Data Governance & Information Security @ UH

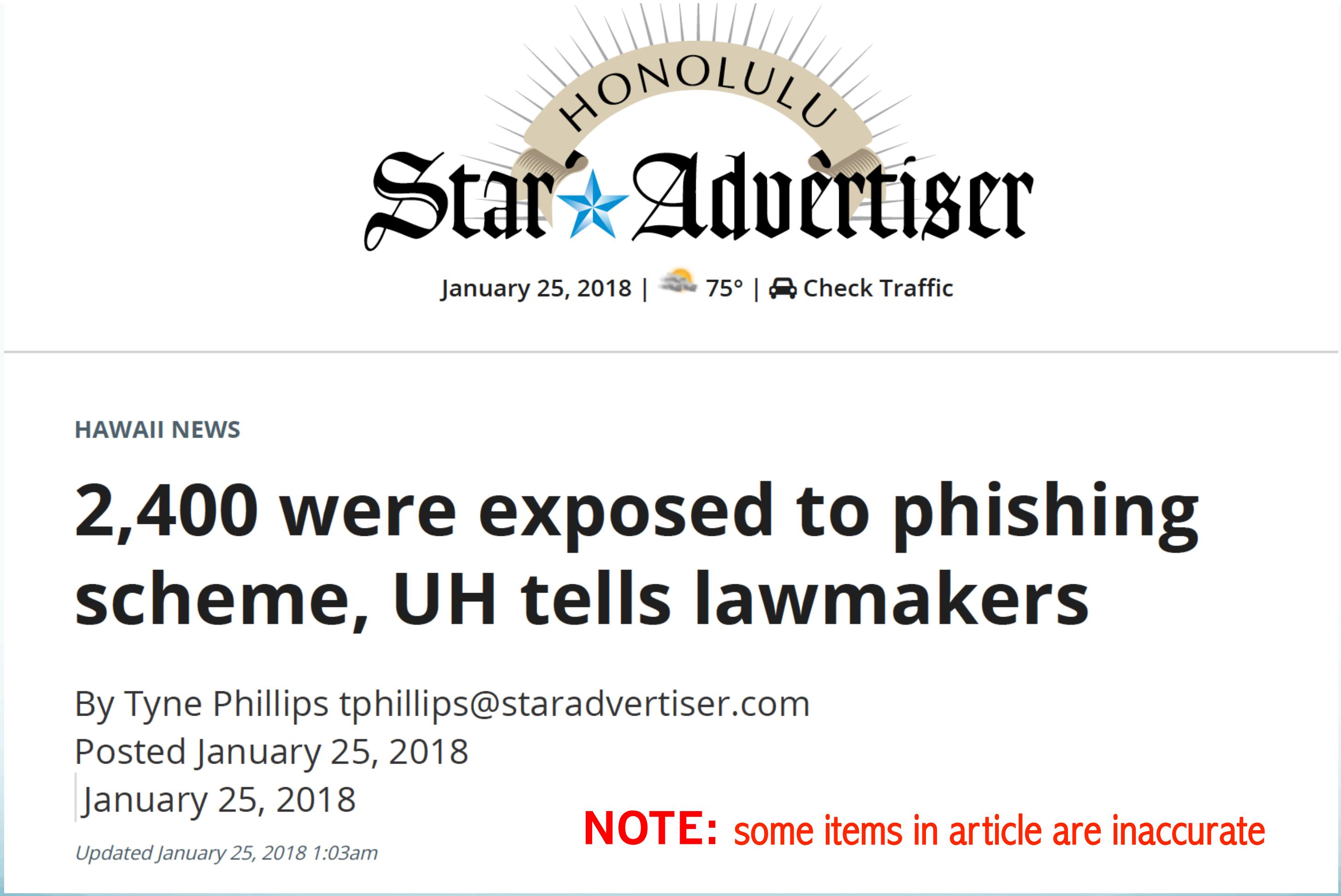
Abbreviated presentation
for UH App Developers Meeting

All Campus IT Workshop:
https://www.hawaii.edu/its/allcampusworkshop/

www.hawaii.edu/uhdatagov
www.hawaii.edu/infosec

Jodi Ito, Chief Information Security Officer, jodi@hawaii.edu

Current Threats at UH



HONOLULU Star Advertiser

January 25, 2018 | 75° | Check Traffic

HAWAII NEWS

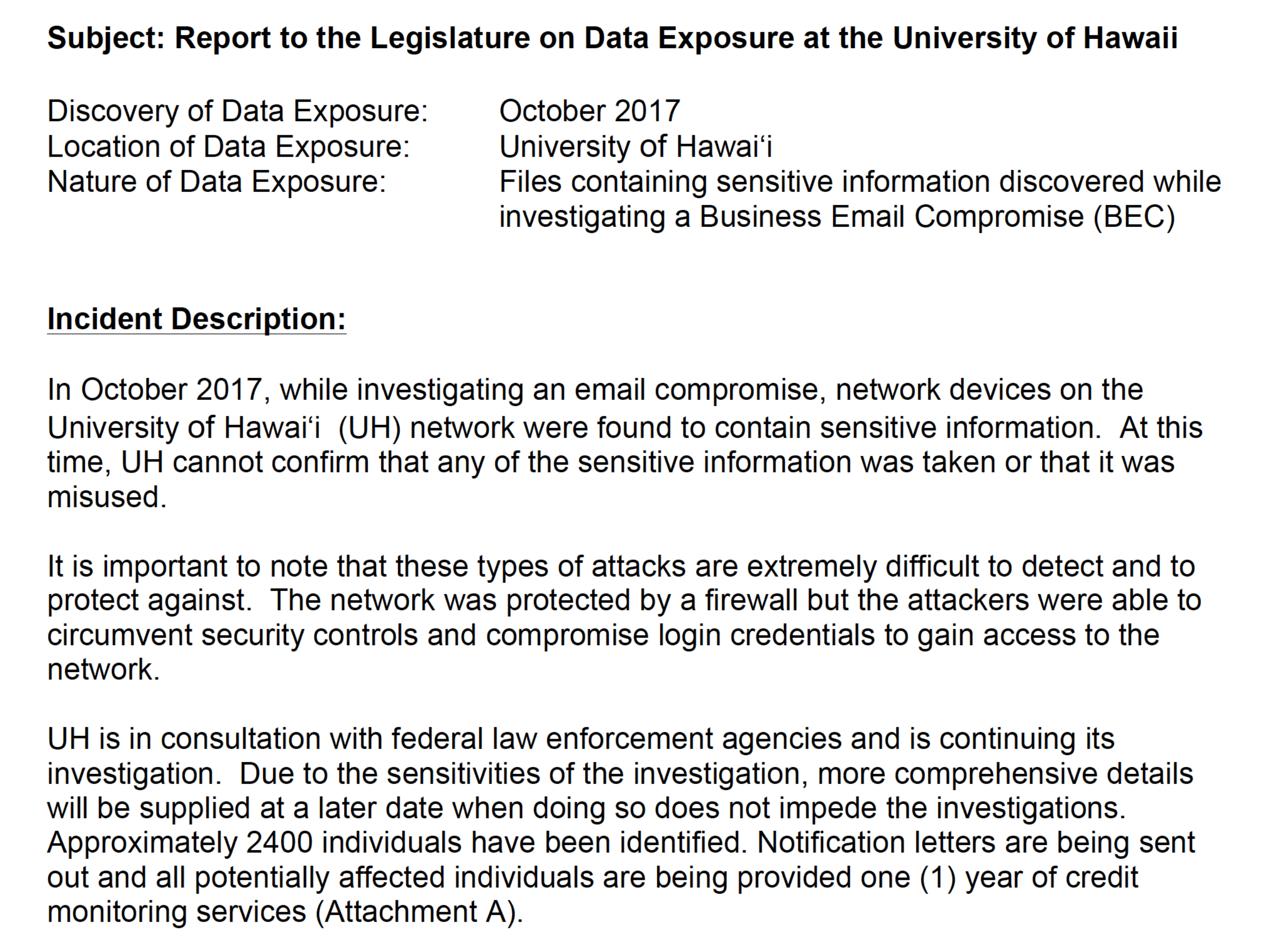
2,400 were exposed to phishing scheme, UH tells lawmakers

By Tyne Phillips tphillips@staradvertiser.com
Posted January 25, 2018
January 25, 2018

Updated January 25, 2018 1:03am

NOTE: some items in article are inaccurate

http://www.staradvertiser.com/2018/01/25/hawaii-news/2400-were-exposed-to-phishing-scheme-uh-tells-lawmakers/



Subject: Report to the Legislature on Data Exposure at the University of Hawaii

Discovery of Data Exposure:	October 2017
Location of Data Exposure:	University of Hawaiʻi
Nature of Data Exposure:	Files containing sensitive information discovered while investigating a Business Email Compromise (BEC)

<u>Incident Description:</u>

In October 2017, while investigating an email compromise, network devices on the University of Hawaiʻi (UH) network were found to contain sensitive information. At this time, UH cannot confirm that any of the sensitive information was taken or that it was misused.

It is important to note that these types of attacks are extremely difficult to detect and to protect against. The network was protected by a firewall but the attackers were able to circumvent security controls and compromise login credentials to gain access to the network.

UH is in consultation with federal law enforcement agencies and is continuing its investigation. Due to the sensitivities of the investigation, more comprehensive details will be supplied at a later date when doing so does not impede the investigations. Approximately 2400 individuals have been identified. Notification letters are being sent out and all potentially affected individuals are being provided one (1) year of credit monitoring services (Attachment A).

http://www.hawaii.edu/govrel/docs/reports/2017/hrs487n-4_2017_october-2017-breach_report.pdf

Periscope / Leviathan APT Group

Attacker TTPs
(Tactics, Techniques, Procedures)

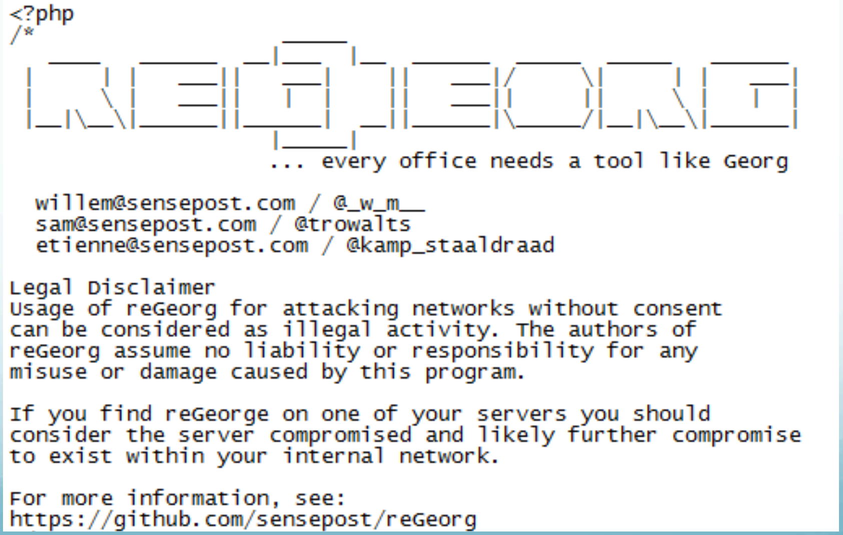
- Two distinct backdoor methods:
  - Windows XP - StickyKey
  - Windows 7/10 - JS + Beacon (Beacon re-downloaded and executed each time the JavaScript is executed)
- Persistence methods include StickyKey, Task Scheduler, Windows Service
- Lateral movement methods appear to be focused around obtaining passwords via MimiKatz, SpiderLabs Responder, NTDSDumpEx, Shadow Copy > NTDS.dit > offline cracking
- Defense and evasion methods are hiding malware files in existing folders with legitimate-sounding names, running CMD via c:\windows\temp\system, deleting event logs, memory-only malware

Attacker TTPs

- Another (new?) method involves compromising the victim PC and executing a single JavaScript file
- If this script executes, the only sign of infection is a running process called "wscript.exe" which is a legitimate Windows program
- When the victim PC connects with the C&C, the main malicious script is downloaded into memory and executed
- C&C commands are limited but enough to upload more powerful tools
- Callback to the C&C is done via a cookie in GET request encoded in base64

Attacker TTPs

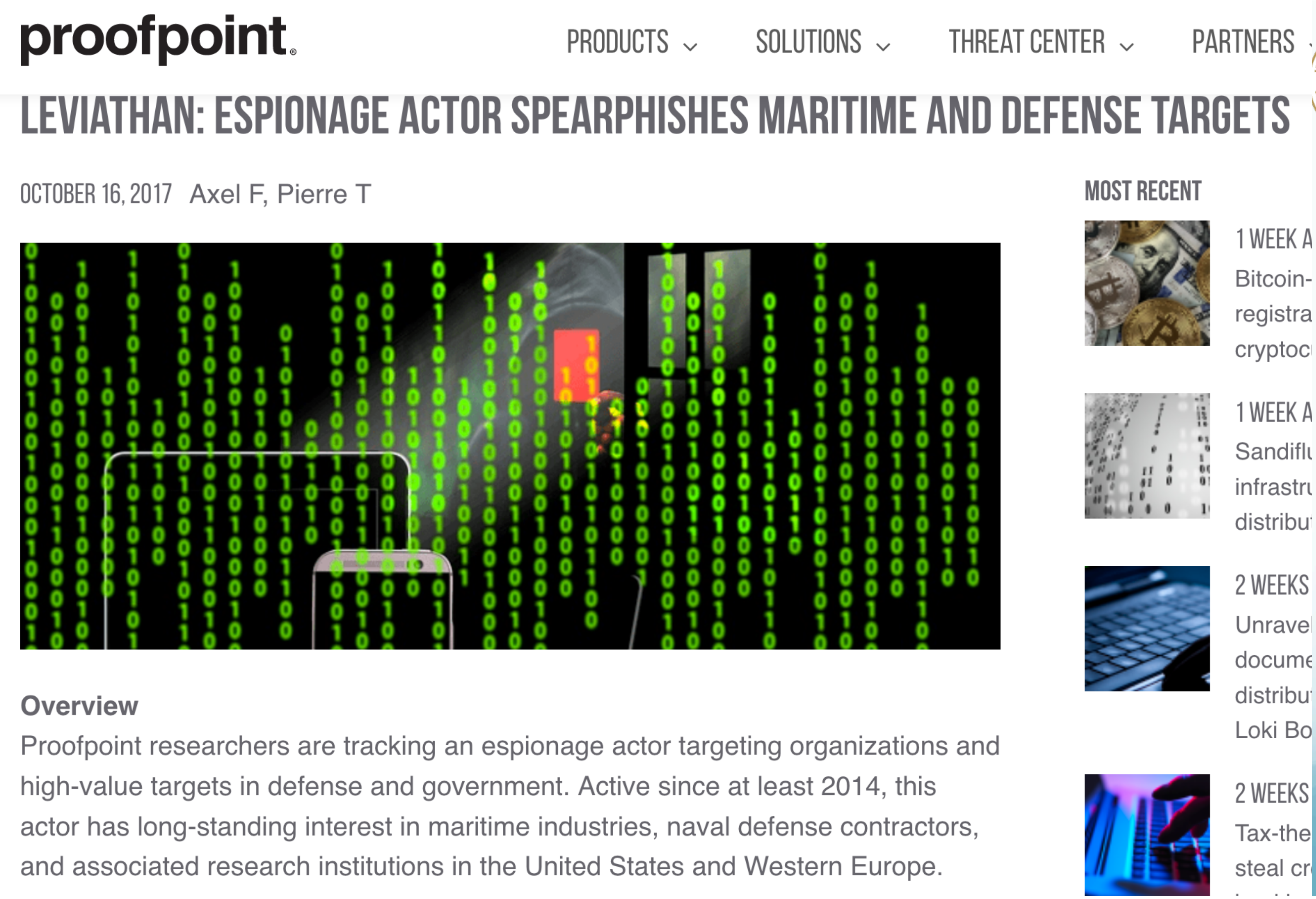
- The Group also used a proxy called reGeorg (available from Github) to hide its origination during the first part of their campaign and later abandoned its use and accessed the PHP scripts directly



```
<?php
/*
                    _____
  _____   ______  __|___  |__  ______  _____  _____   ______
 |     | |   ___||   ___|    ||   ___|/     \|     | |   ___|
 |     \ |   ___||   |  |    ||   ___||     ||     \ |   |  |
 |__|\__\|______||______|  __||______|\_____/|__|\__\|______|
                    |_____|
                    ... every office needs a tool like Georg

  willem@sensepost.com / @_w_m__
  sam@sensepost.com / @trowalts
  etienne@sensepost.com / @kamp_staaldraad

Legal Disclaimer
Usage of reGeorg for attacking networks without consent
can be considered as illegal activity. The authors of
reGeorg assume no liability or responsibility for any
misuse or damage caused by this program.

If you find reGeorge on one of your servers you should
consider the server compromised and likely further compromise
to exist within your internal network.

For more information, see:
https://github.com/sensepost/reGeorg
```

More Reading

- F-Secure: NanHaiShu:
  - https://labsblog.f-secure.com/2016/08/04/nanhaishu-rating-the-south-china-sea/
- FireEye: TEMP.Periscope:
  - https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
- ✓ Proofpoint: Leviathan:
  - https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets



LEVIATHAN: ESPIONAGE ACTOR SPEARPHISHES MARITIME AND DEFENSE TARGETS

OCTOBER 16, 2017 Axel F, Pierre T

Overview

Proofpoint researchers are tracking an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor has long-standing interest in maritime industries, naval defense contractors, and associated research institutions in the United States and Western Europe.

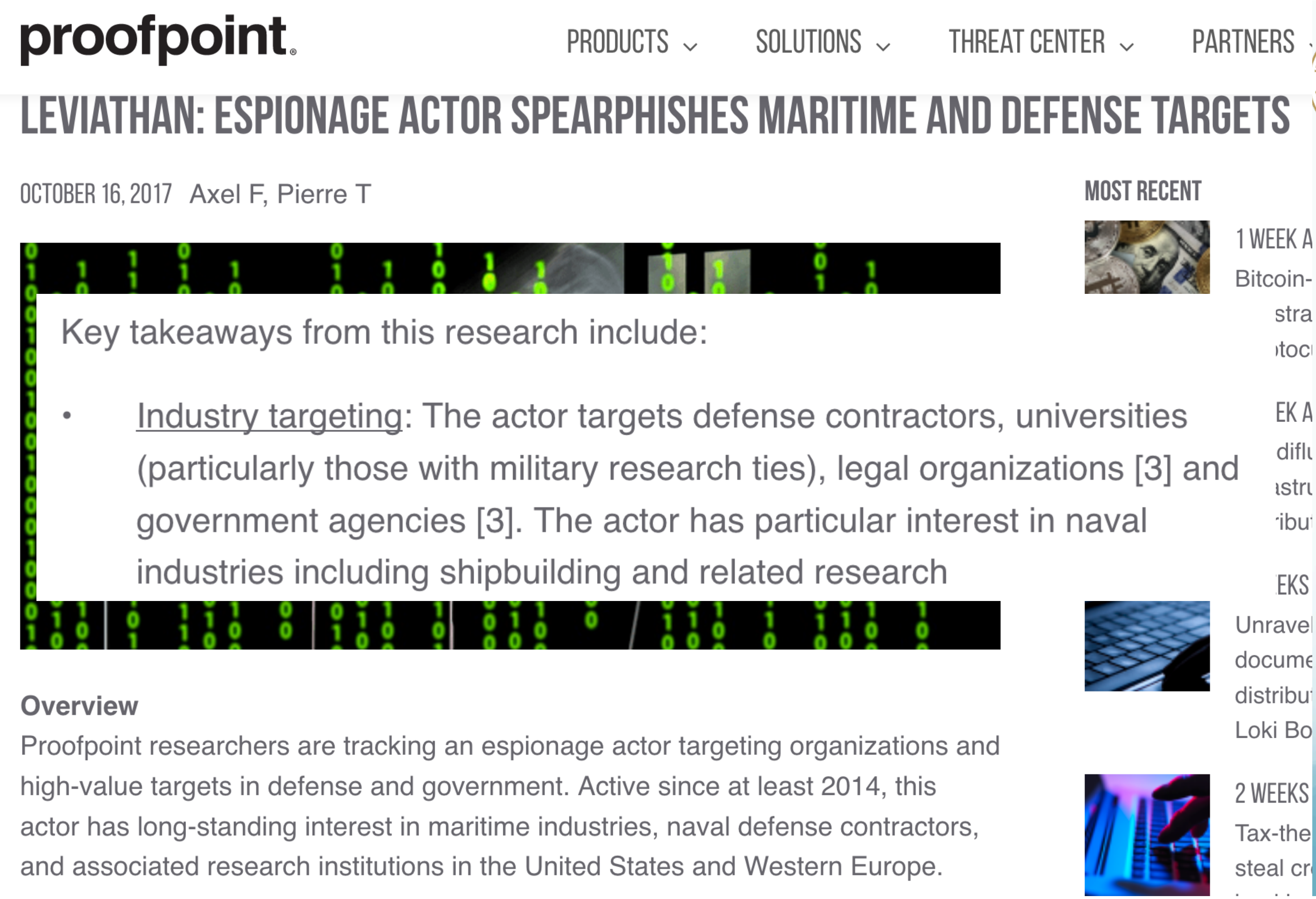
MOST RECENT

1 WEEK A
Bitcoin-
registra
cryptoc

1 WEEK A
Sandiflu
infrastru
distribu

2 WEEKS
Unravel
docume
distribu
Loki Bo

2 WEEKS
Tax-the
steal cr



LEVIATHAN: ESPIONAGE ACTOR SPEARPHISHES MARITIME AND DEFENSE TARGETS

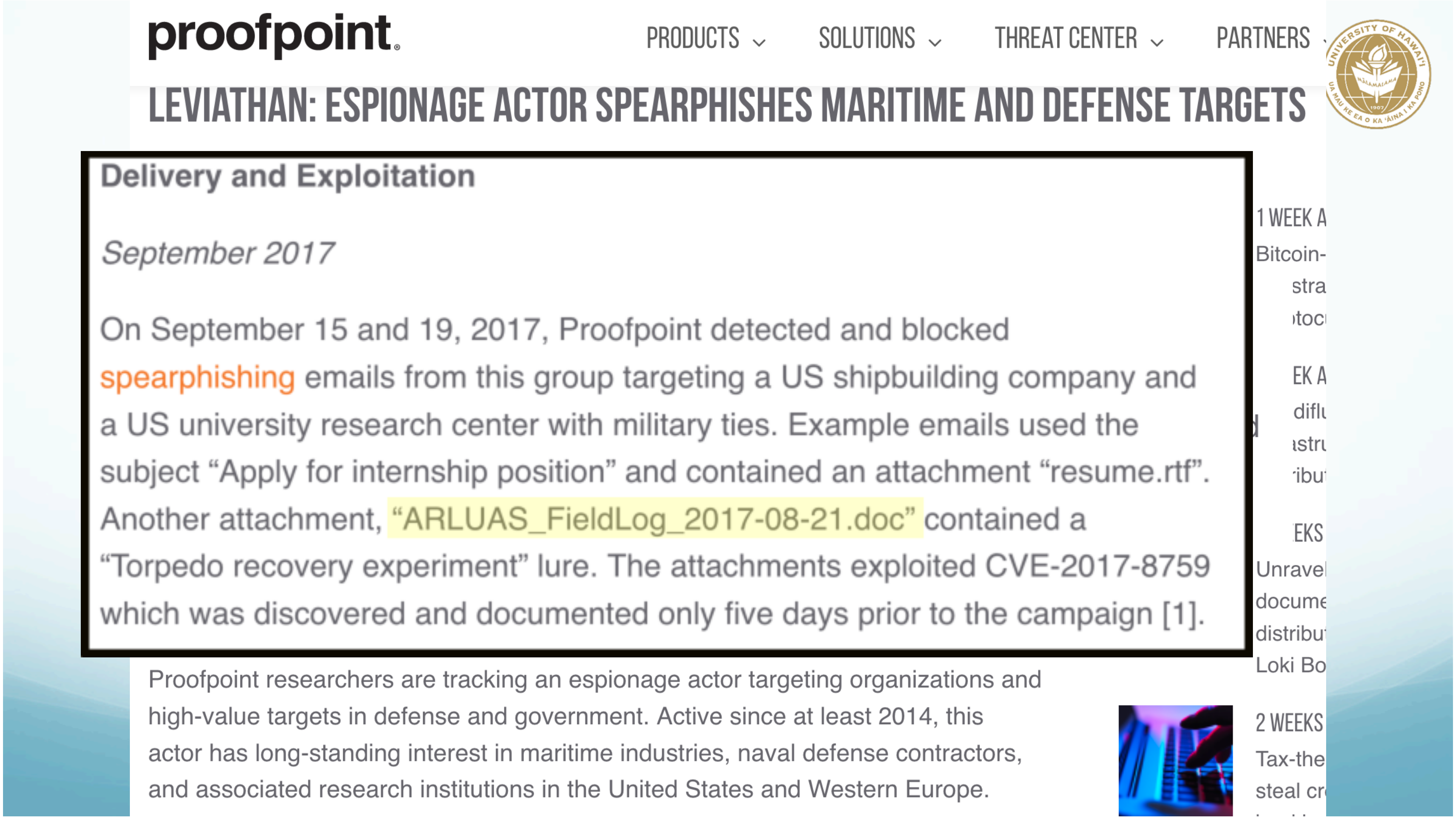
OCTOBER 16, 2017 Axel F, Pierre T

Key takeaways from this research include:

- Industry targeting: The actor targets defense contractors, universities (particularly those with military research ties), legal organizations [3] and government agencies [3]. The actor has particular interest in naval industries including shipbuilding and related research

Overview

Proofpoint researchers are tracking an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor has long-standing interest in maritime industries, naval defense contractors, and associated research institutions in the United States and Western Europe.



LEVIATHAN: ESPIONAGE ACTOR SPEARPHISHES MARITIME AND DEFENSE TARGETS

Delivery and Exploitation

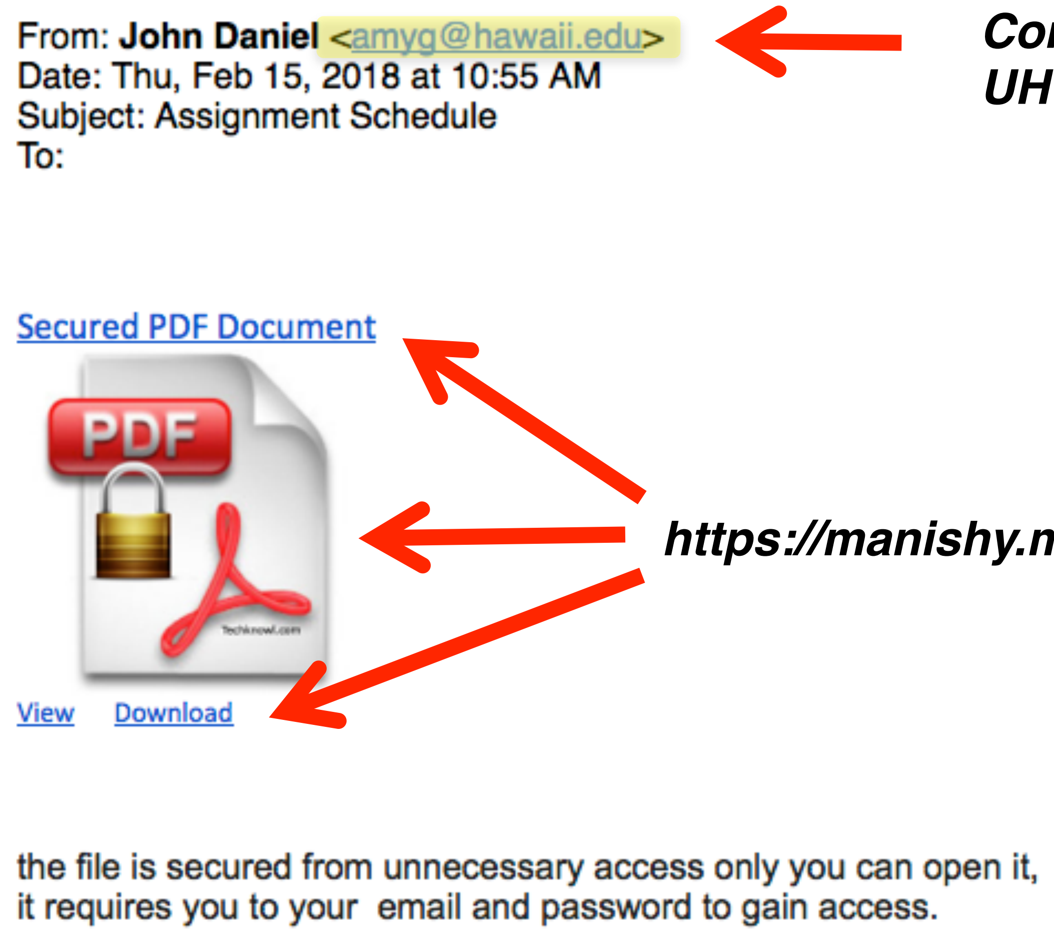
September 2017

On September 15 and 19, 2017, Proofpoint detected and blocked spearphishing emails from this group targeting a US shipbuilding company and a US university research center with military ties. Example emails used the subject “Apply for internship position” and contained an attachment “resume.rtf”. Another attachment, “ARLUAS_FieldLog_2017-08-21.doc” contained a “Torpedo recovery experiment” lure. The attachments exploited CVE-2017-8759 which was discovered and documented only five days prior to the campaign [1].

Proofpoint researchers are tracking an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor has long-standing interest in maritime industries, naval defense contractors, and associated research institutions in the United States and Western Europe.

Business Email Compromise (BEC)

- Phishing & Spear Phishing
- Want your personal information:
  - username/password: gain access to YOUR email account, YOUR computer & information systems that you use
  - SSN, credit/bank account information, home address – financial crimes
- Will use that information for other malicious/criminal purposes



From: **John Daniel** <amyg@hawaii.edu>
Date: Thu, Feb 15, 2018 at 10:55 AM
Subject: Assignment Schedule
To:

Secured PDF Document

View Download

the file is secured from unnecessary access only you can open it,
it requires you to your email and password to gain access.

Compromised
UH email account

https://manishy.ml/ll/doc/doc/doc/index.php

Highly Targeted Spear Phishing

- Appears to be from someone you know (supervisor, colleague, friend, President of the University…)
- Leveraging your relationship to attempt to get you to give up very specific information
- Email from the UH President apparently addressed to the Director of FMO/UH Controller
- Asking for bank account information
- Possible reconnaissance; leading to a targeted attack

Vulnerabilities/Compromises

- Web:
  - Drupal/CVE-2018-7602
  - Drupal/CVE-2018-2628
- LDAP exploit/DDoS:
  - LDAP service responds on port 389
  - 5/29/2018 – Tuesday:
    - BEGIN PERIMETER BLOCKING: 389/TCP and 389/UDP

Data Governance Update

What is Data Governance

> "…a framework that enables us to effectively manage data"

- Defines how data are collected, stored, and used
- Defines who can access data, when, and under what conditions
- Establishes decision rights
- Establishes clear lines of accountability
- Gives a voice to all appropriate parties
- Provides a mechanism for conflict resolutions involving data

UH Data Governance Goals

Protect the privacy and security of Institutional Data

(i.e., data created, received, maintained, and/or transmitted by UH in the course of meeting its administrative and academic requirements)

- Produce higher quality data for informed decision making
- Promote efficient use of resources
- Increase transparency and accountability

Key Regulations and Penalties (1)

Regulation	Description	Penalty
Family Educational Rights and Privacy Act (FERPA)	• Federal law that protects the privacy of student education records • Access to personally identifiable information (PII) is based on a legitimate educational interest • UH's FERPA policy: AP7.022 • Data subject to regulation: • All student data EXCEPT directory information (e.g., name, major, class standing, date of attendance, full- or part-time status, degrees conferred, honors and awards, height/weight of athletes, etc.)	Potential loss of federal financial aid funding
Higher Education Act (HEA)	• Federal law that protects the federal financial aid information • Much more restrictive than FERPA Data subject to regulation: • FAFSA data • PII cannot be shared even with student consent – waiting for clarification from USDOE	Potential loss of federal financial aid funding

Key Regulations and Penalties (2)

Regulation	Description	Penalty
Health Insurance Portability and Accountability Act (HIPAA)	• Federal law that protects the privacy of individually identifiable health information • UH's HIPAA policy: EP2.217 Data subject to regulation: • Health	Financial fines; also requires a breach notification to HHS & in accordance with SoH HRS §487N
Hawaiʻi Revised Statute (HRS) Chapter 92F	• State law also known as the Uniform Information Practices Act (UIPA) which requires open access to government records • Governs open records requests Data subject to regulation 92F-12: • Employee data that must be made available to the public (e.g., name, salary range, bargaining unit, job title, business address/ phone, employing agency, etc.)	If data is intentionally revealed that should not be, could be convicted of a misdemeanor unless a greater penalty is provided for by law.

Key Regulations and Penalties (3)

Regulation	Description	Penalty
Payment Card Industry Data Security Standard (PCI-DSS) information	- A widely accepted set of policies / procedures that protects cardholders' credit/debit/cash card transactions Data subject to regulation: - Credit Card	Financial fines; also requires a breach notification in accordance with HRS §487N
Hawai'i Revised Statutes (HRS) §487N	- State law that defines the breach notification to the legislature - Written report to the legislature within 20 days after the discovery of a data breach Data subject to regulation: - First Name or First Initial/Last Name combined with: - Social Security Number (SSN) - Driver license or state ID # - Info to access a person's financial account (account #, access codes, passwords, etc.)	

Key Regulations and Penalties (4)

Regulation	Description	Penalty
National Institute of Standards and Technology Special Programs (NIST SP) 800-171r1	• Dept. of Defense (DoD) Defense Federal Acquisition Regulations Supplement (DFARS) clause 252.704.2012 • To protect Controlled Unclassified Information (CUI) Data subject to regulation: • Data defined by DoD as requiring protection (primarily research project data sponsored by the DoD) • Near future: Educational data (future US Dept. of Education mandate)	
National Industrial Security Program	• DoD Directive 5220.22-M • National Industrial Security Program Operating Manual Data subject to regulation: • Classified data	

Key Regulations and Penalties (5)

Regulation	Description	Penalty
Biological Safety Program	Governs all research, teaching, and testing activities involving infectious agents and recombinant materials • Section 511 of the Antiterrorism and Effective Death Penalty Act of 1996 • Public Health Security and Bioterrorism Preparedness and Response Act of 2002 • Executive Order 13546 • 7 CFR Part 331, 9 CFR Part 121, and 42 CFR Part 73	
Export Control & International Traffic in Arms Regulations (ITAR)	• Federal regulations that impose access, dissemination or participation restrictions on the use and/or transfer of commodities, technical data, or the provision of services subject to United States (US) export controls for reasons of national security, foreign policy, anti-terrorism or non-proliferation • 22 Code of Federal Regulations (CFR) Parts 120-130 • 15 CFR Parts 730-774 • 31 CFR Parts 500-599	

Key Regulations and Penalties (6)*

Regulation	Description	Penalty
General Data Protection Regulation (GDPR)	A EU data protection law that imposes strict new rules on maintaining and processing PII about residents of 28 EU countries. • Specifies how consumer data should be used and protected in today's digital environment • Applies to all organizations holding and processing personal data in connection with the offering of goods and services • Focus is on companies like Facebook, Google, and Amazon, however the regulation also applies to colleges and universities • Goes into effect May 25, 2018	Up to 4% of global turnover or 20m Euros, whichever is higher

Breaking news:
"Facebook and Google hit with $8.8 billion in lawsuits on day one of GDPR"
https://www.theverge.com/2018/5/25/17393766/facebook-google-gdpr-lawsuit-max-schrems-europe
http://www.bbc.com/news/technology-44252327

***NOTE: This is a new slide added on April 24, 2018**

Impact of Data Breaches

- Loss of federal financial aid funding (FERPA, HEA)
- Financial fines (HIPAA, PCI-DSS)
- Class action lawsuits
- Expenses, financial and human capital
- Loss of reputation / unfavorable publicity
- Additional legislative scrutiny

UH Data Related Policies and Procedures

Executive Policies

Institutional Data Governance
EP2.215

Use and Management of Information Technology Resources
EP2.210
(to be updated)

System and Campus Wide Electronic Channels for Communicating with Students
EP2.213

Data Classification Categories & Info Security Guidelines
EP2.214

Institutional Records Management and Electronic Approvals / Signatures
EP2.216
(to be updated)

HIPAA
EP2.217

Online Approvals of Internal University Transactions
EP2.218

Administrative Procedures

FERPA
AP7.022

Data System Authorizations
(TBD)

Mandatory Training & Continuing Education Requirements
AP2.215

Open Records Requests
(TBD)

Data Sharing Request Process
(in progress)

Specialized Purchasing
AP8.265

Records Retention Schedule
(in progress)

Credit Card Program
AP8.710

Data Breaches
(coming soon)

Electronic Payments via University Websites
AP8.711

EP2.214, Data Classification Categories

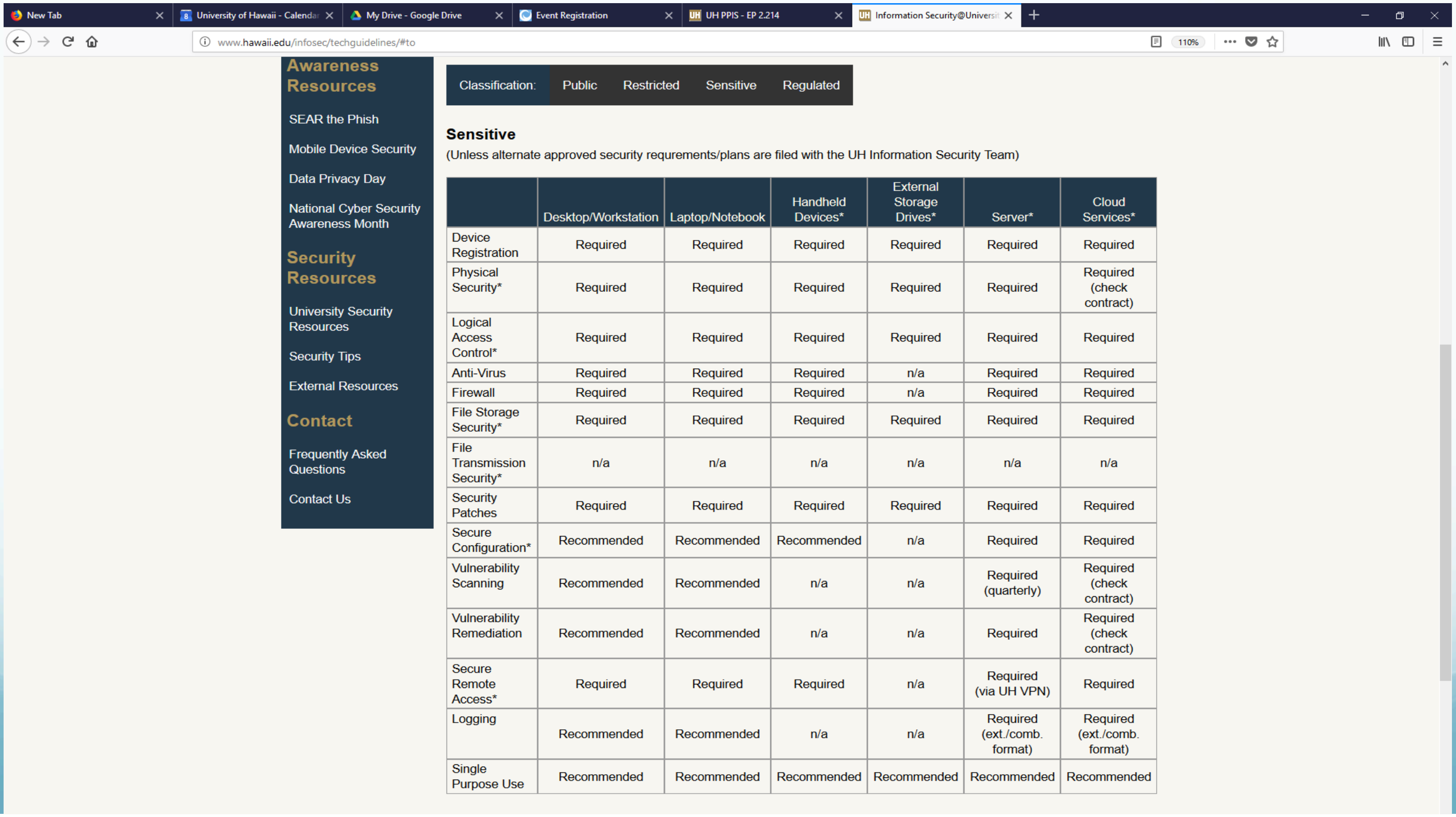
Category	Definition	Examples
Public	Access is not restricted and is subject to open records requests	Student directory information, employee's business contact info
Restricted	Used for UH business only; will not be distributed to external parties; released externally only under the terms of a written MOA or contract	Student contact information, UH ID number
Sensitive	Data subject to privacy considerations	Date of birth, job applicant records, salary/payroll information, most student information
Regulated	Inadvertent disclosure or inappropriate access requires a breach notification by law or is subject to financial fines	FN or first initial/LN in combination with SSN, driver license number, or bank information; credit card, HIPAA, or financial aid information

Examples of Data / Information by Category

Public	Restricted	Sensitive	Regulated
Student Data • Name • Major field of study • Class (i.e., freshman, sophomore, etc.) **Employee Data** • Name • Job title, description • Business address, phone number • Education and training background • Previous work experience • Dates of first and last employment • Position number, type of appointment, service computation date, occupational group or class code, bargaining unit code	**Student Data** • UH email address/ username • Address (street name and number) • Personal phone number • UH ID card photographs for University use **Student and Employee Data** • UH ID number • Banner PIDM • ODS PIDM	**Student Data** • Gender • Ethnicity • Grades • Courses taken • GPA **Employee Data** • Address (street name and number) • Personal phone number **Student and Employee Data** • Date of birth • Non-UH email address • Job applicant records (names, transcripts, etc.) • Salary and payroll information	**FN and first initial and LN with the following:** • Social Security Number • Driver's license • Hawai‘i ID card number • Financial account (checking, savings, brokerage, CD, etc.), credit card, or debit card numbers **Business/Financial Data** • Payment Card Industry Data Security Standard (PCI-DSS) information **Protected Health Information (PHI)** • Health status • Healthcare treatment • Healthcare payment **Financial Aid Data** • FAFSA data

Technical Guidelines

http://www.hawaii.edu/infosec/techguidelines/



Sensitive

(Unless alternate approved security requrements/plans are filed with the UH Information Security Team)

	Desktop/Workstation	Laptop/Notebook	Handheld Devices*	External Storage Drives*	Server*	Cloud Services*
Device Registration	Required	Required	Required	Required	Required	Required
Physical Security*	Required	Required	Required	Required	Required	Required (check contract)
Logical Access Control*	Required	Required	Required	Required	Required	Required
Anti-Virus	Required	Required	Required	n/a	Required	Required
Firewall	Required	Required	Required	n/a	Required	Required
File Storage Security*	Required	Required	Required	Required	Required	Required
File Transmission Security*	n/a	n/a	n/a	n/a	n/a	n/a
Security Patches	Required	Required	Required	Required	Required	Required
Secure Configuration*	Recommended	Recommended	Recommended	n/a	Required	Required
Vulnerability Scanning	Recommended	Recommended	n/a	n/a	Required (quarterly)	Required (check contract)
Vulnerability Remediation	Recommended	Recommended	n/a	n/a	Required	Required (check contract)
Secure Remote Access*	Required	Required	Required	n/a	Required (via UH VPN)	Required
Logging	Recommended	Recommended	n/a	n/a	Required (ext./comb. format)	Required (ext./comb. format)
Single Purpose Use	Recommended	Recommended	Recommended	Recommended	Recommended	Recommended

Google Drive:

Cannot be used for:

sensitive or regulated information

Institutional Data Governance Principles and Guidelines (1)

- Access to Institutional Data will be based on a need-to-know
- Minimal access will be granted whenever possible
    - i.e., the most restrictive set of permissions and privileges will be granted, and only for the duration needed
- De-identified data will be provided whenever possible
- Duplication of data is discouraged
- Data requested for a specific purpose cannot be used for another purpose, i.e., re-purposed and re-disclosed

Institutional Data Governance Principles and Guidelines (2)

- Data within a record or document will be protected based on the data element with the highest level of sensitivity
- Be aware that a data element may not be personally identifiable, but when combined with other data elements, it may become personally identifiable
- Be aware of small cell sizes in reports
- When accessing data outside of work, do not use unprotected or public wireless connections
- When data is no longer needed—redact, remove, or destroy it!

What Constitutes Personally Identifiable Information (PII) under FERPA

"…information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty."

AP2.215, Mandatory Training and Continuing Education Requirements for Data Users

Requirements	Renewal
Information Security Awareness Training (ISAT)	Every 2 years
General Confidentiality Notice (GCN) acknowledgment	Annually

Other information:

- Both requirements are located at www.hawaii.edu/its/acer
- The training modules are being updated this spring 2018
- Users will be given 2 months advance notice to complete requirements

Who needs to take the training? (1)

1. UH Data Users with access to
   - non-public data AND
   - multiple quantities / bulk records (accessed electronically, on paper, or through other media)

   Note individuals with electronic (view) access to a single record at a time are not required to take the training at this time
2. Those who submit a data sharing request (process where a copy of Institutional Data will be released to an individual who does not normally have access to the data or to a third party)

Who needs to take the training? (2)

- UH personnel with login privileges to Institutional Data Systems (and who have access to bulk records)
  - Examples: Banner/ODS, Peoplesoft/HR Data Mart, KFS/eThority, STAR, Laulima
- Pilot will be ODS in summer 2018
- Those who are requesting login privileges to an Institutional Data System for the first time (and who will have access to bulk records)
- New hires - incorporate training into the onboarding process (future goal)

Questions?

Jodi Ito
Chief Information Security Officer
Office of the Vice President for Information Technology
Information Technology Services
jodi@hawaii.edu
http://www.hawaii.edu/infosec