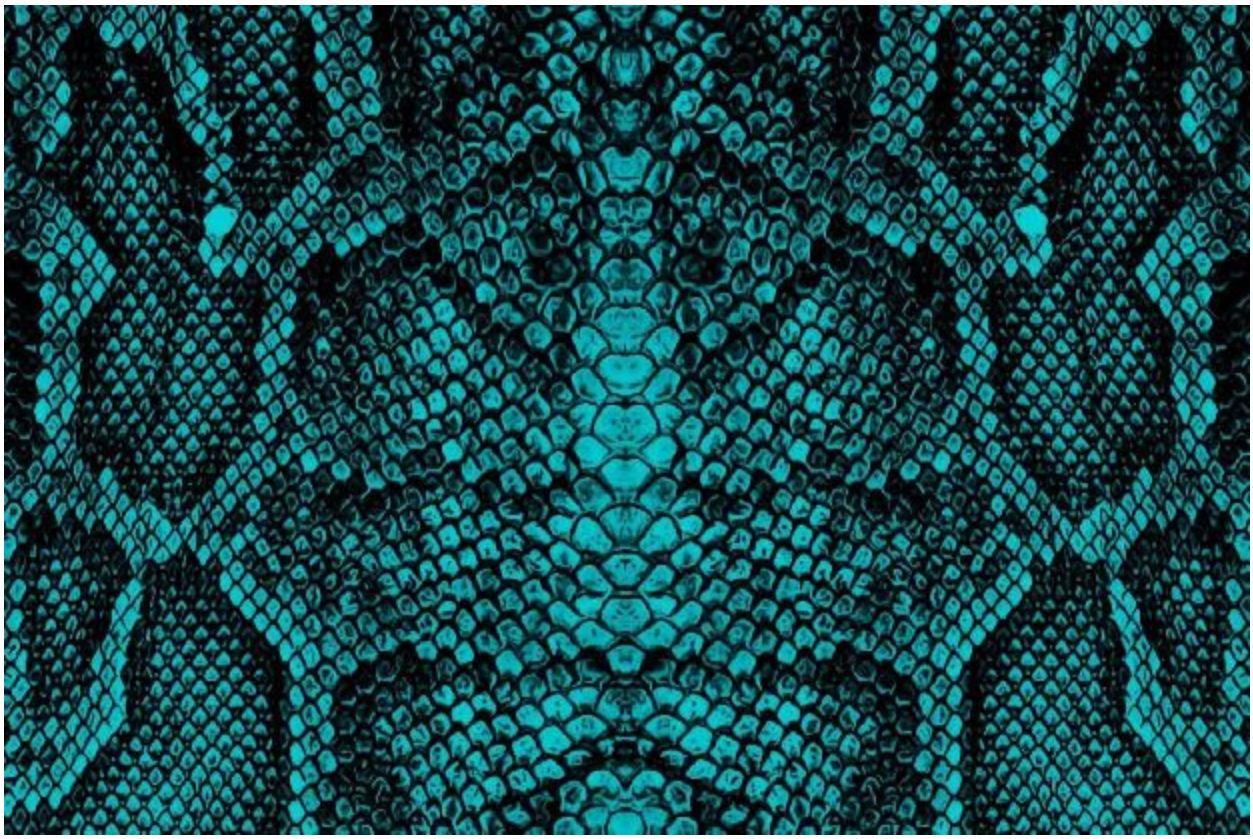
IISerpent: Malware-driven SEO fraud as a service

welivesecurity.com/2021/08/11/iiserpent-malware-driven-seo-fraud-service/

August 11, 2021



The last in our series on IIS threats introduces a malicious IIS extension used to manipulate page rankings for third-party websites

Zuzana Hromcová
11 Aug 2021 - 11:30AM

The last in our series on IIS threats introduces a malicious IIS extension used to manipulate page rankings for third-party websites

ESET researchers have discovered and analyzed a previously undocumented server-side trojan that manipulates search engine results by hijacking the reputation of the websites it compromises. We named the trojan IISerpent to highlight its two main features: being implemented as a malicious extension for *Internet Information Services* (IIS) web server, and using shady techniques to manipulate *search engine result pages* (SERPs). IISerpent's operators use a variety of techniques for *search engine optimization* (SEO), in an attempt to improve page ranking for third-party websites – likely the paying customers of these criminals.

This blogpost is the last installment in our series where ESET researchers put IIS web server threats under the microscope – the previous parts discuss IIS malware used for cybercrime and cyberespionage. For a comprehensive guide on how to detect, analyze and remove IIS malware, refer to our white paper Anatomy of native IIS malware, where IISerpent is featured as one of the studied families (Group 13).

Anatomy of native IIS malware

Download Research Paper

Attack overview

IISerpent is implemented, and configured, as a malicious extension for IIS – Microsoft's web server software. That allows the malware to intercept all HTTP requests made to the websites hosted by the compromised server, but also to actively change the server's HTTP responses. In the previous installments of this series, we discussed how other IIS malware families leverage these powers – for example, to steal credit card information from e-commerce website customers (IIStealer), or to execute backdoor commands on the compromised IIS server (IISpy).

Contrary to those families, IISerpent directly affects neither the compromised server nor the server's users – in fact, this malware completely ignores all requests coming from legitimate visitors of the compromised websites. The malware listens to and parses all HTTP requests sent to the compromised server, only to search for those originating from specific search engine crawlers. As shown in Figure 1, IISerpent relays these requests to its C&C server (or uses its local configuration) to modify the content served to these crawlers.

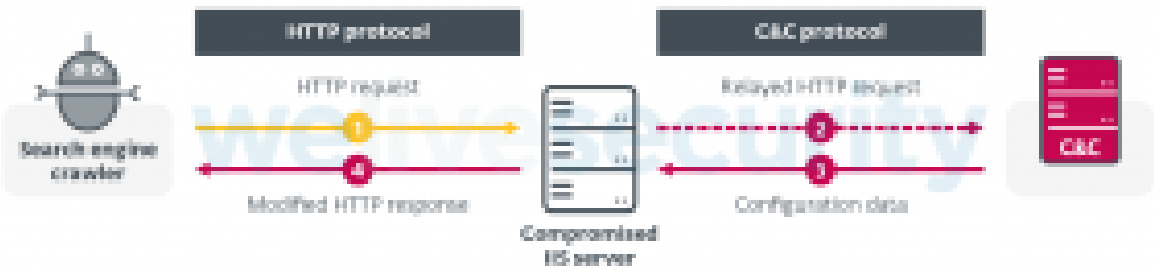


Figure 1. IISerpent operating mechanism

SEO fraud

What is the purpose of this scheme? Search engines regularly crawl the internet, and then index (record) all the content found online, building associations between search terms and the content and using various algorithms to calculate rankings of the results for particular search terms.

Various legitimate techniques can be used to increase page ranking in search engine result pages – buying advertisements or employing *search engine optimization* (SEO) strategies – but not all digital marketers play by the rules. The term *unethical SEO* (historically known as black hat SEO) refers to SEO-boosting techniques (which, however, violate webmaster guidelines), such as loading pages with irrelevant keywords, or buying backlinks to increase a website's reputation.

IISerpent's attack pattern uses some of these unethical SEO techniques, and could be best described as "SEO fraud as a service" – as it employs SEO fraud techniques on compromised IIS servers for the benefit of a third party without webmaster consent. IISerpent's operators use this malware to boost page ranking for third-party websites by leeching off the compromised website's ranking and by employing the following techniques:

- Redirecting the search engines to the particular website chosen by the attacker, effectively making the compromised website a doorway page
- Injecting a list of backlinks (pre-configured or obtained from the C&C server on the fly) into the HTTP response for search engine crawlers, making the servers compromised by IISerpent something of a link farm

In an example scenario shown in Figure 2, an adversary compromises a number of IIS servers with IISerpent, and uses its capabilities to inject backlinks to all websites hosted by these servers. Websites 1 – N are legitimate, with good reputations; from the perspective of a search engine crawler, they all link to a third-party website of the attacker's choice (in this case, a scam website). As a result, the scam website may seem more popular – since it is referenced by reputable websites – which may boost its page ranking.

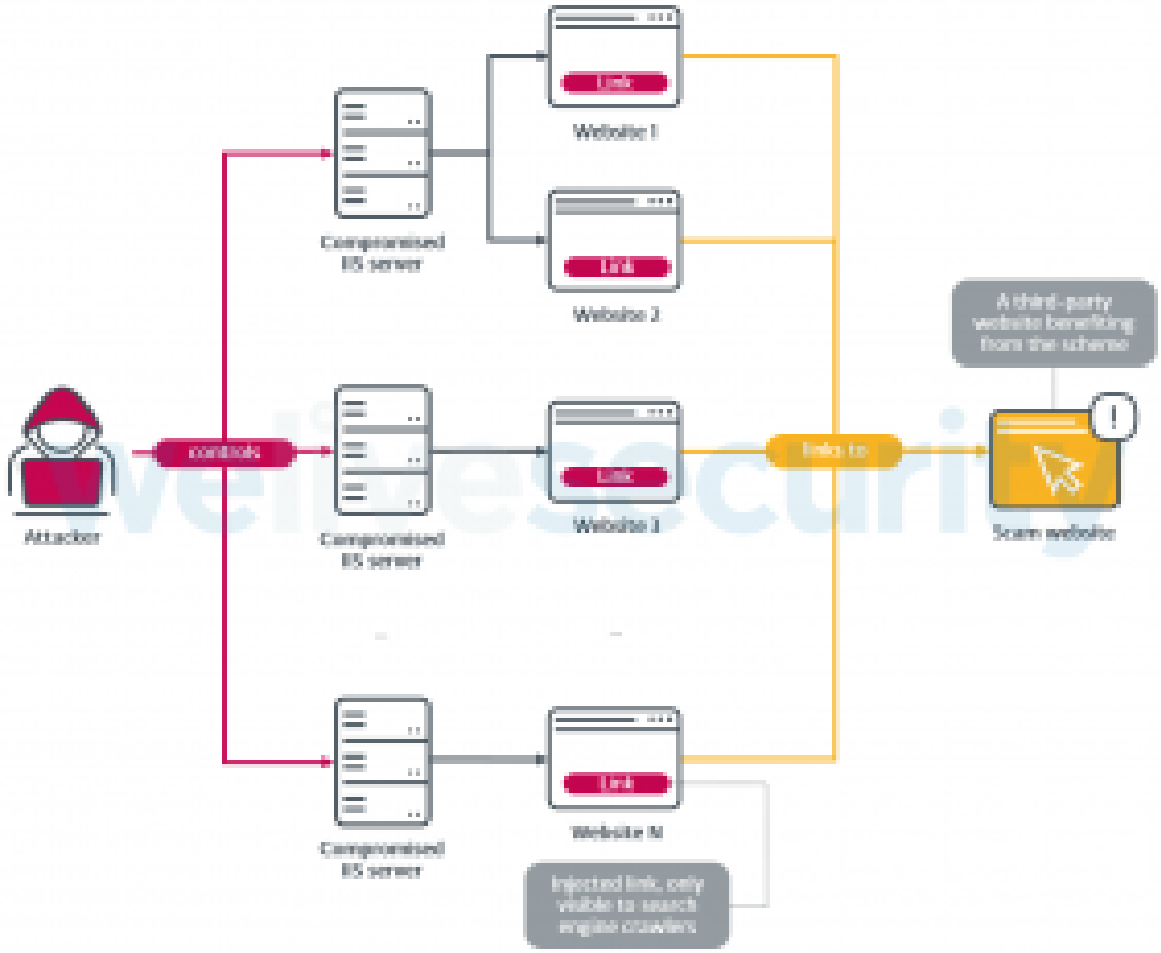


Figure 2. Example of an SEO fraud mechanism

Note that the legitimate visitors of the compromised server will still be served the expected content, so the users and the webmaster may fail to notice that something is wrong with the server. This sets IISerpent apart from other malware families that inject artificial backlinks into compromised sites – by operating as a server extension, IISerpent can reserve these modifications for the search engine crawlers, without interfering with content served to standard visitors (as opposed to permanently modifying the compromised website by adding the undesired backlinks for all its visitors to see).

Of course, the misused websites hosted on the compromised IIS servers do not benefit at all in this scheme – on the contrary, it is against the webmaster guidelines to fool the search engine crawlers by displaying a different version of the website to them than the one shown to the regular visitors, and so these websites could even end up penalized by the search engines, lowering *their* SEO statistics.

Technical analysis

Under its skin, IISerpent is a native IIS module – implemented as a C++ DLL and configured in the %windir%\system32\inetsrv\config\ApplicationHost.config file. That way, IISerpent secures both persistence and execution, as all IIS modules are loaded by the IIS

Worker Processes (w3wp.exe) and used to handle inbound HTTP requests.

We don't have any information about how IISerpent's operators initially penetrate IIS servers, but we know that administrative privileges are required to configure it as a native IIS module, which reduces the number of plausible scenarios. A configuration weakness or vulnerability in a web application or the server are likely culprits.

As with all native IIS modules, IISerpent exports a function called RegisterModule (see Figure 3), which implements the module initialization. The core malicious functionality is hidden in its *event handlers* – methods of the module class (inherited from CHttpModule) that are called on certain *server events*. More specifically, IISerpent's code class overrides its OnBeginRequest and OnSendResponse methods, which means that the malware's handlers will be called every time the IIS server starts processing a new inbound HTTP request, and every time it sends the response buffer.

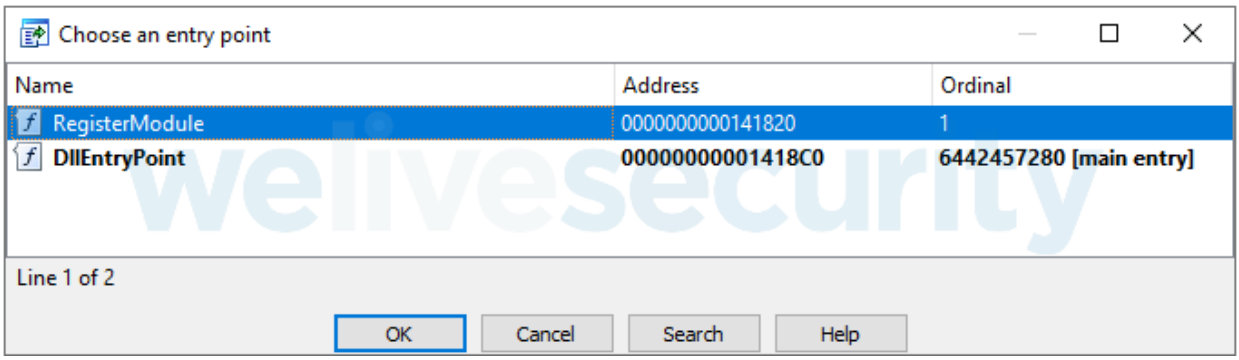


Figure 3. IISerpent's DLL exports

IISerpent parses the incoming requests and uses its complex configuration data to manipulate content served to search engine crawlers. As Table 1 lists in full, the configuration includes fields such as a redirect URL, or a list of backlinks to be injected. The attackers can display or update the malware's configuration by sending any HTTP request to the compromised IIS server with the query parameter ?DisplayModuleConfig=1 or ?ReloadModuleConfig=1, respectively, in the request URI.

Upon receiving the update request, IISerpent obtains the configuration from the C&C server by sending an HTTP GET request to this URL:

http://sb.qrfy[.]net/mconfig/<host>.xml

The value <host> is taken from the original attacker request, and it is probably used as a victim ID. The libcurl library is used for the network communication.

Table 1. Configuration fields used by IISerpent

Configuration field	Comment

Configuration field	Comment
banip	List of IP addresses. The malware ignores HTTP requests from these IP addresses.
redirectreferer	Binary flag – set if the malware should handle requests with the strings spider, bot or baidu.com/ in the Referer header.
onlymobilespider	Binary flag – set if the malware should only handle crawler requests with the strings Android or AppleWebKit in the Referer header.
redirect	If these values are set, the malware will redirect all crawler requests to the configured URL via an HTTP 301 response.
redirecturl	
proxy	If these values are set, the malware will forward the search engine crawler requests to its C&C server, and replace the HTTP response with the obtained data, instead of redirecting the crawlers to a malicious URL directly.
proxyurl	
proxymode	
folderlink	If these values are set, the malware will add all of them as backlinks to the response for any HTTP request with the strings spider or bot in the User-Agent header.
folderlinkcount	
folderlinkpath	
proxyfolder	
locallink	
locallinkext	
locallinkfolder	
locallinkcount	

IISerpent recognizes search engine crawler requests by parsing the User-Agent header and looking for specific substrings, as seen in Figure 4. If the redirecturl field is configured, the malware redirects all requests with the strings spider or bot in the User-Agent header to this URL by setting the Location header in the HTTP response. The HTTP status is set to 301 (“Moved Permanently”).

```
.text:10009AE7                  mov     eax, [esi]
.text:10009AE9                  mov     ecx, esi
.text:10009AEB                  mov     edx, [eax+IHttpContextVtbl.GetRequest]
.text:10009AEE                  call    edx
.text:10009AF0                  mov     edi, eax
.text:10009AF2                  mov     eax, [edi]
.text:10009AF4                  push    0
.text:10009AF6                  push    offset aUserAgent ; "User-Agent"
.text:10009AFB                  mov     ecx, edi
.text:10009AFD                  mov     edx, [eax+IHttpRequestVtbl.GetHeader]
.text:10009B00                  call    edx
.text:10009B02                  push    eax             ; Source
.text:10009B03                  lea     ecx, [ebp+userAgentHeaderValue] ; Dest
.text:10009B06                  call    copyString
.text:10009B06 ;   } // starts at 10009A9E
.text:10009B0B ;   try {
.text:10009B0B                  mov     byte ptr [ebp+res], 1
.text:10009B0F                  push    0
.text:10009B11                  push    offset aSpider  ; "spider"
.text:10009B16                  lea     ecx, [ebp+userAgentHeaderValue] ; Str
.text:10009B19                  call    findSubstring
.text:10009B1E                  cmp     eax, -1
.text:10009B21                  jnz     short redirectToUrl
.text:10009B23                  push    0
.text:10009B25                  push    offset aBot     ; "bot"
.text:10009B2A                  lea     ecx, [ebp+userAgentHeaderValue] ; Str
.text:10009B2D                  call    findSubstring
.text:10009B32                  cmp     eax, -1
.text:10009B35                  jnz     short redirectToUrl
.text:10009B35 ;   } // starts at 10009B0B
```

Figure 4. IISerpent recognizes search engine crawler requests by parsing the User-Agent header

If proxymode is set, instead of redirecting the crawlers to a malicious URL, IISerpent forwards the crawler request to its C&C server proxyurl, and replaces the HTTP response body with the acquired data. This is applied to all the HTTP requests with spider, bot or baidu.com/ in the Referer header, or optionally to requests with the strings Android or AppleWebKit in the Referer header. Additionally, the malware can be configured to:

- Only handle those HTTP requests where the IIS server has set the response status to 404
- Ignore requests coming from a configurable list of banned IP addresses

Finally, IISerpent can have a list of links configured and add these links to the HTTP response body for any search engine crawler requests. These links are added as HTML entities to the existing HTTP response body:

<a href='/<link><timestamp1>_<timestamp2>_<randomId>.html'>

Other notable serpents

IISerpent is not the only known malicious IIS module with SEO fraud capabilities – out of the 14 malware families we analyzed for our paper *Anatomy of native IIS malware*, six have support for SEO fraud techniques. In these families, the SEO fraud functionality is often bundled with other malicious capabilities (such as backdoor support, or serving malicious content to legitimate website visitors).

While we first detected IISerpent in May 2021, we were able to trace the SEO fraud phenomenon to the first publicly known case in 2019, when Secpulse published an incident report in Chinese on unnamed malware affecting IIS servers. The analysis of that malware and its SEO fraud capabilities is featured in our white paper under the Group 9 category.

The various SEO fraud families that we analyzed differ in the unethical SEO techniques supported, and target a wide range of search engine crawlers – specified in the clear (Group 12 in the paper, as shown in Figure 5), as an encrypted list (Group 9), or obtained on the fly by querying DNS TXT records of the C&C server hostname (Group 11). All these families are detected by ESET security solutions as Win32/BadIIS.

```
aIfengIvcSogouS db 'ifeng|ivc|sogou|so.com|baidu|google|youdao|yahoo|bing|118114|biso'
                                        ; DATA XREF: CHttpModule_OnBeginRequest+293↑o
                                        ; CHttpModule_OnBeginRequest+110B↑o
                db '|gougou|sooule|360|sm|uc',0
                align 10h
aSogouSoComBaid db 'sogou|so.com|baidu|google|youdao|yahoo|bing|gougou|sooule|360|sm.'
                db 'cn|uc',0
                align 8
aHotcssHotjs    db 'Hotcss/|Hotjs/',0   ; DATA XREF: CHttpModule_OnBeginRequest+47D↑o
                                        ; CHttpModule_OnBeginRequest:loc_180004208↑o
                align 8
aHotimgHotpic   db 'HotImg/|HotPic/',0  ; DATA XREF: CHttpModule_OnBeginRequest:loc_1800042CF↑o
                                        ; CHttpModule_OnBeginRequest:loc_1800042FA↑o ...
                dq offset aOoooo        ; "                 _ooOoo_                 "...
                dq offset aO8888888o    ; "                o8888888o                "...
                dq offset a8888         ; "                88* . *88                "...
                dq offset asc_1800211D8 ; "                (| -_- |)                "...
                dq offset aOO           ; "                O\\ = //O                "...
                dq offset asc_180021238 ; "             ___//`---'\\____             "...
                dq offset asc_180021268 ; "           .   ' \\| |// `.               "...
                dq offset asc_180021298 ; "          // \\||| : ||// \\              "...
                dq offset asc_1800212C8 ; "        / / _||||| -:- |||||- \\           "...
                dq offset asc_1800212F8 ; "          | | \\  -  // | |               "...
                dq offset asc_180021328 ; "        | \\_| ''\\---//'' | |           "...
                dq offset asc_180021358 ; "        \\ .-\\__ `-` ___//-. //           "...
                dq offset asc_180021388 ; "      ___`. .' //--.--\\ `. . __          "...
                dq offset asc_1800213B8 ; "   . '< `.___\\_<|>_//___.' >'.           "...
                dq offset asc_1800213E8 ; "  | | : `- \\`.;`\\ _ //`;.`// - ` : |    "...
                dq offset asc_180021418 ; "    \\ \\ `-. \\_\t__\\ //__ _// .-` /    "...
                dq offset asc_180021448 ; "======`-.____`-.___\\_____//___.-`____.-`  "...
                dq offset asc_180021478 ; "                  `=---='                  "...
                dq offset asc_1800214A8 ; "                                           "...
                dq offset unk_1800214D8
                align 20h
```

Figure 5. Example of strings used to recognize search engine crawler requests by IIS malware

For a complete breakdown of these other IIS malware families, refer to our white paper.

Conclusion

IISerpent is a malicious IIS module with unusual targets and purpose, designed to aid in shady practices aimed at boosting the page rank of third-party websites. Even though it doesn't affect legitimate visitors of the compromised server, it nevertheless still deserves attention for distorting search results, and its potential for monetization.

On top of hijacking the reputation of the compromised websites, IISerpent can be a cause for headaches for the digital marketers, as any website participating in unethical SEO practices can be penalized by search engine algorithms. The best bet to prevent a compromise by IISerpent (and other IIS malware) is keeping your IIS servers up to date, and being careful not to download IIS extensions from untrusted sources – be especially aware of modules promising too-good-to-be-true features such as magically improving SEO. For additional protection, consider using a web application firewall, and/or a security solution on your IIS server.

Additional mitigation recommendations and Indicators of Compromise can be found in our comprehensive white paper, and on GitHub. For any inquiries, or to make sample submissions related to the subject, contact us at: threatintel@eset.com.

Indicators of Compromise (IoCs)

ESET detection names

Win32/BadIIS.H

SHA-1

D0F274EBD2A0636FEF9D9C48A7AC2FAD7B661653

Filename

stati.dll

Network indicators

URL query parameters

?DisplayModuleConfig=1
?ReloadModuleConfig=1

C&C server

http://sb.qrfy[.]net

MITRE ATT&CK techniques

Note: This table was built using version 9 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1587.001	Develop Capabilities: Malware	IISerpent is a custom-made malware family.
Execution	T1569.002	System Services: Service Execution	IIS server (and by extension, IISerpent) persists as a Windows service.
Persistence	T1546	Event Triggered Execution	IISerpent is loaded by the IIS Worker Process (w3wp.exe) when the IIS server receives an inbound HTTP request.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	Adversaries send HTTP requests with specific query parameters to the compromised IIS server to control IISerpent.
Impact	T1565.002	Data Manipulation: Transmitted Data Manipulation	IISerpent modifies content served by the compromised server to search engine crawlers.

11 Aug 2021 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion