WHO?
Are the bad guys?
Six Silos of Sinister Cyber Skunks!
By David Perry
Threat Strategist, F-Secure
Everything is Different

SIX main types of Cyber PERPETRATORS! (PERPS)
NEW KINDS OF THREATS

- ADVANCED PERSISTENT THREAT
- SERVER BASED POLYMORPHISM
- ADVANCED COMMERCIAL ROOTKITS
- MOBILE MALWARE
- THE INTERNET OF THINGS
SIX SILOS

DIFFERENT DAY, DIFFERENT SCALES, DIFFERENT AIMS
SIX KINDS

- TROLLS
- HACKERS
- HACKTIVISTS
- CRIMINALS
- CORPORATIONS
- GOVERNMENTS
TROLLS

NOT HIDING UNDER A BRIDGE, BUT TROLLING FOR ATTENTION

F-Secure
TROLLS

- YOU SEE THEM IN CHAT ROOMS AND ON SOCIAL MEDIA
- YOU COULD SAY BULLIES INSTEAD
- THESE HAVE THE LEAST IMPACT ON NETWORK SECURITY
- BUT SOMETIMES, IT’S LIFE AND DEATH!
The threat of TROLLS

- Trolls disrupt normal conversation
- They are bullying
- They will personally threaten
- They normally have no skills
- They may have scripts they download
- Watch out for your children
- DON’T FEED THE TROLLS!
HACKERS

KEEPING THE INTERNET SAFE FOR GEEKS EVERYWHERE
HACKERS

- THE WORD IN ITSELF IS NOT PEJORATIVE
- THESE PEOPLE ARE ABOUT BUILDING AND IMPROVING THEIR SKILLS
- THEY BECOME DANGEROUS IN THE EMPLOY OF CATEGORIES 3-6
HACKER threats!

- They research and discover flaws
  - That lead to malware, etc.
- They break into systems
  - Just to prove it can be done
- They have and are gaining skill
- And they might work for worse sorts.
HACKTIVISTS

BANDING TOGETHER AS ANONYMOUS, OR ARE THEY?

F-Secure
HACKTIVISTS

- More dangerous than pure hackers
- People in a group are always more dangerous
- Ideologues are the most dangerous of all
HACKTIVISTS in action!

- Might disrupt operations of public services
- Operate out of a sense of morality
- Do not see themselves as bad guys
- Are not often driven by profit
- Have skills
- Are most likely to get hackers to help them
CRIMINALS

NOT THE WILD WEST, BUT PROHIBITION ERA CHICAGO
CRIMINALS

- Common assumption is that all malware is criminal
- Criminals come in all shapes and sizes
- There is bleed over from criminal to every other silo
CRIMINALS move online

- Willy Sutton
- Fastest growing and soon to be largest area of crime
- Assists in all normal victimless crime
- Associated with all sorts of crime, from robbery to extortion, drugs, pornography and prostitution
- Are actually eliminating some traditional crimes
- Are almost impossible to prosecute
CORPORATIONS

YESTERDAY'S CRIMINAL IS TOMORROW'S MULTINATIONAL

F-Secure
CORPORATIONS

- Grayware of the oughts is **AD supported software** today

- AD supported is 95% **snooping** and 5% advertising

- If you did not pay for the product, you **are** the product
CORPORATIONS are legal (?)

- "Capitalism is the extraordinary belief that the nastiest of men, for the nastiest of reasons, will somehow work for the benefit of us all." - John Maynard Keynes
GOVERNMENTS

CYBERPUNKS BELIEVE THAT CORPORATIONS WILL SOMEDAY REPLACE GOVERNMENTS

F-Secure.
GOVERNMENTS

- BRADLEY MANNING
- EDWARD SNOWDEN
- MORE REVELATIONS EVERY DAY
- NOT JUST THE US GOVERNMENT, BUT ALL GOVERNMENTS
The whistleblower
I can't allow the US government to destroy privacy and basic liberties
SIX SILOS

AND THE WORLD GETS MORE COMPLICATED EVERY DAY
PRIVACY

*Why* is it the worst threat facing us today?
PRIVACY

- Without privacy, how can you protect your right to a job?
- Without privacy, how can you protect your right to a vote?
- Without privacy how can you protect any right?
- You cannot get back what you lose with the loss of privacy
- Without privacy, no civil rights are possible or enforceable
- How are we losing our privacy or choosing to give it up?
People use multiple devices wherever they go.
NUMBER OF ANDROID SAMPLES RECEIVED, Q3 2012

Q1 2012: 3,063
Q2 2012: 5,033
Q3 2012:
TANSTAAFL

There ain't no such thing as a free lunch
No such thing as a free lunch
No such thing as a free search engine
No such thing as a free webmail
No such thing as a free cloud storage
Mikko Hypponen
@mikkko

The most expensive in-app purchases for "free" mobile games are simply outrageous. Here's Farm Heroes, for ages 4+
pic.twitter.com/is0H4DmTi6

