A Perspective on Malware Summer 2008

Lenny Zeltser

www.zeltser.com

Malware is the infrastructure that drives illicit activities on-line.

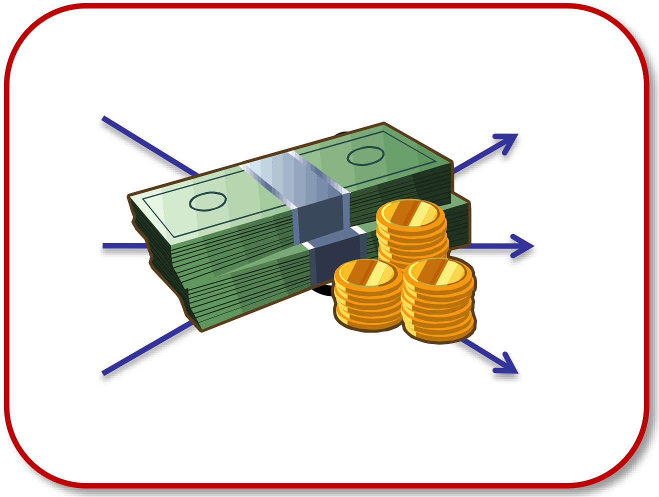
Modern malware is…

Targeted

Distributed

Self-Defending

Money-Making

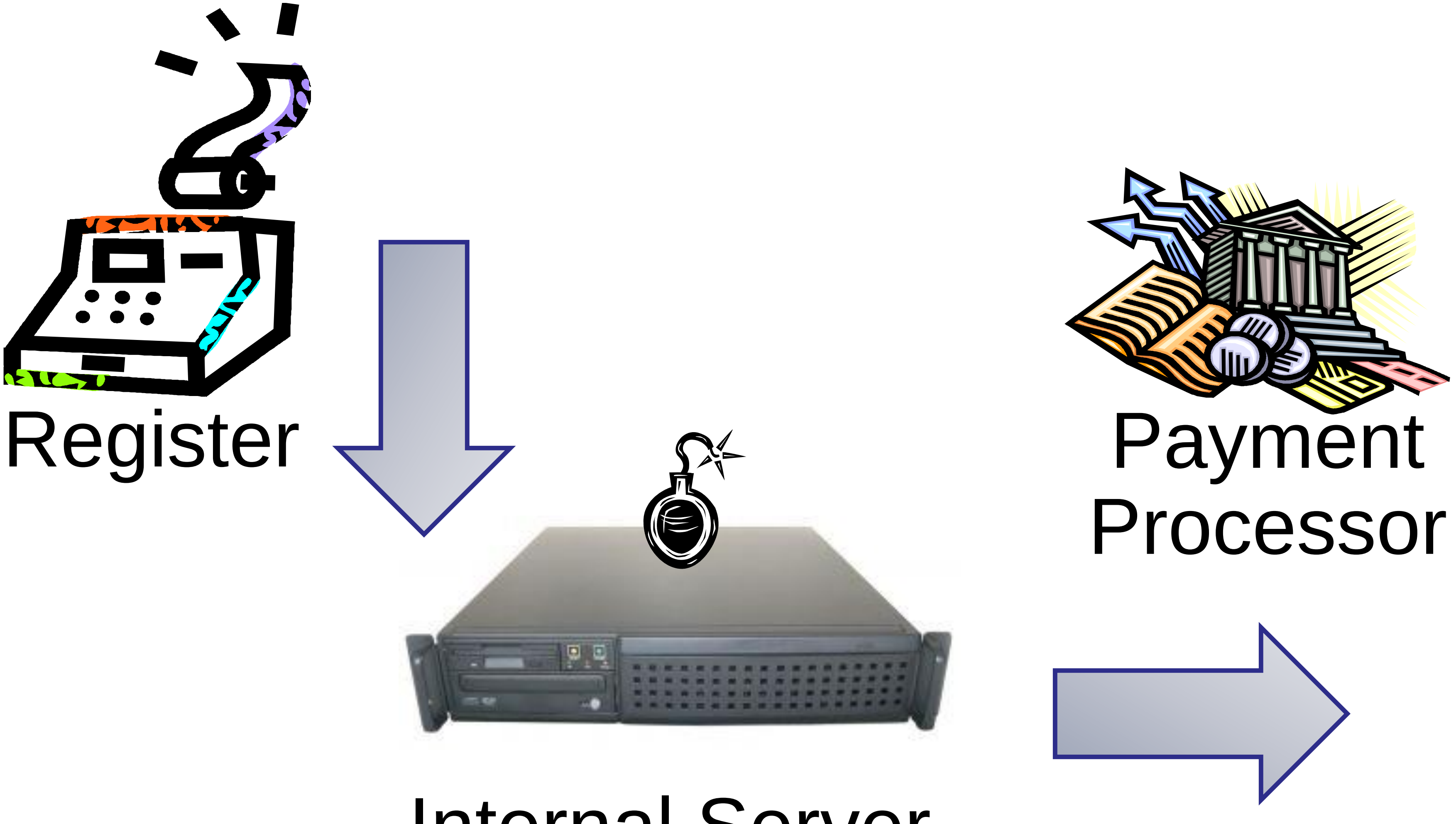


Survey the malware landscape to account for threats.

Targeted Characteristics

Malware on 300 compromised servers captured credit card data.

Captured data in transit during authorization (12/07-3/08)



Register

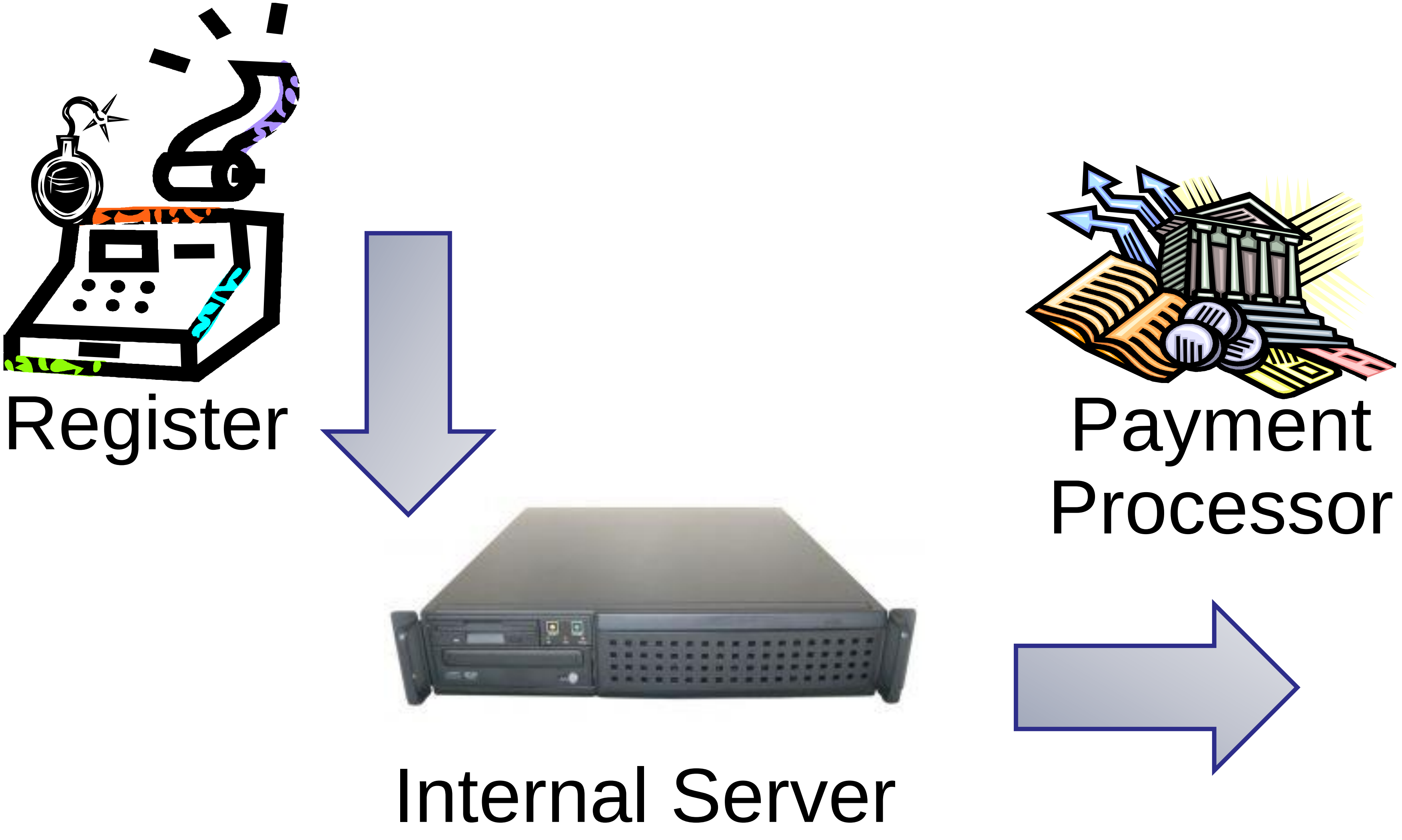
Internal Server

Payment Processor

1,800 cases of reported fraud

Captured Track 2 data allows creation of physical cards.

Track 2 data was also captured in an attack on Dave & Buster's.



Register

Internal Server

Payment Processor

Focused, polished attacks on pro-Tibet groups.

Documents attached to emails carried exploits.

Spoofed as if from a trusted source.

