Naikon APT: Cyber Espionage Reloaded

research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/

May 7, 2020

May 7, 2020

Introduction

Recently Check Point Research discovered new evidence of an ongoing cyber espionage operation against several national government entities in the Asia Pacific (APAC) region. This operation, which we were able to attribute to the **Naikon APT group**, used a new backdoor named **Aria-body**, in order to take control of the victims' networks.

In 2015, an extensive report by ThreatConnect and Defense Group revealed the APT group's infrastructure and even exposed one of the group's members. Since this report, no new evidence has come to light of further activity by the group, suggesting that they had either gone silent, increased their emphasis on stealth, or drastically changed their methodology of operations. That is, until now.

In the following report, we will describe the tactics, techniques, procedures and infrastructure that have been used by the Naikon APT group over the 5 years since the last report, and offer some insight into how they were able to remain under the radar.

Targeting

By comparing with previously reported activity, we can conclude that the Naikon APT group has been persistently targeting the same region in the last decade. In operations following the original 2015 report, we have observed the use of a backdoor named **Aria-body** against several national governments, including **Australia, Indonesia, the Philippines, Vietnam, Thailand, Myanmar** and **Brunei**.

The targeted government entities include ministries of foreign affairs, science and technology ministries, as well as government-owned companies. Interestingly, the group has been observed expanding its footholds on the various governments within APAC by launching attacks from one government entity that has already been breached, to try and infect another. In one case, a foreign embassy unknowingly sent malware-infected documents to the government of its host country, showing how the hackers are exploiting trusted, known contacts and using those them to infiltrate new organizations and extend their espionage network.

Given the characteristics of the victims and capabilities presented by the group, it is evident that the group's purpose is to gather intelligence and spy on the countries whose Governments it has targeted. This includes not only locating and collecting specific documents from infected computers and networks within government departments, but also extracting data from removable drives, taking screenshots and keylogging, and of course harvesting the stolen data for espionage. And if that wasn't enough, to evade detection when accessing remote servers through sensitive governmental networks, the group compromised and used servers within the infected ministries as command and control servers to collect, relay and route the stolen data.

Targeted countries

Infection Chains

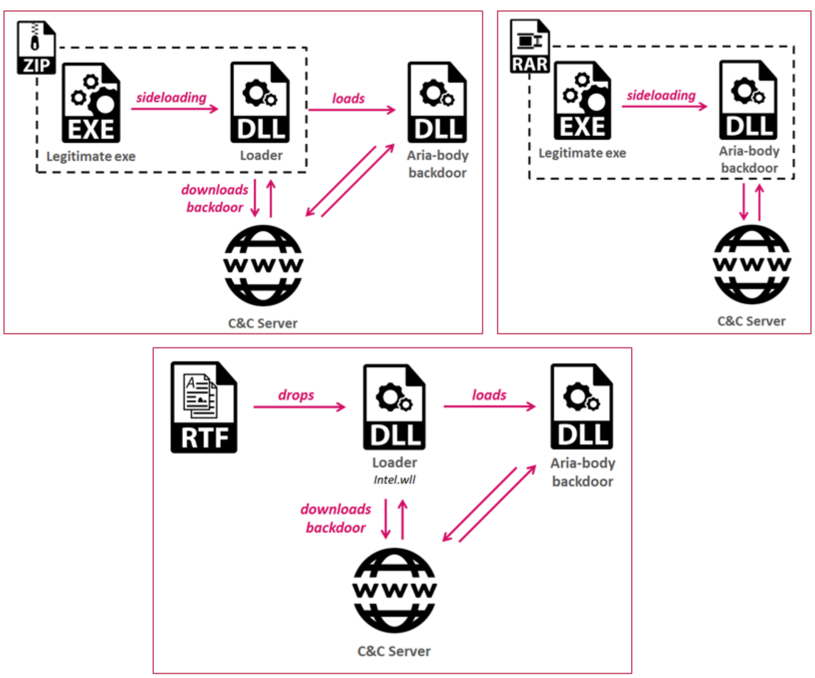
Throughout our research, we witnessed several different infection chains being used to deliver the **Aria-body** backdoor. Our investigation started when we observed a malicious email sent from a government embassy in APAC to an Australian state government, named `The Indians Way.doc`. This RTF file, which was infected (weaponized) with the RoyalRoad exploit builder, drops a loader named `intel.wll` into the target PC's Word startup folder. The loader in turn tries to download and execute the next stage payload from `spool.jtjewifyn[.]com`.

This is not the first time we have encountered this version of the **RoyalRoad** malware which drops a filename named `intel.wll` – the **Vicious Panda** APT group, whose activities we reviewed in March 2020, utilizes a very similar variant.

