McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service – Crescendo

securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-crescendo/

October 21, 2019

Episode 4: Crescendo

This is the final installment of the McAfee Advanced Threat Research (ATR) analysis of Sodinokibi and its connections to GandGrab, the most prolific Ransomware-as-a-Service (RaaS) Campaign of 2018 and mid 2019.

In this final episode of our series we will zoom in on the operations, techniques and tools used by different affiliate groups spreading Sodinokibi ransomware.

Since May we have observed several different modus operandi by different affiliates, for example:

- Distributing the ransomware using spear-phishing and weaponized documents
- Bat-files downloading payloads from Pastebin and inject them into a process on the operating system
- Compromising RDP and usage of script files and password cracking tools to distribute over the victim's network

- Compromise of Managed Service Providers and usage of their distribution software to spread the ransomware

To understand more about how this enemy operates, we in McAfee Advanced Threat Research (ATR) decided to operate a global network of honeypots. We were aware of the lively underground trade market of RDP credentials and were curious about what someone would do with a compromised machine. Would they distribute the Sodinokibi ransomware? Would they execute the DejaBlue or BlueKeep exploits? Our specially designed and built RDP honeypots would give us those insights.

Like Moths to a Flame

From June until September 2019, we observed several groups compromise our honey pots and conduct activities related to Sodinokibi; we were able to fully monitor attackers and their actions without their knowledge.

It is important to note the golden rule we operated under: the moment criminal actions were prepared or about to be executed, the actor would be disconnected and the machine would be restored to its original settings with a new IP address.

We noticed some of our honeypot RDP servers were attacked by Persian-speaking actors that were actively harvesting credentials. Our analysis of these attacks led us to various Persian underground channels offering the same tools we observed appearing in Sodinokibi intrusions. Some of these tools are closed source and custom made, originating from within the channels in our analysis.

In this blog we will highlight a few of the intrusions we observed.

Group 1 – Unknown Affiliate ID

McAfee ATR observed initial activity against our South American honey pot begin in late May 2019. We had full visibility as the actor loaded a number of tools, including Sodinokibi, during the initial intrusion period.

The following ransom note (uax291-readme.txt) was dropped onto the system on June 10th, 2019. The actor utilized Masscan and NLBrute to scan and target other assets over RDP which fits with the behavior we have seen in all other Sodinokibi intrusions tracked by McAfee ATR. The actor then created a user account ‘backup’ and proceeded to consistently connect from an IP address range in Belgrade, Serbia.

Group 2 – Affiliate ID 34

Campaign 295 (based on sub-ID in the malware configuration)

The following Sodinokibi variant appeared in our South American honey pot with the original file name of H.a.n.n.a.exe.

8d7d333574708c2fe5c37fad1bdfbc5a9664b33d (June 8th, 2019)

Extracting the configuration from the ransomware sample as we conducted during our affiliate research, the affiliate-id is nr 34.

Upon initial intrusion, the actor created several user accounts on the target system between June 10th and June 11th. The malware Sodinokibi and credential-harvesting tool Mimikatz were executed under the user account “ibm” that the actor created as part of the entry into the system

Further information revealed that the actor was connecting from two IP addresses in Poland and Finland via the ‘ibm’ account. These logins originated from these countries in a 24hr period between July 10th and 11th with the following two unique machine names WIN-S5N2M6EGS5J and TS11. Machine name WIN-S5N2M6EGS5J was observed to be used by another actor that created the account “asp” and originated from the same Polish IP address.

The actor deployed a variant of the Mimikatz credential harvester during the intrusion, with the following custom BAT file:

```
@echo off
move %userprofile%\Desktop\mimi\x64\admin.bat C:\windows\debug
move %userprofile%\Desktop\mimi\x64\back.bat C:\windows\debug
regedit /s %userprofile%\Desktop\mimi\x64\registery.reg
@setlocal enableextensions
@cd /d "%~dp0"
IF "%PROCESSOR_ARCHITECTURE%"=="x86" (
Win32\mimikatz.exe privilege::debug sekurlsa::logonPasswords exit> "%userprofile%\Desktop\mimi\qwe.txt" | echo Executed 32. You can close .
) else (
echo bit=x64
x64\mimikatz.exe privilege::debug sekurlsa::logonPasswords exit> "%userprofile%\Desktop\mimi\qwe.txt" | echo Executed 64. You can close .
)
pause
edit
```

We have seen a consistent usage of various custom files used to interact with hacking tools that are shared among the underground communities.

