Stealer Malware
Unmasked

OSINT Detection and Proactive Defense

Robert Fernandes

CISSP, CISM, CASP+, GPEN, GWAPT, GCPN, GCFA, OSIP, CCZT

CYBERCHANCE.ORG

SALTED HASH SECURITY, LLC

linkedin.com/in/robert-fernandes-cybersecurity

MGM Resorts confirms hackers stole customers' personal data during cyberattack

Carly Page @carlypage_ / 8:05 AM EDT • October 6, 2023

Comment

Image Credits: Arcimoto

MGM Resorts has confirmed hackers stole an unspecified amount of customers' personal information during a September cyberattack that will cost the hotel and casino giant an estimated $100 million.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory

CYBERSECURITY ADVISORY

#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability

Release Date: June 07, 2023

Alert Code: AA23-158A

Mr. Cooper remains shut down one week after cyberattack

Over 4M mortgage customers have been unable to make their payments since the company announced it had been attacked on Oct. 31

Image by Getty Images

The MGM hack caused MGM to shut down services for 10 days

Cl0p Ransomware has affected over 2600 organizations.

> 4M mortage customers unable to make payments for days

Orange Spain Faces BGP Traffic Hijack After RIPE Account Hacked by Malware

TLDR

Orange Spain experienced an internet outage due to a threat actor using malware to hijack BGP traffic. No personal data was compromised, but browsing services were affected.

#cyber | + #malware | +

Jan 05, 2024 • 2m read time • From thehackernews.com

If only we had a crystal ball...

There is no crystal ball...

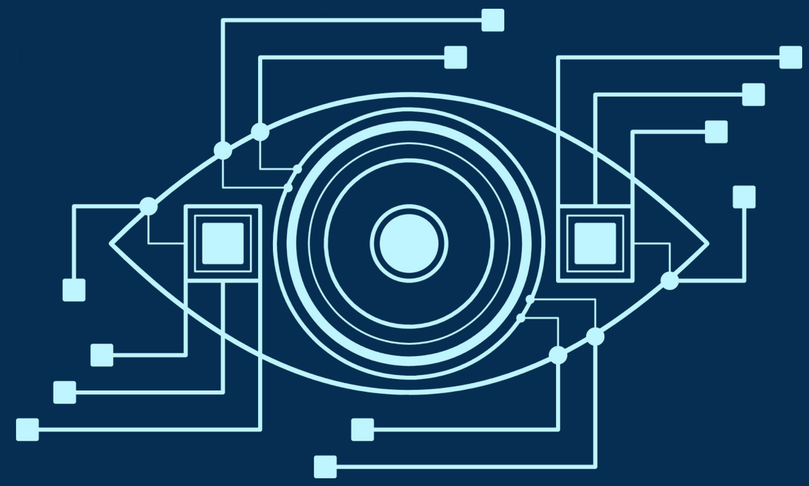
...but there is OSINT

Open Source Intelligence (OSINT)

The method of collecting, analyzing, and making decisions based on publicly available data.

External Exposure

What are we looking for?



Exposed Source Code

Leaked Credentials

Ports, Services, Software

Communications

Infected Devices

External Exposure

Where are we looking?

Criminal Forums and Marketplaces

Paste and Dump Sites

Telegram

Public Internet Scans

Code Repositories

Misconfigured Buckets

Stealer Logs

Stealer malware is a type of malicious software designed to collect and exfiltrate sensitive information from infected devices. The information stolen by stealer malware is contained in a stealer log.

Racoon, Redline, Titan, Aurora, and Vidar are all popular types of Stealer Malware.

Malware-as-a-Service (MaaS) makes it easy for even non-technical criminals to implement and deploy malware to victims.

Stealer Malware exfiltrates data from victims' computers.

Initial infection through phishing, fake software downloads, trojan downloads, etc.

