NASAA

Cybersecurity Compliance and Best Practices and Other Cyber Stuff

Fighting Back

- Led by Retired US Secret Service Agent K. Gus Dimitrelos & former National Security Agency Analyst Steven A. Williams
- Conducted more than 3000 Cyber and Cellular Investigations since 1996 for more than 40 state, federal, and international law enforcement agencies including:
  - US Secret Service - USSS
  - Federal Bureau of Investigations – FBI
  - Immigration Customs Enforcement - US-ICE
  - Environmental Protection Agency - EPA
  - Drug Enforcement Administration – DEA
  - Alcohol Tobacco and Firearms – ATF
  - Mexican Federal Police
  - Jamaican National Police
  - Colombian CTI and DIJIN

Department of State
Cyber anti-Terrorism Program

Subject Matter Experts for the US State Department, Cyber anti-Terrorism and Bureau of International Narcotics and Law Enforcement Affairs (INL) Program and have completed over 100 task orders in more than 30 countries including:

Jamaica, Pakistán, Kenya, Uganda, Bosnia, Bahamas, Mexico, Chile, Uruguay, Ecuador, Turkey, Colombia, Antigua, Trinidad, Malaysia, Philippines, Indonesia, Thailand, India, Egypt, Azerbaijan, Jordan, Morocco, Bahrain, Greece

Breach Cost

Breach Calculator

- It is estimated that in the US this many firms will have a material cyber breach in the next 24 months?
  - 27.7%
- The average cost for a material breach was?
  - 7.35 million
- In the United States who causes the most breaches?
  - 59% hackers and criminal insiders
- Average number of records lost in each hack
  - 28,512 per hack Also the more records lost, the higher the cost of the data breach
- What industries have the highest costs related to breaches?
  - Answer Financial, Health and Service industry

Breach Cost

- Direct or indirect costs for a breach which is the most expensive in the U.S.
  1. Indirect costs 146 billion (EE time lost)
  2. 79 billion is expert help regarding computer system
- Number one loss factor for financial services is?
  - Churn rate, Loss of customers
- Top factors in causing a breach are?
  1. Compliance failures
  2. Use of mobile platforms
  3. Employees not following procedures
- Key factors in reducing the costs of a breach
  1. Incident response team (#1 factor is how fast can I stop the breach)
  2. Use of encryption
  3. Employee training
- These above three factor reduce data breach costs by?
  - 47%

Breach Cost

- The number four things that increase the cost of a breach are?
  1. Third party involvement
  2. Cloud migration
  3. Compliance failures (employees) and
  4. Mobile platforms.

