Cyber Security: What’s the Big Deal?
(and why it matters to you!)

Debasis Bhattacharya, UHMC
Jodi Ito, CISO, UH ITS
maui.hawaii.edu/cybersecurity
What is Cybersecurity?

cy·ber: adjective
of, relating to, or characteristic of the culture of computers, information technology, and virtual reality. "the cyber age“

Cybersecurity: noun
the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.
“Cyber” Affects Everyone!

- Technology is deeply embedded into Critical Infrastructures
- Technology touches every facet of our lives
- Vulnerable to:
  - Losing access to services
  - Losing personal data
  - Financial losses
...why Cybersecurity matters for our State

- Cybersecurity is one of the most strategic threats that Federal, State and private sector industries face in Hawai‘i.

- Operation-critical systems in every sector have a dependency on cyber, which expands capacity and range of capability but also introduces new and evolving forms of vulnerabilities that threaten the security of our infrastructure.

- Hawai‘i is in a very unique position – the U.S. Pacific Command, as well as the Army, Navy, Marine Corps, Air Force and Special Operations Service Commanders are all located here.

- Directly related, Oahu is home of the Pacific’s primary signals intelligence center, the National Security Agency Hawai‘i, and its world-class all-source intelligence center, the Joint Intelligence Operations Center Pacific.
Currents Threats
What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don’t pay in 7 days, you won’t be able to recover your files forever. We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information,
Dridex: Financial Trojan aggressively spread in millions of spam emails each day

Built to harvest the banking credentials of victims, the virulent Dridex is now one of the most dangerous pieces of financial malware in circulation.

By: Dick O'Brien

Created 16 Feb 2016
Security researchers have discovered a new variant of Dridex – one of the most nefarious banking Trojans actively targeting financial sector – with a new, sophisticated code injection technique and evasive capabilities called "AtomBombing."
Exclusive: SWIFT confirms new cyber thefts, hacking tactics
**WHAT IS SPEARPHISHING?**

Spearphishing is a tool (among many) used by attackers to penetrate a company’s network to facilitate a targeted attack through malicious emails. It is also the most commonly used and successful method - 95% of all successful targeted attacks were made via spearphishing.

1.攻撃者は、ターゲットの会社内の個人の情報収集
2.攻撃者は、ターゲットに特別作成されたメールメッセージを送信。メールは、ターゲットのメール共有フォルダに開きます。メールに含まれるマルウェアの添付ファイルまたはリンクが含まれる場合があります。
3.ターゲットは、メールをインボックスに受信し、メールに含まれるマルウェアの添付ファイルまたはリンクをクリックします。
4.添付ファイルまたはリンクは、ターゲットにアクセスを提供し、システムを攻撃します。両方のスキャナで、ターゲットのシステムが攻撃者にアクセスを提供し、システムとネットワークにアクセスします。
Almost three quarters (74 percent) of Dridex spam campaigns used real company names in the sender address and frequently in the email text. The vast majority of spam campaigns were disguised as financial emails, such as invoices, receipts, and orders. The spam was heavily focused on English speakers, with the majority of emails purporting to come from English-speaking companies.

**Victims**

Dridex is mainly used to steal banking credentials. The malware is configured to target the customers of nearly 300 different organizations in over 40 regions.

Dridex is heavily focused on customers of financial institutions in wealthy, English-speaking countries, with the majority of targeted organizations located in these countries. The attackers also prioritized other European nations, along with a range of Asia-Pacific regions.
March 20, 2017

Report: Dark web vendor selling millions of Gmail and Yahoo accounts

The dark web vendor SunTzu583, which was recently discovered selling over one million Gmail and Yahoo accounts along with their decrypted passwords, is now selling tens of millions more, HackRead has reported.

According to the report, one of SunTzu583’s new listings is offering approximately 21.8 million compromised Gmail accounts for $450.48 – 75 percent of which, the vendor claims, include decrypted passwords (the other 25 percent feature hashed passwords). HackRead has confirmed that this data was aggregated from past breaches of Nulled.cr, MPGH.net, and Dropbox.

A separate set of SunTzu583 listings is offering up to 5 million Gmail accounts – $300.49 for the full data set or $125.48 for half. HackRead has determined that these compromised accounts stem primarily from the 2014 breach of Russian's Bitcoin Security Forum, but also from the LinkedIn and Adobe breaches.

In a third listing, SunTzu583 is selling over 5.7 million Yahoo users accounts – offering a third of the data set of $100.48, or the entire lot for $250.48. The vendor claims that each listing contains unique accounts – "however, after scanning the sample data, we found the majority of accounts were disabled while some were still working and stolen from MySpace, LinkedIn and Adobe data breaches," HackRead reported.
Hackers hit D.C. police closed-circuit camera network, city officials disclose

Hackers infected 70 percent of storage devices that record data from D.C. police surveillance cameras eight days before President Trump’s inauguration, forcing major citywide reinstallation efforts, according to the police and the city’s technology office.

City officials said ransomware left police cameras unable to record between Jan. 12 and Jan. 15. The cyberattack affected 123 of 187 network video recorders in a closed-circuit TV system for public spaces across the city, the officials said late Friday.
Own a Vizio TV? It May Have Spied on You

BY TOM BRANT  FEBRUARY 6, 2017 03:53PM EST  22 COMMENTS

Vizio secretly collected viewing data from 11 million TVs, according to an FTC complaint.

Vizio has been watching you watch TV. The flat-panel display maker, which was acquired last year by Chinese giant LeEco, will pay $2.2 million to settle claims that it collected viewing data from 11 million TVs without their owners' consent.

According to a complaint from the Federal Trade Commission, Vizio was able to capture second-by-second information about what its TVs were displaying. The monitoring wasn't limited to built-in smart TV apps, either. It included video from cable set-top boxes, DVD players, and over-the-air broadcasts. Vizio also recorded and tracked the TVs' IP addresses, according to the FTC complaint.
The cost of cybercrime could reach $6 trillion by 2021 (global annual cybercrime costs has been estimated $3 trillion in 2015).

The global cost of cybercrime continues to increase, this isn’t a surprise due to the intensification of this kind of illegal practice. According to an analysis conducted by Cybersecurity Ventures, the cost of cybercrime could reach $6 trillion by 2021 (global annual cybercrime costs has been estimated $3 trillion in 2015).

Default Passwords Online

- https://cirt.net/passwords
- http://www.defaultpassword.com/
US-CERT Enterprise Recommended Mitigations

- **Application whitelisting** – helps prevent malicious software and unapproved programs from running

- **Patch applications** – e.g., Java, PDF viewers, Flash, web browsers, Microsoft Office

- **Patch operating system vulnerabilities** – used for extreme risk vulnerabilities
Enterprise Recommendations cont.

- **Control administrative privileges** – based on user roles & responsibilities; secure remote access; use strong passwords; monitor logs

- **Network segmentation and segregation into security zones** – helps protect sensitive information & critical services
Recommendations

- Know your adversary
- Know your assets – hard & soft
  - Know & understand your network
  - Know what technologies are being used and why
  - Know your data and how it is used; know what needs to be protected
  - Know your business processes
Enterprise Security Considerations

- Have a robust security program (e.g. NIST 800-53 or NIST 800-171)
- Develop a robust security awareness program
- Stay abreast of threats and trends
It’s not if... it’s WHEN

- Assume you WILL be breached or have a “cyber” incident
- DR & BC situation
- Incident Response Plan (& practice it!)
  - Chain of Command
  - Reporting Requirements
  - Communications Plan
Top 10 Cyber Security Practices

- Recognize that YOU AND YOUR DEVICES are a target; know the threats
- Apply operating system and application updates frequently and regularly
- Install and update protective software such as anti-virus software
More… (#4-7)

- Practice good password management; use STRONG passwords
- Never leave your devices logged-in & unattended; control access to your machines
- Use email & the Internet safely; be careful when clicking on attachments or links in email
- Use a secure network for sensitive transactions
Last 3... (#8-10)

- Back up your data regularly and protect sensitive information
- Monitor your accounts for suspicious activity
- Be careful what you share online & on social media (know your digital footprint)
Email Address Exposure

- Check if your email address has been exposed:
  - https://haveibeenpwned.com
';--have i been pwned?

Check if you have an account that has been compromised in a data breach

jodi@hawaii.edu

Oh no — pwned!

Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)

Notify me when I get pwned  Donate

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords