VERACODE

STRANGE FAILURES

BUT TRUE APPLICATION SECURITY

When insecure applications are exploited, weird stuff can happen — and it's never good. Here are six strange and mind-bending application security failures of 2016.

ILLINOIS STATE BOARD OF ELECTIONS

INFOMOCRACY: HACKING THE ELECTION

FACTS

Hacked emails played a big role in the 2016 U.S. presidential campaign. Meanwhile, voter databases in at least two U.S. states were compromised by a nation state, according to the FBI.

FLAW

Nation-state actors breached a voter database in Illinois via SQL injection and downloaded information on 200,000 voters. A voter database breach in Arizona was detected before data was stolen.

32% of applications have a SQL injection vulnerability.

POKÉMON GO

I, GOBOT

FACTS

The Pokémon Go augmented-reality game was an overnight sensation, but a privacy bug allowed the iOS app full access to users' Google accounts, including Gmail, Google Photos and more.

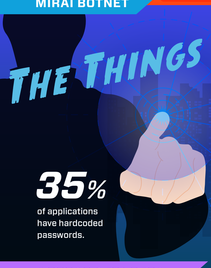
FLAW

Pokémon Go's developer Niantic and Google both made a big mistake in granting Pokémon Go access to private information the app didn't need.

61% of iOS apps have an information leakage vulnerability and 17% abuse APIs.

MIRAI BOTNET

THE THINGS



FACTS

Twitter, Netflix, GitHub and other big websites were knocked offline by a massive distributed denial of service (DDoS) attack on the Domain Name System services provider for those sites.

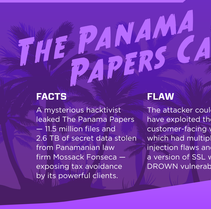
FLAW

The DDoS attack came from an enormous botnet of hijacked Internet of Things devices infected by Mirai, a malware that targets IoT devices that use hardcoded passwords.

35% of applications have hardcoded passwords.

MOSSACK FONSECA

THE PANAMA PAPERS CAPER



FACTS

A mysterious hacktivist leaked The Panama Papers — 11.5 million files and 2.6 TB of secret data stolen from Panamanian law firm Mossack Fonseca — exposing tax avoidance by its powerful clients.

FLAW

The attacker could have exploited the firm's customer-facing website, which had multiple SQL injection flaws and used a version of SSL with the DROWN vulnerability.

DROWN was the long-tail result of intentionally weak cryptography in the 1990s.

ADULT FRIENDFINDER

INVASION OF THE DATA SNATCHERS

FACTS

The notorious hacker "Peace" claimed to have stolen data on .73 million users of the online hook-up community Adult FriendFinder, and offered to sell their credentials on a Dark Web forum.

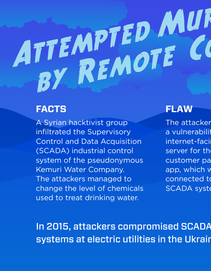
FLAW

The attacker exploited a local file inclusion vulnerability, which can lead to sensitive document exposure, code execution, denial of service and more.

3 BITCOINS was the starting price for 200 million Yahoo credentials on the Dark Web.

KEMURI WATER COMPANY

ATTEMPTED MURDER BY REMOTE CONTROL



FACTS

A Syrian hacktivist group infiltrated the Supervisory Control and Data Acquisition (SCADA) industrial control system of the pseudonymous Kemuri Water Company. The attackers managed to change the level of chemicals used to treat drinking water.

FLAW

The attackers exploited a vulnerability in the internet-facing web server for the utility's customer payment app, which was also connected to the SCADA system.

In 2015, attackers compromised SCADA systems at electric utilities in the Ukraine.

TRUE SECURITY

Align security goals with development realities.
Learn how developers think about application security.

VERACODE SECURE DEVELOPMENT SURVEY
veracode.com/developersurvey

VERACODE

SOURCES

1. "Foreign Hack Attack on State Voter Registration Site," Capitol Fax, July 26, 2016, capitolfax.com/2016/07/21/foreign-hack-attack-on-state-voter-registration-site/

2. "Pokémon Go Is a Huge Security Risk." Adam Reeve, July 8, 2016, adamreeve.tumblr.com/post/147129122059/pokemon-go-is-a-huge-security-risk

3. "How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet," Motherboard, September 29, 2016, motherboard.vice.com/read/15-million-connected-cameras-ddos-botnet-brian-krebs

4. "The Security Flaws at the Heart of the Panama Papers," Wired, April 6, 2016, www.wired.co.uk/article/panama-papers-mossack-fonseca-website-security-problems

5. "Hookup Service Adult FriendFinder May Have Been Hacked Again," Motherboard, October 19, 2016, motherboard.vice.com/read/hookup-service-adult-friendfinder-may-have-been-hacked-again

6. Verizon Data Breach Digest, March 2016, www.verizonenterprise.com/verizon-insights/data-breach-digest/2016/

LEARN MORE AT
VERACODE.COM