Computer Security

06. Malware

Paul Krzyzanowski

Rutgers University

Fall 2019

July 29, 2019: URGENT/11

11 critical vulnerabilities found in Wind River VxWorks, a Real Time Operation System (RTOS)

- Most vulnerabilities relate to the TCP/IP stack (IPnet)
  - Six vulnerabilities enable Remote Code Execution
- Other operating systems used the same network stack
  - VxWorks, ENEA's Operating System Embedded (OSE), GreenHills INTEGRITY, Microsoft ThreadX, TON's ITRON, IP Infusion's ZebOS
- FDA issued an alert on October 1, 2019
- Billions of embedded devices exposed: firewalls, routers, modems, VoIP phones, printers, SCADA systems (industrial controllers), patient monitors, MRI machines

https://www.armis.com/urgent11/

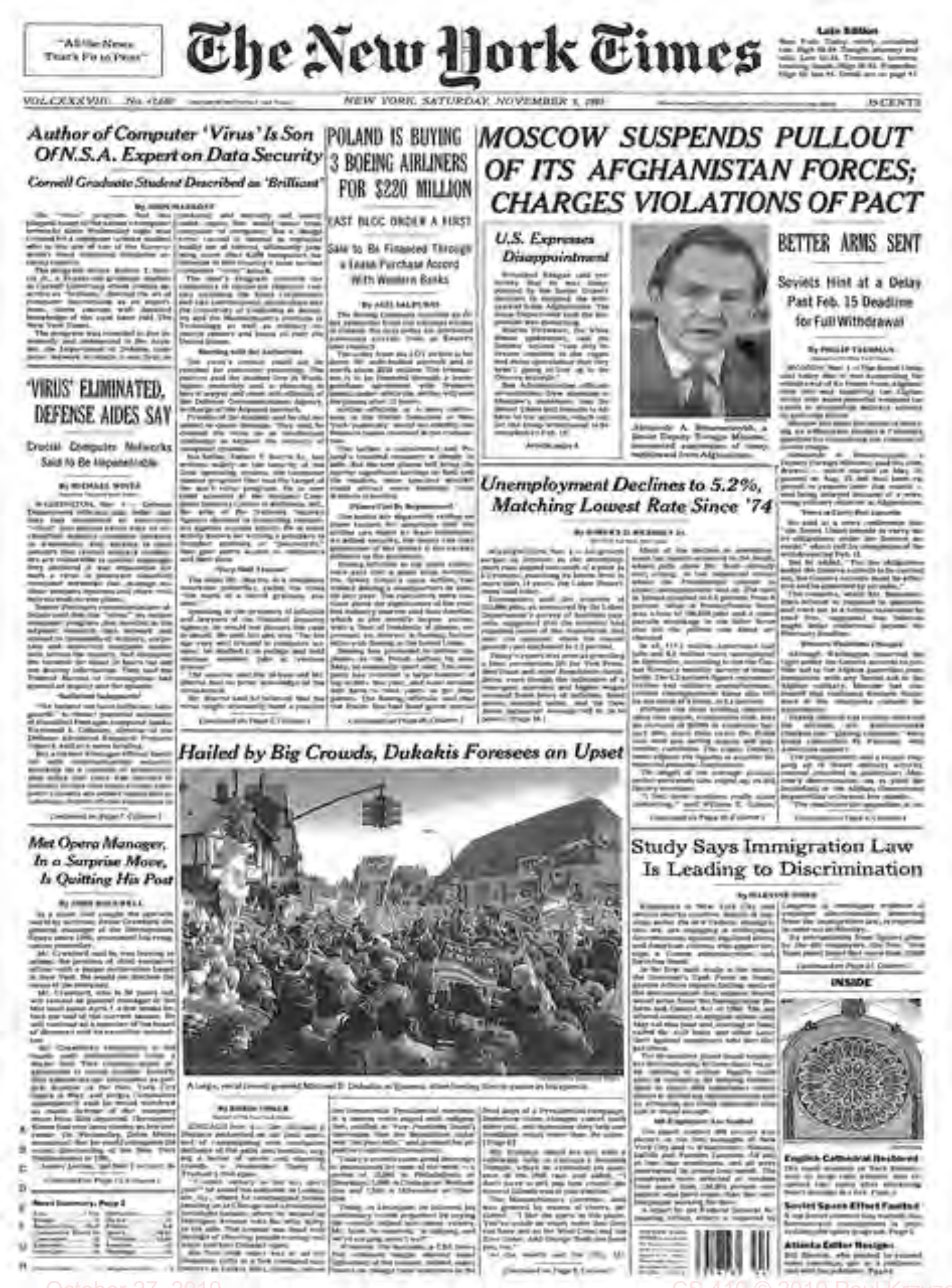
https://www.forescout.com/company/blog/solving-urgent11-identifying-vxworks-and-defending-ot-devices/

URGENT/11 Vulnerabilities

1. Use of the Urgent Pointer field in a TCP header
   If set to 0, it will cause an integer underflow
2. Stack buffer overflow in parsing IP options
3. Heap overflow in DHCP offer/ack parsing
4. DoS of TCP connection via malformed TCP options
5. DoS via NULL dereference in IGMP (IP multicast) parsing
6. TCP Urgent Pointer state confusion via malformed TCP authentication option
7. TCP Urgent Pointer state confusion during connect
8. Improper handling of unsolicited Reverse ARP replies
9. TCP Urgent Pointer state confusion due to race condition
10. Flow in IP address assignment by DHCP due to a bad address in a DHCP response
11. IGMP information leak via membership report

https://www.forescout.com/company/blog/solving-urgent11-identifying-vxworks-and-defending-ot-devices/

November 5, 1988



"All the News That's Fit to Print"

The New York Times

Late Edition

NEW YORK, SATURDAY, NOVEMBER 5, 1988

Author of Computer 'Virus' Is Son Of N.S.A. Expert on Data Security

Cornell Graduate Student Described as 'Brilliant'

'VIRUS' ELIMINATED, DEFENSE AIDES SAY

Crucial Computer Networks Said to Be Impenetrable

POLAND IS BUYING 3 BOEING AIRLINERS FOR $220 MILLION

EAST BLOC ORDER A FIRST

Sale to Be Financed Through a Lease-Purchase Accord With Western Banks

MOSCOW SUSPENDS PULLOUT OF ITS AFGHANISTAN FORCES; CHARGES VIOLATIONS OF PACT

U.S. Expresses Disappointment

BETTER ARMS SENT

Soviets Hint at a Delay Past Feb. 15 Deadline for Full Withdrawal

Unemployment Declines to 5.2%, Matching Lowest Rate Since '74

Hailed by Big Crowds, Dukakis Foresees an Upset

Met Opera Manager, In a Surprise Move, Is Quitting His Post

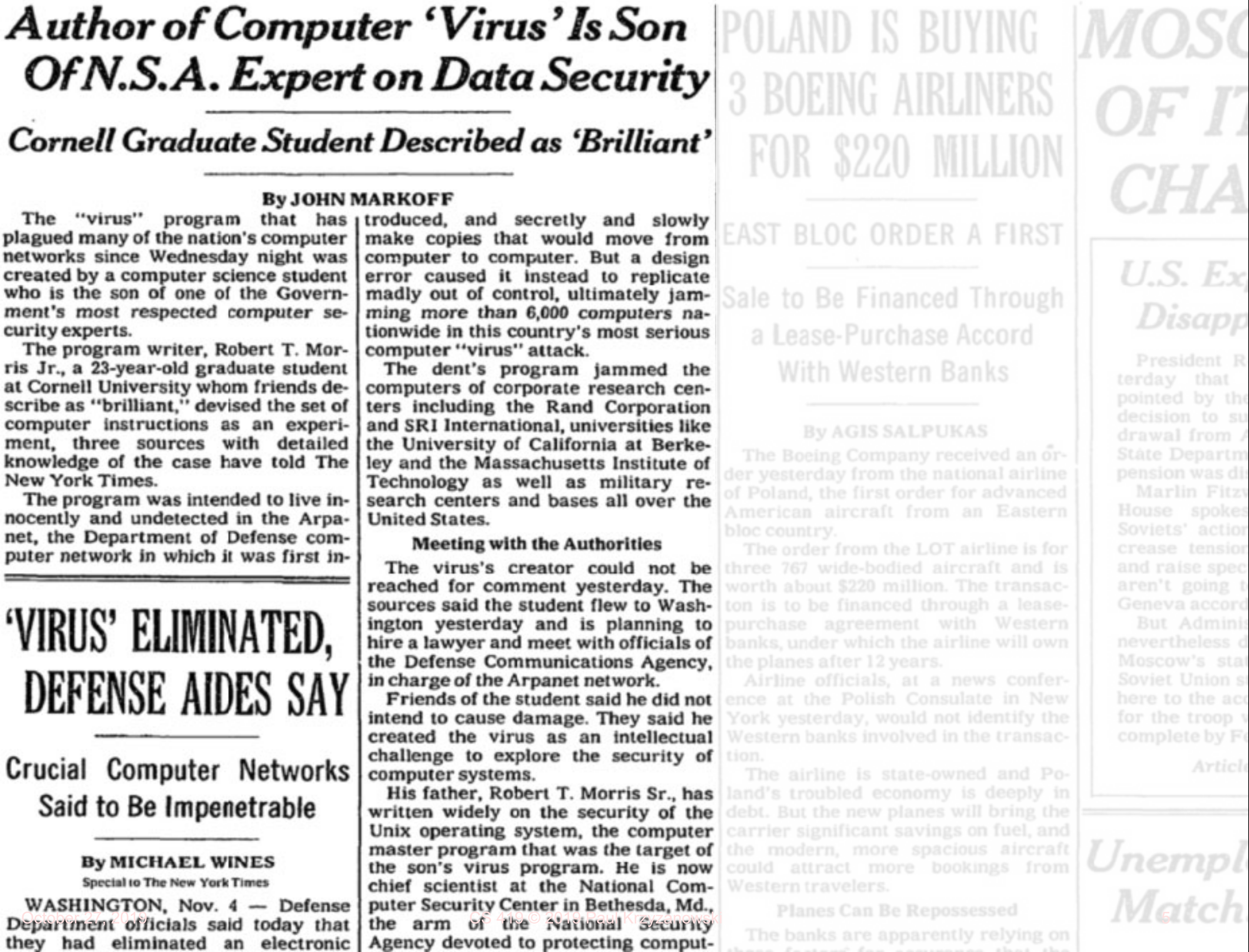
Study Says Immigration Law Is Leading to Discrimination

INSIDE

English Cathedral Restored

Soviet Space Effort Faulted

Atlanta Editor Resigns



Author of Computer 'Virus' Is Son Of N.S.A. Expert on Data Security

Cornell Graduate Student Described as 'Brilliant'

By JOHN MARKOFF

The "virus" program that has plagued many of the nation's computer networks since Wednesday night was created by a computer science student who is the son of one of the Government's most respected computer security experts.

The program writer, Robert T. Morris Jr., a 23-year-old graduate student at Cornell University whom friends describe as "brilliant," devised the set of computer instructions as an experiment, three sources with detailed knowledge of the case have told The New York Times.

The program was intended to live innocently and undetected in the Arpanet, the Department of Defense computer network in which it was first introduced, and secretly and slowly make copies that would move from computer to computer. But a design error caused it instead to replicate madly out of control, ultimately jamming more than 6,000 computers nationwide in this country's most serious computer "virus" attack.

The dent's program jammed the computers of corporate research centers including the Rand Corporation and SRI International, universities like the University of California at Berkeley and the Massachusetts Institute of Technology as well as military research centers and bases all over the United States.

Meeting with the Authorities

The virus's creator could not be reached for comment yesterday. The sources said the student flew to Washington yesterday and is planning to hire a lawyer and meet with officials of the Defense Communications Agency, in charge of the Arpanet network.

Friends of the student said he did not intend to cause damage. They said he created the virus as an intellectual challenge to explore the security of computer systems.

His father, Robert T. Morris Sr., has written widely on the security of the Unix operating system, the computer master program that was the target of the son's virus program. He is now chief scientist at the National Computer Security Center in Bethesda, Md., the arm of the National Security Agency devoted to protecting comput-

'VIRUS' ELIMINATED, DEFENSE AIDES SAY

Crucial Computer Networks Said to Be Impenetrable

By MICHAEL WINES

Special to The New York Times

WASHINGTON, Nov. 4 — Defense Department officials said today that they had eliminated an electronic

POLAND IS BUYING 3 BOEING AIRLINERS FOR $220 MILLION

EAST BLOC ORDER A FIRST

Sale to Be Financed Through a Lease-Purchase Accord With Western Banks

By AGIS SALPUKAS

The Boeing Company received an order yesterday from the national airline of Poland, the first order for advanced American aircraft from an Eastern bloc country.

The order from the LOT airline is for three 767 wide-bodied aircraft and is worth about $220 million. The transacton is to be financed through a lease-purchase agreement with Western banks, under which the airline will own the planes after 12 years.

Airline officials, at a news conference at the Polish Consulate in New York yesterday, would not identify the Western banks involved in the transaction.

The airline is state-owned and Poland's troubled economy is deeply in debt. But the new planes will bring the carrier significant savings on fuel, and the modern, more spacious aircraft could attract more bookings from Western travelers.

