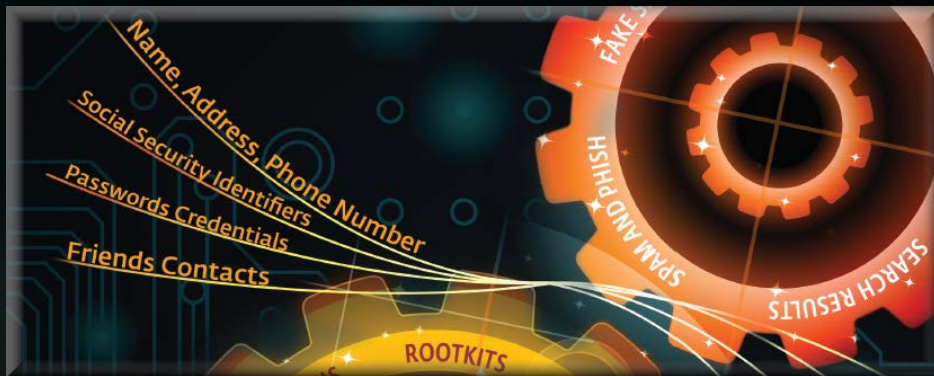


Facing the Challenge

The reality of malware today...





The Industrialization of malware

- Well-funded production and distribution systems
- Well-documented in security circles
- Not well understood at C-level
- Not well known at the user-level
- Produces over 200,000 threats per day (new malware + variants)





