

CSE508

Network Security



2024-01-25

Ethics

Michalis Polychronakis

Stony Brook University

“You mean you teach kids how to break into computers and steal stuff?”

Teaching offensive skills is a prerequisite for effective defense

Adversaries are going to develop (or already have) those skills anyway

Offensive skills can be used in different ways

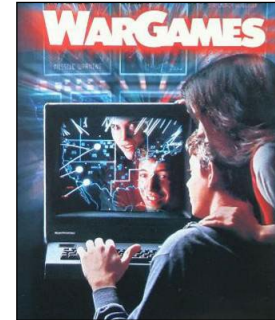
Use them gently and wisely

Use them for the good of society

There are lines that should not be crossed

Motives Have Changed

Threat actors are different



Then: the thrill of figuring out how to exploit vulnerabilities

Now: the thrill of making money

Financial objectives can be achieved in *ethical* and *unethical* ways

What *is* ethical?

Gray areas are everywhere

Most technology can be used for both good and bad

There is a (not always clear) fine line that separates the two

Examples:

Search engine optimization: what tactics are acceptable and when does cheating begin?

Facial recognition: may catch a criminal, but surveils everyone

End-to-end encryption: protects everyone's privacy, including criminals'

The Dual Nature of Encryption

Never-ending debate from a policy perspective

70s–90s: **Crypto wars**

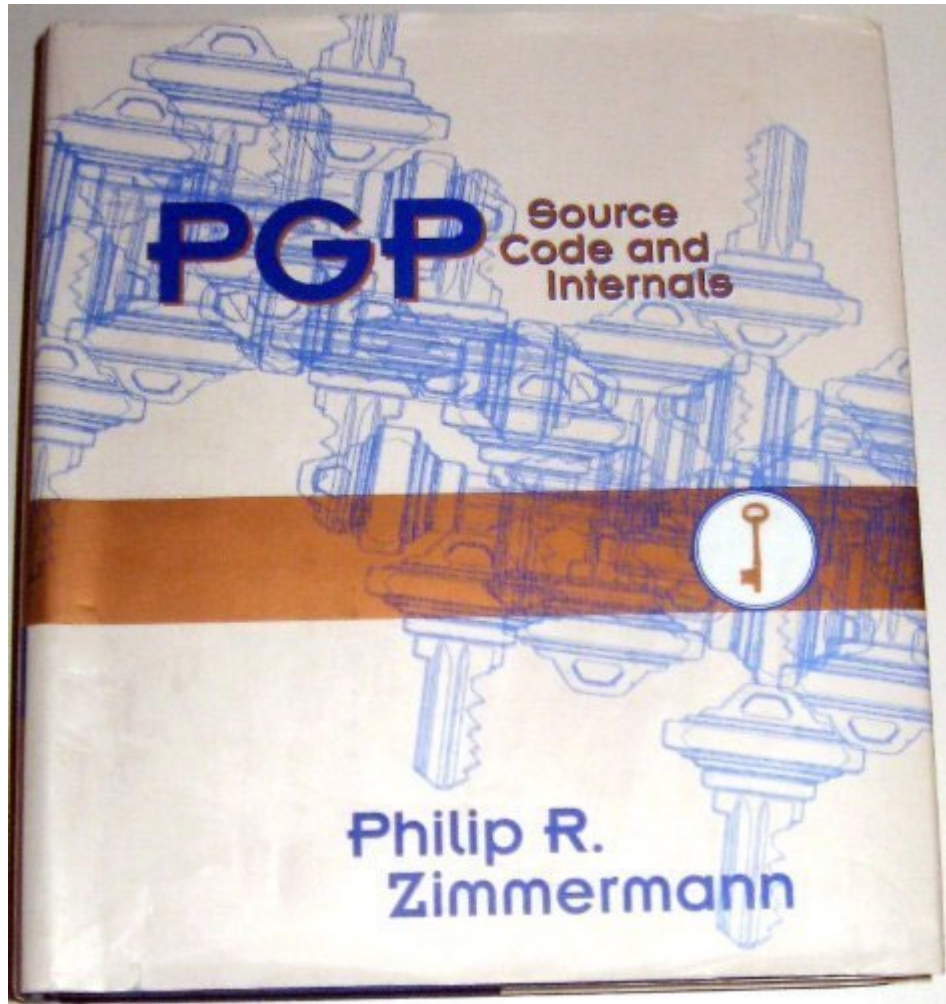
Government-imposed limits to the public's and foreign nations' access to "strong" cryptography (i.e., not breakable by intelligence agencies)

