

EDR 스토리보드 v1.0.00

Revision History

[illegible]

Information

설계자	컨설팅 / 권혁재
설계일	2018.01.17
화면 설명	
01	
02	
03	
04	
05	
06	
07	
08	
09	
10	

화면 코드	UIN-0000	화면 명칭	조사	설계 타입	페이지
화면 경로	메인 페이지 → 조사: 메인				

☰

🔍

⚠

🔄

⚙

Notification 3 | Logged on

Investigation

Search Processes, IPs, Users, Hostnames, MACs, and #Tag...

Information

설계자	컨설팅 / 권혁재
설계일	2018.01.17
화면 설명	
01	
02	
03	
04	
05	
06	
07	
08	
09	
10	

화면 코드	UIN-0000	화면 명칭	조사 - 검색결과	설계 타입	페이지
화면 경로	메인 페이지 → 조사: 검색				

☰

🔍

⚠

🔄

⚙

Investigation

#Malicious

Endpoint	MAC Address	Hostname	IP Address	OS	
fr3aerf3@!34gr4	9E-D3-88-CC-4E-FE	Jekicv			
#\$GF@!R	9E-D3-88-CC-4E-FE	WinTest7			
#\$GF@!R	9E-D3-88-CC-4E-FE	Linud			
#\$GF@!R	9E-D3-88-CC-4E-FE				
#\$GF@!R	9E-D3-88-CC-4E-FE				
#\$GF@!R	9E-D3-88-CC-4E-FE				

Notification 3 | Logged on

Information

설계자 컨설팅 / 권혁재

설계일 2018.01.17

화면 설명

01

02

03

04

05

06

07

08

09

10

화면 코드

UIN-0000

화면 명칭

프로세스 상세분석

설계 타입

페이지

화면 경로

메인 페이지 → 조사 → 상세분석: 프로세스

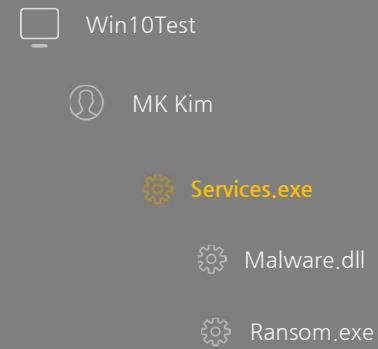
Notification ³ | Logged on

Process Analysis: Services.exe #Tag

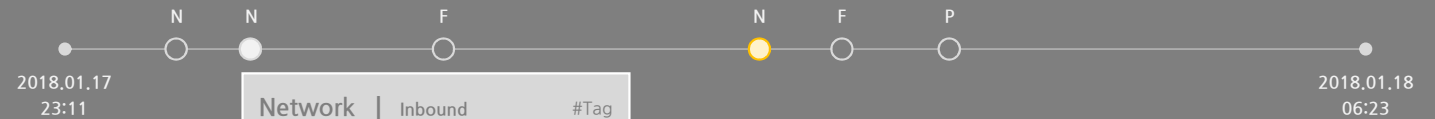
Overview

Reputation	Unknown
Size	241KB
MD5	dfdfREF34t34rtt1!FG43!
SHA256	dfdfREF34t34rtt1!FG43!dfdfREF34t34rtt1!FG43!
Start Time	2018.01.17 23:11
End Time	Unknown
Signed	Unknown
Product Name	Microsoft® Windows® Operating System
Product Version	10.0.16299.15

Hierarchy



Timeline



Network | Inbound #Tag

Dest.	8.8.8.8
Protocol	HTTP
Port	90057
Application	Internet Explorer