Increased Truebot Activity Infects U.S. and Canada Based Networks | CISA

Published: 2023-07-06 · Archived: 2026-04-05 18:30:46 UTC

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Canadian Centre for Cyber Security (CCCS) are releasing this joint Cybersecurity Advisory (CSA) in response to cyber threat actors leveraging newly identified Truebot malware variants against organizations in the United States and Canada. As recently as May 31, 2023, the authoring organizations have observed an increase in cyber threat actors using new malware variants of Truebot (also known as Silence.Downloader). Truebot is a botnet that has been used by malicious cyber groups like CL0P Ransomware Gang to collect and exfiltrate information from its target victims.

Previous Truebot malware variants were primarily delivered by cyber threat actors via malicious phishing email attachments; however, newer versions allow cyber threat actors to also gain initial access through exploiting CVE-2022-31199—(a remote code execution vulnerability in the Netwrix Auditor application), enabling deployment of the malware at scale within the compromised environment. Based on confirmation from open-source reporting and analytical findings of Truebot variants, the authoring organizations assess cyber threat actors are leveraging both phishing campaigns with malicious redirect hyperlinks and CVE-2022-31199 to deliver new Truebot malware variants.

The authoring organizations recommend hunting for the malicious activity using the guidance outlined in this CSA, as well as applying vendor patches to Netwrix Auditor (version 10.5—see Mitigations section below).[1] Any organization identifying indicators of compromise (IOCs) within their environment should urgently apply the incident responses and mitigation measures detailed in this CSA and report the intrusion to CISA or the FBI.

Download the PDF version of this report:

Read the associated Malware Analysis Report MAR-10445155-1.v1 Truebot Activity Infects U.S. and Canada Based Networks or download the PDF version below:

For a downloadable copy of IOCs in .xml and .json format, see:

TECHNICAL DETAILS

Note: *This advisory uses the MITRE ATT&CK® for Enterprise framework, version 13. See the MITRE ATT&CK Tactics and Techniques section below for cyber threat actors' activity mapped to MITRE ATT&CK tactics and techniques.*

Initial Access and Execution

In recent months, open source reporting has detailed an increase in Truebot malware infections, particularly cyber threat actors using new tactics, techniques, and procedures (TTPs), and delivery methods.[2] Based on the nature of observed Truebot operations, the primary objective of a Truebot infection is to exfiltrate sensitive data from the compromised host(s) for financial gain [TA0010].

- Phishing:
  - Cyber threat actors have historically used malicious phishing emails as the primary delivery method of Truebot malware, which tricks recipients into clicking a hyperlink to execute malware. Cyber threat actors have further been observed concealing email attachments (executables) as software update notifications [T1189] that appear to be legitimate [T1204.002], [T1566.002]. Following interaction with the executable, users will be redirected to a malicious web domain where script files are then executed. Note: Truebot malware can be hidden within various, legitimate file formats that are used for malicious purposes [T1036.008].[3]
- Exploitation of CVE-2022-31199:
  - Though phishing remains a prominent delivery method, cyber threat actors have shifted tactics, exploiting, in observable manner, a remote code execution vulnerability (CVE-2022-31199) in Netwrix Auditor [T1190] —software used for on-premises and cloud-based IT system auditing. Through exploitation of this CVE, cyber threat actors gain initial access, as well as the ability to move laterally within the compromised network [T1210].

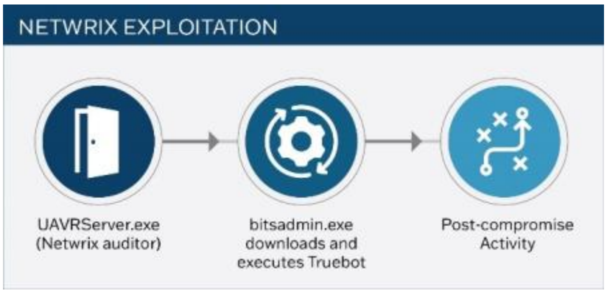

Figure 1: CVE-2022-31199 Delivery Method for Truebot

Following the successful download of the malicous file, Truebot renames itself and then loads FlawedGrace onto the host. Please see the FlawedGrace section below for more information on how this remote access tool (RAT) is used in Truebot operations.

After deployment by Truebot, FlawedGrace is able to modify registry [T1112] and print spooler programs [T1547.012] that control the order that documents are loaded to a print queue. FlawedGrace manipulates these features to both escalate privilege and establish persistence.

During FlawedGrace's execution phase, the RAT stores encrypted payloads [T1027.009] within the registry. The tool can create scheduled tasks and inject payloads into `msiexec[.]exe` and `svchost[.]exe`, which are command processes that enable FlawedGrace to establish a command and control (C2) connection to `92.118.36[.]199`, for example, as well as load dynamic link libraries (DLLs) [T1055.001] to accomplish privilege escalation.

Several hours post initial access, Truebot has been observed injecting Cobalt Strike beacons into memory [T1055] in a dormant mode for the first few hours prior to initiating additional operations. Please see the Cobalt Strike section below for more information on how this remote access tool (RAT) is used in Truebot operations.

