Microsoft

Microsoft® Research Faculty Summit 2012

ADVANCING THE STATE OF THE ART

Internet Service Security:

Attacks and Defenses

Robert Sim
Applied Research Manager
Windows Live Safety Platform
July 16, 2012

Abuse by the numbers

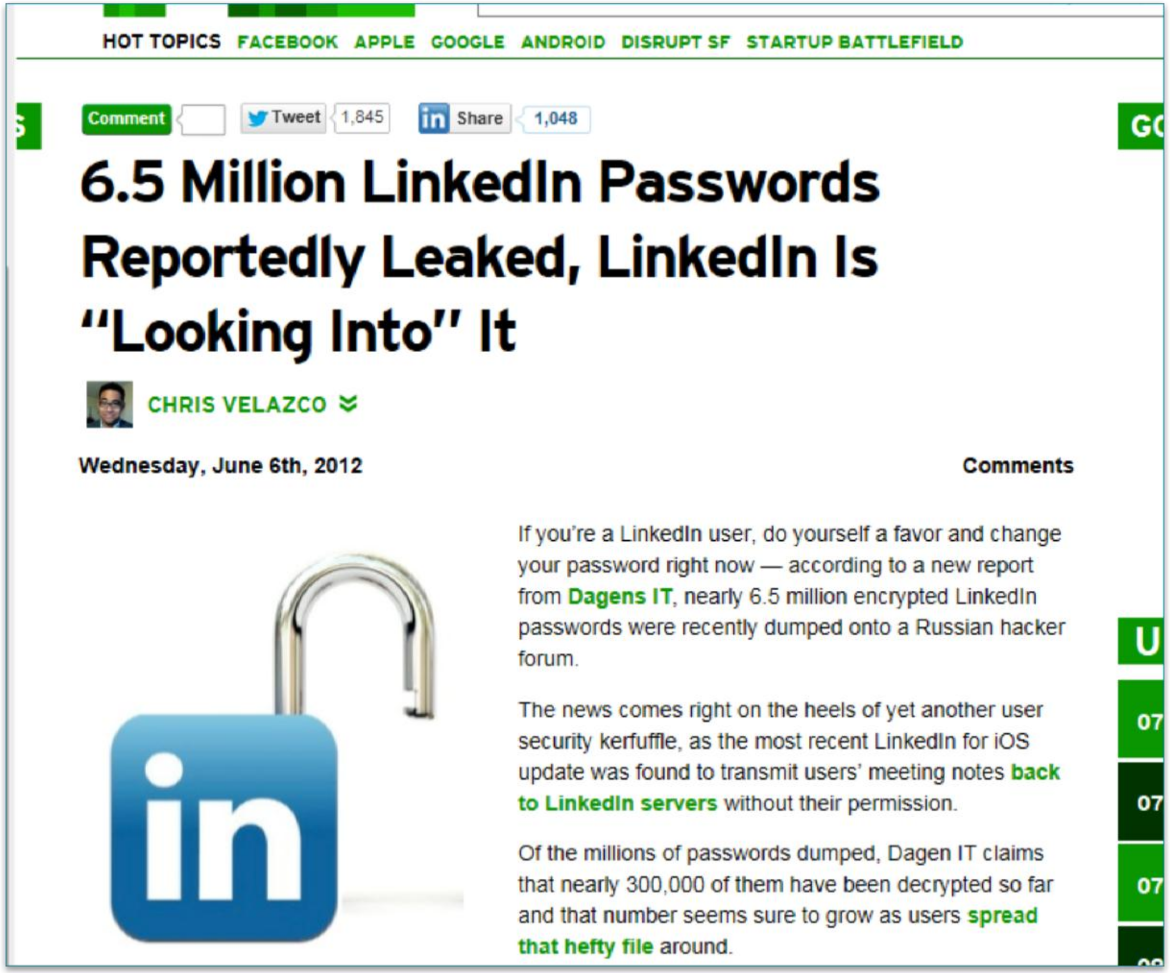
- 93 trillion spam messages
- 3 trillion malware attachments
- 21 billion phishing messages
- 2.1 billion malware downloads
- 243 million malicious page views (browser exploits)
- 192 million phish page views

