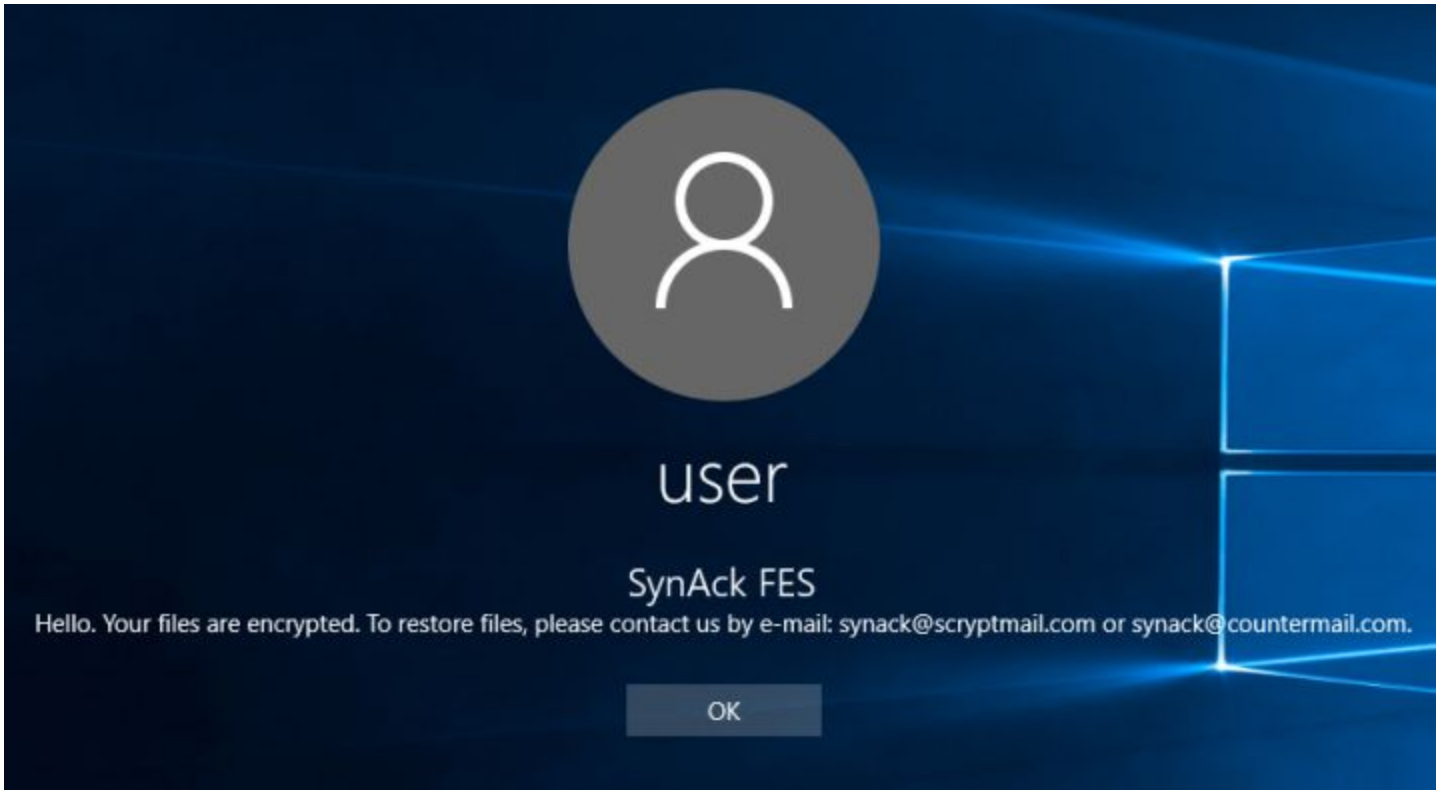
# Security Now! #662 - 05-08-18

# Spectre - NextGen

## This week on Security Now!

This week we begin by updating the status of several ongoing security stories: Russia vs Telegram, DrupalGeddon2, and the return of RowHammer. We will conclude with MAJOR new bad news related to Spectre. We also have a new cryptomalware, Twitter's in-the-clear passwords mistake, New Android 'P' security features, a crazy service for GDPR compliance, Firefox's sponsored content plan, another million routers being attacked, More deliberately compromised JavaScript found in the wild, a new Microsoft Meltdown mistake, a comprehensive Windows command reference, and signs of future encrypted Twitter DMs.

## Our Picture of the Week



## Security News

**Russia Blocks 50 VPNs and Proxy Services Providing Access to Telegram**
After Telegram refused to provide Russia's FSB intelligence agency with their customer encryption keys, Russia banned Telegram on April 13 by blocking all of Telegram's known IP addresses.

So Telegram switched to new IPs. And they chose IPs that they figured Russia could not ban without blocking many hundreds of other legitimate websites and services.

In response, Russian authorities then banned about 20 million IP addresses belonging to the Amazon and Google cloud services.  And, indeed, many hundreds of non-Telegram services were explicitly blacked out.

After a week and a half of this, Russia was forced to abandon the Amazon and Google Cloud ban. However, many observers suspect that both Amazon and Google caved to the Russian telecommunications' watchdog pressure because both companies began blocking the practice of "domain fronting" which was a popular  hack being used to circumvent censorship.

(In "Domain Fronting" the HOSTS header within a query is used to specify the actual machine being queried -- rather than the DNS lookup, IP and SNI indication in the pre-encrypted handshake.)

Note that Moxie's Signal has also been using Domain Fronting to circumvent state level blocking of their services and Amazon has threatened to cancel Signal's use of their services unless they cease using Domain Fronting.

Amazon:

Subject: Notification of potential account suspension regarding AWS Service Terms

Moxie,

Yesterday, AWS became aware of your Github and Hacker News/ycombinator posts describing how Signal plans to make its traffic look like traffic from another site, (popularly known as “domain fronting”) by using a domain owned by Amazon —Souq.com. You do not have permission from Amazon to use Souq.com for any purpose. Any use of Souq.com or any other domain to masquerade as another entity without express permission of the domain owner is in clear violation of the AWS Service Terms (Amazon CloudFront, Sec. 2.1: “You must own or have all necessary rights to use any domain name or SSL certificate that you use in conjunction with Amazon CloudFront”). It is also a violation of our Acceptable Use Policy by falsifying the origin of traffic and the unauthorized use of a domain.

We are happy for you to use AWS Services, but you must comply with our Service Terms. We will immediately suspend your use of CloudFront if you use third-party domains without their permission to masquerade as that third party.

But now back to Russia...

And so now, 50 VPN and proxy services have been blocked since they were being used by people to avoid Russian monitoring.

**Drupal Sites Fall Victims to Cryptojacking Campaigns**
http://bit.ly/SN-662
https://docs.google.com/spreadsheets/d/14TWw0lf2x6y8ji5Zd7zv9sIIVixU33irCM-i9CIrmo4/edit#gid=0

More than 350 known Drupal sites =HAVE= been compromised.

US security researcher Troy Mursch discovered a campaign that was compromising Drupal sites and hiding a version of the Coinhive in-browser cryptocurrency miner inside a file named "jquery.once.js?v=1.2," loaded on each of the compromised sites.

EVERY VISITOR to those sites has the in-browser mining script injected into their pages.

Among the victim sites are many government, university and religious portals. One notable name on the list is Chinese hardware maker Lenovo. Every visitor to Lenovo has malicious and unwanted mining script running in their browsers.

And that's not all...

Cyber-Security firm Imperva discovered and named the "Kitty" malware campaign on Drupal sites. It places a in-browser cryptocurrency miner in a file named "me0w.js." which uses a Monero miner from webminerpool.com.

And, in addition to dropping an in-browser miner, the "Kitty" perps also installed a persistent PHP backdoor into the site giving them long-term access after the site's owner updates and patches their distribution. And it also leaves a server-side miner running because... why not?

**GLitch: New 'Rowhammer' Attack Can Remotely Hijack Android Phones**
https://thehackernews.com/2018/05/rowhammer-android-hacking.html

A team of academics from the University in Amsterdam has developed a new startlingly effective REMOTE hack against Android smartphones using the user's web browser and the device's built-in GPU via the JavaScript WebGL API.

The new technique is the first Rowhammer attack to leverage GPUs to leak the computer's memory contents.

It turns out that GPUs are far more effective (and fast!) at leveraging Rowhammer RAM vulnerabilities than CPUs. And the WebGL timing system provides the precision needed to more accurately detect success. GPUs have much simpler caching to RAM, making cache bypassing much easier.

However, this also means that GLitch works only on platforms where CPUs and GPUs share the same memory which will restrict its use to smaller devices such as smartphones and tablets.

- The GLitch technique required just two minutes to compromise the researcher's test device.
- The remote attack is JavaScript based and worked through both the Chrome and Firefox browsers.
- So... in other words: You visit a site, spend two minutes reading a article... and your device is compromised!

https://www.kb.cert.org/vuls/id/283803 Vulnerability Note VU#283803
Integrated GPUs may allow side-channel and rowhammer attacks using WebGL ("Glitch")
https://www.vusec.net/wp-content/uploads/2018/05/glitch.pdf

**Firefox 60's forthcoming sponsored content on newly opened tabs can be turned off.**
https://www.bleepingcomputer.com/news/software/firefox-60-to-show-sponsored-content-for-us-users/

- We want to support Firefox.
- Right-Click the settings "gear" on the new tab page and disable "Show Sponsored Stories."
- Note, however, that this content comes from Mozilla's acquisition of Pocket and is fully privacy protecting. Advertisers promoting stories will receive no user data, such as age, gender, location, etc. Only story impressions and anonymized user clicks.

**Somebody Tried to Hide a Backdoor in a Popular JavaScript npm Package**
https://www.bleepingcomputer.com/news/security/somebody-tried-to-hide-a-backdoor-in-a-popular-javascript-npm-package/

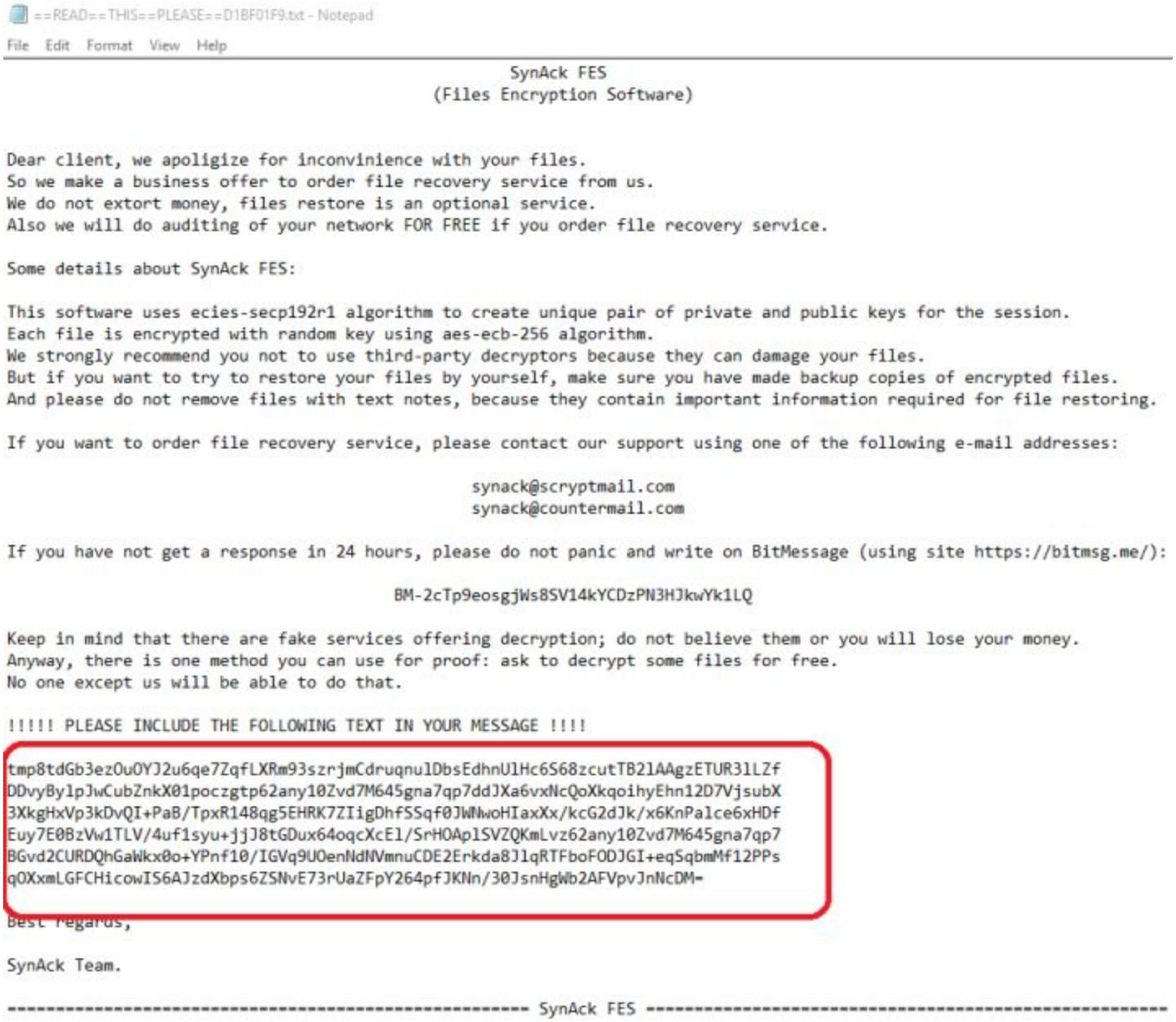
The specific story itself is interesting, but the background and the trend is deeply worrying: There are an increasing number of instances of JavaScript packages being compromised... on an ongoing basis.

As we know, the entire security model which has quietly evolved is deeply deeply flawed: The websites we visit are causing our web browsers to indiscriminantly download EXECUTABLE CODE from multiple and many random code library providers.

You couldn't make this up.

**Unfortunately, it's not =all= CryptoMining: CryptoMalware**
https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/
SynAck targeted ransomware uses the Doppelgänging technique
Heavily obscured ransomware using ‘Process Doppelgänging’ to evade detection
https://thehackernews.com/2018/05/synack-process-doppelganging.html

NTFS transactions to inject malware to bypass A/V detection.



==READ==THIS==PLEASE==D1BF01F9.txt - Notepad

File Edit Format View Help

SynAck FES
(Files Encryption Software)

Dear client, we apoligize for inconvinience with your files.
So we make a business offer to order file recovery service from us.
We do not extort money, files restore is an optional service.
Also we will do auditing of your network FOR FREE if you order file recovery service.

Some details about SynAck FES:

This software uses ecies-secp192r1 algorithm to create unique pair of private and public keys for the session.
Each file is encrypted with random key using aes-ecb-256 algorithm.
We strongly recommend you not to use third-party decryptors because they can damage your files.
But if you want to try to restore your files by yourself, make sure you have made backup copies of encrypted files.
And please do not remove files with text notes, because they contain important information required for file restoring.

If you want to order file recovery service, please contact our support using one of the following e-mail addresses:

synack@scryptmail.com
synack@countermail.com

If you have not get a response in 24 hours, please do not panic and write on BitMessage (using site https://bitmsg.me/):

BM-2cTp9eosgjWs8SV14kYCDzPN3HJkwYk1LQ

Keep in mind that there are fake services offering decryption; do not believe them or you will lose your money.
Anyway, there is one method you can use for proof: ask to decrypt some files for free.
No one except us will be able to do that.

!!!!! PLEASE INCLUDE THE FOLLOWING TEXT IN YOUR MESSAGE !!!!

tmp8tdGb3ezOuOYJ2u6qe7ZqfLXRm93szrjmCdruqnulDbsEdhnUlHc6S68zcutTB2lAAgzETUR3lLZf
DDvyBylpJwCubZnkX01poczgtp62any10Zvd7M645gna7qp7ddJXa6vxNcQoXkqoihyEhn12D7VjsubX
3XkgHxVp3kDvQI+PaB/TpxR148qg5EHRK7ZIigDhfSSqf0JWNwoHIaxXx/kcG2dJk/x6KnPalce6xHDf
Euy7E0BzVw1TLV/4uf1syu+jjJ8tGDux64oqcXcEl/SrHOAplSVZQKmLvz62any10Zvd7M645gna7qp7
BGvd2CURDQhGaWkx0o+YPnf10/IGVq9UOenNdNVmnuCDE2Erkda8J1qRTFboFODJGI+eqSqbmMf12PPs
qOXxmLGFCHicowIS6AJzdXbps6ZSNvE73rUaZFpY264pfJKNn/30JsnHgWb2AFVpvJnNcDM=

Best regards,

SynAck Team.

---------- SynAck FES ----------

**Twitter discovers a mistake. 330 million people: please change your passwords.**

Hi @SGgrc,

When you set a password for your Twitter account, we use technology that masks it so no one at the company can see it. We recently identified a bug that stored passwords unmasked in an internal log. We have fixed the bug, and our investigation shows no indication of breach or misuse by anyone.

Out of an abundance of caution, we ask that you consider changing your password on all services where you've used this password. You can change your Twitter password anytime by going to the password settings page.

About The Bug

We mask passwords through a process called hashing using a function known as bcrypt, which replaces the actual password with a random set of numbers and letters that are stored in Twitter's system. This allows our systems to validate your account credentials without revealing your password. This is an industry standard.

Due to a bug, passwords were written to an internal log before completing the hashing process. We found this error ourselves, removed the passwords, and are implementing plans to prevent this bug from happening again.

Tips on Account Security

Again, although we have no reason to believe password information ever left Twitter's systems or was misused by anyone, there are a few steps you can take to help us keep your account safe:

1. Change your password on Twitter and on any other service where you may have used the same password.
2. Use a strong password that you don't reuse on other services.
3. Enable login verification, also known as two factor authentication. This is the single best action you can take to increase your account security.
4. Use a password manager to make sure you're using strong, unique passwords everywhere.

We are very sorry this happened. We recognize and appreciate the trust you place in us, and are committed to earning that trust every day.

Team Twitter

---
Twitter is securely protecting its users passwords with the Bcrypt PBKDF hashing function. But it turned out that an internal log was being kept of pre-hashed raw user passwords.

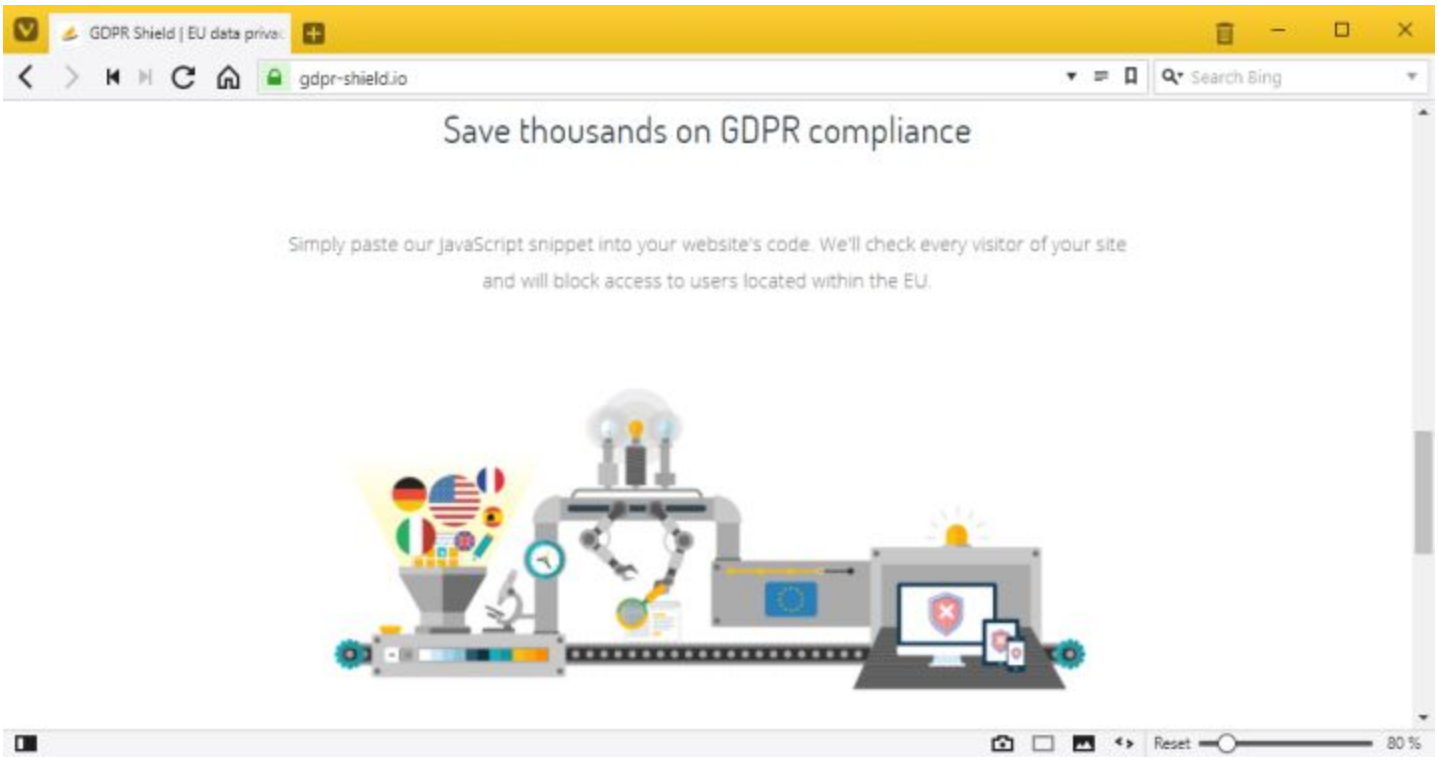
(This is just one of the many things SQRL protects from. SQRL only gives websites a user's public key for that one website.)
Should you change your password?