Discovery and Defense Evasion

During the first stage of Truebot's execution process, it checks the current version of the operating system (OS) with `RtlGetVersion` and processor architecture using `GetNativeSystemInfo` [T1082].[4] **Note:** This variant of Truebot malware is designed with over one gigabyte (GB) of junk code which functions to hinder detection and analysis efforts [T1027.001].

Following the initial checks for system information, Truebot has the capability to enumerate all running processes [T1057], collect sensitive local host data [T1005], and send this data to an encoded data string described below for second-stage execution. Based on IOCs in table 1, Truebot also has the ability to discover software security protocols and system time metrics, which aids in defense evasion, as well as enables synchronization with the compromised system's internal clock to facilitate scheduling tasks [T1518.001][T1124].

Next, it uses a `.JSONIP` extension, (e.g., `IgtyXEQuCEvAM.JSONIP`), to create a thirteen character globally unique identifier (GUID)—a 128-bit text string that Truebot uses to label and organize the data it collects [T1036].

After creating the GUID, Truebot compiles and enumerates running process data into either a base64 or unique hexadecimal encoded string [T1027.001]. Truebot's main goal is identifying the presence of security debugger tools. However, the presence of identified debugger tools does not change Truebot's execution process—the data is compiled into a base64 encoded string for tracking and defense evasion purposes [T1082][T1622].

Data Collection and Exfiltration

Following Truebot's enumeration of running processes and tools, the affected system's computer and domain name [T1082][T1016], along with the newly generated GUID, are sent to a hard-coded URL in a `POST` request (as observed in the user-agent string). **Note:** A user-agent string is a customized HTTP request that includes specific device information required for interaction with web content. In this instance, cyber threat actors can redirect victims to malicious domains and further establish a C2 connection.

The `POST` request functions as means for establishing a C2 connection for bi-lateral communication. With this established connection, Truebot uses a second obfuscated domain to receive additional payloads [T1105], self-replicate across the environment [T1570], and/or delete files used in its operations [T1070.004]. Truebot malware has the capability to download additional malicious modules [T1105], load shell code [T1620], and deploy various tools to stealthily navigate an infected network.

Associated Delivery Vectors and Tools

Truebot has been observed in association with the following delivery vectors and tools:

Raspberry Robin (Malware)

Raspberry Robin is a wormable malware with links to other malware families and various infection methods, including installation via USB drive [T1091].[5] Raspberry Robin has evolved into one of the largest malware distribution platforms and has been observed deploying Truebot, as well as other post-compromise payloads such as IcedID and Bumblebee malware.[6] With the recent shift in Truebot delivery methods from malicious emails to the exploitation of CVE-2022-31199, a large number of Raspberry Robin infections have leveraged this exploitable CVE.[2]

Flawed Grace (Malware)

FlawedGrace is a remote access tool (RAT) that can receive incoming commands [T1059] from a C2 server sent over a custom binary protocol [T1095] using port 443 to deploy additional tools [T1105].[7] Truebot malware has been observed leveraging (and dropping) FlawedGrace via phishing campaigns as an additional payload [T1566.002].[8] **Note:** FlawedGrace is typically deployed minutes after Truebot malware is executed.

Cobalt Strike (Tool)

Cobalt Strike is a popular remote access tool (RAT) that cyber threat actors have leveraged—in an observable manner—for a variety of post-exploitation means. Typically a few hours after Truebot's execution phase, cyber threat actors have been observed deploying additional payloads containing Cobalt Strike beacons for persistence and data exfiltration purposes [T1059].[2] Cyber threat actors use Cobalt Strike to move laterally via remote service session hijacking [T1563.001][T1563.002], collecting valid credentials through LSASS memory credential dumping, or creating local admin accounts to achieve pass the hash alternate authentication [T1003.001][T1550.002].

Teleport (Tool)

Cyber threat actors have been observed using a custom data exfiltration tool, which Talos has named "Teleport."[2] Teleport is known to evade detection during data exfiltration by using an encryption key hardcoded in the binary and a custom communication protocol [T1095] that encrypts data using advanced encryption standard (AES) and a hardcoded key [T1048][T1573.002]. Furthermore, to maintain its stealth, Teleport limits the data it collects and syncs with outbound organizational data/network traffic [T1029][T1030].

Truebot Malware Indicators of Compromise (IOCs)

Truebot IOCs from May 31, 2023, contain IOCs from cyber threat actors conducting Truebot malspam campaigns. Information is derived from a trusted third party, they observed cyber threat actors from `193.3.19[.]173` (Russia) using a compromised local account to conduct phishing campaigns on May 23, 2023 and spread malware through: `https[:]//snowboardspecs[.]com/nae9v` , which then promptly redirects the user to: `https://www.meditimespharma[.]com/gfghthq/` , which a trusted third party has linked to other trending Truebot activity.

After redirecting to `https://www.meditimespharma[.]com/gfghthq/` , trusted third parties have observed, the cyber threat actors using Truebot to pivot to `https://corporacionhardsoft[.]com/images/2/Document_16654.exe` , which is a domain associated with `snowboardspecs[.]com` . This malicious domain has been linked to UNC4509, a threat cluster that has been known to use traffic distribution systems (TDS) to redirect users to either a benign or malicious website to facilitate their malicious phishing campaigns in May 2023.

According to trusted third parties, the MD5 Hash: `6164e9d297d29aa8682971259da06848` is downloaded from `https://corporacionhardsoft.com/images/2/Document_16654[.]exe` , and has been flagged by numerous security vendors, as well as is linked to UNC4509 Truebot campaigns. **Note:** These IOCs are associated with Truebot campaigns used by Graceful Spider to deliver FlawedGrace and LummaStealer payloads in May of 2023.

After Truebot is downloaded, the malware copies itself to `C:\Intel\RuntimeBroker.exe` and—based on trusted third party analysis—links to `https://essadonio.com/538332[.]php` (which is linked to `45.182.189[.]71` (Panama) and is associated with other trending Truebot malware campaigns from May 2023).

Please reference table 1 for IOCs described in the paragraph above.

Table 1: Truebot IOCs from May of 2023		
Indicator Type	**Indicator**	**Source**
Registrant	GKG[.]NET Domain Proxy Service Administrator	Trusted Third Party
Compromised Account Created:	2022-04-10	Trusted Third Party

Table 1: Truebot IOCs from May of 2023		
Malicious account created	1999-11-09	Trusted Third Party
IP	193.3.19[.]173 (Russia)	Trusted Third Party
URL	https://snowboardspecs[.]com/nae9v	Trusted Third Party
Domain	https://corporacionhardsoft[.]com/images/2/Document_16654.exe	Trusted Third Party
File	Document_16654[.]exe	Trusted Third Party
MD5 Hash	6164e9d297d29aa8682971259da06848	Trusted Third Party
File	Document_may_24_16654[.]exe	Trusted Third Party
File	C:\Intel\RuntimeBroker[.]exe	Trusted Third Party
URL	https://essadonio.com/538332[.]php	Trusted Third Party
IP	45.182.189[.]71 (Panama)	Trusted Third Party
Account Created	2023-05-18	Trusted Third Party

Table 2: Truebot malware IOCs from May of 2023		
Indicator Type	**Indicator**	**Source**
File Name	Secretsdump[.]py	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
Domain	Imsagentes[.]pe	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
URL	https://imsagentes[.]pe/dgrjfj/	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
URL	https://imsagentes[.]pe/dgrjfj	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
URL	https://hrcbishtek[.]com/{5	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
URL	https://ecorfan.org/base/sj/document_may_24_16654[.]exe	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
Domain	Hrcbishtek[.]com	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
MD5 Hash	F33734DFBBFF29F68BCDE052E523C287	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/

Table 2: Truebot malware IOCs from May of 2023		
MD5 Hash	F176BA63B4D68E576B5BA345BEC2C7B7	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
MD5 Hash	F14F2862EE2DF5D0F63A88B60C8EEE56	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
Domain	Essadonio[.]com	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
Domain	Ecorfan[.]org	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
SHA256 Hash	C92C158D7C37FEA795114FA6491FE5F145AD2F8C08776B18AE79DB811E8E36A3	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
File Name	Atexec[.]py	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
MD5 Hash	A0E9F5D64349FB13191BC781F81F42E1	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
IPv4	92.118.36[.]199	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
IPv4	81.19.135[.]30	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
MD5 Hash	72A589DA586844D7F0818CE684948EEA	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
SHA256 Hash	717BEEDCD2431785A0F59D194E47970E9544FBF398D462A305F6AD9A1B1100CB	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
IPv4	5.188.86[.]18	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
IPv4	5.188.206[.]78	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
IPv4	45.182.189[.]71	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
IPv4	139.60.160[.]166	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
SHA256 Hash	121A1F64FFF22C4BFCEF3F11A23956ED403CDEB9BDB803F9C42763087BD6D94E	https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/

Table 3: Truebot IOCs from May 2023 (Malicious Domains, and Associated IP addresses and URLs)		
Malicious Domain	**Associated IP(s)**	**Beacon URL**
nitutdra[.]com	46.161.40[.]128	
romidonionhhgtt[.]com	46.161.40.128	
midnigthwaall[.]com	46.161.40[.]128	
dragonetzone[.]com	46.161.40[.]128	hxxps://dragonetzone[.]com/gate_info[.]php
rprotecruuio[.]com	45.182.189[.]71	
essadonio[.]com	45.182.189[.]71	hxxps://nomoresense[.]com/checkinfo[.]php

Table 3: Truebot IOCs from May 2023 (Malicious Domains, and Associated IP addresses and URLs)		
nomoresense[.]com	45.182.189[.]91	hxxps://nomoresense[.]com/checkinfo[.]php
ronoliffuion[.]com	45.182.189[.]120	hxxps://ronoliffuion[.]com/dns[.]php
bluespiredice[.]com	45.182.189[.]119	
dremmfyttrred[.]com	45.182.189[.]103	hxxps://dremmfyttrred[.]com/dns[.]php
ms-online-store[.]com	45.227.253[.]102	
ber6vjyb[.]com	92.118.36[.]252	hxxps://ber6vjyb[.]com/dns[.]php
jirostrogud[.]com	88.214.27[.]101	hxxps://ber6vjyb[.]com/dns[.]php
fuanshizmo[.]com	45.182.189[.]229	
qweastradoc[.]com	92.118.36[.]213	hxxp://nefosferta[.]com/gate[.]php
qweastradoc[.]com	92.118.36[.]213	hxxp://nefosferta[.]com/gate[.]php
qweastradoc[.]com	92.118.36[.]213	hxxp://nefosferta[.]com/gate[.]php
hiperfdhaus[.]com	88.214.27[.]100	hxxp://nefosferta[.]com/gate[.]php
guerdofest[.]com	45.182.189[.]228	hxxp://qweastradoc[.]com/gate[.]php
nefosferta[.]com	179.60.150[.]139	hxxp://nefosferta[.]com/gate[.]php

***Table 4: Truebot IOCs from May 2023 Continued (*Malicious Domains and Associated Hashes)**			
Malicious Domain	**MD5**	**SHA1**	**SHA256**
nitutdra[.]com			
romidonionhhgtt[.]com			
midnigthwaall[.]com			
dragonetzone[.]com	64b27d2a6a55768506a5658a31c045de	c69f080180430ebf15f984be14fb4c76471cd476	e0178ab0893a4f25c68ded11
rprotecruuio[.]com			
essadonio[.]com	9a3bad7d8516216695887acc9668cda1	a89c097138e5aab1f35b9a03900600057d907690	4862618fcf15ba4ad15df35a
essadonio[.]com	6164e9d297d29aa8682971259da06848	96b95edc1a917912a3181d5105fd5bfad1344de0	717beedcd2431785a0f59d19
nomoresense[.]com	8f924f3cbe5d8fe3ecb7293478901f1a	516051b4cab1be74d32a6c446eabac7fc354904f	6b646641c823414c2ee30ae
nomoresense[.]com	ac6a2f1eafaae9f6598390d1017dd76c	1c637c2ded5d3a13fd9b56c35acf4443f308be52	f9f649cb5de27f720d58aa44
ronoliffuion[.]com	881485ac77859cf5aaa8e0d64fbafc5f	51be660a3bdaab6843676e9d3b2af8444e88bbda	36d89f0455c95f9b00a8cea8
bluespiredice[.]com			
dremmfyttrred[.]com	e4a42cbda39a20134d6edcf9f03c44ed	afda13d5365b290f7cdea701d00d05b0c60916f8	47f962063b42de277cd8d22
dremmfyttrred[.]com	aa949d1a7ebe5f878023c6cfb446e29b	06057d773ad04fda177f6b0f6698ddaa47f7168a	594ade1fb42e93e64afc96f13
dremmfyttrred[.]com	338476c2b0de4ee2f3e402f3495d0578	03916123864aa034f7ca3b9d45b2e39b5c91c502	a67df0a8b32bdc5f9d224db1
ms-online-store[.]com			
ber6vjyb[.]com	46fe07c07fd0f45ba45240ef9aae2a44	b918f97c7c6ebc9594de3c8f2d9d75ecc292d02b	c0f8aeeb2d11c6e751ee87c4
jirostrogud[.]com	89c8afc5bbd34f160d8a2b7218b9ca4a	16ecf30ff8c7887037a17a3eaffcb17145b69160	5cc8c9f2c9cee543ebac3069
jirostrogud[.]com	5da364a8efab6370a174736705645a52	792623e143ddd49c36f6868e948febb0c9e19cd3	80b9c5ec798e7bbd71bbdfff
fuanshizmo[.]com			