Know the enemy

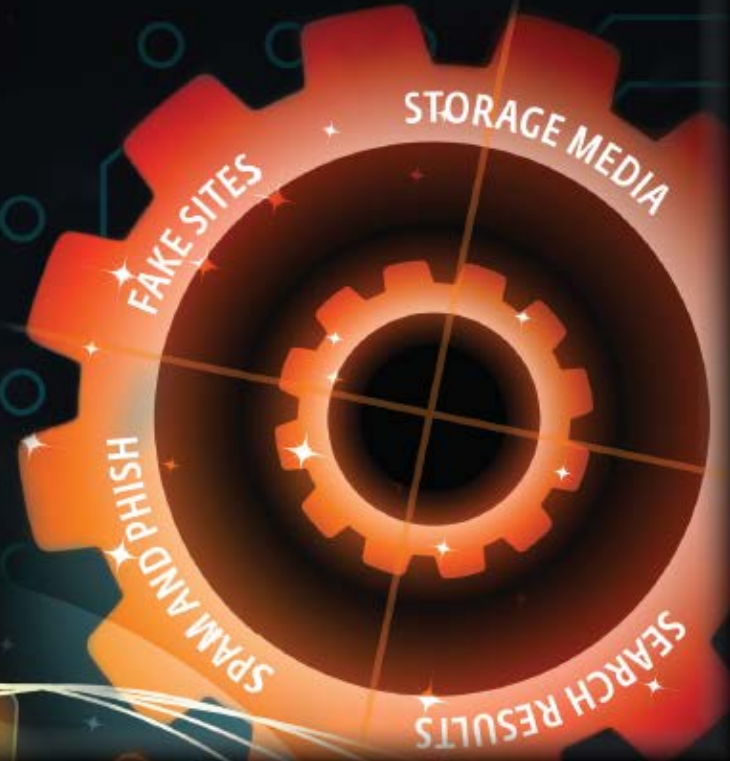


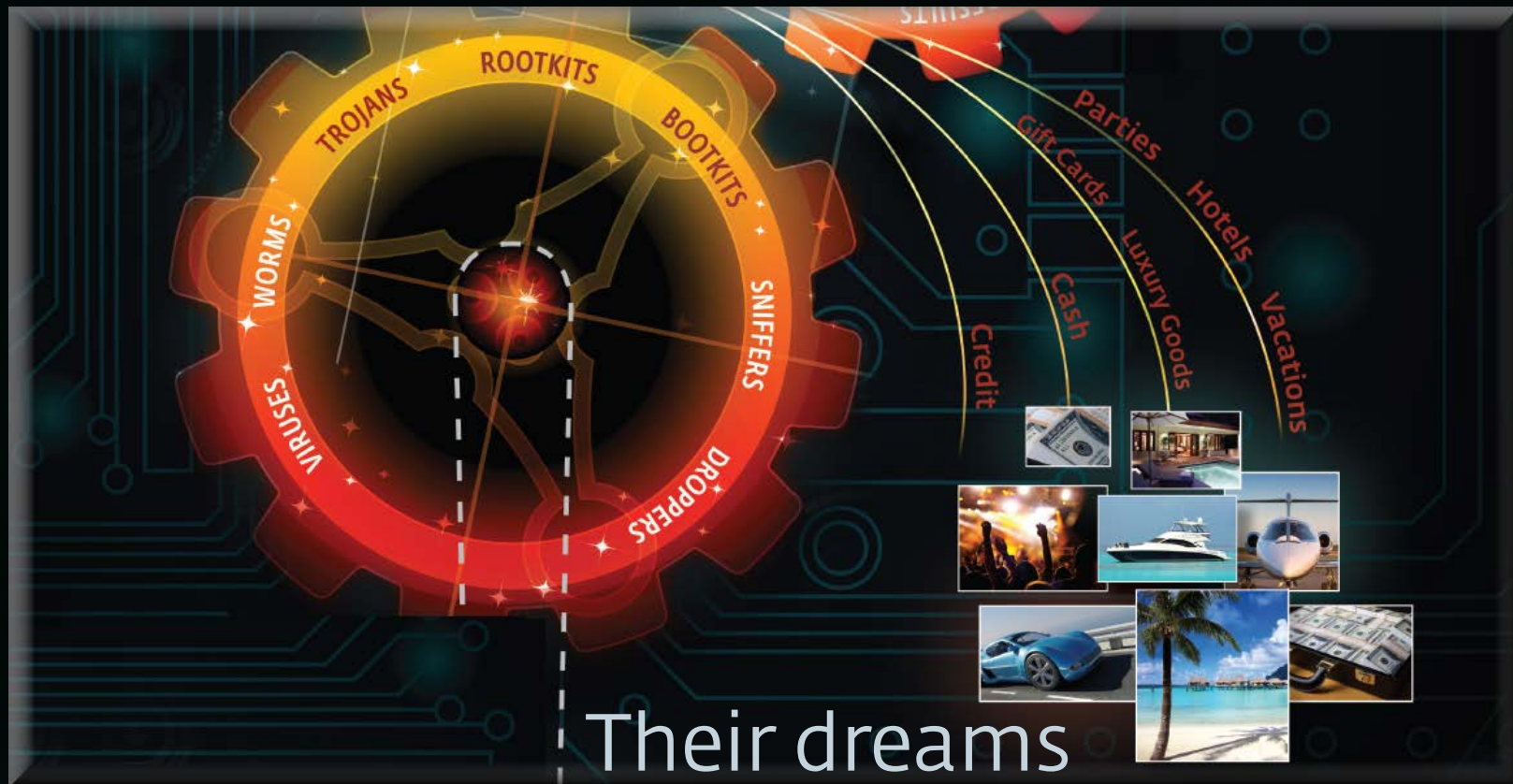
MALWARE, INC.

Turning your **data** into **our** dreams

Your data

Name, Address, Phone Number
Social Security Identifiers
Passwords Credentials
Friends Contacts





Hallmarks of a mature industry

- Division of labor
 - Leveraging specialized skill sets
- Market-based pricing
 - From raw materials to skills
- Productized and packaged
 - Point-and-click GUIs
 - Support services
 - Marketing metrics and A/B testing

NOW HIRING:

- Malware Authors
- Zero Day Vulnerability Researchers
- Social Media Experts
- Botmasters and Botherders
- Exploit Researchers and Packers
- SEO Poisoning Experts
- Mule Recruiters and Drivers
- Carders and Captcha Breakers
- Webmasters (Malicious and Compromised)
- And many more...

Examples



*Thanks to Brian Krebs for sharing screenshots: krebsonsecurity.com
And to Dr. Mark Vriesenga, BAE systems

CRIMEPACK 3.1.3

127.0.0.1/crimepack/control.php

crimepack

MAIN • REFRESH • REFERRERS • COUNTRIES • BLACKLIST CHECK • DOWNLOADER • iFRAME • CLEAR STATS • SETTINGS • LOGOUT

overall stats

unique hits	loads	exploit rate
0	0	0%




exploit stats

iepeers	msiemc	pdf	mdac	hcp	java	webstart	java-getval	activex	other	aggressive
0	0	0	0	0	0	0	0	0	0	0

os stats

os	hits	loads	rate
windows 2k	0	0	0%
windows 2k3	0	0	0%
windows xp	0	0	0%
windows vista	0	0	0%

browser stats

		
0 (0 loads) 0%	0 (0 loads) 0%	0 (0 loads) 0%

Steel SKIN

Info Build Support About

Status: Connected to HPMCE

[Jojo-THINK] Log sent to incognitorat@gmail.com.
[HPMCE] Log sent to incognitorat@gmail.com.

Online: 24

Update Update All
Remove Server Clear Logger

File Manager

Active Window	UpTime	Remote Time	Webcam
Adsense Clicker Fr...	4 minute(s)	12:45 0803	No
Menú Inicio	4 minute(s)	10:45 PM	No
Pemesanan Agoda...	4 minute(s)	10:49 AM	No
??? ???? ????? 201...	4 minute(s)	6:45 0	Yes
	4 minute(s)	9:45 PM	No
Tim Dirks The Gre...	4 minute(s)	7:45 PM	No
Dodge Challenger ...	4 minute(s)	10:45 PM	No
Nothing site now	4 minute(s)	0:45 PM	No

FIND

TeamHAVOC

CRIMEPACK 3.1.3

127.0.0.1/crimepack/control.php

</xssed>

xss attacks information

[Home](#) | [News](#) | [Articles](#) | [Adv.](#) | [Submit](#) | [Alerts](#) | [Links](#) | [XSS info](#) | [About](#) | [Contact](#)

[XSS Archive](#) | [XSS Archive](#) ★ | [TOP Submitters](#) | [TOP Submitters](#) ★ | [TOP Pagerank](#) |

[Free Online Advertising](#) See What \$75 of Google Ads Can Do For Your Business. Try It Now! [www.Google.com/AdWords](#)
[SEO For Small & Local Biz](#) Affordable SEO That Gets Your Site Ranked With Big Boys! Free Analysis [OrangeSoda.com/SEO](#)
[DISA IAVA Compliance](#) IAVA Automated Management Tool DoD Certified GOTS product [www.iavacms.org](#)

AdChoices ▶

Syndicate

R Domains already xss'ed.

S Famous and Government web sites.

F Status: Fixed/Unfixed.

PR Pagerank by [Alexa](#)®.

You can subscribe to our [mailing list](#) to receive alerts by mail.

Date	Author	Domain	R	S	F	PR	Category	Mirror
22/02/12	CyberBellona	ghrc.nsstc.nasa.gov		★	✗	846	XSS	mirror
22/02/12	longrifle0x	catalogue.adidas.com	R	★	✗	4378	XSS	mirror
22/02/12	Anshul katta	www.hcltech.com			✗	35647	XSS	mirror
22/02/12	longrifle0x	www.college.harvard.edu		★	✗	1386	XSS	mirror
22/02/12	NetFuzzer	noticias.uol.com.br		★	✗	7128	XSS	mirror
22/02/12	IrIsT.Ir	www.safedrive.ge			✗	6809324	XSS	mirror
21/02/12	BoxHead	unlock.tacobell.com		★	✗	20763	XSS	mirror
19/02/12	NetFuzzer	www.windows7download.com			✗	10707	XSS	mirror

Steel SKIN

Info Build Support About

Status: Connected to HPMCE

[jojo-THINK] Log sent to incognitorat@gmail.com.

