SecureIT New York

Protecting the enterprise: Threats, risk and AI

PRODUCED BY CSO | IDC

FANCY BEAR GOES PHISHING

THE DARK HISTORY OF THE INFORMATION AGE, IN FIVE EXTRAORDINARY HACKS

SCOTT J. SHAPIRO

How can the history of hacking tell us anything about future cyber threats?

Cybersecurity:
Technical problems, Engineering solutions

SecureIT New York

CSO | IDC

Cybersecurity:
Human problems, Human solutions

SecureIT New York

CSO | IDC

CORNELL SUSPENDS COMPUTER STUDENT

School Says He Was Author of Program That Jammed a Nationwide Network

How a Need for Challenge Seduced Computer Expert

By JOHN MARKOFF

Robert Tappan Morris spent many weeks painstakingly creating the computer "virus" that beleaguered many of the nation's computer networks Wednesday night and Thursday.

By all accounts the 23-year-old computer science student intended no harm. But in the end, working with great intensity and little sleep, he made a single programming error that ultimately jammed more than 6,000 computers in what is being called this country's most serious computer "virus" attack.

That mistake also brought Robert Morris's life crashing down around him, three friends have told The New York Times. He quickly recognized that things had gone terribly wrong and, they disclosed, he arranged for a friend to send out instructions on eradicating the virus to the same computers plagued by it. But, in another miscue, the instructions were electronically posted in a place where few would see them.

Harvard University

Robert T. Morris, who created the computer virus.

Exploring the Crannies

Then he turned himself in to his father, Robert Morris, a top Government expert on computer security. The elder Mr. Morris said he met with F.B.I. agents yesterday to discuss the matter.

Also yesterday, officials at Cornell University, where the younger Morris is a first-year graduate student in computer science, said they had discovered that his computer files had a list of passwords like those found in the computer virus.

Computer viruses are the computer equivalent of biological viruses, spreading largely on their own from computer to computer. They consume computer processing power and storage space and can sometimes destroy stored information.

The case, with all its bizarre twists, illuminates the cerebral world of a father and son — and indeed a whole modern subculture — obsessed with the intellectual challenge of exploring the in-

Continued on Page 30, Column 1

Student Blamed for Rogue Computer Program

By JOHN MARKOFF

A Cornell University commission said yesterday that a graduate student in computer science, working alone, created the rogue program that produced havoc in nationwide computer networks last November.

The commission, which was formed to investigate the incident, issued a report calling the work of the student, Robert Tappan Morris, "a juvenile act that ignored the clear potential consequences." In reviewing the ethical issues raised by Mr. Morris's program,

Morris was a 'completely absorbed' hacker.

the commission said, "It may have been the unfocused intellectual meanderings of a hacker completely absorbed with his creation."

The program released by Mr. Morris last November rapidly copied itself into computers through an interconnected series of computer networks, the Internet, infecting as many as 6,000 computers at universities, private corporations and military installations.

The program did not destroy data, but slowed the computers and in some cases caused them to cease operations because they were overloaded. Computer managers around the country spent days working to restore their computer systems to normal operations, and the incident raised serious concerns about the security of the nation's computers.

Provost Robert Barker of Cornell said the university was beginning a disciplinary proceeding against Mr. Morris now that the report was complete.

The involvement of Mr. Morris, at the time a first-year graduate student in computer science, has been widely reported. However, Mr. Morris, who received a leave of absence from Cornell last year, has not publicly commented on whether he was responsible for the program.

No charges have been brought as a result of the incident. A Federal attorney in New York State recommended that Mr. Morris be charged with a single misdemeanor count for writing the program, law-enforcement officials said in late January.

No Decision on Prosecution

But the Justice Department rejected the recommendation because some senior officials said Mr. Morris should be more severely punished, said a law-enforcement official who asked not to be identified. The department has not yet decided if Mr. Morris will be prosecuted for violating more serious computer abuse statutes.

The commission did not attempt to estimate the amount of damage done by the program. A report by an industry association for computer security saying that the program cost about $96 million was called "grossly exaggerated" and "self serving" by the Cornell commission, which said the industry group overvalued the cost of computer downtime.

Two Arrested in

Special to The New

MIAMI, April 3 — The Dade County police said today that they had arrested two suspects over the weekend and were looking for up to three more suspects in the March 20 killing of a grocery store owner who had waged a campaign against drug dealers in his neighborhood.

The police said the two suspects, who did not know the grocer, 51-year-old Arthur Lee Lawrence, had been hired to execute him. But pending further arrests, the police refused to say who they believe hired the killers or how much they were paid.

The police, at a news conference this afternoon, said they would not comment on the specific motive for the killing until the arrests had been completed.

Family members and friends of Mr. Lawrence have speculated that he was gunned down because he had antagonized drug dealers in West Perrine, a community just south of Miami where he lived and ran the store.

The two arrested were Ronnie John-

The long read

On the trail of the Dark Avenger: the most dangerous virus writer in the world

Bulgaria in the 1980s became known as the 'virus factory', where hundreds of malicious computer programs were unleashed to wreak havoc. But who was writing them, and why?

by Scott J Shapiro

WANTED BY THE FBI

CONSPIRACY TO COMMIT AN OFFENSE AGAINST THE UNITED STATES; FALSE REGISTRATION OF A DOMAIN NAME; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS


Boris Alekseyevich Antonov


Dmitriy Sergeyevich Badin


Anatoliy Sergeyevich Kovalev


Nikolay Yuryevich Kozachek

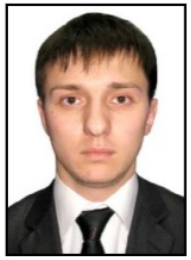

Aleksey Viktorovich Lukashev


Artem Andreyevich Malyshev


Sergey Aleksandrovich


Aleksandr Vladimirovich


Aleksey Aleksandrovich


Ivan Sergeyevich Yermakov


Pavel Vyacheslavovich

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediat

CHANGE PASSWORD

Secur

__PATCH_ME_IF_YOU_CAN___

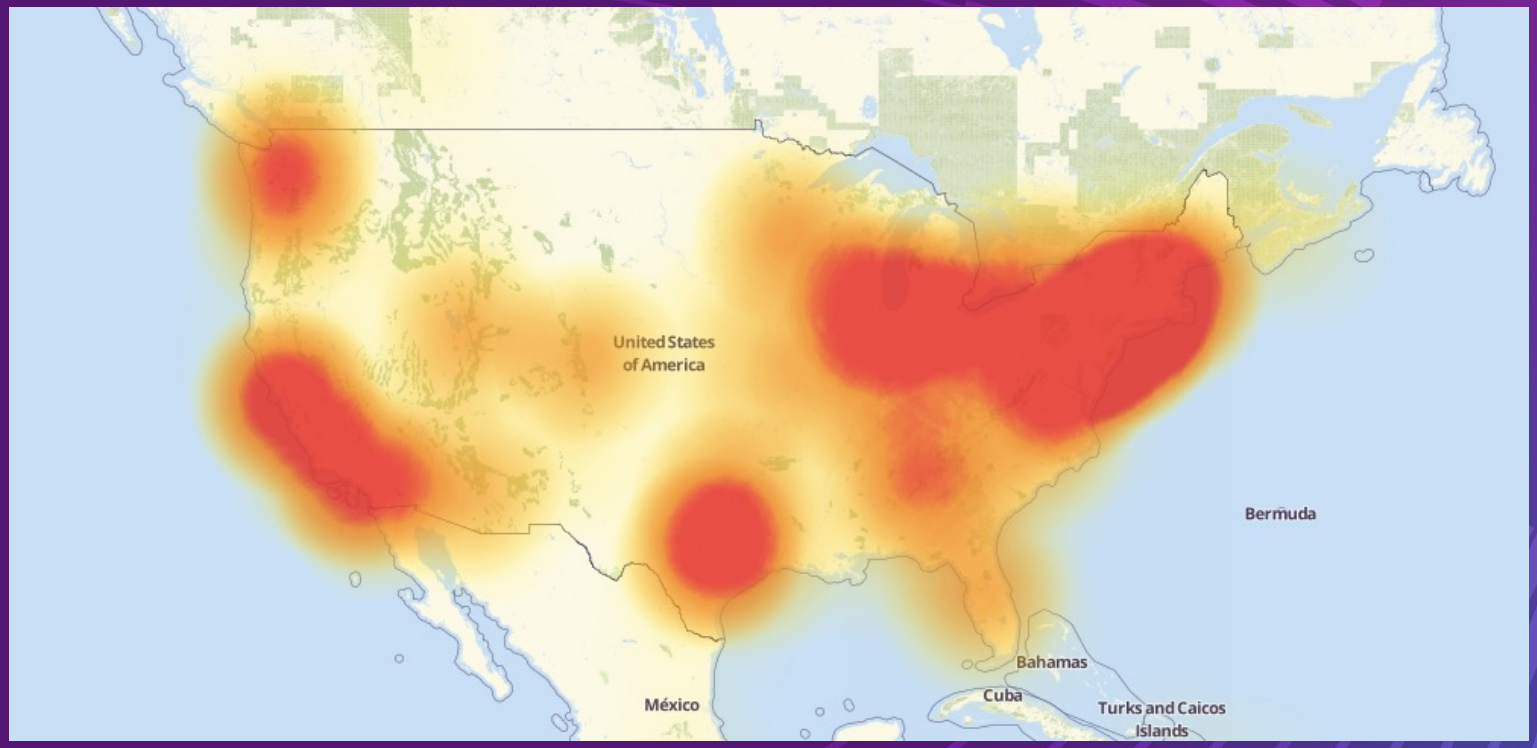
How a New Jersey teenager's malware threatened the entire Internet

