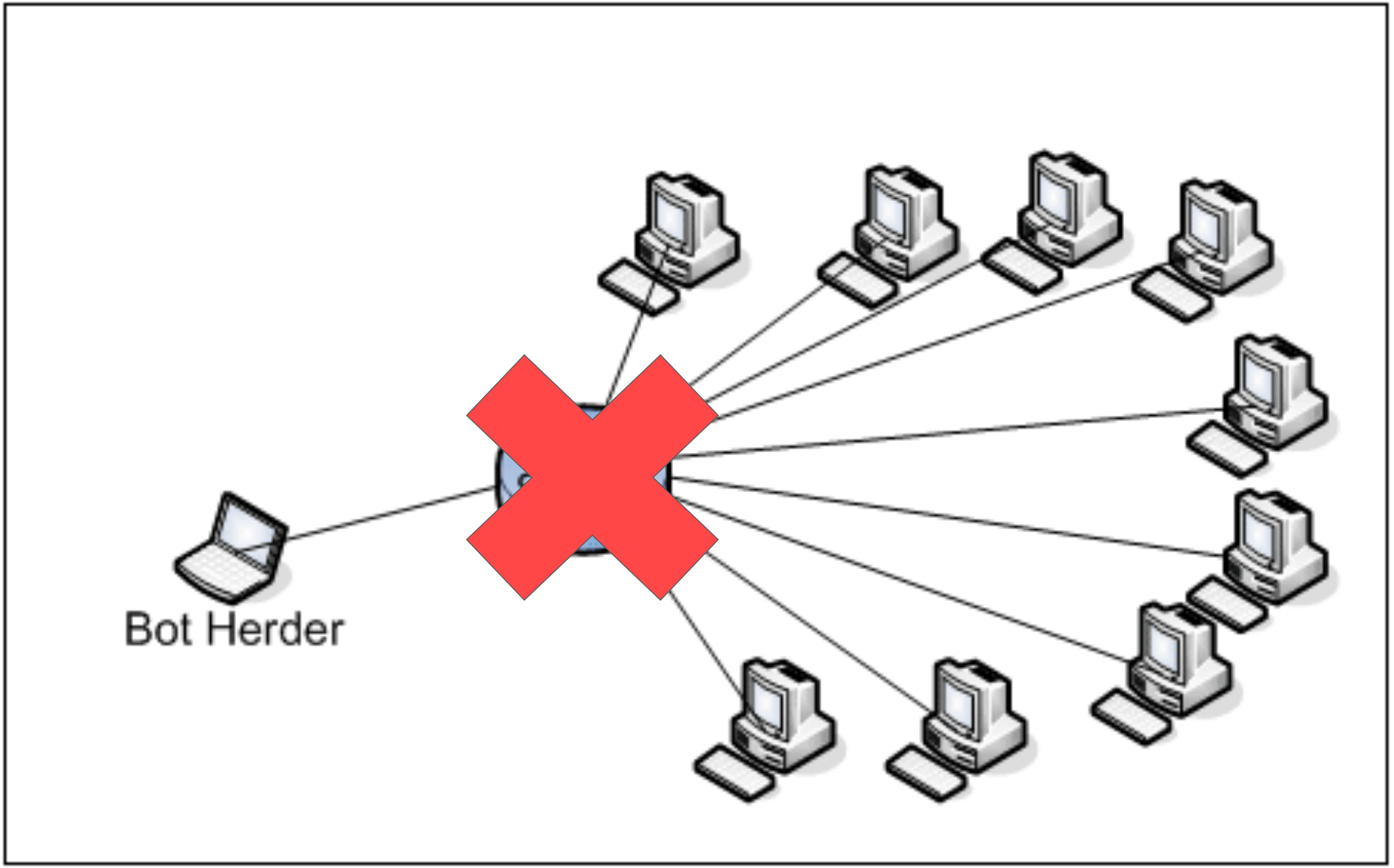
TREND MICRO™ Securing Your Web World

Taking Down a Botnet:
The Story Behind Rove Digital's Takedown

Ryan Flores – Forward Looking Threat Research

Confidential


What is a takedown?


Bot Herder

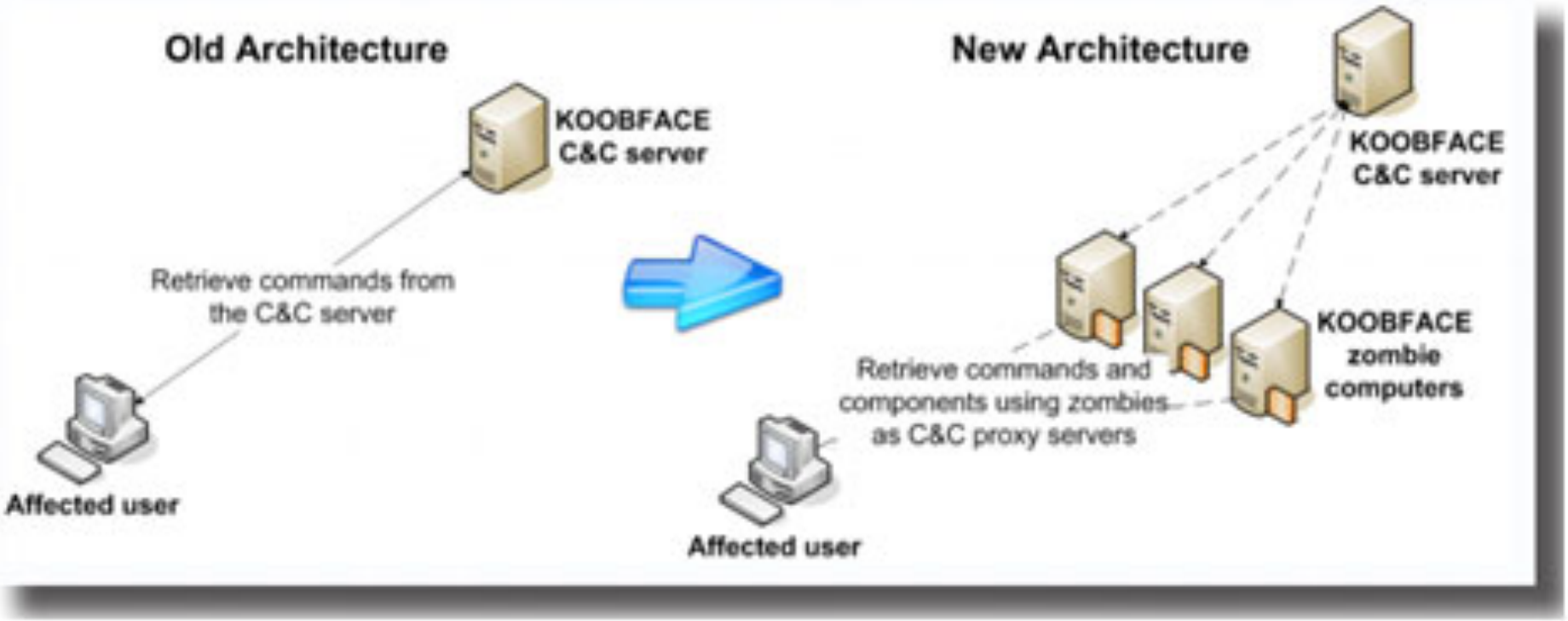
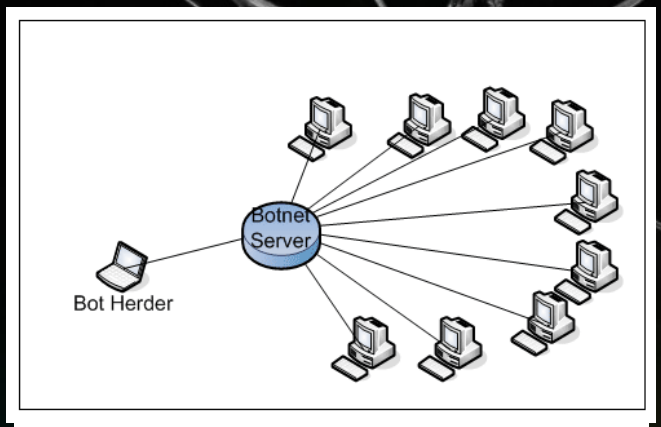
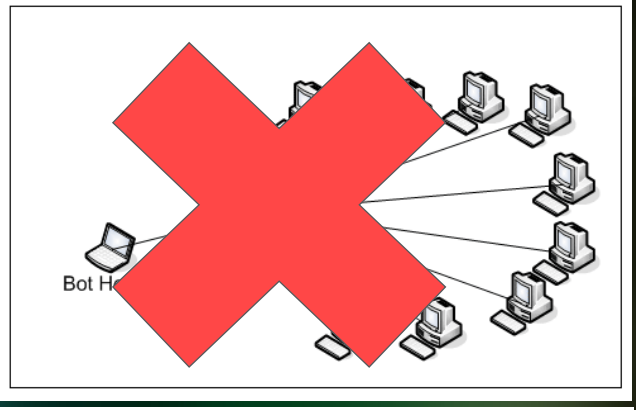


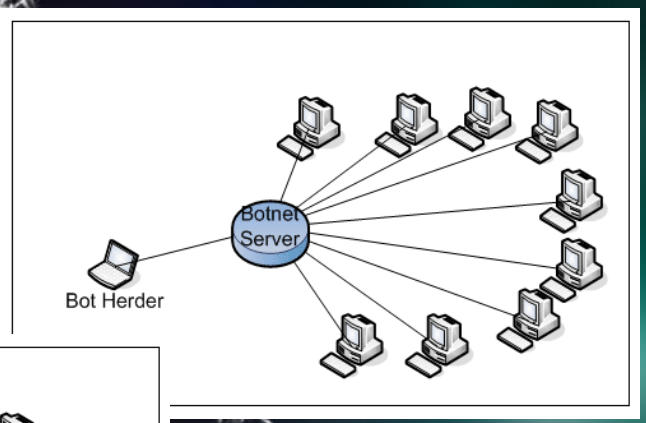
Figure 4. Evolution of KOOBFACE architecture as seen in our fourth paper

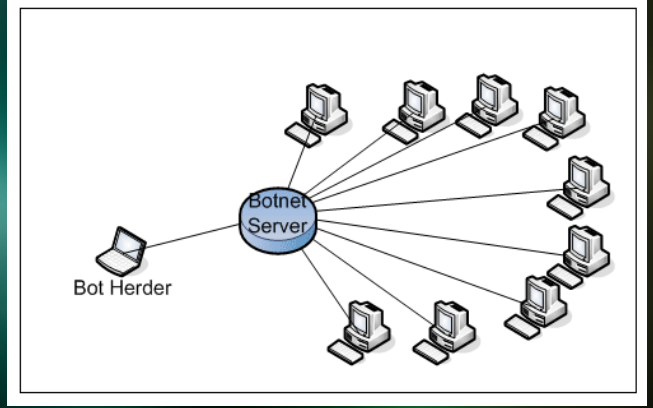
MICROSOFT
DIGITAL
CRIMES
UNIT

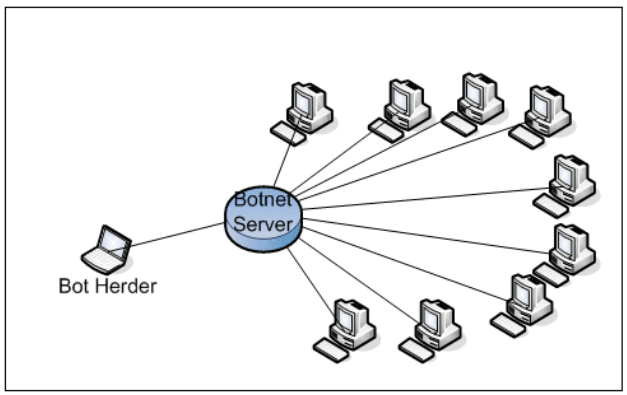
ZEUS





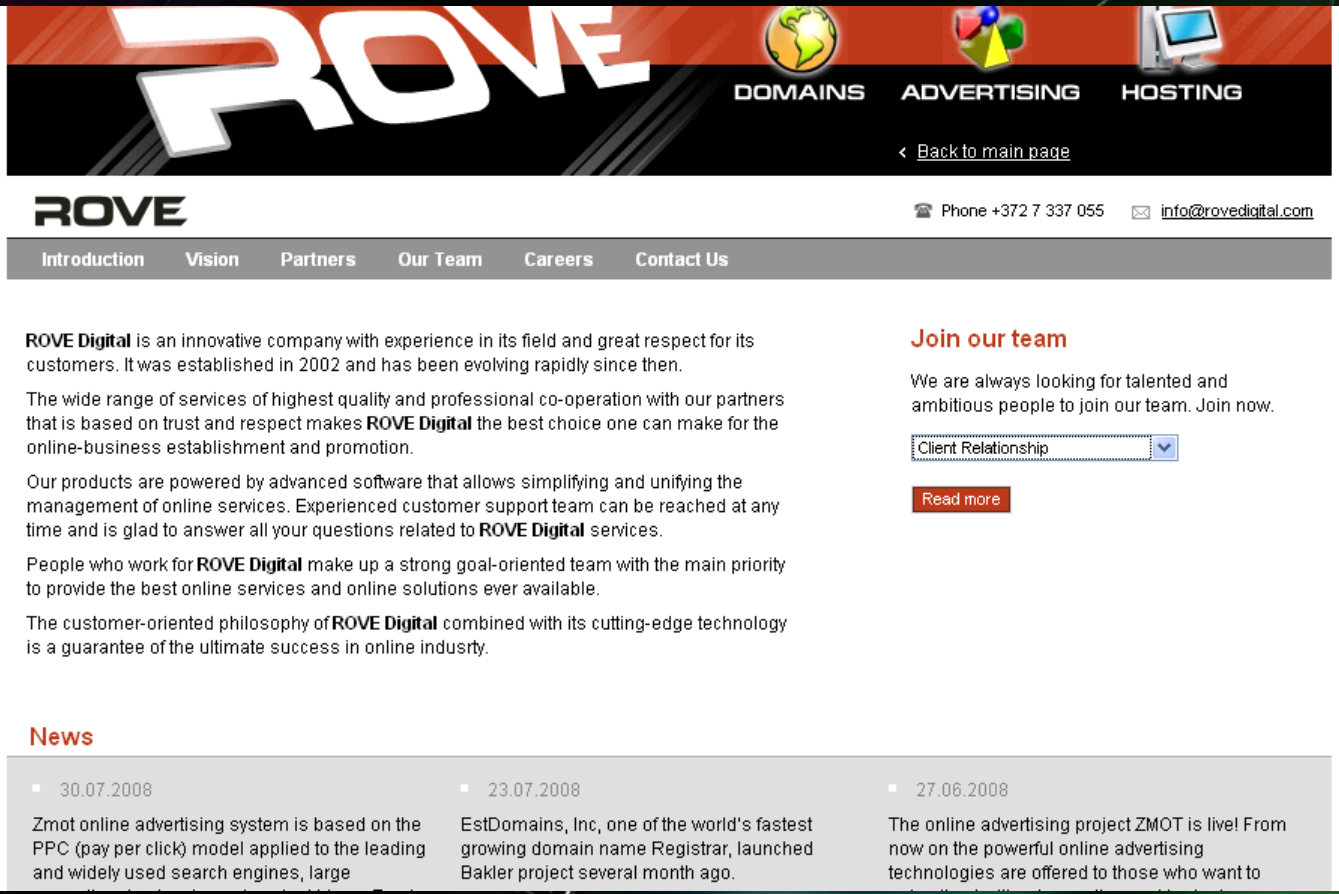






Takedowns aren’t easy

Rove's website

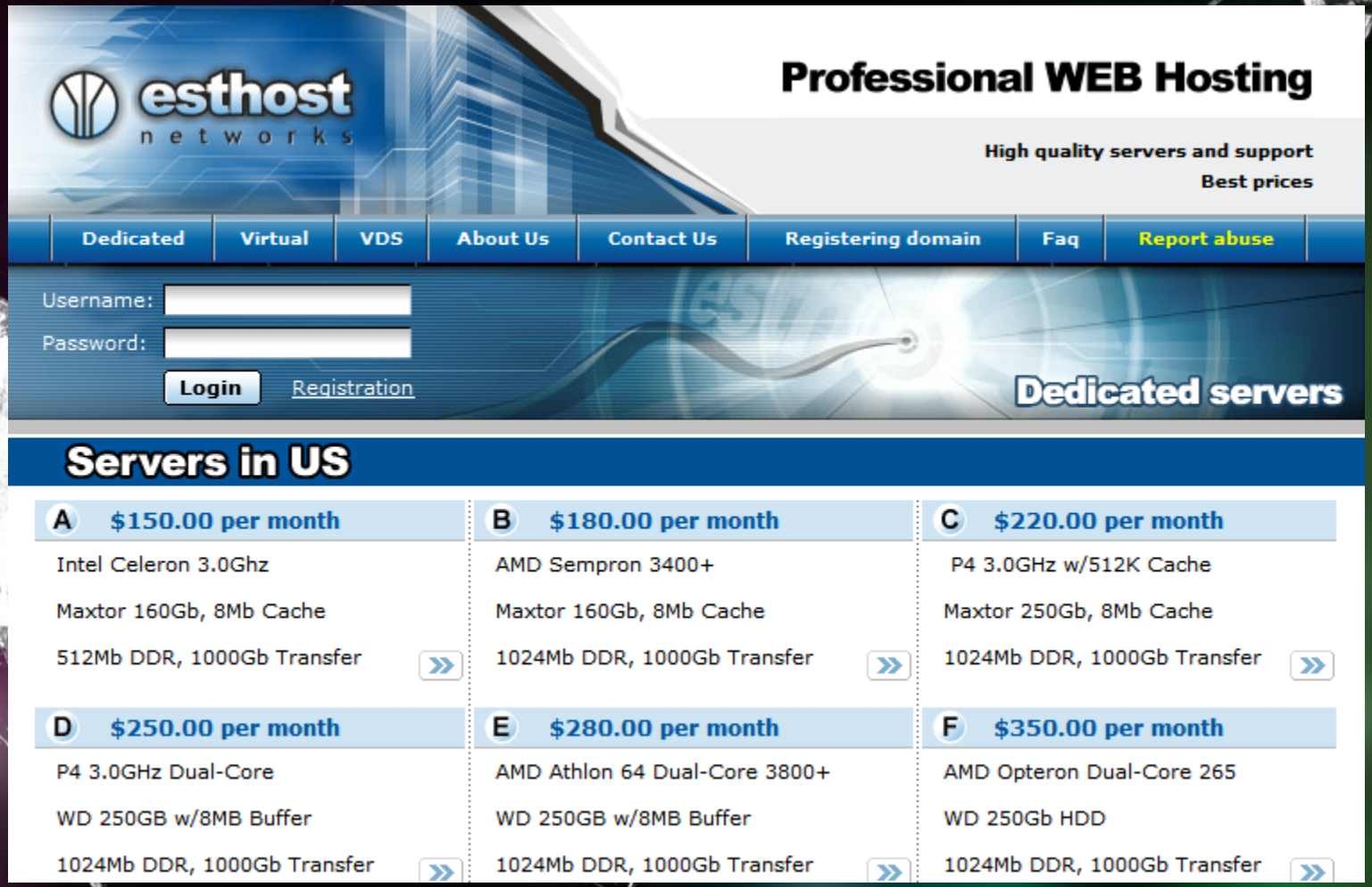


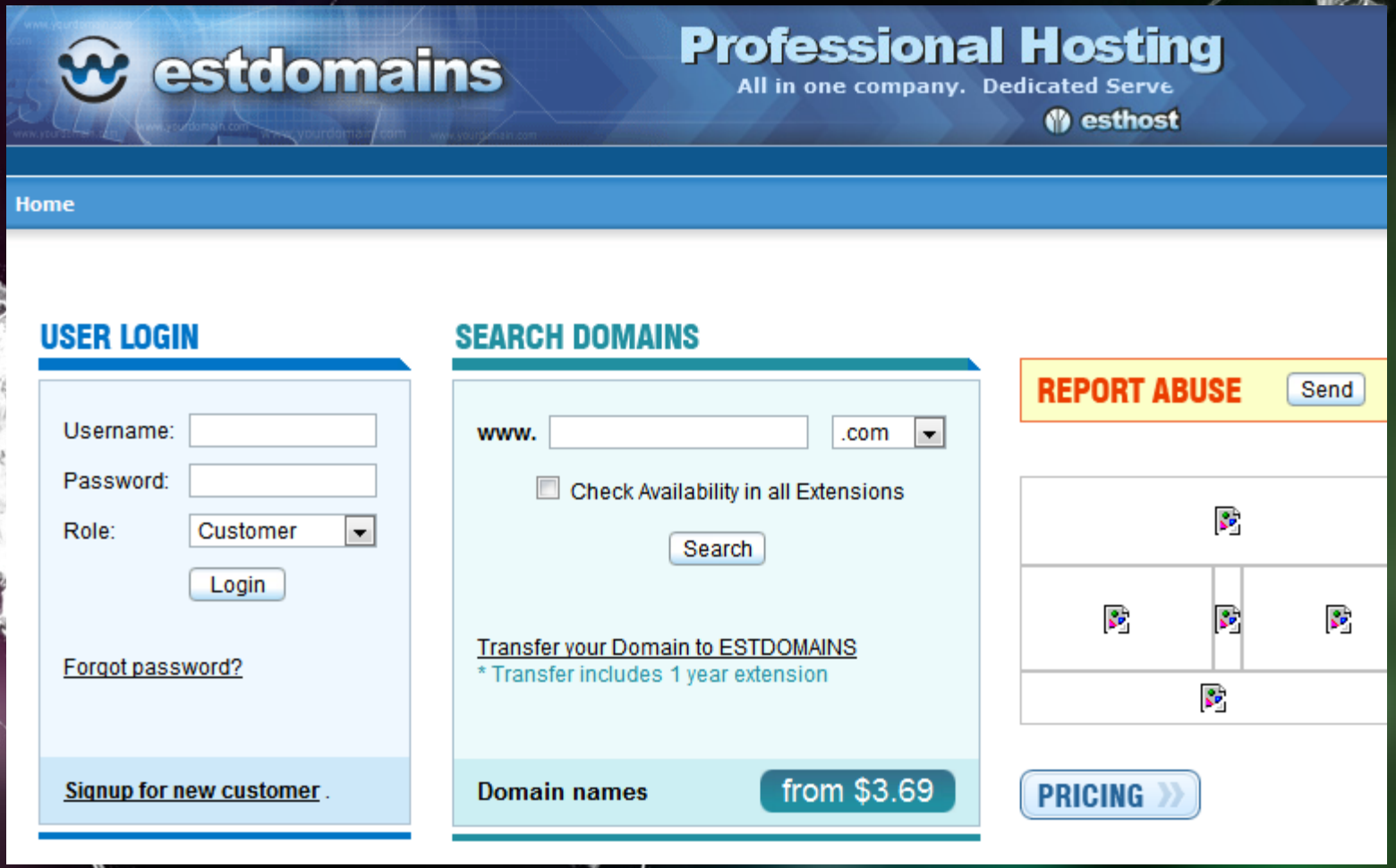
An IT company in Estonia

- "The most innovative IT company" in Estonia (2007)
- Among top 3 IT companies in Estonia (revenue)
- 2008: revenue > 9,000,000 USD.
- 2007: > 50 employees

ROVE DIGITAL

(Tamme Arendus)


esthost networks
Professional WEB Hosting
High quality servers and support
Best prices
Dedicated
Virtual
VDS
About Us
Contact Us
Registering domain
Faq
Report abuse
Username:
Password:
Login
Registration
Dedicated servers
Servers in US
A $150.00 per month
Intel Celeron 3.0Ghz
Maxtor 160Gb, 8Mb Cache
512Mb DDR, 1000Gb Transfer
B $180.00 per month
AMD Sempron 3400+
Maxtor 160Gb, 8Mb Cache
1024Mb DDR, 1000Gb Transfer
C $220.00 per month
P4 3.0GHz w/512K Cache
Maxtor 250Gb, 8Mb Cache
1024Mb DDR, 1000Gb Transfer
D $250.00 per month
P4 3.0GHz Dual-Core
WD 250GB w/8MB Buffer
1024Mb DDR, 1000Gb Transfer
E $280.00 per month
AMD Athlon 64 Dual-Core 3800+
WD 250GB w/8MB Buffer
1024Mb DDR, 1000Gb Transfer
F $350.00 per month
AMD Opteron Dual-Core 265
WD 250Gb HDD
1024Mb DDR, 1000Gb Transfer


estdomains
Professional Hosting
All in one company. Dedicated Serve
esthost
Home
USER LOGIN
Username:
Password:
Role:
Customer
Login
Forgot password?
Signup for new customer .
SEARCH DOMAINS
www.
.com
Check Availability in all Extensions
Search
Transfer your Domain to ESTDOMAINS
* Transfer includes 1 year extension
Domain names
from $3.69
REPORT ABUSE
Send
PRICING

Rove's "advertising" services

NULLOR.COM

HOME | NEWS | ADVERTISERS | PUBLISHERS | CONTACT US

