

1. Cybercrime: Threat Landscape

Digital Forensics and Cybercrime course
Prof. Zanero

Recall: Security, Risk, Threat

Risk: statistical and economical evaluation of the exposure to damage because of the presence of vulnerabilities and threats.

$$\text{Risk} = \underbrace{\text{Asset} \times \text{Vulnerabilities}}_{\text{controllable variables}} \times \underbrace{\text{Threats}}_{\text{independent variable}}$$

Security: managing risk vs. cost

Threat landscape

Three “dimensions” for threats:

- **Internal vs external**
- **Generic vs targeted**
- **Financially motivated vs others**

A Gartner quadrant of threats

	Generic	Specific
Internal	Disgruntled employee	Socially-engineered or dishonest employee 
External	Criminals, usually looking to make \$\$\$ 	A variety of advanced attackers 



= financially motivated (mostly/exclusively, if solid)

Internal threats



MALICIOUS INSIDERS

Employees or partners who misuse their legitimate access to confidential data for personal gain



INSIDE AGENTS

Malicious insiders recruited by external parties to steal, alter, misuse or delete confidential data



EMOTIONAL EMPLOYEES

Emotional attackers who seek to cause harm to their organization as revenge for something perceived wrongly



RECKLESS EMPLOYEES

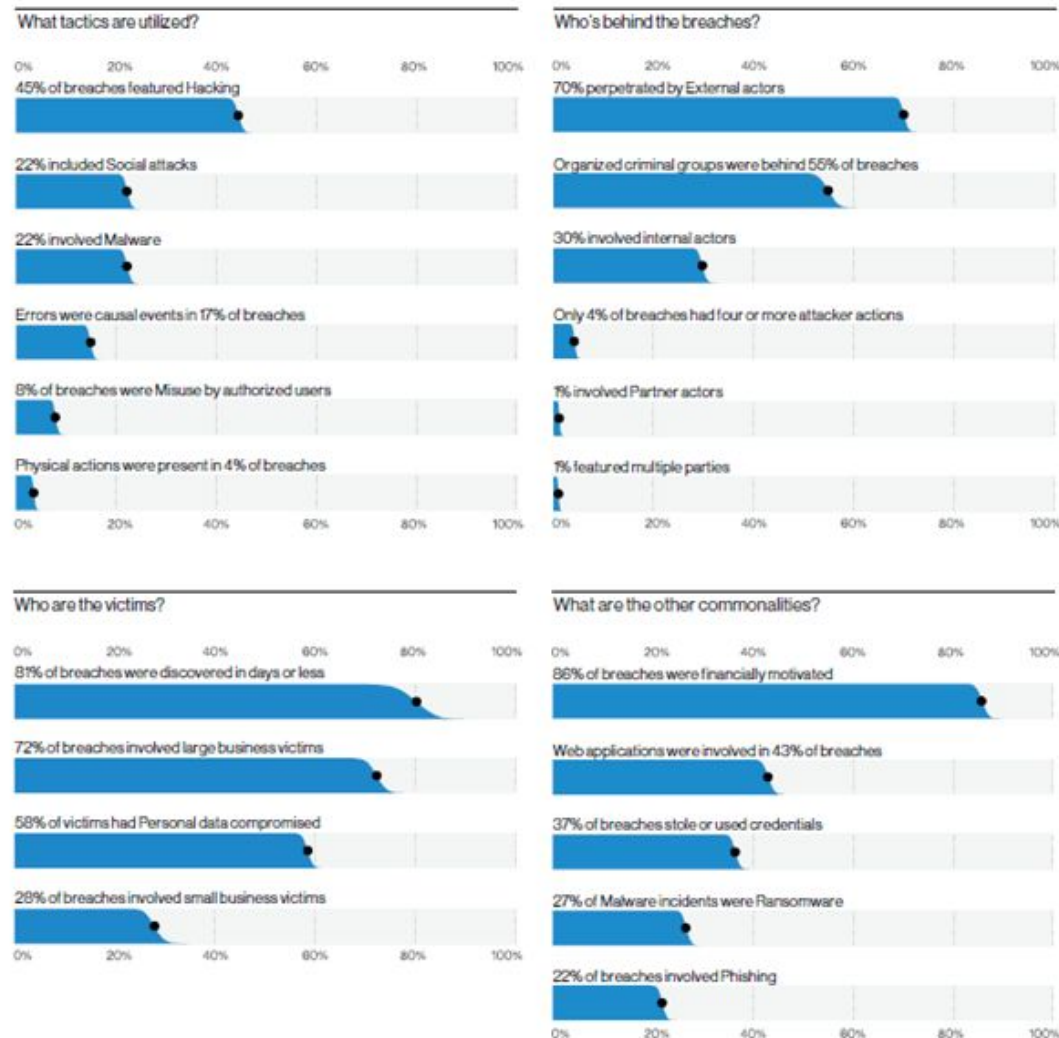
Employees or partners who neglect the rules of an organization's cybersecurity policy



THIRTY-PARTY USERS

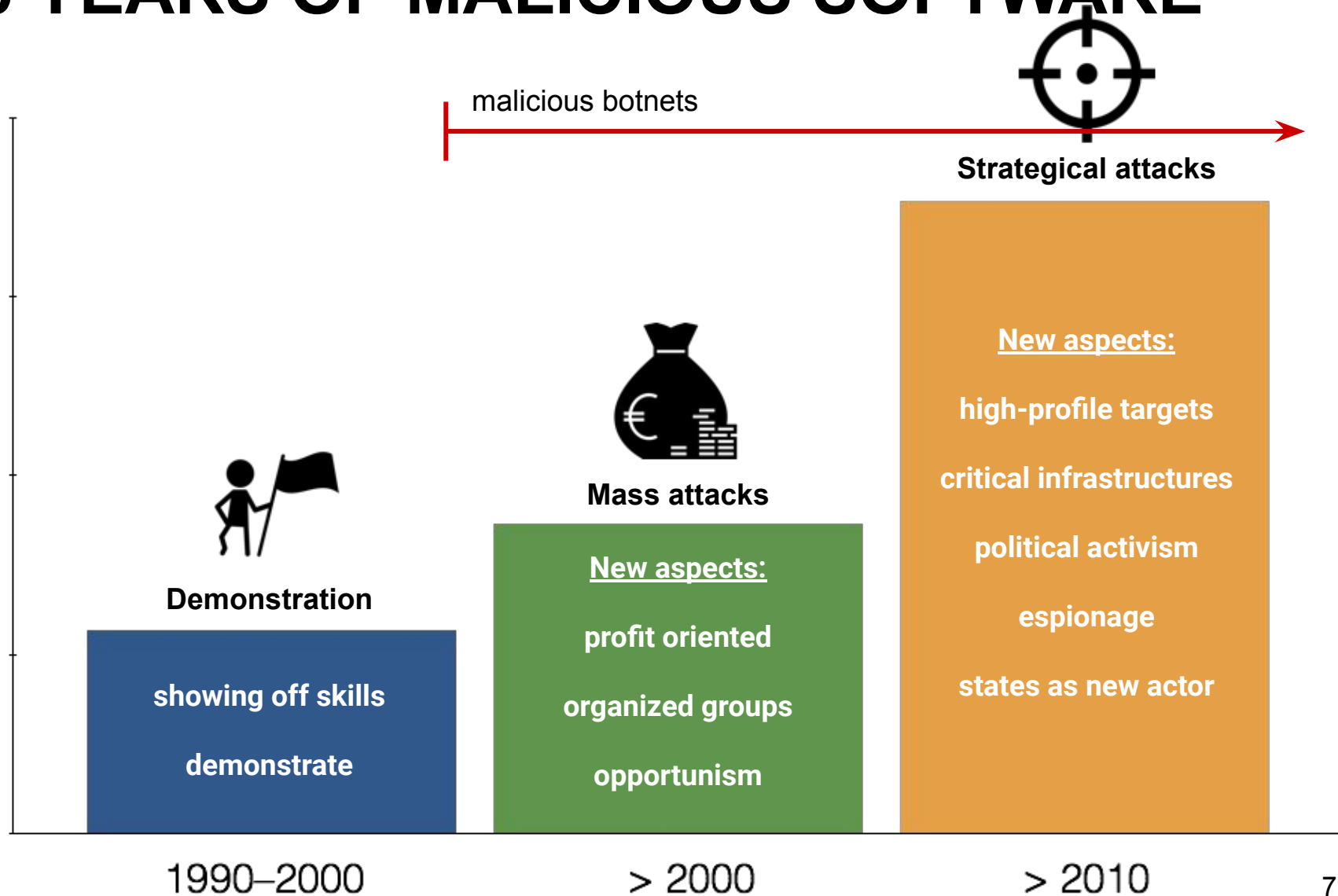
Third-party vendors who take advantage of their access to compromise the security of sensitive information

Data breaches and targeted attacks



Source: <https://enterprise.verizon.com/resources/reports/dbir/>

30 YEARS OF MALICIOUS SOFTWARE

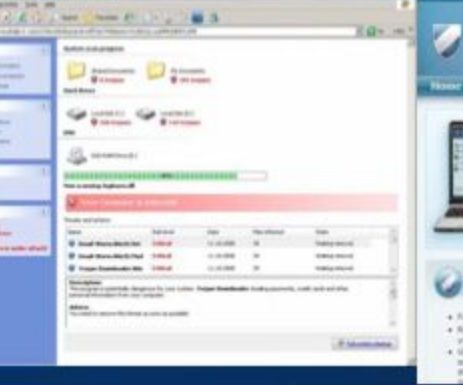
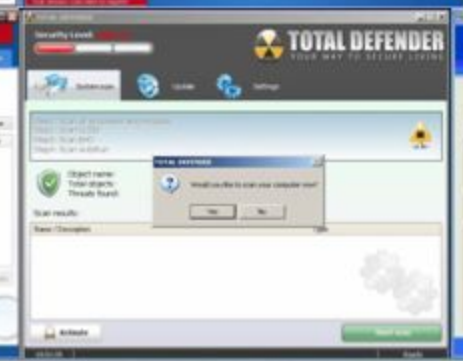


Financially-oriented attacks

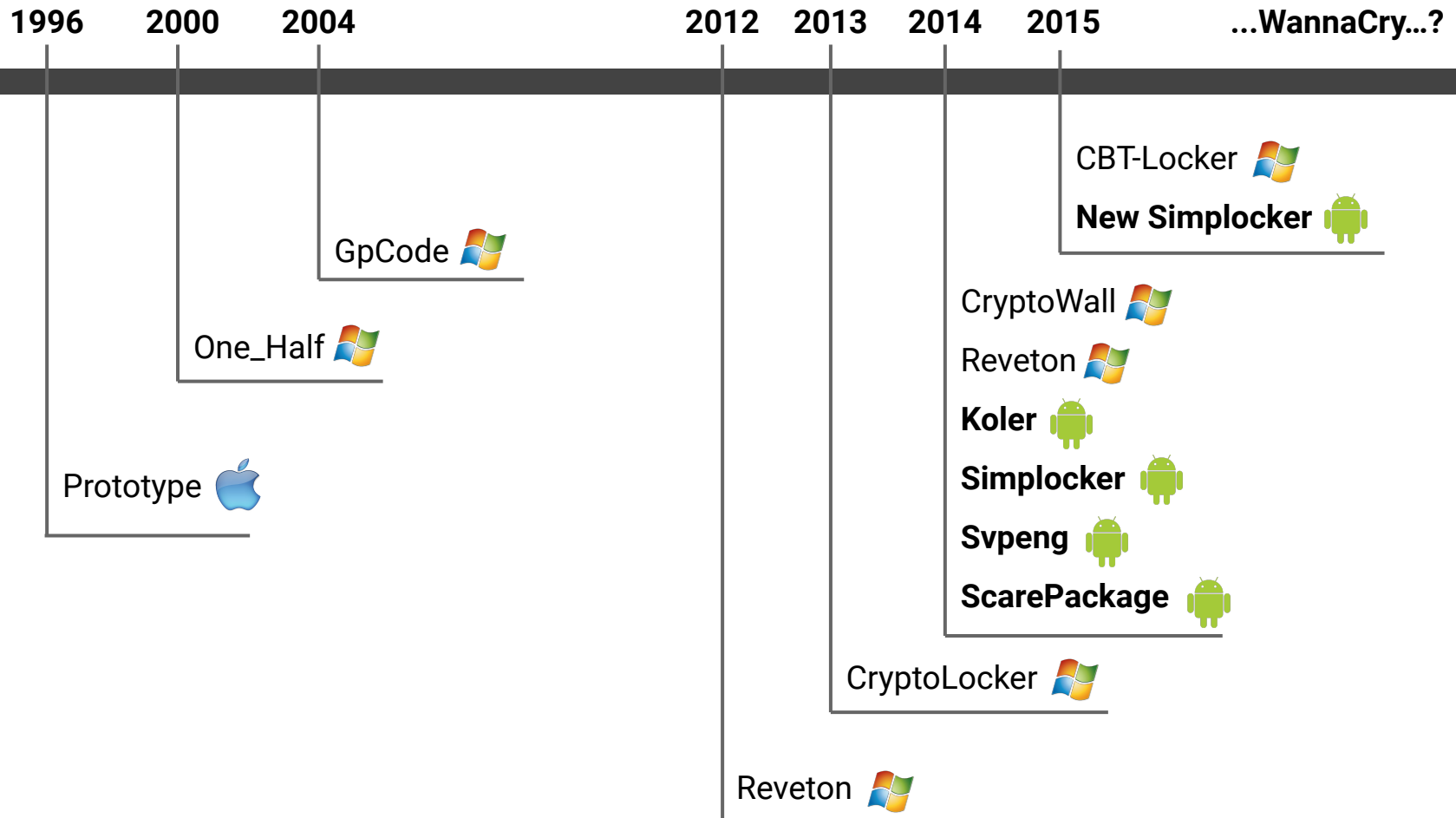
- The attackers are now interested in **monetizing** their attacks

Financially-oriented attacks

- The attackers are now interested in **monetizing** their attacks
- **Direct** monetization
 - Credit card / bank account fraud
 - Ransomware
 - Fake AVs
 - Premium calls (dialers) - almost extinguished



BRIEF HISTORY OF RANSOMWARE



Your personal files are encrypted.



Your personal files are encrypted.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 72 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' to connect to the secret server and follow instructions.



WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

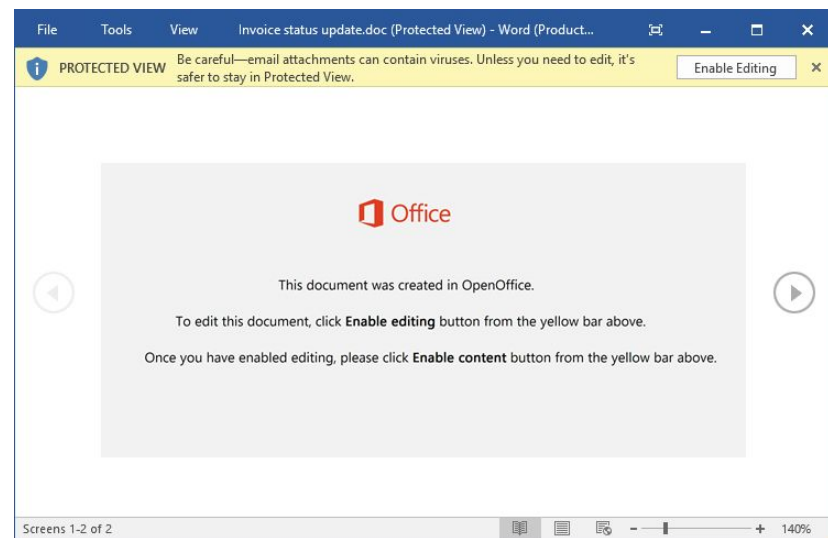
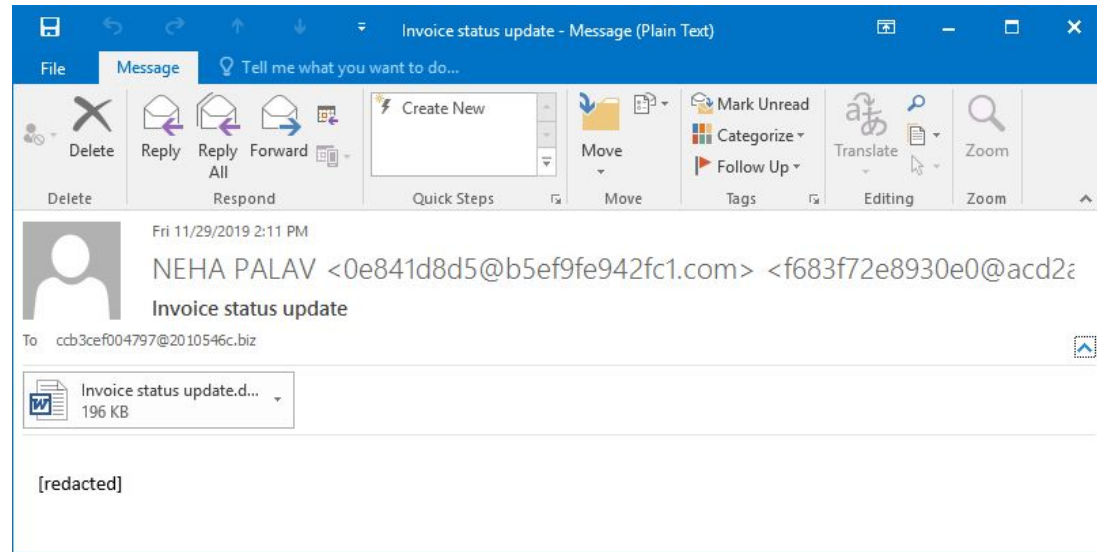
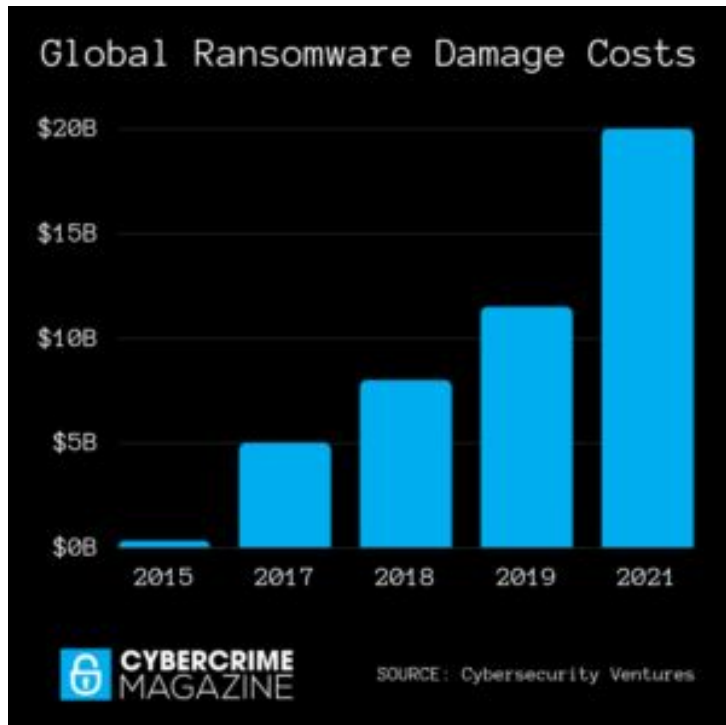
View

