Spike in DanaBot Malware Activity

zscaler.com/blogs/security-research/spike-danabot-malware-activity

Key Points

- Two large software supply chain attacks distributed the DanaBot malware.
- DanaBot is a malware-as-a-service platform discovered in 2018 that focuses on credential theft and banking fraud.
- DanaBot's popularity has waned in recent years, but these campaigns may signal a return of the malware and its affiliates to the threat landscape.

Introduction

The DanaBot malware had a spike in new activity recently, including being distributed via two large software supply chain attacks and being used in a Distributed Denial of Service (DDoS) attack on a Russian language electronics forum.

DanaBot, first discovered by Proofpoint in May 2018, is a malware-as-a-service platform where threat actors, known as "affiliates" and identified by "affiliate IDs", purchase access to the platform from another threat actor who develops the malware and command and control (C2) panel, sets up and maintains the shared C2 infrastructure, and provides sales and customer support. Affiliates then distribute and use the malware as they see fit--mostly to steal credentials and commit banking fraud.

While it was a prominent banking malware for a number of years and despite a new major update being spotted at the end of 2020 (as documented by Proofpoint, ESET, and LEXFO), DanaBot has been relatively quiet in the recent threat landscape.

Large Software Supply Chain Attack (October 22, 2021)

As reported by the Cybersecurity and Infrastructure Security Agency (CISA), GitHub, the developer, and others the NPM JavaScript package for "UAParser.js" was compromised on Friday, October 22, 2021 and used to distribute a cryptocurrency miner and DanaBot. UAParser.js is a "JavaScript library to detect Browser, Engine, OS, CPU, and Device type/model from User-Agent data with relatively small footprint." Based on its NPM stats, it has 7 million weekly downloads.

The DanaBot malware was downloaded from:

hxxps://citationsherbe\.at/sdd.dll

The packed/crypted loader component has a SHA-256 hash of:

2a3acdcd76575762b18c18c644a745125f55ce121f742d2aad962521bc7f25fd

The loader downloads a main component which has a SHA-256 of:

77ff83cc49d6c1b71c474a17eeaefad0f0a71df0a938190bf9a9a7e22531c292

The main component was configured with the following configuration:

```
int set_config()
{
  int result; // eax

  *&g_s_config.affiliate_id = 40;
  *&g_s_config.arch = get_arch();
  *&g_s_config.win_version = get_win_version();
  *&g_s_config.timezone_bias = get_timezone_bias();
  qmemcpy(&g_s_config.build_hash, " AD14EA44261341E3690FA8CC1E236523", 0x21u);
  *&g_s_config.malware_version = 2052;
  *&g_s_config.field_28 = 0;
  *&g_s_config.field_10 = *&g_s_config.field_C + 1;
  *&g_s_config.field_14 = *&g_s_config.field_C + 2;
  result = *&g_s_config.field_C + 3;
  *&g_s_config.field_18 = *&g_s_config.field_C + 3;
  *&g_s_config.field_20 = 360000;
  *&g_s_config.c2_0 = 0xD8FA9EB9;               // 185.158.250.216
  *&g_s_config.c2_1 = 0x2EE14CC2;               // 194.76.225.46
  *&g_s_config.c2_2 = 0x99B40B2D;               // 45.11.180.153
  *&g_s_config.c2_3 = 0x3DE14CC2;               // 194.76.225.61
  *&g_s_config.port_0 = 443;
  *&g_s_config.port_1 = 443;
  *&g_s_config.port_2 = 443;
  *&g_s_config.port_3 = 443;
  return result;
}
```

Figure 1: DanaBot malware configuration used in supply chain attack

The malware was also configured with a backup TOR C2:

bjij7tqwaipwbeig5ubq4xjb6fy7s3lknhkjojo4vdngmqm6namdczad\.onion

As highlighted in Figure 1 above, the affiliate ID for this sample was 40. Based on Zscaler ThreatLabz tracking, this is a new affiliate to the DanaBot ecosystem. At the time of the incident, the affiliate had only configured the malware's credential stealing component to be active--the person-in-the-browser and webinject bank fraud component was not activated.

While the post-infection intentions of the threat actor aren't known, given the focus on credentials, the size of the attack, and the crimeware landscape being dominated by initial access brokers selling access to ransomware affiliates, this outcome can't be ruled out.

Second Large Software Supply Chain Attack (November 4, 2021)

As reported by Twitter, GitHub, and others, another NPM package was compromised and used to distribute DanaBot. The package is called "COA" and it "is a parser for command line options that aim to get maximum profit from formalization your program API". Based on NPM stats, it had almost 9 million weekly downloads. The attack took place on Thursday, November 4, 2021 and it was by the same DanaBot affiliate ID 40 threat actor as in the October 22, 2021 attack on "UAParser.js".

The DanaBot loader component used in this campaign was distributed from:

hxxps://pastorcryptograph\.at/3/sdd.dll

It has a SHA-256 hash of:

26451f7f6fe297adf6738295b1dcc70f7678434ef21d8b6aad5ec00beb8a72cf

and was used to download a DanaBot main component with the SHA-256 hash of:

e7c9951f26973c3915ffadced059e629390c2bb55b247e2a1a95effbd7d29204

Similar to the first incident, the threat actor had only configured the malware's credential stealing component to be active.

DDoS Attack on Russian Language Electronics Forum

DanaBot affiliate ID 4 was also active last week. While this affiliate isn't new, there hasn't been a change to their component configurations for some time. On Wednesday October 20, 2021, the affiliate configured its DanaBot victims to download and execute a new executable with a SHA-256 hash of:

8b64b8bfd9e36cc40c273deccd4301a6c2ab44df03b976530c1bc517d7220bce

The downloaded executable is written in the Delphi programming language and its only functionality is to implement a bare-bones HTTP-based DDoS attack on a hardcoded IP address and host. The template used to generate the HTTP requests is shown in Figure 2:

```
.text:0041A44C aGetHttp11HostA:                        ; DATA XREF: get_request+1A↑o
.text:0041A44C                  text "UTF-16LE", 'GET / HTTP/1.1',0Dh,0Ah
.text:0041A44C                  text "UTF-16LE", 'Host: arduino.ru',0Dh,0Ah
.text:0041A44C                  text "UTF-16LE", 'User-Agent: Power Off',0Dh,0Ah
.text:0041A44C                  text "UTF-16LE", 'Accept: text/html,application/xhtml+xml,application'
.text:0041A44C                  text "UTF-16LE", '/xml;q=0.9,image/avif,image/webp,*/*;q=0.8',0Dh,0Ah
.text:0041A44C                  text "UTF-16LE", 'Accept-Language: en-US,en;q=0.5',0Dh,0Ah
.text:0041A44C                  text "UTF-16LE", 'Accept-Encoding: gzip, deflate',0Dh,0Ah
.text:0041A44C                  text "UTF-16LE", 'Connection: keep-alive',0Dh,0Ah
.text:0041A44C                  text "UTF-16LE", 'Referer: http://arduino.ru/',0Dh,0Ah
.text:0041A44C                  text "UTF-16LE", 'Cookie: ',0
```

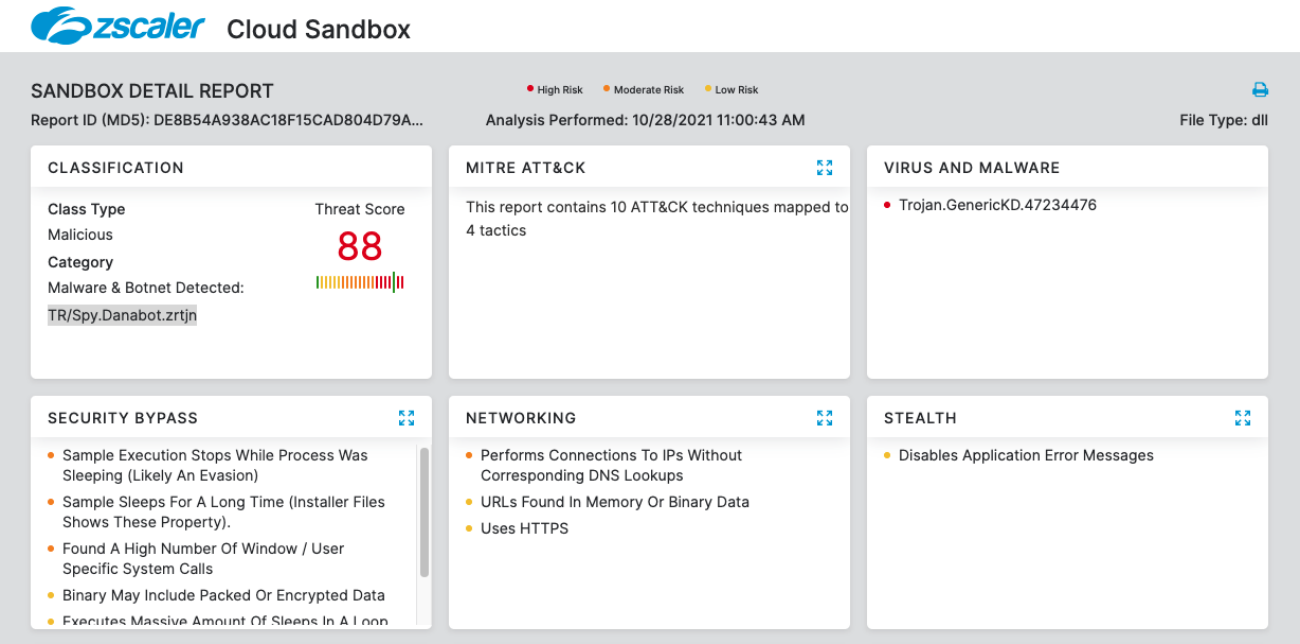
Figure 2: HTTP request template used in DDoS attack

