FLASHPOINT

FLASHPOINT HUNT TEAM:

Zeppelin Ransomware Analysis

Flashpoint's Hunt Team comprises talented researchers who specialize in identifying, investigating, and mitigating cyber threats. One of the recent examples of work provided by The Hunt Team analysts was extensive analysis of Zeppelin ransomware. Zeppelin was one of the most sophisticated and, therefore, expensive ransomware builders put on the underground market. It was one of the first examples of a sophisticated ransomware builder for sale that did not require affiliation with the criminal group in order to operate the ransomware. Because of this, it is impractical to associate "Zeppelin" attacks with any group since their business model essentially made it a Ransomware-as-a-Franchise.

The following outlines Zeppelin's origins and a technical analysis from the Flashpoint Hunt Team:

ZEPPELIN ORIGINS:

It all started on November 5, 2019, when a threat actor posted on top-tier Russian-language hacking forums offering a new ransomware builder named "Zeppelin."

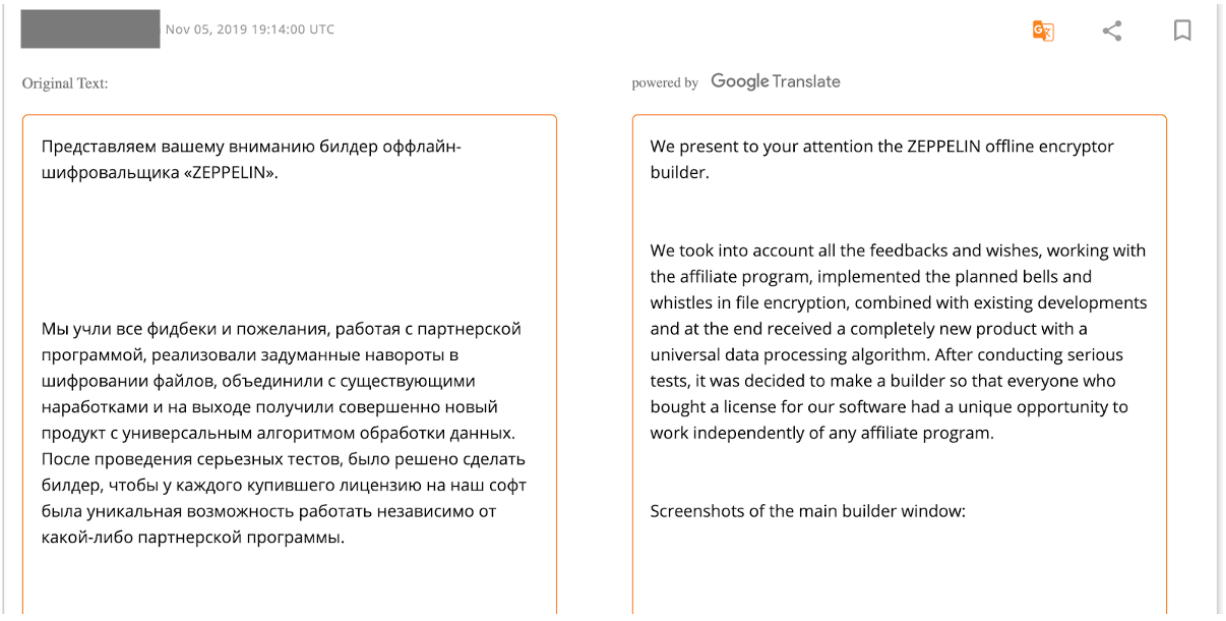
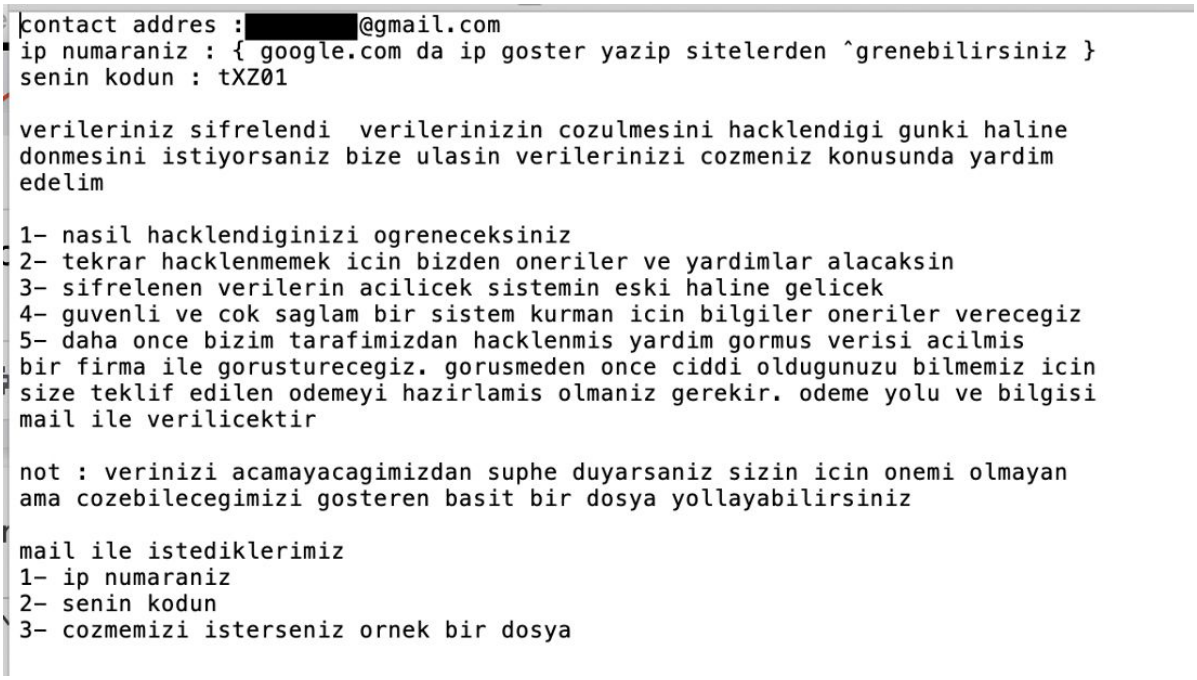


Image 1: Original Zeppelin offering for sale

The Zeppelin builder's notable features included the ability to execute arbitrary commands before starting the search, data encryption, and deliberate inability to execute on systems of the countries of the Commonwealth of Independent States (including Russia, Ukraine, Belarus, and Kazakhstan). In addition, the ransom note is completely customisable including content, language, and method of contacting the malicious actor.

For example this ransom note was written in Turkish and listed the contact address as a Gmail account.



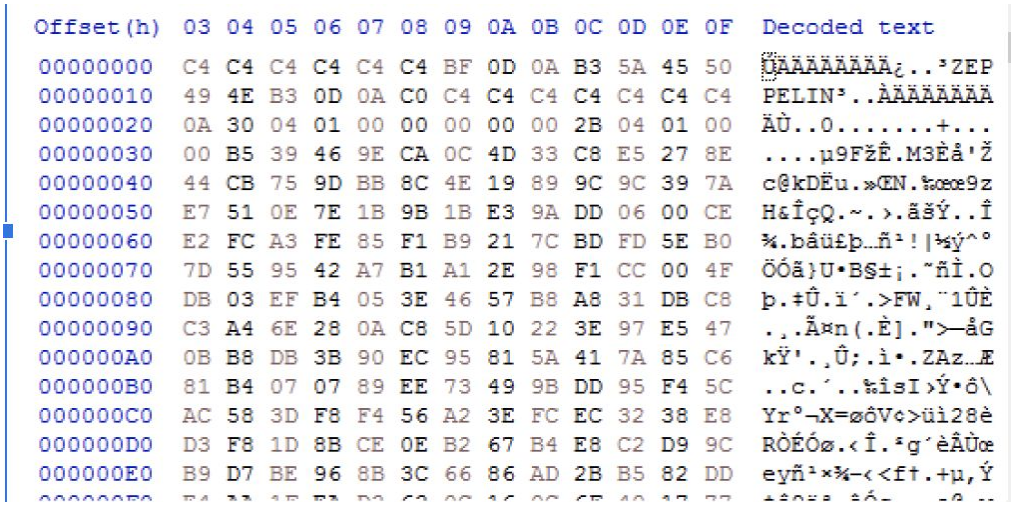
```
contact addres : [redacted]@gmail.com
ip numaraniz : { google.com da ip goster yazip sitelerden ^grenebilirsiniz }
senin kodun : tXZ01

verileriniz sifrelendi  verilerinizin cozulmesini hacklendigi gunki haline
donmesini istiyorsaniz bize ulasin verilerinizi cozmeniz konusunda yardim
edelim

1- nasil hacklendiginizi ogreneceksiniz
2- tekrar hacklenmemek icin bizden oneriler ve yardimlar alacaksin
3- sifrelenen verilerin acilicek sistemin eski haline gelicek
4- guvenli ve cok saglam bir sistem kurman icin bilgiler oneriler verecegiz
5- daha once bizim tarafimizdan hacklenmis yardim gormus verisi acilmis
bir firma ile gorusturecegiz. gorusmeden once ciddi oldugunuzu bilmemiz icin
size teklif edilen odemeyi hazirlamis olmaniz gerekir. odeme yolu ve bilgisi
mail ile verilicektir

not : verinizi acamayacagimizdan suphe duyarsaniz sizin icin onemi olmayan
ama cozebilecegimizi gosteren basit bir dosya yollayabilirsiniz

mail ile istediklerimiz
1- ip numaraniz
2- senin kodun
3- cozmemizi isterseniz ornek bir dosya
```

Image 2: Zeppelin ransom note

The first reports of Zeppelin ransomware infections appeared just a day after the initial offering, targeting tech and healthcare companies in Europe as well as the United States. Samples were hosted on water-holed websites and in the case of the PowerShell loader, on Pastebin. According to various researchers, at least some of the attacks were conducted through managed security service providers (MSSPs).

TECHNICAL ANALYSIS:

The distinct feature of the Zeppelin ransomware is that it encrypts files on the victim's computer with a custom extension and always prepends each with the same bytes. Ransomware prepends the hardcoded marker string "ZEPPELIN" to the beginning of each encrypted file. This is followed by an 8-byte length of encrypted data and an 8-byte length of original data, which includes a 3-byte "666" string that the ransomware adds to every file before the encryption.



Offset(h)	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	C4	C4	C4	C4	C4	C4	BF	0D	0A	B3	5A	45	50	ÛÄÄÄÄÄÄÄÄ¿..³ZEP
00000010	49	4E	B3	0D	0A	C0	C4	C4	C4	C4	C4	C4	C4	PELIN³..ÀÄÄÄÄÄÄÄÄ
00000020	0A	30	04	01	00	00	00	00	2B	04	01	00		ÄÙ..0.......+...
00000030	00	B5	39	46	9E	CA	0C	4D	33	C8	E5	27	8E	....µ9FžÊ.M3Èå'Ž
00000040	44	CB	75	9D	BB	8C	4E	19	89	9C	9C	39	7A	c@kDËu.»ŒN.‰œœ9z
00000050	E7	51	0E	7E	1B	9B	1B	E3	9A	DD	06	00	CE	H&ÎçQ.~.›.ãšÝ..Î
00000060	E2	FC	A3	FE	85	F1	B9	21	7C	BD	FD	5E	B0	¾.bâü£þ…ñ¹!|½ý^°
00000070	7D	55	95	42	A7	B1	A1	2E	98	F1	CC	00	4F	ÖÓã}U•B§±¡.˜ñÌ.O
00000080	DB	03	EF	B4	05	3E	46	57	B8	A8	31	DB	C8	þ.‡Û.ï´.>FW¸¨1ÛÈ
00000090	C3	A4	6E	28	0A	C8	5D	10	22	3E	97	E5	47	.¸.Ã¤n(.È]."›—åG
000000A0	0B	B8	DB	3B	90	EC	95	81	5A	41	7A	85	C6	kŸ'.¸Û;.ì•.ZAz…Æ
000000B0	81	B4	07	07	89	EE	73	49	9B	DD	95	F4	5C	..c.´..‰îsI›Ý•ô\
000000C0	AC	58	3D	F8	F4	56	A2	3E	FC	EC	32	38	E8	Yr°¬X=øôV¢>üì28è
000000D0	D3	F8	1D	8B	CE	0E	B2	67	B4	E8	C2	D9	9C	RÒÉÓø.‹Î.²g´èÂÙœ
000000E0	B9	D7	BE	96	8B	3C	66	86	AD	2B	B5	82	DD	eyñ¹×¾–‹<f†.+µ‚Ý

Image 3: Zeppelin encrypted file with the prepend

Flashpoint analysts were able to uncover key features of the ransomware builder such as it's position among the existing RaaS ecosystem, anti-analysis and anti-execution techniques, geopolitical affiliations, encryption standards and unique features allowing for the creation of precise signatures that can be used by intrusion detection systems.

Analysts uncovered that although the Zeppelin ransomware is an enhanced version of "Buran" ransomware and using the same implementation of RSA + RSA + AES and RNG for encryption and decryption functionality, the rest of the build, from functionality to installation mechanisms, is completely different and a stand-alone product.

The builder executable is able to create any number of 2048-bit RSA keys, which it saves in the "master.key" file. The public key from the RSA pair is hard-coded in several executables that are also generated by the builder: the master unlocker executable and the ransomware itself (in EXE, DLL, or PS1 form).

It is possible to generate numerous keys and therefore create numerous strains of the ransomware, each of which requires its own master unlocker. As an additional level of complexity, the seed that the builder uses for key generation is a time stamp counter, which is different for every actor and machine that uses the builder to generate a set of master keys.

Flashpoint analysts confirmed that the master builder that is generated with one set of keys cannot decrypt files that have been encrypted with different sets of master RSA-2048 keys. This feature ensures only the operator who creates the particular strain of Zeppelin ransomware can subsequently decrypt files encrypted with this strain.

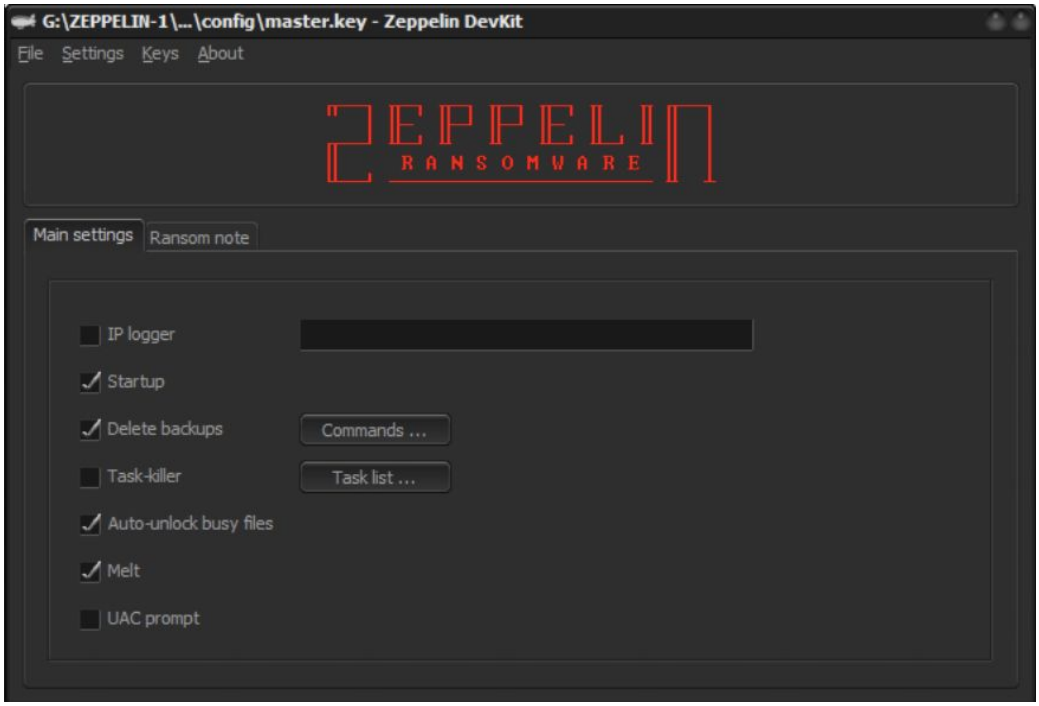


Image 4: Zeppelin builder user interface

It is not unusual for malware writers to use various obfuscation methods to make executables more difficult to detect or analyze. Zeppelin Raas creators went a step further and created various methods to thwart not only analysis, but also a usage of the ransomware builder by unwanted groups.

By examining the API calls, Flashpoint analysts were able to view the check that the executable performs to make sure the operator of the ransomware is a Russian speaker and/or a citizen of countries of the Commonwealth of Independent States. The program checks the computer locale, as well as the user's preferred and default languages, keyboard layout, and calendar information.

FINAL THOUGHTS:

Zeppelin offering showed that the RaaS made a leap in maturation in the tactics, techniques, and procedures (TTPs) of threat actors leveraging ransomware—either for more substantial financial gain or as a distraction from other illicit activities which brings ransomware once again to the top of the list of information security teams.

This comprehensive approach to the analysis of Zeppelin provided our clients with extensive IOCs related to this specific ransomware as well as unique insight into trends of modern ransomware in general. Ultimately, this leads the private and public sector to better determine the appropriate alerting capabilities needed and a thorough threat assessment of this ransomware for potential similar ransomware in the future.

ABOUT FLASHPOINT

Flashpoint is the globally trusted leader in risk intelligence for organizations that demand the fastest, most comprehensive coverage of threatening activity on the internet. From bolstering cyber and physical security, to detecting fraud and insider threats, Flashpoint partners with customers across the private and public sectors to help them rapidly identify threats and mitigate their most critical security risks.

For more information, visit **www.flashpoint-intel.com** or follow us on Twitter at **@FlashpointIntel**