Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

August 5, 2020

August ISOAG AGENDA

- **Mike Watson, Opening & Welcome Remarks**
- **Bob Austin, VSCP Welcoming Remarks**
- **Elliott Casey, Commonwealth's Attorneys' Services Council**
- **Christopher Cope, U.S. Department of Justice**
- **Robert Reese, Virginia State Police**

Welcoming Remarks
Bob Austin, VSCP
No slides

THERE IS NO WORLD-WIDE WEB

HOW EXTERNAL FORCES WILL CHANGE U.S. CYBER LAW IN THE NEXT DECADE

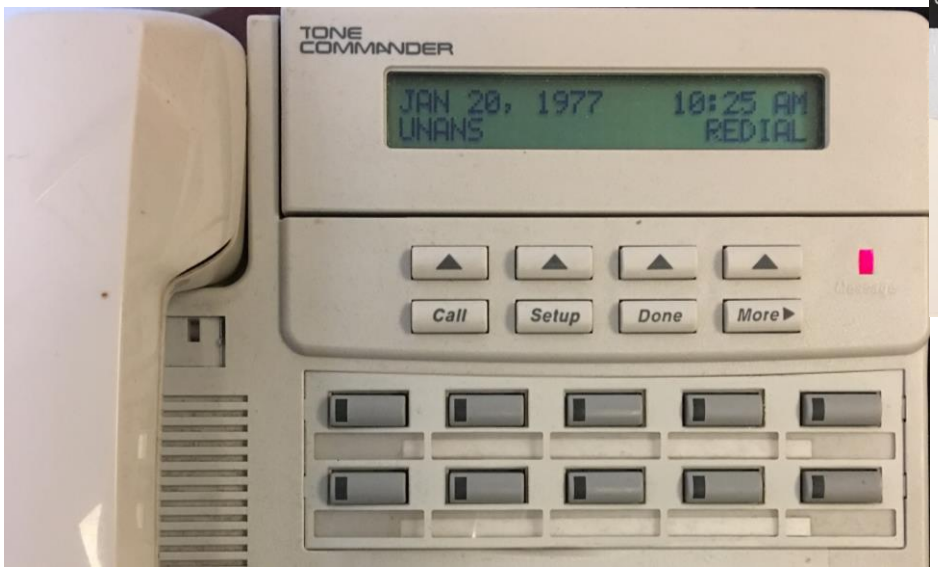
COMMONWEALTH'S ATTORNEYS' SERVICES COUNCIL

Training Virginia's Prosecutors for the 21st Century

DISCLAIMER:
I DO NOT SPEAK FOR ANYONE.

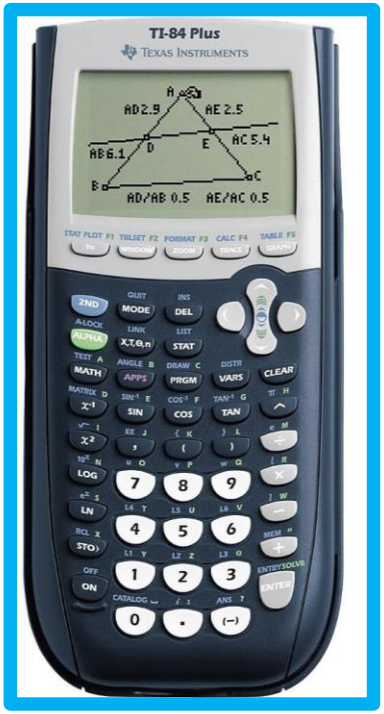
- I am a Virginia State Employee.
- I do not speak for the Commonwealth of Virginia.
- I do not speak for the Executive Branch.
- I do not speak for my agency.
- I have no opinions, nor if I had opinions, would I be authorized to confirm or deny their existence.

WHERE WERE WE?



WHERE ARE WE?

- Same phones, same price.
- Same TI: 24 kilobytes of RAM, a 96×64 pixel screen, and a power system that still relies on 4 AAA batteries,
- While the cost of its components has dramatically decreased, its price ($150 MSRP) has not.
- Why no change?
- They are safe, schools didn't want to allow smartphones, and no one wanted to change.



WHERE WERE WE?

- 1986: Congress enacts the Electronic Communications Privacy Act (ECPA), which governs how and when the law permits courts and legal authorities to issue legal demands for electronic records.
- 1988: The New York Times discusses "The Internet" for the first time.
- 1990: The first "web server" and web browser are launched by MIT.
- 1992: Congress enacts "must-carry" rules for cable television broadcasters.
- 1996: Congress enacts Communications Decency Act (CDA), which includes immunity from liability for providers and users of an "interactive computer service" who publish information provided by third-party users. (§230)

WHERE ARE WE?

- We are stuck with our 30-year old mentality

1. "Territoriality:" Focus on U.S. as running the Internet.
2. "Terrestriality:" Viewing devices as physical objects.
3. "Telecomality:" Focus on Communications Law from the 1970's and telecom from the 1990's.

TERRITORIALITY

THERE IS NO WORLD-WIDE WEB

"THE 26 WORDS THAT CREATED THE INTERNET"

- Section 230 of the Communications Decency Act (CDA) of 1996, 47 U.S.C. §230, provides immunity from liability for providers and users of an "interactive computer service" who publish information provided by third-party users:
  - "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."
- Also provides "Good Samaritan" protection from civil liability for operators of interactive computer services in the removal or moderation of third-party material they deem obscene or offensive, even of constitutionally protected speech, as long as it is done in good faith.

SO, SECTION 230 PROTECTS FREE SPEECH, RIGHT?

- *Jian Zhang v. Baidu.com Inc., 10 F.Supp.3d 433 (S.D. N.Y. 2014).*
- Plaintiffs alleged that Baidu conspired to prevent "pro-democracy political speech" from appearing in its search-engine results here in the United States.
- Court: "To allow such a suit to proceed would plainly "violate the fundamental rule of protection under the First Amendment, that a speaker has the autonomy to choose the content of his own message."
- The law protects *Baidu*'s free speech, not the speaker's.

CHINA & "THE GREAT FIREWALL"

- Techniques deployed by the Chinese government to maintain control of the Great Firewall include:
  - Selectively prevents content from being accessed, blocking IP and filtering URLs.
  - Modifies search results for terms, (e.g. Ai Weiwei's arrest) using liar DNS servers and DNS hijackers returning incorrect IP addresses.
  - Petitions global conglomerates to remove content (e.g. requiring Apple to remove the Quartz business news publication's app from its Chinese App Store after reporting on the 2019–20 Hong Kong protests.)
  - Packet forging and TCP reset attacks.
  - Man-in-the-middle attacks with TLS.

"RIGHT TO BE FORGOTTEN" G.D.P.R. ARTICLE 17

- "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:"
- "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data."

PAUL TERMANN

- In Germany in 1982, an ex-soldier & a member of the crew of a sailing ship named Apollonia, shot and killed two people and severely injured another when the ship was in the Caribbean.
- The man, then in his early 40s, was released from prison in 2002.
- The case became famous enough to be turned into a book and a TV documentary aired by public broadcaster ARD in 2004.
- In 1999, news magazine Der Spiegel put three print reports from 1982 and 1983, in which the man's full name appeared, in its freely available online archive.
- German Court: While it was allowable for search engines to provide news reports on current crimes, the justifiable public interest in reports that made perpetrators identifiable decreased with time.

CAN'T THEY JUST LIMIT THE RESULTS FOR EUROPE?

- Google had complied with the erasure requirement by partially delisting search results on its domains, specifically targeting its European sites, such as France's google.fr and Germany's google.de.
- In 2016, France's National Commission on Informatics and Liberty (CNIL) fined Google 100,000 euros ($111,790) for not delisting web search results across all of its domains under the "right to be forgotten" ruling.

