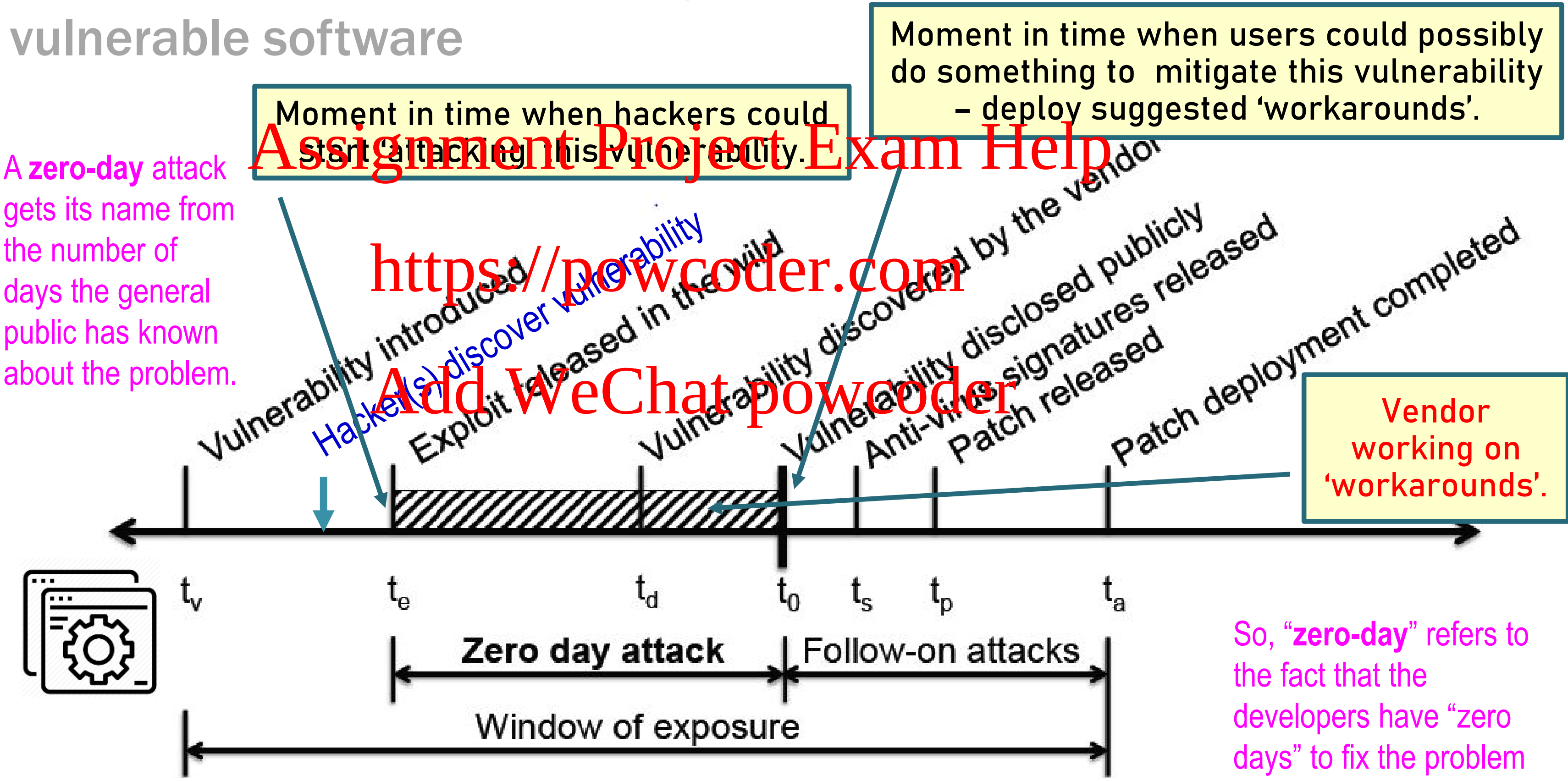
Threat Events: Software Attacks (cont.)

Zero-Day Vulnerability – a computer-software vulnerability NOT known to or addressed by the vendor and users of the vulnerable software



Moment in time when hackers could start attacking this vulnerability.

Moment in time when users could possibly do something to mitigate this vulnerability – deploy suggested 'workarounds'.

A **zero-day** attack gets its name from the number of days the general public has known about the problem.

Vulnerability introduced
Hacker(s) discover vulnerability
Exploit released in the wild
Vulnerability discovered by the vendor
Vulnerability disclosed publicly
Anti-virus signatures released
Patch released
Patch deployment completed
t_v
t_e
t_d
t_0
t_s
t_p
t_a
Zero day attack
Follow-on attacks
Window of exposure

Vendor working on 'workarounds'.

http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf

http://securityaffairs.co/wordpress/9566/hacking/wrong-response-to-zero-day-attacks-exposes-to-serious-risks.html

So, "**zero-day**" refers to the fact that the developers have "zero days" to fix the problem that has just been exposed — and perhaps already exploited by hackers.

Threat Events: Software Attacks (cont.)

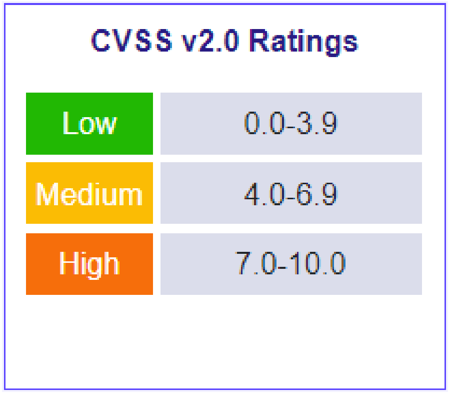
Common Vulnerability Exposure (CVE) – program launched in 1999 by MITRE to identify and catalog vulnerabilities in software and firmware

- MITRE – US non-profit funded by Cybersecurity and Infrastructure Security Agency, part of the US Department of Homeland Security

- CVE database – list of publicly disclosed computer security flaws

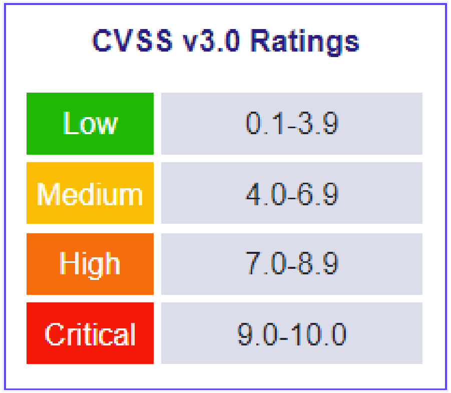
- CVE entry/report – brief description of a reported vulnerability – does not include technical data or information about risk and fixes
- CVE reports can come from anywhere: a vendor, a researcher, a clever user …
- CVSS = CV Scoring System - set of open standards for assigning a number/score to a vulnerability to assess its severity [scores range from 0 to 10]