As highlighted in the “Host” header in Figure 2 above, the attack targets a Russian language forum focused on the discussion of electronics. The “User-Agent” header, hardcoded target, and simple functionality seems to imply that the payload was designed to settle a personal grudge instead of indicating a larger change in the threat actor’s tactics, techniques, and procedures (TTPs).

Conclusion

While the popularity and activity of DanaBot has declined in recent years, the UAParser.js and COA software supply chain attacks shows that the malware is still an active threat. It is currently unclear whether these attacks were a one-off opportunity for a threat actor or whether this and other activity signals the return of DanaBot and its affiliates.

Cloud Sandbox Detection



MITRE ATT&CK TTP Mapping

Tactic	Technique

T1586	Compromise Accounts
T1195	Supply Chain Compromise
T1204	User Execution
T1555	Credentials from Password Stores
T1003	OS Credential Dumping
T1539	Steal Web Session Cookie
T1115	Clipboard Data
T1573	Encrypted Channel
T1008	Fallback Channels
T1041	Exfiltration Over C2 Channel

Indicators of Compromise

IOC	Notes
hxxps://citationsherbe\.at/sdd.dll	October 22, 2021 affiliate ID 40 distribution URL
2a3acdcd76575762b18c18c644a745125f55ce121f742d2aad962521bc7f25fd	October 22, 2021 affiliate ID 40 loader component

77ff83cc49d6c1b71c474a17eeaefad0f0a71df0a938190bf9a9a7e22531c292	October 22, 2021 affiliate ID 40 main component
185.158.250.216:443	October 22, 2021 affiliate ID 40 configured C2
194.76.225.46:443	October 22, 2021 affiliate ID 40 configured C2
45.11.180.153:443	October 22, 2021 affiliate ID 40 configured C2
194.76.225.61:443	October 22, 2021 affiliate ID 40 configured C2
bjij7tqwaipwbeig5ubq4xjb6fy7s3lknhkjojo4vdngmqm6namdczad\.onion	October 22, 2021 affiliate ID 40 configured backup C2

hxxps://pastorcryptograph\.at/3/sdd.dll	November 4, 2021 affiliate ID 40 distribution URL
26451f7f6fe297adf6738295b1dcc70f7678434ef21d8b6aad5ec00beb8a72cf	November 4, 2021 affiliate ID 40 loader component
e7c9951f26973c3915ffadced059e629390c2bb55b247e2a1a95effbd7d29204	November 4, 2021 affiliate ID 40 main component
185.117.90.36:443	November 4, 2021 affiliate ID 40 configured C2
193.42.36.59:443	November 4, 2021 affiliate ID 40 configured C2
193.56.146.53:443	November 4, 2021 affiliate ID 40 configured C2

185.106.123.228:443	November 4, 2021 affiliate ID 40 configured C2
f4d12a885f3f53e63ac1a34cc563db0efb6d2d1d570317f7c63f0e6b5bf260b2	Recent Affiliate ID 4 loader component
ad0ccba36cef1de383182f866478abcd8b91f8e060d03e170987431974dc861e	Recent Affiliate ID 4 main component
192.119.110.73:443	Affiliate ID 4 configured C2
192.236.147.159:443	Affiliate ID 4 configured C2
192.210.222.88:443	Affiliate ID 4 configured C2
gcwr4vcf72vpcrgevcziwb7axooa3n47l57dsiwxvzvcdlt7exsvk5yd.onion	Affiliate ID 4 configured backup C2