Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-04-24 14:35:04
Submitter	Manual Submission
Type	ISO image

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	Possible_GENISO-6, TROJ_GEN.R002C0RDJ21		
Exploited vulnerabilities	-		
Analyzed objects	ISO image	1 - Payment.img	14519983EA2F5E57EF45D5FBBA0F455BFD8038FA
	Windows 32-bit EXE file	1.1 - PAYMENT.SCR	DF247D1F45930896E17F102FF0925A53C1E33CA6

Analysis Environments

	CentOS w Docker	W7	W10
Anti-security, self-preservation		✓	✓
Autostart or other system reconfiguration		✓	✓
Deception, social engineering			
File drop, download, sharing, or replication		✓	✓
Hijack, redirection, or data theft			
Malformed, defective, or with known malware traits	✓	✓	✓
Process, service, or memory object change		✓	✓
Rootkit, cloaking			
Suspicious network or messaging activity			

CentOS w Docker

Environment-specific risk level	Low risk The object exhibited mildly suspicious characteristics that are most likely benign.
Detections	Possible_GENISO-6, TROJ_GEN.R002C0RDJ21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - Payment.img (ISO image)

File name	Payment.img
File type	ISO image
SHA-1	14519983EA2F5E57EF45D5FBBA0F455BFD8038FA
SHA-256	430AF8C2476E1845F5C52BE263E38884280DA4765C1F5417584C4C49AAF754FB
MD5	F78C525E5F8642EB4655F10E78B10051
Size	1245184 byte(s)

Risk Level	Low risk
Detection	Possible_GENISO-6
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1)

Notable Threat Characteristics

Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as probable malware	🟥⬜⬜	Source: ATSE Detection Name: Possible_GENISO-6 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: Possible_GENISO-6 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		

Object 1.1 - PAYMENT.SCR (Windows 32-bit EXE file)

File name	PAYMENT.SCR
File type	Windows 32-bit EXE file
SHA-1	DF247D1F45930896E17F102FF0925A53C1E33CA6
SHA-256	1180277FE6D2C8A01916FD50EDC4C1EC703251BBF75AD6BF042A5796A7D46094
MD5	AE434794BA6D5D9B3C07675E5C73819D
Size	214666 byte(s)

Risk Level	Low risk
Detection	TROJ_GEN.R002C0RDJ21
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1)

▼ Notable Threat Characteristics

▼ Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as probable malware	🟥⬜⬜	Source: ATSE Detection Name: TROJ_GEN.R002C0RDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0RDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		

W7

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Possible_GENISO-6, TROJ_GEN.R002C0RDJ21
Exploited vulnerabilities	-
Network connection	Custom

▼ Object 1 - Payment.img (ISO image)

File name	Payment.img
File type	ISO image
SHA-1	14519983EA2F5E57EF45D5FBBA0F455BFD8038FA
SHA-256	430AF8C2476E1845F5C52BE263E38884280DA4765C1F5417584C4C49AAF754FB
MD5	F78C525E5F8642EB4655F10E78B10051
Size	1245184 byte(s)

Risk Level	Low risk
Detection	Possible_GENISO-6
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1)

▼ Notable Threat Characteristics

▼ Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as probable malware	🟥⬜⬜	Source: ATSE Detection Name: Possible_GENISO-6 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

▼ Analysis

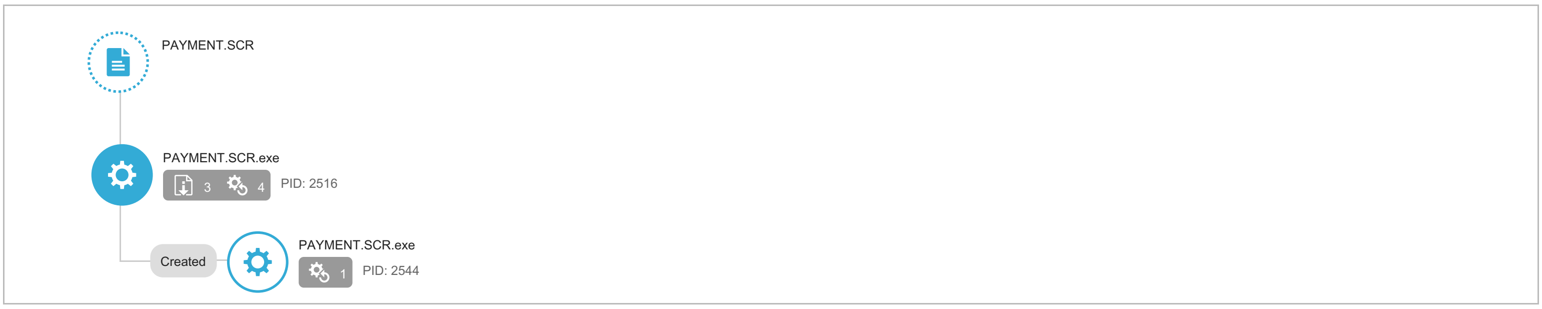
Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: Possible_GENISO-6 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		

▼ Object 1.1 - PAYMENT.SCR (Windows 32-bit EXE file)

File name	PAYMENT.SCR
File type	Windows 32-bit EXE file
SHA-1	DF247D1F45930896E17F102FF0925A53C1E33CA6
SHA-256	1180277FE6D2C8A01916FD50EDC4C1EC703251BBF75AD6BF042A5796A7D4609 4
MD5	AE434794BA6D5D9B3C07675E5C73819D
Size	214666 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.R002C0RDJ21
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (1) File drop, download, sharing, or replication (3) Malformed, defective, or with known malware traits (3) Process, service, or memory object change (5)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics		
Execution	Execution through API	🟥⬜⬜	Characteristics:	1, 2
	Execution through Module Load	🟥⬜⬜	Characteristics:	1
Defense Evasion	Software Packing	🟥⬜⬜	Characteristics:	1
	File Deletion	🟥⬜⬜	Characteristics:	1, 2

Notable Threat Characteristics

Anti-security, self-preservation (1)

Characteristic	Significance	Details
Uses suspicious packer	🟥⬜⬜	File Name: %WorkingDir%\PAYMENT.SCR.exe Packer: UNKNOWN

Autostart or other system reconfiguration (1)

Characteristic	Significance	Details
Modifies file that can be used to infect systems	🟥⬜⬜	%TEMP%\nsk6098.tmp\f3lck4g5lonrri.dll

File drop, download, sharing, or replication (3)

Characteristic	Significance	Details
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 2516 File: %TEMP%\nsk6098.tmp\f3lck4g5lonrri.dll Type: VSDT_DLL_W32
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2516 File: %TEMP%\nsk6098.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2516 File: %TEMP%\nsp6019.tmp Type: VSDT_EMPTY

Malformed, defective, or with known malware traits (3)

Characteristic	Significance	Details
Detected as probable malware	🟥⬜⬜	Source: ATSE Detection Name: TROJ_GEN.R002C0RDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92
Drops probable malware	🟥⬜⬜	Source: ATSE Detection Name: TROJ_GEN.R002C0RDJ21 File Name: f3lck4g5lonrri.dll SHA1: FEB4F10B870BB952D477637D93EB2D55BB9D31BF Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92
Rare executable file	🟥⬜⬜	Global Detections: 1

Process, service, or memory object change (5)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2544 Image Path: %WorkingDir%\PAYMENT.SCR.exe
Creates process	🟥⬜⬜	Process ID: 2516 Image Path: %WorkingDir%\PAYMENT.SCR.exe Shell Command: "%WorkingDir%\PAYMENT.SCR.exe"
Resides in memory to evade detection	🟥🟥🟥	Injecting Process ID: 2516 Injected API: ZwMapViewOfSection Target Process ID: 2544 Target Image Path: %WorkingDir%\PAYMENT.SCR.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2516 Injected API: SetThreadContext Target Process ID: 2544 Target Image Path: %WorkingDir%\PAYMENT.SCR.exe
Uses Windows module loader to load dropped DLLs and execute code	🟥⬜⬜	Process ID: 2516 File: %TEMP%\nsk6098.tmp\f3lck4g5lonrri.dll

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
f3lck4g5lonrri.dll	Low	TROJ_GEN.R002C0RDJ21	Drops probable malware	-	15360	FEB4F10B870BB952D477637D93EB2D55BB9D31BF
c8jd3njjpvajds8	No risk	-	-	-	6661	BEDC1D70B06180364893A8D26E7086B5789F95BB
nsk6098.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
nsp6019.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
nsu6039.tmp	No risk	-	-	-	189500	138FE62CF65C9A99E517670CC3DBFA0CE2AB2A6C
y017mns1qito4dl9cyd8	No risk	-	-	-	164352	E92F020BC8932A6EE0E9ECAB657998EB5CD09D5C

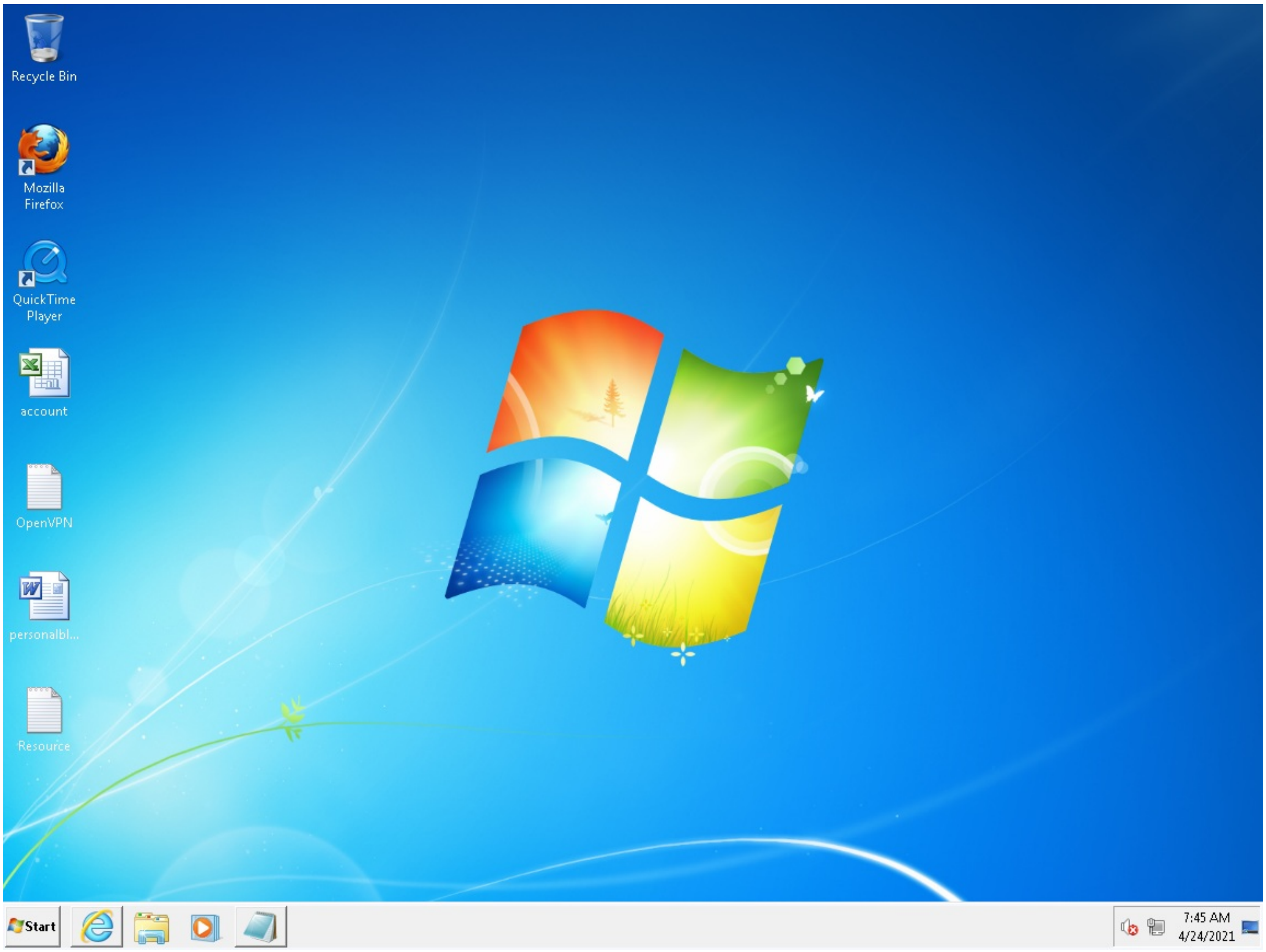
Suspicious Objects

Type	Object	Risk Level
File (SHA1)	DF247D1F45930896E17F102FF0925A53C1E33CA6	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0RDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0RDJ21 File Name: f3lck4g5lonrri.dll SHA1: FEB4F10B870BB952D477637D93EB2D55BB9D31BF Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		
Detection	Threat Characteristic: Rare executable file Global Detections: 1		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\PAYMENT.SCR.exe Packer: UNKNOWN		
Delete File	Path: %TEMP%\nsp6019.tmp Type: VSDT_EMPTY		2516
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2516 File: %TEMP%\nsp6019.tmp Type: VSDT_EMPTY		
Add File	Path: %TEMP%\c8jd3njjpvajds8 Type: VSDT_COM_DOS		2516
Write File	Path: %TEMP%\c8jd3njjpvajds8 Type: VSDT_COM_DOS		2516
Add File	Path: %TEMP%\y017mns1qito4dl9cyd8 Type: VSDT_COM_DOS		2516
Write File	Path: %TEMP%\y017mns1qito4dl9cyd8 Type: VSDT_COM_DOS		2516
Delete File	Path: %TEMP%\nsk6098.tmp Type: VSDT_EMPTY		2516
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2516 File: %TEMP%\nsk6098.tmp Type: VSDT_EMPTY		
Add File	Path: %TEMP%\nsk6098.tmp\f3lck4g5lonrri.dll Type: VSDT_DLL_W32		2516
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2516 File: %TEMP%\nsk6098.tmp\f3lck4g5lonrri.dll Type: VSDT_DLL_W32		
Write File	Path: %TEMP%\nsk6098.tmp\f3lck4g5lonrri.dll Type: VSDT_DLL_W32		2516
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\nsk6098.tmp\f3lck4g5lonrri.dll		
