BLINDINGCAN Threat Report

Date: **23/10/2020**

Sampada Kanitkar,
Krupa Gajjar

A RAT or Remote Access Trojan is a form of malware which allows hackers to control victim machine remotely. It allows hacker for covert surveillance of the victim machine. Hackers can use the compromised machine to perform various activities such as installing additional malwares, deleting programs, webcam hijacking, read the data from keyboard, acquiring login credentials, and clipboard data.

Overview

The newly discovered RAT known as `BLINDINGCAN` targets defense organizations and aerospace business. It is mainly used for espionage and reconnaissance activity. This RAT was spotted as a part of malware attacks carried out by North Korea called the Operation North Star and the `Operation DreamJob`. This malware runs when a loader loads a DLL file, and so far have targeted United States and other prominent countries.
The sample analyzed in this blog has some enhanced features to use more stealthily approach for scanning and transfer of system information.

Technical Analysis

The variant discovered propagated as an email attachment to a targeted group of audience which is most vulnerable during this pandemic, in the form of malicious Office or PDF Documents.

The main aim of this malware is to gain access to the victim machine and perform reconnaissance, and then gather intelligence surrounding the key military and energy technologies. The malware runs when the loader loads a DLL file, in some cases the DLL file is encoded and the loader has to decode the file before it gets executed.

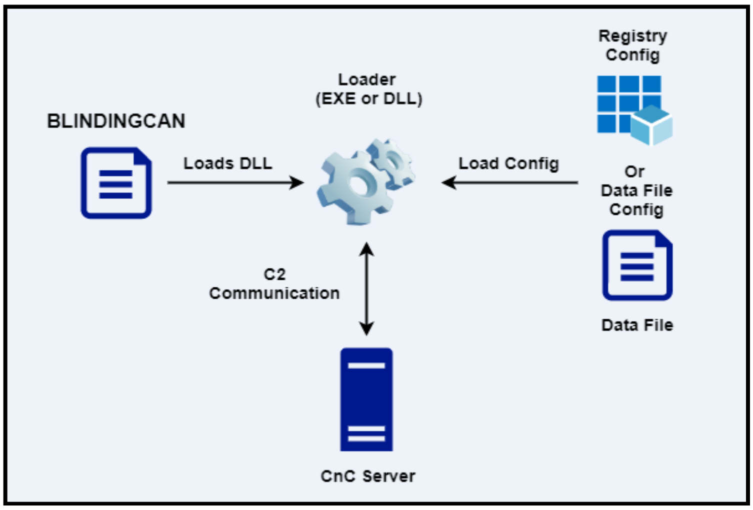


Fig 1

Fig 1 shows the flow of the infection in which the victim is affected by the malware, once the loader loads a file, the DLL for the BLINDINGCAN gets loaded on to the loader and configuration files are stored on victim machine, after which the DLL communicates with the CnC Server to download the final payload to be executed on the victim machine.

Upon execution by the loader, the configuration files of the BLINDINGCAN are stored in the victim machine, the location can be:

- Hardcoded in the malware itself
- Stored in a registry entry
- Saved as a file

The sample analyzed, stores the configuration files in the registry entry as shown in the screen shot.

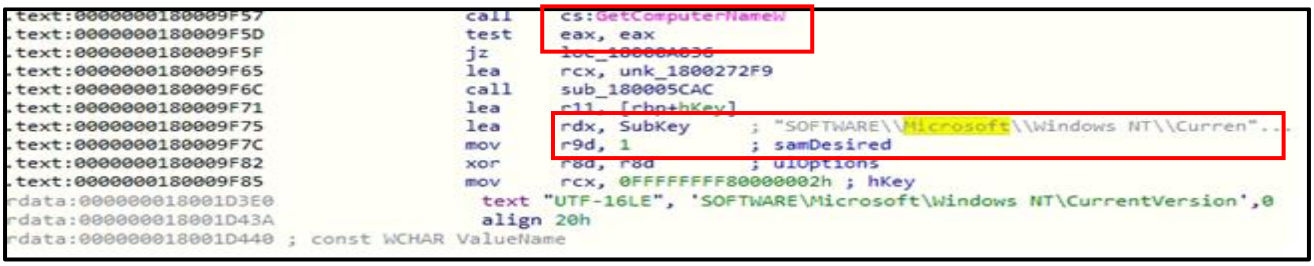
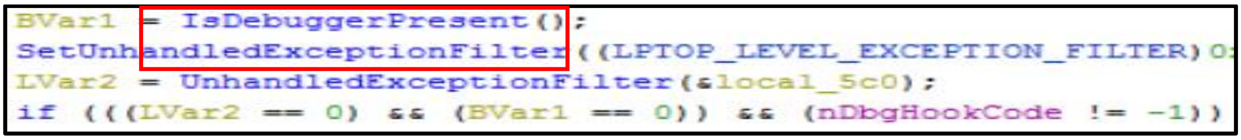


Fig 2

As shown in Fig 2 the malware gets the computer name calling the function "`GetComputerNameW`", once it calls this function and obtains the computer name, than it stores the configuration file in the registry key.



As shown in the above Fig 3 we can see that the malware tries to check if it is being executed in a debugger or not by using the function `IsDebuggerPresent`. If the malware is running inside the debugger, than it will conceal its actual behavior and hide the true functionality to avoid identification.

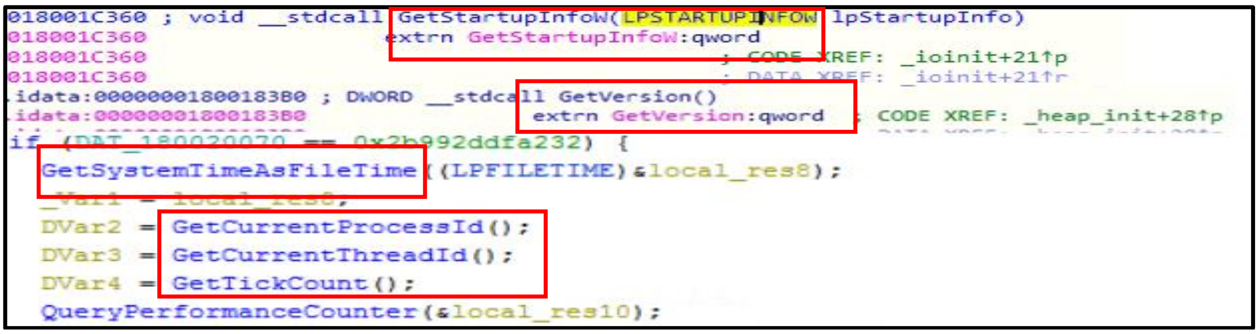


Fig 4

The malware steals multiple sensitive data from the victim machine such as Startup info, Time Zone information, Current Process Id, Current Thread Id as shown in Fig 4.

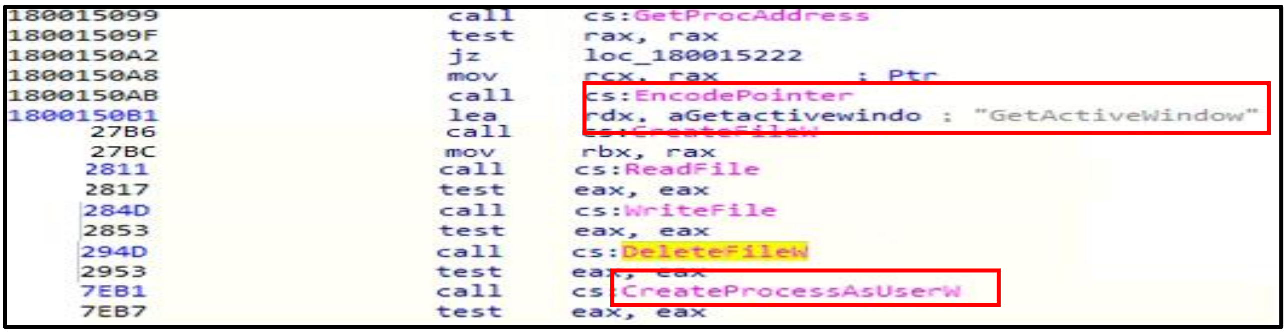


Fig 5

As shown in the above fig 5 it is clear that after collecting the system information like the system name, time zone, system version it further calls the functions to get the address of the processes on the system, also encodes the pointer value. Further to that it calls various functions to create a file, write a file and after that delete the file once the task is completed. It also creates some processes as a user which can be clearly seen in the above figure which calls the function `CreateProcessAsUserW`.

Fig 6

After communicating with the CnC server binary uses `HTTP POST` request with its custom header and body to connect to the C&C server to get further information and communication. The HTTP request uses `application/x-www-form-urlencoded` as content-type. Some of the code downloaded is in encrypted form, which uses `RC4` and `Base64` encoding techniques.

As shown in the above Fig 6 it can be seen that it establishes a communication with the CnC and keeps the connection alive until the payload to be executed can be obtained. Once the payload is downloaded it terminates the connection with the CnC server by calling the function End Session with CnC server.

Communicating IP addresses: 54[.]241[.]91[.]49
104[.]26[.]0[.]60

External Domain: www[.]curiofirenze[.]com
www[.]automercado[.]co[.]cr

While communicating with the CnC server the victim machine receives several commands such as to upload the file, download the file, modify the file creation time and many more. It also resets the communication interval with the CnC server.

File Hash: f337e8beb02dade38a860c2025de439b

IOCs:

f337e8beb02dade38a860c2025de439b
e7718609577c6e34221b03de7e959a8c
https://www[.]automercado[.]co[.]cr/empleo/css/main[.]jsp
https://www[.]curiofirenze[.]com/include/inc-site[.]asp
https://www[.]ne-ba[.]org/files/news/thumbs/thumbs[.]asp
https://www[.]sanlorenzoyacht[.]com/newsl/include/inc-map[.]asp

MITRE Techniques:

T1497.001 – System Checks	T1059.003 – Windows Command Shell
T1083– File and Directory Discovery	T1190 – Spearphishing Attachment
T1057–Process Discovery	T1055 – Process Injection
T1012–Query Registry	T1129–Shared Modules
T1082 - System Information Discovery	T1112 – Modify Registry
T1016–System Network Configuration Discovery	

CVE:

CVE-2017-0199

Subexsecure Protection

- Subexsecure detects the malware as 'SS_Gen_BLINDINGCAN_PE_A'.

OUR HONEYPOT NETWORK

This report has been prepared from threat intelligence gathered by our honeypot network that is today operational in 62 cities across the world. These cities have at least one of these attributes:

- Are landing centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research centers focusing on IoT
- Have the potential to host multiple IoT projects across domains in the future

There are more than 3.5 million attacks registered in a day across this network of individual Honeypot are studied, analyzed, categorized and marked according to a threat rank index, there is a priority assessment framework that we have developed within Subex. The network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity flavors globally. Devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.