Planning for the unthinkable

WARNING: This presentation references child sexual abuse material (CSAM)

But first, a quick mental break


gifak.net

Who’s in control?

We the People of the United

insure domestic Tranquility, provide for the common defence, promote the

and our Posterity, do ordain and establish this Constitution for the United

Article. I.

Section. 1. All legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives.

Section. 2. The House of Representatives shall be composed of Members chosen every second Year by the People of the several States, and the Electors in each State shall have the Qualifications requisite for Electors of the most numerous Branch of the State Legislature.

No Person shall be a Representative who shall not have attained to the Age of twenty five Years, and been seven Years a Citizen of the United States, and who shall not, when elected, be an Inhabitant of that State in which he shall be chosen.

Representatives and direct Taxes shall be apportioned among the several States which may be included within this Union, according to their respective Numbers, which shall be determined by adding to the whole Number of free Persons, including those bound to Service for a Term of Years, and excluding Indians not taxed, three fifths of all other Persons. The actual Enumeration shall be made within three Years after the first Meeting of the Congress of the United States, and within every subsequent Term of ten Years, in such Manner as they shall by Law direct. The Number of Representatives shall not exceed one for every thirty Thousand, but each State shall have at least one Representative; and until such Enumeration shall be made, the State of New Hampshire shall be entitled to chuse three, Massachusetts eight, Rhode Island and Providence Plantations one, Connecticut five, New York six, New Jersey four, Pennsylvania eight, Delaware one, Maryland six, Virginia ten, North Carolina five, South Carolina five, and Georgia three.

When vacancies happen in the Representation from any State, the Executive Authority thereof shall issue Writs of Election to fill such Vacancies.

The House of Representatives shall chuse their Speaker and other Officers; and shall have the sole Power of Impeachment.

Section. 3. The Senate of the United States shall be composed of two Senators from each State, chosen by the Legislature thereof for six Years; and each Senator shall have one Vote.

Immediately after they shall be assembled in Consequence of the first Election, they shall be divided as equally as may be into three Classes. The Seats of the Senators of the first Class shall be vacated at the Expiration of the second Year, of the second Class at the Expiration of the fourth Year, and of the third Class at the Expiration of the sixth Year, so that one third may be chosen every second Year; and if Vacancies happen by Resignation, or otherwise, during the Recess of the Legislature of any State, the Executive thereof may make temporary Appointments until the next Meeting of the Legislature, which shall then fill such Vacancies.

No Person shall be a Senator who shall not have attained to the Age of thirty Years, and been nine Years a Citizen of the United States, and who shall not, when elected, be an Inhabitant of that State for which he shall be chosen.

The Vice President of the United States shall be President of the Senate, but shall have no Vote, unless they be equally divided.

The Senate shall chuse their other Officers, and also a President pro tempore, in the Absence of the Vice President, or when he shall exercise the Office of

Article 2, section 1

“In Case of the Removal of the President from Office, or of his Death, Resignation, or Inability to discharge the Powers and Duties of the said Office, the Same shall devolve on the Vice President, and the Congress may by Law provide for the Case of Removal, Death, Resignation or Inability, both of the President and Vice President, declaring what Officer shall then act as President, and such Officer shall act accordingly, until the Disability be removed, or a President shall be elected.”

Amendment XXV

“Whenever the Vice President and a majority of either the principal officers of the executive departments or of such other body as Congress may by law provide, transmit to the President pro tempore of the Senate and the Speaker of the House of Representatives their written declaration that the President is unable to discharge the powers and duties of his office, the Vice President shall immediately assume the powers and duties of the office as Acting President.”

Constitutionally, gentlemen, you have the President, the Vice President and the Secretary of State, in that order, and should the President decide he wants to transfer the helm to the Vice President, he will do so. As for now, I'm in control here, in the White House, pending the return of the Vice President and in close touch with him. If something came up, I would check with him, of course.