Nullor.com launched in 2002 has become one of the leading companies in the online advertising industry. We connect thousands of advertisers with millions of consumers. Our ultimate goal is to provide our customers with contemporary e-business and website technologies. We continue to balance the supply and demand from both of our advertisers and publishers by providing them with high-quality services and applying the latest technologies in order to increase their advertising value.

With years of professional knowledge and experience in the Internet advertising industry, **Nullor.com** employs the advanced and innovative technology to meet the needs of valuable advertisers and quality publishers.

Nullor.com aims to increase the benefits and revenue for our clients and members by bringing Internet advertising to a new higher level. We unite all advertising networks into one.

Login:

User:

Pass:

Login

Create New Account for:

» Advertiser

» Publisher

Are You A Brand Advertiser?

Extend your reach with diverse advertising and targeting options by applying performance-based advertising solutions. Sign up today and get advanced solutions to fit your advertising campaign.

Are You A Web Publisher?

Diversify and control you business by choosing Nullor.com. We expand advertising options and let your network revenues grow. Nullor.com will partner with you to meet your goals.

NEWS

23.09.2008

Nullor.com, rapidly growing Ad Network, announces that it has more than 10 million searches per month throughout its entire advertising network of targeted search. This rise in volume is due in part to the company's broad advertiser base as well as having secure and reliable partners. Read more...

28.11.2007

Nullor.com, the developing advertising network, announces today a significant traffic increase for 2007 compared with 2006. Nullor.com site had nearly 20% overall traffic increase since last year.

Read more...

