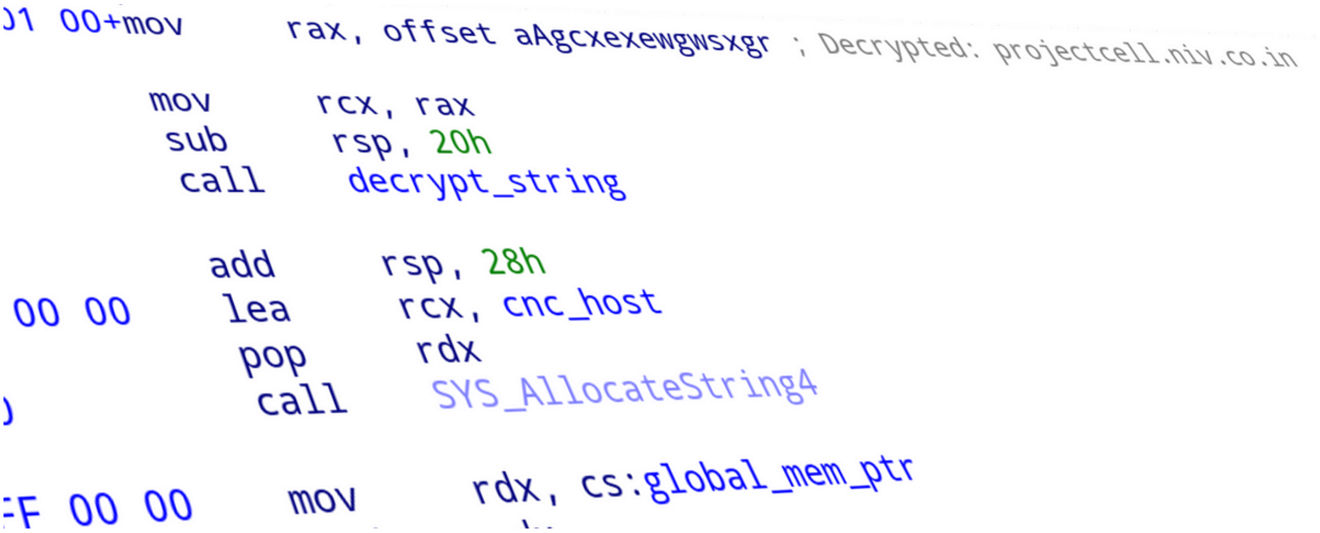
Andariel’s “Jupiter” malware and the case of the curious C2

medium.com/@DCSO_CyTec/andariels-jupiter-malware-and-the-case-of-the-curious-c2-dbfe29f57499

DCSO CyTec Blog May 16, 2023



```
01 00+mov       rax, offset aAgcxexewgwsxgr ; Decrypted: projectcell.niv.co.in
          mov       rcx, rax
          sub       rsp, 20h
          call      decrypt_string

          add       rsp, 28h
00 00     lea       rcx, cnc_host
          pop       rdx
)         call      SYS_AllocateString4

F 00 00       mov       rdx, cs:global_mem_ptr
```

DCSO CyTec Blog

--

Image of code from malware

Since 2020 DCSO has been monitoring a publicly undocumented malware family attributed to the Andariel group, a subgroup of the infamous North Korean Lazarus Group. The malware family has remained largely unchanged over the years and only made few appearances.

In early 2023 however, one such appearance seemed particularly noteworthy as the configured Command & Control suggests that the attackers have managed to compromise the web presence of the National Institute of Virology in India and possibly used it to control computers infected with the malware family.

In this blog post, we document the malware and discuss how this finding fits the attacker profile.

Blog authored by , , , , and colleagues.

Basic case information

In 2020, DCSO first came across an unknown malware family uploaded to VirusTotal. During our analysis we discovered that we weren’t the first to notice — we believe it to belong to the malware family dubbed “Jupiter” by BAE Systems, and attributed to the Andariel group.

Interestingly, the malware is written in PureBasic, a programming language that’s rarely used in malware creation (however, exceptions do exist). While the choice of programming language is rather exotic, the malware itself only offers basic download and shell command execution capabilities.

We then added custom rules for this family to our monitoring. Around a year later the rule produced another hit (the “OSPREY sample”, based on its code signature by “OSPREY VIDEO, INC.”) which we could attribute to a targeted attack attempt against a German medical/pharma company.

Code signing of the “OSPREY sample”

The malware family then disappeared from our radar, producing no hits in all of 2022. In the beginning of February 2023 however, it resurfaced in CISA’s AA23–040A alert (the “CISA sample”) hidden away in the IoCs related to the H0lygh0st ransomware, which is assessed to be of DPRK origin.

The “CISA sample” found in the IoCs of CISA’s AA23–040A alert

Analysis of the “CISA sample” revealed it to likely be older, with the timestamps dating it to 2021, the same year as the “OSPREY sample”. Then, a few weeks later our monitoring finally detected another sample and this time it appeared to be a fresh catch too, with timestamps indicating a compile time in mid January 2023.

The new sample, functionally unchanged, contained a very interesting Command & Control server, suggesting that the threat actors behind it might have managed to compromise the web server for the *National Institute of Virology* of India, or NIV in short, a designated BSL-4 research center authorized to test highly contagious viruses impacting humans.

Sample recorded trying to fetch commands on VirusTotal

At the time of finding the sample, we were unable to receive actual commands from the configured C2 so it remains inconclusive if the compromise took place. However, the configured path does closely resemble another path that we believe was used by the real web page at some point — further indicating that a compromise took place and was intentionally chosen to blend in:

Resource path indexed by Google, note the additional “s” in “scientifics”

For similar attacks it is also documented that commands are closely guarded and only issued to requests coming from expected source IPs, typically returning 404 for anyone else in order to keep a low profile.

Background

So while we do not have definite proof of a compromise, DPRK actors targeting the NIV (either as the intended target or in order to attack other targets in the general nexus of the NIV such as other medical companies) would fit the attacker profile very well.

DPRK actors and India

DPRK actors targeting India is not new either. North Korea-linked threat actors have continued to target public and private sectors in India with a broad-based victimology including a space agency, a nuclear power plant, as well as the energy sector and medical research previously. Campaigns against strategically sensitive targets have mostly been motivated by the need to siphon-off sensitive information.

The healthcare and medical research sector has been continuously targeted by DPRK threat actors with a significantly increased tempo during the COVID-19 pandemic. In 2020, suspected North Korean hackers tried to break into various healthcare companies, likely for intelligence gathering and espionage purposes, including Oxford’s AstraZeneca. Additionally, Microsoft reported that North Korean ZINC and Cerium have taken aim at multiple healthcare entities, including vaccine makers and COVID test developers. Furthermore, South Korean intelligence suspected that North Korea attempted to steal the COVID-19 vaccine from Pfizer in February 2021.

The DPRK and COVID-19

The outbreak of the COVID-19 pandemic isolated the “hermit state” even further from the international community. Following the rapid spread of COVID-19 infections in China, North Korea shut down any cross-border exchanges in January 2020, which has largely been maintained ever since. In August 2022, Kim Jong-un announced that COVID-19 was eradicated. (According to state media reporting, only 74 people died between the first publicly disclosed case in April and August 2022.) However, Pyongyang again saw a rising numbers of “respiratory illness” in January 2023, leading to a 5-day lockdown in the capital indicating that North Korea still continues to struggle with COVID-19 infections.

So far, Pyongyang has repeatedly turned down international offers for vaccines such as Russia’s Sputnik V in April 2021, offers by South Korea in May 2021, and three million doses of Chinese SINOVAC vaccines as part of a United Nations-backed COVAX initiative in September 2021. One year later, in September 2022, North Korea started its first vaccination campaign in border cities to China and Russia. Media reporting claimed they had received doses from China, probably SINOVAC, alongside other medical supplies to ensure an adequate health care provision.

Country-wide distribution of a vaccine poses a bigger challenge though. mRNA vaccines like Pfizer and Moderna require ultra-cold temperatures but the country's existing cold chain distribution system is only designed for 2°C — 8°C. With the refusal of SINOVAC, Sputnik V and AstraZeneca, the state might thus be looking for alternatives. As such, the Indian vaccine COVAXIN may be of special interest, as COVAXIN is relatively easy to store, making it particularly attractive to lower and middle-income countries like North Korea.

The DPRK's present COVID situation and the country's vaccine supply restraints as well as previous patterns provide strong motive for targeting the NIV as a leading health research center with a focus on COVID. The NIV has played a crucial role in India's fight against COVID-19 for example, being a forerunner in the areas of vaccine development, genome sequencing and testing supplies. The NIV has also been recognized by the WHO as "a collaborating centre for emerging and re-emerging infectious diseases."

Technical Details

Investigating the Command & Control

The Command & Control `projectcell.niv[.]co.in` resolves to `173.249.33[.]80`, which is allocated to German mass-hosting provider Contabo GmbH. No other FQDNs have been seen on this IP address thus far.

`niv[.]co.in`, however, resolves to `173.249.44.87`, also allocated to Contabo GmbH, and appears to be used as a mass-hosting web server by an Indian marketing and web development company, I Knowledge Factory (IKF). Perhaps unsurprisingly, a variety of legitimate domains resolve to it, all seemingly belonging to legitimate Indian entities. An IKF mail server is also used (through a CNAME) as an MX record for niv[.]co.in.

It remains unclear at the time of writing why IKF chose to host at least some of their customers' infrastructure in Germany, far away (in both geographic and network terms) from their (presumed) main audience in the India vicinity.

Further, IKF's nameserver setup struck us as odd, with the primary nameserver serving niv[.]co.in and others, ns.iknowledgefactory.com, resolving to `103.73.189.76` — allocated to Evoke Digital Solutions in India — while having its PTR DNS record set to email.Ikf.in. This domain (note the similarity of "I" and "i") however is currently available for sale, and does not seem to be under control of IKF anymore.

According to `niv[.]co.in`'s SPF policy, any IP address `projectcell.niv[.]co.in` resolves to is explicitly permitted to emit e-mails for this domain. This includes `173.249.33[.]80`, which DCSO assesses as likely being under control by Andariel.

Lastly, it has to be noted that the official website of the National Institute of Virology is `niv.icmr.org.in`, a fact also advertised on `niv[.]co.in` — which appears to have been abandoned by NIV or IKF commencing October 2022. Rather than letting previously used domains orphan or even expire, it is crucial to set up proper redirects to the new primary domain, and ensure the respective organization maintains control over its domain set all the time.

Malware analysis

The malware itself is a basic loader. It can download files, execute shell commands and send back the console output.

Communication happens via HTTP which is manually implemented using socket functions, and as such it is not capable of communicating with HTTPS servers.

The client transfers data via POST requests, in which the data fields are encrypted using a simple rotating xor + base64.

Example request
We've identified the following fields:

```
id=          Xor keypage=        Status code (not encrypted)query=       Basic client
inforep0=        Shell command output
```

The `page` field contains basic client info, such as:

`10.0.0.1|DESKTOP-BI961TX|batman|110|64`

where the first field is a collection of local IP addresses, followed by the computer name, username, Windows version as well as bitness of the system.

The server then responds either with HTTP 504, which signals the bot to stop running, or HTTP 500 which may contain a command and/or download payload in the HTTP body.

In case of HTTP 500 (shell command and/or download task) the HTTP body adheres to the following format:

```
[10 bytes unused][8 bytes check string][8 bytes xor key][1 byte shell command length]
[* shell command][1 byte download target path length][* download target path][*
download payload]
```

All fields following the xor key are encrypted with it using a simple rolling xor scheme.

The check string appears to be a magic 8 byte value the client verifies with a simple algorithm, which is satisfied by the following magic bytes:

```
0b 15 1f 29 33 3d 47 51
```

Example code of the check algorithm in Python:

```
for i in range(8):    assert(check_string[i] == ((i+1)*10+1))
```

Based on this, we've created a Suricata rule which we're distributing as part of the IoCs.

If a download target path is specified in the response, the malware will write the payload to the specified path and copy `Explorer.exe`'s timestamps to it in order to disguise the file. In case the downloaded file is an EXE file it will also pad the executable with 40,000,000 (~40MB) random bytes on disk, likely to exceed some security software's file limits and/or generate a unique hashsum for downloaded binaries.

If a shell command is specified, the malware will execute the shell command, capture the output and send the contents back to the C2 using the `rep0` POST request field.

IoCs

You can also find the accompanying IoCs in form of a MISP event on our GitHub.

```
Samples
c28bb61de4a6ad1c5e225ad9ec2eaf4a6c8ccfff40cf45a640499c0adb0d8740
9a5504dcfb7e664259bfa58c46cfd33e554225daf1cedea2ec2a9d83bbbfe238
aa29bf4292b68d197f4d8ca026b97ec7785796edcb644db625a8f8b66733ab54
772b06f34facf6a2ce351b8679ff957cf601ef3ad29645935cb050b4184c8d51
664f8d19af3400a325998b332343a9304f03bab9738ddab1530869eff13dae54
34d5a5d8bec893519f204b573c33d54537b093c52df01b3d8c518af08ee94947



C2
hxxp://projectcell.niv.co[.]in/non_scientific/service.php
hxxp://40.121.90[.]194/help.php
hxxp://3.89.226[.]234/login.php
hxxp://sora[.]bz/xoops_root_path/uploads/information/about.php
hxxp://sora[.]bz/xoops_root_path/templates_c/login.php
hxxp://eflow.co[.]kr/member_image/about.php



Mutex
P_FLY_H@CK

alert http any any -> [$HOME_NET] any (msg: "DCSO MALWARE Andariel C2";
flow:to_client; http.response_body; content:"|0b 15 1f 29 33 3d 47 51|"; offset:10;
depth:10; reference:url,https://medium.com/@DCSO_CyTec/49a9d04acbc6;
classtype:command-and-control; sid:3200000; rev:1;)
```