CRYXOS MALWARE

PHISHING, SCAM, TROJAN

Vairav Advisory Report

3rd May 2023

Vairav Technology Security Pvt. Ltd.

Phone: +977 014441540

Thirbam Sadak 148
Baluwatar, Kathmandu

Mobile: +977-9820105900

Email: mail@vairav.net

SUMMARY

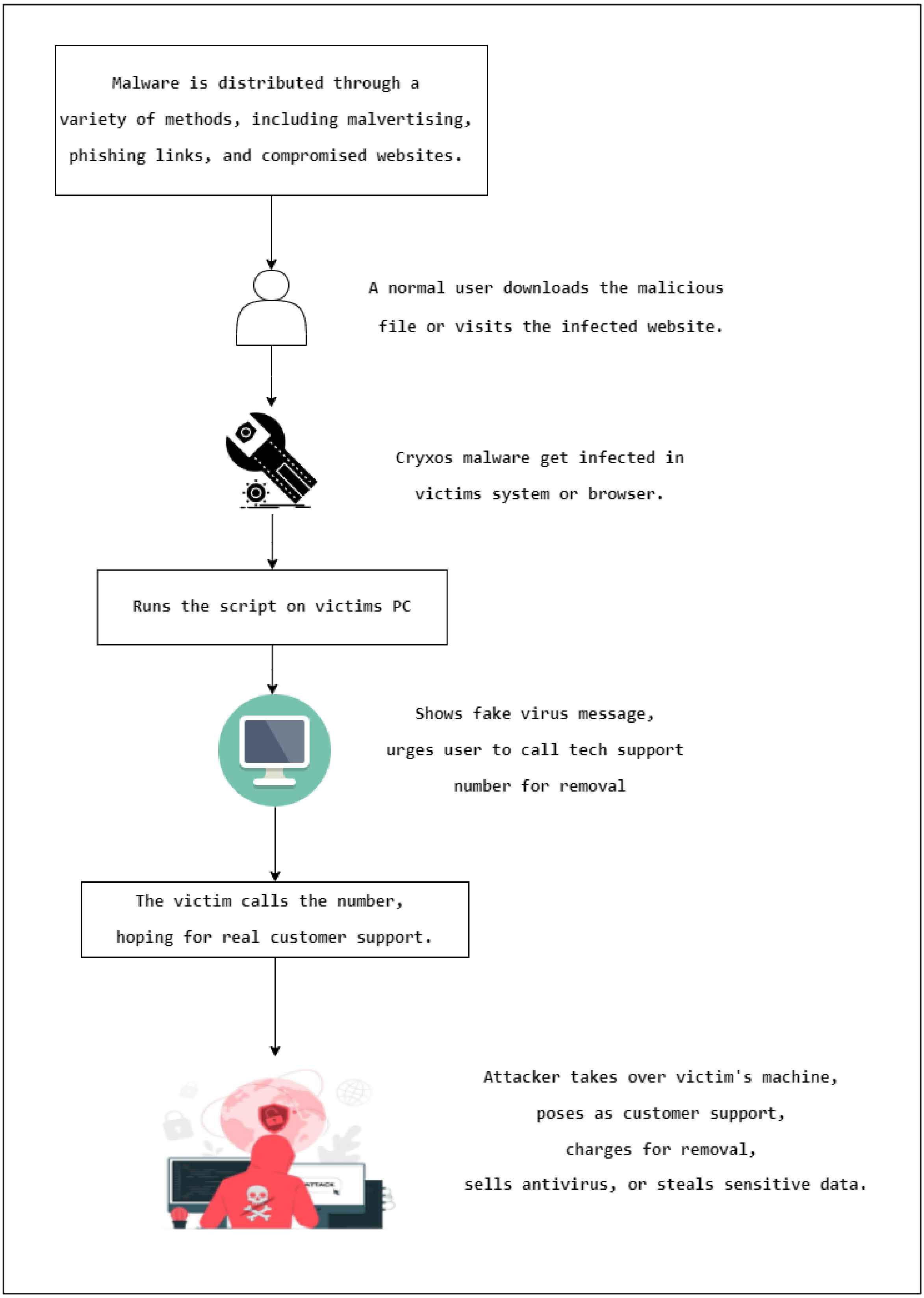
Cryxos Trojans are a form of Trojan software that causes users to see phony viruses or error notifications when they visit compromised or malicious websites. These websites may have been infected with a malicious JavaScript file, which causes the alert to be triggered. The alerts are frequently disguised as genuine Microsoft or Windows Operating System messages, saying that the user’s machine is infected with a virus and prompting them to call a specific number for technical help.

Introduction of Cyber Adversary

The fraudsters behind Cryxos Trojans intend to mislead users into believing that their computer has been compromised and that personal information, such as financial information, has been taken. In certain situations, the Trojan will even play an audio recording that repeats the alert's message. All of these alerts, however, are fake and should never be believed.

Cryxos Trojan scammers generally try to extort money from innocent visitors by urging them to utilize their online technical services or buy the software. They may request that consumers grant remote access to their computers, allowing the scammers complete control of the machine. This allows scammers to access personal information and data and infect the device with harmful software such as ransomware. As a result, it is critical to never believe these fake warnings and to take precautions to safeguard your computer and personal information from such assaults.

Tactics, Techniques, and Procedure



Malware is distributed through a variety of methods, including malvertising, phishing links, and compromised websites.

A normal user downloads the malicious file or visits the infected website.

Cryxos malware get infected in victims system or browser.

Runs the script on victims PC

Shows fake virus message, urges user to call tech support number for removal

The victim calls the number, hoping for real customer support.

Attacker takes over victim's machine, poses as customer support, charges for removal, sells antivirus, or steals sensitive data.

Figure 1: Attack phases of Cryxos Malware.

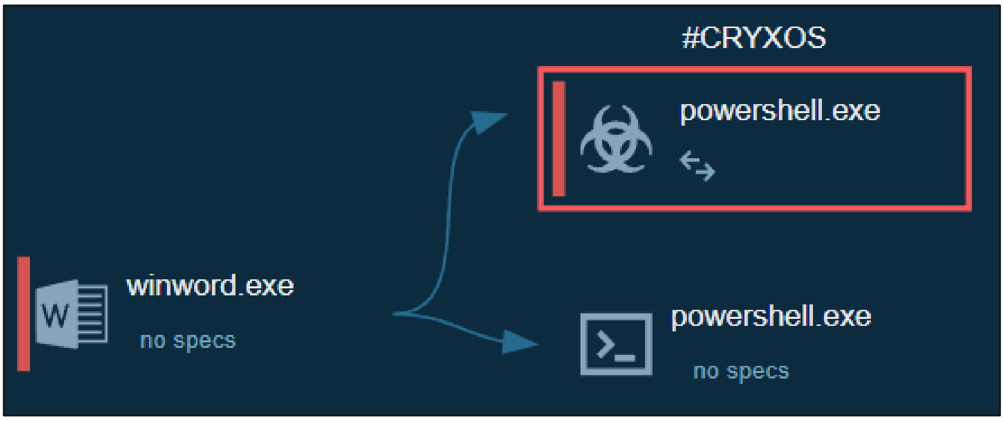
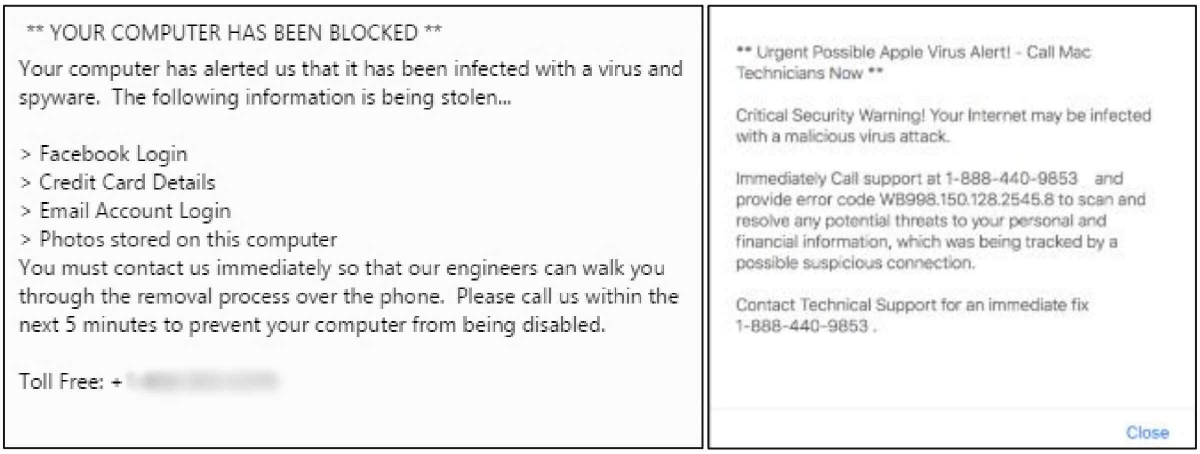


Figure 2: Process graph.

The user opens the file which he thinks is a legit file. But without the user's knowledge, it also executes the process in the background. The file opens PowerShell and downloads the Cryxos script from C2 or a website that was hosted by the attacker. The hacker develops harmful Cryxos code and distributes it via hijacked websites, often embedding it into supposedly genuine documents such as Microsoft Word documents or with the help of phishing emails. Cryxos Trojans are usually found when a user unintentionally views an unauthorized or hacked webpage that contains a malicious JavaScript file. When the script runs, it displays a notification message that appears to be a virus infection on the user's device; the user is advised to dial a given phone number for technical assistance in removing the infection.



** YOUR COMPUTER HAS BEEN BLOCKED **
Your computer has alerted us that it has been infected with a virus and spyware. The following information is being stolen...

> Facebook Login
> Credit Card Details
> Email Account Login
> Photos stored on this computer

You must contact us immediately so that our engineers can walk you through the removal process over the phone. Please call us within the next 5 minutes to prevent your computer from being disabled.

Toll Free: + [redacted]

** Urgent Possible Apple Virus Alert! - Call Mac Technicians Now **

Critical Security Warning! Your Internet may be infected with a malicious virus attack.

Immediately Call support at 1-888-440-9853   and provide error code WB998.150.128.2545.8 to scan and resolve any potential threats to your personal and financial information, which was being tracked by a possible suspicious connection.

Contact Technical Support for an immediate fix 1-888-440-9853 .

Figure 3: Message displayed on the Victim.

The screenshots shown above are only samples. There are dozens of versions of this deception, with the precise design and language varying. There are also millions of variations on the "toll-free" phone numbers they supply, which can easily originate on the other side of the world. These frauds are simple to produce and spread, and fresh instances surface every day. Some Cryxos variants will also play an audio recording that repeats the information displayed in the notification message and provides the phone number that the user should call for further assistance. In addition to the warning, certain Cryxos variations will reveal the user's IP address, open numerous web browser pages, or execute other alarming behaviors.

These scams may appear to be genuine because they often include information such as IP address and a recognizable browser icon. Voiceovers and irritating alarm noises are among them. Some of them may launch hundreds of tabs or windows. There may be no way to close the windows or dismiss the popups. You may be unable to operate the browser and may be unable to exit the program. Even if you shut down and restart your system, the irritating popups may continue to show. These Trojans are essentially part of a 'call help' or 'tech support' scam, aiming to deceive the consumer into thinking their device is infected. If the consumer does phone the number given, they are then often forced into paying for the help. In other situations, the user may be caused to allow the technician remote access to the system, which might result in device hijacking and the compromising of any data saved on the device.

MITRE ATT&CK techniques

The Cryxos malware makes the usage of various attack tactics, techniques, and procedures based on the MITRE ATT&CK framework to attack victimized users or organizations.

Tactic	Technique
Initial Access	Phishing (T1566) • Spear phishing Attachment (T1566.001)
Execution	Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • JavaScript (T1059.007)
	User Execution (T1204) • Malicious Link (T1204.001) • Malicious File (T1204.002)
Defense Evasion	Indicator Removal (T1070) • File Deletion (T1070.004)
	Modify Registry (T1112)
Credential Access	Input Capture (T1056) • Credential API Hooking (T1056.004)
Discovery	Application Window Discovery (T1010)
	Query Registry (T1012)
	System Information Discovery (T1082)
Collection	Input Capture (T1056) • Credential API Hooking (T1056.004)
	Email Collection (T1114)

Indicators of Compromise (IOCs)

IP Addresses

23[.]202[.]231[.]167

23[.]217[.]138[.]108

Hashes

F1CD8322FA2F0A04C9B04D2F5ADB6513

Domains

Hxxp://gokeenakte[.]top

hxxp://videoanalystes[.]webcam

More IOC can be found here

Threat Summary	
Name	Cryxos malware
Threat Type	Trojan
Detection Names	Arcabit (JS: Trojan.Cryxos.DB69), BitDefender (JS: Trojan. Cryxos.2921), Emsisoft (JS: Trojan. Cryxos.2921 (B)), Adwind (Adwind-FDYD.jar!80CB885577CE), The Full List Of Detections Names can be found here.
Symptoms	False error messages, fraudulent system alerts, pop-up errors, and fake computer scans.
Distribution methods	Hacked websites, deceptive online pop-up advertisements, and unwanted applications may pose a risk.
Damage	Exposure of confidential personal information, financial losses, identity theft, and potential infections from malicious software.
Malware Removal (Windows)	Scan your PC with authorized antivirus software to remove any potential malware infestations.

Vairav Recommendations

1. Avoid using third-party downloads

Always download software and files from reputable, official websites. Peer-to-peer networks, unauthorized websites, and third-party downloaders should not be used since they might result in the installation of malware or other undesirable software on your computer.

2. Implement robust email security

Organizations should implement email security measures such as spam filters, email gateways, and advanced threat protection to block malicious emails, including those containing malware.

2. Blocking unwanted extension files in emails

The organization should block receiving of unwanted file extensions to be delivered via email. Some suggested file extensions to block are .js, .exe, .com, .cmd, .scr, .ps1, .vbs, and .lnk. However, as threat actors discover new file extensions to abuse, this list may be bypassed by other malicious file types.

3. Educate employees about phishing and scam

Employees should be educated on identifying and avoiding phishing emails, which are often used to spread malware. This can include providing training on how to spot and report suspicious emails, as well as regularly testing employees with simulated phishing emails.

4. Implement multi-factor authentication

Organizations should implement multi-factor authentication for all remote access and sensitive systems to prevent attackers from stealing login credentials.

5. Keep software and operating systems up to date

Organizations should ensure that all software and operating systems are kept up to date with the latest security patches and updates. This is especially important for software that is commonly targeted by malware, such as web browsers and Office applications.

6. Use endpoint protection software

Organizations should use endpoint protection software to detect and remove malware from infected systems. This software should be kept up to date with the latest malware signatures and configured to conduct regular scans.

7. Regularly back up important data

Organizations should regularly back up important data and store it in a secure location, in case the data is lost or stolen due to a malware infection.

8. Monitor network traffic

Organizations should monitor network traffic for signs of malware and investigate any suspicious activity. This can include monitoring for data exfiltration and connections to known command and control servers.

9. Have an incident response plan

Organizations should have an incident response plan in place and ensure that all employees know how to respond in the event of a malware infection. This should include procedures for isolating infected systems and reporting the incident to the appropriate parties.

10. Perform Vulnerability Assessment and Penetration Testing

We recommend performing vulnerability assessment and penetration testing of the networks, server, and end-user zones. The host-based vulnerability assessment is a must.

It is important to remember that cyber adversaries are likely to constantly evolve their methods, tools, and techniques to evade detection and continue to be successful in their attacks. Therefore, organizations and individuals must stay informed about the latest TTPs and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4441540

Mobile: +977-9820105900

Email: mail@vairav.net

Website: https://vairav.net