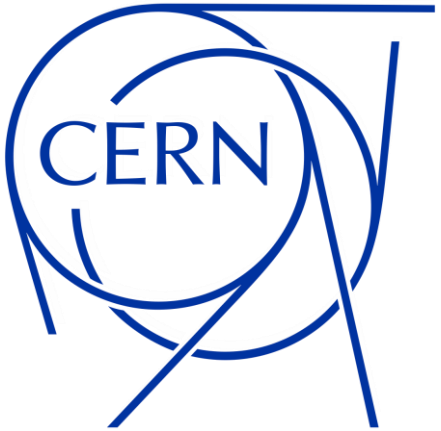


Computer Security Update

Roman Sumailov

roman.sumailov[@]cern.ch

CERN Computer Security Team

HEPiX Spring 2024, 17.04.2024

Content

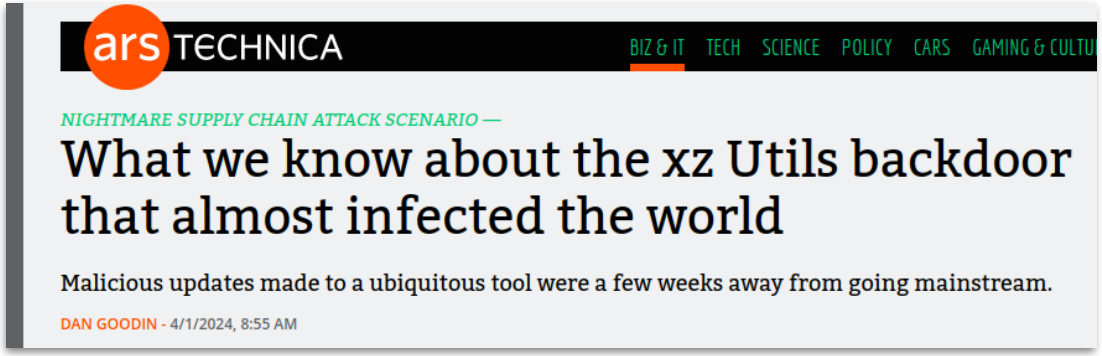
1. Supply-chain problems
2. Phishing for 2FA → Less secure & more secure 2FA
3. Email security
4. R&E community security

Content

1. **Supply-chain problems**
2. Phishing for 2FA → 2FA
3. Email security
4. R&E community security

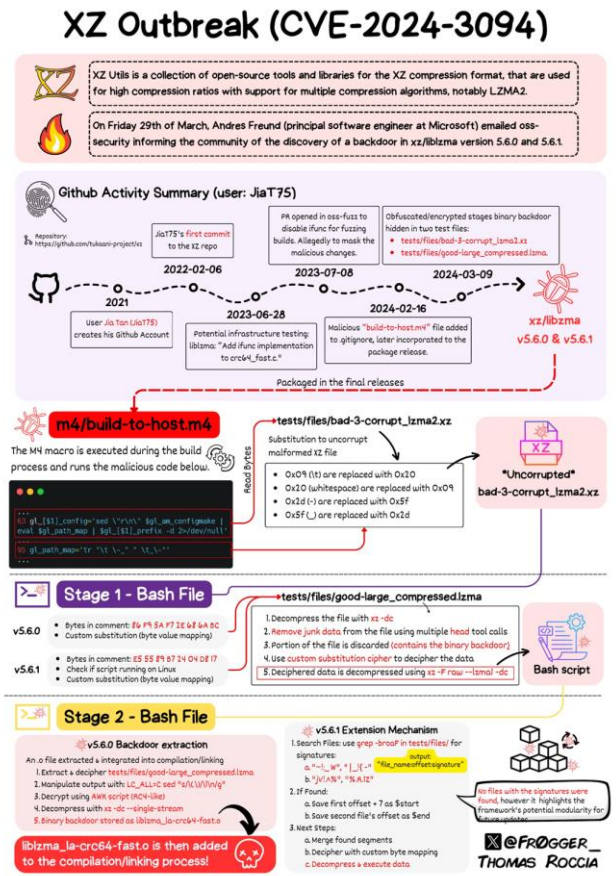
Less secure & more secure

xz-utils (CVE-2024-3094)



- Is an open source data-compression utility available almost in every Linux distro (.deb, .rpm…)
- Exploitable under certain conditions:
  - Sophistically backdoored versions 5.6.0 & 5.6.1
  - Distro needs to run *glibc*
  - More conditions for backdoor to run
  - Rolling-release distros are vulnerable
- Backdoor discovered on the March 29th
- Took at least 3 years to prepare with social engineering

"In a nutshell, it allows someone with the right private key to hijack sshd, the executable file responsible for making SSH connections, and from there to execute malicious commands."



https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/
https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27
https://www.sentinelone.com/blog/xz-utils-backdoor-threat-actor-planned-to-inject-further-vulnerabilities/
https://tukaani.org/xz-backdoor/

PyPI and typosquatting – still a thing

- Always had problems with malicious packages
- In the last campaign 500 malicious packages uploaded to PyPI posing as legitimate popular tools (March 2024)
- One account per one malicious package

Typosquatting campaign, malicious packages slam PyPI

Threat actors used automated typosquatting attacks to lead victims to malicious python packages in yet another campaign targeting the open-source software supply chain.

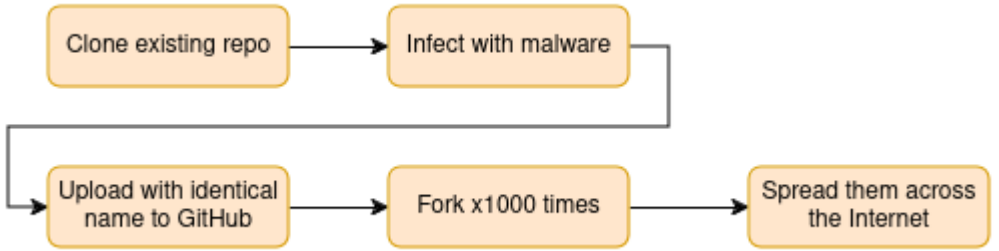
By **Alexander Culafi,** Senior News Writer

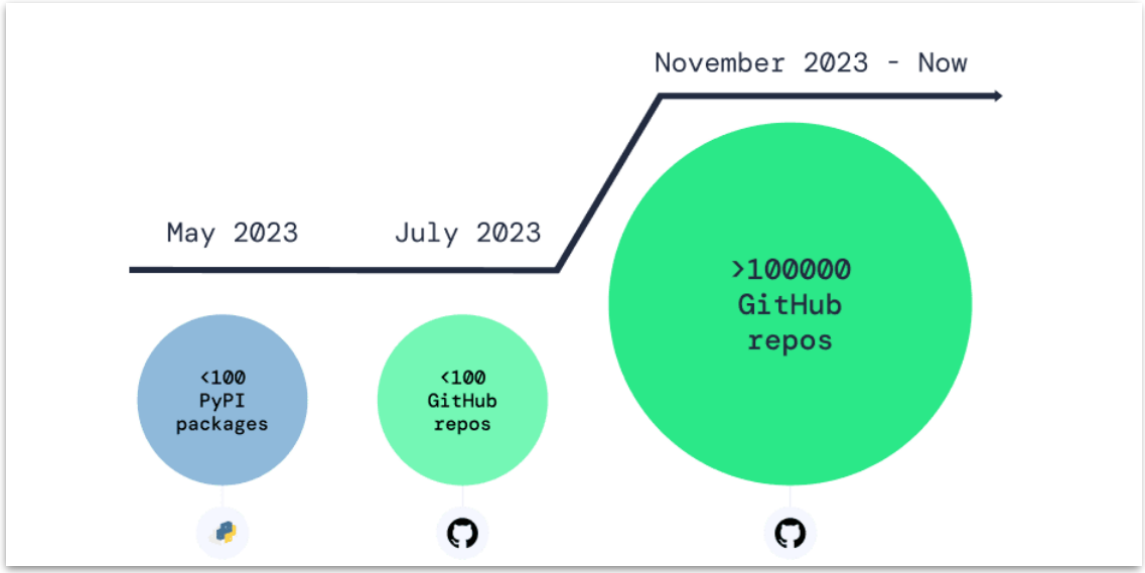
Published: **29 Mar 2024**

https://blog.dachary.org/2020/08/29/pypi-is-responsible-for-distributing-malware/
https://www.techtarget.com/searchsecurity/news/366577455/Typosquatting-campaign-malicious-packages-slam-PyPi

Malicious GitHub repositories

- Over 100k infected repositories (discovered Feb 2024)
- Repository confusion attack that relies on human error



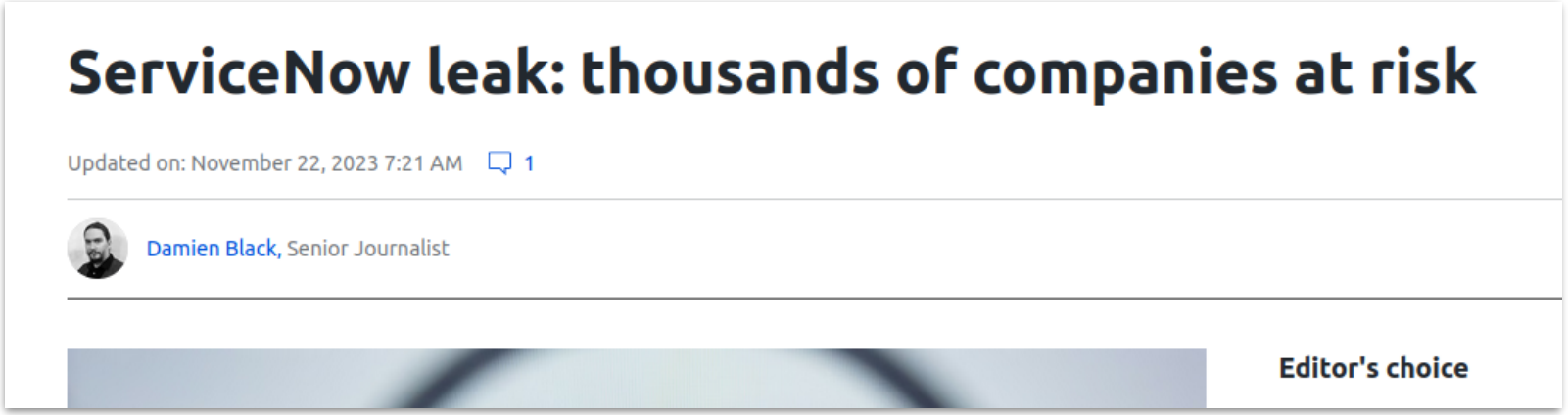


https://www.developer-tech.com/news/2024/feb/29/github-suffers-over-100k-infected-repos/

Commercial suppliers

servicenow®

- Vulnerability existing since 2015
- Allows unauthenticated users to access confidential records
- ServiceNow was given by researcher 6 months to react
- Vulnerability published in Oct 2023
- ServiceNow did not deny/confirm or warn customers (CERN was not warned either)



https://www.enumerated.ie/index/servicenow-data-exposure
https://cybernews.com/news/servicenow-leak-thousands-companies-risk/

Solutions

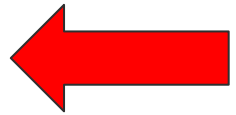
- As usual – no silver bullet, but things like SBOM (Software Bill of Materials) can help
- SBOM is a document providing list of libraries and dependencies used in a project

https://scribesecurity.com/fr/sbom/#definition-of-software-bill-of-materials

https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF?utm_source=the+new+stack&utm_medium=referral&utm_content=inline-mention&utm_campaign=tns+platform

Content

1. Supply-chain problems
2. **Phishing for 2FA → Less secure & more secure 2FA**
3. Email security
4. R&E community security



Two-Factor Authentication – SMS confirmation phishing

- If possible, better to have 2FA as something tied to device, something you HAVE (TOTP, WebAuthn like Yubikey)
- SMS codes are phished for
- CERN users were phished for WhatsApp confirmation 2FA SMS codes

To: service-desk@cern.ch
Subject: Message from Microsoft

Good morning

in the last few days I am getting regularly an SMS from Microsoft

xxxxxx als Sicherheitscode fuer das Microsoft-Konto verwenden

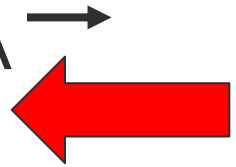
where xxxxxx is a 6 digit code that I should use to access my Microsoft account.

The fact, is that I am not trying to use my Microsoft account except for the Outlook mails which I can in any case access without problems.

Do you have any idea why am I receiving this SMS and how can this be stopped?

Content

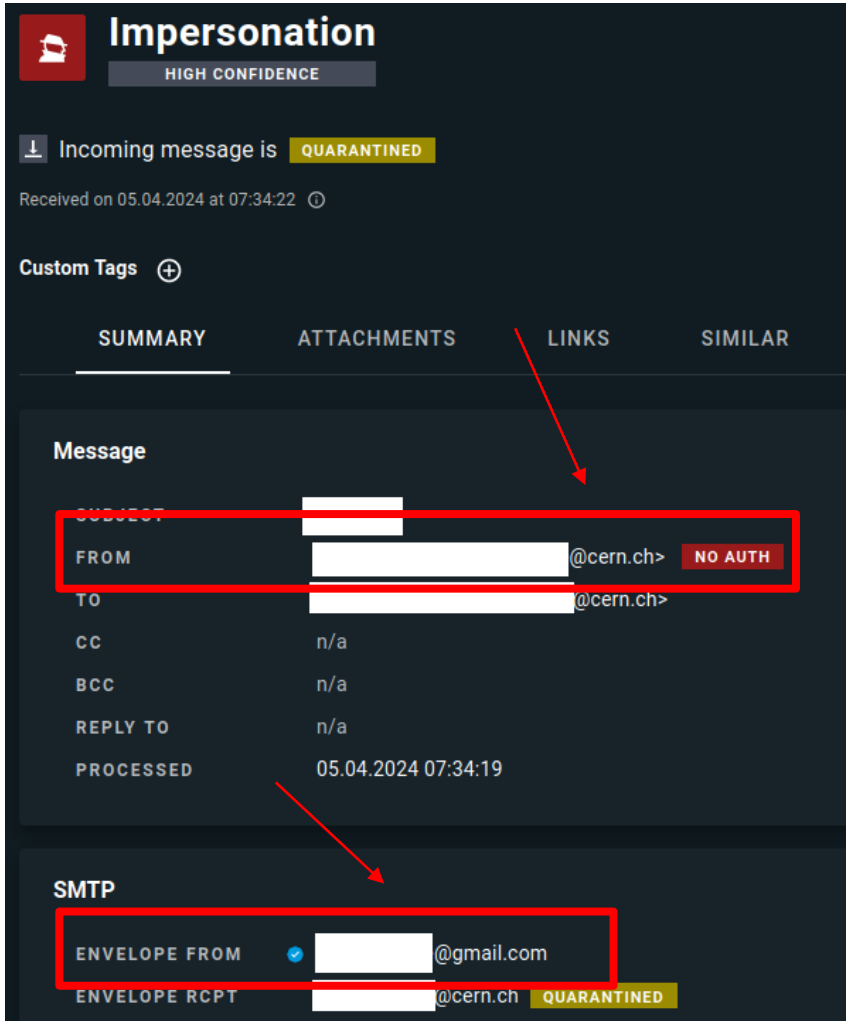
1. Supply-chain problems
2. Phishing for 2FA
   2FA
3. **Email security**
4. R&E community security



Less secure & more secure

Email security DMARC/DKIM/SPF

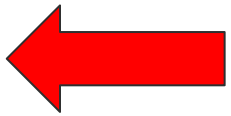
- DMARC – Domain-based Message Authentication, Reporting & Conformance - Policy that ties together two emails authentication protocols SPF and DKIM
- CERN enforced DMARC in 2023
- Google & Yahoo enforcing DMARC since Feb 2024 so most admins must adjust
- DMARC enforcement caused lots of problems for users mostly due to spoofing:
    a. Users spoofing themselves via 3rd party, i.e gmail
    b. Many problems come due to personal use of professional emails
    c. Forwarding sometimes makes email auth impossible (breaking DKIM signature, failing SPF)
    d. Mailing lists spoofing senders



https://www.proofpoint.com/us/blog/email-and-cloud-threats/google-and-yahoo-set-new-email-authentication-requirements

Content

1. Supply-chain problems
2. Phishing for 2FA → Less secure & more secure 2FA
3. Email security
4. **R&E community security**



Tier-3 compromise in Asia (summer 2023)

- Account was discovered scanning CERN servers
- Turned out compromised account at Tier-3 site
- Attacker performed lateral movement infecting other servers in Tier-3

Tier-3 compromise in Asia (summer 2023)

- Servers were lacking updates ‘***yum***
- ‘***pkexec***’ exploit was used to e
- Site had to reinsta

MULTI-FACTOR AUTHENTICATION

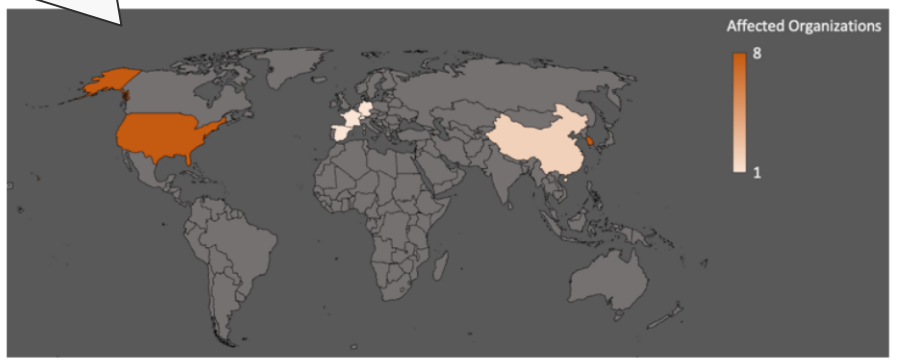
MICI-BICA case (summer 2023)

- 200+ servers compromise[illegible] impact[illegible] organisations
- Infected hosts botnetted/us[illegible]
- Operating for 3 [illegible]
- Directed at Resear[illegible]
- Initial access:
  - Passw[illegible] against u[illegible]
  - Credential stu[illegible] account to a[illegible]
- TTP old & not s[illegible]
  - IRC for bot control, b[illegible]pting[illegible] malware orchestration
  - Vanilla bruteforce SSH scanners, open source cryptominers…

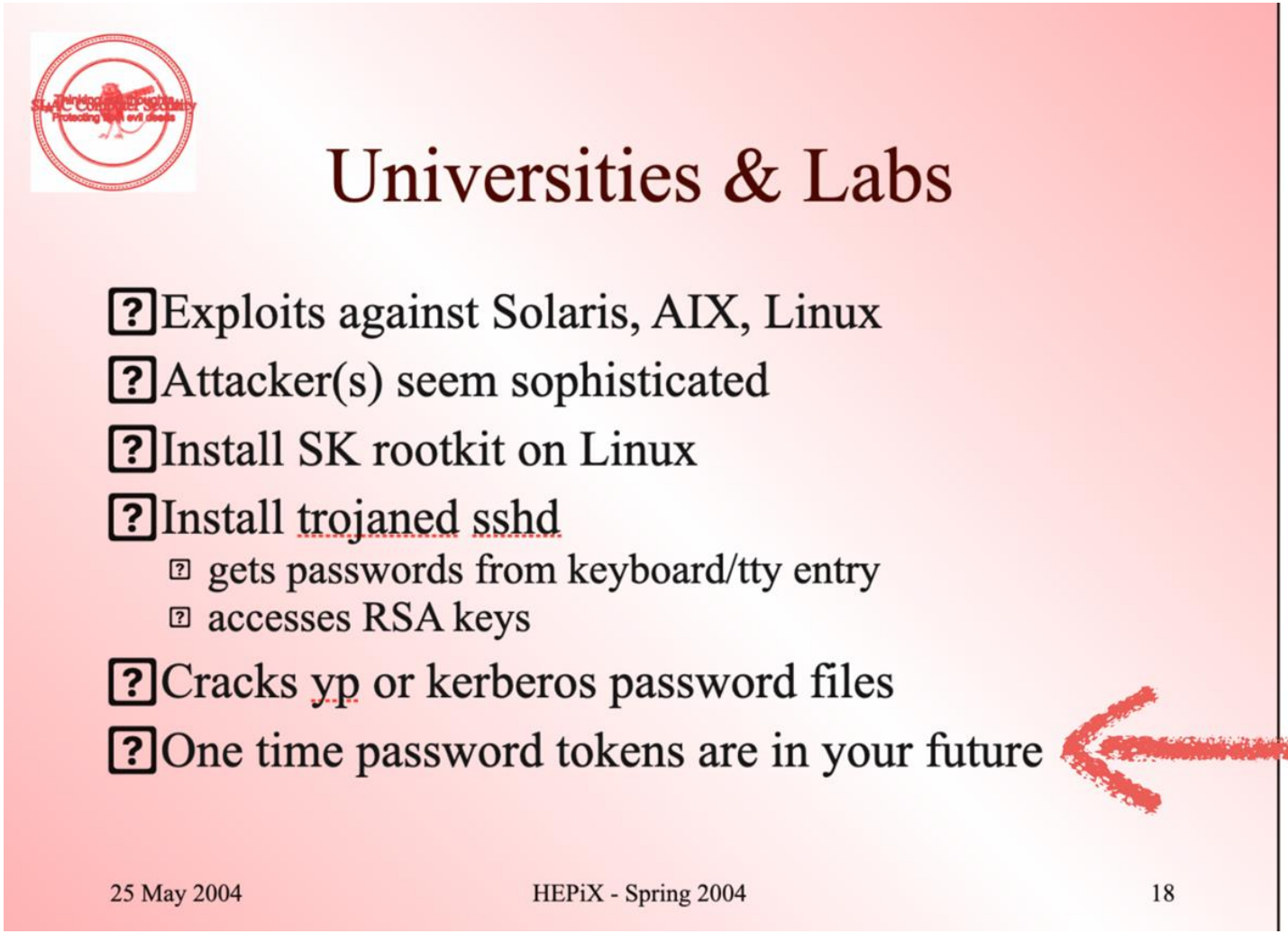
MULTI-FACTOR AUTHENTICATION

[illegible]arch & Education

Affected Organizations	Infected Hosts
	110
	34
	17
	14
8	8
	5
e 1	1



20 years later we talk about 2FA…



(Credits:
Bob Cowles)

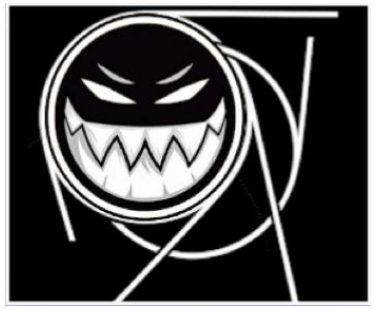
17

Collaboration in R&E

- SAFER – Security Assistance For Education & Research Trust Group
- SICURA-LAC – Collaboration with 2000+ South American universities for cybersecurity initiatives
- WLCG SOC Working Group – Cooperation to establish SOC building guidelines for WLCG sites
- REN-ISAC – Cybersecurity collaboration for five-eyes
- EGI – Computing security for EGI infrastructure (Europe)
- China IHEP security
- pDNSSOC
- Cooperation with French hospitals cybersecurity teams

https://safer-trust.org/

Merci beaucoup !



home.cern