How the Iranian Cyber Security Agency Detects Emissary Panda Malware

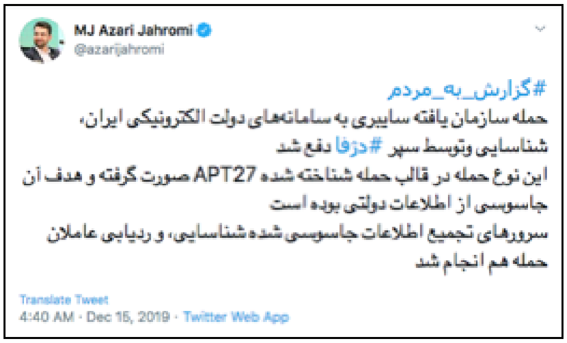
team-cymru.com/2020/03/25/how-the-iranian-cyber-security-agency-detects-emissary-panda-malware/

S2 Research Team View all posts by S2 Research Team March 25, 2020

View all posts

Other threat intelligence groups have previously publicised that the Chinese-attributed threat group, Emissary Panda (aka *APT27*, *TG-3390*, *BRONZE UNION, Iron Tiger* and *LuckyMouse*), have been targeting various sectors in the Middle East, including government organisations.

On 15 December 2019, Iran's Minister of Communications and Information Technology, Mohammad Javad Azari-Jahromi, announced that Iranian authorities had detected foreign spying malware on their government servers which they attributed to the "well-known APT27" (Figure 1).



MJ Azari Jahromi
@azarijahromi

#گزارش_به_مردم
حمله سازمان یافته سایبری به سامانه‌های دولت الکترونیکی ایران،
شناسایی وتوسط سپر #دژفا دفع شد
این نوع حمله در قالب حمله شناخته شده APT27 صورت گرفته و هدف آن
جاسوسی از اطلاعات دولتی بوده است
سرورهای تجمیع اطلاعات جاسوسی شده شناسایی، و ردیابی عاملان
حمله هم انجام شد

Translate Tweet
4:40 AM · Dec 15, 2019 · Twitter Web App

Figure 1: Announcement about APT27 by Iran's Minister of Communications and Information Technology

We decided to take a look at our data in an attempt to identify any malware indicators of this compromise.

Although Emissary Panda are known to utilise a wide-array of tools, they are most often associated with HyperBro, an in-memory RAT. Therefore, we decided to start by searching for any previously unobserved samples of this malware we have within our datasets. HyperBro malware is installed on a system via three components:

- A legitimate executable used to side-load
- A malicious DLL used to decrypt and load
- A third file as a DLL (the malicious payload)

We also know from previous analysis that HyperBro creates various unique artefacts on a victim system, including:

1. A registry key that contains configuration information that the malware relies on to function.
2. A service created by the malware which is used to install itself on a victim system.
3. A process mutex created by HyperBro to ensure that only one instance of the malware is running at any time.

1 – REGISTRY

HyperBro stores configuration data in a registry key. The path of this registry key is dynamically generated based on information collected on the victim system.

HyperBro queries the registry key HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0 for the value of Identifier(Figure 2).

