TLP: WHITE

2021-009: Malicious actors deploying Gootkit Loader on Australian Networks

From April 2021, the Australian Cyber Security Centre (ACSC) has received an increase in reporting of malicious actors targeting Australian networks with Gootkit JavaScript (JS) Loaders. Open-source reporting confirms that Gootkit JS Loaders are a precursor to several malware families traditionally used for cybercrime, notably, Gootkit, REvil ransomware, Kronos, or CobaltStrike.

The ACSC is providing this information to enable organisations to undertake their own risk assessments and take appropriate actions to secure their systems and networks. The ACSC will update this advisory if more information becomes available.

Background

Gootkit JS Loaders have been deployed onto Australian networks through search engine de-optimisation, including targeting the word 'agreement'.

This advisory provides technical analysis of identified cyber activity on Australian networks for the purposes of computer network defence. The technical analysis is based on two specific Gootkit JS Loader samples; however, additional indicators of compromise (IOCs), sourced from multiple samples, have been included below.

The malicious JavaScript identified was obfuscated in several stages. Once unpacked, Gootkit malware was retrieved. Open-source reporting indicates that:

a. Gootkit JS Loaders are a precursor to several malware families traditionally used for cybercrime, notably, Gootkit, REvil ransomware, Kronos, or CobaltStrike.

b. The JavaScript-based obfuscated loader shares capability with various other JS Downloaders identified in open-source reporting.

c. Users are targeted based on specific “search-engine query de-optimisations”.

Mitigation

Application Control should be implemented to prevent execution of unapproved/malicious programs, including .exe, DLL, scripts (Windows Script Host, PowerShell and HTA) and installers.

Technical Details

The analysed Gootkit JS Loader samples shared underlying code-structure and multi-stage obfuscation techniques. The analysed samples differed slightly in the presented order and structure of functions.

ACSC Comment:

It is likely that a broad set of function naming exists within this malware family code due to the obfuscation. Previously identified open-source samples had obfuscated all aspects of the code with randomly generated alphanumeric strings. The samples analysed by the ACSC were specifically obfuscated with word-substitution.

Identified Gootkit JS Loader samples were obfuscated with simple word substitution for variables, functions, and strings (other than required system function: e.g. wscript). Additional stages of execution were obfuscated with a simple substitution cypher that was easily reversed.

The JavaScript loaded, slept and deobfuscated the next stage of the loader. Once all stages were deobfuscated, the JavaScript would generate a pseudorandom integer and beacon to hard-coded compromised domains, with a specific search-term.

The hard-coded domains could be retrieved via dynamic execution in a sandbox environment, or via manual deobfuscation and reversal of the encoded variables and functions.

ACSC Comment:

The analysed samples had different code-structures, and differed slightly from previously reported samples targeting European victims. The obfuscation method differed to open-source reporting on Gootkit JS Loaders. This suggests a change in the search engine targeting methodology, and a distinct revision or renewal of the underlying Gootkit builder codebase when pivoting to non-European users.

Indicators of Compromise (IOCs)

Command and Control

HTTP GET requests were made to specific URI **/search.php** with the parameter **{randomised 13 character string}** set to **{pseudorandom integer}**

HTTP GET Request Sample

```
GET /search.php?tgtytnbwtmelg=5599961917583517 HTTP/1.1
Host: www[.]kucukisletmeler[.]com
```

Domains Hosting C2 / Second Stage Retrieval

```
"kucukisletmeler[.]com",
"kidzee[.]com",
"kiyindo-shiatsu[.]com",
"kettlebellgie[.]be",
"vin-aire[.]com",
"vesperience[.]com",
"travelogue.grecotel[.]com",
"uumu[.]fi",
"sundance.usc[.]edu"
```

Execution on host

To identify this activity, look for execution chain of 7-Zip (or other zip file manager) launching wscript.exe with the command line argument containing a .js file

Malware Samples

Identified malware sample details below:

a. Sample One

   i. Filename: which_australian_prime_minister_signed_the_lima_agreement.js

   ii. MD5: `333d5f9d50c1b67bae4cc811a59ef94c`

   iii. SHA256: `c1c01fa53f45e751cc26213f1ff5c6f3a70f9fa1af725499a8d34f50eb7f4733`

b. Sample Two

   i. Filename: difference_between_supplemental_agreement_and_amendment_agreement.js

   ii. MD5: `2bd52b710f6f7f994f3e80261cc56e61`

   iii. SHA256: `1344146efb830df320496948569560102476d84df393a766345f6d0d8eee14c0`

c. Sample Three

   i. Filename: brisbane_city_council_enterprise_agreement.js

   ii. MD5: `f864f333c609c397c921a9bd6fe1c684`

   iii. SHA256: `9d059411604fb00c0d407ef4eac5ff00c38db0e9935a842cdd363419f4378304`

d. Sample Four

   i. Filename: bapi_for_outline_agreement.js

   ii. MD5: `b30c431c55293bc174eba6a3d33eb178`

   iii. SHA256: `2fcca5598f5e0c9d486e6c1c4bfc7a3652b7ba2b88b49406f05221b2f982ed94`

e. Sample Five:

   i. Filename: bapi_for_outline_agreement.js

   ii. MD5: `f9f782e6a23a64b913750036aa390d1e`

   iii. SHA256: `65b86bbbc46da97816a8e26f909a164adf77c84bb5ee8f824b6fdbc3e0269abe`

Traffic light protocol

The following table lists the classification levels used in the traffic light protocol (TLP) and describes the restrictions on access and use for each classification level.

TLP classification	Restrictions on access and use
RED	Access to and use by your ACSC security contact officer(s) only. You must ensure that your ACSC security contact officer(s) does not disseminate or discuss the information with any other person, and you shall ensure that you have appropriate systems in place to ensure that the information cannot be accessed or used by any person other than your ACSC security contact officer(s).
AMBER	Restricted internal access and use only. Subject to the below, you shall only make AMBER publications available to your employees on a 'need to know basis' strictly for your internal processes only to assist in the protection of your ICT systems. In some instances you may be provided with AMBER publications which are marked to allow you to also disclose them to your contractors or agents on a need-to-know basis—strictly for your internal purposes only to assist in the protection of your ICT systems.
GREEN	Restricted to closed groups and subject to confidentiality. You may share GREEN publications with external organisations, information exchanges, or individuals in the network security, information assurance or critical network infrastructure community that agree to maintain the confidentiality of the information in the publication. You may not publish or post on the web or otherwise release it in circumstances where confidentiality may not be maintained.
WHITE	Not restricted. WHITE publications are not confidential. They contain information that is for public, unrestricted dissemination, publication, web-posting or broadcast. You may publish the information, subject to copyright and any restrictions or rights noted in the information.
NOT CLASSIFIED	Any information received from ACSC that is not classified in accordance with the TLP must be treated as AMBER classified information, unless otherwise agreed in writing ACSC.