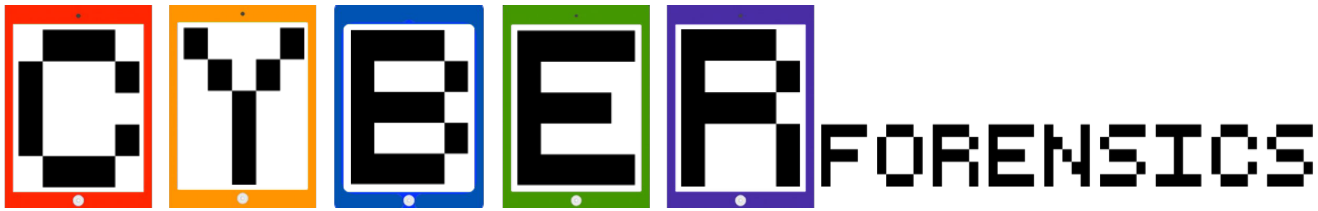
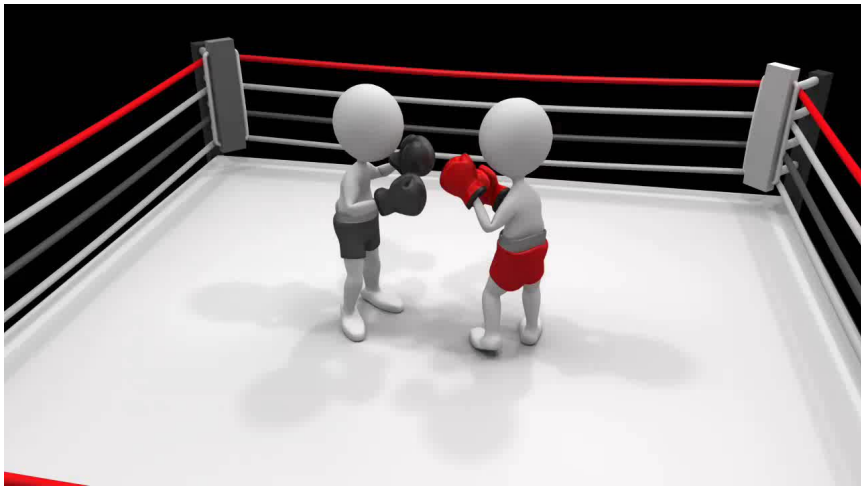


Cyber Threats and Solutions and Other Cyber Stuff

Presented by K. Gus Dimitrelos
Retired US Secret Service and CEO of Cyber Forensics, Inc