71:59:07

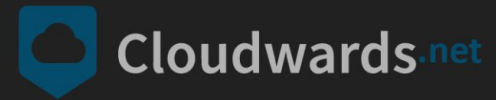
Next >>

can open it and use copy-paste for address and key.

Ransomware attacks



RANSOMWARE STATISTICS



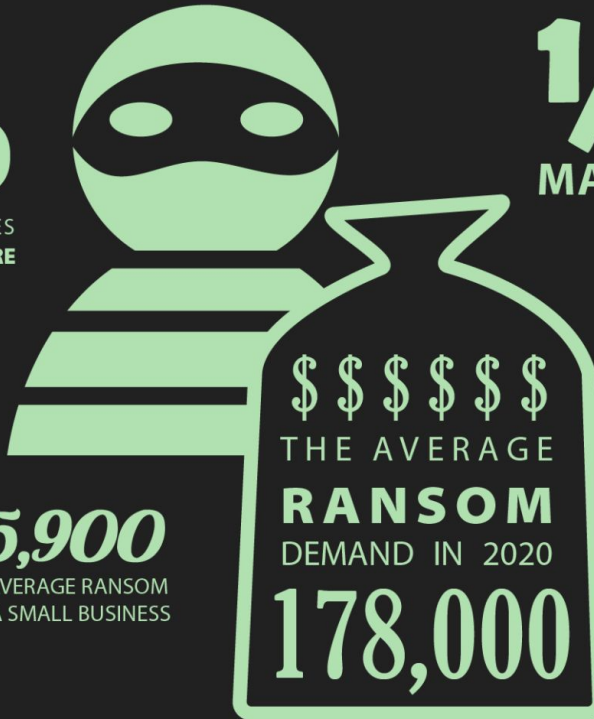
51%
OF SURVEYED BUSINESSES
WERE HIT BY RANSOMWARE
IN 2020

HOW MUCH

RANSOMWARE KITS
COST ON THE DARK WEB



\$5,900
THE AVERAGE RANSOM
FOR A SMALL BUSINESS



\$\$\$
THE AVERAGE
RANSOM
DEMAND IN 2020
178,000

1/4 OF RANSOMWARE
VICTIMS
MAKE PAYMENTS
TO HACKERS

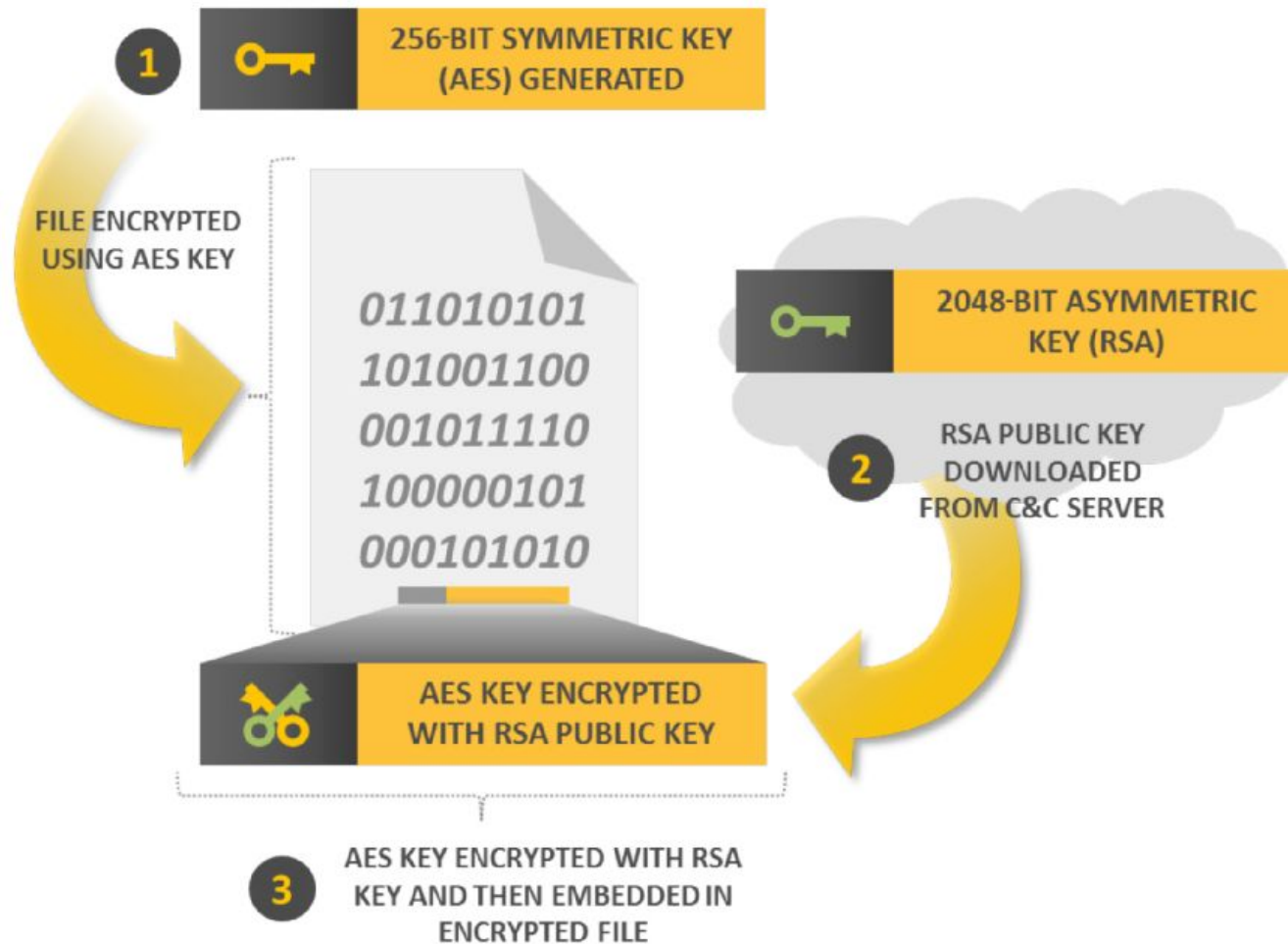
HOW
OFTEN
a company will be hit
by ransomware in
2021



