COMPUTER SECURITY UPDATE

Nikolaos Filippakis

CERN Security Team

HEPiX workshop, Autumn 2020

Overview

Phishing and CEO Fraud

Malware in apps

Data leaks

Teleconferencing

Vulnerabilities

Ransomware

HPC attacks

Software library curation

Vishing (voice phishing)

"The social engineering that occurred on July 15, 2020, targeted a small number of employees through a phone spear phishing attack."

https://en.wikipedia.org/wiki/2020_Twitter_bitcoin_scam

Vishing (voice phishing)

Subject: Strange phonecall

Dear Colleagues,

A few moments ago I was called on my office phone by somebody called "Artur from Technical Support". He told me there was a serious problem with my computer and I should close all of the windows. I told him I was in the middle of something and asked him to confirm who he was. He repeated he is "Artur from Technical Support" and I basically told him I didn't believe him and hung up.

The COVID-19 pandemic has resulted in a mass shift to working from home, resulting in increased use of corporate virtual private networks (VPNs) and elimination of in-person verification. In mid-July 2020, cybercriminals started a vishing campaign—gaining access to employee tools at multiple companies with indiscriminate targeting—with the end goal of monetizing the access. Using vished credentials, cybercriminals mined the victim company databases for their customers' personal information to leverage in other attacks. The monetizing method varied depending on the company but was highly aggressive with a tight timeline between the initial breach and the disruptive cash-out scheme.

CEO Fraud

Subject: Re: [PROJECT]

Dear Martin,

Thanks for the reply. I need your help with the Rules & Practices of the [PROJECT]. The [PROJECT] has an urgent payment of 2,963 EUR to Ireland for the payment of support for the IAEA's Research and Training workshop.

The treasurer is not available due to a recent family emergency and will return to the office on December 1st.
As the [PROJECT] President, it is my duty to facilitate this payment as soon as possible. However, I am out of the country for an event and I am not available to facilitate payment until I return from my trip because I do not have access to my phone to receive a bank token for any transfer until I return.

I would like to ask you for support to help me pay this amount while I will reimburse you next week as soon as I return.

Please, can I send the beneficiary bank details if it is convenient for you to make this payment today?

We will refund the amount as soon as possible next week.

I really count on you while I wait for your email.

Best wishes,

Subject: Re: Are you available?

Good morning Petra, Your reply came in at the right time I need you to get Google Play gift cards from any store around now.There are some Prospects i need to send Gift Cards today but I can't do that right now because I'm currently in a meeting.Let me know if its possible to get them right now, so i can tell you what amount. I'll reimburse you later today.

Sent from my iPad

Cher(e) Client(e),

Vous avez un colis au bureau de DHL Express.
Vous disposez d'un délai de 48 heures pour récupérer votre colis ,Sinon il sera
Veuillez confirmer l'envoi du colis à votre domicile en suivant les étapes au de:

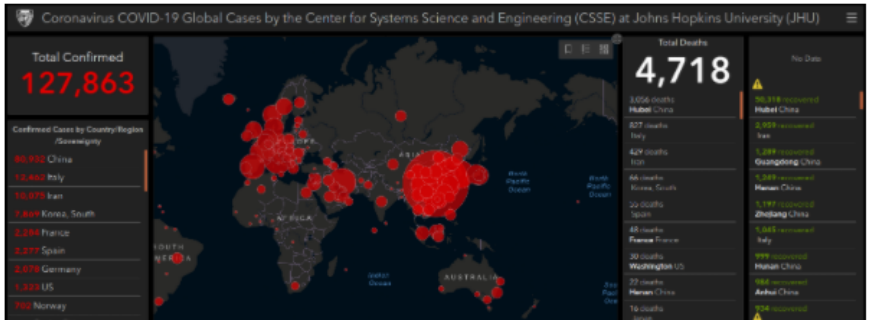
1. Envoyez psc75 au n° 474 par SMS
2. Recevoir le code PIN de confirmation
3. Envoyez le code PIN (16 chiffres) à l'adresse suivant en cliquant sur le Mail :

COVID-19 & phishing

12 Live Coronavirus Map Used to Spread Malware

MAR 20

Cybercriminals constantly latch on to news items that captivate the public's attention, but usually they do so by sensationalizing the topic or spreading misinformation about it. Recently, however, cybercrooks have started disseminating real-time, accurate information about global infection rates tied to the **Coronavirus/COVID-19** pandemic in a bid to infect computers with malicious software.



I know every dirty little secret about your life. To prove my point, tell me, does "[redacted]" rin

What do I know about you?
To start with, I know all of your passwords. I am aware of your whereabouts, what you eat, wit

What am I capable of doing?
If I want, I could even infect your whole family with the CoronaVirus, reveal all of your secrets.

What should you do?
You need to pay me $4000. You'll make the payment via Bitcoin to the below-mentioned addre
buy bitcoin" in Google.

Bitcoin Address:
bc1qun739g0k45lnqa57s3v4nhkppsn6npn8am0vwp
(It is cAsE sensitive, so copy and paste it)

You have 24 hours to make the payment. I have a unique pixel within this email message, and

- Cybercriminals exploit the fear & uncertainty caused by COVID-19
- Doubling of phishing e-mails, exponential increase in malware
- Stay vigilant, stay patched!

https://home.cern/news/news/computing/computer-security-tele-protect

https://www.schneier.com/blog/archives/2020/04/cybersecurity_d.html

2nd Factor Authentication

- 2FA support was developed and tested in the beginning of the year
- Important computing services such as SSH / Puppet / Foreman / tbag are now asking for 2FA (starting March 2020)
- CERN supports WebAuthn (ie. Yubikey) or TOTP
- New SSO with more capabilities planned, ie. notifying users when their p/w has been found in a dump by integrating with HIBP

  https://security.web.cern.ch/reports/en/monthly_reports/2019/2019-12.shtml

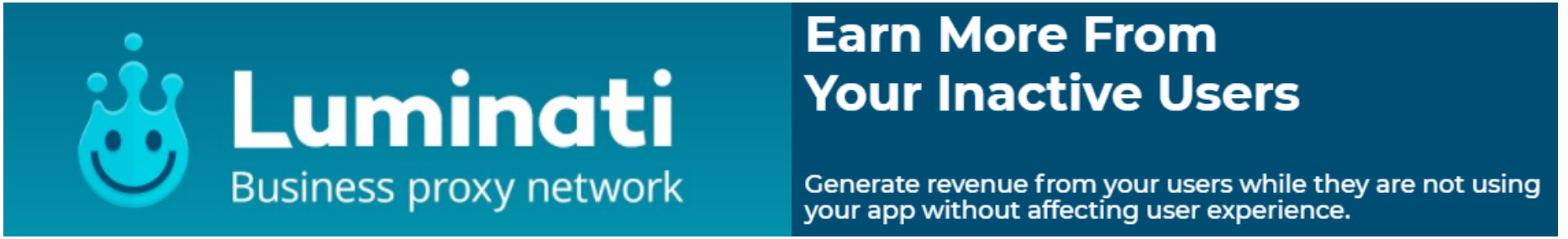
- No longer request yearly password changes once deployment is complete

  https://home.cern/news/news/computing/computer-security-password-revolutions

- 2FA also planned for other services critical to the agile infrastructure, such as OpenStack, Gitlab, Koji

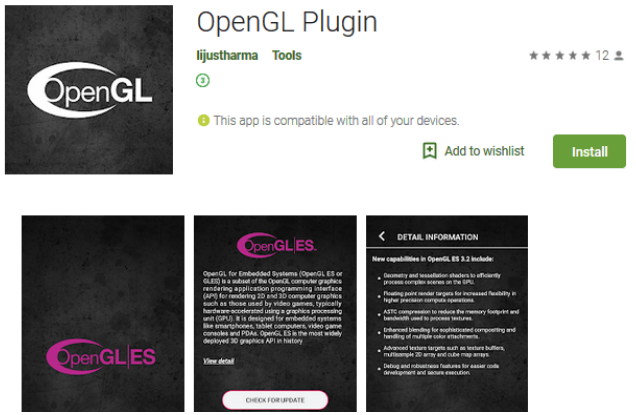
  https://security.web.cern.ch/reports/en/monthly_reports/2020/2020-01.shtml

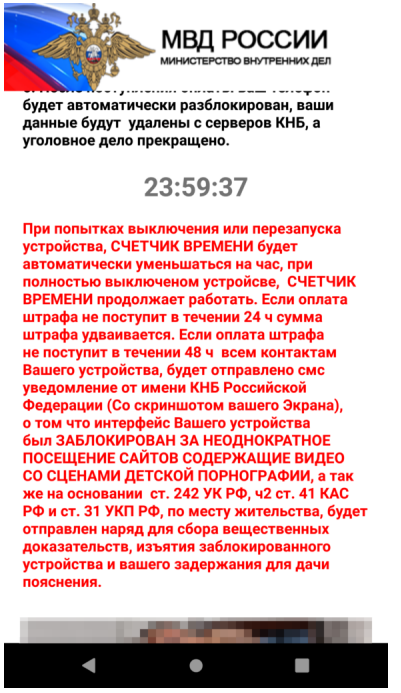
Luminati SDK (aka. Hola VPN)



- Apps use the Luminati SDK to monetize user installs
- On numerous Play Store apps (Hola Unblocker and VPN, Mobdro, Peel Smart Remote, TV streaming apps, many more)
- Provides a VPN service with your device as the exit node
- Detected because of spamming activity from users' devices
- Personal devices used as exit nodes
- When a service is free, you are the product

Malware in Play Store





https://home.cern/news/news/computing/computer-security-when-apps-lead-mishaps

https://www.schneier.com/blog/archives/2020/05/malware_in_goog_1.html

...and also in web extensions

The malicious code is:

```
<script async="" src="//[redacted]21db1c5c8b372aecca.js" type="text/javascript"></script><script src="https://[redacted]/optout/set/lat?
jsonp=__mtz_cb_528816334&amp;key=21db1c5c8b372aecca&amp;cv=1580407174&amp;t=1580407173759" type="text/javascript"></script><script src="https://[redacted]net/optout/set/lt?
jsonp=__mtz_cb_339507639&amp;key=21db1c5c8b372aecca&amp;cv=187590&amp;t=1580407173759" type="text/javascript"></script></div></div></div>
```

The JavaScript in question is flagged as malicious by 7 AV products on VirusTotal: https://www.virustotal.com/gui/url/c367c485578f06afa64c5154e8d87c79c31f9d3ee8cdade9a4955d9a3cd7265c/detection

Data leaks in 2020*

*according to HaveIBeenPwned

Jan: BtoBet, HtcMania, Mathway, Ulmon, Wishbone, Zoosk

Feb: AnimeGame, Covve, Slickwraps, Straffic, Tamodo, TrueFire

Mar: Catho, Chatbooks, Lead Hunter, 집꾸미기

Apr: Aptoide, OGUsers, Tokopedia, Vianet

May: Nulled.ch

Jun: ProctorU, Promo, Scentbird, Swvl, Vakinha, Wattpad

Jul: Drizly, Utah gun exchange, Wizishop

Aug: Experian, Unico Campania

Over 500 million credentials were exposed in total (incl. hashed passwords)!

Wattpad alone leaked 268 million credentials.

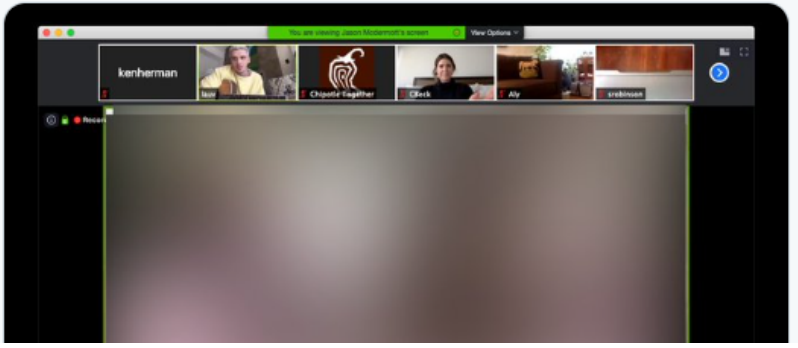
Data leaks cont.

- 31 CERN and associated non-CERN users were notified in relation to Ulmon, Artsy and LiveJournal leaks
- A collection of other leaks analyzed by CERN's Security Team in April resulted in alerts to 43 CERN and 83 partnering institutes' users
- Millions of other e-mails and passwords processed, several users notified, new ones received daily
- Contact us if you want to be included in future alerts!

Zoom: Meet unexpected new friends

Okay so someone started screensharing extremely graphic porn during the Lauv and Chipotle + Zoom hangout and it abruptly ended lol. Maybe these platforms need to be thoroughly tested first?

blurred for obvious reasons



Normally I log in to cern zoom, it takes me here and I click 'schedule a meeting'.

then I copy the link of the new meeting and send it to the participants.

The meetings I set up never have a password

So what did this person get into?

Protect your meetings with a password!

... but don't put the password on a public page for everyone to see

You can also use the "waiting room" feature to approve attendees!

Tour of vulns, 2020 edition

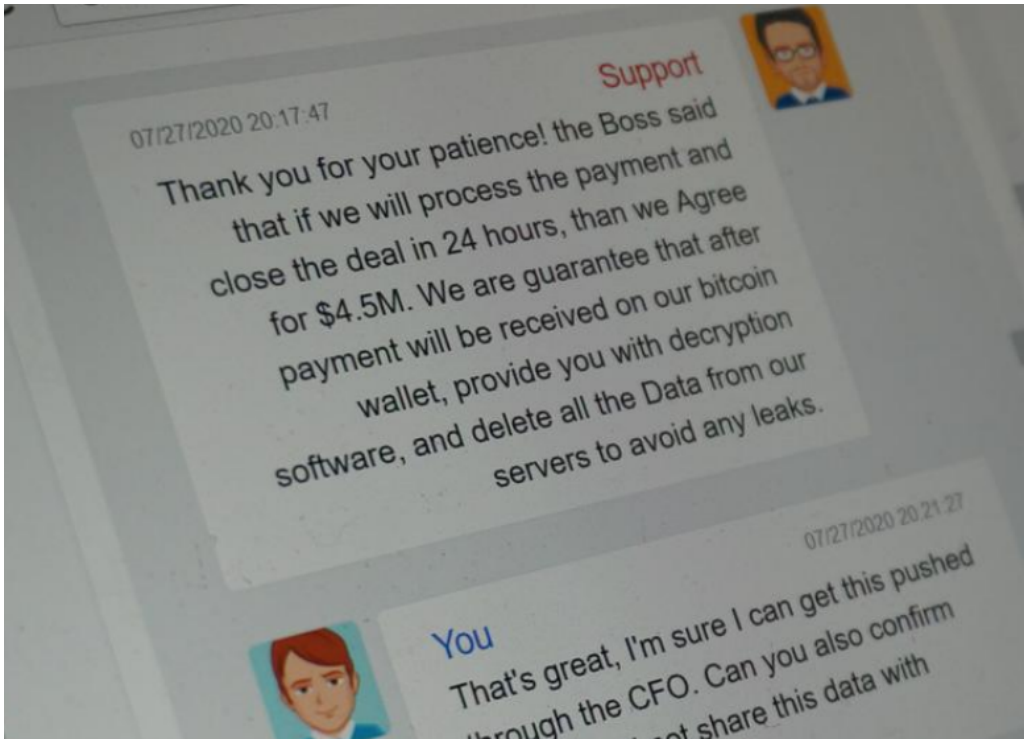
> *WordPress and Apache Struts account for 55% of all weaponized vulnerabilities since 2010, with Drupal coming in third*
>
> https://www.zdnet.com/article/wordpress-and-apache-struts-account-for-55-of-all-weaponized-vulnerabilities/

- critical vulnerabilities in "Popup Builder" and "ThemeREX" WordPress plugins
- critical flaw in "File Manager" plugin affecting >350,000 WordPress sites
- 10-year-old phpmyadmin exploit was abused on a CERN website to perform DDoS attacks as part of a botnet
- "Ghostserv" vulnerability on Tomcat's Jserv protocol can lead to RCE
- SLC6 end-of-life is next month! Service managers should migrate to CentOS7 or preferably CentOS8

Tour of vulns 2020: Windows' corner

- CVE-2020-0601: Elliptic-curve certificates could be spoofed to sign malicious executables or conduct MITM attacks
- CVE-2020-0609, CVE-2020-0610, CVE-2020-0611: RDP clients and servers vulnerable to low (or no) interaction RCE
- CVE-2020-0796: Wormable SMBv3 vulnerability in Windows 10
- CVE-2020-1472: Connect to your Domain Controller over Netlogon Remote Protocol, gain admin privileges!
- CVE 2020-13699: TeamViewer versions 8 - 15 could be launched by a malicious website, causing it to pass NTLM hashes
- Windows 7 reached end of life in January: no support, no security fixes, upgrade to Windows 10 if you haven't already!