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

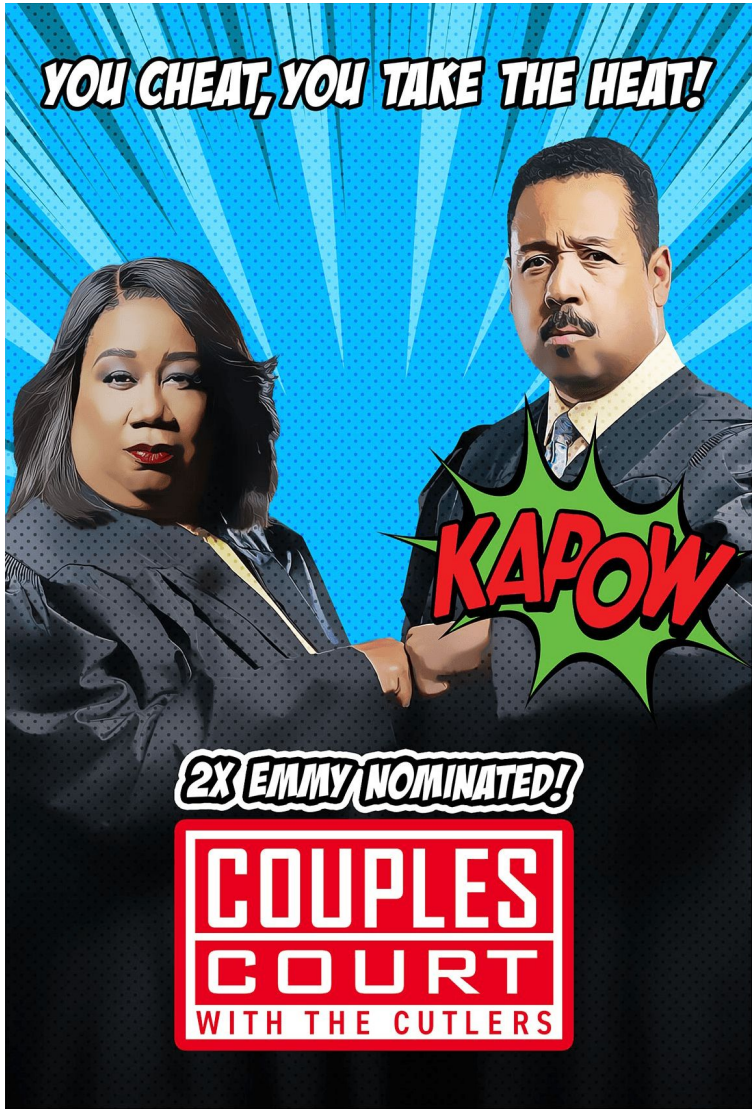


Department of State
Cyber anti-Terrorism Program

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

Cyber Expert on the CW Show Couples Court with the Cutlers



Gaining Knowledge - Firewalls

Purchasing a Home Firewall is a great Place to Start

Home Firewall Comparison

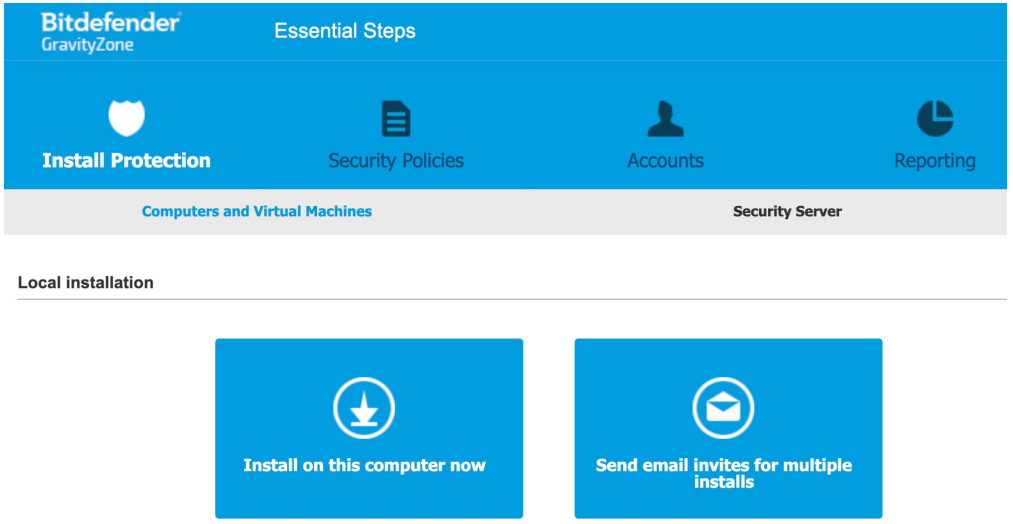
	Cujo	Dojo	RATtrap	BitdefenderBox 2
Price	$99	$199	$199	$249
Best For	Protecting your home network, including smart home devices.	Protecting your smart home devices.	Protecting your home network, including smart home devices.	Protecting your home network, including smart home devices.
How It Protects 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.

