Karkoff 2020: a new APT34 espionage operation involves Lebanon Government

blog.yoroi.company/research/karkoff-2020-a-new-apt34-espionage-operation-involves-lebanon-government/

March 2, 2020

Introduction

In November 2018, researchers from Cisco Talos tracked and detailed a "*DNSEspionage"* campaign against targets in Lebanon and UAE. At the time of the report, the threat actor carried out a cyber espionage campaign by redirecting DNS traffic from domains owned by the Lebanon government to target entities in the country.

In April 2019, Cisco Talos discovered evidence of the link between APT34 (codename Helix Kitten or OilRig) and the "*DNSEspionage" operation*. Talos analysts discovered several overlaps in the infrastructure employed by attackers and identified common TTPs. They tracked this new implant "Karkoff".

Experts from Cybaze/ Yoroi Zlab, as part of ordinary Threat Intelligence activities, spotted a new sample which they believe to be an update of the Karkoff implant. It could prove that APT34 is still active and threat actors used it in a new campaign that appears to be active at the time of writing. The APT group made some changes in its technique, tactics, and procedures, but the target is the same, the Lebanon Government.

In this campaign, the APT group may have compromised a Microsoft Exchange Server belonging to a Lebanon government entity, in fact, we found some evidence in the communication logic.

This new implant has some similarities with the samples of Karkoff involved in past campaigns, including:

- similar Macro structure
- .NET modular implant with similar logic
- exploit Microsoft Exchange Server as communication channel

Moreover, the new Karkoff implant implements a new reconnaissance logic in order to drop the final payload only to specific targets, gathering system information, the domain name, hostname and running Operating System.

Update

A few hours before this report has been publicly disclosed, malware researchers at the Italian cyber security firm Telsy also published their analysis.

Both reports are related to the same sample, but let me suggest reading both analyses to have a clear vision of the threat actors and all the technical details related to the implant. The report published by Telsy is available here: LINK.

Technical Analysis

Hash	926e29f9242feb3e11c532616f7c90c5d7acab115d38ebf748cabaaa6a2a3667
Threat	APT34 Karkoff macro loader
Brief Description	Malicious Excel macro
Ssdeep	24576:zLNkxqHOPi1K5sLMKd2rVIehO/KBhjPyVuVX/+2PPbK:wl4E

Table 1. Sample information

The Malware is an Excel Document with a malicious macro embedded. The following image (Fig:1) shows the highlights of the extracted code.

Fig.1. Malicious Macro: drop and execute monitor.exe

The macro extracts a custom base64 code from the body of the file and, after a decoding routine, it downloads an executable file into the following path "*C:\Users\public\.Monitor\monitor.exe*". Persistence is assured by scheduling a new task named SystemExchangeService.

Fig.2.Persistence with SystemExchangeService

The extracted payload is summed up as follows: :

Fig.3.Static details of monitor.exe

The payload were not obfuscated at all. This made a simple and quick analysis.

As shown in the above figure, the creation date is on 29 February, this is an indicator of the recent build of this implant. Moreover, a small file size (1.13MB) allows malicious content to be downloaded and executed quickly.

Fig.4. details of compromised mail exchange server parameters

As the first step, as shown in Fig 4, the sample tries to connect to its own command and control server, which happens to be an Exchange mail server belonging to the Lebanon government. Once it connects, the C2 answers back with the list of available commands as attachments in a replied e-mail. Fig 5 shows the GetList function from where we might appreciate the eMail body decoding process. From the body, a custom encoded string is decoded and later it is interpreted as a command.

Fig.5. detail of GetList function responsible for getting the list of available commands as mail attachments

Following our analysis, we noticed the malware tries to connect back and forth to its C2 to get authorization and to share detailed information about the infected system. It used "UserAgent" of the exchange client. Fig 6 shows details on what is hijacked from the victim's side.

Fig.6. details of Information stolen on the victim's machine

Another evidence is the domain registration of the second command control: it has been registered on January, 27, probably indicating the date of the beginning of the new attack.

Fig.7. details of domain registration godoycrus[.com

Conclusions

APT34 is still active, and this campaign against the Lebanon government demonstrates it. The new version of the Karkoff malware is the demonstration that the Iran-linked APT34 cyberespionage group continues to improve its arsenal. The sample involved in this campaign implements new reconnaissance capabilities, it implements a covert and effective C2 communication channel through the use of the Microsoft Exchange Protocol.

The Group likely exploited or brute-forced a Lebanon related mail account with another tool of its arsenal, the JASON tool. The Jason tool was leaked at the end of 2019, it could be used by attackers to carry out bruteforce attacks on exchange servers.

Indicators of Compromise

- Hashes
  - 59cbc7e788425120c2dde50f037afbf3b1d2108c0b7e27540e924cad2463fe5b
  - 26995a1cd99a5c70fd7bfa925cb0bbbdbd419bedc2d664dffd3b7c57ad07de66
  - 1b2c5354eb567132a341c1b15ad5cc71c3f5ba8e2788b67c0fbc0e7993beb1d2
  - ebae23be2e24139245cc32ceda4b05c77ba393442482109cc69a6cecc6ad1393
  - 678d59bcd469e4cf236c7af7517c54ab9ad643523383875bd875131d7130941f
- C2

  godoycrus[.com
- Persistence

  Set Task scheduler

Yara Rules

```
rule Karkoff_Attack_2020_Excel_macro {
        meta:
        description = "Yara Rule for new APT34 Karkoff campaign excel malicious
macro"
        author = "Cybaze Zlab_Yoroi"
        last_updated = "2020-03-02"
        tlp = "white"
        category = "informational"

        strings:

           $a1 = "EncodedData0"
           $a2 = "NewTask9"
           $a3 = "EAAMYEKwUAAEsEWQUAAMYEnQUAAMYEqAUAAJwSrgU"
           $a4 = "TVqQAAMAAAAEAAAA"
    condition:
        all of them

}


rule Karkoff_Campaign_2020 {
        meta:
                description = "Yara Rule for new APT34 Karkoff campaign"
                author = "Cybaze Zlab_Yoroi"
                last_updated = "2020-03-02"
                tlp = "white"
                category = "informational"

        strings:

           $a1 = "SystemExchangeService" ascii wide
           $a2 = "getWindowsVersion" ascii wide
           $a3 = "GetCommands" ascii wide
           $s1 = {0A 7A 1E 02 7B 9C 12 00 04 2A}

    condition:
        uint16(0) == 0x5A4D and all of them

}
```