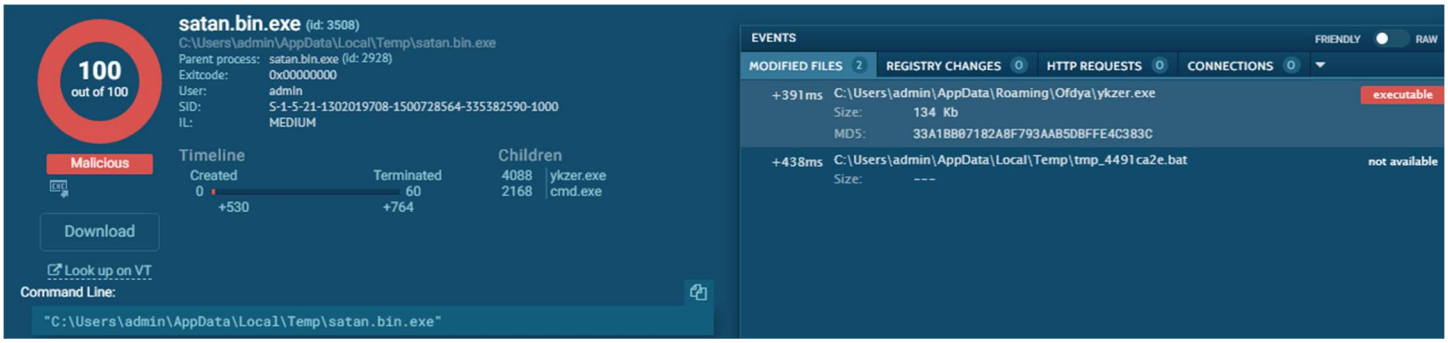
Satin Malware Report

The Trojan Backdoor

By: Bryan Hernandez, Brian Zuniga, Ben Halpern, Guadalupe Luna

Static Analysis

Synopsis of Executable



This section contains a summary of the uploaded executable: `Satan.bin ( backdoor )`

SATAN.BD (Back Door) is a .bin.exe file, a executable binary file made for Windows operating systems. The compilation date of the back door is unknown, however the malware is polymorphic and changes over time as it infiltrates more systems. The backdoor malware was first discovered in 1998 in the Philippines. The malware was initially a macro trojan which infiltrated the system through Microsoft Office. The malware is still active and is considered to be at a medium threat level, however most anti-virus and anti-malware are able to detect the back door trojan. Most anti-virus scanners detect this malware to be a backdoor trojan, however not all anti-virus scanners are capable at removing the trojan. The Satan trojan is known to communicate over port 666, it makes a DNS request to a masked ip behind the tor network to establish a connection with the attacker.

- The file type and file size: .bin (Binary) .exe (executable) (PE32 executable)
- Compilation date: Unknown ;
- Analysis Date; 12/1/2018, 01:26:39 ;
- First Discovered: 1998 in the philippines and still active up until today.
- Most anti-virus scanners think this malware is a backdoor/ Trojan
    - [Kaspersky] Backdoor.Satan.a, Backdoor.SBD.10, Backdoor.SBD.20
    - [Eset] Win32/Satan's_Back_Door.1_0_x trojan
    - [McAfee] BackDoor-W
    - [F-Prot] W32/Backdoor.Satan, W32/Backdoor.SBD, security risk or a "backdoor" program
    - [Panda] Bck/Satan.A, Trj/SBD.Clt, Trj/SBD.Srv, Bck/SBD.2.0b
    - [CA] Backdoor/WinVMM32, Win32.Satan, Backdoor/SBD!Server, Win32.SBD, Backdoor/SBD.20_Server, Win32.SBD.20

Initial Behavior

(Malware has flow control : different amount of files created depending where the start file is located.)

The table below summarizes the initial activity generated by the sample upon upload to Any.Run.

Activity Type	Count
HTTP Requests	**0**
DNS Requests	**1**
Connections	**0**
Files Changed	**288 in 60 seconds (recursive process deleting explorer.exe shadow copies)**

In addition, Any.Run reported the following threats.

- DNS Request: 1 DNS Request to 6pi3jrqjbssfh6gu.onion.pw
    - Svchost - “Potentially Bad Traffic”

Dynamic Analysis

The results below were generated by executing the malware sample on Any.Run’s hosted platform.

Process Environment

The environment in which the trojan was tested in was a Windows 7, 32 bit operating sub-system. The Process environment was compiled on February 23, 2017. Indicators of suspicious activity are the process injection of an infected executable, removal of all shadow instances of Explorer.EXE, as well as a blacklisted DNS request. The trojan has been shown to use privilege escalation since the Process Environment is running as User, but the trojan is running as Admin.

- The user the process runs as : User
- Version information:
    - OS: Windows 7 Professional Service Pack 1 (Build:7601, 32 bit)
    - Machine Type: intel 386
    - Architecture: IMAGE_FILE_MACHINE_I386
    - Subsytem: IMAGE_SUBSYSTEM_WINDOWS_GUI
    - Compilation Date:23-Feb-2017 19:28:24
- Indicators of suspicious activity:
    - Injection: C:\\Windows\Explorer.EXE
        - Injects process explorer.exe and then begins to copy internet setting(proxyEnable)
            - Transverses into the savedLegacySettings
    - DNS request to a Tor Address
    - Removal of all shadow instances of Explorer.EXE

Network Activity

The malware makes one DNS request to a blacklisted URL hidden in the Tor network. From simply deductive reasoning it can be assumed that this DNS request is an attempt at contacting the attacker to establish connection from the infected computer to the onion URL to gain control. Through this connection it would allow the attacker to send commands to be run on your system. Aside from the singular DNS request no HTTP or other DNS were made. Any request to a blacklisted URL would be considered suspicious. The malware opens up all the ports on the system as well as the DNS request making it even more vulnerable and accessible for the attacker to infiltrate and control the infected system.

- Makes a DNS request to an onion url to mask whoever is trying to gain access (.onion.pw)
- Opens up all the ports on the computer

The following table describes the servers that the sample communicated with.

Request Type	Target Domain	Target IP Address	Reputation
DNS	6pi3jrqjbssfh6gu.onion.pw	209.99.40.224 (uses proxy)	Blacklisted

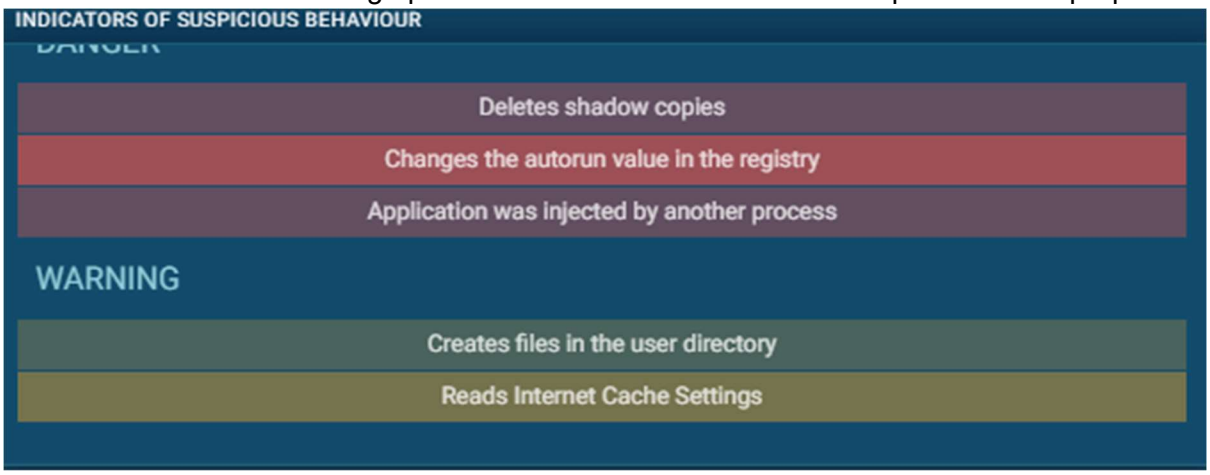
The DNS request seems to be attempting to create a connection between the infected computer and the attackers computer to allow infiltration.

Filesystem Modifications

The file modification are used to gain access to the machine by injecting an infected version of Explorer.exe into the system and overwriting shadow copies of the instance in order to retain its persistency in the system. From there it transverses to write a hexdump to update all versions of Explorer.exe to the infected copies. The malware then, all using the infected explorer, to turn off proxy settings so the IP of the client is visible. From the Internet Settings it moves to connections and uses a hexdump to send a DNS request to a blacklisted IP. The majority of file modifications are generated by the system as it is using

- Any.Run reports suspicious file modifications:
    - Rewrites all shadow copies of explorer.exe

- Write to the version of windows your running and writes a hexdump
    - Uses windows settings to overwrite the shadow copies of Explorer.exe to the infected one
- Disable any proxy that is running on the system
- Changes SavedLegacySetting with hexdump using the connections in internet settings to attempt to conceal it's DNS request.
- Imports .dll into the system
    - Setting up an environment to be used for multiple malicious purposes



Summary

While the satan.exe malware we are covering does not have a payload right out of the box, besides opening the the backdoor for the attacker, it can be used to do run anything the attacker commands your system to do. This means that the attacker could potentially run ransomware, cryptomining, data extract, espionage, botnet, use it to gain access to other personal account information, the possibilities are endless.

It can be very hard to detect the backdoor without the proper tools. After the malware runs it takes less than 60 seconds to fully execute. During this process the malware will inject itself into explorer.exe which would escalate it's privileges, delete shadow volume copies, and hide itself in the explorer application. This makes it really hard to detect the malware for removal. If you restore from your shadow copies, you are essentially restoring the malware with it.

The malware also tricks your firewall when it hides itself in explorer.exe since it is an allowed firewall application by default. The malware then proceeds to modifying your registry values, more specifically, the autostart value for explorer. This sets the malware to automatically run at startup so that it can immediately establish the connection when rebooted.

Lastly, after completing the execution process it will proceed to making a DNS request to a blacklisted IP. This IP is most likely a command and control server (C&C server) that will execute payloads to all infected computers so that the attacker can manage them as one. With a C&C server your computer is essentially sending information back like personal information, passwords, financial information, amongst other things depending on the attackers intents.

Since the malware is just a backdoor you might not notice anything suspicious for a very long time until the attacker decides to make a more obvious attack. Due to this, the best way to detect or attempt to remove it would be by ensuring your machine is constantly updated and that you are using updated malware protection

at all times. Now a days, most malware protection services are able to detect the malware before it is executed saving you a headache to begin with if you can just manage to constantly update your software.

Below are some key notes about the malware:

- Creates a backdoor in the system to allow outside connection to the system
- DNS requests to a blacklisted IP
- Process infection of Explorer.exe and creation of a malicious process injector
- Hides itself inside of explorer.exe
- Sets autostart value to true so that the malware automatically runs at startup
- Deletes/Overwrites shadow copy volume
- Runs with escalated privileges allowing the attacker to run any payload they wish to run on your computer.

Containment Strategy

This document contains counsel as to the scope and severity of infections by `Satan.BD`, as well as steps to fix infected computers and prevent future attacks.

Scope

Since the Satan.BD trojan runs out of an Executable extension, it limits its infections to Windows operated systems. The back door can be injected into all windows operating systems and most versions of microsoft office.

- Affected operating systems/services and versions
    - All windows operating systems.
- Types of devices usually targeted
    - Personal Computers with access to sensitive information

Severity

The malware is considered moderately severe, since it is still an active threat and embeds itself inside the file system, back ups, and program files, it is difficult to remove. Most anti-virus anti-malware software is able to detect it, however not all are capable of removing it. The malware does little to no damage to the computer, but it opens up the computer to more attacks by opening up all the ports in some cases. The malware injects a malicious ‘explorer.exe’ file into the system. While the majority of windows applications and services run off of explorer.exe this makes it very difficult to remove at the trojan to be at the core of the machine. The trojan using dll injection, builds an environment in which it can do a lot of harm if the attacker desires to.

- How much damage the malware does to the infected computer (e.g., is it destroyed vs inaccessible vs just a little bit slower?)
    - The malware does little to no damage, instead it nests itself inside a victim's computer and prepares itself for further attacks and usage of the computer in the future.
- How hard is it to remove without replacing the computer
    - It is hard to identify, however most antivirus software are known to identify this trojan.
    - It is difficult to remove, since the trojan embeds itself inside the Explorer.Exe functionality.

- How much data it can get access to—is it just adware, or does it expose a full root shell to an attacker?
    - The trojan can get full access to everything on the victim's computer as it runs itself as administrator. It then opens all the ports on the machine, making it yet even more vulnerable.

Based on the above, we conclude that this sample is of **moderate** severity, and should be patched.

Awareness Training

Identification

Since the Satan malware has a plethora of uses, identifying it can be both easy and difficult to detect. Satan can be used as a ransomware, a worm, or a trojan, but the most common use for it is ransomware. Most antiviruses and scanners can detect Satan malware. AlienVault USM is an example of a high premium antivirus that can detect and safely delete Satan. AlienVault USM states that they are constantly upgrading their detection system to catch new versions of Satan. The most important part about relying on a antivirus or scanner is to check to see if the antivirus installed on the computer is up to date with the latest Satan update. Another way to detect whether or not Satan is on your computer is to see bizarre behavior in the explorer.exe. The first thing that the Satan malware does on the computer is to take control of the explorer on a windows system.

Quarantine and Response

In the event that a computer has been infected with a Satan malware, here are some steps to safely respond to the threat before removing it from the infected device. The first step in response to the Satan malware is to disconnect the computer from the internet and any other networks connected to the infected system. This step takes priority before any of the other procedures. Disconnecting from the internet cuts off communication from the attacker to the malware from sending any new commands to the Satan malware. Disconnecting from other networks stops the malware from infecting other computers or systems. The next important step to take after the first one is to not plug in any device into the computer because the Satan malware may be able to jump onto the connected device. The next few steps can be taken in any order only after the first step has been completed. Closing port 666 is necessary because the malware uses this port to enter the computer. The only main use for port 666 is to play the video game DOOM created by ID Software. Other companies and people don’t use this port because this number is associated with evil in the christian based religions. The next step is to check all the files in the computer and the various backups to see which ones have been infected, are still safely secured, and no change. If any files that have not been affected by Satan and are not secured, secure those files as soon as possible. The main reason for this step is because most attackers that use Satan as malware to extort the victim for money. Finally, turning off the computer won't magically remove the malware from the system but it may accidently make the situation worse. Satan is mainly used as ransomware and most ransomware encrypt the data on the computer.The easiest way to release the information is with a key and that key is stored in the computer’s short term memory which gets deleted when the computer is shut down. Also, Satan can move from one location to another to avoid detection and the attacker may have programed it to move to a new location every time the computer is turned off and on.

Escalation

When a computer is infected with the Satan malware the best people to contact is the manager and the IT department. The first person to contact is the manager so that they determine how bad the situation is with respect to the entire company/department and take the necessary actions. The IT department is important to

contact because they should know how to remove the malware from the computer and determine if any additional actions need to be taken.

Works Cited

"BD Satan 2.0." *BD Satan 2.0: Attack Signature - Symantec Corp.* N.p., n.d. Web. <https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20236>.

"How to Remove Backdoor.Satan From Your PC? – Malware Uninstall Guide." *Easily Remove Malware From PC*. N.p., n.d. Web. <http://www.removeadwares.com/how-to-remove-backdoor-satan-from-your-pc-malware-uninstall-guide/>.

"How to Remove Backdoor.Satan From Your PC? – Malware Uninstall Guide." *Easily Remove Malware From PC*. N.p., n.d. Web. <http://www.removeadwares.com/how-to-remove-backdoor-satan-from-your-pc-malware-uninstall-guide/>.

"Ransom.Satan." *Symantec*. N.p., n.d. Web. <https://www.symantec.com/security-center/writeup/2018-051806-5250-99>.

"Satan Ransomware Spawns New Methods to Spread." *AT&T Cybersecurity*. N.p., n.d. Web. <https://www.alienvault.com/blogs/labs-research/satan-ransomware-spawns-new-methods-to-spread>.

"Satan.bin - Interactive Analysis." *ANY.RUN*. N.p., n.d. Web. <https://app.any.run/tasks/ca760e76-be9b-4a4b-97f8-159ab1c3b425>.

"Satans.Back.Door." *Satans.Back.Door Removal Tool. Remove Satans.Back.Door Now*. N.p., n.d. Web. <https://www.exterminate-it.com/malpedia/remove-satans-back-door#mlw_aliases>.

SpeedGuide. "Port 666 (tcp/udp)." *SpeedGuide*. N.p., n.d. Web. <https://www.speedguide.net/port.php?port=666>.

SpeedGuide. "Port 666 (tcp/udp)." *SpeedGuide*. N.p., n.d. Web. <https://www.speedguide.net/port.php?port=666>.

"The Virus Encyclopedia." *Satan - The Virus Encyclopedia*. N.p., n.d. Web. <http://virus.wikidot.com/satan>.

VMRay. N.p., n.d. Web. <https://www.vmray.com/analyses/1a0a2fd546e3/report/overview.html>.