Planes Can Be Repossessed

The banks are apparently relying on

MOSC OF IT CHA

U.S. Ex Disapp

President R terday that pointed by the decision to su drawal from A State Departm pension was di

Marlin Fitzw House spokes Soviets' action crease tension and raise spec aren't going t Geneva accord

But Adminis nevertheless d Moscow's sta Soviet Union s here to the acc for the troop w complete by Fe

Article

Unempl Match

Robert Tappan Morris Jr.'s Internet Worm

Attacked VAX systems running BSD

1. Attempt to crack local passwords
   - Guess passwords via dictionary attack
   - 432 common passwords and combinations of account name and user name
2. Look for readable .rhost files – that may give you free *rsh* access to another system
3. Do a buffer overflow exploit on *fingerd* via *gets* to load a small program
   - 99 lines of C
   - Program connects to sender and downloads the full worm
4. Use the DEBUG command of *sendmail*
   - Allowed remote command execution on a remote system

Then repeat … propagate the program onto any system it could log into

Robert Tappan Morris Jr.’s Internet Worm

Attacked DEC VAX systems running BSD

1. Attempt to crack local passwords
2. Look for readable .rhost files
3. Do a buffer overflow exploit on *fingerd* via *gets* to load a small program
4. Use the DEBUG command of *sendmail*

Then repeat … propagate the program onto any system it could log into

Malware

Etymology

Mal = prefix: bad, wrong

French *mal*; Old French *mal;* Latin *male/malus/mala*

Ware = suffix: software

Proto-Germanic *warjaz* (“dwellers of”)

Any malicious software

- Viruses
- Worms
- Trojan horses
- Spyware
- Adware
- Backdoors
- Ransomware

Motivation

- Steal account credentials
  - Get credentials for other systems
- Espionage
  - Steal content
  - Spyware: monitor user activity
- Sabotage: destroy content or connected devices
- Host services
  - Host contraband data
  - Send spam
  - Mine cryptocurrency
  - Botnet for DDoS attacks
- $$$ – ransomware

Infiltration mechanisms

Some ways in which malware enters a system

How does malware get onto a computer?

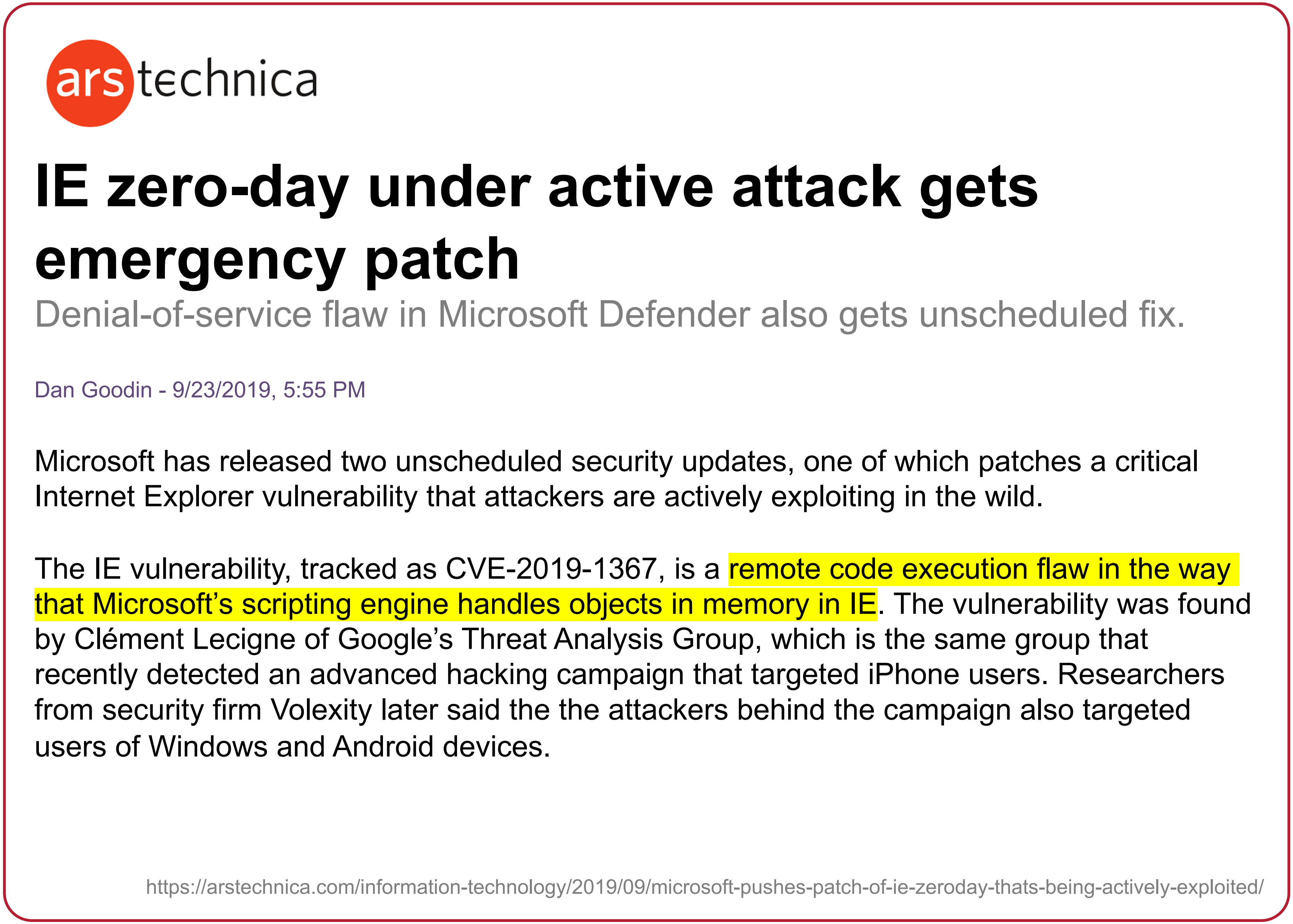
- **You installed it**
  - Social engineering (convincing you to install it)
    - E.g., security software, “cleaner” software, software “updates”
    - Clicking on an attachment or a URL
  - File sharing downloads
    e.g., pirated software from peer-to-peer services like BitTorrent
- **Infected removable media**
  - Initially floppies & CDs, then USB media
- **Direct attack to system services** (code injection, SQL injection, …)

Zero-day exploits

Take advantage of **zero-day vulnerabilities** to break into a system or elevate privileges.

Zero-day vulnerabilities: Bugs that have been discovered but not reported & not patched.

N-day vulnerabilities: bugs that have been reported, possibly patched, but patches have not yet been widely installe



ars technica

IE zero-day under active attack gets emergency patch

Denial-of-service flaw in Microsoft Defender also gets unscheduled fix.

Dan Goodin - 9/23/2019, 5:55 PM

Microsoft has released two unscheduled security updates, one of which patches a critical Internet Explorer vulnerability that attackers are actively exploiting in the wild.

The IE vulnerability, tracked as CVE-2019-1367, is a remote code execution flaw in the way that Microsoft's scripting engine handles objects in memory in IE. The vulnerability was found by Clément Lecigne of Google's Threat Analysis Group, which is the same group that recently detected an advanced hacking campaign that targeted iPhone users. Researchers from security firm Volexity later said the the attackers behind the campaign also targeted users of Windows and Android devices.

https://arstechnica.com/information-technology/2019/09/microsoft-pushes-patch-of-ie-zeroday-thats-being-actively-exploited/

Anonymous researcher drops vBulletin zero-day impacting tens of thousands of sites

New zero-day could trigger a new forum hacking spree across the internet.

By Catalin Cimpanu for Zero Day | September 24, 2019

An anonymous security researcher has published details about a zero-day in vBulletin, today's most popular internet forum software.

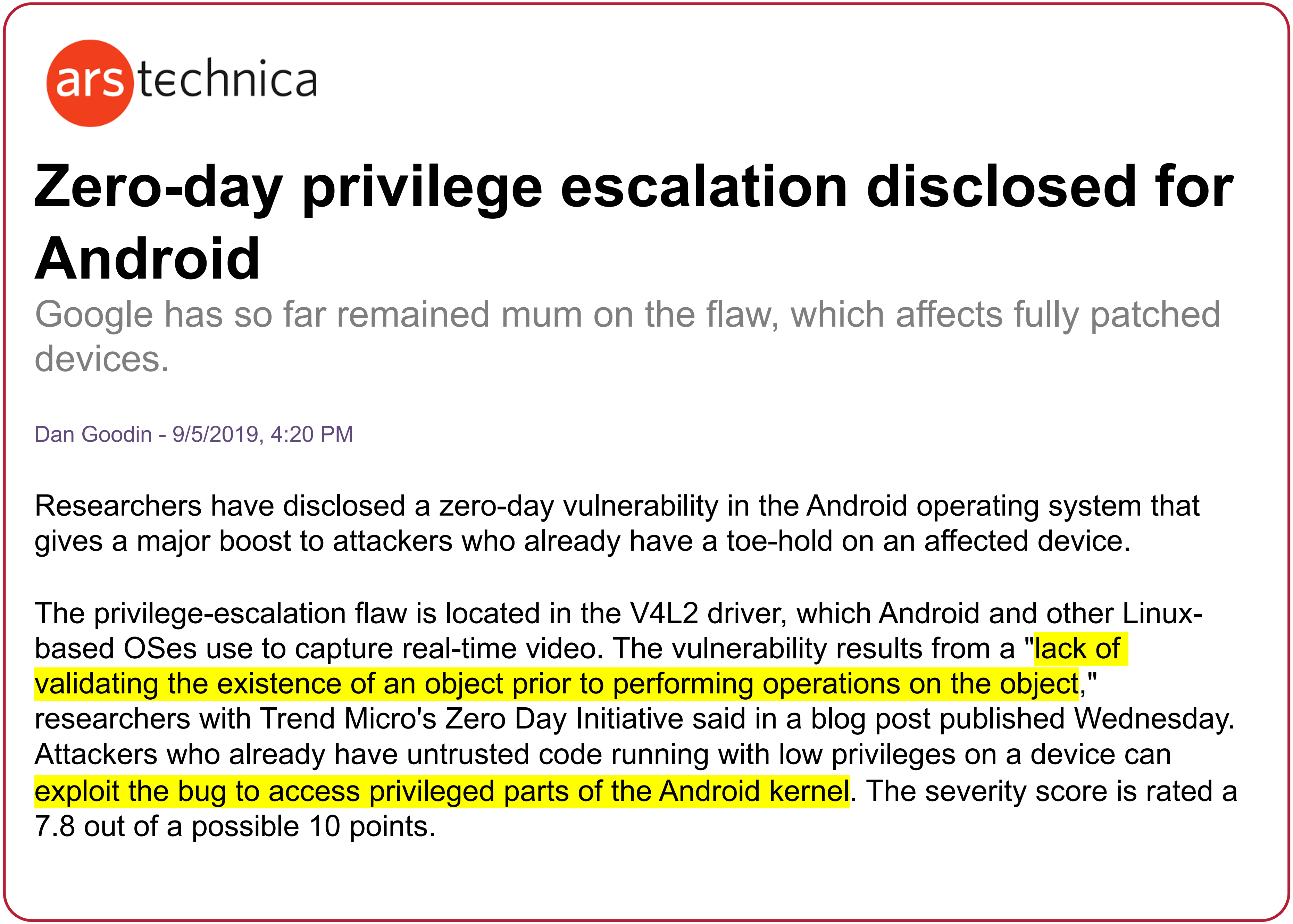
Because of this individual's actions, security experts are now concerned that the publication of details about this unpatched vulnerability could trigger a wave of forum hacks across the internet, with hackers taking over forum installations and stealing user information in bulk, as a result.

Zero-day details

According to an analysis of the published code, the zero-day allows an attacker to execute shell commands on the server running a vBulletin installation. The attacker doesn't need to have an account on the targeted forum.

In infosec lingo, this is what security experts call a "pre-authentication remote code execution" vulnerability, one of the worst types of security flaws that can impact a web-based platform.

https://arstechnica.com/information-technology/2019/09/microsoft-pushes-patch-of-ie-zeroday-thats-being-actively-exploited/



ars technica

Zero-day privilege escalation disclosed for Android

Google has so far remained mum on the flaw, which affects fully patched devices.

Dan Goodin - 9/5/2019, 4:20 PM

Researchers have disclosed a zero-day vulnerability in the Android operating system that gives a major boost to attackers who already have a toe-hold on an affected device.

The privilege-escalation flaw is located in the V4L2 driver, which Android and other Linux-based OSes use to capture real-time video. The vulnerability results from a "lack of validating the existence of an object prior to performing operations on the object," researchers with Trend Micro's Zero Day Initiative said in a blog post published Wednesday. Attackers who already have untrusted code running with low privileges on a device can exploit the bug to access privileged parts of the Android kernel. The severity score is rated a 7.8 out of a possible 10 points.

New Mac malware abuses recently disclosed Gatekeeper zero-day

ZDNet

Researchers find new OSX/Linker malware abusing still-unpatched macOS Gatekeeper bypass.

By Catalin Cimpanu for Zero Day | June 25, 2019

Mac malware developers have jumped on a recently disclosed macOS Gatekeeper vulnerability and are actively developing malware that abuses it.

The new malware has been named OSX/Linker and has been tied to the same group that operates the OSX/Surfbuyer adware, according to an investigation carried out by Joshua Long, Chief Security Analyst for Mac security software maker Intego.

THE UNPATCHED GATEKEEPER BYPASS

The new OSX/Linker malware abuses a security flaw that was disclosed in Gatekeeper, a macOS security system that scans and approves for execution apps downloaded from the Internet.

In late May, security researcher Filippo Cavallarin disclosed a bug in Gatekeeper that would allow a malicious binary downloaded from the Internet to bypass the Gatekeeper scanning process.

The trick involved packing a symlink (symbolic link) inside an archive file and having the symlink link back to an attacker-controlled Network File System (NFS) server.

All macOS versions are affected, including the latest 10.14.5, and Apple has yet to release a patch to this day, a full month after Cavallarin's public disclosure.

https://www.zdnet.com/article/new-mac-malware-abuses-recently-disclosed-gatekeeper-zero-day/

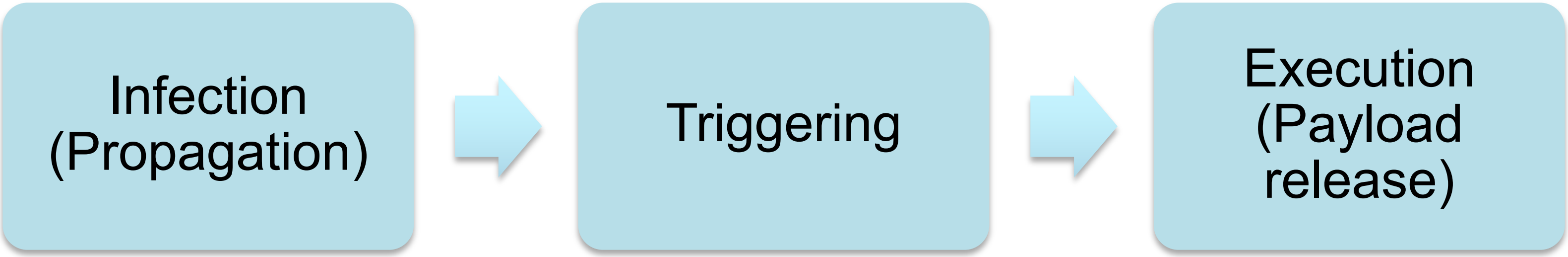
Virus

- Software that attaches itself to another piece of software or content that will be accessed by specific software
- Replicates by copying itself or modifying:
  - Other programs
  - Files read by other programs
  - Boot sector
- Usually spread by sharing files or software

Virus components

- Infection mechanism
  - Search for infection targets: other programs, specific files, disk areas
- Payload
  - The malicious part of the virus
- Trigger (logic bomb)
  - Executed whenever a file containing the virus is run
  - Determines whether the *payload* should be delivered
    - Virus may stay dormant for some time

Sequence of operations



Infection (Propagation)

Triggering

Execution (Payload release)

Worms vs. Viruses

- Conceptually similar
  - Software that replicates itself onto other systems
    - May be spread automatically (via network access) or manually (e.g., email attachments, flash drives)
  - Key distinction is whether they are standalone
- Worm
  - Standalone software
- Virus
  - Requires a host program: a virus attaches itself to another piece of software

Infected flash drives

Microsoft tried to make software installation super-convenient

- Insert a CD or USB key and the installer runs
- The instructions on what to run were contained in an **autorun.inf** file on the removable media
- If you can get someone to insert the media, you get them to run your commands
- Microsoft removed this feature … but there might be old versions running

KDE on Linux had a similar problem

- Using the KDE file viewer to navigate to a directory runs **.desktop** or **.directory** files in that directory
- If you can get a user to navigate to a directory, you get them to execute any commands you want
- This was fixed as of August 9, 2019 by removing support for shell commands

Infected flash drives

- **The main problem now:**
  - Unprotected firmware
  - Malware can replace firmware on a USB device to make it act like another device: e.g., make a flash drive behave like a keyboard
  - Can act like a regular storage device until the system is rebooted and the firmware detects it is talking to the BIOS
- **The other problem with flash drives**: data leakage
  - They're easy to lose

Macro viruses

- Microsoft Office apps have a powerful macro language
  - VBA – Visual Basic for Applications
  - Extra features make it easy to get to
    - Network printers
    - Network shares
    - Special folders
    - User information
    - Script execution on remote systems
    - Etc.

- Microsoft Office documents can be used to spread viruses
  - Spread by ordinary business behavior of sharing documents
  - Run arbitrary code to propagate – or infiltrate other software
  - Infect `normal.dot` – default template file
    - This will cause new Word documents to get infected

Bypassing macro warnings

- Microsoft Office apps now warn you if there’s a VBA macro
  - But users often click on *Enable macros* because they believe the content is legitimate

- Another technique to pass malware emerged (2017)
  - Send an RTF file with a .docx extension
  - MS Word will open it
  - It will result in the PC downloading a file with malicious HTML application content
  - Does not work if Microsoft’s Protected View feature is enabled
    - Opens Office documents with macros in read-only mode

- Yet another (2018)
  - Embedding a specially-crafted settings file into an office document bypasses macro warnings

Social engineering helps a lot

Dominant form of transporting malware

- Early examples
  - ILOVEYOU
    - Mail often came from a sender you knew
  - Melissa (earlier virus)
    - Promised a list of passwords for X-rated web sites

Email-based transmission dramatically increased the spread of malware

Macro viruses

- **ILOVEYOU** virus: 2000
  - Propagated via email
  - Subject of the message stated it’s a love letter from a secret admirer
  - **`LOVE-LETTER-FOR-YOU.TXT.vbs`**

MAY 15, 2000 $3.50
TIME
MOMS MARCH AGAINST GUNS
THE TRUTH ABOUT BANKRUPTCY
THE LOVE BUG
How it works
How to protect yourself against viruses
BILL GATES defends the Microsoft monolith
www.time.com AOL Keyword: TIME

- .vbs suffix = Visual Basic Scripting

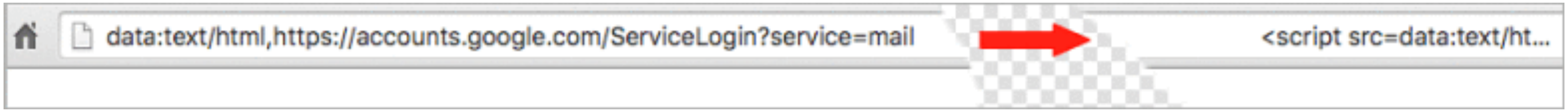
- What it did:
  - Copied itself several times into various folders
  - Added new files to the victim’s registry keys
  - Replaced several different kinds of files (music, multimedia) with copies of itself
  - Sent itself through Internet Relay Chat clients and email
  - Download a file called **`WIN-BUGSFIX.EXE`** & executed it
    - Instead of fixing bugs, this stole passwords and emailed them to the hacker

Phishing

- Social engineering attack
- Try to get personal information or login data
- Instilling panic helps
  - Your eBay or PayPal accounts may be canceled
  - We noticed a fraudulent transaction in your account
  - We couldn’t deliver your package and it will be sent back

Gmail spear phishing

- Hackers send email to contacts of compromised accounts
  - Email contains an innocent-looking attachment
- When the user clicks the attachment
  - A new tab opens that looks like the Google sign-in page
  - Login information goes to the attacker
- Attackers log in to your account immediately
  - Use one of your actual attachments & one of your actual subject lines
  - Send mail to people in your contact list
  - Mail contains a thumbnail image of the attachment
    - But the link is a script (but pre-padded with spaces)



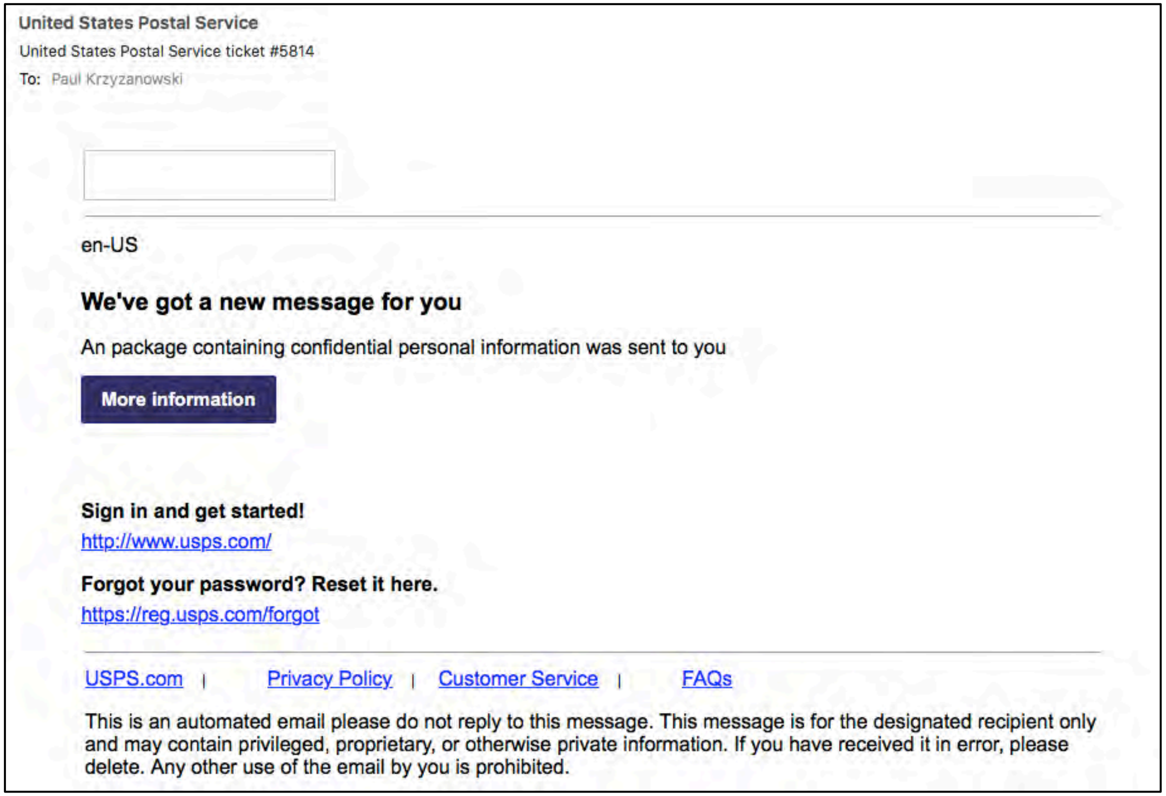
data:text/html,https://accounts.google.com/ServiceLogin?service=mail

<script src=data:text/ht...

http://bgr.com/2017/01/17/gmail-phishing-attack-attachment-address-bar/

Deception

A package from the postal service …
“containing confidential personal information”



United States Postal Service
United States Postal Service ticket #5814
To: Paul Krzyzanowski

en-US

We've got a new message for you

An package containing confidential personal information was sent to you

Sign in and get started!
http://www.usps.com/

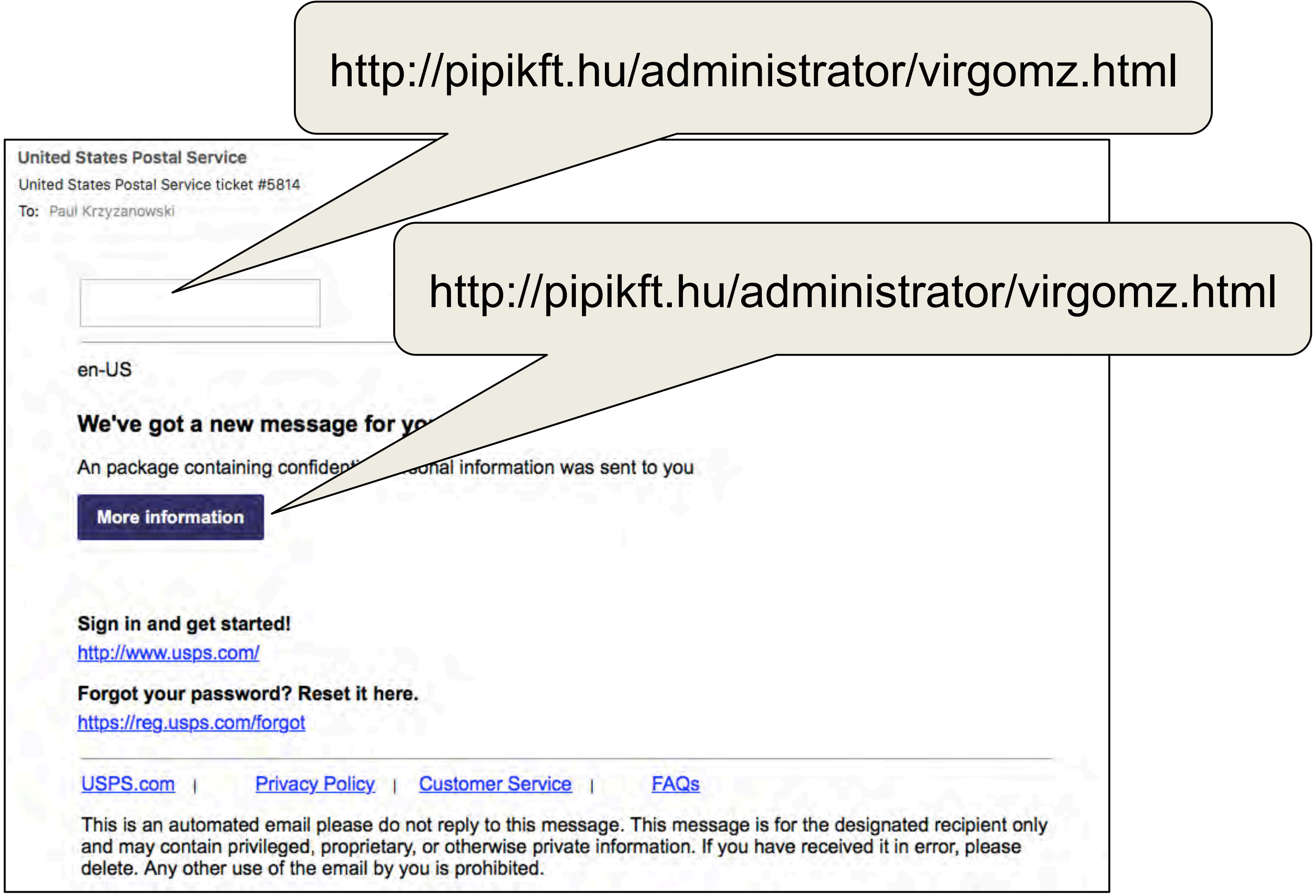
Forgot your password? Reset it here.
https://reg.usps.com/forgot

USPS.com | Privacy Policy | Customer Service | FAQs

This is an automated email please do not reply to this message. This message is for the designated recipient only and may contain privileged, proprietary, or otherwise private information. If you have received it in error, please delete. Any other use of the email by you is prohibited.

Deception

Weird URLs – I'd expect usps.com



http://pipikft.hu/administrator/virgomz.html

http://pipikft.hu/administrator/virgomz.html

United States Postal Service

United States Postal Service ticket #5814

To: Paul Krzyzanowski

en-US

We've got a new message for yo

An package containing confiden onal information was sent to you

Sign in and get started!

http://www.usps.com/

Forgot your password? Reset it here.

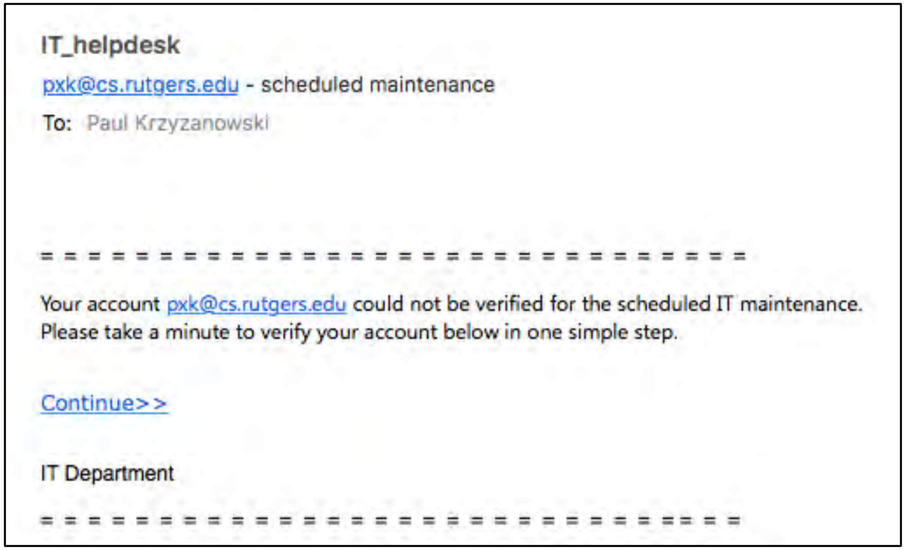
https://reg.usps.com/forgot

USPS.com | Privacy Policy | Customer Service | FAQs

This is an automated email please do not reply to this message. This message is for the designated recipient only and may contain privileged, proprietary, or otherwise private information. If you have received it in error, please delete. Any other use of the email by you is prohibited.

Deception

Uh oh! Something's wrong with my Rutgers account??



IT_helpdesk

pxk@cs.rutgers.edu - scheduled maintenance

To: Paul Krzyzanowski

= =

Your account pxk@cs.rutgers.edu could not be verified for the scheduled IT maintenance. Please take a minute to verify your account below in one simple step.

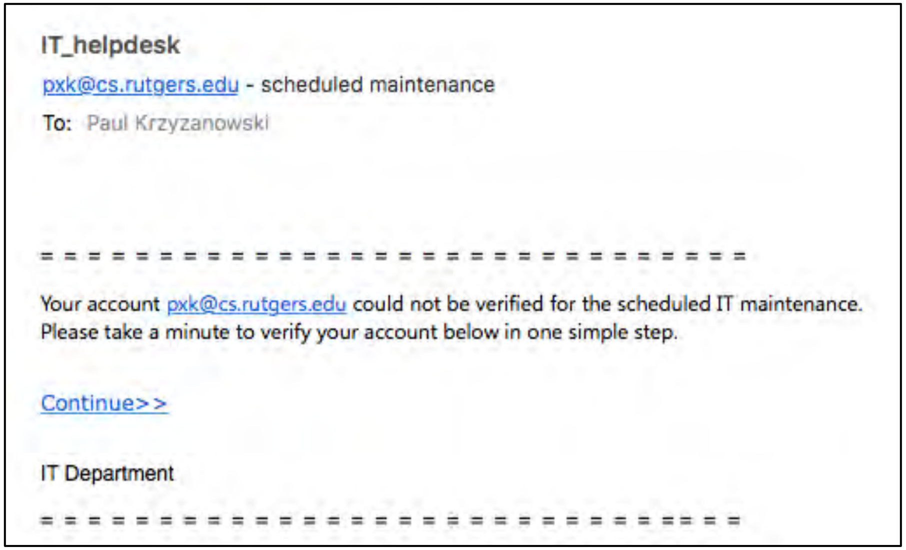
Continue>>

IT Department

= =

Deception

Uh oh! Something's wrong with my Rutgers account??



IT_helpdesk

pxk@cs.rutgers.edu - scheduled maintenance

To: Paul Krzyzanowski

Your account pxk@cs.rutgers.edu could not be verified for the scheduled IT maintenance. Please take a minute to verify your account below in one simple step.

Continue>>

IT Department

But why is this link taking me to https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.iglemdv.com%2F031MWCS3D%2Findex&data=....

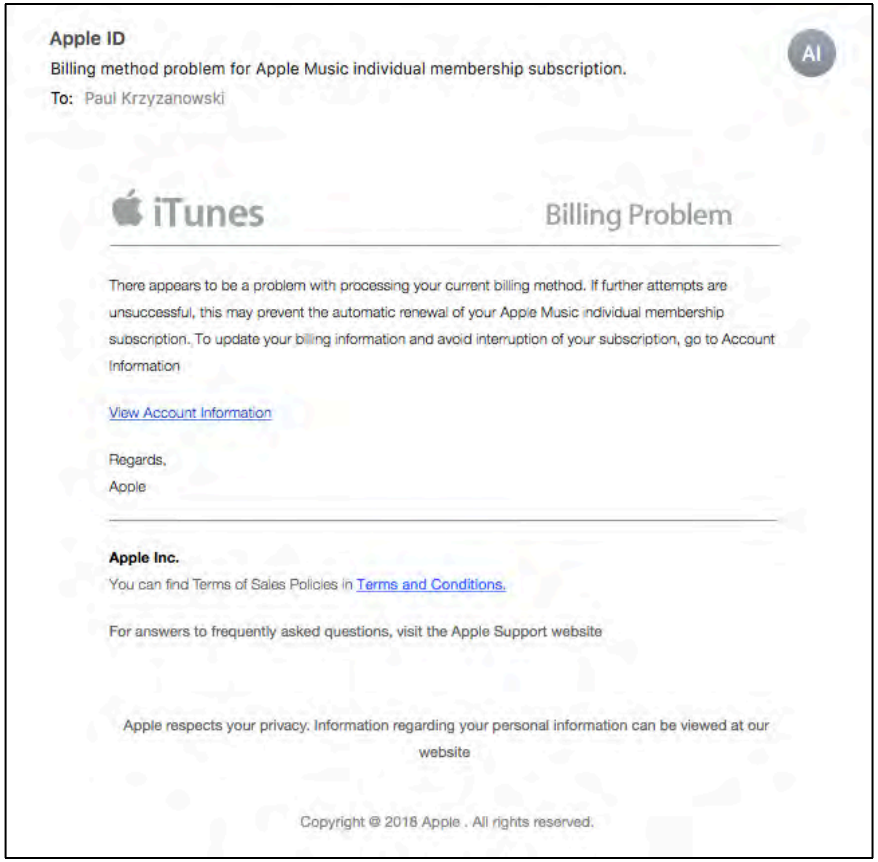
protection.outlook.com is a URL rewrite by Microsoft Office 365 and takes you to Microsoft's Threat Protection service, which checks the requested URL

But why is Rutgers trying to send me to iglemdv.com, which is registered in Argentina?

Deception

Uh oh! A billing problem with my iTunes account

But I don't even subscribe to Apple Music!



Apple ID

Billing method problem for Apple Music individual membership subscription.

To: Paul Krzyzanowski

There appears to be a problem with processing your current billing method. If further attempts are unsuccessful, this may prevent the automatic renewal of your Apple Music individual membership subscription. To update your billing information and avoid interruption of your subscription, go to Account Information

View Account Information

Regards,
Apple

Apple Inc.
You can find Terms of Sales Policies in Terms and Conditions.

For answers to frequently asked questions, visit the Apple Support website

Apple respects your privacy. Information regarding your personal information can be viewed at our website

Copyright @ 2018 Apple . All rights reserved.

Deception

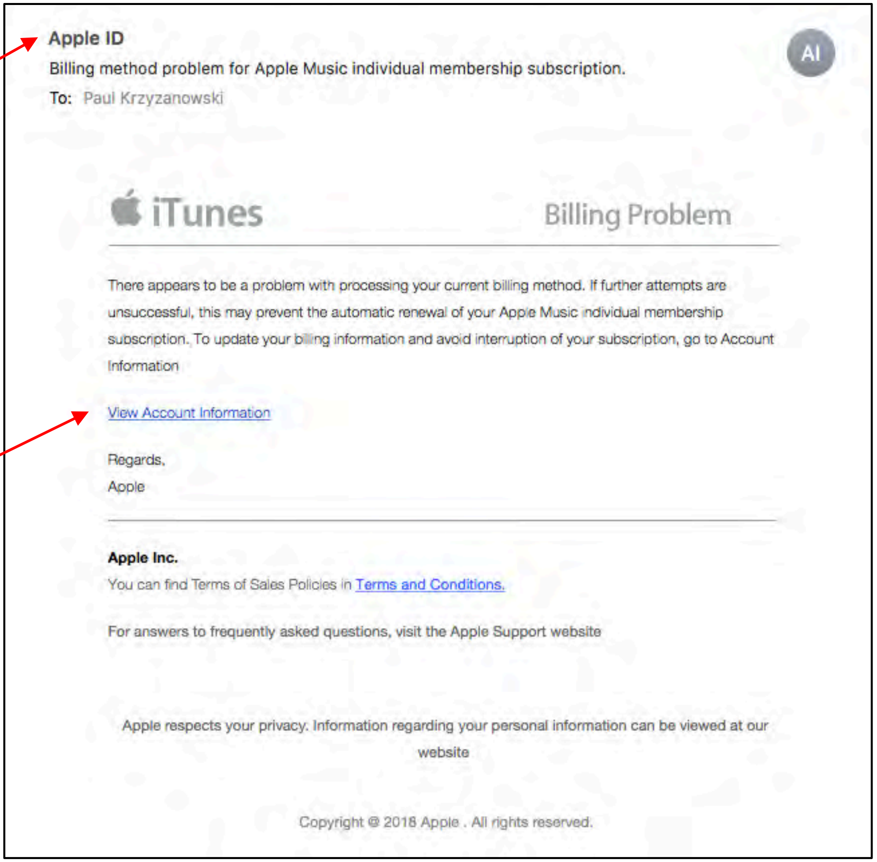
Uh oh! A billing problem with my iTunes account

But the return address is vormweg@t-online.de

vormweg@t-online.de sounds German
T-online is Deutsche Telekom

But "View Account Information" is a link to https://novoleather.com.tr/libraries/joomla/..."

Huh?



Apple ID
Billing method problem for Apple Music individual membership subscription.
To: Paul Krzyzanowski

There appears to be a problem with processing your current billing method. If further attempts are unsuccessful, this may prevent the automatic renewal of your Apple Music individual membership subscription. To update your billing information and avoid interruption of your subscription, go to Account Information

View Account Information

Regards,
Apple

Apple Inc.
You can find Terms of Sales Policies in Terms and Conditions.

For answers to frequently asked questions, visit the Apple Support website

Apple respects your privacy. Information regarding your personal information can be viewed at our website

Copyright © 2018 Apple . All rights reserved.

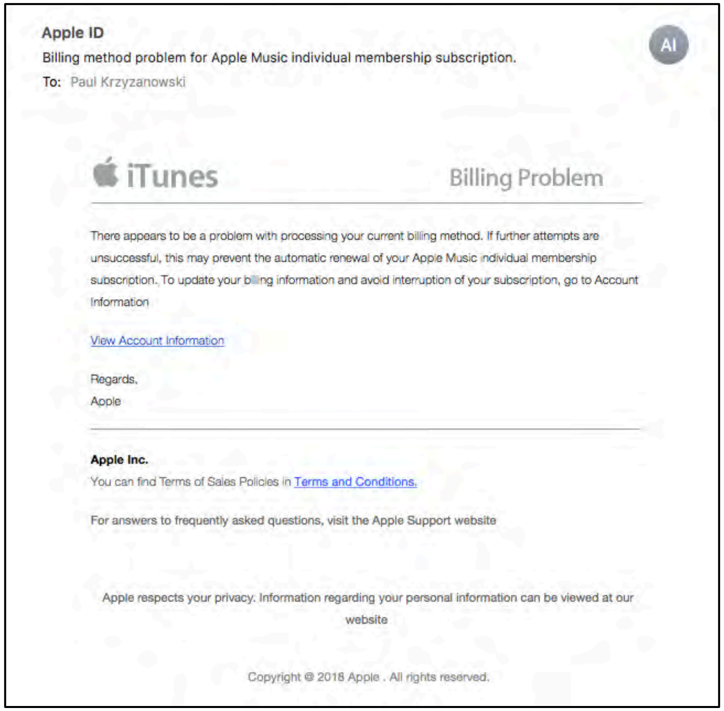
Deception

Mail clients try show a clean interface so they hide most mail headers

Fair enough: there are 71 lines of headers

If we look through them we see:

```
Return-path: <vormweg@t-online.de>
Received: from mailout07.t-online.de (mailout07.t-online.de [194.25.134.83])
 by st11p00im-smtpin012.me.com ...
Received: from fwd12.aul.t-online.de (fwd12.aul.t-online.de [172.20.26.241])
        by mailout07.t-online.de (Postfix) with SMTP id A510442E0CE3...
Received: from WIN-HDR0OI256J4
 (EXJhz2Zeg … 399RFV6EzsetTEwa+J5gJgtA@[89.43.30.27])
 by fwd12.t-online.de   with (TLSv1:DES-CBC3-SHA encrypted)
        esmtp id 1efGxq-0LcoTI0; Sat, 27 Jan 2018 04:15:34 +0100
From: Apple ID <vormweg@t-online.de>
```



Apple ID
Billing method problem for Apple Music individual membership subscription.
To: Paul Krzyzanowski

Billing Problem

There appears to be a problem with processing your current billing method. If further attempts are unsuccessful, this may prevent the automatic renewal of your Apple Music individual membership subscription. To update your billing information and avoid interruption of your subscription, go to Account Information

View Account Information

Regards,
Apple

Apple Inc.
You can find Terms of Sales Policies in Terms and Conditions.

For answers to frequently asked questions, visit the Apple Support website

Apple respects your privacy. Information regarding your personal information can be viewed at our website

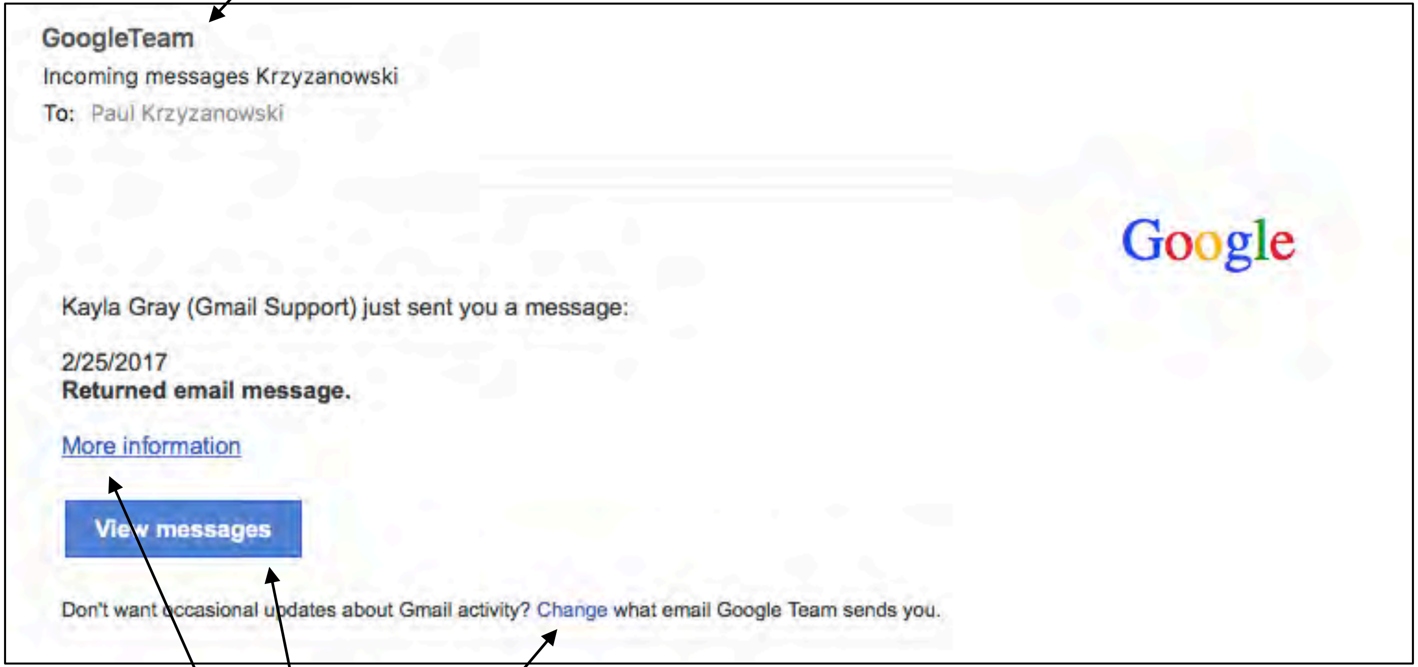
Copyright @ 2018 Apple . All rights reserved.

Mail headers can be forged but they give us some opportunities to do basic forensics
… or at least set off alarms that there's something suspicious.

The first IP address we see is 89.43.30.27.
That's provided by the ISP Netinternet Bilisim Teknolojileri AS in Turkey
Why is Apple sending me a message from Turkey, relaying it through Deutsche Telekom mail relays, and sending it back to Apple?

From: GoogleTeam <csalans@salans.com>

But it came from 107.170.47.71, which is lemp.frosticsatellite.com.



GoogleTeam
Incoming messages Krzyzanowski
To: Paul Krzyzanowski

Kayla Gray (Gmail Support) just sent you a message:

2/25/2017
Returned email message.

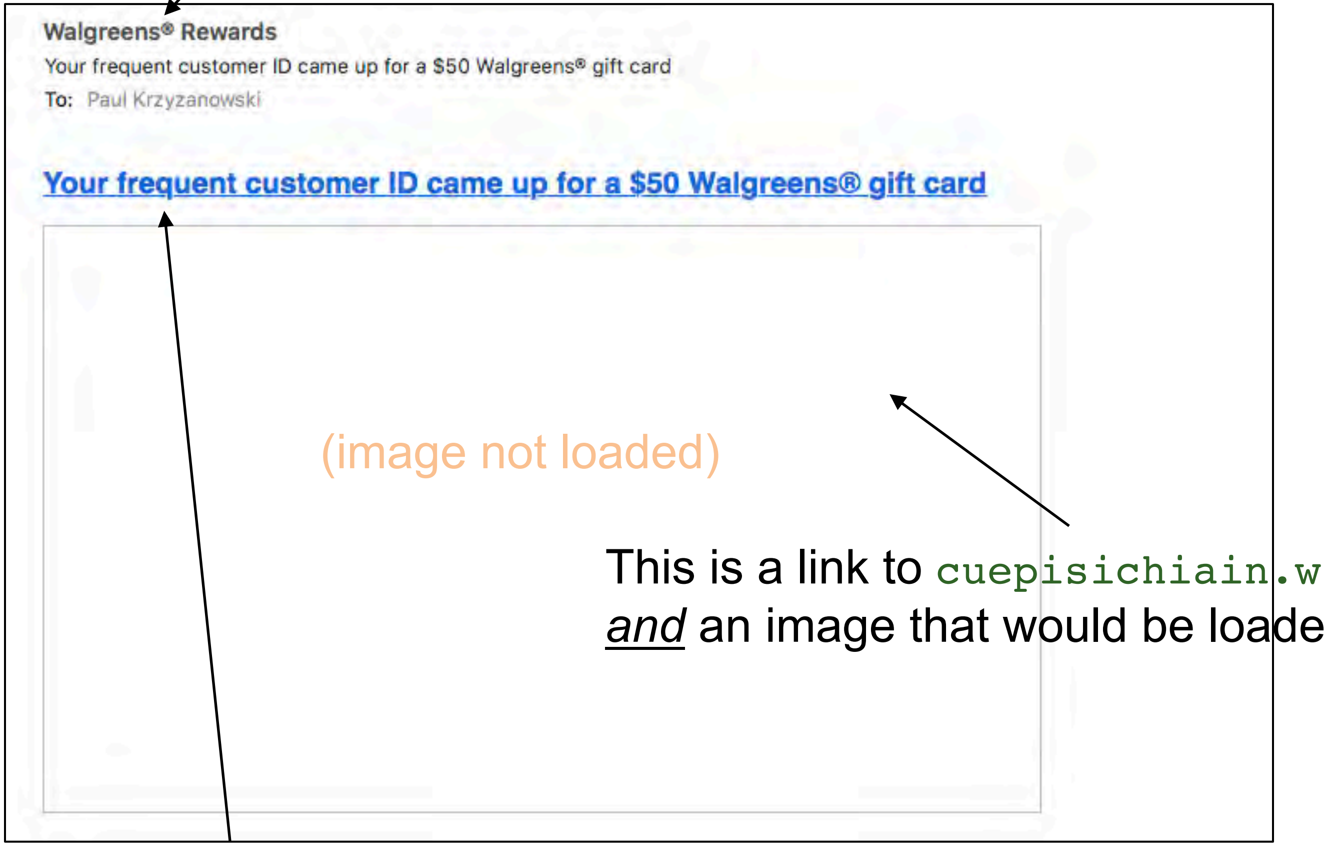
More information

Don't want occasional updates about Gmail activity? Change what email Google Team sends you.

These are links to `playground.omg-bg.com/...`, not Google!

`From: Removal.walg1gmco27890@cuepisichiain.w220.luamev.top`

But came from 46.3.221.220,
which belongs to Vyacheslav S. Bashin of Moscow



Walgreens® Rewards

Your frequent customer ID came up for a $50 Walgreens® gift card

To: Paul Krzyzanowski

Your frequent customer ID came up for a $50 Walgreens® gift card

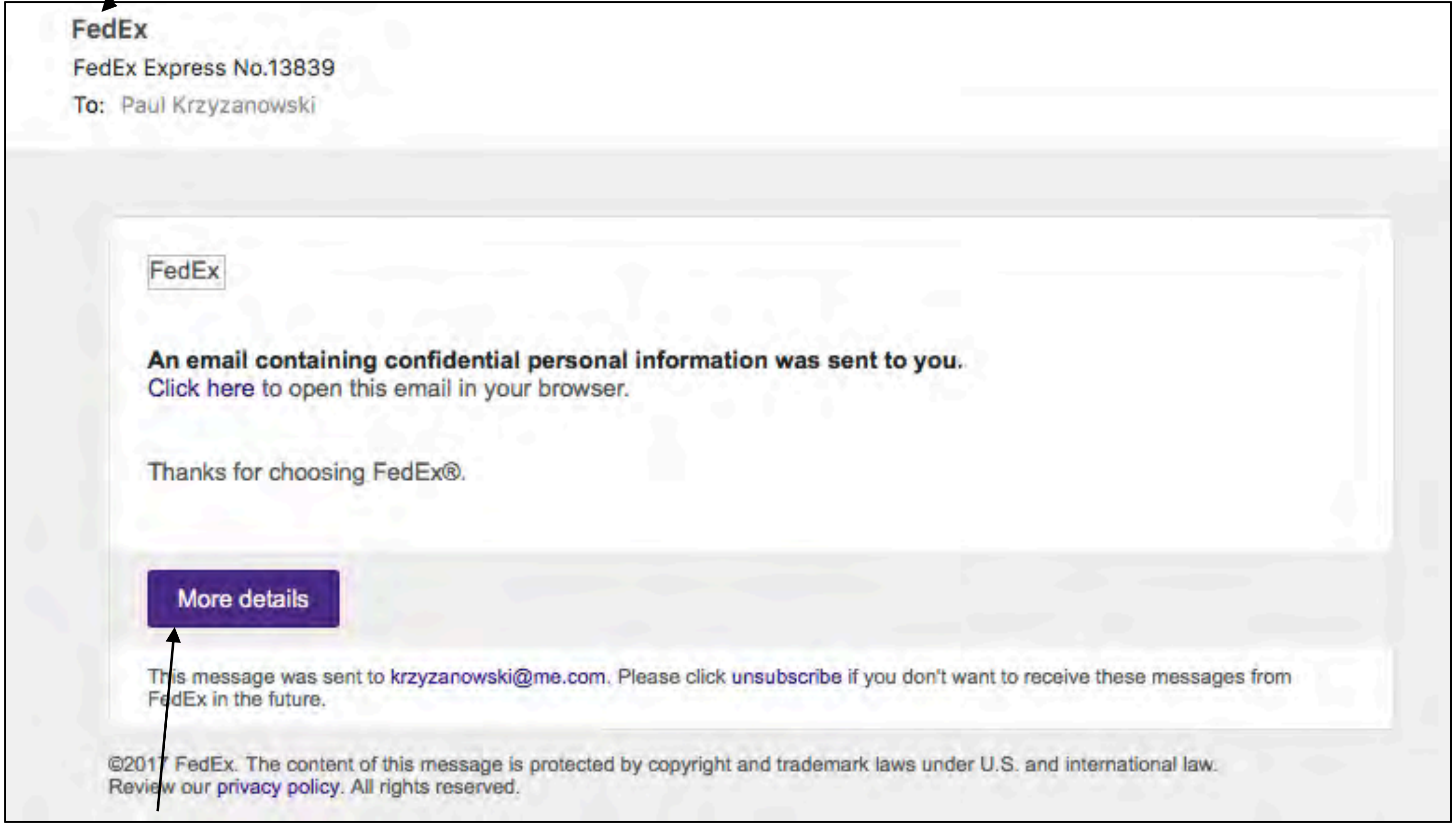
(image not loaded)

This is a link to `cuepisichiain.w220.luamev.top/…`
and an image that would be loaded from the site

This is a link to `cuepisichiain.w220.luamev.top/…`

`From: FedEx <detacher@net4webmail.com>`

But came from `detacher@net4webmail.com`



FedEx
FedEx Express No.13839
To: Paul Krzyzanowski

FedEx

An email containing confidential personal information was sent to you.
Click here to open this email in your browser.

Thanks for choosing FedEx®.

This message was sent to krzyzanowski@me.com. Please click unsubscribe if you don't want to receive these messages from FedEx in the future.

©2017 FedEx. The content of this message is protected by copyright and trademark laws under U.S. and international law. Review our privacy policy. All rights reserved.

This is a link to `www.ethoscontabilidade.net.br/…`

Spear phishing

Phishing attacks are impersonal

Spear phishing

- Attacks are customized with information about the target
- More likely to trick a target into thinking the content is legitimate

The 2016 Democratic National Committee (DNC) attack was facilitated by spear phishing

- Russian hacking group Fancy Bear used bit.ly links
  - Short URLs help mask malicious URLs
- Redirect victims to a URL: looks like a legitimate Google accounts login page
  - Prepopulated with the victim’s Gmail address
- From October 2015 – May 2016, 8,909 bit.ly links targeted 3,907 accounts
  - 20 clicks on malicious links were recorded on hillaryclinton.com
  - 4 clicks were recorded on dnc.org

Residence

Some ways in which malware lives in system

Where can malware live?

Malware needs to run … but wants to stay hidden

- Affix itself to legitimate files (e.g., Word macros)
- Run at startup as as system service
  - Ideally, disguise the name as a legitimate service
  - Or installed because the user thought it was a legitimate program (e.g., Adobe FlashPlayer installer)
- Install as a browser plugin
- Install itself as an operating system extension or driver
- Modify a local hosts file to redirect specific web pages
- Modify the bootloader
- Sit in memory

File infector viruses

- Virus adds itself to the end of an executable program file
- Patches a branch to that code at the start of the program
- Ideally
  - Hidden in some unused part of the file so file length remains unchanged

Difficult with systems where users have restricted permissions or where the OS validates the digital signature of software and system files

System services

- System startup scripts, profiles, scheduled tasks (cron)
- Microsoft Windows registry: lots of locations!

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler

- macOS LaunchAgents

  /Library/LaunchAgents
  /Library/LaunchDaemons
  ~/Library/LauchAgents
  /System/Library/LaunchAgents
  /System/Library/LaunchDaemons

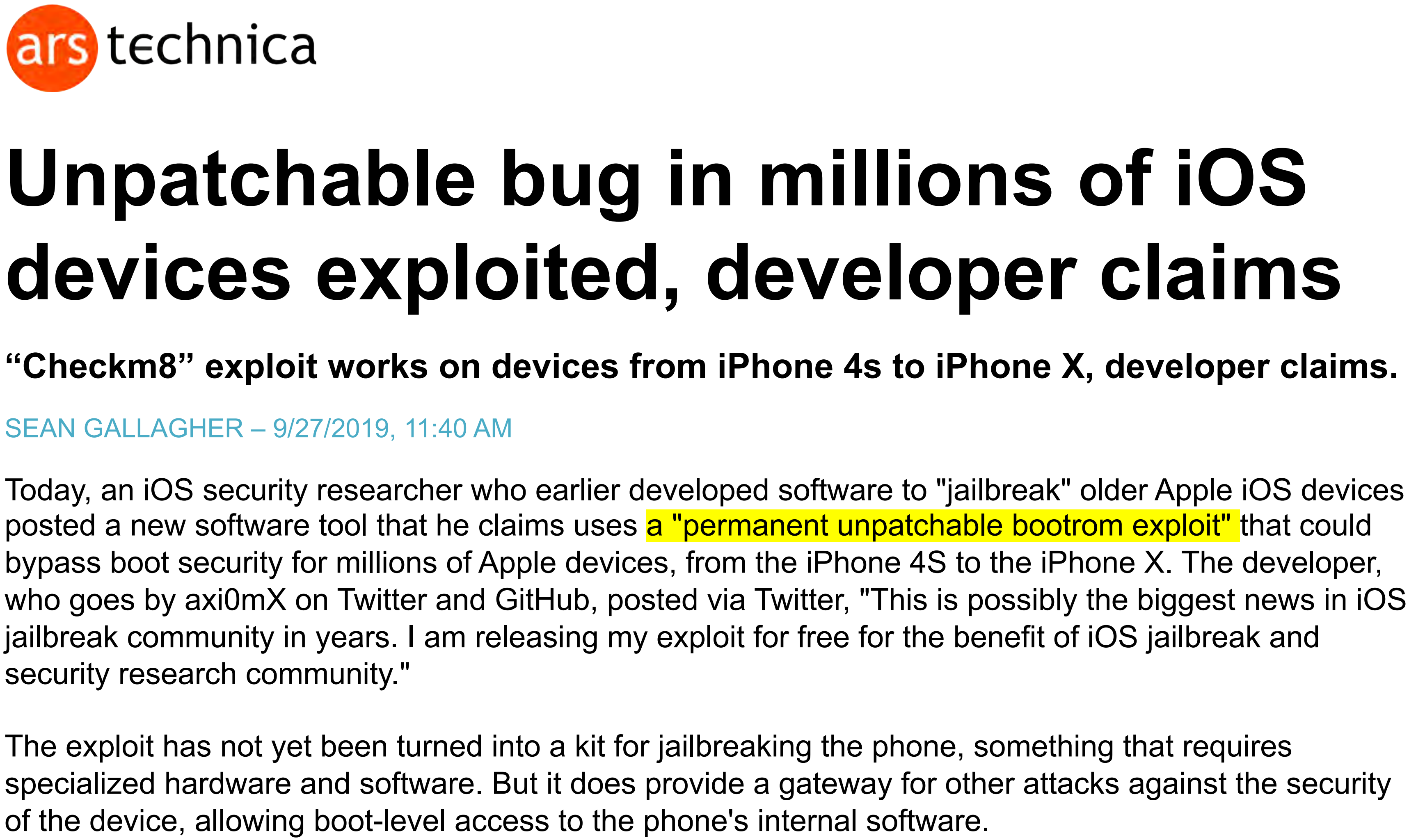
  - Launch Daemons: run on behalf of root user (or other specified user)
  - Launch Agent: run on behalf of logged-in user
- Linux startup, profiles, preload
  - Boot scripts: /etc/rc.d/*, /etc/init.d
  - Profiles: /etc/profile, /etc/bashrc, ~/.bashrc, ~/.bash_profile, …
  - LD_PRELOAD environment to load different libraries

Registry keys: https://www.symantec.com/connect/articles/most-common-registry-key-check-while-dealing-virus-issue

Bootloader (boot sector) viruses

- Infect the Master Boot Record (MBR) of a drive
  - Originally – infect boot sector of floppy drives
- Infected code runs when the system is booted
  - Will try to infect other disks
- Far less common now
  - Used DOS commands to spread to floppy disks
  - We don't use floppy disks
  - Harder to spread but still possible to write – still around as of 2015
- Bootkits: malware to place code in the MBR
  - Runs before the operating system starts!

Buggy bootloaders can also be a problem



ars technica

Unpatchable bug in millions of iOS devices exploited, developer claims

“Checkm8” exploit works on devices from iPhone 4s to iPhone X, developer claims.

SEAN GALLAGHER – 9/27/2019, 11:40 AM

Today, an iOS security researcher who earlier developed software to "jailbreak" older Apple iOS devices posted a new software tool that he claims uses a "permanent unpatchable bootrom exploit" that could bypass boot security for millions of Apple devices, from the iPhone 4S to the iPhone X. The developer, who goes by axi0mX on Twitter and GitHub, posted via Twitter, "This is possibly the biggest news in iOS jailbreak community in years. I am releasing my exploit for free for the benefit of iOS jailbreak and security research community."

The exploit has not yet been turned into a kit for jailbreaking the phone, something that requires specialized hardware and software. But it does provide a gateway for other attacks against the security of the device, allowing boot-level access to the phone's internal software.

https://arstechnica.com/information-technology/2019/09/unpatchable-bug-in-millions-of-ios-devices-exploited-developer-claims/

Trojan Horses

Program with two purposes

- – **Overt** purpose: known to a user
- – **Covert** purpose: unknown to a user

Name the script *`ls`*

Place it in someone’s shell PATH to get them to execute it

You get a setuid shell to their ID

They think they ran the real *`ls`* command

```
cp /bin/sh /tmp/.xyz
chmod u+s,o+x /tmp/.xyz
rm ./ls
ls $*
```

Trojan Horses

- What they *might* do
  - Add **backdoors** – secret access that bypasses OS authentication
  - Enable remote camera access
  - Run key loggers
  - Run web clickers
  - Enable proxy services (allow your machine to help anonymize connections)
  - Run spam engines – enable the sending of spam
  - Run DDoS engines – be part of a botnet running a DDoS attack
  - Mine cryptocurrency
- How do you get people to install them?
  - Lure the user to think it's useful software – *hacker tools, anti-virus tools*

PDF, JavaScript

- JavaScript can be dangerous (powerful scripting)
  - Most browser security holes involve JavaScript
  - Deception via overlaying images, controlling clicks, form entry, etc.
  - PDF files now can contain JavaScript

- JavaScript can connect to other sites
  - It can do things like port scans
  - Any web site you connect to can leverage your machine

Source repositories

Do you just download and compile code from github?

- Or do you inspect it? … or assume someone else has?

Hackers can plant Trojan horses (often back doors) in popular software

- July 7, 2019

  Canonical GitHub account hacked

  Github accout of Canonical Ltd, company behind the Linux Ubuntu distribution was hacked. Ubuntu distribution was safe

- May 9, 2019

  Hackers breached 3 US antivirus companies, researchers reveal

  Source code, network access being sold online by "Fxmsp" collective for $300,000

- October 13, 2013

  PHP source code compromised?

  It was announced that the PHP website was hacked and serving malware. If the attackers had access to their internal servers, can we trust the PHP sourcecode anymore?

https://arstechnica.com/information-technology/2019/05/hackers-breached-3-us-antivirus-companies-researchers-reveal/

https://barracudalabs.com/2013/10/php-net-compromise/

https://www.helpnetsecurity.com/2011/09/01/linux-source-code-repository-compromised/

Source repositories

- September 1, 2011

  Linux source code repository compromised

  The Kernel.org website – home to the Linux project and the primary repository for the Linux kernel source code – sports a warning notifying its users of a security breach that resulted in the compromise of several servers in its infrastructure.

- March 5, 2012

  GitHub hacked, millions of projects at risk of being modified or deleted

  GitHub, one of the largest repositories of commercial and open source software on the web, has been hacked. Over the weekend, developer Egor Homakov exploited a gaping vulnerability in GitHub that allowed him (or anyone else with basic hacker know-how) to gain administrator access to projects such as Ruby on Rails, Linux, and millions of others. Homakov could've deleted the entire history of projects such as jQuery, Node.js, Reddit, and Redis.

- October 4, 2013

  Adobe Source Code and Customer Data Hacked

  Adobe has confirmed the company was the victim of a long term network breach which exposed consumer data including passwords and credit card data, as well as exposing the source code for some of their leading products.

https://www.extremetech.com/computing/120981-github-hacked-millions-of-projects-at-risk-of-being-modified-or-deleted

Source repositories

- June 28, 2018

  Gentoo repository at GitHub hacked

  Hackers gained access to the GitHub repositories and tampered the source code of Gentoo by introducing a malicious script to delete all of your files.

- July 31, 2018

  Homebrew's GitHub repository hacked

  Eric Holmes, a security researcher gained access to Homebrew's GitHub repo easily.

  Homebrew is a free and open-source software package management system with well-known packages like node, git, and many more. It simplifies the installation of software on macOS.

- Sept 4, 2018

  Almost 400k websites risk hacking, data theft via open .git repos

  Smitka recently scanned 230 million "interesting" sites across the globe over one month and found 390,000 web pages with an open .git directory.

Rootkits

- Mechanisms to
  - Install software (usually malware)
  - Hide its existence
- Goal
  - A user or administrator can look around the system and not see anything abnormal
- Started on Unix Systems in 1990
  - NTRootkit in 1999
  - HackerDefender for Windows NT/2000/95 in 2003
  - Mac OS X rootkit in 2009
  - Stuxnet worm

Rootkits

- User mode
  - Replace commands
    - Replace common admin commands (*ps, ls, find, top, netstat*) with ones that conceal the existence of the intruder
  - Intercept messages
  - Exploit vulnerabilities
  - Patch commonly-used APIs
    - Use LD_PRELOAD to hook & intercept system calls & common library functions

- Kernel mode
  - Installed as kernel modules
  - Gives the rootkit unrestricted access
    - Can modify the system call table and any kernel structures
  - Difficult to detect
    - All commands and libraries look normal

Sony BMG DRM (2005)

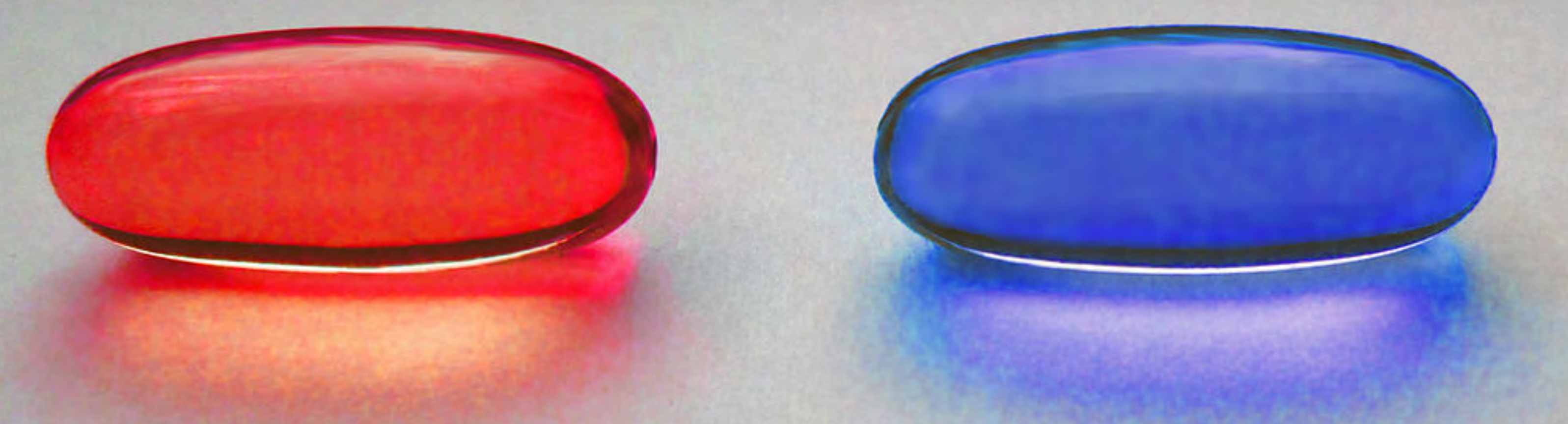
- Sony didn't want you making copies of their music
  - .. So they added digital rights management (DRM) software
- When you played certain Sony music CDs on your computer, Sony installed a DRM package
  - It modified the operating system to prevent copying the CD
- Sony also installed a rootkit to "protect" the DRM software
  - The software could not be installed
- The software also phoned home every time you played the CD

Hypervisor rootkits

- A system with no virtualization software installed but with hardware support for virtualization can have a hypervisor-based rootkit installed

- Rootkit runs at a higher privilege level than the OS.
  - It's possible to write it in a way that the kernel will have a limited ability to detect it.

"You take the blue pill, the story ends. You wake up in your bed and believe whatever you want to believe. You take the red pill, you stay in Wonderland, and I show you how deep the rabbit hole goes."



The term *red pill* refers to a human who is aware of the true nature of the **Matrix**.

Hypervisor attacks

- A hypervisor sits below the operating system
- All device access goes through the VM
  - Memory page tables, interrupts, clock, display, disk I/O, network I/O, etc.

Blue Pill – rootkit based on x86 virtualization (AMD & Intel)

- The hypervisor *is* the rootkit
- Essentially undetectable
  - OS, all system programs, all libraries, all applications, and all files look clean
  - Hypervisors are designed to be seamless – an OS cannot query to see if it's running on a hypervisor
- Detection may be possible via a *timing attack*
  - Analyze time it takes for privileged operations to take place
  - An OS running on a hypervisor will take longer
  - You don't know if it's malicious, but you can suspect that you're running over a hypervisor
  - A really good blue pill will adjust the time – you'll need to check via the network

Detecting hypervisor attacks

Red Pill – detect the presence of a hypervisor (AMD & Intel)

- Intel/AMD SIDT instruction
  - Returns address of interrupt descriptor table register (IDTR)
  - IDTR has the memory location of the interrupt descriptor table
- The CPU has only one IDTR, so the VMM needs to juggle copies
- If the address of the interrupt descriptor table is higher in memory and not the typical address, that indicates the a VMM was swapping these values

- Not foolproof!

File-less malware

- Anti-malware software catches a lot of malware via file scanning
- File-less malware
  - Goal: escape detection by anti-virus software
  - Often leverage zero-day exploits for privilege escalation
  - Malware code resides in RAM or Windows registry
    - Registry entries can help restart scripts after a system has been restarted
  - Propagates through scripts (e.g., Windows PowerShell)
- Still not common … but its use is increasing

Function

Some things malware can do

Spyware

- Type of malware that monitors some set of activities
  - Browsing history
  - Messages sent/received
  - Files accessed
  - Keyboard activity
  - Camera/microphone access

Adware

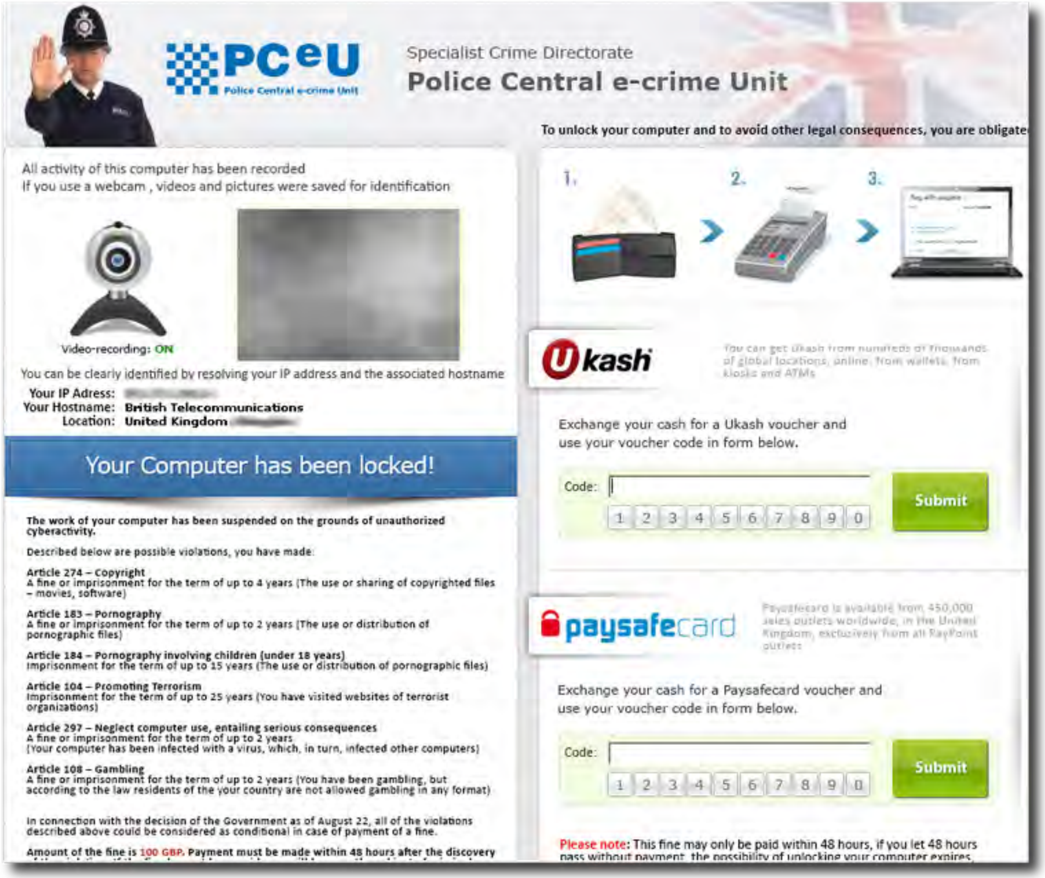
- Ads show up when a user is online
- Collects marketing data & other information without the user's knowledge
- A lot of peer-to-peer software includes third-party adware
  - What does it really monitor?

Ransomware

- Denial-of-service malware that:
  - Encrypts victim’s data
    - Or even encrypts the Master File Table (NTFS version of inode table)
  - Threatens to publish victim’s data
  - Or locks the system
- Demands payment to decrypt
- Usually distributed via a Trojan whose payload looks like a legitimate file
- MacAfee collected >250,000 unique samples of ransomware in 2013
  - CryptoLocker spread via infected email attachments
    - Got $3 million before it was shut down by the FBI and Interpol
  - Cryptowall
    - Spread via spam emails, exploit kits hosted through malicious ads or compromised sites
    - Got $18 million before it was shut down in 2015

Ransomware

- Ransomware is directly lucrative
  - Cryptocurrency made it hugely popular
    - Anonymous payments



Specialist Crime Directorate

Police Central e-crime Unit

To unlock your computer and to avoid other legal consequences, you are obligate

All activity of this computer has been recorded
If you use a webcam , videos and pictures were saved for identification

Video-recording: **ON**

You can be clearly identified by resolving your IP address and the associated hostname

Your IP Adress: [redacted]
Your Hostname: **British Telecommunications**
Location: **United Kingdom** [redacted]

Your Computer has been locked!

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.

Described below are possible violations, you have made:

Article 274 – Copyright
A fine or imprisonment for the term of up to 4 years (The use or sharing of copyrighted files – movies, software)

Article 183 – Pornography
A fine or imprisonment for the term of up to 2 years (The use or distribution of pornographic files)

Article 184 – Pornography involving children (under 18 years)
Imprisonment for the term of up to 15 years (The use or distribution of pornographic files)

Article 104 – Promoting Terrorism
Imprisonment for the term of up to 25 years (You have visited websites of terrorist organizations)

Article 297 – Neglect computer use, entailing serious consequences
A fine or imprisonment for the term of up to 2 years
(Your computer has been infected with a virus, which, in turn, infected other computers)

Article 108 – Gambling
A fine or imprisonment for the term of up to 2 years (You have been gambling, but according to the law residents of the your country are not allowed gambling in any format)

In connection with the decision of the Government as of August 22, all of the violations described above could be considered as conditional in case of payment of a fine.

Amount of the fine is 100 GBP. Payment must be made within 48 hours after the discovery

You can get Ukash from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs

Exchange your cash for a Ukash voucher and use your voucher code in form below.

Code:

Paysafecard is available from 450,000 sales outlets worldwide, in the United Kingdom, exclusively from all PayPoint outlets

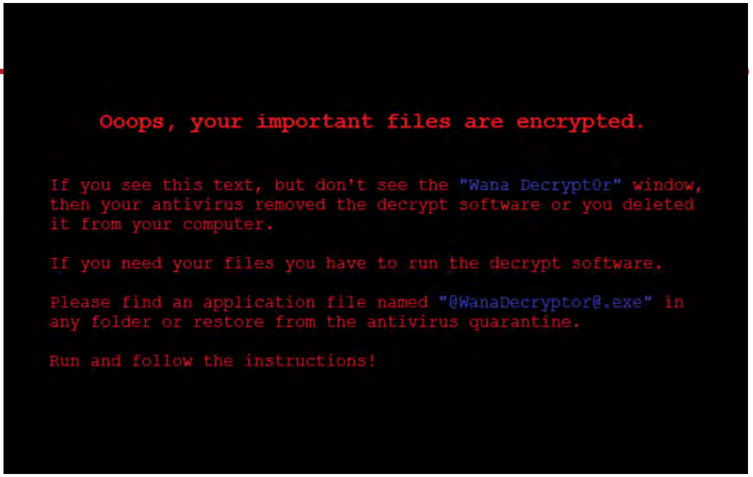
Exchange your cash for a Paysafecard voucher and use your voucher code in form below.

Code:

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/

WannaCry ransomware



```
Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.

Run and follow the instructions!
```

- Spread rapidly through Windows computers in May 2017
  - Spread to 74 countries within days – initial target may have been Russia
  - Estimated to have infected 200,000 computers across 150 countries
  - Hit some high-profile systems, such as Britain's National Health Service

- What does it do?
  - Encrypts files
  - Demands ransom payment in bitcoin
  - $300 in bitcoin to unlock files
  - Price doubles after three days
  - Permanently deleted if ransom not paid in one week

