INTER PROBE

INTELLIGENCE & ANALYTICS

Malware Trends

Prepared by

INTERPROBE

July,2022

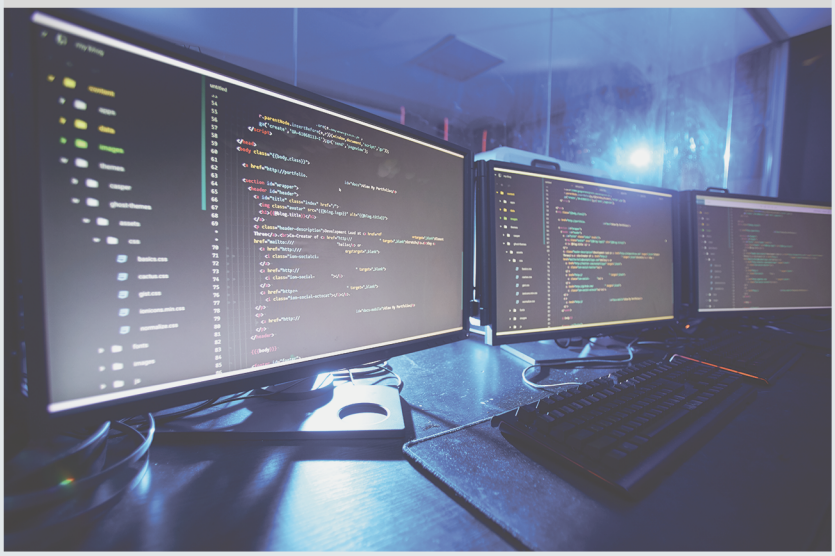
Table of Contents

INTELLIGENCE ANALYTICS

InterProbe

July 2022 – Malware Trends

About InterProbe



InterProbe designs unique products, solutions, and services to address varying technological needs of organizations from any industry, including especially of those organizations that are engaged in a sensitive field of activity. Our team of highly qualified engineers and experts design and manufacture next-generation technologies. We are a real partner that strives to add value to your business through software that we continuously develop.

With our headquarters in Ankara, Istanbul Technopark branch as well as our offices in Azerbaijan, Qatar and Kazakhstan, we offer strategic solutions to all organizations around the world. Our R&D investments mean that we closely follow trends in security technologies and collaborate with other organizations around the world to create value. We have a strong sense of responsibility for the development and growth of Turkey, and this is the strongest aspiration that guides our operations. InterProbe organizes training and internship programs intended to improve the competencies and skills of especially young graduates and university students. We also allocate resources to give project support to young software developers. Being a part of Pavo Group companies and bringing many projects to successful completion, we offer end-to-end solutions developed with national resources and capabilities within the group of the following companies.

PAVOTEK, a company that has been operating in the defense industry for many years and providing services mainly in the fields of digital communication and embedded software,

PANOD, a company that specializes in electro-mechanical production, assembly (SMD and THT), and testing,

PAVELSIS, a company that operates in the fields of avionics systems, military electronics and communication systems, biomedical solutions, power electronics and IoT,

PNETWORKS, a company that designs and manufactures network security products and switching-routing devices, and

INTERDATA, a company that offers construction, infrastructure and installation services for data centers.

Introduction

InterProbe

Cyber security gains more importance day by day. Neither protecting a system nor compromising it is not as easy as before. 2000's that could be compromised with a simple telnet vulnerability is much rarer thanks to standardized libraries and the increase in cyber security awareness. That's why adversaries adopted new strategies and techniques. Now it became clearer that the weakest link in cyber security is human itself which is the reason behind increase of phishing activities. At the same time adversaries started to chase vulnerabilities that can't be patched easily anytime soon. Of course, as much as these techniques effective adversaries need to alter their techniques if they want to bypass signature-based scans quickly. That why adversaries developed fast ways to change malicious code. As signature-based systems are not good enough to detect these threats the cyber security experts that understand the turn is on them noticed that tracing behaviors of malwares is much more effective.

At this point, as the InterProbe Fusion Center team, we are here with the first issue of the InterProbe Malware Newsletter, to make it easier for cybersecurity teams to follow current trends. Our newsletter will be published every month with trending malware, recent activities related to malware and new techniques of the actor that uses the malware in a language that almost everyone interested in cyber security can understand.

We wish you a happy reading.

.

Executive Summary

InterProbe

Cyber security universe is lively as always. Here is the malware researches we gathered for you this month:

- Researchers at ESET said that there is a new malware that threatens MacOS users. Dubbed as CloudMensis, this malware targets private data of MacOS users.
- Malwares has infiltrated to Google Play Store. Malware named Autolycos is downloaded from Google Play Store around 3 million times.
- Malwares started to use new techniques to infiltrate to system. ChromeLoader malware threatens users through malicious QR codes.
- MedusaLocker Ransomware continues to threaten health care sector. FBI warned against recent activities of MedusaLocker malware.
- A new ransomware is born. It seems like new Lilith Ransomware contains similarities with BABUK Ransomware.

CloudMensis

CloudMensis

InterProbe

Researchers at ESET said that they discovered a new malware that threatens users. Dubbed as “CloudMensis”, this spyware targets MacOS, IOS and iPadOS platforms. CloudMensis spyware is developed using Objective-C language. Malware analysts said that they still couldn’t determine how this malware infects systems, but they determined at what stage malware executes code and escalate privileges.

CloudMensis spyware has been seen to evade a control mechanism named “Transparency Consent and Control” in MacOS systems that is used to control application permissions. Integrity of TCC rules is protected by security mechanism named “System Integrity Protection”. If SIP is not active, malicious application can change permissions it has by itself. In some systems even if SIP is active, if system version is lower than “Catalina 10.15.6”, they can be exploited using CVE-2020-9943 which is the case in CloudMensis spyware.

After analyzing malicious code and obfuscation methods used in the malware, researchers at ESET thinks that the malware author may not be an advanced Mac developer.

CloudMensis

InterProbe

> *"We still do not know how CloudMensis is initially distributed and who the targets are. The general quality of the code and lack of obfuscation shows the authors may not be very familiar with Mac development and are not so advanced. Nonetheless, a lot of resources were put into making CloudMensis a powerful spying tool and a menace to potential targets."*

Figure 1 - Comments from researchers | Source: https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/

After CloudMensis spyware gains necessary permissions by code execution, it downloads a spyware agent from cloud servers like Dropbox, pCloud or Yandex. Downloaded agent is more capaple than the initial access payload. Finally, spyware agent communicates with cloud servers to exfiltrate data.

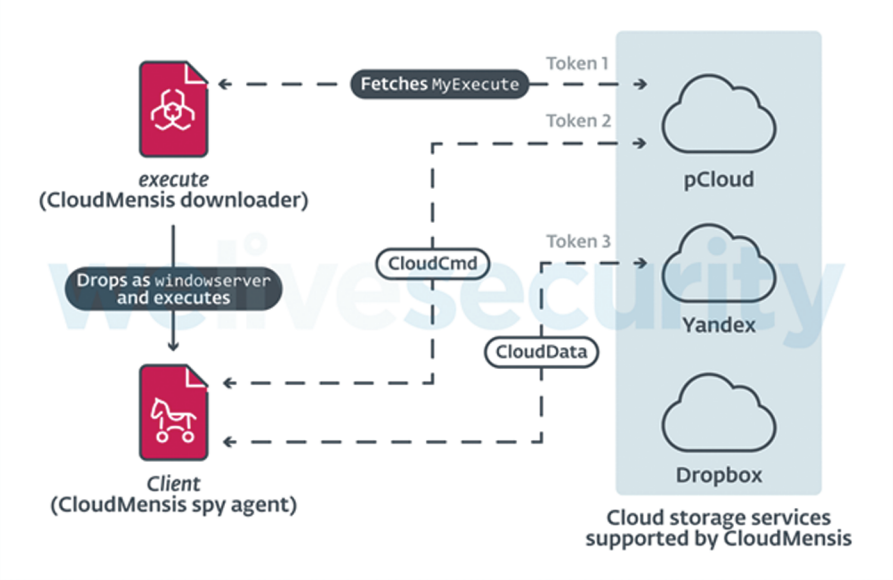


Figure 2 – How Cloudmensis uses cloud storage services. | Source: https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/

CloudMensis

CloudMensis MITRE ATT&CK Matrix

InterProbe

Persistence	T1543.004	Create or Modify System Process: Launch Daemon	The CloudMensis downloader installs the second stage as a system-wide daemon.
Defense Evasion	T1553	Subvert Trust Controls	CloudMensis tries to bypass TCC if possible.
Collection	T1560.002	Archive Collected Data: Archive via Library	Archive Collected Data: Archive via Library CloudMensis uses SSZipArchive to create a password-protected ZIP archive of data to exfiltrate.
	T1056.001	Input Capture: Keylogging	CloudMensis can capture and exfiltrate keystrokes.
	T1113	Screen Capture	CloudMensis can take screen captures and exfiltrate them.
	T1005	Data from Local System	CloudMensis looks for files with specific extensions.
	T1025	Data from Removable Media	CloudMensis can search removable media for interesting files upon their connection.
	T1114.001	Email Collection: Local Email Collection	CloudMensis searches for interesting email messages and attachments from Mail.
Command and Control	T1573.002	Encrypted Channel: Asymmetric Cryptography	The CloudMensis initial report is encrypted with a public RSA-2048 key.
	T1573.001	Encrypted Channel: Symmetric Cryptography	CloudMensis encrypts exfiltrated files using password-protected ZIP archives.
	T1102.002	Web Service: Bidirectional Communication	CloudMensis uses Dropbox, pCloud, or Yandex Drive for C&C communication.
Exfiltration	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	CloudMensis exfiltrates files to Dropbox, pCloud, or Yandex Drive.

Recommendations and Mitigations

- Don't open e-mail attachments came from unknown sources.
- Use only trusted resources like "App Store" to download apps.
- Make sure "System Integrity Protection (SIP)" is active on MacOS devices.

Properties

Properties

InterProbe

01 Ability to download files to infected system.

02 Keylogging

03 Ability to take screenshots from infected systems.

04 Ability to exfiltrate private content like documents and e-mail contents.

05 Ability to use pCloud, Yandex Disk, Dropbox or similar cloud services to download files, exfiltrate data and take commands.

06 Bypassing MacOS system protections without using exploits.

07 Ability to list running processes on the infected system.

Autolycos

InterProbe

Autolycos

In June 2021, one of the researchers of the Evina company named Maxime Ingaro discovered that a malware is hiding in Google Play Store. This newly discovered malware is variant of "SpyJoker" malware. Ingaro named this new variant "Autolycos" and informed Google about his findings but Google took action only after 6 months later and found 6 of 8 malware samples in Google Play then removed them.

On July 13th, Maxime Ingaro posted that there are still 2 malwares hiding Google Play Store to 2022 July. After that post Google took action quickly and removed the last 2 malicious apps from Google Play Store. Terrifying part of this is these apps downloaded more than 3 million time and maybe they are still active in some users devices.

Autolycos

Autolycos

InterProbe

If there is any application mentioned in the below is downloaded in your device, you should remove those applications.

These Applications are:

- Vlog Star Video Editor (com.vlog.star.video.editor): **1 million downloads**
- Creative 3D Launcher (app.launcher.creative3d): **1 million downloads**
- Wow Beauty Camera (com.wowbeauty.camera): **100.000 downloads**
- Gif Emoji Keyboard (com.gif.emoji.keyboard): **100.000 downloads**
- Razer Keyboard & Theme (com.razer.keyboards): **10.000 downloads**
- Freeglow Camera 1.0.0 (com.glow.camera.open): **5.000 downloads**
- Coco Camera v1.1 (com.toomore.cool.camera): **1.000 downloads**

Autolycos

Autolycos MITRE ATT&CK Matrix

Hash: 95547426cd892cc50547d65aef7edb82212c68a44257318cb89fbfcfa04889bb

InterProbe

MITRE ATT&CK™ Techniques Detection

Execution

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1402	Broadcast Receivers	• Persistence • Execution	An intent is a message passed between Android application or system components. Learn more	• 1 confidential indicators		

Persistence

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1402	Broadcast Receivers	• Persistence • Execution	An intent is a message passed between Android application or system components. Learn more	• 1 confidential indicators		

Defense Evasion

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1418	Application Discovery	• Defense Evasion • Discovery	Adversaries may seek to identify all applications installed on the device. Learn more		• 1 confidential indicators	

Discovery

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1418	Application Discovery	• Defense Evasion • Discovery	Adversaries may seek to identify all applications installed on the device. Learn more		• 1 confidential indicators	
T1421	System Network Connections Discovery	• Discovery	On Android, applications can use standard APIs to gather a list of network connections to and from the device. Learn more			• Tests the internet connectivity

Collection

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1114	Email Collection	• Collection	Adversaries may target user email to collect sensitive information. Learn more		• Found a potential E-Mail address in binary/memory	
T1429	Capture Audio	• Collection	Adversaries may capture audio to collect information on a user of a mobile device using standard operating system APIs. Learn more		• Has the ability to record audio	

Command and Control

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1573	Encrypted Channel	• Command and Control	Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Learn more			• Possibly tries to communicate over SSL connection (HTTPS)

Impact

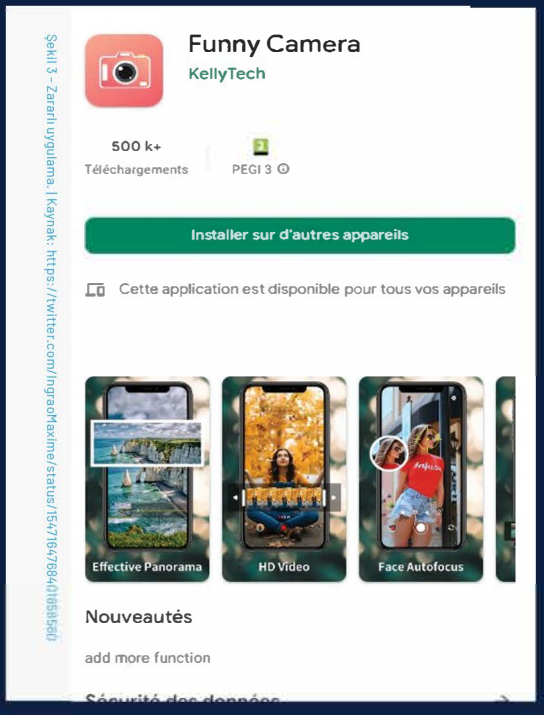
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1486	Data Encrypted for Impact	• Impact	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. Learn more		• Found a cryptographic related string	

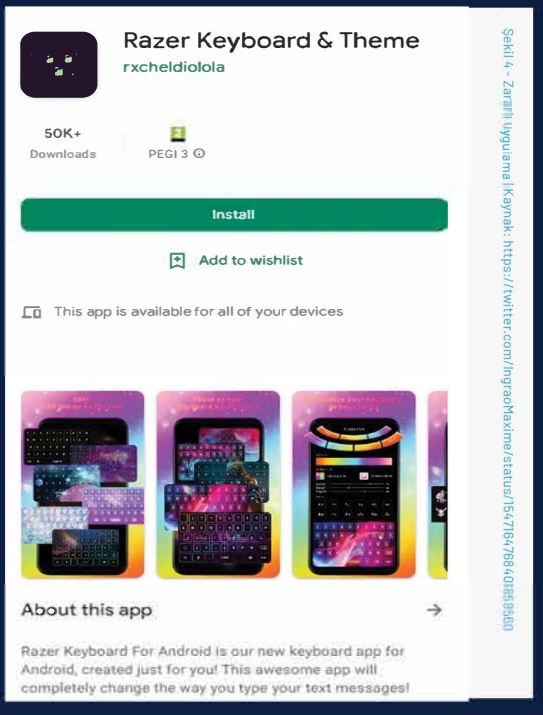
Recommendations and Mitigations

- Control what permissions applications want when downloading it from Google Play Store and other application stores.
- Check comments to see if there is something unusual about the application you want to download.
- Beware of malicious applications that is advertised through social media platforms.

Autolycos

InterProbe





Properties

- Access to SMS content
- Access to OTP data
- Registering premium services by sending HTTP requests through remote browser rather than using Webview.

ChromeLoader

ChromeLoader

InterProbe

In July, cyber security researchers found new variants of malware named as “ChromeLoader” and “Choziosi Loader”. ChromeLoader malware made his debut at January 2022 and targets Chrome application installed on MacOS and Windows platforms by downloading malicious plugins to take control of Chrome browser. Compared to other malwares, ChromeLoader uses a different infection technique. ChromeLoader infects systems through malicious QR code posts on Twitter. When users scan the malicious QR codes, it downloads malicious .iso, .dmg and .dhk files. In Windows systems, it installs malicious files with the help of Powershell. Researchers at Red Canary said that this technique is not common and it is often goes undetected by most of security solutions.

Malicious plugin manipulates browser to redirect users to ad sites and gather information from the browser.

A researcher named Colin Cowie published an analysis report of MacOS variant of ChromeLoader. MacOs variant is seen infecting Safari browser too. Like Windows version, malware still uses scripting languages to infect the system.

ChromeLoader

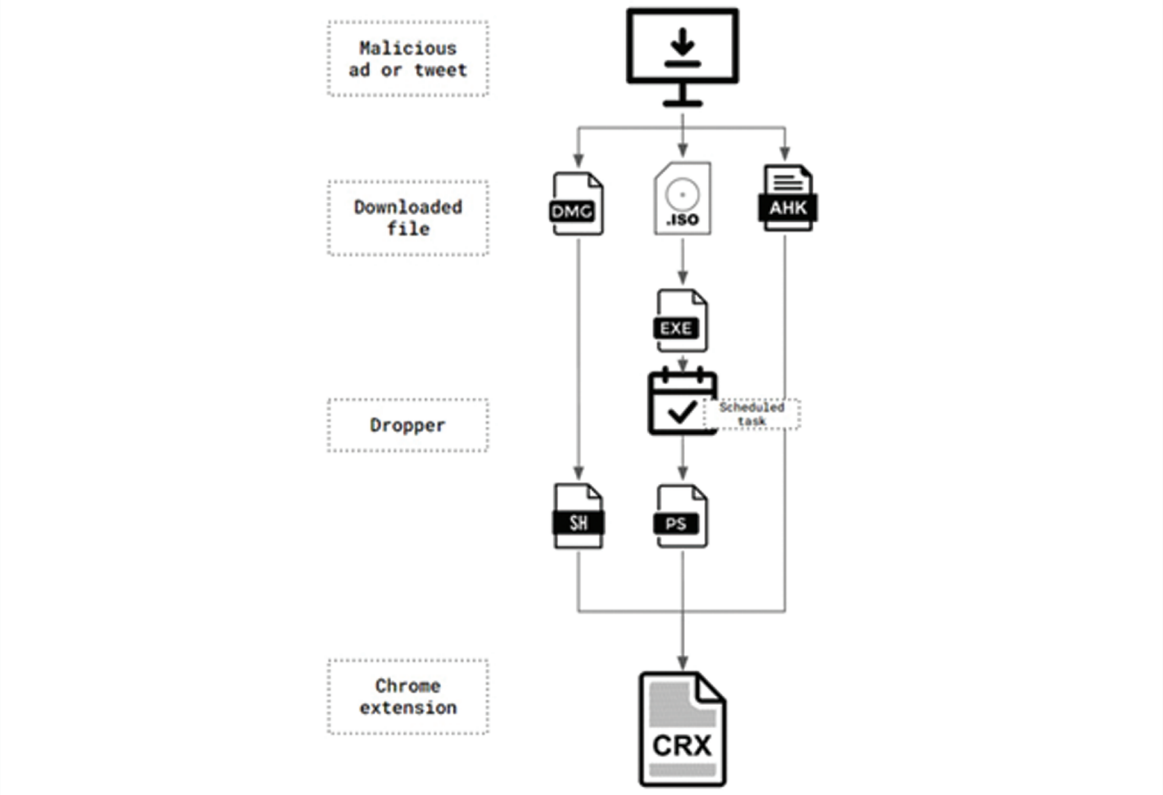


Figure 5 – ChromeLoader execution scheme | Source: https://unit42.paloaltonetworks.com/chromeloader-malware/

Properties

01 Ability to bypass security measures using obfuscation and evasion techniques.

02 Accessing browser data and manipulating it.

03 Redirects users to advertising websites.

ChromeLoader

ChromeLoader MITRE ATT&CK Matrix

InterProbe

Defense Evasion

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1027.002	Software Packing	• Defense Evasion	Adversaries may perform software packing or virtual machine software protection to conceal their code. Learn more			• Matched Compiler/Packer signature ◦ 61d8...c9c1

Credential Access

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1056.004	Credential API Hooking	• Credential Access • Collection	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more		• Installs hooks/patches the running process ◦ 61d8...c9c1	

Discovery

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1120	Peripheral Device Discovery	• Discovery	Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. Learn more			• Queries volume information ◦ 61d8...c9c1
T1082	System Information Discovery	• Discovery	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Learn more		• Reads the cryptographic machine GUID ◦ 61d8...c9c1	• Contains ability to read software policies ◦ 61d8...c9c1
T1012	Query Registry	• Discovery	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. Learn more		• Reads information about supported languages ◦ 61d8...c9c1 • Reads the active computer name ◦ 61d8...c9c1	

Collection

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1056.004	Credential API Hooking	• Credential Access • Collection	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more		• Installs hooks/patches the running process ◦ 61d8...c9c1	

Recommendations and Mitigations

- Use trusted resources only to download plugins.
- Don't use pirated software.
- Be careful against social engineering attacks that can be executed using e-mails and messages.
- Make sure your security softwares are up to date.
- Suspicious powershell/bash processes should be controlled. As an example, if they had base64 encoded parameters that would be suspicious.

MedusaLocker Ransomware

InterProbe

FBI(Federal Bureau of Investigation), CISA(Cybersecurity and Infrastructure Security Agency) and FinCEN warned against MedusaLocker Ransomware which made its debut into Ransomware Sector in 2019 and showed new activities around May 2022. Medusalocker ransomware targets healthcare sector and it is one of the malwares that abused Covid-19 pandemic.

The Malware thought to be adopted RaaS(Ransomware as a Service) business model which can be summarized as a business model where malware developer sells its ransomware to other adversaries to spread the malware then split the ransom. %55-60 of the ransom is paid to one account and remaining ransom is transferred to another. This supports RaaS model is used in MedusaLocker

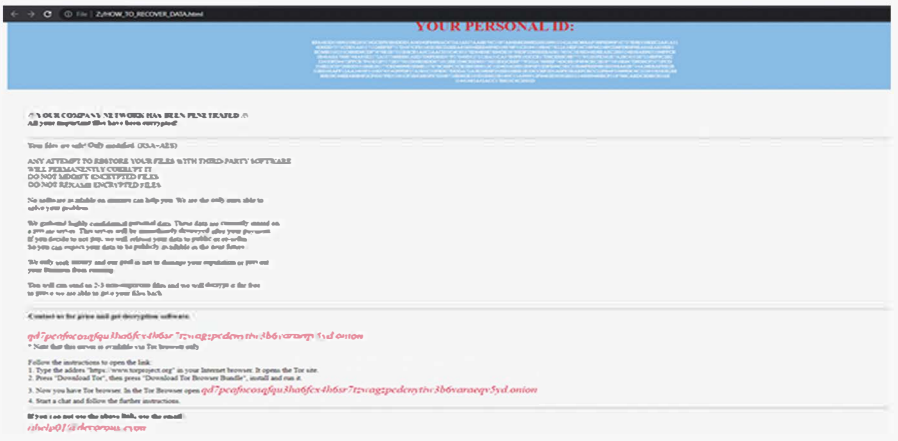


Figure 6 - Ransom note, it contains e-mail and .onion domains that is used to communicate the attacker.

Malware drops ransom note on every folder that contains encrypted files. Extension of the encrypted files differ on different variants.

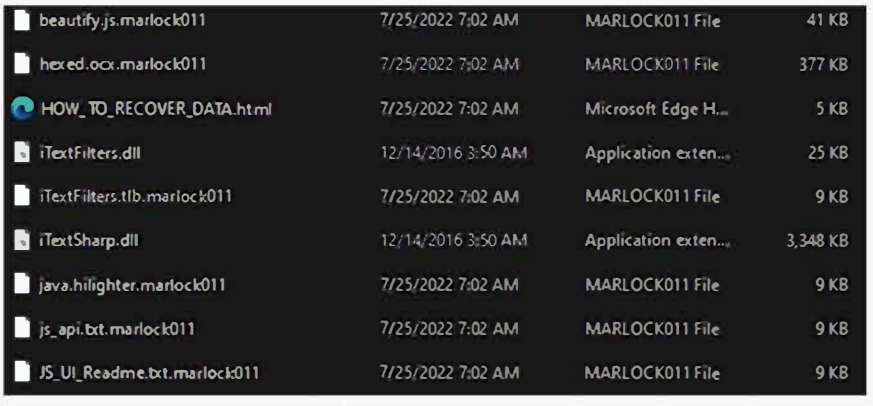


Figure 7 - Encrypted files and ransom note. In this variant extension for encrypted files is ".marlock011".

Threat actors mostly uses Phishing e-mails and poorly configured RDP(Remote Desktop Protocol) services to gain access.

MedusaLocker Ransomware

MedusaLocker Ransomware
MITRE ATT&CK Matrix

InterProbe

Execution

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1047	Windows Management Instrumentation	• Execution	Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. Learn more		• Contains references to WMI/WMIC ◦ 6250...0812 • Reads system information using Windows Management Instrumentation Commandline (WMIC) ◦ 6250...0812	
T1559.001	Component Object Model	• Execution	Adversaries may use the Windows Component Object Model (COM) for local code execution. Learn more	• 1 confidential indicators		

Privilege Escalation

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1055	Process Injection	• Privilege Escalation • Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more	• Writes data to a remote process ◦ 6250...0812		
T1548.002	Bypass User Account Control	• Privilege Escalation • Defense Evasion	Adversaries may bypass UAC mechanisms to elevate process privileges on system. Learn more		• References COM interfaces strings prone to UAC bypass ◦ 6250...0812	
T1055.012	Process Hollowing	• Privilege Escalation • Defense Evasion	Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Learn more	• Allocates virtual memory in a remote process ◦ 6250...0812		

Defense Evasion

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1055	Process Injection	• Privilege Escalation • Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more	• Writes data to a remote process ◦ 6250...0812		
T1548.002	Bypass User Account Control	• Privilege Escalation • Defense Evasion	Adversaries may bypass UAC mechanisms to elevate process privileges on system. Learn more		• References COM interfaces strings prone to UAC bypass ◦ 6250...0812	
T1055.012	Process Hollowing	• Privilege Escalation • Defense Evasion	Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Learn more	• Allocates virtual memory in a remote process ◦ 6250...0812		
T1027.002	Software Packing	• Defense Evasion	Adversaries may perform software packing or virtual machine software protection to conceal their code. Learn more			• Matched Compiler/Packer signature ◦ 6250...0812
T1112	Modify Registry	• Defense Evasion	Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Learn more	• Modifies the UAC/LUA settings (Account Control) ◦ 6250...0812		
T1497	Virtualization/Sandbox Evasion	• Defense Evasion • Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more		• Possibly tries to implement anti-virtualization techniques ◦ 6250...0812	
T1564.004	NTFS File Attributes	• Defense Evasion	Adversaries may use NTFS file attributes to hide their malicious data in order to evade detection. Learn more		• 1 confidential indicators	

MedusaLocker Ransomware

MedusaLocker Ransomware MITRE ATT&CK Matrix

InterProbe

Credential Access

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1056.004	Credential API Hooking	• Credential Access • Collection	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more		• Installs hooks/patches the running process ◦ 6250...0812	

Discovery

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1120	Peripheral Device Discovery	• Discovery	Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. Learn more			• Queries volume information ◦ 6250...0812
T1012	Query Registry	• Discovery	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. Learn more		• Reads information about supported languages ◦ 6250...0812 • 3 confidential indicators	
T1057	Process Discovery	• Discovery	Adversaries may attempt to get information about running processes on a system. Learn more		• Queries process information ◦ 6250...0812	• Observed Process32First/Process32Next/CreateToolhelp32Snapshot API string ◦ 6250...0812
T1082	System Information Discovery	• Discovery	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Learn more		• Reads the cryptographic machine GUID ◦ 6250...0812	• Contains ability to read software policies ◦ 6250...0812
T1083	File and Directory Discovery	• Discovery	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Learn more	• Tries to access unusual system drive letters ◦ 6250...0812		
T1497	Virtualization/Sandbox Evasion	• Defense Evasion • Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more		• Possibly tries to implement anti-virtualization techniques ◦ 6250...0812	

Collection

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1056.004	Credential API Hooking	• Credential Access • Collection	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more		• Installs hooks/patches the running process ◦ 6250...0812	
T1114	Email Collection	• Collection	Adversaries may target user email to collect sensitive information. Learn more		• Found a potential E-Mail address in binary/memory ◦ 6250...0812	

Impact

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1490	Inhibit System Recovery	• Impact	Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. Learn more	• Deletes volume snapshots (often used by ransomware) ◦ 6250...0812		

Recommendations and Mitigations

- Backup your valuable data. Make sure your backup isolated from your original system.
- Educate your employees against phishing and social engineering attacks.
- Configure Powershell policy to only execute signed scripts.
- Make sure your remote desktop services are not accessible from external network. In cases which you need access from external network use services like VPN.
- Use multi factor authentication.

Lilith Ransomware

Lilith Ransomware is discovered by a researcher named JAMESWT and made public around mid-July. Malware targets 64-bit Windows systems and developed in C/C++ language. It drops a ransom note to every folder enumerated while file encryption and adds .lilith extension to encrypted files.

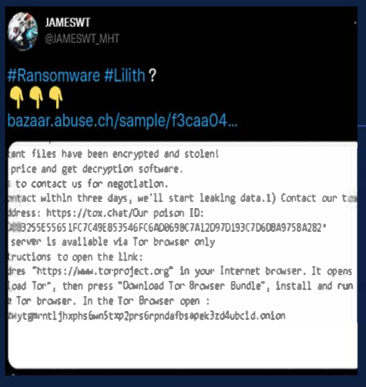


Figure 8 - Post that made Lilith Ransomware public | Source: https://twitter.com/JAMESWT_MHT/status/1544946534915219456

In ransom note, it says encrypted files are leaked before the encryption and will be publicly available via Tor if victim doesn't contact to threat actor in 3 days. Threat actor uses a messaging application named Tox Chat to communicate with victims. Ransom note also contains Tox Chat id to communicate with threat actor.

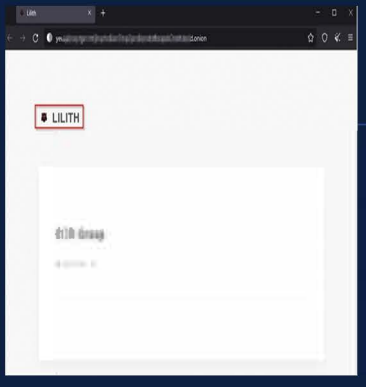


Figure 9 - Lilith Onion leak site |Source: https://blog.cyble.com/2022/07/12/new-ransomware-groups-on-the-rise/

Researchers at Cyble have obtained interesting findings about the malware. According to these findings, it is a possibility that Lilith Ransomware gotten some of its code with BABUK Ransomware. The ransomware enumerates and kills a list processes which could prevent ransomware from encrypting important data (Database applications as example).

Figure 10 - Lilith Ransomware exclusion list | Source: https://blog.cyble.com/2022/07/12/new-ransomware-groups-on-the-rise/

Ransomware seen while excluding files with .exe,.dll and .sys extensions. In addition to those files ransomware also contains an exclusion list, which is thought to be list of files that would break the system or ransomware itself if any of them is encrypted. Researchers at Cyble noticed that this exclusion list contains a file named "ecdh_pub_k.bin". This file is known as a part of BABUK Ransomware encryption module. This finding supports that Lilith ransomware gets some of its code from BABUK ransomware.

Lilith Ransomware

Lilith Ransomware
MITRE ATT&CK Matrix

InterProbe

Defense Evasion

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1497	Virtualization/Sandbox Evasion	• Defense Evasion • Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more	• The input sample contains a known anti-VM trick ◦ 62c3...3589		
T1027.002	Software Packing	• Defense Evasion	Adversaries may perform software packing or virtual machine software protection to conceal their code. Learn more		• 1 confidential indicators	
T1070.004	File Deletion	• Defense Evasion	Adversaries may delete files left behind by the actions of their intrusion activity. Learn more		• Opens file with deletion access rights ◦ 62c3...3589	

Discovery

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1012	Query Registry	• Discovery	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. Learn more		• Reads information about supported languages ◦ 62c3...3589 • Queries the display settings of system associated file extensions ◦ 62c3...3589 • 1 confidential indicators	
T1518.001	Security Software Discovery	• Discovery	Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment. Learn more		• Possibly checks for the presence of a forensics/monitoring tool ◦ 62c3...3589	
T1057	Process Discovery	• Discovery	Adversaries may attempt to get information about running processes on a system. Learn more		• Queries process information ◦ 62c3...3589	• Observed Process32First/Process32Next/CreateToolhelp32Snapshot API string ◦ 62c3...3589
T1497	Virtualization/Sandbox Evasion	• Defense Evasion • Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more	• The input sample contains a known anti-VM trick ◦ 62c3...3589		
T1120	Peripheral Device Discovery	• Discovery	Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. Learn more			• Queries volume information ◦ 62c3...3589
T1082	System Information Discovery	• Discovery	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Learn more		• Reads the cryptographic machine GUID ◦ 62c3...3589	

Collection

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1074.001	Local Data Staging	• Collection	Adversaries may stage collected data in a central location or directory on the local system prior to Exfiltration. Learn more			• Creates a writable file in a temporary directory ◦ 62c3...3589
T1114.001	Local Email Collection	• Collection	Adversaries may target user email on local systems to collect sensitive information. Learn more	• Reads mail related files ◦ 62c3...3589		

Recommendations and Mitigations

- Backup your valuable data. Make sure your backup isolated from your original system.
- Educate your employees against phishing and social engineering attacks.

References

- https://9to5mac.com/2022/07/20/cloudmensis/
- https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/
- https://www.binarydefense.com/threat_watch/cloudmensis-backdoors-mac-users-to-steal-credentials%ef%bf%bc/
- https://www.bleepingcomputer.com/news/security/new-android-malware-on-google-play-installed-3-million-times/
- https://lifehacker.com/delete-these-sneaky-malware-apps-from-your-android-asap-1849182983
- https://twitter.com/IngraoMaxime/status/1547164768401858560
- https://www.hybrid-analysis.com/sample/95547426cd892cc50547d65aef7edb82212c68a44257318cb89fbfcfa04889bb?environmentId=200
- https://redcanary.com/blog/chromeloader/
- https://www.pcrisk.com/removal-guides/23957-chromeloader-malware
- https://cyware.com/news/researchers-uncovered-new-variants-of-the-chromeloader-malware-f382ff70
- https://unit42.paloaltonetworks.com/chromeloader-malware/
- https://www.hybrid-analysis.com/sample/ded20df574b843aaa3c8e977c2040e1498ae17c12924a19868df5b12dee6dfdd
- https://www.hybrid-analysis.com/sample/dbac4f2fffcb4e09aad772895647e8f161b1ac713592fe47c5e8207c85722f13
- https://www.cisa.gov/uscert/ncas/alerts/aa22-181a
- https://id-ransomware.blogspot.com/2019/10/medusalocker-ransomware.html
- https://blog.cyble.com/2022/07/12/new-ransomware-groups-on-the-rise/
- https://twitter.com/JAMESWT_MHT/status/1544946534915219456
- https://www.hybrid-analysis.com/sample/f3caa040efb298878b99f883a898f76d92554e07a8958e90ff70e7ff3cfabdf5

INTER
PROBE
INTELLIGENCE & ANALYTICS

Mutlukent Mah. Fesleğen Sok. No:9 Çankaya Ankara Türkiye
Phone: +90 312 225 10 93, **Email:** info@interprobe.com.tr, **Web:** https://interprobe.com.tr