Models reflected above may not be the newest ones available

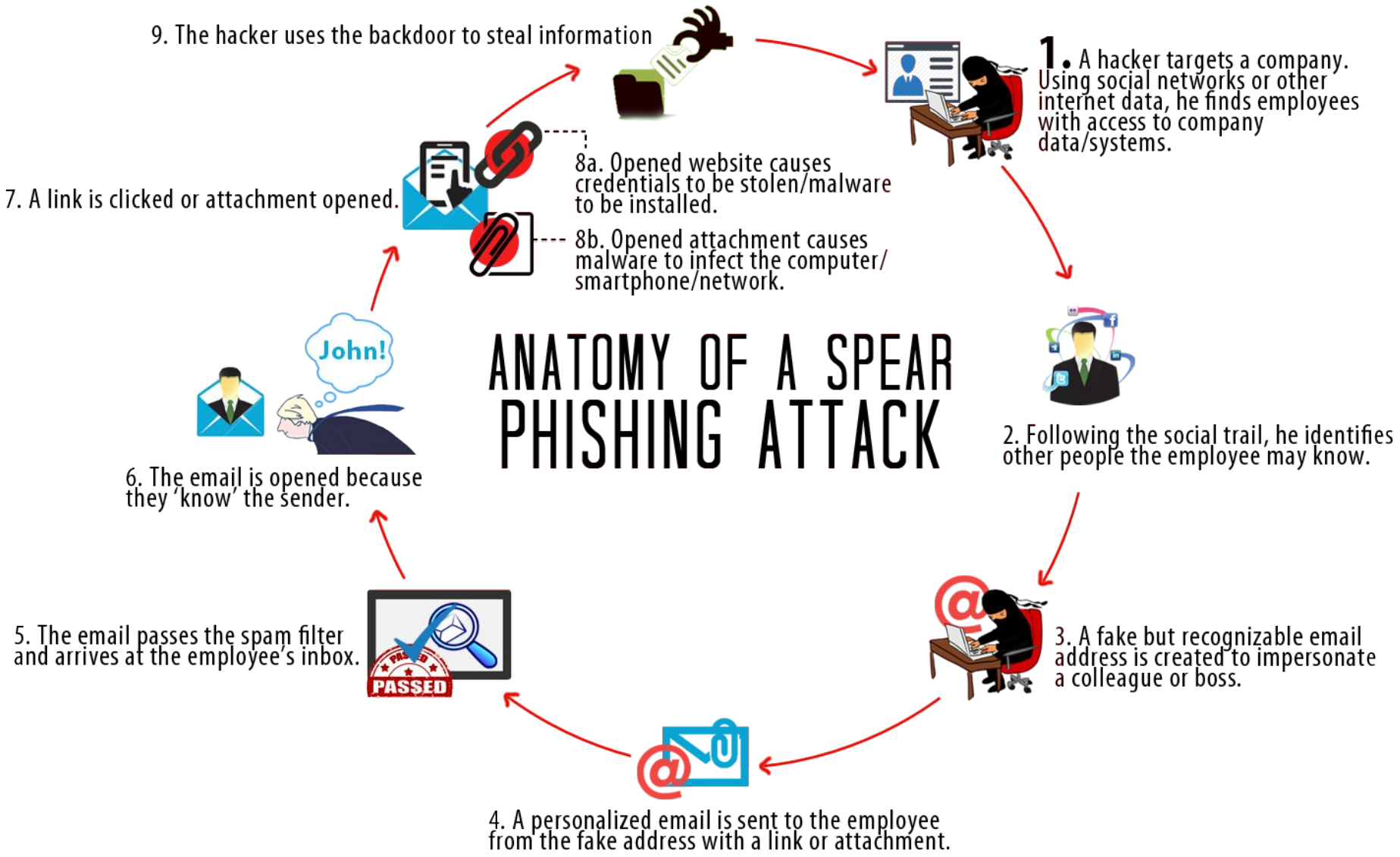
Fighting Back - Anti-Everything

- 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



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/

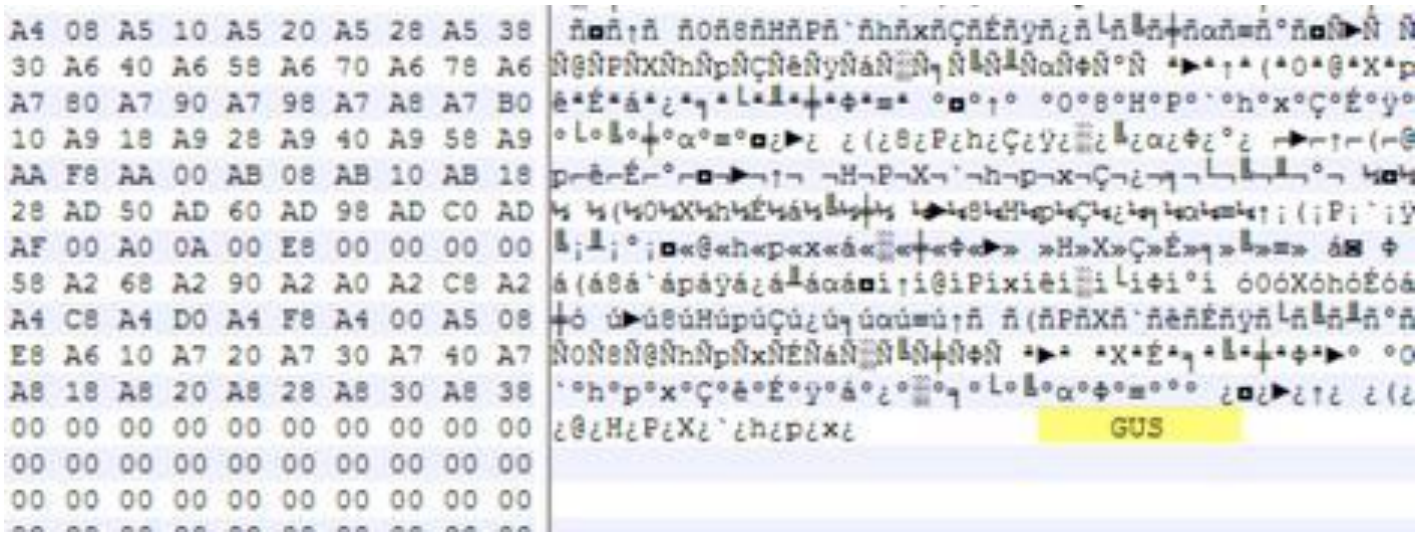
Problem with anti-Virus and anti-Malware

POLYMORPHIC – OBFUSCATION

MIMIKATZ Original Digital Fingerprint:
f3eb271434185f8c5c2cc80f90ce0ca1

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

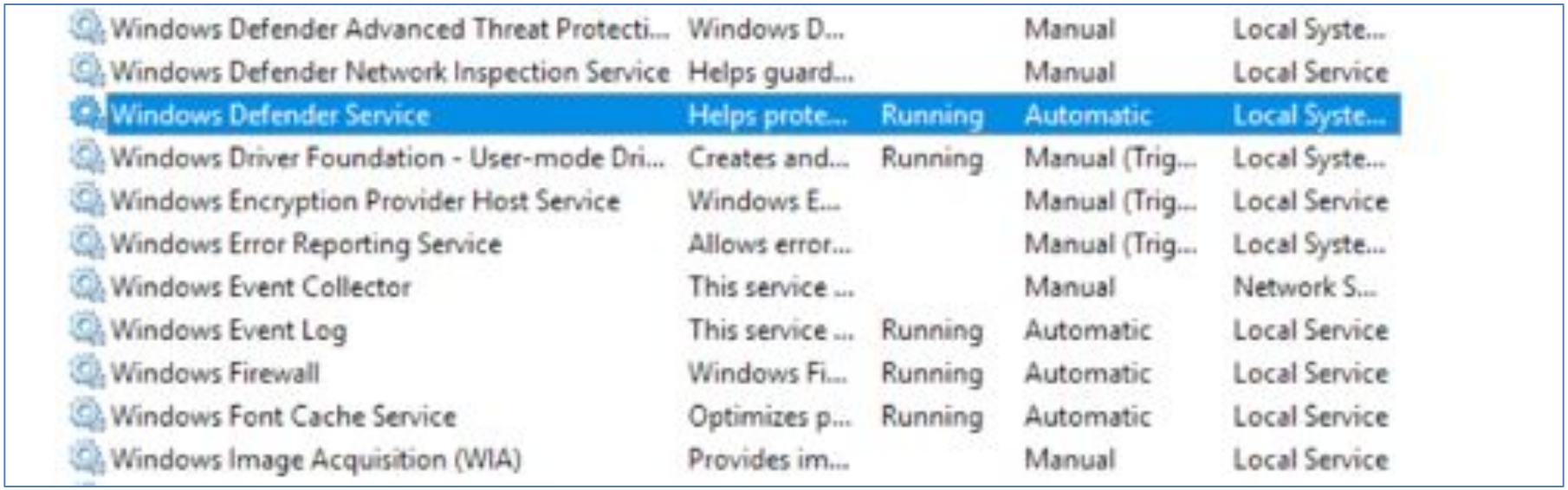
Digital Fingerprint Changed using free Hex Editor:
3ababf95703545db30b6d8a1705251ed



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.