Export controls eventually loosened by USA and EU at the turn of the millennium

00-20s: **End-to-end encryption**

Law enforcement agencies "going dark:" E2EE hampers their ability to access digital evidence in criminal investigations: child sexual abuse material (CSAM), terrorism, ...

Privacy advocates: E2EE is critically important in protecting individual privacy and securing communications against unauthorized access





The Dual Nature of Tools

In most instances, the toolset used by threat actors is the same toolset used by security professionals

Many people don't understand this

The mixed use of the term "hacking" by media and the government doesn't help

Emulating the activities of attackers is the only way to truly test an environment's security level → *penetration testing*

Security policies and intentions are not always reflected by the actual configuration of the systems involved

Example: password policies vs. password cracking

The latter can uncover the use of weak passwords (e.g., due to dictionary words) that still conform to the enforced policy

One way to look at this...

“The hardest problem that I’ve ever had to deal with in software development is to accept that:

1) Bad people exist, and

2) Bad people may use my software to their advantage,

...which I have chosen to accept on the basis that:

3) There are many more good people than bad people, and

4) Enabling the good people is a net win.

I first ran into this problem in 1991 when I first released the [Crack](#) password cracker”

– Alec Muffett

Penetration Testing

Step 1: Establish ground rules

Testing objectives

Attack surface and acceptable tactics

Red vs. Blue team coordination (or not)

Start and stop dates

Legal issues

Confidentiality/nondisclosure

Reporting requirements

Formalized approval and written agreement with signatures and contact information

Mandatory step of even the simplest security assessment engagement

Penetration Testing

Step 2: Reconnaissance

Intelligence gathering and active probing

Step 3: Attack surface enumeration

Identify, enumerate, and document each exposed device

Step 4: Fingerprinting

Identify OS type and version, application patch level, user accounts, ...

Step 5: Target system selection

Identify the most useful targets

Step 6: Exploitation

Select appropriate exploits for the uncovered vulnerabilities

Penetration Testing

Step 7: Privilege escalation

Gain local administrative rights, steal domain controller password, ...

Step 8: Lateral movement

Compromise other hosts if necessary

Step 9: Persistence

Establish a robust command and control channel

Step 10: Documentation and reporting

Document everything: what vulnerabilities were found, how they were found, how they were exploited, precise timeline of events, ...

How would an unethical actor differ?

Step 1: there is no step 1

Motivation: profit, revenge, politics, espionage, ...

No ground rules

Stepping stones/OPSEC to hide the real source of the attack

Steps 2–9 are the same (!)

Step 10: Cover the tracks

Scrub event and audit logs (or alter them for misdirection)

Erase any planted files/executables

Disable/tamper with AVs and other security monitors

(optional) patch the vulnerability to prevent others from gaining access in the future

The main thing that separates a penetration tester from a malicious attacker is **permission**

Ethical and unethical actors carry out basically the same operations, but with different intentions

If an ethical actor does not identify a vulnerability in the system first, an unethical actor may eventually find it and exploit it

Legal Framework (“Cyberlaw”)

Encompasses many elements of the legal structure associated with information security

- How a company contracts and interacts with its suppliers and customers

- Sets policies for employees handling data and accessing company systems

- Uses computers to comply with government regulations and programs

A very important subset for security professionals:

- Laws directed at preventing and punishing unauthorized access to computer networks and data

18 USC 1029: Fraud and Related Activity in Connection with Access Devices

Purpose: curb unauthorized access to accounts, theft of money/products/services, and similar crimes

Criminalizes the possession, use, or trafficking of counterfeit or unauthorized **access devices**

Can be an application or piece of hardware that is created specifically to generate access credentials (e.g., credit card skimmer, keylogger, phishing page)

Or the actual credential itself

Examples:

Hack into a DB and steal credit card numbers

Sniff passwords and use them

Sell fake products online by accepting credit card payments

18 USC 1030: Fraud and Related Activity in Connection with Computers (CFAA)

Outlaws conduct that victimizes computer systems

Prohibits unauthorized access to computers and network systems

Extortion through threats of such attacks

The transmission of code or programs that cause damage to computers

Other related actions

Examples:

Break into a system to obtain private data

Violate the integrity or availability of a system, even if no information is gathered (e.g., DoS)

Break into a system and use its CPU for ~~password cracking~~ cryptocurrency mining

Disgruntled employees use their access to delete a whole database

Selling of stolen credentials

Encrypting data on a drive and demanding money (ransomware)



WIKIPEDIA
The Free Encyclopedia

[Main page](#)
[Contents](#)
[Featured content](#)
[Current events](#)
[Random article](#)
[Donate to Wikipedia](#)
[Wikipedia store](#)

Interaction

[Help](#)
[About Wikipedia](#)
[Community portal](#)
[Recent changes](#)
[Contact page](#)

Tools

[What links here](#)
[Related changes](#)
[Upload file](#)
[Special pages](#)
[Permanent link](#)
[Page information](#)
[Wikidata item](#)
[Cite this page](#)

Print/export

[Create a book](#)
[Download as PDF](#)
[Printable version](#)

In other projects

[Wikimedia Commons](#)
[Wikiquote](#)
[Wikisource](#)

Article [Talk](#)

[Read](#) [Edit](#) [View history](#)

Aaron Swartz

From Wikipedia, the free encyclopedia

For other people with similar names, see [Aaron Swartz \(actor\)](#) or [Aaron Schwartz \(disambiguation\)](#).

Aaron Hillel Swartz (November 8, 1986 – January 11, 2013) was an American computer programmer, entrepreneur, writer, political organizer, and Internet **hacktivist**. He was involved in the development of the **web feed** format **RSS**^[3] and the **Markdown** publishing format,^[4] the organization **Creative Commons**,^[5] the website framework **web.py**,^[6] and the social news site **Reddit**, in which he became a partner after its merger with his company, **Infogami**.^[7]

Swartz's work also focused on civic awareness and activism.^{[7][8]} He helped launch the **Progressive Change Campaign Committee** in 2009 to learn more about effective **online activism**. In 2010, he became a research fellow at **Harvard University**'s **Safra Research Lab** on Institutional Corruption, directed by **Lawrence Lessig**.^{[9][10]} He founded the online group **Demand Progress**, known for its campaign against the **Stop Online Piracy Act**.

On January 6, 2011, Swartz was arrested by **MIT police** on state breaking-and-entering charges, after connecting a computer to the MIT network in an unmarked and unlocked closet, and setting it to download **academic journal** articles systematically from **JSTOR** using a guest user account issued to him by MIT.^{[11][12]} **Federal prosecutors** later charged him with two counts of **wire fraud** and eleven violations of the **Computer Fraud and Abuse Act**,^[13] carrying a cumulative maximum penalty of **\$1 million in fines**, **35 years in prison**, **asset forfeiture**, **restitution**, and **supervised release**.^[14]

He committed suicide while under **federal indictment** for his **alleged computer crimes**, a prosecution that was characterized by his family as being "the product of a criminal-justice system rife with intimidation and prosecutorial overreach".^[15] Swartz declined a **plea bargain** under which he would have served six months in federal prison. Two days after the prosecution rejected a counter-offer by Swartz, he was found dead in his **Brooklyn** apartment, where he had **hanged himself**.^{[15][16]}

In June 2013, Swartz was inducted posthumously into the **Internet Hall of Fame**.^{[17][18]}

Aaron Swartz



Aaron Swartz at a Creative Commons event on December 13, 2008

Born	Aaron H. Swartz ^[1] <div>November 8, 1986</div> Highland Park, Illinois, ^[2] U.S.
Died	January 11, 2013 (aged 26) <div>Brooklyn, New York, U.S.</div>
Cause of death	Suicide
Alma mater	Stanford University
Occupation	Software developer, writer,

Electronic Communication Privacy Act (ECPA)

Purpose: protect communications from unauthorized access

18 USC 2510: Wire and Electronic Communications Interception and Interception of Oral Communications

18 USC 2701: Stored Wire and Electronic Communications and Transactional Records Access

The Digital Millennium Copyright Act (DMCA)

Not directly related, but relevant: protects certain (copyrighted) content from being accessed without authorization

The Cyber Security Enhancement Act of 2002

Increased penalties

Loosened restrictions on ISPs as to when, and to whom, they can voluntarily release information about subscribers

At what point does “hacking” become illegal? (US)

[Ask Question](#)

Asked 9 years, 5 months ago Active 3 years, 11 months ago Viewed 58k times

[Home](#)[Questions](#)[Tags](#)[Users](#)[Unanswered](#)[Jobs](#)

Hypothetical situation: before I hire a web development company I want to test their ability to design secure web apps by viewing their previous client's websites.

60



Issue: this situation raises a big red flag: with regards to viewing a website, what is and is not within the breadth of the law? Or in other words: *at what point does poking around a website become illegal?*



27



- View Source with Firebug? Naturally that would be legal.
- But what if I change HTML (like a hidden form value before submission)?
- Perhaps I then edit or remove JavaScript, like a client side validation script. Would that be legal?
- What if I put `%3Cscript%3Ealert(1)%3C/script%3E` at the end of the URL.
- Or perhaps I type the URL: `example.com/scripts/` and I'm able to view their directory due to faulty permission settings?
- What if I manipulate data passed in HTTP headers, for instance a negative product qty/price to see if they do server side validation (naturally, I wont complete the checkout).

To me, all of this seems perfectly harmless because:

1. I'm not causing undue stress to their server by spamming, mirroring the site with wget, or injecting potentially dangerous SQL.
2. I'm not causing any potential loss or monetary damages, because I wont ever exploit the vulnerabilities, only test for their existence (proof of concept).
3. None of my actions will have any implication for user data privacy. In no way would any of my actions potentially reveal confidential or private information about anyone.
4. If I did find anything I would immediately notify the webmaster of the potential exploit so they could patch it.

Linked

- 539 Why can I log in to my Facebook account with a misspelled email/password?
- 131 Should I contact the manufacturer if their product allows access to other users' location information?
- 9 Found security vulnerability, what should I do?
- 1 Random check for SQLi/XSS - legal?
- 2 How to proceed if the admin and the responsible CERT do not resolve the issue?
- 2 Is information gathering usually authorized?
- 1 Is there any need to penetration test a GoogleAppEngine solution?
- 1 What are good, safe, not necessarily anonymous ways to disclose vulnerabilities?
- 1 Opinions: To report or not to report? CFAA vs the White Hat

Related

- 4 What particular concerns should one bear in mind when wardriving?

6 Answers

Active Oldest Votes

- Home
- Questions**
- Tags
- Users
- Unanswered
- Jobs

48

Don't do it! Don't do it! If you are in the US, the law is very broad. You don't want to even tiptoe up to the line.

✓

The relevant law is the Computer Fraud and Abuse Act (18 U.S.C. 1030). In a nutshell (and simplifying slightly), under the CFAA, it is a federal crime to "intentionally access a computer without authorization or exceed authorized access". This language is very broad, and I imagine an ambitious prosecutor could try to use it to go after everything on your list except #1 (view source).

🔄

Orin Kerr, one of the leading legal scholars in this area, calls the statute "vague" and "[extraordinarily broad](#)", and has said that "[no one actually knows what it prohibits](#)".

And, as @Robert David Graham explains, there have been cases where folks were prosecuted, threatened with prosecution, or sued for doing as little as typing a single-quote into a textbox, adding a `../` to a URL, or signing up to Facebook under a pseudonym. It's pretty wild that this alone constitutes a federal offense, even if there is no malicious intent. But that's the legal environment we live in.

