Recorded Future®
Sandbox

Malware Analysis Report

2025-08-06 19:11

Sample ID	250806-xrrl8a1zcw			
Target	a.exe			
SHA256	e0a69439563c8534c2ef842d4ffcb16696f286d16585186de20351892f9917f1			
Tags	quasar	office04	discovery	persistence
	spyware	trojan		

score

10/10

Table of Contents

Part 1. Analysis Overview

score

10/10

SHA256
e0a69439563c8534c2ef842d4ffcb16696f286d16585186de20351892f9917f1

Threat Level: Known bad

The file a.exe was found to be: Known bad.

Malicious Activity Summary

quasar
office04
discovery
persistence
spyware
trojan

- 🟥 **Quasar family**
- 🟥 **Quasar payload**
- 🟥 **Quasar RAT**
- 🟨 **Executes dropped EXE**
- 🟨 **Adds Run key to start application**
- 🟨 **Codesign digest Mismatch**
- 🟨 **Suspicious use of SetThreadContext**
- ⬜ **System Location Discovery: System Language Discovery**
- ⬜ **Suspicious use of AdjustPrivilegeToken**
- ⬜ **Suspicious use of WriteProcessMemory**
- ⬜ **Suspicious behavior: AddClipboardFormatListener**
- ⬜ **Suspicious use of SetWindowsHookEx**

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16

Reconnaissance TA0043	
Resource Development TA0042	
Initial Access TA0001	
Execution TA0002	
Persistence **TA0003**	Boot or Logon Autostart E… T1547
	Registry Run Keys …T1547.001
Privilege Escalation **TA0004**	Boot or Logon Autostart E… T1547
	Registry Run Keys …T1547.001
Defense Evasion **TA0005**	Modify Registry T1112
Credential Access TA0006	
Discovery **TA0007**	System Location Discovery T1614
	System Language … T1614.001
Lateral Movement TA0008	
Collection TA0009	
Command and Control TA0011	
Exfiltration TA0010	
Impact TA0040	

Part 3. Analysis: static1

3. 1. Detonation Overview

Reported
2025-08-06 19:05

3. 2. Signatures

Codesign digest Mismatch

Description	Indicator	Process	Target
N/A	N/A	N/A	N/A

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-08-06 19:05	2025-08-06 19:08	win11-20250610-en	135s	152s

4. 2. Command Line

```
"C:\Users\Admin\AppData\Local\Temp\a.exe"
```

4. 3. Signatures

Quasar RAT

quasar trojan spyware

Quasar family

quasar

Quasar payload

Description	Indicator	Process	Target
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A

Executes dropped EXE

Description	Indicator	Process	Target
N/A	N/A	C:\Users\Admin\Documents\a.exe	N/A

Adds Run key to start application

persistence

Description	Indicator	Process	Target
Set value (str)	\REGISTRY\USER\S-1-5-21-903960561-1545645218-4290906778-1000\Software\Microsoft\Windows\CurrentVersion\Run\a.exe = "C:\\Users\\Admin\\Documents\\a.exe"	C:\Windows\system32\reg.exe	N/A

Suspicious use of SetThreadContext

Description	Indicator	Process	Target
PID 4600 set thread context of 5336	N/A	C:\Users\Admin\Documents\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
PID 1536 set thread context of 1364	N/A	C:\Users\Admin\AppData\Local\Temp\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

System Location Discovery: System Language Discovery

discovery

Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	N/A

Suspicious behavior: AddClipboardFormatListener

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	N/A

Suspicious use of AdjustPrivilegeToken

Description	Indicator	Process	Target
Token: SeDebugPrivilege	N/A	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	N/A

Suspicious use of SetWindowsHookEx

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 1536 wrote to memory of 5744	N/A	C:\Users\Admin\AppData\Local\Temp\a.exe	C:\Windows\System32\cmd.exe
PID 1536 wrote to memory of 5744	N/A	C:\Users\Admin\AppData\Local\Temp\a.exe	C:\Windows\System32\cmd.exe
PID 5744 wrote to memory of 5592	N/A	C:\Windows\System32\cmd.exe	C:\Windows\system32\reg.exe
PID 5744 wrote to memory of 5592	N/A	C:\Windows\System32\cmd.exe	C:\Windows\system32\reg.exe
PID 3440 wrote to memory of 4600	N/A	C:\Windows\system32\cmd.exe	C:\Users\Admin\Documents\a.exe
PID 3440 wrote to memory of 4600	N/A	C:\Windows\system32\cmd.exe	C:\Users\Admin\Documents\a.exe
PID 4600 wrote to memory of 5336	N/A	C:\Users\Admin\Documents\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
PID 4600 wrote to memory of 5336	N/A	C:\Users\Admin\Documents\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
PID 4600 wrote to memory of 5336	N/A	C:\Users\Admin\Documents\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
PID 4600 wrote to memory of 5336	N/A	C:\Users\Admin\Documents\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
PID 1536 wrote to memory of 1364	N/A	C:\Users\Admin\AppData\Local\Temp\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
PID 1536 wrote to memory of 1364	N/A	C:\Users\Admin\AppData\Local\Temp\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
PID 1536 wrote to memory of 1364	N/A	C:\Users\Admin\AppData\Local\Temp\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
PID 1536 wrote to memory of 1364	N/A	C:\Users\Admin\AppData\Local\Temp\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
PID 4600 wrote to memory of 5336	N/A	C:\Users\Admin\Documents\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
PID 1536 wrote to memory of 1364	N/A	C:\Users\Admin\AppData\Local\Temp\a.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

4. 4. Processes

C:\Users\Admin\AppData\Local\Temp\a.exe

```
"C:\Users\Admin\AppData\Local\Temp\a.exe"
```

C:\Windows\System32\cmd.exe

```
/c reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "a.exe" /t REG_SZ /d "C:\Users\Admin\Documents\a.exe" /f
```

C:\Windows\system32\reg.exe

```
reg  add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "a.exe" /t REG_SZ /d "C:\Users\Admin\Documents\a.exe" /f
```

C:\Windows\system32\cmd.exe

```
C:\Windows\system32\cmd.exe /c C:\Users\Admin\Documents\a.exe
```

C:\Users\Admin\Documents\a.exe

```
C:\Users\Admin\Documents\a.exe
```

C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

```
C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe
```

C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

```
C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe
```

4. 5. Network

Country	Destination	Domain	Proto
NL	213.209.150.188:2106		tcp
GB	57.128.140.217:443	ipwho.is	tcp
NL	213.209.150.188:2106		tcp

4. 6. Files

C:\Users\Admin\Documents\a.exe

MD5	2db32339fa151276d5a40781bc8d5eaa
SHA1	adf4fe80ccef030466c9d12b4340ea0a3fd02d9a
SHA256	e0a69439563c8534c2ef842d4ffcb16696f286d16585186de20351892f9917f1
SHA512	73b94263875881d4104b36d0e195aa7277d060dbab1674cfe0a5dbff290b9832ffbfcaa962f7ca6136d0f7e8d3fa0b2012479edb39d27ec36b0b01ac05b1ca55

memory/5336-4-0x0000000000B90000-0x0000000000D24000-memory.dmp

memory/1364-5-0x0000000001100000-0x0000000001294000-memory.dmp

memory/5336-6-0x0000000005AF0000-0x0000000006096000-memory.dmp

memory/5336-7-0x0000000005480000-0x0000000005512000-memory.dmp

memory/5336-8-0x0000000005530000-0x0000000005540000-memory.dmp

memory/1364-9-0x00000000031E0000-0x00000000031F0000-memory.dmp

memory/5336-10-0x0000000005430000-0x000000000544C000-memory.dmp

memory/5336-11-0x0000000005670000-0x000000000567A000-memory.dmp

memory/5336-12-0x0000000005930000-0x0000000005942000-memory.dmp

memory/5336-13-0x0000000005940000-0x000000000597A000-memory.dmp

memory/5336-14-0x00000000059E0000-0x0000000005A30000-memory.dmp

memory/5336-16-0x0000000006200000-0x00000000062B2000-memory.dmp

memory/5336-17-0x0000000006160000-0x00000000061AE000-memory.dmp

memory/5336-19-0x0000000006310000-0x000000000635A000-memory.dmp

memory/5336-18-0x00000000062C0000-0x000000000630C000-memory.dmp

memory/5336-20-0x0000000006360000-0x000000000638A000-memory.dmp

memory/5336-23-0x0000000007480000-0x0000000007492000-memory.dmp

memory/5336-24-0x00000000074E0000-0x000000000751C000-memory.dmp

memory/5336-25-0x0000000007890000-0x00000000078F6000-memory.dmp

memory/5336-26-0x0000000005530000-0x0000000005540000-memory.dmp

memory/5336-27-0x0000000007F80000-0x00000000084AC000-memory.dmp