**Android P adds a useful collection of security & privacy features:**

- Restricted access to the /proc/net process:
  Up until 'P' =any= application running on any previous edition of Android had unrestricted access to /proc/net. A user-installed app that obtains the permission to access the user's network data can tap into the Android OS "/proc/net" process and detect any time the user is initiating a network connection and to what server. The app cannot access the data in that network connection, but often enough, knowing where the user is connecting is enough for apps that collect user data to sell it to advertisers. In the future, Android engineers said that only VPN apps will be allowed access to this process and that any other app that needs it must undergo a code audit.

- This update is just the latest security-focused change made to the upcoming Android P operating system. Below are others:
- Android P will block cleartext (HTTP) traffic from apps. HTTPS is the new norm.
- 'P' will use the same UI when requesting fingerprint authentification across apps and devices.
- It will block background apps from accessing the phone's camera and microphone.
- It will encrypt backups on the device with a local secret key before sending the backup for storage on Google's servers.
- It will begin experimenting support for MAC address randomization. (Recall that Apple's iOS has long been doing this to mask users' presence when not associated with an access point.)
- Support for DNS over TLS.

**New Service Blocks EU Users So Companies Can Save Thousands on GDPR Compliance**
https://www.bleepingcomputer.com/news/security/new-service-blocks-eu-users-so-companies-can-save-thousands-on-gdpr-compliance/




The EU's General Data Protection Regulation (GDPR) compliance deadline, for every business everywhere doing business in the EU is 25th May 2018.

The ultimate goal of the regulation is to give individuals more rights over their data and restrict

how companies process private information.

What has caught everyone's attention is the impossible-to-sanely-ignore fines which the legislation imposes: Under GDPR, firms can be fined up to €20 million ($28m) or four percent of group worldwide turnover, whichever is greater.

The DPO - Data Protection Officer:
Not every organization needs a Data Protection Officer The role of Data Protection Officer (DPO) becomes "mandatory" under GDPR. However, not every organisation will need to rush out to appoint one. DPOs are only a pre-requisite at public authorities, and businesses where data processing and monitoring are done on a large scale.

Smaller firms have reduced burden:
Companies having 250 employees or fewer do not have to comply with every GDPR regulation. Small firms do not need to have documentation explaining why personal data is being collected and processed, the information being stored or for how long. Small firms are also not required to maintain a record of processing activities unless this carries a risk to the rights and freedoms of data subjects as a regular occurrence, or relates to certain data like criminal convictions and offences.

Customers DO need to be able to access and view ALL data stored about them and also to requet its complete deletion.

**More than one million Dasan GPON Routers are under attack**
https://www.vpnmentor.com/blog/critical-vulnerability-gpon-router/
https://www.exploit-db.com/exploits/44576/

<quote> We conducted a comprehensive assessment on a number of GPON home routers. Many routers today use GPON internet, and we found a way to bypass all authentication on the devices (CVE-2018-10561). With this authentication bypass, we were also able to unveil another command injection vulnerability (CVE-2018-10562) and execute commands on the device.

South Korean manufacturer Dasan produces GPON routers. GPON = Gigabit Passive Optical Network.

These routers are provided by ISPs to their fiber-enabled customers.

Unfortunately, they are not secure.  More than one million of these routers have been identified throughout Vietnam, Kazakhstan and Mexico where ISPs have used these routers.

And 360 Netlab researchers have identified a botnet, controlled from Vietnam, that is currently scanning and exploiting these devices.

CVE-2018-10561: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10561
An issue was discovered on Dasan GPON home routers. It is possible to bypass authentication simply by appending "?images" to any URL of the device that requires authentication, as demonstrated by the /menu.html?images/ or /GponForm/diag_FORM?images/ URI. One can then manage the device.

CVE-2018-10562: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10562
An issue was discovered on Dasan GPON home routers. Command Injection can occur via the dest_host parameter in a diag_action=ping request to a GponForm/diag_Form URI. Because the router saves ping results in /tmp and transmits them to the user when the user revisits /diag.html, it's quite simple to execute commands and retrieve their output.

**Microsoft Working on a Fix for Windows 10 Meltdown Patch Bypass**
Alex Ionescu (@aionescu) May 2, 2018 (a security researcher with Crowdstrike)

Tweet: Welp, it turns out the #Meltdown patches for Windows 10 had a fatal flaw: calling NtCallEnclave returned back to user space with the full kernel page table directory, completely undermining the mitigation. This is now patched on RS4 but not earlier builds -- no backport??

https://twitter.com/aionescu/status/991675604469669890/photo/1

Back at the end of March, the "Total Meltdown" bug exposed the system's page tables for Windows 7 and Server 2008 R2 systems.

**Windows Command Reference:**
Microsoft has published a comprehensive Windows command reference detailing more than 250 Windows console commands.

https://download.microsoft.com/download/5/8/9/58911986-D4AD-4695-BF63-F734CD4DF8F2/ws-commands.pdf

**Twitter has an unlaunched 'Secret' encrypted messages feature**
https://techcrunch.com/2018/05/07/encrypted-dms/

## SpinRite

Bree Duffy / Location: Oregon
Subject: Security concern, Spinrite saves my sister's hard drive, and me, a headache
Date: 26 Apr 2018 00:19:50
:
When I heard about the virtual card numbers from Capital One on your show I was highly intrigued. However, I'm also highly distrustful of apps from most companies due to concerns of snooping, or down right sloppy programming causing issues. Do you have any thoughts on the safety of Capital Ones Eno plugin for desktop, or the phone app?

Now to Spinrite. I have the rather unfortunate distinction of being the go-to guy in the family whenever there is computer trouble. I love helping them, but figuring out obscure problems can be quite the headache. My sister brought me her computer which wouldn't boot into Windows, it couldn't even see the boot record. I had fortuitously just bought Spinrite and decided to give it a go. As with many such stories, while no errors were reported, all of a sudden the computer booted properly saving me the headache of either formatting, or buying a new hard drive and re-installing Windows and all of my sister's applications, etc.

Thank you very much for making this very useful tool. I look forward to the new versions when you get to it, and SQRL when it becomes available.

---

# Spectre - Next Gen

**8 New Spectre-Class Vulnerabilities (Spectre-NG) Found in Intel CPUs**
https://thehackernews.com/2018/05/intel-spectre-vulnerability.html
https://www.heise.de/ct/artikel/Exclusive-Spectre-NG-Multiple-new-Intel-CPU-flaws-revealed-several-serious-4040648.html

Eight new CVEs have been allocated bug identifiers but their contents are being kept secret.

Google Project Zero discovered one of the Spectre-NG flaws.

Intel has internally classified 4 of the Spectre-NG vulnerabilities as "high risk"; the remaining four are rated as "medium". According to Heise's research, the risks and attack scenarios for the Spectre-NG flaws are similar to those for Spectre – with one exception:

One of the Spectre-NG flaws simplifies attacks across system boundaries to such an extent that the threat estimate is significantly higher than it ever was with Spectre. Specifically, an attacker could launch exploit code in a virtual machine (VM) and attack the host system from there – the server of a cloud host, for example. Alternatively, it could attack the VMs of other customers running on the same server. Intel's Software Guard Extensions (SGX), which are designed to protect sensitive data on cloud servers, are not Spectre-safe.

Heise believes that Intel is planning two waves of patches. The first is scheduled to start in May; a second is currently planned for August.

ARM systems are also believed to be affected by at least some of these eight new vulnerabilities and the impact, if any, for AMD is not yet known.