Quorum
Cyber

Threat Intelligence
Gootloader
Payload Distribution

TLP Status: CLEAR

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

Table of Contents

Document Control

Revision History

Version	Date	Summary of Changes
0.1	15/08/2023	Initial Report Drafted
1.0	30/08/2023	PDF Formatting

Related Documents

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

Document Name	Date	Version
-	-	-

Gootloader

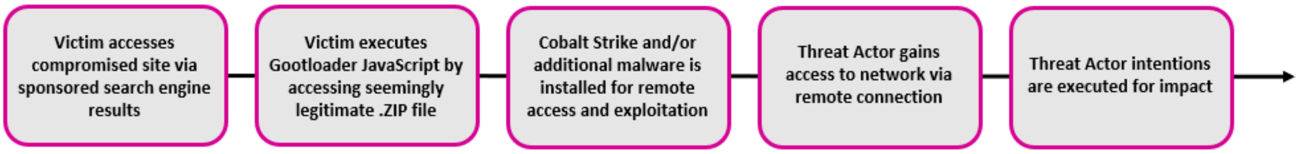
Overview

Active since 2018, GootLoader is a malware downloader that can deliver secondary payloads such as Cobalt Strike, REvil ransomware, Gootkit, BlueCrab and the Kronos trojan. The malware's primary method of distribution is conducted via search engine optimisation (SEO) poisoning techniques, including the use of sponsored search engine links. Accessing one of these links will direct victims to legitimate but compromised WordPress sites that host the malware contained within a .ZIP file.

Recent targeting trends show that the malware has been observed in attacks against law firms in the US, Canada, the UK, and Australia. This suggests that the malware is more likely to be incorporated with sponsored search engine adverts mimicking sites of interest for those operating within the law industry such as search results for legal documents and agreements.

Historic reporting indicates that Gootloader was primarily used to deploy ransomware, however, recent examples of the malware's use has not involved the deployment of ransomware, suggesting a potential shift in operations and motivation by threat actors towards cyber espionage activities.

GOOTLOADER METHODOLOGY


Victim accesses compromised site via sponsored search engine results
Victim executes Gootloader JavaScript by accessing seemingly legitimate .ZIP file
Cobalt Strike and/or additional malware is installed for remote access and exploitation
Threat Actor gains access to network via remote connection
Threat Actor intentions are executed for impact

Impact

Successful exploitation by Gootloader will almost certainly result in loss of network integrity and enable further access to exploiting threat actors. Once infected with Gootloader, a threat actor will highly likely deploy additional malware payloads depending on their intentions and requirements. Common deployments include Gootkit, Cobalt Strike and various ransomware variations. The application of additional malware will likely result in loss of sensitive data for exploitation and loss of company reputation.

Incident Detection

Recent campaigns have shown that GootLoader is evolving, adding new components and obfuscation techniques to conceal its infection chain. However, a comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide additional protection against ransomware threats like that implemented by the Knight ransomware. EDR solutions can alert system users of potential breaches and stop further progress before the malware can do significant damage.

Microsoft Defender Antivirus detects threat components as the following malware:

- Gootloader
- Gootkit.

Targeted Products

Windows OS.

Containment, Mitigations & Remediations

As mentioned previously, a primary method of reducing the threat of distribution malware such as Gootloader is to detect it in the early stages through the use of an effective and monitored EDR solution. An effective EDR tool such as the Microsoft Defender suite will block Gootloader, and further malware exploitation attempts, triggering alerts.

Once detected and if possible to do so, immediately isolate the affected device, because if Gootloader has been launched, the device might already be under the control of the attacker and therefore will need to be removed from the network to limit impact and halt lateral movement.

Additionally, if compromise is suspected, logs should be checked for Cobalt Strike alerts as threat actors may have dropped further malware to enable credential access, lateral movement, or other malicious activities.

Indicators of Compromise

GOOTLOADER ASSOCIATED HASHES:

SHA-256

- c41a2ddf8c768d887b5eca283bbf8ea812a5f2a849f07c879808845af07409ed

SHA-1

- eaad989098815cc44e3bcb21167c7ada72c585fc

MD5

- 3416b560bb1542af1124b38fb344fa1f
- 3d768691d5cb4ae8943d8e57ea83cac1
- 7a1369922cfb6d00df5f8dd33ffb9991
- 92a271eb76a0db06c94688940bc4442b
- 04746416d5767197f6ce02e894affcc7
- 08fa99c70e90282d6bead3bb25c358dc
- 2eede45eb1fe65a95aefa45811904824
- 35238d2a4626e7a1b89b13042f9390e9
- 53c213b090784a0d413cb00c27af6100
- 7352c70b2f427ef4ff58128a428871d3
- 82607b68e061abb1d94f33a2e06b0d20

- a0b7da124962b334f6c788c27beb46e3
- ab1171752af289e9f85a918845859848
- aef6d31b3249218d24a7f3682a00aa10
- af9b021a1e339841cfdf655964088 62d
- d6220ca85c44e2012f76193b38881185
- ec17564ac3e10530f11a455a475f9763
- f9365bf8d4b021a873eb206ec98453d9

Threat Group

The Gootloader malware has been associated with threat actors tracked as UNC2565.

Threat Landscape

The Gootloader malware has been developed and solely utilised by the threat actor tracked as UNC2565. The malware is designed to be an Initial-Access-as-a-Service (IAaaS) which can be sold on to other threat actors for use in other attacks, such as ransomware. The delivery mechanism utilised for this malware presents a challenge for detection and it is expected that this trend will continue.

Mitre Methodologies

Reconnaissance

T1593.002 - Search Engines[1]

Discovery

T1057 - Process Discovery[2]

Initial Access

T1189 - Drive-by Compromise[3]

Resource Development

T1608.006 - SEO Poisoning[4]

Collection

T1005 - Data from Local System[5]

[1] https://attack.mitre.org/techniques/T1593/002/
[2] https://attack.mitre.org/techniques/T1057/
[3] https://attack.mitre.org/techniques/T1189/
[4] https://attack.mitre.org/techniques/T1608/006/
[5] https://attack.mitre.org/techniques/T1005/

Defence Evasion

T1070.001 - Clear Windows Event Logs[6]
T1070.004 - File Deletion[7]
T1134.002 - Create Process with Token[8]
T1140 - Deobfuscate/Decode Files or Information[9]
T1218.011 - Rundll32[10]

Execution

T1059.001 - PowerShell[11]
T1059.003 - Windows Command Shell[12]
T1059.007 - JavaScript[13]
T1106 - Native API[14]
T1204.002 - Malicious File[15]

Privilege Escalation

T1547.001 - Registry Run Keys / Startup Folder[16]
T1574.002 - DLL Side-Loading[17]

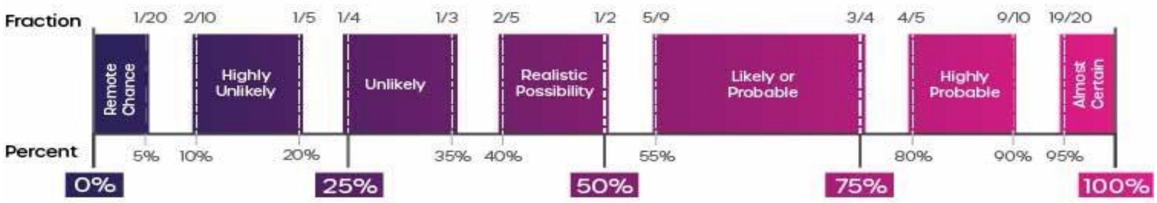
Impact

T1486 - Data Encrypted for Impact[18]
T1489 - Service Stop[19]

Further Information

Intelligence Cut-off Date (ICoD): 15/08/2023 10:00 UTC

Intelligence Terminology Yardstick



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

[6] https://attack.mitre.org/techniques/T1070/001/
[7] https://attack.mitre.org/techniques/T1070/004/
[8] https://attack.mitre.org/techniques/T1134/002/
[9] https://attack.mitre.org/techniques/T1140/
[10] https://attack.mitre.org/techniques/T1218/011/
[11] https://attack.mitre.org/techniques/T1059/001/
[12] https://attack.mitre.org/techniques/T1059/003/
[13] https://attack.mitre.org/techniques/T1059/007/
[14] https://attack.mitre.org/techniques/T1106/
[15] https://attack.mitre.org/techniques/T1204/
[16] https://attack.mitre.org/techniques/T1547/001/
[17] https://attack.mitre.org/techniques/T1574/002/
[18] https://attack.mitre.org/techniques/T1486/
[19] https://attack.mitre.org/techniques/T1489/