

File Name	e912266ca2b77bf0524ffe7ea8b5f3d89db34da5cadaaa24c9eed8687d3972b3	Threat Level	● 4 - High
Malware Name	Malware.Dynamic	Engine	Sandbox
File Submitted	2018-04-24 08:33:25	Processing Time	195 seconds
File Size	263,176 bytes	Sandbox Replication	170 seconds
Show More	<a href="#">Hash Values</a>	<a href="#">File Details</a>	<a href="#">Environment</a>
MD5 Hash Identifier	DCBDC671400AC177685EA80E1969371D		
SHA-1 Hash Identifier	BC720087FD73BCF525F1EB48F8FA766AA097FADD		
SHA-256 Hash Identifier	E912266CA2B77BF0524FFE7EA8B5F3D89DB34DA5CADA24C9EED8687D3972B3		
	<a href="#">Hide hash values</a>		
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		
	<a href="#">Hide file details</a>		
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			
	<a href="#">Hide environment</a>		

Baitexe activated but not infected

**Behavior Classification**

Behavior	Severity
<ul style="list-style-type: none"> <li>Persistence, Installation Boot Survival</li> </ul>	● 4 - High
<div style="border: 1px solid #ccc; padding: 5px;"> <ul style="list-style-type: none"> <li>Provided activities from kernel level, see <a href="http://en.wikipedia.org/wiki/Ring_(computer_security)">http://en.wikipedia.org/wiki/Ring_(computer_security)</a> ● 4 - High</li> <li>Altered auto-run registry entry that executed at next Windows boot ● 3 - Medium</li> <li>Manipulated an existing Windows service by its handle ● 2 - Low</li> </ul> </div>	
<ul style="list-style-type: none"> <li>Hiding, Camouflage, Stealthiness, Detection and Removal Protection</li> </ul>	● 4 - High
<div style="border: 1px solid #ccc; padding: 5px;"> <ul style="list-style-type: none"> <li>Enumerated system processes and injected code into their memory space ● 4 - High</li> </ul> </div>	

Encrypted and uploaded data to suspicious webserver	● 3 - Medium
Modified time attribute of the specified file after its creation	● 2 - Low
Manipulated an existing Windows service by its handle	● 2 - Low
Connected to a specific service provider	● 2 - Low
Set a filter function to supersede the top-level exception handler ( <a href="http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx">http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx</a> )	● 1 - Informational
Created new PE file	● 1 - Informational
Changed the protection attribute of the process	● 1 - Informational

✓ Spreading

● 4 - High

Enumerated system processes and injected code into their memory space	● 4 - High
Hid content by modifying its attributes	● 2 - Low
Read data from a handle opened on previous URL's request	● 1 - Informational

✓ Networking

● 4 - High

Provided activities from kernel level, see <a href="http://en.wikipedia.org/wiki/Ring_(computer_security)">http://en.wikipedia.org/wiki/Ring_(computer_security)</a>	● 4 - High
Enumerated Device drivers present in the victim machine and collects system information and send to attacker	● 3 - Medium
Encrypted and uploaded data to suspicious webserver	● 3 - Medium
Downloaded data from a webserver	● 2 - Low
Connected to a specific service provider	● 2 - Low
Altered Web Proxy Auto-Discovery Protocol (WPAD) for rerouting of the network traffic	● 2 - Low
Set a filter function to supersede the top-level exception handler ( <a href="http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx">http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx</a> )	● 1 - Informational
Read data from a handle opened on previous URL's request	● 1 - Informational

✓ Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection

● 2 - Low

Manipulated an existing Windows service by its handle	● 2 - Low
Created named mutex object	● 2 - Low
Set a filter function to supersede the top-level exception handler ( <a href="http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx">http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx</a> )	● 1 - Informational
Obtained user's logon name	● 1 - Informational
Contained long sleep	● 1 - Informational

✓ Data spying, Sniffing, Keylogging, Ebanking Fraud

● 1 - Informational

Contained long sleep	● 1 - Informational
----------------------	---------------------

✓ Exploiting, Shellcode

● Unverified

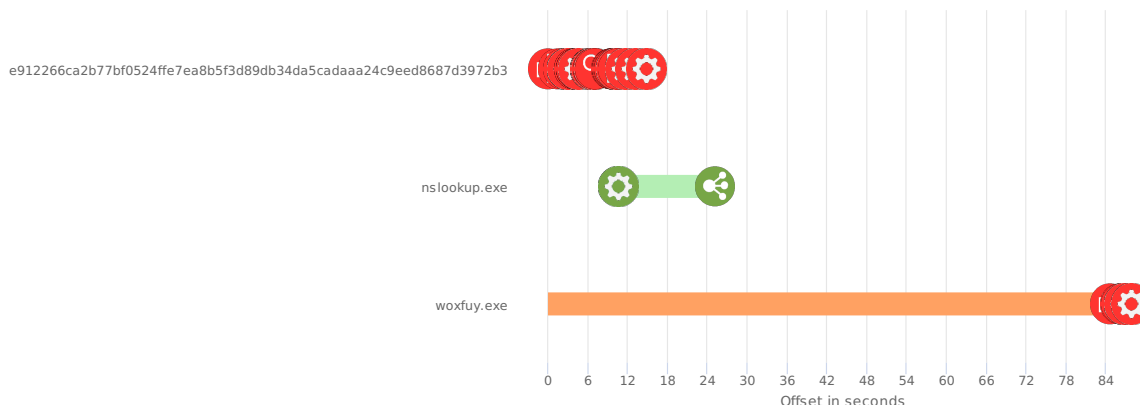
Processes Analyzed

Name	Reason	Severity
<a href="#">e912266ca2b77bf0524ffe7ea8b5f3d89db34da5cadaaa24c9eed8687d3972b3</a>	loaded by MATD Analyzer	● 4 - High
<a href="#">nslookup.exe</a>	executed by <a href="#">e912266ca2b77bf0524ffe7ea8b5f3d89db34da5cadaaa24c9eed8687d3972b3</a>	● 2 - Low
<a href="#">woxfuy.exe</a>	dropped by <a href="#">e912266ca2b77bf0524ffe7ea8b5f3d89db34da5cadaaa24c9eed8687d3972b3</a>	● 4 - High

### 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	Process Operations, miscellaneous	Enabled an application to supersede the top-level exception handler
00:01:719	Files Modified	Replaced one file with another file
00:02:328	Files Copied	Xepinepotarera ladosavawujaso ge mifojape Vukaso tewabere zici vovacawideti bivoce
00:03:030	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x2677e0, new attribute: Execute_ReadWrite
00:03:046	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x400000, new attribute: Execute_ReadWrite
00:03:046	Process Opened	[system process] 0
00:03:046	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x4120c0, new attribute: Execute_ReadWrite
00:03:078	Thread Created	3a4b20
00:03:078		}"64767015
00:04:078	Registry Opened	HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0
00:04:078	Registry Read	HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0 ProcessorNameString
00:04:078	Registry Opened	HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters
00:04:078	Registry Read	HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0 Identifier
00:04:078	File Operations, miscellaneous	Retrieved the path of the Windows directory
	File	