Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs

us-cert.cisa.gov/ncas/alerts/aa21-148a

Summary

This Joint Cybersecurity Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 9. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are engaged in addressing a spearphishing campaign targeting government organizations, intergovernmental organizations (IGOs), and non-governmental organizations (NGOs). A sophisticated cyber threat actor leveraged a compromised end-user account from Constant Contact, a legitimate email marketing software company, to spoof a U.S.-based government organization and distribute links to malicious URLs.[1] CISA and FBI have not determined that any individual accounts have been specifically targeted by this campaign.

Note: CISA and FBI acknowledge open-source reporting attributing the activity discussed in the report to APT29 (also known as Nobelium, The Dukes, and Cozy Bear).[2,3] However, CISA and FBI are investigating this activity and have not attributed it to any threat actor at this time. CISA and FBI will update this Joint Cybersecurity Advisory as new information becomes available. Note:

This Joint Cybersecurity Advisory contains information on tactics, techniques, and procedures (TTPs) and malware associated with this campaign. For more information on the malware, refer to Malware Analysis Report MAR-10339794-1.v1: Cobalt Strike Beacon.

CISA and FBI urge governmental and international affairs organizations and individuals associated with such organizations to adopt a heightened state of awareness and implement the recommendations in the Mitigations section of this advisory.

For a downloadable list of indicators of compromise (IOCs), refer to AA21-148A.stix, and MAR-10339794-1.v1.stix.

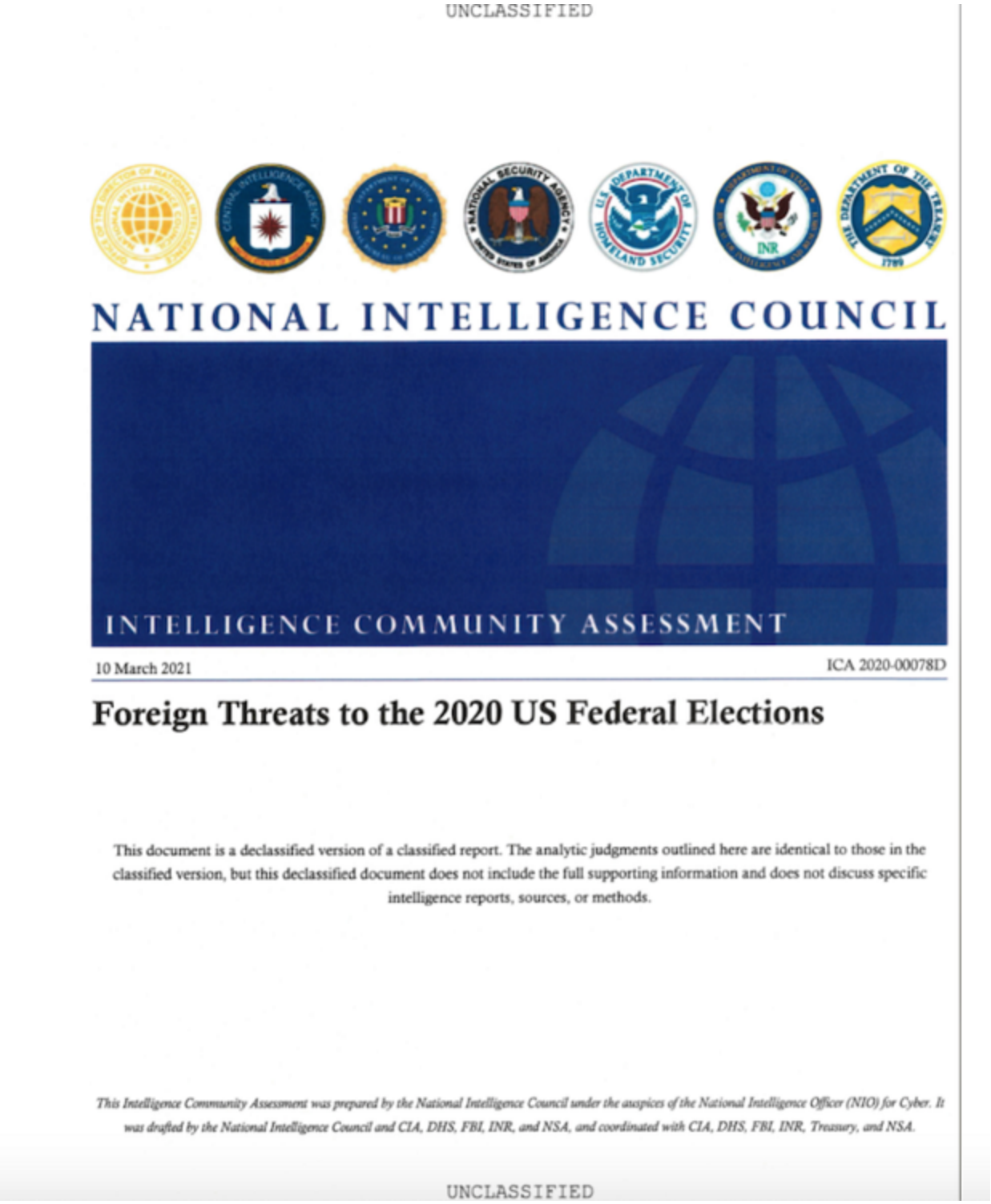
Click here for a PDF version of this report.

Technical Details

Based on incident reports, malware collection, and trusted third-party reporting, CISA and FBI are engaged in addressing a sophisticated spearphishing campaign. A cyber threat actor leveraged a compromised end-user account from Constant Contact, a legitimate email

marketing software company, to send phishing emails to more than 7,000 accounts across approximately 350 government organizations, IGOs, and NGOs. The threat actor sent spoofed emails that appeared to originate from a U.S. Government organization. The emails contained a legitimate Constant Contact link that redirected to a malicious URL [T1566.002, T1204.001], from which a malicious ISO file was dropped onto the victim's machine.

The ISO file contained (1) a malicious Dynamic Link Library (DLL) named Documents.dll [T1055.001], which is a custom Cobalt Strike Beacon version 4 implant, (2) a malicious shortcut file that executes the Cobalt Strike Beacon loader [T1105], and (3) a benign decoy PDF titled "Foreign Threats to the 2020 US Federal Elections" with file name "ICA-declass.pdf" (see figure 1). Note: The decoy file appears to be a copy of the declassified Intelligence Community Assessment pursuant to Executive Order 13848 Section 1(a), which is available at https://www.intelligence.gov/index.php/ic-on-the-record-database/results/1046-foreign-threats-to-the-2020-us-federal-elections-intelligence-community-assessment.


UNCLASSIFIED

NATIONAL INTELLIGENCE COUNCIL

INTELLIGENCE COMMUNITY ASSESSMENT

10 March 2021

ICA 2020-00078D

Foreign Threats to the 2020 US Federal Elections

This document is a declassified version of a classified report. The analytic judgments outlined here are identical to those in the classified version, but this declassified document does not include the full supporting information and does not discuss specific intelligence reports, sources, or methods.

This Intelligence Community Assessment was prepared by the National Intelligence Council under the auspices of the National Intelligence Officer (NIO) for Cyber. It was drafted by the National Intelligence Council and CIA, DHS, FBI, INR, and NSA, and coordinated with CIA, DHS, FBI, INR, Treasury, and NSA.

UNCLASSIFIED

Figure 1: Decoy PDF: ICA-declass.pdf

Cobalt Strike is a commercial penetration testing tool used to conduct red team operations. [4] It contains a number of tools that complement the cyber threat actor's exploitation efforts, such as a keystroke logger, file injection capability, and network services scanners. The Cobalt Strike Beacon is the malicious implant that calls back to attacker-controlled infrastructure and checks for additional commands to execute on the compromised system [TA0011].

The configuration file for this Cobalt Strike Beacon implant contained communications protocols, an implant watermark, and the following hardcoded command and control (C2) domains:

- `dataplane.theyardservice[.]com/jquery-3.3.1.min.woff2`
- `cdn.theyardservice[.]com/jquery-3.3.1.min.woff2`
- `static.theyardservice[.]com/jquery-3.3.1.min.woff2`
- `worldhomeoutlet[.]com/jquery-3.3.1.min.woff2`

The configuration file was encoded via an XOR with the key `0x2e` and a 16-bit byte swap.

For more information on the ISO file and Cobalt Strike Beacon implant, including IOCs, refer to Malware Analysis Report MAR-10339794-1.v1: Cobalt Strike Beacon.

Indicators of Compromise

The following IOCS were derived from trusted third parties and open-source research. For a downloadable list of IOCs, refer to AA21-148A.stix and MAR-10339794-1.v1.stix.

- **URL:** `https[:]//r20.rs6.net/tn.jsp?f=`
  Host IP: `208.75.122[.]11 (US)`
  Owner: Constant Contact, Inc.
  Activity: legitimate Constant Contact link found in phishing email that redirects victims to actor-controlled infrastructure at
  `https[:]//usaid.theyardservice.com/d/<target_email_address>`

- **URL:** `https[:]//usaid.theyardservice.com/d/<target_email_address>`
  Host IP: `83.171.237[.]173` (Germany)
  Owner: [redacted]
  First Seen: May 25, 2021
  Activity: actor-controlled URL that was redirected from `https[:]//r20.rs6.net/tn.jsp?f=`; the domain `usaid[.]theyardservice.com` was detected as a malware site; hosted a malicious ISO file
  " `usaid[.]theyardservice.com` "

- **File:** `ICA-declass.iso` [MD5: `cbc1dc536cd6f4fb9648e229e5d23361`]
  File Type: Macintosh Disk Image
  Detection: `Artemis!7EDF943ED251`, Trojan: `Win32/Cobaltstrike!MSR`, or other malware
  Activity: ISO file container; contains a custom Cobalt Strike Beacon loader; communicated with multiple URLs, domains, and IP addresses

- **File:** `/d/` [`MD5: ebe2f8df39b4a94fb408580a728d351f`]
  File Type: Macintosh Disk Image
  Detection: Cobalt, Artemis!7EDF943ED251, or other malware
  Activity: ISO file container; contains a custom Cobalt Strike Beacon loader; communicated with multiple URLs, domains, and IP addresses

- **File:** ICA-declass.iso [MD5: 29e2ef8ef5c6ff95e98bff095e63dc05]
  File Type: Macintosh Disk Image
  Detection: Cobalt Strike, Rozena, or other malware
  Activity: ISO file container; contains a custom Cobalt Strike Beacon loader; communicated with multiple URLs, domains, and IP addresses

- **File:** `Reports.lnk` [MD5: `dcfd60883c73c3d92fceb6ac910d5b80`]
  File Type: LNK (Windows shortcut)
  Detection: Worm: `Win32-Script.Save.df8efe7a` , Static AI - Suspicious LNK, or other malware
  Activity: shortcut contained in malicious ISO files; executes a custom Cobalt Strike Beacon loader

- **File:** `ICA-declass.pdf` [MD5: `b40b30329489d342b2aa5ef8309ad388`]
  File Type: PDF
  Detection: undetected
  Activity: benign, password-protected PDF displayed to victim as a decoy; currently unrecognized by antivirus software

- **File:** `DOCUMENT.DLL` [MD5: `7edf943ed251fa480c5ca5abb2446c75`]
  File Type: Win32 DLL
  Detection: Trojan: `Win32/Cobaltstrike!MSR` , Rozena, or other malware
  Activity: custom Cobalt Strike Beacon loader contained in malicious ISO files; communicating with multiple URLs, domains, and IP addresses by antivirus software

- **File:** `DOCUMENT.DLL` [MD5: `1c3b8ae594cb4ce24c2680b47cebf808`]
  File Type: Win32 DLL
  Detection: Cobalt Strike, Razy, Khalesi, or other malware
  Activity: Custom Cobalt Strike Beacon loader contained in malicious ISO files; communicating with multiple URLs, domains, and IP addresses by antivirus software

- **Domain:** `usaid[.]theyardservice.com`
  Host IP: `83.171.237[.]173` (Germany)
  First Seen: May 25, 2021
  Owner: Withheld for Privacy Purposes
  Activity: subdomain used to distribute ISO file according to the trusted third party; detected as a malware site by antivirus programs

- **Domain:** worldhomeoutlet.com
  Host IP: `192.99.221[.]77` (Canada)
  Created Date: March 11, 2020
  Owner: Withheld for Privacy Purposes by Registrar
  Activity: Cobalt Strike C2 subdomain according to the trusted third party; categorized as suspicious and observed communicating with multiple malicious files according to antivirus software; associated with Cobalt Strike malware

- **Domain:** `dataplane.theyardservice[.]com`
  Host IP: `83.171.237[.]173` (Germany)
  First Seen: May 25, 2021
  Owner: [redacted]
  Activity: Cobalt Strike C2 subdomain according to the trusted third party; categorized as suspicious and observed communicating with multiple malicious files according to antivirus software; observed in phishing, malware, and spam activity

- **Domain:** `cdn.theyardservice[.]com`
  Host IP: `83.171.237[.]173` (Germany)
  First Seen: May 25, 2021
  Owner: Withheld for Privacy Purposes by Registrar
  Activity: Cobalt Strike C2 subdomain according to the trusted third party; categorized as suspicious and observed communicating with multiple malicious files according to antivirus software

- **Domain:** static.theyardservice[.]com
  Host IP: 83.171.237[.]173 (Germany)
  First Seen: May 25, 2021
  Owner: Withheld for Privacy Purposes
  Activity: Cobalt Strike C2 subdomain according to the trusted third party; categorized as suspicious and observed communicating with multiple malicious files according to antivirus software

- **IP:** `192.99.221[.]77`
  Organization: OVH SAS
  Resolutions: 7
  Geolocation: Canada
  Activity: detected as a malware site; hosts a suspicious domain `worldhomeoutlet[.]com` ; observed in Cobalt Strike activity

- **IP:** `83.171.237[.]173`
  Organization: Droptop GmbH
  Resolutions: 15
  Geolocation: Germany
  Activity: Categorized as malicious by antivirus software; hosted multiple suspicious domains and multiple malicious files were observed downloaded from this IP address; observed in Cobalt Strike and activity

- **Domain:** `theyardservice[.]com`
  Host IP: `83.171.237[.]173` (Germany)
  Created Date: January 27, 2010
  Owner: Withheld for Privacy Purposes
  Activity: Threat actor controlled domain according to the trusted third party; categorized as suspicious by antivirus software; observed in Cobalt Strike activity

Table 1 provides a summary of the MITRE ATT&CK techniques observed.

Table 1: MITRE ATT&CK techniques observed

Technique Title	Technique ID
Process Injection: Dynamic-link Library Injection	T1055.001
Ingress Tool Transfer	T1105
User Execution: Malicious Link	T1204.001
Phishing: Spearphishing Link	T1566.002

Mitigations

CISA and FBI urge CI owners and operators to apply the following mitigations.

- Implement multi-factor authentication (MFA) for every account. While privileged accounts and remote access systems are critical, it is also important to ensure full coverage across SaaS solutions. Enabling MFA for corporate communications platforms (as with all other accounts) provides vital defense against these types of attacks and, in many cases, can prevent them.
- Keep all software up to date. The most effective cybersecurity programs quickly update all of their software as soon as patches are available. If your organization is unable to update all software shortly after a patch is released, prioritize implementing patches for CVEs that are already known to be exploited.
- Implement endpoint and detection response (EDR) tools. EDR allows a high degree of visibility into the security status of endpoints and is can be an effective tool against threat actors.
  Note: Organizations using Microsoft Defender for Endpoint or Microsoft 365 Defense should refer to Microsoft: Use attack surface reduction rules to prevent malware infection for more information on hardening the enterprise attack surface.
- Implement centralized log management for host monitoring. A centralized logging application allows technicians to look out for anomalous activity in the network environment, such as new applications running on hosts, out-of-place communication between devices, or unaccountable login failures on machines. It also aids in troubleshooting applications or equipment in the event of a fault. CISA and the FBI recommend that organizations:
  - Forward logs from local hosts to a centralized log management server—often referred to as a security information and event management (SIEM) tool.
  - Ensure logs are searchable. The ability to search, analyze, and visualize communications will help analysts diagnose issues and may lead to detection of anomalous activity.
  - Correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the organization as a whole.
  - Review both centralized and local log management policies to maximize efficiency and retain historical data. Organizations should retain critical logs for a minimum of 30 days.
- Deploy signatures to detect and/or block inbound connection from Cobalt Strike servers and other post-exploitation tools.
- Implement unauthorized execution prevention by disabling macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.

- Configure and maintain user and administrative accounts using a strong account management policy.
    - Use administrative accounts on dedicated administration workstations.
    - Limit access to and use of administrative accounts.
    - Use strong passwords. For more information on strong passwords, refer to CISA Tip: Choosing and Protecting Passwords and National Institute of Standards (NIST) SP 800-63: Digital Identity Guidelines: Authentication and Lifecycle Management.
    - Remove default accounts if unneeded. Change the password of default accounts that are needed.
    - Disable all unused accounts.
- Implement a user training program and simulated attacks for spearphishing to discourage users from visiting malicious websites or opening malicious attachments and re-enforce the appropriate user responses to spearphishing emails.

RESOURCES

- Volexity Blog: Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns | Volexity
- Microsoft Blog: New sophisticated email-based attack from NOBELIUM - Microsoft Security
- Microsoft Blog: Another Nobelium Cyberattack

Contact Information

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

References

Revisions

May 28, 2021: Initial version

May 29, 2021: Added final sentence of first paragraph in Summary section

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.