CYBERARK \ LABS

LastPass

March Office Hours Session

Overview

Goals from this Session

- Intelligently understand the breach.
- What's at Stake? What's their exposure?
    - Corporate or Consumer

What is LastPass

- Password Manager
- Freemium Model with limited functionality.
  - Web Interface
  - Browser Plugins
  - Smart Phone Apps

Security Incident Timeline

(very brief review)

Security Incident Timeline

2011

TLDR: umm...whoops!

May 3rd

- Detected volumetric anomaly in network traffic
- No signs of breach and couldn't determine cause of anomalies.
  - The size of the anomalies made it possible that data such as email addresses, server salt, and salted password hashes could have been copied from the LastPass database.
- LastPass took the "breached" servers offline and requested users to change their master passwords on May 4, 2011.
- There was no direct evidence that customer information was compromised, but LastPass preferred to err on the side of caution.
- The login servers were overwhelmed by user traffic after the password change request, and users were asked to delay changing their passwords until further notice.

Security Incident Timeline

2011 2015

TLDR: ITS OKAY. IT'S ENCRYPTED

June 15

- Detected & stopped suspicious activity on their network.
- Email Addresses, password reminders, server per user salts, and authentication hashes were compromised.
- Encrypted user vault data was not affected.
- LastPass stated that their encryption measures were sufficient to protect the majority of users.
- LastPass strengthened the authentication hash with a random salt and 100,000 rounds of server-side PBKDF2-SHA256 to make it difficult to attack the stolen hashes.

Security Incident Timeline

2011 2015 2016

TLDR: BUGS IN BROWSER EXTENSION

July

- Detectify published a blog post detailing a vulnerability in LastPass that allowed reading plaintext passwords for arbitrary domains from a user's vault.
- The vulnerability was caused by poorly written URL parsing code in the LastPass extension.
- Detectify notified LastPass privately before publicly disclosing the vulnerability.
- LastPass responded by acknowledging the vulnerability and revealing knowledge of an additional vulnerability, discovered by a member of the Google Security Team, that had already been fixed.

Security Incident Timeline

2011 2015 2016 2017

TLDR: TAVIS SAVES LASTPASS

- March 20th - Tavis Ormandy discovered a vulnerability in the LastPass Chrome extension that applied to all clients.
- The vulnerabilities were disabled on March 21 and patched on March 22.
- March 25th - Ormandy discovered another security flaw that allowed remote code execution from a malicious website.
- This vulnerability was also patched.

https://twitter.com/taviso

Security Incident Timeline

TLDR: TAVIS HATES LASTPASS!!!

- In August 2019, Tavis Ormandy reported a vulnerability in the LastPass browser extension that allowed malicious websites to obtain a username and password inserted by the password manager on a previously visited site.
- The vulnerability was limited to the Google Chrome and Opera extensions.
- LastPass publicly announced the vulnerability on September 13, 2019.
- All platforms received the vulnerability patch.

Security Incident Timeline

2011 2015 2016 2017 2019 2020

TLDR: AUDITING SNAFU. NBD.

April 6th, 2020

- Vulnerability was found in LastPass regarding the storage of the master password within the web extension.
- LastPass stored the master password in a local file when the "Remember password" option was activated.
- LastPass did not use the Windows Data Protection API.
- No further information was provided regarding the impact of the vulnerability or whether it was patched.

Security Incident Timeline

2011 2015 2016 2017 2019 2020 2121

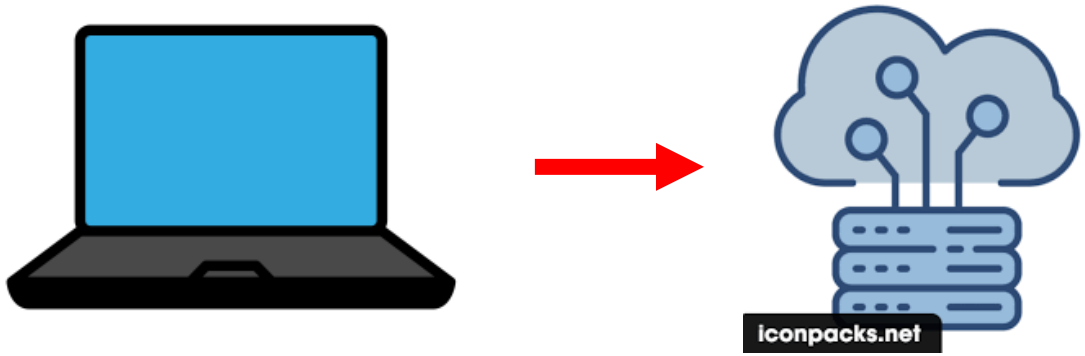
TLDR: LASTPASS IS TRACKING YOU!!!

- February 2021 – Android app contained third-party trackers.
  - AppsFlyer
  - Google Analytics
  - Google CrashLytics
  - Google Firebase Analytics
  - Google Tag Manager
  - MixPanel
  - Segment
- December 2021 – Large Credential Stuffing Attack.
  - Security Email Alert triggered by mistake for warning large number of users that their master passwords were compromised.

Security Incident Timeline

INCIDENT ONE

- Software engineer's corporate laptop was compromised
- Unauthorized threat actor gained access to a cloud-based development environment.
- Source code, technical information, and certain LastPass internal system secrets were stolen.
- No customer data or vault data was taken.
- Incident was declared closed, but the information was later used for second attack.



Incident One

Additional Details

Incident One: Additional Details

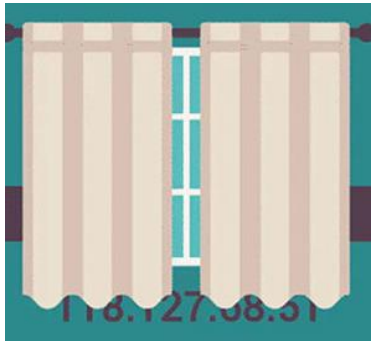
Aug-12-2022:
Suspicious Activity
Detected on non-Prod

Initial threat Vector
Unknown due to Anti-Forensic

MANDIANT

Timeline of Threat
Actor: Aug-08 to Aug-12
on Non-Production

SW Eng. Laptop
Compromised



Hide behind 3rd-Party VPN; Impersonation

Impact: Technical Docs; 14 out of 200 Source Code Repositories

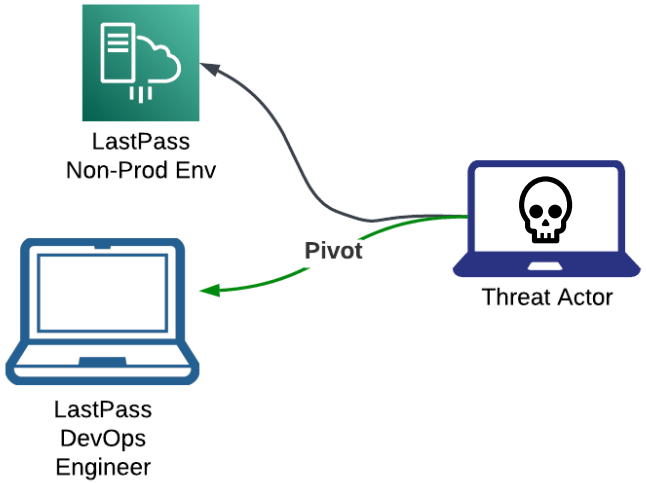
Containment, Eradication & Recovery Actions

- Took possession of the affected software engineer's corporate laptop, performed forensic analysis, replaced the machine with a new device running a different operating system, and deleted and replaced all existing domain credentials.
- Deployed an additional managed EDR solution configured to augment existing security controls of software engineers' laptops.
- preventative and detective security controls on company laptops and enabled additional logging.
- Deployed a Secure Access Service Edge (SASE) solution to manage direct split-tunneled Internet access and began the replacement of VPN access with a Zero Trust Network Access (ZTNA) solution.
- Purchased new hardware authentication devices for software and platform engineering development use cases, including authentication, authorization, and code safety.
- Rotated all LastPass credentials, certificates, and secrets known to have been obtained by the threat actor.
- Updated the upstream managed Web Application Firewall (WAF) service and initiated heightened monitoring for anomalous activity.
- Enabled additional Workload EDR monitoring in development and production and deployed additional container introspection capabilities.
- Deployed a market-leading Cloud Security Posture Management (CSPM) platform to provide additional attack surface visibility, asset, and vulnerability management across the cloud platform.
- Disabled and removed access to the development environment, preserved artifacts for evidence, and ultimately destroyed the environment. Then recreated the entire environment from scratch over a six-week period.
- Deployed updated Kubernetes and Docker configurations in the new development environment, along with additional logging and alerting focused on Cloud Identity and Access Management (IAM) role restrictions.
- Restricted and removed access of engineers/developers to the underlying cloud platform.
- Deployed "canaries" within our production and development environments to augment our intrusion deception and detection capabilities.
- Enabled additional logging in both development and the production environments.
- Engaged a well-known third party to assist with targeted, proactive threat hunting in production environments, in addition to continued engagement with Mandiant for incident response and forensics

Incident Two

Additional Details

Incident TWO: Additional Details



- Pivot from the first attack
- IOCs (Indicators of Compromise
- Different Tactics, Techniques, TTPs

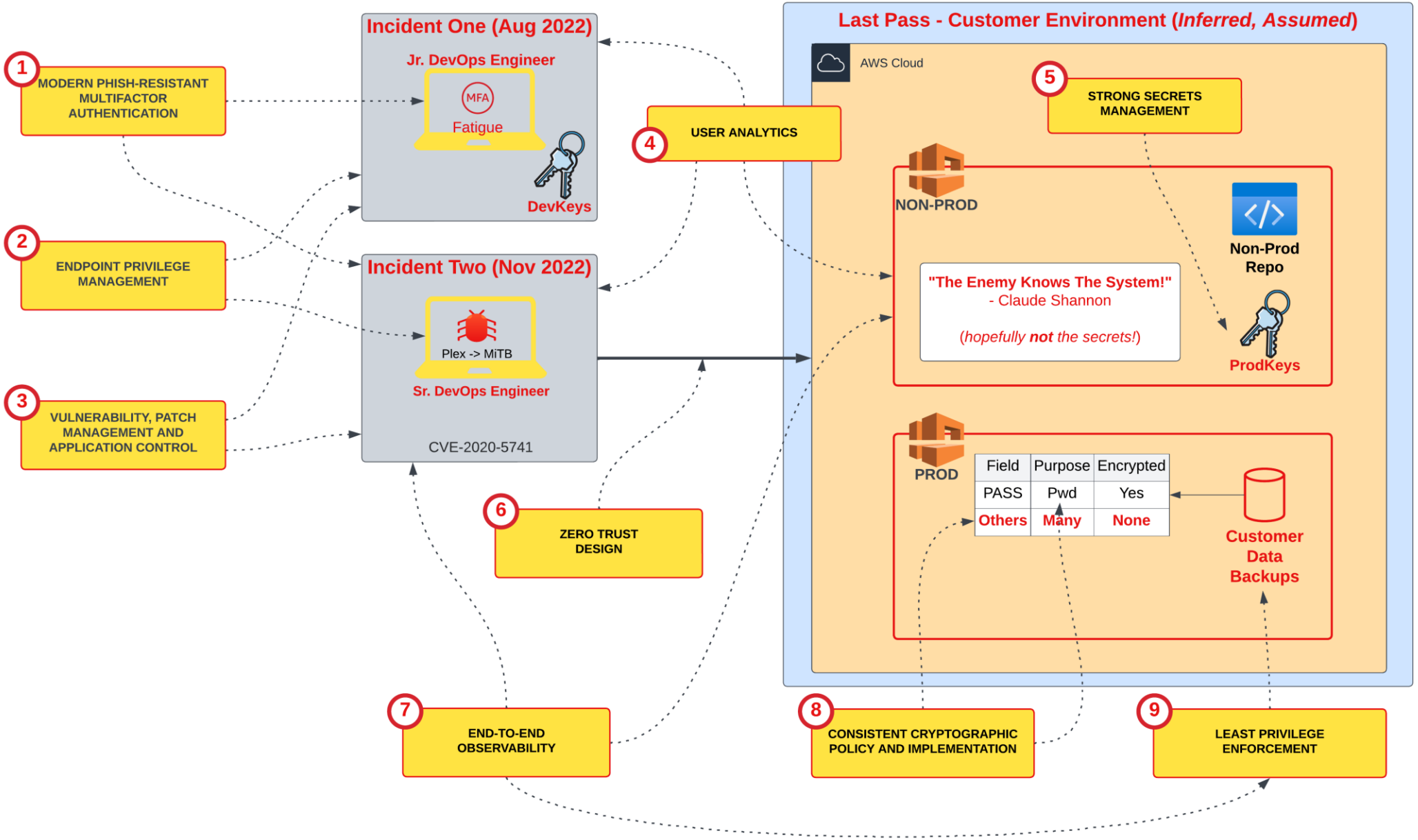
Captured MasterPassword
Gained access to Vault

Amazon GuardDuty

Exported Vault Entries
Then Obtained
Encryption Keys

Decrypt Backup Data
Data Leakage

Take-Aways: **Defense-in-Depth**



Summarizing from a CyberArk Perspective

High Level Control Intention		General Protective, Detective or Responsive Capability
ID	**Description**	**Example**
C01	Phish Resistant MFA	CyberArk Identity + MFA + Security Code (Client Side)
C02	Endpoint Privelege Management	CyberArk Endpoint Privilege Manager (EPM)
C03	Vuln, Patch Management, AppControl	Vendor or Ecosystem Patching
C04	User Analytics	CyberArk Identity with User Behavioral Analytics (UBA)
C05	Strong Secrets Management	CyberArk Conjur
C06	Zero Trust Design	CyberArk Identity + UEM/Conditional Access
C07	End to End Observability	Integrated Logging, Alerting and SOC Playbooks
C08	Consistent Cryptographic Policy	Consistent Application Security Reviews
C09	Least Privilege Enforcement	CyberARK Cloud Entitlements Manager (CEM)

Prevention & Controls

- AWS keys to be managed by PAS
- Limit of access to AWS keys/roles from IP addresses and resources
- Implement MDM/Device control (BYOD)
  - [exploiting a vulnerable third-party media software package on the employee's home computer and implanting keylogger malware]
- Secure notes should not include decryption keys – use Privileged Access Management
- Non-prod included key of production DB backup
- Employee master password (why is there such?) – company level password, password field of old customers encrypted using a low iteration, no enforced password complexity
- CEM to reduce access to be least privileged (access to production backups)
- Access to DB backups- restrict usage of keys/creds

Containment, Eradication & Recovery Actions

- Forensically imaged devices to investigate corporate and personal resources and gather evidence detailing potential threat actor activity.
- Assisted the DevOps Engineer with hardening the security of their home network and personal resources.
- Enabled Microsoft's conditional access PIN-matching multifactor authentication using an upgrade to the Microsoft Authenticator application which became generally available during the incident.
- Rotated critical and high privilege credentials that were known to be available to the threat actor;
  - Continue to rotate the remaining lower priority items that pose no risk to LastPass or our customers.
- Began revoking and re-issuing certificates obtained by the threat actor.
- Analyzed LastPass AWS S3 cloud-based storage resources and applied or started to apply additional S3 hardening measures:
- Put in place additional logging and alerting across the Cloud Storage environment with tighter IAM policies enforced.
- Deactivated prior development IAM users.
- Enabled a policy that prevents the creation and use of long-lived development IAM users in the new development environment.
- Rotated existing production service IAM user keys, applied tighter IP restrictions, and reconfigured policies to adhere to least privilege.
- Deleted obsolete service IAM users from the development and production environment
- Enabling IAM resource tagging enforcement on accounts for both users and roles with periodic reporting on non-compliant resources.
- Rotated critical SAML certificates used for internal and external services.
- Deleted obsolete/unused SAML certificates used for development, services, or third parties.
- Revised our 24x7 threat detection and response coverage, with additional managed and automated services enabled to facilitate appropriate escalation.
- Developed and enabled custom analytics that can detect ongoing abuse of AWS resources.

What data was accessed?

Customer Account Secrets, API Keys, and Third-Party Integration Information

Depending on a customer's specific LastPass account configuration and integrations, data stored in the backups accessed by the threat actor may include LastPass-specific and/or third-party secrets, keys, and integration information. Many of these items only apply if a LastPass customer makes use of these specific features, integrations, or account configurations:

- Multifactor Seeds
- Hashes of customer generated One-Time Passwords (OTP) and account Recovery One-Time Passwords (rOTP)
- Split knowledge component ("K2"" key)
- MFA API Integration secrets
- Time-Based One-time Password (TOTP) seeds
- Splunk SIEM integration secrets
- "Push " site credentials
- SCIM, Enterprise API, and SAML keys

LastPass Customer Database

The threat actor was able to copy a backup of the customer database dated as of August 14, 2022.

The customer database contained unencrypted basic customer account information and related metadata including:

Business & Teams Users

- Company Name
- EIN/Tax ID
- Email Address
- End User Name
- IP Address
- Telephone Number
- Mobile Device Unique Identifier
- PBKDF2 SHA256 Iterations

Free, Premium, and Families Users

- Email Address
- End User Name
- IP Address
- Telephone Number
- Mobile Device Unique Identifier
- PBKDFS SHA256 Iterations

LastPass Customer Vault Data - ENCRYPTED

The threat actor was able to copy five of the Binary Large Objects (BLOBs) database shards that were dated: August 20, 2022, August 30, 2022, August 31, 2022, September 8, 2022, and September 16, 2022. This took place between September 8 - 22, 2022

Sites:

- Site Name
- Site Folder
- Site Username (including change history log)
- Site password (including change history log)
- Site note content (including change history log)
- Encrypted TOTP secret used to generate per-site TOTP codes
- Custom fillable form-field
- Custom fillable form-field content

Secure Notes

- Name
- Folder
- Attachment file name
- Attachment Encrypted attachment encryption key
- Note content

Additionally, the following non-categorized data fields are encrypted:

- Group names
  - Encrypted sharing keys
  - Encrypted Super Admin sharing key

LastPass Customer Vault Data - **UNENCRYPTED**

12 unencrypted data fields which may contain sensitive information which reference specific users or devices. The majority of these items are URL-based or URL-related, and only apply if a LastPass user makes use of certain specific features, functions, or account configurations:

- Application file path for the LastPass Windows or macOS application
- Email address of the LastPass user who edits a shared vault item (recorded in change history)
- Site URLs, including various URL rules and “Never URL” account configurations

Recommended Actions

Recommended Actions for LastPass Free, Premium, and Families

Topic 1: Your Master Password…

- Task 1.1 (Optional): Reset Master Password
- Task 1.2: Ensure your master password isn't reused

Topic 2: Iteration counts for master password

- Task 2.1: Review and increase your master password iteration count settings

Topic 3: Evaluate Password Hygiene

- Task 3.1 Review your overall password strength using the Security Dashboard
- Task 3.2: Turn on dark web monitoring

Topic 4: Multifactor authentication (MFA) for your vault

- Task 4.1: Enable MFA for your LastPass vault
- Task 4.2: Already using MFA? Regenerate your MFA shared secret
- Task 4.3: Using the LastPass Authenticator to store additional TOTP codes

Recommended Actions for LastPass Business

Master Password length and complexity

- Task 1.1: Review master password policies and enforce strong master passwords
- Task 1.2: Review security reports related to master passwords
- Task 1.3 (OPTIONAL): Reset select master passwords

Iteration counts for master passwords

- Task 2.1: Review users' master password iteration count settings
- Task 2.2: Review shared folders accessed by users with a low iteration count

Super Admin best practices

- Task 3.1: Ensure super admins follow master password and iterations best practices
- Task 3.2: Review super admins with “Permit super admins to reset master passwords” policy rights and weak master passwords/iterations
- [HIGH IMPACT/OPTIONAL] Task 3.2.1: Federated login customers only: Consider de-federating and re-federating all users and request users to rotate all vault credentials
- [HIGH IMPACT/OPTIONAL] Task 3.2.2: Non-federated login customers only: Consider resetting user master passwords and request users to rotate all vault credentials
- Task 3.3: Review super admins with "Permit super admins to access shared folders" rights

MFA shared secrets

- Task 4.1: Reset shared secrets for non-federated customers

SIEM Splunk integration

- Task 5.1: Update Splunk instance token

Exposure due to unencrypted data

- Task 6.1: Generate URL reports to assess risk
- Task 6.2: (OPTIONAL) Communicate with users about risks

Deprecation of Password apps (Push Sites to Users)

- Task 7.1: Stop using Push Sites/Apps to Users and take remedial action

Reset SCIM, Enterprise API, SAML keys

Federated Customer Considerations

Additional Considerations

- Task 10.1: Review vault item password policies
- Task 10.2: Review user security scores and remediate as required
- Task 10.3: (OPTIONAL) Enable dark web monitoring for your users
- Task 10.4: Review security of shared folders

Thank you!