Another tool, known as Everything.exe, was also executed during the same period. This tool was used to index the entire file system and what was on the target system. This tool is not considered malicious and was developed by a legitimate company but can be used for profiling purposes. The usage of reconnaissance tools to profile the machine is interesting as it indicates potential manual lateral movement attempts by the actor on the target system.

July 20th to 30th Intrusion

Activity observed during this period utilized tools similar to those used in other intrusions we have observed in multiple regions, including those by Affiliate ID 34.

In this activity McAfee ATR identified NLBrute being executed again to target victims over RDP; a pattern we have seen over and over again in intrusions involving Sodinokibi. A series of logins from Iran were observed between July 25th and July 30th, 2019.

We have also seen crypto currency mining apps deployed in most of the intrusions involving Sodinokibi, which may suggest some interesting side activity for these groups. In this incident we discovered a miner gate configuration file with a Gmail address.

Using Open-Source Intelligence (OSINT) investigation techniques, we identified an individual that is most likely tied to the discovered Gmail address. Based on our analysis, this individual is likely part of some Persian-speaking credential cracking crew harvesting RDP credentials and other types of data. The individual is sharing information related to Masscan and Kport scan results for specific countries that can be used for brute force operations.

ACTOR PROFILE

Further, we observed this actor on a Telegram channel discussing operations which align to the behavior we observed during intrusions on our honey pot. The data shared appears to be results from tools such as Masscan or Kport-scan that would be used to compromise further assets.

DISCUSSION OF SCANNING IN FARSI, ON PRIVATE CHANNEL

Other tools were found to have been executed the same day as the activity documented include:

Mimikatz

Was executed manually from the command line with the following parameters:

mimikatz.exe “privilege::debug” “sekurlsa::logonPasswords full” “exit”

- **Slayer Leecher**
- **MinerGate**

Group 3 – Affiliate ID 19

We observed the following Sodinokibi ransom variants attributed to this affiliate appearing in the honey pot in the Middle East. The attacker downloaded a file, ابزار کرک.zip, which can be mostly found in Farsi language private channels. The tool is basically a VPS Checker (really an RDP cracker) as discussed on the channels in the underground.

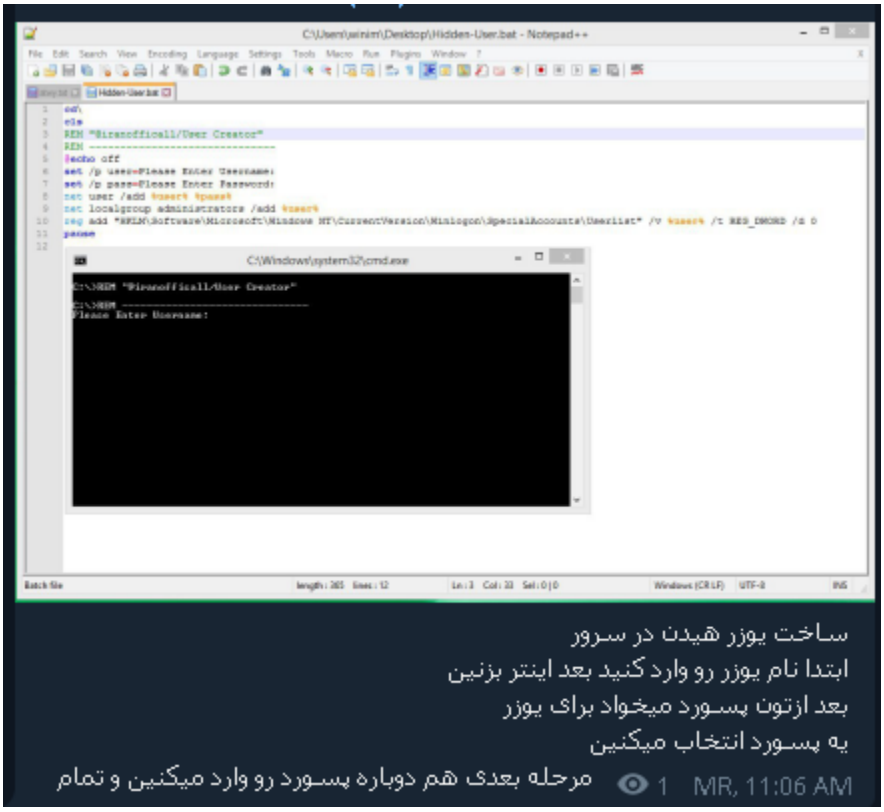
Campaign 36

Activity from June 3rd to 26th indicates that the attacker present on the system was conducting operations involving the Sodinokibi ransomware. When linking back activity, we observed one notable tool the actor had used during the operation.

‘Hidden-User.bat’ was designed to create hidden users on the target system. This tool links back to some underground distribution on Farsi-speaking private channels.

The file being shared is identical to the one we found to be used actively in the Sodinokibi case in different instances in June 2019, in different cities in the Middle East. We found the following Farsi-speaking users sharing and discussing this tool specifically (Cryptor007 and MR Amir), and others active in these groups. McAfee ATR observed this tool being used on June 13th, 2019 and June 26th, 2019 by the same actors in different regions.

HIDDEN-USER.bat



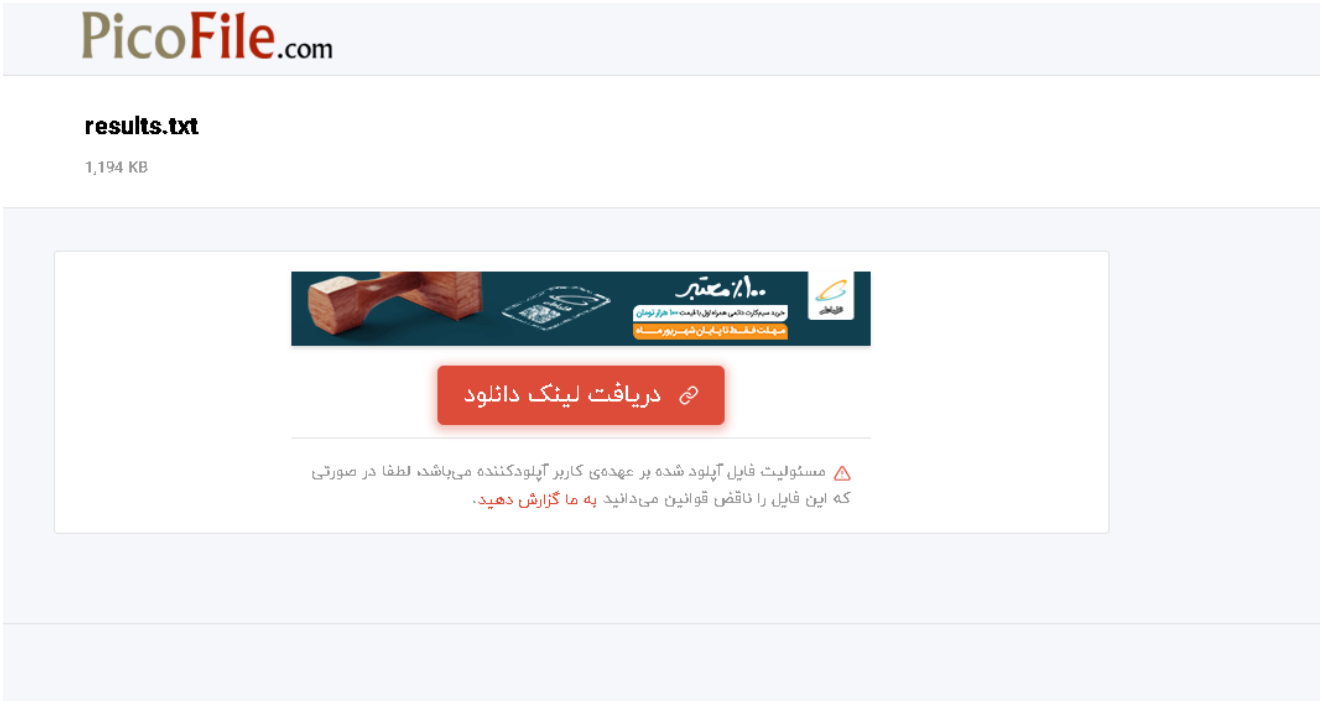
POSTED IMAGE OF THE TOOL IN USE

These Sodinokibi variants are strictly appearing in Israel from our observations:

- a3769a6748ba5d8023bcb161a5274e24d419bd36 (June 3rd, 2019)
- bbabc23525b3852d463ef17ba7b8a2cab831e2b9 (June 11th, 2019)

We observed the actor dropping one of the above-mentioned variants of Sodinokibi. In this case, the login came from an IP address originating in Iran and with a machine with a female Persian name.

The attackers connecting are most likely Farsi-speaking, as is evident by the browsing history uncovered by McAfee ATR, which indicates where a number of the tools utilized originate from, including Farsi language file sharing sites, such as Picofile.com and Soft98.ir, that contain malicious tools such as NLBrute, etc.



FARSI LANGUAGE SITE FOUND IN BROWSING HISTORY

We observed the actor attempting to run an RDP brute force attack using NLBrute downloaded from the Iranian site Picofile.com. The target was several network blocks in Oman and the United Arab Emirates in the Middle East.

In our analysis we discovered an offer to install ransomware on servers posted in Farsi speaking on August 19th,. This posting date corresponds with the timing of attacks observed in the Middle East. The services mentioned are specifically targeting servers that have been obtained via RDP credential theft campaigns. It is possible that these actors are coming in after the fact and installing ransomware on behalf of the main organizer, according to actor chatter. One specific Farsi language message indicates these services for a list of countries where they could install ransomware for the potential client.

FARSI LANGUAGE MESSAGE FROM PERSIAN LANGUAGE CHANNEL

Tools and Methods of Group 1

The operators responsible for intrusions involving Sodinokibi variants with an unknown affiliate ID utilize a variety of methods:

- Initial intrusions made over RDP protocol
- Using Masscan to identify potential victims
- Executing NLBrute with custom password lists

Tools and Methods of Group 2

The operators responsible for intrusions involving Sodinokibi variants with PID 34 utilize a variety of methods:

- Intrusion via RDP protocol
- Manual execution of subsequent stages of the operation
- Deployment of Sodinokibi
- Deployment of Mimikatz
- Utilization of CryptoCurrency mining
- Deployment of other brute force and checker tools
- Running mass port scans and other reconnaissance activities to identify potential targets
- Executing NLBrute with custom password lists
- Some of the operators appear write in Farsi and are originating from Iranian IP address space when connecting to observed targets

Tools and Methods of Group 3

The operators responsible for intrusions involving Sodinokibi variants with PID 19 utilize a variety of methods:

- Intrusion via RDP protocol
- Manual execution of subsequent stages of the operation
- Likely a cracking crew working on behalf of an affiliate
- Deployment of Sodinokibi
- Custom scripts to erase logs and create hidden users
- Usage of Neshta to scan internal network shares within an organization in an effort to spread Sodinokibi
- Running mass port scans and other reconnaissance activities to identify potential targets
- Limited use of local exploits to gain administrative access
- Executing NLBrute with custom password lists
- Some of the operators appear to write in Farsi and are originating from Iranian IP address space when connecting to observed targets

Conclusion

In our blog series about Sodinokibi we began by analyzing the code we asked ourselves the question, “Why Persian?” With the information retrieved from our honeypot investigations, it might give us a hypothesis that the Persian language is present due to the involvement of Persian-speaking affiliates. Time and evidence will tell.

We observed many affiliates using different sets of tools and skills to gain profit and, across the series, we highlighted different aspects of this massive ongoing operation.

To protect your organization against Sodinokibi, make sure your defense is layered. As demonstrated, the actors we are facing either buy, brute-force or spear-phish themselves into your company or use a trusted-third party that has access to your network. Some guidelines for organizations to protect themselves include employing sandboxing, backing up data, educating their users, and restricting access.

As long as we support the ransomware model, ransomware will exist as it has for the last four years. We cannot fight alone against ransomware and have to unite as public and private parties. McAfee is one of the founding partners of NoMoreRansom.org and are supporting Law Enforcement agencies around the globe in fighting ransomware.

We hope you enjoyed reading this series of blogs about Sodinokibi.

Jessica Saavedra-Morales
With a degree in networking and a degree in information technology, Jessica has a background in the tech field for almost two decades. Being fluent in Spanish has steered her...