€ 10 MILLION

The largest 2020 ransomware demand, totalling around \$11.8 million,
made to French construction firm Bouygues

Encryption mechanism



Financially-oriented malware

- The attackers are now interested in **monetizing** their malware
- **Direct** monetization
 - Credit card / bank account fraud
 - Ransomware
 - Fake AVs
 - Premium calls (dialers) - almost extinguished
- **Indirect** monetization
 - Information gathering
 - abuse of computing resources
 - rent or sell botnet infrastructures

BOTNET

is a combination of the words "robot" and "network"

Infection

1

The computers are infected with malicious software



Rise of the Bots

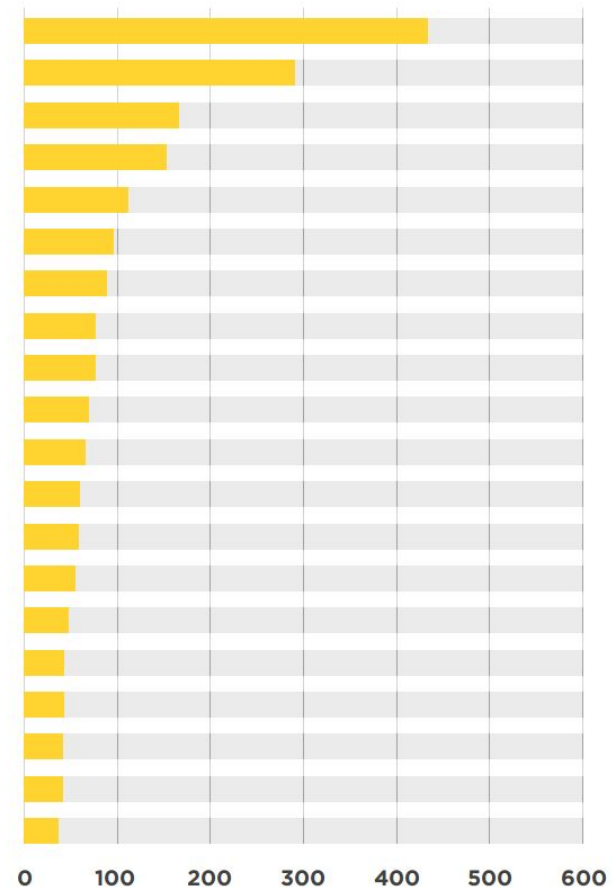
- Abuse of IRC bots (IRCwars):
 - IRCwars: one of the first documented DDoS attacks
- 1999: trino0 "DDoS attack tool"
 - originally ran on Solaris (later ported to Windows)
 - setup of the botnet was mostly manual
 - August 1999: DDoS attack against a server at University of Minnesota using at least 227 bots
(<http://staff.washington.edu/dittrich/misc/trino0.analysis>)
- 2000s: DDoS attacks against high profile websites (Amazon, CNN, eBay) got huge media coverage

Geolocation of botnet C&Cs

Rank	Country		Q2 2020	% Change Q on Q
#1	United States		896	7%
#2	Russia		812	32%
#3	Netherlands		337	61%
#4	Germany		185	7%
#5	Singapore		131	157%
#6	France		108	35%
#7	Great Britain		89	37%
#8	China		74	-15%
#9	Bulgaria		72	38%
#10	Hungary		70	New Entry

Type of malware families

Rank	Q2 2020	% Change Q on Q	Malware Family	Description
#1	436	772%	AgentTesla	Credential Stealer
#2	290	-46%	Lokibot	Credential Stealer
#3	169	New entry	RedLineStealer	Credential Stealer
#4	156	51%	NanoCore RAT	Remote Access Tool (RAT)
#5	112	-27%	Gozi	e-banking Trojan
#6	98	-5%	AZORult	Credential Stealer
#7	92	1%	RemcosRAT	Remote Access Tool (RAT)
#8	74	23%	njrat	Remote Access Tool (RAT)
#9	74	New entry	DanaBot	Credential Stealer
#10	69	17%	ArkeiStealer	Credential Stealer
#11	67	63%	KPOTStealer	Credential Stealer
#12	62	New entry	IcedID	e-banking Trojan
#13	61	New entry	AveMaria	Remote Access Tool (RAT)
#14	55	-18%	Adwind	Remote Access Tool (RAT)
#15	51	21%	NetWire	Remote Access Tool (RAT)
#16	47	New entry	QNodeService	Remote Access Tool (RAT)
#17	47	57%	RaccoonStealer	Credential Stealer
#18	46	-4%	Pony	Credential Stealer
#19	45	105%	AsyncRAT	Remote Access Tool (RAT)
#20	43	New entry	Zloader	Loader





Identity Theft Resource Center

2015 Data Breach Stats



How is this report produced? What are the rules? See last page of report for details.

Report Date: 5/26/2015

Page 11 of 11

Totals for All Categories :

of Breaches: 315

of Records:

102,962,007

% of Breaches: 100.0

% of Records:

100.0%

2015 Breaches Identified by the ITRC as of: 5/26/2015

Total Breaches: 315
Records Exposed: 102,962,007

Federal Eye

Hackers stole personal information from 104,000 taxpayers, IRS says



A



By **Lisa Rein** and **Jonnelle Marte** May 26 at 5:08 PM

Follow @Reinlwapo

Follow @jonnelle



Most Read Politics

1 **How the U.S. can arrest FIFA officials in Switzerland, explained**



Your Identity Is Worth \$5 on the Black Market

In other words, significantly less than it's worth to you

By [Eliana Dockterman @edockterman](#) | Aug. 26, 2013 | 10 Comments



Hackers have access to your data, and they're selling it for only \$5, according to an article in GigaOm.

You enter a great deal of information about yourself online every day. Whether you're inputting your credit card information on a site like Amazon, verifying an account with your social security number or simply checking your Twitter feed, you're exposing yourself to hackers. All your online information can be bundled and sold



Nease / MCT Graphics via Getty Images

Anatomy of a drive-by download

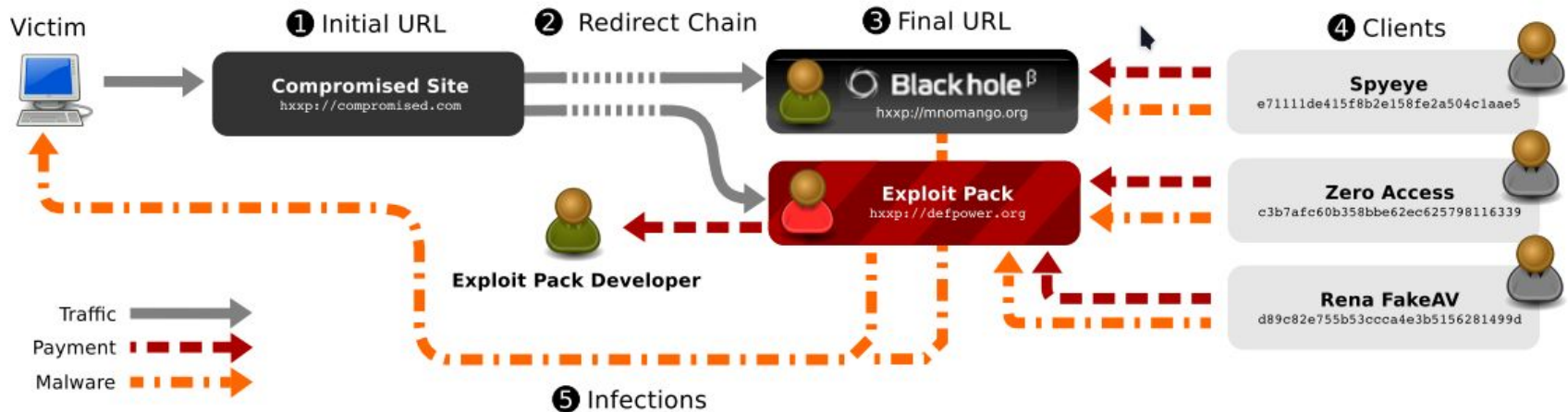


Figure 1: The drive-by-download infection chain. Within the exploit-as-a-service ecosystem, two roles have appeared: *exploit kits* that aid miscreants in compromising browsers (③), and *Traffic-PPI* markets that sell installs to clients (④) while managing all aspects of a successful exploit (①,②,③).

"Manufacturing Compromise: The Emergence of Exploit-as-a-Service"

<http://cseweb.ucsd.edu/~voelker/pubs/eaas-ccs12.pdf>

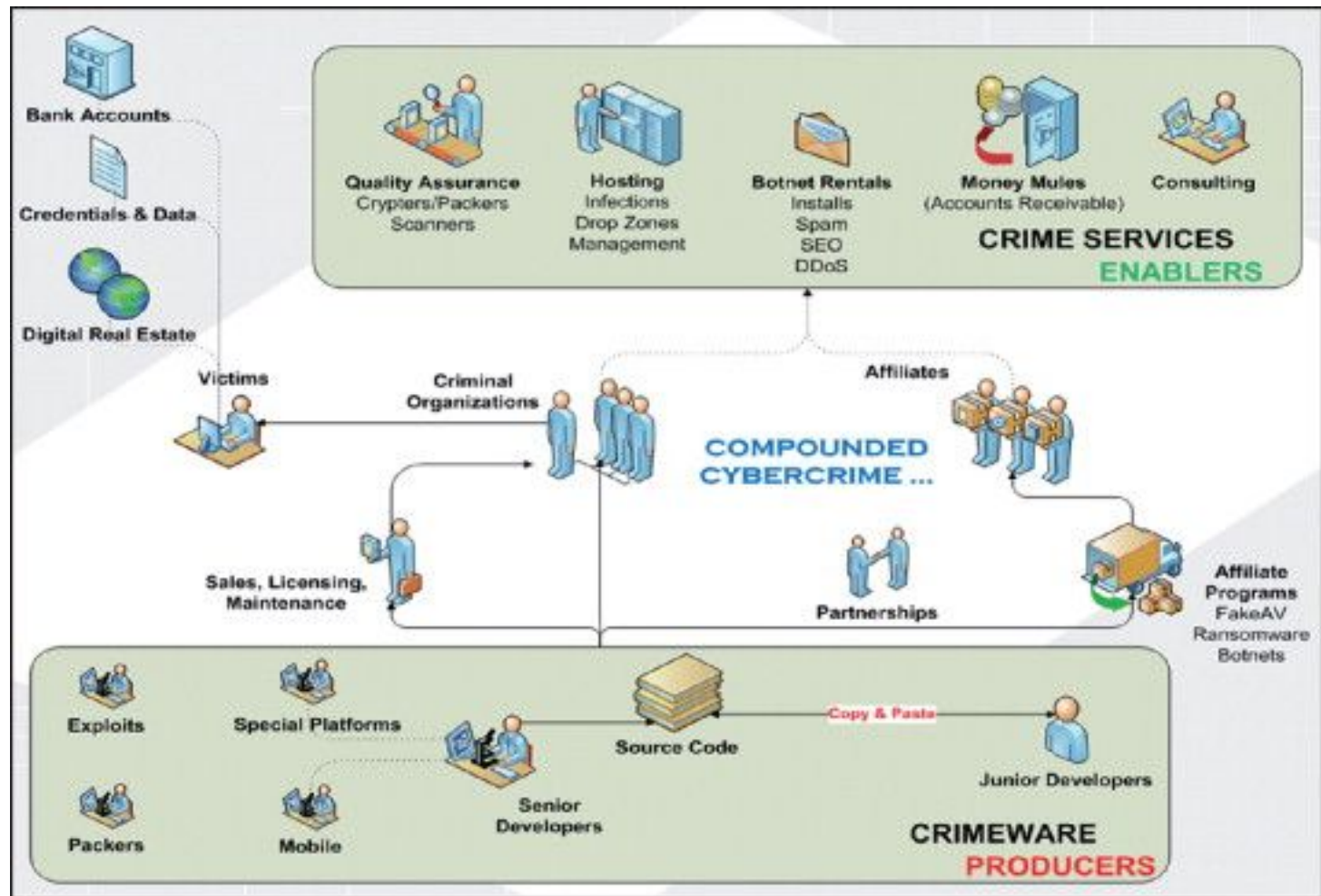
The Cybercrime Ecosystem

- Organized groups
- Various "activities"
 - exploit development and procurement
 - site infection
 - victim monitoring
 - selling "exploit kits"
 - They even offer support hotlines...

The screenshot shows the homepage of LoadsSell.com, a website for botnet rental services. The header features the title "Botnet Rental for Installs" and a service offering: "Load Service: Buy \$110 / 1K installs (USA)". A central logo for LoadsSell.com is displayed. To the right, there are language selection buttons for "RUS" and "ENG", and a "CONTACTS" section listing support channels: "Support #1: ICQ 59612", "Support #2: ICQ 59076", and "Support #3: ICQ 975". The main content area is divided into two columns. The left column, titled "ABOUT US", describes the service as a brand new offering for unique loads from different countries, offering a discount for regular customers. The right column, titled "OUR PRICE:", contains a table of pricing for various regions.

OUR PRICE:	
United States	\$110
All world	\$16
Mix with no Asia	\$30
Asia	\$8
Canada	\$100
Gb	\$150
Please contact with supports about prices for other countries	

Ecosystem (a partial view)



Exploitation kits sales

Post Reply darkode.com Forum Index » BUY / SELL / TRADE View previous topic View next topic

Buy spoils and vulnerabilities of a browser

Author	Message
J.P.MORGAN LEVEL 1 Joined: 16 Jan 2013 Posts: 8 Rep: 1425 Location: Private	<p>Buy spoils and vulnerabilities of a browser QUOTE</p> <p>Dear ladies and gentlemen! In light of recent events, we look to build a new exploit kit framework. Truly original and set apart from anything else on today's market. This will be the new dap age.</p> <p>Project's core: We have budgeted \$450,000 to buy vulnerabilities of a browser and its plugins, which will be used only by us afterwards! Without participating in public (except force majeure events, when a vulnerability becomes public not through our fault).</p> <p>We buy not only ready exploits, but also descriptions of vulnerabilities (with further combined finalization by our specialists).</p> <p>Verification : https://darkode.com/viewtopic.php?t=11759 (L1)</p> <p>Contacts : Jabber: gugusik7d@default.rs or PM</p> <p>P.S: You can't flog a public exploit. P.S.S: People without reputation use a mutually agreed backer to work with us. P.S.S.S: As you understand, not every exploit costs 450,000, we guarantee appropriate prices.</p> <p>Fraud ,cash out , malware,Spam, DDOS .</p>

Sun Oct 13, 2013 4:59 am PROFILE PM WWW AIM YIM MSN ICQ

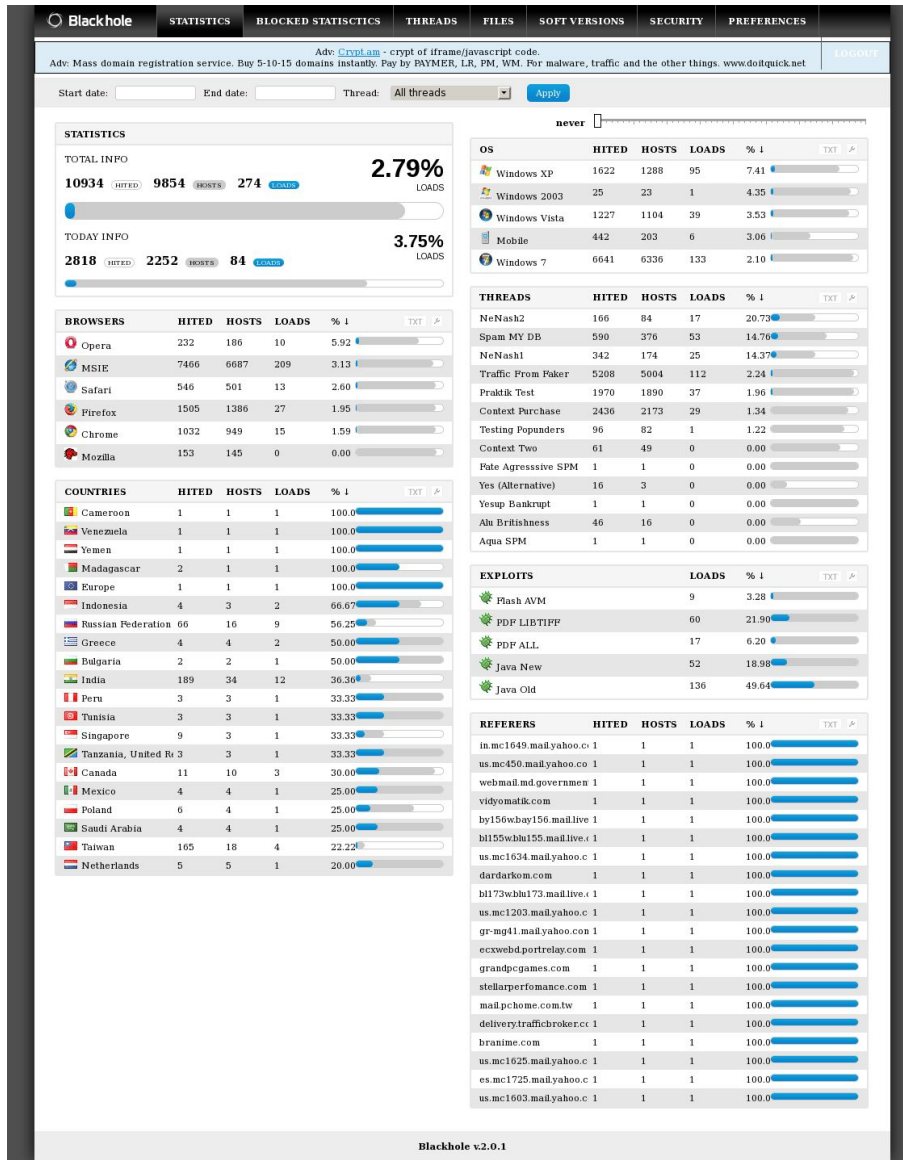
Display posts from previous: All Posts Oldest First Go

Post Reply darkode.com Forum Index » BUY / SELL / TRADE All times are GMT



Gudmunds, indicted for running dark0de

Blackhole: famous exploit kit



Dmitry "Paunch" Fedotov, arrested
October 2013 - Author of Black Hole



Tox - Viruses

toxic [redacted] .onion

Summary

Viruses

1

Infected

2

Of which paid

0

Total profit

0.00 \$

To withdraw (net)

0.00 \$

Your BTC address

Withdraw

Create a virus

Ransom - \$

Ransom in dollars (min. 50)

Notes*

Optional, ex: For Mr. Smith

Message**

Optional message for the victims

Captcha

Captcha

BYaLdGxCM



Create

* Notes are private, they're just to keep track of your virus. Victims will not see them! (max 200 chars)

** Message will be shown in the ransom page to the victims (max 1500 chars | no html)

Your viruses


Monetization on the dark web

Buy CC	CC Orders	Buy Dumps	Dump orders	Checker	Tickets	Hello, 	 Cart (1) 9.45\$	Balance: 3.0\$	Add mo
									<input checked="" type="checkbox"/>

Didn't find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - [Bulk Orders - Low Prices!](#)

<input type="checkbox"/>	Bin	Card	Debit/Credit	Mark	Expres	Track 1	Code	Country	Bank	Base	Price
<input type="checkbox"/>	371736	 AMEX	CREDIT		07/15	Yes	110	 United States, 23456, Virginia Beach, VA	BANK OF AMERICA	American Sanctions 14 	30\$
<input type="checkbox"/>	371555	 AMEX	CREDIT		09/16	Yes	101	 United States, 80123, Littleton, CO	BANK OF AMERICA	American Sanctions 14 	30\$
<input type="checkbox"/>	371736	 AMEX	CREDIT		03/17	Yes	101	 United States, 60540, Naperville, IL	BANK OF AMERICA	American Sanctions 14 	30\$
<input type="checkbox"/>	371564	 AMEX	CREDIT		05/15	Yes	110	 United States, 77081, Houston, TX	BANK OF AMERICA	American Sanctions 14 	30\$
<input type="checkbox"/>	371554	 AMEX	CREDIT		04/17	Yes	101	 United States, 37027, Brentwood, TN	BANK OF AMERICA	American Sanctions 14 	30\$

Dark web caters also to other crimes



Currency
฿ ₺ \$


Shopping Cart
0 item(s) - \$0.00

Welcome visitor you can [login](#) or [create an account](#)


[Home](#) | [Wish List \(0\)](#) | [My Account](#) | [Shopping Cart](#) | [Checkout](#)

Package DealsPistolsRiflesShotgunsNFA WeaponsAccessoriesArmorAmmunitionMilitary


Specials



AKM Gen2
~~\$3,605.98~~ \$2,800.00
[Add to Cart](#)















CIA Model PAP
~~\$1,956.64~~ \$1,401.56
[Add to Cart](#)



CZ-USA P07 DUTY
~~\$920.82~~ \$820.00
[Add to Cart](#)

This is a site catalog, please email us with your order. All items sold under your choice of .onion escrow.

Bestsellers

 <p>Walther P22 \$752.65 Add to Cart</p>	 <p>Glock 17 & Gemtech Tundra \$2,223.45 \$1,599.99 Add to Cart</p>	 <p>Beretta PX4 Storm Type F \$1,223.90 Add to Cart</p>	 <p>9x19mm Parabellum \$0.30 Add to Cart</p>
 <p>Glock 26 Gen4 \$1,027.94 Add to Cart</p>	 <p>Glock 17 Gen4 \$1,027.94 Add to Cart</p>	 <p>CIA Model PAP \$1,956.64 \$1,401.56 Add to Cart</p>	 <p>Glock 32 Gen4 \$1,027.94 Add to Cart</p>
			

Categories

- Package Deals (4)
- Pistols (87)
- Rifles (66)
- Shotguns (4)
- NFA Weapons (84)
- Accessories (68)
- Armor (28)
- Ammunition (33)
- Military (44)

Shipping Points

- Australia (NewCastle) - \$290
- Australia (Perth) - \$340
- Austria (Graz) - \$270
- Canada (Toronto) - \$190
- Canada (Vancouver) - \$190
- France (Le Mans) - \$270
- Germany (Dresden) - \$220
- Ireland (Tuam) - \$290
- Italy (Modena) - \$280
- N. Ireland (Belfast) - \$340
- Netherlands (Breda) - \$320
- Norway (Drammen) - \$240
- Russia (Vyborg) - \$190
- Finland (Tornio) - \$290

Money mules

