IRS

IRS Nationwide TaxFORUM 2012

Data Compromises

The Bulls-eye is on You

Mark P Kahler
National ID Theft Coordinator
IRS Criminal Investigation

IRS

IRS Nationwide TaxFORUM

Internal Revenue Service
Criminal Investigation

Criminal Investigation serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law.

IRS Nationwide TaxFORUM

Overview

- Computer Security - The Critical Necessity
- Security - The Cyber Crime Threat
  - Cyber Criminal Underground
- Actions When Compromised
- Cyber Security Resources

IRS

IRS Nationwide Tax FORUM 2018

Security Questions

- How many in the audience think their tax software has built in security measures?
- Tax software packages commonly have optional capabilities to use a login and password to get to return files, as well as options to **password protect** individual return files. How many use these features?
- How many of you know if your computers have malware protection built in to your software?

IRS

IRS Nationwide TaxFORUM 2012

Where it all Starts: The Cyber Underground

- 2002: Less than 12 forums
- More than 800 Criminal Forums
- Represent 25+ languages
- More than 50 roles/specializations
- Nearly every cyber criminal has a membership on a forum (95%)

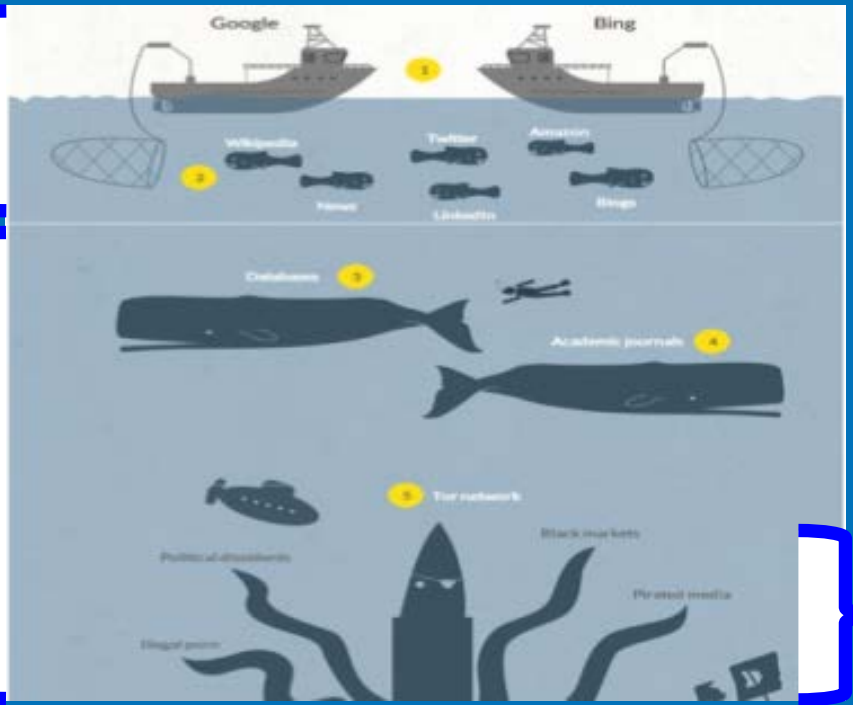
IRS

IRS Nationwide TaxFORUM

Surface Web v Deep Web v Dark Web

Surface Web
Social media sites, sites indexed by search engines

Deep Web
Private databases, forums, password protected sites



Graphic: CNN

Dark Web
Only accessible via special software; intentionally hidden; anonymous

IRS Nationwide TaxFORUM

The Cyber Crime Threat

- Cyber criminals have adapted to today's technology in exploiting the cyber arena
- These groups continually attack systems for monetary gain
  - Malware
  - Remote Access Software Products (Weak or no Passwords)
  - Spam and phishing
  - Email and Web Browser Protections
- **News-4-Investigates-The-Dark-Net-with-an-exclusive-look-at-th--KMOV.com**

IRS

IRS Nationwide TaxFORUM

162.233...
United States, [redacted]
[redacted]

Checked	Uptime
05.04.2016	18 Hours

[redacted]$

Windows 7 | x64 | EN
Intel(R) Core(TM)2 Duo CPU E8500...
Ram: ***3.9 GB*** | *CPU Cores:* ***2***

14.63 Mbit/s *920 Kbit/s*

Check IP-Score (0.20$)

Admin Privilege: *Yes*
Direct IP: *No*
Antivirus: [redacted]
Browsers:
Blacklist: Check
Opened Ports: *No*
Virtual: *No*

Payment Systems

Not Found.

Poker Systems

Not Found.

Internet Shops

Not Found.

Dating Sites

Not Found.

Other Files

1. [redacted]2015
2. [redacted]2014
3. *2200 Records*

Other Sites

1. [redacted]

Cancel | Check for Blacklist | Buy

IRS

IRS Nationwide TaxFORUM

162.233...
United States, [redacted]
[redacted]

Checked	Uptime
05.04.2016	18 Hours

4000.00$

Windows 7 | x64 | EN
Intel(R) Core(TM)2 Duo CPU E8500...
Ram: ***3.9 GB*** | *CPU Cores:* ***2***

14.63 Mbit/s *920 Kbit/s*

Check IP-Score (0.20$)

Admin Privilege: *Yes*
Direct IP: *No*
Antivirus: [redacted]
Browsers:
Blacklist: Check
Opened Ports: *No*
Virtual: *No*

Payment Systems

Not Found.

Poker Systems

Not Found.

Internet Shops

Not Found.

Dating Sites

Not Found.

Other Files

1. [redacted] 2015
2. [redacted] 2014
3. 2200 Records

Other Sites

1. [redacted]

Cancel | Check for Blacklist | Buy

IRS

IRS Nationwide TaxFORUM

23.30.34.147 [redacted]

Checked	Uptime
04.02.2016	24 Days

300.00$

Windows Server 2008 R2 | x64 | EN
Intel(R) Xeon(R) CPU E5620...
Ram: ***8 GB*** | *CPU Cores:* ***8***

11.91 Mbit/s *6.51 Mbit/s*

Check IP-Score (0.20$)

Admin Privilege: *Yes*
Direct IP: *No*
Antivirus: [redacted]
Browsers: [redacted]
Blacklist: **1** / 178
Opened Ports: 80
Virtual: [redacted]

Payment Systems

Not Found.

Poker Systems

Not Found.

Internet Shops

1. [redacted]

Dating Sites

Not Found.