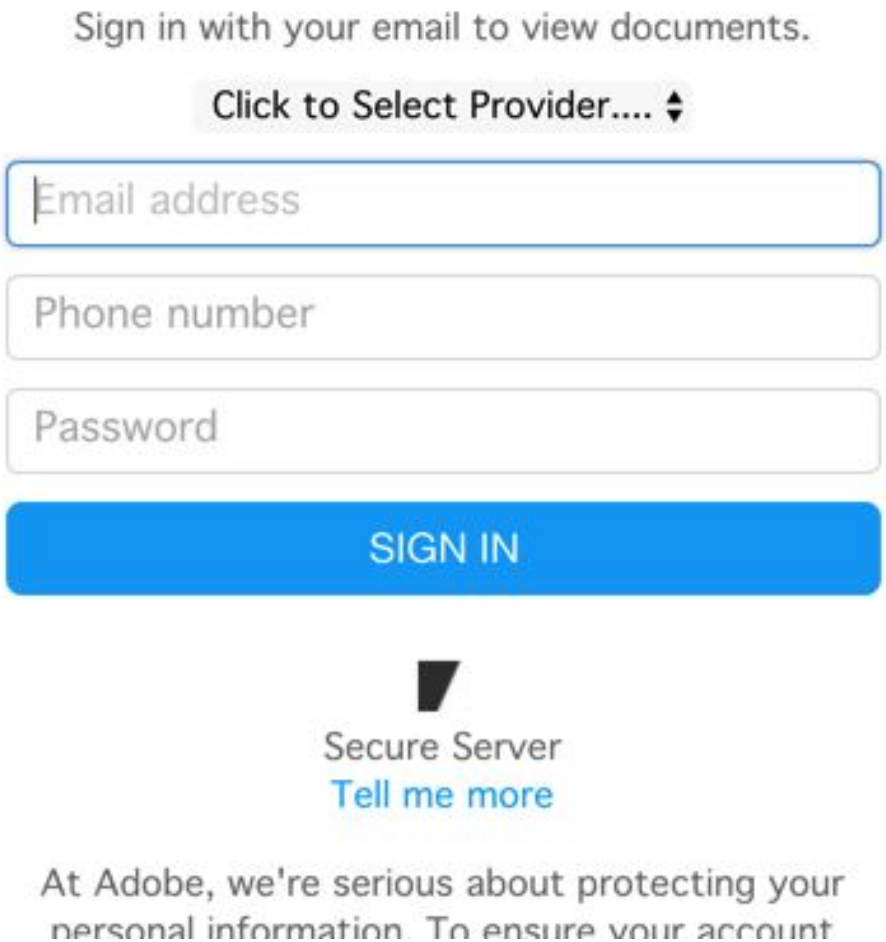
To view file online CLICK HERE

2

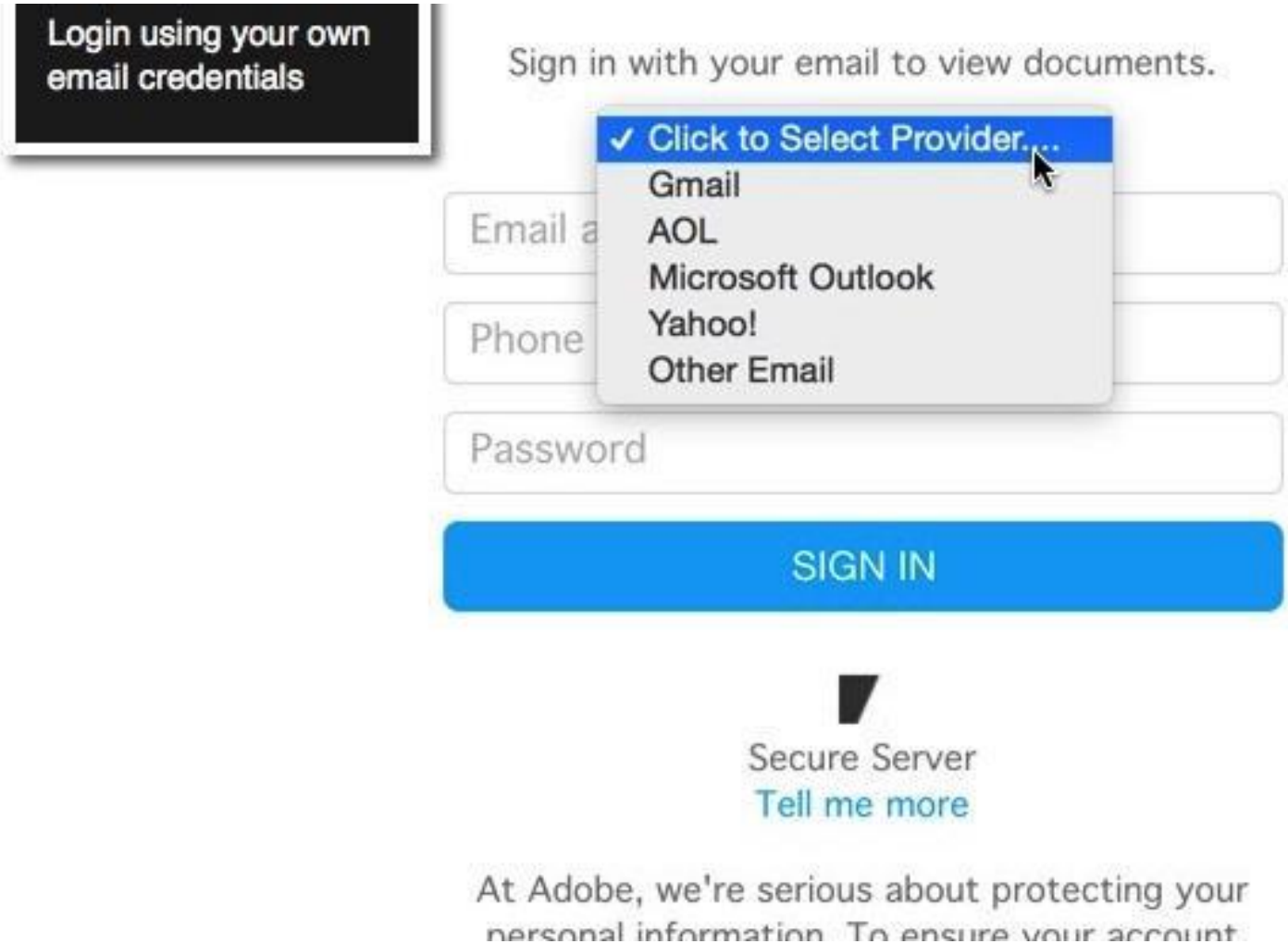
Elias Dimitrelos
Chief Financial Officer
+1.251.202.9237
elias@cyberforensics360.org
Cyber Forensics 360
7450 Griffin Rd
Davie, FL 33314-4104

