

”His computer virus crashed 1507 systems including Wall Street trading systems, single-handedly causing a seven point drop in the New York stock market.”

THEIR CRIME IS CURIOSITY

HACKERS

BOOT UP OR SHUT UP!

UNITED ARTISTS PICTURES PRESENTS AN IAIN SOFTLEY FILM "HACKERS" JOHNNY LEE MILLER ANGELINA JOLIE FISHER STEVENS AND LORRAINE BRACCO MUSIC BY SIMON BOSWELL
EDITED BY CHRISTOPHER BLUNDEN MARTIN WALSH PRODUCTION DESIGNER JOHN BEARD DIRECTOR OF PHOTOGRAPHY ANDRZEJ SEKULA EXECUTIVE PRODUCER IAIN SOFTLEY CO-PRODUCER JANET GRAHAM
WRITTEN BY RAFAEL MOREU PRODUCED BY MICHAEL PEYSER RALPH WINTER DIRECTED BY IAIN SOFTLEY

ON LINE - THIS FALL

UNITED
ARTISTS

WANTED

BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ V721460021).

NAME:MITNICK, KEVIN DAVID

AKS (S):MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex:MALE
Race:WHITE
Place of Birth:VAN NUYS, CALIFORNIA
Date(s) of Birth:08/06/63; 10/18/70
Height:5'11"
Weight:190
Eyes:BLUE
Hair:BROWN
Skin tone:LIGHT
Scars, Marks, Tattoos:NONE KNOWN
Social Security Number (s):550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09



ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS

VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.

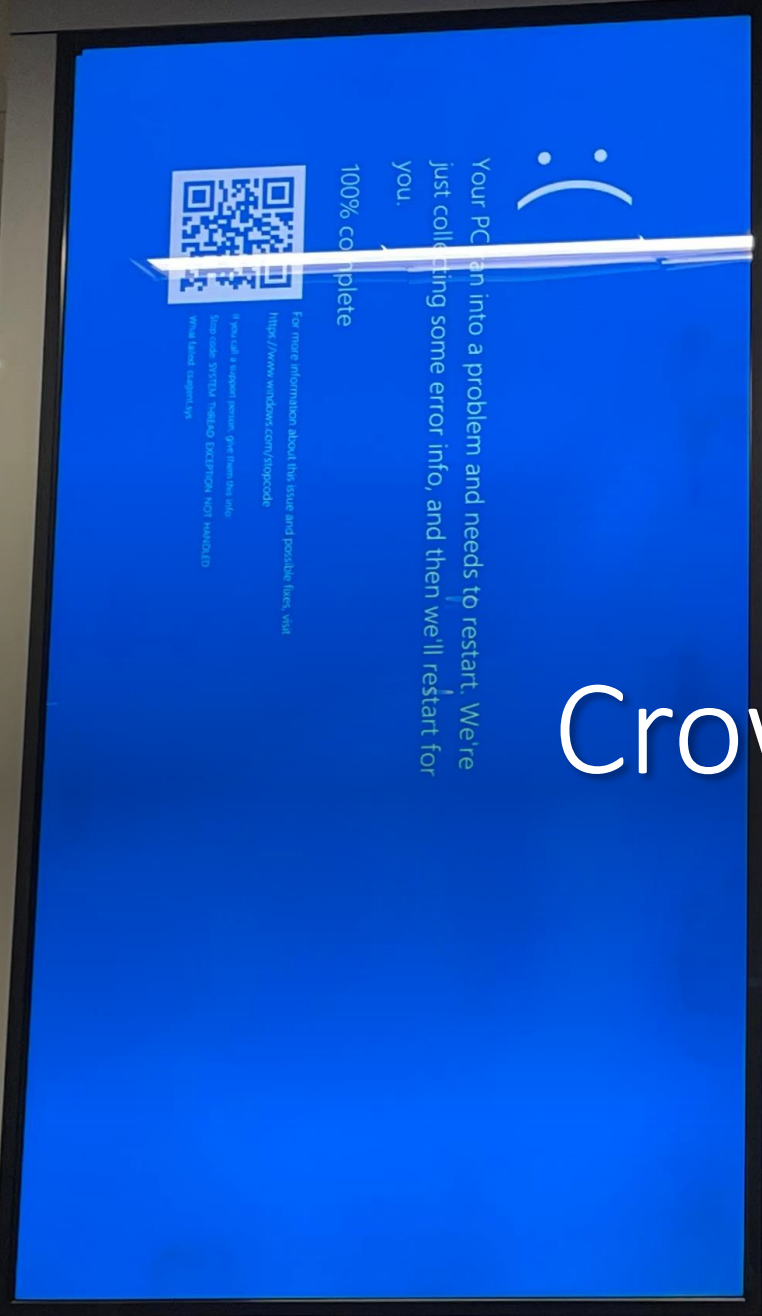
Telephone (800)336-0102: (24 hour telephone contact) NLETS access code is VAUSM0000.