Call System API	API Name: LdrLoadDll Args: (3cacdc, 0, %TEMP%\nsk6098.tmp\f3lck4g5lonrri.dll, 10000000) Return: 0		2516
Detection	Threat Characteristic: Uses Windows module loader to load dropped DLLs and execute code Process ID: 2516 File: %TEMP%\nsk6098.tmp\f3lck4g5lonrri.dll		
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\PAYMENT.SCR.exe, "%WorkingDir%\PAYMENT.SCR.exe", , , , CREATE_SUSPENDED, , , , Process:2544:%WorkingDir%\PAYMENT.SCR.exe) Return: 1		2516
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2516 Injected API: ZwMapViewOfSection Target Process ID: 2544 Target Image Path: %WorkingDir%\PAYMENT.SCR.exe		
Detection	Threat Characteristic: Creates process Process ID: 2516 Image Path: %WorkingDir%\PAYMENT.SCR.exe Shell Command: "%WorkingDir%\PAYMENT.SCR.exe"		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2544:%WorkingDir%\PAYMENT.SCR.exe) Return: 1		2516
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2516 Injected API: SetThreadContext Target Process ID: 2544 Target Image Path: %WorkingDir%\PAYMENT.SCR.exe		
Detection	Threat Characteristic: Creates process Process ID: 2544 Image Path: %WorkingDir%\PAYMENT.SCR.exe		

▼ Screenshot



W10

Environment-specific risk level	Low risk The object exhibited mildly suspicious characteristics that are most likely benign.
Detections	Possible_GENISO-6, TROJ_GEN.R002C0RDJ21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - Payment.img (ISO image)

File name	Payment.img
File type	ISO image
SHA-1	14519983EA2F5E57EF45D5FBBA0F455BFD8038FA
SHA-256	430AF8C2476E1845F5C52BE263E38884280DA4765C1F5417584C4C49AAF754FB
MD5	F78C525E5F8642EB4655F10E78B10051
Size	1245184 byte(s)

Risk Level	Low risk
Detection	Possible_GENISO-6
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1)

Notable Threat Characteristics

Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as probable malware	🟥⬜⬜	Source: ATSE Detection Name: Possible_GENISO-6 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

Analysis

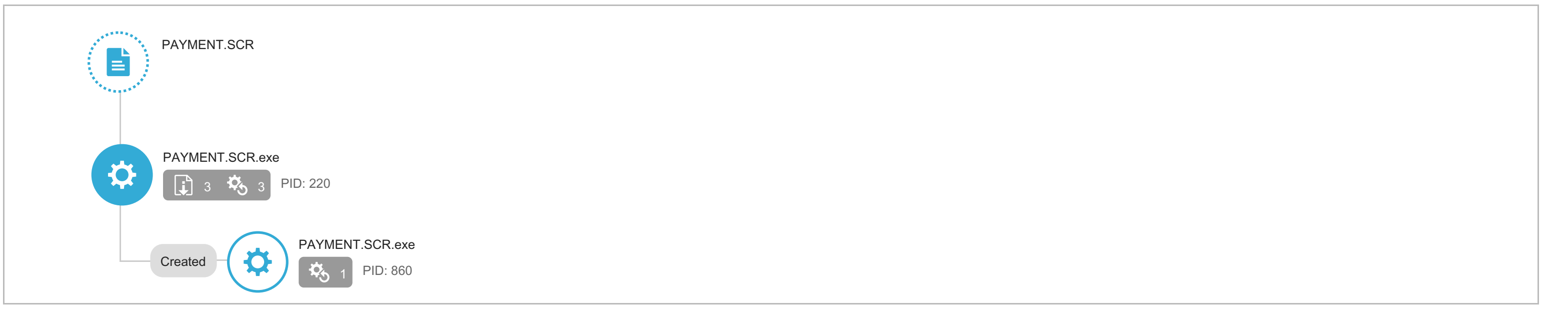
Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: Possible_GENISO-6 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		

Object 1.1 - PAYMENT.SCR (Windows 32-bit EXE file)

File name	PAYMENT.SCR
File type	Windows 32-bit EXE file
SHA-1	DF247D1F45930896E17F102FF0925A53C1E33CA6
SHA-256	1180277FE6D2C8A01916FD50EDC4C1EC703251BBF75AD6BF042A5796A7D46094
MD5	AE434794BA6D5D9B3C07675E5C73819D
Size	214666 byte(s)

Risk Level	Low risk
Detection	TROJ_GEN.R002C0RDJ21
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (1) File drop, download, sharing, or replication (3) Malformed, defective, or with known malware traits (3) Process, service, or memory object change (4)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics	
Execution	Execution through API	🟥⬜⬜ Characteristics:	1, 2
	Execution through Module Load	🟥⬜⬜ Characteristics:	1
Defense Evasion	Software Packing	🟥⬜⬜ Characteristics:	1
	File Deletion	🟥⬜⬜ Characteristics:	1, 2

Notable Threat Characteristics

Anti-security, self-preservation (1)

Characteristic	Significance	Details
Uses suspicious packer	🟥⬜⬜	File Name: %WorkingDir%\PAYMENT.SCR.exe Packer: UNKNOWN

Autostart or other system reconfiguration (1)

Characteristic	Significance	Details
Modifies file that can be used to infect systems	🟥⬜⬜	%TEMP%\nss7A1E.tmp\f3lck4g5lonrri.dll

File drop, download, sharing, or replication (3)

Characteristic	Significance	Details
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 220 File: %TEMP%\nss7A1E.tmp\f3lck4g5lonrri.dll Type: VSDT_DLL_W32
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 220 File: %TEMP%\nss7A1E.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 220 File: %TEMP%\nsy79EE.tmp Type: VSDT_EMPTY

Malformed, defective, or with known malware traits (3)

Characteristic	Significance	Details
Detected as probable malware	🟥⬜⬜	Source: ATSE Detection Name: TROJ_GEN.R002C0RDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92
Drops probable malware	🟥⬜⬜	Source: ATSE Detection Name: TROJ_GEN.R002C0RDJ21 File Name: f3lck4g5lonrri.dll SHA1: FEB4F10B870BB952D477637D93EB2D55BB9D31BF Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92
Rare executable file	🟥⬜⬜	Global Detections: 1

Process, service, or memory object change (4)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 860 Image Path: %WorkingDir%\PAYMENT.SCR.exe
Creates process	🟥⬜⬜	Process ID: 220 Image Path: %WorkingDir%\PAYMENT.SCR.exe Shell Command: "%WorkingDir%\PAYMENT.SCR.exe"
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 220 Injected API: SetThreadContext Target Process ID: 860 Target Image Path: %WorkingDir%\PAYMENT.SCR.exe
Uses Windows module loader to load dropped DLLs and execute code	🟥⬜⬜	Process ID: 220 File: %TEMP%\nss7A1E.tmp\f3lck4g5lonrri.dll

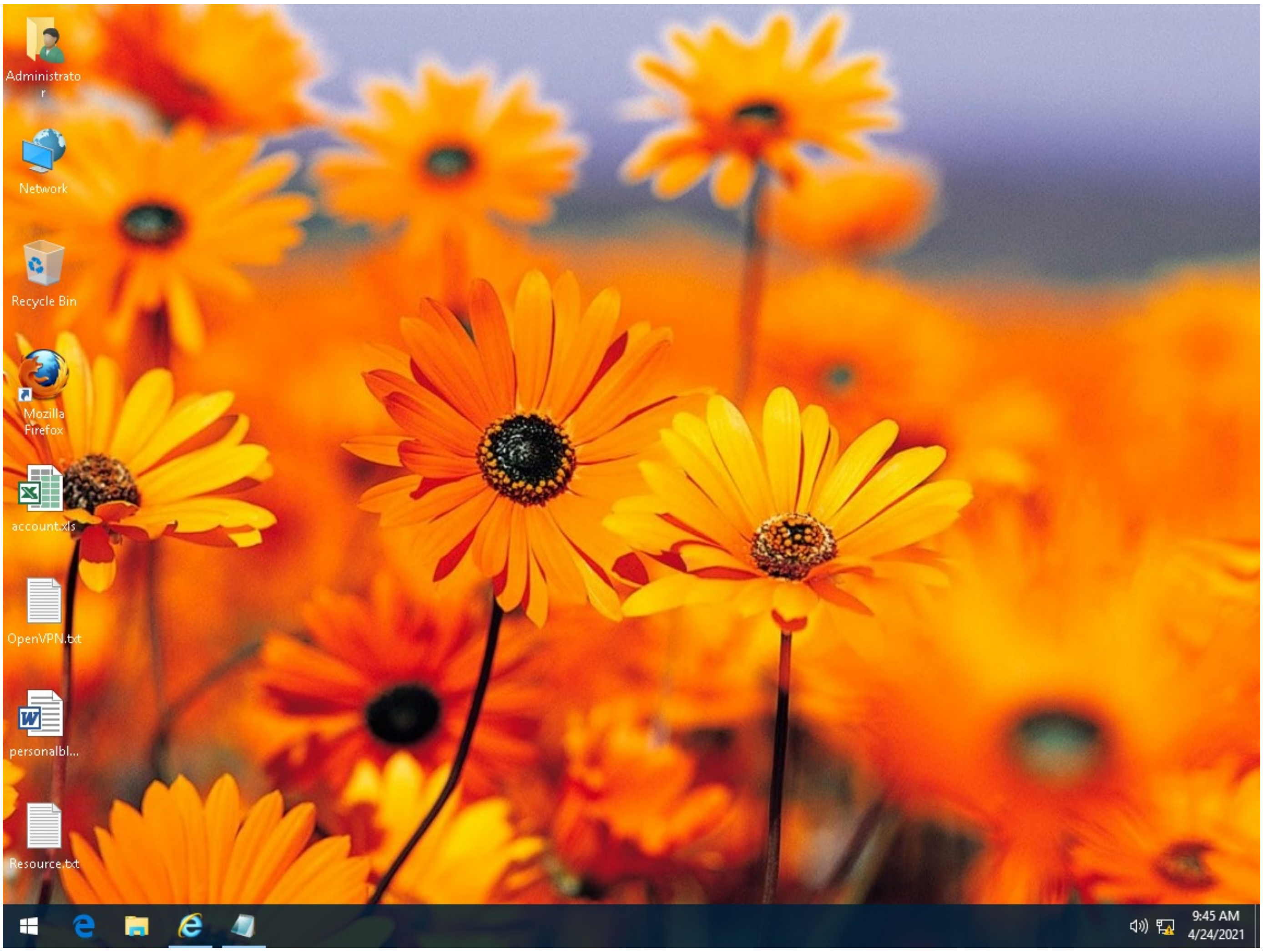
Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
f3lck4g5lonrri.dll	Low	TROJ_GEN.R002C0RDJ21	Drops probable malware	-	15360	FEB4F10B870BB952D477637D93EB2D55BB9D31BF
c8jd3njjpvajds8	No risk	-	-	-	6661	BEDC1D70B06180364893A8D26E7086B5789F95BB
nss7A1E.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
nsy79EE.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
nsy79EF.tmp	No risk	-	-	-	189500	138FE62CF65C9A99E517670CC3DBFA0CE2AB2A6C
y017mns1qito4dl9cyd8	No risk	-	-	-	164352	E92F020BC8932A6EE0E9ECAB657998EB5CD09D5C

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0RDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0RDJ21 File Name: f3lck4g5lonrri.dll SHA1: FEB4F10B870BB952D477637D93EB2D55BB9D31BF Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		
Detection	Threat Characteristic: Rare executable file Global Detections: 1		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\PAYMENT.SCR.exe Packer: UNKNOWN		
Delete File	Path: %TEMP%\nsy79EE.tmp Type: VSDT_EMPTY		220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 220 File: %TEMP%\nsy79EE.tmp Type: VSDT_EMPTY		
Call System API	API Name: LdrLoadDll Args: (9, 0, %TEMP%\nss7a1e.tmp\f3lck4g5lonrri.dll, 10000000) Return: 0		220
Detection	Threat Characteristic: Uses Windows module loader to load dropped DLLs and execute code Process ID: 220 File: %TEMP%\nss7A1E.tmp\f3lck4g5lonrri.dll		
Add File	Path: %TEMP%\c8jd3njjpvajds8 Type: VSDT_COM_DOS		220
Write File	Path: %TEMP%\c8jd3njjpvajds8 Type: VSDT_COM_DOS		220
Add File	Path: %TEMP%\y017mns1qito4dl9cyd8 Type: VSDT_COM_DOS		220
Write File	Path: %TEMP%\y017mns1qito4dl9cyd8 Type: VSDT_COM_DOS		220
Delete File	Path: %TEMP%\nss7A1E.tmp Type: VSDT_EMPTY		220
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 220 File: %TEMP%\nss7A1E.tmp Type: VSDT_EMPTY		
Add File	Path: %TEMP%\nss7A1E.tmp\f3lck4g5lonrri.dll Type: VSDT_DLL_W32		220
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 220 File: %TEMP%\nss7A1E.tmp\f3lck4g5lonrri.dll Type: VSDT_DLL_W32		
Write File	Path: %TEMP%\nss7A1E.tmp\f3lck4g5lonrri.dll Type: VSDT_DLL_W32		220
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\nss7A1E.tmp\f3lck4g5lonrri.dll		
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\PAYMENT.SCR.exe, "%WorkingDir%\PAYMENT.SCR.exe", , , , CREATE_SUSPENDED, , , , Process:860:%WorkingDir%\PAYMENT.SCR.exe) Return: 1		220
Detection	Threat Characteristic: Creates process Process ID: 220 Image Path: %WorkingDir%\PAYMENT.SCR.exe Shell Command: "%WorkingDir%\PAYMENT.SCR.exe"		
Call Thread API	API Name: SetThreadContext Args: (Process Name:860:%WorkingDir%\PAYMENT.SCR.exe) Return: 1		220
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 220 Injected API: SetThreadContext Target Process ID: 860 Target Image Path: %WorkingDir%\PAYMENT.SCR.exe		
Detection	Threat Characteristic: Creates process Process ID: 860 Image Path: %WorkingDir%\PAYMENT.SCR.exe		

▼ Screenshot



Process Graph Legend

Node

Submitted sample

Root process

Child process

——— Direct event

- - - - Indirect event

Created Event actions

Notable Threat Characteristics

Anti-security, self-preservation

Autostart or other system reconfiguration

Deception, social engineering

File drop, download, sharing, or replication

Hijack, redirection, or data theft

Malformed, defective, or with known malware traits

Process, service, or memory object change

Rootkit, cloaking

Suspicious network or messaging activity