3

Which Leads To Normal Login Screen



To a Common File Downloading Account



Gaining Knowledge - Headers

To View Your Header Choose Your [Email Provider]

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 (P
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

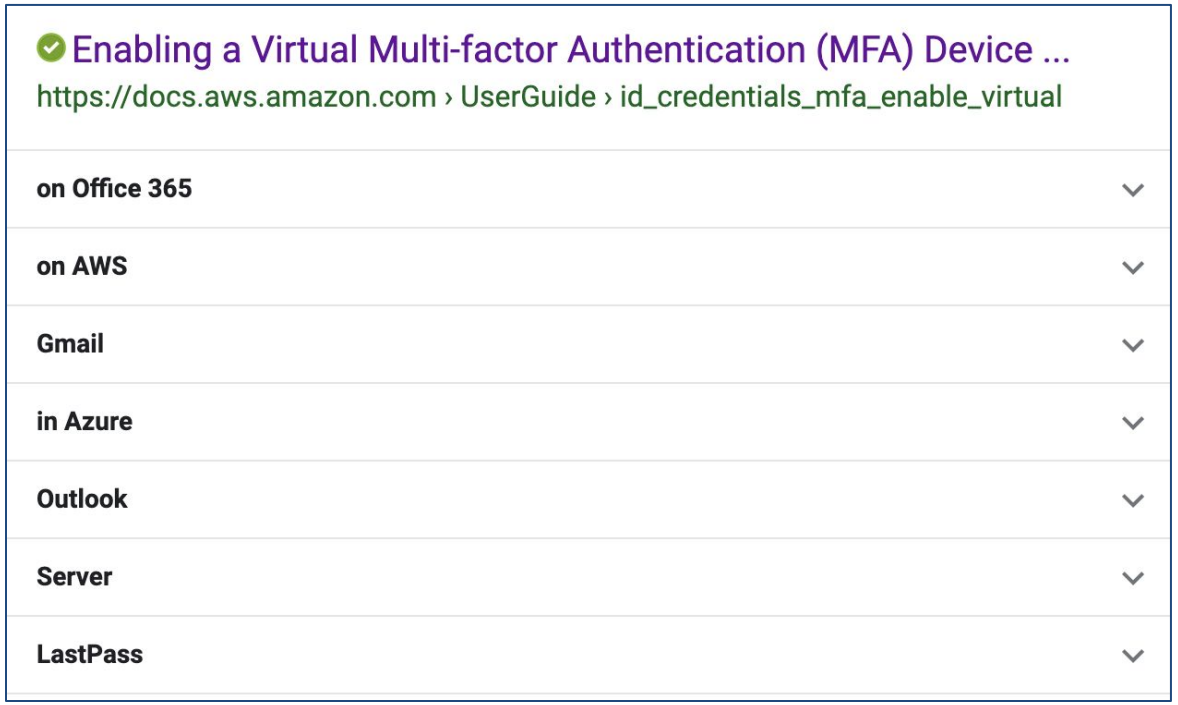
sjferalin@ email account was compromised and sent this malicious PDF LINK attachment.