”His computer virus crashed 1507 systems including Wall Street trading systems, single-handedly causing a seven point drop in the New York stock market.”

-
- An unknown number of Linux systems affected
 - 8.5 million Windows devices affected
 - Total financial losses are at least \$15 billion

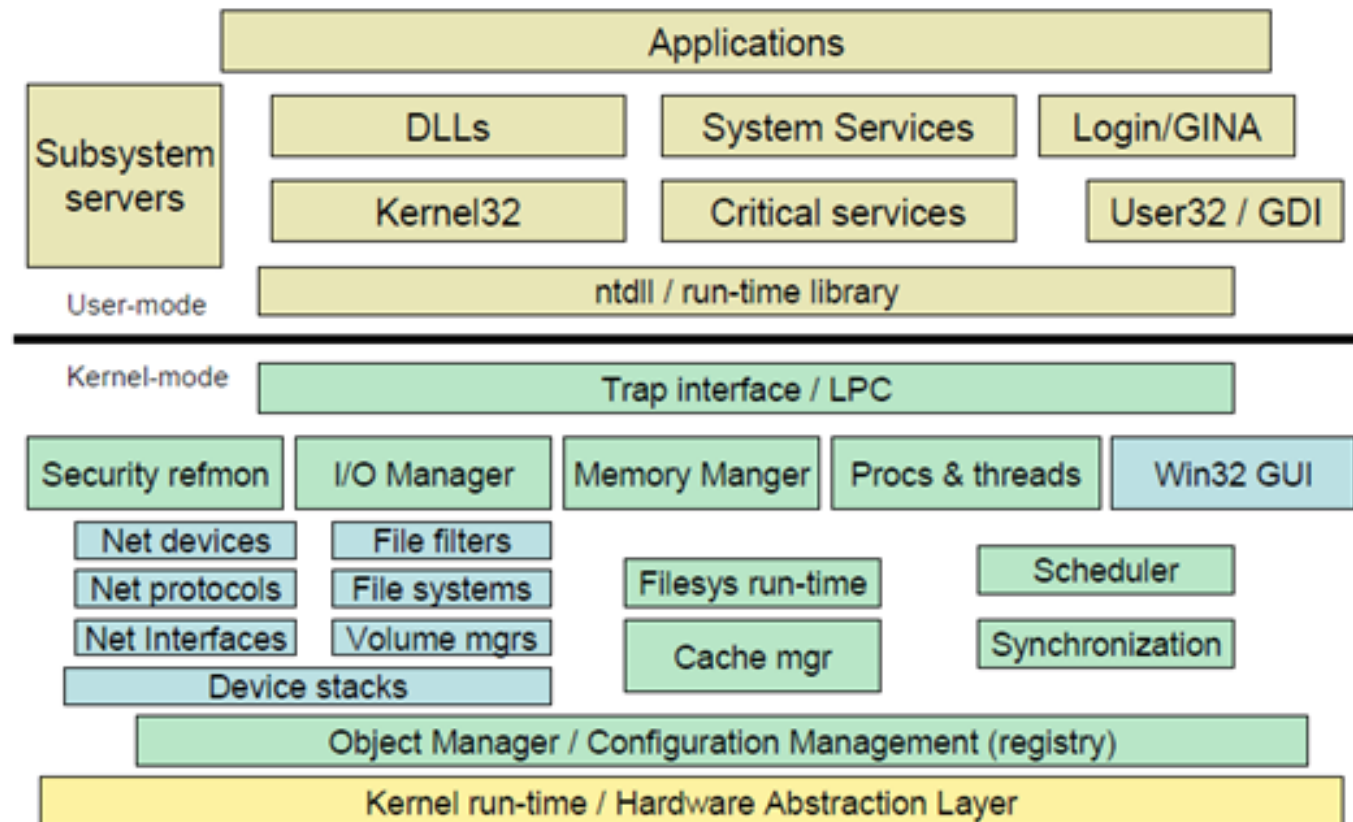
CrowdStrike



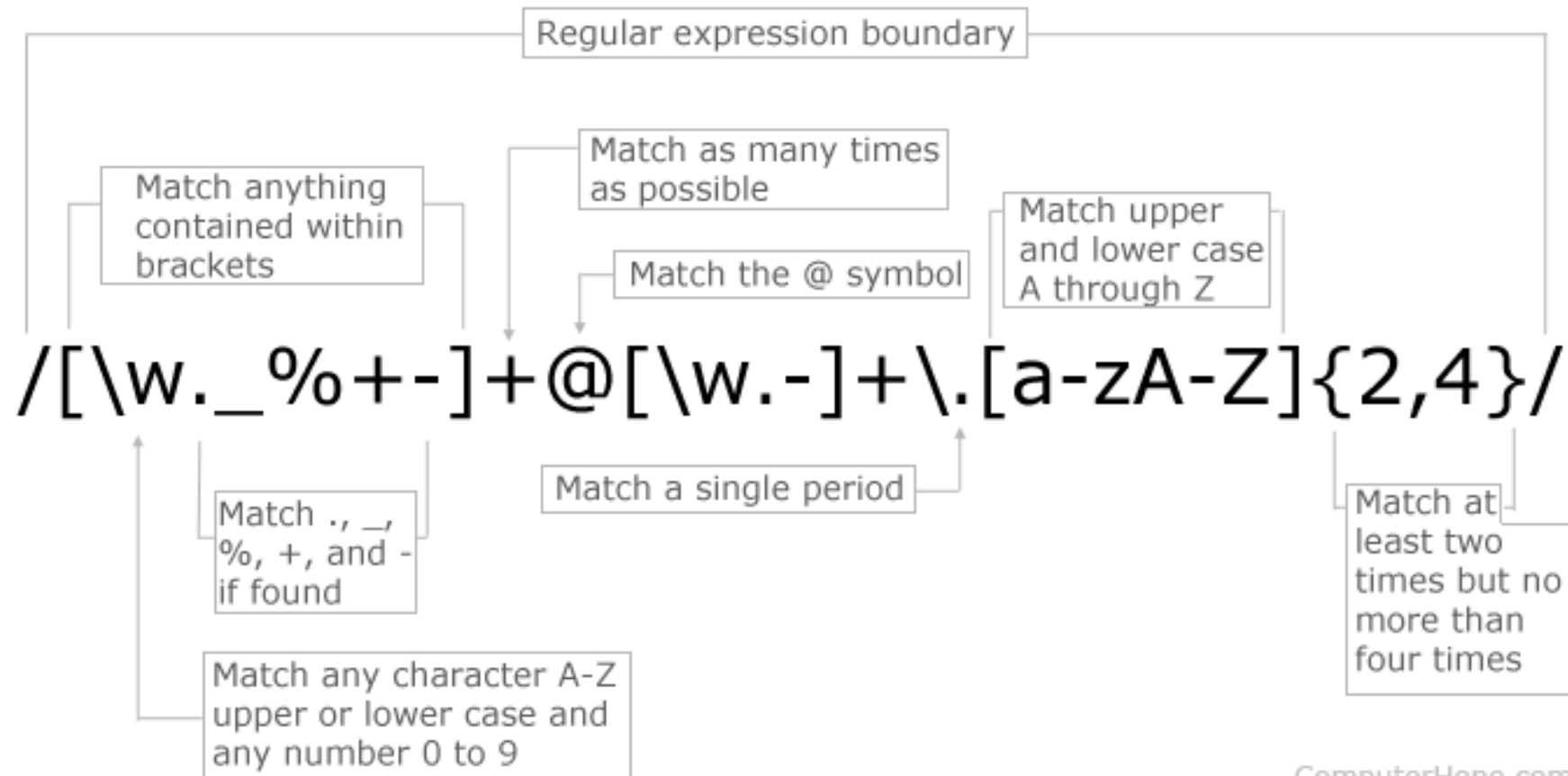
 Clear Channel



Windows Architecture




Regular Expression E-mail Matching Example





CrowdStrike Falcon

- Enterprise level endpoint protection
- Uses AI for some parts
- Template instance files containing regular expression templates
- Partly a kernel-mode driver
- Marked as Early Launch AntiMalware
- New ability to analyze Windows Interprocess Communication (IPC) (February 2024)

- 
- Content Interpreter
 - Template Types
 - Template Type Definitions file
 - Template Instances

ContentInterpreter(TemplateInstance template, TemplateInput[] templateInputs)



Out of Bounds Read




Your PC ran into a problem and needs to restart.
Restart will be available:(15% completed)

You can search for this error online: `HAL_INITIALIZATION_FAILED`

How did we
get here?



- 
- Content Interpreter
 - Template Types
 - Template Type Definitions file
 - Template Instances
 - Content Validator
 - Content Configuration System
 - Channel Files

No validation that number of inputs in
Template Type code matched Template
Type Definition

No validation of expected vs given input
length in Content Interpreter

Template Type testing only uses a few
handcrafted Template Instances

Logic error in the Content Validator with
regards to input length

Content Interpreter not used when
testing Template Instances

Template Instances didn't have a
staged deployment



What can
we learn?

Test your code

Test configuration changes

Use staged deploys

Everybody can make mistakes

Communicate good when shit happens

What can you learn?
Think about it.



jakob@jakobcarlsson.se