Ransomware on the Rise: Buran's transformation into Zeppelin

By G DATA Security Center

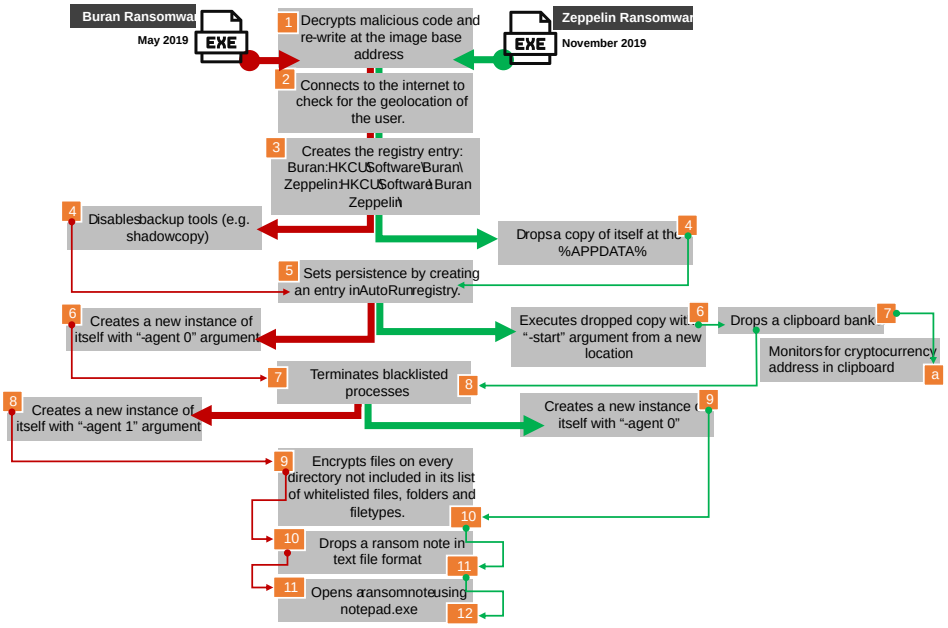
Published: 2020-06-30 · Archived: 2026-04-05 13:41:24 UTC

06/30/2020

Reading time: 5 min (1451 words)

Ransomware is still evolving. Evidence for this can be seen every day. Our analysts have taken a look at Buran and Zeppelin, a particularly devastating exhibit of this evolution.

Ransomware made a strong comeback in 2019 after its hiatus in 2018. Many high-profile attacks were reported by the end of 2019[1]. According to Emsisoft, in U.S. alone, the victims of ransomware include at least 113 government agencies, 89 educational establishments and 764 healthcare providers. The total amount of ransom demands tallies over $7.5 billion . [2]. In a report by Coveware, the average cost of ransom payment increased by 104% from third to fourth quarter of 2019[3]. It is therefore hardly surprising that cybercriminals are enticed once again into developing and creating new ransomware variants. Amongst the prevalent ransomware last year was the Buran ransomware that emerged early May 2019 and continues to proliferate until now. In a matter of just 9 months, this ransomware released over 5 updates by changing its code and attack vectors in order to stay stealthy and cause more damage. By the end of last year, a new variant of ransomware known as Zeppelin was released. Upon initial analysis of Zeppelin, certain behaviors and parts of its source code have been found to have similarities with Buran. This led us to identify Zeppelin as a new variant of Buran.



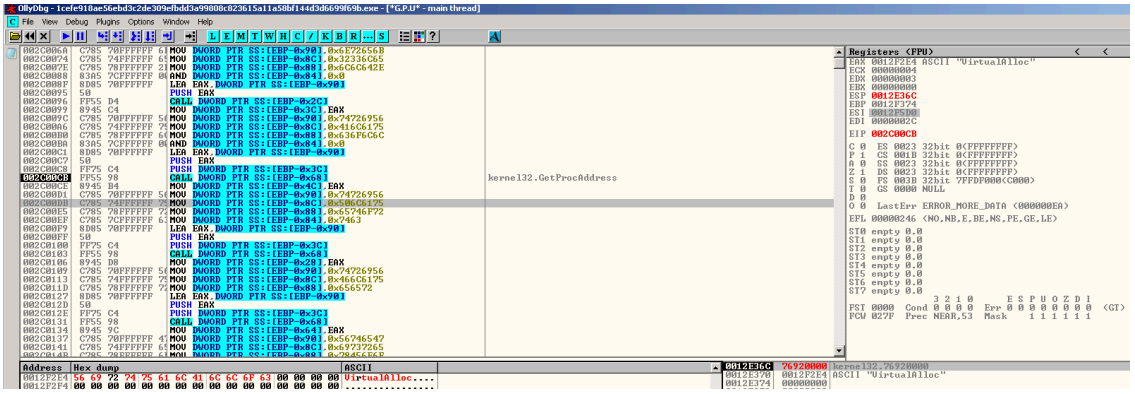
Buran and Zeppelin ransomware Overview

Attack Vector

Zeppelin is reaching its target networks primarily through phishing emails. These emails contain macro-enabled documents that will initiate the download and execution of the ransomware file on the victim's machine.
Moreover, other Zeppelin samples were also distributed through malicious advertisements (malvertising) that are designed to trick its victims into clicking fake advertisements which will trigger the download of the malicious file. Lastly, Zeppelin, like other ransomware, utilizes the use of public remote desktop software via web interfaces to remotely control a victim's machine and execute the ransomware.

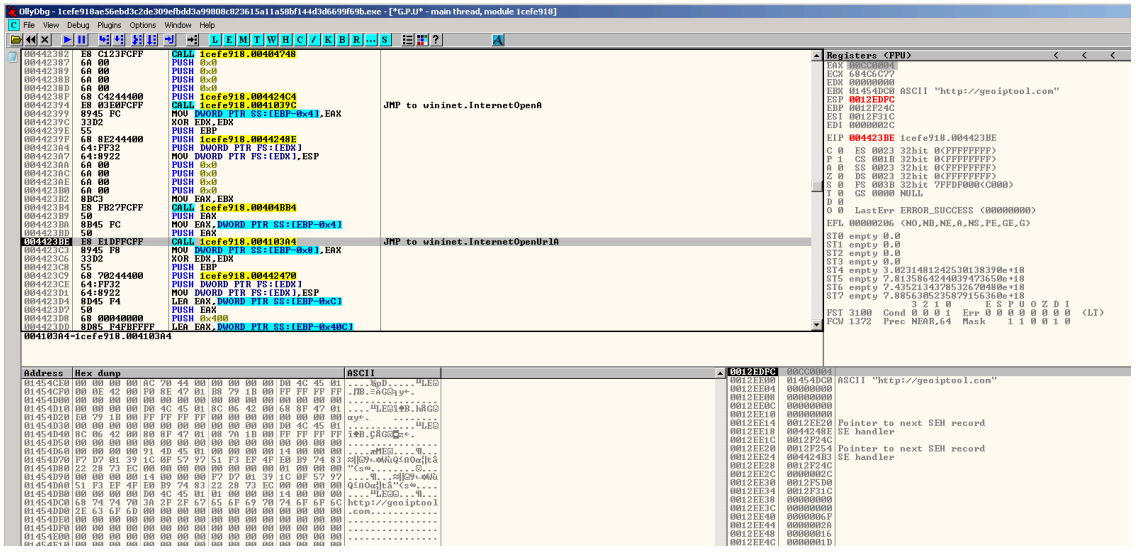
Installation

Like Buran, Zeppelin will allocate a space in memory. When executed, it will perform its decryption routine. However, compared to Buran's straight forward routine, Zeppelin has some changes to its code. For instance, it now harvests application programming interface(APIs) that it will use later by loading it in the stack. After decrypting, it will re-write the decrypted code to the base address of the file and execute it. It uses this obfuscation technique to make the analysis and signature detection of the file difficult.