Estimates, annual world-wide impressions for the internet as a whole

Compromise is Equal-Opportunity

- Affects every major internet service.
- Est >500,000 account credentials *per day* across major email providers.
- Painful for users: double whammy of spamming their social network and trying to remember an ancient SQSA or fake birthdate…

Accounts under Siege


HOT TOPICS FACEBOOK APPLE GOOGLE ANDROID DISRUPT SF STARTUP BATTLEFIELD
Comment
Tweet 1,845
Share 1,048
Comments

6.5 Million LinkedIn Passwords Reportedly Leaked, LinkedIn Is "Looking Into" It

CHRIS VELAZCO

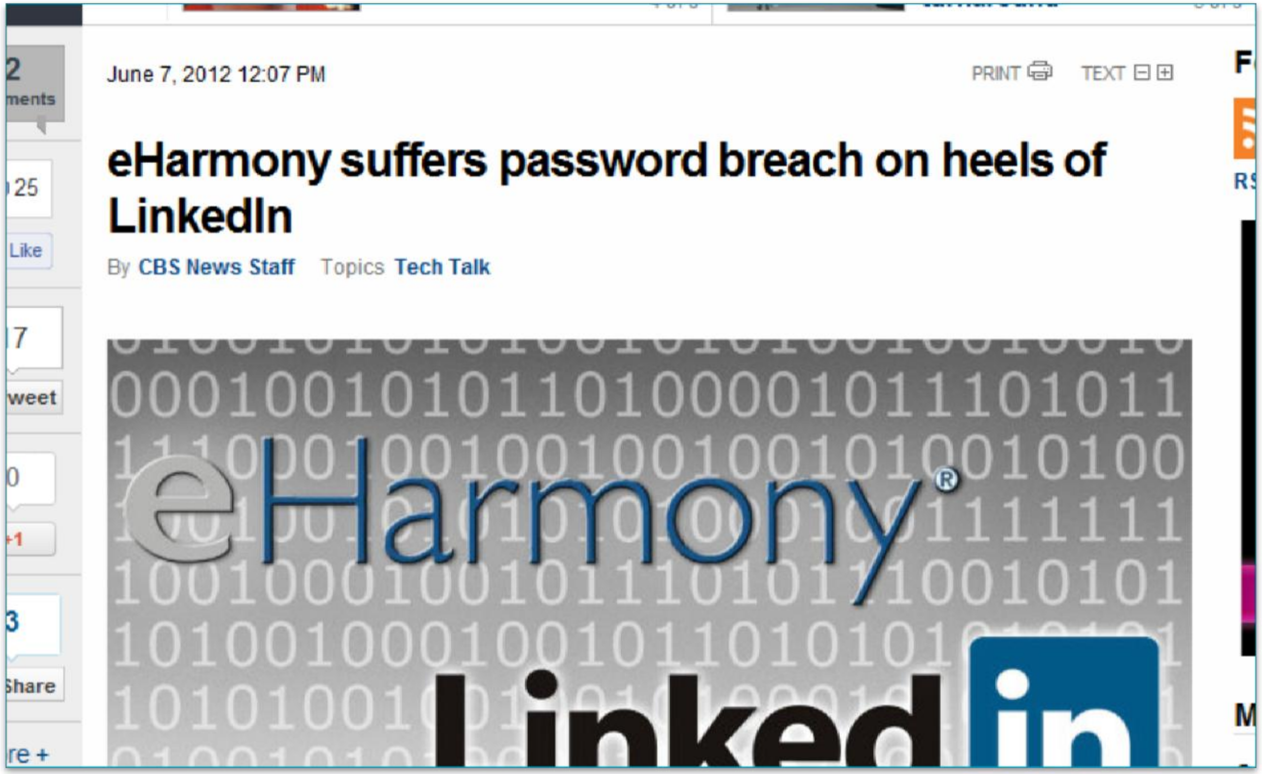
Wednesday, June 6th, 2012

If you're a LinkedIn user, do yourself a favor and change your password right now — according to a new report from **Dagens IT**, nearly 6.5 million encrypted LinkedIn passwords were recently dumped onto a Russian hacker forum.

The news comes right on the heels of yet another user security kerfuffle, as the most recent LinkedIn for iOS update was found to transmit users' meeting notes **back to LinkedIn servers** without their permission.

Of the millions of passwords dumped, Dagen IT claims that nearly 300,000 of them have been decrypted so far and that number seems sure to grow as users **spread that hefty file** around.

http://techcrunch.com/2012/06/06/6-5-million-linkedin-passwords-reportedly-leaked-linkedin-is-looking-into-it/



June 7, 2012 12:07 PM

eHarmony suffers password breach on heels of LinkedIn

By CBS News Staff Topics Tech Talk

http://www.cbsnews.com/8301-501465_162-57448965-501465/eharmony-suffers-password-breach-on-heels-of-linkedin/

... Sony, Gawker, Zappos, etc, etc ...

Why Compromise?

- Symptom of two factors:
- Industry-wide increased effectiveness at spam filtering [reputation hijacking]
- Industry-wide increased captured value
  - Paypal, Amazon, Ebay, XBox, Itunes, App Stores, Banking, etc, etc.

Understanding the Threat

- The attackers are not a monolithic group of people
- They can be categorized based on types of attacks and capabilities

The personas

Script Kiddies

- Use crime kits to make spending money
- Little to no business or technical expertise

Gray-Hats

- They believe they are offering legitimate services. However, their customers can be both “legitimate” or criminal
- Ran as a business

Black-Hats

- Treats cybercrime as a business
- Business and technical expertise
- Often works in a closed group of other professional cybercriminals
- Criminal reputation is everything

Hactivists

- Individuals or groups who hack for a social cause, without economic motivation
- Has both technical people and minions

