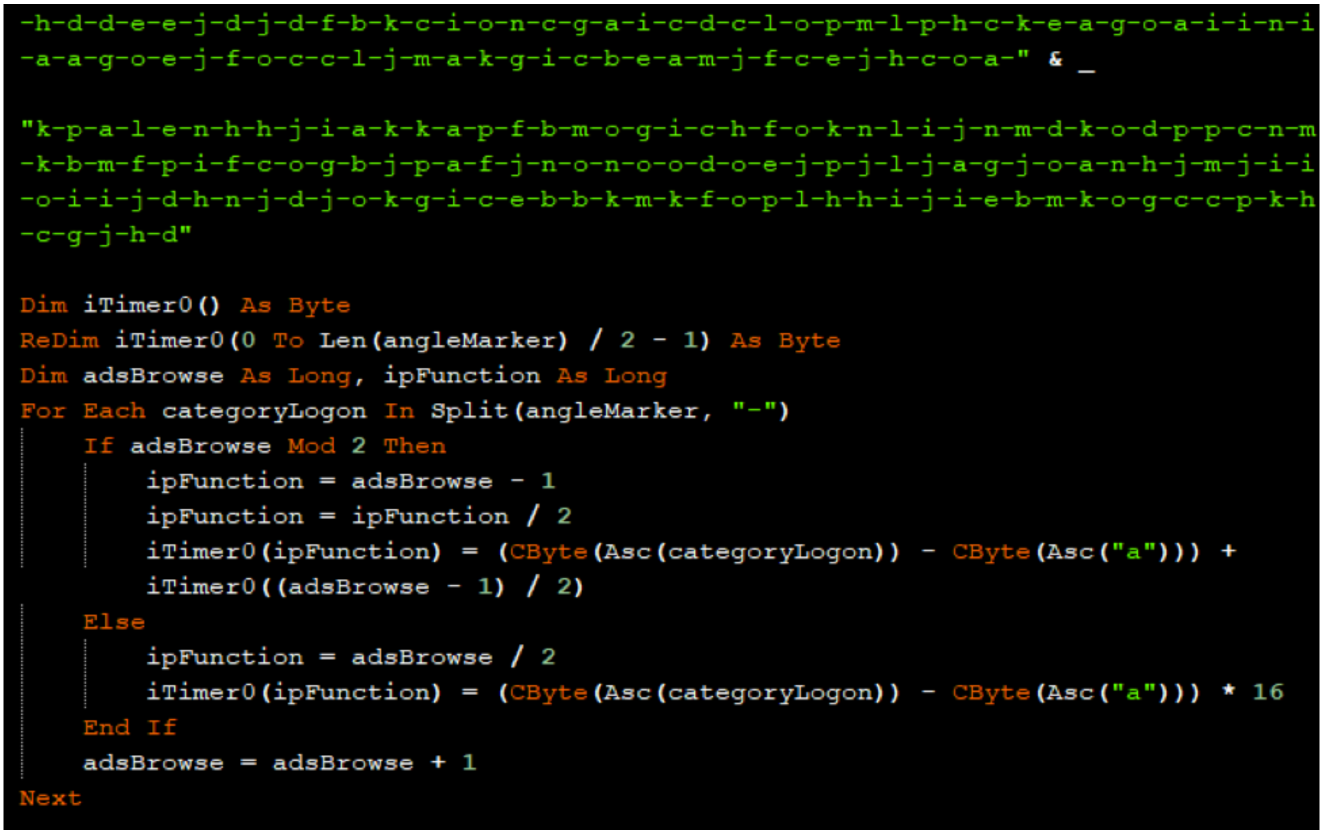
Global Malicious Spam Campaign Using Black Lives Matter as a Lure

fortinet.com/blog/threat-research/global-malicious-spam-campaign-using-black-lives-matter-as-a-lure

June 15, 2020



```
-h-d-d-e-e-j-d-j-d-f-b-k-c-i-o-n-c-g-a-i-c-d-c-l-o-p-m-l-p-h-c-k-e-a-g-o-a-i-i-n-i
-a-a-g-o-e-j-f-o-c-c-l-j-m-a-k-g-i-c-b-e-a-m-j-f-c-e-j-h-c-o-a-" & _

"k-p-a-l-e-n-h-h-j-i-a-k-k-a-p-f-b-m-o-g-i-c-h-f-o-k-n-l-i-j-n-m-d-k-o-d-p-p-c-n-m
-k-b-m-f-p-i-f-c-o-g-b-j-p-a-f-j-n-o-n-o-o-d-o-e-j-p-j-l-j-a-g-j-o-a-n-h-j-m-j-i-i
-o-i-i-j-d-h-n-j-d-j-o-k-g-i-c-e-b-b-k-m-k-f-o-p-l-h-h-i-j-i-e-b-m-k-o-g-c-c-p-k-h
-c-g-j-h-d"

Dim iTimer0() As Byte
ReDim iTimer0(0 To Len(angleMarker) / 2 - 1) As Byte
Dim adsBrowse As Long, ipFunction As Long
For Each categoryLogon In Split(angleMarker, "-")
    If adsBrowse Mod 2 Then
        ipFunction = adsBrowse - 1
        ipFunction = ipFunction / 2
        iTimer0(ipFunction) = (CByte(Asc(categoryLogon)) - CByte(Asc("a"))) +
        iTimer0((adsBrowse - 1) / 2)
    Else
        ipFunction = adsBrowse / 2
        iTimer0(ipFunction) = (CByte(Asc(categoryLogon)) - CByte(Asc("a"))) * 16
    End If
    adsBrowse = adsBrowse + 1
Next
```

FortiGuard Labs Threat Analysis

Affected platforms:	Windows 10 & Windows Server 2019
Impacted parties:	Windows 10 version 1809 + and Windows Server version 1903 +
Impact:	Privilege Escalation & User-Privacy Settings Violation
Severity level:	Important

On June 10, 2020, FortiGuard Labs came across a global malicious spam campaign that is targeting users who may be sympathetic to the Black Lives Matter movement that began in the United States. With all of the calamity of 2020, such as the ongoing COVID-19 pandemic and the numerous protests in the United States and elsewhere, attackers are leveraging the global news cycle to lure unsuspecting victims to download and open malicious attachments.

The campaign uses a variety of subject lines for emails with an attached malicious Microsoft Word document to compel the user into opening the attachment. The content of the body is written in haste and uses poor grammar, but the Black Lives Matter subject is used to compel victims into opening the attachment:

Leave a review confidentially about [various Black Lives Matter subjects]
Claim in attached file

These emails utilize variations in subjects and sender names to either circumvent spam filters or to simply create confusion. An example of the variety of subjects and senders being used is shown below:

Figure 1. Variants of Black Lives Matter Spam and Subject lines

Technical Details of the Malicious Spam Campaign Using Black Lives Matter to Lure Victims

The attachment is a standard Microsoft Word document with a generic image enticing the user to enable macros.

Figure 2. Image in Word Document Compelling User to Enable Macros.

When we try to examine the macro, we find that it is protected by a password, as is the case with many malicious documents. This adds an additional layer of protection to prevent casual analysis. And after extracting the macro, we also see that an obfuscated string is used to hide the payload.

Figure 3. Obfuscation to hide payload

Once it goes through the deobfuscation process, we can see that it is using injection to deliver its malicious payload. In this case, it is loading the stage 1 downloader.

Figure 4. Thread created after call to VirtualProtectEx that contains the injection instruction to download and execute Trickbot

Once a memory region is created by the call to VirtualProtectEx, a thread is created and executed. This new thread contains the actual payload to execute assembly instructions in memory. It then unpacks itself and proceeds to contact C2 servers in order to download and execute Trickbot.

The campaign utilizes that same strategy as previous Trickbot attacks. The individuals behind Trickbot have used trending topics before to lure victims and extend their installed base. The campaign just prior to the current one leveraging the Black Lives Matter movement in the United States, was focused on COVID-19, which we previously analyzed. Performing OSINT research, it appears that the command and control servers used by the actors behind this latest campaign have also compromised two specific sites, a city government website based in South East Asia using the Joomla CMS, and a manufacturer in the United States that is using WordPress as its CMS.

At the time of discovery, FortiGuard Labs was one of a handful of vendors who had detected the sample used in this analysis:

File name: e-vote_form_78211.doc

[SHA256 -
35E1F022861474407246F0C66218A83019381E8745E4C6B294CF150F401C16DC

Detected as: VBA/Agent.KJMLBSB!tr

Figure 5. Limited Coverage During Time of Discovery

Global Spread

Analyzing the domains and infrastructure used by the threat actors, we find that they are all hosted in the Czech Republic (CD-Telematika a.s.). While this does not mean anything in terms of attribution, it is still interesting that this is the ISP chosen by the actors behind this latest Trickbot campaign. Scouring our passive DNS records has revealed nothing in terms of past campaigns originating from the identified servers, which is increasingly the case given the reality of easy-to-spin-up virtual private servers and on-demand cloud infrastructures.

We can also see that a spike developed quite noticeably on the day this was discovered (June 10th). This is true for all domains related to this specific campaign:

Figure 6. Brand new spike for all domains used in this campaign observed on June 10

While the US and Canada are its primary targets, we have detected variations of this campaign affecting other countries as well. Here is a brief breakdown of what we have discovered.

Name: mnjcszrh.monster

Address: 82.202.65.177

Figure 7: Domain Name - mnjcszrh.monster

Based on our telemetry, the top 5 countries targeted by this specific campaign are Canada (48%) and the United States (46%), with France, Cyprus, and Italy having seen activity averaging less than one percent.

Name: shmbidgp.monster

Address: 82.202.65.178

Figure 8: Domain Name - shmbidgp.monster

The top 5 countries targeted by this specific campaign are Canada (48%) and the United States (46%). This time, France, Thailand, and Cyprus have seen less than 1% of activity.

Name: ygzggxeh.monster

Address: 82.202.65.125

Figure 9: Domain Name - ygzggxeh.monster

We can now see a pattern developing. The top countries targeted by this specific campaign are again, the United States (46%) and Canada (45%), this time with Italy, Cyprus, and Oman averaging less than one percent of activity. While the US and Canada are clearly the primary targets, Cyprus is consistently included in the spillover.

Name: vmrriktf.monster

Address: 89.203.251.79

Figure 10: Domain Name - vmrriktf.monster

Interestingly, based on our telemetry, there were only 4 countries targeted by this specific campaign. And other than the usual targets of the United States (49%) and Canada (48%), the other countries impacted this time are Rwanda and United Kingdom, averaging less than one percent of activity.

Name: copsbiau.monster

Address: 89.203.248.175

Figure 11: Domain Name - copsbiau.monster

Finally, our telemetry shows that the top 5 countries targeted by this specific campaign again include the United States (61%) and Canada (36%), and with Italy and Cyprus again showing up, but this time with Germany included. These three countries have also seen activity averaging less than one percent.

Mitigation of the Malicious Spam Campaign

FortiGuard Labs recommends that all AV and IPS definitions are kept up to date on a continual basis, and that organizations maintain a proactive patching routine when vendor updates are available. If it is deemed that patching is not feasible, it is recommended that IPS be used for proximity control, also known as virtual patching, and that a risk assessment is conducted to determine additional mitigation safeguards within an environment.

In the meantime, organizations are strongly encouraged to conduct ongoing training sessions to educate and inform personnel about the latest phishing/spearphishing attacks. They also need to encourage their employees to never open attachments from someone they don’t know, and to always treat emails from unrecognized/untrusted senders with caution.

Initial Access Mitigation: FortiMail or other secure mail gateway solutions can be used to block specific file types such as the ones outlined in this blog. FortiMail can also be configured to send attachments to our FortiSandbox solution (ATP), either on-premises or in the cloud, to determine if a file displays malicious behavior. FortiGate firewalls with anti-virus enabled, combined with a valid subscription, are able detect and block this threat if properly configured.

Execution: Since it has been reported that this threat has been delivered via social engineering distribution mechanisms, it is crucial that end users within an organization are made aware of the various types of attacks being delivered using this method. This can be accomplished through regular training sessions and impromptu tests using predetermined templates by internal security departments within an organization. Simple user awareness training on how to spot emails with malicious attachments or links could stop initial access into the network.

Fortinet Solutions: If user awareness training fails and a user opens a malicious attachment or link, FortiEDR is able to prevent TrickBot from executing. FortiClientrunning the latest up-to-date virus signatures will also detect and block this file and associated files.The file(s) highlighted in our report are currently being detected with the current definition:

78.072 (Added Jun 10, 2020)

Exfiltration and C&C: A FortiGate located at each of your ingress and egress points with its Web Filtering service enabled, and with up-to-date definitions and/or Botnet Security enabled will detect and block any observable outbound connections if configured correctly.

Web Filtering: All network IOCs in this report have been placed on the block list by the FortiGuard Web Filtering service.

Malicious Word Document Protection: FortiGuard CDR (Content Disarm & Reconstruction) supported by FortiMail and FortiGate, processes all incoming files, deconstructs them, and then strips all active content from those files in real-time to create a flat, sanitized file. CDR fortifies zero-day file protection strategies by proactively removing any possibility of malicious content in your files.

Other Fortinet Safeguards: It is important to note that as attacks continue to become more sophisticated they can sometimes circumvent your security defenses. This is why it is important to ensure that, in addition to a layered security strategy, you also have the ability to detect anomalous activity that could be malicious.

In addition, our Enterprise Bundle addresses this and similar attacks. The Enterprise Bundle consolidates all the cybersecurity services you need to protect and defend against all cyberattack channels, from the endpoint to the cloud, including IoT devices, providing you with the integrated defense needed to tackle today’s advanced threats such as the one outlined here, as well as address today's challenging risk, compliance, management, visibility, and Operational Security (OT) concerns.

MITRE ATT&CK

Spearphishing Attachment

ID: T1193

Tactic: Initial Access

Platform: Windows

Scripting

ID: T1064

Tactic: Defense Evasion, Execution

Platform: Windows

Defense Evasion

ID: T1064

Tactic: Defense Evasion, Execution

Platform: Windows

Standard Application Layer Protocol

ID: T1071

Tactic: Command And Control

Platform: Windows

Standard Cryptographic Protocol

ID: T1032

Tactic: Command And Control

Platform: Windows

Indicators of Compromise

File name: e-vote_form_78211.doc

[SHA256 -
35E1F022861474407246F0C66218A83019381E8745E4C6B294CF150F401C16DC

Detected as: VBA/Agent.KJMLBSB!tr

Network IOCs:

copsbiau.monster

vmrriktf.monster

ygzggxeh.monster

mnjcszrh.monster

shmbidgp.monster

Other Samples Related to this Campaign:

Detected as VBA/Agent.KJMLBSB!tr:

3C1639044254CF6359062245277F56404D344A21BE60F61D0EBD94476140F45F

2CABAA75A44532D4FD4064AD9C6F6E1C5E5FDDFE012310591908D79EC71FB7E6

7295626EBB7105FAE83C12C0FAC28DF28F86B534E91F6FB37EA27E75BECC8868

B8DB4896C48BAF52BCD63CB77B5823F572BF3873A2BF80C8FD138559119CA231

153179D234D351C03908FDF7A8D5AE208D7F3CD033931C633F2F376B1C6C1CBB

8724262B8712118BDFA5FFA33AE86D3598AD988031F085D9EF5738335DFB9B57

BC0EEF72D7B1BF11866E36A9782C353AF9FA554278B8A356A7AAC825AE752D5D

D33E69B4AA5E339BAB3DCE17A8239D5EB5C28C029FA8E1C0CECEA69CB1A4BC1B

C9D7BDCEDDC35B22087FBE25B31226941A85D45FF942CC057DE4077131BA2FAD
1FDAA84F98E629A987EF1ECFD6776AA2EA1D9864A422F26B046F37B2C3464C8C
024A8F2A3970DF1C34F96770122707A6A60C48931835587851 7C5A0BAAFC2453
EEDAB538265E5AB516970BA552C3FBD00E932B1A0317A490C60F619283D601E8
84E3CFCE2B0F54C908EB2E7E0B2732C86D9CDDC4A2B1BC59D13D8FFD51F54A53
AD0C6D76CEE136E36C6D7A3D8BBA806B5A81DB35999E1183BC2DF58C8E8DB000
C269CBFFEC913FE22458EBAF05A0B70FDD339F39123C9809C4997BB40107A73F
1404CEC62F967DAE0F5BC3E59254210F254430ACA6A4FF47907DB9E03863575F
67588AE687109031D7D6B428AAA14708110DAB5C9F117E3D30D5B0D234CF5DAE
7289D1B123109CB001A8C9F03C1EC087FEC85E958C63DC0315DDEBBAE82E0E10
50B3D47D816B27F2E57C6BFC9CEC866E0A1DFA64226679B3D434443016D1DE0A
DB16691F55FCF190C8F7CB3B64D9E4E003739E07F153DA18F58C4525E6CCDB95
17FFF7062C525CC1F0293FC9693982D793F44E483BAB57FD2330CA5769CF4BF1
ED6E0DD584A9901710538217F410C73DE2C9EFF8DBDEB5DF57E7D42936135A65
35E1F022861474407246F0C66218A83019381E8745E4C6B294CF150F401C16DC
2781A00A240926AF3EA55E84F1700908200F5C7DBF889CD3F006DE6B2BC73F43
E449FC1EF3C8AA7BB6C3B6C323A9E465F26C05381912F128FDE901234C8E5596
55BFD2C3B70CB561EC87721B871C1B87DFAA6FCF22778E67063E86A1E6CFBA7E

AF1FD845B7488CE9582409FD9A7A8A8E9FCA0C4D366966CD3B8DFDFFADA99F98
CF16FB4DBE65217577DDAEA92FC4A9EE614689DCAFD2FD781A469277CE2E35F8

Empowering CTA

FortiGuard Labs has shared the findings in this report with fellow Cyber Threat Alliance members, including file samples and indicators of compromise. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit cyberthreatalliance.org.

Learn more about FortiGuard Labs threat research and the FortiGuard Security Subscriptions and Services portfolio. Sign up for the weekly Threat Brief from FortiGuard Labs.

Learn more about Fortinet's free cybersecurity training initiative or about the Fortinet Network Security Expert program, Network Security Academy program, and FortiVet program.

Know your vulnerabilities – get the facts about your network security. A Fortinet Cyber Threat Assessment can help you better understand: Security and Threat Prevention, User Productivity, and Network Utilization and Performance.