



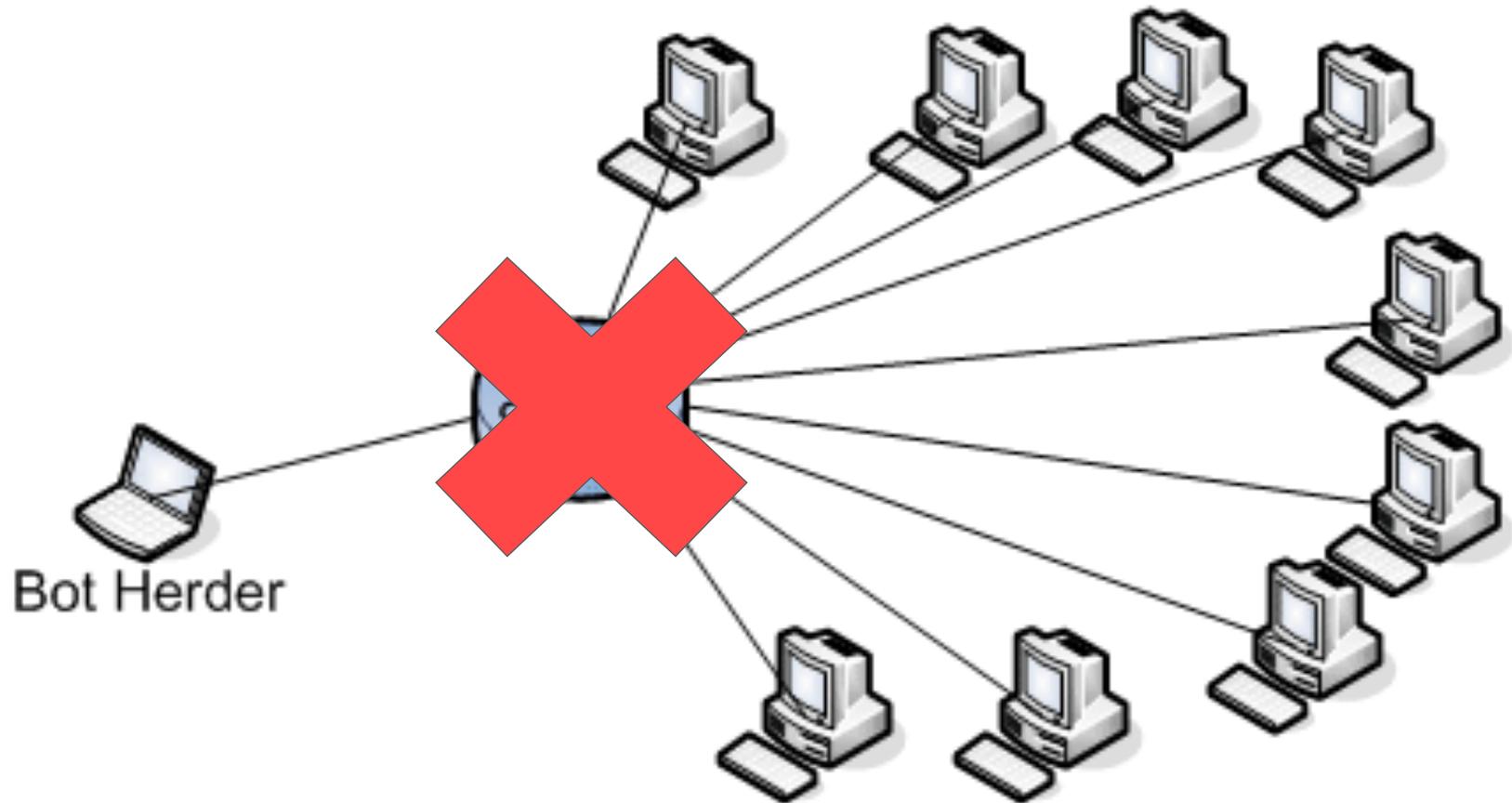
Taking Down a Botnet: The Story Behind Rove Digital's Takedown

Ryan Flores – Forward Looking Threat Research

Confidential



What is a takedown?



Old Architecture



New Architecture

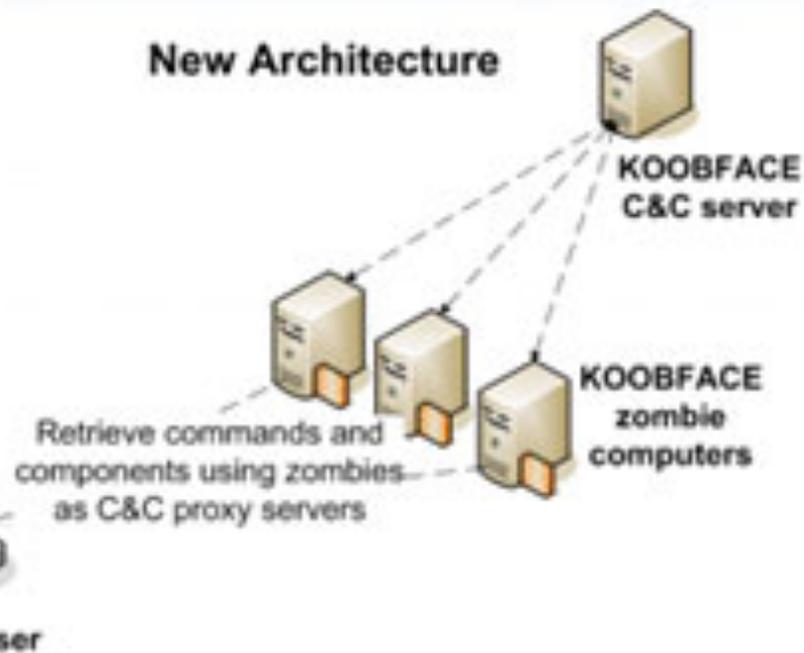
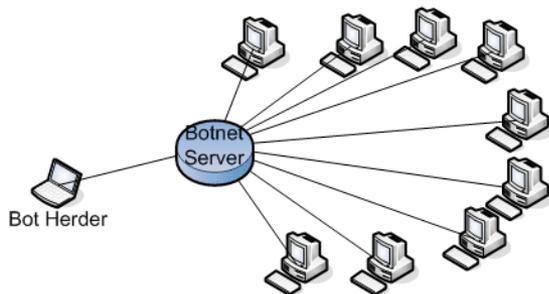
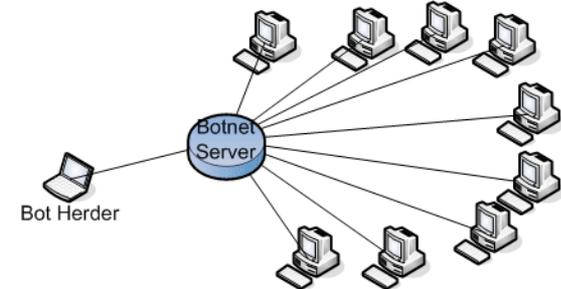
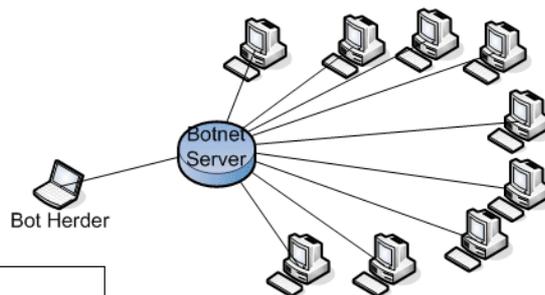
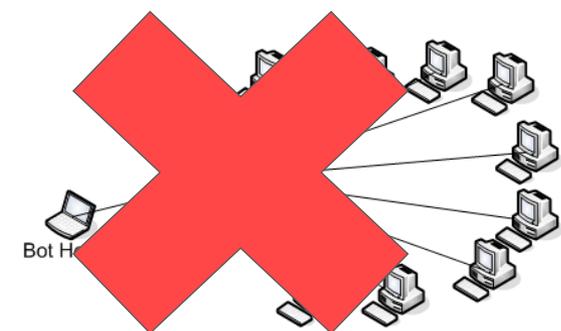
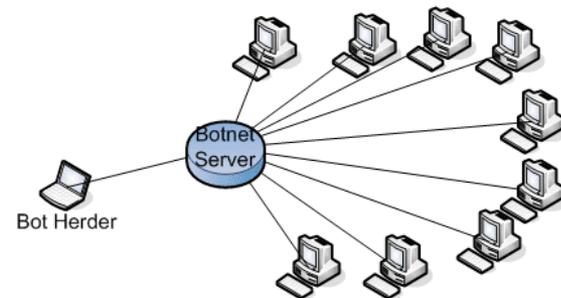


Figure 4. Evolution of KOOBFACE architecture as seen in our fourth paper



MICROSOFT
DIGITAL
CRIMES
UNIT





Takedowns aren't easy

Rove's website

ROVE DOMAINS ADVERTISING HOSTING

[Back to main page](#)

ROVE Phone +372 7 337 055 info@rovedigital.com

[Introduction](#) [Vision](#) [Partners](#) [Our Team](#) [Careers](#) [Contact Us](#)

ROVE Digital is an innovative company with experience in its field and great respect for its customers. It was established in 2002 and has been evolving rapidly since then.

The wide range of services of highest quality and professional co-operation with our partners that is based on trust and respect makes **ROVE Digital** the best choice one can make for the online-business establishment and promotion.

Our products are powered by advanced software that allows simplifying and unifying the management of online services. Experienced customer support team can be reached at any time and is glad to answer all your questions related to **ROVE Digital** services.

People who work for **ROVE Digital** make up a strong goal-oriented team with the main priority to provide the best online services and online solutions ever available.

The customer-oriented philosophy of **ROVE Digital** combined with its cutting-edge technology is a guarantee of the ultimate success in online industry.

Join our team

We are always looking for talented and ambitious people to join our team. Join now.

Client Relationship

[Read more](#)

News

- 30.07.2008
Zmot online advertising system is based on the PPC (pay per click) model applied to the leading and widely used search engines, large
- 23.07.2008
EstDomains, Inc, one of the world's fastest growing domain name Registrar, launched Bakler project several month ago.
- 27.06.2008
The online advertising project ZMOT is live! From now on the powerful online advertising technologies are offered to those who want to

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)



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

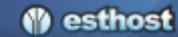




estdomains

Professional Hosting

All in one company. Dedicated Serve



Home

USER LOGIN

Username:

Password:

Role:

Login

[Forgot password?](#)

[Signup for new customer](#)

SEARCH DOMAINS

www. .com

Check Availability in all Extensions

Search

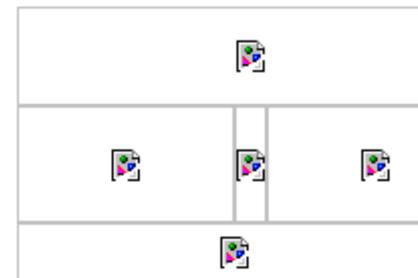
[Transfer your Domain to ESTDOMAINS](#)
* Transfer includes 1 year extension

Domain names

from \$3.69

REPORT ABUSE

Send



PRICING >>

Rove's "advertising" services



- 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...](#)



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)



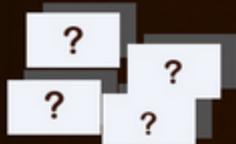
ON THE RADAR

2007

MALICIOUS ACTIVITY



INFRASTRUCTURE



- USED A SPOOFED *GOOGLE ADS* SITE THAT REPLACED THE *GOOGLE ADS* THAT *DNS CHANGER* VICTIMS SAW ON LEGITIMATE SITES

- 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

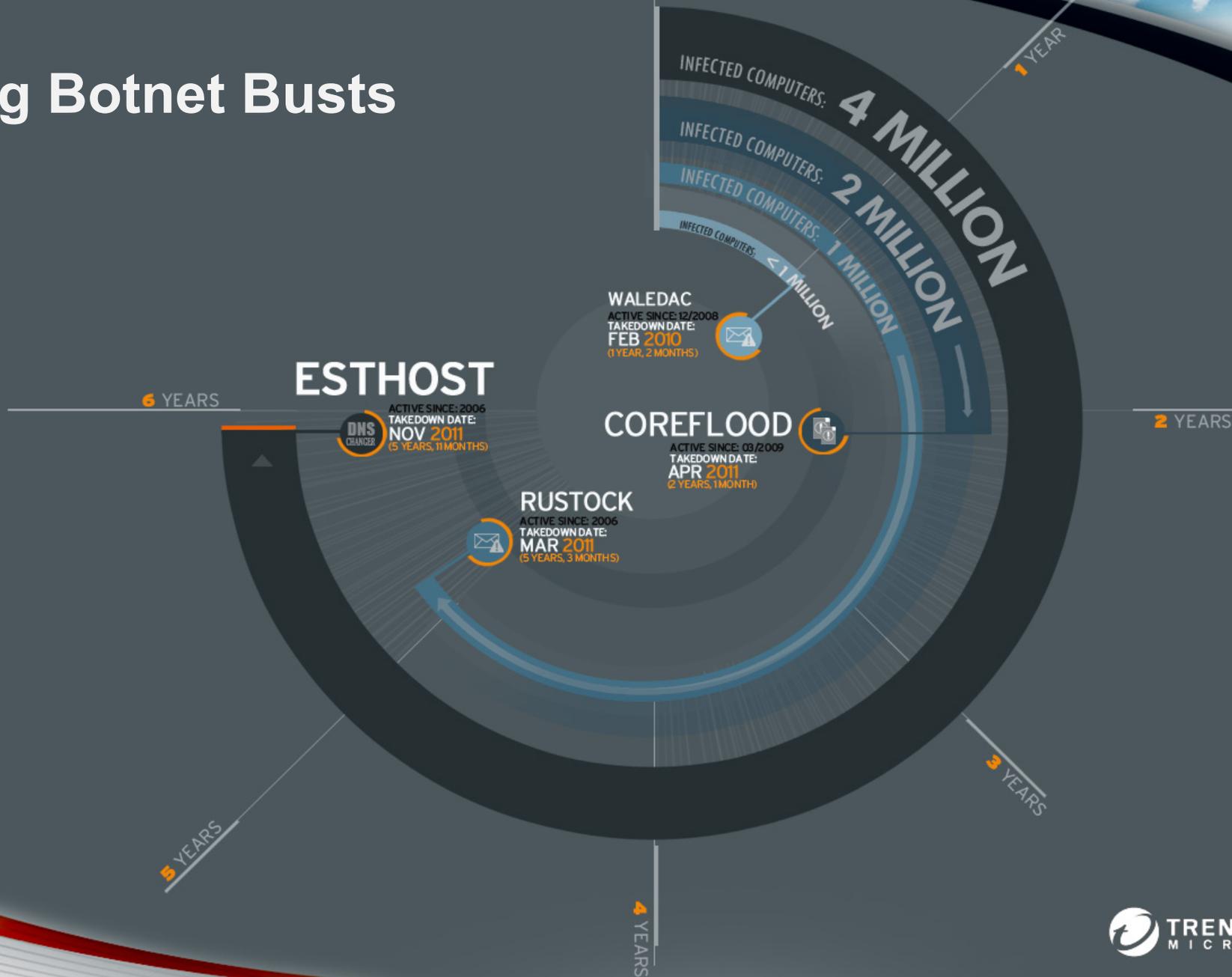
OTHER EVENTS

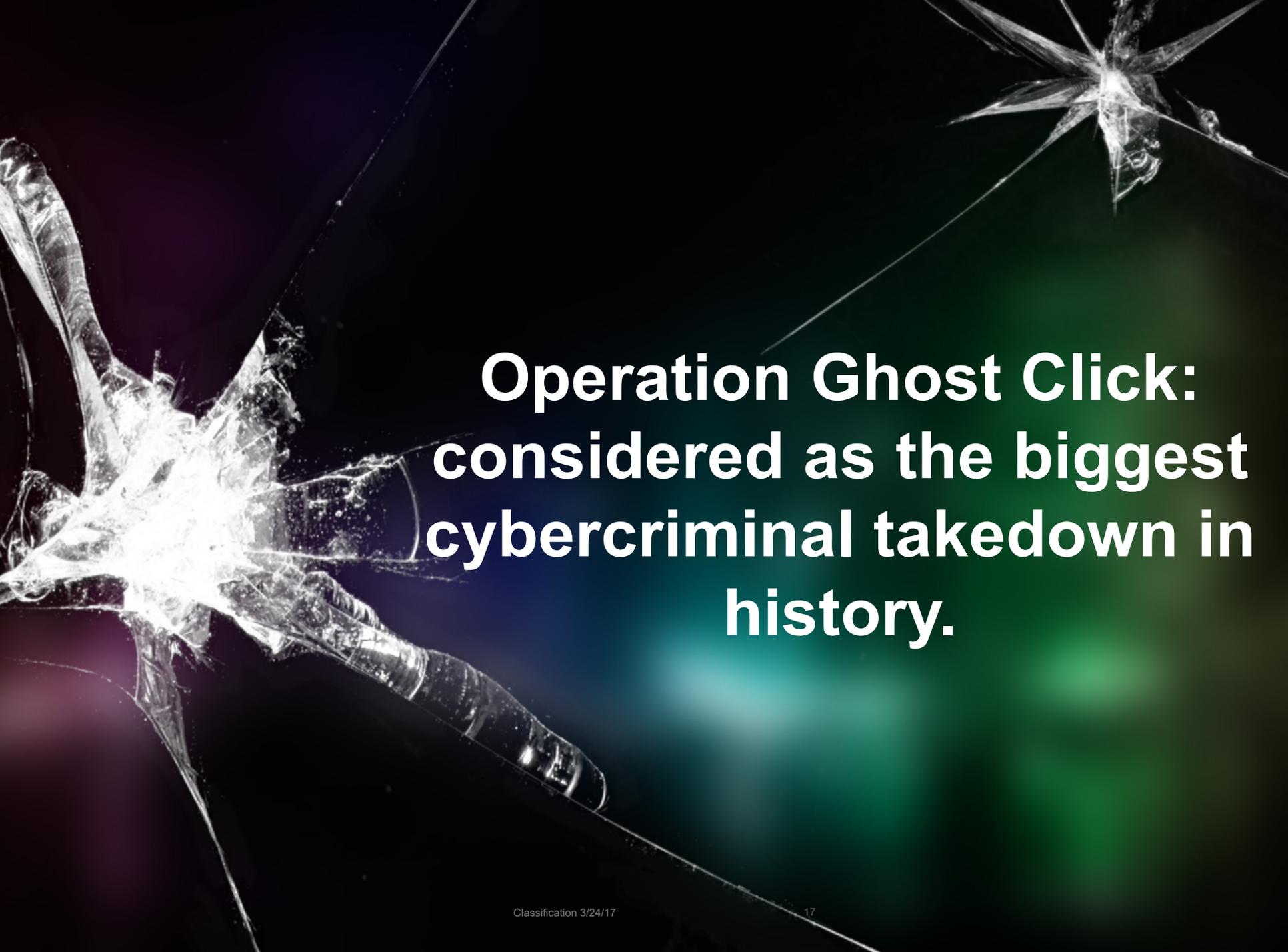


- COLLABORATIVE INVESTIGATION AMONG THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE OFFICE OF INSPECTOR GENERAL (OIG), AS WELL AS TREND MICRO AND ITS INDUSTRY PARTNERS ENSUED



Big Botnet Busts



The background of the slide features a dark, almost black, surface with several large, intricate patterns of shattered glass. These patterns are bright white and translucent, with sharp, radiating lines and jagged edges, suggesting a recent impact or explosion. A soft, green-to-blue gradient is applied to the right side of the image, creating a subtle glow behind the text.

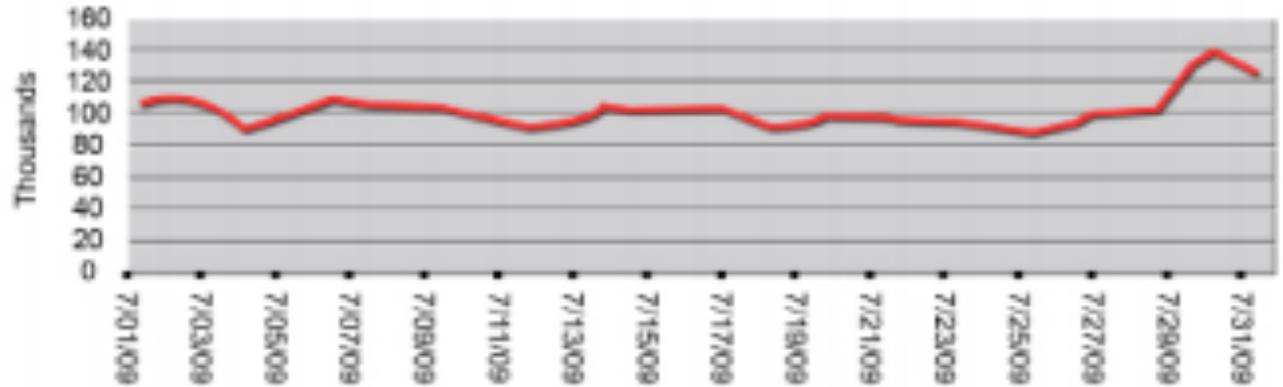
**Operation Ghost Click:
considered as the biggest
cybercriminal takedown in
history.**

Rove Digital/Esthosts ... ISP? Cybercrime hub?

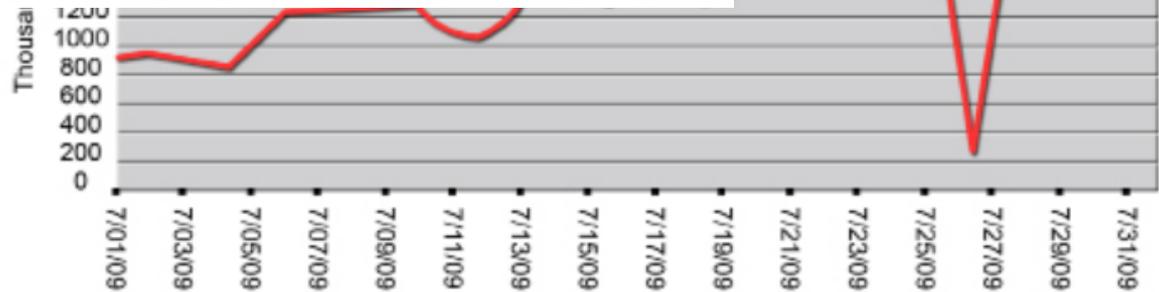
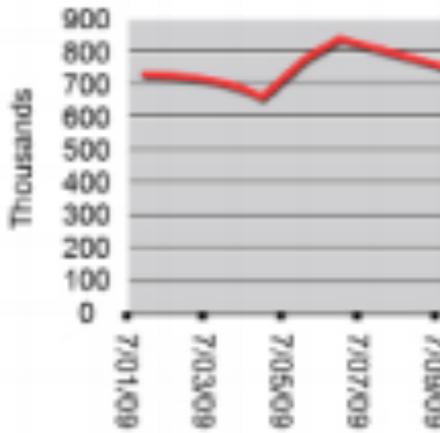
An entrepreneurial professional CEO



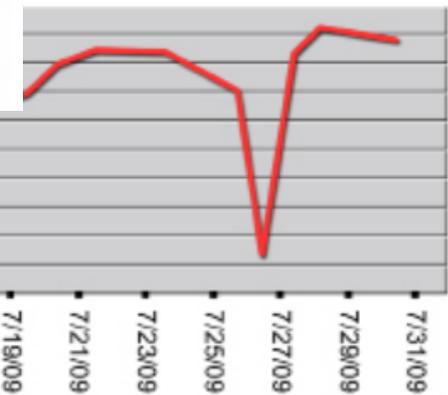
Unique IPs Exposed to Fake Antivirus Instead of Porn



Legitim



Exposed by Vimax Ads



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	

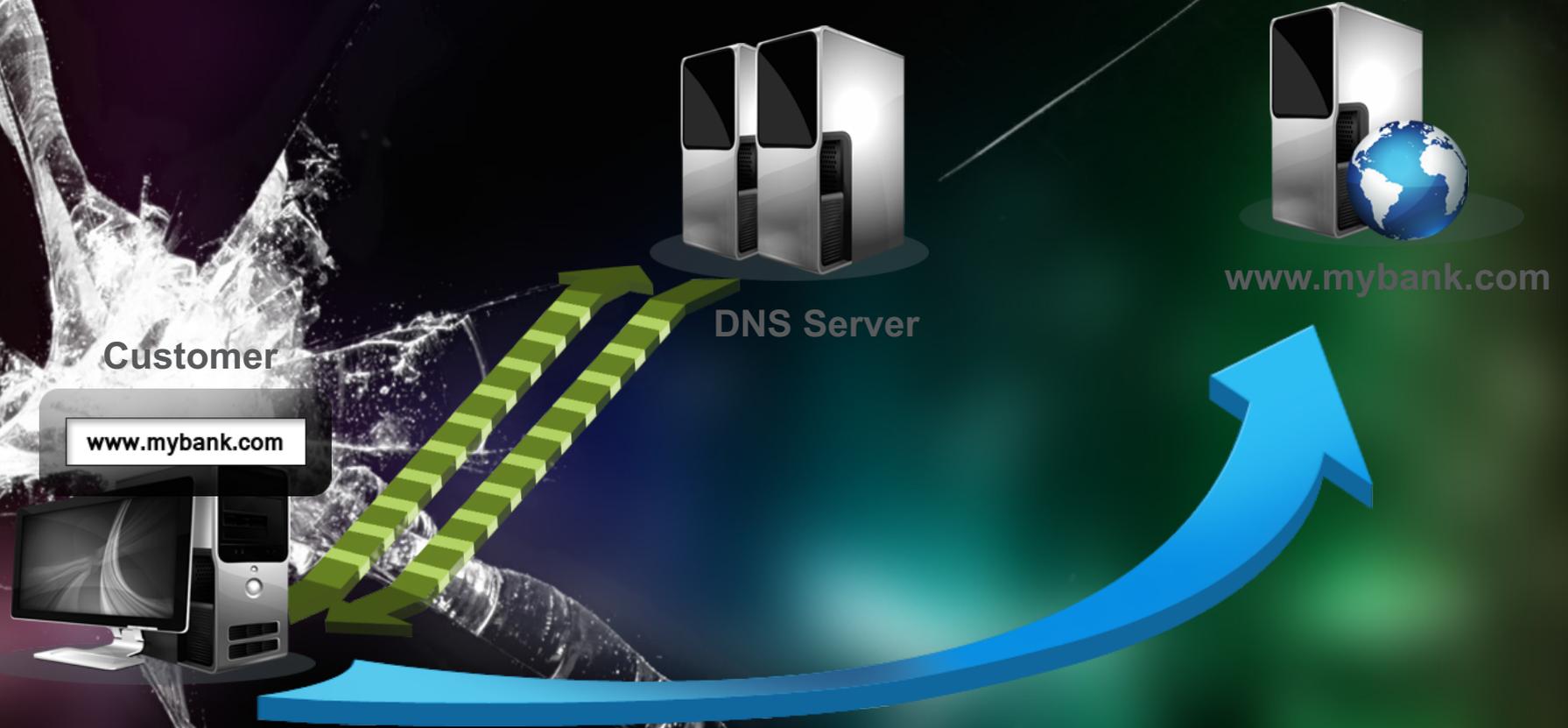
Table 1. One-day earnings of a browser hijack botnet

4,000,000 machines = ?

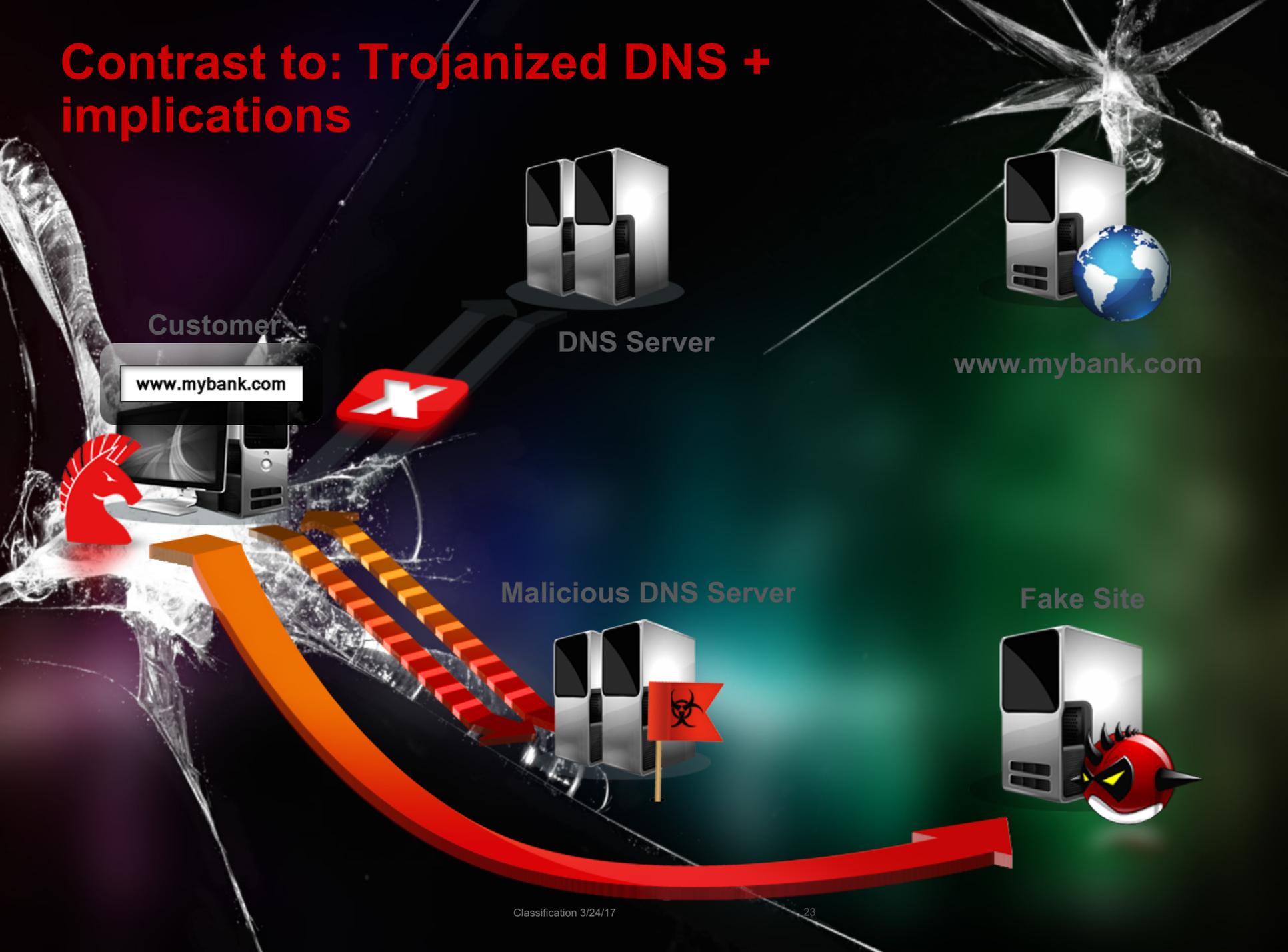
THE PROBLEM

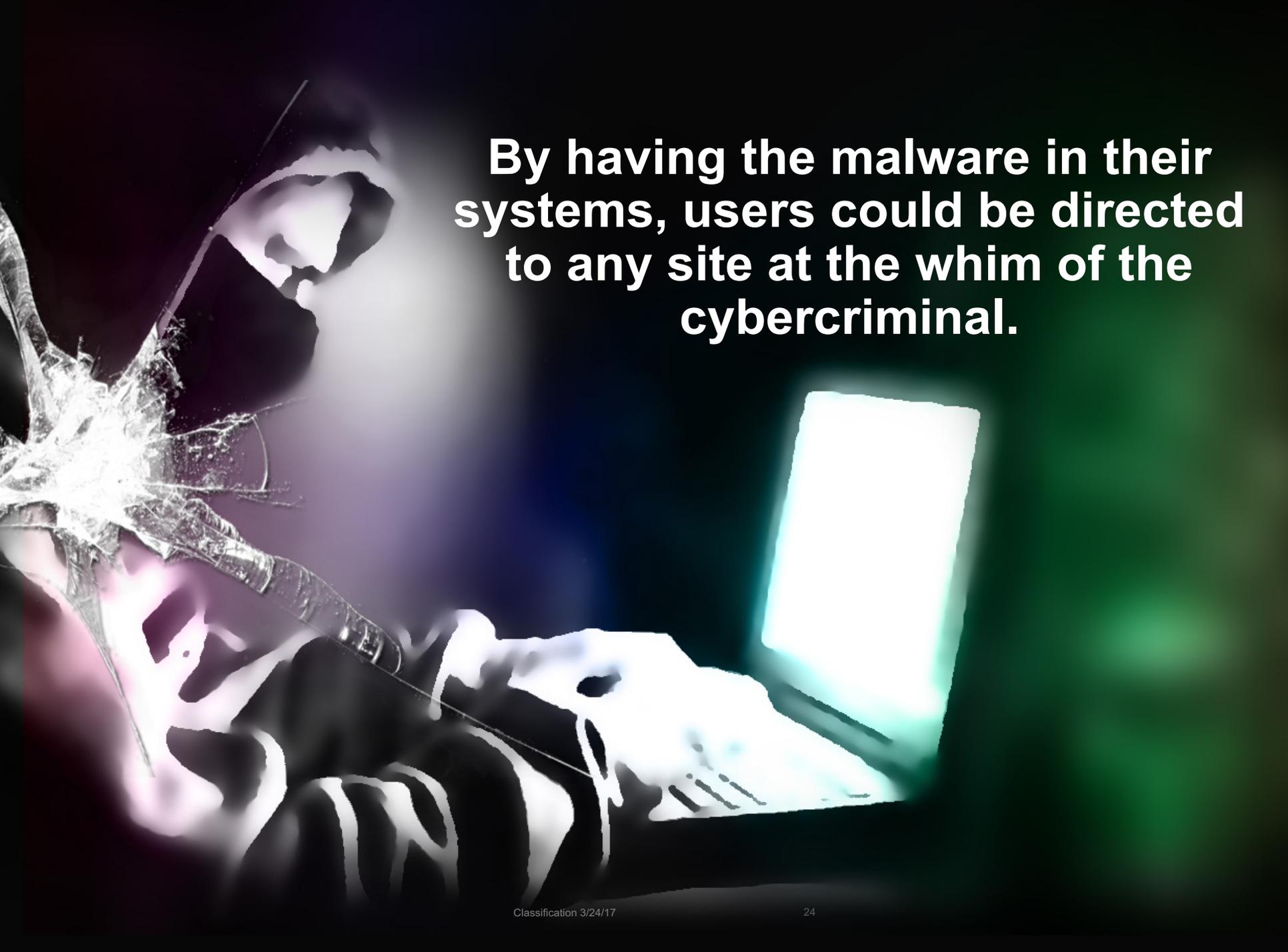


How DNS Works



Contrast to: Trojanized DNS + implications



A person wearing a dark hoodie and a mask is shown in profile, typing on a laptop. The scene is dimly lit, with a strong green glow emanating from the laptop screen, which illuminates the person's hands and the surrounding area. The background is dark, and the overall atmosphere is mysterious and high-tech.

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

CNN website (original)

The screenshot shows the original CNN website interface. At the top, there is a navigation bar with categories like HOME, WORLD, U.S., POLITICS, CRIME, ENTERTAINMENT, HEALTH, TECH, TRAVEL, LIVING, BUSINESS, SPORTS, and TIME.COM. Below this is a search bar and a weather forecast. The main content area is divided into several sections:

- Updated:** 9:17 p.m. EST, Mon January 5, 2009
- Other News:** A list of headlines including "Franken claims victory as lawsuit looms", "Dem senator unhappy with Obama CIA pick", "Obama, Spears Twitter accounts hacked", "Obama pushes huge tax cuts", "Sales plummet for U.S. automakers", "German battlefield yields Roman surprises", "Sheriff: Boy not reported missing for 10 years", "Richard Simmons kisses anchor's foot", "Pictures of Obama girls' first day of school", "Old ladies bowl better than Obama", "Tickler: Candidates for RNC chair knock Bush", "Boy, 4, at rest stop says mom was shot", "People: Source says seizure killed Travolta son", "Parents share heartbreak of children's deaths", "Sex, violence common topics for MySpace teens", "Apple's Steve Jobs explains weight loss", "'Batman' character actor Pat Hingle dies", "SUV goes airborne, flies toward gas pump", and "CNN Wire: Asia, Pacific stocks up early".
- Video:** A section with three video thumbnails: "Simmons kisses anchor's foot 2:14", "Four-year-old: Mom was shot 2:10", and "Madoff hearing 3:20". Below them is a "LIVE: CNN International's global perspective" link.
- Main Article:** A large image of a tank barrel with the headline "'Friendly fire' kills three Israeli soldiers". The text below reads: "The Israeli military surrounded densely populated Gaza City late Monday as the death toll continued to mount in the war-torn territory and both sides showed little interest in international calls for a truce. Military officials also said 'friendly fire' killed three Israeli troops in an explosion in northern Gaza. full story".
- Popular News:** A section with a "SEE TOP 10" button and a large advertisement for "Over 1 Million Men Have Already Tried Vimax Pills" featuring a woman and a man.

CNN website (infected)

The screenshot shows the CNN website interface. At the top, there is a navigation bar with the CNN logo and a search bar. Below the navigation bar, there are several menu items including HOME, WORLD, U.S., POLITICS, CRIME, ENTERTAINMENT, HEALTH, TECH, TRAVEL, LIVING, BUSINESS, SPORTS, and TIME.COM. A "Hot Topics" section lists items like Hamas, Bill Richardson, John Travolta, Gaza Crisis, and Year in Review. The main content area features a large article titled "'Friendly fire' kills three Israeli soldiers" with a photo of a tank. To the right, there is a "Video" section with three video thumbnails. A red dashed box highlights a "CONSUMERGUIDE 2009 BEST BUY AWARD WINNER" advertisement for a black SUV.

updated 9:17 p.m. EST, Mon January 5, 2009

Make CNN Your Home Page

CNN.com

SEARCH

HOME WORLD U.S. POLITICS CRIME ENTERTAINMENT HEALTH TECH TRAVEL LIVING BUSINESS SPORTS TIME.COM VIDEO IREPORT IMPACT

Hot Topics + Hamas - Bill Richardson - John Travolta - Gaza Crisis - Year in Review - more topics »

Weather Forecast Editors: International | Set Pref

Set your CNN.com Edition CNN U.S. CNN International SET EDITION

Other News

- Franken claims victory as lawsuit looms 60 min
- Dem senator unhappy with Obama CIA pick 22 min
- CNNMoney: Obama pushes huge tax cuts
- Obama, Spears Twitter accounts hacked
- CNNMoney: Sales plummet for U.S. automakers
- German battlefield yields Roman surprises
- Sheriff: Boy not reported missing for 10 years
- Richard Simmons kisses anchor's foot 1:31
- Pictures of Obama girls' first day of school
- Old ladies bowl better than Obama 5:17
- Ticker: Candidates for RNC chair knock Bush
- Boy, 4, at rest stop says mom was shot 1:31
- People: Source says seizure killed Travolta son
- Parents share heartbreak of children's deaths
- Sex, violence common topics for MySpace teens
- Apple's Steve Jobs explains weight loss
- 'Batman' character actor Pat Hingle dies
- SUV goes airborne, flies toward gas pump 1:31
- CNN Wire: Asia, Pacific stocks up early

Video

- Simmons kisses anchor's foot 1:31
- Four-year-old: Mom was shot 2:10
- Maddoff hearing 3:35

LIVE: CNN International's global perspective

CONSUMERGUIDE 2009 BEST BUY AWARD WINNER

Porn ?

WiniFighter Help protect your PC

Scan | Quarantine | Report | Tasks | Realtime protection

Threat	Type	Threat Level	Location
<input type="checkbox"/> Advanced Po...	Remote Co...	Medium	C:\WINDOW
<input type="checkbox"/> HellFire Trojan	Malware	High	C:\WINDOW
<input type="checkbox"/> Bubbel	Remote Co...	Medium	C:\WINDOW
<input type="checkbox"/> Hungry	Malware	High	C:\WINDOW
<input type="checkbox"/> Trojan-PSW....	Malware	High	C:\WINDOW
<input type="checkbox"/> Email-Worm.J...	Worm	High	C:\WINDOW
<input type="checkbox"/> EICAR Trojan	Malware	High	C:\WINDOW
<input type="checkbox"/> DFch Grisch	Remote Co...	Medium	C:\WINDOW
<input type="checkbox"/> Trojan-Spy....	Malware	High	C:\WINDOW
<input type="checkbox"/> Trojan-MS22	Malware	High	C:\WINDOW

713 SPYWARE Found

Attention: DANGER!

WiniFighter has detected **713 Critical SPYWARE Objects** while scanning the system. Following object will shortly interrupt system running by:

- Annoying advertisements wasting your traffic.
- Slow page downloading speed. Web browser is not working properly.

ANAL CAMS | ASIAN CAMS
BRUNETTE CAMS | LESBIAN CAMS
LATINA CAMS | AMATEUR CAMS

et eine Anfrage über DOS Angriff an unsere
ervorgerufen, das "Troj/Rustok-N?" heißt. Wir
rem Kontent zu gewährleisten, damit Sie
vermeidlichen Zerstörung unserer Web-Seite
ntivirusprogramm zu aktivieren und, wenn es
ungen/Updates zu prüfen. **Sie können also das
von vielen unseren Internet-Besuchern gebilligt
gramm benutzen, um Problem zu lösen.**

bevor Sie weiter recherchieren.
e Beute für die Hacker werden.

störungen
über Kreditkarte
Datenträger, Zum Beispiel
Zeichen der Infektion in Ihrem
nickt werden.
virusprogramm benutzen. Wir
mit dem Programm, das schon

WiniFighter 1.2.0.63 Setup

Welcome to the WiniFighter 1.2.0.63 Setup Wizard

This wizard will guide you through the installation of WiniFighter 1.2.0.63.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

www.winifighter.com

Next >

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
EST domains
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
codecsft3.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

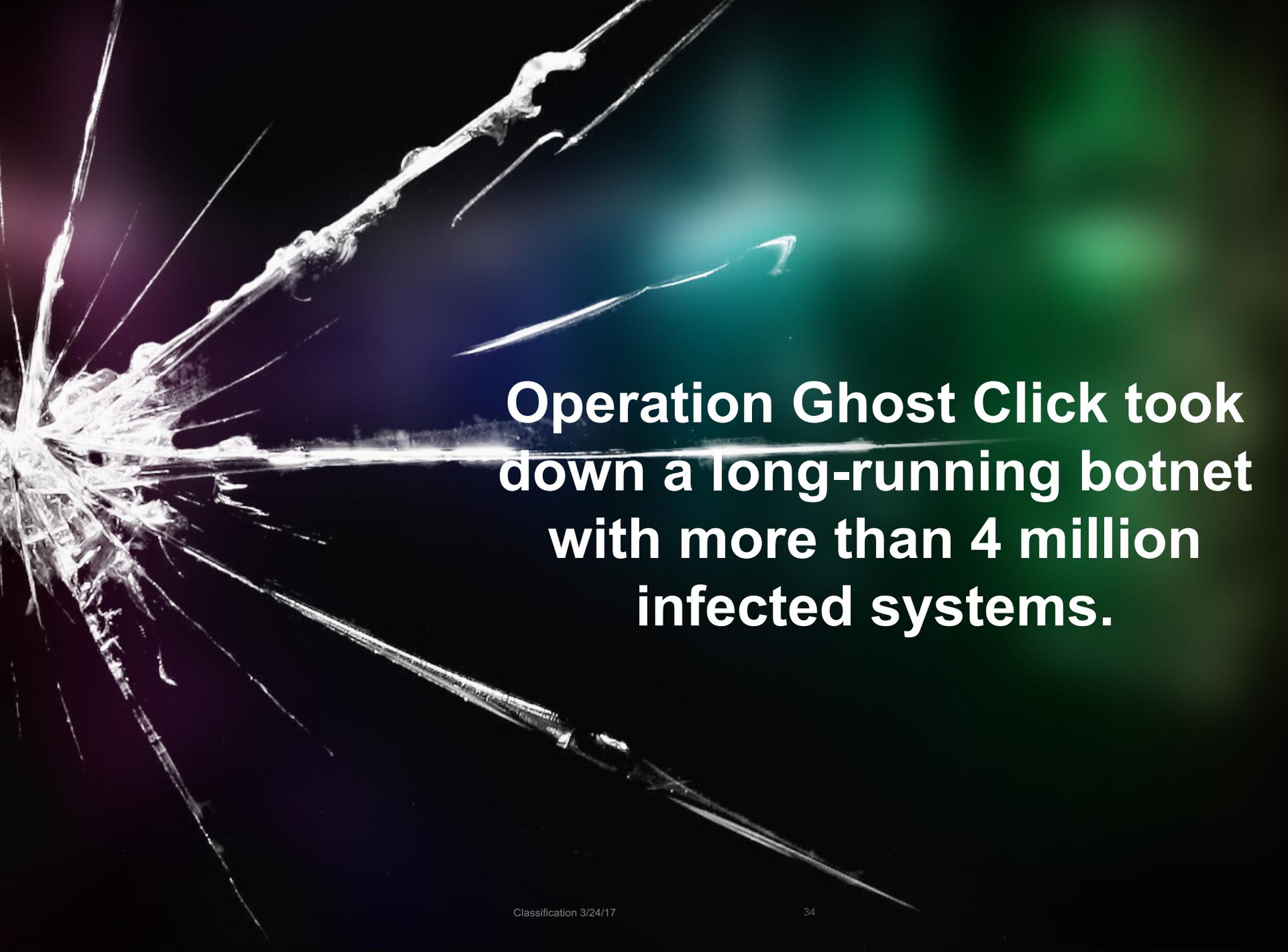
gcache1.intra	86400	IN	A	69.31.x.x
gcache2.intra	86400	IN	A	67.210.x.x

Fake AV sites

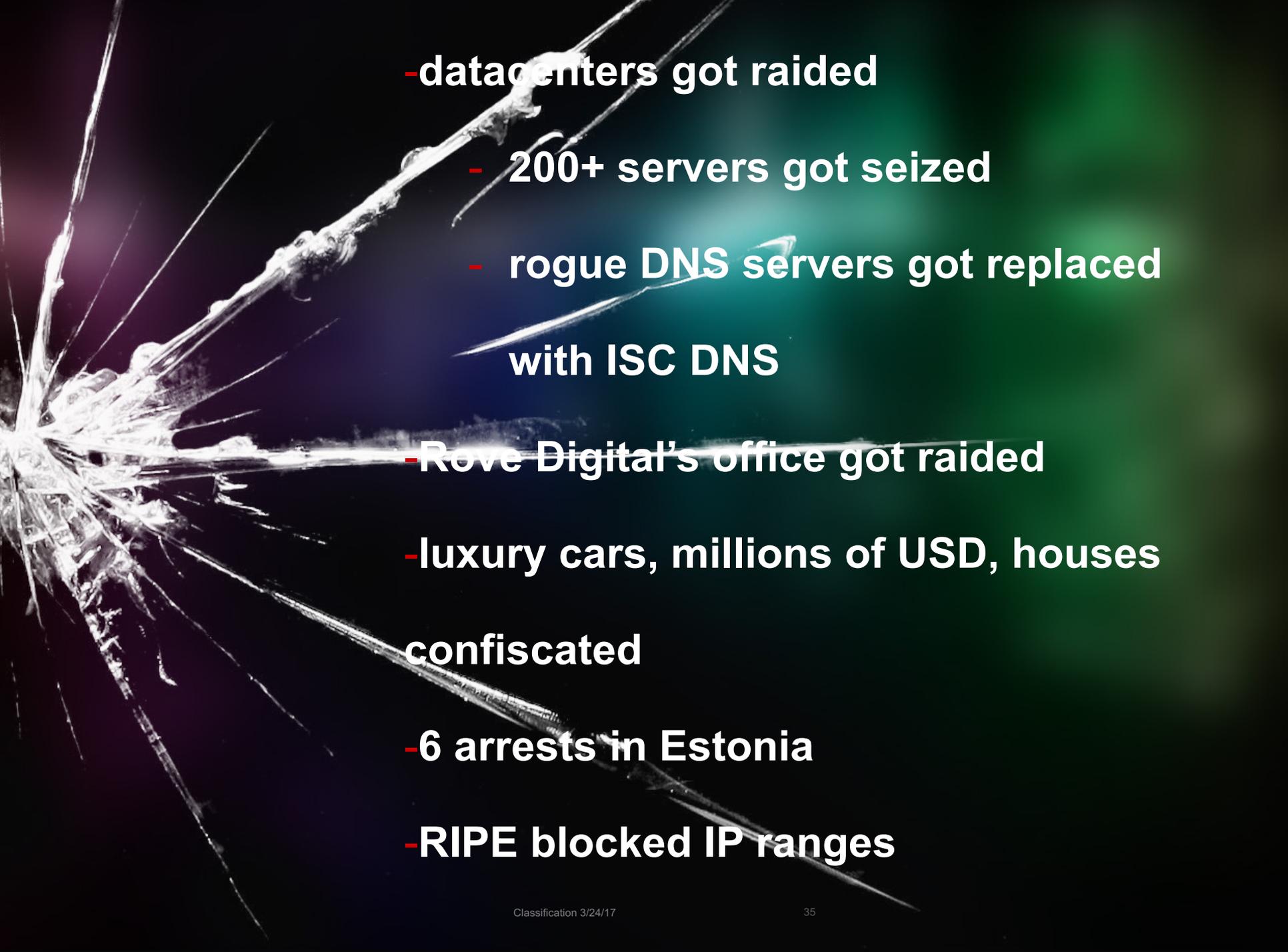
blilling.intra	86400	IN	A	64.28.x.x
blillingproxy1.intra	86400	IN	A	78.159.x.x
blillingproxy2.intra	86400	IN	A	88.198.x.x

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**
 - **RRIPE 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**

A magnifying glass with a white frame and a black handle is positioned on the left side of the image. The lens is focused on a city map, likely Indianapolis, which is overlaid with a red, semi-transparent threat map. The background of the entire image is a dark, multi-colored map with green, blue, and red hues. The text is centered in the right half of the image.

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	<ul style="list-style-type: none">• DNS knowledge,• knowledge how Websites work• knowledge how advertising work
Investigation	<ul style="list-style-type: none">• Forensic skill (hard disks),• DNS skill ,• Pentesting skill set,• Internet forensics• Sandboxing and reverse engineering
Take down	<ul style="list-style-type: none">• Transnational nature of the crime (different police, different laws),• Number of players high (many DC owner, many ISP's)• confidentiality

The image features a magnifying glass with a white frame and a black handle, positioned over a city map. The map is overlaid on a background of large, overlapping circles in shades of red, orange, green, and blue. The text "Did you lose your Internet last July 9?" is centered in white. The map shows various streets and landmarks, with the word "Indianapolis" visible in the lower-left quadrant.

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 it is 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!

Google Search Fraud – Server Schema

