Inside a VenomRAT Malware Campaign

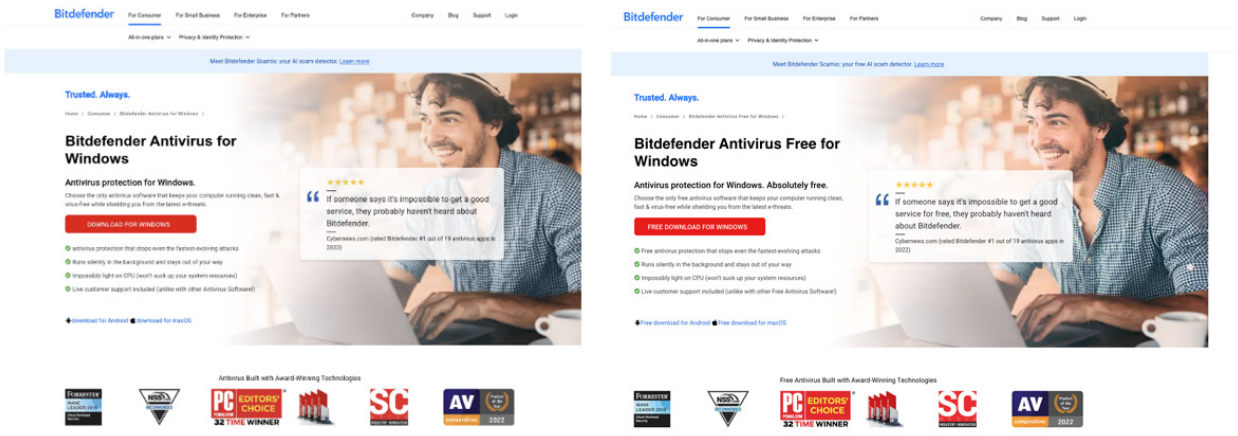
dti.domaintools.com/VenomRAT/

May 27, 2025

A malicious campaign using a fake website to spread VenomRAT, a Remote Access Trojan (RAT), is detailed in this analysis. The malware includes tools for password theft and stealthy access. This research examines the attackers' methods, such as deceptive websites and command infrastructure, indicating a clear intent to target individuals for financial gain by compromising their credentials, crypto wallets, and potentially selling access to their systems.

VenomRAT, StormKitty, and SilentTrinity Deployment

Malicious domain "bitdefender-download[.]com" resolves a website titled "DOWNLOAD FOR WINDOWS," which spoofs Bitdefender's Antivirus for Windows download page.



The left shows the spoofed version of Bitdefender's Antivirus for Windows download page while the right shows the legitimate page. There are subtle differences between them such as the legitimate page using the word "free" in several places whereas the spoofed version does not.

The "Download For Windows" button initiates a file download from the following bitbucket URL:

"https[:]//bitbucket[.]org/sadsafsadfsadf/dsfgdsgssdfgdsg/downloads/BitDefender.zip,"

The bitbucket URL redirects to its content source on Amazon S3.

"https[:]//bbuseruploads.s3.amazonaws[.]com/9e2daa63-bae3-4cbb-9f88-8154ba43261f/downloads/aa7b9593-2ccd-4cd0-9e04-9b4a7da9276b/BitDefender.zip."

File Name	SHA256
BitDefender.zip	59a08decb8b960b65afe4d5446ef0e00e3a49ab747599b5ee6e7d43813040287
StoreInstaller.exe	e33b8b32bccfb50f604f06a306d1af89ae7b0d583bca20c41fa5811f526aa420

The bundled executable StoreInstaller.exe was found to contain malware configurations associated with VenomRAT. It also contained code associated with open source post-exploitation framework SilentTrinity and StormKitty stealer.

A report by Arconis describes VenomRAT as a RAT that originated as a fork of the open-source Quasar RAT. It is often used for initial access and persistence. Capabilities include remote access, stealing credentials, keylogging, exfiltration and more.

At a high level, the three malware families function as follows:

- VenomRAT provides initial and ongoing access to victim machines
- StormKitty quickly gathers credentials on the system
- SilentTrinity is used for exfiltration and stealthy long term access

The inclusion of SilentTrinity and StormKitty (both open-source malware tools) indicates the attacker's dual focus: rapidly harvesting financial credentials and crypto wallets during initial access, while also establishing stealthy, persistent access for potential long-term exploitation. The implications of long term access may include repeat compromise or selling access.

VenomRAT

Observed VenomRAT configurations showed multiple identifiable attributes that allowed for reliable pivots to other samples likely created by the same actor including the reuse of the same IP and port, 67.217.228[.]160:4449, for command and control.

Related samples using the same VenomRAT configurations:

File Name	SHA256
StoreInstaller.exe	eb2b61a5f15b19bf7dd0ff3914d3019c26499dd693647b00c1b073037db72e35
File[@nightcore_4].exe	2d3dc51e6752c4fe95b2b7928ed11b5e06c6a68d19b7d884ab2c8eaab97d4e07
ClientAny.exe	b1810daed3653b8c2047ff05a01a67d840ce045b17b39c60f335d798612e96aa ab81ceeb26e22a7c6981a8479cccaa184675ad194b83e447185a1ce42abfbcb0 aa136a75b8fd954cf753c2c17fcde993b37b79af2f6b5a49556183e9f420fd56 f0e479cf0dadc7f7d1f999e091b013d236f2c7959591a6b1268ba31b89442ec6 72b7856f3c6851a36642e952b4fb772b9ea0a6a4075c2ed4b59e60cb922f82e3 7c3a49906e67a1928113554ff75f684ee54ab74abcf26ac1211d0cd8726cb086 68f6ff2543066ec8028d9bc101a17a60c47b693bdc0ee4d6167f17d5d4921ab9 4541fd01a19f1e484f24eff86f42ac36ea9b30686fd405ca0a50f3e517657a61 505ab745198ddb59201abd0292af2b2bb0b6360d5807a2969c1518ae60a396c8
WEXTRACT.EXE.MUI	ab5e758b27ca23fb06cccb7a5d0e337757b30f5eb0093c03071792516e64ed76 6c8d7f5c3d035f134b7d24594c0c409f1fce4bd460d0b2c634fe49c758c44b13 47e1270376345760986d86218c23c66c74afec864fbf6f1d300a6f39ab13f341 5129e8833504d66bb7332a60e1677697bf3a4ecb2f763acee926e4a6add24160
rasdlui.exe	e07f8aa872a5bc6da07e6ddad3a3e9b7e1a57cec33b5bf16d6b56a150318fd81
Debris.exe	1b6ed428a5e8255860a44ed6ed3c06079625b6a35762f363029ccb1b322392d4

VenomRAT C2 IPs

67.217.228[.]160:4449
172.93.222[.]102:4449
15.228.248[.]225:5552
94.141.123[.]234:4449
157.20.182[.]72:4449
185.208.159[.]121:6000
109.248.144[.]175:4449
95.216.115[.]242:9090

A reused 3389 service configuration was identified via Shodan “hash:-971903248” allowing for pivots to additional IP addresses with the same configurations. Multiple of the IPs were confirmed to be used as C2s for VenomRAT and are suspected to have also been configured by the same actor.

157.20.182[.]35
185.23.253[.]204
157.20.182[.]68
185.23.253[.]138
157.20.182[.]167
212.232.22[.]77
157.20.182[.]72

Delivery Sites:

bitdefender-download[.]com
http[:]//185.156.72[.]2/files/5297474040/aNXlZBn.exe
https[:]//github[.]com/legendary99999/fbvsfdbafdbdqba/releases/download/fdbagbagdbad/adsqwe.exe/
https[:]//bitbucket[.]org/sadsafsadfsadf/dsfgdsgssdfgdsg/downloads/BitDefender.zip
https[:]//bbuseruploads.s3.amazonaws[.]com/9e2daa63-bae3-4cbb-9f88-8154ba43261f/downloads/aa7b9593-2ccd-4cd0-9e04-9b4a7da9276b/BitDefender.zip

Credential Harvesting Sites

The lure website domain spoofing as Bitdefender was observed with infrastructure and time proximity overlaps to other malicious domains impersonating banks and generic IT services, suspected of being used for phishing activity.

NameServer: cloudflare.com

IP ISP: cloudflare.com

Registrar:

- PDR Ltd
- GMO Internet
- NameSilo

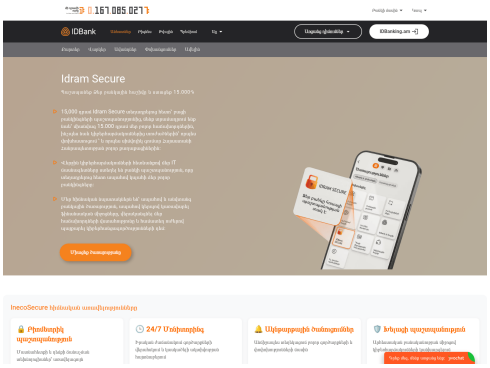
SSL Issuer:

- Cloudflare TLS
- WE1

Server Type: cloudflare

idram-secure[.]live

Spoofs as Armenian IDBank page



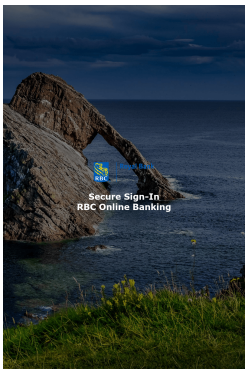
idram-secure[.]live

Clicking directs to a site titled “ArmCoin” and the content alleges to be IDBank.

The text is in Armenian and translates to: “To connect you to Idram Secure, please write to us in the chat. 🎉
Our chat is located in the bottom right corner of the page”

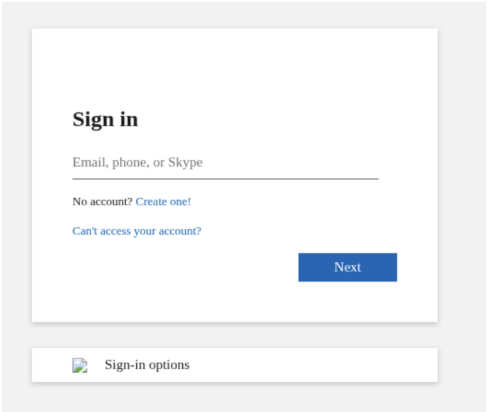
royalbanksecure[.]online

Spoofs as Royal Bank of Canada online banking login portal



dataops-tracxn[.]com

Spoofs as Microsoft login page



Protection from Open-Source Malware

This investigation reveals a deceptive campaign using VenomRAT, a powerful remote access tool, disguised as a legitimate Bitdefender antivirus download. Imagine clicking a button on what looks like a trusted site, only to unleash a trio of malicious programs – VenomRAT, StormKitty, and SilentTrinity –

onto your system. These tools work in concert: VenomRAT sneaks in, StormKitty grabs your passwords and digital wallet info, and SilentTrinity ensures the attacker can stay hidden and maintain control. We tracked down the attackers' command centers, identified other malware they likely used, and uncovered their web of fake download sites and phishing traps spoofing as banks and online services.

This campaign underscores a constant trend: attackers are using sophisticated, modular malware built from open-source components. This "build-your-own-malware" approach makes these attacks more efficient, stealthy, and adaptable. While the open-source nature of these tools can help security experts spot them faster, the primary victims here are everyday internet users. These criminals are after your hard-earned money, targeting your bank accounts and cryptocurrency wallets with fake login pages and malware disguised as safe software.

This isn't just a problem for big companies – it's a threat to everyone online. So, what can you do?

- **Be extremely cautious** when downloading software. Double-check website addresses to make sure they're legitimate, especially for banking or login pages.
- **Never enter your credentials** on a site you're not 100% sure about.
- **Practice safe internet habits:** avoid clicking on suspicious links or opening unexpected email attachments.

IOCs on GitHub

https://github.com/DomainTools/SecuritySnacks/blob/main/2025/VenomRAT-Malware-Campaign.csv

If the community has any additional input, please let us know.

Sign Up For DomainTools Investigations' Newsletter for the Latest Research

Want more from DomainTools Investigations? Be sure to sign up for our monthly newsletter to get the latest research from the team – available on LinkedIn or email.