Overall, during our investigation we observed several different infection methods:

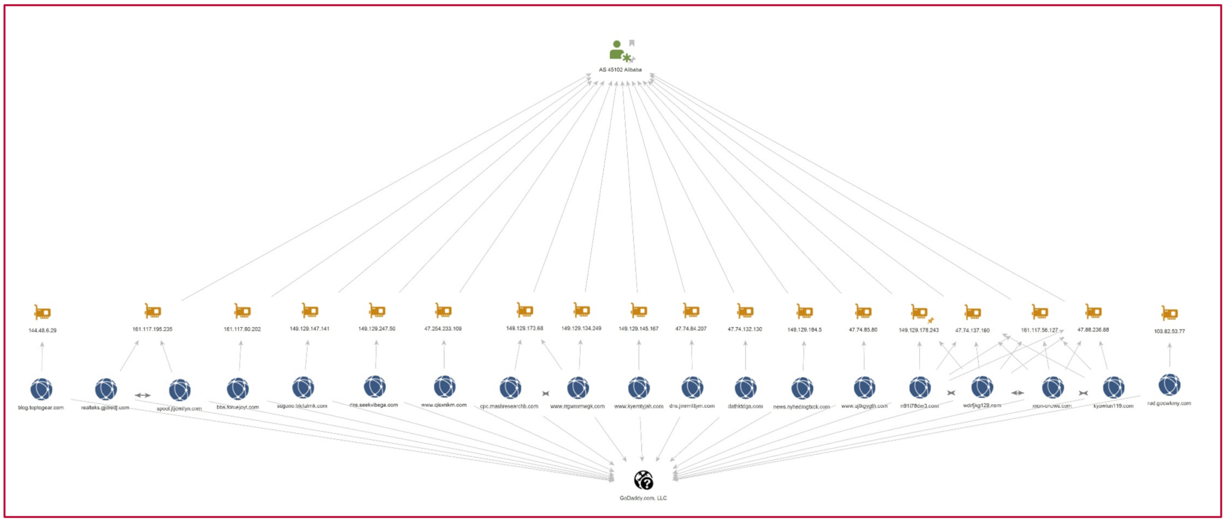
- An RTF file utilizing the **RoyalRoad** weaponizer.
- Archive files that contain a legitimate executable and a malicious DLL, to be used in a DLL hijacking technique, taking advantage of legitimate executables such as **Outlook** and **Avast proxy,** to load a malicious DLL.
- Directly via an executable file, which serves as a loader.

Infection chain examples



Infrastructure

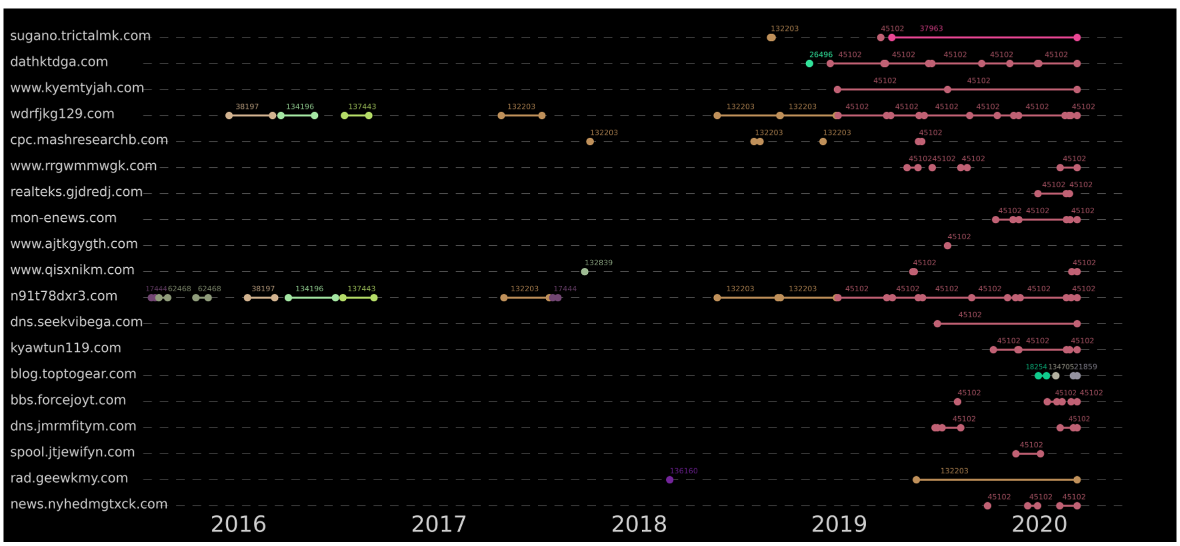
In recent operations, the attackers used the same hosting and DNS services for most of their C&C servers: **GoDaddy** as the registrar and **Alibaba** for hosting the infrastructure. On several occasions, the attackers even reused the same IP address with more than one domain:



Maltego – latest infrastructure overview

A full view of the entire infrastructure is available here.

In order to get a clearer picture of how the attackers operated their infrastructure throughout the years, we have plotted the various malicious domains, according to the ASN they were hosted on, based on periodic passive DNS information. The results are presented in the figure below:



Correlation between domains and ASNs over time

Observations:

- Several domains were utilized for a very long time.
- Multiple domains jumped to the **same** new ASN within a short time frame.
- Since 2019, most of the infrastructure has been concentrated on ASN 45102 (Alibaba).
- In some occasions, the attackers would change the IP address / server, on the same ASN (represented by two consecutive incidental ASN's on the graph).

In addition, one of the more interesting infrastructure properties we observed, is the possible use of hacked government infrastructures as C&C servers. In one of the samples we analyzed, `outllib.dll` (`63d64cd53f6da3fd6c5065b2902a0162`), there is a backup C&C server which is configured as `202.90.141[.]25` – an IP which belongs to the ***Philippines department of science and technology.***

Tool Analysis

In the following section, we will dive into the technical analysis of the **Aria-body** backdoor, utilized throughout the observed activity, as well as an analysis of the loader executable that comes before it.

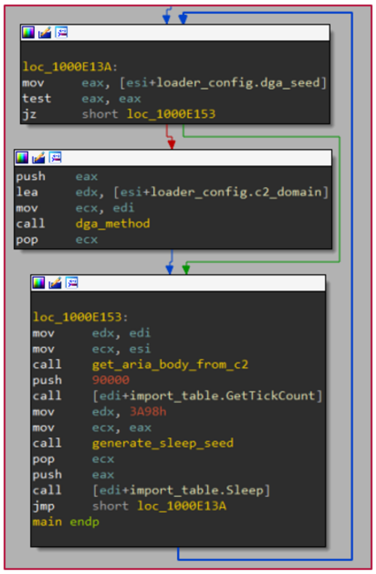
Utilizing the loader at an early stage of an infection allows the attackers to establish a persistent presence on the target's network, as well as perform basic reconnaissance, before using their more advanced tools. While we observed **Aria-body** backdoor variants being compiled as early as 2018, we have observed **Aria-body's** loaders going back to 2017.

Loader Analysis

The functionality of the **Aria-body loader** has not changed significantly since 2017, but the implementation varied from version to version. **This loader appears to be specifically created for the Aria-body backdoor.**

Overall, the loader is responsible for the following tasks:

1. Establish persistence via the `Startup` folder or the `Run` registry key (some variants).
2. Inject itself to another process such as `rundll32.exe` and `dllhost.exe` (some variants).
3. Decrypt two blobs: Import Table and the loader configuration.
4. Utilize a DGA algorithm if required.
5. Contact the embedded / calculated C&C address in order to retrieve the next stage payload.
6. Decrypt the received payload DLL (**Aria-body** backdoor).
7. Load and execute an exported function of the DLL – calculated using `djb2` hashing algorithm.



Main logic of the loader – entering dga_method only if dga_seed ≠ 0

Loader: Configuration & DGA

The loader configuration comes encrypted and contains the following information: C&C domain, port, user-agent and a seed for the Domain Generation Algorithm (DGA). In case seed is not zero, the loader uses a DGA method to generate its C&C domain, based on the seed and the calendar day of the communication. The configuration of the loader is decrypted using the following algorithm:

```
def decrypt_buf(buf):
    k = 8
    j = 5
    for i in range(len(buf)):
        xor_byte = (k + j) % 0xff
        buf[i] = buf[i] ^ xor_byte
        j = k
        k = xor_byte
```

Configuration decryption algorithm

The DGA method is fully described in **Appendix B**.

Loader: C&C Communication

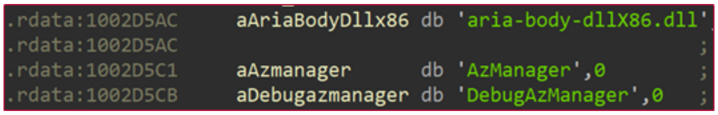
After getting the C&C domain, the loader contacts it to download the next and final stage of the infection chain. Although it sounds simple, the attackers operate the C&C server in a limited daily window, going online only for a few hours each day, making it harder to gain access to the advanced parts of the infection chain.

Loader: Next stage payload

At the next and final stage of the loader, the downloaded RAT is decrypted using a single byte XOR key, received from the C&C. Once the RAT's DLL is downloaded and decrypted, the DLL is loaded into the memory. The loader will then check the exported function against a hardcoded `djb2` hash value, and will call it upon a match.

Aria-body RAT analysis

The downloaded payload is a custom RAT dubbed **Aria-body**, based on the name given by the authors: `aria-body-dllX86.dll`.
Although the below analysis is of the 32bit variant malware, we have observed a 64bit variant as well, with similar functionality.



Strings found inside the "Aria-body" backdoor

The RAT includes rather common capabilities of a backdoor, including:

- Create/Delete Files/Directories
- Take a screenshot
- Search file
- Launch files using `ShellExecute`
- Enumerate process loaded modules
- Gather files' metadata
- Gather TCP and UDP table status listing
- Close a TCP session
- Collect OS information
- Verify location using `checkip.amazonaws.com`
- (Optional) Inter-process pipe based communication

Some of **Aria-body** variations also included other modules such as:

- USB data gathering module
- Keylogger module to collect raw input device-based keystrokes – added by February 2018
- Reverse socks proxy module – added by February 2018
- Loading extensions module – added by December 2019

All the supported functionality of the backdoor is described in the table of **Appendix A**.

Unique Characteristics

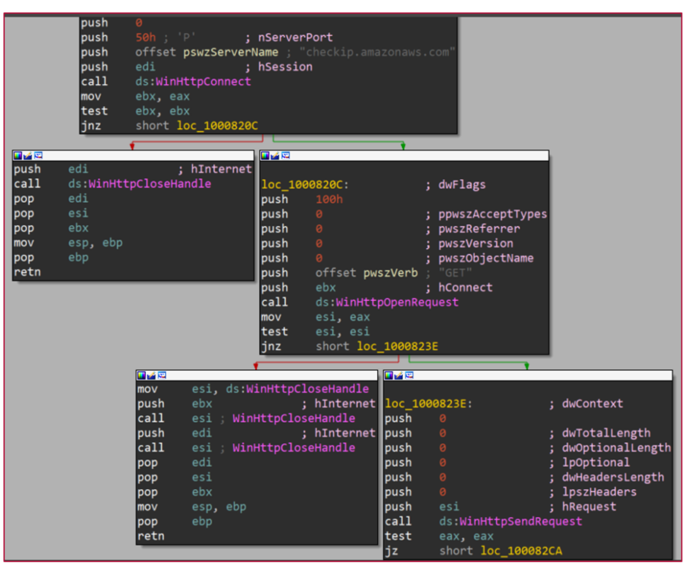
In the following section, we go over some of the techniques by which the backdoor was implemented, and highlight the characteristics that might help other researchers recognize this backdoor and correlate it with other samples.

Initialization

As previously mentioned, the backdoor contains an exported function, which the previous loader calls after loading the payload into the memory. Upon executing the backdoor, it initializes a struct named `MyDerived` and several structs used for HTTP and TCP connection.

Information Gathering

Aria-body starts with gathering data on the victim's machine, including:
Host-name, computer-name, username, domain name, windows version, processor ~MHz, MachineGuid, 64bit or not, and public IP (using `checkip.amazonaws.com`).

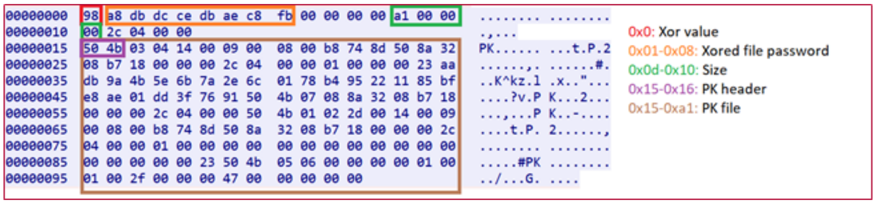


Aria-body using checkip.amazonaws.com service to get victim's IP

This data is gathered into an information structure which the RAT zips with an 8 bytes random generated password, which is then XORed with one byte.

C&C Communication

The communication to the C&C server is available by either HTTP or TCP protocols. The malware decides which protocol to use by a flag in the configuration of the loader. The collected data is sent to the C&C domain along with the XORed password, and the XOR key in the following format:



C&C communication structure

Whether the message is sent by TCP or HTTP, the payload format is the same. However, when HTTP is selected, the following GET request format is used:
`https://%s:%d/list.html?q=<random string>`

After the initial request to the C&C server, the backdoor then keeps listening to additional commands from the server. When a command is received, it is matched against a list of commands, and executed accordingly. A full list of supported commands is available in **Appendix A**.

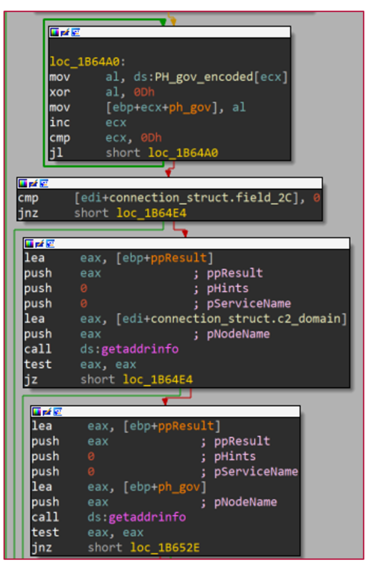
The Outlook DLL Variant

During our research we have found another, quite a unique variant of Aria-body, uploaded to VirusTotal from the **Philippines**. This variant's DLL was named `outllib.dll`, and it was part of a RAR archive named `Office.rar`. It utilized a DLL side-loading technique, abusing an old **Outlook** executable.

What was unusual in this variant was the fact that there has no loader as part of the infection chain, unlike all the other versions of Aria-body. As a result, it did not get any configuration from the loader, and included hardcoded configuration within it.

The payload has two different C&C domains:

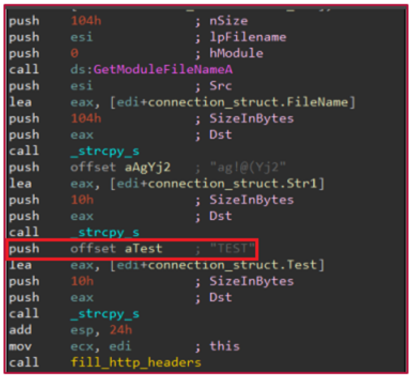
- `blog.toptogear[.]com` – which it gets by XORing an encrypted string with the byte `0x15`.
- `202.90.141[.]25` – an IP associated with a **Philippine government website**, which is being used in case that the first C&C domain cannot be resolved.



Usage of Philippines govt' C&C server as backup

This variant also has some extra features that the main variant of **Aria-body** does not include, such as a USB-monitor module. On the other hand, this variant is missing the keylogger component and the reverse-socks module, observed with the main **Aria-body** variants. This evidence suggests that this is an out of scope variant of the backdoor, tailored for a specific operation.

Moreover, we have seen that **Aria-body's** main variant has a version that was compiled sometime after `outlib.dll` variant was, and some strings within this variant could suggest that it was a test variant of this special version:



"TEST" string as part of the connection struct of "outllib.dll"

Finally, this version of Aria-body includes the following string: `c:\users\bruce\desktop\20190813\arn\agents\verinfo.h` , with the "**ar**" in "**ar**n" possibly standing for "**Ar**ia".

Attribution

We were able to attribute our campaign to the Naikon APT group using several similarities we observed to the previously disclosed information about Naikon's activity by Kaspersky in 2015: 1, 2. In this original operation, the Naikon APT group utilized a backdoor against different government institutions in APAC.

Going forward, we will refer to the backdoor analyzed by Kaspersky as **XsFunction** due to **PDB** path found in one of its samples: `g:\MyProjects\xsFunction\Release\DLL.pdb`

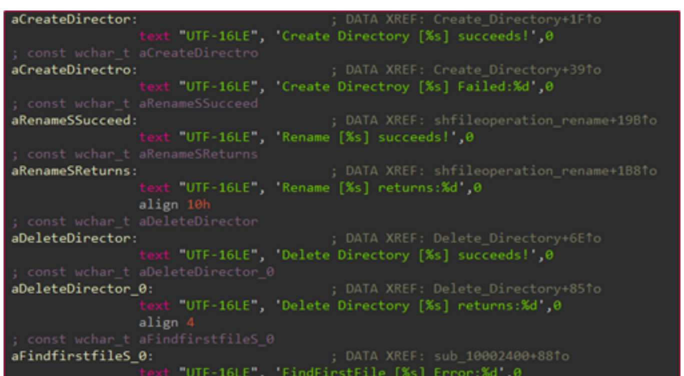
XsFunction is a full featured backdoor which supports 48 different commands. It allows the attacker to gain full control on the victim computer, perform file and process operations, shell commands execution, as well as to upload and download data and additional plugins.

We were able to find several similarities to previous operations (besides the obvious overlap in targeting), as well as specific similarities to the **XsFunction** backdoor.

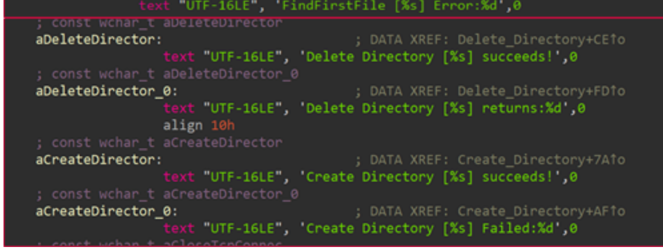
String Similarity

Aria-body backdoor has several **debug strings** that describe the functionality of the malware.

Some of these **exact** debug strings, can also be found in the **XsFunction** backdoor:



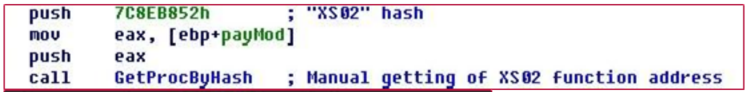
Strings found in Aria-body backdoor



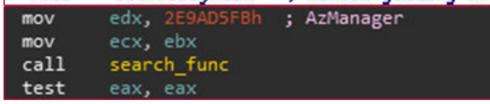
Strings found in XsFunction (d085ba82824c1e61e93e113a705b8e9a)

Hashing Function Similarity

Both **XsFunction** and **Aria-body loaders** utilize the same hashing algorithm `djb2` to find which exported function should be run. In **XsFunction** the name of that function is `XS02` and in **Aria-body** it is `AzManager` .



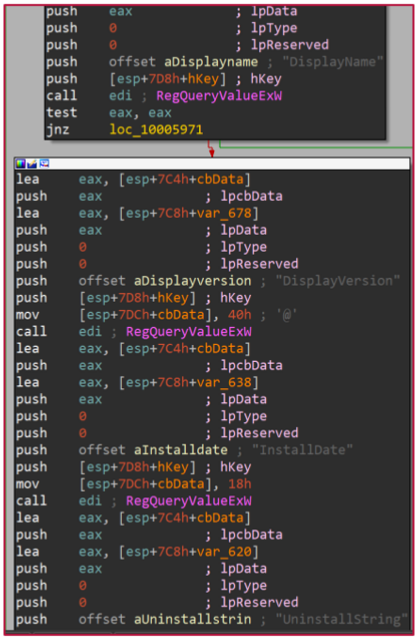
XsFunction loader (Image by Kaspersky)