Harvesting of API

The main similarities of Zeppelin with Buran are its several system checks. It will first attempt to connect to the internet to make a query to hxxp://*geoiptool.com.* This isa valid web service that checks the geolocation of a system with the use of an IP address,to verify where the file is currently being executed. If found to be running in either Ukraine, Belarus, Kazakhstan or Russian Federation, it won't proceed with its infection and terminate instantly. The malware authors did this to make sure that the ransomware won't infect any user living at the mentioned countries. This could be a hint that the ransomware originated from any of these countries.

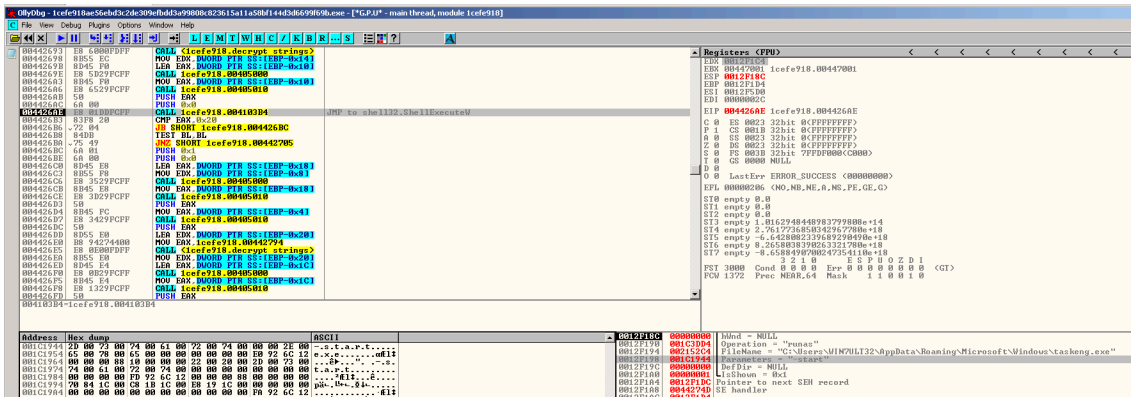


Harvesting of API

Country Protection Check

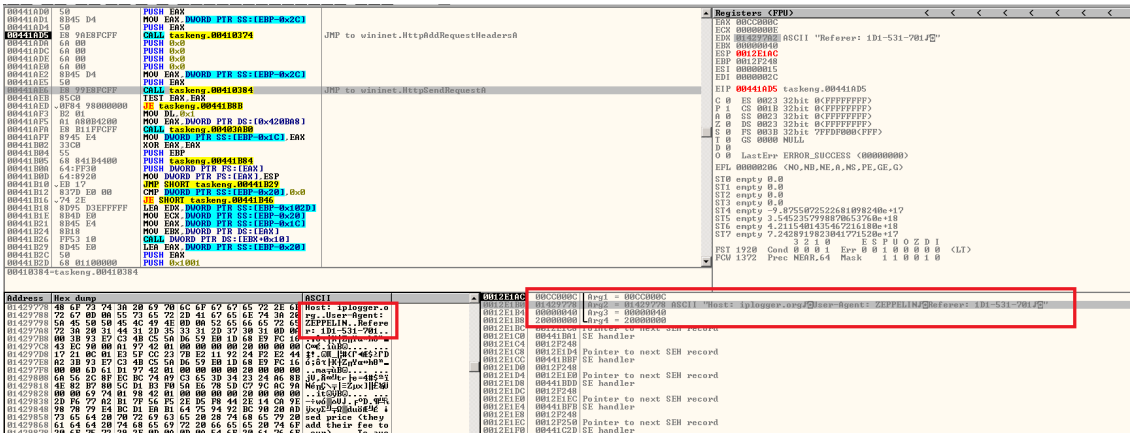
Zeppelin also creates a registry key that will be used to store data. In the early variants of Zeppelin, it still creates a “Buran” registry key which was later changed to Zeppelin. This is one of the links between Buran and Zeppelin. Compared to Buran, which just creates several instances of itself, Zeppelin drops an executable file inside the %APPDATA% directory with a filename randomly chosen from a list of possible names. To ensure its persistence, it adds an autorun key to the registry that points to the path of the dropped file.

Compared to Buran, which just creates several instances of itself, Zeppelin drops an executable file inside the %APPDATA% directory with a filename randomly chosen from a list of possible names. To ensure its persistence, it adds an autorun key to the registry that points to the path of the dropped file. The dropped file is a copy of itself which will be executed by using the “Shell Execute” API with “-start” argument.



Execution of its copy with “-start”

Second Instance



Discovery of victim's IP address using iplogger.org

Upon execution of the dropped copy, it will decrypt the contents of its ransom note, then store it in an allocated memory space for later use. Meanwhile, it will connect once again to the Internet and make a query to geoiptools.com to recheck where it was executed. After that, it will initiate a connection to iplogger.org, once again a legitimate web service used to track IP addresses, with the user-agent field id set to "ZEPPELIN" and the referrer field containing the unique ID of the victim. The malware author can use the IPLogger service to view the list of victims Zeppelin ransomware has.

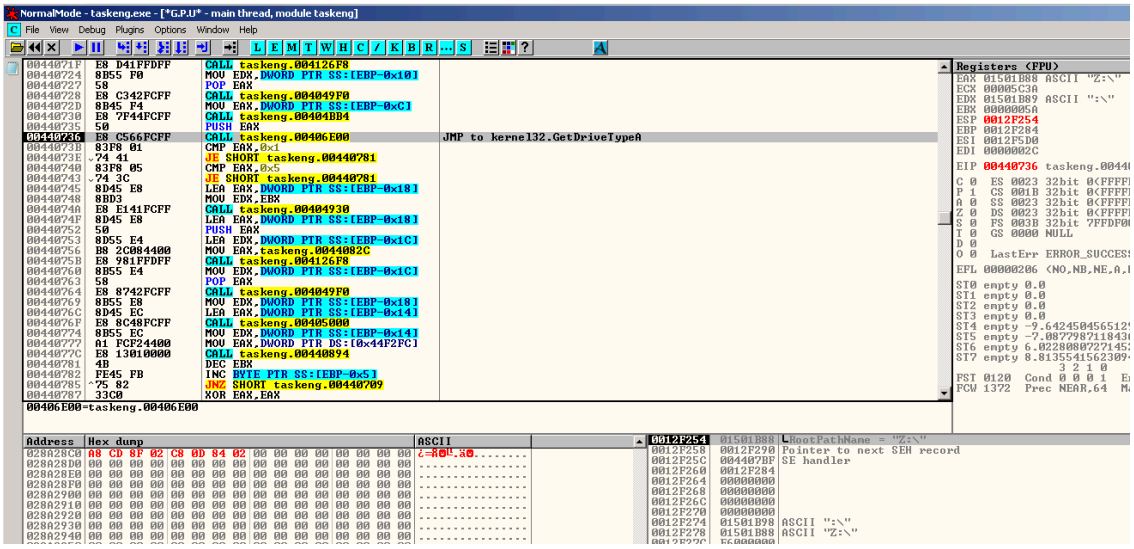
The processes running in the victim's system will be checked against a list of applications associated with monitoring system processes and services, database, backups and web services. If the name of the process can be found in the list, Zeppelin will force terminate the said processes, to ensure that maximum number of important data files will be encrypted.

agntsvc.exe	msaccess.exe	sql.exe
agntsvc.exeagntsvc.exe	msftesql.exe	sqlagent.exe
agntsvc.exeencsvc.exe	mspub.exe	sqlbrowser.exe
agntsvc.exeisqlplussvc.exe	mydesktopqos.exe	sqlserver.exe
anvir.exe	mydesktopservice.exe	sqlservr.exe
anvir64.exe	mysqld-nt.exe	sqlwriter.exe
apache.exe	mysqld-opt.exe	synctime.exe
backup.exe	mysqld.exe	taskkill.exe
ccleaner.exe	ncsvc.exe	tasklist.exe
ccleaner64.exe	ocautoupds.exe	taskmgr.exe
dbeng50.exe	ocomm.exe	tbirdconfig.exe
dbsnmp.exe	ocssd.exe	tomcat.exe

encsvc.exe	oracle.exe	tomcat6.exe
far.exe	u8.exe	firefoxconfig.exe
procexp.exe	ufida.exe	infopath.exe
regedit.exe	visio.exe	isqlplussvc.exe
sqbcoreservice.exe	xfssvccon.exe	kingdee.exe

The second instance of Zeppelin enables the malware author to drop a version of Clipbanker in the %appdata%\local\temp directory and execute it as “winupas.exe”. This clipbanker is responsible for monitoring the system’s clipboard for any strings that matches a cryptocurrency address. If a match is identified, clipbanker will replace the string to that of the malware author’s cryptocurrency address so that any amount of cryptocurrency to be transferred will be redirected to the malware author’s address. After that, Zeppelin will create another instance of itself with “-agent 0” argument.

Third instance



Listing of all available drives

The third instance of Zeppelin is mainly for file encryption. First it will check available drives in the system by iterating drives from Z:\ to A:\. It only looks for certain drive types which are: unknown, removable, fixed, remote and RAM disk drives.

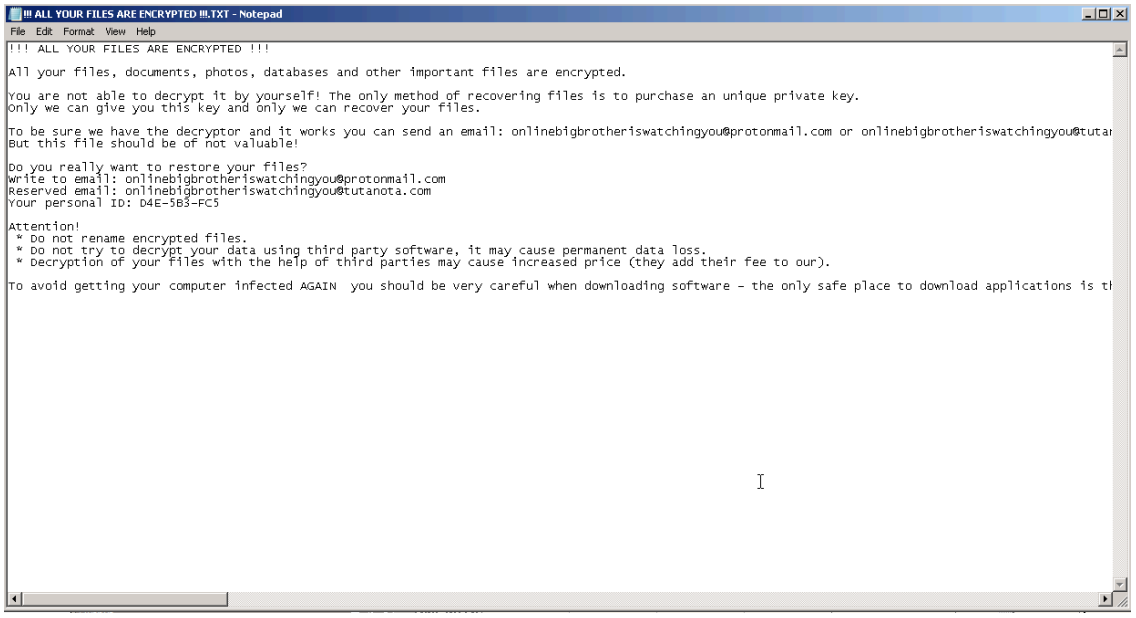
Then, all directories except Windows Operating System-related, Internet browsers and among other folders, will be traversed to encrypt all files in it. These whitelisted folders and its files are avoided to ensure the proper execution of the malware.

:\$Windows.~bt\	\Application Data\	\Internet Explorer\	\Windows Security\
:\System VolumeInformation\	\Boot\	\Windows Defender\	\Embedded Lockdown Manager\
:\Windows.old\	\Google\	\Windows Mail\	\Windows Journal\
:\Windows\	\Google\Chrome\	\Windows Media Player\	\MSBuild\
:\intel\	\Mozilla Firefox\	\Windows Multimedia Platform\	\Reference Assemblies\
:\nvidia\	\Mozilla\	\Windows NT\	\Windows Sidebar\
:\inetpub\logs\	\Opera Software\	\Windows Photo Viewer\	\Windows Defender Advanced Threat Protection\
\All Users\	\Opera\	\Windows Portable Devices\	\Microsoft\
\AppData\	\Tor Browser\	\WindowsPowerShell\	\Package Cache\
\Apple Computer\Safari\	\Common Files\	\Windows Photo Viewer\	\Microsoft Help\

Whitelisted File Paths

.bat	boot.ini
.cmd	bootfont.bin
.com	bootsect.bak
.cpl	desktop.ini
.dll	iconcache.db
.msc	ntdetect.com
.msp	ntldr
.pif	ntuser.dat
.scr	ntuser.dat.log
.sys	ntuser.ini
.log	thumbs.db
.lnk	
.zeppelin	

One of the evident changes in Zeppelin is that the infection coverage is wider as it infects more filetypes than Buran. For instance, Zeppelin not only infects document files but also executable files with ".exe" extension. This makes Zeppelin more destructive than Buran as it renders the victim's machine pretty much unusable by encrypting all software installed, unless the installation path is included in the whitelisted file paths. Every Zeppelin encrypted file can easily be distinguished by an infection marker "ZEPPELIN" that can be seen at the beginning of the file's content. This infection marker makes it distinct from Buran, but at the same time an indication that they are from the same family as they both leave infection markers at the start of each file using the same encryption routine. After all files in the directory are encrypted, a ransom note in text file format will be dropped. Lastly, it will open a ransom note using notepad.exe to inform the victim of the infection.



Ransom Note displayed by Zeppelin

Conclusion

In this day where we create faster solutions and detections, malware authors also adapt to this by creating and releasing more malware updates to make sure that it stays relevant. This is evident in ransomware campaigns as malware authors get an extra motivation by gaining huge sums of money in exchange for file recovery. Normally, ransomware only infects document files which is also the case with Buran. However, Zeppelin takes things a step further by targeting not only document related files but also applications and tools installed in the victim's system . This extent of damage gives Zeppelin more leverage for the victim to pay the ransom. With this, delivering more advanced detections and solutions that will withstand fast-paced changes of ransomware is needed. Just like G Data's DeepRay technology that uses artificial intelligence and machine learning to protect its user from such sophisticated tactics of criminal hackers.

Information for fellow researchers

G DATA Detections:

Buran: Win32.Trojan-Ransom.Buran.A
Zeppelin: Win32.Trojan-Ransom.Zeppelin.A

IOC

Buran:
7f0dcd4b9d8881fd0c42a6d605f843c496b7ed1fc3ae3a29d0bd37e851eaadfb

Zeppelin:
1cefe918ae56ebd3c2de309efbdd3a99808c823615a11a58bf144d3d6699f69b

References

[1] hxxps://www.symantec.com/blogs/expert-perspectives/ransomware-activity-declines-remains-dangerous-threat

[2] hxxps://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

[3] hxxps://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

---

Share Article

Content