- Alexander Haig -

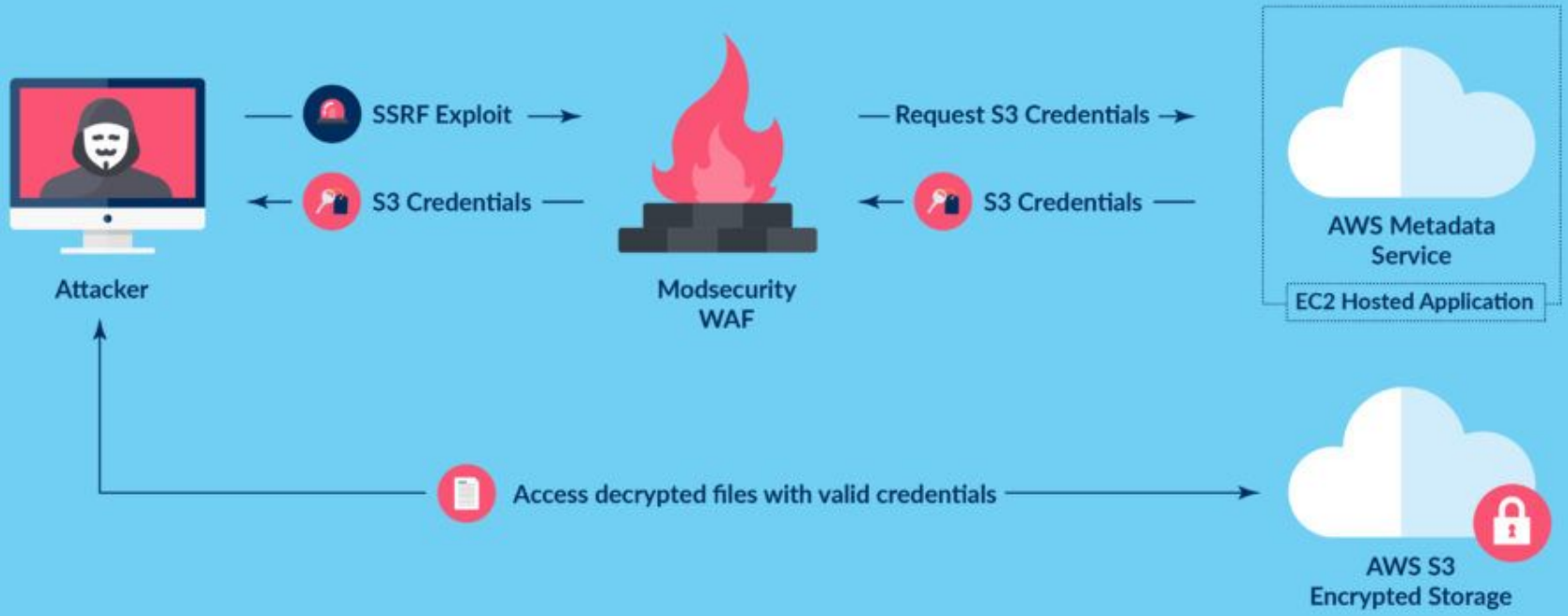
How does that apply to cybersecurity?


Capital One Bank

July 2019 Data Breach

- CapitalOne was one of the largest AWS customers
- This included leveraging several AWS native solutions, such as the web application firewall (WAF)
- The WAF was configured using a version of ModSecurity
- CapitalOne’s use of ModSecurity was misconfigured
- As a result, the attacker was able to request arbitrary URLs inside the CapitalOne AWS space

How the Attacker Got in



Timeline

- CapitalOne Notified by the FBI on July 17th, 2019
- Immediately setup a warroom in the SOC
- Key personnel are read into the incident, and dedicated to working on the problem
- Very quickly identified the problem and had identified the attacker, who the FBI arrested
- July 29th, 2019 CapitalOne sent out a public announcement of the breach, and began customer remediation efforts
- This public announcement is later amended to remove incorrect statements about what data was stolen

Additional Context

- CapitalOne had been rife with rumors about layoffs in the days and weeks leading up to the breach
- ALL senior cyber executives were in the warroom
- Legal locked down who could be read in after around 24 hours. Reading someone else in now required approval from the general counsel or the CEO

The response from team members NOT read into the incident boiled down to two basic responses


STOP
ALL WAY

Does your IR plan include who is tasked with keeping things running during an incident?

Once everyone knew about the incident, morale dropped even further as people realized how badly things had gone wrong

How does your IR plan address the employee morale aftermath of an incident?

The 2008 Internet

USENET

- AKA NetNews
- AKA NewsGroups
- Original Internet-wide chat groups
- First Internet Spam (January, 1994)
- By 2008, most USENET traffic was UUEncoded binaries: Combination of warez (cracked software), vids, & pr0n

The Incident

N.Y. attorney general forces ISPs to curb Usenet access

Time Warner Cable pulls the plug on all newsgroups after Andrew Cuomo's office finds child porn on 88 of them. Verizon Communications and Sprint plan to limit Usenet too.

Declan McCullagh
June 10, 2008 12:09 p.m. PT

4 min read

[**Update 6/12 11:40 a.m.** *Verizon has offered more details on what newsgroups will be removed. And here's background on whether or not Usenet is being blocked.*]

New York Attorney General Andrew Cuomo announced on Tuesday that Verizon Communications, Time Warner Cable, and Sprint would "shut down major sources of online child pornography."

What Cuomo didn't say is that his agreement with broadband providers means that they will broadly curb customers' access to Usenet--the venerable pre-Web home of some 100,000 discussion groups, only a handful of which contain illegal material.

Time Warner Cable said it will cease to offer customers access to any Usenet newsgroups, a decision that will affect customers nationwide. Sprint said it would no longer offer any of the tens of thousands of alt.* Usenet newsgroups. Verizon's plan is to eliminate some "fairly broad newsgroup areas."

The Outcome

PAUL ADAMS JUN 11, 2008 8:26 AM

Verizon, Time Warner Cable, and Sprint to Block Usenet

New York's Attorney General has just launched a blacklist-based initiative to quell undesirable Internet content. Child pornography is the target, although like all blacklists there will be a large number of blocked innocents and civilian casualties. An undercover investigation by the Attorney General's office uncovered a major source of online child pornography known as "Newsgroups," [...]

18 U.S. Code § 2258A

---

18 U.S. Code § 2258A requires certain service providers to report child sexual abuse material (CSAM) to the National Center for Missing and Exploited Children's (NCMEC) CyberTipline:

Reporting requirements:
Providers must report CSAM as soon as they become aware of it, but no later than 60 days after that. They must also report "apparent" and "imminent" violations of CSAM laws.

Penalties:
Providers who knowingly and willfully fail to report CSAM may be fined:

- Up to $850,000 for providers with more than 100 million monthly active users
- Up to $600,000 for providers with less than 100 million monthly active users

18 U.S. Code § 2258A - definitions

———

the term “provider” means an electronic communication service provider or remote computing service;

“electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications;

“electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include— (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

the term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system;

Does your IR plan cover how to respond if your company is accused of violating the law?

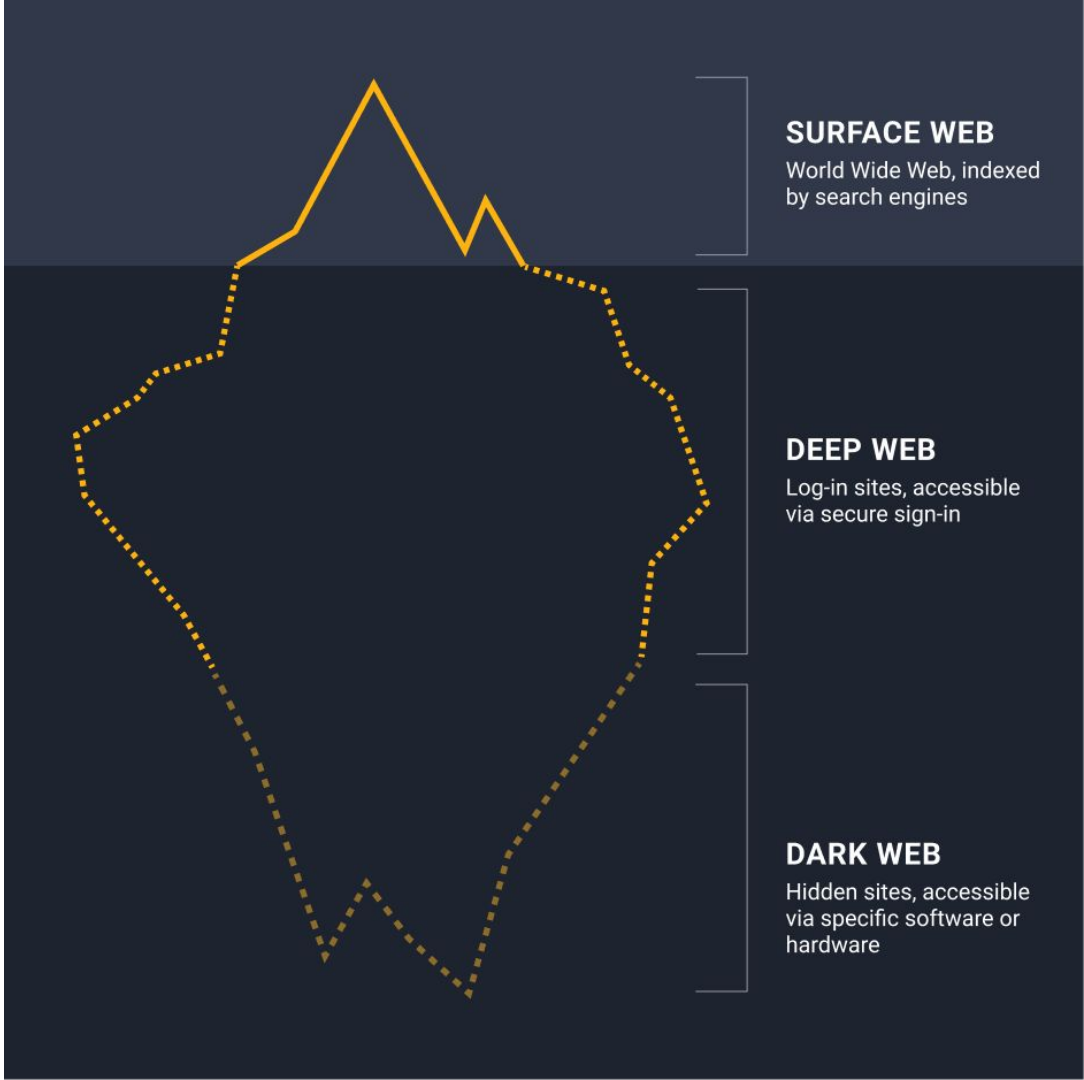
The Dark Web


DARK WEB INVESTIGATIONS:
UNCOVERING
THE HIDDEN
WEB

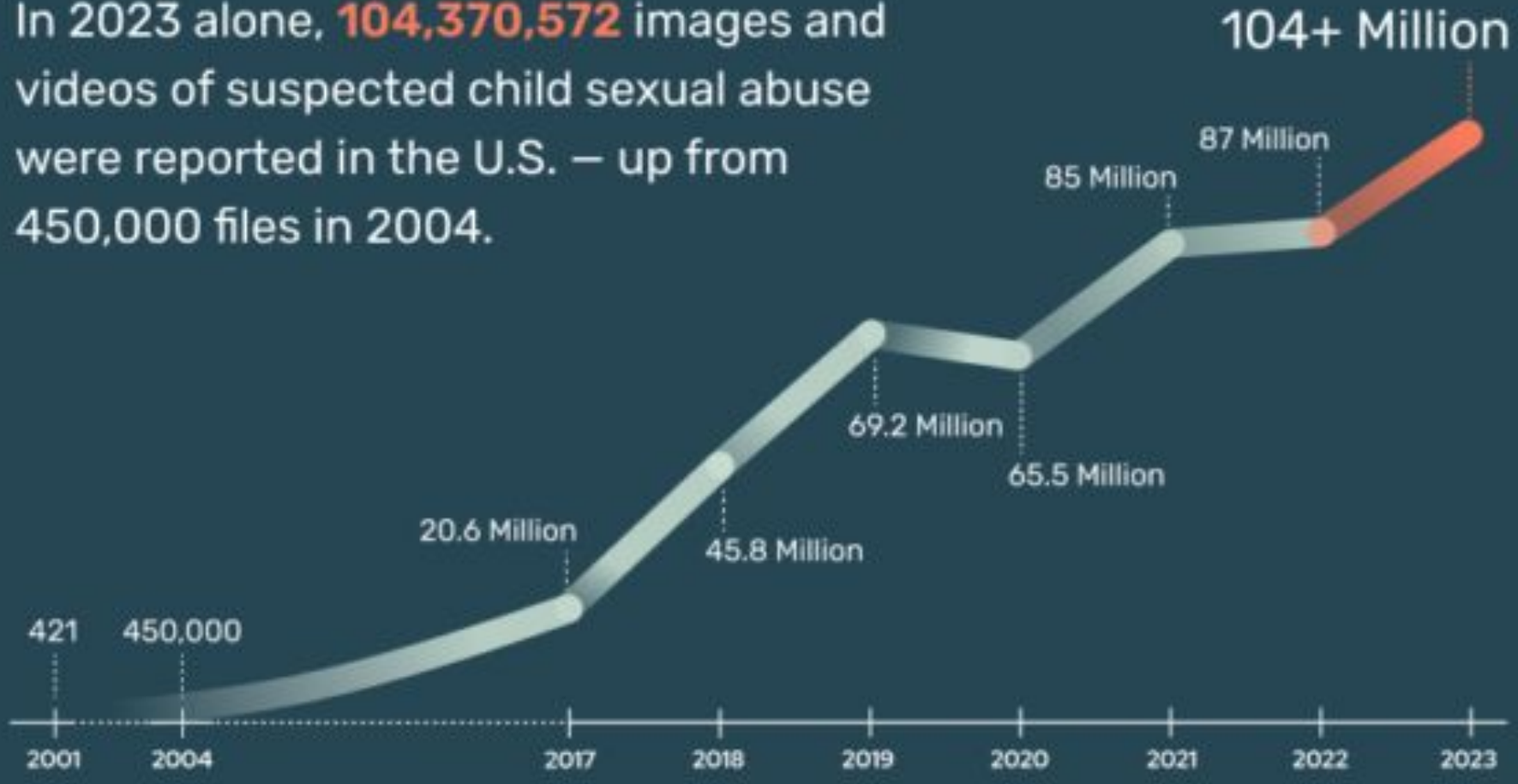
Definitions

For the purposes of this section, we define the “Dark Web” as something that:

- Requires special software such as TOR to access
- Not indexed by any search engine



In 2023 alone, **104,370,572** images and videos of suspected child sexual abuse were reported in the U.S. — up from 450,000 files in 2004.



Most CSAM users operate in a circle of trust model. They distribute content to people they think they know.

Reality & Open Questions

- The chances of someone stumbling across this material by accident are VERY low. But not zero
- Possession of this material is a crime. Sharing it with others is also likely a crime
- The only researchers who are legally allowed to investigate this material are either law enforcement or work for NCMEC / ICMEC / IWF / etc
- Is sharing the URL for such content illegal? I do not know, and I really don’t want to find out

What is your IR response if you find illegal content on a corporate device?

Do you have a plan to support employees who are potentially exposed to this content?

Being Punched in the Face

No plan survives contact with the enemy?

1871 Helmuth von Moltke wrote: *“Kein Operationsplan reicht mit einiger Sicherheit über das erste Zusammentreffen mit der feindlichen Hauptmacht hinaus.”*

Translation: “No plan of operations extends with any certainty beyond the first encounter with the main enemy forces.”


Everyone has a plan until they get punched in the face.
— Mike Tyson

How does your IR plan address who is able to make decisions?

Has your IR plan been approved at the most senior level?

Chris Roosenraad