Stealer Logs

Autofills

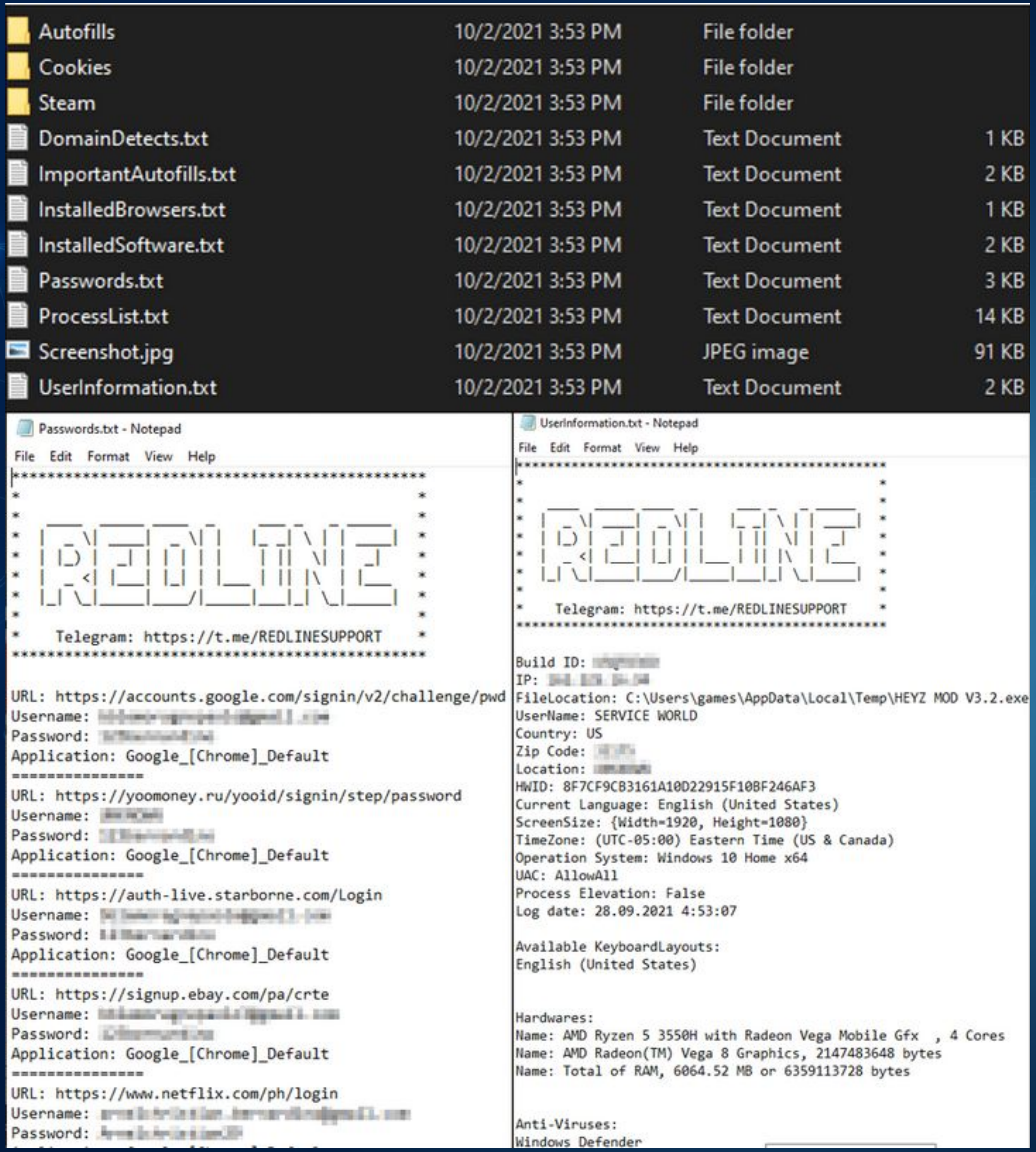
User and Computer Info

Computer Files

Credit Cards

Screenshots

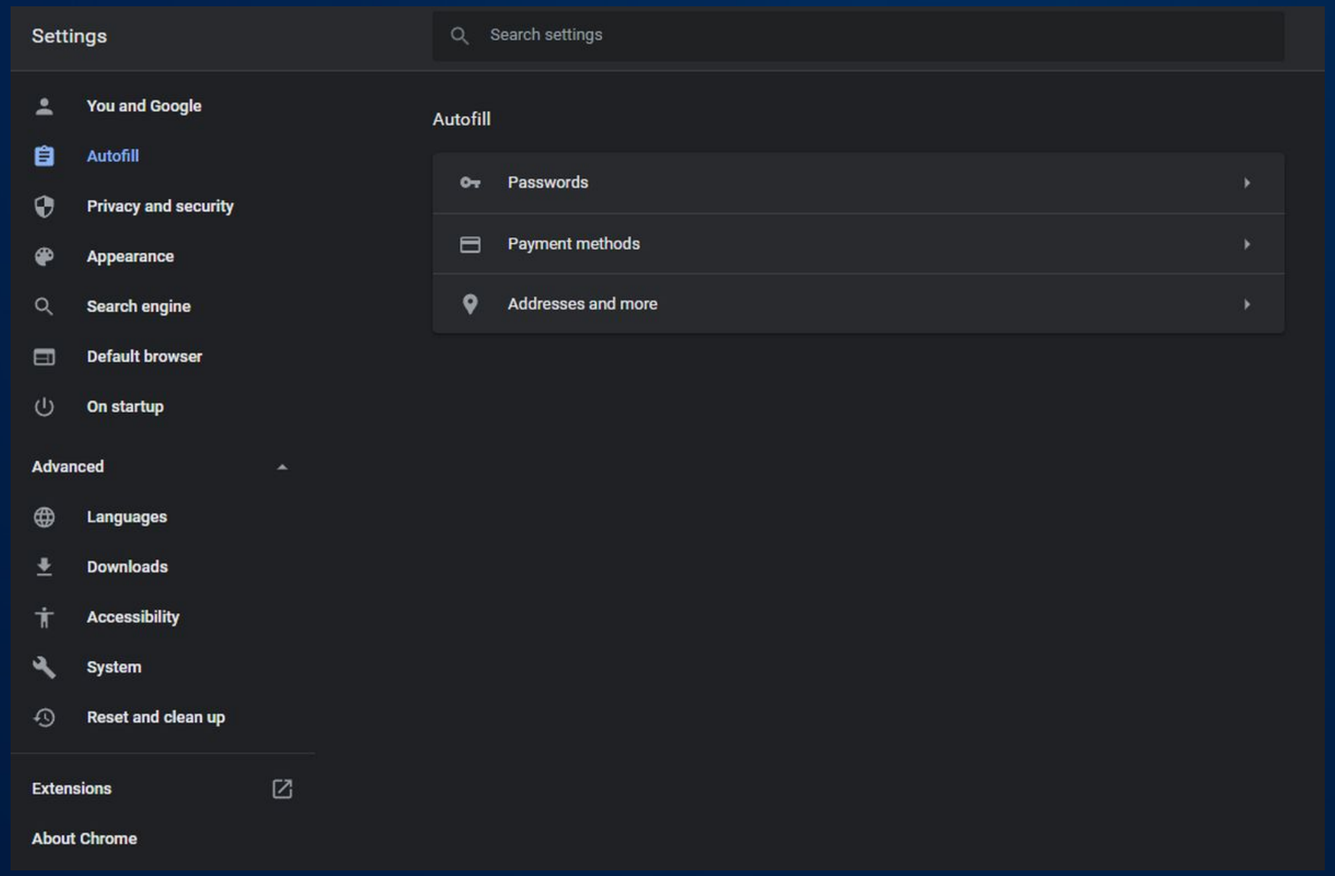
Cookies



Saved Passwords - Autofill Forms

- Do you want Google Chrome to save your password for this site?

- Autofill Forms
  - Credit Cards
  - Names
  - Addresses
  - Social Security Numbers



MFA BYPASS!

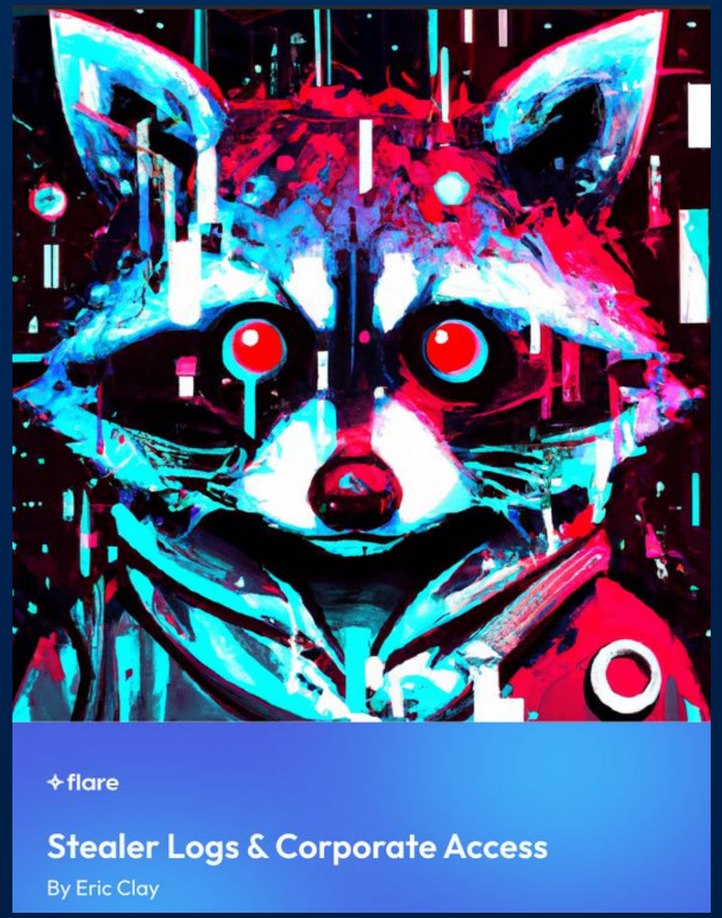
- Persistent Session Cookies
  - “Remember this browser” checkbox

- Browser Fingerprints
- Computer Fingerprints
- User Details

These can be used to bypass MFA

REPORT: Stealer Logs & Corporate Access

- Flare.io analyzed over 19 million stealer logs
- More than 376K logs contained access for business applications (Salesforce, AWS, Okta, Docusign)
- More than 48K logs contained access to okta.com (SSO)
- Almost half of these logs contained access to GMAIL Credentials
- Russian Market and VIP Telegram groups were the most common sources of corporate data



flare

https://flare.io/wp-content/uploads/stealer-logs-and-corporate-access.pdf

Stealer Logs & Corporate Access

- More Remote Workers
- Employees storing passwords in browser
- ACCESS TO CORPORATE RESOURCES
  - CRM, RDP, VPN, SSO
  - aws.amazon.com
  - cloud.google.com
  - accounts.intuit.com
  - account.docusign.com
  - domain.okta.com
  - salesforce.com

Orange Spain Outage

- Orange Spain is a Mobile Network Operator
- Jan 3, 2024 - Outage caused by attack
- The threat actor caused significant disruptions and a 50% loss in traffic.
  - Hudson Rock
- Threat actor stated on twitter that compromised the admin account after using admin credentials that were acquired using Stealer Malware
- The email of the admin account was associated with the computer of an Orange Spain employee who was infected with Racoon Stealer Malware on September 4, 2023
- The incident serves to highlight the consequences of infostealer infections

HudsonRock

An ounce of prevention...

Device Management

Ensure that employees can only only access company resources using trusted, corporate managed devices.

Patch Management

Make sure that all devices are regularly updated with security patches. Don’t forget about third party apps!

Zero Trust Architecture

The days of authenticating with only username, password, and MFA need to be gone. Zero-trust is a more comprehensive approach to authentication and access.

Cyber Insurance

Do you know what’s in your policy? Make sure you have appropriate coverage and the right controls implemented for the best coverage. Insurance Companies re-evaluate the requirements regularly.

An ounce of prevention...

Strong Passwords

Require strong, unique passwords for all systems.

16 Characters or more.

MFA

While not perfect. It adds an additional layer of protection.

Session Expiration

ADMINS: Implement policies that force user sessions to expire after a specific set time. (e.g. 8 hours)

Password Manager

Never store credentials in browsers. Only use trusted Password Managers such as Dashlane

DASHLANE

Thank You

linkedin.com/in/robert-fernandes-cybersecurity/