



Governments As Malware Authors: The Next Generation

 @mikko

Mikko Hypponen
CRO
F-Secure

A world map with colored outlines (green, red, blue) and a semi-transparent white text box overlaid on the left side. The text box contains a list of governmental uses for malware. At the bottom of the map, there is a block of white text on a black background.

- **Different governmental uses for malware**

- **Law Enforcement**

- **Espionage**

- **Surveillance**

- **Sabotage**

- **Warfare**

STS D: SOVIET NAVAL DEPLOYMENT
T: STRATEGIC NUCLEAR SUBMARINE
CT DPLY REF 3525F: NVOP EF 324
BN DTA AVLB: CH 704 SELECT 612



中华人民共和国国防部

MINISTRY OF NATIONAL DEFENSE OF THE PEOPLE'S REPUBLIC OF CHINA

WWW.MOD.GOV.CN

首页 高层 权威发布 解放军 武警 国防动员 边海防 军校 军工 防务 武器 法规 图片
要闻 军情 新闻发布 预备役 民兵 国防教育 国防生 医院 军史 视点 涉外 专题 视频

国防搜索

全部

搜索

【近万名官兵已进入全部重灾乡镇救灾】 【遇难者人数已上升至407人】 【成都空军派运输机驰灾区】



实战刀锋：解放军年度最大军演背后的改革期待

【高清图】一切为了灾区群众

【一周热点】国防部记者会首度向外国媒体开放

- 习近平：弘扬“两路”精神 助推西藏发展
- 习近平：把救人放在第一位
- 李克强震中现场指挥部署抗震救灾工作
- 国防部回应日本防卫省发表2014版《防卫白皮书》
- 国防部：解放军和武警部队迅速投入云南鲁甸抗震救灾
- 武警黄金部队绘制完成首张震区地质灾害排查评估地图
- 万余官兵继续并肩战斗 数百将校奋战救灾一线
- 总参通知要求认真宣传贯彻军事设施保护法
- “军中焦裕禄”：追忆二炮某基地原司令员杨业功
- 解放军和武警部队迅速投入震灾救援 抢抓“黄金72小时”
- 军中红十字驰援抗震一线 及时救治危重伤员
- 我海军舰艇编队前往美国圣迭戈访问

军委总部领导

>更多

- 习近平：把救人放在第一位
- 习近平对昆山爆炸事故作重要指示
- 习近平向台湾遇难同胞表示哀悼
- 习近平：我临东海情同深
- 习近平八一前看望驻福建部队官兵
- 范长龙许其高对救灾工作提出要求

