



# **WATERING-HOLES**

**PRESENTED BY ARRON FINNON**

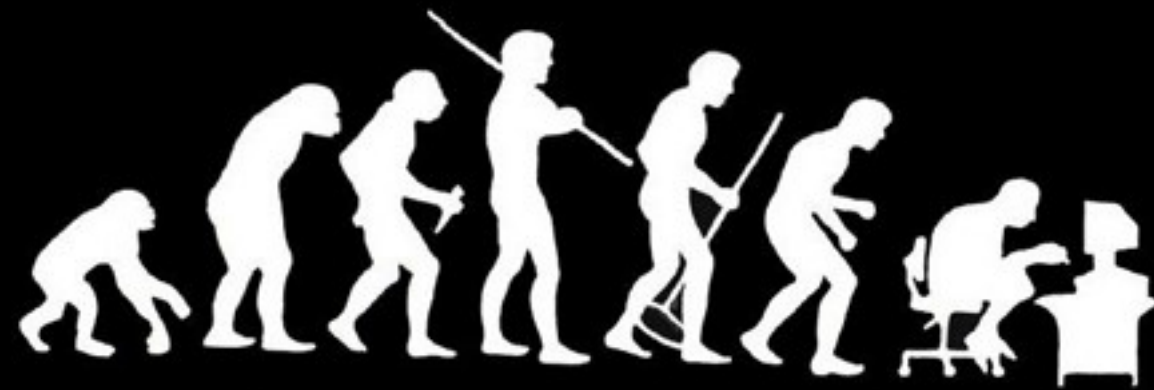




**SO WHO IS FINUX?**



**YOU AIN'T LISTENING**





**SO WHAT IS A HACKER?**





**THIS IS HOW THE MEDIA USED TO SEE HACKERS**





**THEN THEY SAW HACKERS LIKE THIS**



**THEN THIS HAPPENED!**

A person wearing a black hoodie is crouching in a dark room, illuminated by a red light. The person's face is obscured by a black mask. In the foreground, a red binder with two punch holes is visible. The background is dark and indistinct.

**HOW BUSINESSES HAVE ALWAYS SEEN HACKERS**



**BUT THESE ARE JUST STEREOTYPES!**

**WE ALL KNOW WHAT HACKERS LOOK LIKE  
TODAY!**



**DELETE.DELETE.DELETE**





**ALWAYS LISTENING TO YOUR CUSTOMERS**



**CYBERZ NOM.NOM.NOM**





**AND DON'T FORGET THE  
MEDIA AGAIN!**





**CYBERWEAPONS**

# *Cyberwar*







**ANONYMOUS**

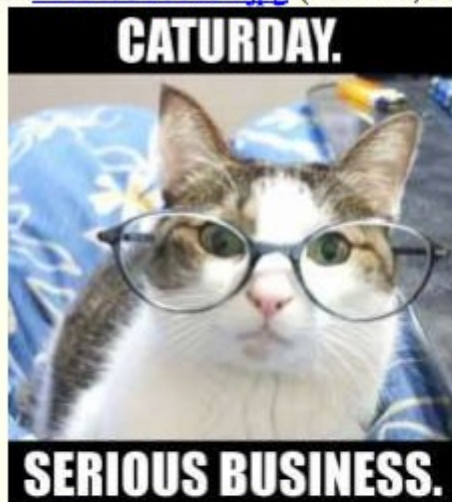




**POOL'S CLOSED**



File : [1165699268254.jpg](#)-(163 KB, 567x630, 1165657948445.jpg)



☐ [Anonymous](#) 12/09/06(Sat)16:21:08 No.17033053

It's Caturday!

>> ☐ [Anonymous](#) 12/09/06(Sat)16:21:54 No.17033084

File : [1165699314228.jpg](#)-(61 KB, 640x480, muffinz ploz.jpg)



[>>17033053](#)

>> ☐ [Anonymous](#) 12/09/06(Sat)16:23:30 No.17033154

File : [1165699410578.jpg](#)-(91 KB, 444x617, car\_bearcat\_awakened.jpg)







**OPERATION CHANOLOGY**



**Lee Hutchinson** ✓

@Lee\_Ars

 Follow

The hacker known as 4Chan better watch out. CNN's crack investigative team is googling as hard as they can to uncover his identity.

3:55 PM - 2 Sep 2014

109 RETWEETS 106 FAVORITES



**DON'T FORGET; 'IF YOU HAVE NOTHING TO HIDE YOU  
HAVE NOTHING TO FEAR', RIGHT?**











A photograph of a man with long brown hair tied in a ponytail, wearing glasses and a black shirt, sitting at a long wooden table in a conference room. He is looking towards the right. On the table in front of him are several items: a clear glass bottle of water, a small green bottle, a dark bottle, a glass of orange juice, and some papers. Other people are seated at tables in the background, some looking towards the camera and others looking away. The text "SO, WHAT TYPE OF HACKER AM I?" is overlaid in white, bold, sans-serif font on the left side of the image.

**SO, WHAT TYPE OF HACKER AM I?**





**THAT'S RIGHT, I'M A WHITE-HAT**



**SO, WATERING-HOLES? WHAT ABOUT THEM**





**EVERYONE LIKES TO GO VISIT THE  
WATERING-HOLE**



A close-up photograph of an elephant and a crocodile in a body of water. The elephant's trunk is extended towards the crocodile's open mouth, which is filled with sharp teeth. The background is a muddy, brownish-yellow shore. A semi-transparent blue banner with white text is overlaid across the middle of the image.

**BUT THEY CAN BE DANGEROUS PLACES**





**VERY DANGEROUS PLACES**





**THE WEB HAS A LOT OF  
WATERING-HOLES TOO**





# http://www

**NO GREAT HACKING STORY STARTS  
WITHOUT SOMEONE CLICKING  
SOMETHING**





## LOTS OF OPPORTUNITIES

```
window.open(theURL,winName,"width=600px,height=400px");
```

```
</script>
```

```
<SCRIPT language=JavaScript>
```

```
var img_preload = new Array;
```

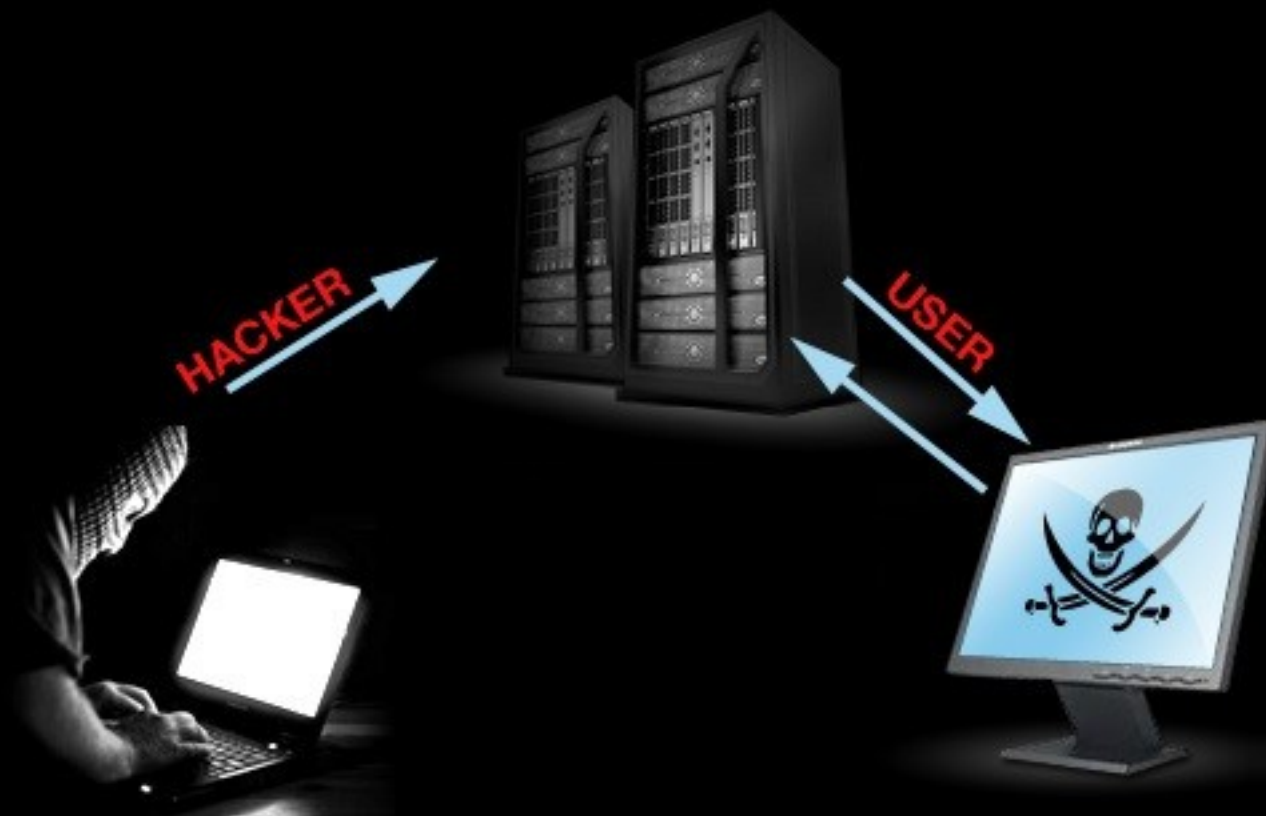
```
img_preload[0] = new Image;
```

```
img_preload[0].src = "Images/01.jpg";
```

```
img_preload[1] = new Image;
```

```
img_preload[1].src = "Images/02.jpg";
```

```
var now = new Date();
```

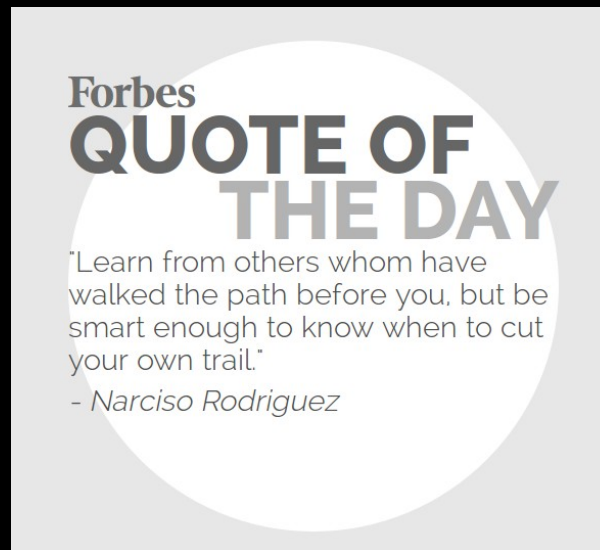




GAME OVER




# “CHINESE ATTACKERS HACKED FORBES WEBSITE IN WATERING-HOLE ATTACK”



The malware infection was inside the “Thought of the Day” Flash widget which appears whenever users try to access a Forbes.com page. Visitors didn't need to do anything other than to try to load Forbes.com in their browser to get infected.

**“FACEBOOK, APPLE, AND TWITTER EMPLOYEES VISITED  
IPHONEDEVSDK, WHERE THEIR COMPUTERS WERE  
COMPROMISED BY JAVA EXPLOITS”**





USERNAME:

PASSWORD:



A full-body photograph of a spearfisher underwater. The diver is wearing a camouflage-patterned wetsuit, a black Cressi diving mask, and a speargun. They are holding the speargun vertically in their right hand. The background is a clear blue ocean with some light rays visible. A semi-transparent blue banner with white text is overlaid on the left side of the image.

**SPEARPHISING IS INCREDIBLY EFFECTIVE**



**CENTRALISED-SERVICES AND CLOUD-SERVICE MAKE  
GREAT WATERING-HOLES TOO**



**WATERING-HOLES SOON BECOME BEACHHEADS**



THE CONSEQUENCES OF HACKS ARE  
VERY REAL

WE TRACKED THE VICTIMS OF  
TWO GLOBAL WEB-SITES THAT WERE  
COMPROMISED AND HAD THEIR  
CUSTOMER DETAILS RELEASED





423,183

UNIQUE USERNAME IN GERMANY





9,399  
ARE FROM FRANKFURT



A group of men in suits are shown in a medium shot. The man in the foreground, on the right, has a surprised expression with wide eyes and an open mouth. He is wearing a dark suit, a white shirt, and a dark tie. To his left, another man with glasses and a red tie looks on with a neutral expression. In the background, other men are partially visible, some looking down. The scene appears to be from a formal event or a news broadcast.

**681** ACCOUNTS

email:info@ AND email:\*.de AND isvalid:1



A photograph of Kanye West speaking at a press conference. He is wearing a dark blue short-sleeved button-down shirt and has a surprised or emphatic expression with his mouth open. He is gesturing with his right hand. In the background, there are blurred figures of people, including one holding a camera.

email:admin@ AND email:\*.de AND isvalid:1

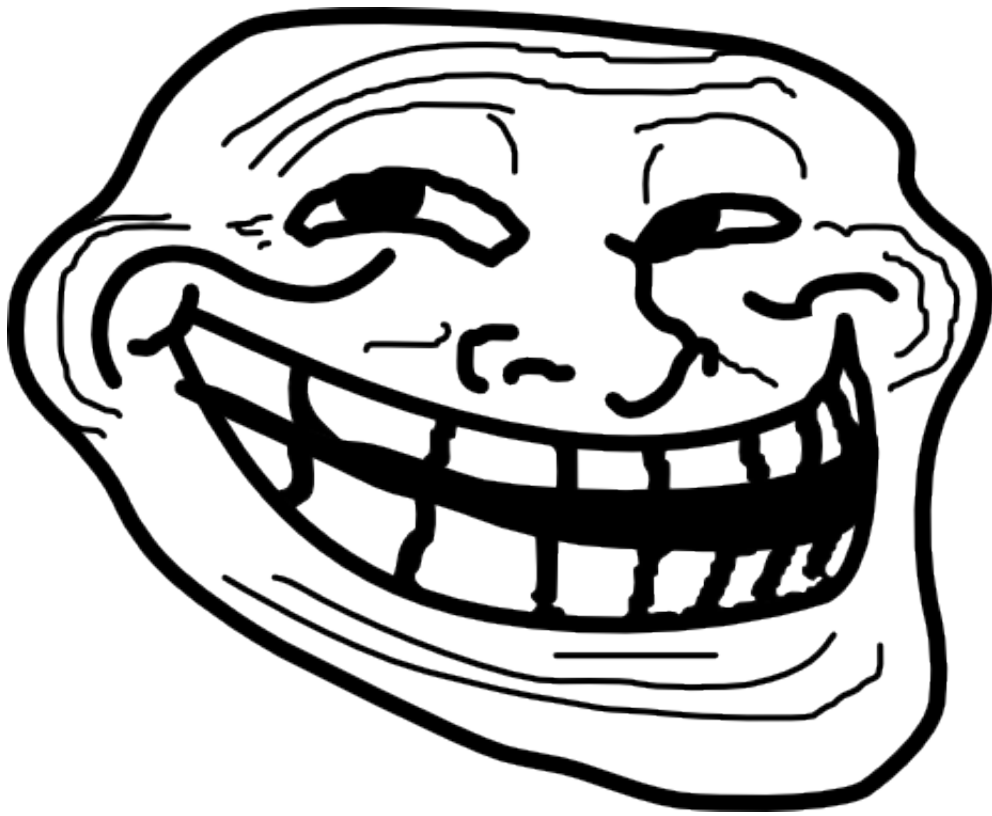
**12**  
**ACCOUNTS**

**ALL OF THESE PEOPLE AND MILLIONS MORE COULD BE  
IN YOUR SUPPLY-CHAIN**

**THEY ARE SOFT-TARGETS AND A BLACKHAT ONLY  
NEEDS TO BE LUCKY ONCE!**



**SOMETIMES YOU'RE LUCKY TWICE**



[email:commerzbank.com](mailto:email:commerzbank.com)

2  
**ACCOUNTS**

**SOMETIMES YOU'RE LUCKY 29 TIMES**





[email:db.com](mailto:email:db.com)

29  
ACCOUNTS

REMEMBER THESE 3 FACT

THE ONLY THING THE SCALES WELL



IS INCOMPETENCE

**SECURITY-HYGIENE IS YOUR ONLY REAL DEFENCE**

*We teach people to wash their hands, not  
to wash their hands only when at work!*





**BEING SECURITY-CONSCIOUS DOESN'T START AT YOUR  
OFFICE FRONT DOOR**

AND FINALLY...

IF YOU THINK THE SOLUTION IS TO



STOP YOUR USERS GOING ONLINE

YOU JUST DIDN'T GET IT!

\*For more information visit - <http://tiny.cc/DIRK>



Threema: D233EH2S  
email: [finux@finux.co.uk](mailto:finux@finux.co.uk)