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

MFA/2FA/2FV

- Two factor AKA multi-factor authentication has been available for years
- Visit https://twofactorauth.org to identify if your organization offers Multi Factor Authentication
- To setup MFA identify your host and follow the steps provided



Gaining Knowledge - Patches

Always Check for Updates Each and Everyday

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

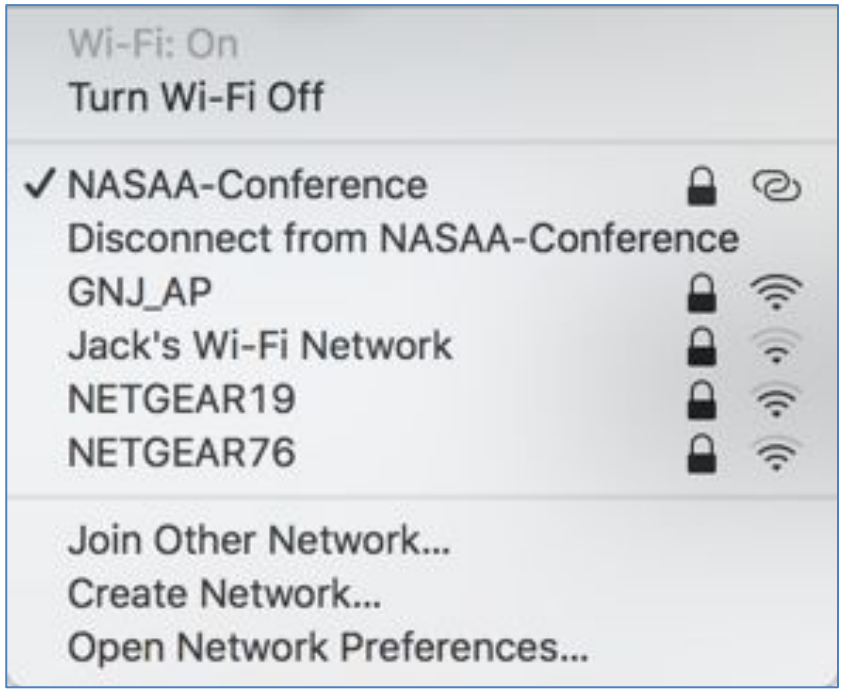
Users who do not own the knowledge of securing their data are in effect voluntarily giving their data away

Virtual Private Networks VPNs

Be Invisible

Always Protect Your WiFi Activity

- Use your Mobile Hotspot as the WiFi NOT Public Ones
- Most VPN providers in the USA are trusted
- View 12 VPN Providers and Options

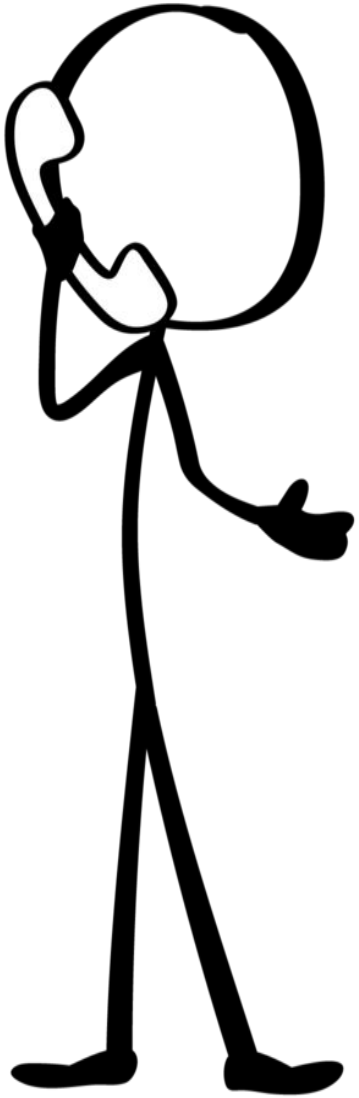


Internet of Things (IoTs)

- 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

Getting in Touch With Us



Gus@CyberForensics.com

www.CyberForensics.com