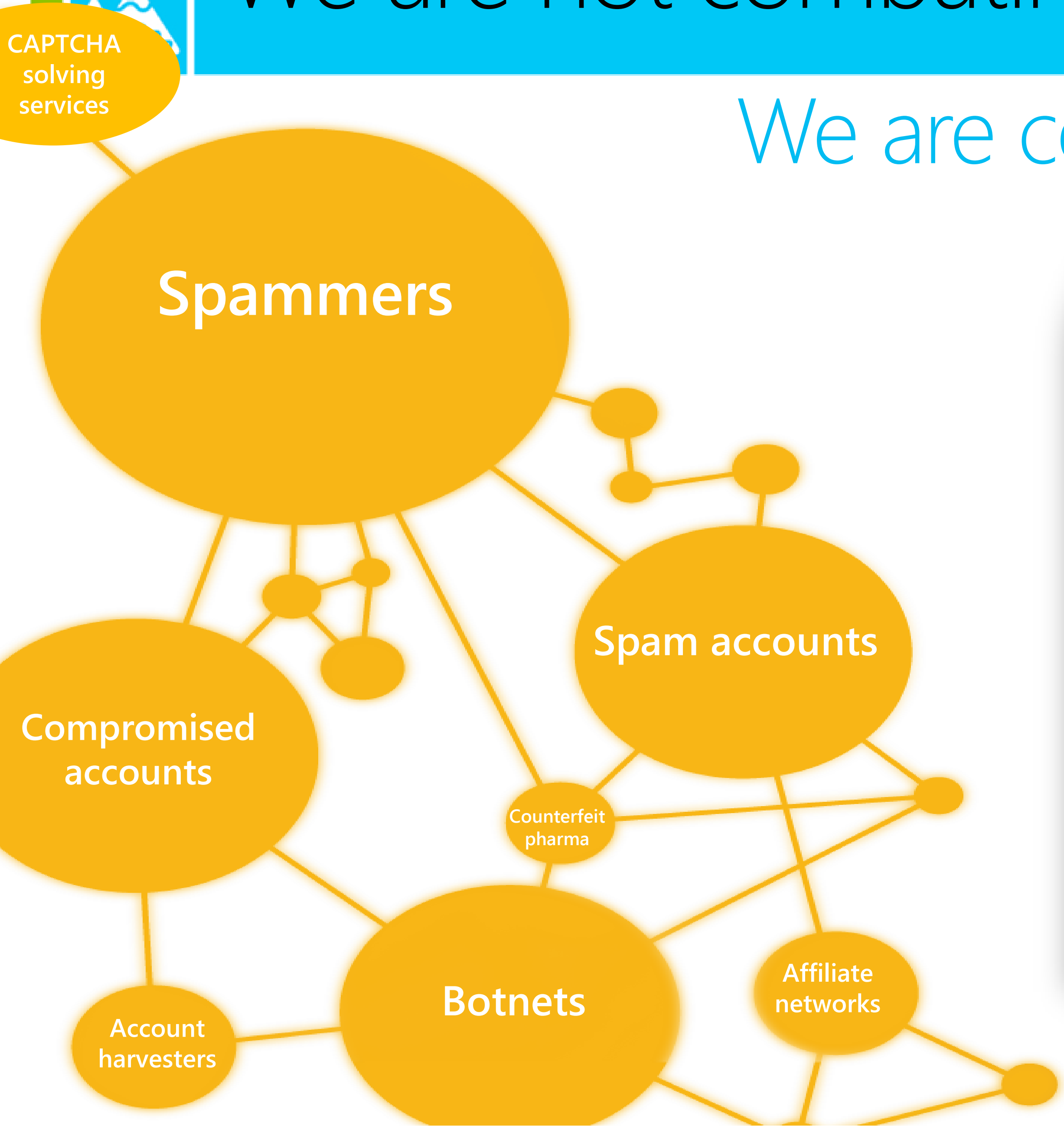
State Sponsored

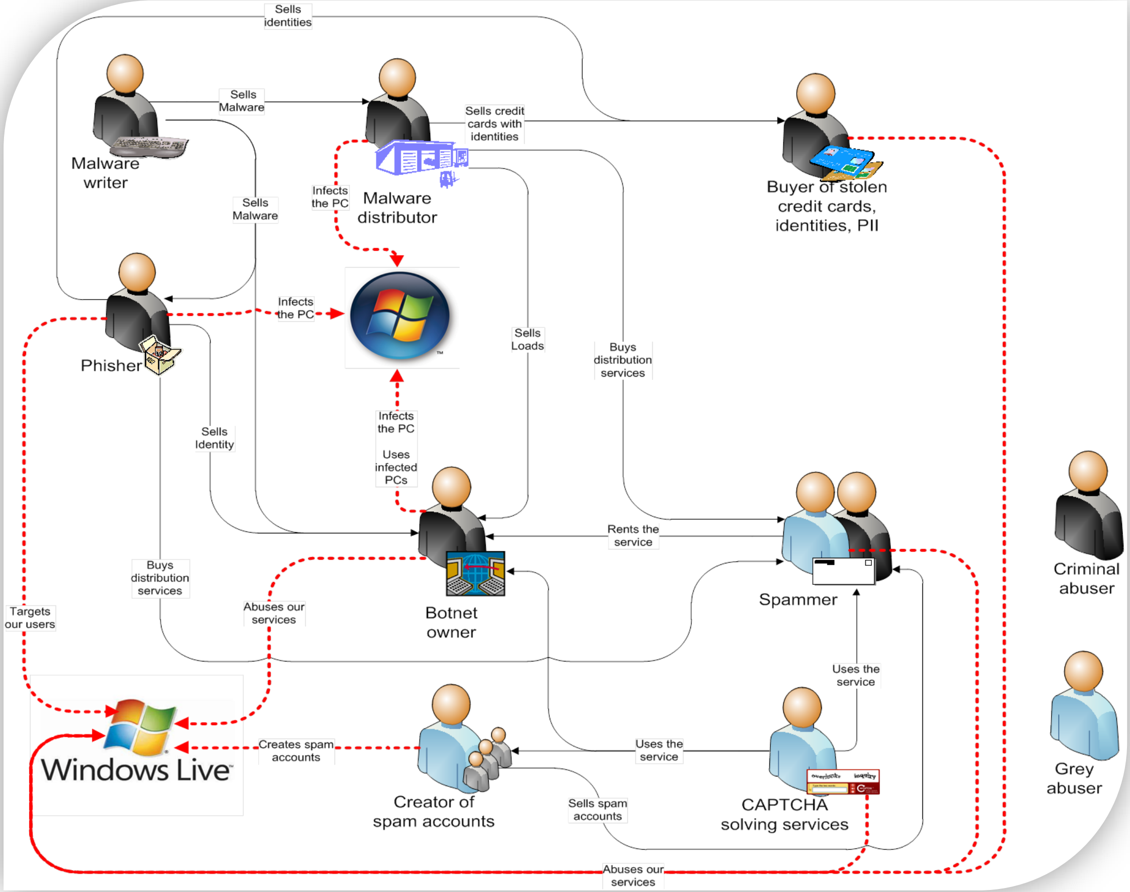
- National security and/or economic motivation
- Technical expertise
- Work in a closed group of other professionals
- Often uses Black-Hat resources and/or techniques to mask their identity

