NCSC
National Cyber Security Centre

2207071000-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Compromised WordPress Websites Distributing SolarMarker Malware
2022-07-07

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Summary

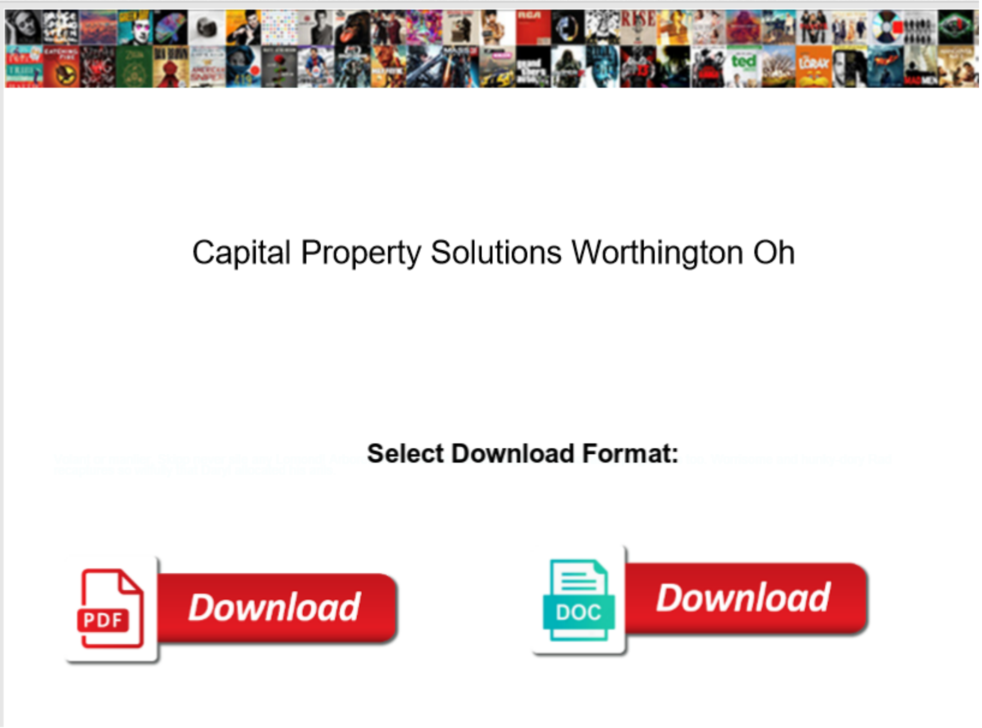
The NCSC has observed a number of WordPress websites which appear to be compromised. These compromises match the Tactics, Techniques and Procedures used in order to distribute **SolarMarker** malware.

SolarMarker has two major capabilities, it installs a **backdoor** or an **infostealer** as soon as the victim runs the payload. Both SolarMarker's modules can damage organisations as the backdoor can be leveraged by an attacker to deploy additional malware or steal sensitive information.

The threat actors behind this malware have been observed primarily delivering payloads via two methods:

1. Google Groups pages
2. In this case, compromised WordPress websites are used. The malicious download lures are uploaded through the Formidable plugin with the following path **"/wp-content/uploads/formidable/*.pdf"**, which is the default file uploads page

These compromised WordPress websites are hosting a number of malicious files which may be used during the SolarMarker infection process. If you are hosting a website that uses WordPress and in particular WordPress websites that use the ***Formidable*** plugin, please check your systems to ensure that compromise of your system has not occurred.



Capital Property Solutions Worthington Oh

Select Download Format:

Figure1: Content of Malicious PDF file

There is a risk to potential victims who may download these documents from an infected website which they would usually trust. It is advised that users are made aware of the risk of downloading and clicking on documents which may be suspicious in their content.

Analysis

SolarMarker malware that uses PDF implants as an infection vector has been observed making use of Search Engine Optimisation (SEO) in order to promote clicks to their malicious payloads. In most of the cases, compromised WordPress sites were used to host PDF files, specifically in the **wp-content/uploads/formidable** directories on those websites.

The corresponding code in the PDF file source links these buttons to a distribution site, when we parse the pdf code we can see a number of URLs included as below:

```
/Type /Annot
      /Subtype /Link
      /Rect [18.00 459.00 275.00 381.00]
      /Border [0 0 0]
      /A
        <<
          /S /URI
          /URI (http://[REDACTED].site/Is-A-Lien-Title-Bad/pdf/[REDACTED].ie)
        >>
```

Re-directors

During the infection chain associated with these attacks, the NCSC has observed a number of re-directs. The distribution sites re-direct victims to other malicious/compromised websites in order to deliver a malicious payload.

SolarMarker makes use of Freenom[1] domains (e.g. .ga, .ml, .cf and .gq TLDs):

```
<meta http-equiv="refresh" content="0;URL=hxxps[:]//griscurviejamahun[.]ga/
c9122dd3c044216dc2a0627b231759da/Is-A-Lien-Title-Bad/am65704/doc">
```

This process will eventually lead to the download of the SolarMarker payload which can act as a backdoor and an infostealer.

Malware Backdoor and Infostealer capabilities

The majority of SolarMarker deployments result in backdoor deployments as it provides the threat actor(s) with the option to deliver additional payloads.

The backdoors are obfuscated with .NET DLLs (Dynamic Link Libraries) which recently have been observed employing a number of layers of obfuscation in order to avoid detection, such as encrypting all traffic to C2 Servers using a hard-coded RSA key and a symmetric AES CBC (Cipher Block Chaining) algorithm.

The infostealer stealer element of this malware targets crypto currency wallets which may be on the victims machine and also has the capability to steal VPN and RDP configurations as well as cookies and browser credentials from:

Opera, Brave, Microsoft Edge, Mozilla Firefox, and Google Chrome.

[1] https://www.freenom.com/en/index.html

Recommendations

There are two distinct groups at risk from these attacks, **Websites Owners** that use WordPress and **Victims who will install the SolarMarker malware**.

Website Owners
The NCSC has observed a significant amount of WordPress websites that have recently been compromised in this manner. Owners of WordPress websites, particularly ones that use the **Formidable** plugin should check their systems to ensure that compromise has not occurred.

In the event that a website has been compromised and malicious content is being hosted there, incident response procedures should be initiated. If the technical knowledge is not available to the affected organisation, they should engage third party support in order to remediate and recover.

SolarMarker Malware Infection

- Organisations should train users about the risks of SEO poisoning and how to identify potentially malicious results.
- Organisations should also ensure that a defense-in-depth approach to cybersecurity is employed [2]
- Use an email security solution that can block phishing, spam, and other malicious emails from reaching inboxes
- Run phishing simulation exercises to test and renew employees' security awareness

[2] https://assets.gov.ie/205834/1727388a-02d6-47d4-bebe-38774da2f321.pdf

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie