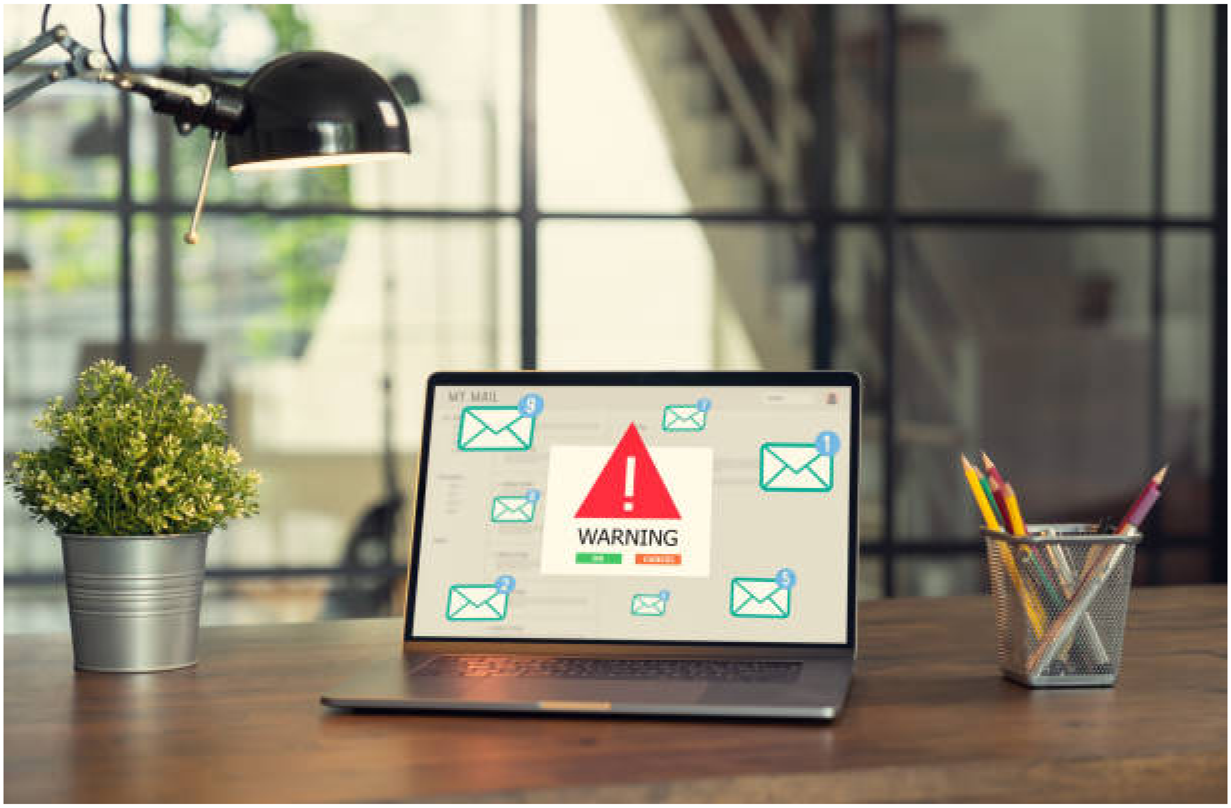
Malspam Campaign Delivers Dark Crystal RAT (dcRAT)

blogs.infoblox.com/cyber-threat-intelligence/cyber-campaign-briefs/malspam-campaign-delivers-dark-crystal-rat-dcrat/

Infoblox Cyber Intelligence Group

October 12, 2021



Author: Avinash Shende

1. Overview

From 30 September to 4 October, Infoblox observed a malicious email campaign distributing the remote access trojan (RAT) Dark Crystal, which is also known as dcRAT. This malware is propagated via a Microsoft Word document that contains a malicious VBA script.

A May 2020 report[1] said that dcRAT was being sold on hxxp://dcrat[.]ru. Since then, the site has been taken down, the content of the landing page has been replaced with Russian profanities, and distribution of dcRAT has shifted to hacking forums and P2P platforms.

2. Customer impact

Cybercriminals use dcRAT for various purposes, such as to:

- Browse the internet by using victims' machines
- Collect clipboard data
- Collect cookies

- Compile and execute C# code
- Execute remote commands
- Exfiltrate files
- Initialize UDP/TCP flood attacks
- Log keystrokes
- Manage file systems
- Manage running processes
- Turn on webcams and microphones on victims' machines

These and other capabilities allow dcRAT to steal information and use a victim's machine for subsequent attacks.

3. Campaign analysis

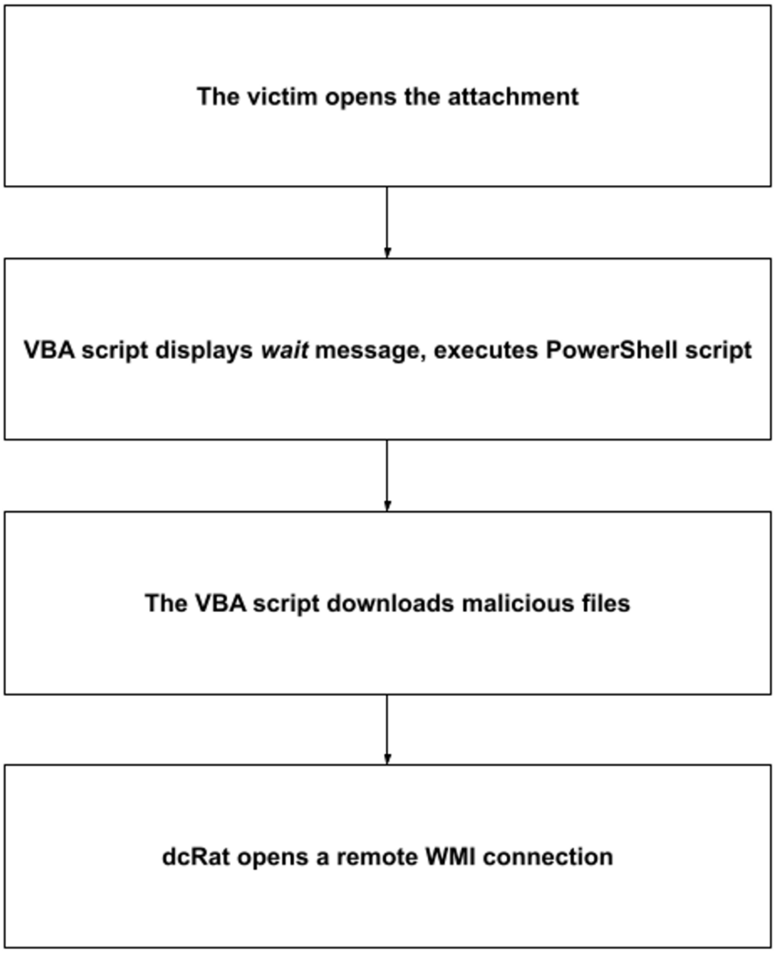
The email's subject is *Don't Miss Your Luck* or *Hi Friend*, the attachment is called *MoneyMake.doc*, and the sender's alias is *James Leclar*, *Paul Maccartney*, *Money Center, Money Development*, *Martin Garix*, *or ADS center.* To lure the victims into confirming their email addresses and opening the attachment, the actors use the following text in the email:

Please confirm your email address link below. Online training, the purpose of which is to acquaint students with the technology of remote earnings on TUZIR Internet advertising. This system has proven to be highly effective and is used by many newbies and experienced directors to earn remotely without leaving their main place of work. The author of the technology of earning money from advertising and the speaker of the program is Evgeny Andrianov. All info in Attachment — The Advertising Company.

4. Attack chain

Opening the Word attachment executes the password-protected VBA script, which starts a series of downloads and displays the message *Running Document. Please Wait.* The script also contacts a URL, from where it executes a PowerShell script to download a JavaScript file, loader.js, which downloads a malicious JavaScript-encoded file, KEiZizen[.]jse, and deletes itself. KEiZizen[.]jse then downloads the malicious screensaver file found[.]scr, which downloads savesrefruntimeCrtCommonMonitordhcp.exe. This executable attempts to determine whether it is working on a virtual machine, creates or modifies registry values, creates processes, connects to the C&C server, and performs other tasks.

Next, dcRAT opens a URL in Google Chrome to create a remote WMI connection, which the actors use to connect to the victim's machine. dcRAT also downloads malicious cookies and tries to use them to authenticate itself with the victim's Google account.


The victim opens the attachment
VBA script displays *wait* message, executes PowerShell script
The VBA script downloads malicious files
dcRat opens a remote WMI connection

5. Vulnerabilities and mitigation

Infoblox recommends the following measures for reducing the risk of infection by dcRAT:

- Keep antivirus signatures and engines up to date.
- Turn on automatic updates. This will keep the operating system up to date with the latest security patches.
- Do not expose email addresses to the internet.
- Exercise caution when opening all email attachments, especially those that come from unfamiliar senders.
- Avoid opening emails with generic subject lines.

Endnotes

1. **https://www.spywareremove.com/removedarkcrystalrat.html**