



22 FEBRUARY 2021

IA-49193-21

CYBERSECURITY

(U//FOUO) Malicious Domains Associated with APT Spear-Phishing Campaign

*(U//FOUO) **Scope Note:** This Network Defender Bulletin provides federal, state, local, and private sector network defenders information to help detect and mitigate malicious cyber activity. While I&A considers this network defense information to be credible and actionable, this Bulletin is not considered finished intelligence and is being shared for the purpose of informing cybersecurity protection activities.*

(U//FOUO) An advanced persistent threat cyber actor from June to September 2020 targeted several US persons with social engineering and spear-phishing e-mails containing malicious links and attachments – at least one US person was compromised, according to government reporting.

(U) Support to Computer Network Defense

This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

Malicious Domains
https://tinyurl[.]com/y9jmmzlh
https://tinyurl[.]com/y5nv8lm2
https://tinyurl[.]com/y55knsww
https://tinyurl[.]com/y29a55kt
https://tinyurl[.]com/yxrlsq55
https://continuetogo[.]me/private-sharings/id=jlbabbin=54541253/index[.]php
https://mailer-daemon-message[.]co/continuetothefile/-Old-Radicals-Never-Die-They-Multiply[.]php

Source, Reference, and Dissemination Information

Reporting Suspicious Activity	<p>(U) To report a computer security incident, please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form. The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.</p> <p>(U) To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov. DHS I&A Field Operations officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.</p>
Dissemination	<p>(U) Federal, state, local, and private sector network defenders.</p>
Warning Notices & Handling Caveats	<p>(U) Warning: This document contains UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO) information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with critical infrastructure and key resource personnel or private sector security officials without further approval from DHS.</p> <p>(U) All US person information has been minimized. Should you require US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@HQ.DHS.GOV. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.</p> <p>(U//FOUO) This report includes sensitive technical information related to computer network operations that could be used against US Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, e mail addresses, or user names identified in this document is strictly prohibited.</p>



Product Title:

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: and function:

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's relevance to your mission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's timeliness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's responsiveness to your intelligence needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. How do you plan to use this product in support of your mission? *(Check all that apply.)*

- | | |
|--|---|
| <input type="checkbox"/> Drive planning and preparedness efforts, training, and/or emergency response operations | <input type="checkbox"/> Initiate a law enforcement investigation |
| <input type="checkbox"/> Observe, identify, and/or disrupt threats | <input type="checkbox"/> Intiate your own regional-specific analysis |
| <input type="checkbox"/> Share with partners | <input type="checkbox"/> Intiate your own topic-specific analysis |
| <input type="checkbox"/> Allocate resources (e.g. equipment and personnel) | <input type="checkbox"/> Develop long-term homeland security strategies |
| <input type="checkbox"/> Reprioritize organizational focus | <input type="checkbox"/> Do not plan to use |
| <input type="checkbox"/> Author or adjust policies and guidelines | <input type="checkbox"/> Other: <input type="text"/> |

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product not address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This product provided me with intelligence information I did not find elsewhere.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. How did you obtain this product?

10. Would you be willing to participate in a follow-up conversation about your feedback?

To help us understand more about your organization so we can better tailor future products, please provide:

Name: <input type="text"/>	Position: <input type="text"/>
Organization: <input type="text"/>	State: <input type="text"/>
Contact Number: <input type="text"/>	Email: <input type="text"/>



[Privacy Act Statement](#)