MENLO SECURITY

Holy SEO Poisoning

The Menlo Labs team has seen a rise in attacks designed to target users, as opposed to organizations, bypassing traditional security measures. One example is Menlo Labs we are tracking is an active campaign called SolarMarker. We've seen an increase in attackers using SEO poisoning, with high success rates, to serve malicious payloads to customers. These types of highly evasive attacks have been seen before, but the velocity, volume, and complexity of this new wave has increased in recent months.

Holy SEO Poisoning

Executive Summary

Menlo Labs is currently tracking an active campaign called SolarMarker. We've seen an increase in attackers using SEO poisoning, with high success rates, to serve malicious payloads to customers. In the past few months, we've observed at least two campaigns across our global customer base.

1. **Gootloader Campaign:** This campaign was seen dropping the REvil ransomware.

2. **SolarMarker Campaign:** This campaign was seen dropping the SolarMarker backdoor.

Several blogs are available that provide details about the malware and post-compromise CnC traffic. In this blog, we are providing insight into the delivery mechanism and the scope of the attack as we see it unfold.

In addition to SolarMarker, the Menlo Labs team has seen a rise in attacks designed to target users, as opposed to organizations, bypassing traditional security measures. These types of highly evasive attacks have been seen before, but the velocity, volume, and complexity of this new wave has increased in recent months. Bad actors are exploiting the new world order in which the lines between business and personal device use are blurred. In these attacks, threat actors turn advances in web browsers and browser capabilities to their advantage to deliver ransomware, steal credentials, and drop malware directly to their targets. We will be sharing more about these attacks in a future blog.

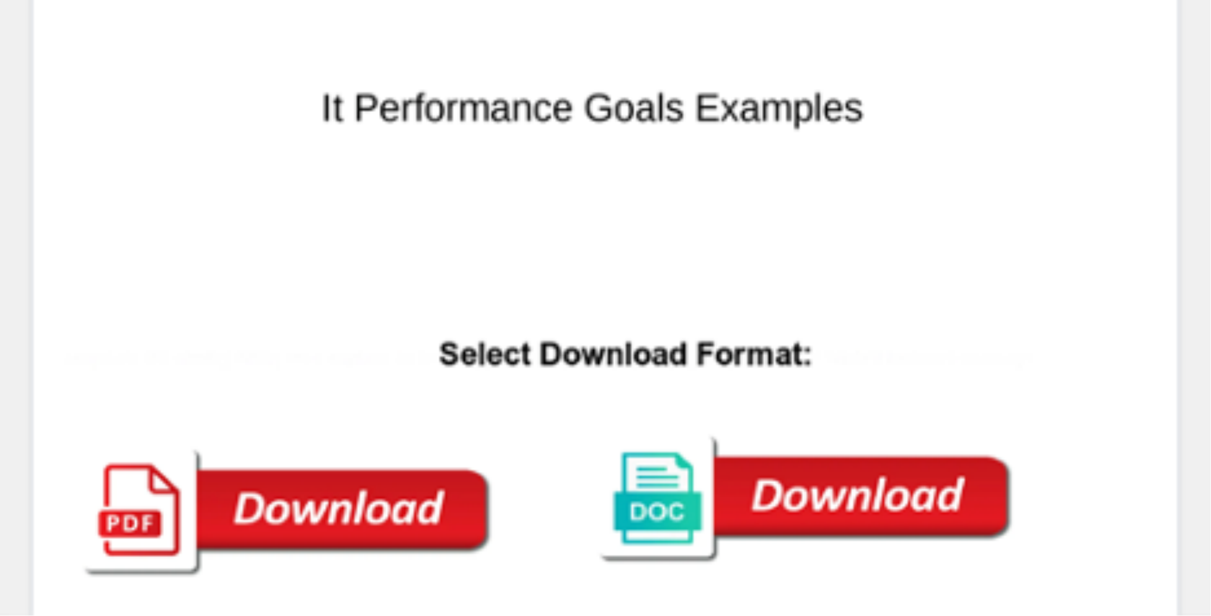
Infection Vector

The SolarMarker campaign employs SEO poisoning. Attackers commonly use this technique to artificially increase the ranking of their malicious pages. They do this by injecting the malicious website with keywords that users search for. Across our customer base, we have seen a wide variety of search terms that led to malicious pages. We have observed **over 2,000 unique search terms** that led to malicious websites. The following search terms are some examples we have seen:

- blue-jacket-of-the-quarter-write-up-examples
- industrial-hygiene-walk-through-survey-checklist
- 5-levels-of-PD-eval
- Sports Mental Toughness Questionnaire

The attack works in the following manner:

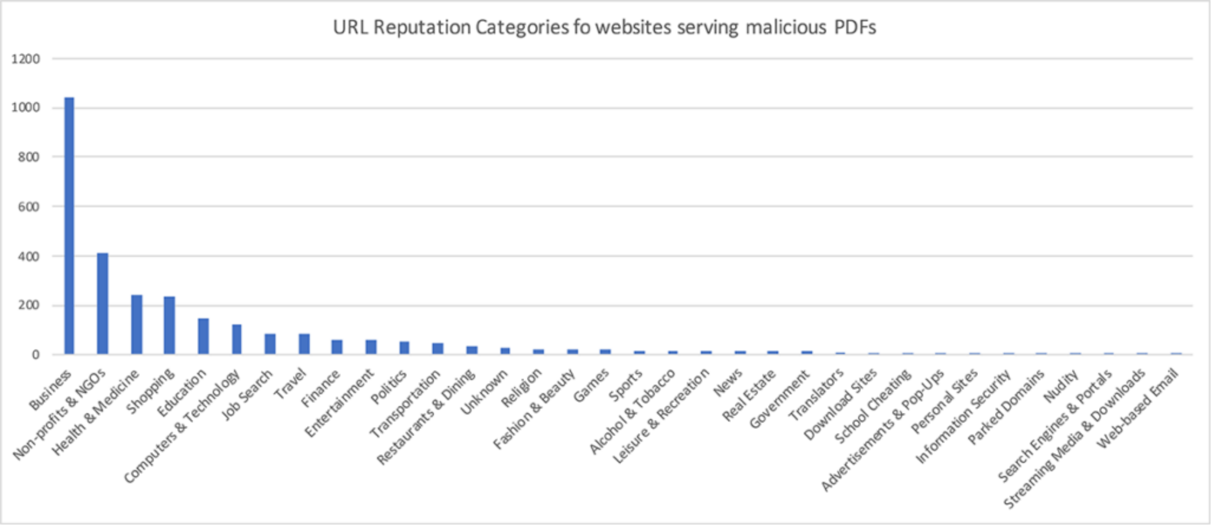
1. A user searches for something using their preferred search engine.
2. Compromised websites that host malicious PDFs show up in their search results.
3. The user clicks on the SEO poisoned link.
4. The user lands on a malicious PDF that looks like the one in Figure 1.
5. Clicking on either of the download buttons takes the user through multiple HTTP redirections, after which a malicious payload is downloaded onto the endpoint.
6. We observed payloads with three different payload sizes being downloaded in this campaign. The smallest payload we saw was about 70MB, while the largest was about 123MB. The large sizes of the malicious payloads exceed file size limits defined by sandboxes and other content inspection engines.


It Performance Goals Examples

Select Download Format:

Figure 1

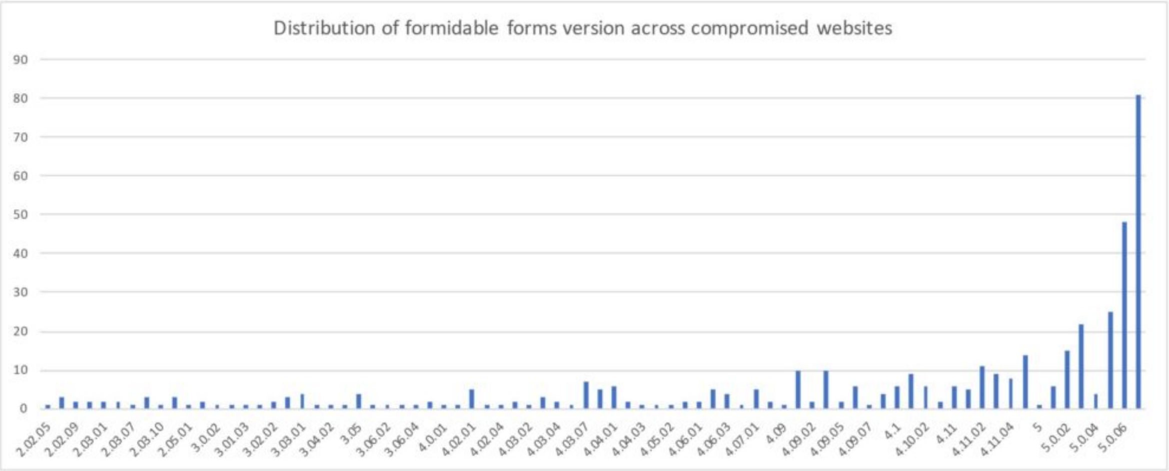
All the compromised sites hosting the malicious PDFs were observed to be WordPress sites. The following chart shows the various categories of websites that were seen serving the malicious PDFs across our customer base. As you can tell from the categorization, most of the sites were benign sites that were compromised to host the malicious content. During our analysis, we found some well-known educational and .gov websites serving the malicious PDFs. As part of our commitment to ensuring a safe Internet, we notified all the affected parties, and these malicious PDFs were taken down.



The malicious PDFs were being served from a specific directory, namely

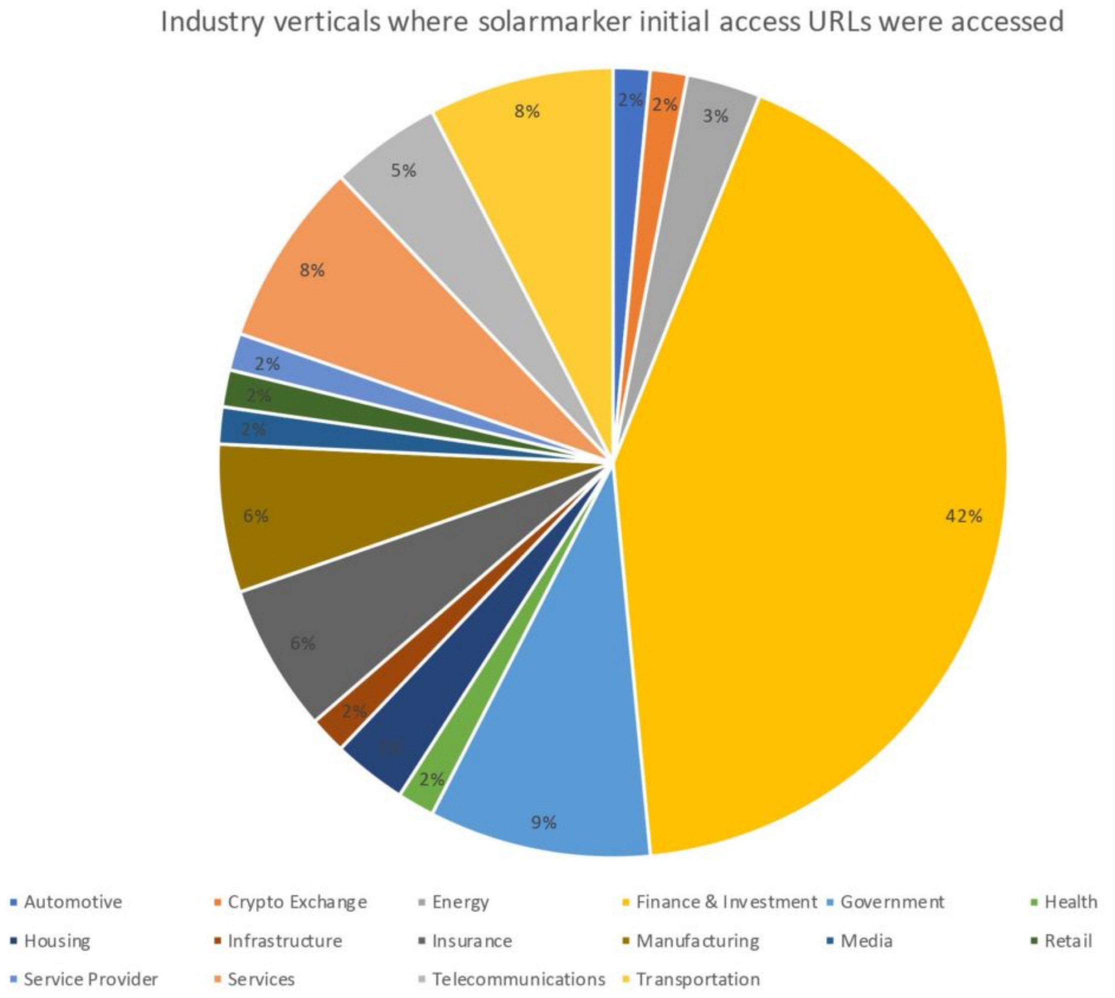
/wp-content/uploads/formidable/. This directory is created when a WordPress plug-in called Formidable Forms is installed on the website. Formidable Forms is a plug-in that lets admins easily create a form. As of this writing, **100 percent of the compromised URLs** in our dataset were hosting malicious PDFs under this specific directory location.

The following chart represents the versions of the Formidable Forms plug-in installed on the compromised websites that we analyzed.

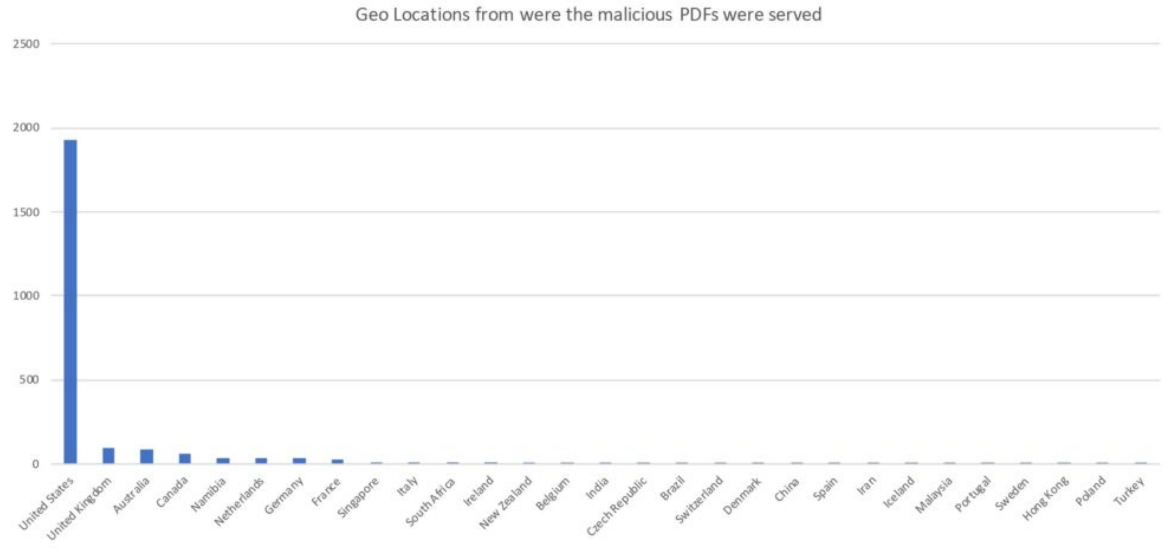


Version 5.0.07 was the latest version of the Formidable Forms plug-in at the time of this research, and it was the version that was most used by compromised websites. The minimum version that we observed was 2.02.05.

Looking at the changelog of Formidable Forms, it looks like the plug-in was updated and a security issue was fixed. We are not sure if this was the security issue responsible for the initial vector in the SolarMarker campaign or if Formidable Forms was the vulnerable plug-in in question, but it was the common plug-in installed across all the compromised websites we analyzed. We reached out to Formidable Forms via LinkedIn to collaborate, but unfortunately did not get a response.
The SolarMarker campaign was pretty prevalent and we saw it affect every geo and vertical across our customer base. The following industry verticals were observed clicking on the malicious links hosting the PDF files.



The following chart shows the various locations from where malicious PDFs were served. While the U.S. topped the list, we noticed that sites in Iran and Turkey were also being used in this campaign.



Command and Control

The SolarMarker backdoor itself has been widely documented. CrowdStrike has an analysis of the backdoor. In addition to the CnC IPs listed in CrowdStrike's blog post, the Menlo Labs researchers were able to identify six other CnC IPs. The identified CnC IPs have been pushed to the Menlo Isolation Core™ platform, so our customers are protected.

1. **POST http://45.42.201.248/**
2. **POST http://37.120.237.251/**
3. **POST http://5.254.118.226/**
4. **POST http://23.29.115.175/**
5. **POST http://216.230.232.134/**
6. **POST http://146.70.24.173/**

Conclusion

As the world moved to remote work, the browser became the location where work happens. In fact, a study by Google found that end users spend on average 75 percent of their workday in a browser. A recent survey by Menlo Security found that three-quarters of respondents believe that hybrid and remote workers accessing applications on unmanaged devices pose a significant threat to their organization's security. And while the majority (79 percent) of respondents have a security strategy in place for remote access by third parties and contractors, they have growing concerns about the risks that remote workers present, with over half (53 percent) of respondents planning to reduce or limit third-party/contractor access to systems and resources over the next 12 to 18 months.

While SolarMarker is a classic example of a supply chain–style attack in which attackers can take advantage of vulnerable sites to launch their malicious campaigns, it is also an example of how attackers have quickly found ways to exploit the increased usage of the browser, as well as companies pivoting to cloud-based applications. What makes this type of attack especially dangerous is the method used to initiate it. As mentioned earlier in this blog, these attacks have been specifically designed to target the user directly by evading traditional methods of detection.

Recommendations

- Menlo recommends blocking Windows executable file downloads from unwanted categories.
- Most of the websites in the redirects are either hosted on .site or .tk TLDS If policy permits, Menlo recommends blocking all sites that end in either of these TLDS.