

Amadey C2 Hunt

08 May 2023 18:42

Nice report from @McAfee_Labs on recent #Amadey intrusion and related #malware distribution.

I fancied a stab at some analysis of any #c2 IoCs available in the report to see what else we can find.

Let take a look at:

Lebro.exe

Lebro.exe, a component of Amadey, is a 235 KB file, compiled in C/C++. Lebro.exe is responsible for executing nbveek.exe, which is a next stage of the malware. The file is again dropped in TEMP folder.

lebro.exe	//28	CreateFile	C:\Userstest\AppData\Local\Temp\9e0894bcc4\nbveek.exe
lebro.exe	7728	CreateFile	C:\Userstest\AppData\Local\Temp\9e0894bcc4\nbveek.exe
lebro.exe	7728	CreateFile	C:\Userstest\AppData\Local\Temp\9e0894bcc4\nbveek.exe
lebro.exe	7728	CreateFile	C:\Userstest\AppData\Local\Temp\9e0894bcc4\nbveek.exe
lebro.exe	7728	CreateFile	C:\Userstest\AppData\Local\Temp\9e0894bcc4\nbveek.exe
lebro.exe	7728	CreateFile	C:\Userstest\AppData\Local\Temp\9e0894bcc4\nbveek.exe
lebro.exe	7728	CreateFile	C:\Userstest\AppData\Local\Temp\9e0894bcc4\nbveek.exe

Figure 27: Dropping another executable in TEMP folder

Stage 7: Analyzing nbveek.exe

The hashes of lebro.exe and nbveek.exe are same, they are the same binaries, hence it is Amadey. It is connecting to IP **62.204.41.88**.

Lets take a look in Shodan:

SHODAN Explore Downloads Pricing Search... **62.204.41.88** Regular View Raw Data History // TAGS: eot-product

General Information

Country	Russian Federation
City	Moscow
Organization	HORIZON LLC
ISP	HORIZON LLC
ASN	AS59425

Open Ports
22 80 443 // 22 / TCP
OpenSSH 8.0
SSH-2.0-OpenSSH_8.0
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAQABAAQgQDGcotaLc5vVcb1Fe+e0T+Nyg1FeYrzCIDzRMADM0JxH6Ca4acwtoukjmh4eFLYCcldxONTOM+s5BwSNITxJmzeR7LTpZv1RLTLnWmpkRtDwNgYLd4mDhf6f04j9zBcFcab4xY3bq1BHkf8mAscdK/7gTadnzdX1uhcvok9jNRIJwOe5CEVgk7k3YGwc/7j3l0MnugtFTcrFWruzh9B...

A nice friendly geolocation :D hosted at HORIZON LLC. First pivot off the SSH key, unfortunately it yields no results.

SHODAN Explore Downloads Pricing hash:-1675585631 **62.204.41.88** Russian Federation, Moscow // TOTAL RESULTS 1 Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

SSH-2.0-OpenSSH_8.0
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAQABAAQgQDGcotaLc5vVcb1Fe+e0T+Nyg1FeYrzCIDzRMADM0JxH6Ca4acwtoukjmh4eFLYCcldxONTOM+s5BwSNITxJmzeR7LTpZv1RLTLnWmpkRtDwNgYLd4mDhf6f04j9zBcFcab4xY3bq1BHkf8mAscdK/7gTadnzdX1uhcvok9jNRIJwOe5CEVgk7k3YGwc/7j3l0MnugtFTcrFWruzh9B...

Next lets take a look at the service running on port 443:

```
nginx 1.11.13

HTTP/1.1 404 Not Found
Content-Type: text/html
Server: nginx/1.11.13
Date: Tue, 02 May 2023 18:18:11 GMT
Content-Length: 162

<html>
<head><title>404 Not Found</title></head>
<body bgcolor="white">
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.11.13</center>
</body>
</html>
```

Nothing on the hash, lets modify the query slightly to remove the date

information: <https://www.shodan.io/search?query=HTTP%2F1.1+404+Not+Found+Content-Type%3A+text%2Fhtml+Server%3A+nginx%2F1.11.13+Date%3A+GMT+Content-Length%3A+162++%3Chtml%3E+%3Chead%3E%3Ctitle%3E404+Not+Found%3C%2Ftitle%3E%3C%2Fhead%3E%3Cbody+bgcolor%3D%22white%22%3E+%3Ccenter%3E%3Ch1%3E404+Not+Found%3C%2Fh1%3E%3C%2Fcenter%3E+%3Chr%3E%3Ccenter%3Enginx%2F1.11.13%3C%2Fcenter%3E+%3C%2Fbody%3E++%3C%2Fhtml%3E>

Bingo we have some results:

The screenshot shows Shodan search results for the specified query. It includes a search bar, navigation links for Explore, Downloads, Pricing, and a search icon. Below the search bar are sections for TOTAL RESULTS (24), TOP COUNTRIES (Russia, Netherlands, United States, Germany, Switzerland), and TOP PORTS (443, 4433). A Product Spotlight for InternetDB is displayed. The main results table lists IP addresses with their details, including hostnames, locations, and raw response snippets.