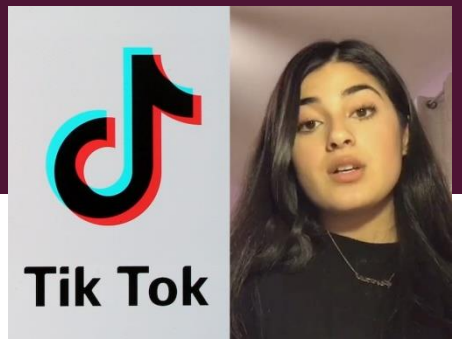
BUT THAT CAN'T HAPPEN HERE… RIGHT?!

- Google Inc. v. Equustek Solutions Inc., 2017 SCC 34
- Canadian enforces an IP injunction against Google worldwide
- "The Internet has no borders — its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates — globally. If the injunction were restricted to Canada alone or to google.ca, the remedy would be deprived of its intended ability to prevent irreparable harm, since purchasers outside Canada could easily continue purchasing from D's websites, and Canadian purchasers could find D's websites even if those websites were de-indexed on google.ca."

WE ARE NOT ALONE.

- TikTok has 10% of the earth's population.
- Tik Tok is owned by ByteDance, a $100 billion Beijing-based IT company.
  - ByteDance has an internal committee of the Chinese Communist Party as well as strategic partnerships with Chinese Communist Party-supported ventures in Beijing and Shanghai.
  - In January 2019, the Chinese government said that it would start to hold app developers like ByteDance responsible for user content shared via apps and listed 100 types of content that the Chinese government would censor.

WHAT ABOUT U.S. USERS? FEROZA AZIZ



- Posted a video discussing the mass detentions of minority Muslims in northwest China.
- The 40-second clip amassed more than 498,000 likes and was viewed 1.5 million times.
- In another video, she addressed a slur that she said she and other Muslims heard regularly, that they would marry Osama Bin Laden.
- In response, TikTok suspended her account after she posted the clip.
- After an outcry, TikTok had to apologize and restore her account.

TAKEDOWN AS DEFAULT

- In the EU, providers now have as little as one hour to takedown terrorist, dangerous, or hateful material, or face massive fines.
- Each EU member state can have its own definition of what needs to be taken down.
- The U.S. has sometimes tried to fight excessive censorship, but the public has also demanded takedown of various material.

DATA PROTECTION COMMISSIONER V. FACEBOOK IRELAND AND MAXIMILLIAN SCHREMS

- On July 16, the Court of Justice of the European Union (CJEU) invalidated a 2016 agreement that allows companies to transfer data while ensuring compliance with privacy laws on either side of the Atlantic.
- Court ruled that companies operating in Europe cannot move data to or through any country that fails to provide persons in Europe with "actionable rights" of challenge that are "essentially equivalent" to privacy rights enjoyed within the EU.
- Surprise! The U.S. does not qualify, nor does any other country except maybe Argentina.

THERE IS NO WORLD WIDE WEB

"The cosmopolitan ideal for the Internet—whether the product of naivete, utopian dreams, or strategic interest—is dead. States, being jealous of their sovereignty, and users, wanting to make the digital world their own, will inevitably resist the idea of a single, shared online experience. What is appropriate in New York may not be appropriate in Bangkok and vice versa."

- Andrew Keane Woods, *Litigating Data Sovereignty*, 128 Yale L.J. 328 (2018)

QUESTION:
WHO REGULATES?
WHY?

SIMPLE QUESTIONS THAT GET REALLY COMPLICATED FAST

TERRESTRIALITY

THERE IS NO SPOON.

”DATA MUST BE STORED IN VIRGINIA!!”

- Question: If you request a Search Warrant for bank records of an embezzler, where do you get the warrant? “Where” are you searching?
  - Do you have to find the server that has the data first?
- Question: What if the file is in a sharded format? (e.g. Google, Dropbox, etc.)
- Question: What if the provider has no idea ”where” the file is?

U.S. V. MICROSOFT, 2ND CIRCUIT 2016

- Microsoft objected to a search warrant, arguing that, to comply fully with the Warrant, it would need to access customer content that it stores and maintains In Ireland and to import that data into the United States.
- 2nd Circuit: "Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas. Three decades ago, international boundaries were not so routinely crossed as they are today, when service providers rely on worldwide networks of hardware to satisfy users' 21st–century demands for access and speed and their related, evolving expectations of privacy.
- The case never reached the U.S. Supreme Court.
- Instead, Congress passed the "Cloud Act" in response.

CLOUD ACT: SHIFT FROM "PRESENCE" TO "CONTROL"

- Any warrant issued must satisfy several requirements, including that:
  - The entity targeted must be under the personal jurisdiction of U.S. courts.
  - The evidence sought must be under the "possession, custody, or control" of the targeted entity.
  - The application of the warrant must not violate principles of international comity.

PROBLEM SOLVED!
EXCEPT…

- Under the GDPR, a "controller" or "processor" of data may only comply with a demand for data from a non- EU court if the demand is "based on an international agreement" between the two nations.
- We have no international agreements with any EU countries.
  - (We do have an agreement with the U.K.)
- If a company violates this directive, it may suffer economic penalties.
- GDPR penalties can be up to 4% of global revenue!

WE WANT TO GET DATA – WE JUST DON'T WANT OTHER PEOPLE TO GET IT!

- In 2016, Indian police demanded the account information of a Facebook user who allegedly posted material that was critical of a Hindu god.
- Facebook resisted.
- The police raided Facebook's offices in Mumbai.
- Police registered a case under Indian law for "promoting enmity between different groups on grounds of religion" and "deliberate and malicious acts intended to outrage religious feelings of any class by insulting religious beliefs"

IT'S EASY TO CONTROL A COMPANY IF "WE" OWN IT…

- In 2019, The Committee on Foreign Investment in the United States (CFIUS) forced Chinese gaming company Beijing Kunlun Tech Co Ltd to divest from the dating app Grindr.
- CFIUS cited national security concerns, since it was within the Chinese government's power to extract any information it wants.
- CFIUS feared that Grindr's inherently sensitive data could be used to blackmail U.S. government personnel or citizens.
- What about TikTok?
  - A pending Committee on Foreign Investment in the United States (CFIUS) investigation that could potentially force ByteDance to sell TikTok or cease operations in the U.S.

DATA SOVEREIGNTY: APPLE & ENCRYPTION

- In 2017, Apple, for example, announced it would build a Chinese datacenter in accordance with China's data localization law, making that data vulnerable to government authorities.
- Apple promised that there would be "no backdoors" and that Apple would retain control over the encryption keys which would be stored in the United States.
- However, less than a year later, it announced plans to move the keys to its Chinese iCloud accounts to Chinese territory.

YIKES!
EXCEPT… WE DON'T LIKE ENCRYPTION EITHER!

- Everyone attacked Zoom for lacking end-to-end encryption.
- Zoom pointed out, however, that child predators were using its service to contact and exploit children and they wanted to be able to stop that – which meant sometimes monitoring communications.
- If you end-to-end encrypt communications, that provides a shield for human rights organizations – and child rapists.
  - Example: Buster Hernandez, a.k.a. Brian Kil

MOHAMMED SAEED ALSHAMRANI

- Saudi Royal Air Force Lieutenant who, in 2019, killed three U.S. sailors and severely wounded eight other Americans at the Pensacola Naval Air Station.
- The FBI obtained a search warrant to examine his two iPhones.
- The phones were encrypted and Apple refused to assist the FBI.
- After 4 months and considerable expense, the FBI got into the phones and discovered his ties to Al Qaeda in the Arabian Peninsula (AQAP).

"LAWFUL ACCESS TO ENCRYPTED DATA ACT"

- In the case of a lawful search warrant, would require:
  - Assistance to law enforcement in "decrypting or decoding information on the electronic device or remotely stored electronic information that is authorized to be searched, or otherwise providing such information in an intelligible format, unless the independent actions of an unaffiliated entity make it technically impossible to do so; &
  - Technical support as necessary to ensure effective execution of the warrant for the electronic devices particularly described by the warrant.

ENCRYPTION – TWO ISSUES, WRAPPED IN ONE

Data At Rest

- The Device itself is encrypted
- However, government would have at least one "factor" in hand – the device itself.

Data in Motion

- The Data is held by the provider, but in an encrypted format.
- Government wants access – and the user may be on the run or unavailable (Like Buster Hernandez).

WE SEIZED AN IPHONE!!
SO… WHICH IS IT?

Is it Data At Rest?

- Can we get everything off of the device, standing alone, without connecting to the Internet?
- Do we need to connect it to the Internet or to a Network to get the data?
  - If so, where is the data? Where is the search?

Is it Data in Motion?

TELECOM-ALITY

OUR LAW IS OUTDATED

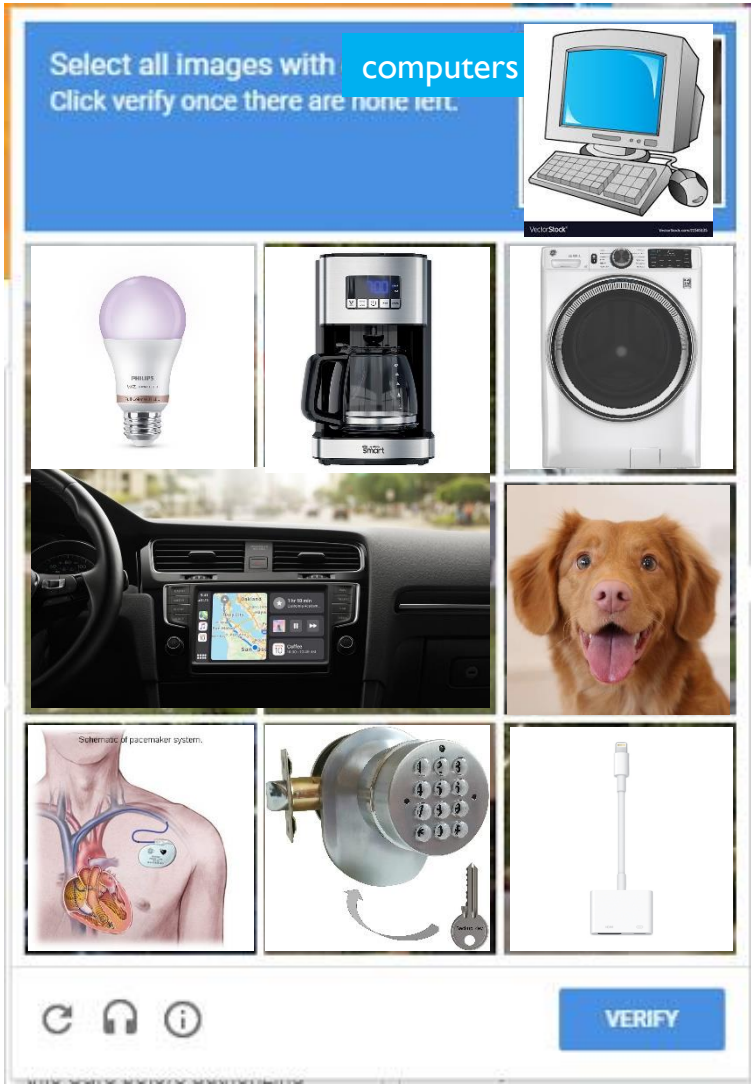
VA. CODE § 19.2-61, ET. SEQ

- Virginia's statutory scheme for governing law enforcement lawful access to electronic communications
- Under the code, an "Electronic communication service" means:
  - any service which provides to users thereof the ability to send or receive wire or electronic communications;
- Question: Who DOESN'T qualify nowadays?

VITA ACT

- § 2.2-2009: VITA shall provide "policies, standards, and guidelines shall include requirements that (i) any state employee or other authorized user of a state technology asset provide passwords or other means of authentication to use a technology asset and access a state-owned or state-operated computer network or database"
- § 2.2-2006: ""Technology asset" means hardware and communications equipment not classified as traditional mainframe-based items, including personal computers, mobile computers, and other ***devices capable of storing and manipulating electronic data***.

Identify anything that is a: "***device capable of storing and manipulating electronic data***.



SOLUTION #1: SHUT IT DOWN. FORBID ANYTHING FROM CONNECTING TO THE INTERNET

- Worked for him!
- Problem: Your users will bail and everyone but you will die in the apocalypse.
- You do not know how to make buffalo wings taste the way you like them.

TO ZOOM OR NOT TO ZOOM, THAT IS THE QUESTION

- May 2020: Germany orders not to use Zoom.
  - They do not like the lack of end-to-end encryption (i.e. that people can call in).
  - They do not like their traffic being routed out of Germany and back again.
- What alternative?
- Teams? Nope. Skype? Nope ….
- Oh! Maybe What'sApp?
  - Nope, that's owned by Facebook, and they don't trust Facebook.
- ….

© Andre M. Chang

24.05.2020, 14:39 Uhr

Bundesdatenschutzbeauftragter rät von Videochat-Dienst Zoom ab

Familien, Freundeskreise aber auch Firmen und Schulklassen setzen in der Coronakrise auf Videokonferenzen mit dem US-Dienst Zoom. Doch es gibt Bedenken. Der Bundesdatenschutzbeauftrage rät nun ausdrücklich von Zoom ab.

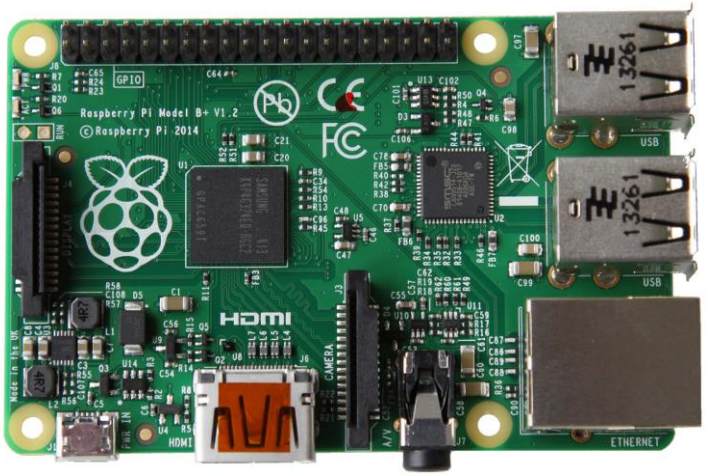
SOLUTION: BAN ZOOM
….AND THEN USE IT ANYWAY.

German Federal Commissioner for Data Protection

SOLUTION #2: FRIENDS-ONLY
BAN ANYTHING YOU DON'T ALREADY TRUST

- E.g. U.S. ban on all Huawei products
- Problem: This solution requires that you know your suppliers, and your suppliers' suppliers
- Problem: This solution requires you to have market power AND a viable alternative.
- Problem: This approach probably violates GATT and our WTO treaty obligations.
  - The WTO's Appellate Body has found that where products that are competitively "like" experience impaired market access, there can be a violation of the relevant anti-discrimination provisions.

SOLUTION #3: BUCKLE DOWN AND REGULATE IT ALL



- If it can manipulate data, then regulate it!
- Problem: That's <u>everything</u>.
- You will have to regulate an Apple Lightning-to-HDMI adapter, which has ARM chip inside and a mini-OS that translates the image.
- You will have to regulate refrigerators, cars, TVs, coffee makers, lightbulbs, etc. etc.

SOLUTION #4: PRODUCTS-LIABILITY

- Why don't children's clothes burst into flames anymore?
- Who is responsible? The consumer? The retailer? The wholesaler? The manufacturer?
- E.g.: In 2016, Dutch regulators sued Samsung over a lack of consistent updates to its Android-powered phones. The regulator contended that Samsung should be responsible for pushing updates two years after the sale of a phone.

SOLUTION #5: FEDERAL/INTERNATIONAL SAFETY REGULATION

- How do we protect our food supply?
- Under the 2011 Food Safety Modernization Act (FSMA), the FDA maintains a foreign inspection program to "ensure the U.S. food supply is safe by shifting the focus from responding to contamination to preventing it.
- Requires shifting IoT security from a consumer-level concern to a distributor responsibility

PROBLEMS:

- This approach will potentially cripple small retailers and small companies with compliance & liability costs.
- This approach is useless against judgment-proof companies.
- It means more lawyers ... and who wants that?