Privacy policy · Terms of Use


2002–2004
The Early Years
Malicious Activity
Rented out servers to mainly cybercriminal customers for use as spambot command-and-control (C&C), data-stealing Trojan, phishing site, and Domain Name System (DNS) changer hosts
Infrastructure
Rented servers in 3 data centers in New York (Pilosoft), San Francisco (Atrivo), and Estonia (Elion)

On the Radar

2007

Malicious Activity

- Used a spoofed *Google Ads* site that replaced the Google ads that DNS changer victims saw on legitimate sites

Infrastructure

- Rogue DNS servers hosted at Pilosoft seemingly disappeared in fall 2007 though these remained part of Rove Digital's infrastructure as back-end servers that did recursive DNS lookups

- A nonprofit organization blacklisted the IP addresses of Rove Digital's spoofed *Google Ads* site

- Deliberately waited months before spoofing the *Google Ads* site elsewhere in order to avoid suspicion and protect its operation

2009 A New Venture

Malicious Activity

- Directly entered the FAKEAV business

Geography: United States

Business Model: Decided to form its own FAKEAV affiliate program, NeliCash/NewlineCash

- Contractors from Eastern European countries fulfilled most of its advanced coding and Trojan creation requirements
- Pirated movies
- Created and spread adware
- Started working with *Clicksor* for ad replacement

2010–2011 The Takedown

Malicious Activity

- Tried to enter the market for pirated movies
- Malicious operation was shut down
- Rove Digital employees were arrested
- Réseaux IP Européens (RIPE) froze Rove Digital's IP domain ranges

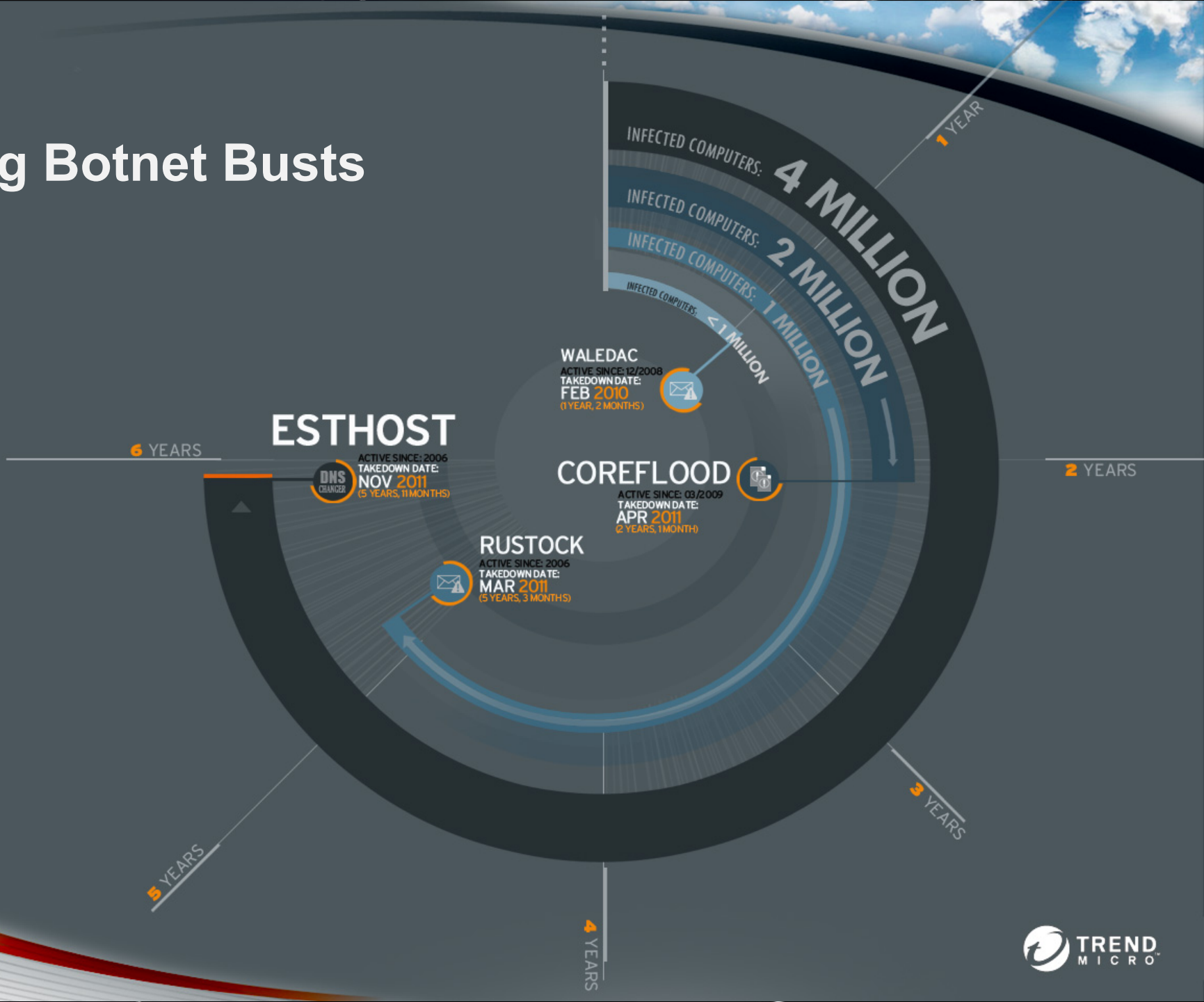
Infrastructure

- Had a DNS botnet with more than 4M bots
- Had more than 100 servers in its infrastructure

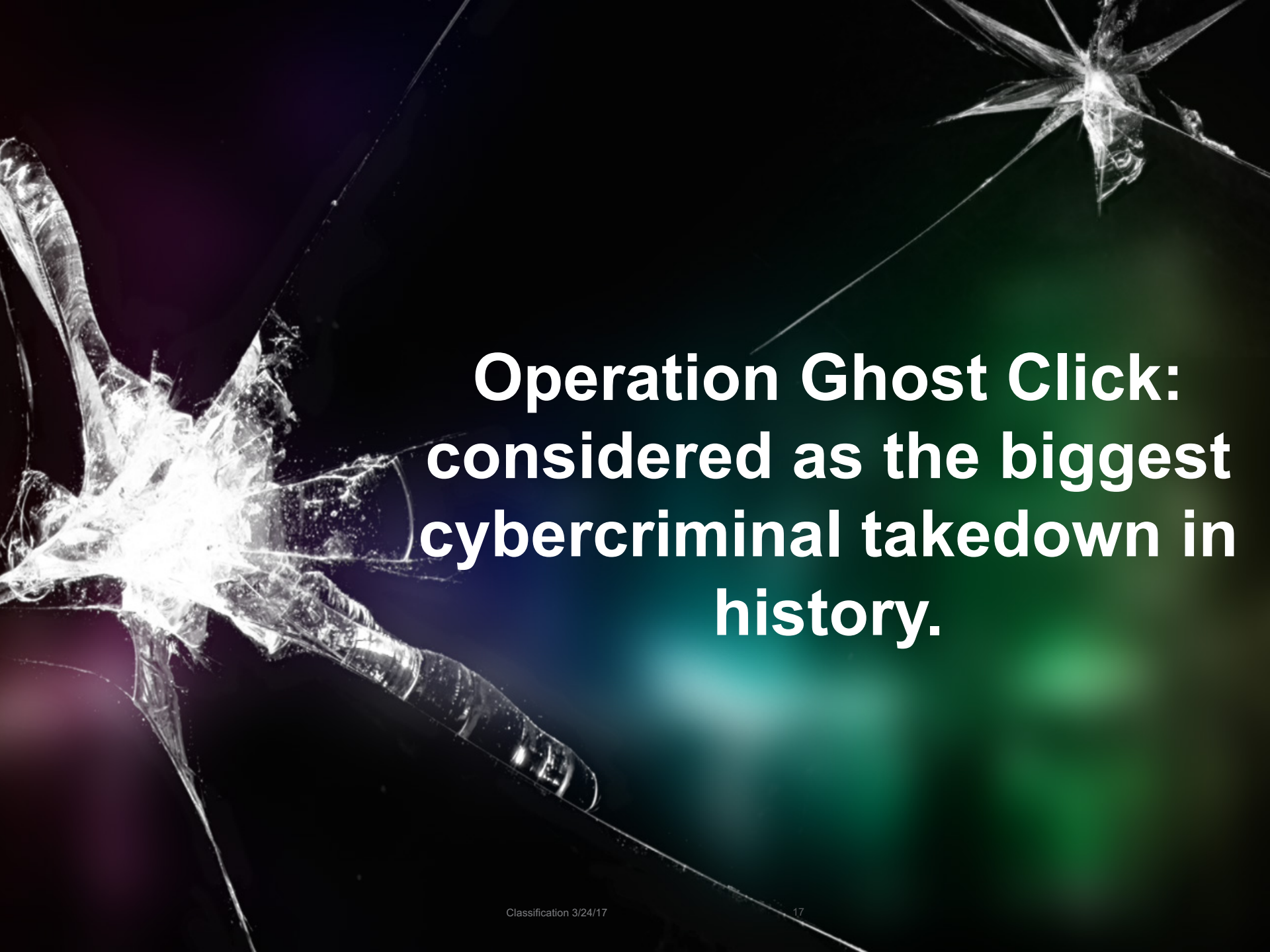
Other Events

- Collaborative investigation among the Federal Bureau of Investigation (FBI), the Office of Inspector General (OIG), as well as Trend Micro and its industry partners ensued

Big Botnet Busts

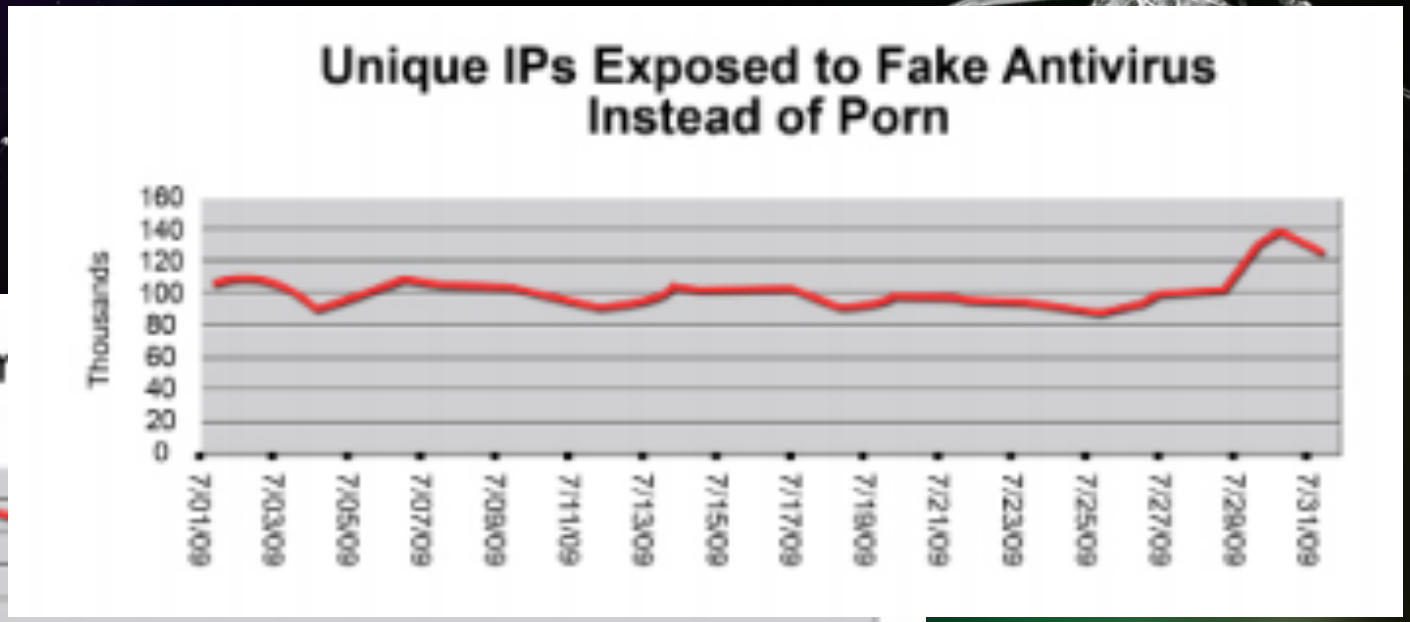


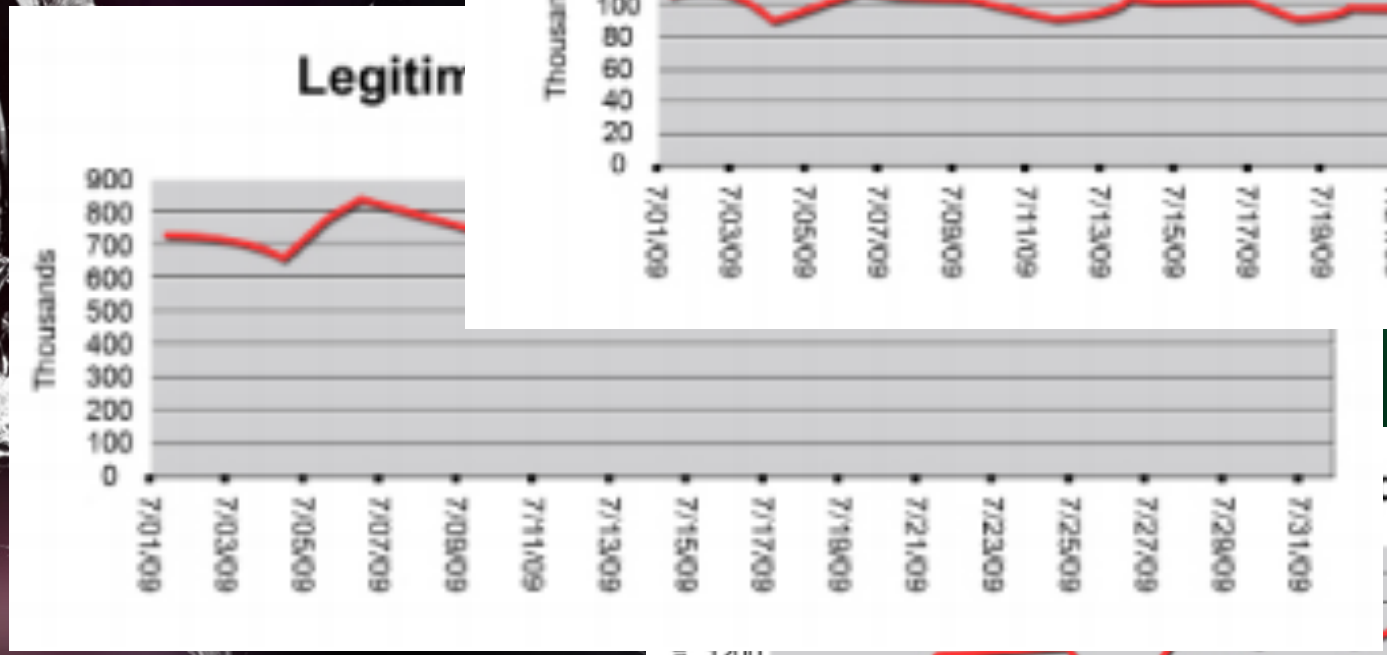
TREND MICRO

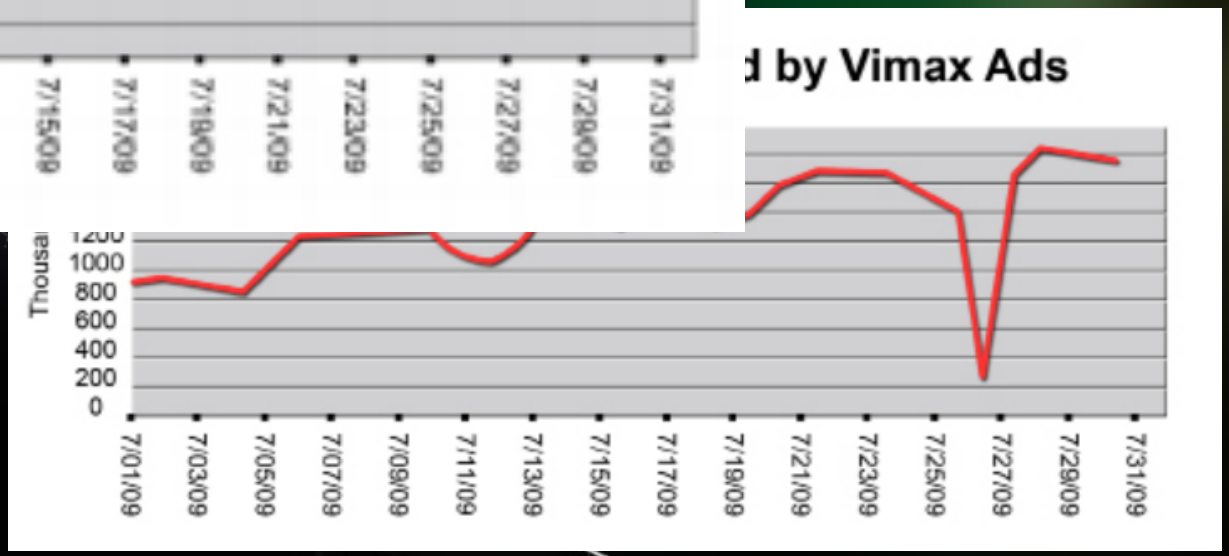

Operation Ghost Click: considered as the biggest cybercriminal takedown in history.

Rove Digital/Esthosts … ISP? Cybercrime hub?

An entrepreneurial professional CEO


Unique IPs Exposed to Fake Antivirus Instead of Porn
Thousands
160
140
120
100
80
60
40
20
0
7/01/09
7/03/09
7/05/09
7/07/09
7/09/09
7/11/09
7/13/09
7/15/09
7/17/09
7/19/09
7/21/09
7/23/09
7/25/09
7/27/09
7/29/09
7/31/09


Legitim
Thousands
900
800
700
600
500
400
300
200
100
0
7/01/09
7/03/09
7/05/09
7/07/09
7/09/09
7/11/09
7/13/09
7/15/09
7/17/09
7/19/09
7/21/09
7/23/09
7/25/09
7/27/09
7/29/09
7/31/09


d by Vimax Ads
1000
800
600
400
200
0
7/01/09
7/03/09
7/05/09
7/07/09
7/09/09
7/11/09
7/13/09
7/15/09
7/17/09
7/19/09
7/21/09
7/23/09
7/25/09
7/27/09
7/29/09
7/31/09

So what's it worth?

150,000 machines = 1,000,000 clicks per day

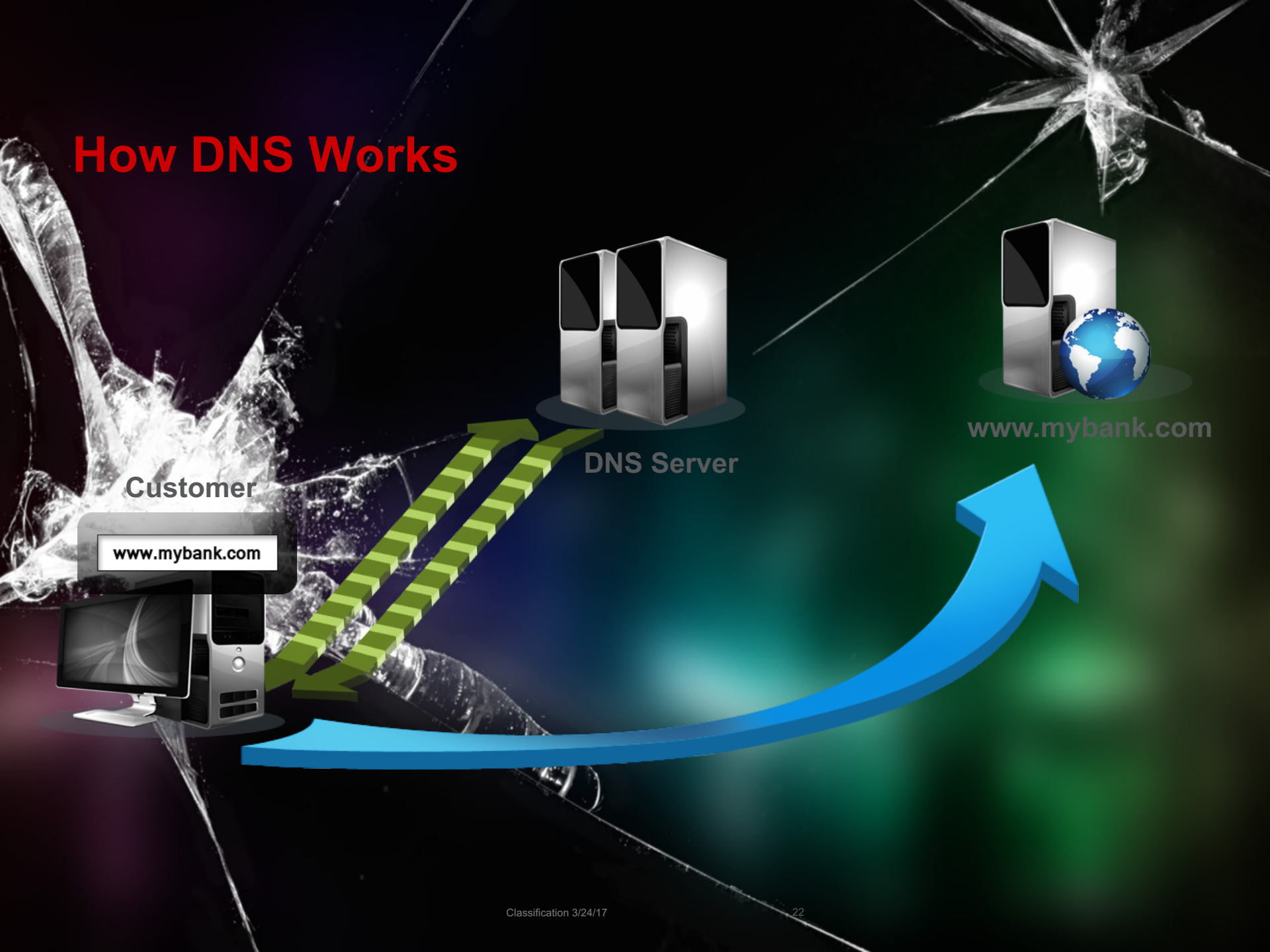
earnings (USD)	keyword	clicks	CPC
35.48	facebook	4917	0.0072
33.64	dating	1244	0.027
16.43	free credit report	275	0.0598
15.7	ebay	911	0.0172
15.25	credit card processing	136	0.1122
15.24	direct tv	232	0.0657
14.09	malwarebytes	313	0.045
14.06	accept credit cards	105	0.1339
13.89	car insurance	63	0.2205
13.76	mcafee	87	0.1581
...			
Total: 12933		**1070253**	

Table 1. One-day earnings of a browser hijack botnet

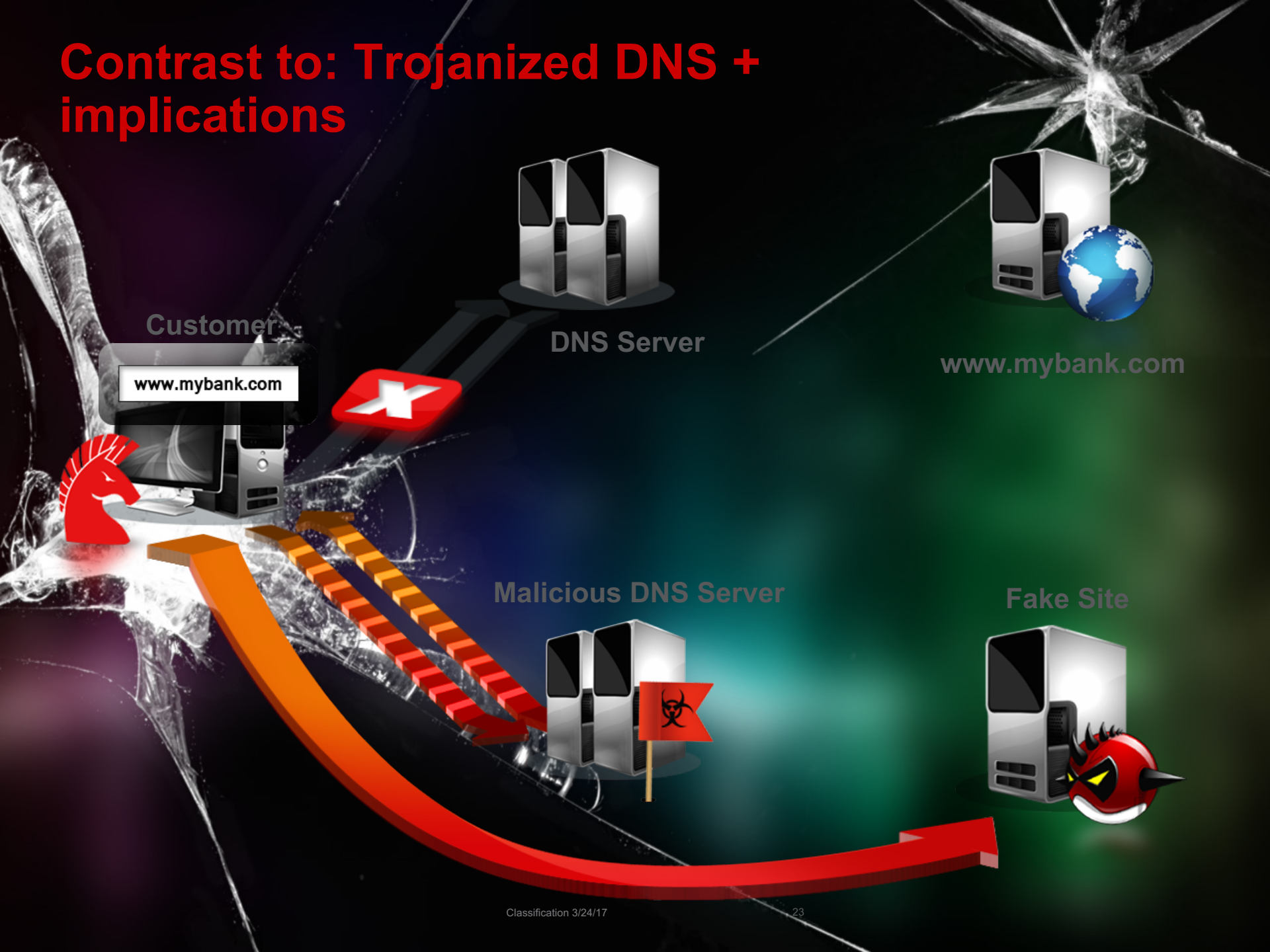
4,000,000 machines = ?

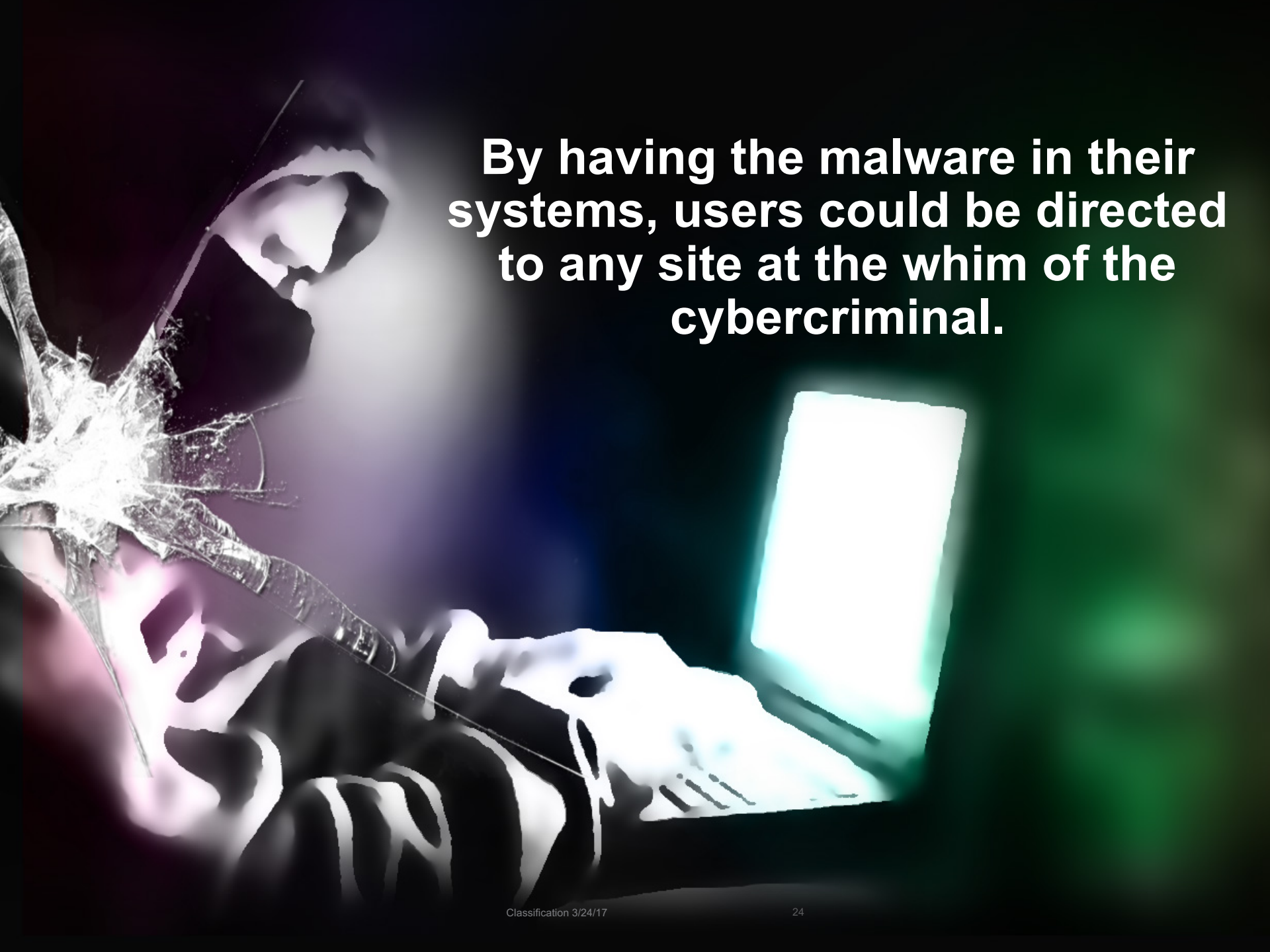
THE PROBLEM

How DNS Works



Contrast to: Trojanized DNS + implications





By having the malware in their systems, users could be directed to any site at the whim of the cybercriminal.

CNN website (original)

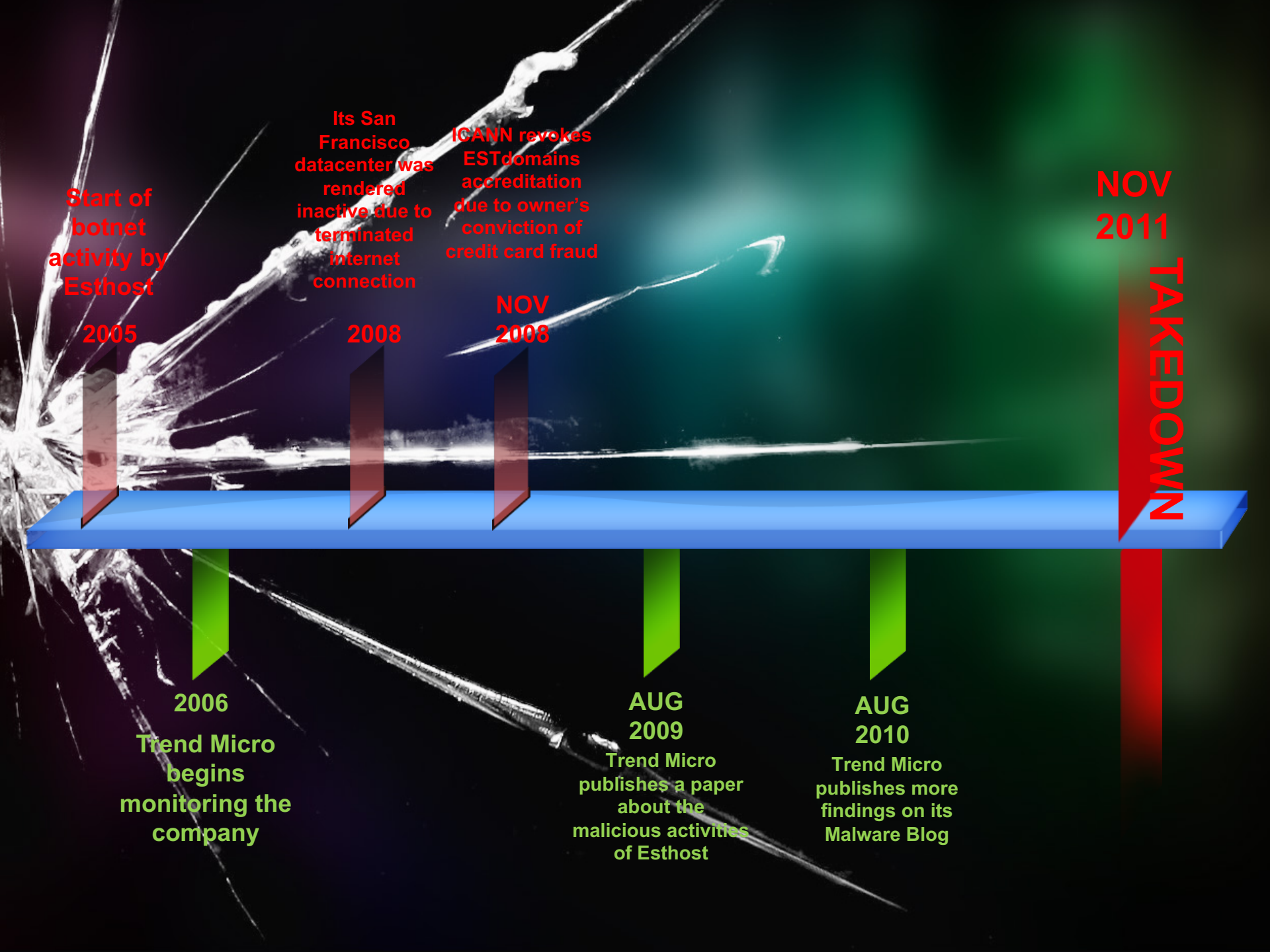
CNN website (infected)

Porn ?

Fake AV - Big Business

THE INVESTIGATION


Trend Micro has been monitoring these cybercriminal activities since 2006


Start of botnet activity by Esthost
2005
Its San Francisco datacenter was rendered inactive due to terminated internet connection
2008
ICANN revokes ESTdomains accreditation due to owner's conviction of credit card fraud
NOV 2008
NOV 2011
TAKEDOWN
2006
Trend Micro begins monitoring the company
AUG 2009
Trend Micro publishes a paper about the malicious activities of Esthost
AUG 2010
Trend Micro publishes more findings on its Malware Blog

We had a lot of flies on the walls of Rove.

Laughable security of Rove's servers.**

100+ servers given .intra domains

looked at SMTP banners & DNS servers (often open resolvers)

DNS zone files transfers for domains of Rove.

All .intra domains, IPs and additions

Identify and follow the new domain names that got resolution from rogue dns

we got two hard drive of C&C servers.

**no password protection or encryption broken

.intra
Convenient
Consistent
Codeless

portal2.intra	86400	IN	A	93.190.x.x
codecsoft3.intra	86400	IN	A	213.163.x.x
metaparser.intra	86400	IN	A	67.210.x.x
adsclick.intra	86400	IN	A	174.142.x.x
pharma1.intra	86400	IN	A	87.118.x.x
tds.intra	86400	IN	A	64.86.x.x

