ETH zürich

Cyber Security

Parlamentariertreffen 2017 – Offiziersgesellschaft des Kt. St. Gallen

Dr. Stefan Frei

- Senior Cyber Security Principal / Accenture

- Dozent Cyber Security / ETH Zurich

frei@techzoom.net | @stefan_frei | 079 222 99 22

What makes the cyber world different?

- Safety vs. security
- Risk perception
- Ownership vs. control
- Plausible deniability
- Innovation & price erosion
- Software eats the world
- Product liability & testing

- Internet of Things
- Data Breaches
- Supply Chain Security

Safety

- the protection against random incidents - unwanted incidents resulting from one or more coincidences.
- **Safety relates to protection from accidents.**

Security

- The protection against intended incidents – incidents resulting from a deliberate and planned act.
- **Security relates to deliberate acts.**

Big Difference

Cyber risks are abstract, a compromise stays undetected for extended periods

- Nature and evolution built humans to survive in the primeval forest
- **Humans have no built-in concept to deal with abstract risks**

No training needed to act instantly and get out of danger

Is this machine infected?
Is data already stolen?

It is extremely difficult to get resources to protect against abstract risks.

Ownership vs. Possession vs. Control

There is a legal distinction between ownership (Eigentum) and possession (Besitz) of an object:

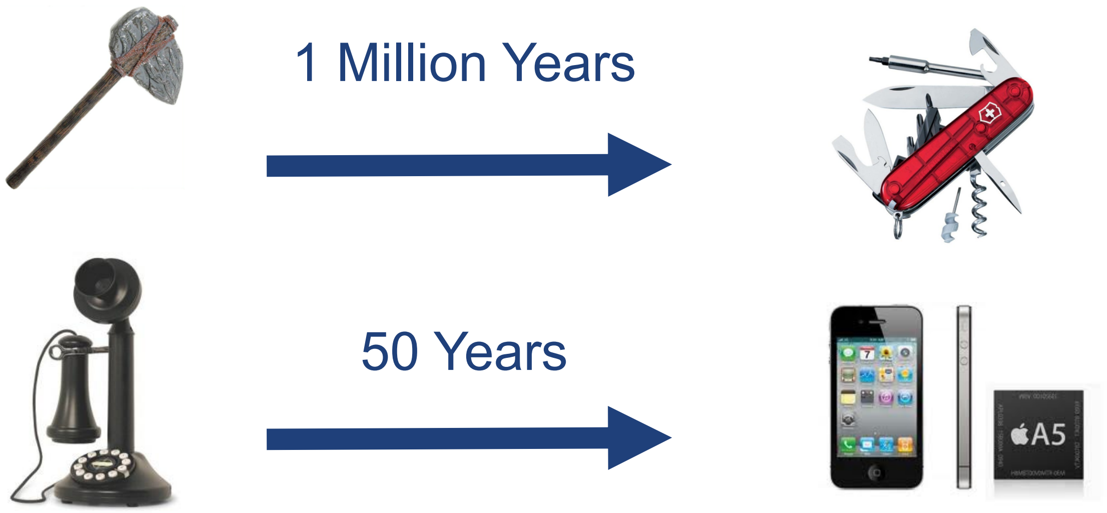
- I am the owner of my car, even if I have lent it to a friend and it is not in my possession. He is in control of the car.

For networked digital goods, neither possession nor ownership imply control

In cyber: Loss of control over your own digital infrastructure – without change of ownership or possession.

In just two decades, new technologies and the Internet transformed society and businesses alike

- We had little time to learn or adopt – as individuals, society nor industry
- We have to adopt to permanent change and high dynamics



1 Million Years

50 Years

Criminals proofed repeatedly to be very fast adopters of new technology.

Nonstop innovation and development of new technologies

Continued miniaturization with increased capabilities while prices erode:

- Todays transistors are **90,000x** more efficient and **60,000x** cheaper than 1971
- A car today would cost **CHF 0.25** and consume **0.2 ml/100 km** of fuel

Drones

3D Printer

Robots

Software Defined Radios

Security assumptions based on the price or the limited availability / performance of a tool become invalid.