IP Address	Hostname	Location	Raw Response Snippet
179.43.142.172	hostedby.privateLayer.com	Switzerland, Zürich	HTTP/1.1 404 Not Found Content-Type: text/html Server: nginx/1.11.13 Date: Sat, 06 May 2023 03:52:46 GMT Content-Length: 162
88.210.12.126	host-88-210-12-128.hosted-by-ydsina.ru	Russian Federation, Moscow	HTTP/1.1 404 Not Found Content-Type: text/html Server: nginx/1.11.13 Date: Thu, 04 May 2023 23:28:00 GMT Content-Length: 162
95.214.27.214	Fuse Hosting Web	United States, University Center	HTTP/1.1 404 Not Found Content-Type: text/html Server: nginx/1.11.13

The results look interesting and all appear to be using ports 443/4433. Lets check the first result in VirusTotal, it has a very low detection rate (1 hit) and appears associated with #Rhadamanthys stealer C2. Lets check a few more to validate the results, yep they all appear to be infrastructure related to stealer malware.

Σ 179.43.142.172

DETECTION DETAILS RELATIONS COMMUNITY 1

Crowdsourced context ⓘ

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

⚠️ CnC Panel - according to source ViriBack - 1 month ago
↳ A domain seen in a CnC panel URL for the Rhadamanthys malware resolved to this IP address

Security vendors' analysis ⓘ

ViriBack	Malware	Abusix	Clean
----------	---------	--------	-------

So lets take a look at Censys and see if we have any variation on the results:

Hmm no results for the report IP:

censys

Hosts 62.204.41.88 Search F

62.204.41.88

Summary Explore History WHOIS Raw Data ▾

Basic Information

- Network HORIZONMSK-AS (RU)
- Routing 62.204.41.0/24 via AS59425
- Protocols no publicly accessible services

We haven't found any publicly accessible services on this host or the host is on our blocklist.

55°45'08.0"N 37°36'56"E
View larger map

Geographic Location

- City Moscow
- Province Moscow
- Country Russia (RU)
- Coordinates 55.75222, 37.61556
- Timezone Europe/Moscow

Lets try another:

censys

Hosts
88.210.12.126
Search

Fingerprint b3daab087be16148dc49489af121508163a8463c4c1a334c0a388c59674f385d

Negotiated

Key Exchange curve25519-sha256@libssh.org
 Symmetric Cipher aes128-ctr [+] aes128-ctr [-]
 MAC hmac-sha2-256 [+] hmac-sha2-256 [-]

80/HTTP TCP

Observed May 08, 2023 at 1:14am UTC

Software

nginx 1.11.13 []

[VIEW ALL DATA](#)

[GO](#)

Details

http://88.210.12.126

Request GET /index.html
 Protocol HTTP/1.1
 Status Code 200
 Status Reason OK
 Body Hash sha1:56ee59f33d94e2e396b33442e389e1032f7753c6
 HTML Title Welcome to nginx!
 Response Body [EXPAND](#)

443/HTTP TCP

Observed May 07, 2023 at 6:39pm UTC

Software

nginx 1.11.13 []

[VIEW ALL DATA](#)

[GO](#)

Details

http://88.210.12.126:443

Request GET /
 Protocol HTTP/1.1
 Status Code 404
 Status Reason Not Found
 Body Hash sha1:f459d7f3b810646fc8efb680afbfe68940413e90
 HTML Title 404 Not Found
 Response Body [EXPAND](#)

Next lets search on the HTTP services.banner present on port 443:

https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUDE&q=services.banner%3D%22HTTP%2F1.1+404+Not+Found%5Cr%5CnContent-Type%3A+text%2Fhtml%5Cr%5CnServer%3A+nginx%2F1.11.13%5Cr%5CnDate%3A++%3CREDACTED%3E%5Cr%5CnContent-Length%3A+162%5Cr%5Cn%22

443/HTTP TCP

[View Definition](#)

Attribute	Value
services.banner	HTTP/1.1 404 Not Found\r\nContent-Type: text/html\r\nServer: nginx/1.11.13\r\nDate: <REDACTED>\r\nContent-Length: 162\r\n

10 results, at first glance we have some overlap with Shodan but there are some newly identified hosts.

censys

Hosts
services.banner="HTTP/1.1 404 Not Found\r\nContent-Type: text/html\r\nServer: n
Search

[Results](#) Try CensysGPT Beta

[Report](#)

Host Filters

Labels:

Hosts

Results: 10 Time: 0.19s

Stealer C2s:

108[.]61[.]189[.]120142[.]11[.]215[.]202142[.]11[.]215[.]202144[.]76[.]33[.]241159[.]65[.]13[.]48176[.]11

3[,]115[,]86179[,]43[,]142[,]172179[,]43[,]154[,]245185[,]225[,]73[,]180185[,]246[,]220[,]162185[,]43[,]2
23[,]200192[,]30[,]243[,]151194[,]180[,]48[,]102216[,]250[,]255[,]120216[,]250[,]255[,]1552607:5500:3
000:1954::231[,]41[,]244[,]8145[,]77[,]66[,]15146[,]151[,]25[,]14662[,]204[,]41[,]21062[,]204[,]41[,]8879
[,]137[,]194[,]24080[,]66[,]88[,]7284[,]54[,]50[,]15884[,]54[,]50[,]15985[,]217[,]144[,]8288[,]210[,]12[,]12
689[,]22[,]230[,]17591[,]215[,]85[,]15795[,]214[,]27[,]214