KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New “IceXLoader” Variant Targets Thousands of Users Worldwide, Exfiltrates Data

Tracker ID: TN1117 **Date:** 17/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

Background

In an ongoing phishing campaign, thousands of personal and enterprise users have been infected by a new version of the IceXLoader malware (v3.3.3), that ultimately leaks the exfiltrated data. The malware loader's capabilities have been strengthened with the addition of a multi-stage delivery chain and improved functionality in this new version. In June 2022, IceXLoader v3.0, a Nim-based malware, came to light. However, the loader lacked certain essential features and appeared to be a work in progress. The most recent version of IceXLoader represents a significant divergence from the project's beta development phase. Any such development results in a surge in the use of the malware loader, which has been vigorously marketed in the criminal underground.

The initial infection begins when a phishing email delivers a ZIP file containing the first-stage extractor. The extractor drops the next-stage executable, "STOREM~2.exe," in a new hidden folder (.tmp) beneath "C:\Users\\AppData\Local\Temp." The infected system can then be rebooted, depending on the extract parameters selected by the operator. Also, a new registry key is inserted to delete the temporary folder when the system restarts. The dropped malware is a downloader that retrieves a PNG file from a hardcoded URL and converts it into the IceXLoader payload, an obfuscated DLL file. To avoid sandboxes, the dropper makes checks to ensure it is not running within an emulator and waits 35 seconds before launching the malware loader. Furthermore, utilizing process hollowing, IceXLoader is injected into the STOREM2.exe process.

After launching IceXLoader 3.3.3, it duplicates itself into two directories named after the operator's nickname before gathering and exfiltrating the following host information to the C2: IP address, UUID, username, and system name, Windows OS version, installed security products, presence of .NET Framework (v2.0 and/or v4.0), hardware information, and timestamp. To ensure persistence across reboots, the malware loader also generates a new registry key at "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run." It also uses an in-memory patching approach in AMSI.DLL to bypass the Microsoft Windows Antimalware Scan Interface, which is used by Windows Defender and other security products.

Furthermore, the loader creates and executes a ".bat" file that disables Windows Defender's real-time scan and adds exclusions to prevent Windows Defender from inspecting the directory where IceXLoader was copied. The loader supports the following commands: Stop the execution; gather system information and leak it to C2; display the selected message in a dialogue box; restart IceXLoader; submit a GET request to download a file, then use "cmd/ C" to open it; execute an executable from memory, then send a GET request for the executable. It also loads and runs the .NET assembly, modifies the C2 server beaconing interval, updates IceXLoader, and stops and deletes all disc copies.

The SQLite database holding the stolen data is available at the C2 location, demonstrating that the threat actors behind this campaign are unconcerned about ensuring the security of exfiltrated data. The leaked database contains information on thousands of victims, with infections from both personal and business systems.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New “IceXLoader” Variant Targets Thousands of Users Worldwide, Exfiltrates Data

Tracker ID: TN1117 **Date:** 17/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial Access, Execution, Defense Evasion, Collection, Exfiltration, Command and Control.

Indicators of Compromise

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Implement regular phishing awareness and training throughout the workplace. Make sure employees are aware of any active phishing threats.
- Verify the email sender and content before downloading attachments or selecting embedded links from emails. Hover the pointer above embedded links to show the link’s target.
- Check the sender’s identity. Unfamiliar email addresses, mismatched email and sender names, and spoofed company emails are some of the signs that the sender has malicious intent.
- Identify and remove any suspicious files in the hidden folder (.tmp) under “C:\Users\<username>\AppData\Local\Temp”.
- Remove unauthorized programs from the startup folder: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and perform a complete "Windows Defender" scan.
- Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New “IceXLoader” Variant Targets Thousands of Users Worldwide, Exfiltrates Data

Tracker ID: TN1117 **Date:** 17/Nov/2022 **Category:** Malware **Industry:** All **Region:** All

References

- Bill Toulas, Phishing drops IceXLoader malware on thousands of home, corporate devices, Bleeping Computer, 10th November 2022, External Link (www.bleepingcomputer.com).
- Ravie Lakshmanan, New IceXLoader Malware Loader Variant Infected Thousands of Victims Worldwide, The Hackers News, 9th November 2022, External Link (thehackernews.com).
- Natalie Zargarov, New updated IceXLoader claims thousands of victims around the world, Minerva, 8th November 2022, External Link (minerva-labs.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

*

SHA256 Hash	URL
49d6552ae5c5027ce1e68edee2438564b50ddc384276fd97360c92503771d3ac	hxxps://www[.]filifilm[.]com[.]br/images/colors/purple/Ejvffhop[.]png
7bb69f98d77ca7609c10b9a0ab1ce32be2e26b160413203d5335f65c1bc8ee72	
9a9981d9bd10d3e004457ca4509aeb2bd828f54213f61b8a547c90e52f0b08eb	
0911819d0e050ddc5884ea40b4b39a716a7ef8de0179d0dfded9f043546cede9	

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.