Quorum Cyber

Threat Intelligence MetaStealer Stealware

TLP Status: CLEAR

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control 3

Revision History 3

Related Documents 3

MetaStealer 4

Overview 4

Impact 4

MetaStealer Upgrades 4

Vulnerability Detection 5

Affected Products 5

Containment, Mitigations & Remediations 5

Indicators of Compromise 6

Threat Landscape 6

Threat Group 7

Mitre Methodologies 7

Further Information 8

Document Control

Revision History

Version	Date	Summary of Changes
0.1	20/02/2023	Initial Report
0.2	20/04/2023	IOC Update
0.3	12/06/2023	Report Update
1.0	12/06/2023	PDF Formatting

Related Documents

The following documents are either referenced within, or are related to the content of this document:

Document Name	Date	Version
-	-	-

MetaStealer

Overview

MetaStealer is an information stealer variant of malware that was initially detected to have emerged on underground marketplaces and later involved in malspam campaigns[1]. The MetaStealer malware has been advertised as an upgrade of the RedLine Stealer variant[2]. MetaStealer can be obtained on a subscription basis for $125 USD per month, or alternatively, for $1,000 USD, as a lifetime subscription. This subscription model enables threat actors, that lack their own infrastructure and self-made capabilities, to engage in credential stealing activities. The relatively affordable malware option is almost certainly an attractive tool for criminal groups of all sizes and ranks MetaStealer as a highly prevalent malware that is emerging across the online domain.

The first stage of the attack chain involves the distribution of MetaStealer via malicious emails, being masqueraded as messages pertaining to financial transactions. These emails are sent attached with an excel document, containing a VBS macro. Following the acceptance of the document by the target, the malware will be downloaded and executed[3]. Following a system reboot, the file will progress to communicate with a command-and-control (C2) server, thus establishing a persistence mechanism[4].

Relevant security research has documented that the MetaStealer malware is associated with various infection techniques and behavioural trends, including Reliance on open-source libraries, Microsoft Defender Bypass, Scheduled Task Persistence, Password stealing, Keylogger activity and Hidden VNC server activity[5].

As with other information stealer variants, MetaStealer is designed to steal sensitive data, such as: login credentials, credit card details and security codes[6].

Impact

Information stealers, such as MetaStealer, are designed to stealthily infiltrate the target system and thus no symptoms are clearly visible on an infected machine, resulting in potential stolen passwords and banking information, identity theft and monetary loss. The compromise of sensitive company and customer credentials by a threat actor can lead to serious implications to the security posture and integrity of company systems, employees, and customers. If compromised credentials remain unactioned, there is a realistic possibility that they will be sold to a range of opportunistic threat actors and will subsequently be used to increase the effectiveness of further targeting. If employees have poor password hygiene in using the same password across multiple sites, a leak of one set of credentials could have a major knock-on effect to a wide array of systems and potentially lead to further compromise.

MetaStealer Upgrades

With regards to being an upgrade to the previous RedLine stealer variant, the threat actor claimed that, although MetaStealer had the same functionality as the former, it was released with several improvements, including:

[1] InfoSec Handlers Diary Blog - SANS Internet Storm Center
[2] Detect META Information Stealer - SOC Prime
[3] MetaStealer Malware Takes Center Stage in Recent Campaigns | Blog (safeguardcyber.com)
[4] Detect META Information Stealer - SOC Prime
[5] Metastealer – filling the Racoon void | NCC Group Research Blog | Making the world safer and more secure
[6] MetaStealer Malware - Malware removal instructions (updated) (pcrisk.com)

1) Removed unnecessary functionality from the panel

2) Added setting for collecting extensions from the browser

3) Added the Reset default settings button, which allows you to return the default settings of the panel if you suddenly need it

4) Cleaned stub

5) Changed the color scheme of the panel

6) Removed AntiCNG

7) Added the ability to view the private key for the generator (needed for auto-build in your bots for the team), to view it, you must re-enter the password from the panel (2FA, not to steal the key)

8) The weight of the build is reduced to 88KB, thanks to the new stub

9) Cleaned build runtime

Vulnerability Detection

A comprehensive Endpoint Detection and Response (EDR) solution, such as Microsoft Defender, can provide effective protection against malware threats, such as MetaStealer. EDRs can alert system users of potential breaches and stop the malware process during early signs of an attack attempt, therefore limiting the scope of damage.

Affected Products

- Windows Operating System

Containment, Mitigations & Remediations

It is recommended that upon the detection of compromised credentials, customers act in a prompt manner and issue password changes to affected users. Additionally, if password changes cannot be implemented or the account is no longer in active use, it is recommended that the account is added to the 'deny list' so that it cannot be targeted in further attack campaigns. Moreover, the enforcement of the multi-factor authentication (MFA) requirement is strongly recommended, as this can prevent adverse system access, even when a credentials have been compromised.

Threat intelligence has also detected a lack of strong password security and the use of basic, easy to crack passwords by several industry sector employees, an example being that of, 'password1'. It is strongly recommended that customers follow the National Cyber Security Centre (NCSC) guidance[7] of having passwords composed of three unrelated words and the incorporation of uppercase, lowercase, and symbol characters.

Additionally, the use of an effective and monitored Endpoint Detection and Response (EDR) solution is advised. An effective EDR will increase the detection of malicious attempts of executable stealware files on a system, thus alerting the user to potential credential leaks.

[7] Three random words - NCSC.GOV.UK

Finally, it is strongly recommended that employees receive training on how to detect markers of phishing emails and potentially malicious websites, as this is the main method of initial access for MetaStealer. Regular in-house training will prove to be effective in reducing the potency of future MetaStealer campaigns.

Indicators of Compromise

MetaStealer Associated URL:

- https[://]fled[.]store/install[.]msi

Associated MetaStealer File Hashes (SHA-265):

- aa3ef811cfeacbe782715219b91eb5f798780b6e81a3dd31eb4c2a8851689b54
- 76c73380cc4deb30cbfbe8a7fd551da5aba1150505fb5b0b66599e4ba491848b
- 4201978c9a5c160a6092fd51aa7391adf86c8e9c1baa39745f5f2116bc1e9423
- 725c26f1ce66cb2dbf4e6ac8bc28107d0b8cefe6cfaf6c4fb8b344e4146203eb
- 9cdd1ff2fd5e75f71bf55170e2232f912db81d2803383b465b378446aad94eb9
- 5ec516966f34ccbb02bc0697b907b3feaee4ffae4637015fccef69e8f1ed3775
- 936da1ec5f873d3ffb9cfa1c03f1e30dcbdeb76edce626f9a005909cd3af9fca
- 9c00c6a2739829cb91b37d09623b3c8a89d9e69ac3c3dd7110c82b5637687729
- c5c8b86f81e8cca5b874229d8a05f6eb75c582fd1517bfb209c29571358261d8
- d8e3114c2bcd2c32905a16e178ce1c84fdd871742f763c9c53426f58a9c01db0
- e09552719fe6094f5d5ef4dc58df848f7c01a56cfff2818302e75244390e732a
- 0e2b91976c40a13b22d0b1b90ec01c92dd62255f7d05537792b8b872b921d9c7
- 0f337100b6cae4bd8a6a1119e211a037a73624c9cc1f1107f7cb1afa1f8e34b3
- 12abe688f77652d244010c851fe20df5c7c44e3bf5f09909e7eae41d44394d1e
- 2a73cd2b05eb64e6c6e40459ad4ef657f77c67797a6b2e1ab7079cf6c6e8c9e8
- 2cbe4ef6b3bd140f2f587bc965606cc7beb4e006215f141829b96caee3c7b5fb
- 44f0803d062db5a20a04100703ae22cd0d5ac0c8061e026d4f0d0678cb4eda4b
- 6c3529b9bc1132ce261a16c157f38b2e7e1f5b602c1987b3611c61a7b12c5615
- 6e648bf88fefe0a4e98036c71d9bc24a3eb8c538d3bd9379312e092f4400616b
- 77359a68855e3745cc63b992197b13f42d16f25218131f6d8d61074afb12989e

Threat Landscape

Typical motives for the implementation of information stealer malware, such as MetaStealer include the generation of financial income for the associated cyber threat actors. It is common for such malware variants to operate in the background of a target system to avoid detection.

In recent years, information stealing malware, such as MetaStealer, have become prevalent infection vectors. More specifically, MetaStealer is a 'Commodity' information stealer and as such, data harvested by these malware variants are often sold within the illicit marketplace, whereby threat actors have the opportunity to purchase them[8]. The acquisition of the credentials by threat actors will ultimately lead to further targeting, inevitably resulting in the implementation of additional attack vectors, such as ransomware.

[8] The Next Generation of Info Stealers • KELA Cyber Threat Intelligence

Information stealers, such as MetaStealer, will remain undetected within the target landscape, and as such, they possess the ability to execute covertly, without their presence being detected. While MetaStealer currently spreads through malicious emails, its distribution could navigate towards alternative means, due to the availability to purchase the information stealer online[9].

Threat Group

The threat actor, '_META_', was responsible for releasing the MetaStealer malware on March 7th, 2022[10].

Mitre Methodologies

Initial Access
T1566.001 - Phishing: Spearphishing Attachment[11]

Execution
T1053 - Scheduled Task/Job[12]
T1059.005 - Visual Basic[13]

Persistence
T1078 - Valid Accounts[14]
T1543.003 - Create or Modify System Process: Windows Service[15]
T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder[16]

Privilege Escalation
T1574.002 - Hijack Execution Flow: DLL Side-Loading

Defence Evasion
T1027 - Obfuscated Files or Information[17]
T1027.002 - Obfuscated Files or Information: Software Packing[18]
T1027.004 - Obfuscated Files or Information: Compile After Delivery[19]
T1562.001 - Impair Defences: Disable or Modify Tools[20]

Credential Access
T1555.003 - Credentials from Password Stores: Credentials from Web Browsers[21]

Collection
T1005 - Data from Local System[22]

[9] MetaStealer Malware Takes Center Stage in Recent Campaigns | Blog (safeguardcyber.com)
[10] MetaStealer (Malware Family) (fraunhofer.de)
[11] Phishing: Spearphishing Attachment, Sub-technique T1566.001 - Enterprise | MITRE ATT&CK®
[12] Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®
[13] Command and Scripting Interpreter: Visual Basic, Sub-technique T1059.005 - Enterprise | MITRE ATT&CK®
[14] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®
[15] Create or Modify System Process: Windows Service, Sub-technique T1543.003 - Enterprise | MITRE ATT&CK®
[16] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[17] Obfuscated Files or Information, Technique T1027 - Enterprise | MITRE ATT&CK®
[18] Obfuscated Files or Information: Software Packing, Sub-technique T1027.002 - Enterprise | MITRE ATT&CK®
[19] Obfuscated Files or Information: Compile After Delivery, Sub-technique T1027.004 - Enterprise | MITRE ATT&CK®
[20] Impair Defenses: Disable or Modify Tools, Sub-technique T1562.001 - Enterprise | MITRE ATT&CK®
[21] Credentials from Password Stores: Credentials from Web Browsers, Sub-technique T1555.003 - Enterprise | MITRE ATT&CK®
[22] Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®

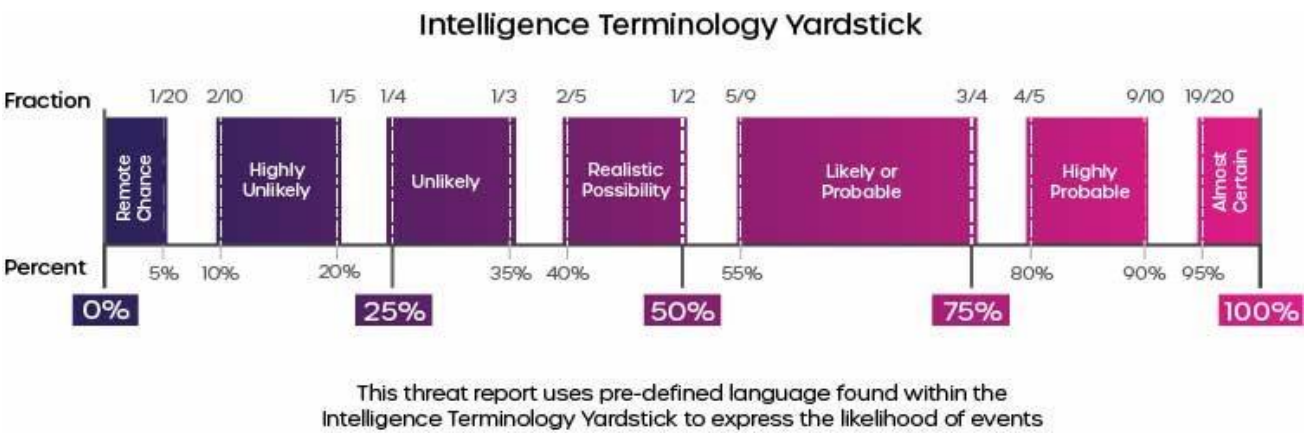
Command and Control
T1071.001 - Application Layer Protocol: Web Protocols[23]
T1105 - Ingress Tool Transfer[24]

Impact
T1496 - Resource Hijacking[25]

Further Information

- Fortiguard Threat Profile
- SANS Malware Analysis

Intelligence Cut-off Date (ICoD): 12/06/2023 10:00 UTC



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events

[23] Application Layer Protocol: Web Protocols, Sub-technique T1071.001 - Enterprise | MITRE ATT&CK®
[24] Ingress Tool Transfer, Technique T1105 - Enterprise | MITRE ATT&CK®
[25] Resource Hijacking, Technique T1496 - Enterprise | MITRE ATT&CK®