	Script Kiddies	Gray-Hats	Black-Hats	Hactivists	State Sponsored
Estimated number WW	> 1M	> 10k	> 30k	>1k professionals > 10k minions	Unknown

We are not combating hackers

We are combating an ecosystem





Simplified diagram of the abuse supply chain

The ecosystem is adaptable

Fluidity

Few barriers or costs to switch business models, tools, and techniques within their persona

R&D

The ecosystem is always evolving to mitigate new protections

CaaS

Script Kiddies and Black-Hats have moved to "cybercrime-as-a-service" that have matured in the last few years

Consolidation

The professional ecosystem is moving to a closed value-chain that allows for specialization, scale, and reduced risk

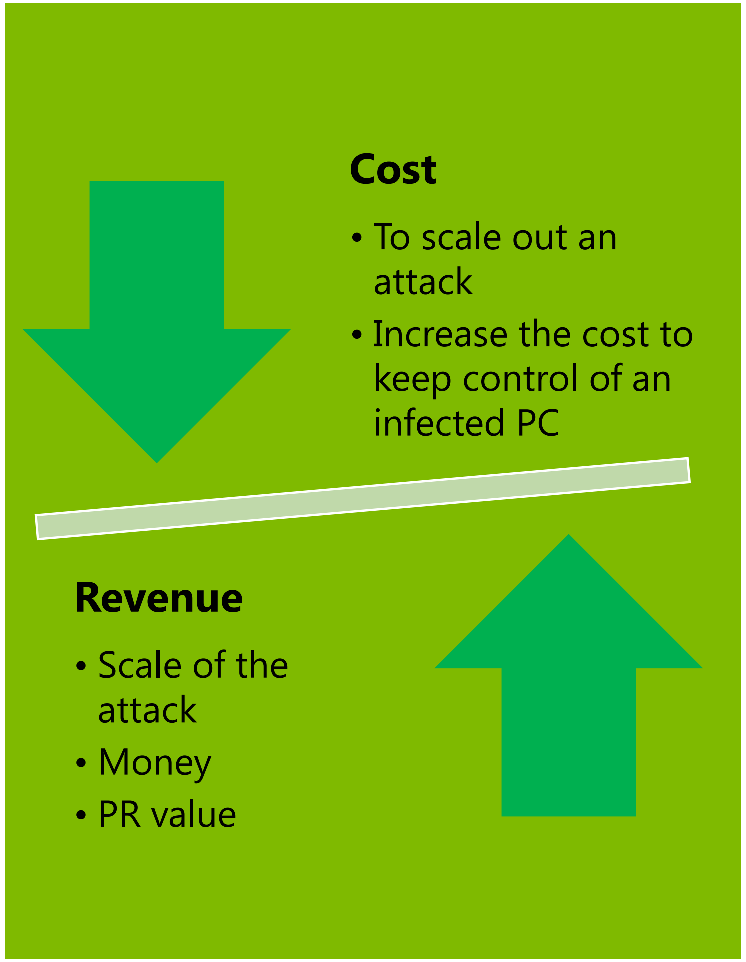
Abuse is largely an economics problem, not a technical one