Ransomware



https://www.reuters.com/article/us-cyber-cwt-ransom/payment-sent-travel-giant-cwt-pays-4-5-million-ransom-to-cyber-criminals-idUSKCN24W25W

Ransomware

- In 2020 there's 7 times as many ransomware attacks as last year
- According to a presentation by the FBI, 144 million dollars have been paid in ransoms before 2020
- Some try to DDoS victims or expose personal information to force them to continue ransom negotiations
- RDP is the primary vector of attack: whether through insecure credentials or unpatched services, over 50% of ransomware attacks began with an RDP logon
- (Spear-)phishing comes second, at just over 25% of attacks
- More than half of the victims pay up, to the point the U.S. treasury is threatening with sanctions against paying
- It can happen to you, and you should be ready: have detection in place, keep backups, patch up
- Have a plan for recovery

HPC attacks

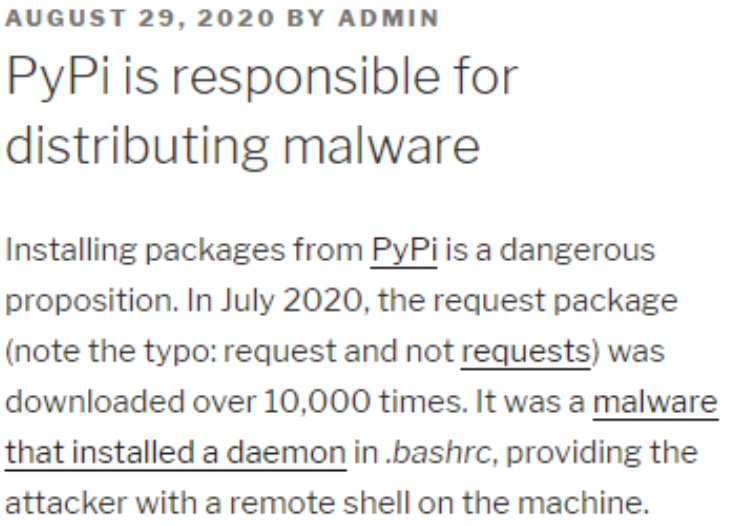
In May 2020, multiple academic High Performance Computing centers were taken offline in the aftermath of a cyber-attack.

- Attackers gained access by using compromised SSH private keys to login, and then escalating privileges using other vulnerabilities
- A SUID binary that launches bash was found at /etc/fonts/.fonts, as well as a log cleaner at /etc/fonts/.low

- Protect your SSH private keys with a strong passphrase!
- You can add a "from" clause to the authorized_keys file to allow connections only from specific hosts

https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH-Security-Report-2020-03.pdf

Software library verification



AUGUST 29, 2020 BY ADMIN

PyPi is responsible for distributing malware

Installing packages from PyPi is a dangerous proposition. In July 2020, the request package (note the typo: request and not requests) was downloaded over 10,000 times. It was a malware that installed a daemon in *.bashrc*, providing the attacker with a remote shell on the machine.

Are you using Python module 'SSH Decorator'? Newer versions include a backdoor

May 9, 2018 By Pierluigi Paganini

A Ruby software package that contained a malicious backdoor has been removed from the Ruby Gems repository after compromising over ten libraries.

Called *rest-client*, the gem was designed to help Ruby developers send REST requests to their web apps and is highly popular, with over 113 million downloads on rubygems.org.

- 78% of vulnerabilities are found in transitive dependencies
- > 30 vulnerabilities in 10 most popular Docker images
- **Solution**: centralized curation of software libraries and images, scanning of dependencies files

Pinned Tweet

Elon Musk
@elonmusk

Thank you! Questions?

09:15 AM · Oct 13, 2020 · Twitter for iPhone