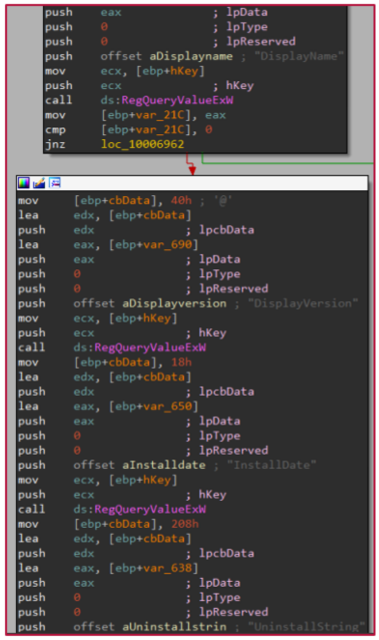
Aria-body loader

Code Similarity

Some functions in the **Aria-body** backdoor are identical to functions used in the old **XsFunction** backdoor. One example is the function which gathers information about the installed software on the PC:



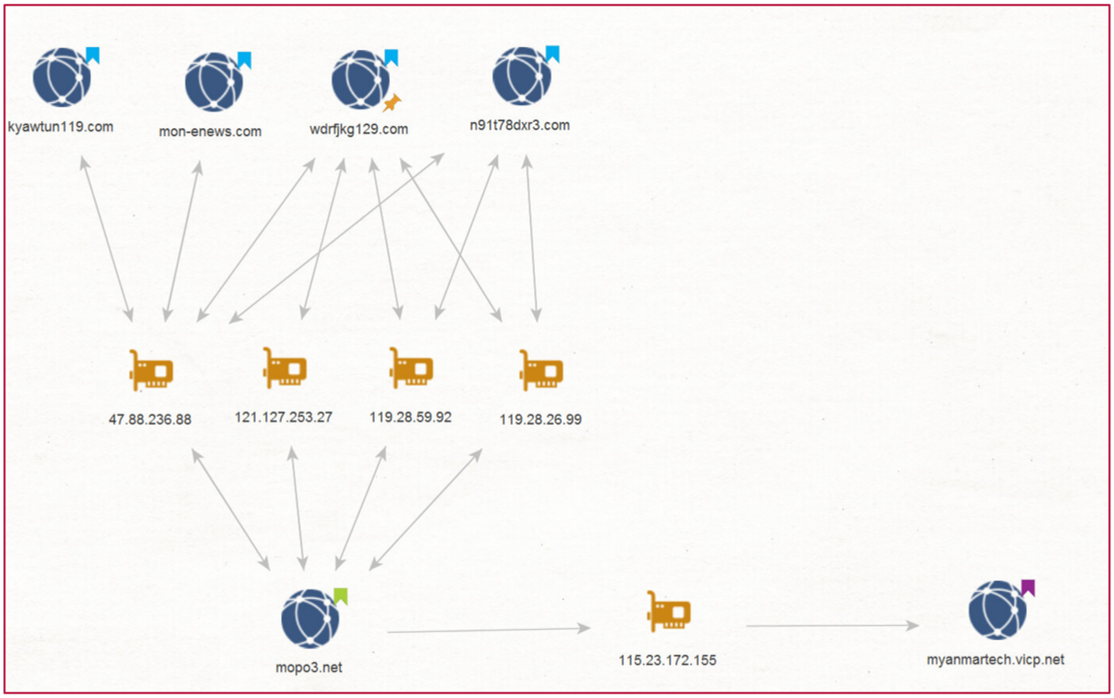
Aria-body information gathering



XsFunction information gathering

Infrastructure overlap

Four of our C&C servers shared IPs with `mopo3[.]net` domain, this domain resolves to the same IP as the domain mentioned in Kaspersky's report: `myanmartech.vicp[.]net` .



Maltego – graph of infrastructure overlap

Conclusion

In this campaign, we uncovered the latest iteration of what seems to be a long-running Chinese-based operation against various government entities in APAC. This specific campaign leveraged both common toolsets like RoyalRoad RTF weaponizer, as well as a specially crafted backdoor named **Aria-body**.

While the Naikon APT group has kept under the radar for the past 5 years, it appears that they have not been idle. In fact, quite the opposite. By utilizing new server infrastructure, ever-changing loader variants, in-memory fileless loading, as well as a new backdoor – the Naikon APT group was able to prevent analysts from tracing their activity back to them.

Check Point SandBlast Agent protects against such APT attacks, and is capable of preventing them from the very first step.

Appendix A: Aria-body – Supported Commands

Command ID (Sent from C&C)	Sub Command ID (Sent from C&C)	Description	Command add date
0x1	0x0	Gather installed software's information	–
0x2	0x0	Get Disks information	–
0x2	0x1	File Search by name	–
0x2	0x2	Find Directory	–
0x2	0x4	Create Directory	–
0x2	0x6	SHFileOperaion – Delete Directory	–
0x2	0x7	SHFileOperaion – rename file	–
0x2	0x9	Delete File in a given path	–
0x2	0xa	ShellExecute 'open' command	–
0x2	0xb	ShellExecute 'open' command	–
0x2	0xe	Create new file and write its data	–
0x3	0x0	Get active processes information	–
0x3	0x2	Terminate Process	–

0x3	0x3	Get loaded modules information	–
0x4	all	Unique modules command: ARN – USB monitor module	only in outllib.dll variant
0x4	all	Unique modules command: aria-body – reverse socks proxy module	Feb 2018 – not in outllib.dll
0x5	0x0	Get MD5 of file	–
0x6	0x0	Get titles of running windows	–
0x6	0x1	Send WM_CLOSE message to given window name	–
0x7	0x0	Get TCP and UDP tables	–
0x7	0x1	Close given TCP connection	–
0x8	0x0	Start keylogger	Feb 2018 – not in outllib.dll
0x8	0x1	Stop keylogger	Feb 2018 – not in outllib.dll
0X9	0X0	Inject itself into rundll32.exe – spawn module	July 2018 – not in outllib.dll
0X9	0X1	Inject itself into rundll32.exe with UAC	July 2018 – not in outllib.dll
0X9	0X2	Inject itself to every process except explorer.exe	July 2018 – not in outllib.dll
0xa	0x1	Collect services data	Dec 2018 – not in outllib.dll
0xaa	0x1	Load extensions	Dec 2018 – not in outllib.dll
0xaa	0x2	'runas' with given process	–
0xaa	0x3	Zip-Directory	–
0xaa	0x4	Create Process and inject itself into it.	–
0xaa	0x5	UAC method (duplicate token from ntprint.exe)	–
0xaa	0x6	Send screenshot	–
0xaa	0x7	Send command to given extension	Dec 2018 – not in outllib.dll
0xaa	0x9	Destruction method	Dec 2018 – not in outllib.dll

Appendix B: DGA method

```
def DGA_method(seed_value):
    domain = ""
    tld = [".com", ".org", ".info"]
    ta = time.localtime(time.time())
    temp1 = math_s(ta.tm_year)
    temp2 = math_s(dword(temp1 + ta.tm_mon + 0x11FDA))
    temp3 = math_s(dword(temp2 + ta.tm_mday))
    temp4 = math_s(dword(seed_value + temp3))
    temp5 = math_s(dword(temp4 + 9))
    length = (temp5 % 0xe) + 8
    if length > 0:
        for i in range(length):
            temp6 = math_s(i + temp5)
            domain += chr ( ( temp6 % 0x1a) + 0x61)
            temp5 = math_s(dword(temp6 + 0xcdcdef))

    domain += tld[temp6 % 3]
    print(domain)
```

Appendix C: IOC list

Delivery:

MD5	SHA-1	SHA-256
f9d71f32de83f9ecfdc77801a71da7bf	560423901a746055a4890c87dabe2c2a59ee917a	d6841b2a82904efc52c6b0b9375ddd3aa70de360c
08428c94f45fb8ff568a4a288778dfb7	00934d22fb37b2def8276bc22ace5dc950b66227	7df5442e5c334eb81a2f871623fcbed859148223ef
5e37131cbd756e10a9392d2280907592	c0c39b4ffe6fa7ff627654fbdd53a3bf638da4cb	6a8f59ad46ad22f272d5617e8d8101af820772abd5

Aria-body loaders – 32bit

e9a23e084eb8cf95b70cde3afc94534b	96a918b4e54090c0294470c872c1b2075af1a822	1747fb340794c0c4e746b86c9a77fc568042be9d1
8561fa029f2158dc9932deee61febdac	3cecff13388d6ab45797ca2455caf5fd04ca9dd9	fe845ac7525daa5050dc17ca90352afe0f53c04a26
31a4400789ae43b255464481320baa9e	1e3f303bbb35e709ff9d962c28c071656070aa98	8c38a9f38fd472867479cbaab9c138df616e60e3bb
32b1916abff8bf0e7c51a2584c472451	513d99d714985ab53d75894357e4e87c69374862	a9f0df941172cc4a9c8b242fd41094033e15fa9c5e3
c2dc85559686575c268c8e97205b7578	b01d9454d84d04dd7a594dd2f899c77a40248618	fe02467d457e214e82a561de7cfa5e534efdb6beba
b779742b94b9265338c9b21f0cc88ba4	3f7190d530a98e157d799bdbe4fef8e69f1c50de	f31a5d3d586924ea2fe274cc644e3d9501efcc452c
ca3d5f02f453455f2b5522b8dceca658	0289a6db2fdda581b413768cd9318f33b5c005e7	ca2da542ffdbf551a1fa46d073c63162747df7ab45b
bd1ef60ee835dd996ddcf4f22adaa142	1d7056e1bec6fadfba8b69d725e4a930bdb6fa40	510d91994c02e92e5354a9cdd51fd2be23583779e
1dd0e12a886f3d1bded6e26f53592720	896e44af5a6f88c7be21d2f7225462f273f067f5	4dcac1b42a0d2308136ce87db28856f1c1888dea0
07f724bdc662518ce6eac0ca723c929f	1eb758bcb0fc640835962aaa80199bdc867c79e7	45f2dbc7240023308e3193f29cc68320a176714e4
dde75e82b665fc7d47cd870dae2db302	2f17d1f1766b2814d6347763c9ad94863e5bd35c	249ca984c1a508c4adbd58c3e3675bf22c8e36475
20cdf05867967642742d6b947ba71284	31cf5cb37d1d6e62add2cd4e59c2821a1a3c54e5	a5a0f9117a49ad7246882c938017a6f603180b37e
9b0cb194dd5e49ab6fbf490de42e6938	396c0c1dce196e9dc4e65aeb57d2bd1ec5e85ba9	1732639fe36c3ffbe860c09a3b8b92115f31e94e93
b8292fe24db8f86b11e6bf303c5f3ac5	69ea467bdfe5b7739553da7f93096a3ac944270c	bfdf1c7437189306998cf6b9f1197bd5c77d85ae55
357a9f8268438d487303b267b26bde65	722b3dafbc14f8dce1048264451017d3f473f1ac	7b336c7828027d6080617e0a619a0eb048be3c97
40c49ecbe1b7bd0dbb935138661b6ca4	fe84b53aa8bb4e8ac3d2d9f86d2397d4a3cf5c08	0db51c4a2bd94f2b56f821a013fa42e0e67e3a7b69
85e5d261c810e13e781f24505bb265ce	6a5a96f5637c898c0792ca9e76fc1854cf960d59	d389780b530557e4076eecfd0b2f92c955c581b23
77ea1eb5f6fd2605454764cd9b7ef62e	653aae2210a256a00ead6495e2c128d36d2ed531	3d0e3136ed28397eaf4414aaa072ab11a1787ae09
ab260f3dc1ead01dfc6b7139d1eb983c	c2d3d9d7d7b64bbc6e522695105c31d5f1185800	d29692b12f865e5480ae97b507ccec96b32ab6784
897994f378577ec1e09eaeb953cf603f	799ffe499b1a0d4b58ad9fa7b065b03432b96a09	7463d0f064a31b61ffedd0895ab242700d0d80fc2fa
1f8f70afcd1a29920cb75e403bc590ff	441dfedf0583e799d2b37619316f8d924250d878	741597e84ddd01ada0183d1345fd9e1a611cc2848
3d0320af4aeffa12660a3d4d8d6a5cf8	9dcf0be40d415c9cd86df39d608046a845b4a9e3	ee345b36a171cad3e0d3d010c0869901582de6a9

Aria-body loaders – 64bit

b65e38b86bdd048638e17487a9cce181	6fbd039cbdf2137a64390b80ba473949a3db5965	9033c75777e32c4014914272f78917e3d409c3191
97f3d2710d7b05fda7e53bda3cdbb3c8	088a603d6d144abb40145b6426acdad4b5813942	481a7868effd2d356f85d9372d1ab5e35e9345e5c1

Aria-body payload

2ce4d68a120d76e703298f27073e1682	a84bde7bd58616e6f20ba106ca6ef138e8cb6904	4cab6bf0b63cea04c4a44af1cf25e214771c4220ed4
a8ee5b59d255a13172ec4704915a048b	48d4fe2ca8e4d71eaa8dead6bae629de47ef77a7	04416f97890a7bbee354e1382b40823dfd74a69a23

e4f097ff8ce8877a6527170af955fc9b	4e76ad95cbfea448cb177c2de9c272141c11b8f4	2b67693cd1ba08b502d02e63550ad438b12b93b35
537b21c71eb8381ed7d150576e3e8a48	be04013156a96ffb50646c5de1b9a1d7de99f0d1	9728197c938baddbd638279f4bd5168c8ace09c5e3
43798a772bc4c841fc3f0b0aa157c1df	3223e64a1bfb25bc5ea95890ca438232adcc7c35	6e1591f794feca36f5aca5999f367525f58008c2722(
c4397694368a0bfcb27ee91457878ef1	608f101efc89fbaf3aa7737b248a91c3d7540d9d	7b4adfb5a6779bd0c89c470ed9aeea0e3a352e6d9e

Outlib.dll

63d64cd53f6da3fd6c5065b2902a0162	09690a61e5271619910a32efdc91e756d0a6dc1e	f0e40b94e5e4ccbf94c94843dd1eb8db21e36f5ec5d7

C&C Servers

realteks.gjdredj[.]com
spool.jtjewifyn[.]com
blog.toptogear[.]com
mon-enews[.]com
wdrfjkg129[.]com
n91t78dxr3[.]com
kyawtun119[.]com
www.ajtkgygth[.]com
news.nyhedmgtxck[.]com
dathktdga[.]com
www.rrgwmmwgk[.]com
dns.jmrmfitym[.]com
www.kyemtyjah[.]com
rad.geewkmy[.]com
cpc.mashresearchb[.]com
www.qisxnikm[.]com
dns.seekvibega[.]com
sugano.trictalmk[.]com
bbs.forcejoyt[.]com