Increase cost to the attacker

- Cost of creating and distributing malware
- Cost of solving CAPTCHA -> cost of new account creation
- Cost of recovering a suspended account

Decrease revenue/scale for the attacker

- Decrease the value of a compromised PC.
- Decrease the value of data stolen from the PC.
- Decrease the value of a URL in the inbox.



Cost

- To scale out an attack
- Increase the cost to keep control of an infected PC

Revenue

- Scale of the attack
- Money
- PR value

Abuse-related revenue/cost streams

Bank credentials
$15 to 10% of the user's balance
(Per account)

Freshly compromised accounts
$4 to $50
(Per 1k accounts)

Spam accounts
$4-$20
(Per 1k accounts)

Spearphishing services
$13 to $150
(Per account)

Spam accounts proofed with SMS
$200-$300
(Per 1k accounts)

Sending SMS spam
Up to $10
(per message)

Loads (freshly infected PCs)
$8-$400
(Per 1k PCs)

DDoS services
$5-$300
(est. to be for 1K attackers)

Criminal proxy services
$150 to $1,000
(est. for 1k end points)

Tools that automate breaking into websites
$100-$300

Internet traffic
$3 to $21
(Per visit/visitor)

Spam services
$75-$350
(Per 100k messages delivered)

CAPTCHA solving services
$0.70-$1.9
(Per 1k solved)

Other revenue steams for abusers:

- Click fraud
- IP Theft
- PII theft
- Blackmail / e-whoring
- Buyer-seller collusion
- SEO
- Counterfeit apps
- Ratings/reviews
- Zero-day exploits

Based on various sources These prices are averages. True price varies per many factors

How do users lose their email credentials?

- [Estimates, based on various sources]
- 65%: Malware (<1% 0-day)
- 20%: Combination of unsecured 3rd party web sites + password reuse [e.g. Sony/Gawker leaks]
- 10% conventional Phish
- 5% weak passwords [e.g. 123456]
- 1% 1st Party service exploits

Trends

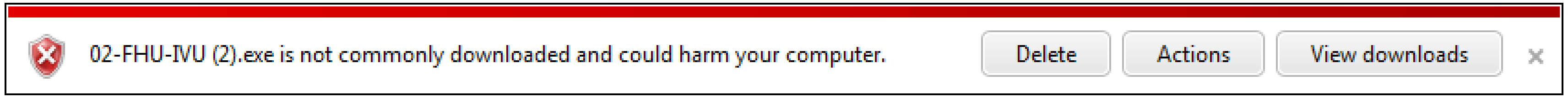
- The password reuse/3rd party problem is growing:
  - Much bigger concern in the recent months vs past years.
- Rise in mobile malware, poor app store QC
- Increasing sophistication among harvesters:
  - Evidence of account sorting
  - Not all compromised accounts send spam
- Geo-targeted abuse proxies
- Identity bundling: email, banking, credit card, billing address, etc