- These four factors increase the costs of a breach by?
  - 51%

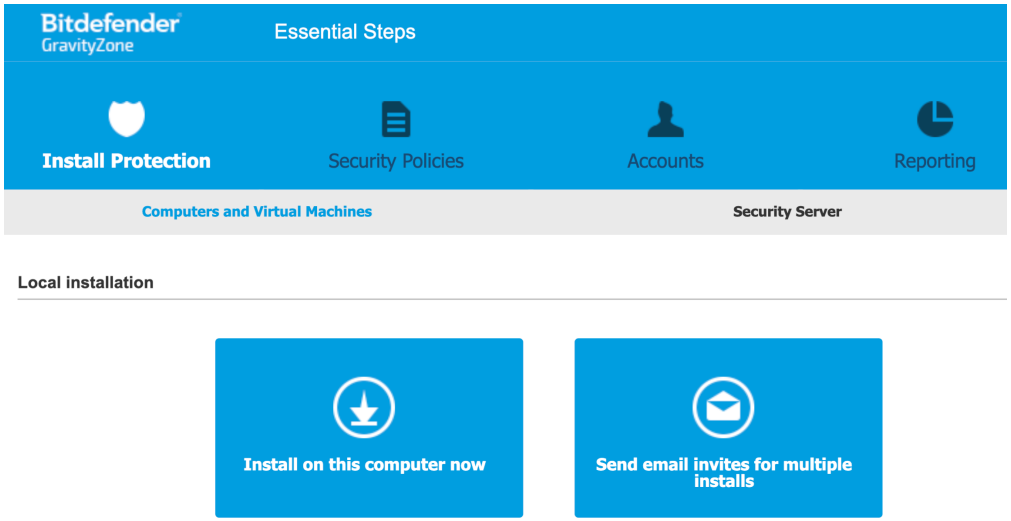
Gaining Knowledge - Firewalls

Fighting Back - Home Firewalls

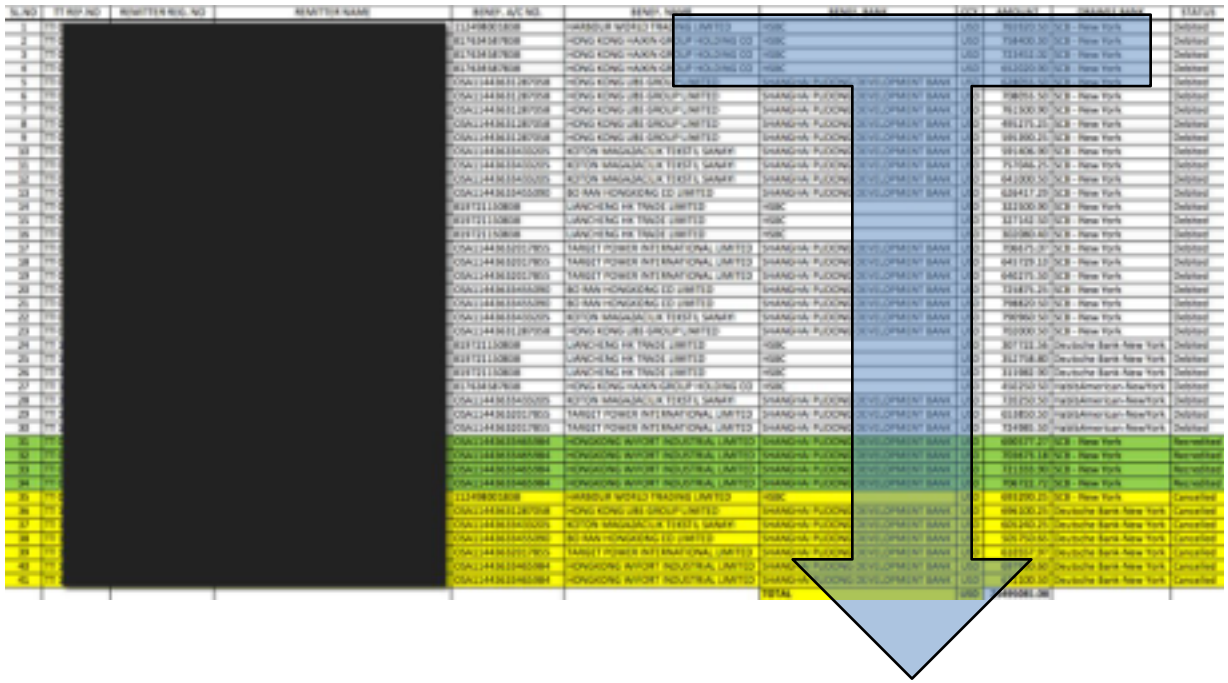
	Cujo	Dojo	RATtrap	BitdefenderBox 2
Price	$99	$199	$199	$249
Best For	Protecting your home network, including smart home devices.	Protecting your smart home devices.	Protecting your home network, including smart home devices.	Protecting your home network, including smart home devices.
How It Protects You	Smart Firewall, Anti-Virus, Anti-Malware	Analyzes Metadata	Tracks Malicious Websites and Analyzes Packet Metadata	Analyzes Packet Data, Behavioral Analysis, Brute Force Attack Protection
Works with Wi-Fi Devices	Yes	Yes	Yes	Yes
Ethernet	Yes	Yes	Yes	Yes
Monthly or Yearly Service Fee	$8.99/month or $59/year	$9.99/month or $99/year (includes a 1-year subscription)	$9/month	$99/year
Optional Lifetime Service Fee	$150	No	No	No
Can you use the system without paying for a subscription?	No, you cannot.	Yes, but limited updates, limited reporting, and no support.	No, you cannot.	No, you cannot.

Fighting Back - Anti-Everything

- Even though anti-malware software can be defeated, not having it installed, running and up-to-date is not an option
- Identify software which is multi-platform and easy to manage
- In 24 years have never endorsed a single product but after testing Bitdefender GravityZone I was extremely impressed with its business endpoint protection, alerting and reporting functions
- We are not resellers of the product and can only refer you to our contact persons to discuss its functions and costs
- Rob CHOMKO rchomko@bitdefender.com
- Joseph SYKORA jsykora@bitdefender.com
- Elia COHEN ecohen@bitdefender.com



Banks Accounts are Being Emptied



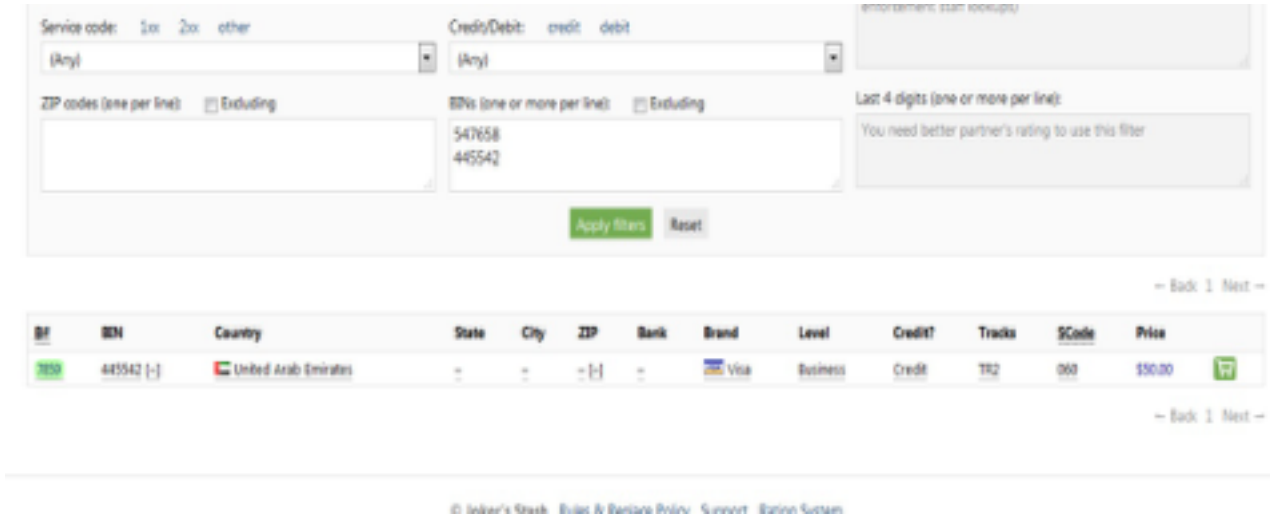
BENEF. NAME	BENEF. BANK	CCY	AMOUNT	DRAWEE BANK	STATUS
HARBOUR WORLD TRADING LIMITED	HSBC	USD	765920.50	SCB - New York	Debited
HONG KONG HAIXIN GROUP HOLDING CO	HSBC	USD	758400.30	SCB - New York	Debited
HONG KONG HAIXIN GROUP HOLDING CO	HSBC	USD	723452.02	SCB - New York	Debited
HONG KONG HAIXIN GROUP HOLDING CO	HSBC	USD	652020.90	SCB - New York	Debited
HONG KONG UBS GROUP LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	628055.50	SCB - New York	Debited

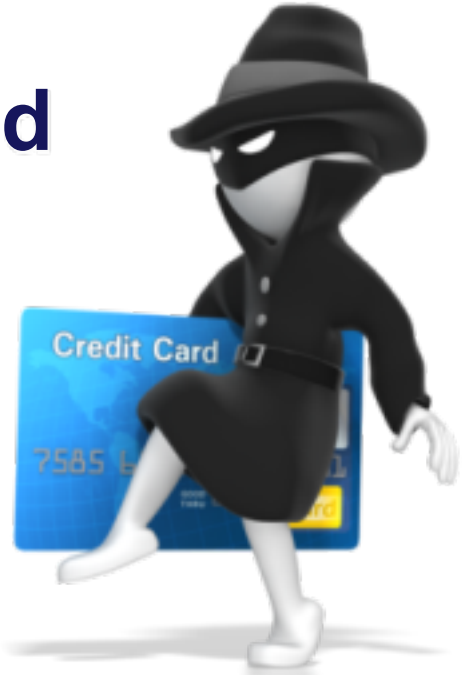
Current SWIFT fraud investigation revealed over 25M Stolen

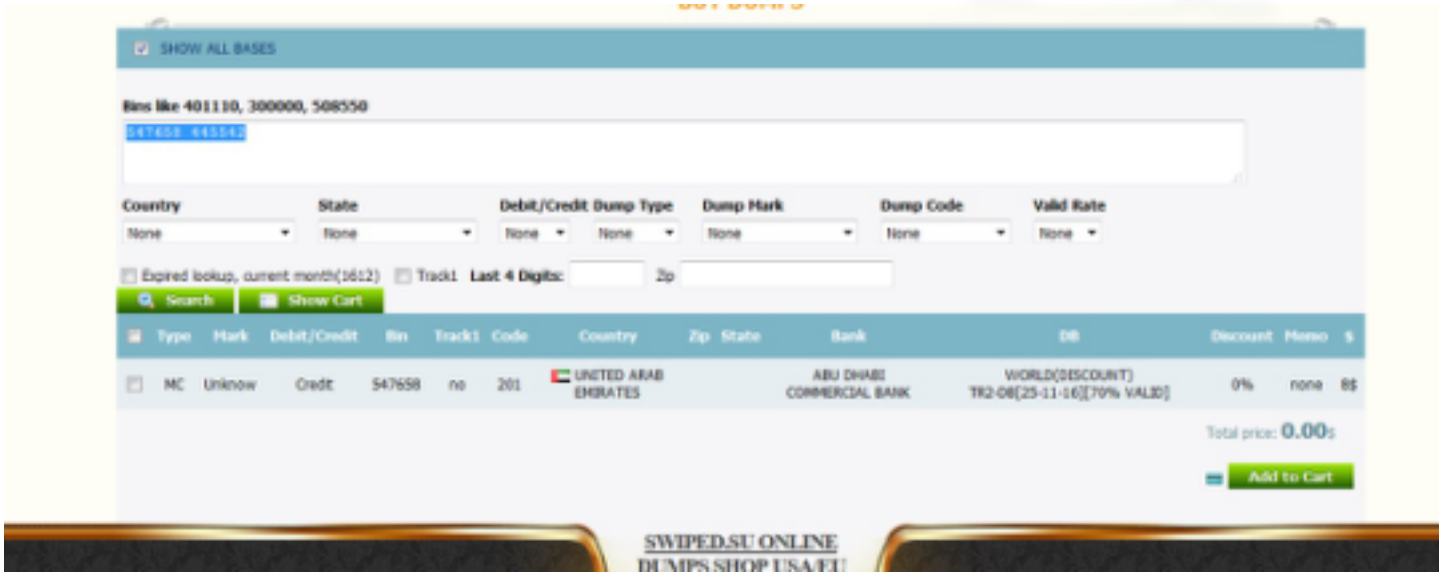
The Dark Web

"Where illegal activity is openly the new normal"

Financial **Data is Being Sold**







How Financial Institutions and Clients are Being Compromised

Attachments and Trusted Documents

Accounts Payable Ledger

Tip: Set your beginning balance in the first row.

ACCOUNT 1

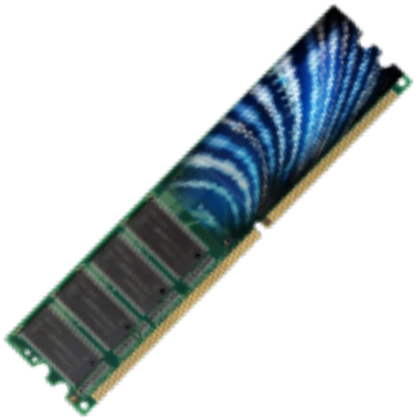
DATE	REFERENCE	TYPE	MEMO	ACCOUNT	DEBIT	CREDIT	BALANCE
2/2/12	Beginning Balance						$5,015,321.00
2/2/12	1003	Payment	Invoice 3	500 Cash in bank	$1,500.00		$5,016,821.00
2/2/12	1003	Payment	Invoice 3	550 Accounts payable		$140.00	$5,016,681.00
2/17/12	111	Purchase	Invoice 111	550 Accounts payable	$200.00		$5,016,881.00
2/17/12	111	Purchase	Invoice 111	120 Uniforms		$200.00	$5,016,681.00
2/27/12	1009	Payment	Invoice 9	500 Cash in bank	$450.00		$5,017,131.00
2/27/12	1009	Payment	Invoice 9	550 Accounts payable		$450.00	$5,016,681.00
2/28/12	1003	Payment	Invoice #3 final	550 Accounts payable		$10.00	$5,016,671.00
				Ending Balance	**$2,150.00**	**$800.00**	**$5,016,671.00**

ACCOUNT 2

DATE	REFERENCE	TYPE	MEMO	ACCOUNT	DEBIT	CREDIT	BALANCE
2/15/12	Beginning Balance						$602,448.00
2/15/12	112	Purchase	Invoice 112	550 Accounts payable		$650.00	$601,798.00

International Hackers Targeting Financial Institutions

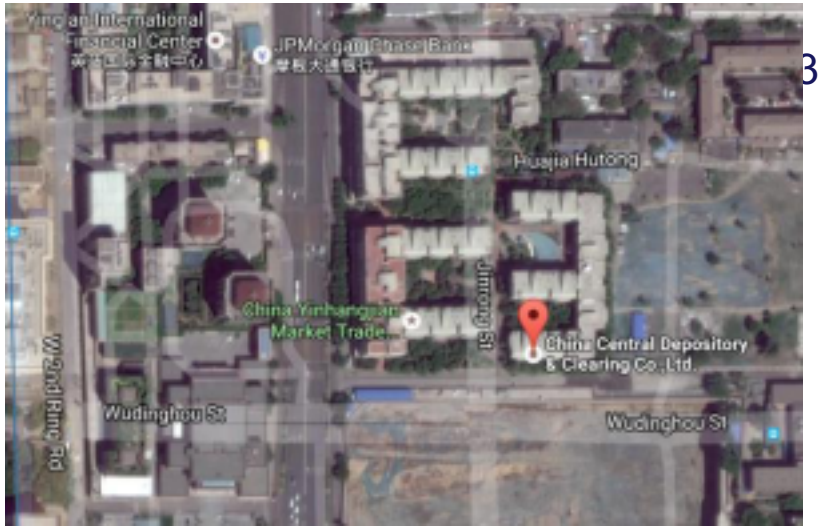
Case Study #1: Memory resident malware was executed in RAM and processes are hidden and not identified by Malware scanners, AV, or IT **Financial accounts and passwords were actively being captured at a Bank in the UAE. Below is the capture data destination and source of stolen info:**



Hacker commands
and stolen data information:

.CREATE TEXT FTP.TXT

IP Address: 202.108.90.13
Country: China (CN)
City: Beijing
China Government Securities Depository



Targeting Your Financial Accounts

Phishing Campaigns

- Creating your own company phishing campaign will prevent employee point and click mistakes and breaches
- One recommendation is to research options such as the company below

- https://www.knowbe4.com/

Malware Defection or Detection

Password Capturing

Case Study #2: MIMIKATZ was installed to capture Admin passwords on a regional university. Mimikatz is and easy tool to gather credential data from Windows.

Suspect used weaponized USB with exploits tools to capture volatile data (Passwords, Credentials, Etc.)

What's the safest computer in the world?

Weaponized USBs can:

- Scan powered-off computers, including Windows, Apple, and Linux

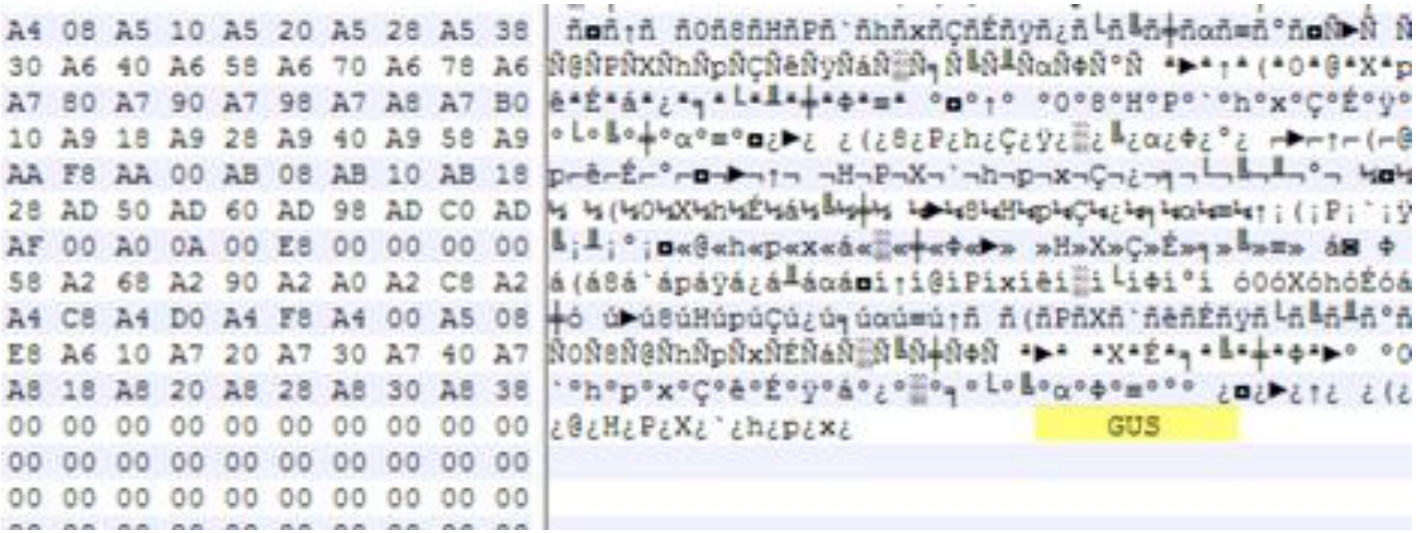
Problem with anti-Virus and anti-Malware