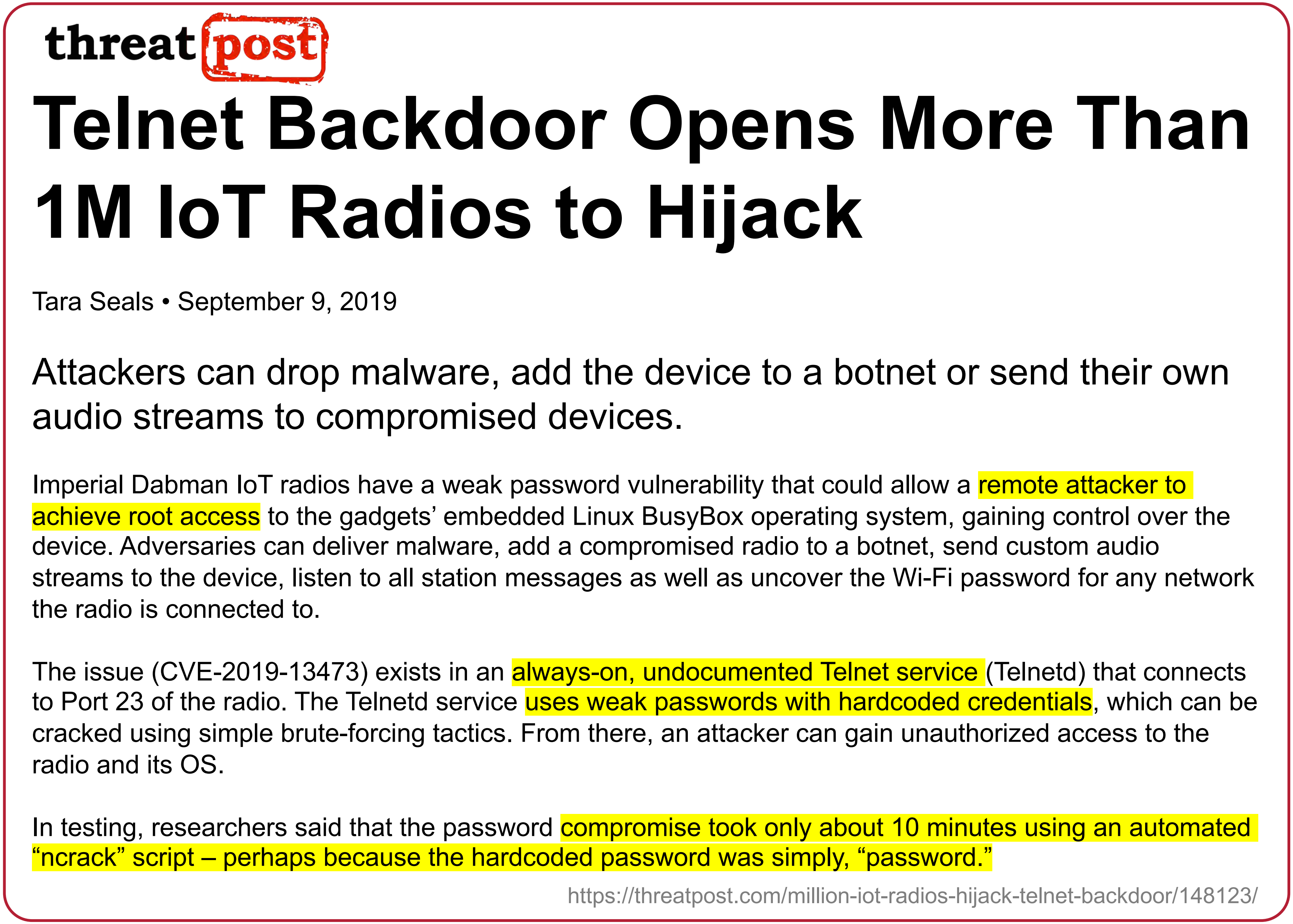
- How did it propagate?
  - Exploited Windows vulnerability in the SMB (Server Message Block protocol)
  - Vulnerability allows use of specially-crafted messages to do remote code execution
    - Vulnerability discovered by the NSA but not reported – kept as part of a cyber arsenal
    - Exploit was stolen by hackers called the Shadow Brokers
    - Shadow Brokers released it in a Medium.com post on April 8 2017
  - Microsoft issued a patch two months before the attacks but

- What's in it?
  - Comes as a "dropper" – self-contained program that extracts other components within it:
    - Encryption/decryption app
    - Files with encryption keys
    - Copy of Tor (anonymous web access)
    - Configuration files

- Speculated that it may have originated in North Korea … but we don't really know

Backdoors

- Remember Robert Morris' Internet worm?
  - Exploited *gets* buffer overflow
  - Tried to crack passwords
  - Connect to remote hosts
  - Also used a back door in `sendmail`
- Sendmail
  - Eric Allman, author of *sendmail*, wanted development access on a production system
  - The sys admin said, "no"
  - He installed a password-protected back door in the next release
    - Back door was generally unprotected
- Ken Thompson's modified C compiler installed a back door to `login`



threatpost

Telnet Backdoor Opens More Than 1M IoT Radios to Hijack

Tara Seals • September 9, 2019

Attackers can drop malware, add the device to a botnet or send their own audio streams to compromised devices.

Imperial Dabman IoT radios have a weak password vulnerability that could allow a remote attacker to achieve root access to the gadgets' embedded Linux BusyBox operating system, gaining control over the device. Adversaries can deliver malware, add a compromised radio to a botnet, send custom audio streams to the device, listen to all station messages as well as uncover the Wi-Fi password for any network the radio is connected to.

The issue (CVE-2019-13473) exists in an always-on, undocumented Telnet service (Telnetd) that connects to Port 23 of the radio. The Telnetd service uses weak passwords with hardcoded credentials, which can be cracked using simple brute-forcing tactics. From there, an attacker can gain unauthorized access to the radio and its OS.

In testing, researchers said that the password compromise took only about 10 minutes using an automated "ncrack" script – perhaps because the hardcoded password was simply, "password."

https://threatpost.com/million-iot-radios-hijack-telnet-backdoor/148123/

Keyloggers

- Record everything you type (sometimes mouse movements too)
  - Allows attackers to get login names, passwords, messages
- Several ways to do this
  - A malicious hypervisor can intercept & log all keyboard & mouse operations
  - Kernel-based rootkit
  - Windows hook mechanism
    - Procedure to intercept message traffic before it reaches a target windows procedure
    - Can be chained
    - Installed via SetWindowsHookEx WH_KEYBOARD and WH_MOUSE
      - Capture key *up*, *down* events and *mouse* events
  - Browser-based
    - JavaScript onKeyUp()
    - Intercept form submission (form grabbing)
- Hardware loggers

Military malware

- Viruses/worms are a key part of most military cyberarsenals
- Espionage & attack
- They get to the target when you cannot reach it directly

Stuxnet

- Most sophisticated known cyberattack
  - 500 KB worm
  - Infected software of at least 14 industrial sites in Iran, including a uranium enrichment plant
  - Used four different 0-day attacks

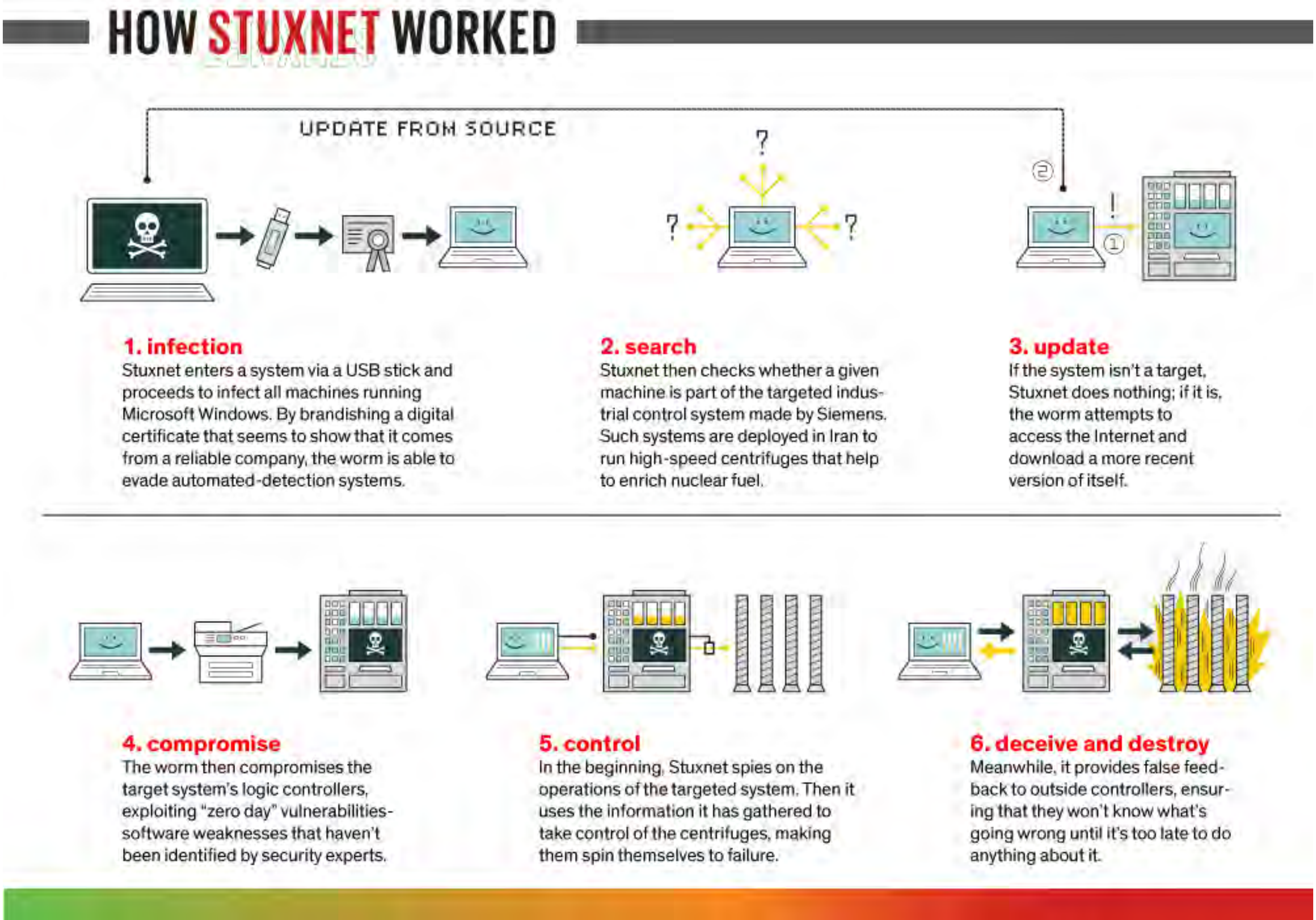
- What it did
  - Targeted Microsoft Windows systems, replicating itself & propagating
    - Via USB thumb drives and LAN attacks
  - Searched for Siemens Step7 software
    - Windows-based software used to program industrial control equipment such as centrifuges
  - Compromised the programmable logic controllers

- Allowed authors to spy on the industrial systems and cause centrifuges to over-spin while the control panel showed everything was OK

Stuxnet: Zero-day exploit

- One zero-day vulnerability used by Stuxnet
  - The rendering of shortcut icons by viewing them in Windows Explorer allowed attackers to run arbitrary code
  - Payload was launched when the target simply viewed the files

See http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568 http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet



HOW STUXNET WORKED

1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Ramifications

- Not much is safe
- Similar attacks can affect
  - Banks
  - Water supplies
  - Power plants
  - Airlines
  - Soon … cars, trucks, buses

Defenses

File Protection

- Embedded devices & older Microsoft Windows systems
  - User processes ran with full admin powers
  - This made it incredibly easy to install malware – even kernel drivers
  - Still a problem with most embedded devices (routers, printers, ...)
- Lack of file protection makes it easier to spread viruses
  - But it can be a pain even if only your files are affected
  - Viruses can override DAC permissions
- Warning users
  - Today's systems warn users about requests for installation or elevated privileges
  - For Trojans, many users will enter their password and say "yes" – they think they want the software
- Mandatory Access Control (MAC) permissions
  - Can stop some viruses if users cannot install or override executable files
  - But macro viruses can still be a problem

Anti-virus software

No way to recognize all possible viruses

Two main approaches

1. Signature-based
2. Behavior-based

Signature-based systems

- Anti-malware companies collect malware
  - Study software in sandboxed environments to see what it tries to do
- **Signature** = set of bytes that are considered to be unique to the malware
- Signature scanning:
  - Presence of those bytes in a file tells us the code as malicious

Anti-virus software: Behavior-based

- Monitor process activity and stop the process if it is deemed malicious
- **Sandboxing**
  - Anti-virus software can run suspected code in a sandbox – or interpreted environment – and see what it tries to do
- **Anomaly detection**
  - Look for abnormal-looking behavior patterns

Behavior-based detection tends to have much higher false positive rates

Most AV products use signature-based detection

Defeating signatures

Viruses can defend themselves

- **Pack** the code – unpack during execution
  - Need run-time detection or else use a signature of the packer
  - **Packers** compress, encrypt, or simply *xor* the payload with a pattern
- Polymorphic viruses:
  - Modify the code but keep it functionally equivalent
  - Add NOPs, use equivalent instruction sequences
  - This changes the signature
  - Do this each time the code propagates

Better yet…

- Write your own malware
- Maybe you can get away with just writing a packer

Block content types

- Detection requires scanning incoming data streams
  - But they can be encrypted

- Malware within HTTP/SMTP content
  - Admins often set up blacklists for SMTP attachments and HTTP content
  - **Blacklisting** = list of disallowed content
    - E.g., people might disallow windows EXE files
  - **Whitelisting** = list of allowed content

  - White lists are preferable it harder to manage
    - There could be a huge number of acceptable file types
    - Similarly, blacklists are dangerous since there are many formats that could transport executable files
    - Microsoft lists 25 file formats that can be directly executable by double clicking
  - Attackers can exploit bugs in allowable content, such as PDF or Excel files

Defeating signatures

- Social engineering based defeats
  - The attacker can pick an arbitrary format and use social engineering to ask a user to rename it
  - Executable malware can also be embedded directly into Microsoft Office documents as an object
  - You then must get users to click on it

Removing admin rights helps a lot

From the BeyondTrust 2019 Microsoft Vulnerabilities Report

- Windows: 499 vulnerabilities reported
- Windows Server: 78% increase in vulnerabilities since 2013
- Internet Explorer & Edge: 137 critical vulnerabilities

- 81% of 189 critical vulnerabilities would be eliminated by enforcing least privilege and removing admin rights
- 100% of critical Microsoft Office vulnerabilities can be fixed by removing admin rights

Note: the analysis only covers ***known*** vulnerabilities

https://www.beyondtrust.com/resources/whitepapers/microsoft-vulnerability-report

Solving the problem

- Access controls don't stop the problem
- Privilege escalation limiting mechanisms work better
  - Removing admin rights is great … but user files remain at risk
  - Containment mechanisms (like containers) work well for servers
    - But not for end-user software
- Running software in a sandbox is great
  - Mobile phones rely on this
  - Often too restrictive for computers
  - You have to trust that users won't be convinced to grant the wrong access rights
- Trojans/worms that exploit human behavior are hard to prevent
  - We're dealing with human nature
  - We're used to accepting a pop-up message and entering a password
  - Better detection in browsers & mail clients helps … but risks junking legitimate content
- Simple software – without automatically-run macros is also good
  - *vi* vs. *MS-Word* … but isn't acceptable to a lot of users

It's still a big problem

The end