I'd say, don't take chances. Get written authorization from the company whose websites you want to test.

edited Feb 17 '17 at 7:07

answered Aug 18 '11 at 6:26

Share Improve this answer Follow

D.W. 95.4k 28 254 545

4 What exactly does the addition of ../ to a URL do? – nitrl Jun 7 '13 at 2:34

2 @nitrl, in some cases (very poorly coded web applications), it may allow bypassing access control restrictions or accessing content that the developer didn't intend/expect for you to be able to access. See also the notion of a path traversal vulnerability. – D.W. Jun 7 '13 at 4:56

8 @D.W., Thanks, couldn't find it on my own. Linked below for anyone else who might come across this. en.wikipedia.org/wiki/Directory_traversal_attack – nitrl Jun 7 '13 at 6:49

- Word for a song with defamatory content, written and spread to mock the one or what the song is about?
- Has politics always been so polarized?
- How to prove no-arbitrage when a long butterfly is strictly positive?
- Where does Martian meaning inhabitant of Mars come from?
- How do I ask people out in an online group?
- I am trying to unzip bz2 file but then I get the error saying No space left
- Why "the" in "looking in the mirror"?
- Bash: value too great for base when using a date as array key
- Brainfuck interpreter in C++ with namespaces
- Can the alarm spell be detected by mundane means such as a normal perception check?
- What can I replace oversized waterproof outlet cover with?
- What happens when you reduce stock all the way?
- Californian resident travelling in EU - which privacy law applies?

Question feed

Security pros savage Tsunami hacker verdict

John Oates, The Register 2005-10-11

Last week Daniel Cuthbert was convicted of breaking the Computer Misuse Act, fined £400, and ordered to pay £600 in costs. As an IT security consultant, it will be a long time before Cuthbert's reputation is restored and it is possible he will never work in the industry again.

But it is going to take just as long for the police to recover their reputation amongst much of the IT security community. The decision to prosecute Cuthbert might be "good PR", as one officer told the Register last week, but it could make it harder for police to chase computer criminals in the future. Some observers believe it will damage the relationship between the police and the security professionals they rely on for information and advice.

Cuthbert, a 28 year old from Whitechapel, London, was a security consultant at ABN Amro, a job he lost as a result of his arrest. He also lectured at Westminster and Royal Holloway universities - ironically he taught some members of the Computer Crime Unit.

On December 31, 2004, Cuthbert, using an Apple laptop and Safari browser, became concerned that a website collecting credit card details for donations to the Tsunami appeal could be a phishing site. After making a donation, and not seeing a final confirmation or thank-you page, Cuthbert put ../../../../ into the address line. If the site had been unprotected this would have allowed him to move up three directories.

After running the two tests, at between 15.12 and 15.15 on New Year's Eve, Cuthbert took no further action.

In fact his action set off an Intrusion Detection System at BT's offices in Edinburgh and the telco called the police. A witness for BT confirmed that the attack would have had no effect on its server, running Unix Solaris, even if it had not been detected by the IDS. The Crown also accepted that there was no malicious motive in Cuthbert's actions.

The police were able to track Cuthbert down because of the donation he made just before running the tests. He was arrested, brought in for questioning and subsequently charged with breaking the Computer Misuse Act.

Feedback to our story on Cuthbert's conviction last week was mostly sympathetic to Cuthbert though some felt he had overstepped the boundaries.

One reader said: "There are occasions where criminal damage charges could be used under this act, but it seems this wasn't one of

Vulnerability Disclosure

An individual or team who uncovers a previously unknown (*zero-day*) vulnerability has several options

Make all information public right away → **full disclosure**

Work with the vendor to fix it → **coordinated disclosure**

Use or provide this knowledge to others (for profit)

If criminal: exploit it as part of illegal activities

If government: exploit it as part of authorized engagements *

Different entities with different interests

Security analyst → Vendor → Consumers

What is the best way?

** Not all governments are the same, more on this later on*

Full vs. Coordinated Disclosure

An old debate: 19th-century locksmithing

Should weaknesses in locks be kept secret in locksmithing circles, or be revealed to the public?