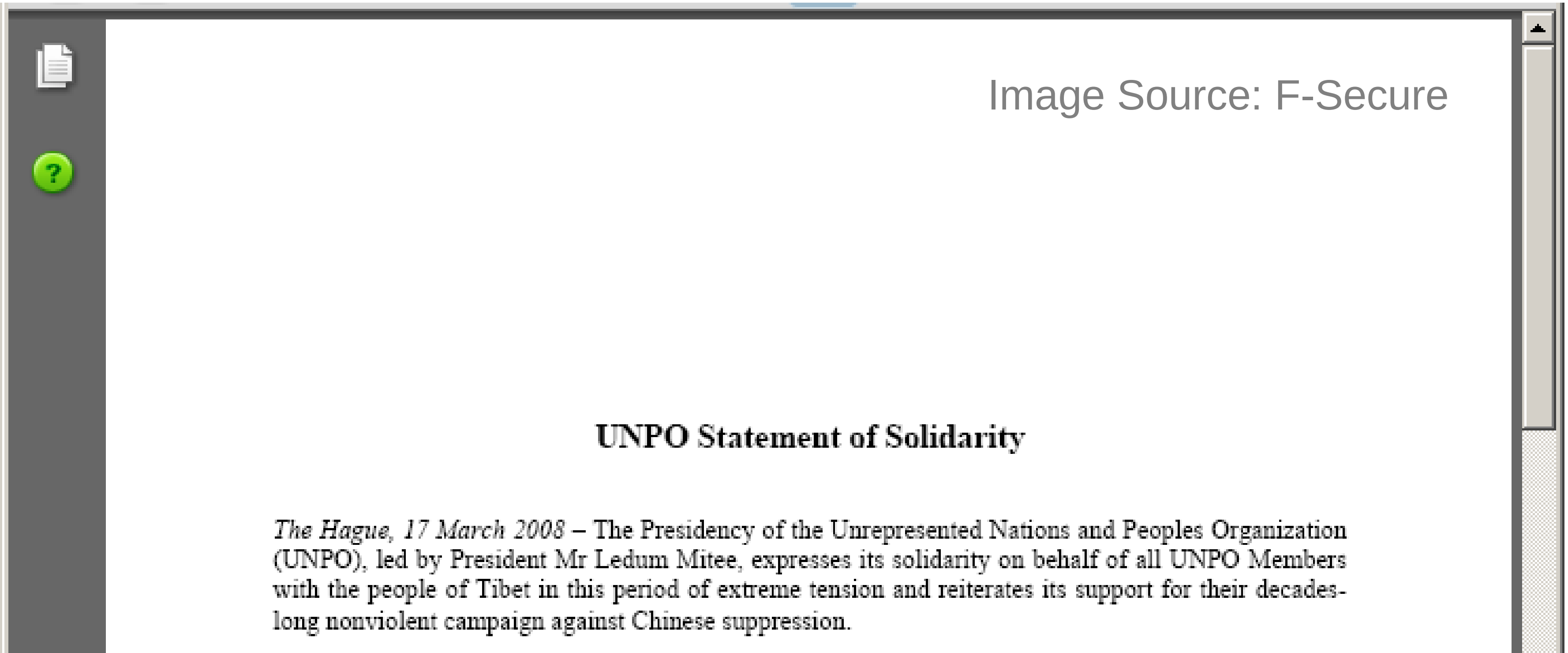
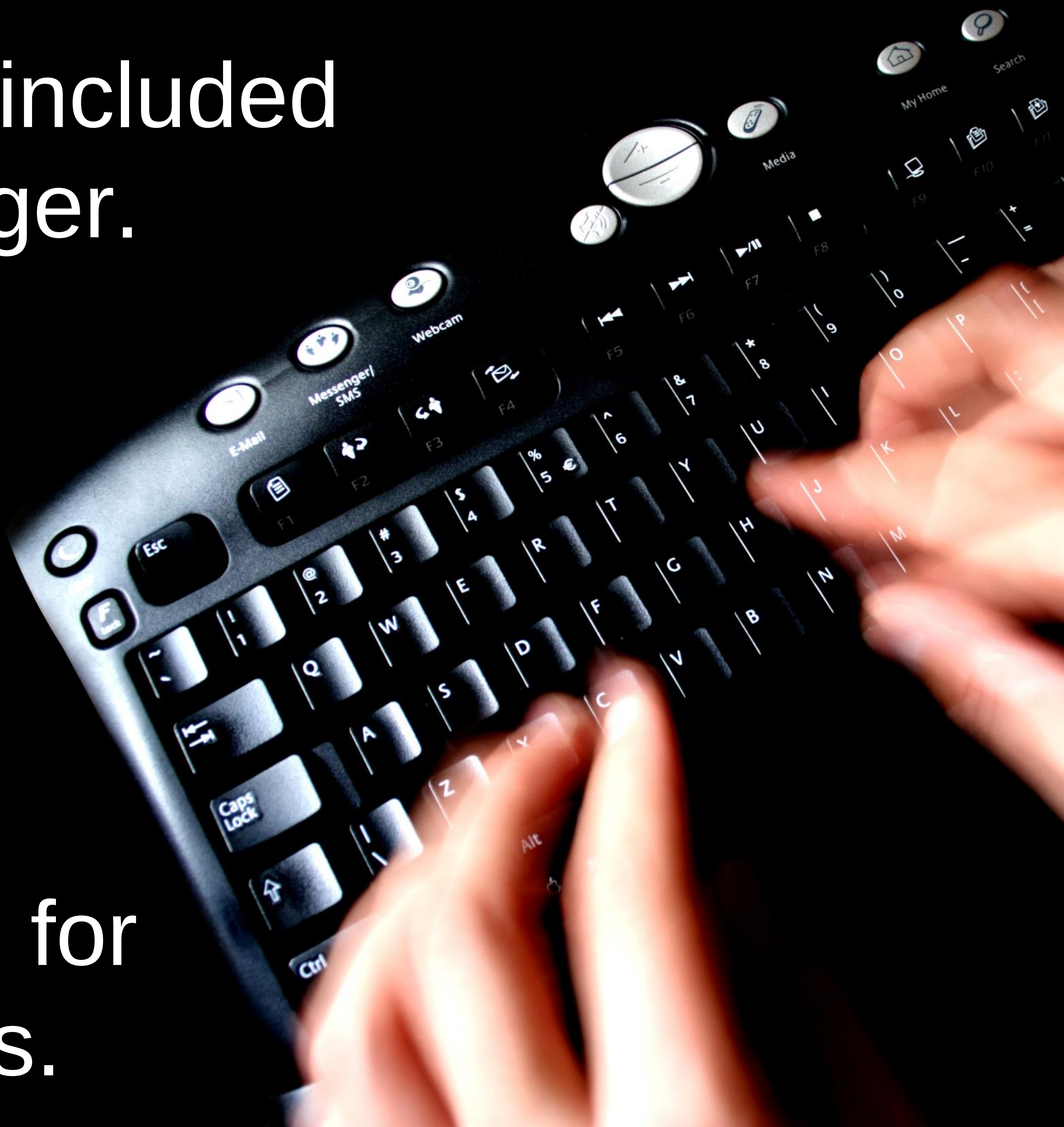


Image Source: F-Secure

UNPO Statement of Solidarity

The Hague, 17 March 2008 – The Presidency of the Unrepresented Nations and Peoples Organization (UNPO), led by President Mr Ledum Mitee, expresses its solidarity on behalf of all UNPO Members with the people of Tibet in this period of extreme tension and reiterates its support for their decades-long nonviolent campaign against Chinese suppression.

Payload included a keylogger.

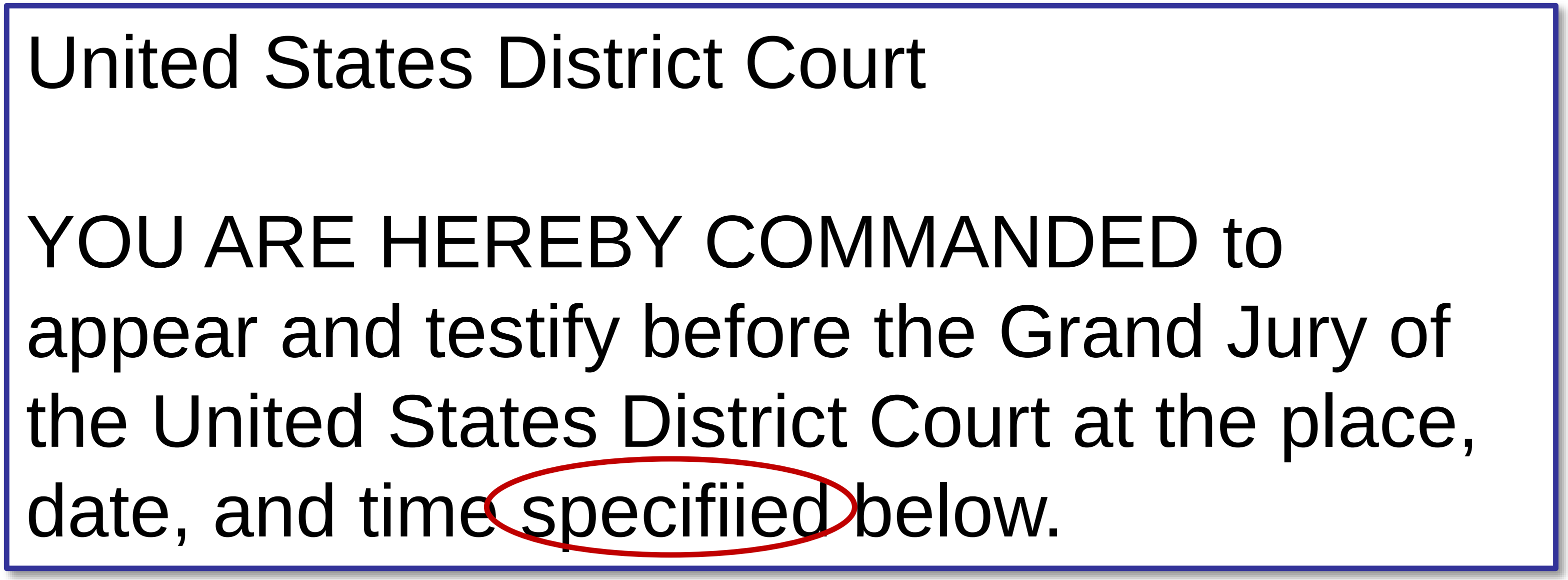


Some searched for PGP keys.

20,000 executives targeted with fake subpoenas via email.

Half at financial institutions.

Included name, company name and phone number.



United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specifiied below.

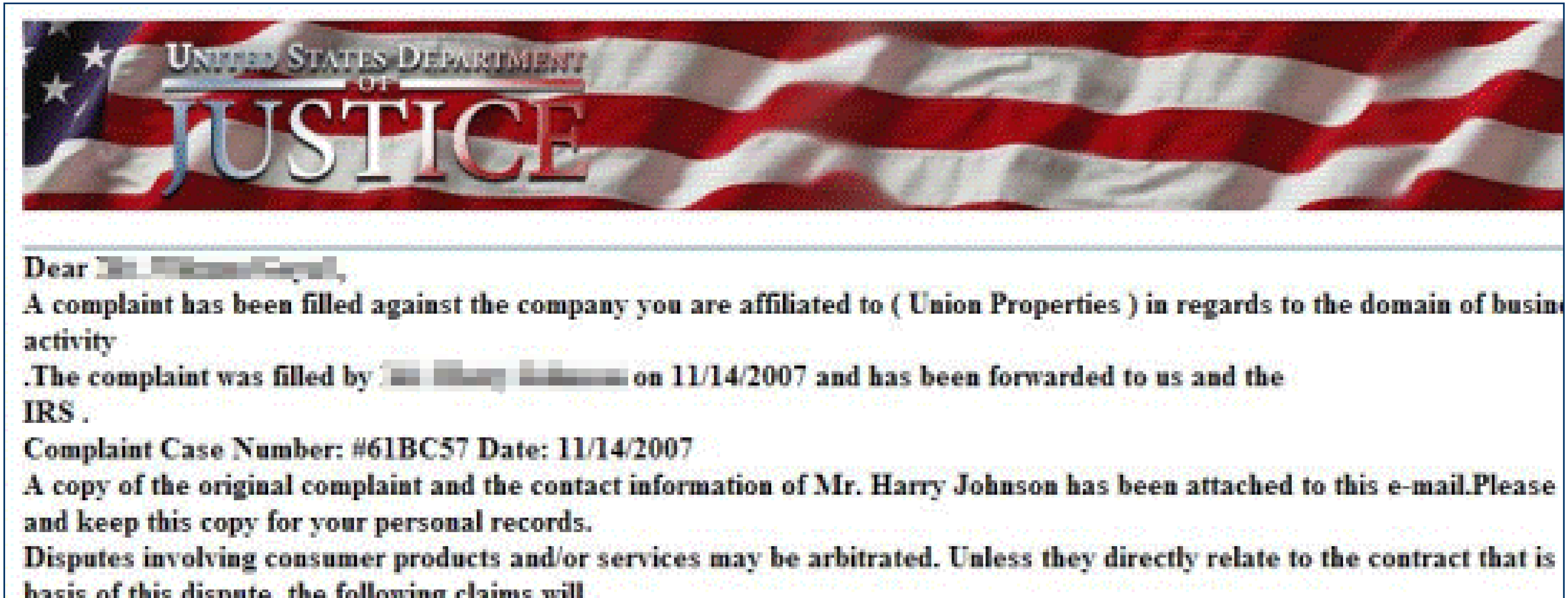
Requested to install an add-on to view the subpoena PDF.