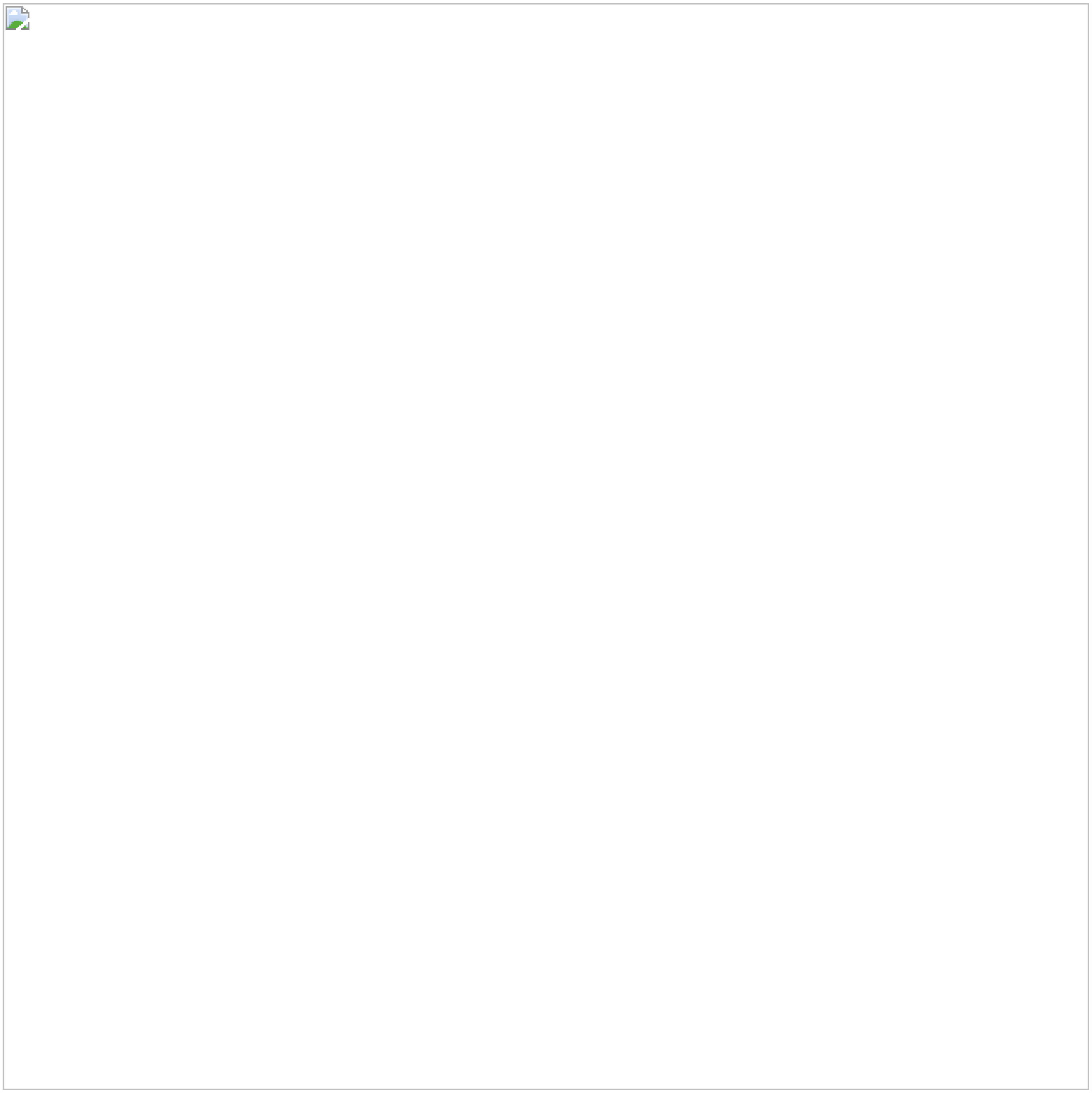


Figure 2: Example value of Identifier

The example in Figure 3 has the value Intel64 Family 6 Model 62 Stepping 4. That value is subsequently used by **HyperBro** to create a registry key in the HKEY_CLASSES_ROOT. In this example, the created key would be HKEY_CLASSES_ROOT\Intel64 Family 6 Model 62 Stepping 4-Il37389743nxshkhjhgee.

The appended value –ll37389743nxshkhjhgee is a part of the malware’s embedded configuration and may change over time.

2 – SERVICE

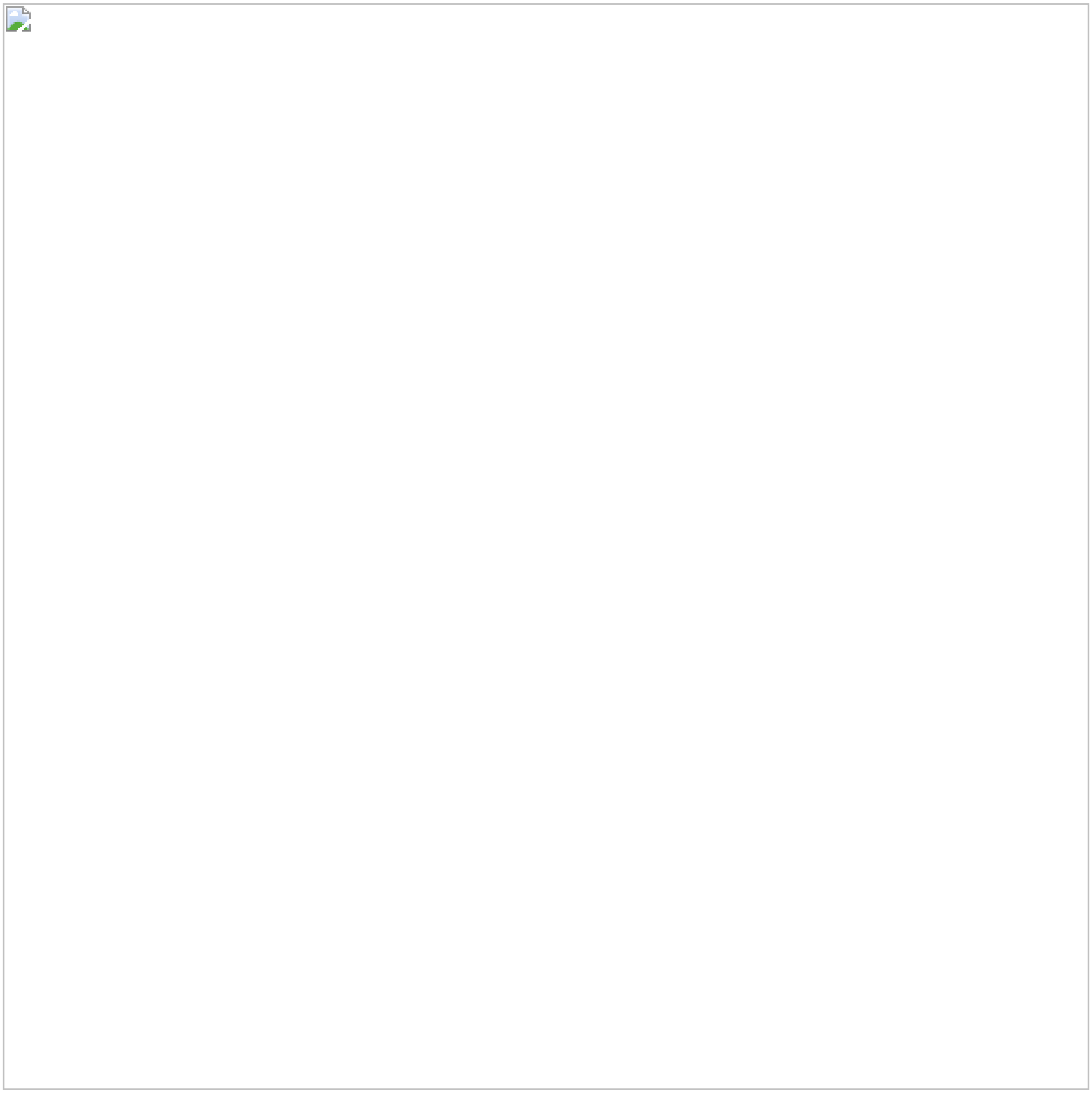
HyperBro installs itself to run as a service by injecting itself into a spawned svchost.exe process. The **HyperBro** process will be an orphaned (no parent process) svchost.exe process.

3 – MUTEX

HyperBro creates a process mutex in order to ensure that only one instance of the malware is running at any given time. The name of the process mutex is created by collecting the name of the user currently logged onto the compromised system and appending a hard-coded string. Samples analysed to-date have used the string Defender. For example, if the current system profile has a username “*Joe*”, **HyperBro** will create a mutex with the name JoeDefender.

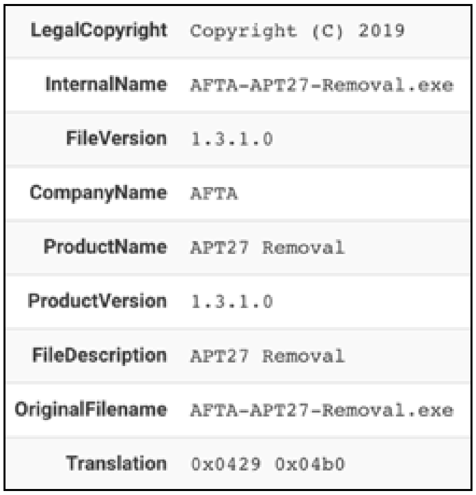
IRANIAN GOVERNMENT DETECTION AND REMOVAL TOOLS

When searching for HyperBro samples via the Malware Add-on for Augury, our data analyst’s portal, one particular sample stood out to us (SHA1: f7979ded11e695448c24a7a8efc1ea2649f9196c) (Figure 3):



F**igure 3: Sample of interest that created a process mutex associated with HyperBro**

We conducted some further analysis on this sample, and while it created a process mutex associated with HyperBro (PhilDefender), the functionality was vastly different from what we expected. In fact, the version information of the sample suggested that this was not HyperBro at all (Figure 4):



LegalCopyright	Copyright (C) 2019
InternalName	AFTA-APT27-Removal.exe
FileVersion	1.3.1.0
CompanyName	AFTA
ProductName	APT27 Removal
ProductVersion	1.3.1.0
FileDescription	APT27 Removal
OriginalFilename	AFTA-APT27-Removal.exe
Translation	0x0429 0x04b0

Figure 4: Version information from sample of interest

AFTA are the Iranian Cyber Security Agency. A screenshot from our malware sandbox showed the following image (Figure 5):

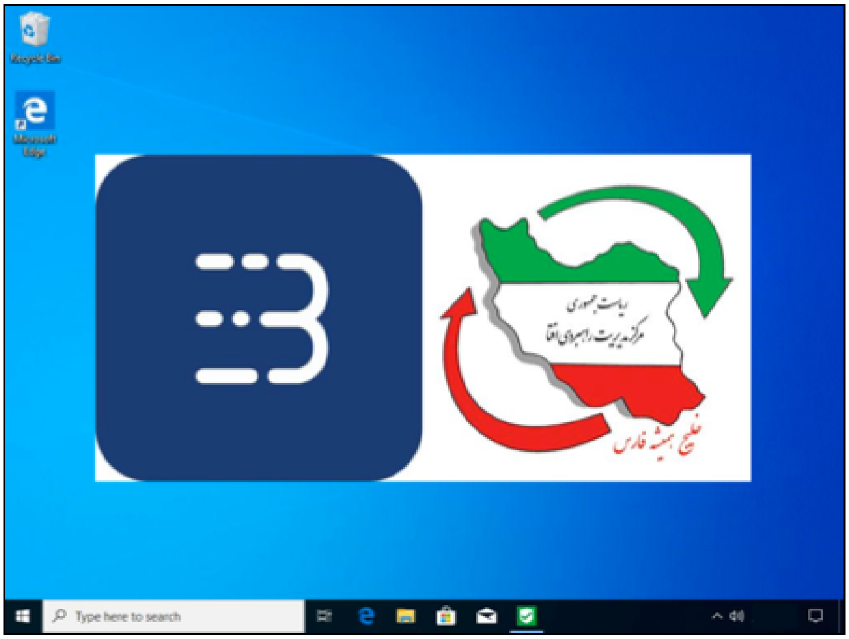


Figure 5: Screenshot from malware sandbox

The logo on the right is for AFTA. Further searches within open source associated the other logo with BitBaan, an Iranian malware analysis laboratory. BitBaan even tweeted about their APT27 remediation tools on 30 December 2019.

BitBaan may be a contractor for the Iranian government and this software was developed to share with government agencies and contractors.

Unpacking the sample provided us with strings – specifically contact details for AFTA – which we used to identify an archive that was submitted to VirusTotal from an Iranian IP address, with the filename AFTA-APT27-Detector.rar (SHA1: e38ab5339aef4fe8b2587e178fc38879dbc34209).

The archive contains tools and documentation for detecting and removing **HyperBro** malware on both single workstations and a Windows domain, including the aforementioned sample that we previously identified. Each set of tools has its own directory.

The tools and documentation for the "stand-alone" deployment (i.e. tools to be used on a single workstation) are in a folder named Stand-alone_APT27_afta; the contents of this folder are shown below:

Filename	AFTA-APT27-Detector.exe
SHA1	f69ab51268efc334616dfe49c6ee8e3808a0674f
Description	HyperBro detection tool

Filename	AFTA-APT27-Removal.exe
SHA1	f7979ded11e695448c24a7a8efc1ea2649f9196c
Description	HyperBro removal tool

Filename	APT27-Help.pdf
SHA1	6cf2dfc970033889883e61977ac7ca49e2bceba2
Description	Technical documentation on using the detection and removal tools

The tools and documentation for deployment to hosts connected to a Windows domain are in a folder named Domain_APT27_afta; the contents of this folder are shown below:

Filename	AFTA-APT27-Detector.exe
SHA1	ee1360de2aec10db6e49b55202bbe280ae40d5b4
Description	HyperBro detection and removal tool.

Filename	APT-27_Detector.pdf
SHA1	9bfb4b4d6c9c1afb5ccea5fee2c97d8f2aa847e2
Description	Technical documentation on using the detection and removal tools.

Filename	detector3.bat
SHA1	4d8479e8fbc59c10a66abf989051f5b6e41bf8b7
Description	Batch script that will run detection/removal utility and store logs.

Filename	summarize-x86.exe
SHA1	e88b5f201f20e6024095c4dca4170d851f7d9cfe
Description	Tool that will create summary analysis of all log files generated by AFTA-APT27-Detector.exe

The documentation describes creating a network share for storing the tools that all workstations can access. Users are then directed to use the batch script (detector3.bat) as a scheduled task on all workstations connected to the domain. Logs generated by the batch script are stored on the previously-created network share. The tool summarize-x86.exe will create a summary of the log files created by workstations that can be reviewed by network incident responders.

The AFTA detection software (AFTA-APT27-Detector.exe) checks for the existence of the three indicators of compromise previously detailed in this blog (registry, service, mutex). When checking for the HyperBro service, the detection utility scans running processes and attempts to identify an orphaned svchost.exeprocess, and if successful will store the name of the DLL file linked to run using that process. The stored name of the DLL file is then used in the removal process (see below).

The removal utility (AFTA-APT27-Removal.exe) will attempt to remove HyperBro (and its artefacts) from an infected host in the following order:

1. The registry key containing the configuration data.
2. The service installed by HyperBro, in order to prevent the malware from running again.
3. The svchost.exe process is then terminated.
4. The executable, DLL and payload are deleted from disk.

While the discovery of these tools does not confirm the full extent of the compromise of Iranian Government systems by Emissary Panda, their existence alone indicates that the compromise was significant enough that the Iranian Cyber Security Agency (in co-operation with BitBaan) needed to develop tools and documentation to distribute across multiple networks/Windows domains.

3 replies on “How the Iranian Cyber Security Agency Detects Emissary Panda Malware”

[…] Read more… […]

[…] blog.team-cymru.com/2020/03/25/how-the-iranian-cyber-security-agency-detects-emissary-panda-malware/ Other threat intelligence groups have previously publicised that the Chinese-attributed threat group, Emissary Panda (aka APT27, TG-3390, BRONZE UNION, Iron Tiger and LuckyMouse), have been targeting various sectors in the Middle East, including government organisations. On 15 December 2019, Irans Minister of Communications and Information Technology, Mohammad Javad Azari-Jahromi, announced that Iranian authorities had detected foreign spying malware on their government servers which they attributed to the well-known APT27 […]

[…] Comment l’agence iranienne de cybersécurité détecte les logiciels malveillants d’APT … […]