Table 4: Truebot IOCs from May 2023 Continued (**Malicious Domains and Associated Hashes)**			
qweastradoc[.]com	ee1ccb6a0e38bf95e44b73c3c46268c5	62f5a16d1ef20064dd78f5d934c84d474aca8bbe	0e3a14638456f4451fe8d76f
qweastradoc[.]com	82d4025b84cf569ec82d21918d641540	bb32c940f9ca06e7e8533b1d315545c3294ee1a0	c042ad2947caf4449295a51f
qweastradoc[.]com	dbecfe9d5421d319534e0bfa5a6ac162	9e7a2464f53ce74d840eb84077472bc29fd1ba05	c9b874d54c18e895face055e
qweastradoc[.]com	b7fed593e8eb3646f876367b56725e6c	44090a7858eceb28bc111e1edd2f0dc98047afb2	ff8c8c8bfba5f2ba2f800325
hiperfdhaus[.]com	8e2b823aac6c9e11fcabecb1d8c19adf	77ad34334a370d85ca5e77436ed99f18b185eee3	a30e1f87b78d1cd529fbe2af
hiperfdhaus[.]com	8a94163ddf956abd0ea92d89db0034e5	abc96032071adeb6217f0a5ba1aff55dc11f5438	b95a764820e918f42b664f3c
guerdofest[.]com	65fb9572171b903aa31a325f550d8778	d8bd44b7a8f136e29b31226f4edf566a4223266c	d5bbcaa0c3eeea17f12a5cc3
nefosferta[.]com	d9d85bdb6a3ac60a8ba6776c661dbace	78e38e522b1765efb15d0585e13c1f1301e90788	092910024190a2521f21658
nefosferta[.]com	20643549f19bed9a6853810262622755	c8227dcc1cd6ecc684de8c5ea9b16e3b35f613f1	1ef8cdbd3773bd82e5be25d4
nefosferta[.]com	e9299fc9b7daa0742c28bfc4b03b7b25	77360abc473dc65c8bdd73b6459b9ea8fddb6f1d	22e3f4602a258e92a0b8deb5
nefosferta[.]com	775fb391db27e299af08933917a3acda	eaaa5e68956a3a3f6113e965199f479e10ae9956	2d50b03a92445ba53ae147d
nefosferta[.]com	f4045710c99d347fe6dfa2c0fcadde29	b7bffdbbaf817d149bbd061070a2d171449afbfc	32ae88cddeeeec255d6d9c82
nefosferta[.]com	587acecdb9491e0897d1067eb02e7c8d	a9eb1ac4b85d17da3a2bae5835c7e862d481c189	55d1480cd023b74f10692c6
nefosferta[.]com	0bae65245e5423147fce079de29b6136	f24232330e6f428bfbb6b9d8154db1c4046c2fc2	6210a9f5a5e1dc27e68ecd61
nefosferta[.]com	5022a85b39a75ebe2bc0411d7b058b2e	a9040ac0e9f482454e040e2a7d874ddc50e6f6ce	68a86858b4638b43d63e8e2
nefosferta[.]com	6a2f114a8995dbeb91f766ac2390086e	edac3cf9533b6f7102f6324fadb437a0814cc680	72813522a065e106ac10aa96
nefosferta[.]com	e9115cc3280c16f9019e0054e059f4b8	dad01b0c745649c6c8b87dbeb7ab549ed039515d	7a64bc69b60e3cd3fd00d442
nefosferta[.]com	b54cc9a3dd88e478ea601dfd5b36805e	318fdfec4575d1530a41c80274aa8caae7b7f631	7c607eca4005ba6415e09135
nefosferta[.]com	f129c12b1bda7426f6b31682b42ee4b0	5bb804153029c97fe23517ae5428a591c3c63f28	7c79ec3f5c1a280ffdf19d000
nefosferta[.]com	f68aa4c92dd30bd5418f136aaf6c07d6	aa56f43e39d114235a6b1d5f66b593cc80325fa4	7e39dcd15307e7de862b9b4
nefosferta[.]com	acac995cee8a6a75fa79eb41bdffa53f	971a00a392b99f64a3886f40b6ef991e62f0fe2f	97bae3587f1d2fd35f24eb21
nefosferta[.]com	36057710279d9f0d023cb5613aa76d5e	e4dd1f8fc4e44c8fd0e25242d994c4b59eed6939	97d0844ce9928e32b11706e
nefosferta[.]com	37e6904d84153d1435407f4669135134	1dcd85f7364ea06cd595a86e3e9be48995d596e9	bf3c7f0ba324c96c9a9bff6cf
nefosferta[.]com	4f3916e7714f2a32402c9d0b328a2c91	87a692e3592f7b997c7d962919e243b665f2be36	c3743a8c944f5c9b17528418
nefosferta[.]com	d9daaa0df32b0bb01a09e500fc7f5881	f9cb839adba612db5884e1378474996b4436c0cd	c3b3640ddf53b26f4ebd4eed
nefosferta[.]com	c87fb9b9f6c343670bed605420583418	f05cf0b026b2716927dac8bcd26a2719ea328964	c6c4f690f0d15b96034b4258
nefosferta[.]com	2be64efd0fa7739123b26e4b70e53c5c	318fdfec4575d1530a41c80274aa8caae7b7f631	ed38c454575879c2546e5fcc

Table 5: Truebot IOCs Connected to Russia, and Panama Locations			
Malicious Domain	**IP Addresses**	**Files**	**SHA256**
Dremmfyttrred[.]com			
	45.182.189[.]103		
	94.142.138[.]61		
	172.64.155[.]188		
	104.18.32[.]68		
		Update[.]exe	

Table 5: Truebot IOCs Connected to Russia, and Panama Locations			
		Document_26_apr_2443807[.]exe	
		3ujwy2rz7v[.]exe	
			fe746402c74ac329231ae1b5dffa8229b509f4c15a0f5085617f14f0c
droogggdhfhf[.]com		3LXJyA6Gf[.]exe	7d75244449fb5c25d8f196a43a6eb9e453652b2185392376e7d44c2

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 6-16 for all referenced cyber threat actor tactics and techniques for enterprise environments in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool .

Table 6: Initial Access		
Technique Title	**ID**	**Use**
Replication Through Removable Media	T1091	Cyber threat actors use removable media drives to deploy Raspberry Robin malware.
Drive-by Compromise	T1189	Cyber threat actors embed malicious links or attachments within web domains to gain initial access.
Exploit Public-Facing Application	T1190	Cyber threat actors are exploiting Netwrix vulnerability CVE-2022-31199 for initial access with follow-on capabilities of lateral movement through remote code execution.
Phishing	T1566.002	Truebot actors can send spear phishing links to gain initial access.

Table 7: Execution		
Technique Title	**ID**	**Use**
Command and Scripting Interpreter	T1059	Cyber threat actors have been observed dropping cobalt strike beacons as a reverse shell proxy to create persistence within the compromised network. Cyber threat actors use FlawedGrace to receive PowerShell commands over a C2 channel to deploy additional tools.
Shared Modules	T1129	Cyber threat actors can deploy malicious payloads through obfuscated share modules.
User Execution: Malicious Link	T1204.001	Cyber threat actors trick users into clicking a link by making them believe they need to perform a Google Chrome software update.

Table 8: Persistence		
Technique Title	**ID**	**Use**
Hijack Execution Flow: DLL Side-Loading	1574.002	Cyber threat actors use Raspberry Robin, among other toolsets to side-load DLLs to maintain persistence.

Table 9: Privilege Escalation		
Technique Title	**ID**	**Use**
Boot or Logon Autostart Execution: Print Processors	T1547.012	FlawedGrace malware manipulates print spooler functions to achieve privilege escalation.

Table 10: Defense Evasion		
Technique Title	**ID**	**Use**
Obfuscated Files or Information	T1027	Truebot uses a .JSONIP extension (e.g., IgtyXEQuCEvAM.JSONIP), to create a GUID.

Table 10: Defense Evasion		
Obfuscated Files or Information: Binary Padding	T1027.001	Cyber threat actors embed around one gigabyte of junk code within the malware string to evade detection protocols.
Masquerading: Masquerade File Type	T1036.008	Cyber threat actors hide Truebot malware as legitimate appearing file formats.
Process Injection	T1055	Truebot malware has the ability to load shell code after establishing a C2 connection.
Indicator Removal: File Deletion	T1070.004	Truebot malware implements self-deletion TTPs throughout its attack cycle to evade detection. Teleport exfiltration tool deletes itself after it has completed exfiltrating data to the C2 station.
Modify Registry	T1112	FlawedGrace is able to modify registry programs that control the order that documents are loaded to a print que.
Reflective Code Loading	T1620	Truebot malware has the capability to load shell code and deploy various tools to stealthily navigate an infected network.

Table 11: Credential Access		
Technique Title	**ID**	**Use**
OS Credential Dumping: LSASS Memory	T1003.001	Cyber threat actors use cobalt strike to gain valid credentials through LSASS memory dumping.

Table 12: Discovery		
Technique Title	**ID**	**Use**
System Network Configuration Discovery	T1016	Truebot malware scans and enumerates the affected system's domain names.
Process Discovery	T1057	Truebot malware enumerates all running processes on the local host.
System Information Discovery	T1082	Truebot malware scans and enumerates the OS version information, and processor architecture. Truebot malware enumerates the affected system's computer names.
System Time Discovery	T1124	Truebot has the ability to discover system time metrics, which aids in enables synchronization with the compromised system's internal clock to facilitate scheduling tasks.
Software Discovery: Security Software Discovery	T1518.001	Truebot has the ability to discover software security protocols, which aids in defense evasion.
Debugger Evasion	T1622	Truebot malware scans the compromised environment for debugger tools and enumerates them in effort to evade network defenses.

Table 13: Lateral Movement		
Technique Title	**ID**	**Use**
Exploitation of Remote Services	T1210	Cyber threat actors exploit CVE-2022-31199 Netwrix Auditor vulnerability and use its capabilities to move laterally within a compromised network.
Use Alternate Authentication Material: Pass the Hash	T1550.002	Cyber threat actors use cobalt strike to authenticate valid accounts
Remote Service Session Hijacking	T1563.001	Cyber threat actors use cobalt strike to hijack remote sessions using SSH and RDP hijacking methods.

Table 13: Lateral Movement		
Remote Service Session Hijacking: RDP Hijacking	T1563.002	Cyber threat actors use cobalt strike to hijack remote sessions using SSH and RDP hijacking methods.
Lateral Tool Transfer	T1570	Cyber threat actors deploy additional payloads to transfer toolsets and move laterally.

Table 14: Collection		
Technique Title	**ID**	**Use**
Data from Local System	T1005	Truebot malware checks the current version of the OS and the processor architecture and compiles the information it receives. Truebot gathers and compiles compromised system's host and domain names.
Screen Capture	T1113	Truebot malware takes snapshots of local host data, specifically processor architecture data, and sends that to a phase 2 encoded data string.

Table 15: Command and Control		
Technique Title	**ID**	**Use**
Application Layer Protocol	T1071	Cyber threat actors use teleport exfiltration tool to blend exfiltrated data with network traffic.
Non-Application Protocol	T1095	Cyber threat actors use Teleport and FlawedGrace to send data over custom communication protocol.
Ingress Transfer Tool	T1105	Cyber threat actors deploy various ingress transfer tool payloads to move laterally and establish C2 connections.
Encrypted Channel: Asymmetric Cryptography	T1573.002	Cyber threat actors use Teleport to create an encrypted channel using AES.

Table 16: Exfiltration		
Technique Title	**ID**	**Use**
Scheduled Transfer	T1029	Teleport limits the data it collects and syncs with outbound organizational data/network traffic.
Data Transfer Size Limits	T1030	Teleport limits the data it collects and syncs with outbound organizational data/network traffic.
Exfiltration Over C2 Channel	T1048	Cyber threat actors blend exfiltrated data with network traffic to evade detection. Cyber threat actors use the Teleport tool to exfiltrate data over a C2 protocol.

DETECTION METHODS

CISA and authoring organizations recommend that organizations review and implement the following detection signatures, along with: `Win/malicious_confidence100% (W)`, `Trojan:Win32/Tnega!MSR`, and `Trojan.Agent.Truebot.Gen`, as well as YARA rules below to help detect Truebot malware.

Detection Signatures

Figure 2: Snort Signature to Detect Truebot Malware

```
alert tcp any any -> any any (msg:"TRUEBOT: Client HTTP Header"; sid:x; rev:1; flow:established,to_server;
content:"Mozilla/112.0 (compatible|3b 20 4d 53 49 45 20 31 31 2e 30 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20
31 30 2e 30 30 29|"; http_header; nocase; classtype:http-header; metadata:service http;)
```

YARA Rules

CISA developed the following YARA to aid in detecting the presence of Truebot Malware.

Figure 3: YARA Rule for Detecting Truebot Malware

```
rule CISA_10445155_01 : TRUEBOT downloader
{
meta:
Author = "CISA Code & Media Analysis"
Incident = "10445155"
Date = "2023-05-17"
Last_Modified = "20230523_1500"
Actor = "n/a"
Family = "TRUEBOT"
Capabilities = "n/a"
Malware_Type = "downloader"
Tool_Type = "n/a"
Description = "Detects TRUEBOT downloader samples"
SHA256 = "7d75244449fb5c25d8f196a43a6eb9e453652b2185392376e7d44c21bd8431e7"
strings:
$s1 = { 64 72 65 6d 6d 66 79 74 74 72 72 65 64 2e 63 6f 6d }
$s2 = { 4e 73 75 32 4f 64 69 77 6f 64 4f 73 32 }
$s3 = { 59 69 50 75 6d 79 62 6f 73 61 57 69 57 65 78 79 }
$s4 = { 72 65 70 6f 74 73 5f 65 72 72 6f 72 2e 74 78 74 }
$s5 = { 4c 6b 6a 64 73 6c 66 6a 33 32 6f 69 6a 72 66 65 77 67 77 2e 6d 70 34 }
$s6 = { 54 00 72 00 69 00 67 00 67 00 65 00 72 00 31 00 32 }
$s7 = { 54 00 55 00 72 00 66 00 57 00 65 00 73 00 54 00 69 00 66 00 73 00 66 }
condition:
5 of them
}
```

- Additional YARA rules for detecting Truebot malware can be referenced from GitHub.[9]

INCIDENT RESPONSE

The following steps are recommended if organizations detect a Truebot malware infection and compromise:

1. Quarantine or take offline potentially affected hosts.
2. Collect and review artifacts such as running processes/services, unusual authentications, and recent network connections.
3. Provision new account credentials.
4. Reimage compromised host.
5. Report the compromise to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 1-844-Say-CISA) or contact your local FBI field office. State, local, tribal, or territorial government entities can also report to MS-ISAC (SOC@cisecurity.org or 866-787-4722).

MITIGATIONS

CISA and the authoring organizations recommend organizations implement the below mitigations, including mandating phishing-resistant multifactor authentication (MFA) for all staff and services.

For additional best practices, see CISA's Cross-Sector Cybersecurity Performance Goals (CPGs). The CPGs, developed by CISA and the National Institute of Standards and Technology (NIST), are a prioritized subset of IT and OT security practices that can meaningfully reduce the likelihood and impact of known cyber risks and common TTPs. Because the CPGs are a subset of best practices, CISA and co-sealers recommend software manufacturers implement a comprehensive information security program based on a recognized framework, such as the NIST Cybersecurity Framework (CSF).

- Apply patches to CVE-2022-31199
- Update Netwrix Auditor to version 10.5

Netwrix recommends using their Auditor application only on internally facing networks. System owners that don't follow this recommendation, and use the application in externally facing instances, are at increased risk to having CVE-2022-31199 exploited on their systems.

Reduce threat of malicious actors using remote access tools by:

- **Implementing application controls to manage and control execution of software**, including allowlisting remote access programs.
  - Application controls should prevent installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.

See the National Security Agency's Cybersecurity Information sheet, Enforce Signed Software Execution Policies, and additional guidance below:

- **Strictly limit the use of RDP and other remote desktop services**. If RDP is necessary, rigorously apply best practices, for example [CPG 2.W]:
  - Audit the network for systems using RDP.
  - Close unused RDP ports.
  - Enforce account lockouts after a specified number of attempts.
  - Apply phishing-resistant multifactor authentication (MFA).
  - Log RDP login attempts.
- **Disable command-line and scripting activities and permissions** [CPG 2.N].
- Restrict the use of PowerShell by using Group Policy, and only grant to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows operating systems (OSs) should be permitted to use PowerShell [CPG 2.E].
- **Update Windows PowerShell or PowerShell Core** to the latest version and uninstall all earlier PowerShell versions. Logs from Windows PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities [CPG 1.E, 2.S, 2.T].
- **Enable enhanced PowerShell logging** [CPG 2.T, 2.U].
  - PowerShell logs contain valuable data, including historical OS and registry interaction and possible IOCs of a cyber threat actor's PowerShell use.
  - Ensure PowerShell instances, using the latest version, have module, script block, and transcription logging enabled (enhanced logging).
  - The two logs that record PowerShell activity are the PowerShell Windows Event Log and the PowerShell Operational Log. The authoring organizations recommend turning on these two Windows Event Logs with a retention period of at least 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.
- **Configure the Windows Registry to require User Account Control (UAC) approval for any PsExec operations** requiring administrator privileges to reduce the risk of lateral movement by PsExec.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts [CPG 4.C].
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege (PoLP) [CPG 2.E].
- Reduce the threat of credential compromise via the following:
  - **Place domain admin accounts in the protected users' group** to prevent caching of password hashes locally.
  - **Implement Credential Guard for Windows 10 and Server 2016** (Refer to Microsoft: Manage Windows Defender Credential Guard for more information). For Windows Server 2012R2, enable Protected Process Light for Local Security Authority (LSA).
  - **Refrain from storing plaintext credentials in scripts**.
- **Implement time-based access for accounts set at the admin level and higher** [CPG 2.A, 2.E]. For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory (AD) level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.

In addition, CISA, FBI, MS-ISAC, and CCCS recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the impact and risk of compromise by ransomware or data extortion actors:

- **Disable File and Printer sharing services**. If these services are required, use strong passwords or Active Directory authentication.
- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (e.g., hard drive, storage device, or the cloud).
- **Maintain offline backups of data** and regularly maintain backup and restoration (daily or weekly at minimum). By instituting this practice, an organization minimizes the impact of disruption to business practices as they can retrieve their data [CPG 2.R].
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) **to comply** with National Institute for Standards and Technology (NIST) standards for developing and managing password policies.
    - Use longer passwords consisting of at least 15 characters [CPG 2.B].
    - Store passwords in hashed format using industry-recognized password managers.
    - Add password user “salts” to shared login credentials.
    - Avoid reusing passwords [CPG 2.C].
    - Implement multiple failed login attempt account lockouts [CPG 2.G].
    - Disable password “hints.”
    - Refrain from requiring password changes more frequently than once per year.
      Note: NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password “patterns” cyber criminals can easily decipher.
    - Require administrator credentials to install software.
- **Require phishing-resistant multifactor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems [CPG 2.H].
- **Keep all operating systems, software, and firmware up to date**. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Organizations should patch vulnerable software and hardware systems within 24 to 48 hours of vulnerability disclosure. Prioritize patching known exploited vulnerabilities in internet-facing systems [CPG 1.E].
- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to various subnetworks, restricting further lateral movement [CPG 2.F].
- Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool. To aid in detecting ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections, as they have insight into common and uncommon network connections for each host [CPG 3.A].
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Disable unused ports** [CPG 2.V].
- **Consider adding an email banner to emails** received from outside your organization [CPG 2.M].
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization’s data infrastructure [CPG 2.K, 2.L, 2.R].

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA recommends exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. CISA recommends testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 5-13).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies’ performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA recommends continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- NIST: NVD - CVE-2022-31199
- Stopransomware.gov (A whole-of-government approach with one central location for U.S. ransomware resources and alerts.)
- #StopRansomware Guide
- CISA: Implement Phishing-Resistant MFA
- CISA: Guide to Securing Remote Access Software
- CISA and MS-ISAC: Joint Ransomware Guide
- CISA: Cross-Sector Cybersecurity Performance Goals
- CL0P Ransomware Uses Truebot Malware for Access to Networks
- Field Offices – FBI
- NSA – Zero Trust Security Model

REFERENCES

[1] Bishop Fox: Netwrix Auditor Advisory
[2] Talos Intelligence: Breaking the Silence - Recent Truebot Activity
[3] The DFIR Report: Truebot Deploys Cobalt Strike and FlawedGrace
[4] MAR-10445155-1.v1 .CLEAR Truebot Activity Infects U.S. and Canada Based Networks
[5] Red Canary: Raspberry Robin Delivery Vector
[6] Microsoft: Raspberry Robin Worm Part of a Larger Ecosystem Pre-Ransomware Activity
[7] Telsy: FlawedGrace RAT
[8] VMware Security Blog: Carbon Black's Truebot Detection
[9] GitHub: DFIR Report - Truebot Malware YARA Rule

Additional Sources

Alarming Surge in TrueBot Activity Revealed with New Delivery Vectors (thehackernews.com)
Truebot Analysis Part 1
Truebot Analysis Part 2
Truebot Analysis Part 3
Truebot Exploits Netwrix Vulnerability
TrueBot malware delivery evolves, now infects businesses in the US and elsewhere
Malpedia-Silence Downloader
Printer spooling: what is it and how to fix it? | PaperCut

ACKNOWLEDGEMENTS

VMware Carbon Black and Mandiant contributed to this CSA.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA and authoring agencies do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA, and co-sealers.
