DEVALUEUING ATTACK

DISINCENTIVIZING THREATS AGAINST THE NEXT BILLION DEVICES
“[I rob banks] because that’s where the money is.”

–WILLIE SUTTON (NOT REALLY)
Bandits Rob Clovis State Bank, Taking $10,000 to $25,000

Unmasked Men Enter Institution At 1 P. M., Bind Cashier And Lock Him In Vault And Make Escape With Gold And Currency In Auto

(CLOVIS (Fresno Co.), Feb. 5.—Two unmasked and armed bandits entered the Clovis State Bank at 1 o’clock this afternoon and after locking Assistant Cashier, Thomas...
The suspect was wearing a black hooded sweatshirt, black pants and a baseball hat.

YONKERS - A man who stole $6,000 from a bank on Central Park Avenue last week remains at large, police said.

The man entered the Atlantic Bank, at 2320 Central Park Ave., around 5:50 p.m. on Friday and handed the bank teller a note, Yonkers police said. The man was given $6,000 in cash and fled from the bank on foot.

Police conducted a search of the area, but the man was not located.
FBI Investigating Bangladesh Bank-Account Heist

Thieves were able to move about $81 million from Bangladesh’s account at the New York Fed to accounts in the Philippines, officials say.

Last month, computer criminals attempted to steal nearly $1 billion from Bangladesh’s account at the New York Fed, according to Bangladeshi officials. PHOTO: CLAUDIO PAPAPIETRO FOR THE WALL STREET JOURNAL

By DEVLIN BARRETT and KATY BURNE
Updated March 18, 2016 11:11 a.m. ET

Most Popular Videos

1. Campaign Fight Club: Wives in the Spotlight

2. Body-Paint Artist Builds ‘Human Car’ at Auto Show

3. Obamas Dance Tango During Official Visit to Argentina

4. iPhone SE Review: Smaller Gets Smarter

5. The Federal Reserve Heist: Where Did the Money Go?
ECONOMICS OF CYBERSECURITY
PART 1
em-pa-thy

noun \ˈem-pə-thē\

the action of understanding, being aware of, being sensitive to, and vicariously experiencing the feelings, thoughts, and experience of another or of either the past or present without having the feelings, thoughts, and experience fully communicated in an objectively explicit manner.
MO CODE

MO PROBLEMS
A world of insecurity

Worldwide

Information-security spending
$bn

Breached records
m

Sources: Gartner; Risk Based Security; Ponemon Institute

*Estimate  †Forecast
THIS. CAN’T. SCALE.
DEVALUATION
CASE STUDIES
In all my years working in this industry I've seen exactly 2 effective security technologies stand the test of time: firewalls and 2fa
The Systemic Value of Compatibly Communicating Devices Grows as the Square of Their Number:
Duo Two-Factor Login for Lightman

Enter a passcode or select one of the following options:

1. Duo Push to XXX-XXX-4545
2. Phone call to XXX-XXX-4545
3. SMS passcodes to XXX-XXX-4545 (next code starts with: 2)

Passcode or option (1-3):
You'll receive a notification from the Yahoo Mail app for you to approve.

Are you trying to sign in?

Tap to try No

Tap to try Yes

Firefox, Mac OS X, Sunnyvale, California
October 14, 2015 2:29PM
@JZdziarski this is true of any hardware security device. Mark my words: strong something-you-have + weak something you know is the future
<html>
<body>
<h1 id="tit">Metaphor</h1>
<br />
<script>
    var PAGE_SIZE = 0x1000;

    // Number of parallel leaks
    // It's only useful if we know we're reading a
    // large region with no holes, such as libcui8n.so
    var NUM_PARALLEL_LEAKS = 1;

    // libc.so base: 0xb6f73000 (Nexus)

    // Address to start leaking from
    var LEAK_START_ADDRESS = 0xb6ed9000;
    var LEAK_OFFSET = 0x88;

    var MAGIC_FAILED = 314;

    // (actual) ELF header value => offset from libcui8n.so
    var LEAKS_LOOKUP_TABLE = {
        0x05000035c4: 0x9a, // libaudioutils.so
        0x050000a64c: 0x94, // libcurl.so
        0x0500004460: 0x87, // libaudiorenderutilso.so
        0x050003b2e8: 0x69, // libaudiocaptureutilso.so
        0x050000028d: 0x26, // libstdc++.so
        0x05000016054: 0x22, // libm.so
        0x0500004154: 0x8, // liblog.so
        0x05000064ebc: 0x0, // libc.so
    }

    // (rounded) ELF header value => offset from libcui8n.so
    for (var key in LEAKS_LOOKUP_TABLE) {
    }
</script>
</body>
</html>
```json
{
    "shellcode_offset": 4096,
    "stack_pivot_padding": 76,
    "readAt_offset": 28,
    "fill_size": 32,
    "groom_count": 80,
    "spray_size": 528384,
    "spray_count": 64,
    "spray_address": 2952794112,
    "gadgets":
    {
        "mprotect": 236764,
        "pop_r0_r1_r2_pc": 313587,
        "pop_pc": 350244,
        "stack_pivot": 77348
    }
}
```
Internet-connected devices

Global forecast, bn

2013 14 15 16 17 18 19 20

0 10 20 30 40 50
ANCHOR FROM U.S.S. HARTFORD

This anchor came from the U.S.S. Hartford, Admiral Farragut's flagship during the Civil War "Battle of Mobile Bay" in August of 1864. It was there that he uttered the now famous words, "Damn the Torpedoes! Full Speed Ahead!"
FIN

@dinodaizovi / ddz@theta44.org