Securing Accounts and Users' PCs: Industry Trends and Future Prospects

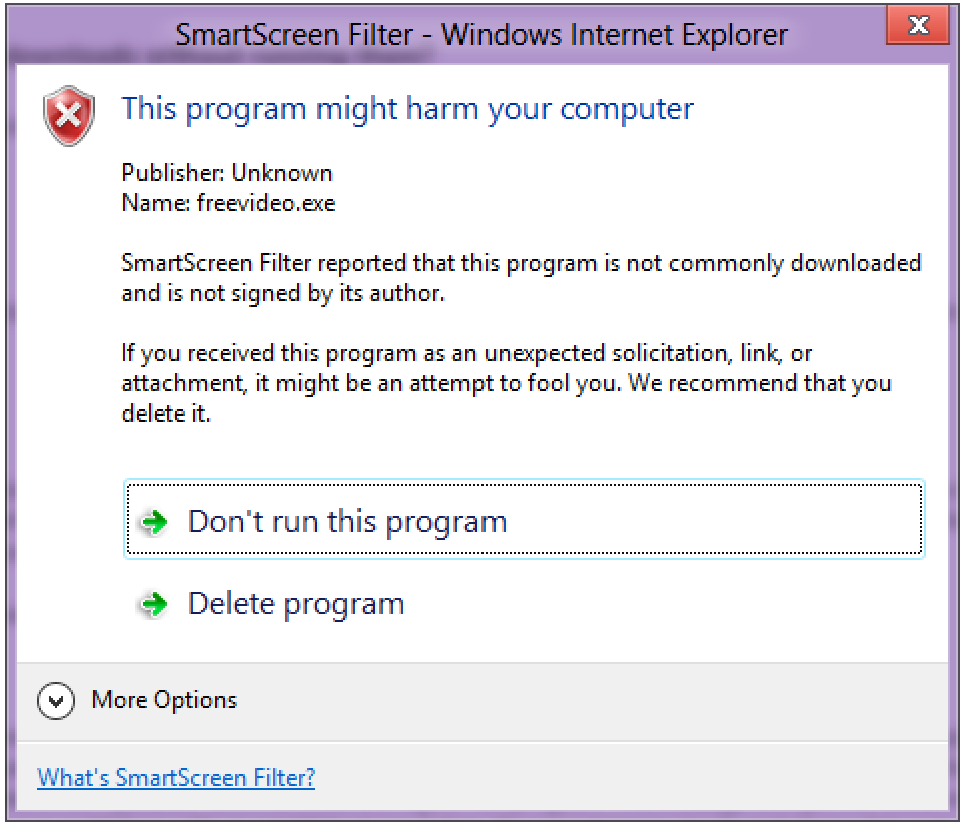
- Involve users in protection
- Ban common passwords
- Two-factor auth, one-time passwords, etc
- Smarter AV and URL reputation
- Smarter behind-the-scenes intelligence
- Fundamentally: reduce the value of compromise.

Securing Accounts and Users’ PCs

- Rethinking Security Dialogs



02-FHU-IVU (2).exe is not commonly downloaded and could harm your computer.



