Day Before Zero Blog

Damballa discovers new toolset linked to Destover
Attacker's arsenal helps them to broaden attack surface

November 18, 2015

Tags: Destover, malware, trojan

Destover is best known as the malware used in the attack on Sony Pictures Entertainment in November 2014, and also for its relationship based on its wiping technique with the Shamoon malware used in the attack on Saudi Aramco in 2012. The Destover trojan is a wiper that deletes files off of an infected system, rendering it useless.

Unlike most malware, the goal of Destover and other wiping malware is to cause damage for ideological and political reasons not for financial gain. For example, at Sony, attackers wiped files off of workstations making them completely inoperative for unclear political goals of the attackers. The Saudi Aramco attack using Shamoon was so destructive it temporarily drove up the price of hard drives because an estimated 50,000 were needed to help Saudi Aramco recover, also for unclear ideological and political motives against the Al-Saud royal family.

Much was revealed In the weeks and months following these breaches, except for how attackers were able to stay undetected within the network long enough to expand their presence and exfiltrate Terabytes of sensitive information.

While researching a newer sample of Destover, we came across two files that were identified by one

antivirus product at the time under a generic signature. After analyzing further, we found two utilities closely related to Destover. Both utilities would be used during an attack to evade detection while moving laterally through a network to broaden the attack surface. Both utilities had usage statements and were named as setMFT and afset.

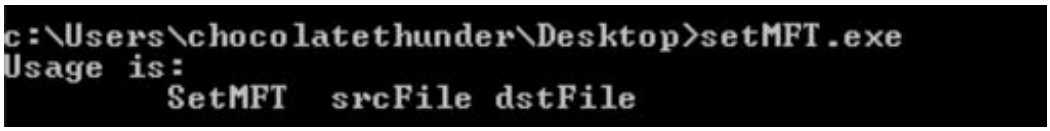
What is setMFT?

setMFT is used to copy the timestamp settings from a source file on disk to a destination file, also called timestomping. Timestomping combined with similar file naming enables a file to blend in with legitimate files in the same directory. This can conceal a file's existence from security personnel looking for malicious files or scans of files created after a certain date. Timestomping can get past a cursory check for malicious files. A thorough forensic examination will reveal that a file has been timestomped based on conflicting record dates and possibly log files.

The sample discovered by Damballa requires the presence of the file 'usbdrv3.sys' in the same directory. It turns out to be the renamed Eldos RawDisk driver used by Destover to gain direct access to disk. Either the driver is meant to be delivered with setMFT or is dropped along with setMFT from Destover itself. Destover and setMFT are related via the lengthy license key used with the Eldos driver:

99E2428CCA4309C68AAF8C616EF3306582A64513E55C786A864BC83DAFE0C78585B692047273
B0E55275102C664C5217E76B8E67F35FCE385E4328EE1AD139EA6AA26345C4F93000DBBC7EF1579D4F

Another feature is that this utility interacts with the attacker through on the command line rather than being delivered and executed by a dropper without interaction. setMFT comes with an English usage statement in case the attacker forgets the placement of arguments:

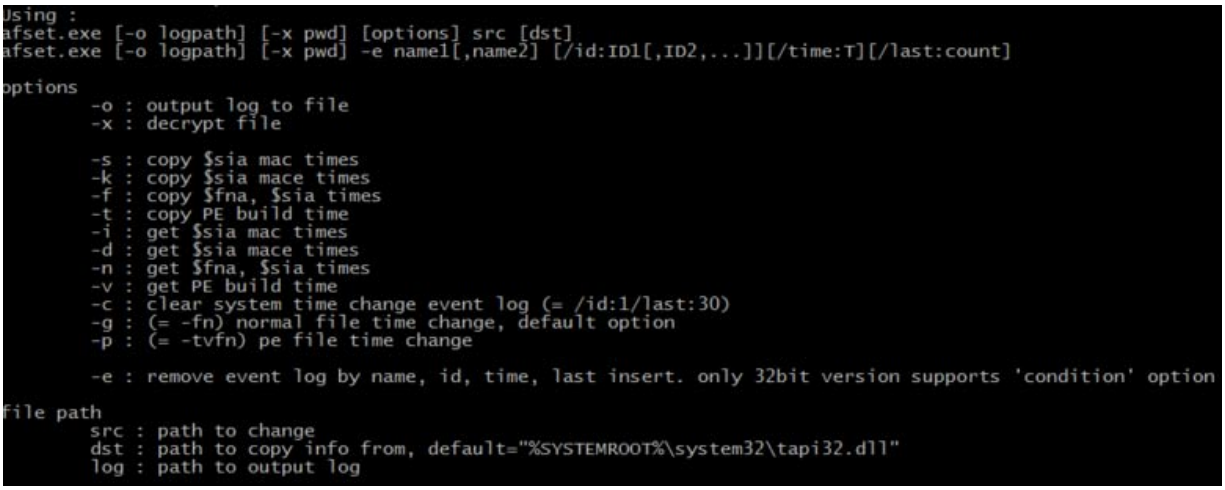


What is afset?

afset, like setMFT is also used to timestomp files plus clean Microsoft Windows logs based on criteria (id, time) from the user. It also changes the PE build time and checksum. afset provides more granular functionality to allow the user to set only certain timestamps on a file (sia, fna or both). To achieve the timestomping and log cleaning functions, afset uses the RawDisk driver with the same lengthy license key.

The afset sample we obtained appeared to be incomplete or a partial development version. The sample attempted to write a randomly named file with a .sys extension to the local directory with the contents of the "ICONS" resource which is supposed to be the encoded RawDisk driver. However, it failed to decode on execution. If the driver write had completed it would have registered as a service using the same random driver name. Plus, it would have been used to obtain a handle to write the MFT record for the target file to match either a user supplied file or by default the file "%SYSTEMROOT%\system32\tapi32.dll".

According to the handy usage statement, conditional log cleaning is only available on 32-bit systems. From our dynamic testing, it appears to clear the event log and then rewrite it without the offending entries. A full reversing of the log cleaning feature was not performed and dynamic analysis failed due to errors in the driver extraction routine from the resources. Fortunately, the usage statement gives insight to the full functionality of the tool:



Afset is used interactively on the target system. It allows the attacker to remain stealthy and erase their tracks as they move through the network. A full forensic analysis of a system would reveal the presence of afset and missing log activity but it's likely this activity would go undetected initially creating high-risk infection dwell time.

For enterprise security teams, the utility of setMFT and afset means that many of the tools and methods they use to identify the presence of attackers would be thwarted. If the adversary gains access to corporate servers and can clean and redirect log files, they can prevent any evidence of their activity from reaching a SIEM or log analysis solution.

These tools appear to have limited distribution, which means that newer versions of the tools could go undetected by standard AV for an extended length of time. Also, as mentioned, the ability to have the tools blend with legitimate system files allows the attacker to evade detection during a cursory glance by personnel. These capabilities, when used together with tools that enable attackers to obtain network credentials and disable defenses, allows them to permeate the network undetected for an extended period of time.

Conclusion

The attackers behind large and long-lasting attacks are very well organized, patient and determined. Toolsets like Destover, afset and setMFT are part of an arsenal used during a cyber attack. These tools are mainly used to help the attackers remain under the radar for months or longer. Gaining a foothold inside the victim's network is a top priority. History tells us that in most of the high-profile hacks making news headlines, the attackers were able to spend months hidden inside the victim's network exfiltrating Terabytes of data.

Attack modus-operandi:

Steps Reconnaissance
Tools Scanners, Open source intelligence gathering
Steps Breach
Tools

Tools Vulns, Exploits,
Steps Foothold
Tools afset, setMFT, RATs, credential theft
Steps Move laterally
Tools Stolen administrative credentials and RATs
Steps Exfiltrate
Tools VPN accounts, RATs, out of band comms
Steps Delete tracks
Tools afset, setMFT, Destover / Shamoon
Steps Exit
Tools Publish stolen data, clean with Destover / Shamoon

The table above, represents the different steps attackers would go through to penetrate a network and where they could use the new afset and setMFT utilities. They are used for different purposes and at different steps. There is no doubt that attackers are using these tools right now and are continuing to develop their capabilities.

IOCs

afset
MD5: b5ddd6ed3bd16c6f438b3bc95a2b49a8
SHA256: 38c87a92694b597e5d402342ab4a9ff88b5b81beb2791405637bdca2b8384eac

setMFT
MD5: f83f9d1797f5dbd419dfa86987790153
SHA256: fe30da9e47010d3522d30ff90fb10d6c30302e8d16001c1a12c149b508888ab8

YARA
rule Destover
{

```
{
meta:
        description = “Rule to detect Destover trojan and associated tools by license key”
        author = “Willis McDonald”
        company = “Damballa Inc.”
        reference = “not set”
        date = “2015/10/30”

strings:
        $key = “99E2428CCA4309C68AAF8C616EF3306582A64513E55C786A864BC83DAFE0C
78585B692047273B0E55275102C664C5217E76B8E67F35FCE385E4328EE1AD139EA6AA2634
5C4F93000DBBC7EF1579D4F”
        $MZ = “MZ”

condition:
        $key and $MZ at 0
}
```

Willis McDonald
Sr. Threat Researcher

Loucif Kharouni
Sr. Threat Researcher

Share this:

You might also like

Point of Sale (POS) and Card Reader Tampering

Learning from DNS

The IMDDOS Botnet Service

The ZitMo Rewind

A Future Security Ecosystem

Is Mac OS X secure?

Talk to Sales

Email Us to Learn More

Checkout the Knowledge Library

ABOUT DAMBALLA

Damballa delivers advanced threat protection for active threats that bypass traditional security layers, rapidly discovering infections with certainty and pinpointing compromises that represent the highest risk to a business.

E V E N T S

2015 Seattle SecureWorld

RSA Conference 2016

N E W S

Hackers can still access your car in more than 15 ways

Scammer turned ‘cybercriminal’ asks Damballa for help installing Pony Loader

5 CyberHacks That Could Affect Your Life in 2016

817 W. Peachtree St. NW I Suite 800
Atlanta, GA 30308

Phone: 404 961 7400

Email: info@damballa.com

Safe Harbor Privacy Policy

Leave a message