Payload included keylogger.

Also looked for local certificates.

May be responsible for earlier campaigns (BBB, IRS).

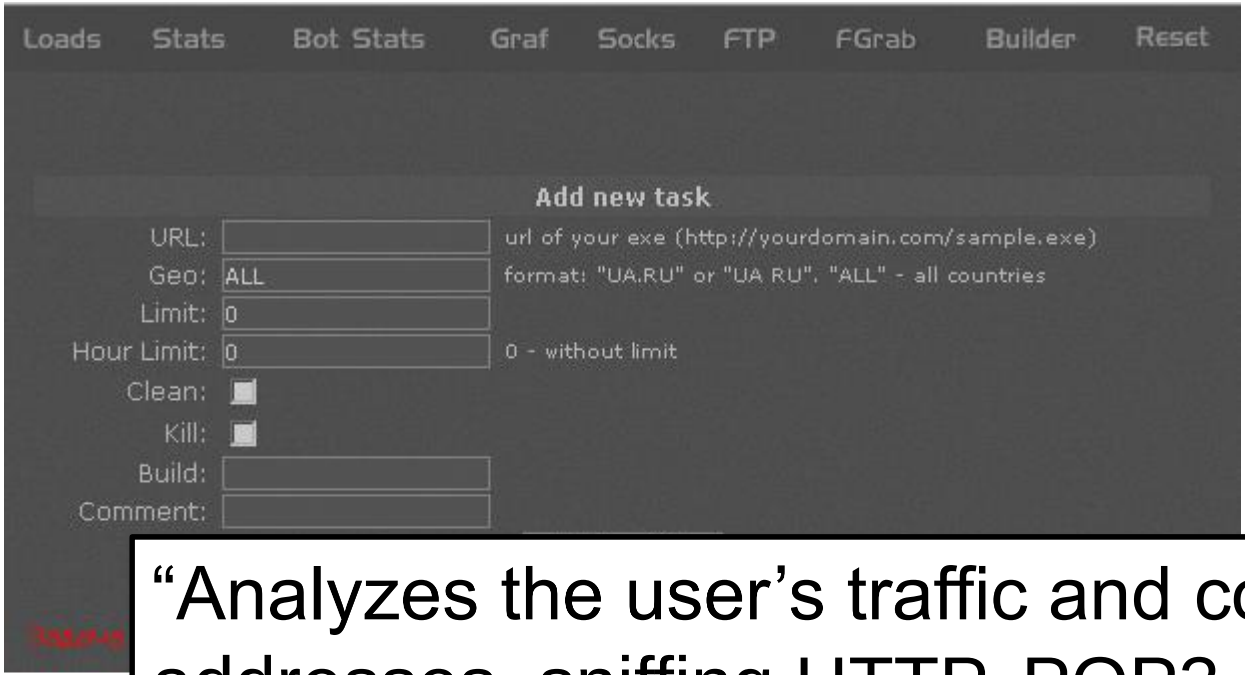
Image Source: Websense



Dear [redacted],
A complaint has been filled against the company you are affiliated to (Union Properties) in regards to the domain of busin
activity
.The complaint was filled by [redacted] on 11/14/2007 and has been forwarded to us and the
IRS .
Complaint Case Number: #61BC57 Date: 11/14/2007
A copy of the original complaint and the contact information of Mr. Harry Johnson has been attached to this e-mail.Please
and keep this copy for your personal records.
Disputes involving consumer products and/or services may be arbitrated. Unless they directly relate to the contract that is
basis of this dispute, the following claims will

Distributed Characteristics

Zalupko is a modular bot with a web control panel.



Add new task

URL: url of your exe (http://yourdomain.com/sample.exe)

Geo: ALL format: "UA.RU" or "UA RU". "ALL" - all countries

Limit: 0

Hour Limit: 0 0 - without limit

Clean: ☐

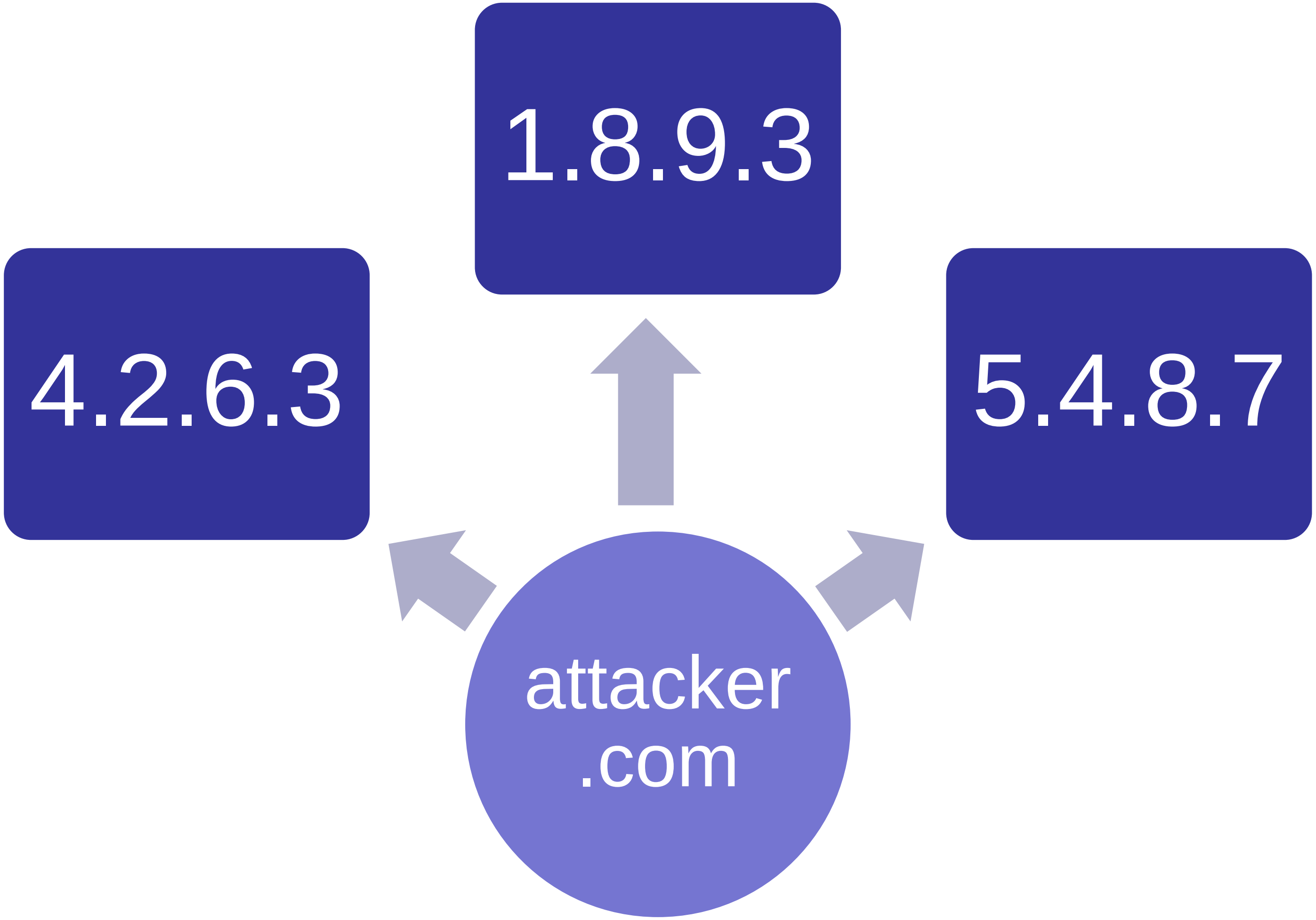
Kill: ☐

Build:

Comment:

"Analyzes the user's traffic and collects all email addresses, sniffing HTTP, POP3, and SMTP protocols. Keeps track of the credential's uniqueness locally for each bot to decrease the load on the server"

Dynamic DNS often used to communicate with the attacker.



1.8.9.3

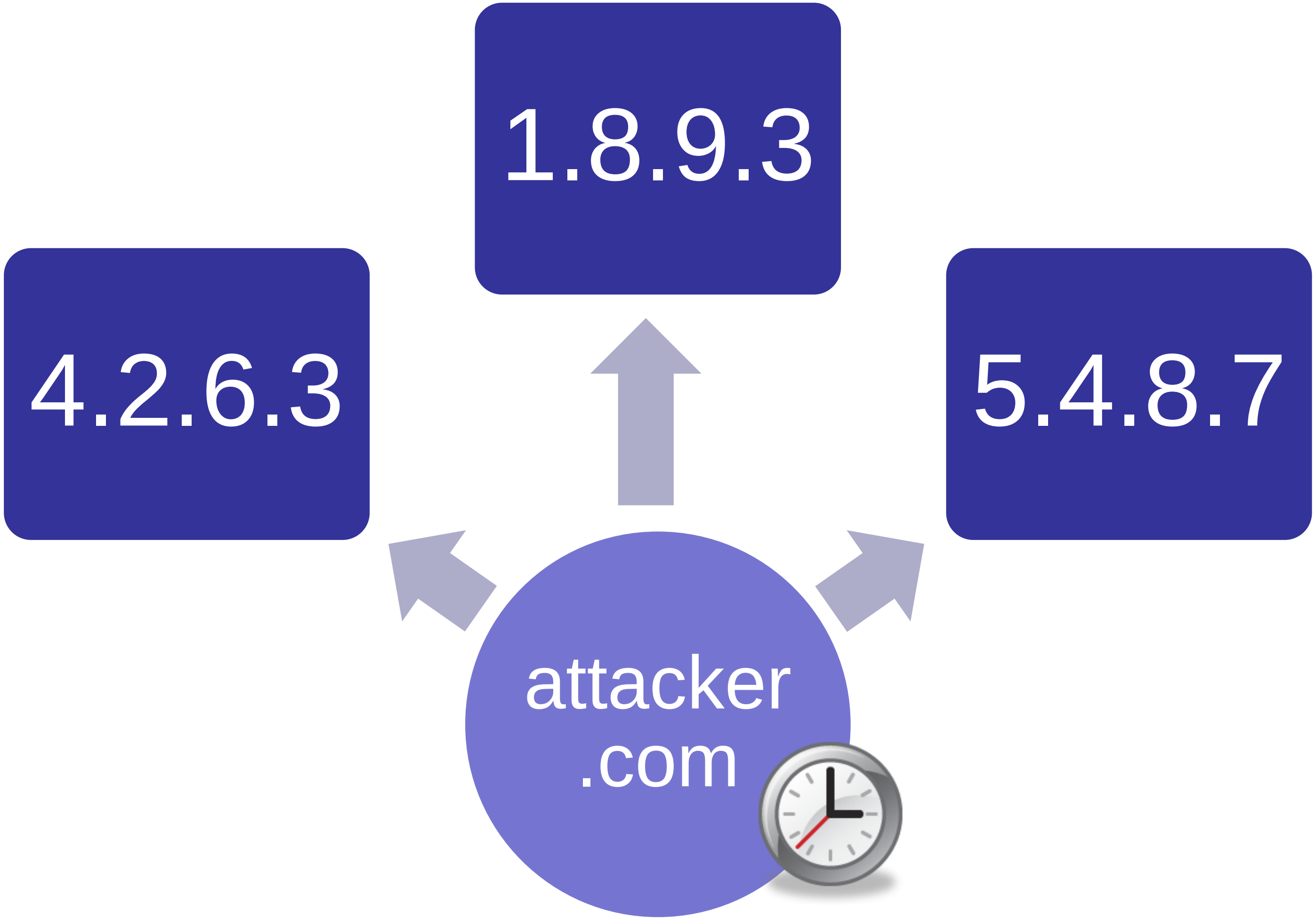
4.2.6.3

5.4.8.7

attacker
.com

Kraken bot pre-generated dynamic DNS names for C&C.

In fast-flux DNS the mappings change every few minutes.

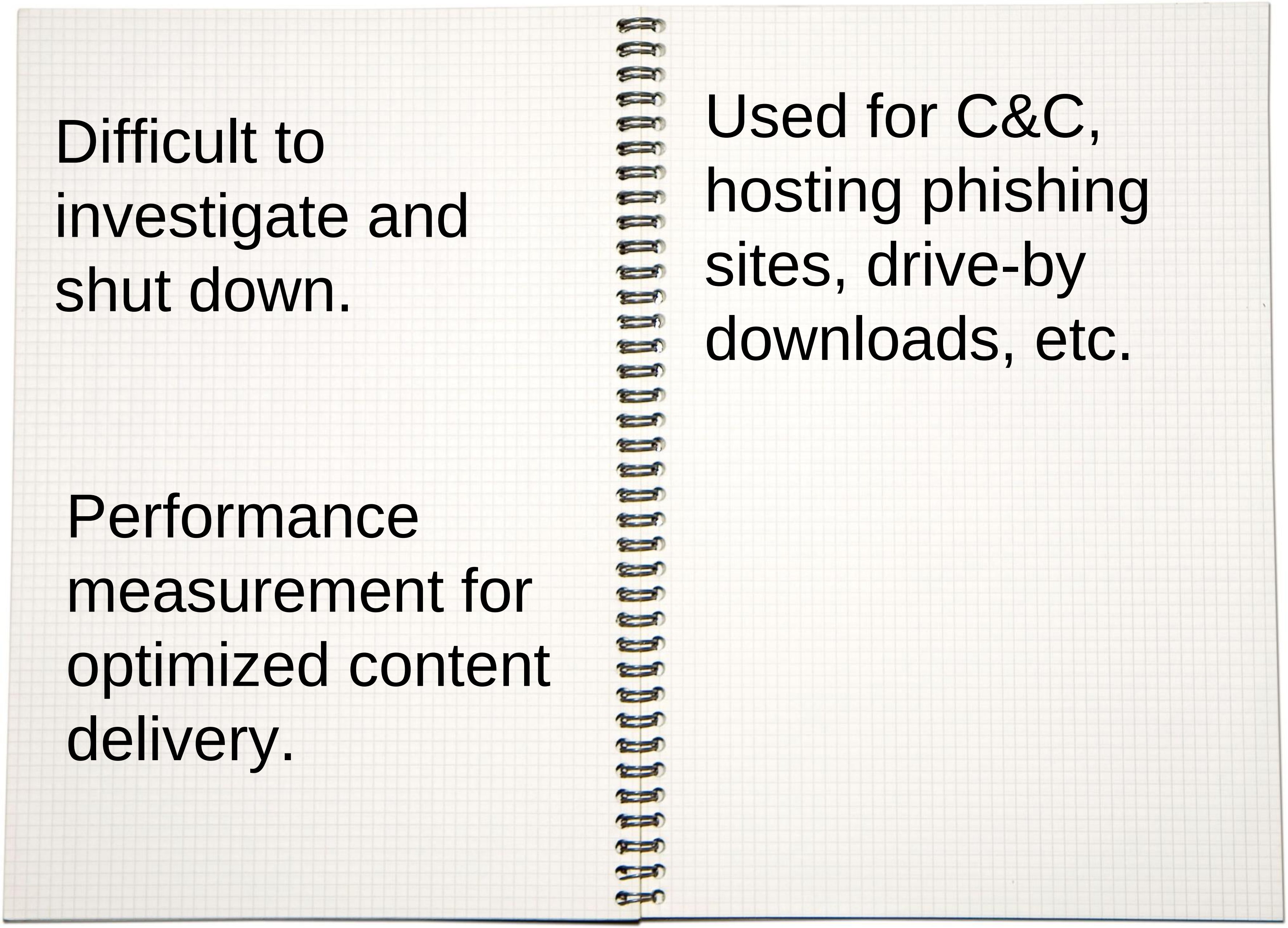


1.8.9.3

4.2.6.3

5.4.8.7

attacker .com



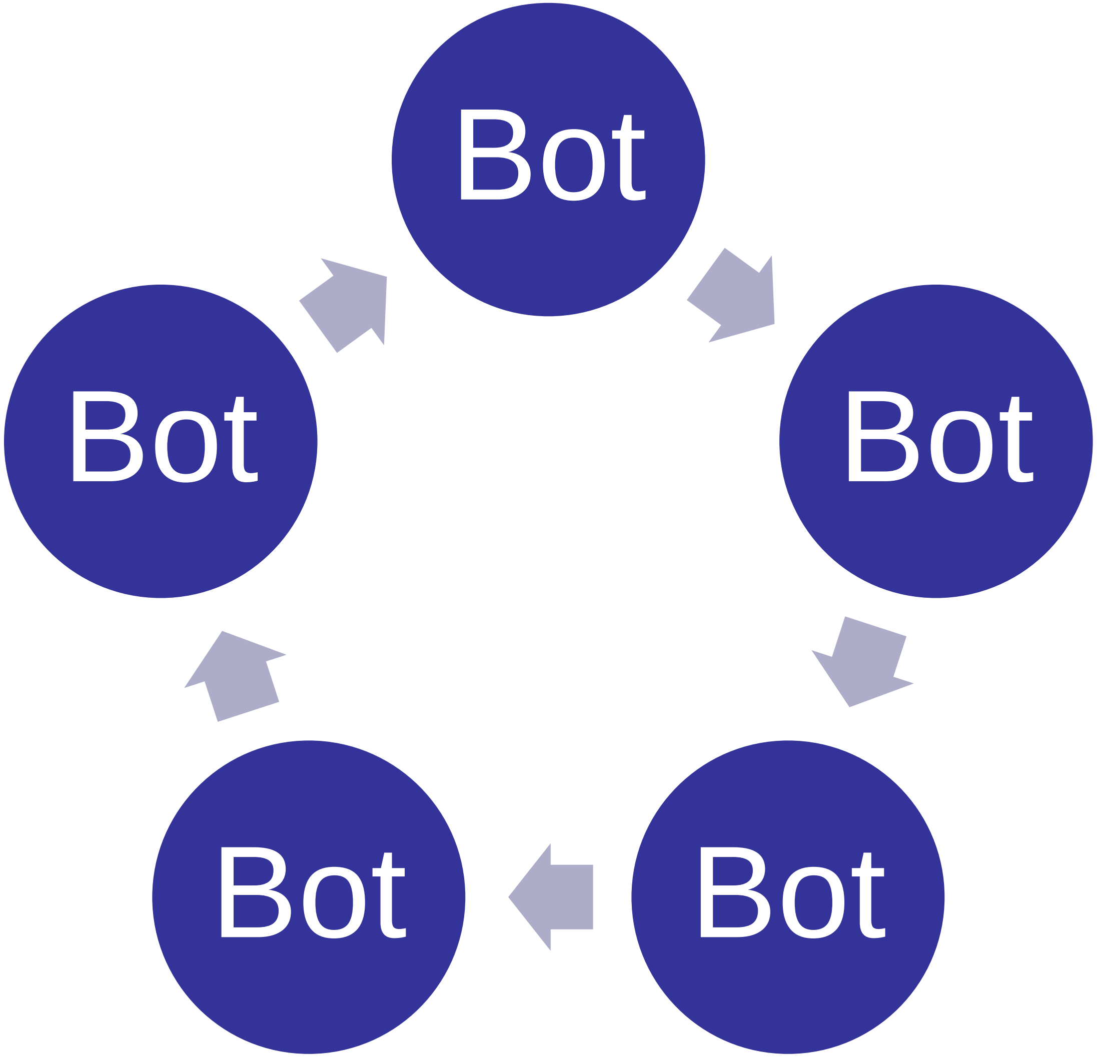
Difficult to investigate and shut down.

Used for C&C, hosting phishing sites, drive-by downloads, etc.

Performance measurement for optimized content delivery.

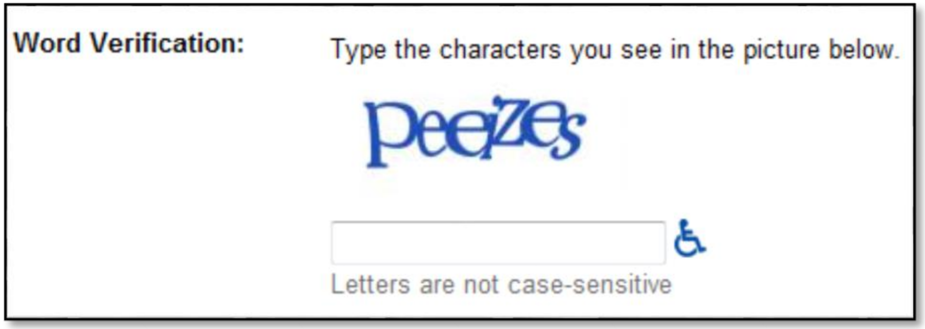
Some bots (e.g. Storm) employ P2P mechanism for C&C.

Shape may change as peers jump in and out (Nugache).



Retransmit to each other, without a central node.

Distributed computing for CAPTCHA breaking via bots.

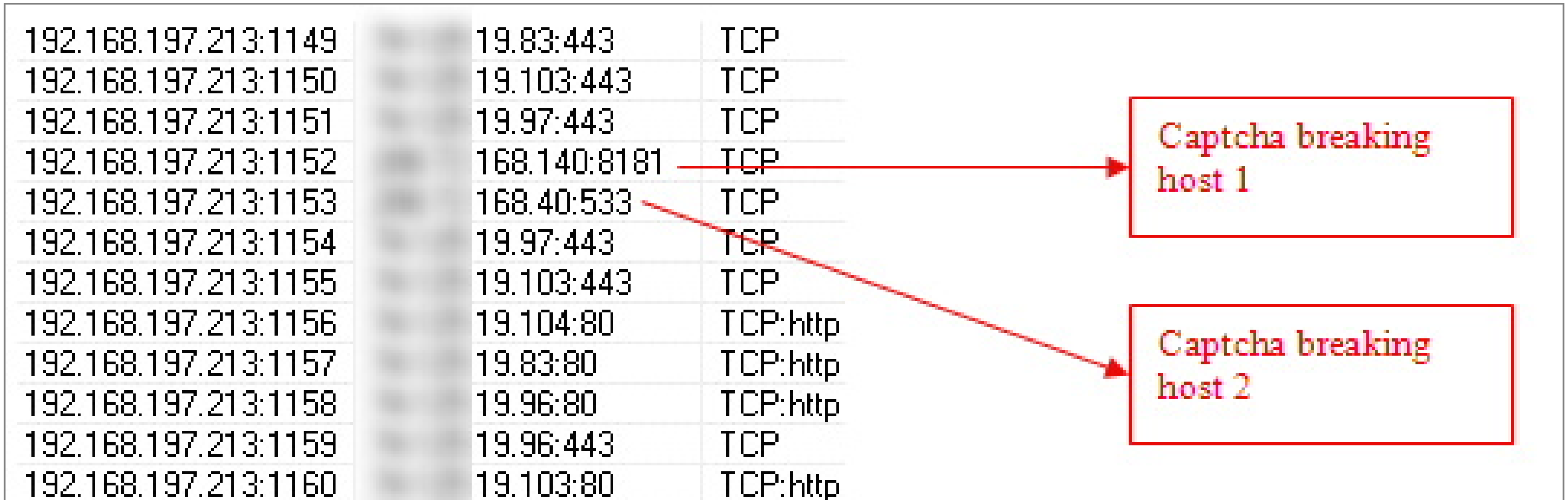


Word Verification:

Type the characters you see in the picture below.

Letters are not case-sensitive

Capture Source: Websense



192.168.197.213:1149	[redacted]	19.83:443	TCP
192.168.197.213:1150	[redacted]	19.103:443	TCP
192.168.197.213:1151	[redacted]	19.97:443	TCP
192.168.197.213:1152	[redacted]	168.140:8181	TCP
192.168.197.213:1153	[redacted]	168.40:533	TCP
192.168.197.213:1154	[redacted]	19.97:443	TCP
192.168.197.213:1155	[redacted]	19.103:443	TCP
192.168.197.213:1156	[redacted]	19.104:80	TCP:http
192.168.197.213:1157	[redacted]	19.83:80	TCP:http
192.168.197.213:1158	[redacted]	19.96:80	TCP:http
192.168.197.213:1159	[redacted]	19.96:443	TCP
192.168.197.213:1160	[redacted]	19.103:80	TCP:http

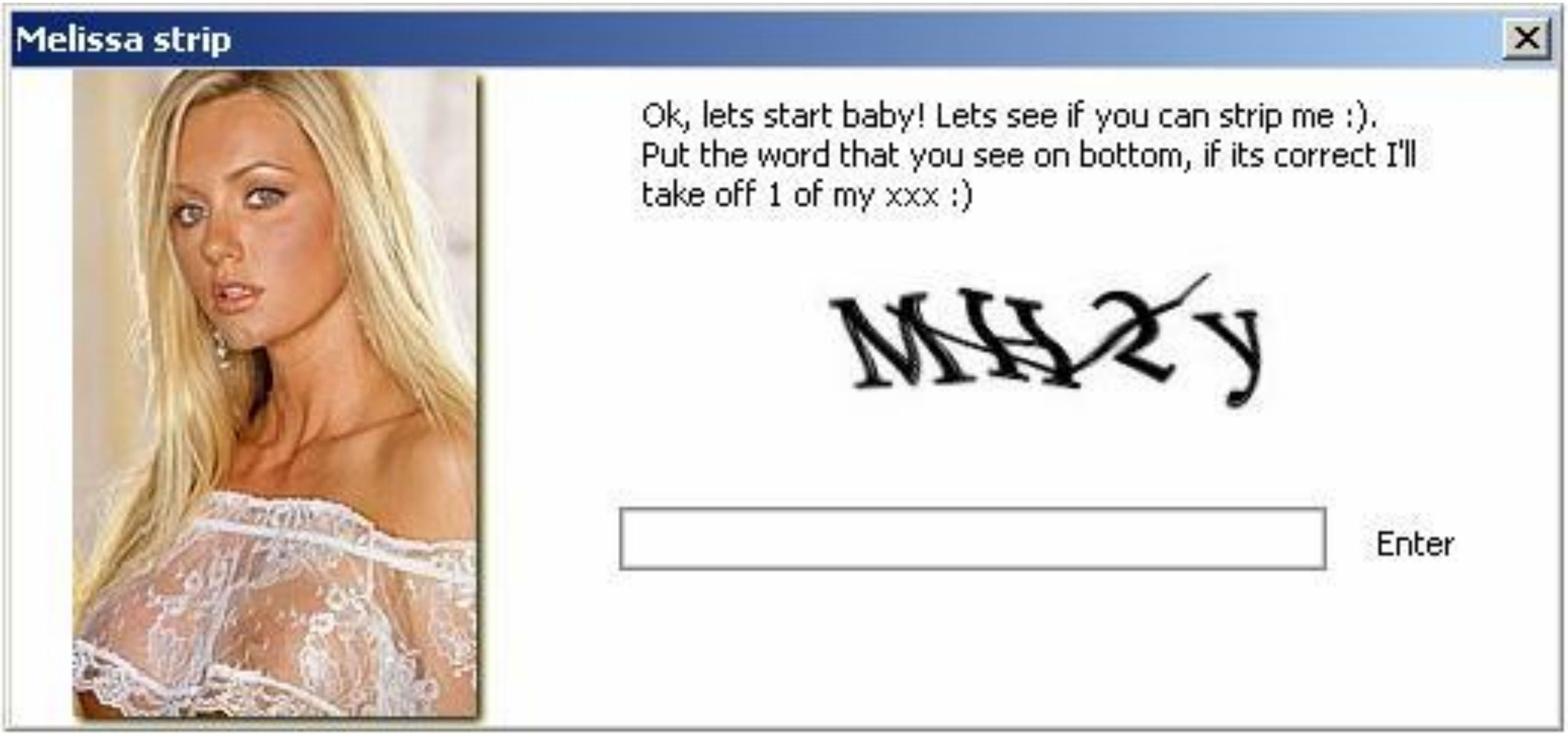
Captcha breaking host 1

Captcha breaking host 2

Human labor supplements the bot network’s efforts.

> “Work for students. Looking for persons to recognize images. Get paid $4 for every 1,000 images recognized. From past experience, it takes about 1 hour to recognize 1,000 pictures, so you could earn $60-70 after a hard day’s work.”

More effective than the stripper method of Trj/RompeCaptchas?

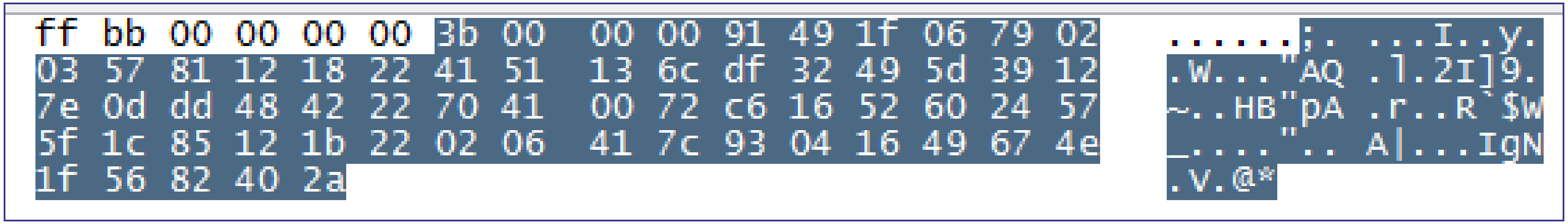


Ok, lets start baby! Lets see if you can strip me :).
Put the word that you see on bottom, if its correct I'll
take off 1 of my xxx :)

Image Source: Security Lab

Self-Defending Characteristics

Communications with attacker are often encrypted.



```
ff bb 00 00 00 00 3b 00  00 00 91 49 1f 06 79 02    ......;. ...I..y.
03 57 81 12 18 22 41 51  13 6c df 32 49 5d 39 12    .W..."AQ .l.2I]9.
7e 0d dd 48 42 22 70 41  00 72 c6 16 52 60 24 57    ~..HB"pA .r..R`$W
5f 1c 85 12 1b 22 02 06  41 7c 93 04 16 49 67 4e    _....".. A|...IgN
1f 56 82 40 2a                                      .V.@*
```

```
0030:4FE38028 3B 00 00 00 32 31 39 33 2E 30 2E 37 35 2E 31 7C ;...2193.0.75.1|
0030:4FE38038 72 65 61 6C 7C 4A 6F 68 6E 20 53 6D 69 74 68 7C real|John Smith|
0030:4FE38048 43 75 72 72 65 6E 74 55 73 65 72 7C 31 2E 31 7C CurrentUser|1.1|
0030:4FE38058 31 32 33 7C 30 7C 30 7C 30 7C 32 36 36 7C 00 00 123|0|0|0|266|..
```

```
0030:4FE38028 3B 00 00 00 91 49 1F 06 79 02 03 57 81 12 1B 22 ;....I..y..W..."
0030:4FE38038 41 51 13 6C DF 32 49 5D 39 12 7E 0D DD 48 42 22 AQ.l.2I]9.~..HB"
0030:4FE38048 70 41 00 72 C6 16 52 60 24 57 5F 1C 85 12 1B 22 pA.r..R`$W_...."
0030:4FE38058 02 06 41 7C 93 04 16 49 67 4E 1F 56 82 40 2A 00 ..A|...IgN.V.@*.
```

Graybird captured keystrokes and local password cache.

Malware can detect the analyst’s toolbox.

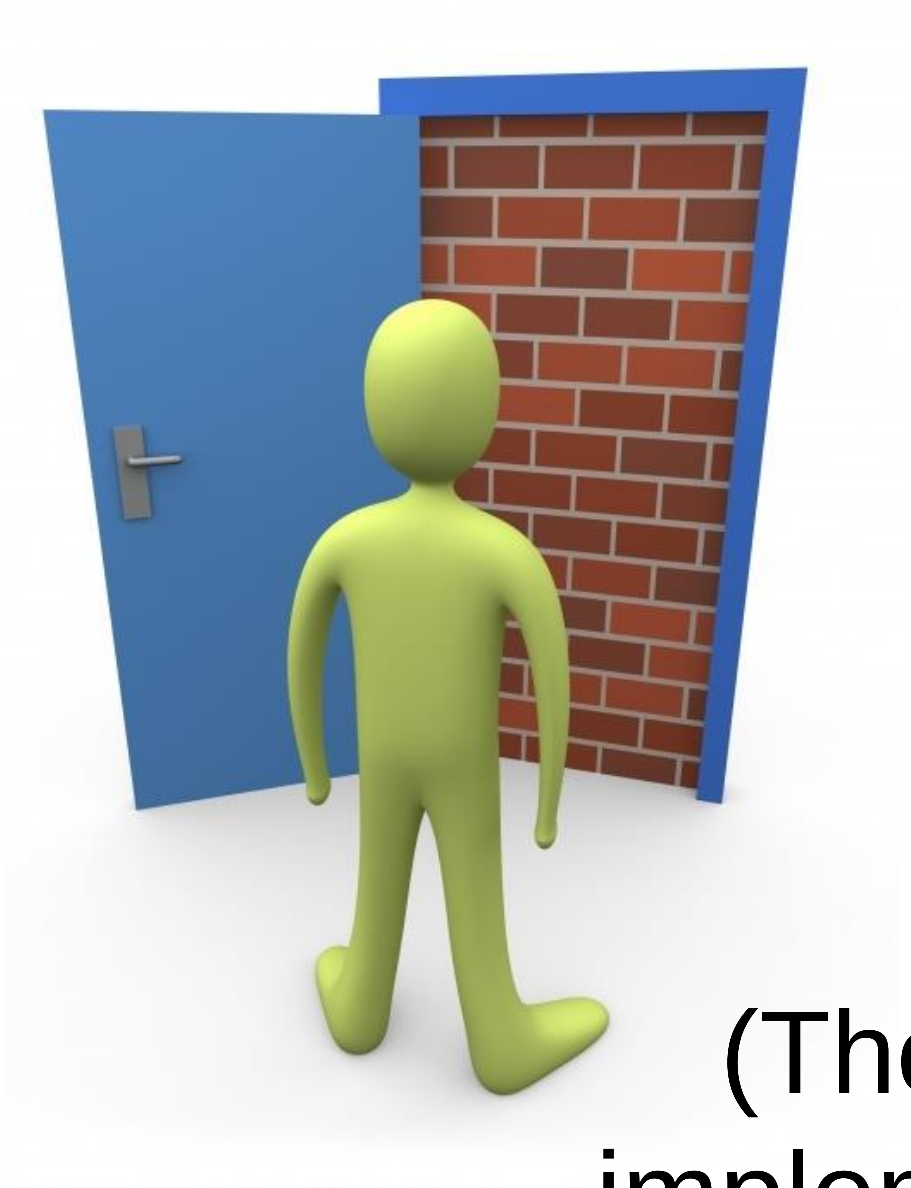
```
if (IsVMWare()) {
  g_pMainCtrl->m_cConsDbg.Log(5,
    "Running inside VMWare, probably honeypot...\n");
  m_bIsDebug=true; return true;
}
```

```
MOV EAX, 564D5868h  ; Magic Number
MOV EBX, COMMAND_SPECIFIC_PARAMETER
MOV ECX, BACKDOOR_COMMAND_NUMBER
MOV DX, 5658h       ; Port Number
IN EAX, DX
```

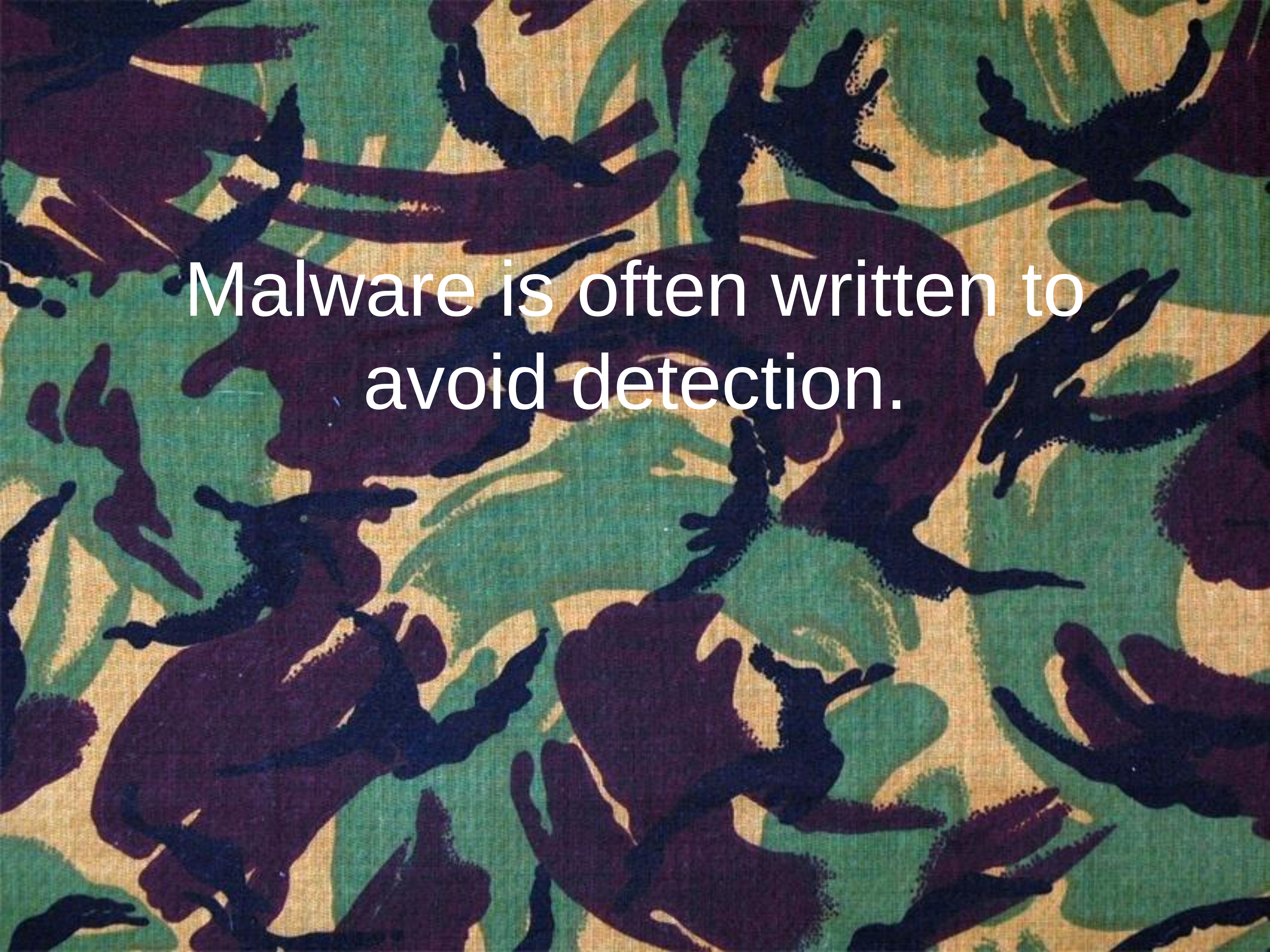
Phatbot detected debuggers by timing its execution.

```
if (IsSICELoaded()) {
  g_pMainCtrl->m_cConsDbg.Log(5,
    "SoftIce is loaded, debugger active...\n");
  m_bIsDebug=true; return true;
}
```

```
if ((GetTickCount()-lStartTime) > 5000) {
  g_pMainCtrl->m_cConsDbg.Log(5,
    "Routine took too long to execute, probably single-step...\n");
  m_bIsDebug=true; return true;
}
```



Some packers (Themida, VMprotect) implement virtualization.



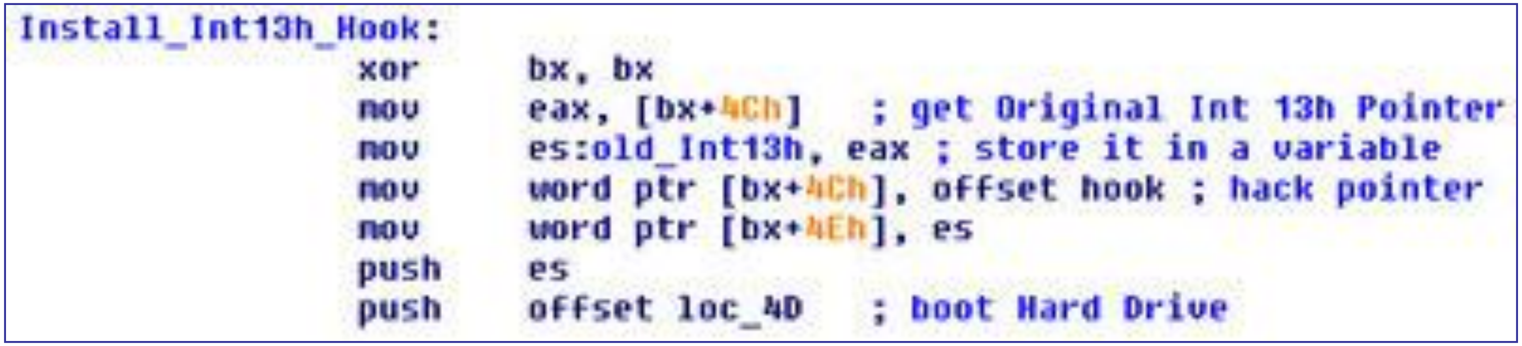
Malware is often written to avoid detection.

AV Killer rendered anti-virus software infective.

```
HKLM\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\Image File Execution
Options\avp.exe
```

Redirected execution via Image File Execution Options (IFEO)

MBR Rootkit hid via hooking and patching drivers in RAM



```
Install_Int13h_Hook:
                xor     bx, bx
                mov     eax, [bx+4Ch]   ; get Original Int 13h Pointer
                mov     es:old_Int13h, eax ; store it in a variable
                mov     word ptr [bx+4Ch], offset hook ; hack pointer
                mov     word ptr [bx+4Eh], es
                push    es
                push    offset loc_4D   ; boot Hard Drive
```

Code Source: PrevX

Pandex/DieHard removed anti-virus software hooks.

Packers assist with polymorphism.

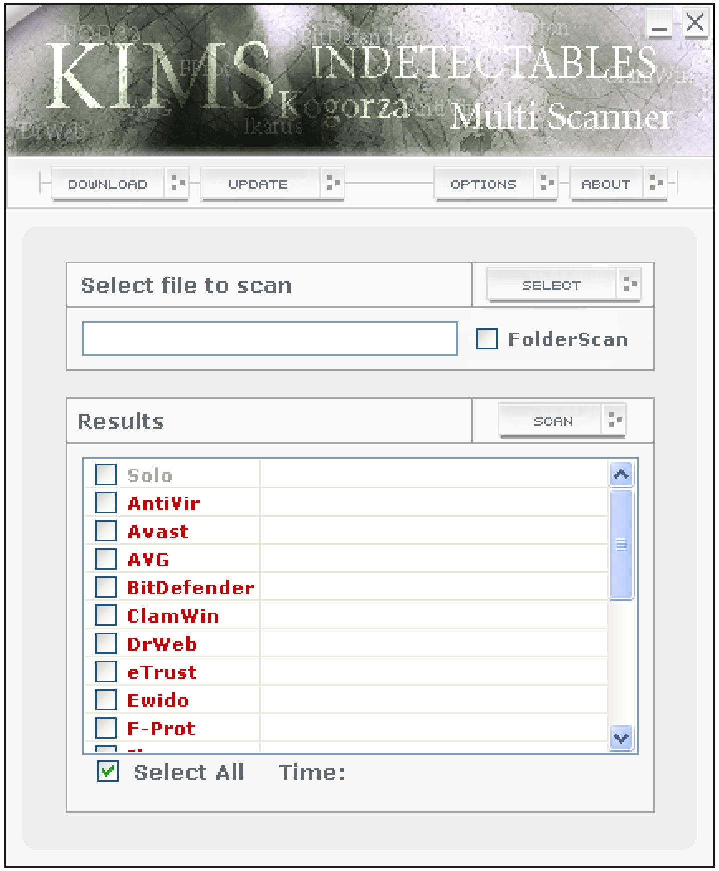
Servers distributing Storm generated varying MD5 files.

Browser scripts employ obfuscation and polymorphism.

```
<script>eval(unescape('function%20ppEwEu%28yJVD%29
%7Bfunction%20xFplcSbG%28mrF%29%7Bvar%20rmO%3DmrF.
length%3Bvar%20wxxwZl%3D0%2CowZtrl%3D0%3Bwhile%28w
xxwZl%3CrmO%29%7BowZtrl+%3DmrF.charCodeAt%28wxxwZl
%29*rmO%3BwxxwZl++%3B%7Dreturn%20%28%27%27+owZtrl%
29%7D%20%20%20try%20%7Bvar%20xdxc%3Deval%28%27a%23
rPgPu%2CmPe%2Cn%2Ct9sP.9ckaPl%2ClPe9e9%27.replace…
```

Also use “arguments.callee” to prevent tampering by analysts.

Authors scan with anti-virus before releasing malware.



Select file to scan

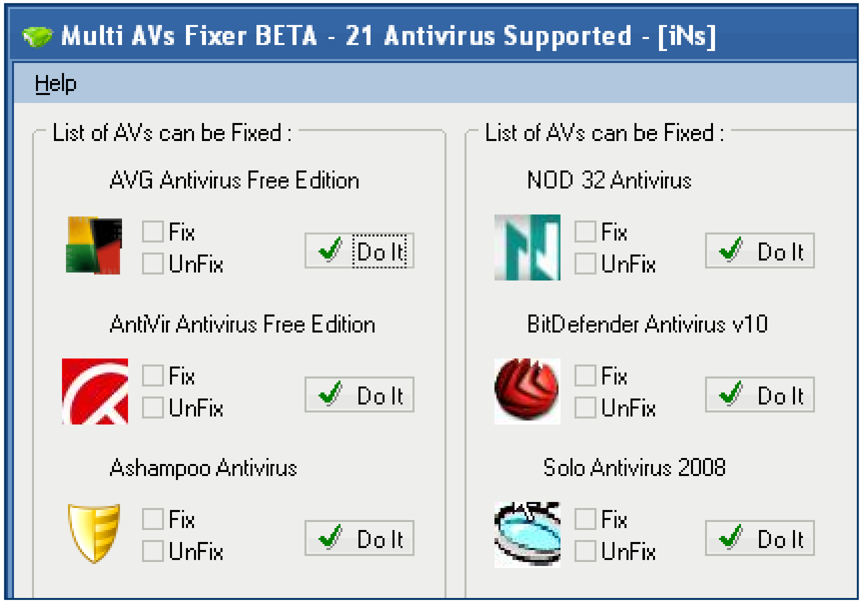
□ FolderScan

Results

□ Solo
□ AntiVir
□ Avast
□ AVG
□ BitDefender
□ ClamWin
□ DrWeb
□ eTrust
□ Ewido
□ F-Prot

☑ Select All   Time:

"So started today this little idea to have all AVs installed in a VMWare without having conflicts with each others"



Multi AVs Fixer BETA - 21 Antivirus Supported - [iNs]

List of AVs can be Fixed :

AVG Antivirus Free Edition

AntiVir Antivirus Free Edition

Ashampoo Antivirus

List of AVs can be Fixed :

NOD 32 Antivirus

BitDefender Antivirus v10

Solo Antivirus 2008

Original Observation by: PandaLabs

Money-Making Characteristics

Spam fuels the malware economy.

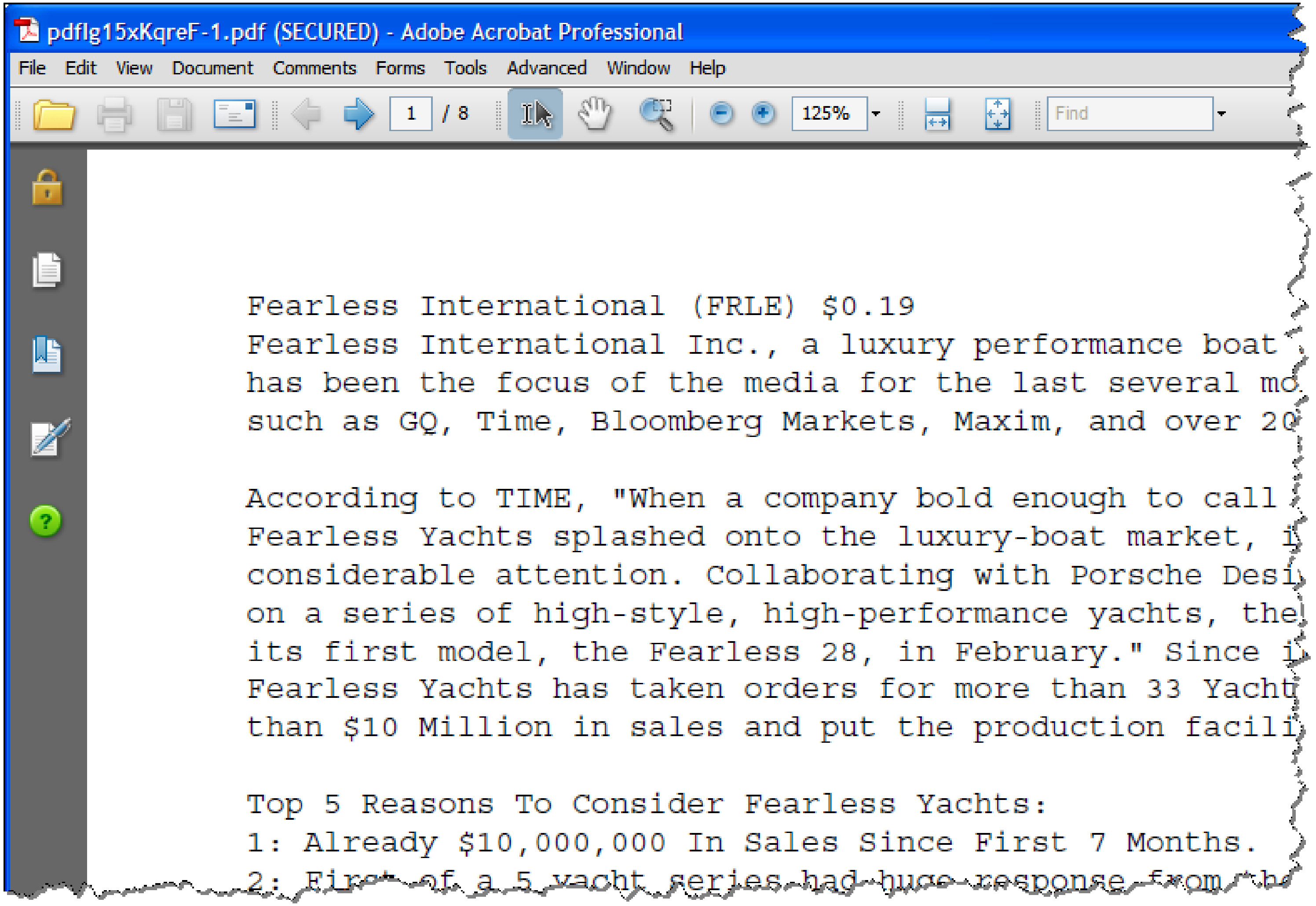
Storm and Kraken relay email through infected systems.

Email brings potential victims to websites for phishing, exploits.

> **Dear MasterCard customer,**
>
> **We regret to inform you that we have received numerous fraudulent emails which ask for personal account information. … Please remember that we will never ask for personal account information via email or web pages…**
>
> **To activate it please call us immediately at (615) 348-6681**

Don’t forget voice phishing.

Drive up the stock price via pump-and-dump techniques.



Fearless International (FRLE) $0.19
Fearless International Inc., a luxury performance boat
has been the focus of the media for the last several mo
such as GQ, Time, Bloomberg Markets, Maxim, and over 20

According to TIME, "When a company bold enough to call
Fearless Yachts splashed onto the luxury-boat market, i
considerable attention. Collaborating with Porsche Desi
on a series of high-style, high-performance yachts, the
its first model, the Fearless 28, in February." Since i
Fearless Yachts has taken orders for more than 33 Yacht
than $10 Million in sales and put the production facili

Top 5 Reasons To Consider Fearless Yachts:
1: Already $10,000,000 In Sales Since First 7 Months.
2: First of a 5 yacht series had huge response from th

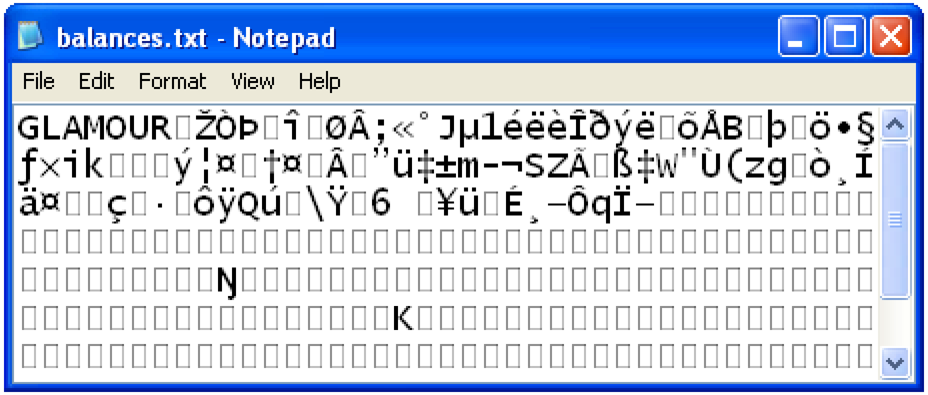
Compromised accounts for trading

Consider spyware at trading firms to anticipate stock movement.

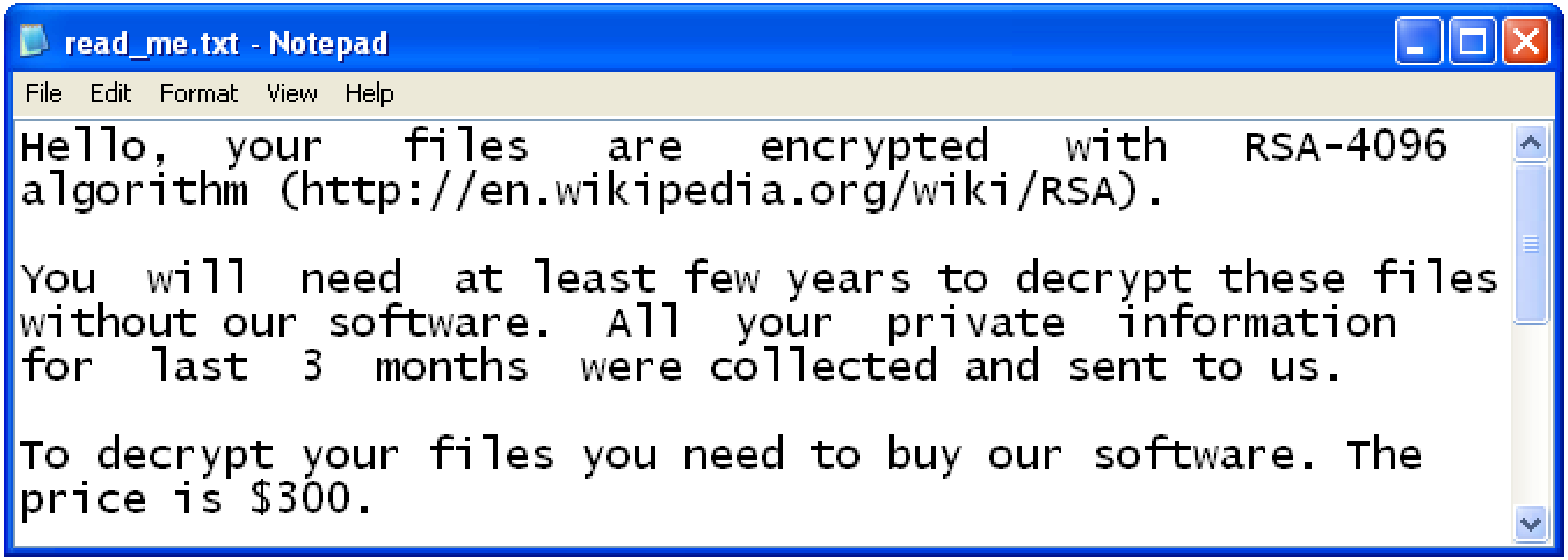
Extortion demands are substantiated by malware.

