TECHIMPACT®

Advanced Security Threats
Fall 2019

Some important principles

- Digital threats are everywhere, and getting worse
- Digital crime is a massive multinational industry, which is constantly “innovating”
- The biggest threats are the ones you’re ignoring
- Security is a core element of your organizational mission
- ✓ Perfect security is neither possible nor desirable

Spear Phishing

Phishing is perhaps the most common attack targeting non-profits at the moment. Once attackers know an organization is vulnerable to phishing, they will typically devote more effort to getting in – via more targeted attacks

Spear phishing incorporates significant background research on the target organization (such as names and phone numbers of of leadership team)

Spear phishing attacks often involve burner email accounts set up solely for the purpose of facilitating this attack, often incorporating organizational info

Spear phishing emails often come from valid accounts that traditional spam checking won't flag, courtesy of either clever spam-checking bypass tricks or true compromise of a trusted contact

Step 1:
Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2:
Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3:
Exchange of Information

E-MAIL

From: Finance Director

SUBJECT: Initiate Acquisition

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4:
Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

Source: FBI

Spear Phishing Defenses

Mail processing rules that flag or block external mail masquerading as internal mail

Remove staff email addresses and phone numbers from your website; have staff do the same to their social media profiles

DKIM enforcement

Security training (Proofpoint/ KnowBe4)

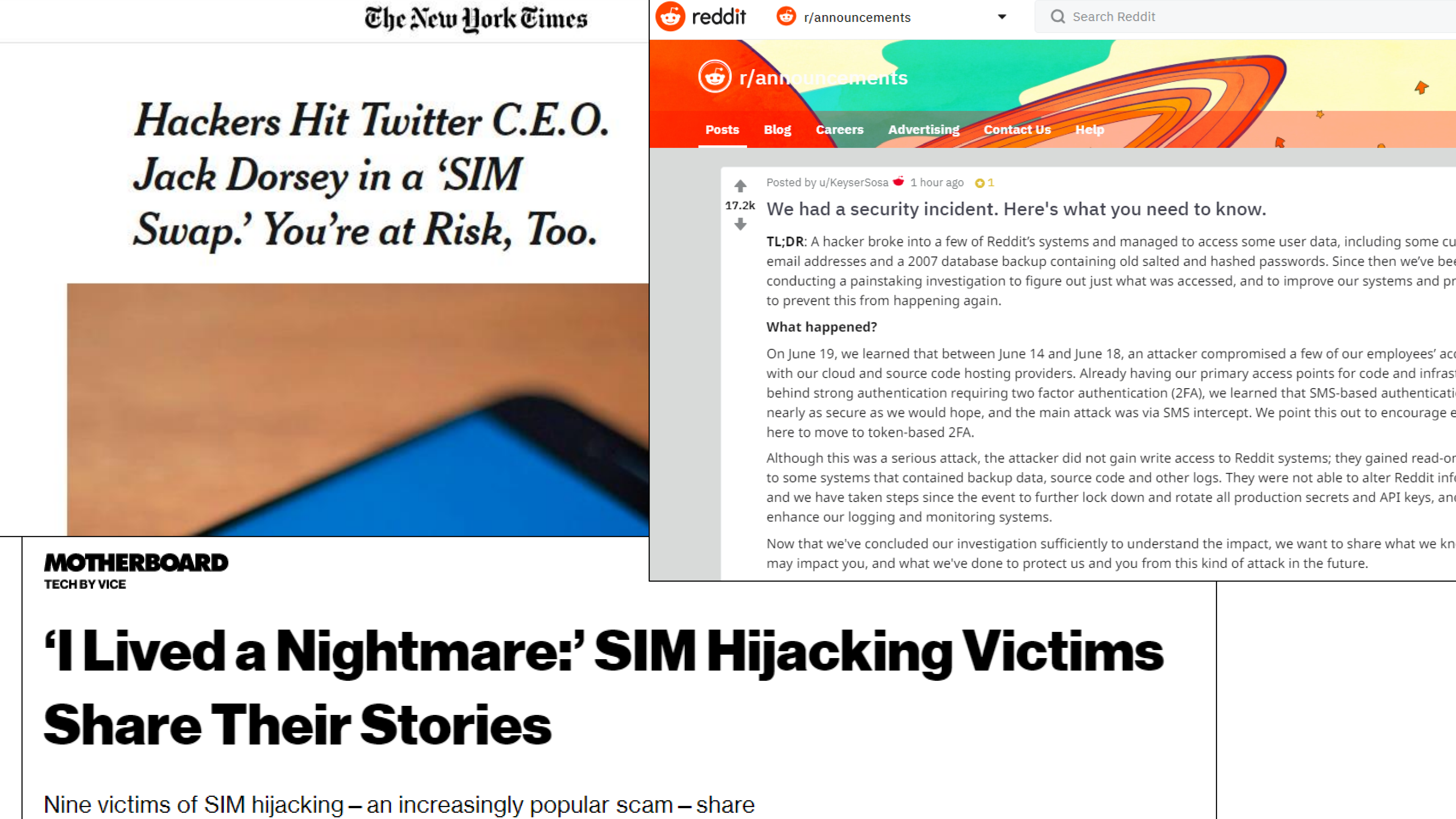
Phone number ID theft

Phone numbers have become digital IDs **and** means for verifying those identities

Many highly-sensitive sites rely on only phone verification for both MFA and password resets

Mobile providers will **not** verify identity in a robust way before performing a SIM replacement

3rd-party billing fraud



The New York Times

Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too.

Posted by u/KeyserSosa 1 hour ago 1

We had a security incident. Here's what you need to know.

TL;DR: A hacker broke into a few of Reddit's systems and managed to access some user data, including some cu
email addresses and a 2007 database backup containing old salted and hashed passwords. Since then we've bee
conducting a painstaking investigation to figure out just what was accessed, and to improve our systems and pr
to prevent this from happening again.

What happened?

On June 19, we learned that between June 14 and June 18, an attacker compromised a few of our employees' acc
with our cloud and source code hosting providers. Already having our primary access points for code and infras
behind strong authentication requiring two factor authentication (2FA), we learned that SMS-based authenticati
nearly as secure as we would hope, and the main attack was via SMS intercept. We point this out to encourage e
here to move to token-based 2FA.

Although this was a serious attack, the attacker did not gain write access to Reddit systems; they gained read-or
to some systems that contained backup data, source code and other logs. They were not able to alter Reddit info
and we have taken steps since the event to further lock down and rotate all production secrets and API keys, and
enhance our logging and monitoring systems.

Now that we've concluded our investigation sufficiently to understand the impact, we want to share what we kn
may impact you, and what we've done to protect us and you from this kind of attack in the future.

MOTHERBOARD
TECH BY VICE

'I Lived a Nightmare:' SIM Hijacking Victims Share Their Stories

Nine victims of SIM hijacking – an increasingly popular scam – share

Phone number defenses

Link sensitive accounts exclusively to a dedicated non-public phone number

Set up a virtual phone number using Google Voice or a similar service, and protect it with MFA

Treat your mobile phone number like a Social Security number, and do not share it casually

Ask your wireless provider about establishing a security PIN (while keeping your expectations low)

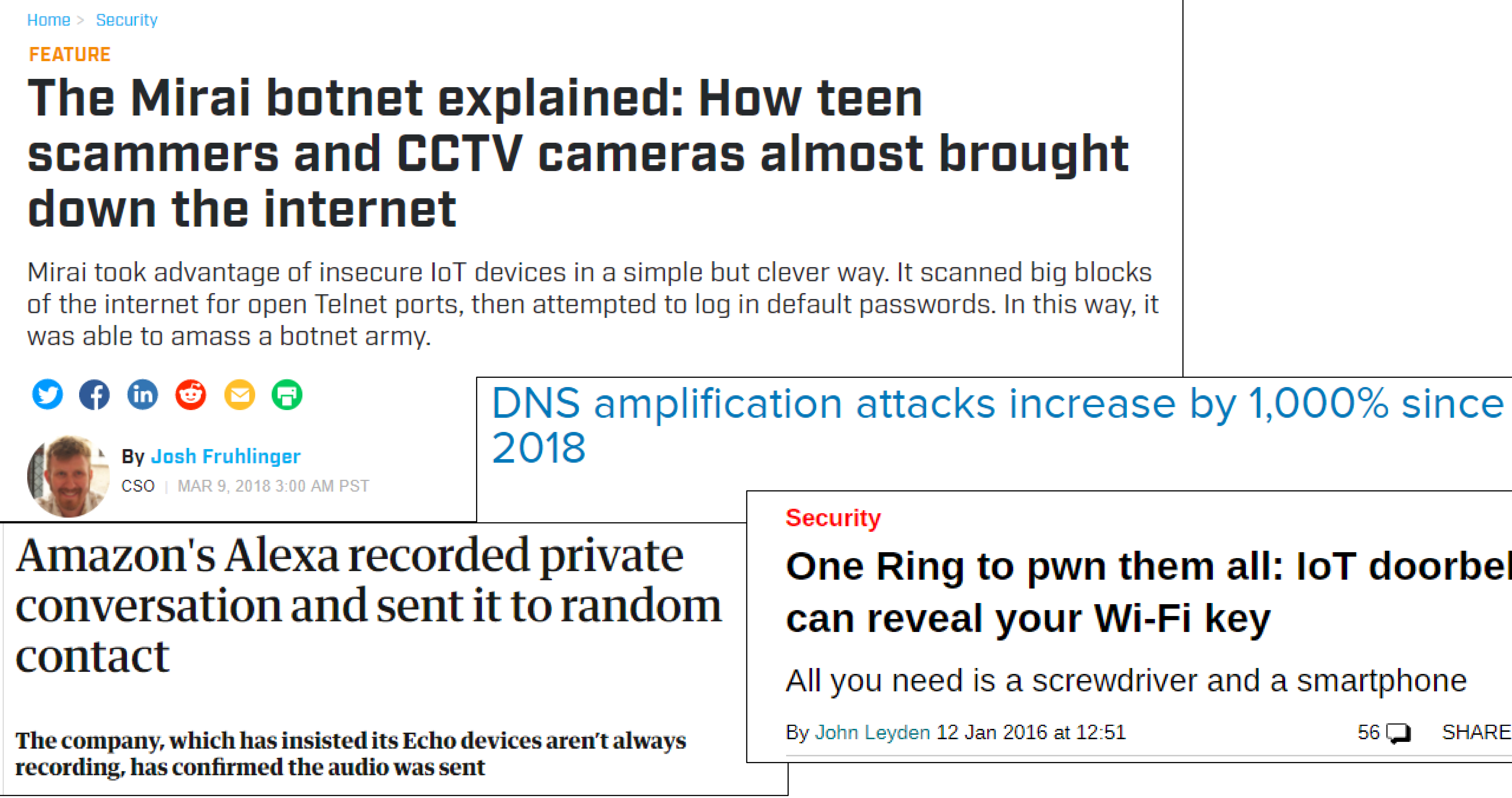
IoT / core infrastructure hijacking

Many network-connected devices can accept remote logins, or be tricked into sending out bogus requests

Many IoT and core infrastructure devices are deployed without changing default credentials or remote access settings

Few IoT / core infrastructure devices are updated as frequently as they should be

Potentially-vulnerable devices include routers, cameras, doorbells, printers, TVs, thermostats, smartlocks, etc.



Home > Security

FEATURE

The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Mirai took advantage of insecure IoT devices in a simple but clever way. It scanned big blocks of the internet for open Telnet ports, then attempted to log in default passwords. In this way, it was able to amass a botnet army.

By Josh Fruhlinger

CSO | MAR 9, 2018 3:00 AM PST

DNS amplification attacks increase by 1,000% since 2018

Amazon's Alexa recorded private conversation and sent it to random contact

The company, which has insisted its Echo devices aren't always recording, has confirmed the audio was sent

Security

One Ring to pwn them all: IoT doorbel can reveal your Wi-Fi key

All you need is a screwdriver and a smartphone

By John Leyden 12 Jan 2016 at 12:51 56 SHARE

IoT / Core Infrastructure defenses

Don’t deploy more gizmos than you really need; each extra device is one more thing to keep updated

Maintain a robust border firewall device whose firmware is kept up-to-date and whose rules are routinely audited

Check for and promptly apply new firmware updates for all IoT / network-connected devices

Crypto ransomware

Searches PCs for any files that look like user-generated data, puts those files into an encrypted zip archive, and deletes the originals

Often employed by more sophisticated groups with specific agendas, targeting larger organizations – especially local government agencies

Crypto ransomware is typically deployed via self-replicating worms that automatically infect every PC on the same network as the point of entry

The New York Times

Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000

Texas Pummeled by Coordinated Ransomware Attack

Cybercrime Campaign Counts 23 Victims - Mostly Local Government Entities

Mathew J. Schwartz (euroinfosec) • August 19, 2019

POLITICS

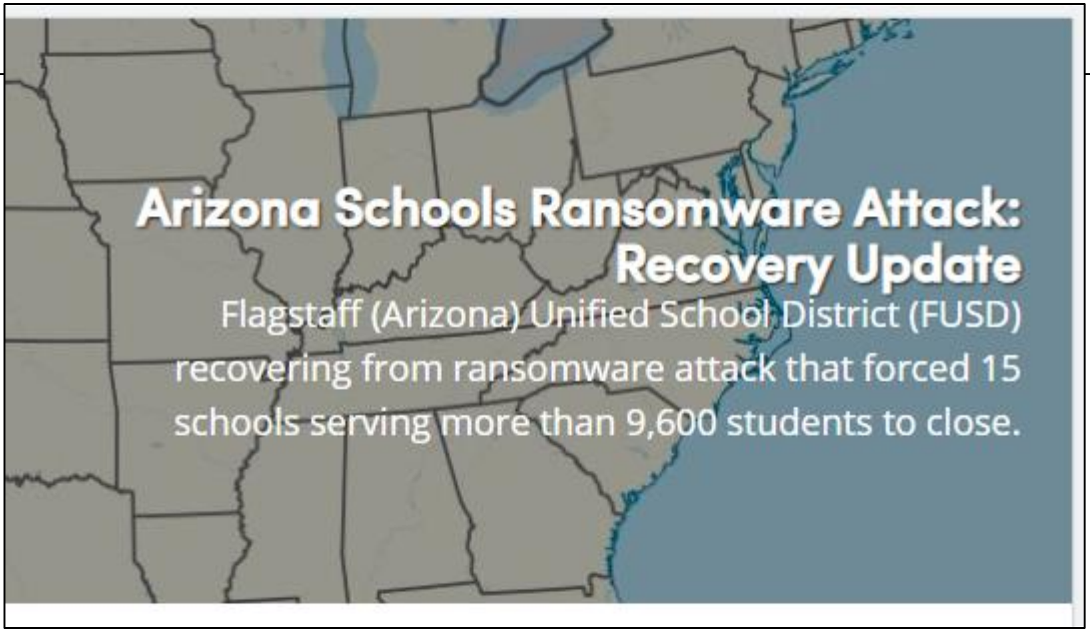
Baltimore City Council committee approves $10 million in funding for ransomware recovery

The New York Times

Another Hacked Florida City Pays a Ransom, This Time for $460,000

By Patricia Mazzei

June 27, 2019



Arizona Schools Ransomware Attack: Recovery Update

Flagstaff (Arizona) Unified School District (FUSD) recovering from ransomware attack that forced 15 schools serving more than 9,600 students to close.

Crypto Ransomware Defenses

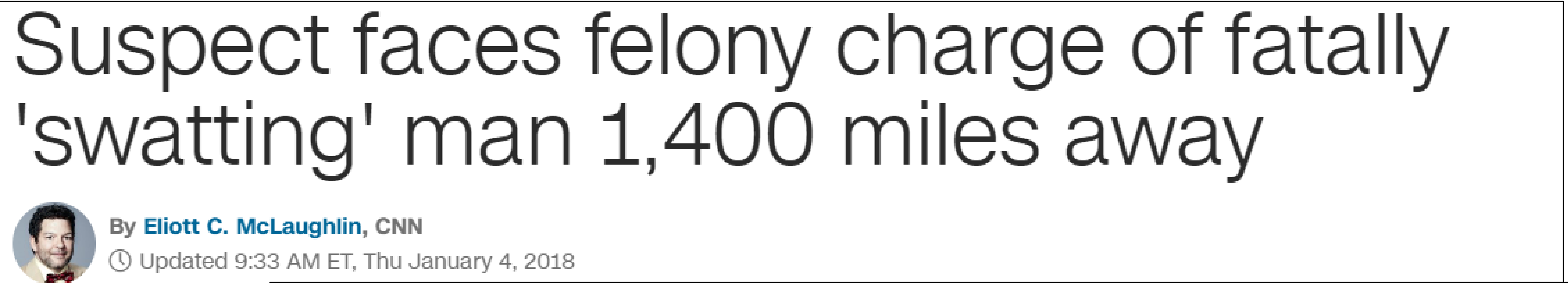
- Daily backups and isolation of critical systems
- Move all critical data off of self-hosted servers
- Centrally-managed software updates and antivirus
- High-grade Firewall with anti-malware subscription
- High-grade email security such as Advanced Threat Protection, Barracuda, etc.

Physical attacks: Doxing, SWATing, and stalking

Leveraging publicly-available information to harass, intimidate, or extort

Most prevalent in contentious spaces, but can happen anywhere trolls live

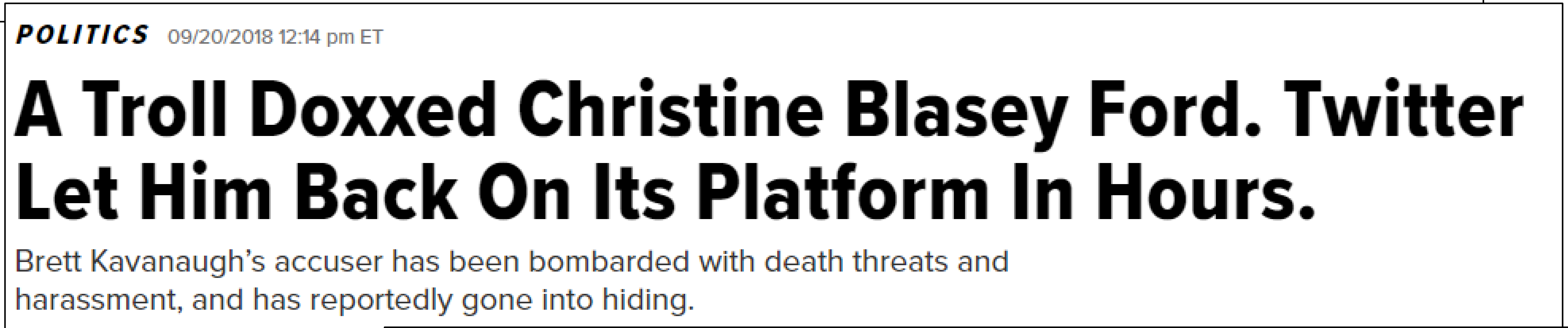
Can be enormously dangerous and destructive



