet\NET1 Capture Window (Station Stats)

C:\temp.cap (Hex)

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
107	13.790	0060975946D8	00104B281213	TCP	.A...., len: 0, seq: 979155433-979155433, ack:
108	13.800	0060975946D8	00104B281213	TCP	.AP..., len: 20, seq: 979155433-979155452, ack:
109	13.919	00104B281213	0060975946D8	TCP	.A...., len: 0, seq: 69314-69314, ack: 97915!
110	14.499	00104B281213	0060975946D8	TCP	.AP..., len: 20, seq: 69314-69333, ack: 97915!
111	14.500	0060975946D8	00104B281213	TCP	.AP..., len: 15, seq:4189009656-4189009670, ack:

⊕ IP: ID = 0x268E; Proto = TCP; Len: 55

⊖ TCP: .AP..., len: 15, seq:4189009656-4189009670, ack: 50432, win:32120, src: 6109 dst: 110

TCP: Source Port = 0x17DD
 TCP: Destination Port = Post Office Protocol - Version 3
 TCP: Sequence Number = 4189009656 (0xF9AF36F8)
 TCP: Acknowledgement Number = 50432 (0xC500)
 TCP: Data Offset = 20 (0x14)
 TCP: Reserved = 0 (0x0000)

⊕ TCP: Flags = 0x18 : .AP...
 TCP: Window = 32120 (0x7D78)
 TCP: Checksum = 0x4EA7
 TCP: Urgent Pointer = 0 (0x0)

TCP: Data: Number of data bytes remaining = 15 (0x000F)

00000000	00 10 4B 28 12 13 00 60 97 59 46 D8 08 00 45 00	..K(...`ùYF+..E.
00000010	00 37 26 8E 40 00 40 06 6F 56 D0 15 02 12 D0 15	.7&Ä@.@.oV-\$..-\$
00000020	02 A0 17 DD 00 6E F9 AF 36 F8 00 00 C5 00 50 18	.á.!.n*»6°.+.P.
00000030	7D 78 4E A7 00 00 70 61 73 73 20 65 6C 31 74 33	}xN*..pass ellt3
00000040	21 21 21 0D 0A	!!!..



Router



Web сервер



E-Mail сервер



UNIX Firewall



UNIX



NT



UNIX



NT



Сеть



Рабочие станции

Вопросы