Cañón del S.XVIII cedido por
la Autoridad Portuaria de
Gijón, utilizado como bolardo
en el Dique de Sta.Catalina
desde 1864 hasta 1987

Gpcoder encrypted local files.



```
GLAMOUR□ŽÒÞ□î□ØÂ;«˚JµléëèÎðýë□õÅB□þ□ö•§
ƒ×ik□□□ý¦¤□†¤□Â□”ü‡±m-¬SZÃ□ß‡W"Ù(zg□ò¸Í
ä¤□□ç□·□ôÿQú□\Ÿ□6 □¥ü□É¸–ÔqÏ–□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□Ŋ□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□K□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
```



Hello, your files are encrypted with RSA-4096 algorithm (http://en.wikipedia.org/wiki/RSA).

You will need at least few years to decrypt these files without our software. All your private information for last 3 months were collected and sent to us.

To decrypt your files you need to buy our software. The price is $300.

Gpcoder originally spread via attachments to email messages.

> “I am writing to you regarding a job. I have a vacancy that is just right for you! The firm ADC Marketing LTD (UK) is opening a division in Moscow, and its leadership have tasked me with filling the corresponding job positions. I will soon be ready to invite you for an interview at a time convenient for you.
> If you are interested in this offer, fill out the enclosed application related to job’s salary.
> Email me the filled-out application.
> Thank you in advance.
>
> Sincerely, Victor Pavlov, HR manager”

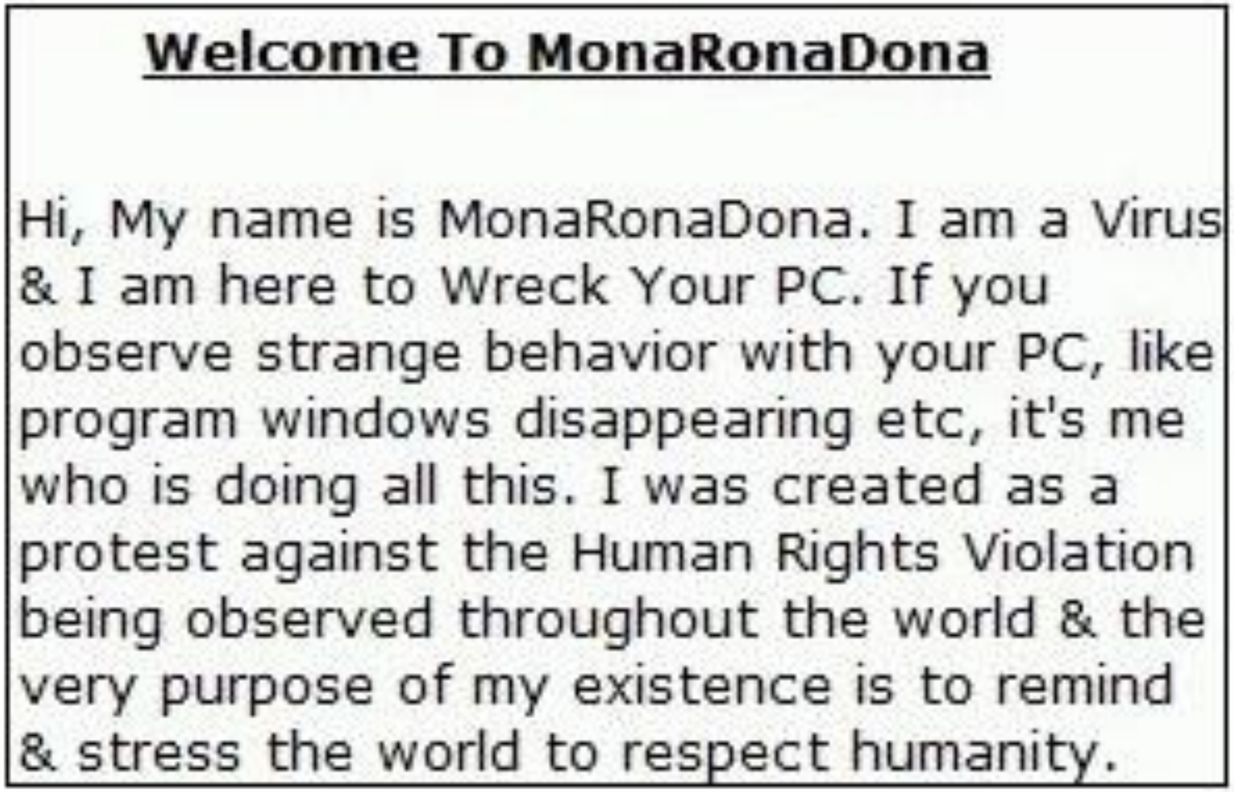
A new and improved version of Gpcoder was released.

Your files are encrypted with RSA-1024 algorithm.
To recovery your files you need to buy our decryptor.
To buy decrypting tool contact us at:
cipher4000@yahoo.com

```
=== BEGIN ===
AD7D6889
0102000016800000A400008EE1630FA688F194
42766F3AE19D5483AAE44C246F66C15F5C6D0E38
0B402EF1B67A0FF10A8A08CADB2DEA19EBD957EF
151ED9365CD730BE54263C3E2FDCEDF8546FF33E
5017032833DCB0C306EA28D79CD6DB4C0E7CE96D
3B84E83EEC84740FED2D64B672148E6F86B06B16
890102FF0D22AE42D3CD4B0F7D7E2AD0A5C0724C
=== END ===
```

Text Source: honeyblog.org

MonaRonaDona wanted the victim to search for a removal tool.



Welcome To MonaRonaDona

Hi, My name is MonaRonaDona. I am a Virus & I am here to Wreck Your PC. If you observe strange behavior with your PC, like program windows disappearing etc, it's me who is doing all this. I was created as a protest against the Human Rights Violation being observed throughout the world & the very purpose of my existence is to remind & stress the world to respect humanity.

Image Source: Washington Post

Botnets may launch DDoS attacks on extortion victims.

Example: A demand placed on a European gambling company (50,000 DNS requests/sec).

Marketplace for stolen data and malware is very healthy.

Goods and Services	Prices
Bank accounts	$10-$1,000
Credit cards	$0.40-$20
Full identities	$1-$15
Email passwords	$4-$30
Proxies	$1.50-$30
Scams	$2.5/week - $50/week for hosting.
Mailers	$1-$10

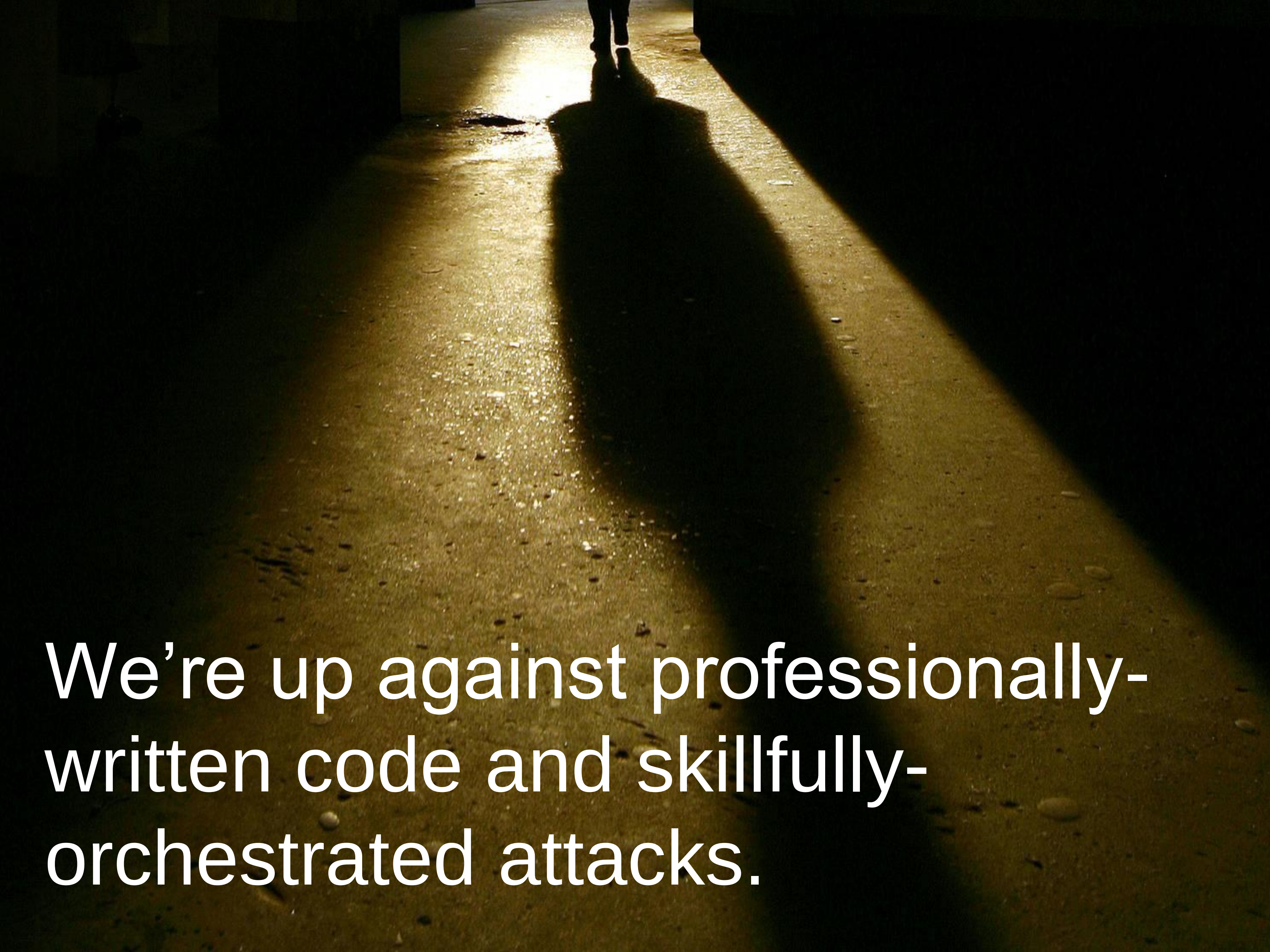
Price Source: Symantec

One could get paid for installing spyware.

Country	Price ($US)
US	$50
UK	$60
Italy	$60
Spain	$25
Asia	$3

Price Source: MessageLabs

Prices per $1,000 downloads.



We’re up against professionally-written code and skillfully-orchestrated attacks.

The defenders need to keep learning and sharing.

Do your defenses account for modern malware characteristics?

Targeted

Distributed

Self-Defending

Money-Making

Lenny Zeltser

www.zeltser.com

lenny.zeltser@savvis.net