By Scott J. Shapiro

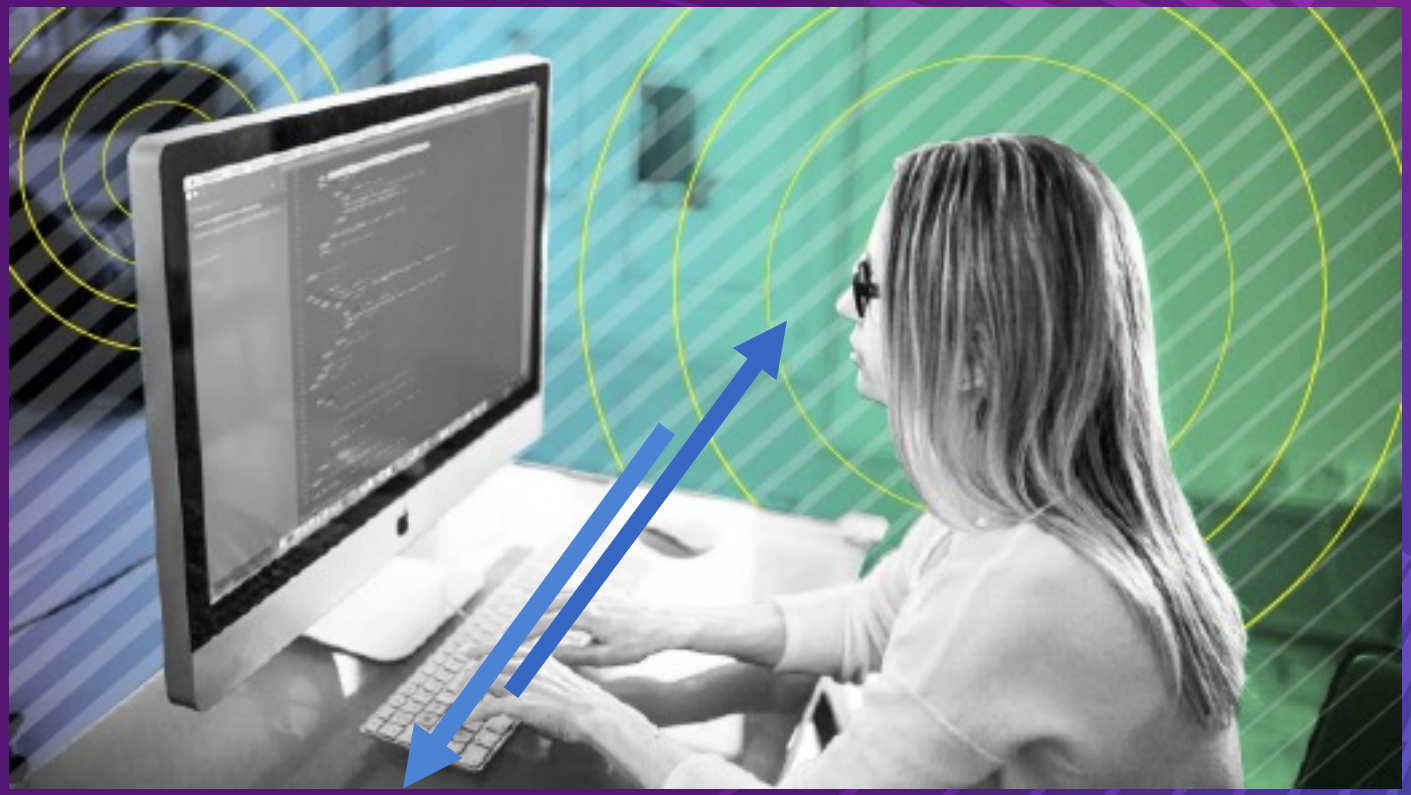
ILLUSTRATION BY MIKE MCQUADE

IDC

October 21, 2016



Upcode/Downcode



Varieties of Downcode

- Microcode
- Machine/Assembly code/Binaries
- Applications
- OS
- Drivers
- Firmware
- Hypervisors
- Network
- Internetwork
- InterAS
- DNS
- API's
- Repositories
- Worms/viruses/Trojans/rootkits

Downcode: Run by computers

Upcode: Run by humans

Varieties of Upcode

- Psychological (System 1 and System 2)
- Personal (ethics, habits, rituals, plans, projects)
- Economic (Terms of service, Employment K, property rules)
- Organizational (corporate, platforms)
- Industrial (internet governance)
- Social (ethics, habits, rituals, projects)
- Legal (domestic, international)

Upcode→Downcode

1) Upcode changes incentives to produce downcode
2) Upcode creates data used by downcode

Notes from Paris Hilton's Sidekick phone

- tell ken about jess trying to bone JT
- Do you wanna leave soon, ill pretend I hsve 2 go pee and u wait 3 mins than come by yourself to the back entrance
- Victor magic tan representative.
- that's hot tank tops like chrome hearts iold english writinh that's hot
- call maroon 5 get birth control kill pill [*Ed: We can relate to this last one* —

How did Cameron Lacroix Hack Paris Hilton's Phone?

1. Bluesnarfing

How did Cameron Lacroix Hack Paris Hilton's Phone?