新闻发布

>更多

国防部长简历

新闻发言人专栏

新闻发布会

国防白皮书

军事外交

军控裁军

国防服务中心

国防部新闻发布 - 国防视频

>更多

权威发布

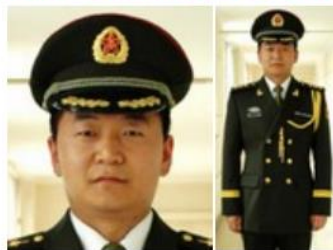
>>更多

WANTED

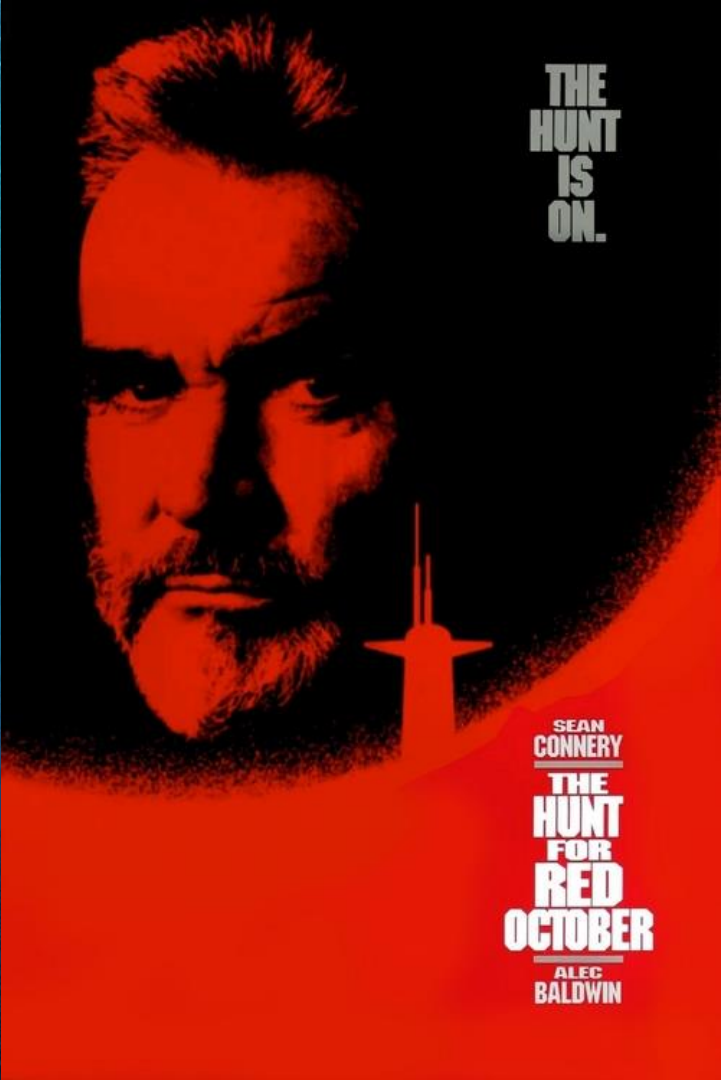
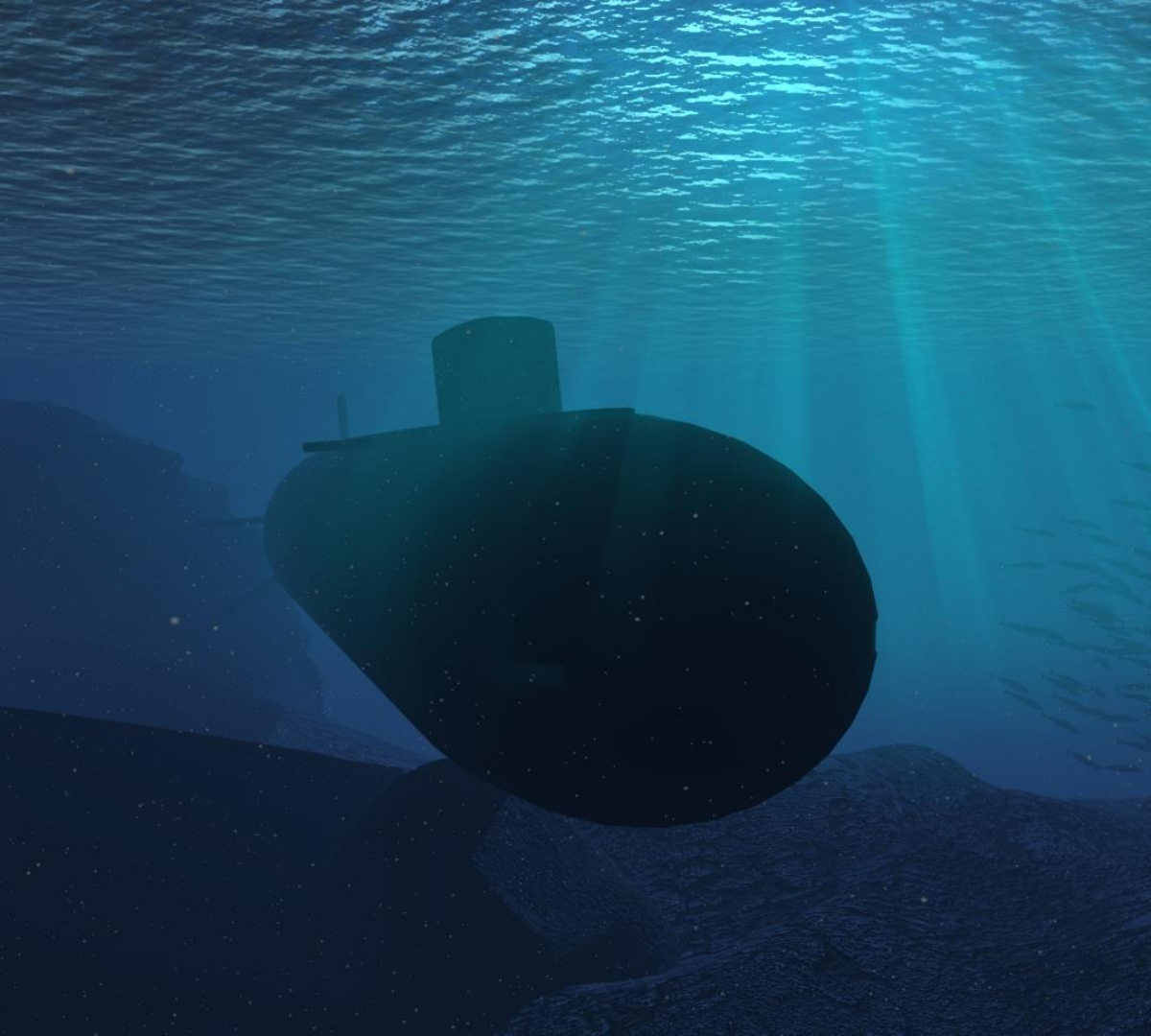
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

SUN KAILIANG



Aliases: Sun Kai Liang, Jack Sun



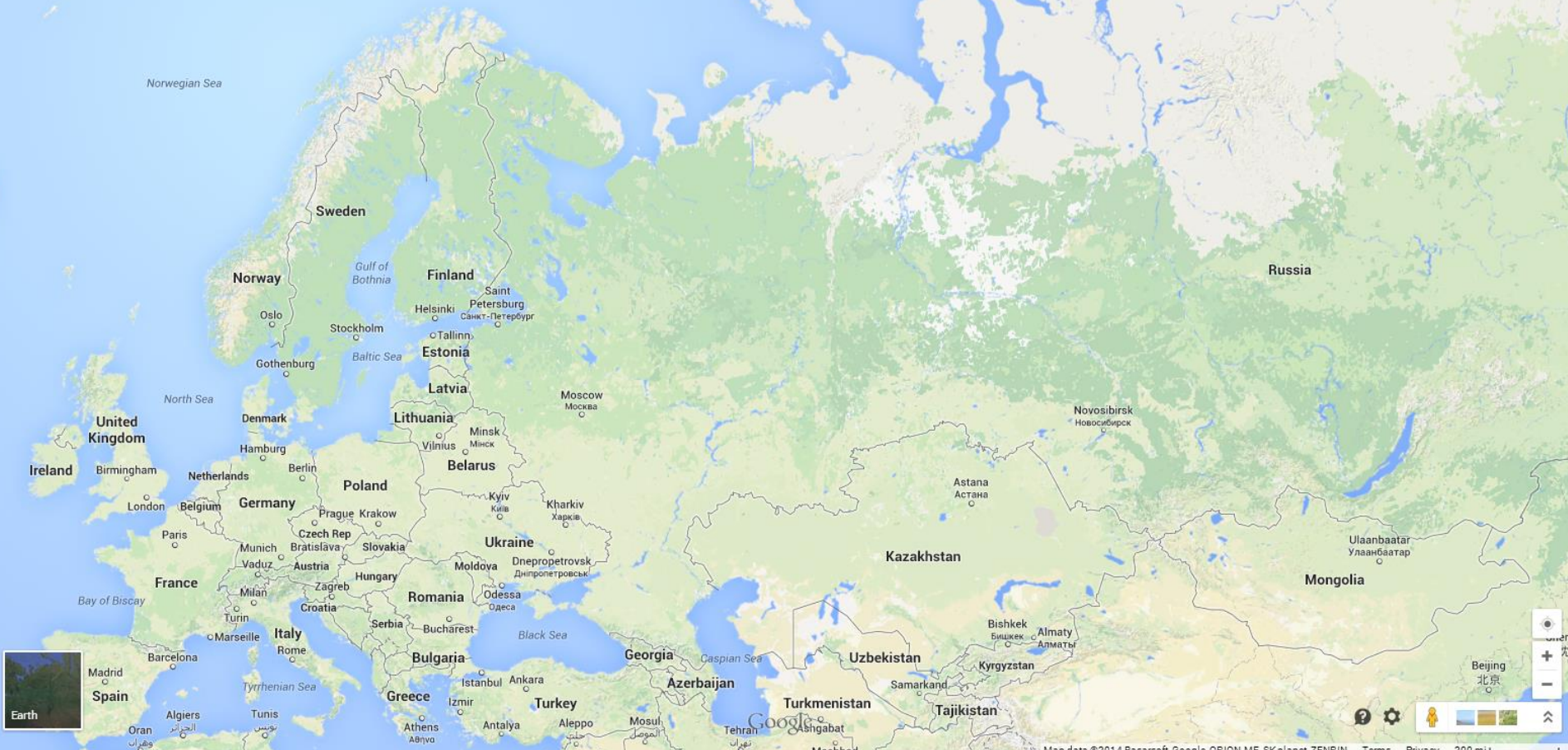
THE
HUNT
IS
ON.

SEAN
CONNERY
THE
HUNT
FOR
RED
OCTOBER
ALEC
BALDWIN

ukraine

Terrain, Directions

CosmicDuke



Masking "file.scr"



file.scr
Screen saver
917 KB



fdp.4102-hcraM-tropeR-ytiruceS-senilepiP-saG-eniarkU.scr



rcs.Ukraine-Gas-Pipelines-Security-Report-March-2014.pdf



rcs.Ukraine-Gas-Pipelines-Security-Report-March-2014.pdf

- rcs.Заказ.doc
- rcs.18.jpg
- rcs.DSC_1365527283.jpg

CosmicDuke remnants

- c:\botgenstudio\generations\8f1777b0\bin\Bot.pdb
- d:\production\nitro\sva\generations\809113dd\bin\Bot.pdb
- d:\sva\nitro\botgenstudio\interface\generations\80ddfcc1\bin\Bot.pdb
- D:\PRODUCTION\NITRO\KSK\Generations\70BCDEA1\bin\Bot.pdb
- C:\Projects\NEMESIS\nemesis-gemina\nemesis\bin\carriers\ezlzma_x86_exe.pdb

MALWARE ANALYSIS

Cosmu with a twist of MiniDuke

TLP: WHITE

CONTENTS

INTRODUCTION	2
Scope	2
Target	2
Arrival	3
Infection	3
Data theft	3
Data transmission	3
TECHNICAL DETAILS	4
Dropper: RLO	4
Dropper: Decoy's	5
Exploit	6
Loader: MiniDuke 3rd Stage	6
Main Component: Info-stealer	7
RC4 Encryption	9
Samples Comparison	9
APPENDIX A SAMPLES	13
APPENDIX B SERVERS	15

In this document we report on our analysis of CosmicDuke - the first malware seen to include code from both the notorious MiniDuke APT trojan and another longstanding threat, the Information-stealing Cosmu Family. When active on an infected machine, CosmicDuke will search for and harvest login details from a range of programs and forward the data to remote servers, some of which were active at the time of writing.

F-SECURE LABS
SECURITY RESPONSE
Whitepaper



F-Secure.

Havex

```
12
MTMxMjMxMg==
5
havex
10800000
12
Explorer.EXE
0
3
47
www.pc-service-fm.de/modules/mod_search/src.php
46
artem.sataev.com/blog/wp-includes/pomo/src.php
48
swissitaly.com/includes/phpmailer/class.pop3.php
354
```

Programm was started at %02i:%02i:%02i
%02i:%02i:%02i.%04i:

Start finging of LAN hosts...
Finding was fault. Unexpective error
Was found %i hosts in LAN:
Hosts was't found.

%02i) [%s]

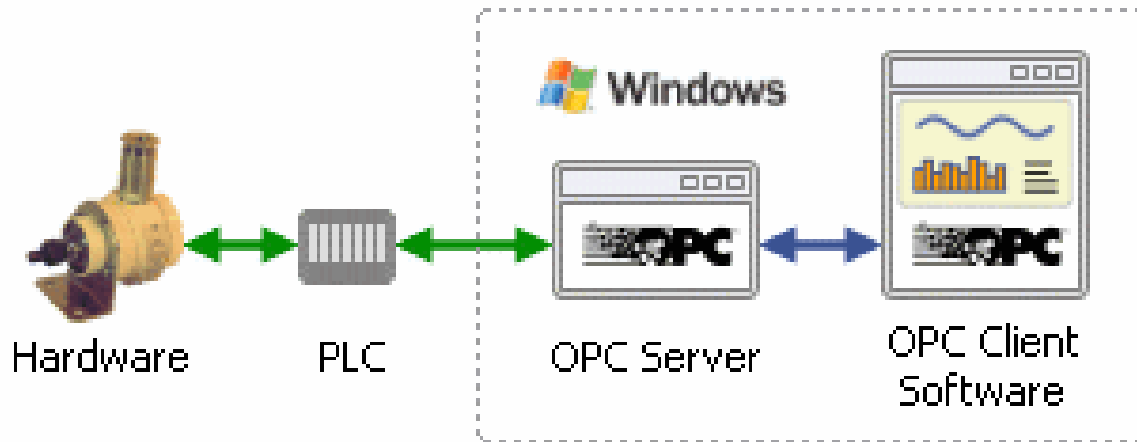
Start finging of OPC Servers...
Was found %i OPC Servers.

%1) [%s\%s]



CLSID: %s
UserType: %s
VerIndProgID: %s
OPC version support: %s

OPC Servers not found. Programm finished



Serial-to-Ethernet Gateway

Industrial Modular M2M
RouterIndustrial Remote Access
Router

eWON COSY 141

eWON 2005CD/4005CD

eWON 2101CD/4101CD

eWON 2104/4104

eWON Flexy 200

WiFi Extension (Flexy)

PSTN Extension (Flexy)

Talk2M

VPN appliance

Companion tools

Find a product

Find an eWON product



Contact us

Industrial Routers, Industrial Wireless Router, VPN Routers

Industrial Remote Access Router

A key strategy for many machine OEMs involves building solid, long-term relationships with their customers by providing dependable, superior after-sales support. They have come to realize the value that remote machine support provides to their customers, as well as to themselves.



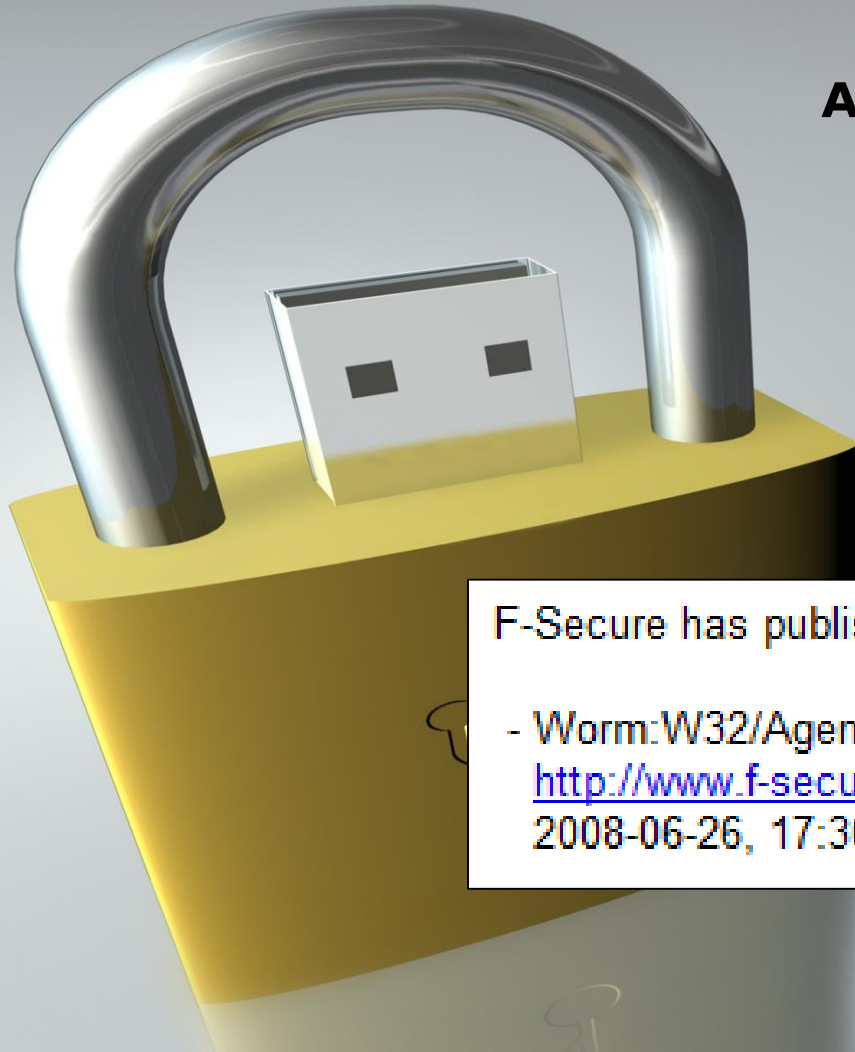
eWON COSY 141
Industrial VPN Router



eWON 2005CD/4005CD
Industrial LAN Router



Agent.BTZ / Turla / Snake / Uroburos



F-Secure has published a new description:

- Worm:W32/Agent.BTZ - Low (1)

http://www.f-secure.com/v-descs/worm_w32_agent_btz.shtml

2008-06-26, 17:30:41

Agent.BTZ

```
[S] .data:10016... 0000000A C Log end.\n[S] .data:10016... 00000010 C %02d:%02d:%02d\n[S] .data:10016... 0000001F C Error in sprintf copy bytes.\n[S] .data:10016... 0000001F C Log: Error(%d) get file size.\n[S] .data:10016... 0000002F C Log: Size of log(%dB) is too big, stop write.\n[S] .data:10016... 0000002A C Size of log(%dB) is too big, stop write.\n[S] .data:10016... 00000018 C %s\\system32\\winview.ocx\n[S] .data:10016... 0000001B C %02d.%02d.%04d Log begin:\n[S] .data:10016... 00000009 C %system%\n[S] .data:10016... 0000000A C %windows%\n[S] .data:10016... 0000000C C %s\\system32
```

Turla

```
[S] .rdata:0041... 0000000A C Log end.\n[S] .rdata:0041... 00000016 C %s\\system32\\vtmon.bin\n[S] .rdata:0041... 0000001A C Exception CEncLog::Open.\n[S] .rdata:0041... 0000001B C %02d.%02d.%04d Log begin:\n[S] .rdata:0041... 00000032 C Buffer is too big(%dB), LogSize(%dB), Limit(%dB)\n[S] .rdata:0041... 00000010 C %02d:%02d:%02d\n[S] .rdata:0041... 00000015 C %02d:%02d:%02d %04x\n[S] .rdata:0041... 00000021 C Error in sprintf, max %d bytes.\n[S] .rdata:0041... 00000011 C assistant_helper\n[S] .rdata:0041... 0000000A C assistant\n[S] .rdata:0041... 0000001F C Log: Error(%d) get file size.\n[S] .rdata:0041... 0000002F C Log: Size of log(%dB) is too big, stop write.\n[S] .rdata:0041... 0000002A C Size of log(%dB) is too big, stop write.
```


Developer Signatures

\$Id: event.c 14097 2010-11-01 14:46:27Z **gilg** \$

\$Id: mime64.c 12892 2010-06-24 14:31:59Z **vlad** \$

\$Id: named_mutex.c 15594 2011-03-18 08:04:09Z gilg \$

\$Id: nt.c 20719 2012-12-05 12:31:20Z gilg \$

\$Id: ntsystem.c 19662 2012-07-09 13:17:17Z gilg \$

\$Id: snake_config.c 5204 **2007-01-04** 10:28:19Z vlad \$



ATIC ET 2005

S7-400
7-3
443-1 adv.

جنگ سایبری

نگاه به مهمترین حملات سایبری در جهان



White hat hackers

هکرهاى کلاه سفید یا هکر خوب، متخصصین شبکه هستند که جالهای امنیتی شبکه را پیدا می کنند



Black hat hackers

هکرهاى کلاه سیاه اشخاصی هستند که با وارد شدن به شبکه و دستبرد اطلاعات یا جاسوسی کردن، سوءاستفاده می کنند



Gray hat hackers

هکرهاى کلاه خاکستری حد وسط دو تعریف بالا می باشند



Pink hat hackers

هکرهاى کلاه صورتی افراد کم سوادی هستند که با چند نرم افزار خرابکارانه به آزار و اذیت دیگران می پردازند

Interception یا شنود
در این روش نفوذگر به شکل مخفیانه از اطلاعات نسخه برداری می کند.

Modification یا تغییر اطلاعات
در این روش نفوذگر به دستکاری و تغییر اطلاعات می پردازد.

Fabrication یا افزودن اطلاعات
در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می کند.

Interruption یا وقفه
در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می شود.

نام حمله، STUXNET
تاریخ، ۲۰۰۹ - ۲۰۱۰
هدف، سیستم های صنعتی
آسیب، ویروسی شدن چند رایانه، اختلال در فعالیت
نیروگاه هسته ای

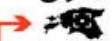


●●●●●
★★★★★

رژیم
صهیونیستی

گرجستان

استونی



علت، جنگ اوستیای جنوبی
تاریخ، ۲۰۰۸ - ۲۰۰۸
آسیب، وب سایت دولت گرجستان
برای چندین ساعت غیر فعال شد

●●●●●
★★★★★

یابود جنگ شوروی، علت
و انتخاب تالین به عنوان پایتخت
تاریخ، ۲۰۰۷ - ۲۰۰۷
وب سایت دولت بانک ها و روزنامه ها، آسیب
برای چندین ساعت غیر فعال شد

●●●●●
★★★★★



روسیه

حمایت دولتی
دور از ذهن
پدید
پذیرفتنی
محتفل
قطعی

نوانمندی
کم
متوسط
زیاد



نام حمله، AURORA
تاریخ، ۲۰۰۹
فعالان حقوق بشر چینی، هدف
پایگاه فناوری مستقر در آمریکا
سرقت رمز عبور کاربران گوگل، آسیب
به خطر افتادن ایمیل فعالان

●●●●●
★★★★★

نام حمله، BYZANTINE CANDOR
تاریخ، ۲۰۰۲ - ۲۰۰۲
هدف، نیروی های نظامی و سازمان های
دولتی آمریکا
آسیب، سرقت بخش زیادی از اطلاعات حساس

●●●●●
★★★★★



نام حمله، GHOSTNET
تاریخ، ۲۰۰۷ - ۲۰۰۹
سفارتخانه های بسیاری از
کشور ها نظیر آمریکا، هدف
دفتر تبعیدیان تبت
نامعلوم، نفوذ به رایانه کاربران، آسیب

●●●●●
★★★★★

نام حمله، Shadow in the cloud
تاریخ، ۲۰۰۹ - ۲۰۱۰
هدف، دفاتر دولتی هند و تبت،
دفتر سازمان ملل
آسیب، تبعیدیان تبت و مکاتبات
محرمانه دولت هند به خطر افتاد

●●●●●
★★★★★



چین



نام حمله، WIKILEAKS TAKE DOWN
تاریخ، ۲۰۱۰
علت، انتشار اسناد محرمانه
آسیب، قطعی مکرر سایت
غیر فعال کردن دامنه سایت





To Kill a Centrifuge

A Technical Analysis of
What Stuxnet's Creators
Tried to Achieve

Ralph Langner

November 2013



The control units in the pictures above display process pressure and setpoints. The picture below shows the same product (MKS PR-4000) as advertised on the Internet for sale (fergutec.com).



The pressure controllers must be compromised in order to disable the Cascade Protection System's stage exhaust valves. This suggests a link between the Cascade Protection System's main controller, the Siemens S7-417, to the pressure controllers. Since the PR-4000 doesn't come with a built-in PROFIBUS interface, communication is most likely established via a PROFIBUS-to-serial gateway, as shown in the diagram below; a configuration that is used in similar

applications. From the attack code it can be inferred that a total of 21 pressure controllers were used per cascade, with the lower 15 controlling stage exhaust valves.



"There was also some music playing randomly on several of the workstations during the middle of the night with the volume maxed out. I believe it was the **american band acdc thunderstruck**. It was all very strange and happened very quickly. the attackers also managed to gain root access to the machine they entered from and removed all the logs."

Gauss encryption

```
mov     ecx, (LENGTHOF tToCrypt)-1
mov     edx, OFFSET tToCrypt
mov     ebx, OFFSET tEncrypt
L1:
```

```
XOR     eax, ACDC
```

```
mov     [ebx], eax
inc     edx

inc     EBX
```

LOOP L1

```
mov     edx, OFFSET tOutEncr
call    WriteString
mov     edx, OFFSET tEncrypt
call    WriteString
call    Crlf
ret
```




Crypto breakthrough shows Flame was designed by world-class scientists

The spy malware achieved an attack unlike any cryptographers have seen before.

by Dan Goodin - June 7 2012, 2:20pm EDT

BLACK HAT

NATIONAL SECURITY

161



Mikko Hypponen

@mikko

I've now been accused of helping al-Qaeda, because our antivirus blocks malware created by the US Government.

[↩ Reply](#) [🗑 Delete](#) [★ Favorite](#) [⋮](#)

8:22 PM - 1 Jun 2012 · ⚙

RETWEETS

280

FAVORITES

39



N.Korea doubles cyber war personnel

JULY 6, 2014

SEOUL, July 6 — North Korea has doubled the number of its elite cyber warriors over the past two years and established overseas bases for hacking attacks, a report said today.

The North's cyber war unit now has 5,900 personnel, compared with 3,000 two years ago, the South's Yonhap news agency said.







"The communist country operates a hacking unit under its General Bureau of Reconnaissance, which is home to some 1,200 professional hackers," a military source was quoted as saying.

FinFly

Usage Example 2: Intelligence Agency

The customer deployed **FinFly ISP** within the main Internet **Service Provider** of their country. It was **combined with FinFly Web** to remotely **infect Targets that visited government offensive websites** by covertly injecting the FinFly Web code into the targeted websites.

2 SUPPORTED PLATFORMS

	Platform	Supported Version	Latest Version on the Market
	Android	2.x.x, 3.x.x, 4.0.x, 4.1.x, 4.2.x, 4.4.x	4.4.x
	Blackberry	5.x, 6.x, 7.x	10.1
	iOS Untethered Jailbreak required	4.3.x, 5.x, 6.x, 7.0.x	7.1
	Symbian	Symbian ^3, Anna, Belle, S60 v5.x v3.x	Symbian ^3 Anna, Belle
	Windows Mobile	6.1, 6.5	6.5
	Windows Phone	Not Supported Yet	8

UAE, Bahrain, Saudi Arabia, Syria...

- Finfisher (Gamma)
- RCS (Hacking Team)
- DarkComet
- BlackShades
- Xtreme RAT
- Spynet

From: Melissa Chan <melissa.aljazeera@gmail.com>

Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights
Bahrain reports of torture on Mr. Nabeel Rajab after his recent
arrest.

Please check the attached detailed report along with torture
images.


 1 attachment: Rajab.rar 1.4 MB

Image Source: When Governments Hack Opponents: A Look at Actors and Technology, Citizen Lab + ICSI

BlackShades

PROFESSIONAL COMPUTER SURVEILLANCE

[Home Page](#)[Home](#)[Products](#)[Product info](#)[Login](#)[Members Area](#)[Register](#)[Join now!](#)[Forums](#)[Forums](#)[VPN](#)[Safe Internet](#)

Blackshades - Home
News and Events



BlackShades RADAR

- ▶ Advanced key recording for perfect surveillance every time.
- ▶ Target exactly what you need with unique keyword filtering. Websites, games, chats and more are within your grasp.

[Special Package](#)

May 10th, 2:25 AM

Special Package

Blackshades Team is proud to present our special package with a combin...

May 10th, 2:25 AM

[Read More »](#)

[NEW] VPN Accounts

New update,
All VPN have once again been temporarily disabled.
Pleas...

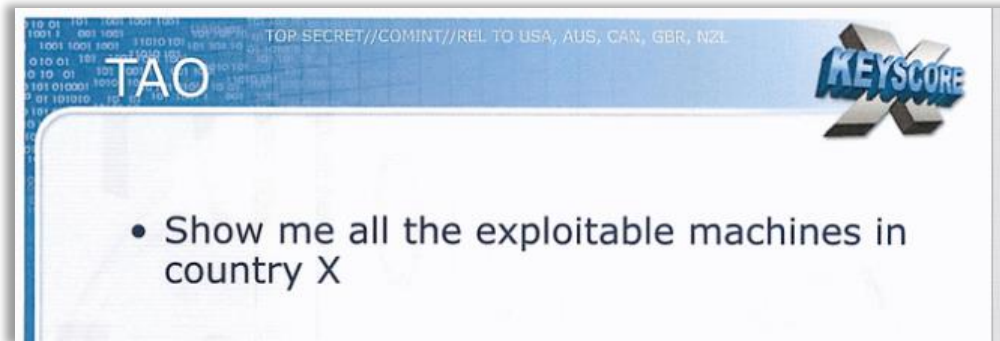
May 2nd, 11:07 PM

[Read More »](#)

VPN Accounts

We've temporarily locked all VPN accounts.
In order to unlock your ac...

Hacker Units inside UKUSA intelligence agencies



JTRIG



THE EYES



- **FIVE EYES:** USA, UK, Canada, Australia, New Zealand
- **NINE EYES:** Five Eyes + Denmark, Norway, The Netherlands and France
- **FOURTEEN EYES:** Nine Eyes + Sweden, Germany, Belgium, Italy and Spain



FREE Peter Sunde



Geneva Convention

"Legitimate military targets are limited to those objects which by their nature make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage"



Thank You

Please fill your feedback form if you have nice things to say. Otherwise, never mind.