COMPUTER SECURITY UPDATE

LIVIU VÂLSAN
FOR THE CERN COMPUTER SECURITY TEAM

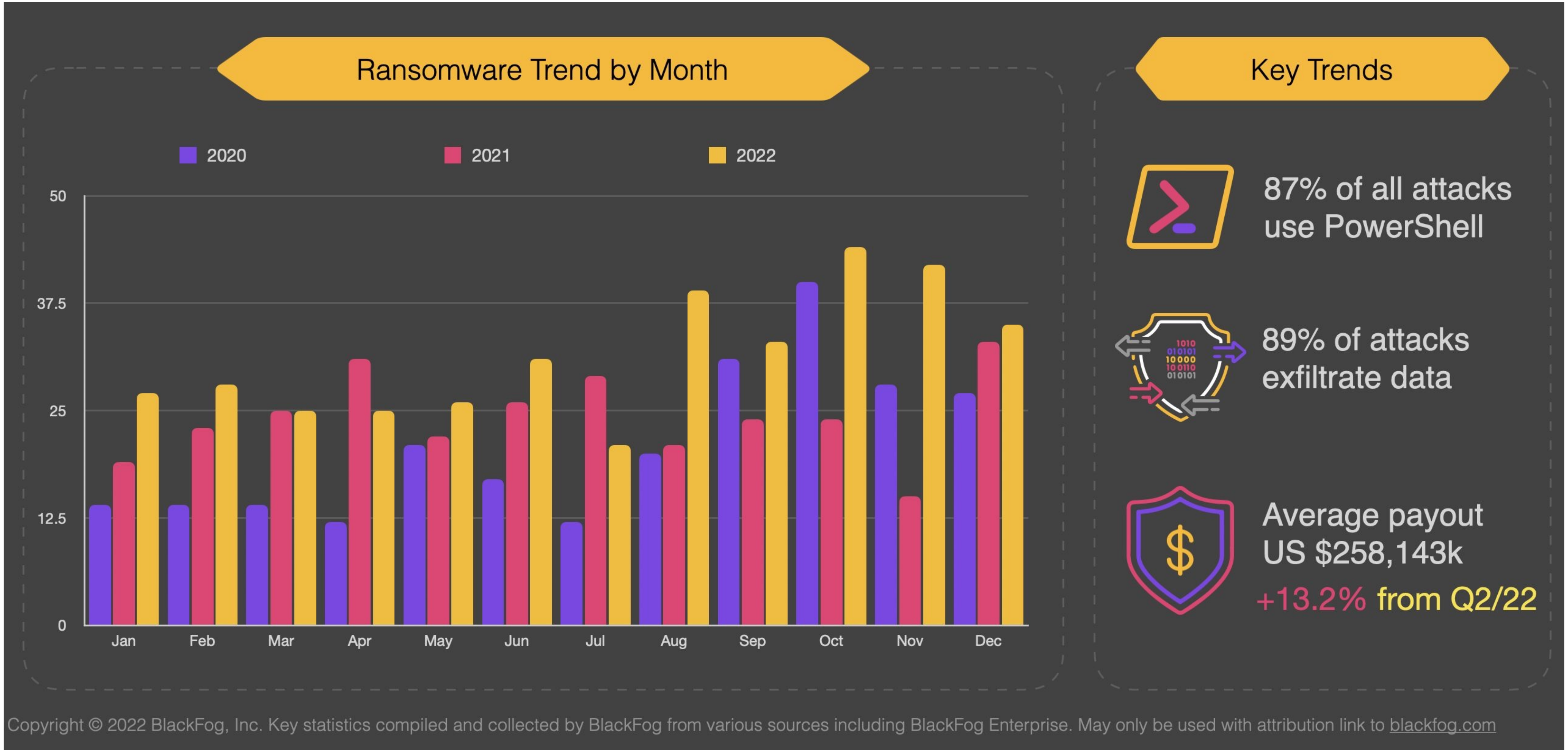
HEPIX SPRING 2023 ONLINE WORKSHOP

AGENDA

- Ransomware trends
- Recent vulnerabilities
- Cloud security
- Authentication / session security
- Credential leaks / code security testing
- Key takeaways

Ransomware Trends

RANSOMWARE TRENDS IN 2022



Ransomware Trend by Month

Key Trends

87% of all attacks use PowerShell

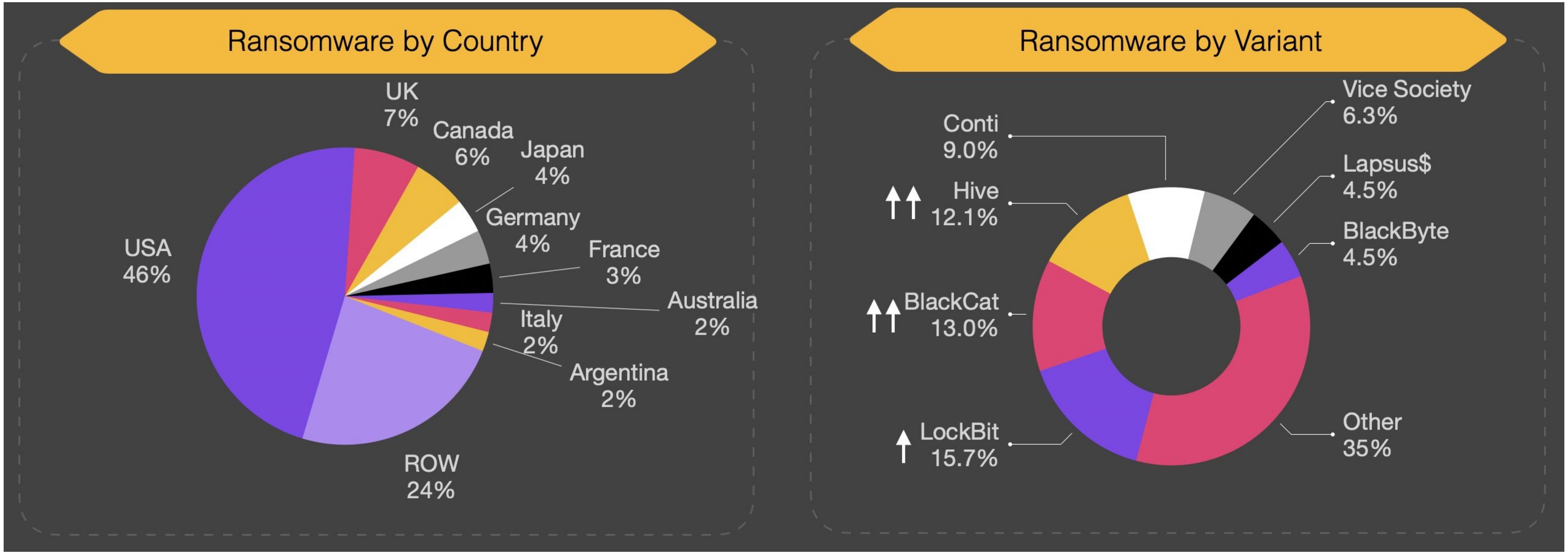
89% of attacks exfiltrate data

Average payout US $258,143k

+13.2% from Q2/22

Source: https://www.blackfog.com/the-state-of-ransomware-in-2022/

RANSOMWARE TRENDS IN 2022

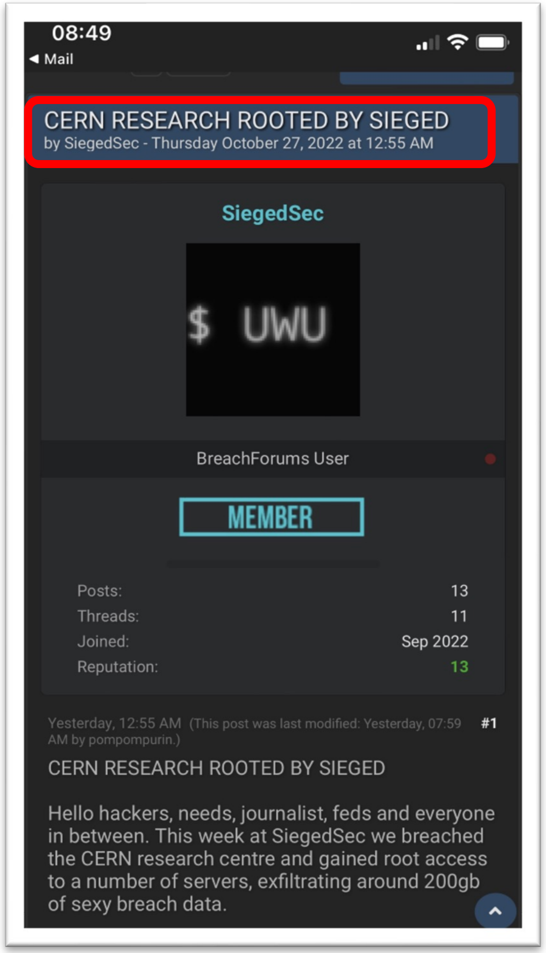


Source: https://www.blackfog.com/the-state-of-ransomware-in-2022/

RANSOMWARE TTP

- Start by compromising accounts (either through phishing or by purchasing from initial access brokers)
- Use compromised accounts to connect to VPN
- Connect to VDI infrastructure or internal PCs
- Downloads and deploy a collection of Powershell scripts to move laterally and escalate privileges
- Gain domain admin
- Exfiltrate data
- Deploy ransomware
- Hope to be paid

CERN "DATA LEAK"