1. Bluesnarfing
2. **Evil Maid Attack**

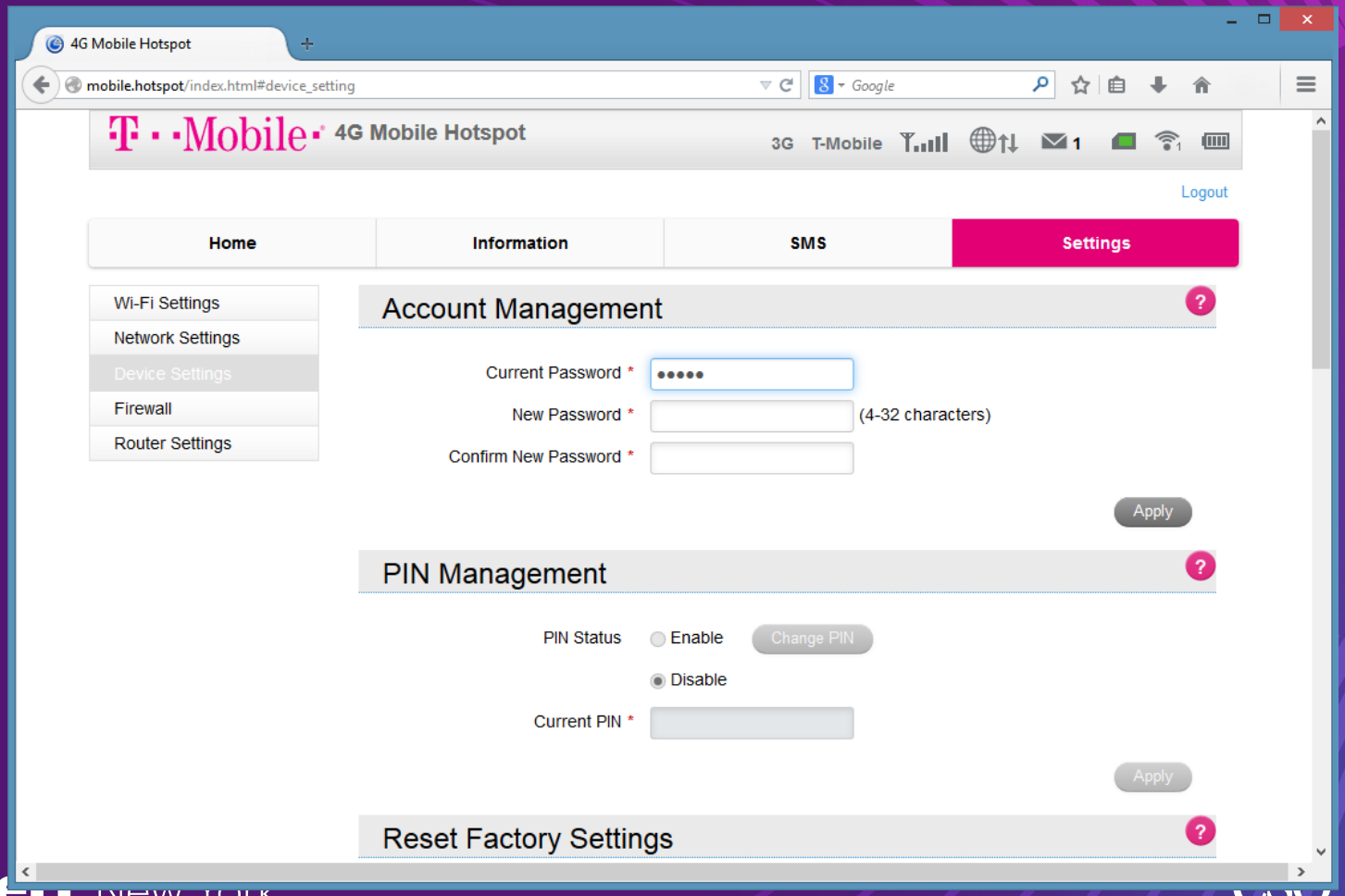
How did Cameron Lacroix Hack Paris Hilton's Phone?

1. Bluesnarfing
2. Evil Maid Attack
3. **Guessing Password**

How did Cameron Lacroix Hack Paris Hilton's Phone?

1. Bluesnarfing
2. Evil Maid Attack
3. Guessing Password
4. **Guessing Security Question**


T · ·Mobile·
VISITING THE U.S.?
SAMSUNG
VISITING THE U.S.?
223A


4G Mobile Hotspot
mobile.hotspot/index.html#device_setting
Google
T-Mobile 4G Mobile Hotspot
3G T-Mobile
Logout
Home
Information
SMS
Settings
Wi-Fi Settings
Network Settings
Device Settings
Firewall
Router Settings
Account Management
Current Password *
New Password *
(4-32 characters)
Confirm New Password *
Apply
PIN Management
PIN Status
Enable
Change PIN
Disable
Current PIN *
Apply
Reset Factory Settings

Vulnerabilities

1) Authentication error
2) Winner take all economics with no liability
3) Insecure corporate policies for managers
4) Social imperative to be famous


© NBC

THANK YOU!