CVE®
Common Vulnerabilities and Exposures



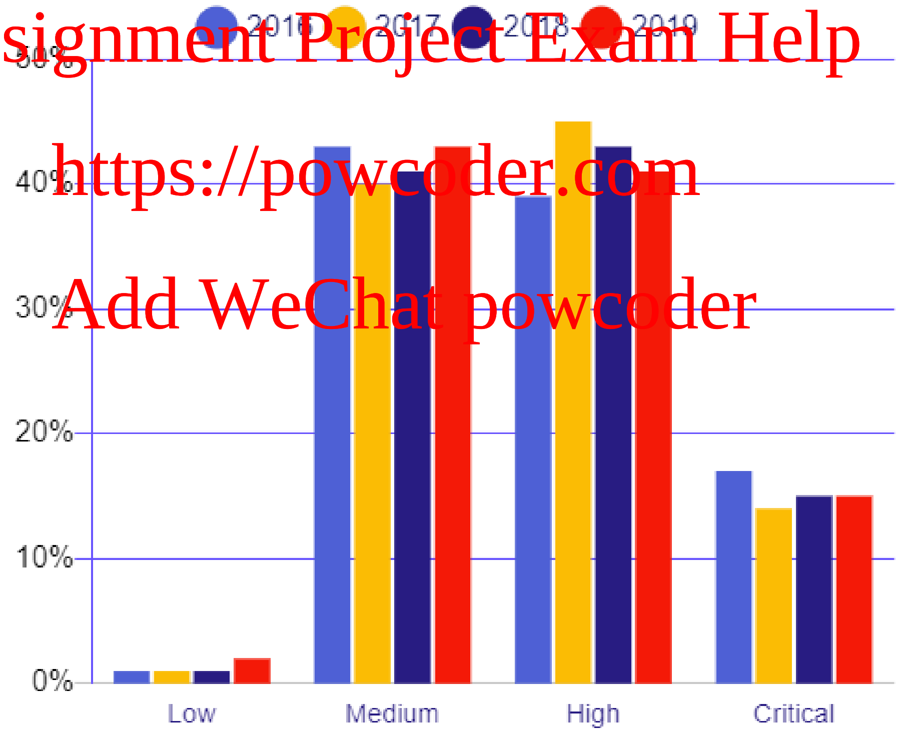
CVSS v2.0 Ratings

Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0



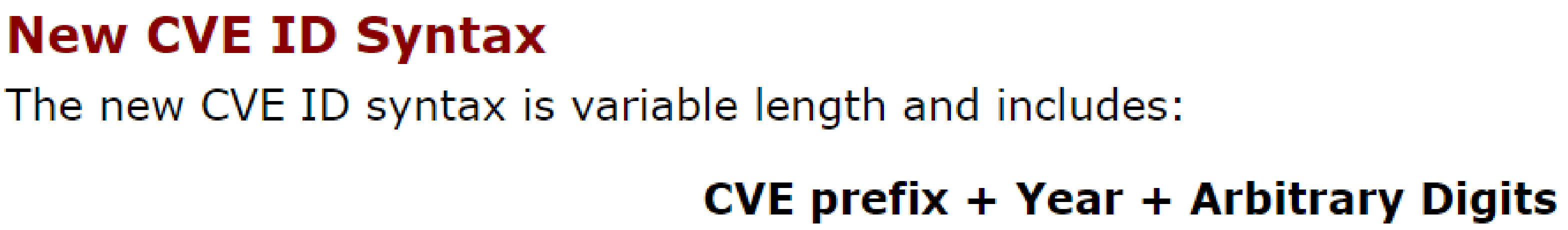
CVSS v3.0 Ratings

Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0



https://www.darkreading.com/vulnerabilities---threats/is-cvss-the-right-standard-for-prioritization/a/d-id/1337712

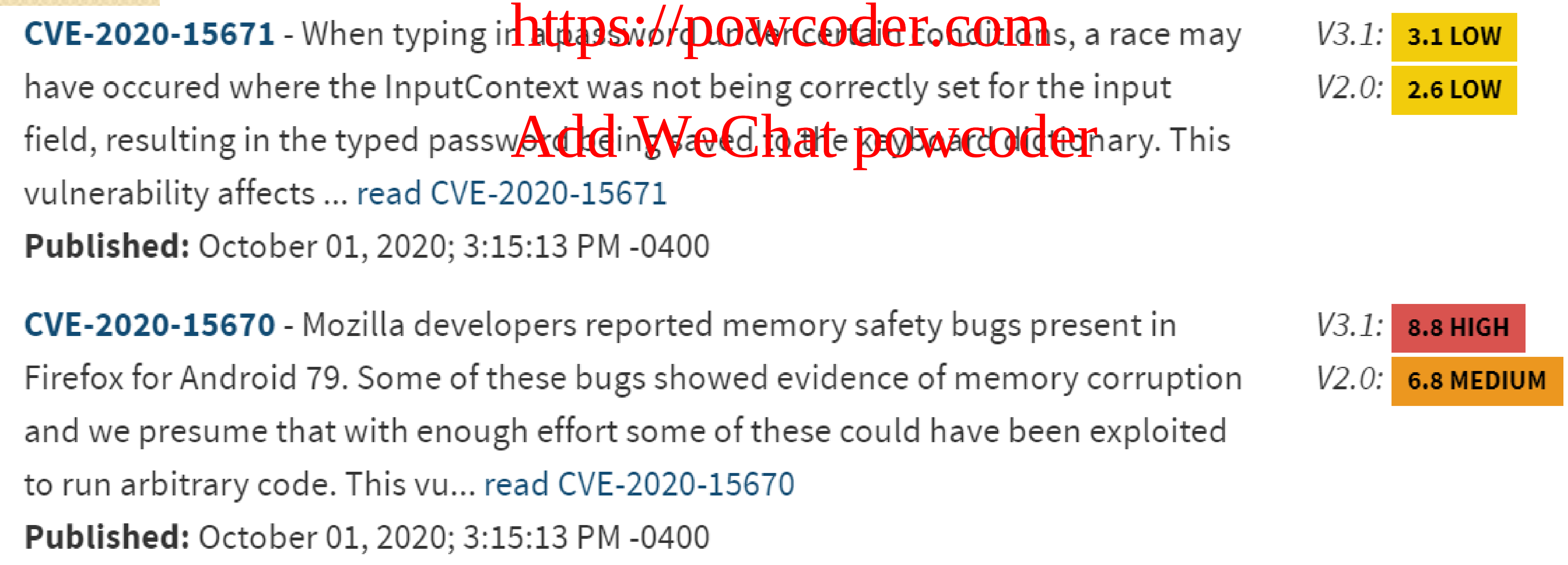
Threat Events: Software Attacks (cont.)



New CVE ID Syntax

The new CVE ID syntax is variable length and includes:

CVE prefix + Year + Arbitrary Digits



CVE-2020-15671 - When typing in a password under certain conditions, a race may have occured where the InputContext was not being correctly set for the input field, resulting in the typed password being saved to the keyboard dictionary. This vulnerability affects ... read CVE-2020-15671

Published: October 01, 2020; 3:15:13 PM -0400

V3.1: **3.1 LOW**

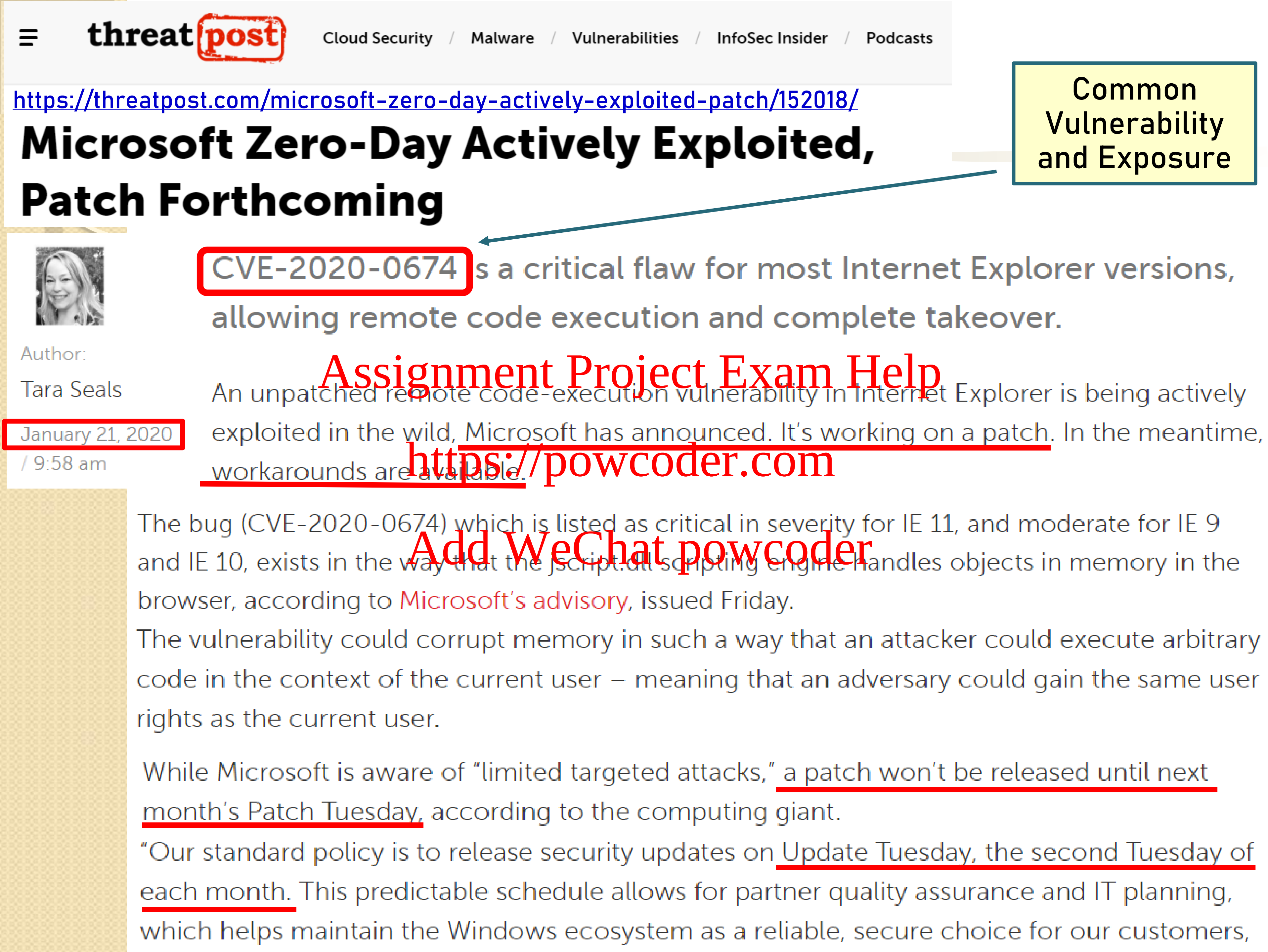
V2.0: **2.6 LOW**

CVE-2020-15670 - Mozilla developers reported memory safety bugs present in Firefox for Android 79. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vu... read CVE-2020-15670

Published: October 01, 2020; 3:15:13 PM -0400

V3.1: **8.8 HIGH**

V2.0: **6.8 MEDIUM**


threatpost
Cloud Security / Malware / Vulnerabilities / InfoSec Insider / Podcasts

https://threatpost.com/microsoft-zero-day-actively-exploited-patch/152018/

Microsoft Zero-Day Actively Exploited, Patch Forthcoming

Common Vulnerability and Exposure

CVE-2020-0674 is a critical flaw for most Internet Explorer versions, allowing remote code execution and complete takeover.

Author:
Tara Seals
January 21, 2020 / 9:58 am

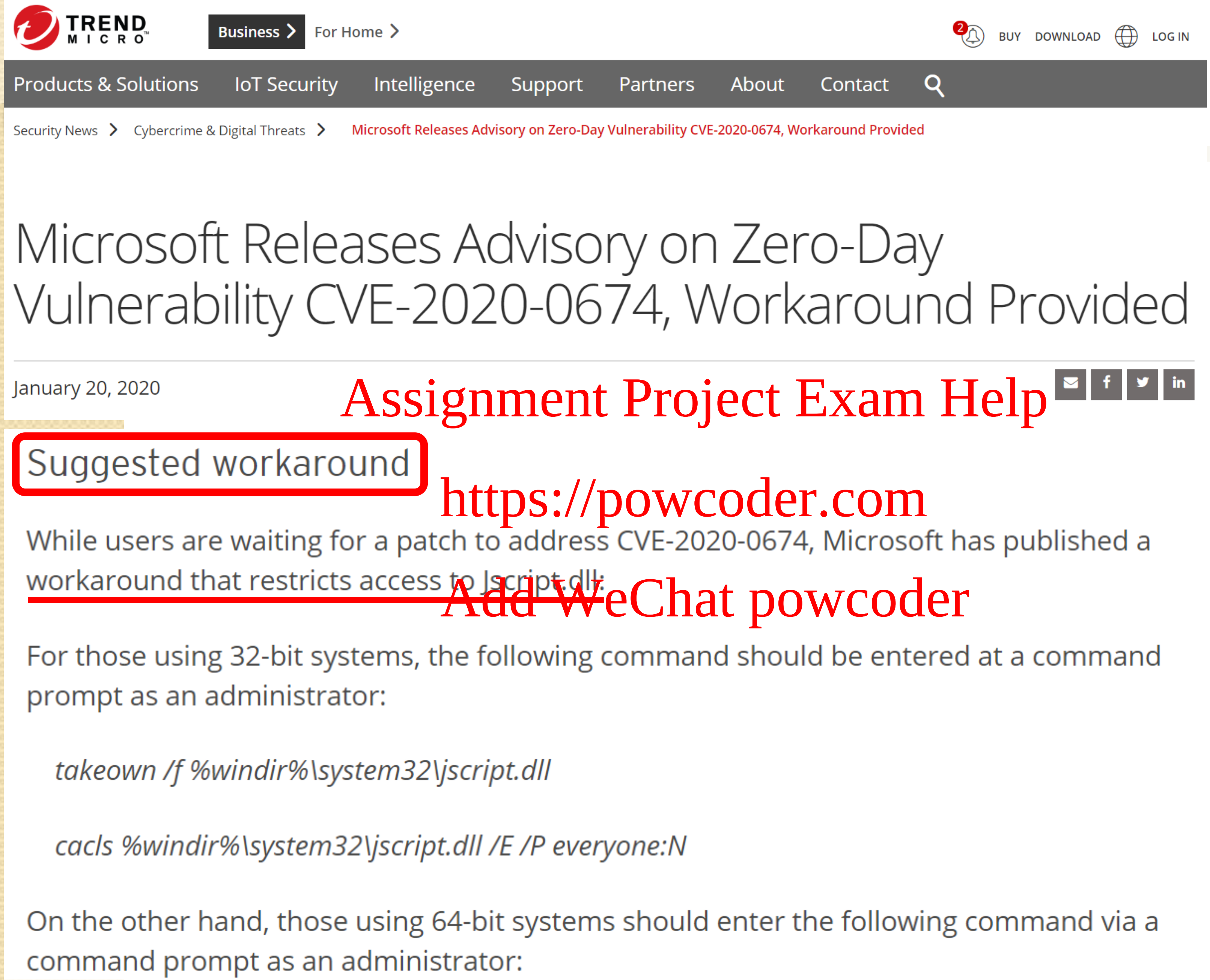
An unpatched remote code-execution vulnerability in Internet Explorer is being actively exploited in the wild, Microsoft has announced. It's working on a patch. In the meantime, workarounds are available.

The bug (CVE-2020-0674) which is listed as critical in severity for IE 11, and moderate for IE 9 and IE 10, exists in the way that the jscript.dll scripting engine handles objects in memory in the browser, according to Microsoft's advisory, issued Friday.

The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user – meaning that an adversary could gain the same user rights as the current user.

While Microsoft is aware of "limited targeted attacks," a patch won't be released until next month's Patch Tuesday, according to the computing giant.

"Our standard policy is to release security updates on Update Tuesday, the second Tuesday of each month. This predictable schedule allows for partner quality assurance and IT planning, which helps maintain the Windows ecosystem as a reliable, secure choice for our customers,



Microsoft Releases Advisory on Zero-Day Vulnerability CVE-2020-0674, Workaround Provided

January 20, 2020

Suggested workaround

While users are waiting for a patch to address CVE-2020-0674, Microsoft has published a workaround that restricts access to Jscript.dll:

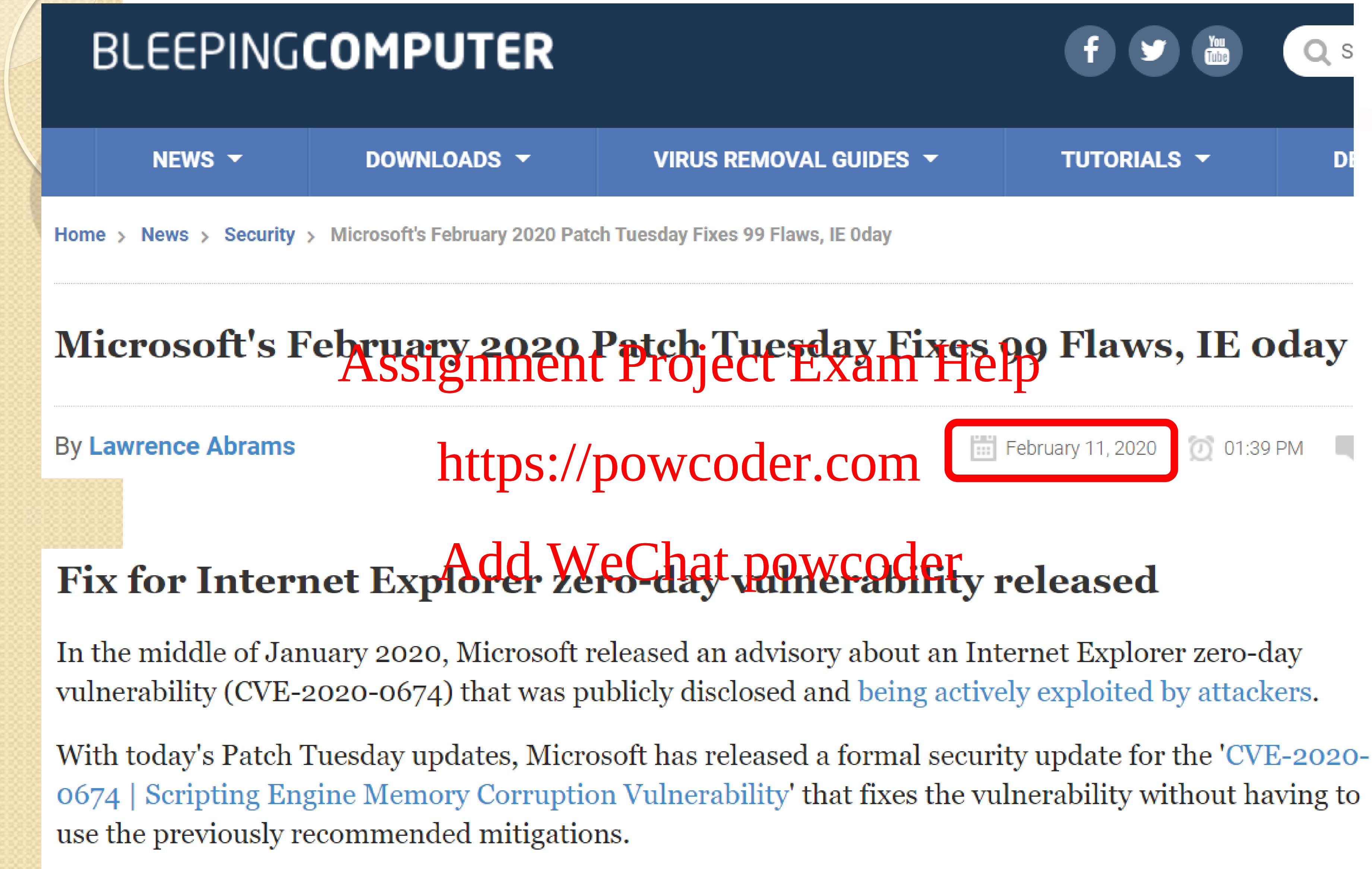
For those using 32-bit systems, the following command should be entered at a command prompt as an administrator:

```
takeown /f %windir%\system32\jscript.dll

cacls %windir%\system32\jscript.dll /E /P everyone:N
```

On the other hand, those using 64-bit systems should enter the following command via a command prompt as an administrator:

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/microsoft-releases-advisory-on-zero-day-vulnerability-cve-2020-0674-workaround-provided


BLEEPINGCOMPUTER
NEWS
DOWNLOADS
VIRUS REMOVAL GUIDES
TUTORIALS
DE
Home › News › Security › Microsoft's February 2020 Patch Tuesday Fixes 99 Flaws, IE 0day

Microsoft's February 2020 Patch Tuesday Fixes 99 Flaws, IE 0day

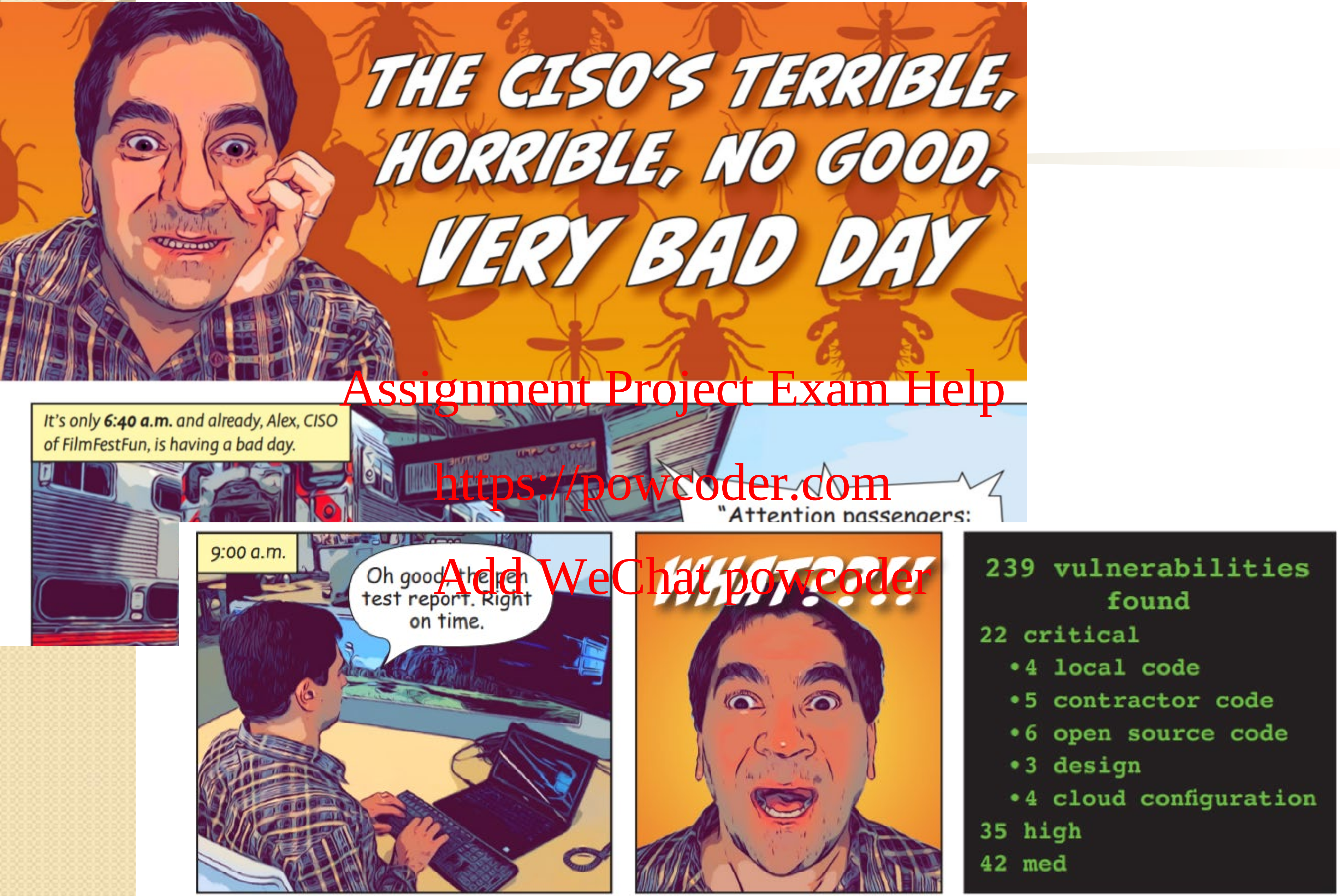
By Lawrence Abrams February 11, 2020 01:39 PM

Fix for Internet Explorer zero-day vulnerability released

In the middle of January 2020, Microsoft released an advisory about an Internet Explorer zero-day vulnerability (CVE-2020-0674) that was publicly disclosed and being actively exploited by attackers.

With today's Patch Tuesday updates, Microsoft has released a formal security update for the 'CVE-2020-0674 | Scripting Engine Memory Corruption Vulnerability' that fixes the vulnerability without having to use the previously recommended mitigations.

https://www.bleepingcomputer.com/news/security/microsofts-february-2020-patch-tuesday-fixes-99-flaws-ie-0day/

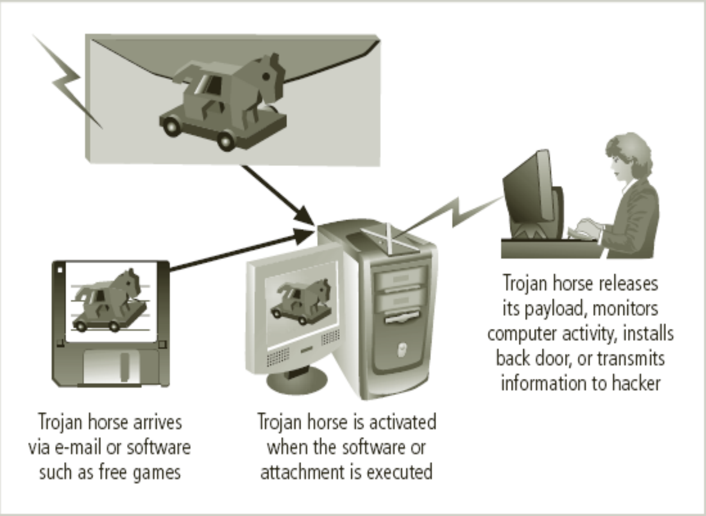

THE CISO'S TERRIBLE, HORRIBLE, NO GOOD, VERY BAD DAY
It's only 6:40 a.m. and already, Alex, CISO of FilmFestFun, is having a bad day.
"Attention passengers:
9:00 a.m.
Oh good, the pen test report. Right on time.
WHAT?!?!

```
239 vulnerabilities
       found
22 critical
  •4 local code
  •5 contractor code
  •6 open source code
  •3 design
  •4 cloud configuration
35 high
42 med
```

https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/cisos-terrible-horrible-no-good-very-bad-day-pdf-1-w-5722.pdf

Threat Events: Software Attacks (cont.)

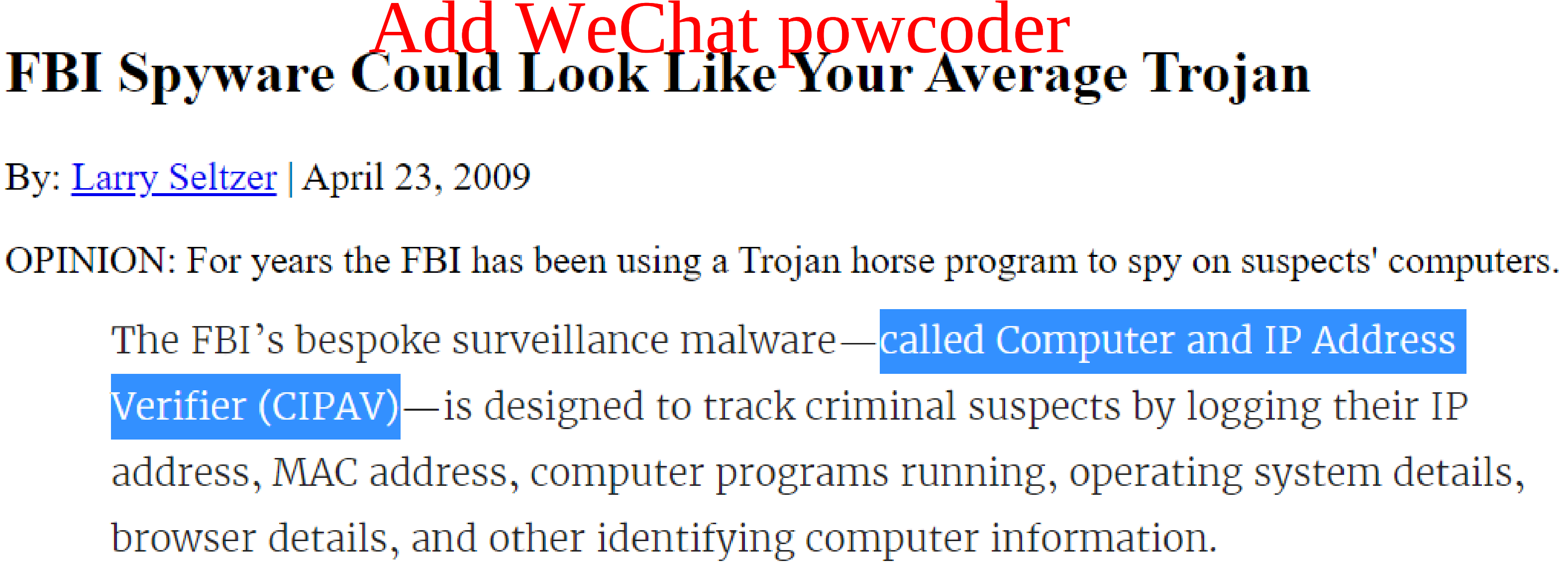
- **TROJAN HORSE** – malware that looks legitimate and is advertised as performing one activity but actually does something else; it does NOT self-replicate
  - example: **AOL4Free** - advertised free access to AOL Internet Service; would delete hard drive
  - common types of Trojans:
    - destructive – designed to destroy data or kill the system – not common today
    - **remote access** – designed to give an attacker control over the victim's system (client-server model)
    - **data sending** – designed to capture and redirect data (keystrokes, passwords, ...) to an attacker


Trojan horse arrives via e-mail or software such as free games
Trojan horse is activated when the software or attachment is executed
Trojan horse releases its payload, monitors computer activity, installs back door, or transmits information to hacker

Threat Events: Software Attacks (cont.)

- common types of Trojans (cont.)
  - **Denial of Service** – designed to conduct a DoS attack on a predefined IP address
  - **FTP** – designed to set up the infected system to serve as an FTP server for illegal software, pirated movies and music, etc.

Example: ‘Legitimate’ Trojans



FBI Spyware Could Look Like Your Average Trojan

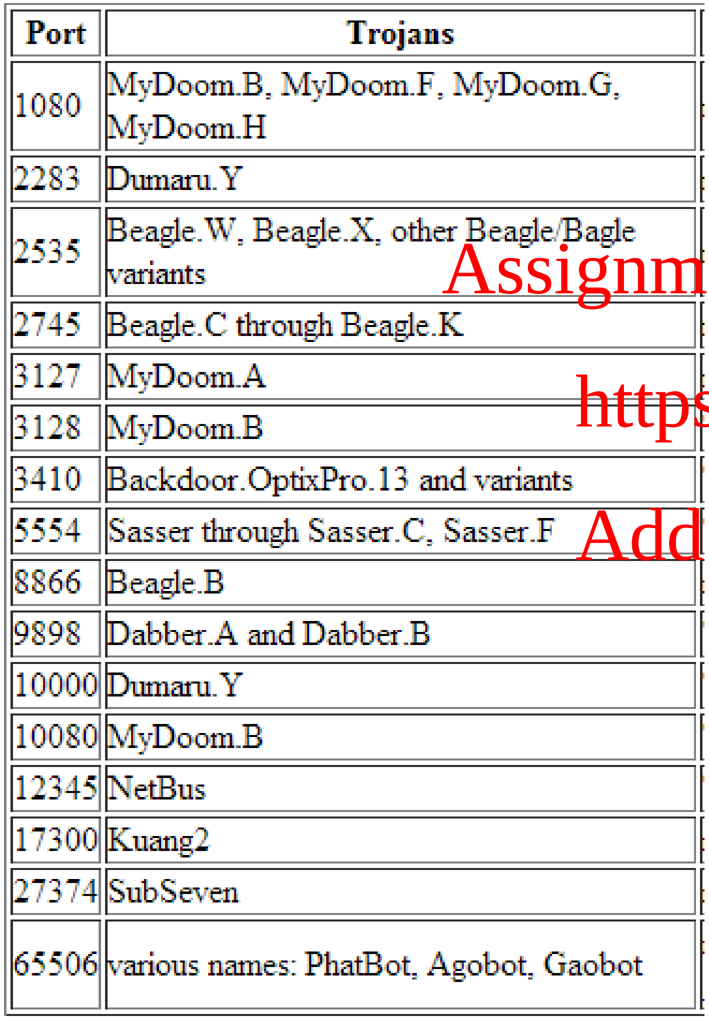
By: Larry Seltzer | April 23, 2009

OPINION: For years the FBI has been using a Trojan horse program to spy on suspects' computers.

> The FBI’s bespoke surveillance malware—called Computer and IP Address Verifier (CIPAV)—is designed to track criminal suspects by logging their IP address, MAC address, computer programs running, operating system details, browser details, and other identifying computer information.

https://www.eweek.com/web/index.php/news/fbi-spyware-could-look-like-your-average-trojan

Threat Events: Software Attacks (cont.)



Port	Trojans
1080	MyDoom.B, MyDoom.F, MyDoom.G, MyDoom.H
2283	Dumaru.Y
2535	Beagle.W, Beagle.X, other Beagle/Bagle variants
2745	Beagle.C through Beagle.K
3127	MyDoom.A
3128	MyDoom.B
3410	Backdoor.OptixPro.13 and variants
5554	Sasser through Sasser.C, Sasser.F
8866	Beagle.B
9898	Dabber.A and Dabber.B
10000	Dumaru.Y
10080	MyDoom.B
12345	NetBus
17300	Kuang2
27374	SubSeven
65506	various names: PhatBot, Agobot, Gaobot

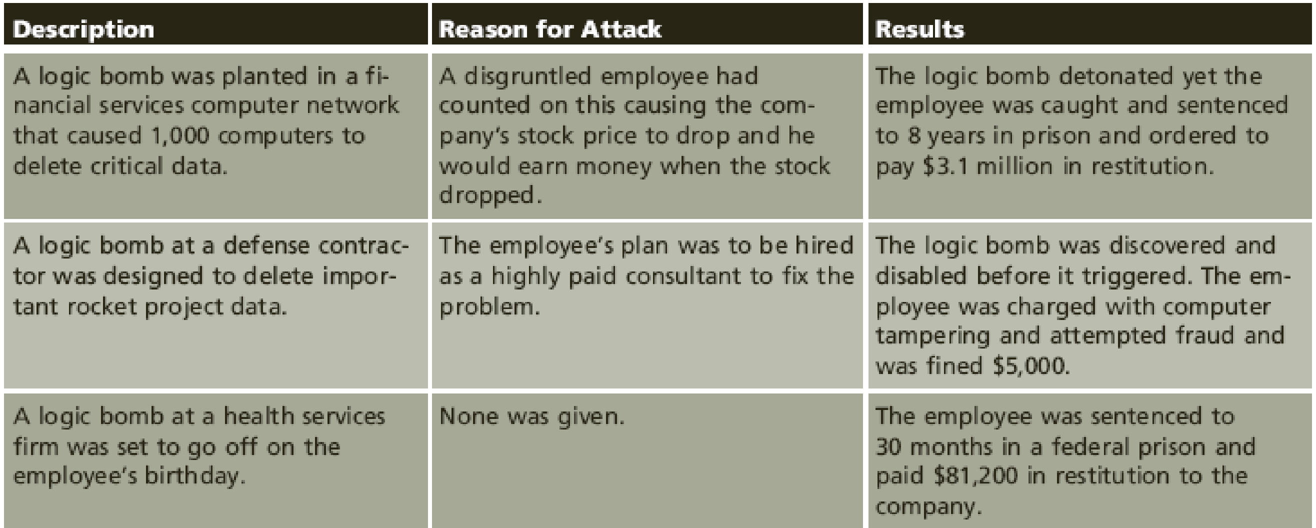
Most Trojans do not 'damage' the host computer, but instead use its resources for illegal purposes through a client-server connection.

How can we detect a Trojan?!

- common techniques of Trojan detection:
  - on the infected computer – run **netstat** and look for unusual ports and connections
  - from the infected network – scan the network with **nmap** and look for systems with unusual open ports

Threat Events: Software Attacks (cont.)

- **LOGIC BOMB** – malware typically installed by an authorized user; lies dormant until triggered by a specific logical event; once triggered, it can perform any number of malicious activities
  - trigger events:
    1) a certain date reached on the calendar – check for organization payroll data;
    2) a person was fired – files deleted once his account got disabled



Description	Reason for Attack	Results
A logic bomb was planted in a financial services computer network that caused 1,000 computers to delete critical data.	A disgruntled employee had counted on this causing the company's stock price to drop and he would earn money when the stock dropped.	The logic bomb detonated yet the employee was caught and sentenced to 8 years in prison and ordered to pay $3.1 million in restitution.
A logic bomb at a defense contractor was designed to delete important rocket project data.	The employee's plan was to be hired as a highly paid consultant to fix the problem.	The logic bomb was discovered and disabled before it triggered. The employee was charged with computer tampering and attempted fraud and was fined $5,000.
A logic bomb at a health services firm was set to go off on the employee's birthday.	None was given.	The employee was sentenced to 30 months in a federal prison and paid $81,200 in restitution to the company.

Threat Events: Software Attacks (cont.)

Example: Roger Duronio story – logic bomb

In 2002, disgruntled system administrator for UBS Investment Bank was accused of planting a logic bomb shortly before quitting his job. The bomb had been designed to wipe out 2,000 files on the main servers for UBS, and cripple the company.

His plan was to drive down the company's stock, and eventually profit from that (*put option contract*).

During the downtime caused by the **logic bomb**, brokers could not access the UBS network or make trades. According to one employer: *"Every branch was having problem. Every single broker was complaining. They couldn't log onto their desktops and [get to] their applications because the servers were down. …"*

In 2006, Duronio was convicted and sentenced to 8 years and 1 month in prison as well as $3.1 million restitution to UBS.

http://www.theregister.co.uk/2006/12/13/ubs_logic_bomber_sentenced/

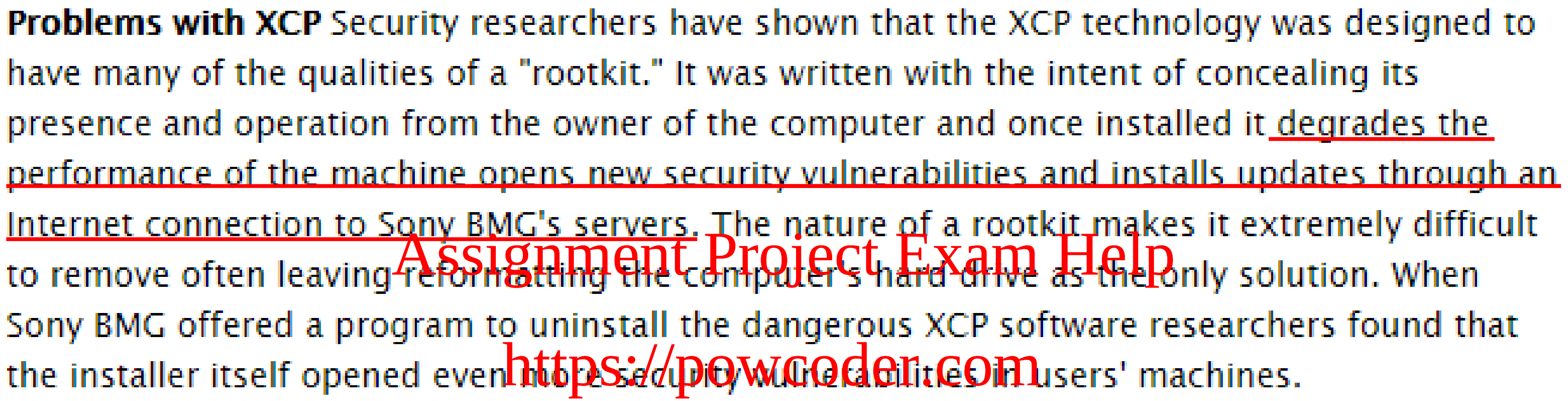
Threat Events: Software Attacks (cont.)

- **ROOTKIT** – stealthy software with root/administrator privileges – aims to modify the operation of the OS in order to facilitate a nonstandard or unauthorized functions
  - unlike virus, rootkit's goal is not to damage computer directly or to spread, but to hide the presence and/or control the function of other (malicious) software
  - since rootkits change the OS, the only safe and foolproof way to handle a rootkit infection is to reformat the hard drive and reinstall the OS

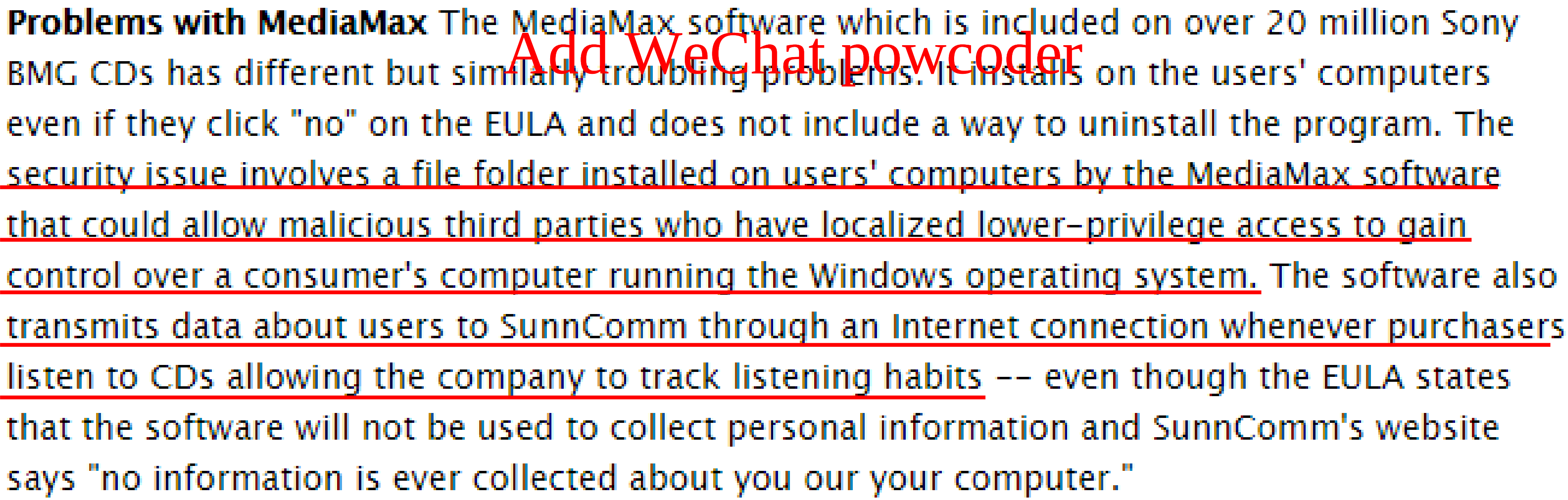
Example: Sony story – rootkit

In 2005, Sony included a rootkit program Extended Copy Protection (XCP) on many of its music CDs in an attempt to limit the user's ability to access the CD and prevent illegal copying.
The software was automatically installed on Windows desktop computers (in a hidden directory + modified the OS) when customers tried to play the CD.

XCP (Extended Copy Protection) and MediaMax - software for copy protection and digital rights management used by Sony

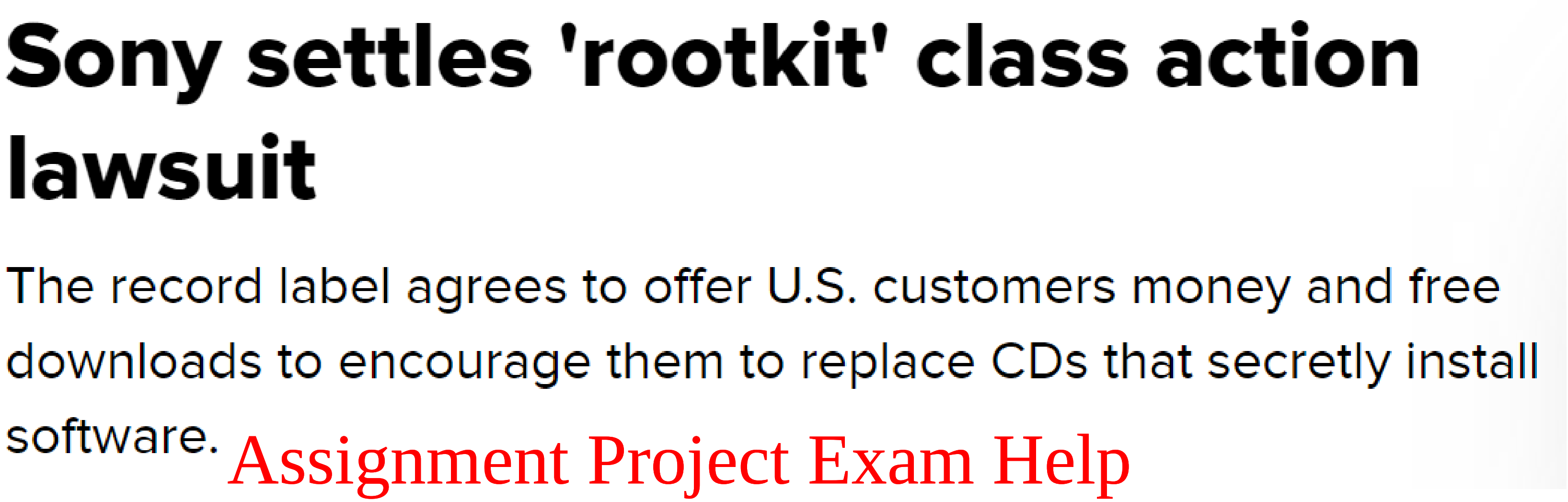


Problems with XCP Security researchers have shown that the XCP technology was designed to have many of the qualities of a "rootkit." It was written with the intent of concealing its presence and operation from the owner of the computer and once installed it degrades the performance of the machine opens new security vulnerabilities and installs updates through an Internet connection to Sony BMG's servers. The nature of a rootkit makes it extremely difficult to remove often leaving reformatting the computer's hard drive as the only solution. When Sony BMG offered a program to uninstall the dangerous XCP software researchers found that the installer itself opened even more security vulnerabilities in users' machines.



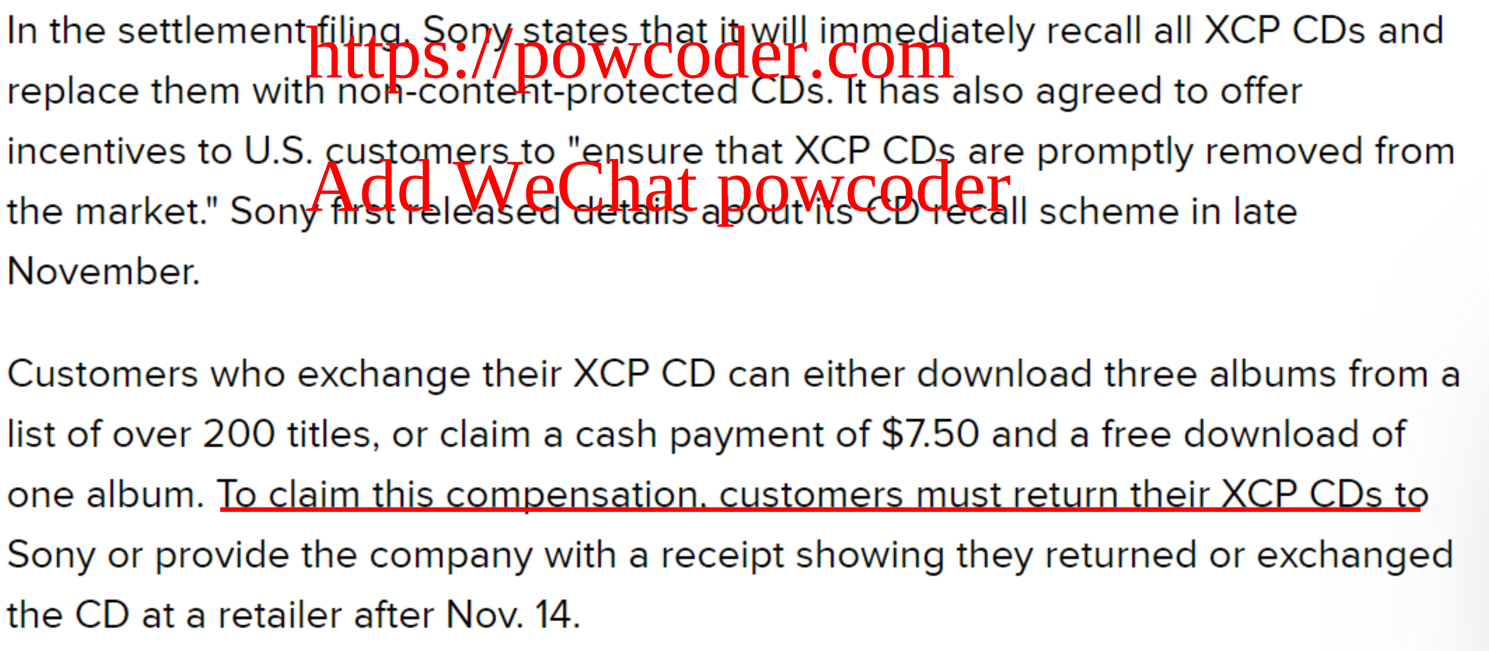
Problems with MediaMax The MediaMax software which is included on over 20 million Sony BMG CDs has different but similarly troubling problems. It installs on the users' computers even if they click "no" on the EULA and does not include a way to uninstall the program. The security issue involves a file folder installed on users' computers by the MediaMax software that could allow malicious third parties who have localized lower-privilege access to gain control over a consumer's computer running the Windows operating system. The software also transmits data about users to SunnComm through an Internet connection whenever purchasers listen to CDs allowing the company to track listening habits -- even though the EULA states that the software will not be used to collect personal information and SunnComm's website says "no information is ever collected about you our your computer."

https://www.eff.org/cases/sony-bmg-litigation-info



Sony settles 'rootkit' class action lawsuit

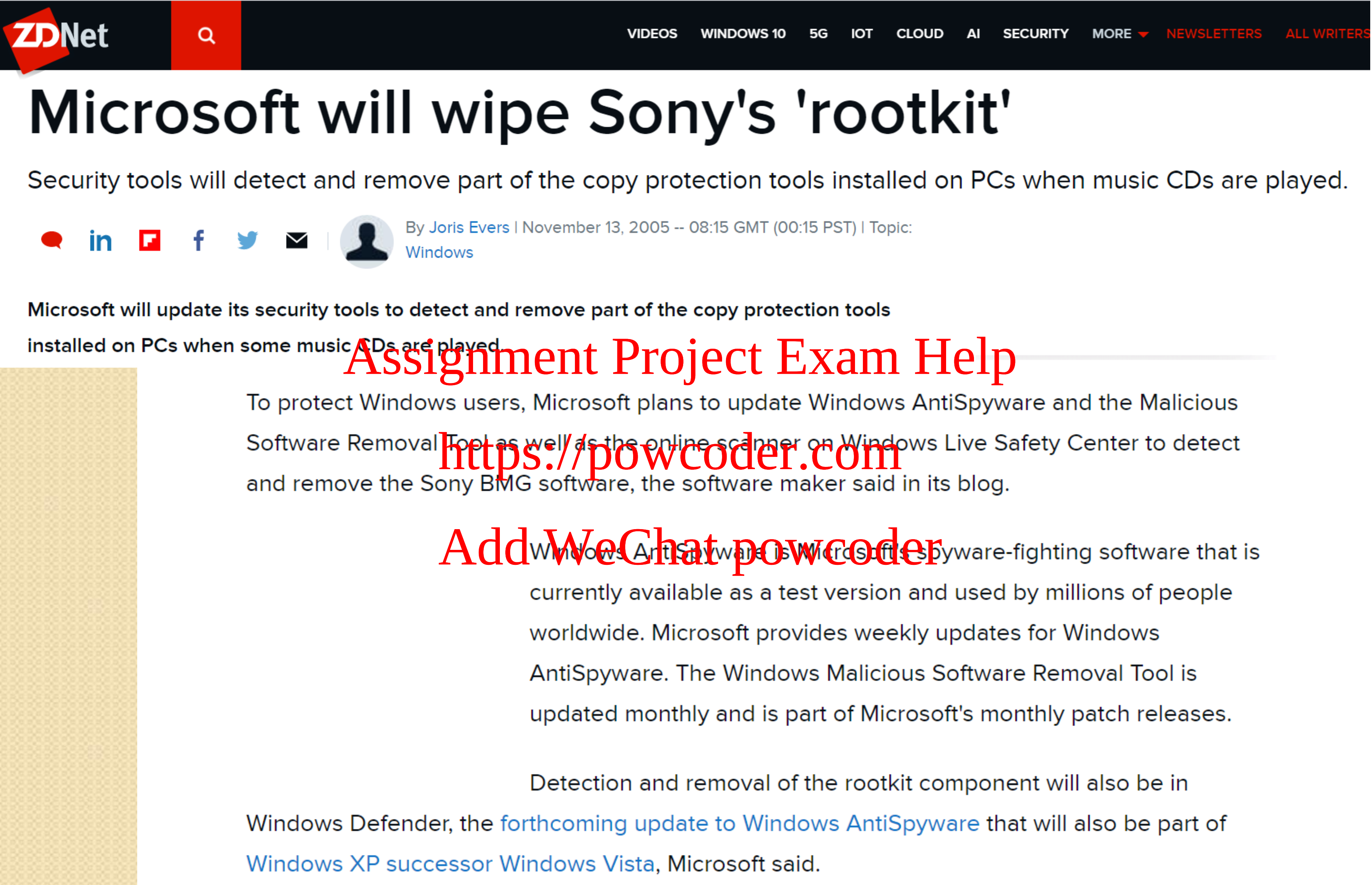
The record label agrees to offer U.S. customers money and free downloads to encourage them to replace CDs that secretly install software.



In the settlement filing, Sony states that it will immediately recall all XCP CDs and replace them with non-content-protected CDs. It has also agreed to offer incentives to U.S. customers to "ensure that XCP CDs are promptly removed from the market." Sony first released details about its CD recall scheme in late November.

Customers who exchange their XCP CD can either download three albums from a list of over 200 titles, or claim a cash payment of $7.50 and a free download of one album. To claim this compensation, customers must return their XCP CDs to Sony or provide the company with a receipt showing they returned or exchanged the CD at a retailer after Nov. 14.

https://www.cnet.com/news/sony-settles-rootkit-class-action-lawsuit/



Microsoft will wipe Sony's 'rootkit'

Security tools will detect and remove part of the copy protection tools installed on PCs when music CDs are played.

By Joris Evers | November 13, 2005 -- 08:15 GMT (00:15 PST) | Topic: Windows

Microsoft will update its security tools to detect and remove part of the copy protection tools installed on PCs when some music CDs are played.

To protect Windows users, Microsoft plans to update Windows AntiSpyware and the Malicious Software Removal Tool as well as the online scanner on Windows Live Safety Center to detect and remove the Sony BMG software, the software maker said in its blog.

Windows AntiSpyware is Microsoft's spyware-fighting software that is currently available as a test version and used by millions of people worldwide. Microsoft provides weekly updates for Windows AntiSpyware. The Windows Malicious Software Removal Tool is updated monthly and is part of Microsoft's monthly patch releases.

Detection and removal of the rootkit component will also be in Windows Defender, the forthcoming update to Windows AntiSpyware that will also be part of Windows XP successor Windows Vista, Microsoft said.

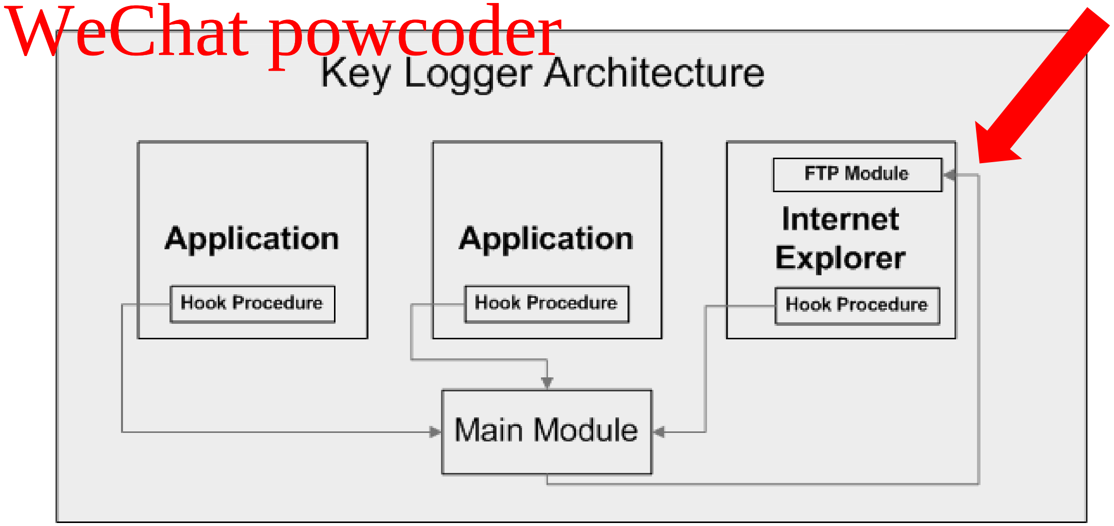
https://www.zdnet.com/article/microsoft-will-wipe-sonys-rootkit/

Threat Events: Software Attacks (cont.)

- **INFORMATION STEALER** – malware that steals information such as: passwords, financial credentials, intellectual property, etc.

  - subcategories of information stealers, based on their implementation, include:

1) Software Keylogger – captures keystrokes in a compromised system



http://www.codeproject.com/Articles/10272/Keyboard-Spy-implementation-and-counter-measures

Threat Events: Software Attacks (cont.)

Example: Hardware Keylogger

Not ‘classical’ malware – does not require any software or drivers to be installed on the victim machine.

Logger is plugged in between USB keyboard and USB port. All keyboard activity is logged to its internal memory.

No ‘physical trace’ stays on the victim machine => challenge for forensics analysis!