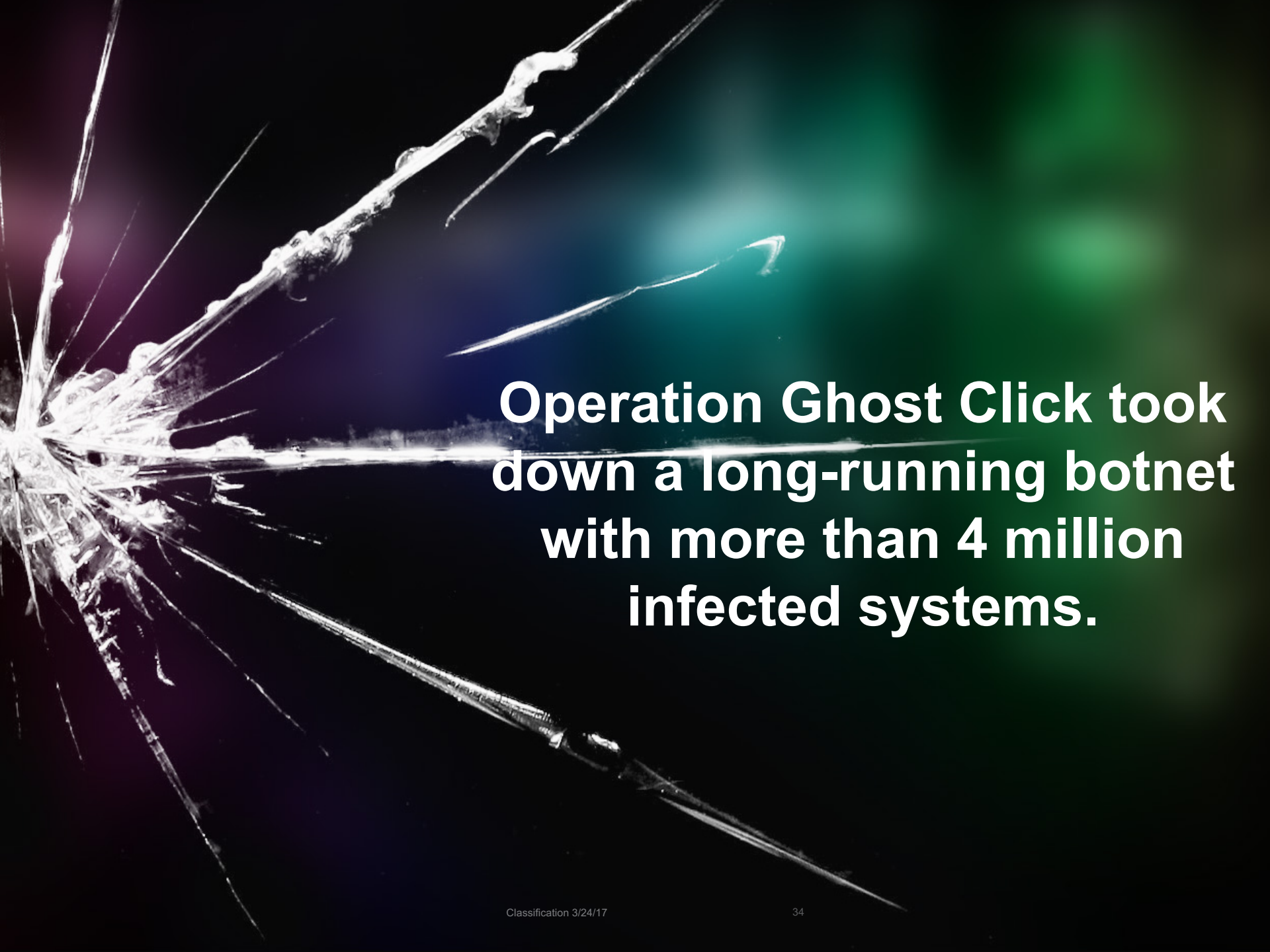
Google Proxies

gcache1.intra	86400	IN	A	69.31.x.x
gcache2.intra	86400	IN	A	67.210.x.x

Fake AV sites

billing.intra	86400	IN	A	64.28.x.x
billingproxy1.intra	86400	IN	A	78.159.x.x
billingproxy2.intra	86400	IN	A	88.198.x.x

TAKEDOWN


Operation Ghost Click took down a long-running botnet with more than 4 million infected systems.


-datacenters got raided
- 200+ servers got seized
- rogue DNS servers got replaced with ISC DNS
-Rove Digital's office got raided
-luxury cars, millions of USD, houses confiscated
-6 arrests in Estonia
-RIPE blocked IP ranges

Vladimir Tsastsin

Tsastsin is the leader of the Rove Digital cybercrime ring. He was Esthost, EstDomains, and Rove Digital's CEO. When he could no longer use his own name to register affiliate companies, he sought his family members' help to sign formal letters in Estonia. Known as *"scr"* in the cybercrime underground, he was convicted of credit card fraud in Estonia in 2008.

Dmitri Jegorov

According to the online newspaper, *Ekspress.ee*, Jegorov had a criminal record as well. As a teenager, he allegedly tried to extort money from a local supermarket and even made a fake bomb but was easily arrested. Part of his role included recruiting new employees and registering several of Rove Digital's shell companies in the United States. He can be considered a Rove Digital program manager. Known for using the alias "Dmitri Dimuskin," he is also known as a pornography webmaster.

Timur Gerassimenko

Gerassimenko had his own company, Infradata, which provided services to Rove Digital. Also known as *"hyper,"* he dabbled in running pornography and malware-hosting sites (photo courtesy of *Ekspress.ee*).

Konstantin Poltev

Poltev was the spokesman for Esthost, EstDomains, and Rove Digital. He also headed Esthost and Cernel's Abuse Department. In 2008, he publicly claimed on NANOG's public mailing list that Esthost was a legitimate company. Also known as *"kokach,"* he was proclaimed EstDomains's new CEO when the ICANN decided to revoke the company's accreditation in 2008 due to "former CEO" Tsastsin's conviction for credit card fraud in Estonia (photo courtesy of *Ekspress.ee*).

Valeri Aleksejev

Aleksejev calls himself a web developer on *LinkedIn* but avoids mentioning what company he works for. He allegedly wrote the code for a Rove Digital monitoring system for its rogue DNS infrastructure. He also appears to be one of the recipients of email alerts whenever the company encountered problems.


Not covered by the
current complaints:
- FakeAv Business
- Affiliate Program
- Payment Service

Trend Micro provided the majority of the threat research in the takedown

Cybercrimes do not occur in isolation. Their reach and effects are far-extending.

Collaboration between

FBI, Estonian Police, Dutch Police,

Trend Micro,

RIPE, ISC, Qwest, Comcast, Bell Canada, AT&T, Neustar,

Spamhaus, Google, others

Challenges

Subject Area	Challenges
Crime	• DNS knowledge, • knowledge how Websites work • knowledge how advertising work
Investigation	• Forensic skill (hard disks), • DNS skill , • Pentesting skill set, • Internet forensics • Sandboxing and reverse engineering
Take down	• Transnational nature of the crime (different police, different laws), • Number of players high (many DC owner, many ISP‘s) • confidentiality


Did you lose your Internet last July 9?

Cyberpolice ? – Which Cyberpolice

- Each country has own laws
- Each country has own law enforcement
- Cyberspace is global (even universal)
- Even within one state ist not clear if Cyber is internal affair or military
- Competition to use cyber defense for own advantage

Result: 1000 initiatives, tons of paper, but no progress

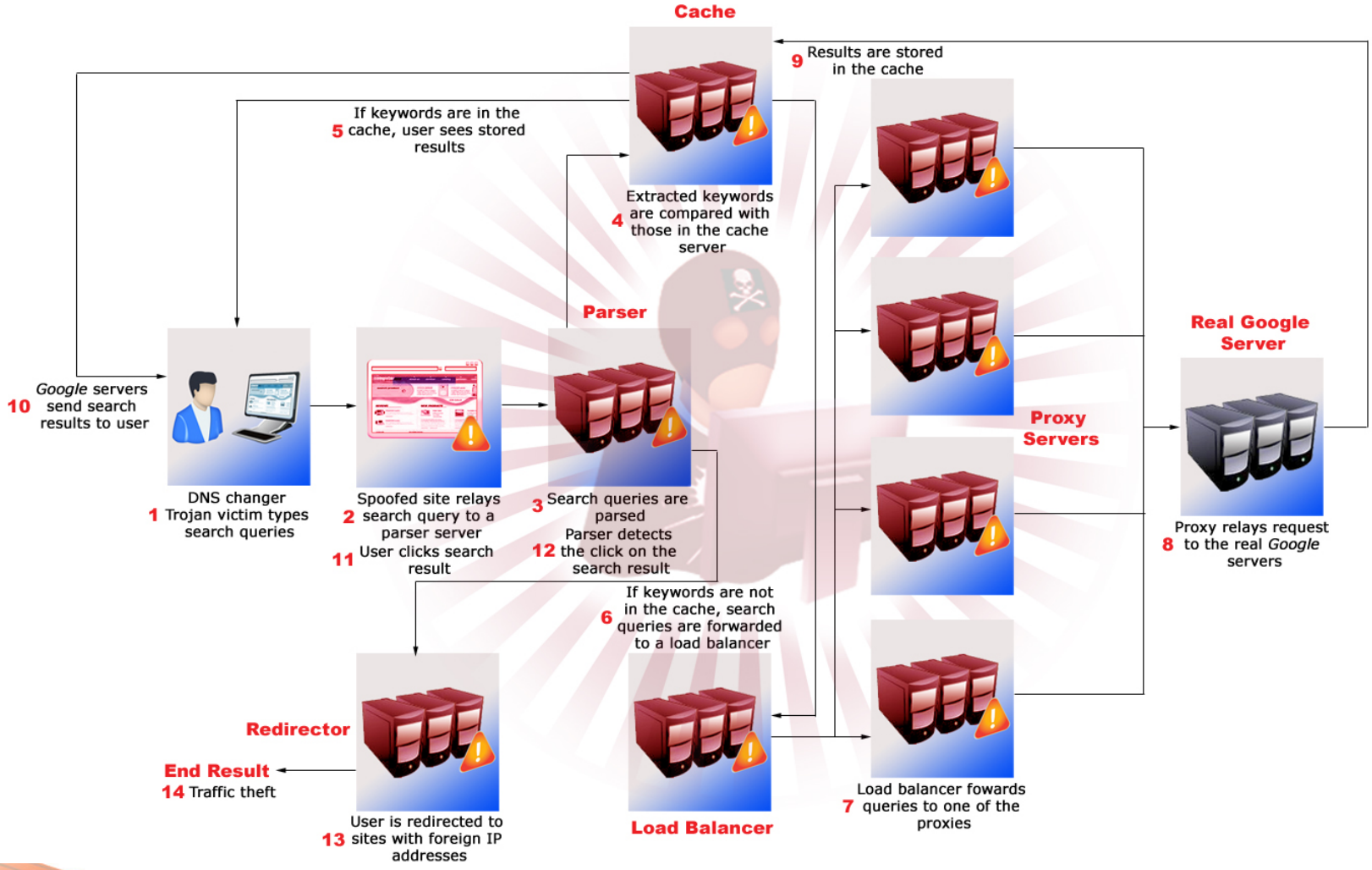
The Problem Continues

- Continuous development of TDSS/TDL4/Alureon rootkit

THANK YOU!

TREND MICRO™

Google Search Fraud – Server Schema



TREND MICRO