James Craig
Dean of Business and Information Technology
Pima Community College
jcraig7@pima.edu

Chris Bonhorst
Academic Director of Information Technology
Pima Community College
cbonhorst@pima.edu

Will McCullen
Program Manager, IT Center of Excellence
Pima Community College
jwmccullen@pima.edu

FAZIO MECHANICAL + TARGET = - $292,000,000

A small Australian subcontractor on a project had not changed its Windows passwords from the defaults “admin” and “guest.”

=

Current Items of concern:

China Activity Increase CISA alert Oct 1, 2020

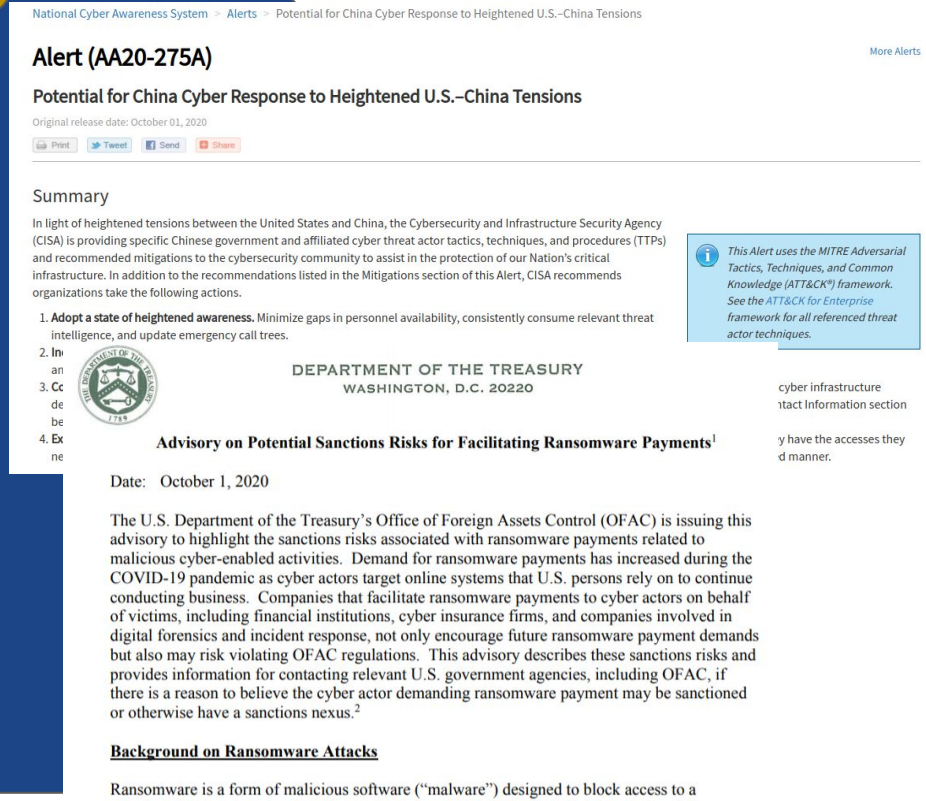
Intent:

- Steal Intellectual Property and Identities
- Suppress perspectives they deem dangerous
- **Harm regional and international opponents**

Every business is a target. On average only 40% that fall victim to a major breach survive.

If **Economic Disruption** is the target, and it is, then so are **YOU!**

October 1, 2020 advisory:
Paying ransomware may put you at risk for violation of OFAC regulations and sanctions.



National Cyber Awareness System > Alerts > Potential for China Cyber Response to Heightened U.S.–China Tensions

Alert (AA20-275A)

More Alerts

Potential for China Cyber Response to Heightened U.S.–China Tensions

Original release date: October 01, 2020

Print | Tweet | Send | Share

Summary

In light of heightened tensions between the United States and China, the Cybersecurity and Infrastructure Security Agency (CISA) is providing specific Chinese government and affiliated cyber threat actor tactics, techniques, and procedures (TTPs) and recommended mitigations to the cybersecurity community to assist in the protection of our Nation's critical infrastructure. In addition to the recommendations listed in the Mitigations section of this Alert, CISA recommends organizations take the following actions.

1. **Adopt a state of heightened awareness.** Minimize gaps in personnel availability, consistently consume relevant threat intelligence, and update emergency call trees.

This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[2]

Background on Ransomware Attacks

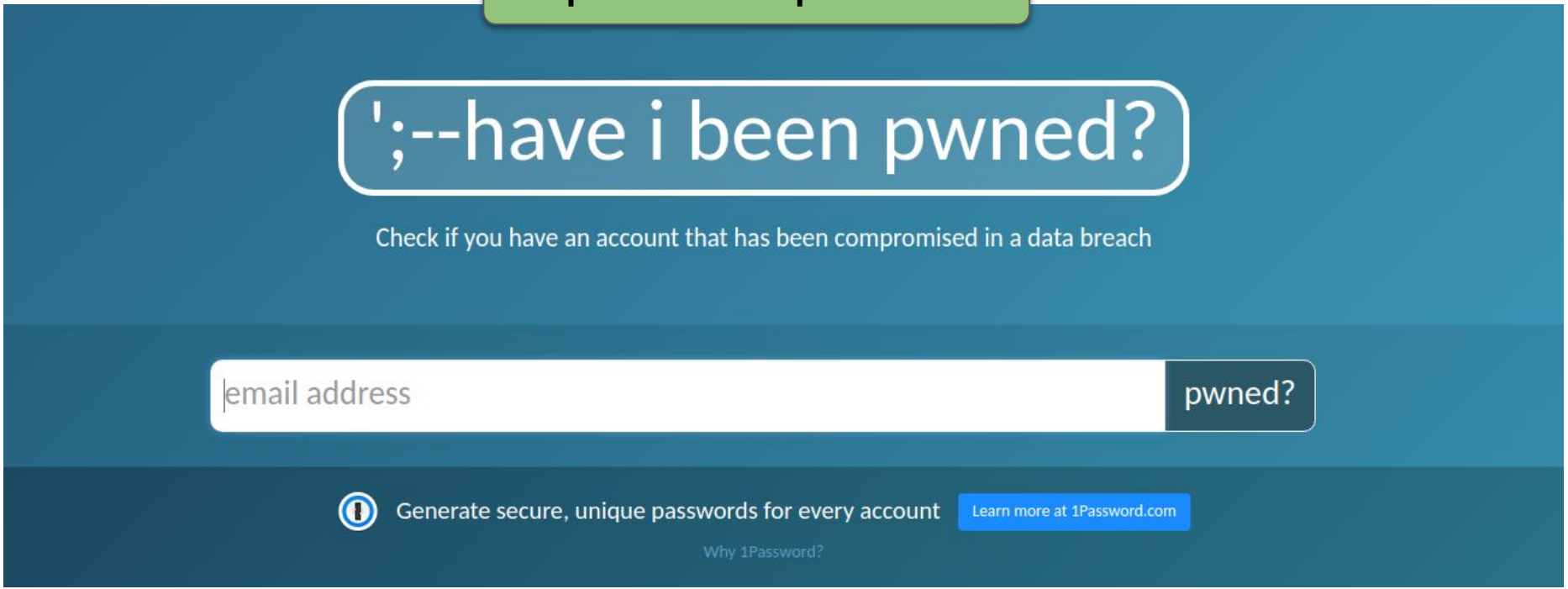
Ransomware is a form of malicious software ("malware") designed to block access to a

Links:
US Treasury: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
DHS CISA: Potential for China Cyber Response to Heightened U.S.–China Tensions https://us-cert.cisa.gov/ncas/alerts/aa20-275a

QUICK ACTIVITY

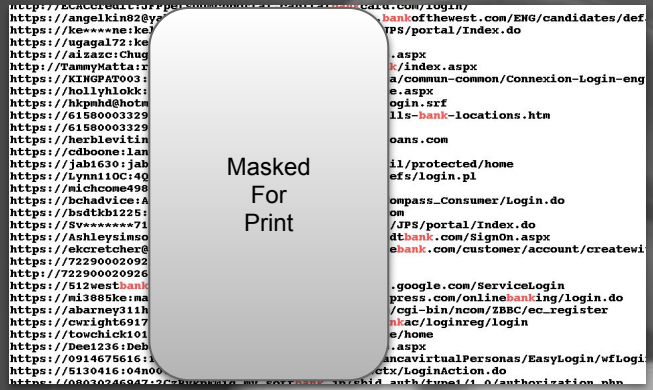
Go to:

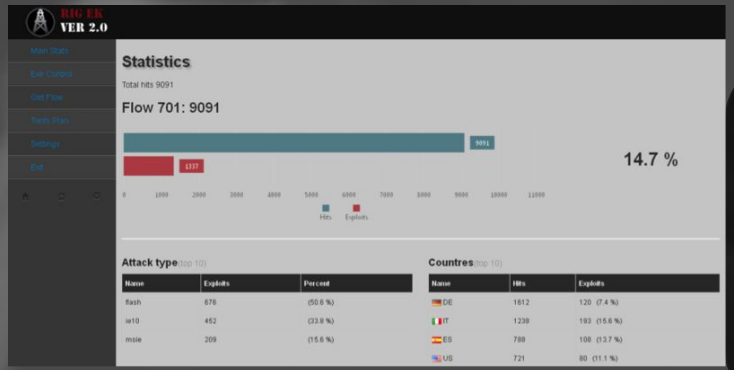
http://haveibeenpwned.com



Attacking is easy with inexpensive and accessible tools

1. Buy malware on the Dark Web
2. Get a cryptor
   Malware bypasses Antivirus





3. Get a Vulnerability attack kit
4. Buy space on hacket web sites

These methods are very effective and inexpensive!

Internet of Things
Good idea?

HUFFPOST

NEWS

Millions Of Private Messages Between Parents And Kids Hacked In Cloud Pets Security Breach

Passwords and emails have also been leaked.

Hello Barbie, Can We Talk About Your Security Issues?

By Richard Adhikari
Dec 8, 2015 9:27 AM PT

Security firm talks safety cam hacked and posted o

By: Danielle Radin
Posted: Aug 12, 2016 10:38 PM PDT
Updated: Aug 13, 2016 12:51 PM PDT

Tech

Alexa, have you been hacked? New research found major security flaws in Amazon's virtual assistant.


New research from security firm Check Point finds flaws in the security of Amazon's Alexa virtual assistant.

IMAGE: JOBY SESSIONS / GETTY

BY MATT BINDER

"Alexa, is a hacker listening to everything I say to you?"

figured out how to infect smart thermostats with ransomware.

Working from home.

Why It's Time Boards Treated Cyber Security Risk Like Financial Risk

cbronline.com • 7 min read

'Alarming' rate of cyberattacks aimed at major corporations, governments and critical infrastructure amid COVID-19: Report

abcnews.go.com • 2 min read

296 views | Sep 8, 2020, 07:40am EDT

Work From Home Is Not Without Security Costs

Forbes

Itzik Kotler Forbes Councils Member

Forbes Technology Council COUNCIL POST | Paid Program

Innovation

Co-Founder & CTO at SafeBreach. I'm a father, husband, hacker, open source enthusiast and entrepreneur.

GETTY

Common Attack Lifecycle

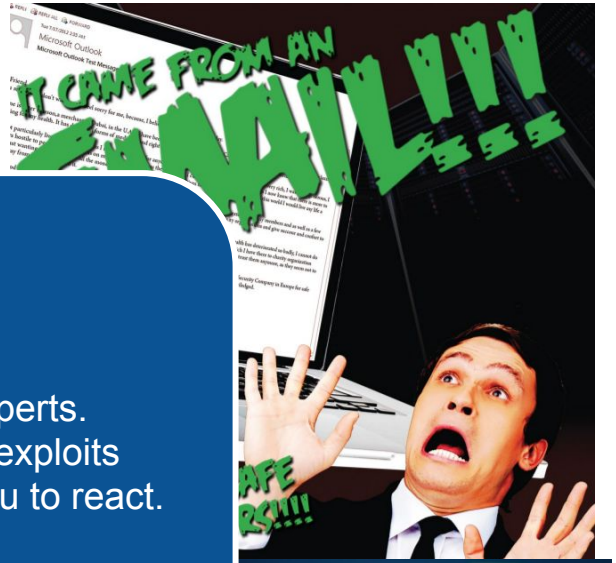
Business Network

Your clients

Data or $$$
-or both-

Infected Home Computer with a corporate VPN connection

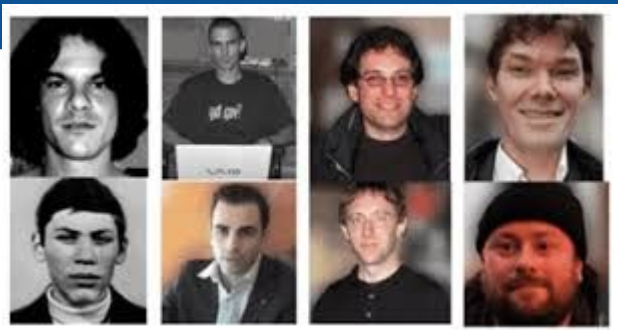
Security awareness training ….a must.

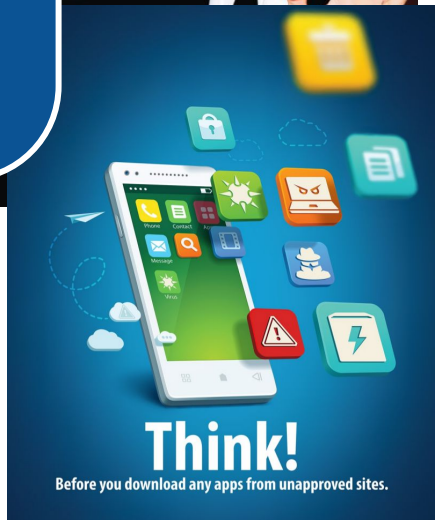


Hackers today are not just talented individuals. They are teams.

Hackers + HR + Facilities + Accountant + Subject matter experts.
Bots = Automated programs searching and using common exploits
Machine Learning using the best known methods to get you to react.

Security awareness now means ...think like a hacker.
Ask yourself, **“How would I fool someone?”**





https://securityawareness.usalearning.gov/

Our culture HAS to change

Everyone is part of the cybersecurity team

Social Engineering mindset

- **Who might be manipulating you?**
- **How would you break in?**

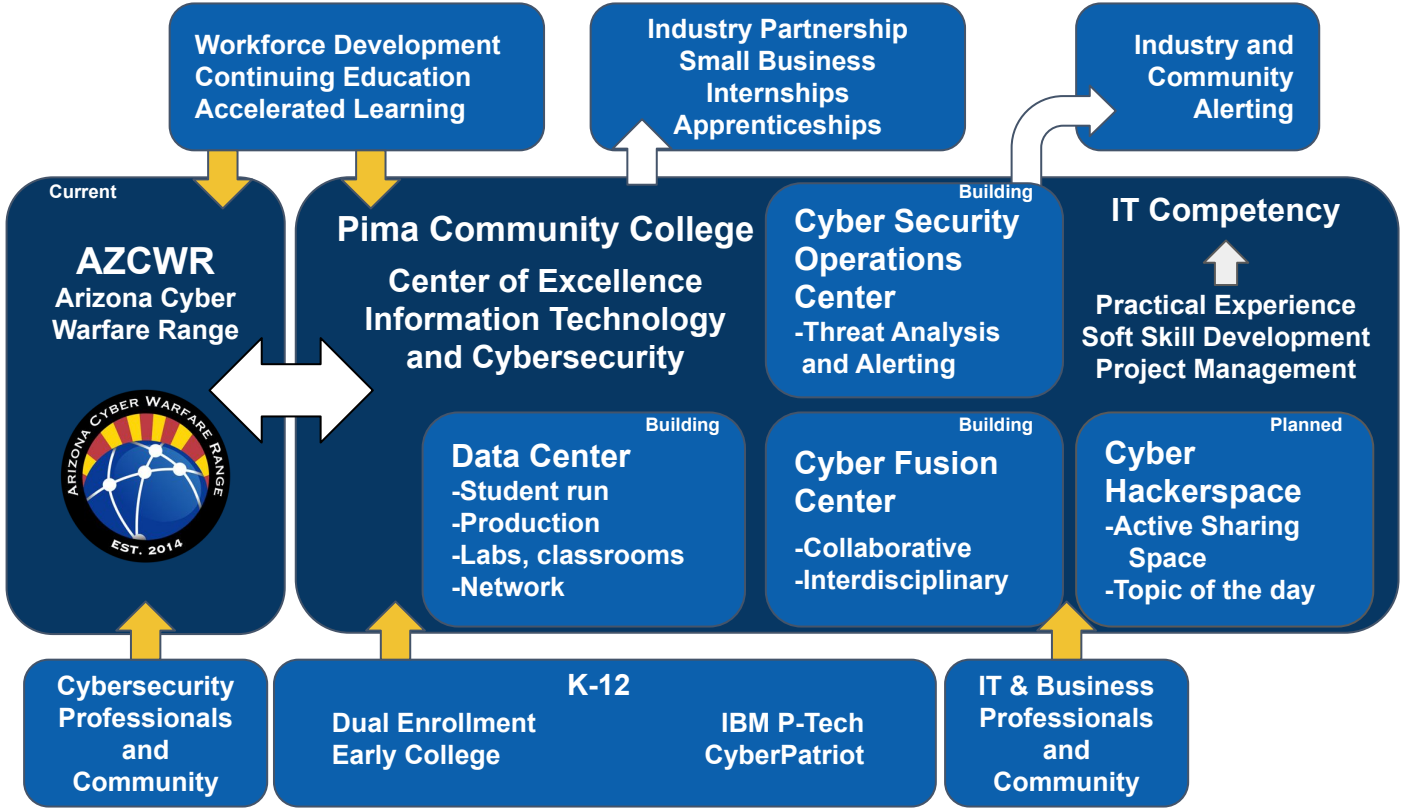
If a hacker can get you angry…

They can OWN you!

(social media, forums, email)

What you think might be a person posting, could **very likely** be a programmed bot and not a person at all. They are designed to either get you, or to destabilize the country.

PimaCommunityCollege



Additional Resources

Small business Cybersecurity Corner - https://www.nist.gov/itl/smallbusinesscyber

FTC - https://www.ftc.gov/tips-advice/business-center/small-businesses/

Stop. Think. Connect. - https://www.stopthinkconnect.org/

National Cybersecurity Alliance -https://staysafeonline.org/

Center for Development of Security Excellence - https://securityawareness.usalearning.gov/

You can HACK it at Pima!

Hack ...to protect

ARIZONA CYBER
WARFARE RANGE

Revolutionary advancements in
cybersecurity happen here.
www.azcwr.org

Questions?