Virginia Information Technologies Agency

Welcome and Opening Remarks

Michael Watson

September 26, 2018

Virginia Information Technologies Agency

ISOAG September 26, 2018

I. Welcome & Opening Remarks	Mike Watson, VITA
II. Cyber Threat Trends	Jayne Holland, NIC
III. VSP Cybersecurity Update	Eric Gowan & Rob Reese, VSP
IV. Upcoming Events	Mike Watson, VITA
V. Partnership Updates	SAIC

CYBER THREAT TRENDS

JAYNE FRIEDLAND HOLLAND, CHIEF SECURITY OFFICER

SEPTEMBER 26, 2018

Overview

- Speaker Background/Bio
- Current and Emerging Security Trends
- Threat Categories
  - Events, Vulnerabilities and Actors
- Threat Intelligence
- Most Common Tactics, Techniques and Procedures (TTPs) & Mitigating Actions
- Other Trends – Legal Update

SPEAKER BACKGROUND

the people behind eGovernment

Jayne Friedland Holland

- Chief Security Officer
- Member of NIC's Executive Leadership Team
- Certified PCI Internal Security Assessor (PCI ISA) and practicing attorney
- Manages the legal, policy and technology practices related to security
- NIC provides 13,000+ digital government services
- NIC serves more than 5,500 federal, state and local agencies
- 220 million online transactions completed using NIC services = $20 billion securely processed annually

TRENDS IN SECURITY

Top Trends

1. Publicly available citizen data will present challenges for digital services
2. Attacks will continue to be cheaper and easier to do
3. Activism and political demonstrations will tend to have a cyber component
4. Growing complexity of solutions will challenge security teams

1 Publicly available citizen data will present challenges for digital services

- Total Records Compromised
- Value of a Data Record

Total Records Compromised

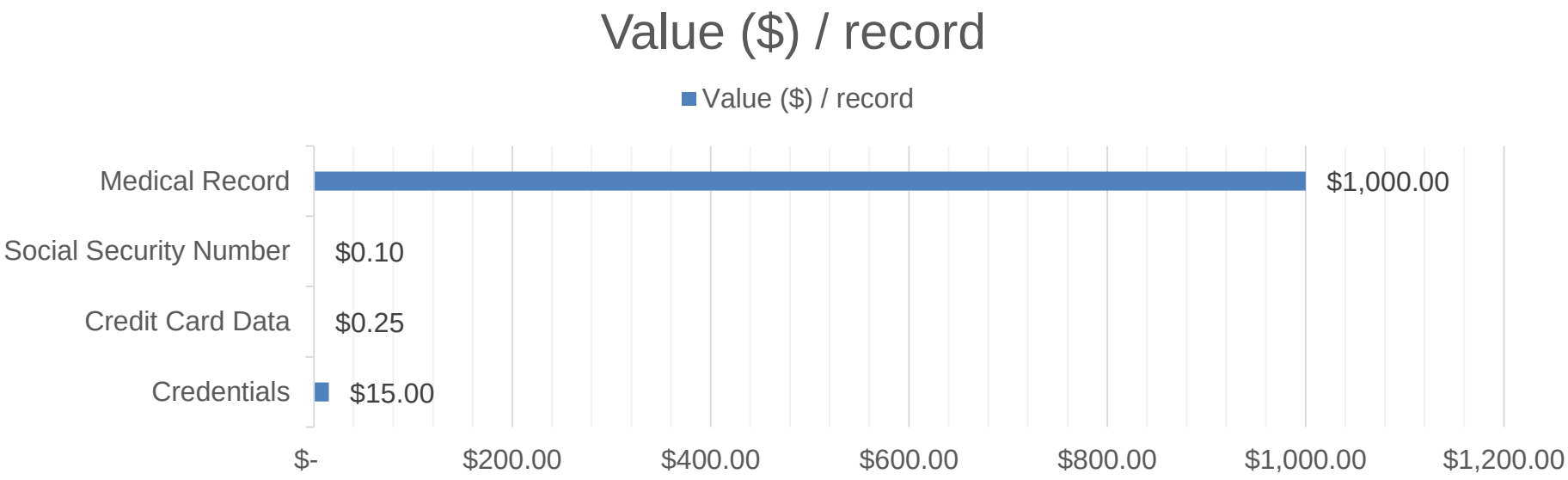
2.6 Billion

Total Records Compromised in 2017

- Equifax – 147.7 million records
- River City Media – 1.34 billion email addresses
- Deep Root Analytics – 198 million records
- Alteryx – 120 million records
- Center for Election Systems at Kennesaw State University – 7.5 million records

https://www.darkreading.com/attacks-breaches/26-billion-plus-data-records-breached-last-year/d/d-id/1331514

Value of Data Record



https://www.forbes.com/sites/mariyayao/2017/04/14/ your-electronic-medical-records-can-be-worth-1000-to-hackers/

2 Attacks will become cheaper and easier

- Cyberweapons
- Cheaper than a cup of coffee
- Dark Market – Cyberservices Market as a Service

Cyberweapons

- Cyber Warfare is real and out in the open now.
- Toolkits are common place and utilized by any entity with medium/high skills.
- Anyone can use a point and click service to deliver an attack.

Cheaper Than Coffee

Dark Web Pricelist

The following table details the price of equipment in a hackers' toolkit that can be bought on the dark web – a full table can be found below:

Category	Average value on dark web	Sales price explained
Anonymity Tool	$13.19	Hackers wanting to cover their tracks can do so cheaply. This price includes crypters, used to disguise malware as benign files.
Carding Software	$44.37	Used alongside readily available hardware, this very powerful software allows con artists to clone credit and debit cards.
Cryptocurrency Fraud Malware	$6.07	Cryptocurrency, such as Bitcoin or Monero, is attractive to cybercriminals due to its potential for anonymous transactions and rocketing value.
Keylogger	$2.07	Simple yet effective software that captures every keystroke on your computer
Malware	$44.99	Among the malware listed on the dark web were custom instances of ransomware that will lock up your computer, permanently encrypting its contents unless a ransom is paid.
Phishing Page	$2.28	There are ready-made phishing pages – set up to mimic trusted brands – for the world's most popular consumer brands across the dark web.
Remote Access Trojan	$9.74	This nasty strain of malware allows a hacker to take full control of your computer. Not only can they log all your keystrokes and access private files in order to commit identity theft and defraud you, but it's also common for voyeurs to use these so-called RATs for webcam spying.
WiFi Hacking Software	$3.00	It's possible to access this type of software for free on the normal web – as security experts use this to stress test wireless networks – so dark web vendors sell cheaply and tend to offer bundles including additional resources and even customer support to tempt buyers.
Total	**$125.71**	

http://www.itsecurityguru.org/2018/08/03/wannabe-fraudsters-can-buy-hacking-tools-dark-web-cost-cup-coffee/

Dark Market – as a Service

- Malware
  (ransomware, miners)
- Exploits
  (known and zero-days)
- Data
  (personal, accounting, etc.)
- Access
  (web shells, passwords, etc.)

https://www.ptsecurity.com/ww-en/analytics/293975/

3 Activism and political demonstrations will tend to have a cyber component

- Historical Events
- Midterm Campaign Hacks

Historical Events

- Indiana Religious Freedom Bill
- West Virginia Elk River Chemical Spill

Midterm Campaign Hacks

- Website impersonating Microsoft
- Three candidates targeted
- Method was phishing emails
- Origination point is unknown

https://www.politico.com/story/2018/07/19/midterm-campaign-hacking-microsoft-733256

4 Growing complexity of solutions will challenge security teams

Growing Complexity

- Big Data
- Cloud Computing
- Mobile
- Internet of Things
- Social Media
- Artificial Intelligence / Machine Learning

The Future Landscape

20-30 Billion

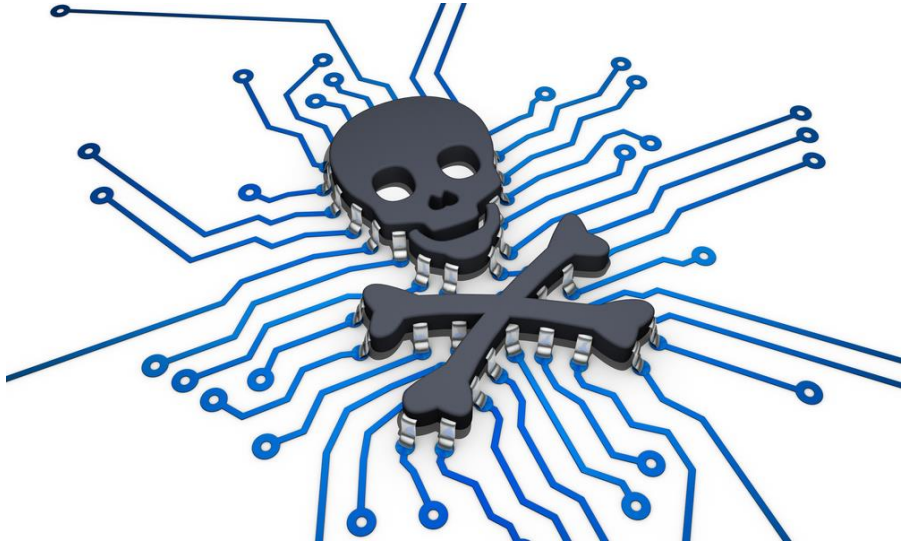
connected things will be in use by 2020

- Gardner, IDC

- The threat landscape is deep and constantly changing.
- Avoid overcommitting on nascent technologies and better manage descending threats to adapt earlier.
- 100% of large enterprises will be asked to report to Board on cybersecurity and technology risk.

THREAT CATEGORIES

Threats



- ✓ Events
- ✓ Vulnerabilities
- ✓ Actors

Events

Activities that occur (scheduled or otherwise) with the potential to evoke negative emotions.

Hacktivism

Conducting cyber attacks as a platform for delivering your message

Legislation

Indiana passed legislation which was interpreted as allowing legal discrimination against the LGBT community.

DDoS attacks launched against Indiana website in protest of legislation.

Lack of Legislation

11 states

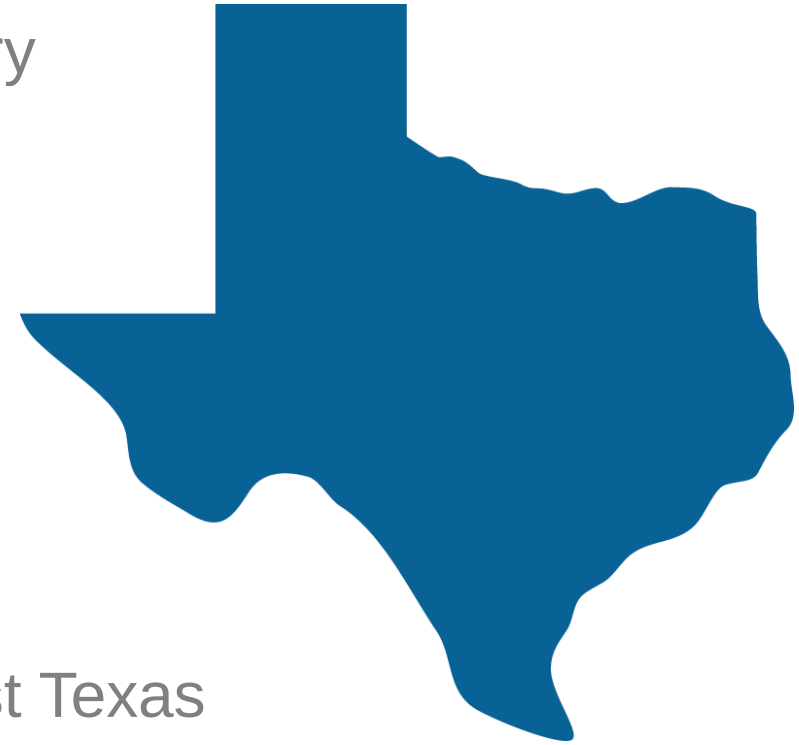
Identified as targets for not explicitly making the act of zoophilia illegal.

Term: Zoophilia

Don't "Google" that term!

Presidential Primaries

At one point in the 2016 primary cycle, five of the Republican candidates were from Texas.



DDoS attacks launched against Texas websites in protest of comments made or viewpoints expressed during the process.

Vulnerabilities

Weaknesses which can be exploited by an actor to perform unauthorized access within a system.

Vulnerabilities

Most successful attacks happen because of a failure of cyber hygiene (patching).

1/2

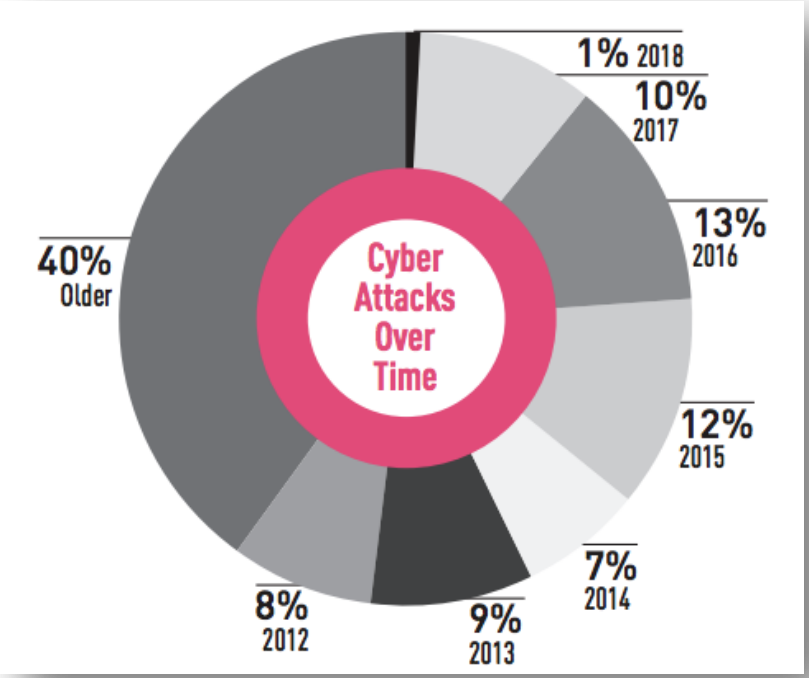
Half of all exploitations happen between 10 and 100 days after the vulnerability announcement, with the median around 30 days. (trending downward)

Adobe and Microsoft are exploited much closer to the announcement than other products like Apple and Mozilla.

Vulnerabilities

99%

of attacks observed in 2018 attempted to exploit vulnerabilities from 2017 or older



From Checkpoint Cyber Attack Trends mid-year 2018 report

Actors

Individuals or groups who use specific Tactics, Techniques and Procedures (TTPs) to conduct their attacks.

- Hackers / hacktivists
- Criminals / organized crime
- Nation states
- Competitors
- Employees / insiders / third parties

We can’t defend against actors, but we can defend against TTPs.

Threat Intelligence

Identifying events, vulnerabilities and actors that might negatively impact your organization.

Analysis

https://www.threatq.com/threat-intelligence/

Ransomware

THREAT: Commonly available malware is more able to evade traditional anti-virus than anti-virus is able to detect malware.

100%

likelihood

IMPACT: San Francisco Light Rail (3 days of free rides)
Hancock Health (disruption, $55K ransom),
City of Atlanta (disruption, costly remediation)

TACTICS TECHNIQUES & PROCEDURES

Most Common TTPs

- DDoS Attacks
- Application Weaknesses
- Social Engineering / Phishing
- Stolen Credentials / Identities
- Ransomware & Extortion

DDoS Attacks
(Distributed Denial of Service)

- 16% increase in DDoS attacks since last year
- February 2018 – Github's code hosting website hit with largest DDoS attack
- Highest volume recorded at 1.35Tbps ← that's fast!!

Mitigating DDoS Attacks

- Proactive Subscription
- Upstream ISP
- Third Party Service or Appliance
- Cloud SaaS also available

Application Weaknesses

Attackers target:

- Interactions with databases (SQLi)
- Presentation of data (XSS)
- Permissions (business logic)

Objective: To reach data protected by the application

Mitigating Application Security Weaknesses

- **IMPLEMENT** secure coding best practices.
- **MAKE** security requirements part of project initiation; and security testing part of success criteria.
- **CONDUCT** periodic penetration testing.
- **HAVE** a solid application patch management program/process in place.
- **DEPLOY** a web application firewall (WAF).

Social Engineering / Phishing

Email phishing attacks

wire fraud, ransomware

Telephone scams

Social media scams

Mitigating Social Engineering

- **Provide employee Security Awareness Training**

Tips for Educating Employees:

- ✓ Trust no one!
- ✓ Don’t reply to the email or do anything to fulfill the request.
- ✓ Confirm if the request is legitimate.
- ✓ Contact appropriate security personnel if you need confirmation the email or attachment is “safe”.
- ✓ Follow the protocol for escalation.
- ✓ Employees should be reminded not to send sensitive information over emails or chats.
- ✓ Install and maintain anti-malware software (next-gen AV).

Stolen Credentials / Identities

- Social engineering used to steal credentials and identities
- Stolen credentials and identities then leveraged to cause a breach of an entity's network
- Examples: Reddit.com breach
  Cici's Pizza breach

Mitigating Stolen Credentials

- Greater assurance of the identity behind the credentials being used
- Consider multi-factor authentication technologies
  - Something you know (password)
  - Something you have (token)
  - Something you are (biometric)
- Consider removing passwords altogether
  - One-time login URLs delivered to registered emails
- Maintain strong permissions and user access controls

Ransomware & Extortion

- Malware that restricts access to infected system and perpetrator demands ransom to remove restrictions
- **1.5 million** phishing websites created each month
- Phishing attempts have grown by **65%**
- **30%** are opened by users
- **12%** click on links or attachments
- **95%** of all attacks on enterprise networks are the result of successful phishing

Mitigating Ransomware & Extortion

- **IMPLEMENT** a comprehensive patch management program for all endpoints.
- **DEPLOY** Next-Gen Antivirus (zero day threat detection).
- **MAINTAIN** backups of data on endpoints that includes multiple revisions of the files.
- **UNDERSTAND** your organization's stance on paying a ransom.

OTHER TRENDS

Legal Update

- Big privacy and consumer protection focus

1. California Privacy Protection Act (CPPA)
2. State Data Breach Notification Statutes

Summary

- Cyber threats are increasing in frequency, complexity and severity.
- Expect to see more advanced attacks that disrupt government activities.
- Tools and services are readily available on The Dark Market.
- To provide your organizations with the best level of protection, security teams must be attuned to the ever-changing landscape and the latest threats and attack methods.
- Use threat intelligence and enhanced threat detection to ID trends / TTPs.
- Be prepared.

QUESTIONS?

the people behind eGovernment

Upcoming Events

National Cyber Security Awareness Month

National Cybersecurity Awareness Month

National Cyber Security Awareness Month is observed every October. It was created as an effort between government and industry to make sure all Americans have the resources they need to stay and secure on the Internet.

National Cyber Security Awareness Month is celebrating its 15th year of promoting internet safety.

Virginia Information Technologies Agency

2019Kids Safe Online Poster Contest

Kick Off: September 26

Deadline or submissions: January 25, 2019

Website Information: https://www.cisecurity.org/ms-isac/ms-isac-toolkit/

Guideline: https://www.cisecurity.org/wp-content/uploads/2018/08/MS-ISAC-Poster-Contest-and-Form.pdf

Virginia winner will grace the cover of the 2019 "Kid Safe Online" poster calendar.

***Virginia has had at least two national winners for the past five years.**

Virginia Information Technologies Agency

2019 Kids Safe Online Poster Contest Cover Winner

ISO Certification

Mandatory ISO Meeting

- *We will have a mandatory meeting of all ISOs on October 3.*
- *We encourage all primary ISOs to attend this meeting in person.*
- *If you are a primary ISO, and cannot attend, you may designate the backup ISO to attend in your place.*

Contacts

If you need a status update on your ISO Certification, please contact:

Edward.Miller@vita.virginia.gov

Tina Harris-Cunningham@vita.virginia.gov

Last IS Orientation

The last IS Orientation for 2018 will be held on

December 13, 2018 @1:00 PM

CESC - Room 1221

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk