Quorum Cyber

Threat Intelligence Raccoon Stealer Stealware

TLP Status: White

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

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version	Date	Summary of Changes
1.0	17/11/2023	Initial Report
1.1	20/02/2023	Report Update
1.2	13/04/2023	Final PDF Formatting
1.3	28/04/2023	Report Update
1.4	10/05/2023	IOC Update

Related Documents

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

Document Name	Date	Version
-	-	-

Raccoon Stealer Threat

Overview

Raccoon Stealer (Raccoon) was first reported back in 2019 and has remained active to the current day with two variants, namely Raccoon and Racoon 2.0. The malware employs similar attack vectors as other stealware variants, including credential stealing, keylogging, PowerShell attack and process hollowing. The primary objective of Raccoon is to steal login data or sensitive banking information from victim systems and subsequently use them to infiltrate valuable online accounts or to commit identity fraud for further financial exploitation.

A significant portion of detected Raccoon credential and domain dark web leaks have come via a Russian Market threat actor. This threat actor, along with many others, uses Raccoon for its credential stealing capabilities and resulting financial gain. Raccoon targets a victim's system after they have visited a compromised web application, often sent to the victim via a phishing email. If alerted by their EDR, a victim can search for the relevant Indicator of Compromise (IOC) to confirm any successful exploitation and initiate the recovery process.

Raccoon is a service that can be subscribed to for as little as £75 per week or £200 per month, and 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 attractive for criminal groups of all sizes and ranks Raccoon as a highly prevalent malware across the online domain.

Raccoon is written in C++ and therefore can compromise all three major operating systems; Windows, MacOS and Linux.

The Federal Bureau of Investigation (FBI) has been monitoring operations pertaining to Raccoon stealer since March 2022 and has identified more than 50 million unique leaked credentials, ranging from emails, credit card numbers and passwords.

Most instances of credential leaks are via third-party exploitation, in which a member of an organisation uses their official business email to log into a personal account. Following the site becoming affected by Raccoon, the official business email flags as a breach for the associated organisation. Therefore, additional investigation is required to assess the level of danger posed by credential leaks.

As of October 2022, the founder of Raccoon was arrested in the Netherlands and now faces significant legal charges[1]. It is unclear how this arrest will affect the future threat landscape, but the stealware appears to remain active as of the time of writing.

In April 2023, The National Technical Research Organisation (NTRO) reported that eight government entities had been targeted by the Raccoon Stealer malware.

Impact

The loss of sensitive company and customer credentials to a threat actor, such as Russian Market or Malware Logs, can lead to serious implications to the security 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 spear phishing campaigns or further cyber-attacks. If employees have poor password hygiene, using the same password across multiple sites, a leak of one set of credentials can have a major knock-on effect to a wide array of systems and potentially lead to further compromise.

[1] US Indicts Ukrainian for 'Raccoon Stealer' Malware That Hit Millions of Computers (pcmag.com)

Incident Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide effective protection against malware threats including Raccoon Stealer. 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.

Moreover, the following advanced hunting query can be implemented, within the Microsoft Defender suite, to detect the presence of the Raccoon Stealer malware[2]:

```
DeviceProcessEvents
| where ((FolderPath matches regex @".*\.*\.exe") and FolderPath endswith @"\RegSvcs.exe" and FolderPath matches regex @".*\\AppData\\Local\\Temp\.*\.exe.*" and (FolderPath matches regex @".*AppData\\LocalLow\.*\.dll.*"))
```

Affected Products

- WindowsOS
- MacOS
- Linux

Containment, Mitigations & Remediations

The US Department of Justice, in coordination with the FBI and other criminal investigation departments, has created a website that enables users to determine whether or not they have been compromised by Raccoon[3].

It is recommended that upon the detection of compromised credentials, customers act fast 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 spear phishing campaigns. Furthermore, the enforcement of multi-factor authentication (MFA) is strongly recommended, as this can prevent adverse system access even when a credential is lost.

Threat intelligence has also detected a lack of strong password security and the use of basic, easy-to-crack passwords in use by customers and council sector employees, an example being that of 'password1'. It is strongly recommended that customers follow the National Cyber Security Centre (NCSC) guidance[4] of having passwords made up of three unrelated words and the incorporation of uppercase, lowercase, and symbols.

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

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 Raccoon. Regular in-house training will prove to be effective in reducing the potency of future Raccoon campaigns.

[2] Raccoon Infostealer Malware Returns with New TTPS – Detection & Response - Security Investigation (socinvestigation.com)
[3] Raccoon Infostealer Disclosure (ic3.gov)
[4] Three random words - NCSC.GOV.UK

Indicators of Compromise

Raccoon Stealer Associated File Hashes (SHA-256):

- a7b25c3995f6bc79c2075efbb0bbdbcc0a3cc7fccb920b6c760981cd866ed89a
- 0a97a2e908bf80d2259014727b5552ba82a145984cbf2d15d659fc95990b0a8c
- 11340b2ce797bc2e816c80de5c81a7e97a2c49cd737497e04ffa634b28dff91d
- 4eb1f72cd4836ffb4ba1982739b6c51608243893a077effe9d010339d80a15c3
- 5404387f44ed0c822de218656745eb70455f7a8826ca0fef70c3f4df3c739f1e
- ab01e44bb60f1ee4ca7359084479125dc356966e12222c3cc408af55f630f930
- acc51942016fa14566b6b88d8a19fa37dfd96ba5507190a67b318017739de2a3
- d341f7290aac5263839df2821ba9a4a8691dda52386d1874c30782a8aa20b4d7
- dff0b944493bf18723367a1125bf0017a87a4a8a7b54bc55ab89b9aa58fa3200
- e0ac3018ac3327e7d7e5d43d9b8b1e30003c31576cb804c49238339e890ab294
- e1c20fd6a261d4bc0efc245bc40346b58160022a179813ff294cfb42d aefedc2
- e356e2aeab59814110ed306feab73184954d3f0e26a10ab1754ea572d6adbdcb
- f8a03935fababe6260de74a71e71b8ac92a23969aeb433f8058ee65a49deca67
- 107953c29a193e80e0744f807acbfad8f4cf533ad811f4bf810b8cd1d58eed32
- 14a889b18ae5a7264923f81a450796ecd418bbd9ef0a21bd4b9cc468690d4264
- 32eb91bc7933a1e99fb1416e60523ecfde0811e5cdeb74b7877f457bf6dfea3e
- 4720bb74fb59d088232fe8562ea606587b4ae627b4f79e000beacbea3b2a5fbe
- 47f6d3a11ffd015413ffb96432ec1f980fba5dd084990dd61a00342c5f6da7f8
- 48849ac3f0808c310277130b423baa51452720f83e03ad534 cd7aee359339c7b
- 5a1181c156e5a4d59ae2cc9ead5e1a610b384bdde50df9cde87e331e404629ab

Raccoon Stealer Associated IP Addresses:

- 185[.]181[.]10[.]208
- 37[.]49[.]230[.]54
- 45[.]143[.]223[.]133
- 79[.]137[.]206[.]158
- 83[.]217[.]11[.]13
- 83[.]217[.]11[.]14
- 217[.]138[.]215[.]83
- 83[.]217[.]11[.]38
- 134[.]209[.]88[.]114
- 217[.]196[.]96[.]11
- 37[.]220[.]87[.]66
- 77[.]91[.]78[.]50
- 83[.]217[.]11[.]36
- 94[.]142[.]138[.]176
- 94[.]142[.]138[.]213
- 185[.]106[.]94[.]215
- 193[.]149[.]176[.]45
- 194[.]163[.]177[.]109
- 45[.]9[.]74[.]97
- 62[.]109[.]29[.]252
- 138[.]84[.]39[.]164

Raccoon Stealer Associated Domains:

- pgf5ga4g4b[.]cn
- adogeevent[.]com
- asfggagsa3[.]xyz
- luxury-limousine[.]com
- novacation[.]cn
- sagbbrrww2[.]cn
- skambio-porte[.]com
- post-make[.]com
- bitbucket[.]org
- dl[.]dropboxusercontent[.]com
- fevruv[.]com
- close-ffe[.]com
- post-make[.]com

Raccoon Stealer Associated URLs:

- hxxp[://]77[.]73[.]134[.]38/MyNewFileChr[.]exe
- hxxp[://]212[.]113[.]119[.]73
- hxxps[://]bitbucket[.]org/dsaddsaf1234/adobeprojectss/downloads/AppSetup[.]rar
- hxxps[://]dl[.]dropboxusercontent[.]com/s/wxh88thgzf2yvxi/BlessedArena_Launcher_1[.]2[.]5[.]zip?dl=1
- hxxps[://]file-toseend[.]com/

Raccoon Stealer Associated Malware Signatures:

- Gene.Win.Harmlet.19786-0
- Gene.Win.Harmlet.22196-79
- HEUR/QVM41.1.E7B6.Malware.Gen
- HEUR/QVM41.1.E7D4.Malware.Gen
- Hacktool.Win32.Shellcode.3!c
- Suspicious:Hacktool.33C0C390558BEC@.mg
- Suspicious:Trojan.8BFF558BEC#744A@2.mg
- Trojan-Ransom.StopCrypt
- Trojan-Spy.Agent
- Trojan.Agent
- Trojan.Antavmu.gen.qldi
- Trojan.DownLoader41.64435
- Trojan.DownLoader42.17886
- Trojan.DownLoader42.41972
- Trojan.DownLoader42.46254
- Trojan.DownLoader42.596
- Trojan.Multi.Generic.4!c
- Trojan.PWS.Siggen3.2819

Threat Landscape

In recent years, information stealing malware, such as Raccoon stealer, have become a prevalent infection vector. More specifically, Raccoon Stealer is a 'commodity' information stealer and, as such, data harvested by the malware is often sold within the illicit marketplace, whereby threat actors have the opportunity to purchase them[5]. 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.

Stealer malware, such as Raccoon , will remain undetected within the target landscape and, as such, they possess the ability to execute covertly without their presence being detected.

Threat Group

Deployment of the Raccoon Stealer malware has been associated with the following threat actor groups:

- Photix or 'black21jack77777'[6]
- Distributed Denial of Secrets
- IT Army of Ukraine
- Killnet
- TA505
- Vermux

Mitre Methodologies

Execution

T1053 – Scheduled Task[7]
T1059 – Command and Scripting Interpreter[8]
T1059.001 – Command and scripting interpreter: PowerShell[9]
T1064 - Scripting[10]
T1204.001 - User Execution: Malicious Link[11]
T1204.002 - User Execution: Malicious File[12]

Persistence

T1053 – Scheduled Task[13]
T1547.001 – Registry Run Keys / Startup Folder[14]

Privilege Escalation

[5] The Next Generation of Info Stealers • Kela (ke-la.com)
[6] Ukrainian Threat Actor Unmasked in Connection With Raccoon Malware (securityintelligence.com)
[7] Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®
[8] Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®
[9] Command and Scripting Interpreter: PowerShell, Sub-technique T1059.001 - Enterprise | MITRE ATT&CK®
[10] Scripting, Technique T1064 - Enterprise | MITRE ATT&CK®
[11] User Execution: Malicious Link, Sub-technique T1204.001 - Enterprise | MITRE ATT&CK®
[12] User Execution: Malicious File, Sub-technique T1204.002 - Enterprise | MITRE ATT&CK®
[13] Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®
[14] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®

T1053 – Scheduled Task[15]
T1547.001 – Registry Run Keys / Startup Folder[16]

Defence Evasion

T1112 – Modify Registry[17]
T1202 – Indirect Command Execution[18]
T1222 – File and Directory Permissions Modification[19]
T1064 - Scripting[20]

Credential Access

T1552.001 – Credentials in Files[21]
T1539 - Steal Web Session Cookie[22]

Discovery

T1012 – Query Registry[23]
T1057 – Process Discovery[24]
T1082 – System Information Discovery[25]
T1120 – Peripheral Device Discovery[26]
T1518 - Software Discovery[27]

Collection

T1005 – Data from Local System[28]
T1114 – Email Collection[29]
T1185 – Browser Session Hijacking[30]

Command and Control

T1071 – Application Layer Protocol[31]
T1071.001 – Application Layer Protocol: Web Protocols[32]
T1102 – Web Service[33]

Impact

T1486 - Data Encrypted for Impact[34]
T1491 - Defacement[35]

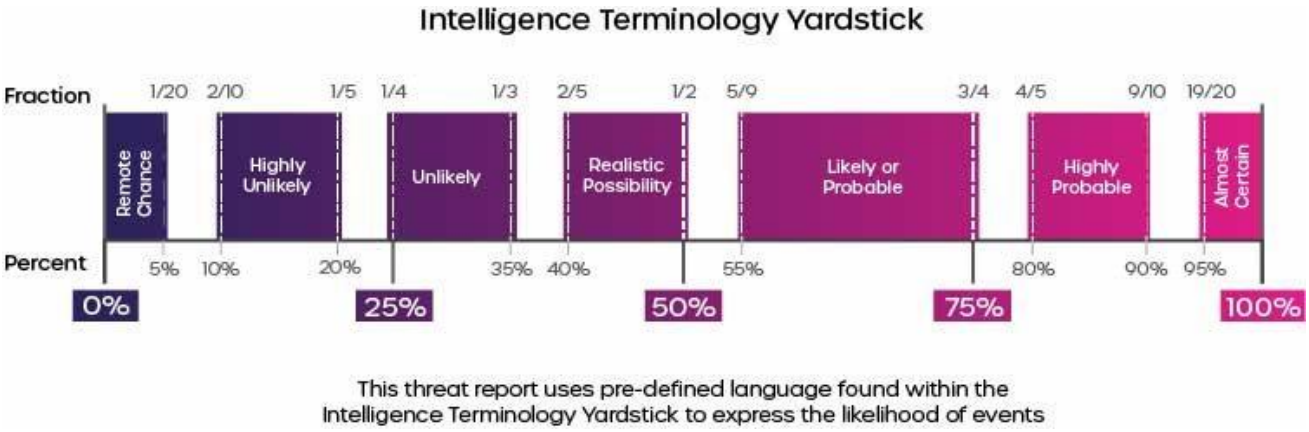
---

[15] Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®
[16] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[17] Modify Registry, Technique T1112 - Enterprise | MITRE ATT&CK®
[18] Indirect Command Execution, Technique T1202 - Enterprise | MITRE ATT&CK®
[19] File and Directory Permissions Modification, Technique T1222 - Enterprise | MITRE ATT&CK®
[20] Scripting, Technique T1064 - Enterprise | MITRE ATT&CK®
[21] Unsecured Credentials: Credentials In Files, Sub-technique T1552.001 - Enterprise | MITRE ATT&CK®
[22] Steal Web Session Cookie, Technique T1539 - Enterprise | MITRE ATT&CK®
[23] Query Registry, Technique T1012 - Enterprise | MITRE ATT&CK®
[24] Process Discovery, Technique T1057 - Enterprise | MITRE ATT&CK®
[25] System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®
[26] Peripheral Device Discovery, Technique T1120 - Enterprise | MITRE ATT&CK®
[27] Software Discovery, Technique T1518 - Enterprise | MITRE ATT&CK®
[28] Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®
[29] Email Collection, Technique T1114 - Enterprise | MITRE ATT&CK®
[30] Browser Session Hijacking, Technique T1185 - Enterprise | MITRE ATT&CK®
[31] Application Layer Protocol, Technique T1071 - Enterprise | MITRE ATT&CK®
[32] Application Layer Protocol: Web Protocols, Sub-technique T1071.001 - Enterprise | MITRE ATT&CK®
[33] Web Service, Technique T1102 - Enterprise | MITRE ATT&CK®
[34] Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®
[35] Defacement, Technique T1491 - Enterprise | MITRE ATT&CK®

Further Information

- Malpedia Raccoon Stealer - Malpedia

Intelligence Cut-off Date (ICoD): 10/05/2023 10:00 UTC



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