SmartScreen Filter - Windows Internet Explorer

This program might harm your computer

Publisher: Unknown
Name: freevideo.exe

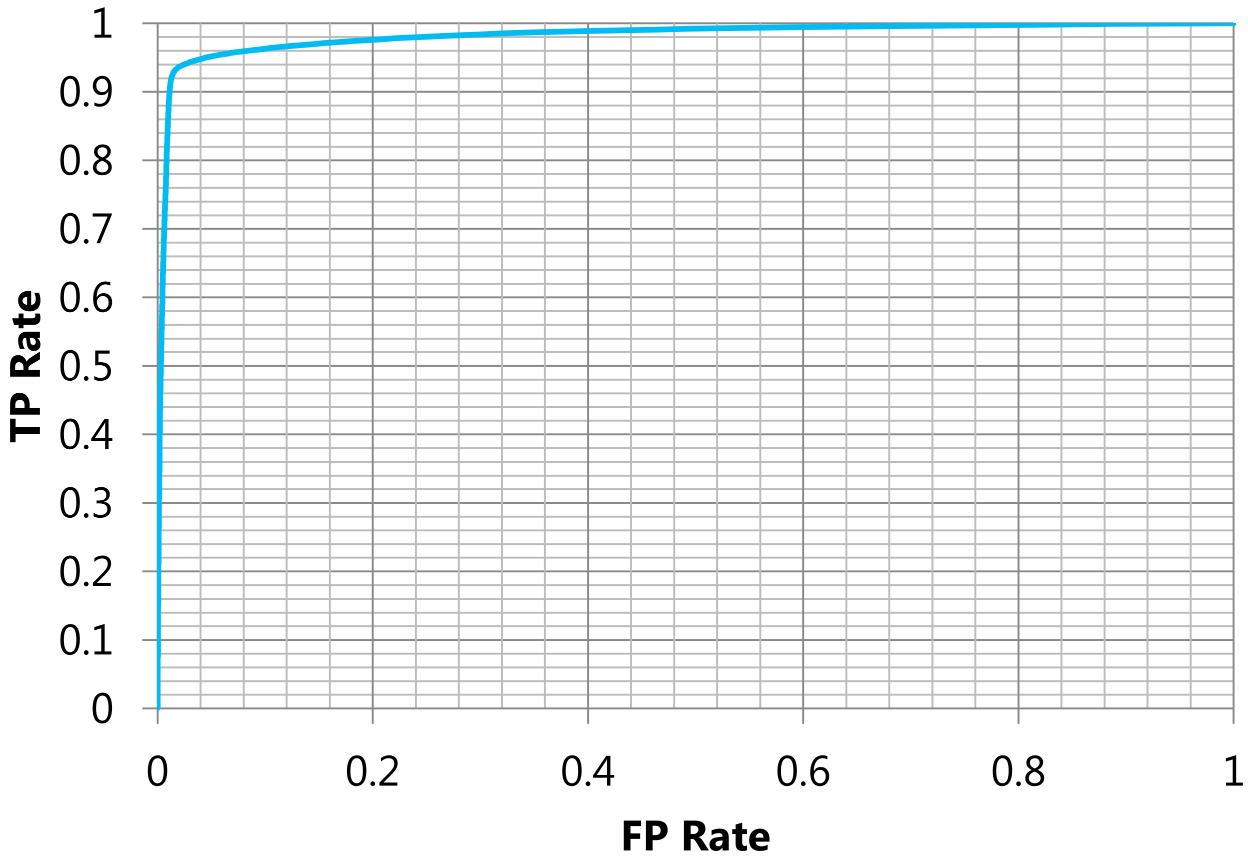
SmartScreen Filter reported that this program is not commonly downloaded and is not signed by its author.

If you received this program as an unexpected solicitation, link, or attachment, it might be an attempt to fool you. We recommend that you delete it.

- Intelligence perspective: identify the good stuff.
- Fewer, but highly targeted warnings
- Two per year for the typical user
- 95% not-run rate when the binary is later confirmed to be malware.

Date Intelligence/Machine Learning

- Works best when combined with effective policy.
- Extremely low tolerance for FPs: don’t hurt the customer.



ROC curve, abuse detection prototype

Open Problems

- How will authentication evolve over the next decade?
- Almost all abuse problems reduce to: “What is the intent of this event?”

P(malicious | user, IP, browser/client, site, action, time of day, recipients, geoloc, billing data, CAPTCHA signals, UI signals, static/dynamic code analysis, etc, etc, etc)

- Challenges: distributed nature of attackers, scalability, generalization, weak labels, low FP tolerance

Protect Yourself

- Be suspicious
- Run Windows Update
- Proof up: add SMS numbers, alternate email address, check your SQSA and verify your birthdate.

  https://account.live.com

- Use unique passwords!

We’re hiring!

- Looking for student research interns with an interest in abuse, machine learning and big data.

rsim@microsoft.com

Acknowledgements

- Shawn Loveland, WL Planning
- Cloud Directory/Microsoft Accounts
- IE Smartscreen/WLSP

Microsoft