Using DDoS, DanaBot targets Ukrainian Ministry of Defense

zscaler.com/blogs/security-research/danabot-launches-ddos-attack-against-ukrainian-ministry-defense

March 7, 2022 Update

DanaBot affiliate ID 5 has stopped DDoSing the Ukrainian Ministry of Defense's webmail server and started DDoSing a hardcoded IP address, 138.68.177[.]158. According to Passive DNS data, this IP address has recently been associated with invaders-rf[.]com. This site claims to be (Google translated):

"...an information resource of the Office of the National Security and Defense Council of Ukraine, which provides information about prisoners of war of the Russian Armed Forces who have invaded the territory of Ukraine since February 24, 2022. The portal will be available to Russian citizens, including soldiers' families or acquaintances, to obtain information on the condition and whereabouts of prisoners."

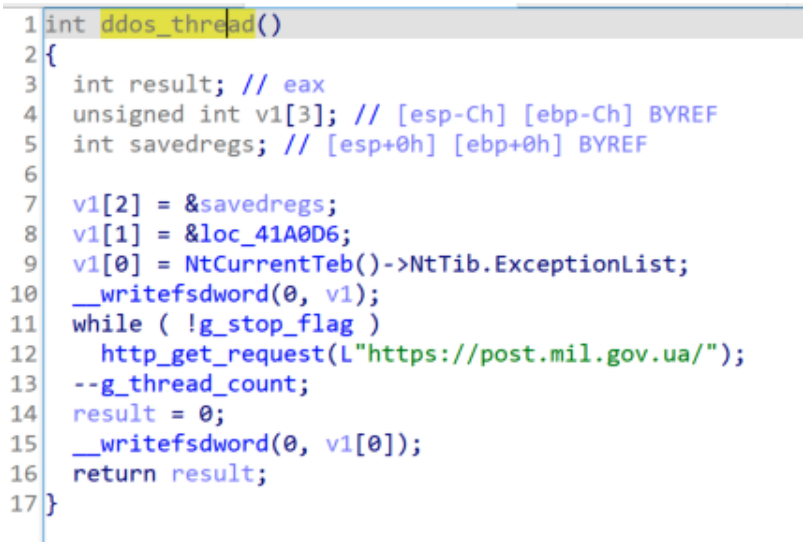
Given the threat actor's previous targeting, this seems like the likely target. The DDoS attack payload was written and distributed similarly to the Ukrainian Ministry of Defense DDoS payload on March 2, 2022:

Key Points

- A threat actor using DanaBot has launched a Distributed Denial of Service (DDoS) attack against the Ukrainian Ministry of Defense's webmail server.
- The DDoS attack was launched by leveraging DanaBot to deliver a second-stage malware payload using the download and execute command.
- It is unclear whether this is an act of individual hacktivism, state-sponsored, or possibly a false flag operation.

DanaBot, first discovered in 2018, is a malware-as-a-service platform where threat actors, known as *affiliates* are identified by *affiliate IDs*. These affiliates 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.

On Wednesday March 2, 2022, in the midst of the 2022 Russian invasion of Ukraine, the threat actor identified by the affiliate ID 5 launched an HTTP-based Distributed Denial of Service (DDoS) attack against the Ukrainian Ministry of Defense's webmail server with the URL hxxps://post.mil.gov[.]ua as shown in Figure 1:



```
int ddos_thread()
{
  int result; // eax
  unsigned int v1[3]; // [esp-Ch] [ebp-Ch] BYREF
  int savedregs; // [esp+0h] [ebp+0h] BYREF

  v1[2] = &savedregs;
  v1[1] = &loc_41A0D6;
  v1[0] = NtCurrentTeb()->NtTib.ExceptionList;
  __writefsdword(0, v1);
  while ( !g_stop_flag )
    http_get_request(L"https://post.mil.gov.ua/");
  --g_thread_count;
  result = 0;
  __writefsdword(0, v1[0]);
  return result;
}
```

Figure 1: Hardcoded DDoS Target Attacked by DanaBot With Affiliate ID 5

At the time of publication, the webmail server is still online and reachable as shown in Figure 2.

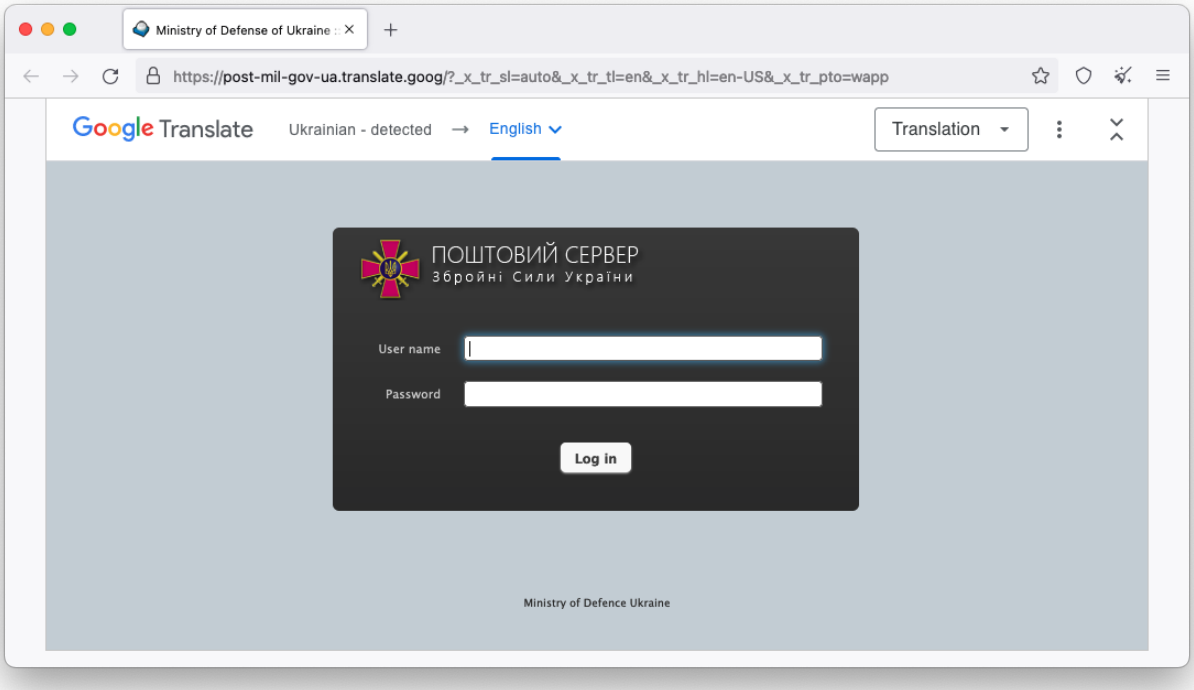


Figure 1: Ukrainian Ministry of Defense's Webmail Server Targeted by DanaBot Affiliate ID 5

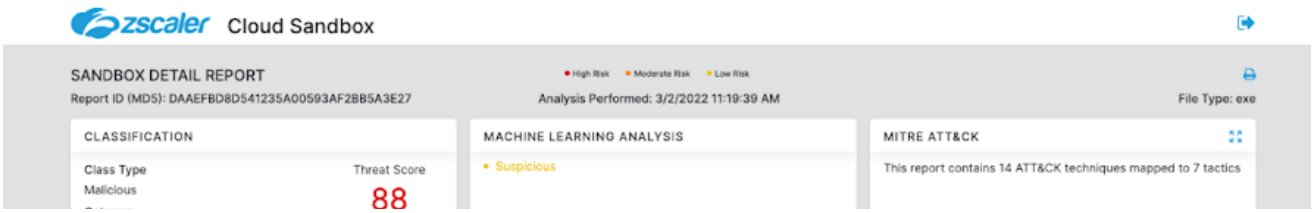
The DDoS attack was launched using DanaBot's download and execute (command 2048 / subcommand 9) to deliver a new executable with the SHA-256 hash: b61cd7dc3af4b5b56412d62f37985e8a4e23c64b1908e39510bc8e264ebad700

Similar to DanaBot, the downloaded DDoS executable is written in the Delphi programming language. Its sole functionality is to implement a bare-bones HTTP-based DDoS attack on a hardcoded target. The executable is very similar to the one used in another DanaBot DDoS attack that was documented in November 2021. In that attack, the DanaBot affiliate ID 4 launched a DDoS attack against a Russian language electronics forum.

Conclusion

While the timing and targeting certainly suggest this new attack is related to the 2022 Russian invasion of Ukraine, it is unclear whether this is an act of individual hacktivism, something state-sponsored, or possibly a false flag operation. If the threat actor's motive is to attack Ukraine, it is quite likely that in addition to the DDoS attack, the actor is using DanaBot's more typical functionality such as credential theft and document theft against any relevant victims as well.

Cloud Sandbox Detection



Category
Malware & Botnet

VIRUS AND MALWARE

No known Malware found

SECURITY BYPASS

- AV Process Strings Found
- May Try To Detect The Virtual Machine To Hinder Analysis

NETWORKING

- May Use The Tor Software To Hide Its Network Traffic
- Performs Connections To IPs Without Corresponding DNS Lookups
- Connects To Several IPs In Different Countries
- HTTP GET Or POST Without A User Agent
- Downloads Files From Web Servers Via HTTP
- URLs Found In Memory Or Binary Data

STEALTH

- System Process Connects To Network
- Tries To Detect Virtualization Through RDTSC Time Measurements
- Disables Application Error Messages
- Overwrites Function Prologues

SPREADING

No suspicious activity detected

INFORMATION LEAKAGE

- Enumerates The File System
- Installs A Raw Input Device

EXPLOITING

- May Try To Detect The Windows Explorer Process
- Runs A DLL By Calling Functions

PERSISTENCE

- Creates Temporary Files
- May Use Bcdedit To Modify The Windows Boot Settings
- PE File Contains Sections With Non-Standard Names

SYSTEM SUMMARY

- Sample Has A GUI, But Cloud Sandbox Has Not Found Any Clickable Buttons, Likely Requires More UI Automation
- Sample Has Functionality To Log And Monitor Keystrokes
- Spawns Processes
- Submission File Is Bigger Than Most Known Malware Samples
- Uses 32bit PE Files
- Uses An In-Process (OLE) Automation Server

DOWNLOAD SUMMARY

Original file	2 MB
Dropped files	5 MB
Packet capture	13 MB

ORIGIN

Origin Information not identified

FILE PROPERTIES

File Type	Windows Executable
Digital Certificate	Vendor File is not digitally signed
File Size	2,390,528 bytes
MD5	daaefbd8d541235a00593af2bb5a3e27
SHA1	428bb7e395f87070d55ef7fa08fe8296d640c20f
SSDEEP	49152:+9v6QHpB80/Mxob4PWt16BNXOUrpiWNF99GTfB:+9v6Q1y-Wt8NXZr0sFU

PROCESS SUMMARY

DROPPED FILES

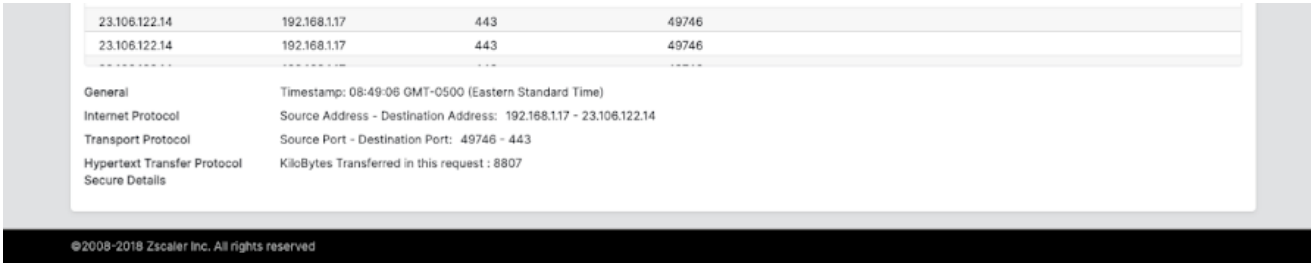
- 647_daaefbd8d541235a00593af2bb5a3e27-Dynamic_yara_data.Zip
- C:\Users\User\AppData\Local\Temp\Tedyyqtuoqfyeed.Tmp

SCREENSHOTS

NETWORK PACKETS

ALL 787 | SMTP 0 | ICMP 0 | HTTP 0 | UDP 0 | TCP 100 | IRC 0 | FTP 0 | DNS 0 | HTTPS 687

SOURCE IP	DESTINATION IP	SOURCE PORT	DESTINATION PORT	JA3	JA3 DIGEST
192.168.1.17	23.106.122.14	49746	443		
23.106.122.14	192.168.1.17	443	49746	771,49196-49195-49200-491...	51C64C77E60F3980EEA9086...
192.168.1.17	23.106.122.14	49746	443		
23.106.122.14	192.168.1.17	443	49746		
192.168.1.17	23.106.122.14	49746	443		
23.106.122.14	192.168.1.17	443	49746		
23.106.122.14	192.168.1.17	443	49746		
23.106.122.14	192.168.1.17	443	49746		
23.106.122.14	192.168.1.17	443	49746		
23.106.122.14	192.168.1.17	443	49746		
23.106.122.14	192.168.1.17	443	49746		



Indicators of Compromise

IOC	Notes
7ea65c1cb2687be42f427571e3223e425d602d043c39f690d0c3c42309aff513	SHA256 hash for the affiliate ID 5 DanaBot loader component
192.236.161[.]4	DanaBot affiliate ID 5 C2 server
23.106.122[.]14	DanaBot affiliate ID 5 C2 server
5.9.224[.]217	DanaBot affiliate ID 5 C2 server
ockiwumgv77jgrppj4na362q4z6flsm3uno5td423jj4lj2f2meqt6ad[.]onion	DanaBot affiliate ID 5 C2 server
b61cd7dc3af4b5b56412d62f37985e8a4e23c64b1908e39510bc8e264ebad700	SHA256 hash for the DDoS attack tool targeting the Ukrainian Ministry of Defense
fd217dde8d03cfb9179f5ad783665bb67c47a92278971e28c3d399e7ac6f0a54	SHA256 hash for the DDoS attack tool targeting invaders-rf\.com
c732d57f5b3354c368e54a16b193457d6f06b707c0388c5643677a9de13e04db	SHA256 hash for the DDoS attack tool targeting invaders-rf\.com

9706a9d8aacea34071f6f1691dc3c1af3d01868fc17deb83a4b8f33e2342a9d3	SHA256 hash for the DDoS attack tool targeting invaders-rf\.com

About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.