TAKEAWAYS:
OUR LAW IS GOING TO HAVE TO INNOVATE.

1. We have to stop thinking we can demand territoriality from providers.
2. We have to stop thinking we can stop beneficial foreign ownership/ties.
3. We have to stop thinking that our content rules are the only ones.

QUESTIONS?

Elliott Casey, Staff Attorney

Commonwealth's Attorneys' Services Council

William and Mary Law School, Room 220

613 South Henry Street, P.O.Box 3549

Williamsburg, Virginia 23187

757.585.4370

ejcasey@wm.edu

VIRGINIA FUSION CENTER (VFC)

Prevention is the Best Response: A Discussion on Preparation for Ransomware Attacks

VFC Cyber Intelligence Unit

DISCLAIMER:

- *This is FOR OFFICIAL USE ONLY information protected by Virginia Code Section 52-48, unless otherwise noted.* ***Further dissemination of this information outside of your organization is prohibited unless written approval is obtained from the VFC prior to dissemination.*** *Pursuant to Virginia Code Section 52-48(D), anyone violating distribution restrictions may be prosecuted and may be prohibited from receiving future reports. Please contact the Virginia Fusion Center at (804) 674-2196 if you have any questions or need additional information*

(U) Ransomware

(U) Ransomware is malicious software that blocks access to computer systems or files until money is paid.

- (U) Victim's computer is infected with malware.
- (U) Malware encrypts victim's data and/or systems, making them unreadable.
- (U) Actor demands payment to decrypt files or network.

FBI • CYBER

(U) The Dynamic Ransomware Ecosystem

- (U) 2016: Explosive growth in terms of:
  - New families, new variants, detections, ransom demands, etc.
- (U) 2017: Reported declines in large-scale ransomware campaigns; Two unprecedented global ransomware outbreaks; Emergence of more targeted ransomware families.
- (U) 2018: Continued emergence of small-scale targeted ransomware families pursuing higher ransoms; Continued decline in large-scale campaigns.
- (U//FOUO) Dynamic Ransomware Ecosystem
  - At the top: Increased sophistication, innovation, experimentation
  - At the bottom: Cheap imitators that fail to gain traction
- (U) What does all of this mean for the future of ransomware?

FBI • CYBER

(U) IC3 Statistics

- (U) FBI Internet Criminal Complaint Center (IC3)
  - 2016 = 2,673 (51% of complaints associated with business)
  - 2017 = 1,783 (65% of complaints associated with business)
  - 2018 = 1,041 (73% of complaints associated with business)
    - *as of 09/27/2018

- (U) Possible reasons for drop in attacks

FBI • CYBER

(U) WannaCry and NotPetya

- (U) 12 May 2017 – WannaCry ransomware infected hundreds of thousands of computers in 150 countries.
  - Attack ebbed when kill switch discovered.
  - The number of US victims was relatively low.

- (U) 27 June 2017 – NotPetya, a destructive malware disguised as ransomware, infected tens of thousands of computers in at least 65 countries.

- (U) Neither required human interaction to infect other computers, execute, or encrypt data for ransom.
  - Both relied on Shadow Broker-released exploits to varying degrees.

(U) When do victims pay?

- (U) 3 Conditions Contributing to Victim Payment
  - Victims just want it to go away
  - Victims are unprepared, often leading to desperation
  - Victims trust that malicious actor will follow through with decryption upon payment.

- (U//FOUO) Why did so few WannaCry and NotPetya victims pay?
  - Very high profile
  - Exposed as unreliable very early

FBI • CYBER

OBJECTIVES

- Discuss Current Ransomware Threat Environment
- Discuss Prevention Methods for Consideration in Your Environment
- Resources and Getting Support

CURRENT RANSOMWARE THREAT CONCERNS:

- Most Common Ransomware Attack Methods (source:Palo Alto)
  - Silent Infections from Exploit Kits
    - Visits to compromised websites which redirect you to an exploit kit landing page to enable drive by download if vulnerability exist
  - Malicious Email Attachments
  - Malicious Links in Emails
- An Important Note: Phishing accounts for 2 of the 3 most common ransomware attack methods

CURRENT RANSOMWARE THREAT CONCERNS:

- 2020 Verizon Data Breach Investigations Report
  - Of malware incidents, ransomware accounts for 27%
  - 80% of malware infections in the education services area were accounted for by ransomware
  - Healthcare and public administration continued to be targeted by financially motivated threat actors through the use of ransomware
- Cyware (article July 20, 2020); 2019 FBI IC3 Report
  - 2, 047 complaints of ransomware; adjusted losses 8.9+ million dollars

CURRENT RANSOMWARE THREAT CONCERNS:

Cyware (article July 20, 2020)

- Eight types of malware within 3 months of July 20:
  - Avaddon
  - AgeLocker
  - Conti
  - ThiefQuest
  - Wasted Locker
  - Try2Cry
  - FileCry
  - Aris Locker

PREVENTION IS THE BEST RESPONSE

- Social Engineering/human element
  - No script for this, has to be a cultural and procedural change
- Configuration Concerns (examples)
- Remote Desktop Protocol (RDP; port 3389)
    - Nonsegmented Network
    - No Two Factor Authentication (2FA)
- What does normal look like? Do I have a baseline understanding?
  - Alerts that identify when thresholds are crossed? (SANS)
  - Do I have a network map? Routine active auditing of logs?
  - What is my network architecture? Interdependencies?
  - How are my backups stored? Offline? Offsite?
  - How frequent are my backups?

PREVENTION IS THE BEST RESPONSE

- Considerations for Prevention (Not comprehensive but a good start)
  - Backup, Backup, and Backup (frequently and maintain offline)
  - Properly segmented network; maintain updated network map; know your network interdependencies
  - 2 Factor Authentication
  - Understanding of baseline normal network activity; Regular review/internal auditing of logs or 3rd party vendor if employed;
  - Consider using “clipping levels”/thresholds where if activity rises above normal, an alert is issued (SANS 401)

VFC CYBER INTELLIGENCE UNIT ASSISTANCE

- Cyber Threat Intelligence:
  - Current Threat Trends (Malware Attacks, Attack Methods, etc.)
  - Evaluation of Indicators of Concern (IoCs)
    - IP addresses, Domains, etc.
    - Assistance with Static Log Analysis
  - Malware Analysis
- Cyber Event Evaluation/Incident Coordination Assistance (coordination of resources to facilitate assistance)
- Support to Law Enforcement in Criminal Investigations
- Information Sharing (finished intelligence products,
- DHS Homeland Security Information Network (HSIN) –
  - Help with Virginia CyberSHIELD Partnership accounts

QUESTIONS OR REQUEST FOR ASSISTANCE

- Contact Information:
- Rob Reese – Lead Analyst Cyber Intelligence Unit Virginia Fusion Center Virginia State Police
- Robert.reese@vsp.virginia.gov
- 804-350-8115
- VFC main – 804-674-2196 vfc@vfc.vsp.virginia.gov

SOURCES:

https://www.paloaltonetworks.com/cyberpedia/ransomware-common-attack-methods#:~:text=The%20three%20most%20common%20attack,use%20to%20deliver%20this%20threat

https://cyware.com/news/in-barely-three-months-eight-new-ransomware-surface-b84173be

https://enterprise.verizon.com/resources/reports/dbir/

https://pdf.ic3.gov/2019_IC3Report.pdf

Upcoming Events

Virginia Information Technologies Agency

VIRTUAL

COVITS

government technology

Sept 9-10, 2020

https://events.govtech.com/Virtual-COVITS.html

Virginia Information Technologies Agency

IS Orientation

IS Orientation - Remote

Sept. 30, 2020

http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

ISOAG meets the first Wednesday of each month in 2020

Future ISOAG

Sept. 2, 2020

Speakers: -David Raymond, Virginia Cyber Range

Raazi Zain, Zscaler

Milty Brizan, Amazon Web Services

Bill Stuart, VITA & Darrell Raymond, ATOS

ISOAG meets the first Wednesday of each month in 2020

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk