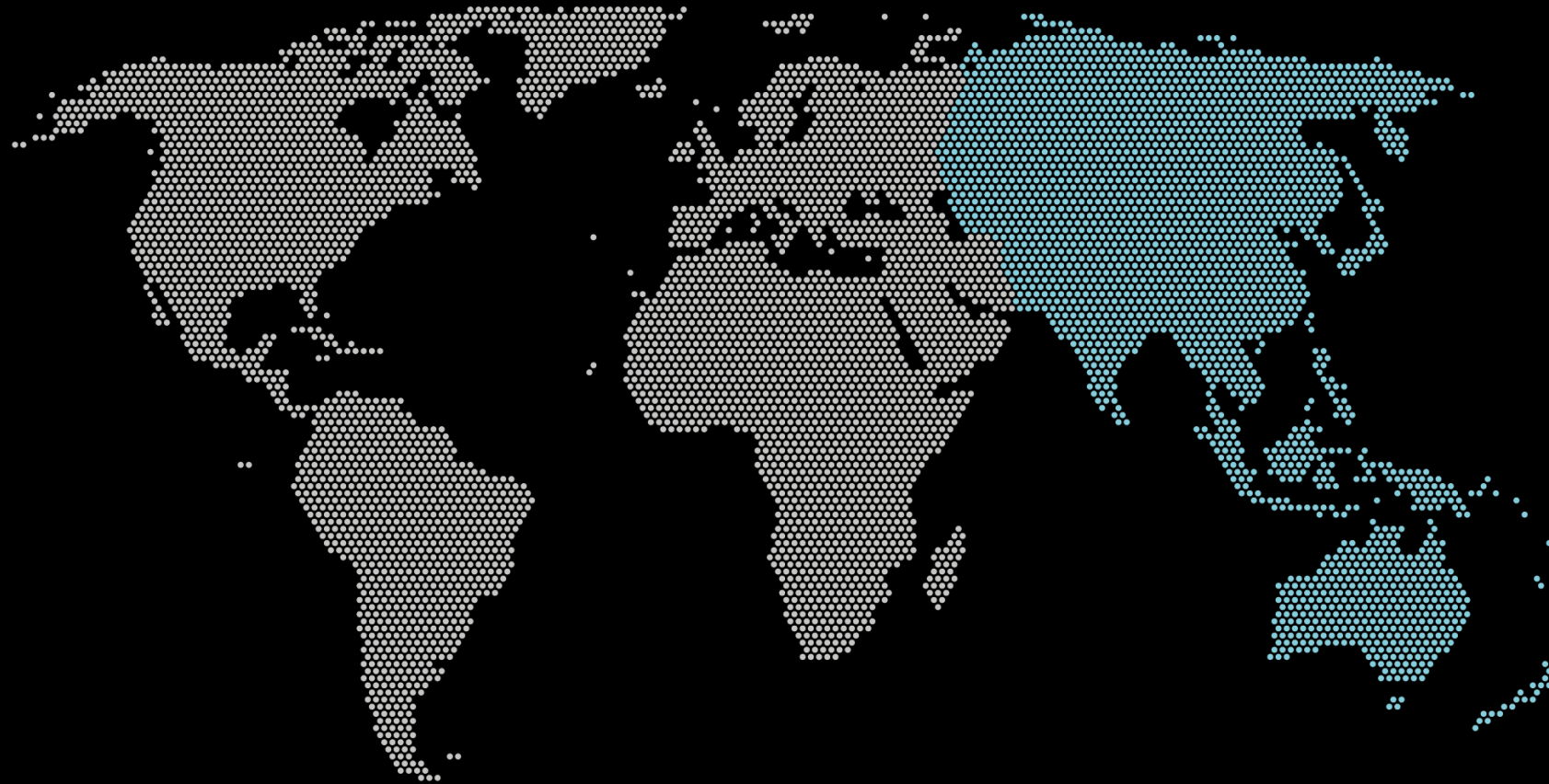


Cyber Espionage Reloaded



Derek Middlemiss

Head of Security Solutions EMEA – Security Evangelist

Cyber Espionage

- Target
- Infection Chains
- Infrastructure
- Tool Analysis
- Attribution
- Who is behind Naikon APT?
- Identifying Naikon



Cyber Espionage

- Target
- Infection Chains
- Infrastructure
- Tool Analysis
- Attribution
- Who is behind Naikon APT?
- Identifying Naikon



Discovered by Check Point

Australia, Indonesia, Philippines,
Vietnam, Thailand, Myanmar & Brunei
May 2020

Mongolian Public Sector
March 2020

Ukraine, Russia & Belarus
2016

Asia 2015
Project CAMERASHY

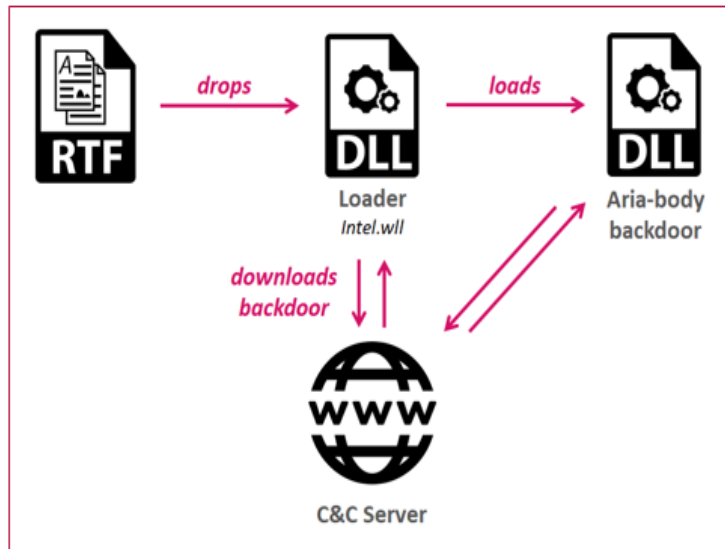
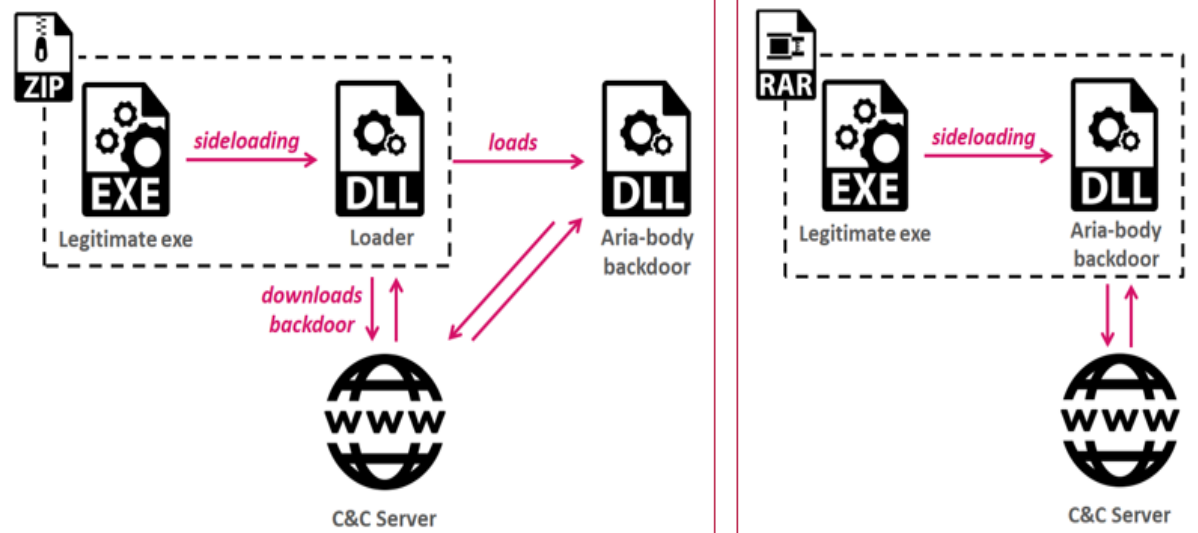
Singapore, Vietnam, Myanmar,
Philippines, Laos & Malaysia
2014 and Prior

Agenda

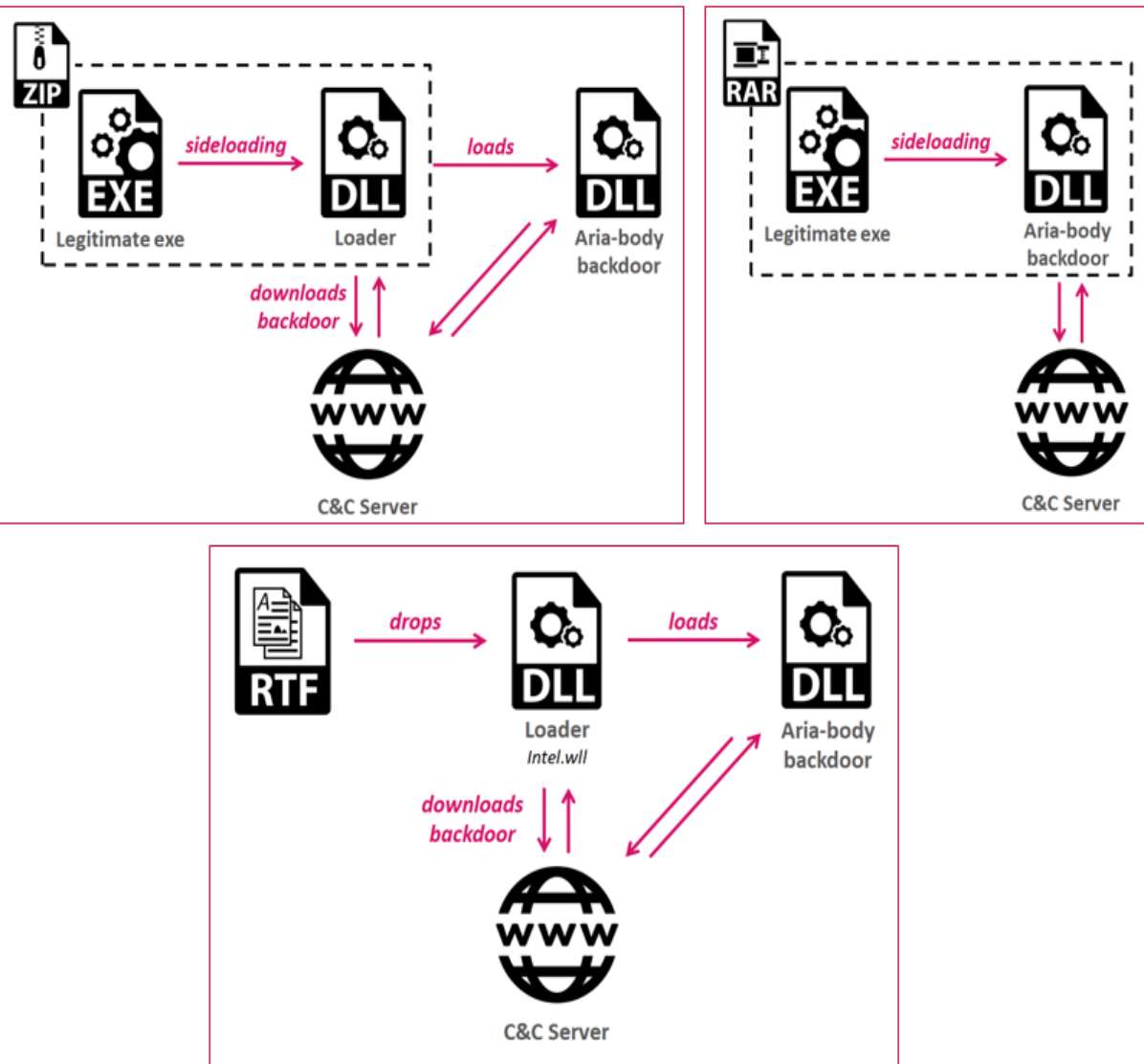
- Target
- Infection Chains
- Infrastructure
- Tool Analysis
- Attribution
- Who is behind Naikon APT?
- Identifying Naikon



Infection Chains



Infection Chains

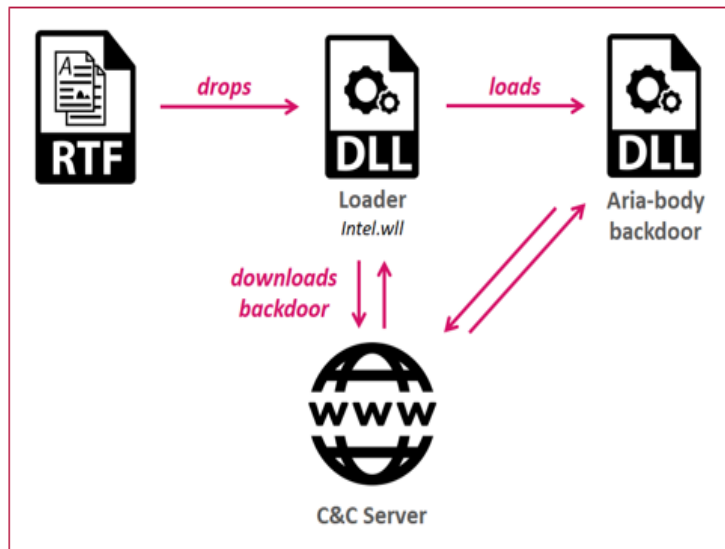
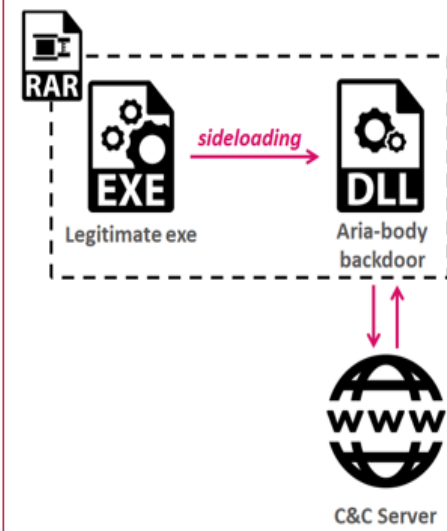
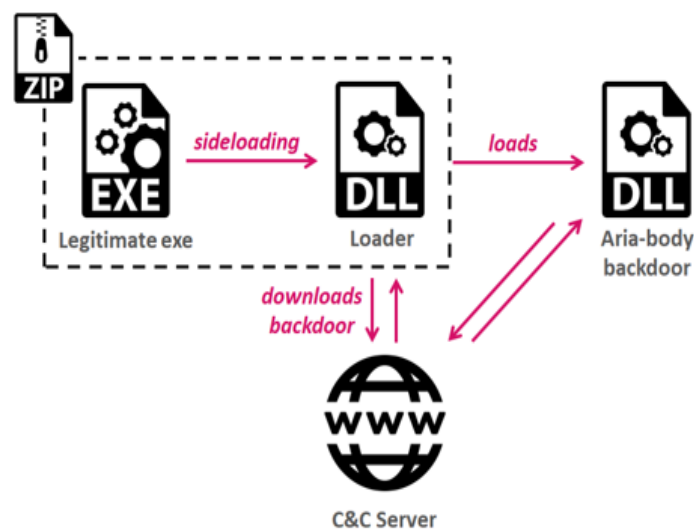


The Indians Way.doc

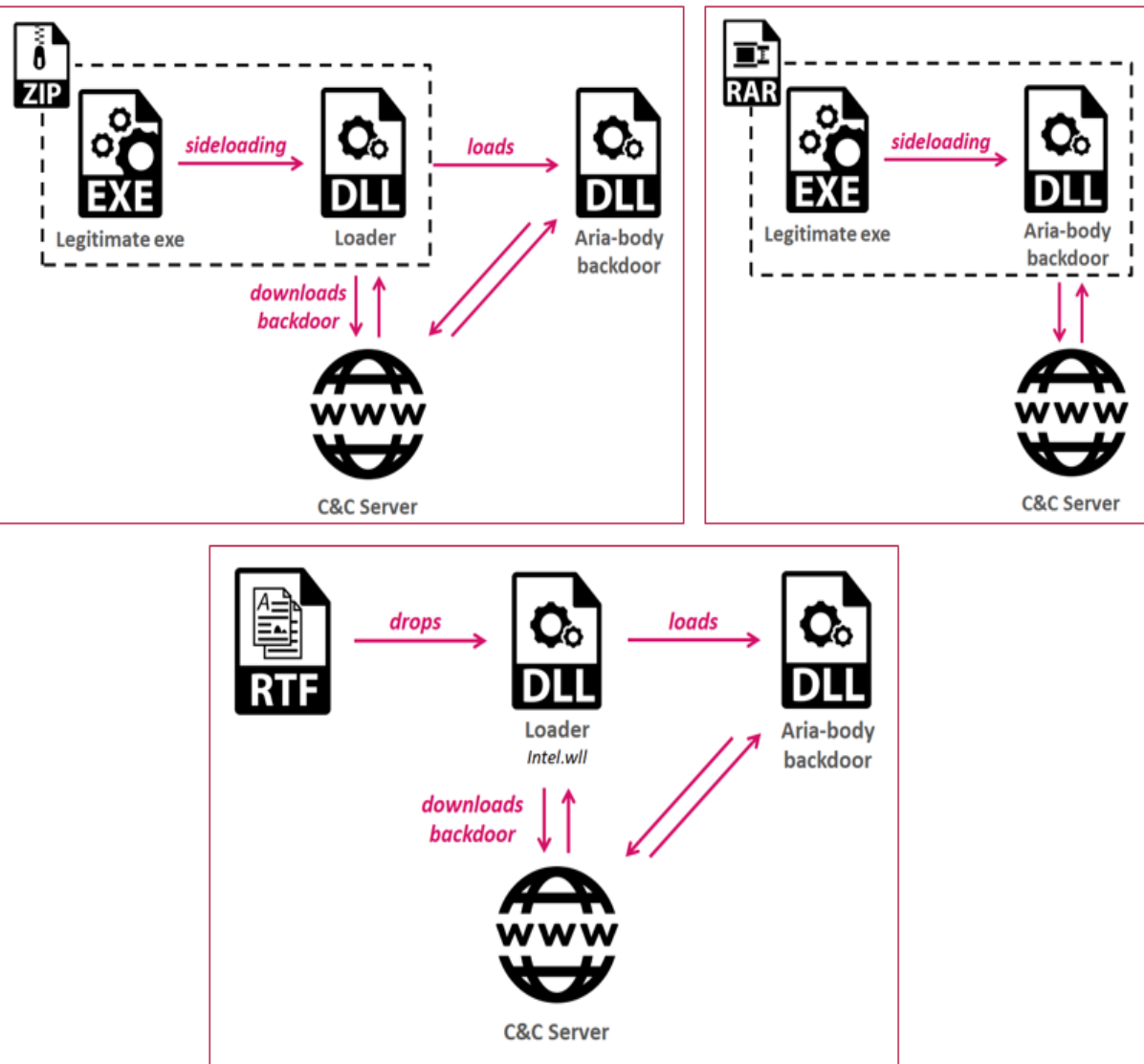
RoyalRoad

Intel.wll → WORD Startup Folder

Infection Chains



Infection Chains



The Indians Way.doc

RoyalRoad

Intel.wll → WORD Startup Folder

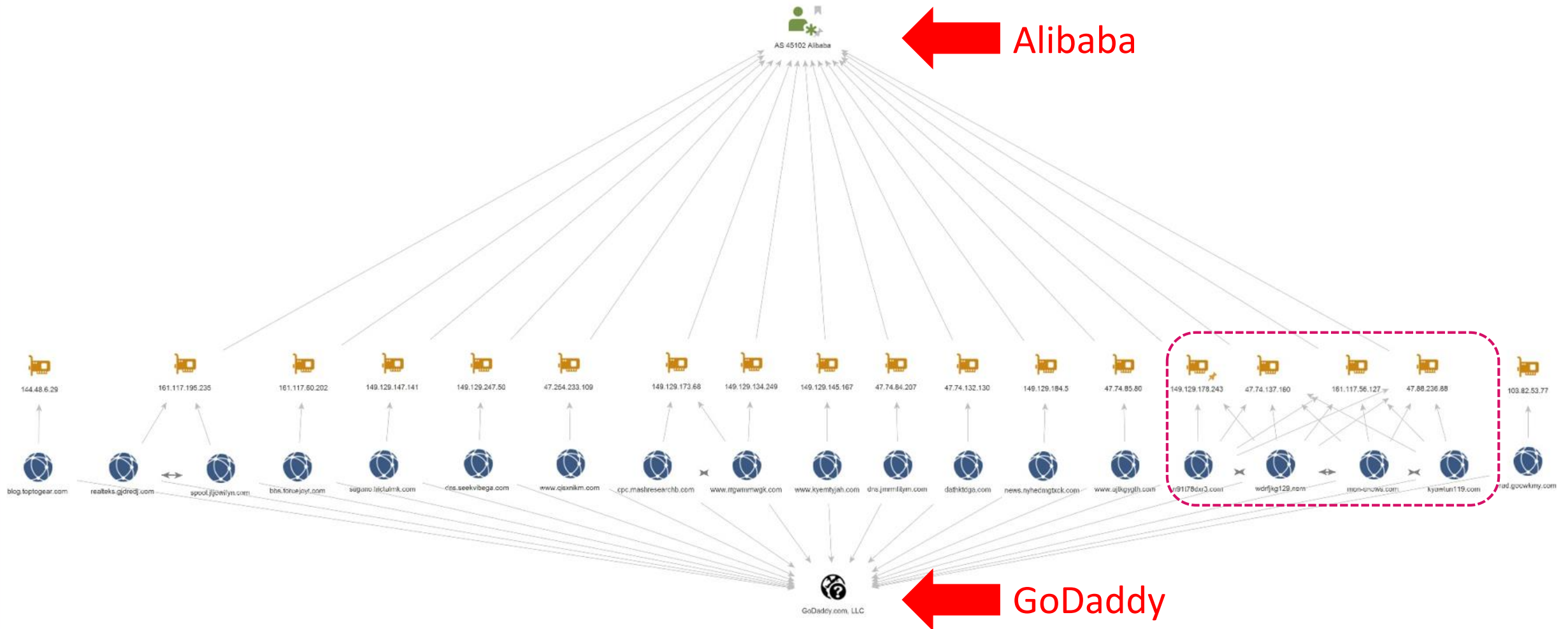
spool.jtjewifyfyn[.]com

Agenda

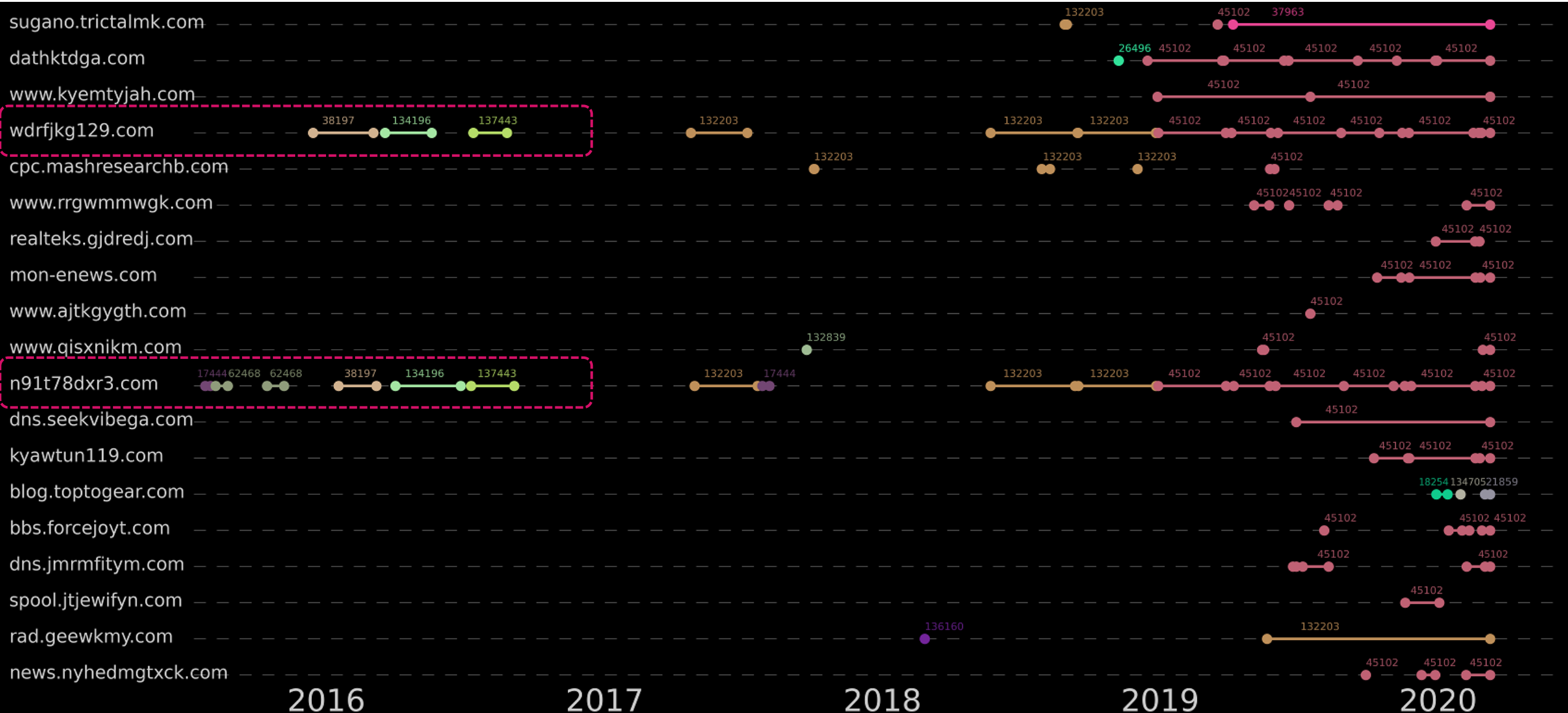
- Target
- Infection Chains
- Infrastructure
- Tool Analysis
- Attribution
- Who is behind Naikon APT?
- Identifying Naikon



Infrastructure



Infrastructure

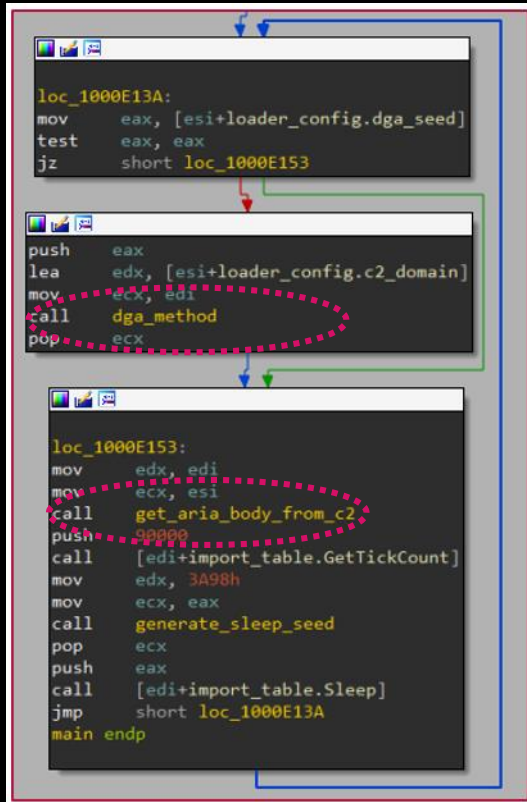


Agenda

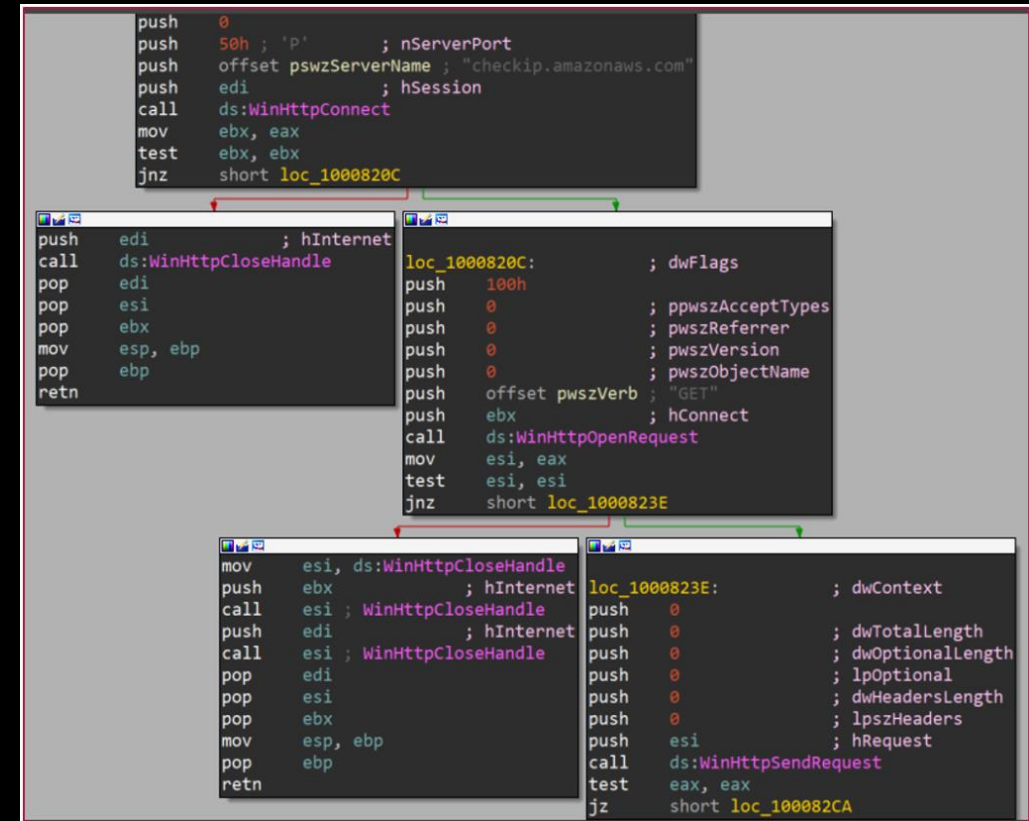
- Target
- Infection Chains
- Infrastructure
- Tool Analysis
- Attribution
- Who is behind Naikon APT?
- Identifying Naikon



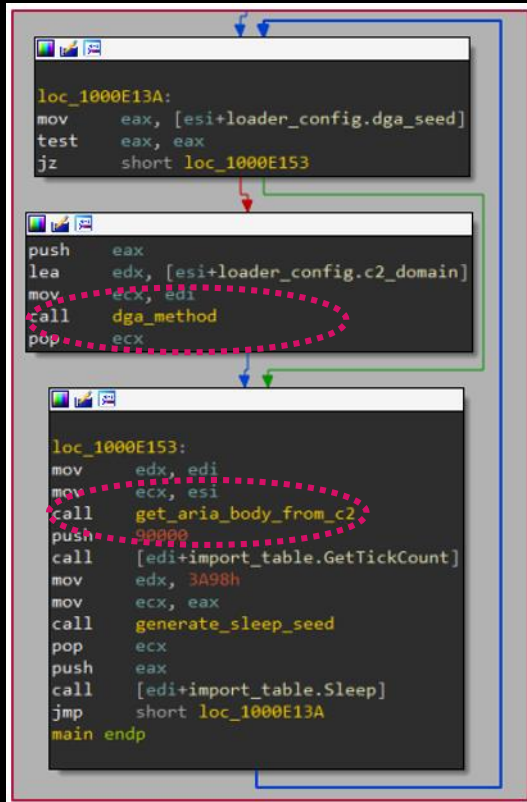
Tool Analysis



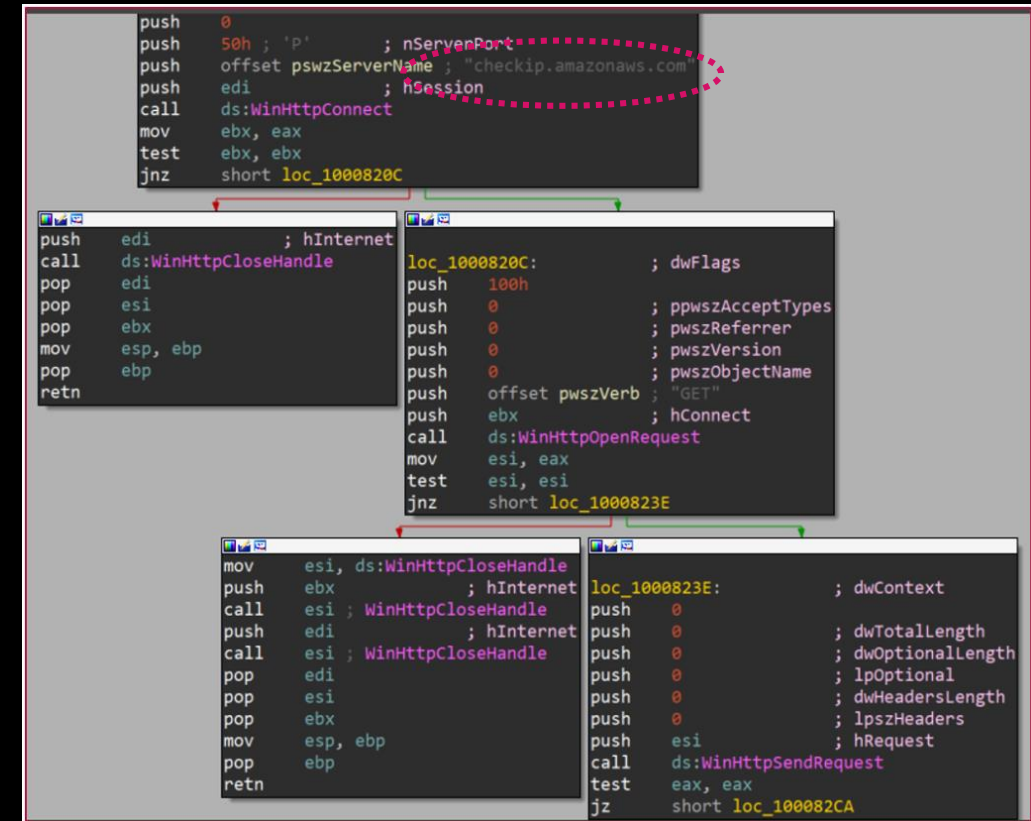
```
.rdata:1002D5AC  aAriaBodyDllx86 db 'aria-body-dllx86.dll'
.rdata:1002D5AC                                     ;
.rdata:1002D5C1  aAzmanager      db 'AzManager',0
.rdata:1002D5CB  aDebugazmanager db 'DebugAzManager',0
;
```



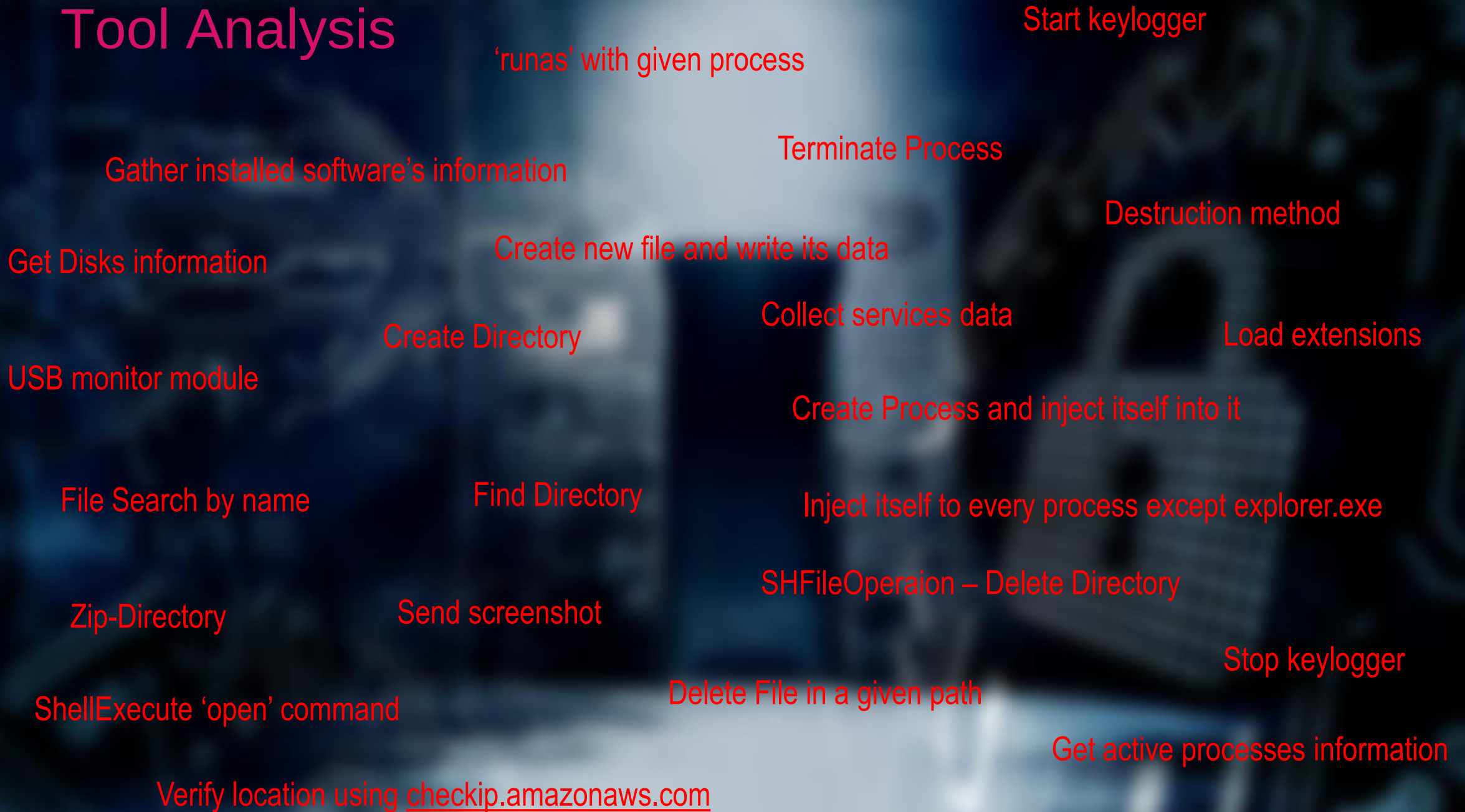
Tool Analysis



```
.rdata:1002D5AC    aAriaBodyDllx86 db 'aria-body-dllx86.dll'
.rdata:1002D5AC    ;
.rdata:1002D5C1    aAzmanager      db 'AzManager',0
.rdata:1002D5CB    aDebugazmanager db 'DebugAzManager',0
;
```



Tool Analysis



Agenda

- Target
- Infection Chains
- Infrastructure
- Tool Analysis
- Attribution
- Who is behind Naikon APT?
- Identifying Naikon



Attribution

1
2
3

```
aCreateDirector:                ; DATA XREF: Create_Directory+1Fto
    text "UTF-16LE", 'Create Directory [%s] succeeds!',0
; const wchar_t aCreateDirector
aCreateDirector:                ; DATA XREF: Create_Directory+39fo
    text "UTF-16LE", 'Create Directroy [%s] Failed:%d',0
; const wchar_t aRenameSSucceed
aRenameSSucceed:               ; DATA XREF: shfileoperation_rename+198fo
    text "UTF-16LE", 'Rename [%s] succeeds!',0
; const wchar_t aRenameSReturns
aRenameSReturns:              ; DATA XREF: shfileoperation_rename+1B8fo
    text "UTF-16LE", 'Rename [%s] returns:%d',0
    align 10h
; const wchar_t aDeleteDirector
aDeleteDirector:              ; DATA XREF: Delete_Directory+6Efo
    text "UTF-16LE", 'Delete Directory [%s] succeeds!',0
; const wchar_t aDeleteDirector_0
aDeleteDirector_0:            ; DATA XREF: Delete_Directory+85fo
    text "UTF-16LE", 'Delete Directory [%s] returns:%d',0
    align 4
; const wchar_t aFindfirstfileS_0
aFindfirstfileS_0:           ; DATA XREF: sub_10002400+88fo
    text "UTF-16LE", 'FindFirstFile [%s] Error:%d',0
```

3
1
2

```
; const wchar_t aDeleteDirector
aDeleteDirector:                ; DATA XREF: Delete_Directory+CEfo
    text "UTF-16LE", 'Delete Directory [%s] succeeds!',0
; const wchar_t aDeleteDirector_0
aDeleteDirector_0:            ; DATA XREF: Delete_Directory+FDfo
    text "UTF-16LE", 'Delete Directory [%s] returns:%d',0
    align 10h
; const wchar_t aCreateDirector
aCreateDirector:              ; DATA XREF: Create_Directory+7Afo
    text "UTF-16LE", 'Create Directory [%s] succeeds!',0
; const wchar_t aCreateDirector_0
aCreateDirector_0:            ; DATA XREF: Create_Directory+AFfo
    text "UTF-16LE", 'Create Directory [%s] Failed:%d',0
; const wchar_t aCloseTcpConne
```



Attribution

```
push    eax            ; lpData
push    0              ; lpType
push    0              ; lpReserved
push    offset aDisplayname ; "DisplayName"
push    [esp+7D8h+hKey] ; hKey
call    edi ; RegQueryValueExW
test    eax, eax
jnz     loc_10005971

lea     eax, [esp+7C4h+cbData]
push    eax            ; lpcbData
lea     eax, [esp+7C8h+var_678]
push    eax            ; lpData
push    0              ; lpType
push    0              ; lpReserved
push    offset aDisplayversion ; "DisplayVersion"
push    [esp+7D8h+hKey] ; hKey
mov     [esp+7DCh+cbData], 40h ; '@'
call    edi ; RegQueryValueExW
lea     eax, [esp+7C4h+cbData]
push    eax            ; lpcbData
lea     eax, [esp+7C8h+var_638]
push    eax            ; lpData
push    0              ; lpType
push    0              ; lpReserved
push    offset aInstalldate ; "InstallDate"
push    [esp+7D8h+hKey] ; hKey
mov     [esp+7DCh+cbData], 18h
call    edi ; RegQueryValueExW
lea     eax, [esp+7C4h+cbData]
push    eax            ; lpcbData
lea     eax, [esp+7C8h+var_620]
push    eax            ; lpData
push    0              ; lpType
push    0              ; lpReserved
push    offset aUninstallstrin ; "UninstallString"
```

Aria-body information gathering



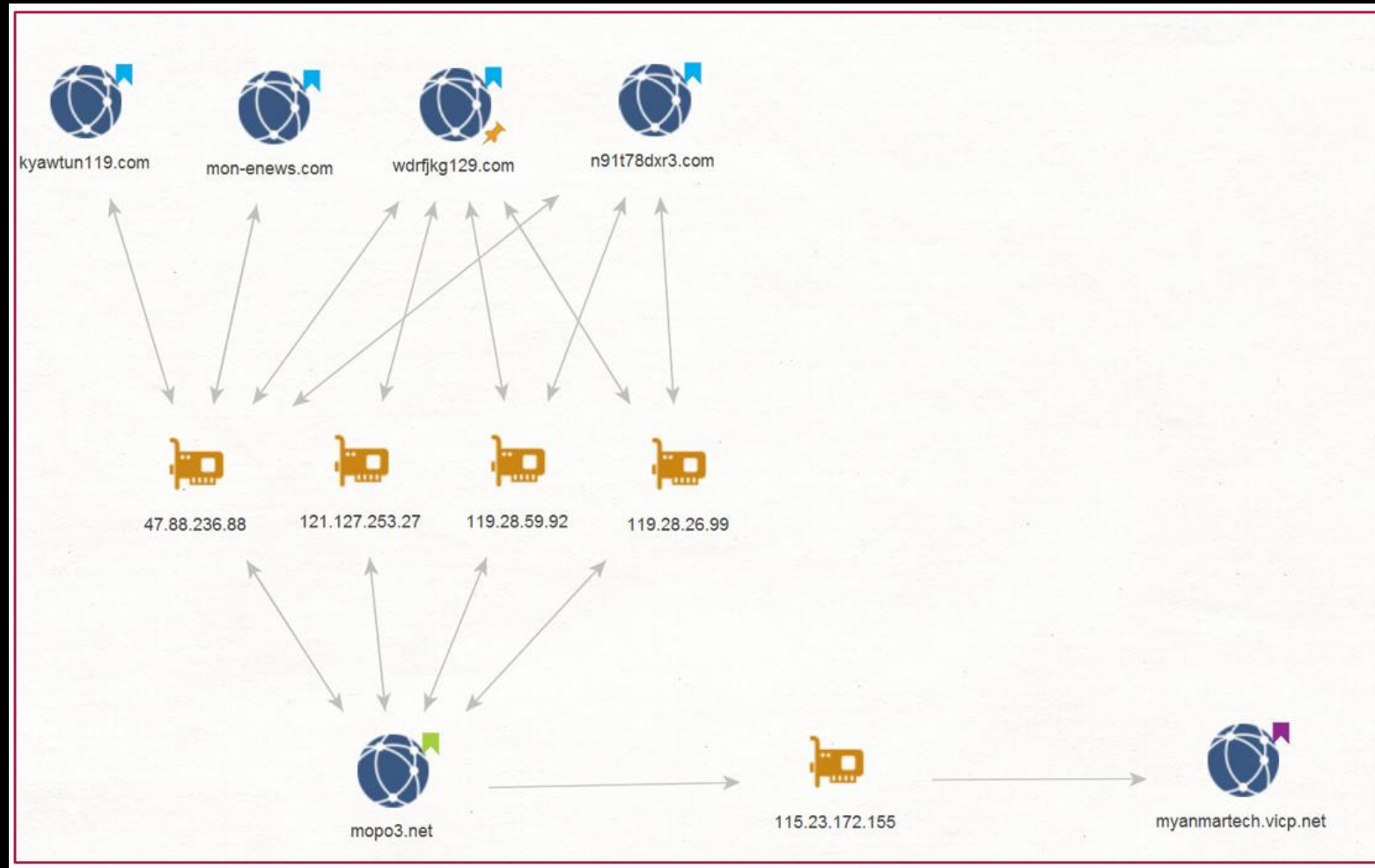
```
push    eax            ; lpData
push    0              ; lpType
push    0              ; lpReserved
push    offset aDisplayname ; "DisplayName"
mov     ecx, [ebp+hKey]
push    ecx            ; hKey
call    ds:RegQueryValueExW
mov     [ebp+var_21C], eax
cmp     [ebp+var_21C], 0
jnz     loc_10006962

mov     [ebp+cbData], 40h ; '@'
lea     edx, [ebp+cbData]
push    edx            ; lpcbData
lea     eax, [ebp+var_690]
push    eax            ; lpData
push    0              ; lpType
push    0              ; lpReserved
push    offset aDisplayversion ; "DisplayVersion"
mov     ecx, [ebp+hKey]
push    ecx            ; hKey
call    ds:RegQueryValueExW
mov     [ebp+cbData], 18h
lea     edx, [ebp+cbData]
push    edx            ; lpcbData
lea     eax, [ebp+var_650]
push    eax            ; lpData
push    0              ; lpType
push    0              ; lpReserved
push    offset aInstalldate ; "InstallDate"
mov     ecx, [ebp+hKey]
push    ecx            ; hKey
call    ds:RegQueryValueExW
mov     [ebp+cbData], 208h
lea     edx, [ebp+cbData]
push    edx            ; lpcbData
lea     eax, [ebp+var_638]
push    eax            ; lpData
push    0              ; lpType
push    0              ; lpReserved
push    offset aUninstallstrin ; "UninstallString"
```

XsFunction information gathering



Attribution



Agenda

- Target
- Infection Chains
- Infrastructure
- Tool Analysis
- Attribution
- Who is behind Naikon APT?
- Identifying Naikon



Who is behind Naikon APT?

State-sponsored operation

Target - Various government entities in APAC

Overlapping infrastructure with other state-based threat groups

Code similarity with another APT in this region

Agenda

- Target
- Infection Chains
- Infrastructure
- Tool Analysis
- Attribution
- Who is behind Naikon APT?
- Identifying Naikon



Identifying Naikon APT

Aria-body loaders – 32bit

e9a23e084eb8cf95b70cde3afc94534b
8561fa029f2158dc9932deee61febdac
31a4400789ae43b255464481320baa9e
32b1916abff8bf0e7c51a2584c472451
c2dc85559686575c268c8e97205b7578
b779742b94b9265338c9b21f0cc88ba4
ca3d5f02f453455f2b5522b8dceca658
bd1ef60ee835dd996ddcf4f22adaa142
1dd0e12a886f3d1bded6e26f53592720
07f724bdc662518ce6eac0ca723c929f
dde75e82b665fc7d47cd870dae2db302
20cdf05867967642742d6b947ba71284
9b0cb194dd5e49ab6fbf490de42e6938
b8292fe24db8f86b11e6bf303c5f3ac5
357a9f8268438d487303b267b26bde65
40c49ecbe1b7bd0dbb935138661b6ca4
85e5d261c810e13e781f24505bb265ce
77ea1eb5f6fd2605454764cd9b7ef62e
ab260f3dc1ead01dfc6b7139d1eb983c
897994f378577ec1e09eae953cf603f
1f8f70afcd1a29920cb75e403bc590ff
3d0320af4aeffa12660a3d4d8d6a5cf8

96a918b4e54090c0294470c872c1b2075af1a822
3cecff13388d6ab45797ca2455caf5fd04ca9dd9
1e3f303bbb35e709ff9d962c28c071656070aa98
513d99d714985ab53d75894357e4e87c69374862
b01d9454d84d04dd7a594dd2f899c77a40248618
3f7190d530a98e157d799bdbbe4fef8e69f1c50de
0289a6db2fdda581b413768cd9318f33b5c005e7
1d7056e1bec6fadfba8b69d725e4a930bdb6fa40
896e44af5a6f88c7be21d2f7225462f273f067f5
1eb758bcb0fc640835962aaa80199bdc867c79e7
2f17d1f1766b2814d6347763c9ad94863e5bd35c
31cf5cb37d1d6e62add2cd4e59c2821a1a3c54e5
396c0c1dce196e9dc4e65aeb57d2bd1ec5e85ba9
69ea467bdfe5b7739553da7f93096a3ac944270c
722b3dafbc14f8dce1048264451017d3f473f1ac
fe84b53aa8bb4e8ac3d2d9f86d2397d4a3cf5c08
6a5a96f5637c898c0792ca9e76fc1854cf960d59
653aae2210a256a00ead6495e2c128d36d2ed531
c2d3d9d7d7b64bbc6e522695105c31d5f1185800
799ffe499b1a0d4b58ad9fa7b065b03432b96a09
441dfedf0583e799d2b37619316f8d924250d878
9dcf0be40d415c9cd86df39d608046a845b4a9e3

1747fb340794c0c4e746b86c9a77fc568042be9d1dd9d7629b85e110aed34425
fe845ac7525daa5050dc17ca90352afe0f53c04a268832f4b0e93b1d90092175
8c38a9f38fd472867479cbaab9c138df616e60e3bb0863eb21531d68470ff302
a9f0df941172cc4a9c8b242fd41094033e15fa9c5e3781656df3888a4d47f834
fe02467d457e214e82a561de7cfa5e534efdb6beba7c624be2c7d854b68d9f97
f31a5d3d586924ea2fe274cc644e3d9501efcc452c150b28f9b1111578ded022
ca2da542ffdbf551a1fa46d073c63162747df7ab45b6c8890077ce783fcbd54e
510d91994c02e92e5354a9cdd51fd2be23583779e07222010a26063bfae2f314
4dcac1b42a0d2308136ce87db28856f1c1888dea0c07f4979f9a3da55268b5a2
45f2dbc7240023308e3193f29cc68320a176714e45dbe2ad7096f6f6445b0e4c
249ca984c1a508c4adbd58c3e3675bf22c8e364755250bc44a48913dfd6fe540
a5a0f9117a49ad7246882c938017a6f603180b37e6c6d134b744fb3fbe57722f
1732639fe36c3ffbe860c09a3b8b92115f31e94e9343cfc346c12048827e9a78
bfdf1c7437189306998cf6b9f1197bd5c77d85ae5595d1d64cb3fc422af1ff7b
7b336c7828027d6080617e0a619a0eb048be3c9724a42ad01739e1484383b284
0db51c4a2bd94f2b56f821a013fa42e0e67e3a7b69e2e8834fe36b10a49e2f66
d389780b530557e4076eecd0b2f92c955c581b23359315acb705cff1c8998f4
3d0e3136ed28397eaf4414aaa072ab11a1787ae0973666745add52d2f471b57b
d29692b12f865e5480ae97b507ccec96b32ab6784a4800be6d503ea6a2906bf9
7463d0f064a31b61ffedd0895ab242700d0d80fc2fa33663da70dcef11451f7d
741597e84ddd01ada0183d1345fd9e1a611cc284820f9af4557b738250f4f21c
ee345b36a171cad3e0d3d010c0869901582de6a992f36005e67843c9a9ead78b

Identifying Naikon APT

Delivery

f9d71f32de83f9ecfdc77801a71da7bf08428c94f45fb8ff568a4a288778dfb75e37131cbd756e10a9392d2280907592	560423901a746055a4890c87dabe2c2a59ee917a00934d22fb37b2def8276bc22ace5dc950b66227c0c39b4ffe6fa7ff627654fbdd53a3bf638da4cb	d6841b2a82904efc52c6b0b9375ddd3aa70de360c9f605341631358331a66ba07df5442e5c334eb81a2f871623fcbcd859148223ef2c543d6ffb0e628d02190d6a8f59ad46ad22f272d5617e8d8101af820772abd5b162e3e9a9cc5dfb2f46ac
--	--	--

Aria-body loaders – 64bit

b65e38b86bdd048638e17487a9cce18197f3d2710d7b05fda7e53bda3cdbb3c8	6fbd039cbdf2137a64390b80ba473949a3db5965088a603d6d144abb40145b6426acdad4b5813942	9033c75777e32c4014914272f78917e3d409c3191a48a47161e1c152520dc204481a7868effd2d356f85d9372d1ab5e35e9345e5c1062f7c9562f96152246da4
--	--	--

Aria-body payload

2ce4d68a120d76e703298f27073e1682a8ee5b59d255a13172ec4704915a048be4f097ff8ce8877a6527170af955fc9b537b21c71eb8381ed7d150576e3e8a4843798a772bc4c841fc3f0b0aa157c1dfc4397694368a0bfcb27ee91457878ef1	a84bde7bd58616e6f20ba106ca6ef138e8cb690448d4fe2ca8e4d71eaa8dead6bae629de47ef77a74e76ad95cbfea448cb177c2de9c272141c11b8f4be04013156a96ffb50646c5de1b9a1d7de99f0d13223e64a1bfb25bc5ea95890ca438232adcc7c35608f101efc89fbaf3aa7737b248a91c3d7540d9d	4cab6bf0b63cea04c4a44af1cf25e214771c4220ed48fff5fca834efa117e5db04416f97890a7bbee354e1382b40823dfd74a69a235373be55ebd28ec80353262b67693cd1ba08b502d02e63550ad438b12b93b355d16eaca3a9a056cc4b0cbd9728197c938baddbd638279f4bd5168c8ace09c5e3441010aa88964f6730e7c66e1591f794feca36f5aca5999f367525f58008c27220deedb69d288a2888915c7b4adfb5a6779bd0c89c470ed9aeea0e3a352e6d9edffb74a1fe3585544ead3a
--	--	--

Outlib.dll

63d64cd53f6da3fd6c5065b2902a0162	09690a61e5271619910a32efdc91e756d0a6dc1e	f0e40b94e5e4ccb94c94843dd1eb8db21e36f5ec5d7ef2a9512b026cef082e1
----------------------------------	--	---

C&C Servers

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

Thank you



Cyber Security Evangelist | Office of the CTO