Almost everyone has access to, and can afford the latest in cyber weapon technology

Main Battle Tank
≈ 5 M

Fighter Aircraft
≈ 50 M

Frigate
≈ 250 M

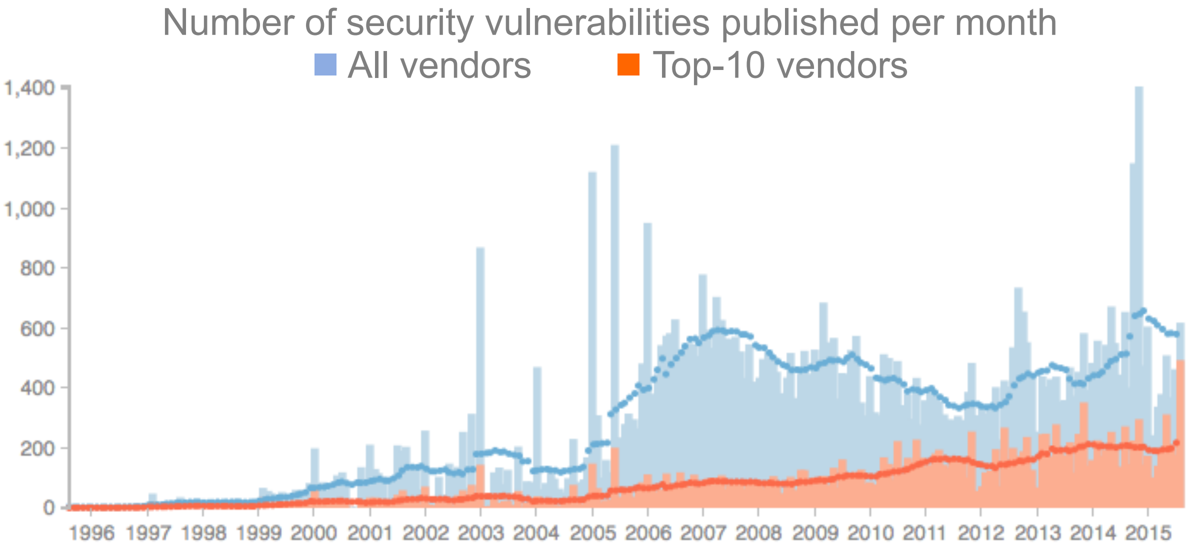
Spy Satellite
≈ 500 M

Market for exploits: 1 Mio for iPhone, 700k for Android exploit
(price ~ market share x security of product)

Plausible Deniability: Cyber weapons can convincingly disguise the origin of the attacker, unlike physical weapons.

The historic monopoly of states to access and operate the latest in weapon technology is now broken.

In spite of increased investment, the software industry at large is still unable to produce secure code



Top 10 vendors

Microsoft
IBM
ORACLE
redhat
mozilla FOUNDATION
Linux
cisco
Google
hp

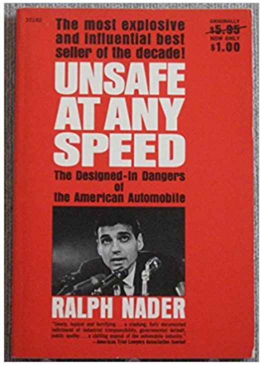
Software eats the world

Complex software with vulnerabilities drives everyday devices – we need to manage vulnerabilities.

There is no product liability for software

Calls for mandatory security standards are always fiercely resisted by the industry using the same arguments:

- The product is safe - accidents are the fault of the user
- Security standards are unnecessary - they will ruin the industry
- Security standards will stifle innovation


10182
The most explosive and influential best seller of the decade!
ORIGINALLY ~~$5.95~~ NOW ONLY $1.00
UNSAFE AT ANY SPEED
The Designed-In Dangers of the American Automobile
RALPH NADER
"Timely, topical and terrifying . . . a slashing, fully documented indictment of industrial irresponsibility, governmental default, public apathy . . . a chilling exposé of the automobile industry."
—American Trial Lawyers Association Journal

- *First tests for aircraft engines: over half of the engines could not pass the initial test.*
- *Ralph Nader's "Unsafe at Any Speed", following disputes, let to the introduction of crash test dummies and seat belts for cars.*

These industries still exist and are major innovators. A lack of quality tests in these industries is unimaginable as of today.

Security updates are product recalls at the user's expense.

Internet of Things

A users perception of risk

Computer	Thermostat	Toaster	Smart Bear	Smart Meter	Smart-TV
dangerous	great	cool	cute	nice	cool
RISKY	**Cool devices**				

The attackers perspective

Computer	Thermostat	Toaster	Smart Bear	Smart Meter	Smart-TV
antivirus, patching	~~great~~	~~cool~~	~~cute~~	~~nice~~	~~cool~~
PREPARED	UNPREPARED				

These devices are complex software driven and networked computers: poorly protected targets facing cyber threats.

Not yet fit for the environment

Personal Computer	IoT Device Industry Control Systems
▪ networked and continuously hardened in battle ▪ designed to withstand **external threats** ▪ secure defaults	▪ ran isolated for decades ▪ designed for **high availability, not security** ▪ insecure defaults
▪ exploit mitigation, antivirus ▪ frequent security updates	▪ old code, no protection ▪ **no security updates**

Known and proven security practice is mostly ignored in the IoT world – we are building a huge future liability.

Traditional products rarely change after delivery, whereas digital products constantly require security updates

- Digital products may have a lifetime of decades and replacement – e.g. when a vendor goes bankrupt – is either very difficult or too expensive

- Many digital devices have to be certified to be used
- By applying a security patch the certification is lost, further use of the device is illegal

Aviation

Medical

You're doomed if you patch – you're doomed if you don't.

Data Breaches

Currently we see a new data breach every 17 days (with 14 Million accounts on average)

215 verified data breaches in the last 10 years with a total of 3’154 Million publicly exposed accounts.

These data breaches became public in 2016:

- Dropbox (68M), LinkedIn (164M) were breached in 2012
- mySpace (359M) in 2008

Until 2016 these 591 Million affected users did not know that their account data was available in the underground for many years.

We must assume that critical data of yet unknown data breaches is silently used in the hands of criminals or nation states **– also today**.

Absence of evidence is not evidence of not being breached

Source: https://haveibeenpwned.com

Data breaches affecting Swiss industry sectors

			Ashley-						Gamerz-		multiple
Data Breaches		Adobe	Madison	Badoo	Dropbox	Gawker	LinkedIn	MySpace	planet	XSplit	breaches
Breach date		Oct 2013	Jul 2015	Jun 2013	Jul 2012	Dec 2010	May 2012	Jul 2008	Oct 2015	Nov 2013	
Publication date		Dec 2013	Aug 2015	Jul 2016	Aug 2016	Dec 2013	May 2016	May 2016	Feb 2016	Aug 2015	
Total exposed accounts	[Millions]	**152.4**	**30.8**	**112.0**	**68.6**	**1.2**	**164.6**	**359.4**	**0.0**	**3.0**	

			Ashley-						Gamerz-		multiple
Industry Sectors	**Total**	Adobe	Madison	Badoo	Dropbox	Gawker	LinkedIn	MySpace	planet	XSplit	breaches
Company Index	[1]										
Fortune 500 (International)	**2,958,767**	441,355	46,143	999,781	200,325	1,039	743,295	616,274	705	719	3%
Consulting (Big 6, International)	**89,672**	24,737	207	2,207	15,925	39	48,038	4,611	2	4	7%
Swiss Market Index SMI	**70,280**	9,180	209	3,832	7,402	9	35,421	17,021	3	3	4%
Industry Sectors - Switzerland											
Banking	**18,565**	2,792	53	512	1,100	22	13,831	677	0	0	2%
Insurance	**5,921**	936	44	671	584	1	3,595	309	0	0	4%
Engergy	**6,107**	1,622	34	466	2,061	1	2,214	213	0	0	8%
Pharma / Chemical	**2,988**	519	18	174	351	1	1,917	127	0	0	4%
Media Sector - Switzerland											
Print Media	**599**	193	10	36	216	0	118	84	0	1	10%
TV & Radio	**93**	23	2	18	28	0	22	14	0	0	16%
Government & Administration - Switzerland											
Federal Administration	**3,070**	907	28	532	545	1	1,123	89	0	0	5%
Cantonal Administration	**7,963**	2,276	45	1,622	2,453	0	1,867	188	1	1	6%
State owned companies	**4,680**	1,222	42	832	1,384	0	1,385	124	0	0	7%
Education (Universities + ETH)	**66,124**	16,794	153	2,937	43,708	6	6,905	2,431	0	20	11%
Popular Mailprovider - Switzerland											
Mail Services	**291,277**	84,242	28,875	110,834	56,317	42	12,769	43,458	180	1,110	16%
Internet Provider (ISP)	**547,796**	241,725	19,234	148,319	118,277	66	54,290	54,731	57	567	17%

Data Source: Stefan Frei

Supply Chain Security

How do you attack an extremely valuable, potentially well defended target?

1. **Find the weakest link**
2. **Attack where they expect it the least**

A lesson from history:
The majority of medieval castles where not taken by direct attack against the enforced perimeter walls
– but through treason or marry-in.

We depend on numerous sub-systems and suppliers, over which we only have limited control.

Long history of supply chain attacks

1970's

- The Soviets managed to replace the comp support bar in IBM typewrites deployed in U.S. embassy to transmit in plain text whatever was written

2008

- Hundreds of card terminals in supermarkets exfiltrate information using mobile network
- The devices were opened, tampered with and perfectly resealed

2012

- NSA's backdoor catalog exposed, targets include Cisco, Juniper, Samsung, and Huawei

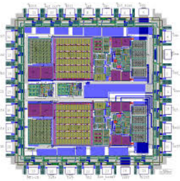
2015

- A clandestine modification of the router's firmware can be utilized to maintain perpetual presence

- NSA employees intercept servers, routers, and other network gear being shipped to organizations targeted for surveillance
- **Others do this as well**

We have limited or no control over the supply chain of everyday (and critical) components

- A globalized production system supplies the components
- Many tiers limit visibility (designers, producers, brokers, sub-system suppliers, major system integrators, etc.)

Design	Build	Integrate	Delivery	Operation
• Code/ logic design development	• Production • Foundry	• Board / System integration	• Delivery	• Operations • Updates
				

> "Frankly, it's not a problem that can be solved . . .
> This is a condition that you have to manage."

Gen Michael Hayden / retired head of CIA and NSA

It is impossible to track the origins of all individual components.

How do we assure the security and integrity of critical devices – in software & hardware?

Industry & Society

Emergency & Defense

Energy, Food & Water

Transport & Logistics

Societies developed binding norms to ensure the safety and security of critical goods – enforced by testing.

Automotive	▪ Extensive testing of new vehicles before admission ▪ Mandatory periodic inspections
Aviation	▪ Extensive testing of new aircraft before admission ▪ Extensive operations and maintenance requirements, periodic inspections
Medicine	▪ Extensive testing of new drugs before admission
Food	▪ Extensive requirements for food processing and delivery ▪ Periodic and surprise inspections

Cyber	▪ **No norms or binding minimum requirements covering the security or the integrity of goods** ▪ **No product liability**	**?!**

We must assume that parts of our critical infrastructure are already compromised

1) **We cannot prevent advanced adversaries from compromising the supply chain of critical devices**

   The bar for such compromises is low - as long as the chance of detection is low

2) **Given the increasing dependency of our society and economy on such devices, we should no longer ignore this threat**

   The integrity of delivered goods will have to be challenged and questioned to a greater extent

We have to systematically verify the integrity & security of critical components

States will have to build a solid cyber testing capability (hardware & software reverse engineering) in the future.

Absence of evidence is not evidence of absence

"Ignoring reality is not an effective way to get healthier, or smarter, or safer, even though it might temporarily make you feel better"

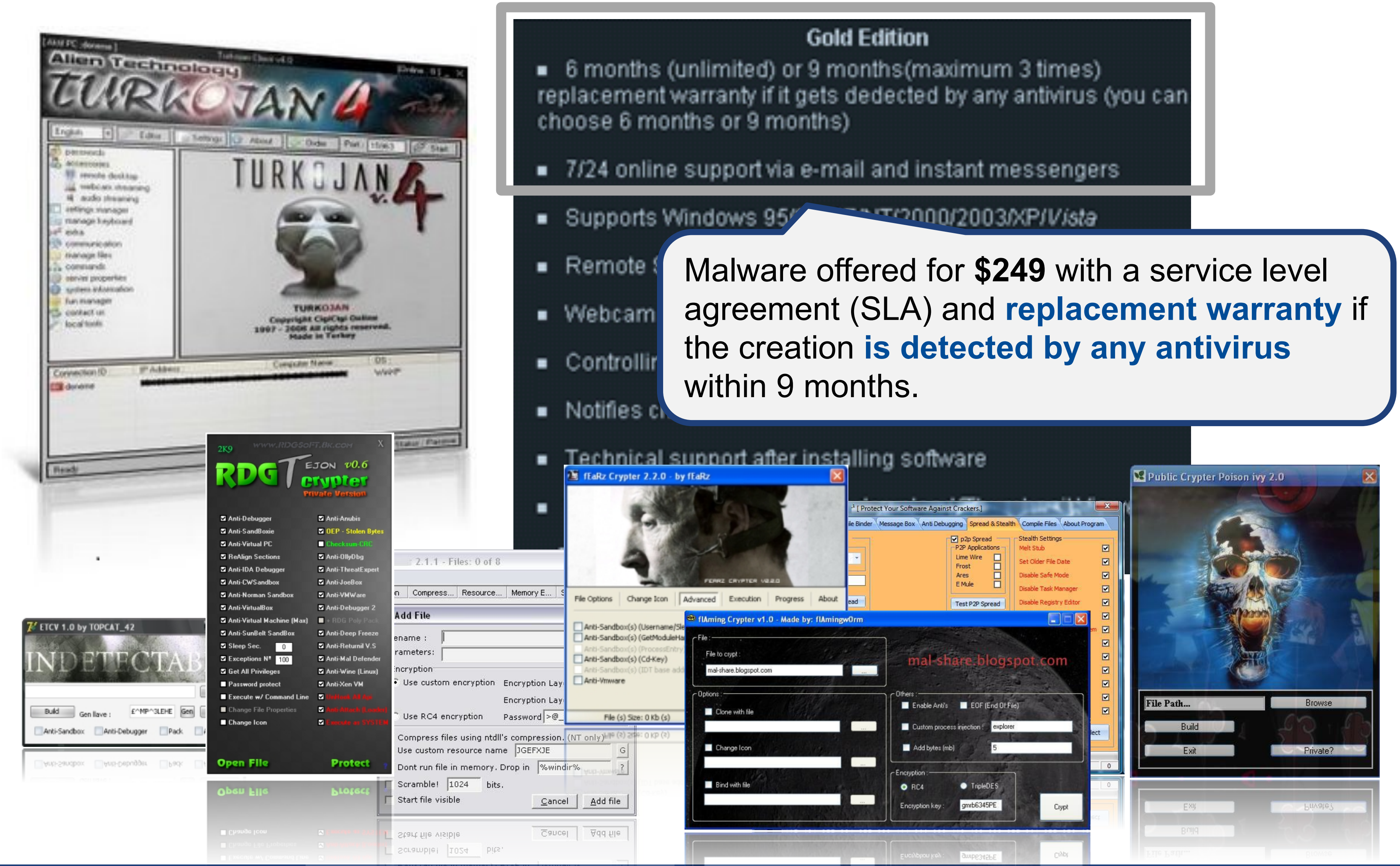
Bruce Schneier

Thank you

Threat Actors & Attackers

	Attacker	Objectives	Resources	Proceeding
Targeted	Nation States, Agencies	• Information • Fighting Crime/Terrorisms • Espionage • Sabotage	• Enormous financial resources • Focus on result, not cost	• Build & buy know-how • Persistent & well hidden attacks • Subversion of supply chain
	Terrorists	• Damage • Attention • Manipulation of politics • Fear Uncertainty and Doubt (FUD)	• Considerable financial resources • Potentially large network of supporters	• Buy know-how on black market • Physical attacks
	(Organized) Crime	• Financial	• Business • Make money on long term • Profit/loss driven	• Existing gangs • Per case groups of specialists • Bribery
Opportunistic	Hacktivists, Groups	• Mass attention • Damage • Denounce vulnerabilities in systems/organizations	• Minimal financial resources • Large reach	• Highly motivated amateurs & specialists • Develops unpredictable momentum
	Vandals, Script Kiddies	• Fame • Reputation	• Minimal financial resources and know-how	• Available tools

Thriving Underground

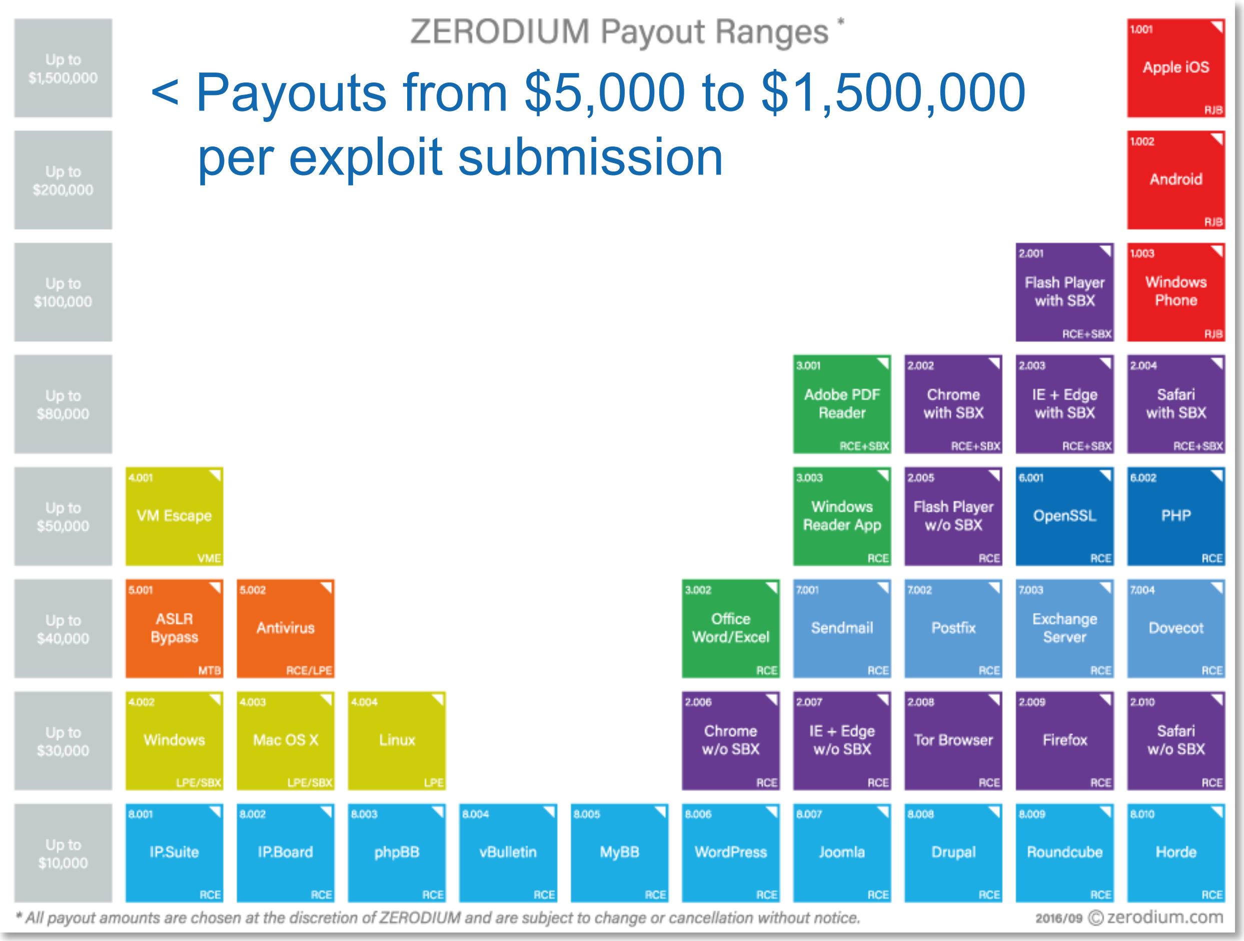


Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/ T/2000/2003/XP/Vista
- Remote
- Webcam
- Controllir
- Notifies c
- Technical support after installing software
-

Malware offered for **$249** with a service level agreement (SLA) and **replacement warranty** if the creation **is detected by any antivirus** within 9 months.

Exploit Broker - Zerodium



ZERODIUM Payout Ranges *

< Payouts from $5,000 to $1,500,000 per exploit submission

Up to $1,500,000										1.001 Apple iOS RJB
Up to $200,000										1.002 Android RJB
Up to $100,000									2.001 Flash Player with SBX RCE+SBX	1.003 Windows Phone RJB
Up to $80,000							3.001 Adobe PDF Reader RCE+SBX	2.002 Chrome with SBX RCE+SBX	2.003 IE + Edge with SBX RCE+SBX	2.004 Safari with SBX RCE+SBX
Up to $50,000	4.001 VM Escape VME						3.003 Windows Reader App RCE	2.005 Flash Player w/o SBX RCE	6.001 OpenSSL RCE	6.002 PHP RCE
Up to $40,000	5.001 ASLR Bypass MTB	5.002 Antivirus RCE/LPE				3.002 Office Word/Excel RCE	7.001 Sendmail RCE	7.002 Postfix RCE	7.003 Exchange Server RCE	7.004 Dovecot RCE
Up to $30,000	4.002 Windows LPE/SBX	4.003 Mac OS X LPE/SBX	4.004 Linux LPE			2.006 Chrome w/o SBX RCE	2.007 IE + Edge w/o SBX RCE	2.008 Tor Browser RCE	2.009 Firefox RCE	2.010 Safari w/o SBX RCE
