IcedID Malware

IcedID, loader, Trojan

Vairav Advisory Report

25th January 2023

Vairav Technology Security Pvt. Ltd.

Tribham Sadak
Baluwatar, Kathmandu

Phone: +977 014441540
Email: mail@vairav.net

SUMMARY

IcedID is a Trojan malware that started in 2017 as a modular banking Trojan but has since evolved into a malware dropper that is commonly used to gain initial access to corporate networks. It is used to steal sensitive information such as login credentials, credit card numbers, social security numbers, and bank account details. The malware is primarily spread through phishing emails. It is known for its high level of evasiveness and ability to evade detection by most anti-virus software. It can also be used as a downloader for other malware, which allows it to install additional malicious software onto the infected device. The IcedID malware poses a significant threat to personal and financial information as well as corporate networks.

Introduction of Cyber Adversary

The identity of the individuals responsible for the IcedID malware is unknown. However, a financially motivated threat group named TA551/Shathak has been linked to the use of IcedID in their attacks. This group is believed to have connections to Eastern European cybercrime groups and to collaborate with the creators and distributors of Emotet and TrickBot. They are a highly skilled cybercrime organization that targets both individuals and organizations worldwide. Over time, they have distributed various types of malware, but consistently utilize password-protected ZIP files with macro-enabled Office documents for delivery. Previously, they have employed malware such as Ursnif and Valak, but since the summer of 2020, they have been seen distributing IcedID.

Tactics, Techniques, and Procedure

In situations where different processes, such as gaining access, are not part of a continuous operation, the different phases of an incursion are assigned to various uncategorized UNC groups. "Access operations" specifically provide a means for remote access to a target environment, which can then be used by a separate party for further activities. An example of an access operation would be the placement of a backdoor to establish a foothold for another group to use.

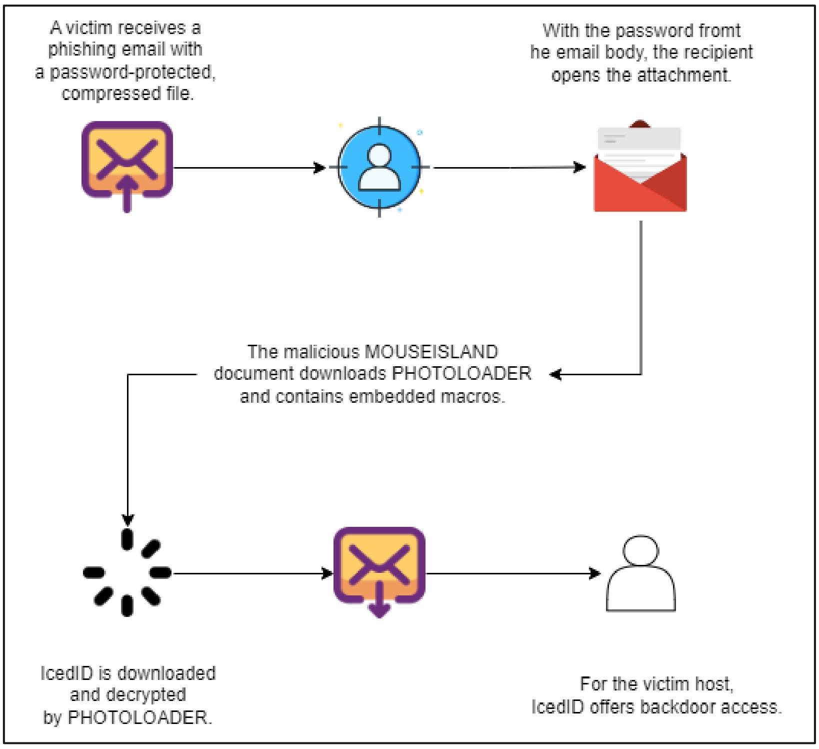
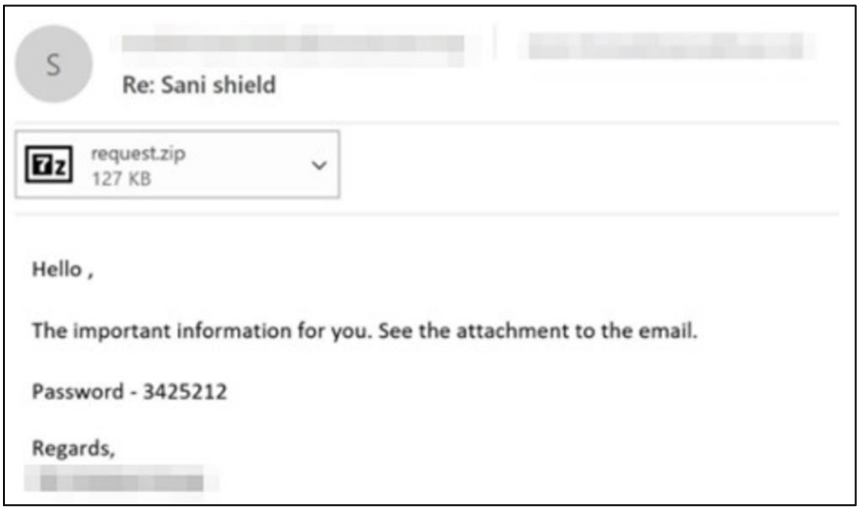

A victim receives a phishing email with a password-protected, compressed file.
With the password fromt he email body, the recipient opens the attachment.
The malicious MOUSEISLAND document downloads PHOTOLOADER and contains embedded macros.
IcedID is downloaded and decrypted by PHOTOLOADER.
For the victim host, IcedID offers backdoor access.

Figure 1: Example of an Infection Chain from UNC2420 MOUSEISLAND to IcedID.

Between July and December 2020, a phishing campaign utilizing the IcedID malware was observed. This infection chain involved multiple stages and techniques, such as MOUSEISLAND and PHOTOLOADER, which were used to initially compromise the target systems. Later versions of the malware were also discovered, which employed additional techniques such as GZIPLOADER and the use of Contact Forms embedded in websites to propagate the infection.

MOUSEISLAND is a malware that is distributed as a Microsoft Word macro inside a password-protected zip file attached to phishing emails, it acts as the first stage of infection. PHOTOLOADER, which serves as an intermediary downloader to install IcedID, is the secondary payload delivered by MOUSEISLAND, as seen in our intrusion data when responding to IcedID-related incidents. The distribution of MOUSEISLAND and PHOTOLOADER as well as other payloads are attributed to UNC2420, a threat cluster created by the Mandiant Threat Pursuit team. This group also known as "Shathak" or "TA551" shares similar activity with UNC2420.



[redacted] [redacted]

Re: Sani shield

request.zip
127 KB

Hello ,

The important information for you. See the attachment to the email.

Password - 3425212

Regards,
[redacted]

Figure 2: UNC2420 MOUSEISLAND Phishing Email.

Once a phishing attack using IcedID is successful, the malware will begin to carry out its intended actions, such as stealing user credentials, establishing a foothold within the infected system, or even installing ransomware. In addition to its primary method of distribution through malspam, IcedID is also commonly spread as a secondary payload from other types of malware, most notably Emotet.

To evade detection by antivirus and other malware detection technologies, IcedID employs techniques such as injecting itself into the operating system's memory and disguising itself as a legitimate process. This allows the malware to operate without being detected by traditional security solutions. Additionally, the malware is known to be updated by its authors to enhance its persistence on an infected system and to evade new detection methods that may have been developed.

MITRE ATT&CK techniques

The IcedID 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) • Visual Basic (T1059.005)
	Native API (T1106)
	Scheduled Task/Job (T1053) • Scheduled Task (T1053.005)
	User Execution (T1204) • Malicious File (T1204.002)
	Windows Management Instrumentation (T1047)
Persistence	Boot or Logon Auto start Execution (T1547) • Registry Run Keys/ Startup Folder (T1547.001)
	Scheduled Task/ Job (T1053) • Scheduled Task (T1053.005)
Privilege Escalation	Boot or Logon Auto start Execution (T1547) • Registry Run Keys/ Startup Folder (T1547.001)
	Process Injection (T1055) • Asynchronous Procedure Call (T1055.004)
	Scheduled Task/ Job (T1053) • Scheduled Task (T1053.005)
Defense Evasion	Obfuscated Files or Information (T1027) • Software Packing (T1027.002) • Steganography (T1027.003)
	Process Injection (T1055)

	- Asynchronous Procedure Call (T1055.004)
	System Binary Proxy Execution (T1218) - Msiexec (T1218.007)
Discovery	Account Discovery (T1087) - Domain Account (T1087.002)
	Permission Groups Discovery (T1069)
	System Information Discovery (T1082)
Collection	Browser Session Hijacking (T1185)
Command and Control	Application Layer Protocol (T1071) - Web Protocols (T1071.001)
	Encrypted Channel (T1573) - Asymmetric Cryptography (T1573.002)
	Ingress Tool Transfer (T1105)

Indicators of Compromise (IOCs)

IP Addresses

207[.]154.202.192

138[.]197.195.62

209[.]97.134.125

104[.]248.153.44

159[.]89.43.72

159[.]223.109.133

134[.]209.170.133

94[.]140.114.143

134[.]209.107.62

137[.]184.94.136

94[.]140.114.184

164[.]92.104.194

103[.]208.86.7

5[.]181.80.214

23[.]202.231.167

23[.]202.231.167

204[.]11.56.48

164[.]90.204.224

68[.]183.184.0

162[.]33.179.149

Hashes

00DFA5FFCC6C024A8C0C8F00A9CF388EAD0DD47617DC341DD4DF5874B68BD54E

B41F6BC6C4C05806D1B9E79DD7B361D425902A9C3A3EA92B9DED8B0B0A76F3AF

3DE8568BC332A346E9A87F9F360C4B1942BA48C2C5ED655E8A2A608FA67D498D

B1EF43379C1AF0ED2BBC2DD710DF65A550B3B80CCE1B734438E20C64F1D5A42E

BD67E49C2CA15156C54956655928723063ECA5B4D90AE22DD6CE1029BA596B35

EE9FD78107CDCAFFC274CF2484D6C74C56C7F3BE39B1896894D9525506118D1E

8D5D36C8FFB0A9C81B145AA40C1FF3475702FB0B5F9E08E0577BDC405087E635

B53F3C0CD32D7F20849850768DA6431E5F876B7BFA61DB0AA0700B02873393FA

F1F61B0E96C172A24FBA71806829C486B43E141493C78EC4BB895DE760134316

405F03534BE8B45185695F68DEB47D4DAF04DCD6DF9D351CA6831D3721B1EFC4

FB188C80159174B092BC8CA3B0721B3550AD5943A999F79FD904E2DAC19D9C07

1FF6AEFC4E45ECE0E3CC73E02D3DD463BB4FE1D2101B1B1AF0FBFB97318264F9

B6B4A5060B407AEE5D4724EFACA8F8336F74989CBD590BB175479D8BB08D3126

893222B345DEB0D1AD76134D5772079681CB174F91B20CC8F6A78A148DE8706F

B3063A902D1ACC5BDAFB98A7976974EA2430B8D62D8AEB414CC3F2FAB190DAFA

8992CB202C810F333F41F55EAC418B2924C5FAB57C883721E9FBE1AB8E06233F

943AA6D0267127142CD9D191C32B138559D67DF2B9A352EACD4B86620336AC2E

30F099660904079AFCD445409CFD2ECA735FAB49DDA522F03ED60D47F9F21BDC

54BC124278E28E06CC75DFA8BD9EF0666D9933F555122102AAFB244C83D4C3C1

31248B5640E4C711934B88FBDB774545469256F08156EA098C2AD5F037AD1DA2

Domains

www[.]myhoneybakeefeedback[.]com

www[.]safety2venture[.]us

www[.]globalunionmortgage[.]com

www[.]bimcellerviss[.]com

cyberchef[.]io

genbicta[.]com

os2[.]fun-media-player[.]com

os[.]fun-media-player[.]com

mycampusjuice[.]com

c11n4[.]i.teaserguide[.]com

down[.]ezoneclick[.]com

www[.]sciencepub123[.]com

proxyfreaks[.]com

89gospel[.]com

decryptor[.]top

heartsongroup[.]com

ypf-serviclub[.]shop

servi22[.]store

viewsdocs[.]com

msupdater[.]com

Recent IOC can be found here: [IOC of IcedID]

Threat Summary	
Name	IcedID
Threat Type	Trojan
Detection Names	Trojan, IcedID, Loader
Symptoms	If names like "lchej" and "ydmfipkzqfsb" is found in the C:\Users\admin\AppData\Local\ directory and files with names like "pczapabclgpba", "mtkdonmlmxelaa", "ozwzefgpkzmzba", and "zcnejolyretaa", we can be sure that IcedID is present on the system.
Additional Information	It's important to keep in mind that IcedID may not be the only malware present in an infected system. It can work in conjunction with other malicious samples and can be downloaded by notorious Trojans such as Emotet or TrickBot.
Distribution methods	Spear-phishing techniques
Damage	Steal sensitive information, data loss, downtime, and financial loss.
Malware Removal (Windows)	Use reputable antivirus software to run a full system scan and remove all detected IcedID-related files and objects.

Vairav Recommendation

We recommend the following to mitigate and prevent ransomware attacks:

1. **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 IcedID malware.

2. **Educate employees about phishing**

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

3. **Implement multi-factor authentication**

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

4. **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.

5. **Use endpoint protection software**

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

6. 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.

7. Monitor network traffic

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

8. 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.

9. 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.

10. Have a Threat Intelligence

Threat intelligence keeps organizations apprised about active and emerging threats in the wild, to help recognize them and fend them off (or remediate them)

It is important to remember that the cyber adversaries behind IcedID 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 of IcedID and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Tribham Sadak, Baluwatar
Kathmandu, Nepal
Phone: +977-01-4441540
Email: mail@vairav.net
Website: https://vairav.net