[HPMCE] Log sent to incognitorat@gmail.com.

Online: 24

Update Update All

Remove Server Clear Logger

File Manager

Active Window	UpTime	Remote Time	Webcam
Adsense Clicker Fr...	4 minute(s)	12:45 0803	No
Menú Inicio	4 minute(s)	10:45 PM	No
Pemesanan Agoda...	4 minute(s)	10:49 AM	No
??? ??? 201...	4 minute(s)	6:45 0	Yes
	4 minute(s)	9:45 PM	No
Tim Dirks The Gre...	4 minute(s)	7:45 PM	No
Dodge Challenger ...	4 minute(s)	10:45 PM	No
Nothing site you	4 minute(s)	0:45 PM	No

FIND

TeamHAVOC

SPAMdot.biz.com.net.info.org
Spam community and vendors services

Spam it .com

Продажа Поиск Личные сообщения Репутация: 4 [-2/+6]

Место свободное Место свободное Место свободное Место свободное

Продам спам-базу или целиком рут сервера + админка

Selling spam-base or the entire server + Root admin

Список форумов SpamDot -> Базы e-mail

Предыдущая тема :: Следующая тема

Автор	Сообщение
Umbro Member Зарегистрирован: 29.12.2007 Сообщения: 215	<p>↑ добавлено: Ср Янв 09, 2008 2:40 pm Заголовок сообщения: Продам спам-базу или целиком рут сервера + админка</p> <p>Оценки: 0 [+ -]</p> <p>ресурс "</p> <p>Resource: 20,049 clients, about 11,500 emails, full info for each address, name, position....a lot of presidents, COO, CIO, etc. Guaranteed working, no problem. Discuss prices, exchange of data in ICQ or private message</p> <p>P.S....sample database entry:...</p> <p>Гаранти/проверки - без проблем.</p> <p>8 одни руки.</p> <p>Вашу асо в пн, для обсуждения цены и варианта прохождения сделки.</p> <p>PS принер базы: uid prefix first_name last_name title company phone fax email url street street2 city state 8416 NULL Xavier Bernat Credit Invest (376) 88 88 25 (376) 88 88 41 xbernat@credinves</p> <p>Последний раз редактировалось: Umbro (Чт Янв 10, 2008 9:03 pm); всего редактировалось 1 раз</p>

Вернуться к началу

22/02/12	IR151.IR	www.saredrive.ge	
21/02/12	BoxHead	unlock.tacobell.com	★
19/02/12	NetFuzzer	www.windows7download.com	

Сообщение

Заголовок сообщения: Продам спам-базу или целиком рут сервера + админка

Resource: 20,049 clients, about 11,500 emails, full info for each address, name, position....a lot of presidents, COO, CIO, etc. Guaranteed working, no problem. Discuss prices, exchange of data in ICQ or private message

P.S....sample database entry:...

Steel SKIN

Info Build Support About

Status: Connected to HPMCE

[jojo-THINK] Log sent to incognitorat@gmail.com.
[HPMCE] Log sent to incognitorat@gmail.com.

Online: 24

Update Update All Clear Logger

anager

Remote Time	Webcam
\$ 0803	No
\$ PM	No
\$ AM	No
\$	Yes
PM	No
PM	No
\$ PM	No
\$	No

FIND

TeamHAVOC

127.0.0.1/crimepack/control.php



USERNAME

admin

PASSWORD

</xssed>
xss attacks information

XSS Archive | XSS Archiv

Free Online Adver
SEO For Small & I
DISA IAVA Compl

Syndicate

R Domains already xss'er
S Famous and Governme
F Status: Fixed/Unfixed.
PR Pagerank by Alexa@.

