Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

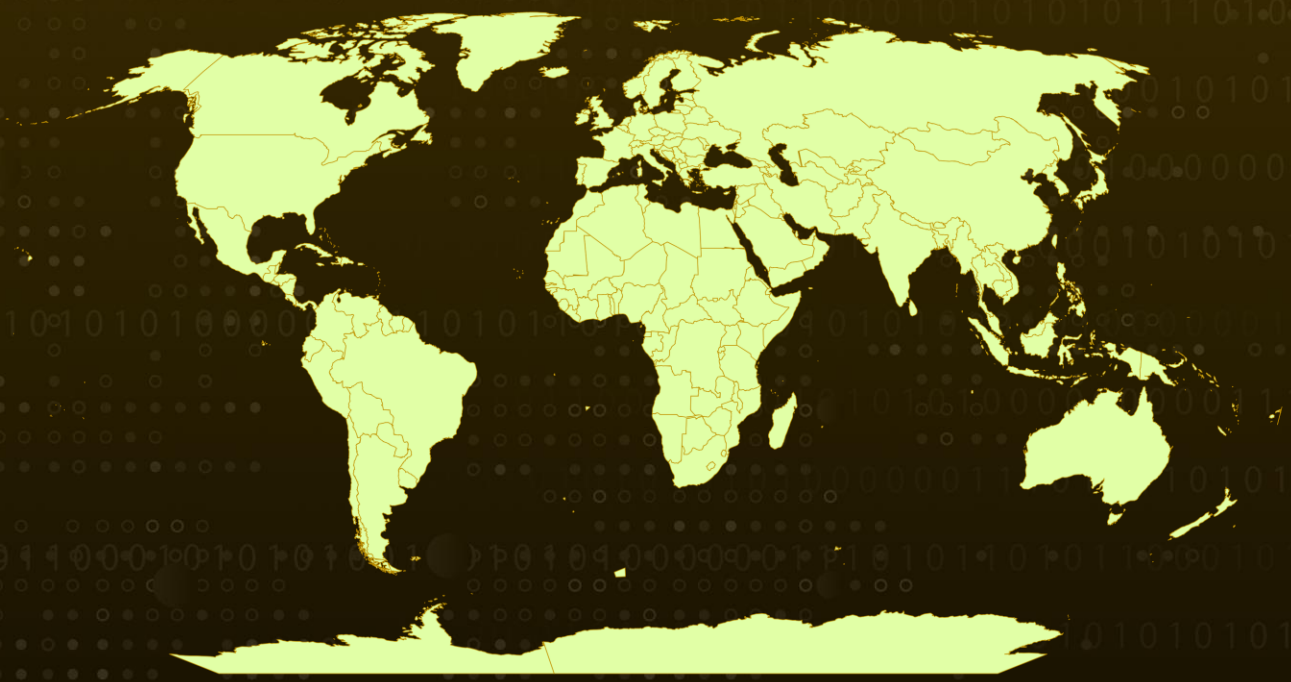
CustomerLoader Disseminating Diverse Malware Payloads

Date of Publication	Admiralty Code	TA Number
July 14, 2023	A1	TA2023300

Summary

First appeared: June 2023
Malware: CustomerLoader
Attack Region: Worldwide
Attack: A covert .NET loader, known as CustomerLoader, was specifically designed to facilitate the retrieval, deciphering, and activation of subsequent payloads. Throughout the early days of June 2023, various malicious entities actively disseminated this novel loader.

Attack Regions



Attack Details

#1 During the initial days of June 2023, multiple malicious actors extensively propagated the innovative .NET CustomerLoader through various mediums, including malicious phishing emails, deceptive YouTube videos, and counterfeit web pages that mimic legitimate websites.

#2 The CustomerLoader effortlessly retrieves dotRunpeX samples, which function as carriers for a diverse range of malware families, encompassing infostealers, Remote Access Trojans (RATs), and commodity ransomware. To conceal its strings, CustomerLoader employs AES encryption in Electronic CodeBook (ECB) mode, while storing the decryption key in plaintext within the PE file.

#3 In a bid to evade detection, CustomerLoader adroitly modifies the AmsiScanBuffer function in amsi.dll, skillfully manipulating it to return AMSI_RESULT_CLEAN, thus circumventing antivirus systems. This manipulation effectively designates the buffer as clean and grants unrestricted execution privileges to the malevolent payloads.

#4 When it comes to executing subsequent stages of the attack in memory, CustomerLoader employs a technique known as reflecting code loading. This method entails injecting and subsequently executing the downloaded payload within the same process, ensuring a covert and seamless operation.

Recommendations

- Strengthen email security measures and user awareness to combat malicious phishing campaigns, a primary channel for distributing the .NET CustomerLoader, to minimize the risk of successful attacks.
- Enhance detection capabilities by updating antivirus systems to detect and block the obfuscated strings and modified AmsiScanBuffer function used by CustomerLoader, thus preventing its execution and the subsequent delivery of malicious payloads.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0005** Defense Evasion	**TA0011** Command and Control	**T1129** Shared Modules
T1027 Obfuscated Files or Information	**T1027.007** Dynamic API Resolution	**T1132** Data Encoding	**T1132.001** Standard Encoding
T1140 Deobfuscate/Decode Files or Information	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools	**T1620** Reflective Code Loading
T1001 Data Obfuscation	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	**T1105** Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp://smartmaster.com[.]my/48E003A01/48E003A01.7z, hxxp://5.42.94[.]169/customer/735, hxxps://telegra[.]ph/Full-Version-06-03-2, hxxps://tinyurl[.]com/bdz2uchr, hxxps://www.mediafire[.]com/file/nnamjnckj7h80xz/v2.4_2023.rar/file, hxxps://www.mediafire[.]com/file/lgoql94feiic0x7/v2.5_2023.rar/file, hxxp://5.42.94[.]169/customer/770, hxxps://slackmessenger[.]site/, hxxps://slackmessenger[.]pw/slack.zip, hxxp://5.42.94[.]169/customer/798
SHA256	d40af29bbc4ff1ea1827871711e5bfa3470d59723dd8ea29d2b19f5239e509e9, 3fb66e93d12abd992e94244ac7464474d0ff9156811a76a29a76dec0aa910f82, 65e3b326ace2ec3121f17da6f94291fdaf13fa3900dc8d997fbbf05365dd518f, 7ff5a77d6f6b5f1801277d941047757fa6fec7070d7d4a8813173476e9965ffc, c05c7ec4570bfc44e87f6e6efc83643b47a378bb088c53da4c5ecf7b93194dc6,

TYPE	VALUE
SHA256	695f138dd517ded4dd6fcd57761902a5bcc9dd1da53482e94d70ceb720092ae6, b8f5519f7d66e7940e92f49c9f5f0cac0ae12cc9c9072c5308475bd5d093cdca
IPV4	45.9.74[.]99, 5.42.65[.]69
C2	missunno[.]com:80

References

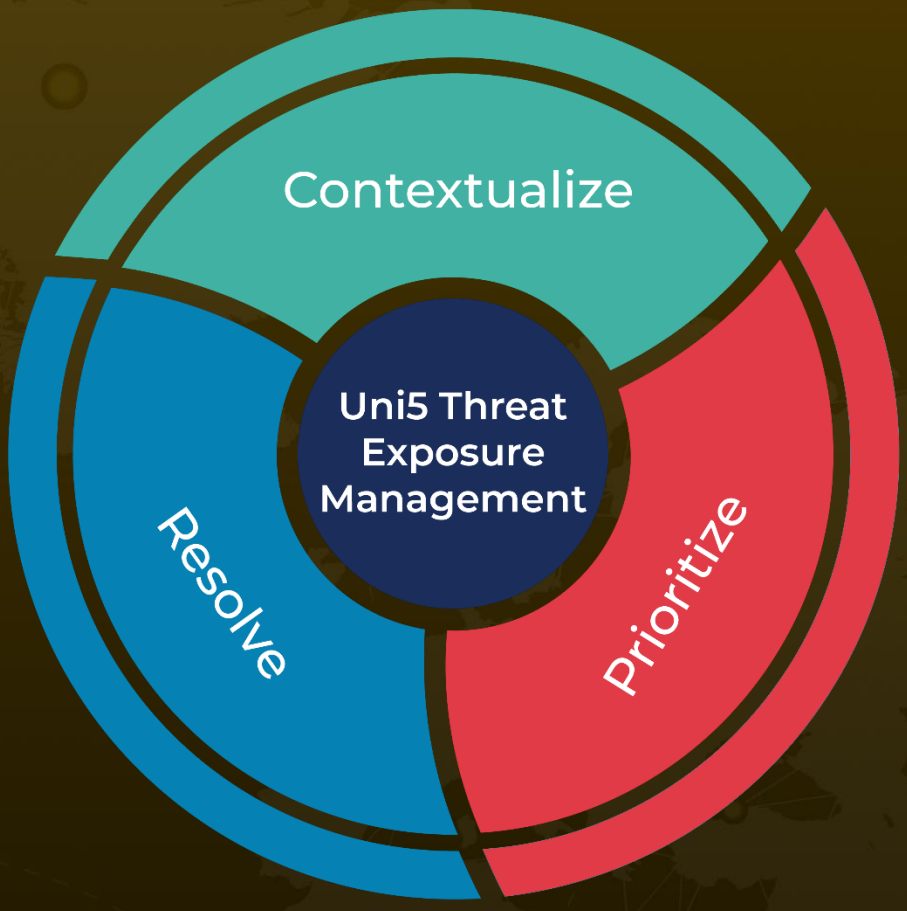
https://blog.sekoia.io/customerloader-a-new-malware-distributing-a-wide-variety-of-payloads/#h-c2-servers

https://www.hivepro.com/dotrunpex-novel-injector-delivers-multiple-malware-strains/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 14, 2023 • 6:30 AM

More at www.hivepro.com