POLYMORPHIC – OBFUSCATION

MIMIKATZ Original Digital Fingerprint:
f3eb271434185f8c5c2cc80f90ce0ca1

By changing the Malware signature, AV Software will not detect it.

Digital Fingerprint Changed using free Hex Editor:
3ababf95703545db30b6d8a1705251ed



Self-Diagnosis

Pay *MORE* Attention to the Obvious Issues

- Failed Logins
- Unexpected shut down or restart of systems
- Stops / Restarts of applications
  - Enabling and disabling the firewall
  - AV and malware scanner stopped/started
  - Running and stopping of processes

Windows Defender Advanced Threat Protecti...	Windows D...		Manual	Local Syste...
Windows Defender Network Inspection Service	Helps guard...		Manual	Local Service
Windows Defender Service	Helps prote...	Running	Automatic	Local Syste...
Windows Driver Foundation - User-mode Dri...	Creates and...	Running	Manual (Trig...	Local Syste...
Windows Encryption Provider Host Service	Windows E...		Manual (Trig...	Local Service
Windows Error Reporting Service	Allows error...		Manual (Trig...	Local Syste...
Windows Event Collector	This service ...		Manual	Network S...
Windows Event Log	This service ...	Running	Automatic	Local Service
Windows Firewall	Windows Fi...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes p...	Running	Automatic	Local Service
Windows Image Acquisition (WIA)	Provides im...		Manual	Local Service

How We Respond To eMail

Most Effective Hack is "Real" Email

From: **Elias Dimitrelos** <elias@cyberforensics360.org>
Date: Mon, Nov 14, 2016 at 12:10 PM
Subject: Re: Please Review PDF
To: gus@cyberforensics360.org

1

I tried sending you a document but failed, saying file too large. so, I have sent you a file using PDF.

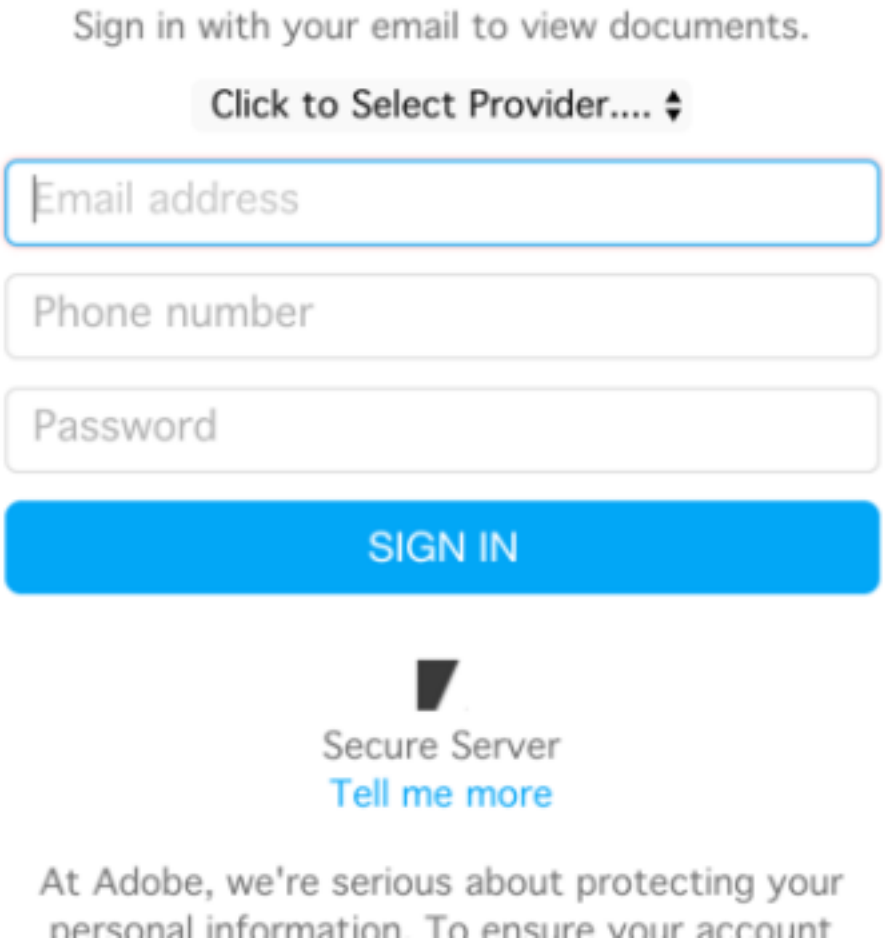
To view file online CLICK HERE

2

Elias Dimitrelos
Chief Financial Officer
+1.251.202.9237
elias@cyberforensics360.org
Cyber Forensics 360
7450 Griffin Rd
Davie, FL 33314-4104

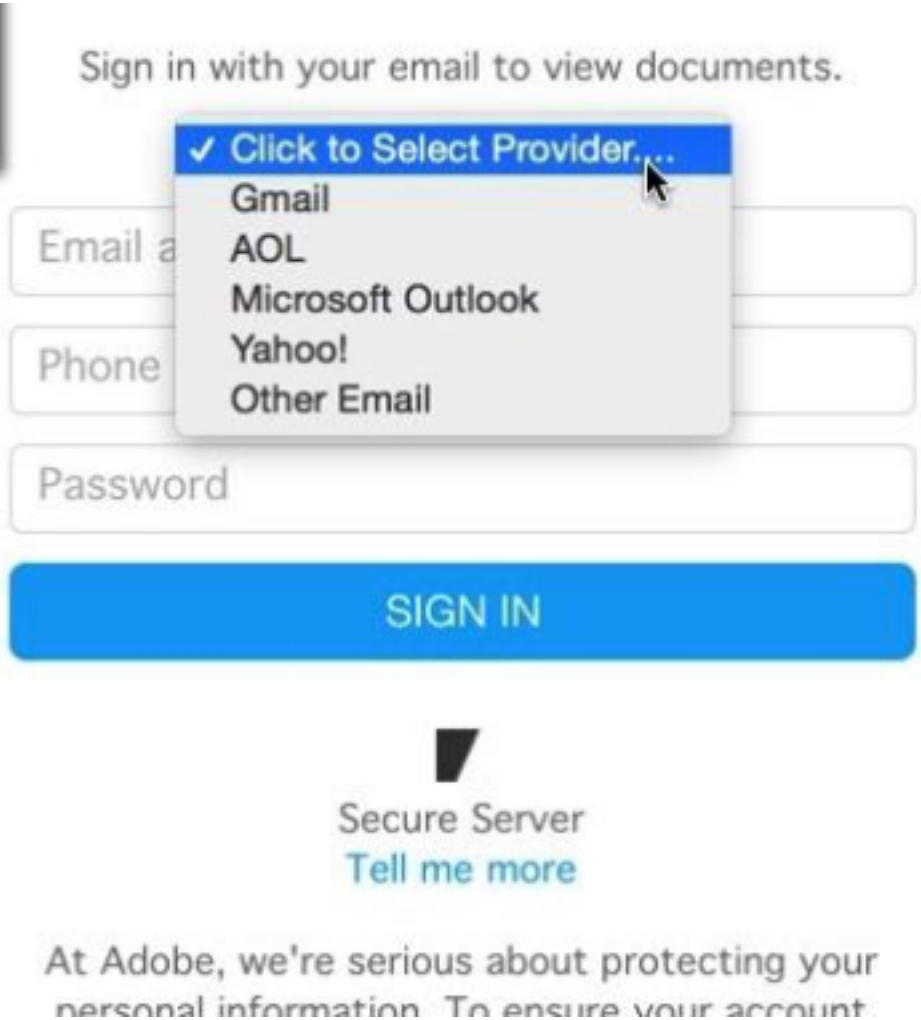
3

Which Leads To Normal Login Screen



To a Common File Downloading Account

Login using your own email credentials



Gaining Knowledge - Headers

I received an email which appeared to come from Elias but the message which read, "the attachment was too large", caught my attention since we have unlimited data with Google Corporate and any large attachments would have come from our GDrive not an outside link.

```
Delivered-To: gus@cyberforensics360.org
Received: by 10.64.66.195 with SMTP id h3csp1180426iet;
        Mon, 14 Nov 2016 10:11:01 -0800 (PST)
X-Received: by 10.99.55.30 with SMTP id e30mr71104305pga.75.1479147061676;
        Mon, 14 Nov 2016 10:11:01 -0800 (I
Return-Path: <sjferalin@c21affiliated.com>
Received: from p3plwbeout06-01.prod.phx3.secureserver.net (p3plsmtp06-01-2.prod.phx3.secureserver.net.
[97.74.135.56])
        by mx.google.com with ESMTPS id b7si23146168pfd.39.2016.11.14.10.11.01
        for <gus@cyberforensics360.org>
        (version=TLS1_2 cipher=AES128-SHA bits=128/128);
        Mon, 14 Nov 2016 10:11:01 -0800 (PST)
Received-SPF: pass (google.com: domain of sjferalin@c21affiliated.com designates 97.74.135.56 as permitted sender)
client-ip=97.74.135.56;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of sjferalin@c21affiliated.com designates 97.74.135.56 as permitted sender)
smtp.mailfrom=sjferalin@c21affiliated.com
Received: from localhost ([97.74.135.17]) by p3plwbeout06-01.prod.phx3.secureserver.net with bizsmtp id
7uB11u0010NhUdt01uB1YF; Mon, 14 Nov 2016 1
X-SID: 7uB11u0010NhUdt01
Received: (qmail 27588 invoked by uid 99); 14 Nov 2016 18:11:01 -0000
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="utf-8"
X-Originating-IP: 72.10.33.117
User-Agent: Workspace Webmail 6.5.5
Message-Id: <20161114111059.09ce04728f096a2fb6e682edd325fd5d.60ce4a8b34.wbe@email06.godaddy.com>
From: Elias Dimitrelos <elias@cyberforensics360.org>
X-Sender: sjferalin@c21affiliated.com
Reply-To: Elias Dimitrelos <ldph231@gmail.com>
To: gus@cyberforensics360.org
Subject: Re: Please Review PDF
Date: Mon, 14 Nov 2016 11:10:59 -0700
Mime-Version: 1.0
```

The hacker used a person's hacked email account which is listed as a permitted sender on Gmail.

Domain is a GoDaddy Site belonging to a legitimate business domain c21affiliated.com

sjferalin@ email account was compromised and sent this malicious PDF LINK attachment.

The email appeared to come from Elias@CyberForensics 360.org account but even I replied to verify legitimacy, my message would have gone to a fake gmail forwarding account and person who probably would have replied back "yes".

100% Use of Two Factor Authentication

2FA/2FV

- Two factor authentication has been in operation for more than 5 years
- 100% Authentication Verification
- https://twofactorauth.org

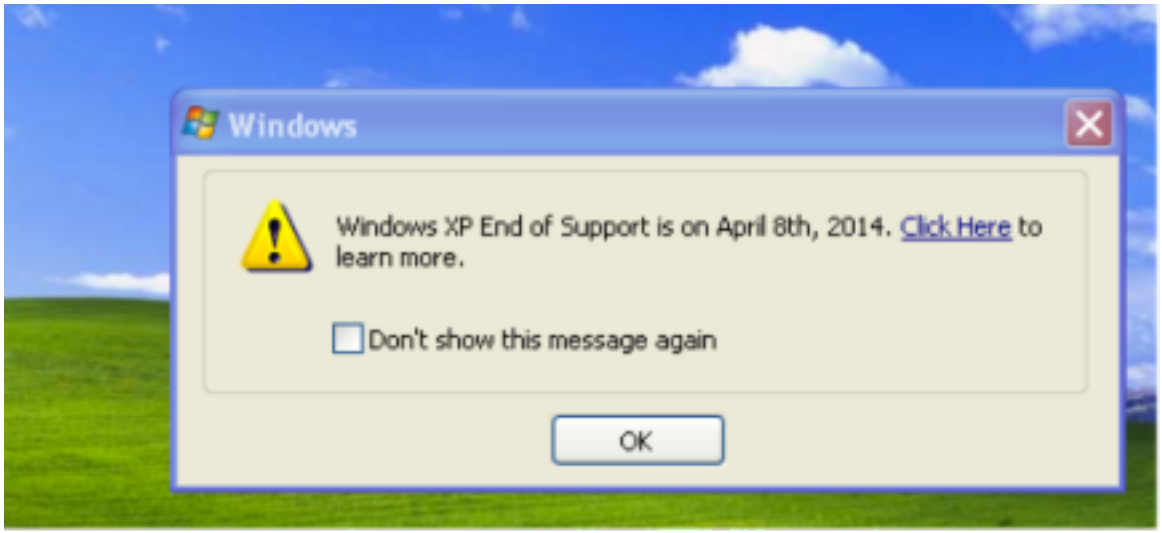
Gaining Knowledge - Patches

After All I Presented Do We All Wannacry #Petya

Déjà vu with NotPetya and the next ransomware strain.

July 4th NOTPetya strain authors asked for 100 bitcoin payments (roughly $256,000) in exchange for the private key to decrypt files encrypted with the NotPetya ransomware. They provided a link to a dark web chatroom where people could contact them.

Since 2015, Our Assessments reveal all XP Systems are Compromised… Windows 7 to Follow

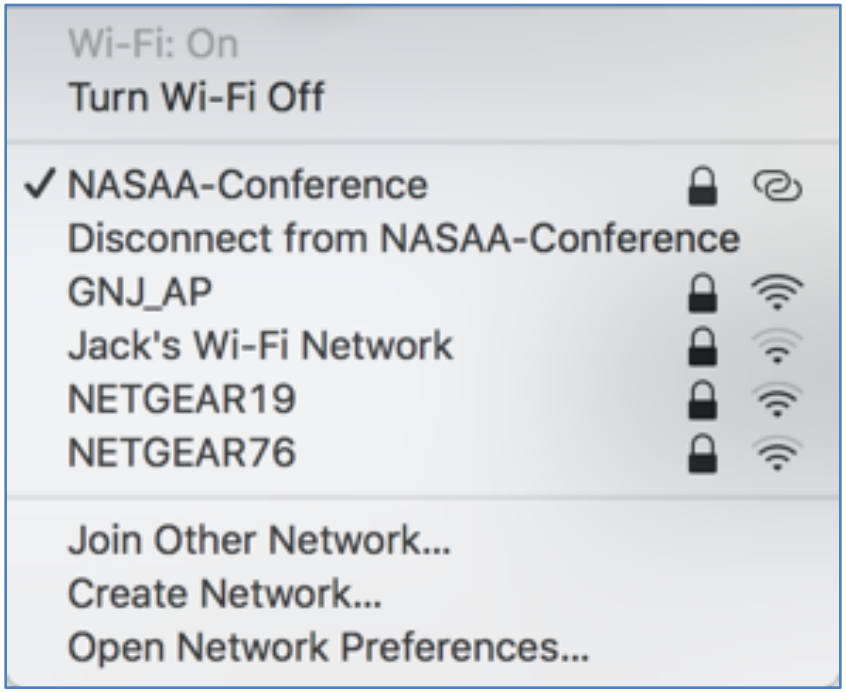


Update or segment if system critical i.e. SCADA System

Users who do not own the knowledge of securing their data are in effect voluntarily giving their data away

VPN

Always Protect Your WiFi Activity

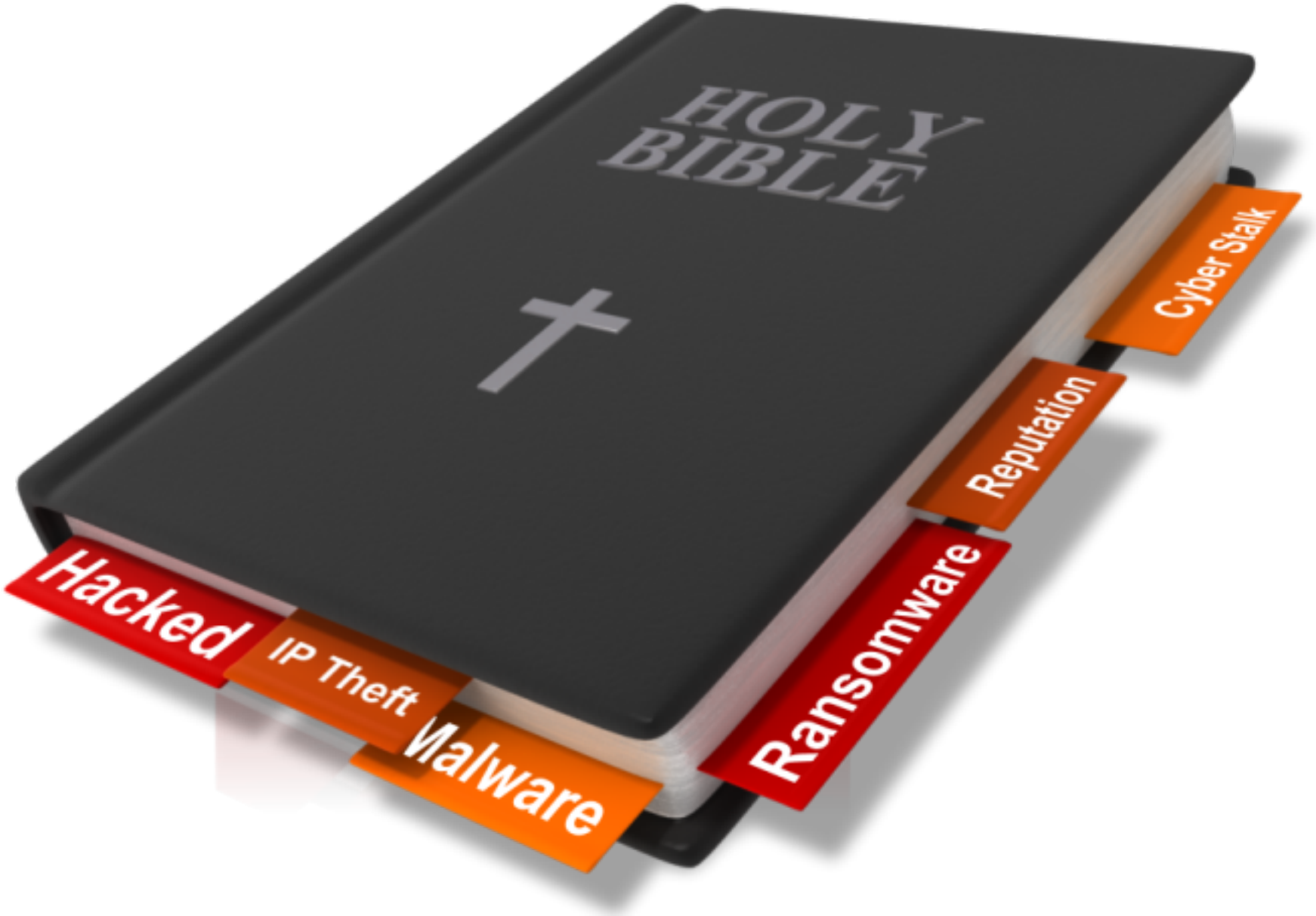


Internet of Things (IoTs)

- Many third party Wi-Fi network devices such as thermostats, voice control (Alexa, Suri, Google Assistant), appliances can cause a data breach because it is normally tied to a network which contains your sensitive data

- https://www.abcactionnews.com/news/local-news/i-team-investigates/privacy-threat-smart-speakers-may-be-recording-you-even-when-not-being-used

Time for Personal Confessions



Commission Statement and Guidance on Public Company Cybersecurity Disclosures

National Institute of Standards and Technology Cyber Security Framework

Asset Management

- The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Risk Assessment

- The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Access Control

- Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Awareness and Training

- The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

Data Security

- Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Information Protection Processes and Procedures

- Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Recovery Planning

- Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

Getting in Touch With Us

Greg.Bordenkircher@asc.alabama.gov

Gus@CyberForensics.com