

File Name	d4799f6db834266cda9fdcecd587eb61ff17d4debbaa03f4cae05bbd085a675e	Threat Level	● 4 - High
Malware Name	Malware.Dynamic	Engine	Sandbox
File Submitted	2018-04-24 08:33:24	Processing Time	46 seconds
File Size	72,500 bytes	Sandbox Replication	25 seconds
Show More	Hash Values	File Details	Environment
MD5 Hash Identifier	43253202D0489B48B360E9A85C855117		
SHA-1 Hash Identifier	A7F6AEF3EC4412AF73942A40B9D6318C1489C6C4		
SHA-256 Hash Identifier	D4799F6DB834266CDA9FDCECD587EB61FF17D4DEBBAA03F4CAE05BBD085A675E		
	Hide hash values		
File Type	PE32 executable (GUI) Intel 80386		
Digital Signature Verified	Unsigned		
Publisher	Not Available		
Description	Not Available		
Product Name	Not Available		
Version Info	Not Available		
File version	Not Available		
Strong Name	Not Available		
Original Name	Not Available		
Internal Name	Not Available		
Copyright	Not Available		
Comments	Not Available		
	Hide file details		
Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601, version 6.1.7601), 64-bit			
Internet Explorer version: 8.0.7601.17514			
Microsoft Office version: 2003			
PDF Reader version: 9.0			
Flash player version: 11.2.202.228			
No Flash player plugin installed			
Platform Version 4.4.0.9			
Detection Package Version 4.4.0.180402			
	Hide environment		

Baitexe activated but not infected

Behavior Classification

Behavior	Severity
<ul style="list-style-type: none"> ▼ Spreading ● 4 - High 	
<ul style="list-style-type: none"> ▶ Injected into memory of the Windows system application ● 4 - High ▶ Wrote (injected) data to an area of a foreign process memory ● 3 - Medium 	
<ul style="list-style-type: none"> ▼ Exploiting, Shellcode ● 3 - Medium 	

Wrote (injected) data to an area of a foreign process memory ● 3 - Medium

Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection ● 2 - Low

Created named mutex object ● 2 - Low

Allowed the process to perform system-level actions that were not enabled previously ● 2 - Low

Hiding, Camouflage, Stealthiness, Detection and Removal Protection ● 1 - Informational

Changed the protection attribute of the process ● 1 - Informational

Persistence, Installation Boot Survival ● Unverified

Networking ● Unverified

Data spying, Sniffing, Keylogging, Ebanking Fraud ● Unverified

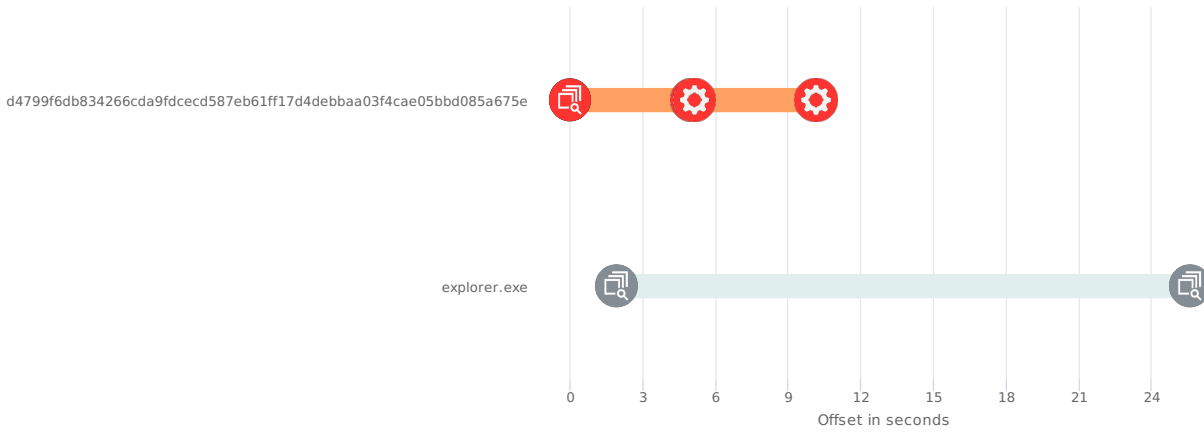
Processes Analyzed

Name	Reason	Severity
d4799f6db834266cda9fdcccd587eb61ff17d4debbaa03f4cae05bbd085a675e	loaded by MATD Analyzer	● 4 - High
explorer.exe	injected & wrote by d4799f6db834266cda9fdcccd587eb61ff17d4debbaa03f4cae05bbd085a675e	● Unverified

Timeline Activity

⚙️ Processes
📄 Files
🔍 Registry Operations
🌐 Network Operations
📁 Multiple Operations

Select Any Area to Zoom In



▼ **Timeline Activity Details**

Time Offset	Event	Details
00:00:00	📄 File Operations, miscellaneous	Retrieved the full path for the module
00:00:00	🔍 Others	Retrieved the locally unique identifier (LUID)
00:00:00	📁 Signal Objects	main
00:00:00	📁 Signal Objects	cmd
00:00:00	⚙️ Process Operations, miscellaneous	Opened the access token associated with a process
00:00:016	⚙️ Process Operations, miscellaneous	Retrieved system information
00:00:016	🔍 Others	Enabled/disabled privileges in an access token
00:01:922	🔍 Others	Obtained the system metric or system configuration setting
00:05:032	⚙️ Foreign Memory Regions Written	Allocated memory in foreign(or local) processes