Suspect faces felony charge of fatally 'swatting' man 1,400 miles away

By Eliott C. McLaughlin, CNN

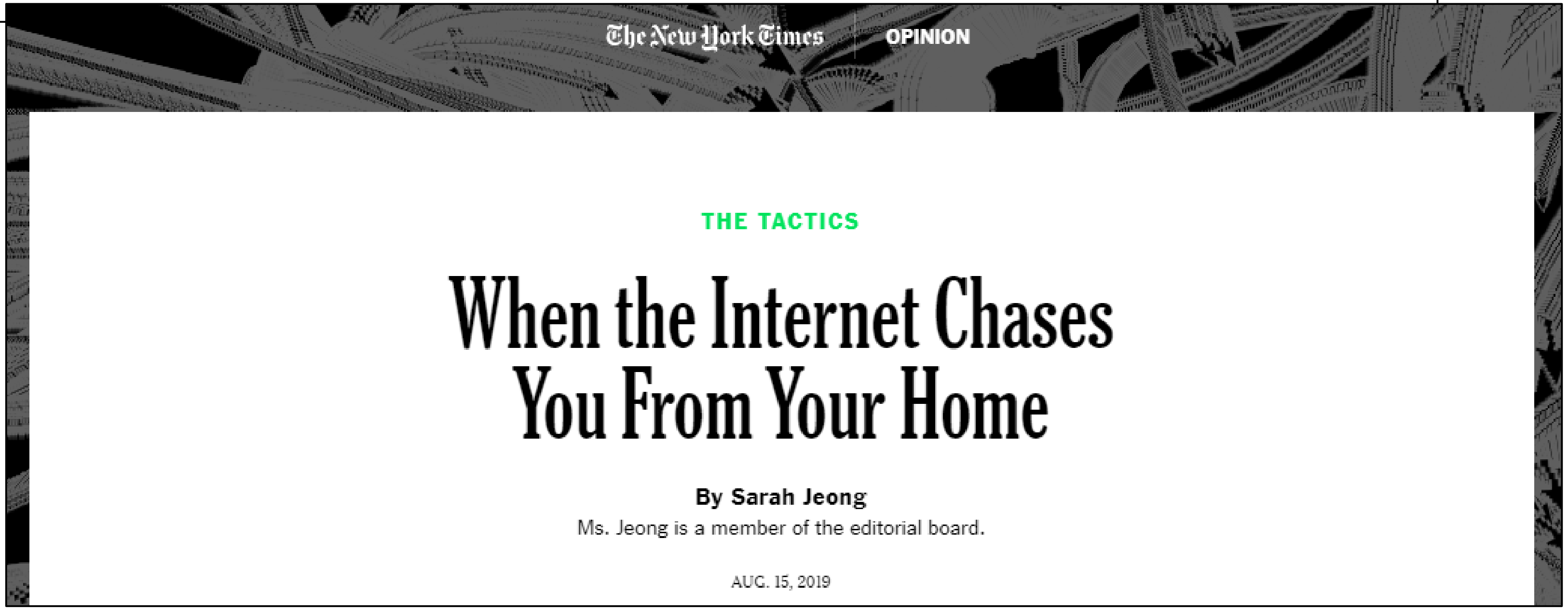
Updated 9:33 AM ET, Thu January 4, 2018



POLITICS 09/20/2018 12:14 pm ET

A Troll Doxxed Christine Blasey Ford. Twitter Let Him Back On Its Platform In Hours.

Brett Kavanaugh’s accuser has been bombarded with death threats and harassment, and has reportedly gone into hiding.



The New York Times | OPINION

THE TACTICS

When the Internet Chases You From Your Home

By Sarah Jeong

Ms. Jeong is a member of the editorial board.

AUG. 15, 2019

Physical Defenses

Sanitize social media profiles, removing any real-world location information for staff and their family

Don’t provide full staff profiles on your website – and particularly omit detailed biographical info

Consider subscribing to identity protection services

Talk to friends and family about what could happen if a stalking campaign begins

Domain Attacks

Most DNS registrar accounts are not protected with MFA

Few organizations have Registrar Lock directives

Making changes to DNS records is often sufficient to “prove” ownership of a website or cloud services account

Many organizations don’t even have direct admin control over their own DNS records