Farm Heroes Saga
King.com Limited
Offers In-App Purchases

*FREE*

In-App Purchases

L Gold Bars package 44,99 €

XL Gold Bars package 94,99 €
Malware distribution across **computer** platforms

Malware distribution across **smartphone** platforms
Disclosure and Disclaimer

By accepting the Terms and Conditions of this Application, you grant Equiliv the authority to use your device's Central Processing Unit ("CPU") to run calculations and process data without limitation. Equiliv will maintain this authority unless the Application has been removed and/or uninstalled from the device. Equiliv will transmit no more than 100MB in data through a wireless or cellular network within a 30 day period. By accepting the terms and conditions, you are granting Equiliv the authority to process data and calculations up to 100MB in total size within a given 30 day period. IN NO EVENT SHALL EQUILIV BE LIABLE (WHETHER UNDER THE LAW OF CONTRACTS, TORTS OR OTHERWISE) FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE OR ANY OTHER MONETARY OR OTHER DAMAGES, FEES, FINES, PENALTIES OR LIABILITIES (COLLECTIVELY "DAMAGES") WHATSOEVER ARISING OUT OF OR RELATING TO THIS APPLICATION OR ANY SOFTWARE CONTAINED IN THIS APPLICATION.
NEW FAMILIES AND VARIANTS RECEIVED
PER QUARTER, Q1-Q4 2012

- ALL THREATS
- Android
- Blackberry
- IOS
- J2ME
- Windows Mobile
- Symbian
MOBILE DEVICES HAVE A PROBLEM

- In each new era of computing, the kind and reach and even the purpose of threats have co-evolved with the current computing model
- The current edge of computing is in mobile devices, and to a certain extent they are not vulnerable to the old threats (viruses, trojans and malware)
- Of course there is malware for mobiles, but pretty much nothing compared to Windows PC’s—this is for several reasons:
  - Mobile systems are more or less a walled garden
  - There is no digital monoculture in mobiles
  - They are new, and have developed in a market wary of security issues
WALLED GARDEN?

- Both the android and the iphone limit the sources of software
- Almost all of the iOS malware has only worked on jailbroken phones
- This also worked for Blackberry and Palm
- Both the Google Play Store and the Apple AppStore can reach out and kill a dirty app for all phones in the world at a single stroke.
MONOCULTURE?

- Whenever a planted forest or field of identical plants exist, they are susceptible to the same diseases and weaknesses.
- This is why the windows environment has taken the brunt of all malware attacks.
- But in mobiles, even the dominant Android OS is configured so differently that the market has **true diversity**.
WHAT IS THE MOBILE THREAT?

- Mobile devices put us in constant and very close proximity to a computing device
- A device with a camera, and microphones, and GPS, and constant internet connection
- The real threat in mobile is not so much to our security, but to our privacy
- And that threat does not have to be mounted on the client device
- The threat can be in the cloud
CLOUD THREAT

- Mobile devices are connected in multiple ways
  - 3GS, 4GS
  - Wi-Fi
  - Bluetooth
  - USB

- Some of these connections can be used for very bad things...

- You might even say, for EVIL!
NO PRIVACY

- When you have no privacy, things can happen to you
- People will know where you are
- People will know what you have said and what you look at
- It is possible to intercept your messages and text, your passwords and credit card numbers, but more important, many people are already tracking nearly everything online.
- Every web page you visit, every friend you make in social media, every location you are at, pretty much everything
- Tracked and recorded and analyzed...think of the possibilities!
FREEDOME

- VPN (encryption tunnel) makes your phone invisible!
- Blocks bad Websites (reputation service)
- Captures malware in the cloud
- Privacy can get you a bargain!
- Log in from anywhere on planet earth
SIMPLE, AND EFFECTIVE
TRY FREEDOME

- Try it for free for two months
- Download it here: freedome.f-secure.com/sticker
- Normal price $5/month, or $29.95/year
- The best protection for your mobile, anytime, anywhere
WE ARE A PIONEER & INNOVATOR IN THE SECURITY INDUSTRY.
Pioneers of security for 25 years

IN SECURITY We make millions of homes and businesses more secure.

EMPLOYEES

OFFICES IN

Europe Asia America

was founded 1988

COUNTRIES

WE WORK WITH OVER 200 OPERATORS

Net Sales (MEUR) 2006

March 2, 2015
We have pioneered security for 25 years.
WE SEE THINGS OTHERS DON'T.
We see things others don't.

MILLIONS
We handle millions of queries to the backend about URLs and binaries.

24/7
We scan, collect and analyze threats.

LAB
F-Secure's security Lab plays a pivotal part in developing security technology and has done for 25 years.

100,000
We detect over 100,000 executables daily.
We protect the irreplaceable anywhere, anytime.
We continue to innovate the future.
WE HAVE A JOB TO DO IN PROTECTING HOW PEOPLE CREATE, SHARE AND STORE CONTENT.
The Big Shift

Mobile Phone Users

1,100,000,000,000

Smartphones

64% of people have more than one device connected to the internet.

24 Billion Internet Users

24/7 People create and share content 24/7.

25% of the people in UK and USA have more than 4 devices connected to the internet.

© F-Secure Confidential
SWITCH
ON
FREEDOM