cybersecurity associates

Zeoticus 2.0 Ransomware

Threat Hunting Report

Dated: 8th February 2021

By Zachary Goggins

This report contains Threat Hunting research carried out by CSA analysts to outline the subject threat to the reader. It highlights information about current and emerging threats to identify countermeasures which can be put into place to thwart the threat.

Contents

Zeoticus 2.0 Ransomware

Threat Hunting Report

Executive Summary

The purpose of this report is to document the current form and methodologies used by the Zeoticus 2.0 Ransomware. The information documented is then used by Cyber Security Associates Ltd (CSA) Cyber Analysts to hunt for the threat within the client environment through the use of our supported SIEM's BorderPoint and LogRhythm and advise on counter measures to monitor and detect for the subject threat.

This report documents the lifecycle of the Zeoticus 2.0 Ransomware and how it operates, with supporting evidence and recommendations to mitigate the emerging threat. The report also includes a list of identified indicators of compromise and references where the information within this report was identified from.

Summary

During December 2019, the ransomware strain Zeoticus (1.0) made its first appearance. It will arrive on a system as a file dropped by other malware or as a file downloaded by victims that were tricked into visiting malicious websites. But during September 2020, Zeoticus (2.0) appeared with new improvements. Unlike its predecessor, it can now execute its payloads without depending on a Command and Control (C2) server and it does not need to be connected or rely on remote commands.

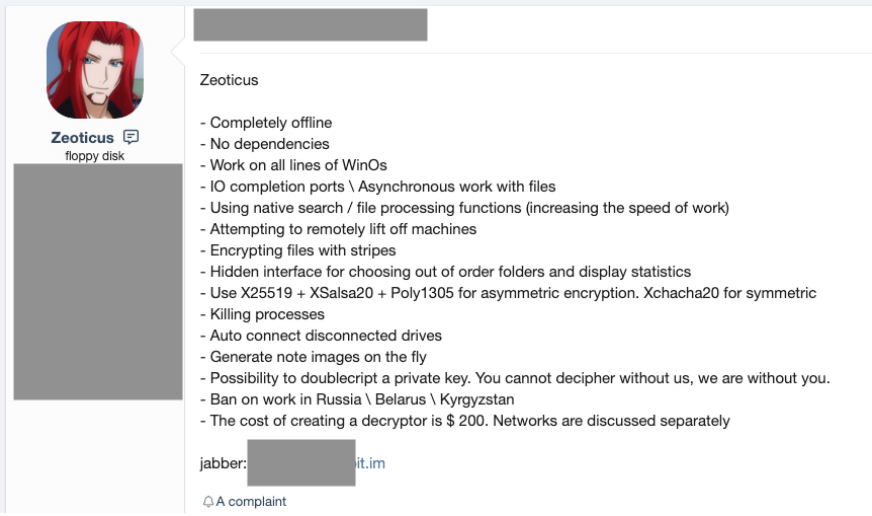

Figure 1: Public Announcement

Zeoticus (2.0) is designed to exclude victims that are based in the regions of Belarus, Kyrgyzstan and Russia, so it is thought that it has been designed by Russian operators. It appeared as an underground ransomware-as-a-service (RaaS) platform that was sold in various dark web forums and markets. The new version (2.0) is more effective and versatile than its predecessor as its upgrades are focused on speed and efficiency, this includes using rapid encryption algorithms. This ransomware is unique to Windows and it functions on all supported versions.

Tactics, Techniques, Procedures

Tactics, Techniques, and Procedures (TTP) describes an approach of analysing an APT's operation or can be used as means of profiling a certain threat actor.

Tactics is meant to outline the way an adversary chooses to carry out his attack from the beginning till the end. Technological approach of achieving intermediate results during the campaign is described by Techniques the attacker uses. Lastly, the organizational approach of the attack is defined by procedures which are used by the threat actor.

In order to understand and fight the enemy one has to understand the Tactics, Techniques and Procedures (TTP) the attacker uses. Understanding the Tactics of an adversary can help in predicting the upcoming attacks and detect those in early stages. Identifying the Techniques used during an attack allows to identify an organisation's blind spots and implement countermeasures in advance. Finally, the analysis of the procedures used by the adversary can help to understand what the adversary is looking for within their target's infrastructure.

TTPs that are described within this research are based of the information which CSA analysts have been able to identify prior to the release of this document. The threat may change and adapt as it matures to increase its likelihood of evading defence.

Hackers
A 'hacker' is a person who finds it interesting to interfere with computer systems. Often seen as a challenge, a hacker will attempt to breach a system because it tests their skills and knowledge.

Hacktivists
A 'hacktivist' is a person who gains unauthorized access to computer files or networks in order to further social or political ends.

Insider Threats
An employee or 'insider' is a person within a group or organisation, especially someone with knowledge of information unavailable to others.

State Sponsored
A 'state actor' is a person who is acting on behalf of a governmental body and is therefore subject to regulation under their human rights.

Organised Crime
A 'criminal gang' is a group of people that take part in organised unlawful activity.
They may target a business to gather information on customers or to gather financial data which could be sold.

Phase 1: Initial Access: Multiple Attack Vectors

Zeoticus (2.0) has numerous ways it could gain access to a system identified through the public reports, but the most common way for this ransomware to gain access is through the use of spam messages within emails. Other ways include the integration of third-party software, such as freeware, using websites that render free hosting services and pirated peer-to-peer (P2P) downloads.

Malicious actors may present Zeoticus (2.0) as a genuine software application which can lead to website pop-ups that instruct users to implement crucial software updates. This is one technique that is used to try and persuade people into downloading and installing the ransomware manually. Another technique revolves around the use of cracked applications, as attackers can pack malicious code into these types of programs that could lead to the download and installation of Zeoticus (2.0). This ransomware will then look to establish persistence by infecting remote drives and terminating processes.

MITRE ATT&CK

MITRE developed the Adversarial Tactics, Techniques and Common Knowledge framework (ATT&CK), which is used to track various techniques attackers use throughout the different stages of cyberattack to infiltrate a network and exfiltrate data.

The framework defines the following tactics that are used in a cyberattack:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Phase 2: Persistence: Kill Processes

After Zeoticus (2.0) has been activated on a system it looks to make a few copies of itself in the following locations: C:\Windows and %AppData% to establish persistence. This is followed up by the ransomware using taskkill.exe to halt a number of running processes that could prevent the encryption from occurring. See Indicators of Comprise section for a full list.

To facilitate the deletion of its own binaries, Zeoticus (2.0) will use the ping command, it will then redirect the output of the command to >nul & del.

- /c ping localhost -n 3 > nul & del %s

To help gather additional information about the local environment, it will issue a Windows Management Instrumentation (WMI) query. See Indicators of Comprise section for the full query.

For persistence, Zeoticus (2.0) creates a Registry Run key:

- \REGISTRY\USER\----\Software\Microsoft\Windows\CurrentVersion\Run\

The registry entry (Run) will execute an instance of the Zeoticus (2.0) payload from C:\Windows.

Cyber Kill-Chain

The cyber kill-chain is a process that traces the stages of a cyberattack. This starts at the early reconnaissance stages that eventually leads to data exfiltration.

The kill-chain can help one to understand and combat ransomware, advanced persistent threats (APTs) and security breaches.

The cyber kill-chain defines the following tactics that are used in a cyberattack:

- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Obfuscation/ Anti-forensics
- Denial of Service
- Exfiltration

Phase 3: Encryption: Ransom Note

Zeoticus (2.0) is focused on speed and efficiency as it relies on rapid encryption algorithms. It uses a combination of asymmetric and symmetric encryption. The symmetric side consists of XChaCha20, and the asymmetric side comprises Poly1305, XSalsa20 and Curve25519. This will aim to lock archives, audio files, databases, documents, images, presentations, spreadsheets, and videos. Encrypted files are modified with extensions, and these include the contact email address of the attackers with the string 2020END.

Symmetric encryption is used to both encrypt and decrypt electronic information, where only one key (a secret key) is used. The entities that communicate via symmetric encryption have to exchange the secret key so that it can be used for the decryption process.

Asymmetric encryption is also used to both encrypt and decrypt data, but this is achieved by using two separate keys that are mathematically connected. These are

known as a **Public Key** and a **Private Key**, together they are known as a **Public and Private Key Pair.**

For the ransom note, Zeoticus (2.0) will mount a new volume which occurs during the encryption process of the host's data. The malicious actor then looks to instruct the victim to make contact via email, as opposed to using an onion-based payment portal like other ransomware gangs. Finally, a copy of the ransom note is left in the root of the system drive: **C:\Windows\README.html.**

Conclusion

Zeoticus (1.0) has contrasting similarities and differences with version 2.0. One difference involves how v1.0 used to alter the desktop wallpaper while presenting the ransom note, whereas v2.0 will mount a new volume that contains the ransom note and the host encrypted data. One similarity is how both versions create the registry run key to achieve persistence. The registry entry is set to launch the Zeoticus payload from: **C:Windows.** V2.0 is compatible with all versions of Windows, its use of rapid encryption algorithms make it difficult for researchers to contain, control and mitigate it and it does not require a C2 server for remote command execution or exfiltration.

Advice

The IOC's identified within this report are monitored by our SIEM solution, BorderPoint, if a host were to demonstrate any of the characteristics CSA would ensure to alarm you. It is imperative that there is a backup strategy in place that is tested and that it also covers worst-case scenarios. CSA recommends:

- **Regular Backups must be kept offline**; this is the only way to mitigate the damage which may be caused by a determined threat actor.
- **Regularly test backups for their integrity and if they can be recovered**. Scan backups for registry persistence.
- **Critical data should be written on WORMs (Write Once Read Many).** This write protection ensures that the data cannot be tampered with once it is written to the device.
- **Disable all macros, except those that are digitally signed.** This will display a security notification for macros that were developed by a certified publisher, allowing one to decide whether to enable or disable them.
- **Implement filters at the email gateway**. Filter out emails with known malspam indicators and block suspicious IP addresses at the firewall.
- **Educate and train employees on social engineering and phishing.** This is a common infection method for malware and ransomware, training employees in this area can reduce the risk of a compromise though emails.

- **Adhere to the Principle of Least Privilege (PLP).** Ensure that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated admins.
- **Use antivirus programs on clients and servers**. Keep it up to date with automatic updates of signatures and software.
- **If there is not a policy regarding suspicious emails, consider creating one**. Specify that all suspicious emails should be reported to the security and/or IT departments. Using CSA's tool **AppGuard** will prevent interaction with the system space.

Indicators of Compromise

Alias:

Vendor	Virus Alias
Avast	Win32:Trojan-gen
BitDefender	Gen:Heur.Ransom.REntS.Gen.1
DrWeb	Trojan.Encoder.33303
Emsisoft	Gen:Heur.Ransom.REntS.Gen.1 (B)
ESET-NOD32	A Variant Of Win32/Filecoder.OBQ
Kaspersky	Packed.Win32.Krap.b
Malwarebytes	Ransom.FileCryptor
Microsoft	Trojan:Win32/Ymacco.AA27
Panda	Trj/GdSda.A
Sophos	Mal/Generic-S
Symantec	ML.Attribute.HighConfidence
TrendMicro	TROJ_GEN.R002C0PLB20
VBA32	BScope.Trojan.Staser
VIPRE	Trojan.Win32.Generic!BT
ZoneAlarm	Packed.Win32.Krap.b

Processes:

sqlagent.exe, sqlbrowser.exe, sqlservr.exe, sqlwriter.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, mydesktopqos.exe, agntsvc.exe, isqlplussvc.exe, xfssvccon.exe, mydesktopservice.exe, ocautoupds.exe, agntsvc.exe, agntsvc.exe, agntsvc.exe, encsvc.exe, firefoxconfig.exe, tbirdconfig.exe, ocomm.exe, mysqld.exe, mysqld-nt.exe, mysqld-opt.exe, dbeng50.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, sqlservr.exe, thebat64.exe, thunderbird.exe, winword.exe, Wordpad.exe

Hashes:

MD5:

- d0e87fd356979aff2a420957ec070d54

SHA1:

- 25082dee3a4bc00caf29e806d55ded5e080c05fa
- d3449118b7ca870e6b9706f7e2e4e3b2d2764f7b

SHA256:

- 33703e94572bca90070f00105c7008ed85d26610a7083de8f5760525bdc110a6
- 279d73e673463e42a1f37199a30b3deff6b201b8a7edf94f9d6fb5ce2f9f7f34

Commands:

- /c ping localhost -n 3 > nul & del %s

Registry Run Key:

- \REGISTRY\USER\----\Software\Microsoft\Windows\CurrentVersion\Run\

Ransom Notes:

- READ_ME.html

Figure 2: Ransom note Zeoticus (1.0)

- README.html

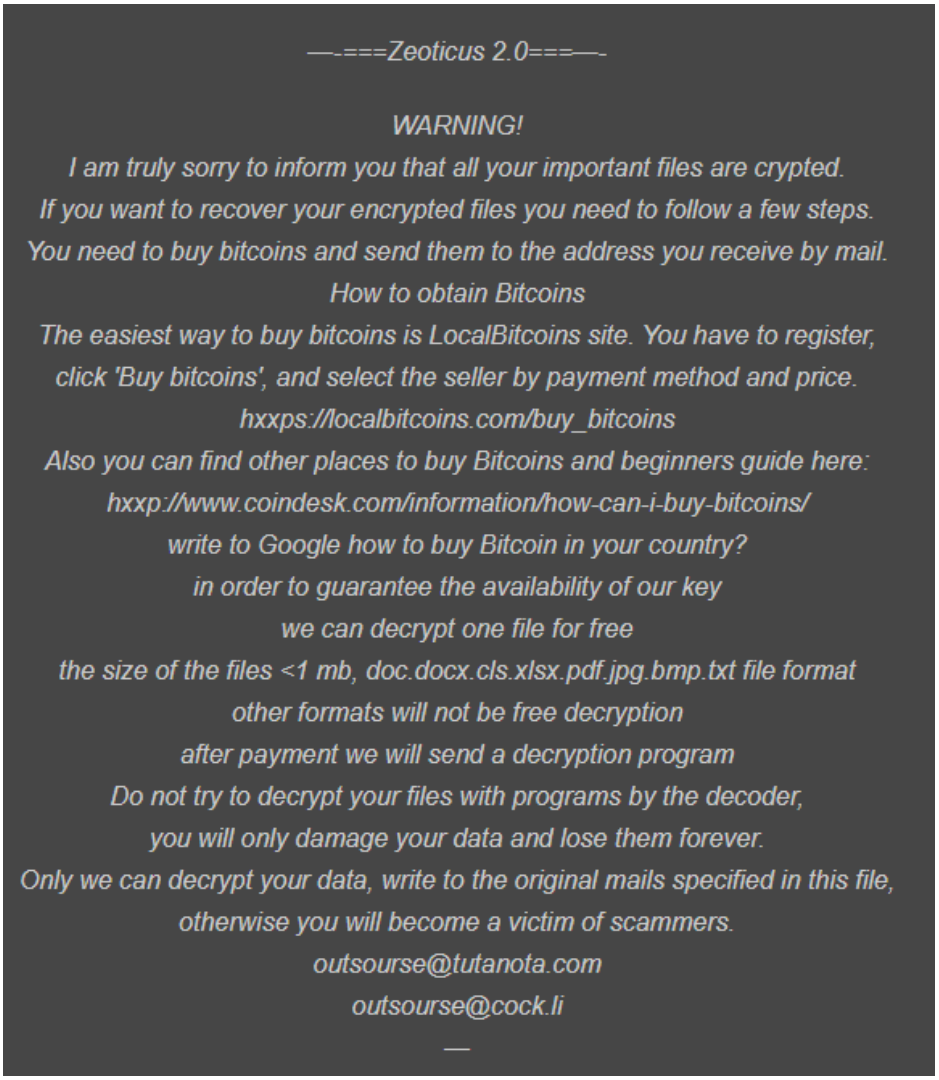

Figure 3: Ransom note Zeoticus (2.0)

Hardcoded Extension (Appended to each encrypted file):

- .zeoticus (v1.0) - This extension appears to have been used during early 2020.
- .immunityyoung@aol.com.young (v2.0) - This extension appears during Sept. 2020.
- .2020END (v2.0) - This extension appears first during Dec. 2020.

WMI Query:

start iwbemservices::execquery - root\cimv2 : select __path, processid, csname, caption, sessionid, threadcount, workingsetsize, kernelmodetime, usermodetime, parentprocessid from win32_process where (caption = "msftesql.exe" or caption =

"sqlagent.exe" or caption = "sqlbrowser.exe" or caption = "sqlservr.exe" or caption = "sqlwriter.exe" or caption = "oracle.exe" or caption = "ocssd.exe" or caption = "dbsnmp.exe" or caption = "synctime.exe" or caption = "mydesktopqos.exe" or caption = "agntsvc.exe" or caption = "isqlplussvc.exe" or caption = "xfssvccon.exe" or caption = "mydesktopservice.exe" or caption = "ocautoupds.exe" or caption = "agntsvc.exe" or caption = "agntsvc.exe" or caption = "agntsvc.exe" or caption = "encsvc.exe" or caption = "firefoxconfig.exe" or caption = "tbirdconfig.exe" or caption = "ocomm.exe" or caption = "mysqld.exe" or caption = "mysqld-nt.exe" or caption = "mysqld-opt.exe" or caption = "dbeng50.exe" or caption = "sqbcoreservice.exe" or caption = "excel.exe" or caption = "infopath.exe" or caption = "msaccess.exe" or caption = "mspub.exe" or caption = "onenote.exe" or caption = "outlook.exe" or caption = "powerpnt.exe" or caption = "sqlservr.exe" or caption = "thebat64.exe" or caption = "thunderbird.exe" or caption = "winword.exe" or caption = "wordpad.exe")

References

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom.win32.zeoticus.b/

https://cyber-reports.com/2021/02/04/zeoticus-2-0-ransomware-raises-stakes-with-c2-free-execution-supercharged-encryption/

https://www.technadu.com/zeoticus-2-0-ransomware-doesnt-need-c2-server/246049/amp/%7B%7B%20url/246049/

https://labs.sentinelone.com/zeoticus-2-0-ransomware-with-no-c2-required/

https://www.enigmasoftware.com/zeoticusransomware-removal/

https://www.pcrisk.com/removal-guides/16695-zeoticus-ransomware

https://portswigger.net/daily-swig/zeoticus-2-0-ransomware-raises-stakes-with-c2-free-execution-supercharged-encryption?&web_view=true

https://adware.guru/remove-zeoticus-2-0-virus/

https://sensorstechforum.com/remove-zeoticus-virus/?utm_source=hs_email&utm_medium=email&utm_content=81475905&_hsenc=p2ANqtz--MZtJQCwb0vrDVqKkjuMvpLYeCviNkargIDjHJQRjGJXaMj8IXC-79NC2K01Ly3sg9gqGOJaTcwdk9ZGEWmmi2JdT41g&_hsmi=81475905

https://intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://www.computips.org/how-to-remove-zeoticus-2-0-ransomware/

https://malware-guide.com/blog/how-to-remove-zeoticus-2-0-ransomware-and-recover-encrypted-files

https://cyware.com/news/zeoticus-20-making-infections-are-now-harder-to-control-contain-and-mitigate-c2bcdb8f

https://malwarefixes.com/remove-2020end-ransomware-zeoticus-2-0/