You can subscribe to our me

Date	Auth
22/02/12	CyberBe
22/02/12	longrif
22/02/12	Anshul
22/02/12	longrif
22/02/12	NetFu:
22/02/12	IrIsT
21/02/12	BoxHi
19/02/12	NetFuzzer

Steel SKIN

About

MCE

incognitorat@gmail.com.
ognitorat@gmail.com.

taylor swift

taylor swift-3542.jpg

e-extras.com

3 x 779 - taylor swift Pictures,
otos & Images
milar - More sizes

FIND

TeamHAVOC

</XSS
xss attacks

XSS Archive | XSS

Free Online

SEO For S

DISA IAV



Syndicate

R Domains already

S Famous and C

F Status: Fixed,

PR Pagerank by

You can subscribe

Date

22/02/12

22/02/12

22/02/12

22/02/12

22/02/12

22/02/12

21/02/12

19/02/12



Spy Eye v1.3



2011
06/06
15:14:57



Find INFO



Statistic



FTP accounts



Settings



Screen shots



BOA Grabber



CC Grabber



Certificate Grabber



13 k
+13700



2011
06/06
15:18:27



Bots Monitoring



Full Statistic



Create Task



Tasks Statistic



VIRTEST



Plugins



FTP backconnect



SOCKS 5



RDP



25
504



Logs



Files



Settings

Hack the Planet!



Take your money!



FIND

TeamHAVOC

Low risk, high reward

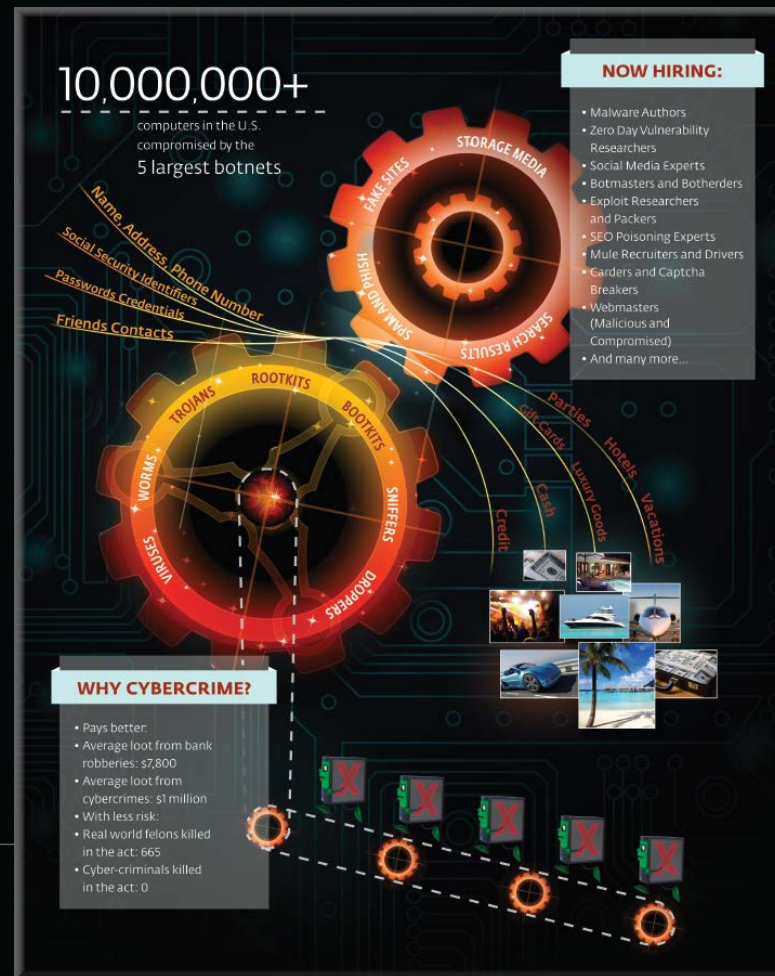
- Bigger payoff with less chance of getting shot
- Traditional crime is dropping
- Cybercrime is rising

WHY CYBERCRIME?

- Pays better:
- Average loot from bank robberies: \$7,800
- Average loot from cybercrimes: \$1 million
- With less risk:
- Real world felons killed in the act: 665
- Cyber-criminals killed in the act: 0

Adds up to?

- Serious threat
- Still gearing up
- Requires serious response
 - From law enforcement
 - To company networks
 - And end users (all of us)





Internet Security