Other Files

1. [redacted]*Software*
2. *450 Records*

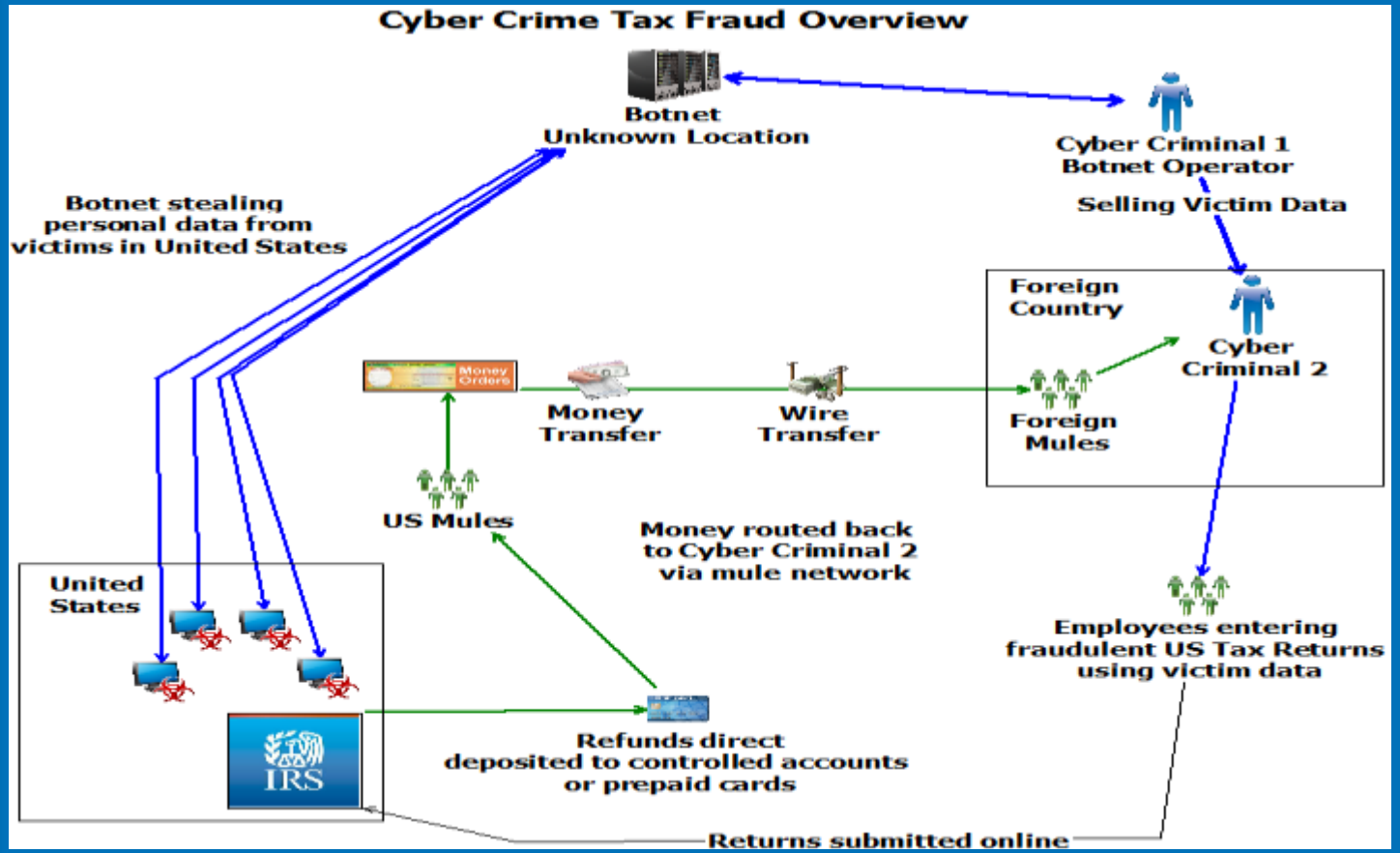
Other Sites

1. [redacted]

Cancel | Check for Blacklist | Buy

IRS

IRS Nationwide TaxFORUM



IRS Nationwide TaxFORUM 2012

Case Example:

Vanyo Minkov

- **Charges alleged that Minkov hacked into the networks of multiple accounting firms to steal 2011 year tax filings from the firms' clients, then using that information to file tax returns in their names the following year;**

IRS

IRS Nationwide TaxFORUM 2013

Vanyo Minkov

- September 2013 Extradited From Bulgaria;
- Charges involved filing false tax returns using hacked information and the sale of stolen payment card data;
- Linked to approximately $6 million in fraudulent tax claims.

IRS

IRS Nationwide TaxFORUM 2016

Vanyo Minkov

- District of New Jersey
- July 2015 Entered Guilty Plea to a Superseding Information Charging Conspiracy to File False and Fraudulent Tax Returns.
- Agencies Involved
  - IRS CI
  - USSS
  - FBI

IRS Nationwide TaxFORUM

Actions When Compromised

- Contact IRS Stakeholder Liaison When Compromise Detected
  - Stakeholder Liaison will refer Information within IRS (i.e. Criminal Investigations, Return Integrity & Compliance Services)
  - http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Stakeholder-Liaison-Local-Contacts-1
- Follow State Reporting Requirements (i.e. State Attorney General, State Consumer Protection Bureaus, State Police)
- Report Compromise to FBI, US Secret Service, Federal Trade Commission

IRS Nationwide TaxFORUM

Cyber Security Resources

- Internal Revenue Service (IRS)
  - Pub 4557
- Center for Internet Security (CIS) - https://www.cisecurity.org/critical-controls.cfm
- Federal Trade Commission
  https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

CIS Critical Security Controls

- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software
- Continuous Vulnerability Assessment and Remediation
- Controlled Use of Administrative Privileges
- Maintenance, Monitoring, and Analysis of Audit Logs

IRS

IRS Nationwide TaxFORUM 2018

CIS Critical Security Controls

- Email and Web Browser Protections
- Malware Defenses
- Limitation and Control of Network Ports
- Data Recovery Capability
- Secure Configurations for Network Devices
- Boundary Defense
- Data Protection
- Controlled Access Based on the Need to Know

IRS

IRS Nationwide TaxFORUM 2018

CIS Critical Security Controls

- Wireless Access Control
- Account Monitoring and Control
- Security Skills Assessment and Appropriate Training to Fill Gaps
- Application Software Security
- Penetration Tests and Red Team Exercises

IRS

IRS Nationwide TaxFORUM 2012

Questions?