Paper: C&C-As-A-Service

(https://labsblog.f-secure.com/2015/11/17/paper-cc-as-a-service/)

2015-11-17

SEAN SULLIVAN (HTTPS://LABSBLOG.F-SECURE.COM/AUTHOR/SEANSULLIVANFS/)

Artturi Lehtiö, (https://labsblog.f-secure.com/author/artturilehtiofs/) a researcher on our Threat Intelligence team, recently presented a paper on abusing third-party web services as C&C channels at VB2015 (https://www.virusbtn.com/conference/vb2015/index).

C&C-AS-A-SERVICE: ABUSING THIRD-PARTY WEB SERVICES AS C&C CHANNELS LEHTIÖ

C&C-AS-A-SERVICE: ABUSING THIRD-PARTY WEB SERVICES AS C&C CHANNELS

Artturi Lehtiö
F-Secure, Finland

Email artturi.lehtio@f-secure.com

ABSTRACT

A secure, reliable and undetectable method of communicating with and controlling malware is essential for modern malware operations. But designing, implementing and maintaining your own communication infrastructure isn't an easy task. Coincidentally, malware operators aren't the only ones interested in secure and reliable communication. Popular web services also want to provide their customers with a secure and reliable service. Add to that the fact that popular web services

Backdoor.Makadocs, which originally used HTTP to communicate with an attacker-operated web server. Later versions of the malware, however, do not connect directly to the malicious server. Instead, they route their traffic through *Google Docs* [1].

Google Docs has a little known feature called *Google Docs Viewer* that allows users to view documents or web pages from anywhere on the Internet via *Google Docs* (see Figure 1). Backdoor.Makadocs exploits this feature to essentially use *Google* as a proxy for its communications. Backdoor. Makadocs will connect to hxxps://docs.google.com/viewer?url=<actual C&C URL> where the URL of the actual Makadocs command-and-control server is passed as a parameter to *Google Docs Viewer*. *Google*'s service will then connect to the actual C&C URL, passing along any parameters specified by Makadocs, and display the C&C server's response back to Makadocs.

The end result of all this is increased anonymity, reliability and stealth for Makadocs' communications. Since the traffic to

(/)
(https://newsfromthelab.files.wordpress.com/2015/11/cc-as-a-service.png)

Here's the abstract:

> A secure, reliable and undetectable method of communicating with and controlling malware is essential for modern malware operations. But designing, implementing and maintaining your own communication infrastructure isn't an easy task. Coincidentally, malware operators aren't the only ones interested in secure and reliable communication. Popular web services also want to provide their customers with a secure and reliable service. Add to that the fact that popular web services generate large amounts of indistinguishable web traffic to blend into and it starts to sound irresistible. Unsurprisingly then, recent years have seen a growing trend among malware operators of abusing third-party web services such as Twitter, Facebook, and Gmail as command and control channels.
>
> This paper explores the multitude of ways in which modern malware abuses third-party web services as command and control channels. Through real life examples – from common cybercrime to targeted nation-state espionage – the paper provides a comprehensive overview of both the methods employed by malware and the web services most commonly abused. This paper further analyses the benefits and disadvantages that are provided to malware operators when they abuse third-party web services as command and control channels. Finally, this paper also examines the challenges that such methods pose to the detection and prevention of malware.

Slides from Artturi's presentation can be downloaded at Virus Bulletin (https://www.virusbtn.com/conference/vb2015/abstracts/R-Lehtio.xml).

And the paper from here: C&C-As-A-Service (https://newsfromthelab.files.wordpress.com/2015/11/cc-as-a-service.pdf). [PDF]

Tags:

#Cyb3r (https://labsblog.f-secure.com/tags/cyb3r/)

#Paper (https://labsblog.f-secure.com/tags/paper/)

#Virus Bulletin (https://labsblog.f-secure.com/tags/virus-bulletin/)

ARTICLES WITH SIMILAR TAGS

Oops!… Dell Did It Again

(https://labsblog.f-secure.com/2015/11/24/oops-dell-did-it-again/)

Bad news: Dell has installed a rogue root CA on customer PCs. Dell ships laptops...

2015-11-24

Security Cloud White Paper: How Do We Handle...

(https://labsblog.f-secure.com/2015/11/13/security-cloud-white-paper-how-do-we-handle-customer-data/)

How F-Secure Labs handles customer data is of the utmost importance for...

2015-11-13

Linux.Encoder.1: We Are Accept Only Bitcoins

(https://labsblog.f-secure.com/2015/11/10/linux-encoder-1-we-are-accept-only-bitcoins/)

There's a new crypto-ransom scheme currently in-the-wild targeting...

2015-11-10

Halloween RAT: NanoCore Served Via PageFair Service

(https://labsblog.f-secure.com/2015/11/02/halloween-rat-nanocore-served-via-pagefair-service/)

Over the weekend, PageFair, a counter ad-block solutions provider, was...

2015-11-02

The Contents Of This CryptoWall Zip File Cost $1,000

(https://labsblog.f-secure.com/2015/10/28/the-contents-of-this-cryptowall-zip-file-cost-1000/)

“Payment is made successfully.” This is CryptoWall’s Decrypter Service after ransom has...

2015-10-28

SLocker Versus Marshmallow

(https://labsblog.f-secure.com/2015/10/22/slocker-versus-marshmallow/)

Android ransomware SLocker recently began taking advantage of...

2015-10-22

Dridex Takedown

(https://labsblog.f-secure.com/2015/10/15/dridex-takedown/)

The UK National Crime Agency together with the FBI and the US Department of...

2015-10-15

Marshmallow Moves Android Towards iOS-like Permissions

(https://labsblog.f-secure.com/2015/10/06/marshmallow-moves-android-towards-ios-like-permissions/)

Android 6.0 a.k.a. “Marshmallow” is now rolling out and its best new feature, from my...

2015-10-06

VB2015

(https://labsblog.f-secure.com/2015/10/05/vb2105/)

Mikko missed VB2015 this year… allegedly. I've been to every Virus Bulletin...

2015-10-05

CISA Q&A

(https://labsblog.f-secure.com/2015/09/29/cisa-qa/)

On September 10, 2015 the US House (Select) Intelligence Committee held...

2015-09-29

(https://www.f-secure.com/)

About (https://labsblog.f-secure.com/about/) ·
Contact Us (https://labsblog.f-secure.com/contact-us/) ·
Useful Stuff (https://labsblog.f-secure.com/useful-stuff/)

Powered by WordPress.com VIP (https://vip.wordpress.com/)