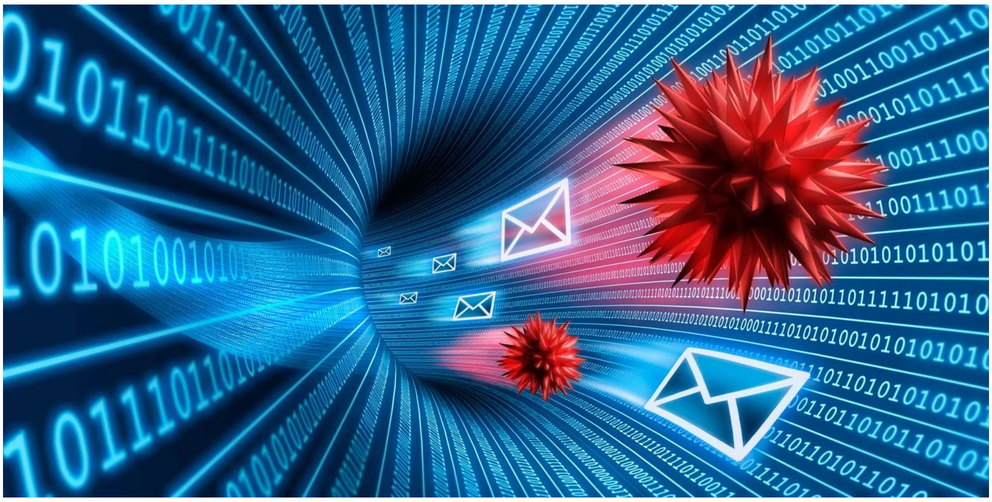
Home (https://www.bleepingcomputer.com/) › News (https://www.bleepingcomputer.com/news/) › Security (https://www.bleepingcomputer.com/news/security/) › New phishing attack infects devices with Cobalt Strike

New phishing attack infects devices with Cobalt Strike

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

June 18, 2022 10:06 AM **0**



Security researchers have noticed a new malicious spam campaign that delivers the 'Matanbuchus' malware to drop Cobalt Strike beacons on compromised machines.

Cobalt Strike is a penetration testing suite that is frequently used by threat actors for lateral movement and to drop additional payloads.

Matanbuchus is a malware-as-a-service (MaaS) project first spotted in February 2021 in advertisements on the dark web promoting it as a $2,500 loader that launches executables directly into system memory.

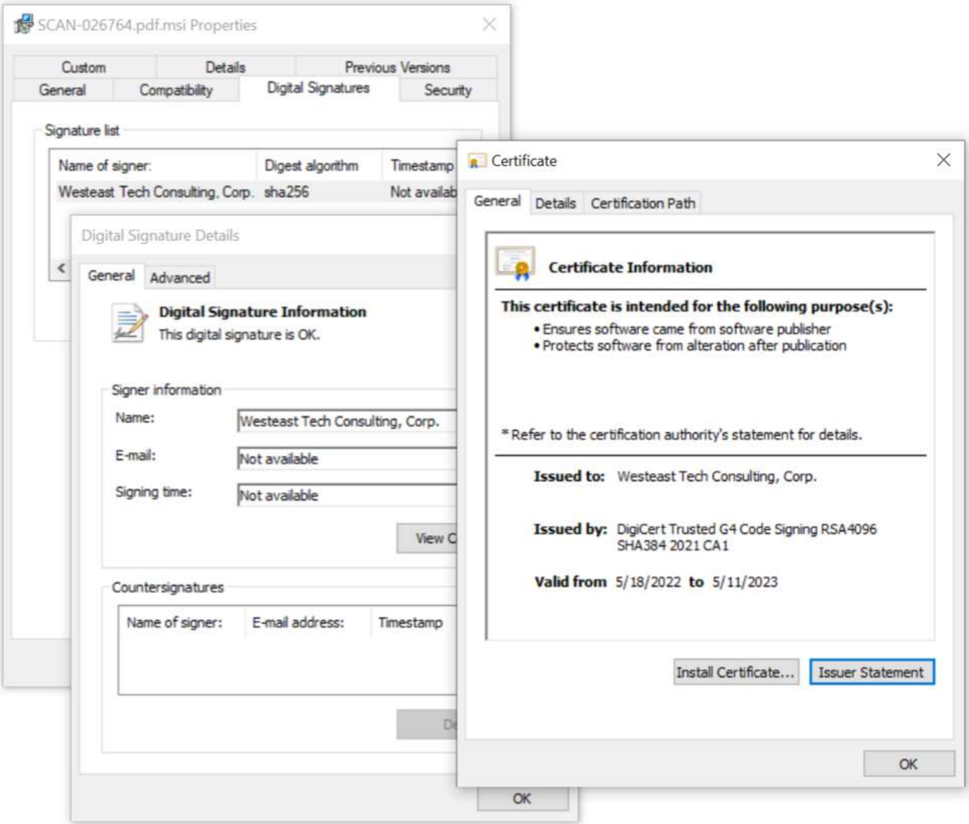
Palo Alto Networks' Unit 42 analyzed it in June 2021 (https://unit42.paloaltonetworks.com/matanbuchus-malware-as-a-service/) and mapped extensive parts of its operational infrastructure. The malware's features include launching custom PowerShell commands, leveraging standalone executables to load DLL payloads, and establishing persistence via the addition of task schedules.

Ongoing campaign

Threat analyst Brad Duncan (https://twitter.com/malware_traffic) captured a sample of the malware and examined (https://isc.sans.edu/forums/diary/Malspam+pushes+Matanbuchus+malware+leads+to+Cobalt+Strike/28752/) how it works in a lab environment.

The malspam campaign currently underway uses lures that pretend to be replies to previous email conversations, so they feature a 'Re:' in the subject line.

The emails carry a ZIP attachment that contains an HTML file that generates a new ZIP archive. This ultimately extracts an MSI package digitally signed with a valid certificate issued by DigiCert for "Westeast Tech Consulting, Corp."



Name of signer:	Digest algorithm	Timestamp
Westeast Tech Consulting, Corp.	sha256	Not availab

Digital Signature Information
This digital signature is OK.

Signer information
Name: Westeast Tech Consulting, Corp.
E-mail: Not available
Signing time: Not available

Countersignatures

Name of signer:	E-mail address:	Timestamp

Certificate Information

This certificate is intended for the following purpose(s):
- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Westeast Tech Consulting, Corp.

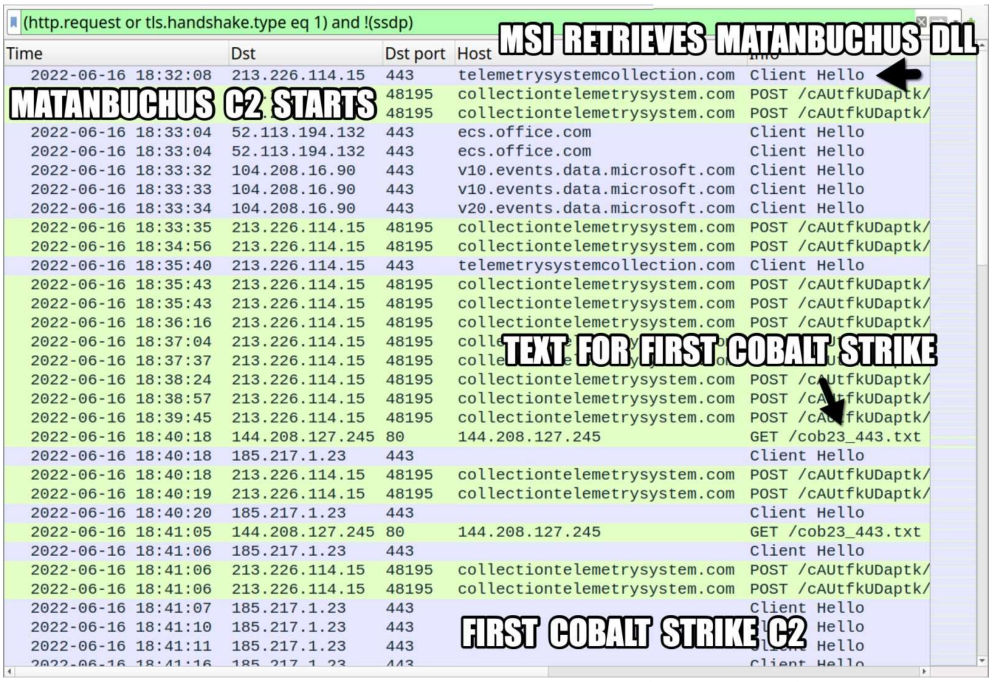
Issued by: DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1

Valid from 5/18/2022 to 5/11/2023

Valid digital certificate used on the MSI file *(isc.sans.edu)*

Running the MSI installer supposedly initiates an Adobe Acrobat font catalog update that ends with an error message, to distract the victim from what happened behind the scenes.

In the background, two Matanbuchus DLL payloads ("main.dll") are dropped in two different locations, a scheduled task is created to maintain persistence across system reboots, and communication with the command and control (C2) server is established.



```
(http.request or tls.handshake.type eq 1) and !(ssdp)
Time                 Dst              Dst port Host                          Info
  2022-06-16 18:32:08 213.226.114.15   443      telemetrysystemcollection.com Client Hello
                                       48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
                                       48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:33:04 52.113.194.132   443      ecs.office.com                Client Hello
  2022-06-16 18:33:04 52.113.194.132   443      ecs.office.com                Client Hello
  2022-06-16 18:33:32 104.208.16.90    443      v10.events.data.microsoft.com Client Hello
  2022-06-16 18:33:33 104.208.16.90    443      v10.events.data.microsoft.com Client Hello
  2022-06-16 18:33:34 104.208.16.90    443      v20.events.data.microsoft.com Client Hello
  2022-06-16 18:33:35 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:34:56 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:35:40 213.226.114.15   443      telemetrysystemcollection.com Client Hello
  2022-06-16 18:35:43 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:35:43 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:36:16 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:37:04 213.226.114.15   48195    colle
  2022-06-16 18:37:37 213.226.114.15   48195    colle
  2022-06-16 18:38:24 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:38:57 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:39:45 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:40:18 144.208.127.245  80       144.208.127.245               GET /cob23_443.txt
  2022-06-16 18:40:18 185.217.1.23     443                                    Client Hello
  2022-06-16 18:40:18 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:40:19 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:40:20 185.217.1.23     443                                    Client Hello
  2022-06-16 18:41:05 144.208.127.245  80       144.208.127.245               GET /cob23_443.txt
  2022-06-16 18:41:06 185.217.1.23     443                                    Client Hello
  2022-06-16 18:41:06 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:41:06 213.226.114.15   48195    collectiontelemetrysystem.com POST /cAUtfkUDaptk/
  2022-06-16 18:41:07 185.217.1.23     443                                    Client Hello
  2022-06-16 18:41:10 185.217.1.23     443                                           Hello
  2022-06-16 18:41:11 185.217.1.23     443                                           Hello
  2022-06-16 18:41:16 185.217.1.23     443                                    Client Hello
```

Snapshot of malicious network traffic *(isc.sans.edu)*

Finally, Matanbuchus loads the Cobalt Strike payload from the C2 server, opening the way to wider exploitation potential.

Matanbuchus current infection chain *(isc.sans.edu)*

Cobalt Strike as a second-stage payload in Metanbuchus malspam campaign was first reported by DCSO (https://medium.com/@DCSO_CyTec/a-deal-with-the-devil-analysis-of-a-recent-matanbuchus-sample-3ce991951d6a), a German security company, on May 23, 2022. They also noticed that Qakbot was also delivered in some cases.

Interestingly, in that campaign, the digital signature used for the MSI file was again a valid one from DigiCert, issued to "Advanced Access Services LTD."

The exposed Matanbuchus dashboard *(Bleeping Computer)*

For recent indicators of compromise, defenders can check out those collected by DCSO (https://github.com/DCSO/Blog_CyTec/blob/main/a_deal_with_the_devil/misp.event.json) and the IoCs posted by 'Execute Malware (https://github.com/executemalware/Malware-IOCs/blob/main/2022-06-16%20Matanbuchus%20IOCs)' about the ongoing campaign.

Duncan has also posted on his website (https://www.malware-traffic-analysis.net/2022/06/16/index.html) traffic samples, artifacts, examples, and indicators of compromise (IoCs).

Related Articles:

Typosquat campaign mimics 27 brands to push Windows, Android malware (https://www.bleepingcomputer.com/news/security/typosquat-campaign-mimics-27-brands-to-push-windows-android-malware/)

Hackers use new stealthy PowerShell backdoor to target 60+ victims (https://www.bleepingcomputer.com/news/security/hackers-use-new-stealthy-powershell-backdoor-to-target-60-plus-victims/)

Ursnif malware switches from bank account theft to initial access (https://www.bleepingcomputer.com/news/security/ursnif-malware-switches-from-bank-account-theft-to-initial-access/)

Hacking group updates Furball Android spyware to evade detection (https://www.bleepingcomputer.com/news/security/hacking-group-updates-furball-android-spyware-to-evade-detection/)

Malware dev claims to sell new BlackLotus Windows UEFI bootkit (https://www.bleepingcomputer.com/news/security/malware-dev-claims-to-sell-new-blacklotus-windows-uefi-bootkit/)

COBALT STRIKE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/COBALT-STRIKE/)

MALSPAM (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MALSPAM/)

MALWARE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MALWARE/)

MATANBUCHUS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MATANBUCHUS/)

(https://www.bleepingcomputer.com/author/bill-toulas/)

BILL TOULAS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/BILL-TOULAS/)

(MAILTO:BILL.TOULAS@BLEEPINGCOMPUTER.COM)

(HTTPS://TWITTER.COM/BILLTOULAS)

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

PREVIOUS ARTICLE

(HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/THE-WEEK-IN-RANSOMWARE-JUNE-17TH-2022-HAVE-I-BEEN-RANSOMED/)

NEXT ARTICLE

(HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/TECHNOLOGY/CH BROWSER-EXTENSION-LETS-YOU-REMOVE-SPECIFIC-SITES-FROM-SEARCH-RESULTS/)

Post a Comment

Community Rules (https://www.bleepingcomputer.com/posting-guidelines/)

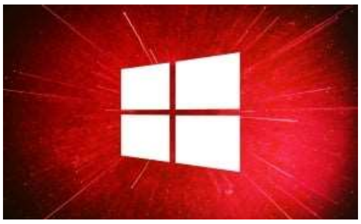
You need to login in order to post a comment

Login

Not a member yet? Register Now (https://www.bleepingcomputer.com/forums/index.php?app=core&module=global&section=register)

You may also like:

POPULAR STORIES



Exploited Windows zero-day lets JavaScript files bypass security warnings (https://www.bleepingcomputer.com/news/security/exploited-windows-zero-day-lets-javascript-files-bypass-security-warnings/)

Hackers exploit critical VMware flaw to drop ransomware, miners (https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-vmware-flaw-to-drop-ransomware-miners/)

NEWSLETTER SIGN UP

To receive periodic updates and news from BleepingComputer (/), please use the form below.

Email Address...

Submit

NEWSLETTER SIGN UP

Email Address...

SUBMIT

Follow us:

[illegible]

MAIN SECTIONS

News (https://www.bleepingcomputer.com/)

Downloads (https://www.bleepingcomputer.com/download/)

Virus Removal Guides (https://www.bleepingcomputer.com/virus-removal/)

Tutorials (https://www.bleepingcomputer.com/tutorials/)

Startup Database (https://www.bleepingcomputer.com/startups/)

Uninstall Database (https://www.bleepingcomputer.com/uninstall/)

Glossary (https://www.bleepingcomputer.com/glossary/)

COMMUNITY

Forums (https://www.bleepingcomputer.com/forums/)

Forum Rules (https://www.bleepingcomputer.com/forum-rules/)

Chat (https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/)

USEFUL RESOURCES

Welcome Guide (https://www.bleepingcomputer.com/welcome-guide/)

Sitemap (https://www.bleepingcomputer.com/sitemap/)

COMPANY

About BleepingComputer (https://www.bleepingcomputer.com/about/)

Contact Us (https://www.bleepingcomputer.com/contact/)

Send us a Tip! (https://www.bleepingcomputer.com/news-tip/)

Advertising (https://www.bleepingcomputer.com/advertise/)

Write for BleepingComputer (https://www.bleepingcomputer.com/write-for-bleepingcomputer/)

Social & Feeds (https://www.bleepingcomputer.com/rss-feeds/)

Changelog (https://www.bleepingcomputer.com/changelog/)

Terms of Use (https://www.bleepingcomputer.com/terms-of-use/) - Privacy Policy (https://www.bleepingcomputer.com/privacy/) - Ethics Statement (https://www.bleepingcomputer.com/ethics-statement/)