SECURITY AND RANSOMWARE UPDATE MARCH 2022

RICHARD P. JEFFRIES
Nebraska HFMA Spring Meeting

CLINE WILLIAMS

1

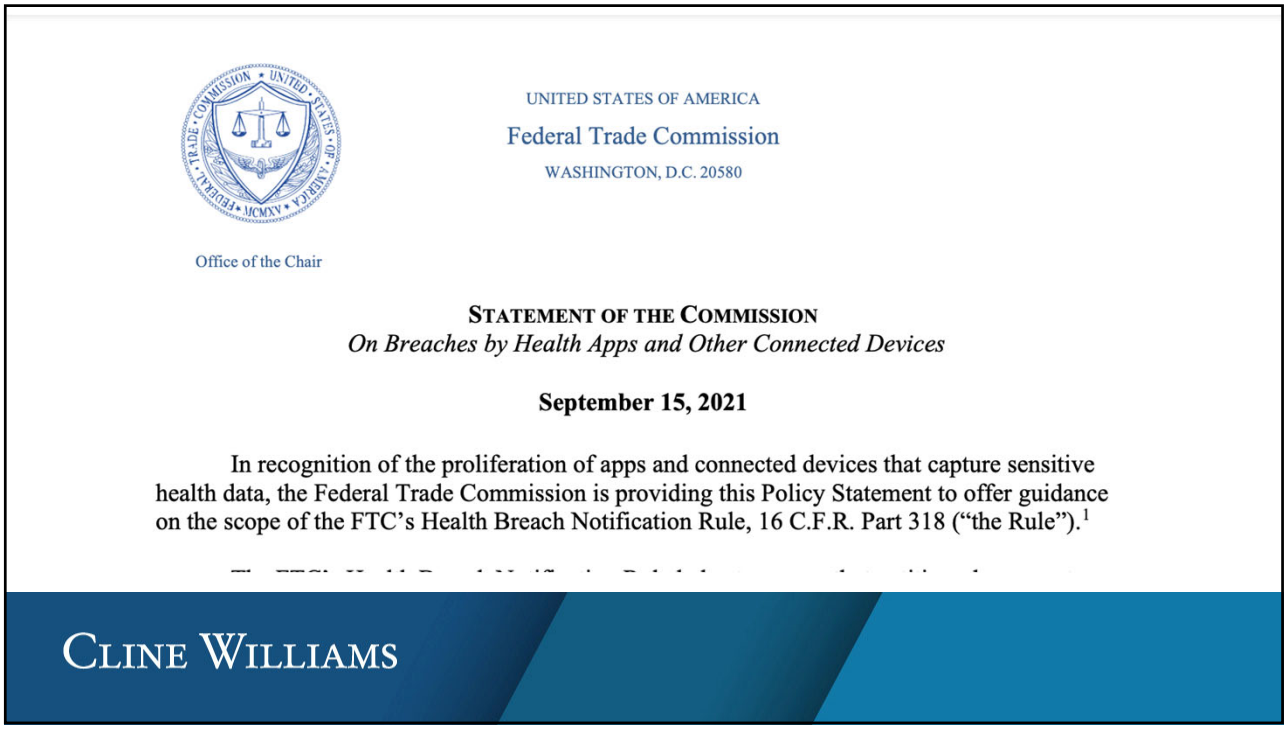
September 30, 2021

CLINE WILLIAMS

2


HEALTHCARE INFO SECURITY
Topics
News
Training
Resources
Events
Jobs
TRENDING: LIVE Webinar: 3/22 | Ransomware Recovery Essentials: Secrets To Reducing Cyber Risk
Governance & Risk Management , Incident & Breach Response , Legislation & Litigation
Banner Health Breach Lawsuit Settled
Plaintiffs' Attorney Says Settlement Totals 'Tens of Millions of Dollars'
Marianne Kolbasuk McGee (HealthInfoSec) • December 9, 2019
CLINE WILLIAMS

3


UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580
Office of the Chair
STATEMENT OF THE COMMISSION
On Breaches by Health Apps and Other Connected Devices
September 15, 2021
In recognition of the proliferation of apps and connected devices that capture sensitive health data, the Federal Trade Commission is providing this Policy Statement to offer guidance on the scope of the FTC's Health Breach Notification Rule, 16 C.F.R. Part 318 ("the Rule").[1]
CLINE WILLIAMS

4

Top Ransomware Groups Impacting Global HPH Sector

- As of May 25, 2021, HC3 tracked 82 HPH sector ransomware incidents globally (including the United States) for the 2021 calendar year.
  - Does not include unknowns where there was an unspecified cyber incident, or where not enough data was available. (8 instances where an unknown variant was tracked.)
  - Avaddon and Conti were the most frequently observed ransomware-as-a-service (RaaS) groups impacting the healthcare sector globally so far this year. The Revil/Sodinokibi, Mespinoza/Pysa, and Babyk variants followed suit, as shown below:

Top 5 Ransomware Actors Impacting Global HPH Sector 2021

Place	RaaS Name	Number of Incidents
1	Avaddon RaaS Operator(s)	16
2	Conti RaaS Operator(s)	16
3	REvil/Sodinokibi RaaS Operator(s)	7
4	Mespinoza/Pysa RaaS Operator(s)	6
5	Babyk RaaS Operator(s)	5

CLINE WILLIAMS

5

TRENDS IN RANSOMWARE - 2021

- More attacks
- Attacks more effective
- Criminals highly organized
- Level of evil more impressive than ever
- Ransom not guaranteed
- Insurance is more expensive and limits lower

CLINE WILLIAMS

6

2022: AN OPPORTUNITY TO GET AHEAD

- Baddest guys shut down
- State-sponsored activity distracted?
- BUT US-Russia cooperation off the table?
- *Maybe* a few months of quiet
- Major FOSS vulnerability exposed
- The cloud: More eggs, fewer baskets
- The pandemic tech boom: are we more vulnerable?

CLINE WILLIAMS

7

threatpost Podcasts / Malware / Vulnerabilities / InfoSec Insiders / Webinars

Researchers: Booming Cyber-Underground Market for Initial-Access Brokers 5

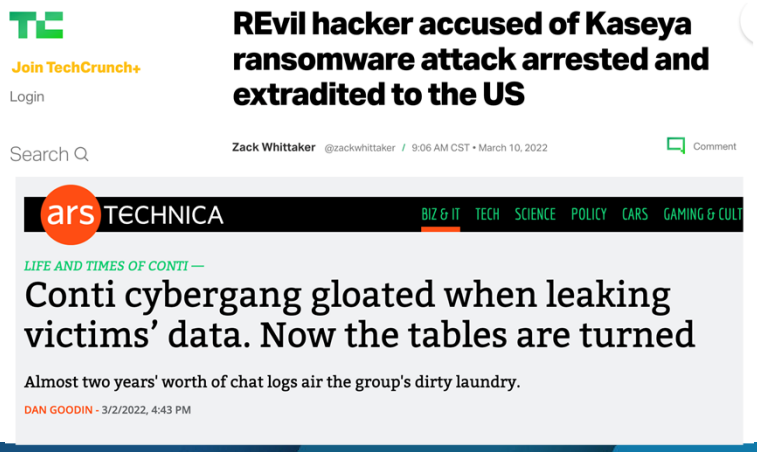
Avaddon Ransomware Gang Evaporates Amid Global Crackdowns

Avaddon, a prolific ransomware-as-a-service (RaaS) provider, released its decryption keys to BleepingComputer — 2,934 in total — with each key belonging to an individual victim. Law enforcement said the average ransom demanded by the group was about $40,000, meaning they quit and just walked away from millions.

CLINE WILLIAMS

8

BAD GUYS TAKE A FALL



TC

Join TechCrunch+

Login

Search

REvil hacker accused of Kaseya ransomware attack arrested and extradited to the US

Zack Whittaker @zackwhittaker / 9:06 AM CST • March 10, 2022

Comment

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULT

LIFE AND TIMES OF CONTI —

Conti cybergang gloated when leaking victims' data. Now the tables are turned

Almost two years' worth of chat logs air the group's dirty laundry.

DAN GOODIN - 3/2/2022, 4:43 PM

CLINE WILLIAMS

9

A NEW TACTIC: PUBLICATION OF DATA

lstaff.com / atworksprofessional / atworks.com

We downloaded whole file server, there are:
-thousands of CVs,
-employee personal information(BIO, phones, DOB,SSN),
-project information,
-(cyber)insurance information,
-finance reports and so on.

1st pack (2K CVS, 700 SSN, 800 DL) Download link: https://privatlab.org/s/v/4jjxzReyRgCj6lrn5yOd

Samles attached.

BCS

BCS Insurance Company
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181

(A stock insurance company, herein the "Company")

Policy No. RPS-P-50091906M

Cyber and Privacy Liability Insurance Policy

CLINE WILLIAMS

10

BARRIERS TO ENTRY ARE SIGNIFICANT

THE WALL STREET JOURNAL.

Subscribe | Sign

U.S. Politics Economy Business **Tech** Markets Opinion Books & Arts Real Estate Life & Work WSJ. Magazine Sports

◆ WSJ NEWS EXCLUSIVE | TECH

Ransomware Gang Masquerades as Real Company to Recruit Tech Talent

Group linked to Colonial Pipeline hack has made offers to potential employees in new ransomware expansion push, researchers say

CLINE WILLIAMS

11

THE THREAT PERSISTS

Cartel Overview

Four ransomware gangs currently exist within the Cartel: Twisted Spider, Viking Spider, Wizard Spider, and the Lockbit Gang as seen in *Figure 1* below.

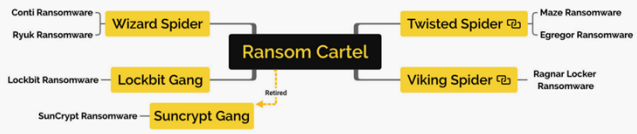


Figure 1: Cartel breakdown

Source: Analyst1.com

CLINE WILLIAMS

12

log4j: The RCE Flavor of the Month

CLINE WILLIAMS

13

KASEYA: NIGHTMARE IN THE CLOUD

- Managed network services company
- Hit by REvil – a ransomware gang
- Infected management software sold to small-medium companies
- Widespread downtime of over 1000 companies
- Chilling – hit a vendor, own its customers

CLINE WILLIAMS

14

HOW KASEYA HAPPENED

- SQL Injection Attack
- SQL is a kind of code language for searching databases
- On a poorly configured system, malicious commands can be injected into the code
- If you can run arbitrary code, you own the system
- The same things that make a system powerful also make it dangerous
- Employees say they warned Kaseya management

CLINE WILLIAMS

15

WHY IT WORKS

CLINE WILLIAMS

16

REASON 1: UNMARKED BILLS

- Cryptocurrency
  - Ransom universally in cryptocurrency
  - Untraceable
  - Heavy encryption
  - Anonymous
  - Valuable
  - Seeing it in other scams
  - NOT GOING AWAY

CLINE WILLIAMS

17

REASON 2: THERE'S NO SUCH THING AS THE CLOUD

- Just other people's computers
  - Rent by the minute
- Can assemble massive computing power for little capital investment
- Capable of brute force attacks
- NOT GOING AWAY

CLINE WILLIAMS

18

Reason 3: COMPLEXITY BEGETS VULNERABILITY

- Windows 10: > 50 million lines of code
- OS X > 85 million lines of code
- Free and open source: Billions of lines of code
- NOT GETTING SIMPLER

CLINE WILLIAMS

19

REASON 4: DATA HAS VALUE

- Positive value – Data can be used to:
  - obtain goods and services
  - open bank accounts
  - borrow money
- Negative value – Data can be used as leverage to extort its owner
  - to get it back
  - to keep it from being disclosed
- NOT BECOMING LESS VALUABLE

CLINE WILLIAMS

20

WHAT YOU CAN DO: THE PILLARS OF SECURITY

CLINE WILLIAMS

21

Pillar 1: Environment Mastery

- Do you know <u>every</u> piece of technology your organization uses?
  - Quarantine Gap?
  - Patch management?
  - EOL?
- Keep software up to date
- Know if anything reaches EOL or is no longer supported

CLINE WILLIAMS

22

NIST FRAMEWORK – IDENTIFY FIRST

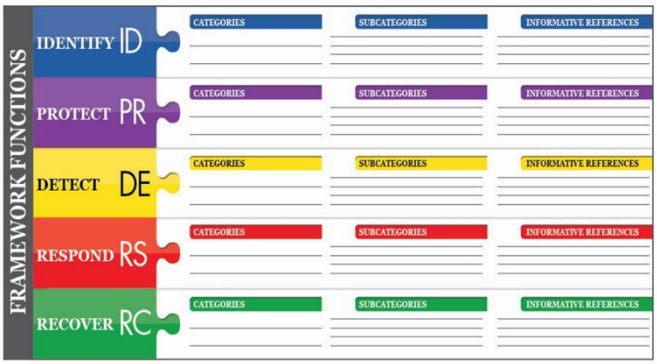


Figure 1: Framework Core Structure

CLINE WILLIAMS

23

HIPAA SECURITY RULE

§ 164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with § 164.306:

(1)

(i) ***Standard: Security management process.*** Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) ***Implementation specifications:***

(A) ***Risk analysis (Required).*** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

CLINE WILLIAMS

24

WHAT IS CAUSING THE VULNERABILITY LAG?

Organizations are unable to keep pace.
Only 61% believe that their organization's security measures have fully kept up since the implementation of COVID-led digital transformation initiatives over the past 18 months

Technologies had to be introduced unexpectedly.
Since COVID-led digital transformation initiatives began, 80% of respondents' organizations newly implemented or expanded their deployment of cloud infrastructure beyond their original plans

There is a lack of clarity around what technology has been introduced.
Only 58% of surveyed senior IT decision makers believe that they can confidently and accurately state the exact number of cloud services that their organization is currently using

There is a lack of clarity on what needs to be protected.
On average, respondents' organizations' data is made up of 35% dark data, 50% redundant, obsolete, or trivial (ROT) data, and only 16% business critical data

Source: veritas.com

CLINE WILLIAMS

25

Pillar 2: Continuous User Education

- Ordinary users represent best target of opportunity
- Constantly teach them how the threat looks and works
- Build a culture of trust and reporting
- Make your people your best infosec allies

CLINE WILLIAMS

26

Pillar 3: Credential Management

- Discipline
  - No sharing
  - Decent strength
  - Instant deactivation
  - Resets where necessary
- Multifactor
- Keep privileges to a minimum
- Segment networks and data

CLINE WILLIAMS

27

Two Principles of Data Segmentation

- Don't confuse executive authority with data privileges
  - Janitors have keys
- Different data = different treatment
  - PHI
  - Cake in the break room

CLINE WILLIAMS

28

Pillar 4: Vendor Diligence

- Compromised SaaS vendor = disaster
  - As vulnerable as their worst customer?
- Monitor vendors in potential financial difficulty
- Understand what they do for security
- Require proof of pen test for critical systems

CLINE WILLIAMS

29

Pillar 5: Leadership Competence

- How good is your CIO/CISO?
- Do you trust them absolutely?
- Exercise: Ask them to explain backup/DR regime like you're five
- Do you have a DR plan?
  - Have you simulated it?

CLINE WILLIAMS

30

Pillar 6: Trust but Verify

- Great CISO/CIO will insist on pen test and audit
- Tech departments should have the humility to not know what they don't know
- Testing vulnerability is a sign of strength, not weakness
- Act on everything identified in audits
- Improve continuously

CLINE WILLIAMS

31

Pillar 7: Plan for the Inevitable

- The Red Binder
  - A plan that does not require an operative system to access
- Comprehensive checklist
  - NIST guide to incident response as framework
  - Phone numbers
    - IT consultants
    - PR
    - Legal
    - Law Enforcement
    - Insurance

CLINE WILLIAMS

32

Pillar 8: Hedge the Financial Risk

- Insurance products
  - Cyber crime
  - Cyber extortion
  - Business interruption
- Applying is an excellent inventory
- Value the business interruption

CLINE WILLIAMS

33

Harvard Business Review

Cybersecurity And Digital Privacy | The Cyber Insurance Market Needs Mo

Cybersecurity And Digital Privacy

The Cyber Insurance Market Needs More Money

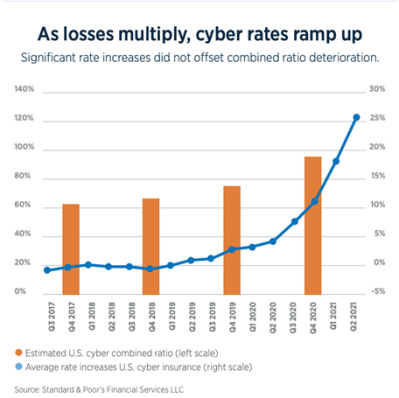
by Tom Johansmeyer

March 10, 2022

CLINE WILLIAMS

34

INSURANCE CONDITIONS DETERIORATING



- Premiums going up
- Limits going down
- Greater underwriting scrutiny
- Will ransom cover become unavailable?
- Beware of sublimits
  - Reduced limits for SaaS

CLINE WILLIAMS

35

Pillar 9: Backups

- A recent backup is a ransomware antidote
- If you haven't restored it, it isn't a backup
- Different Locations
- Different Media
- "Immutability"

CLINE WILLIAMS

36

XIGENT

COMPANY RESULT DRIVEN IT IT SERVICES

6 Ways Cybercriminals Exploit Your Self-Managed Immutable Backup

CLINE WILLIAMS

37

PARTING THOUGHTS

- Maybe you've got a short breather
  - Pandemic
  - Big gangs out or occupied
- Insurance is becoming more limited
- Increased attention to security is best available strategy
- Remote work may have increased your risk

CLINE WILLIAMS

38

QUESTIONS?

Richard P. Jeffries
rickjeffries@clinewilliams.com
@JeffriesInfoSec

39