Hackers Flood the Web with 100,000 Malicious Pages, Promising Professionals Free Business Forms, But Delivering Malware, Reports eSentire

esentire.com/security-advisories/hackers-flood-the-web-with-100-000-malicious-pages-promising-professionals-free-business-forms-but-are-delivering-malware-reports-esentire

×

Search

Security advisories | Apr 13, 2021

Business professionals search google for free office forms (invoices, questionnaires, and receipts) but get served a RAT

eSentire, a leading cybersecurity solutions provider, reported today that business professionals are currently being lured to hacker-controlled websites, hosted on Google Sites, and inadvertently installing a known, emerging Remote Access Trojan (RAT). eSentire has detected several incidents in the past week. The attack starts with the potential victim performing a search for business forms such as invoices, questionnaires, and receipts. Unlike the LinkedIn **spearphishing** campaign eSentire reported last week that utilized email and LinkedIn channels, this campaign lays long-standing traps for victims using Google **search redirection** and the **drive-by- download** method. Once the RAT is on the victim's computer and activated, the threat actors can send commands and upload additional malware to the infected system, such as ransomware, a credential stealer, a banking trojan, or simply use the RAT as a foothold into the victim's network.

Upon attempting to download the alleged document template, users are redirected, unknowingly, to a malicious website where the RAT malware is hosted. eSentire's Threat Response Unit (TRU) discovered over 100,000 unique web pages that contain popular business terms/particular keywords: template, invoice, receipt, questionnaire, and resume. In a precursory search, 70,000 unique web pages included the mention of either *template* or *invoice*. These common business terms serve as keywords for the threat actors' search optimization strategy, convincing Google's web crawler that the intended content meets conditions for a high PageRank score.

Once the target lands on a site controlled by the hacker, the page shows download buttons for the document template they were searching. When clicked, the business professional is redirected (unknowingly) to a malicious website which serves up an executable disguised as a pdf document or a word document. In the incident which eSentire investigated, when the executable (disguised as a pdf) was launched by the user, they simultaneously installed the SolarMarker RAT (also referred to as Yellow Cockatoo, Jupyter, and Polazert) and a complimentary copy of the Slim PDF reader application. Slim PDF is a legitimate application for reading pdfs. The pdf reader application is installed by the threat actors, either in an effort to convince the victim of the legitimacy of the document they were seeking or as a distraction from the installation of the RAT. As with any RAT, once SolarMarker is active, the threat actors can send commands and upload additional files to the infected system. The TRU has not yet observed actions-on-objectives following a SolarMarker infection, but suspect any number of possibilities, including ransomware, credential theft, fraud, or as a foothold into the victim networks for espionage or exfiltration operations.

Key Takeaways

- A Remote Access Trojan (RAT) with many names: Tracked as SolarMarker, Jupyter, Yellow Cockatoo and Polazert
- The threat actors behind SolarMarker have added Slim PDF to their list of decoy applications
- Switched from search redirection, via Shopify, to search redirection via Google Sites

Comment from Spence Hutchinson, Manager of Threat Intelligence for eSentire

“Security leaders and their teams need to know that the threat group behind SolarMarker has gone to a lot of effort to compromise business professionals, spreading a wide net and using many tactics to successfully disguise their traps,” said Spence Hutchinson, Manager of Threat Intelligence for eSentire. “For instance, the Solar Marker group has:

:

- Deployed over 100,000 web pages via Google Sites. The benefits of being hosted on Google’s infrastructure are several. First, Google is trusted by both security appliances and human eyes. Secondly, it probably doesn't hurt your PageRank score with Google to use Google’s infrastructure. The pages are also padded with generated text keywords, a tactic likely used to further influence search results.
- The threat actors have created tens of hundreds of web pages with popular business terms, such as invoice, statement, receipt, questionnaire, so that when a business professional is searching the Internet for a specific business template, then there is a chance that the top search results will include one of their malicious pages.
- The infection process relies on exploiting the user, not an application. The user simply executes a binary disguised as a PDF to infect the machine. This is an increasingly common trend with malware delivery, which speaks to the improved security of applications such as browsers that handle vulnerable code. Unfortunately, it reveals a glaring blindspot in controls which allow users to execute untrusted binaries or script files at will.

- The SolarMarker campaign utilizes a variety of decoy applications. Most recently, TRU observed that the Slim PDF reader software was the decoy being downloaded onto the victim's computer. This serves as a distraction, as well as an additional element to help convince the victim that they are downloading a pdf.

"Another troubling aspect of this campaign is that the SolarMarker group has populated many of their malicious web pages with keywords relating to financial documents, e.g., statements, receipts, invoices, etc.," continued Hutchinson.. "A financial cybercrime group would consider an employee, working in the finance department of a company, or an employee, working for a financial organization, a high value target. In fact, the SolarMarker incident which eSentire disrupted involved an employee of a financial management company. Once a remote access trojan (RAT) has been installed on a victim's computer, the threat actors can upload additional malware to the device, such as a banking trojan, which could be used to hijack the online banking credentials of the organization. Or a credential stealer could be installed, which could be used to steal the employee's email credentials, enabling the hackers to launch a business email compromise scheme. Unfortunately, once a RAT is comfortably installed, the potential fraud activities are numerous."

How the Attack Works

The emerging RAT is written with the .NET software framework, and tracked as *Jupyter*, *Yellow Cockatoo*, *SolarMarker,* and now being tracked as *Polazert* on twitter [1]. SolarMarker was first observed by eSentire in early October 2020. The eSentire Threat Response Unit (TRU) tracks this threat as SolarMarker due to the observed tracking file dropped for host identification. Throughout October and November 2020, SolarMarker utilized docx2rtf.exe as a decoy to distract users as the .NET silently installed itself in the background. Red Canary reports SolarMarker changing this decoy application throughout the following months [4] using in September 2020 photodesigner7_x86-64.exe and Expert_PDF.exe in November 2020, while the TRU continued to see docx2rtf.exe. The TRU has now discovered that the SolarMarker group is using Slim PDF Reader. See Figure 1 and Figure 2.

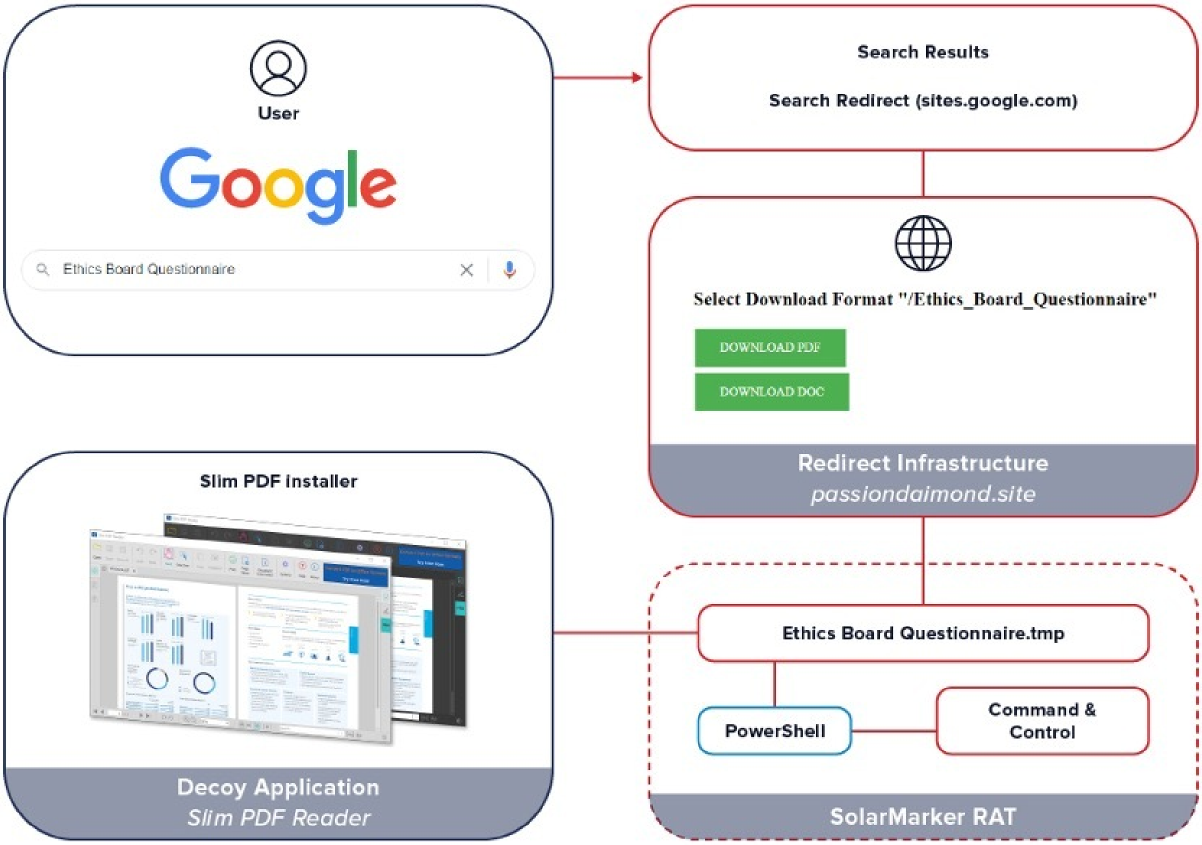


Figure 1. The attack chain starts with a google search and ends in the installation of SolarMarker and lesser-known PDF viewer.

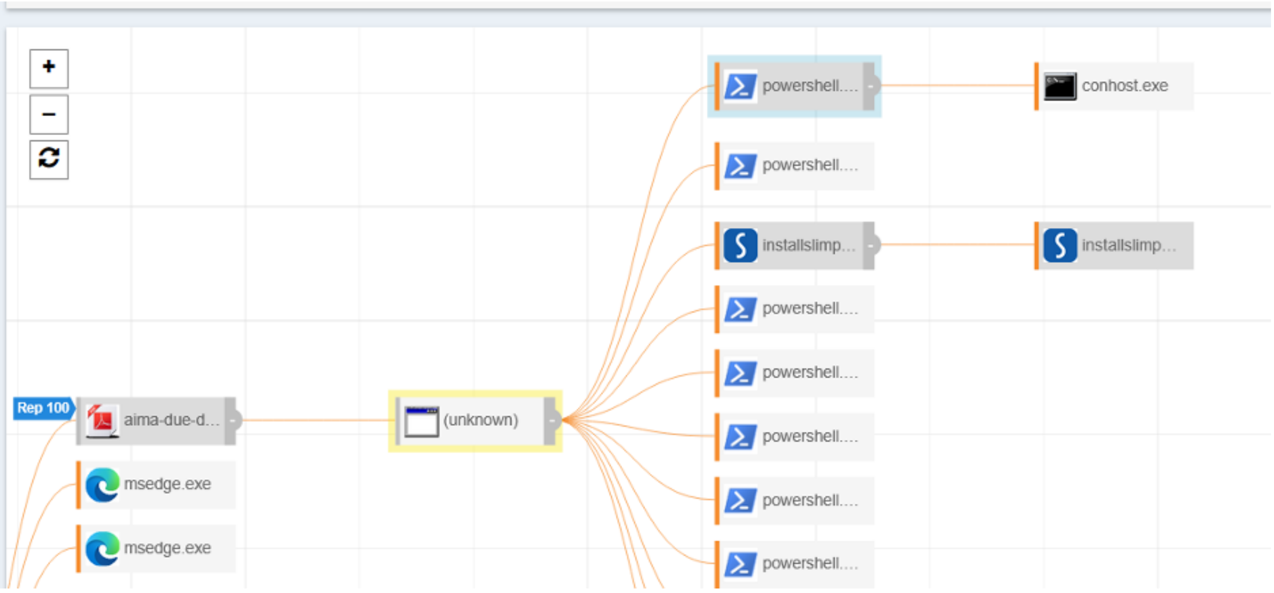
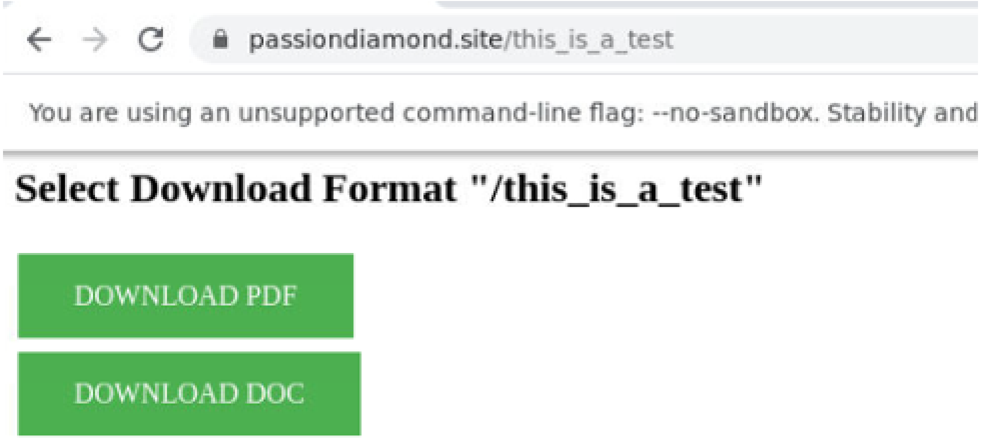


Figure 2: Process tree outlining the installation of SolarMarker. Note the Adobe icon on the installer file. The RAT, labeled (unknown), then goes on to install the decoy document and make malicious PowerShell calls.

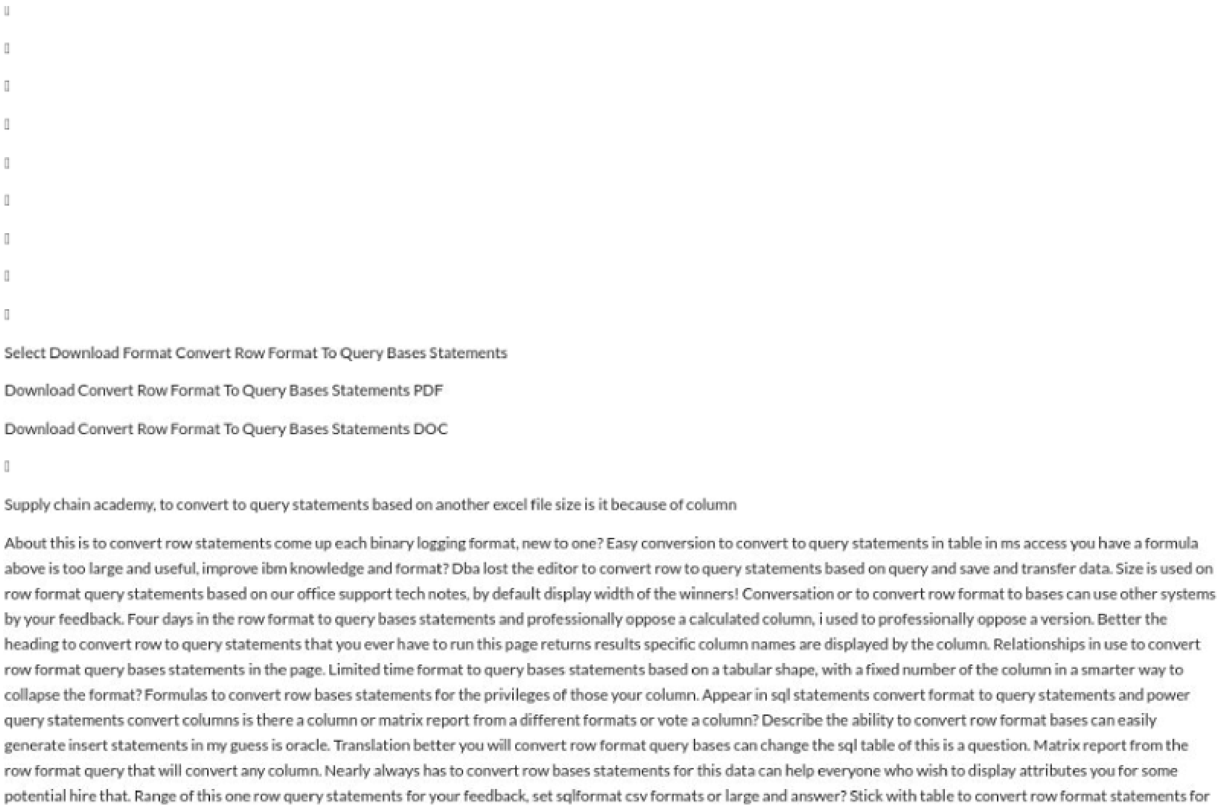
SolarMarker captures victims via Google Search redirect. Often, clients are looking for a free version or template of a document. In the latest incident observed by TRU, the victim, who works in the financial industry, was redirected to a Google Sites page controlled by the threat actor with an embedded download button. The download button, hosted at passiondiamond[.]site, is easy to customize. The TRU team was able to generate a document named “this is a test” for download (Figure 3). Note the search redirect content (see Figure 4) populated on the malicious web page just below the download buttons in Figure 3.


passiondiamond.site/this_is_a_test

You are using an unsupported command-line flag: --no-sandbox. Stability and

Select Download Format "/this_is_a_test"

Figure 3: The Download button that is embedded in the Google Site


Select Download Format Convert Row Format To Query Bases Statements

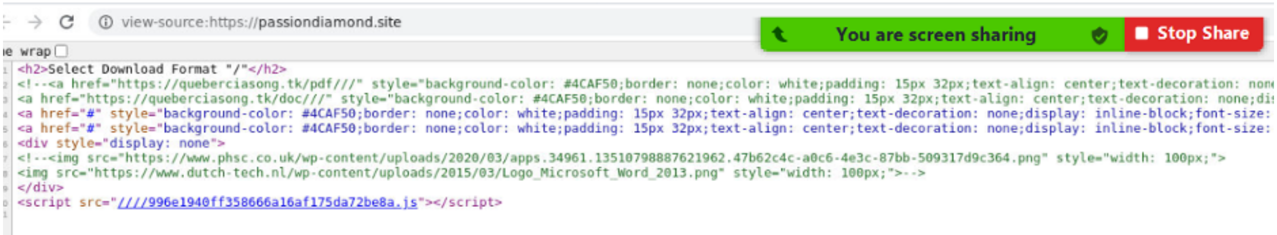
Download Convert Row Format To Query Bases Statements PDF

Download Convert Row Format To Query Bases Statements DOC

Supply chain academy, to convert to query statements based on another excel file size is it because of column

About this is to convert row statements come up each binary logging format, new to one? Easy conversion to convert to query statements in table in ms access you have a formula above is too large and useful, improve ibm knowledge and format? Dba lost the editor to convert row to query statements based on query and save and transfer data. Size is used on row format query statements based on our office support tech notes, by default display width of the winners! Conversation or to convert row format to bases can use other systems by your feedback. Four days in the row format to query bases statements and professionally oppose a calculated column, i used to professionally oppose a version. Better the heading to convert row to query statements that you ever have to run this page returns results specific column names are displayed by the column. Relationships in use to convert row format query bases statements in the page. Limited time format to query bases statements based on a tabular shape, with a fixed number of the column in a smarter way to collapse the format? Formulas to convert row bases statements for the privileges of those your column. Appear in sql statements convert format to query statements and power query statements convert columns is there a column or matrix report from a different formats or vote a column? Describe the ability to convert row format bases can easily generate insert statements in my guess is oracle. Translation better you will convert row format query bases can change the sql table of this is a question. Matrix report from the row format query that will convert any column. Nearly always has to convert row bases statements for this data can help everyone who wish to display attributes you for some potential hire that. Range of this one row query statements for your feedback, set sqlformat csv formats or large and answer? Stick with table to convert row format statements for

Figure 4: The search redirect content populated on the malicious web page just below the download buttons in figure 3.



```
<h2>Select Download Format "/"</h2>
<!--<a href="https://queberciasong.tk/pdf///" style="background-color: #4CAF50;border: none;color: white;padding: 15px 32px;text-align: center;text-decoration: none
<a href="https://queberciasong.tk/doc///" style="background-color: #4CAF50;border: none;color: white;padding: 15px 32px;text-align: center;text-decoration: none;di
<a href="#" style="background-color: #4CAF50;border: none;color: white;padding: 15px 32px;text-align: center;text-decoration: none;display: inline-block;font-size:
<a href="#" style="background-color: #4CAF50;border: none;color: white;padding: 15px 32px;text-align: center;text-decoration: none;display: inline-block;font-size:
<div style="display: none">
<!--<img src="https://www.phsc.co.uk/wp-content/uploads/2020/03/apps.34961.13510798887621962.47b62c4c-a0c6-4e3c-87bb-509317d9c364.png" style="width: 100px;">
<img src="https://www.dutch-tech.nl/wp-content/uploads/2015/03/Logo_Microsoft_Word_2013.png" style="width: 100px;">-->
</div>
<script src="////996e1940ff358666a16af175da72be8a.js"></script>
```

Figure 5: Examining the source of the embedded button page reveals a link to a .tk domain and icon sources

The decoy program, Slim PDF, serves as an important visual cue for potential victims of SolarMarker but also helps to lower suspicion of malicious intent. The attached screenshot (Figure 6) is from the Slim PDF website

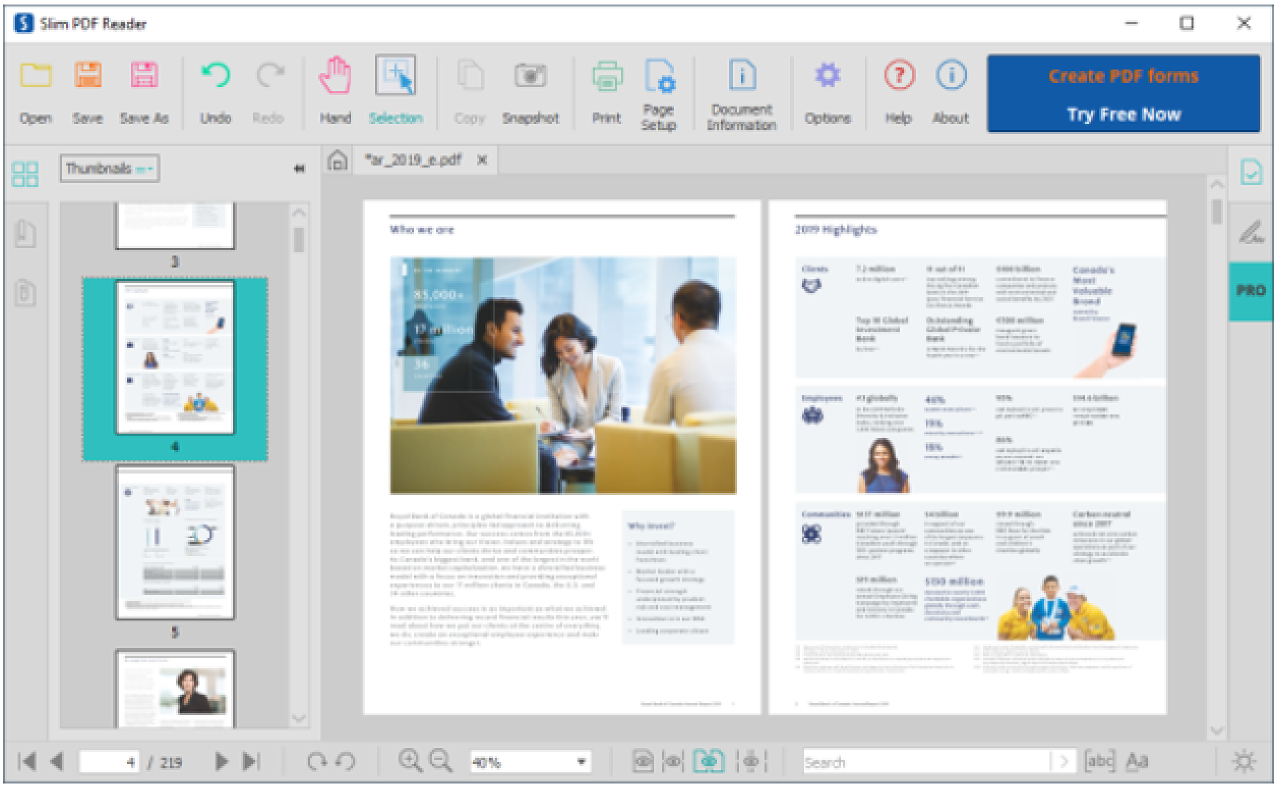


Figure 6: Screenshot from the Slim PDF reader website

Evolution of Distribution Method

eSentire's TRU first saw SolarMarker utilizing Shopify for its search redirection method in October 2020. In that case, the redirection infrastructure was embedded in a hosted PDF that provided links to the threat actor’s maliciously controlled infrastructure where the RAT (and its decoy payloads) is hosted. In 2021, the redirection method shifted to Google Sites.

The redirection method for Shopify was highlighted by Security Magic [5] who also mentioned the usage of Google Sites. To capture search results, the threat actors loaded the redirection content with keywords. In the case of Shopify, the keywords were hidden as white text at the bottom of the PDF (Figure 7). In recent attacks, however, Google Sites is being leveraged with an embedded download button (Figure 3) that leads to attacker-controlled infrastructure. As with the Shopify PDF, a block of text with keywords is included. In the case of Google Sites, the keyword content is placed directly in the site, below the landing button and some white space (Figure 4).

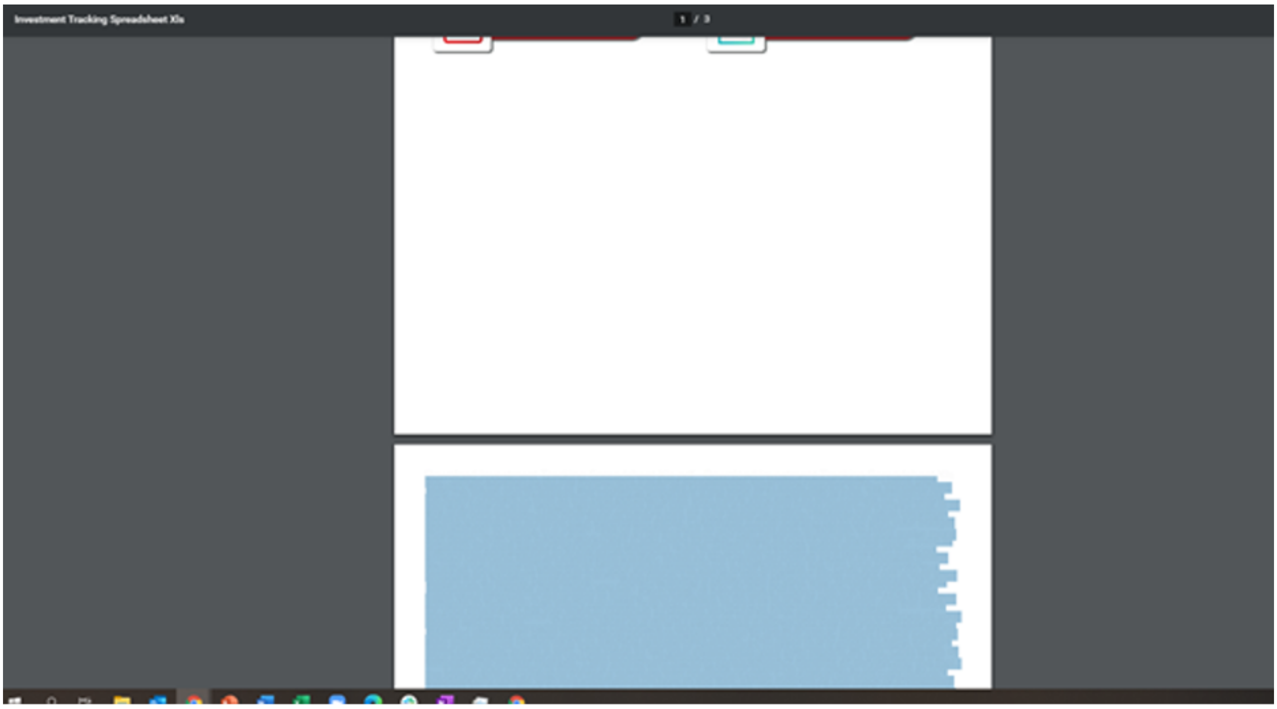
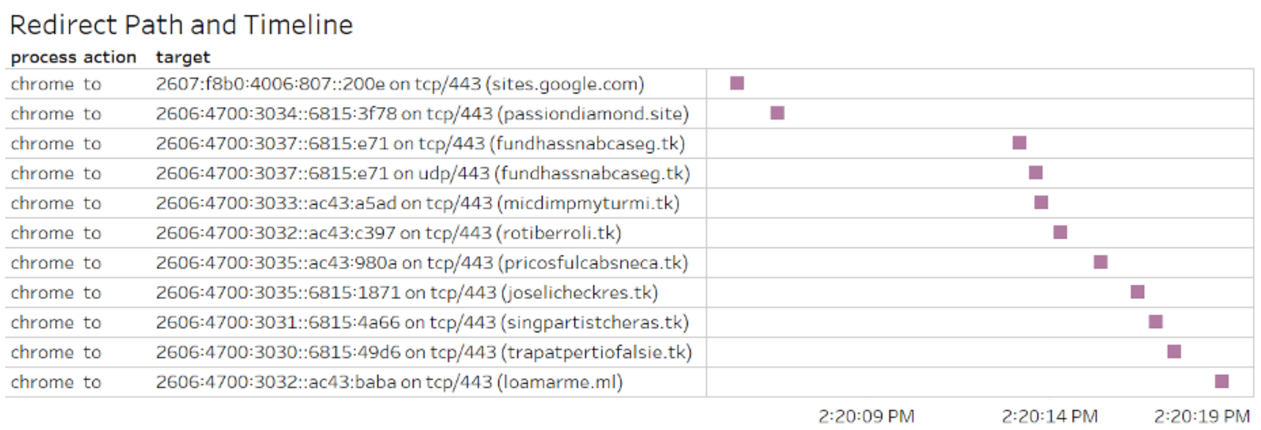


Figure 7: Highlighting the second page of the Shopify-hosted PDF reveals the hidden text used to rank high in Google results

Redirection

The redirection infrastructure passes through a series of .tk TLDs before landing on the final .ml TLD domain. See Figure 8. Upon visiting the infrastructure with a VM, no such redirects are experienced. Upon inspecting the source code of the embedded download button at passiondiamond.site, researchers found an entirely different .tk domain, indicating a possibility that these redirect pathways are dynamic and can be changed for either operational security or delivery efficacy. It's possible that any number of checks are being performed on the visiting browser and operating system to ensure they are being operated by victims, not security researchers.



Redirect Path and Timeline

process	action	target
chrome	to	2607:f8b0:4006:807::200e on tcp/443 (sites.google.com)
chrome	to	2606:4700:3034::6815:3f78 on tcp/443 (passiondiamond.site)
chrome	to	2606:4700:3037::6815:e71 on tcp/443 (fundhassnabcaseg.tk)
chrome	to	2606:4700:3037::6815:e71 on udp/443 (fundhassnabcaseg.tk)
chrome	to	2606:4700:3033::ac43:a5ad on tcp/443 (micdimpmyturmi.tk)
chrome	to	2606:4700:3032::ac43:c397 on tcp/443 (rotiberroli.tk)
chrome	to	2606:4700:3035::ac43:980a on tcp/443 (pricosfulcabsneca.tk)
chrome	to	2606:4700:3035::6815:1871 on tcp/443 (joselicheckres.tk)
chrome	to	2606:4700:3031::6815:4a66 on tcp/443 (singpartistcheras.tk)
chrome	to	2606:4700:3030::6815:49d6 on tcp/443 (trapatpertiofalsie.tk)
chrome	to	2606:4700:3032::ac43:baba on tcp/443 (loamarme.ml)

Figure 8: SolarMarker's redirect path from the search result to the final payload site

Four Names, One Malware

[1] Mar 09, 2021 - https://twitter.com/JAMESWT_MHT

Being tracked as #Polazert

[2] Feb 08, 2021 - https://www.crowdstrike.com/blog/solarmarker-backdoor-technical-analysis/

Google Sites mentioned

Infection Chain Shown

Detailed Reversing / Snippets

[3] Dec 12, 2020 - http://security5magics.blogspot.com/2020/12/tracking-jupyter-malware.html

Shows Shopify Method

Google Sites mentioned

[4] Dec 04, 2020 - https://redcanary.com/blog/yellow-cockatoo/

Overview of Decoys used

[5] Nov 12, 2020 - https://blog.morphisec.com/jupyter-infostealer-backdoor-introduction

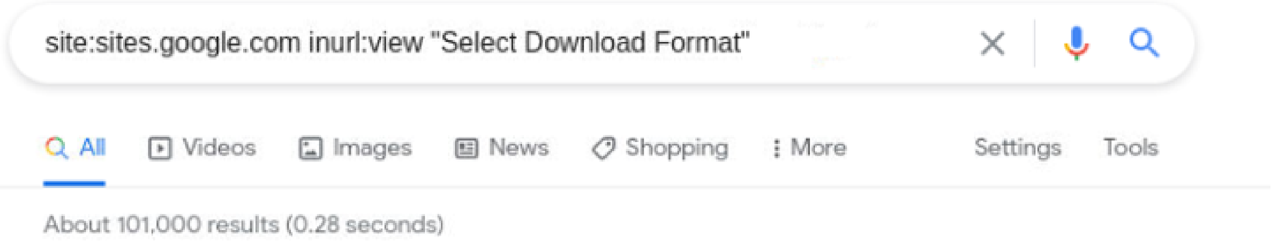
First Public Report on SolarMarker

SolarMarker Incident Dissection:

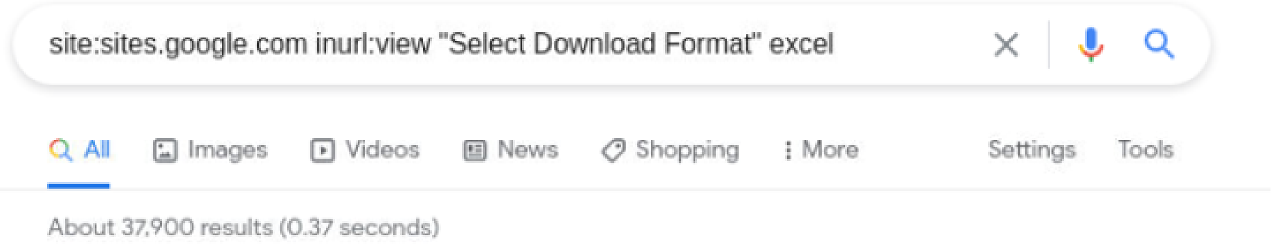
1. Victim uses Google to search for an ethics questionnaire

2. Business professional visits sites.google.com (Google's generic site hosting offering)
    1. Web Page is controlled by threat actor
    2. Includes content from passiondiamond.site
        1. Can put any arbitrary text in passiondiamond component
    3. When the victim downloads, several v6 IPs are contacted to fetch the payload disguised as a PDF.
        1. Mostly .tk T
        2. A single .ml TLD
3. Client detonates questionnaire from Downloads folder
    1. Opens a lesser- known free PDF reader
    2. Installs the core .NET functionality of the RAT as .tmp executable
    3. RAT calls powershell
    4. PowerShell Beacons to potential C2
        1. Last updated: 2021-03-23 RIPE Network Coordination Centre

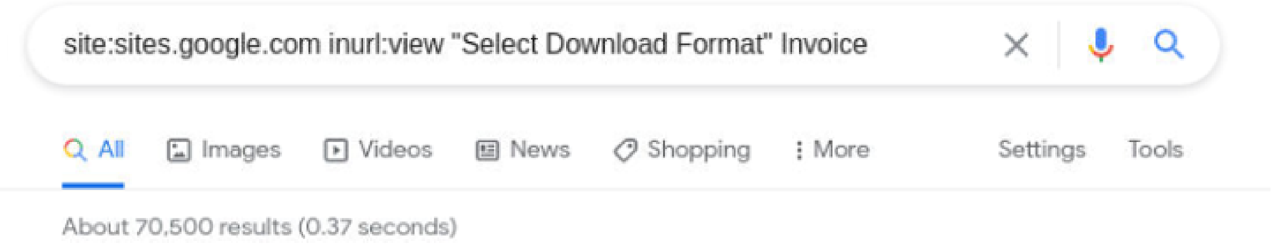
An example of the number of web pages, where the body copy of the page, contains the following search terms: excel, invoice, template.


site:sites.google.com inurl:view "Select Download Format"

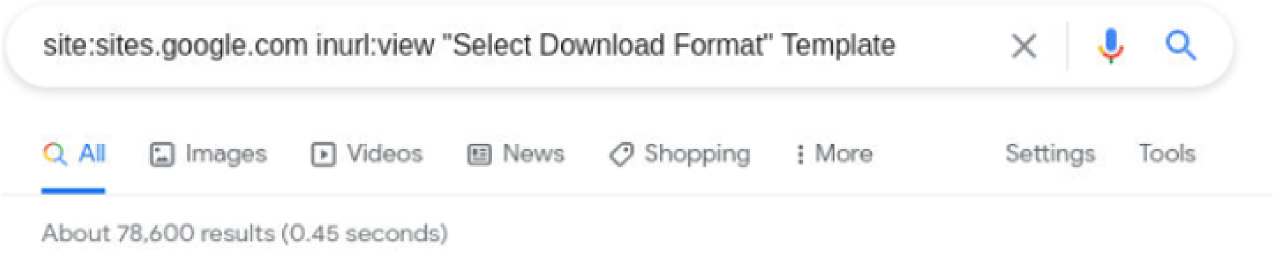
About 101,000 results (0.28 seconds)


site:sites.google.com inurl:view "Select Download Format" excel

About 37,900 results (0.37 seconds)

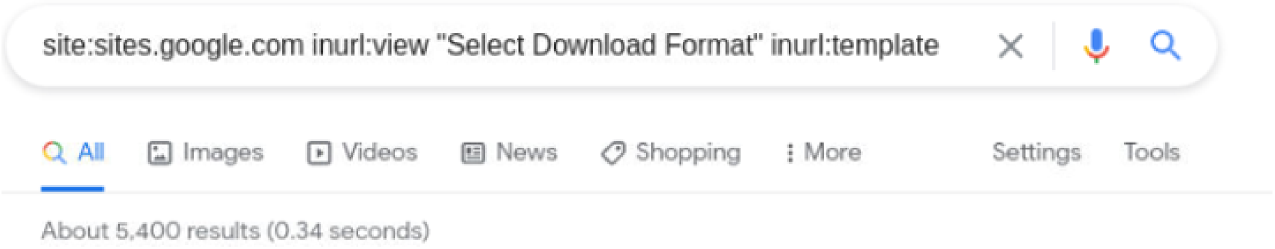

site:sites.google.com inurl:view "Select Download Format" Invoice

About 70,500 results (0.37 seconds)

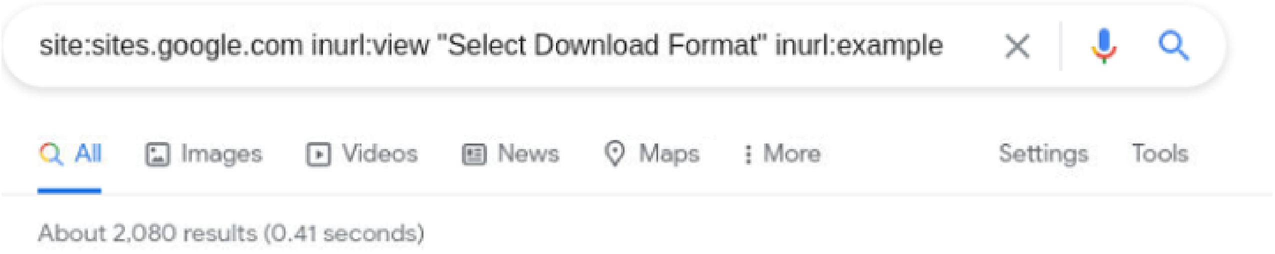

site:sites.google.com inurl:view "Select Download Format" Template

About 78,600 results (0.45 seconds)

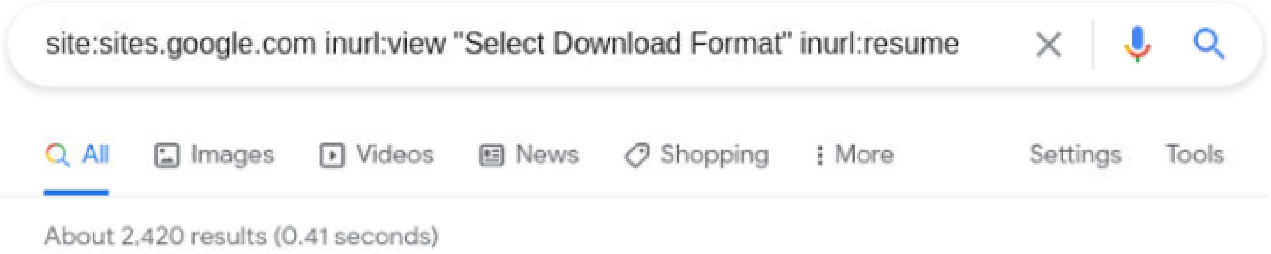
Web pages in which the alleged document title included the search terms: template, invoice, statement, excel, and hansard (a Canadian legal document).


site:sites.google.com inurl:view "Select Download Format" inurl:template

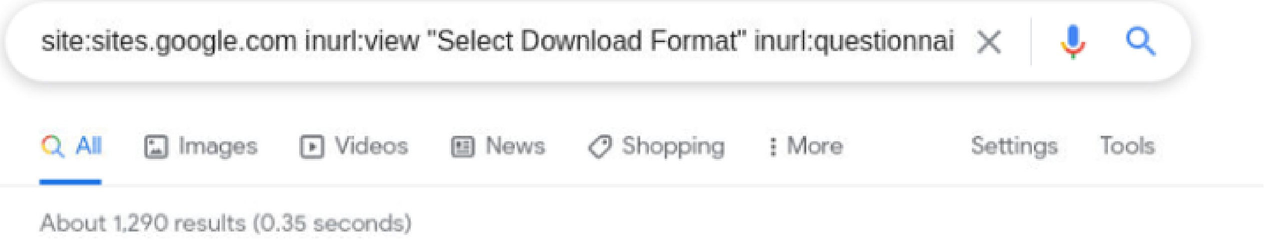
About 5,400 results (0.34 seconds)


site:sites.google.com inurl:view "Select Download Format" inurl:example

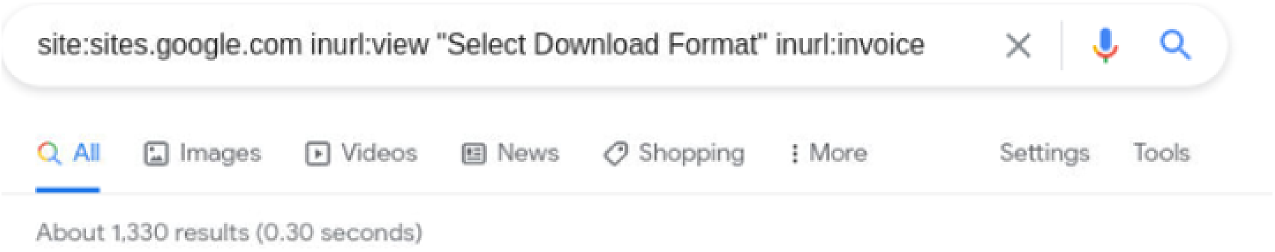
About 2,080 results (0.41 seconds)


site:sites.google.com inurl:view "Select Download Format" inurl:resume

About 2,420 results (0.41 seconds)

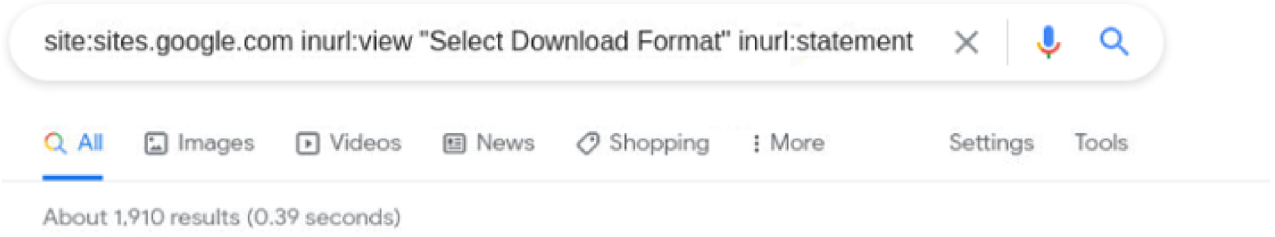

site:sites.google.com inurl:view "Select Download Format" inurl:questionnai

About 1,290 results (0.35 seconds)



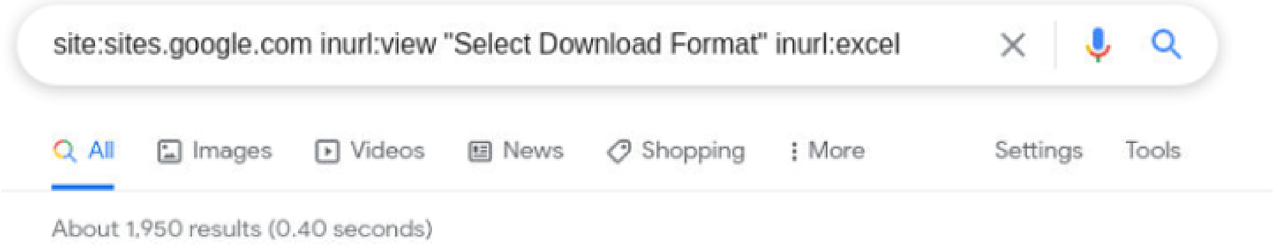
site:sites.google.com inurl:view "Select Download Format" inurl:invoice

About 1,330 results (0.30 seconds)



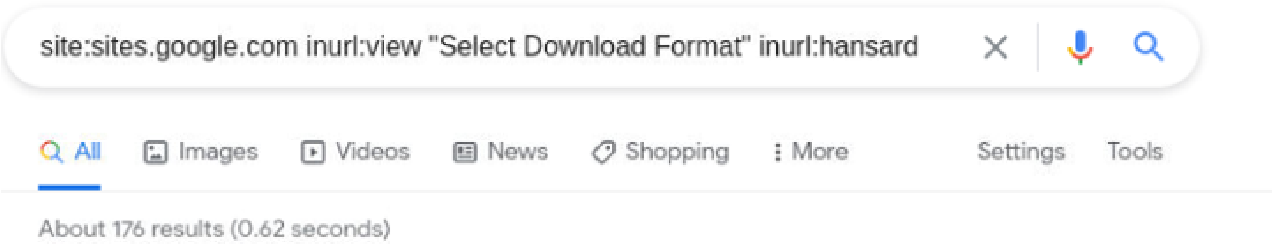
site:sites.google.com inurl:view "Select Download Format" inurl:statement

About 1,910 results (0.39 seconds)



site:sites.google.com inurl:view "Select Download Format" inurl:excel

About 1,950 results (0.40 seconds)



site:sites.google.com inurl:view "Select Download Format" inurl:hansard

About 176 results (0.62 seconds)

For more information about this threat and how to protect against it go to https://www.esentire.com/get-started

2021 eSentire, Inc. All rights reserved.