Full disclosure: publish all information (including PoC) as early as possible

Forces vendors to take immediate action and improve products

Allows administrators to assess the risk to their systems and deploy countermeasures (e.g., firewall rules, IDS signatures, custom patches, disable features)

Malicious actors who may also have the same knowledge will lose their advantage

Malicious actors who didn't know about it can now start using it for malicious purposes

Coordinated disclosure: notify the vendor and wait until a patch is released

Most users cannot benefit from access to vulnerability information but just wait for the patch

Prevent *new* malicious actors (even low-skilled attackers) from exploiting the vulnerability while a patch is under development

Date: Sat, 23 Jun 90 14:49:30 PDT
From: neil (Neil Gorsuch)
Subject: WELCOME to core

[WELCOME TO CORE. Digests will be coming out about once a week. Because of the delays in getting things set up, there is enough stuff waiting here that I am splitting it into two digests to avoid mailer problems. You should receive issue 2 at the same time that you receive this. In case my handy dandy script that adds members didn't send the welcome message to you correctly, here it is again ...

Welcome to the core security mailing list!

THIS IS NOT THE ZARDOZ SECURITY MAILING LIST! The core list is a small subset of the zardoz security list. The core list is much more difficult to join, and the membership is limited to a small select group of people. The zardoz list exists for these reasons:

1. To notify system administrators and other appropriate people of serious security dangers BEFORE they become common knowledge.
2. Provide security enhancement information.

The core list shares those goals, and in addition is meant for the open discussion of NEW and UN-FIXED security holes. The members of the core list are expected to be actively finding and FIXING new security holes. Any new holes that are found to be "pluggable" by the vast majority of binary-only sites that they affect, will have only the directions for "plugging" them forwarded to the zardoz list after about a 2 week delay by me. NO "COOKBOOK" DIRECTIONS for duplicating the holes will leave the core list. If the directions for plugging the holes make the nature of the hole obvious, a brief description of the hole will also be sent to the zardoz list. After an additional 3 or 4 week delay, I will post some even more abbreviated "plugging" directions to the news group alt.security.

CERT/CC's Disclosure Process

Goal: balance the public's need to be informed with the vendors' need for enough time to respond effectively

Reported vulnerabilities will be disclosed to the public 45 days after the initial report

Regardless of the existence or availability of patches or workarounds from affected vendors

CERT/CC will notify the software vendor immediately so that a solution can be created as soon as possible

During the 45-day window, CERT/CC will update the reporter on the current status without revealing confidential information

Disclosures made by the CERT/CC will include credit to the reporter unless otherwise requested by the reporter

Extenuating circumstances, such as active exploitation, threats of an especially serious (or trivial) nature, or situations that require changes to an established standard may result in earlier or later disclosure

What about non-disclosure?

It doesn't improve security in general

Some proponents argue that they simply do not want to assist vendors, and claim no intent to harm others

Entirely opposing perspective compared to both full and coordinated disclosure

The actor who uncovers the vulnerability is in control

Government agency: may keep it for strategic advantage against enemies

Security firm: may keep it for succeeding in security assessment engagements

Researcher: may sell it to the higher bidder or multiple customers

Criminal: may use it to compromise victims

Zero-day exploits provide a powerful capability

Should profit be the only driving factor?

What about the actual *use* of a zero-day?

- By government agencies

- By private companies

The Shadow Brokers Mess x

https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/

WIRED The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days SUBSCRIBE

BUSINESS CULTURE DESIGN GEAR SCIENCE **SECURITY** TRANSPORTATION

SHARE

f SHARE 811

t TWEET

p PIN 5

COMMENT 16

EMAIL


ANDY GREENBERG SECURITY 08.17.16 8:34 PM

THE SHADOW BROKERS MESS IS WHAT HAPPENS WHEN THE NSA HOARDS ZERO-DAYS

ANDREW HARRER/BLOOMBERG/GETTY IMAGES

WHEN THE NSA discovers a new method of hacking into a piece of software or hardware, it faces a dilemma. Report the security flaw it exploits to the product's manufacturer so it gets fixed, or keep that vulnerability secret—what's known in the security industry as a “zero day”—and use it to hack its targets, gathering valuable intelligence. Now a case of data apparently stolen from an NSA hacking team seems to show the risks that result when the agency chooses offense over defense: Its secret hacking tools can fall into unknown hands.

On Wednesday, networking equipment firms Cisco and Fortinet warned customers about vulnerabilities revealed in



GET WIRED
Don't Let The Future Leave You Behind. Get 6 Issues For Just \$5.
SUBSCRIBE NOW

LATEST NEWS

NEWS TODAY
Twitter Shares Revenue With Video Makers
8 HOURS

BUSINESS
Microsoft Launches New Tools For Curbing Online Abuse
1 DAY

ABSURD CREATURES
What Gives With Insects Pretending to Be Sticks and Leaves?

“There’s always that delicate balance: how do they accomplish their mission, hack their adversaries, and still protect the rest of us?”

“Given that the data stolen by Shadow Brokers appears to be three years old, that could mean the NSA may have used the hacking technique in secret for years—and possibly allowed it to fall into the hands of its adversaries for just as long.”

EternalBlue

Microsoft Windows SMB Server Remote Code Execution Vulnerability

CVE-2017-0144, MS17-010

Windows XP, Vista, Server 2003/2008/2012, 7, 8, 8.1, 10

Developed by the NSA

Did not notify Microsoft and held on to it for more than five years

Leaked by the Shadow Brokers on April 14, 2017

One month after Microsoft released the patch

May 12, 2017: used by the WannaCry ransomware

June 27, 2017: used by NotPetya, primarily targeting Ukraine

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am CMT from Mondays Friday

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:

 **bitcoin**
ACCEPTED HERE

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

“Stockpiling” 0-days vs. Fulfilling Tactical Needs

<favorite agency> has two goals

1. Foreign and domestic intelligence and counterintelligence (SIGINT)
2. Defend vital networks and information systems

When a new 0-day is found, there are two options:

Disclose it to help improve security in general

Hampers goal 1

Keep it secret for use in future missions (at least for a while)

Hampers goal 2

“Stockpiling” 0-days vs. Fulfilling Tactical Needs

The longer a 0-day remains secret and is being used, the higher the chance it will eventually be discovered by someone else

- Another team may happen to find the same bug

- A target may capture the exploit while being used against them

- Accidental leak or compromise (e.g., Shadow Brokers case)

OTOH, <favorite agency> needs 0-days for its mission

- Disclosing all vulnerabilities right away will hamper its strategic advantages

Vulnerabilities Equities Process

- Used by the U.S. federal government to determine on a case-by-case basis how it should treat a new 0-day (disclose or keep)

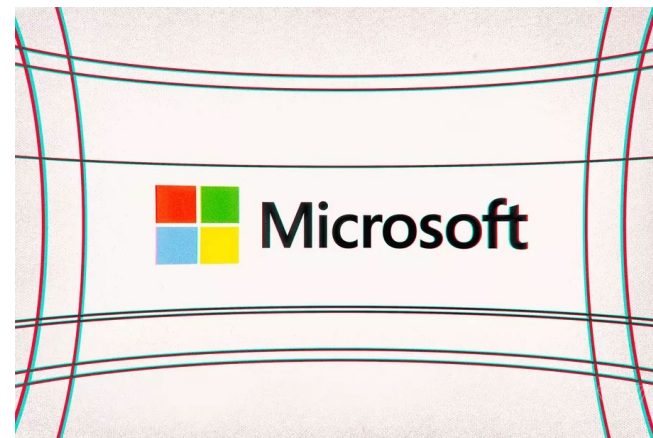
Microsoft patches Windows 10 security flaw discovered by the NSA

The NSA is accepting attribution for the first time in history

By Tom Warren | @tomwarren | Jan 14, 2020, 1:25pm EST

Microsoft is patching a serious flaw in various versions of Windows today after the National Security Agency (NSA) discovered and reported a security vulnerability in Microsoft's handling of certificate and cryptographic messaging functions in Windows. [The flaw](#), which hasn't been marked critical by Microsoft, could allow attackers to spoof the digital signature tied to pieces of software, allowing unsigned and malicious code to masquerade as legitimate software.

The bug is a problem for environments that rely on digital certificates to validate the software that machines run, a potentially far-reaching security issue if left unpatched. The NSA reported the flaw to Microsoft recently, and it's recommending that enterprises patch it immediately or prioritize systems that host critical infrastructure like domain controllers, VPN servers, or DNS servers. Security reporter Brian Krebs first revealed the [extent of the flaw yesterday](#), warning of potential issues with authentication on Windows desktops and servers.



Offensive Capabilities Can Cause Harm

The clients of individual researchers and offensive security companies may use the provided services for shady purposes

- Repressive governments going after activists, journalists, opposition leaders, ...

- Domestic abusers spying on their victims

- Illegal financial gain, intellectual property theft, revenge, ...

It is our choice to whom we provide our skills and services

BIZ & IT —

Hacking Team gets hacked; invoices suggest spyware sold to repressive govts

Invoices purport to show Hacking Team doing business in Sudan and other rogue nations.

DAN GOODIN - 7/6/2015, 12:26 PM

53

A controversial company that sells weaponized spyware has been penetrated by hackers who claim to have plundered more than 400GB worth of e-mails, source code, and other sensitive data—including invoices showing that the firm has done business in countries ruled by highly repressive governments.

f



Italy-based Hacking Team has long denied selling to nations with poor human rights records. It instead markets itself as a supplier of customized software for law enforcement departments and government agencies in countries with good human rights records. Its spyware, company officials have said, helps crack down on criminals and terrorists. Over the weekend, unidentified people claimed to hack Hacking Group computers and social media accounts and to make off with documents contradicting

Hacking Team Hacked

Advanced spyware for Android now available to script kiddies everywhere

Hacking Team may not have had a backdoor, but it could kill client installs

Hacking Team goes to war against former employees, suspects some helped hackers

Firm stops selling exploits after delivering Flash 0-day to Hacking Team

Hacking Team built drone-

Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says

By [David D. Kirkpatrick](#)

Dec. 2, 2018

LONDON — A Saudi dissident close to the murdered journalist Jamal Khashoggi has filed a lawsuit charging that an Israeli software company helped the royal court take over his smartphone and spy on his communications with Mr. Khashoggi.

The lawsuit puts new pressure on the company, [the NSO Group](#), and on the government of Israel, which licenses the company's sales to foreign governments of its spyware, known as Pegasus. More broadly, the suit also calls new attention to Israel's increasingly open alliance with Saudi Arabia and other Persian Gulf monarchies.

Saudi Arabia and its allies like the United Arab Emirates have never recognized the Jewish state but have quietly found common



Stopping the Press

New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator

By Bill Marczak, Siena Anstis, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert

January 28, 2020

Key Findings

- *New York Times* journalist Ben Hubbard was targeted with NSO Group's Pegasus spyware via a June 2018 SMS message promising details about "Ben Hubbard and the story of the Saudi Royal Family."
- The SMS contained a hyperlink to a website used by a Pegasus operator that we call KINGDOM. We have linked KINGDOM to Saudi Arabia. In 2018, KINGDOM also targeted Saudi dissidents including Omar Abdulaziz, Ghanem al-Masarir ¹, and Yahya Assiri, as well as a staff member at Amnesty International.
- Hubbard is among a growing group of journalists targeted with Pegasus spyware. As part of our continued investigation into threats against journalists, Citizen Lab also identified evidence suggesting a Pegasus operator may have been infecting targets while impersonating *the Washington Post* in the weeks leading up to and after Khashoggi's killing in 2018. There is no overlap between this activity and reported events surrounding the mobile phone of Jeff Bezos.

The Great iPwn

Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit

By Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert

December 20, 2020

[Arabic translation](#)

Summary & Key Findings

- In July and August 2020, government operatives used [NSO Group](#)'s Pegasus spyware to hack 36 personal phones belonging to journalists, producers, anchors, and executives at *Al Jazeera*. The personal phone of a journalist at London-based *Al Araby TV* was also hacked.
- The phones were compromised using an exploit chain that we call **KISMET**, which appears to involve an invisible zero-click exploit in iMessage. In July 2020, KISMET was a zero-day against at least iOS 13.5.1 and could hack Apple's then-latest iPhone 11.
- Based on logs from compromised phones, we believe that NSO Group customers also successfully deployed KISMET or a related zero-click, zero-day exploit between October and December 2019.
- The journalists were hacked by four Pegasus operators, including one operator **MONARCHY** that we attribute to Saudi Arabia, and one operator **SNEAKY KESTREL** that