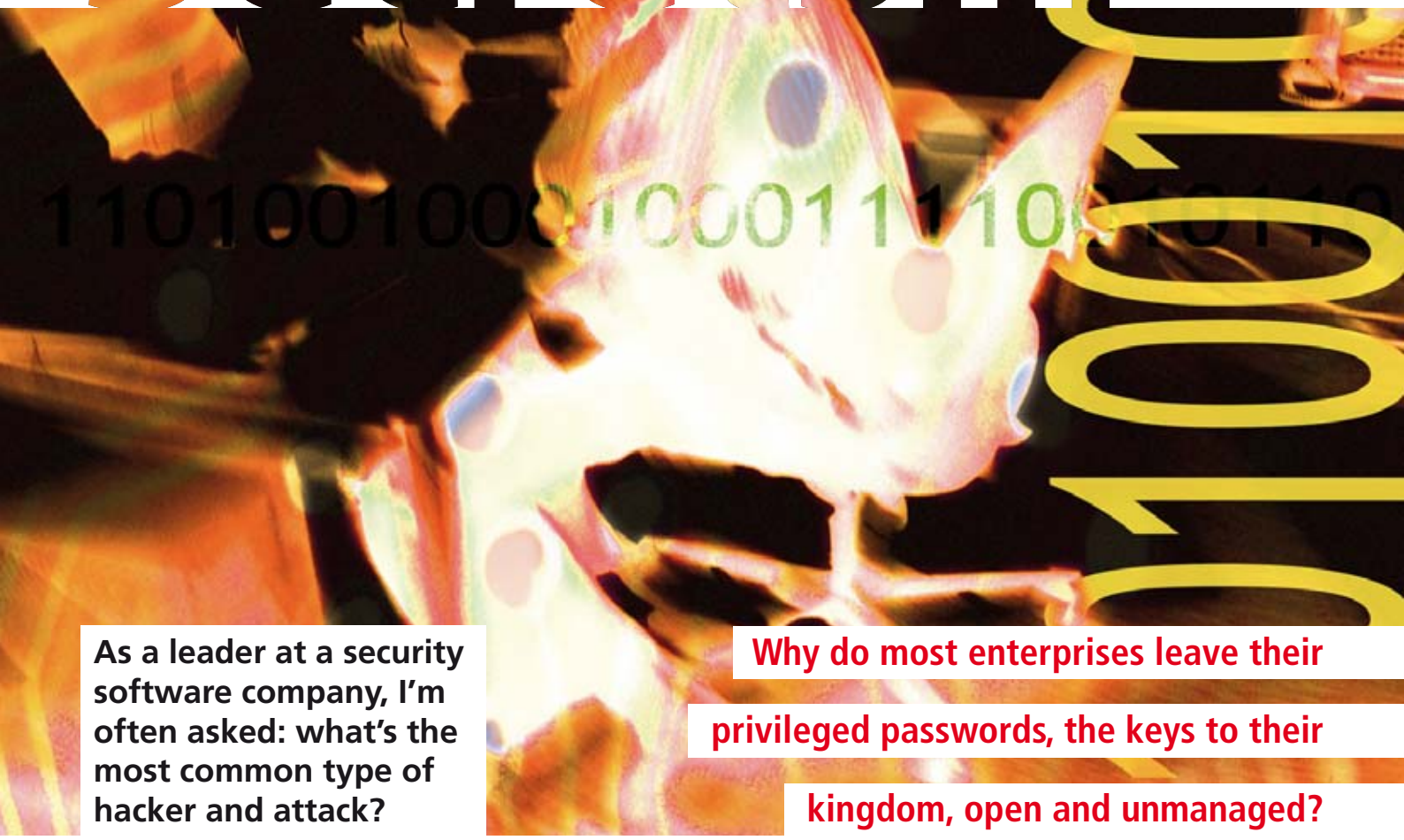
EXPOSED!

Top Hacker Secrets...

By Calum Macleod



As a leader at a security software company, I'm often asked: what's the most common type of hacker and attack?

Why do most enterprises leave their privileged passwords, the keys to their kingdom, open and unmanaged?

As a leader at a security software company, I'm often asked: what's the most common type of hacker and attack? Over time I've discovered that the general public holds a somewhat romantic image of hackers. One mental picture involves an emaciated young man in a poverty-stricken corner of the world. Greasy-haired and red-eyed, he types late into the night on an old TRS-80 workstation, trying desperately to get your American Express account number for nefarious purposes.

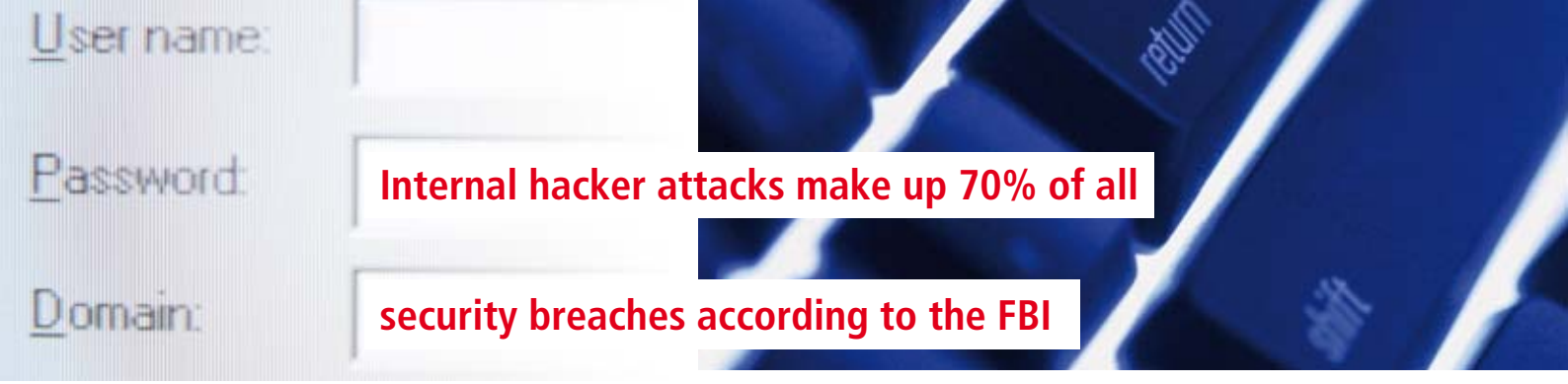
Another favourite image is of a cherub-faced pre-teen with extreme computer skills and little knowledge of law and order. Thanks to too much hardware and too little parental supervision, she creates a new virus that brings down every business on the Eastern seaboard.

Both images couldn't be more wrong.

According to the FBI, the most common hacker is probably sitting in the cubicle next to you, right now. This is someone who gets to work early, takes his or her turn cleaning out the office fridge, tells funny stories at lunch and, at some point, makes a very dumb move. It often starts when this hacker-next-door sees a file directory or workstation that's just too juicy to pass by, like one named 'salary comparison.' It's simply too tempting NOT to peek inside.

Curiosity or espionage

In other words, curiosity is one scenario motivating the most common hacker. Another is revenge. These situations take place when a web-savvy employee gets ticked off. Maybe their Christmas raise didn't make them too merry. Perhaps their boss just handed them a work improvement plan and a reason to cause trouble. This same hacker-next-door spends some time on the network and wonders… what if I could get into the email



Internal hacker attacks make up 70% of all security breaches according to the FBI

server files? What if I could open a few financial statements?

Finally, another common reason is industrial espionage. What organisation has time to do professional, in-depth background checks on every temporary IT consultant? Often this part-time help is called upon when times are roughest, and corners are most easily cut. The result is people who get easy access to the most sensitive and impenetrable systems (more on that later).

However, no matter what the reason, internal hacker attacks make up 70% of all security breaches according to the FBI. The next question is… how do these attackers get access to critical systems?

The answer is: all too easily. Once that hacker-next-door decides to break into a target system, their next stop is a search engine. A few key words later, and anyone can discover that the most common – and effective – type of hack into a target system is to become what's called a 'script kiddie.' Script kiddies use default lists of privileged passwords, or the super-user/administrative codes built into every piece of hardware and software. Have you ever noticed the 'administrator' ID next to your name when you login to your workstation? That's a privileged user and password, a backdoor into your system built by the manufacturer. It cannot be disabled or destroyed.

Easy access

Let's turn back to our hacker-next-door who wants into the 'salary comparison' workstation. They don't know who owns this workstation, but they can search to find what the default administrator passwords are for a Dell Latitude D600. According to a recent survey, 20% of all workstations have an administrator ID that's still set to the default password (*Cyber-Ark Enterprise Privileged Password Survey 2006*, *www.cyber-ark.com/survey.asp*). If the built-in default doesn't work, the would-be hacker may try some simple passwords like CompanyName123. You'd be stunned how often these basic password scenarios – also available as mini computer programs on the web – are the fastest way into any organisation's data.

Once the hacker enters a target system with a privileged password, the evil-doer now has more access to data than the system's legitimate users. I know of one company, for example, where a disgruntled IT professional changed every password on the network. All software had to be reloaded. The company was basically shut down for days. Meanwhile, the angry ex-employee denied all knowledge of the incident. And who could prosecute him? The deed was done under an anonymous identity, the administrator.

Another recent example of a script kiddie in action took place at the FBI (see *Consultant Breached FBI's Computers* by Eric Weiss, Washington Post, 7/6/2006). In this case, the hacker-next-door was a paid consultant. The suspect used computer programs easily found on the internet to go snooping into passwords and files throughout the FBI's organisation, including data related to the witness protection program. In no time, the suspect gained access to the passwords of 38,000 employees, including that of FBI Director Robert S Mueller III.

So there you have it: the most common hacker is actually someone working in your organisation today, a non-professional trouble-maker who – when tempted – can easily find his or her way into your organisation's most sensitive data.

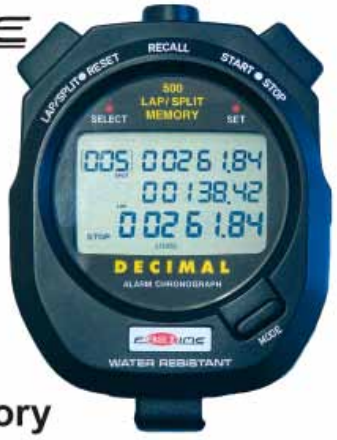
Protection

This leads to another question I am commonly asked: why do most enterprises leave their privileged passwords, the keys to their kingdom, open and unmanaged? The reason is simple: manually changing these codes is extremely time-consuming, so these back doors generally stay open. Visit professional hacker sites, and their biggest complaint about script kiddies is not that they exist... but that once these amateurs do something flagrant and dumb with privileged passwords, these wonderful secret passages into a company's data get closed to the professionals.

Of course there are automated ways to securely change privileged passwords, and to tie an individual ID to a shared one – this very software is now being used by many security savvy enterprises around the world. However until these solutions become standard tools in most enterprises, I'd keep a close eye on the folks around you. You never know who is privileged to YOUR information!

For more information from Cyber-Ark Software contact Calum Macleod on 00 31 621 827253 or email *calum.macleod@cyber-ark.com* or visit *www.cyber-ark.com.*

FASTIME



£40
Including VAT and delivery

500 memory
Decimal Minute Stopwatch

Stopwatch:
Triple display showing: split time, cumulative split time, continuously running cumulative time in 1/100th minute
Data Storage:
Up to 500 splits can be stored in memory.Split times are stored in segments.
Countdown timer and pacer functions
Stroke measurement
In this mode the duration of three strokes is taken and the stroke frequency (counts per minute) is calculated.

AST Limited 01530 411321.
Email: Sales@astopwatch.co.uk
Website: www.astopwatch.co.uk

All major credit cards accepted