Up to $10,000	8.001 IP.Suite RCE	8.002 IP.Board RCE	8.003 phpBB RCE	8.004 vBulletin RCE	8.005 MyBB RCE	8.006 WordPress RCE	8.007 Joomla RCE	8.008 Drupal RCE	8.009 Roundcube RCE	8.010 Horde RCE

* *All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.*

2016/09 © zerodium.com

The more secure or prevalent the software, the higher the price

Source: www.zerodium.com

What do these events have in common

CloudPet Data Breach

In January, the maker of teddy bears that record children's voices and sends them to family and friends via the internet left their database publicly exposed. **821k records with children's names** and references to portrait photos and **voice recordings** were exposed.

January, 2017
https://haveibeenpwned.com

Largest DDoS attack ever delivered by botnet of hijacked IoT devices

A giant botnet made up of hijacked internet-connected things like cameras, lightbulbs, and thermostats has launched the largest DDoS attack ever against a top security blogger Brian Krebs.

September, 2016
http://www.networkworld.com

Smart meters in Spain can be hacked to hit the National power network

The researchers explained that poorly protected credentials stored in the devices could let attackers gain access of smart meters, they were able to take full control of any device, modify its unique ID to impersonate other customer or use the smart meter for launching attacks against the power network.

October, 2014
http://http://securityaffairs.com