08:49

◀ Mail

CERN RESEARCH ROOTED BY SIEGED

by SiegedSec - Thursday October 27, 2022 at 12:55 AM

SiegedSec

BreachForums User

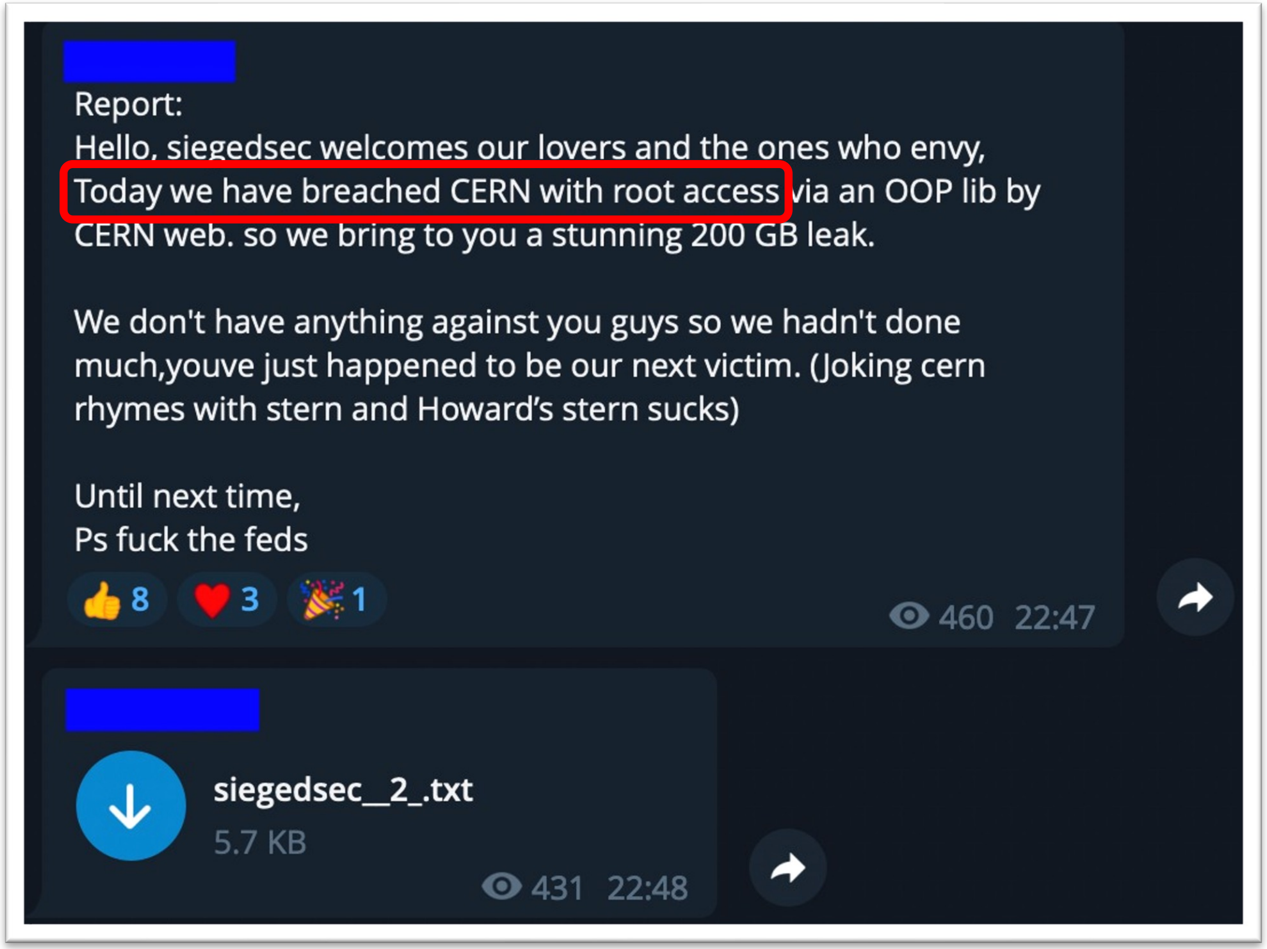
MEMBER

Posts:	13
Threads:	11
Joined:	Sep 2022
Reputation:	13

Yesterday, 12:55 AM (This post was last modified: Yesterday, 07:59 AM by pompompurin.) #1

CERN RESEARCH ROOTED BY SIEGED

Hello hackers, needs, journalist, feds and everyone in between. This week at SiegedSec we breached the CERN research centre and gained root access to a number of servers, exfiltrating around 200gb of sexy breach data.



[redacted]

Report:
Hello, siegedsec welcomes our lovers and the ones who envy,
Today we have breached CERN with root access via an OOP lib by CERN web. so we bring to you a stunning 200 GB leak.

We don't have anything against you guys so we hadn't done much,youve just happened to be our next victim. (Joking cern rhymes with stern and Howard's stern sucks)

Until next time,
Ps fuck the feds

👍 8 ❤️ 3 🎉 1 👁 460 22:47

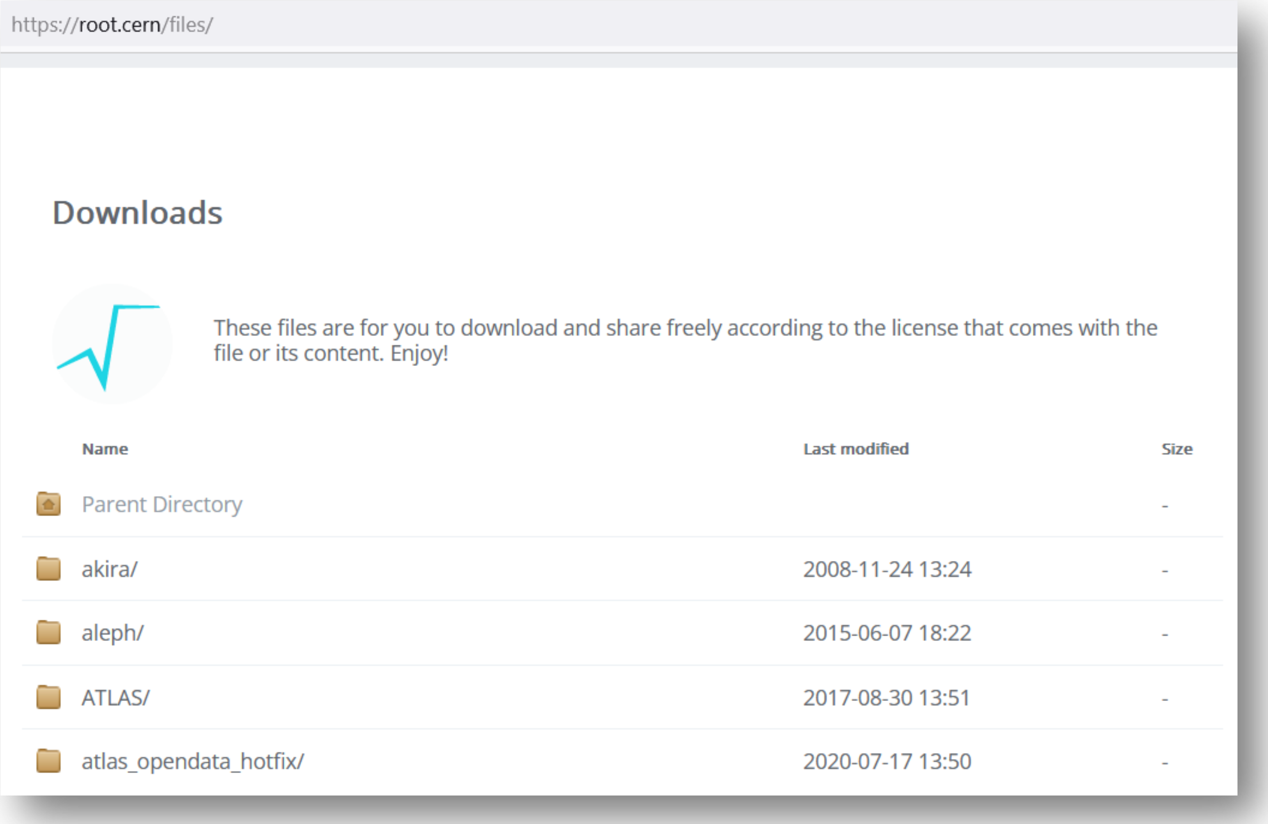
[redacted]

siegedsec_2_.txt

5.7 KB

👁 431 22:48

CERN "DATA LEAK"



https://root.cern/files/

Downloads

These files are for you to download and share freely according to the license that comes with the file or its content. Enjoy!

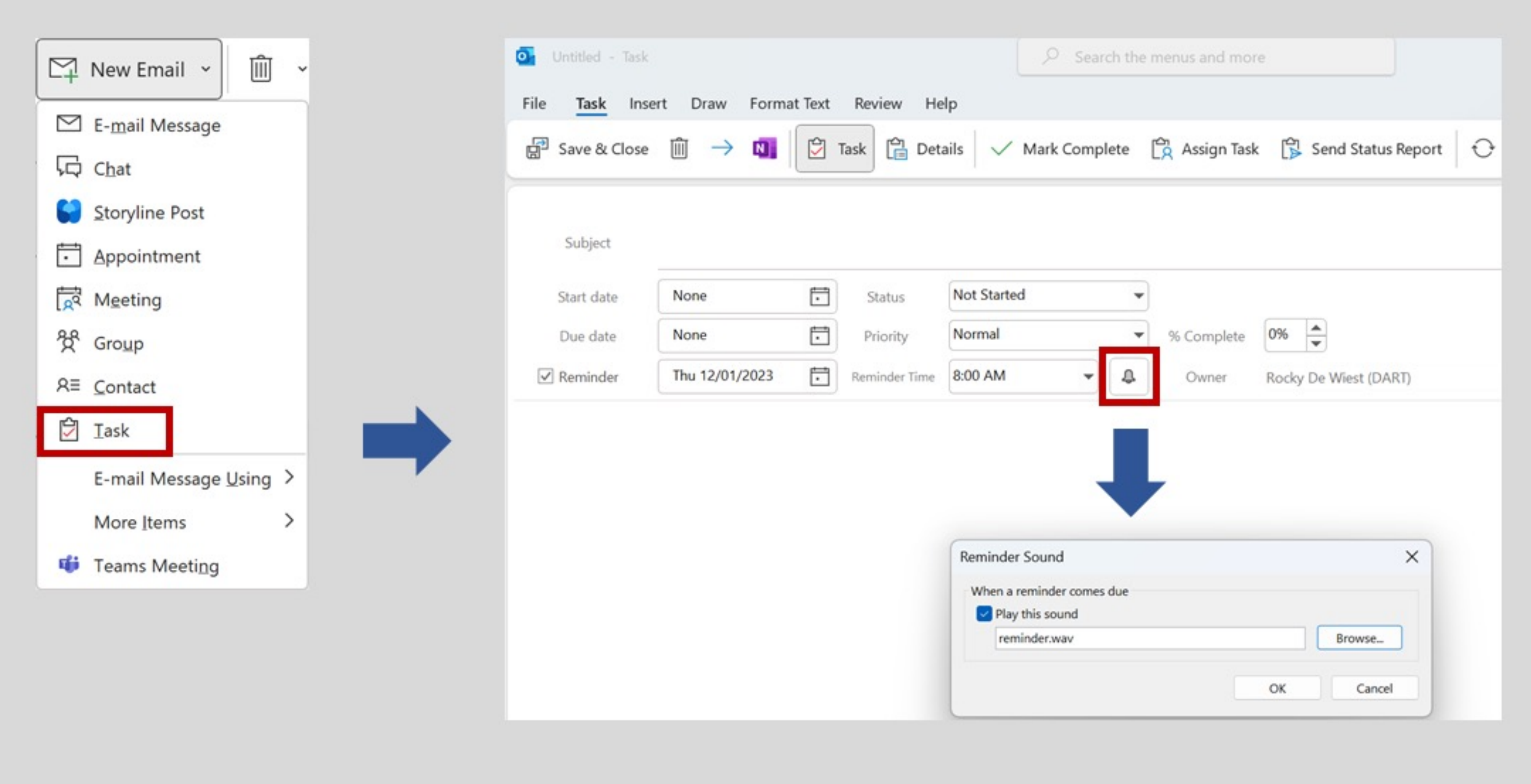
Name	Last modified	Size
Parent Directory		-
akira/	2008-11-24 13:24	-
aleph/	2015-06-07 18:22	-
ATLAS/	2017-08-30 13:51	-
atlas_opendata_hotfix/	2020-07-17 13:50	-

Security Vulnerabilities

MICROSOFT OUTLOOK VULNERABILITY CVE-2023-23397

- Critical vulnerability in Microsoft Outlook on Windows
- Exploited by delivering a specially crafted message to a user
    - Set the `PidLidReminderFileParameter` property to a path on a threat actor-controlled server via SMB (TCP port 445)
    - Leads to Net-NTLMv2 hash leak to threat actor-controlled servers
        - No user interaction needed
        - Leaked Net-NTLMv2 hash used either to relay for authentication against other systems that support NTLMv2 authentication or to perform offline cracking to extract the clear text password

MICROSOFT OUTLOOK VULNERABILITY CVE-2023-23397



Subject

Start date: None

Due date: None

☑ Reminder: Thu 12/01/2023

Status: Not Started

Priority: Normal

Reminder Time: 8:00 AM

% Complete: 0%

Owner: Rocky De Wiest (DART)

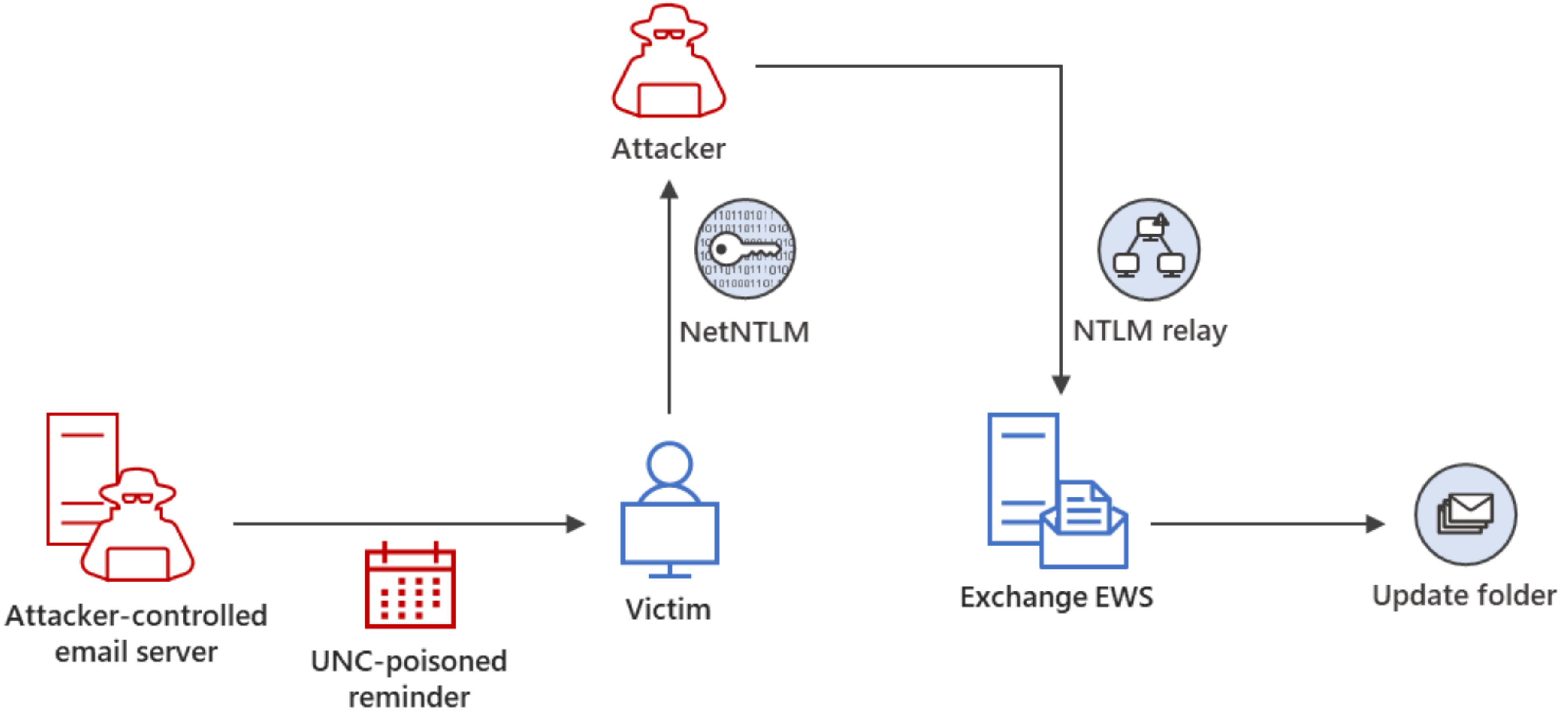
When a reminder comes due

☑ Play this sound

reminder.wav

Source: Microsoft guidance for investigating attacks using CVE-2023-23397

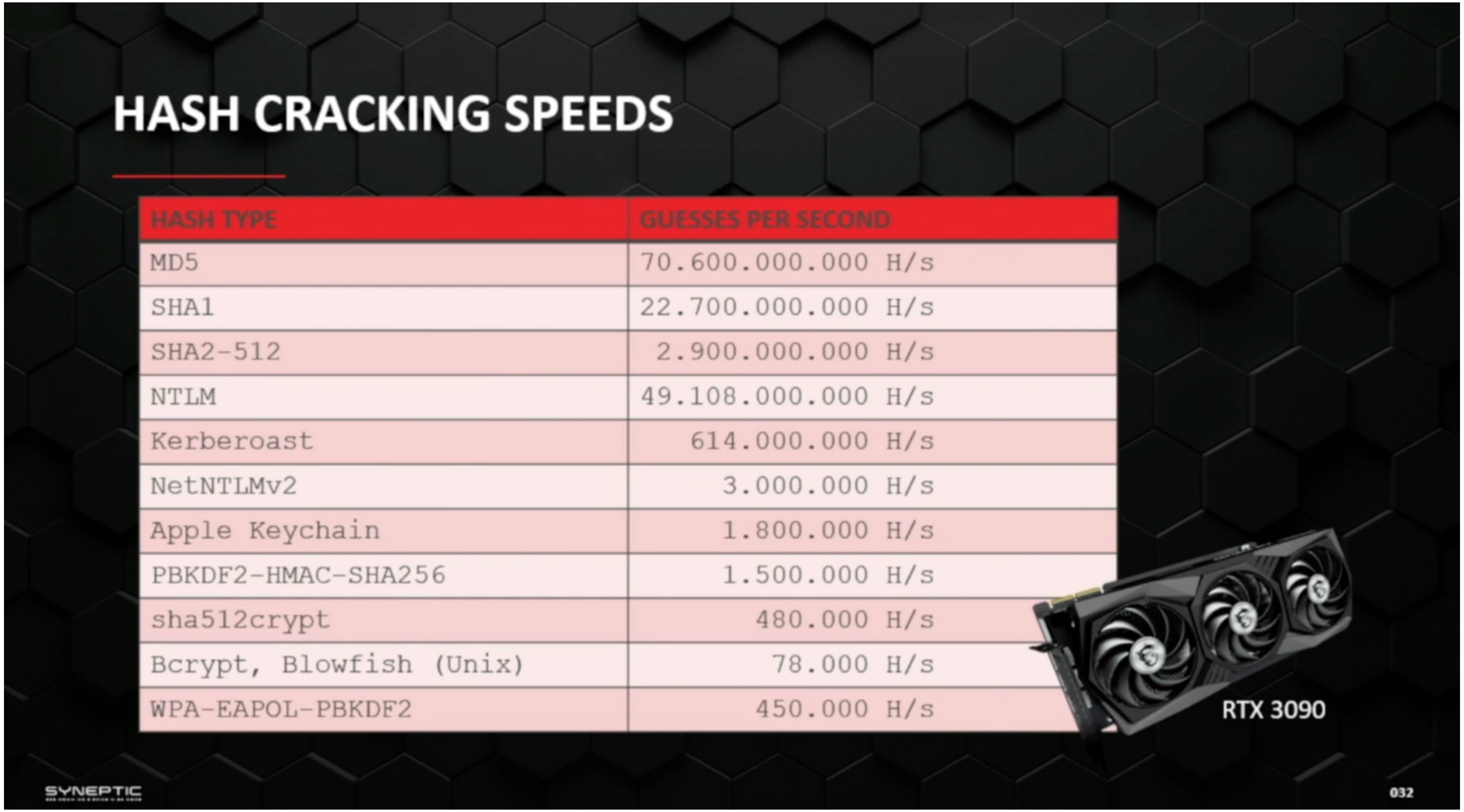
EXPLOITATION



Observed threat actor exploitation of CVE-2023-23397 to gain unauthorized access to Exchange Server and modify mailbox folder permissions for persistent access to the mailbox

Source: Microsoft guidance for investigating attacks using CVE-2023-23397

MICROSOFT OUTLOOK VULNERABILITY CVE-2023-23397



HASH CRACKING SPEEDS

HASH TYPE	GUESSES PER SECOND
MD5	70.600.000.000 H/s
SHA1	22.700.000.000 H/s
SHA2-512	2.900.000.000 H/s
NTLM	49.108.000.000 H/s
Kerberoast	614.000.000 H/s
NetNTLMv2	3.000.000 H/s
Apple Keychain	1.800.000 H/s
PBKDF2-HMAC-SHA256	1.500.000 H/s
sha512crypt	480.000 H/s
Bcrypt, Blowfish (Unix)	78.000 H/s
WPA-EAPOL-PBKDF2	450.000 H/s

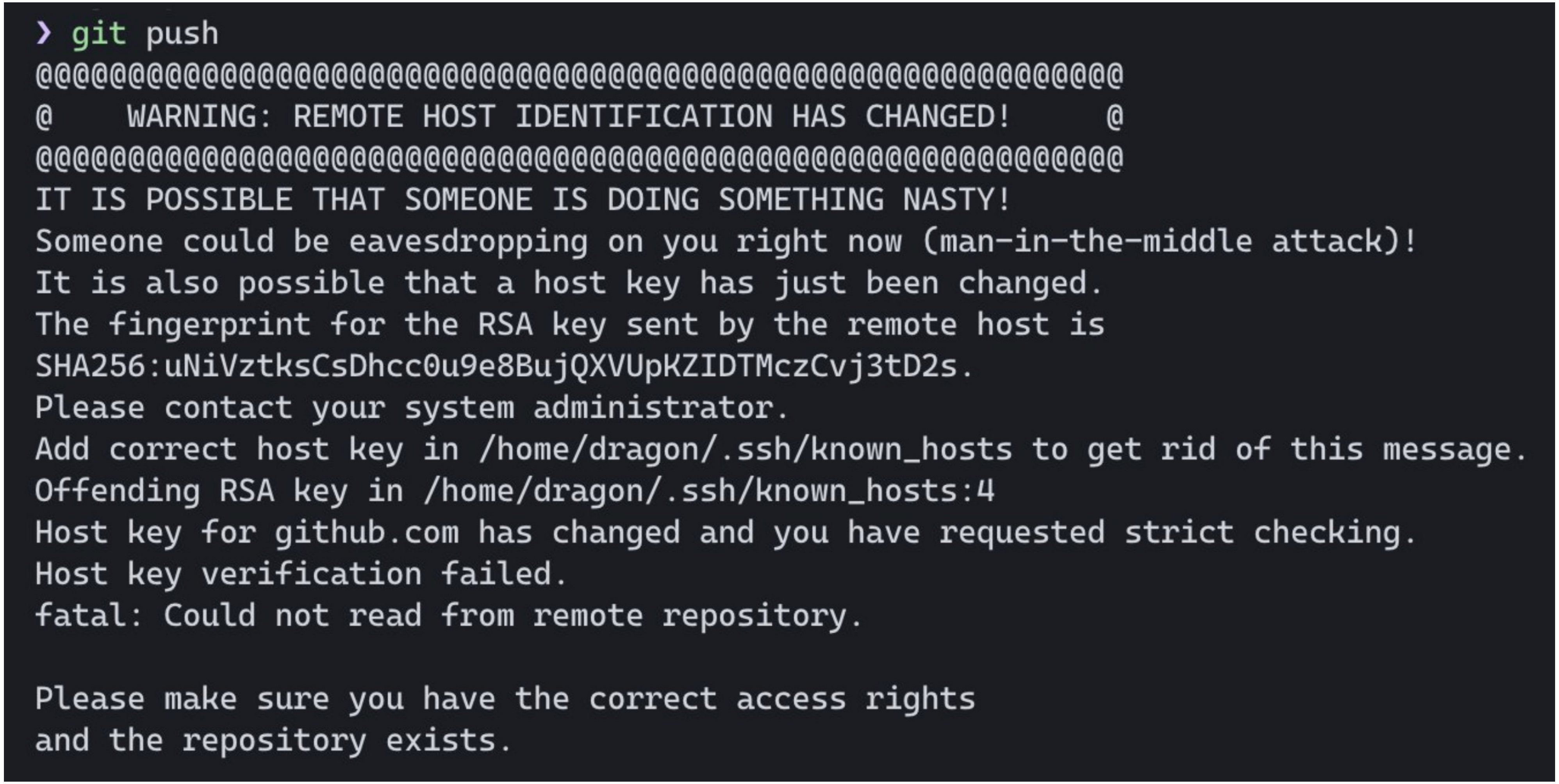
RTX 3090
SYNEPTIC
032

Source: Linus Kvarnhammar Hacked on national television

MITIGATIONS

- Microsoft provided scripts at https://microsoft.github.io/CSS-Exchange/Security/CVE-2023-23397/
  - Works both for Exchange Online and Exchange on-prem
  - Extremely slow to complete
  - Expect some false positives
  - Presents you with results at a specific point in time, will not be able to detect future malicious messages unless you re-run it
- Exchange Online and Exchange on-prem (with March 2023 SU) drop the `PidLidReminderFileParameter` message property when a new message is received.
- Disable outgoing SMB traffic if not already done

CREDENTIALS / SECRETS ACCIDENTAL LEAK



```
❯ git push
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
SHA256:uNiVztksCsDhcc0u9e8BujQXVUpKZIDTMczCvj3tD2s.
Please contact your system administrator.
Add correct host key in /home/dragon/.ssh/known_hosts to get rid of this message.
Offending RSA key in /home/dragon/.ssh/known_hosts:4
Host key for github.com has changed and you have requested strict checking.
Host key verification failed.
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.
```

CREDENTIALS / SECRETS ACCIDENTAL LEAK

- https://github.blog/2023-03-23-we-updated-our-rsa-ssh-host-key/
  - *At approximately 05:00 UTC on March 24, out of an abundance of caution, we replaced our RSA SSH host key used to secure Git operations for GitHub.com.*
  - *We discovered that GitHub.com's RSA SSH private key was briefly exposed in a public GitHub repository.*
- Most code hosting services include built in protections
  - GitLab Auto Secret Detection
  - GitHub Secret Scanning
- While at it, make use of other security tools, e.g.:
  - GitLab Static Application Security Testing (SAST)
  - GitHub Code Scanning
  - GitHub Dependabot

CLOUD SECURITY

- Configure cloud services with security in mind
- Default settings may not always be the most secure ones
- Disable services that you don't need / use in order to reduce your attack surface
- Always check intended behaviour
  - Documentation may be lacking / may make certain assumptions regarding deployment
  - E.g. a password change on AD on-prem doesn't necessarily trigger a revocation of the refresh token in Azure AD
- Follow the principle of least privilege and ensure that ACLs are properly set

AUTHENTICATION / SESSION DURATION

- MFA is the silver bullet in protecting computing accounts
- But MFA it's not of much use in case of device compromise
    - Stealers are commonly exfiltrating browser cookies and passwords stored in the in-browser password manager
- Mitigations:
    - Configure short lived session durations
        - Cloud services prioritise convenience and usually come with very long sessions, e.g. 90 days
    - A password change may not necessarily invalidate session cookies, you may need to force revocation
    - Detection of unusual logins (impossible travel)

CONCLUSIONS AND RECOMMENDATIONS

- Ransomware continues to be a major threat
- Reduce your attack surface as much as possible
  - **Prompt** deployment of **security updates**
  - **Do not** unnecessarily **expose internal services** to the Internet
  - Configure **cloud services** with **security** in mind
  - Configure **automatic code scanning** and detection of secrets
  - **Protect identities** as much as possible

CERN