Administrative Office of the U.S. Courts
Department of Technology Services

Threat Summary:

U.S. Courts Look-a-Like Domain Used in Ransomware Phishing Campaign

AO Security Operations Center

22 June 2018

Report Type: Informational, Situational Awareness

Documentation ID: ACB 20180622 –TIR-072-18 U.S. Courts Look-a-Like Domain Used in Ransomware Phishing Campaign

Summary

Cybercriminals have registered a U.S. Courts look-a-like domain, uscourtsgov.com. The domain is hosted on a Russian server and includes email authentication, which makes it more likely that the emails will get delivered.[1] The domain includes 80 subdomains and is involved in an active phishing campaign that delivers ransomware (See Appendix for complete list of subdomains). The domain was registered in April and the phishing campaign began as early as May. The domain registrar is NameCheap Inc, a popular web hosting service, and uses WhoisGuard to mask the website owner information.

Detail

The look-a-like domain and subdomains are hosted on a Russian server (See Figure 1).[2] The phishing emails have been sent from at least 32 Russian-based (St. Petersburg) IP addresses.[3]

IP	Hostname	City	Region	Country	Organisation
46.161.42.75	mail1.uscourtsgov.com	St Petersburg	St.-Petersburg	RU	AS41995 Barbarich Viacheslav Yuryevich

Figure 1 Domain Hosting Server Information **Source: myonlinesecurity.com**

At least 3,582 users have been targeted by this phishing campaign which is using the United States District Court subpoena lure. As demonstrated in Figure 2, the subpoena lure uses multiple social engineering techniques. Primarily, the malicious actors are attempting to entice the users into opening the attachment by playing on the emotional strings of fear, authority, and curiosity.[4] At first glance the domain uscourtsgov.com may fool potential victims, particularly if they are emotionally stressed by the email. Lastly, the email instructs the user to open the password protected document and

[1] Myonlinesecurity.com. Fake US Courts Unauthorised Tax Return malspam delivers Sigma Ransomware | My Online Security. (2018). My Online Security. Retrieved 22 June 2018, from https://myonlinesecurity.co.uk/fake-us-courts-unauthorised-tax-return-malspam-delivers-sigma-ransomware/

[2] Myonlinesecurity.com. Fake US Courts Unauthorised Tax Return malspam delivers Sigma Ransomware | My Online Security. (2018). My Online Security. Retrieved 22 June 2018, from https://myonlinesecurity.co.uk/fake-us-courts-unauthorised-tax-return-malspam-delivers-sigma-ransomware/

[3] Comodo. New Variant of Sigma Ransomware | Subpoena Scare Users in Russia. (2018). Comodo News and Internet Security Information. Retrieved 22 June 2018, from https://blog.comodo.com/pc-security/subpoena-new-variant-of-sigma-ransomware/

[4] Comodo. New Variant of Sigma Ransomware | Subpoena Scare Users in Russia. (2018). Comodo News and Internet Security Information. Retrieved 22 June 2018, from https://blog.comodo.com/pc-security/subpoena-new-variant-of-sigma-ransomware/

provides the password in the email body. Malicious actors password protect documents and compress malicious attachments in an effort to bypass email filters.

Figure 2 Phishing Email Delivering Sigma Ransomware **Source: Comodo**

Even if the user opens the password protected document, the malware will not run immediately because Microsoft disables macros by default. As seen in Figure 3, when the document opens the attacker uses the "protected document" lure to get the victim to enable macros. Basically, the "protected document" lure convinces the victim that the document is protected and the only

way to read it is to enable content, which is actually enabling macros and bypassing Microsoft's built in protection mechanisms.

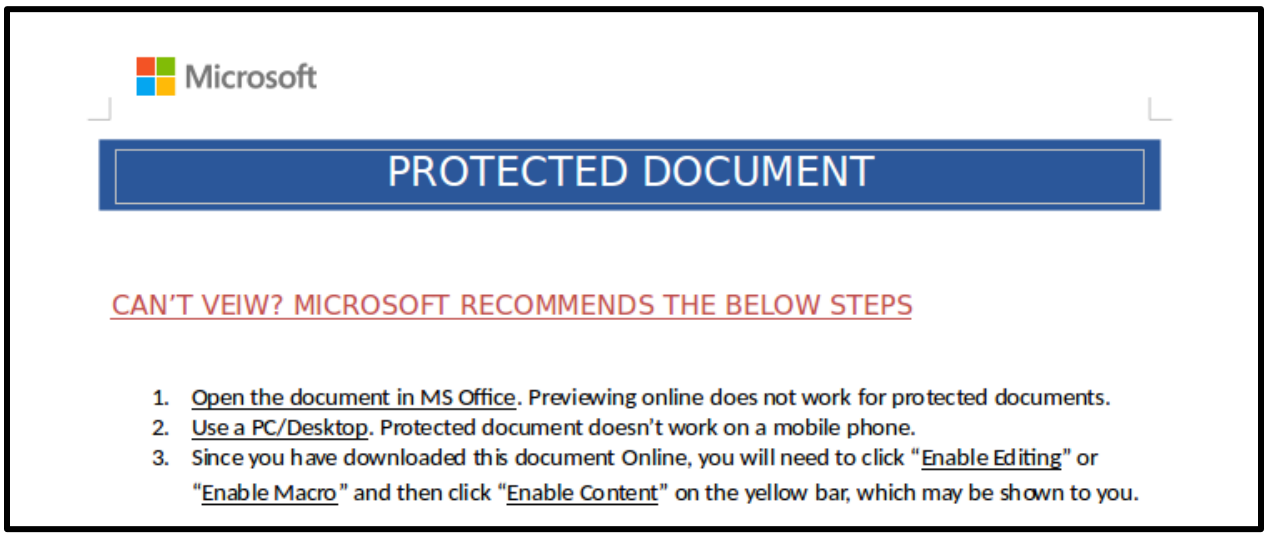

Figure 3 Protected Document Lure **Source: Comodo**

Figure 4, 5, and 6 demonstrates that the phishing campaign consists of different senders and email formats; however, the malicious attachment appears to be the same, based on the same password to open the attachment, even when the attachment is named differently. The format of the sender name appears to be consistent, using a first name, last name, and uscourtsgov.com domain.

Return-Path: <Dominick.Jones@uscourtsgov.com>
Return-path: <Dominick.Jones@uscourtsgov.com>
From: "Dominick Jones" <Dominick.Jones@uscourtsgov.com>
Subject: Re: admin
Date: Tue, 8 May 2018
Message-ID: <orx0yiu-uhqtxp-21@uscourtsgov.com>

8N ESO (Rev RV/R6)
Civil Action No. KXW-J6-F1L

You're instructed to appear at the time, particular date, and place in order to state at a deposition to be taken in this particular civil action.

Security password to view the file: 615145

Warm regards,
Willis Charles
United States District Court

scan_admin.doc

Figure 4 Example Phishing Email **Source: antifraud.org**

Figure 5 Example Phishing Email **Source: Facebook**

Received: from mail1.uscourtsgov.com ([46.161.42.75]:59590)
by my Mail Server with esmtps (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256)
(Exim 4.89_1)
(envelope-from <Travis.Steele@uscourtsgov.com>)
id 1fFvYD-0006Vj-TP
for sales@victimsdomain.com; Tue, 08 May 2018 06:52:38 +0100
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=default; d=uscourtsgov.com;
h=Date:Subject:Message-ID:From:To:MIME-Version:Content-Type;
i=Travis.Steele@uscourtsgov.com;
bh=5bn4+fiwCDWzQa04znLr+YtDq2A=;
b=Uv56GrVsDVez3nkTxKNyvhuBWLyaFXvGlLoCgDjFbmee+t4FISA0EF7hwtMnc4A7v+RtbVqtkmmm
rZJs8kZUkAdgbBa5PY6sZOcwuX46Ls6/7Lg6CajRSAVgtZmvsTKDCSHgoqRo4OVy/MHYLl/n+ex1
+KndzbcvWVoGXeZ84KY=
DomainKey-Signature: a=rsa-sha1; c=nofws; q=dns; s=default; d=uscourtsgov.com;
b=RLeefH6N68wTY4WItjcpO+p6vWzQOl/ifp5nmwVfP5Ow7mAcrrUmhrPfqFgLCpyF0jfHUthCBZT8
XtGyKVZqNa/OlznxPy0fsC+e8VXsf/J/CBYZ9Mwk4LpG9iOAk7r9NiNYpdXVI5Fds0fG0Q3H2nVL
Ls4krWt/gAao84apvto=;
Date: Mon, 7 May 2018 22:52:37 -0700
Subject: Notice – sales
Message-ID: <471f7t4th69e1p7eoxuboj1v.1110676370023@uscourtsgov.com>
From: "Travis Steele" <Travis.Steele@uscourtsgov.com>
To: sales@victimsdomain.com
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="-_com.android.email_3350521342531"

The email looks like:

From: Travis Steele <Travis.Steele@uscourtsgov.com>

Date: Tue 08/05/2018 06:53

Subject: Notice – sales

Attachment: scan_sales.doc

Body content:

> *sales,*
> *We've seen an unauthorized tax return from your account, kindly view the event information and get back to us quickly.*
> *Code to view the document = 615145*
> *Respectfully yours*
> *Lonnie Dickson*

Figure 6 Sample Email with Header **Source: myonlinesecurity.com**

After the macro runs it installs Sigma ransomware. Researchers report that this variant of Sigma uses a variety of tricks to hide and avoid detection. Before running, it checks the environment for virtual machine or sandboxes. If it discovers one, the malware kills itself. The malware disguises its malicious process and registry entries as legitimate ones like "svchost.exe" and "chrome". Additionally, unlike other ransomware variants, Sigma does not act immediately but lurks and makes covert reconnaissance first. It creates a list of valuable files, counts them, and sends this value to its command and control server along with other information about the

victim's machine. If no files were found, Sigma just deletes itself. It also geolocates the computer and will kill itself if the computer is in Russia or Ukraine.[5]

Conclusion

The U.S. Courts look-a-like phishing campaign is elaborate because of the infrastructure (which includes 80 subdomains), the combination of the phishing and social engineering techniques used, and the ransomware itself. All the phishing techniques and ransomware attributes have previously been observed; however, this is the first time that U.S. Courts has observed the combination of look-a-like domains, subpoena lure, password protected lure, protected document lure, and the sophistication of the ransomware that includes sandbox detection and geo-location kill switch all in one phishing campaign related to U.S. Courts.

[5] Comodo. New Variant of Sigma Ransomware | Subpoena Scare Users in Russia. (2018). Comodo News and Internet Security Information. Retrieved 22 June 2018, from https://blog.comodo.com/pc-security/subpoena-new-variant-of-sigma-ransomware/

Appendix: Subdomains

Hostname
blog.uscourtsgov.com
ftp.uscourtsgov.com
ilnd.uscourtsgov.com
mail1.uscourtsgov.com
mail10.uscourtsgov.com
mail11.uscourtsgov.com
mail12.uscourtsgov.com
mail13.uscourtsgov.com
mail14.uscourtsgov.com
mail15.uscourtsgov.com
mail16.uscourtsgov.com
mail17.uscourtsgov.com
mail18.uscourtsgov.com
mail19.uscourtsgov.com
mail2.uscourtsgov.com
mail20.uscourtsgov.com
mail21.uscourtsgov.com

mail22.uscourtsgov.com
mail23.uscourtsgov.com
mail24.uscourtsgov.com
mail25.uscourtsgov.com
mail26.uscourtsgov.com
mail27.uscourtsgov.com
mail28.uscourtsgov.com
mail29.uscourtsgov.com
mail3.uscourtsgov.com
mail30.uscourtsgov.com
mail31.uscourtsgov.com
mail32.uscourtsgov.com
mail4.uscourtsgov.com
mail5.uscourtsgov.com
mail6.uscourtsgov.com
mail7.uscourtsgov.com
mail8.uscourtsgov.com
mail9.uscourtsgov.com
ned.uscourtsgov.com

notice1.uscourtsgov.com
notice10.uscourtsgov.com
notice11.uscourtsgov.com
notice12.uscourtsgov.com
notice13.uscourtsgov.com
notice14.uscourtsgov.com
notice15.uscourtsgov.com
notice16.uscourtsgov.com
notice17.uscourtsgov.com
notice18.uscourtsgov.com
notice19.uscourtsgov.com
notice2.uscourtsgov.com
notice20.uscourtsgov.com
notice21.uscourtsgov.com
notice22.uscourtsgov.com
notice24.uscourtsgov.com
notice25.uscourtsgov.com
notice26.uscourtsgov.com
notice27.uscourtsgov.com

notice28.uscourtsgov.com
notice29.uscourtsgov.com
notice3.uscourtsgov.com
notice31.uscourtsgov.com
notice32.uscourtsgov.com
notice33.uscourtsgov.com
notice4.uscourtsgov.com
notice5.uscourtsgov.com
notice6.uscourtsgov.com
notice7.uscourtsgov.com
notice8.uscourtsgov.com
notice9.uscourtsgov.com
ns1.uscourtsgov.com
ns2.uscourtsgov.com
uscourtsgov.com
www.casd.uscourtsgov.com
www.ilnd.uscourtsgov.com
www.lawb.uscourtsgov.com
www.ne.uscourtsgov.com

www.neb.uscourtsgov.com
www.ned.uscourtsgov.com
www.nep.uscourtsgov.com
www.okwp.uscourtsgov.com
www.pacer.uscourtsgov.com
www.uscourtsgov.com