Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | update.dat.sample |
| *MD5* | C6BEAB9EBB086280F20A7785D9968932 |
| *SHA-1* | B77E272DAC39F3A478B549E8CDFA0EB59925C684 |
| *SHA-256* | 28E2DB43246066CF8E0034FDADE0463EABAA5E24DC968CDE01A841E9513771F9 |
| *File type* | Win32 Dll |
| *File size* | 59.50 KB (60928 bytes) |

# Kết luận chung

|  |  |
| --- | --- |
| *Loại mã độc* | Trojan |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Mã độc lấy shell code tại domain***"www.babyolo.my03.com".*** Tạo threadchạy thực thi file ***“C:\windows\system32\rundll32.exe”*** sau đó suspend thread tạo vùng nhớ để chèn shellcode. |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x64

*Compilation Timestamp*: 2016-09-29 03:18:04 UTC

*Packer*: None

*PE Size*: 27.00 KB (27648 bytes) - Bằng với File Size

*Các hàm import đặc trưng của mã độc*:

* SHELL32.dll
  + SHGetSpecialFolderPathW
* KERNEL32.dll
  + GetProcAddress
  + VirtualProtectEx
  + TerminateProcess
  + CreateProcessA
  + VirtualAlloc
* WININET.dll
  + HttpQueryInfoW
  + InternetQueryDataAvailable
  + InternetReadFile
  + InternetCloseHandle
  + InternetConnectA
  + HttpSendRequestW
  + InternetOpenW
  + HttpOpenRequestW
  + HttpAddRequestHeadersW
* CRYPT32.dll
  + CryptUnprotectData

*Các hàm export nghi ngờ*:

* + enrty
  + mysocket

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 21/70
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Undetected |
| Microsoft | Trojan:Win32/Zpevdo.B |
| Symantec | Undetected |
| McAfee | Undetected |
| BitDefender | Trojan.GenericKD.41509512 |

## Phân tích động cơ bản

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| GetSystemDirectoryW | C:\Windows\system32\ | Truy xuất đường dẫn của thư mục hệ thống |
| CreateProcessA | C:\windows\system32\rundll32.exe | Tạo process để chạy file sau đó suspend |
| ReadProcessMemory | C:\windows\system32\rundll32.exe | Đọc bộ nhớ của process để lấy dữ liệu |
| WriteProcessMemory | C:\windows\system32\rundll32.exe | Chèn shellcode vào process |
| ResumeThread | C:\windows\system32\rundll32.exe | Tiếp tục process đã suspend |

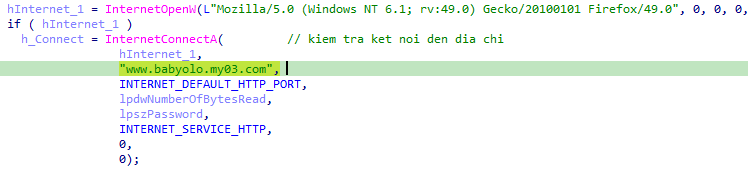
Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| InternetConnectA | www.babyolo.my03.com | Kết nối đến domain chứa shellcode |
| HttpAddRequestHeadersW | www.babyolo.my03.com | Thêm HTTP request header |
| HttpSendRequestW | www.babyolo.my03.com | Gửi request đến doamin chứa shellcode |
| HttpQueryInfoW | www.babyolo.my03.com | Truy xuất thông tin HTTP header |

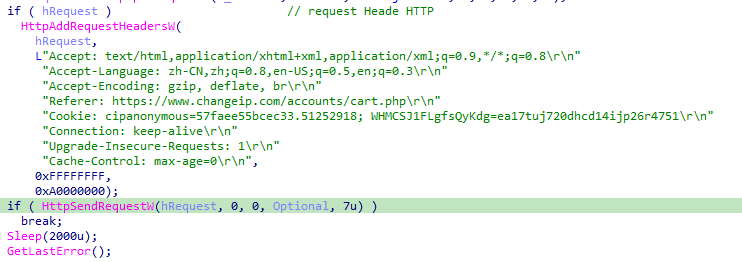
# Phân tích nâng cao

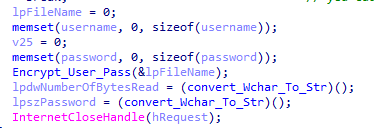
## Luồng hoạt động của mã độc:

Mã độc kiểm tra kết nối Internet và connect tới domain ***"www.babyolo.my03.com".***

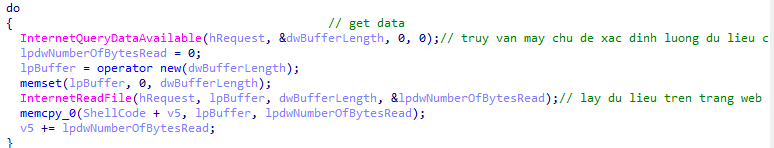


Liên tục gửi request nhằm yêu cầu xác thực username và password.





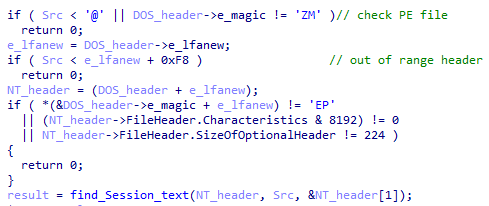
Nếu xác thực thành công mã độc tạo request để lấy dữ liệu trên trang web.



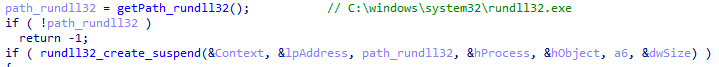
Sau đó thực hiện lấy shellcode tại file đã lấy được.



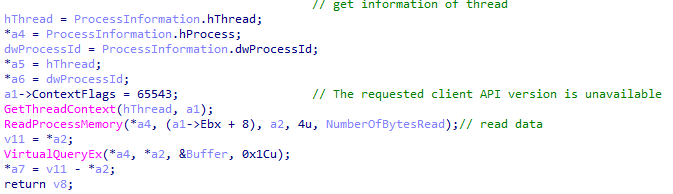
Kiểm tra file có phải là file PE không, nếu là file PE thì thực hiện tìm sesstion “.***text***” để lấy shellcode.



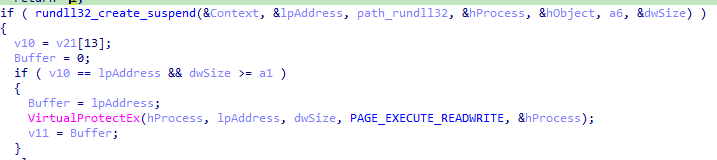
Lấy đường dẫn “***C:\windows\system32\rundll32.exe”*** sau đó tạo thread để thực thi file ***“rundll32.exe”***.



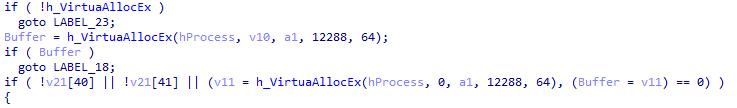
Sau đó thực hiện suspend thread và thực hiện truy xuất thông tin của thread và đọc dữ liệu.



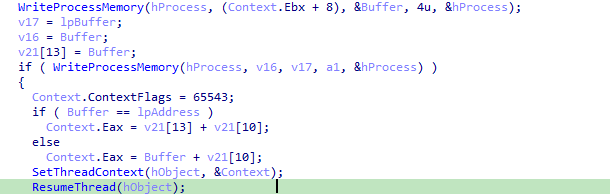
Mã độc thực hiện tìm kiếm trong đoạn dữ liệu vừa đọc được từ thread ***“rundll32.exe”*** xem có đoạn nào trống sẽ inject shellcode vào đó.



Nếu không có đoạn nào trống sẽ thực hiện cấp phát bộ nhớ để inject shellcode.



Sau khi cấp phát thành công bộ nhớ sẽ thực hiện ghi shellcode vào vùng nhớ đó và resume thread. Lúc này process ***“rundll32.exe”*** sẽ chạy tiếp và shellcode sẽ được thực thi.



Tại thời điểm phân tích máy chủ điều khiển đã dừng hoạt động, không lấy được shellcode nên quá trình phân tích dừng tại đây.

## Hành vi hoạt động của loại mã độc:

### Trojan:

Mã độc lấy shell code tại domain***"www.babyolo.my03.com".*** Tạo threadchạy thực thi file ***“C:\windows\system32\rundll32.exe”*** sau đó suspend thread tạo vùng nhớ để chèn shellcode. Khi thread được resume thì shellcode sẽ được thực thi.

# Indicators of Compromise (IoC)

Hashes:

* 49a60be4b95b6d30da355a0c124af82b35000bce8f24f957d1c09ead47544a1e

Network IoC:

* www.babyolo.my03.com