Domain Defenses

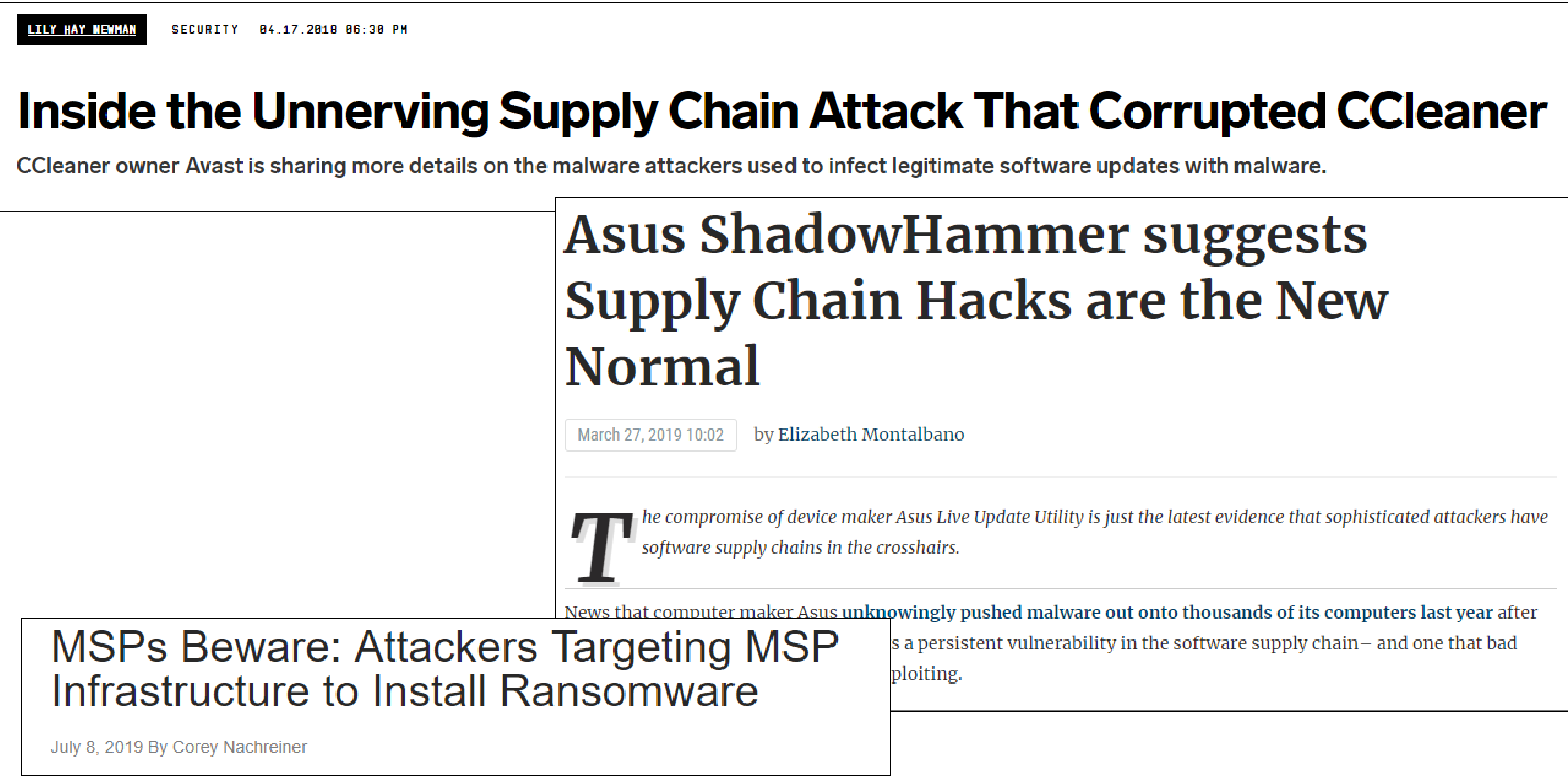
- Registrar locks
- Multi Factor Authentication for DNS Registrar admin login
- Auto-renewal
- Endpoint DNS protection (eg Cisco Umbrella)

Supply Chain / Watering Hole Attacks

Rather than attacking a target directly, attack a commonly-used resource that's easier to compromise

Compromise the software production process, so that exploit is pushed out as part of a normal, signed update

Forbes.com's "Quote of the Day" was hijacked in 2015, with the end goal of attacking visitors from financial and defense firms



LILY HAY NEWMAN SECURITY 04.17.2018 06:30 PM

Inside the Unnerving Supply Chain Attack That Corrupted CCleaner

CCleaner owner Avast is sharing more details on the malware attackers used to infect legitimate software updates with malware.

Asus ShadowHammer suggests Supply Chain Hacks are the New Normal

March 27, 2019 10:02 by Elizabeth Montalbano

The compromise of device maker Asus Live Update Utility is just the latest evidence that sophisticated attackers have software supply chains in the crosshairs.

News that computer maker Asus unknowingly pushed malware out onto thousands of its computers last year after
s a persistent vulnerability in the software supply chain– and one that bad
ploiting.

MSPs Beware: Attackers Targeting MSP Infrastructure to Install Ransomware

July 8, 2019 By Corey Nachreiner

Supply Chain Defenses

Centrally-managed software updates that operate on a short delay

Careful vendor vetting

Lobby Congress

Keep your fingers and toes crossed

What did I miss? Any favorite horror stories?

What are folks most worried about?

Thanks – and good luck out there!

jordan@techimpact.org