


Malware Analysis (AnyRun Playbook)

By: Ryan Stewart



General Info

☒ Add for printing 

File name: payment advice.exe

Full analysis: <https://app.any.run/tasks/1c8f0ad5-c14b-4cbe-aafd-17d03c1f4740>

Verdict: **Malicious activity**

Threats: **Keylogger** Trojan

A keylogger is a type of spyware that infects a system and has the ability to record every keystroke made on the device. This lets attackers collect personal information of victims, which may include their online banking credentials, as well as personal conversations. The most widespread vector of attack leading to a keylogger infection begins with a phishing email or link. Keylogging is also often present in remote access trojans as part of an extended set of malicious tools.

Malware Trends Tracker >>>

Analysis date: May 10, 2022 at 19:06:38

OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)

Tags: evasion trojan snake keylogger

Indicators:

MIME: application/x-dosexec

File info: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows


MD5: 2C4CE1A8EAABB150842428FAD62D3AA5

SHA1: 3B363403E579459A7954C4564C950041327C755C

SHA256: 85F7F26CD9CFB9AB367D083F60B48E1594B1EADF8DD1A792C347273684855013

SSDEEP: 12288:fWmfDfxt7J0iJKfJDbV5wPw2a7iLv1/L5le289QgM8B:72RfJW1Ciblvng

Behavior activities

☒ Add for printing 

MALICIOUS	SUSPICIOUS	INFO
SNAKEKEYLOGGER was detected <ul style="list-style-type: none">RegSvc.exe (PID: 3864) SNAKE detected by memory dumps <ul style="list-style-type: none">RegSvc.exe (PID: 3864) Steals credentials from Web Browsers <ul style="list-style-type: none">RegSvc.exe (PID: 3864) Actions looks like stealing of personal data <ul style="list-style-type: none">RegSvc.exe (PID: 3864)	Checks supported languages <ul style="list-style-type: none">RegSvc.exe (PID: 3864)payment advice.exe (PID: 2884) Reads the computer name <ul style="list-style-type: none">RegSvc.exe (PID: 3864)payment advice.exe (PID: 2884) Loads DLL from Mozilla Firefox <ul style="list-style-type: none">RegSvc.exe (PID: 3864) Reads Environment values <ul style="list-style-type: none">RegSvc.exe (PID: 3864) Checks for external IP <ul style="list-style-type: none">RegSvc.exe (PID: 3864)	No info indicators.

DNS requests

Domain	IP	Reputation
checkip.dyndns.org	132.226.8.169	<div>shared</div>
	158.101.44.242	
	132.226.247.73	
	193.122.130.0	
	193.122.6.168	
mail.stilltech.ro	192.185.100.146	<div>malicious</div>

Malware configuration

☒ Add for printing 

SnakeKeylogger

(PID) Process	(3864) RegSvc.exe
Username (2)	office@stilltech.ro
	princenewman1111@gmail.com
Password	Null!
Host	eurobit555ro
Port	mail.stilltech.ro

***Password:** eurobit555ro

This task involved two processes, "**payment.exe**" and "**RegSvc.exe**." The former process originated from the user's temporary folder, while the latter process executed from the Microsoft .NET Framework folder and acted as a child process of the first. **The key event was the modification of registry keys.**

Specifically, the

"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap" registry key saw a change in the **"UNCAsIntranet"** value to "1," suggesting an attempt to manipulate the user's internet settings. Additionally, modifications to the **"ConsoleTracingMask"** and **"EnableFileTracing"** values in registry keys linked to the **"RegSvc.exe"** process hinted at efforts to conceal or obfuscate its activities.

To sum up, this task encompassed the execution of two processes and modifications to registry keys. The adjusted registry keys, particularly the **"UNCAsIntranet"** value, suggest possible manipulation of internet settings. The alterations in keys linked to **"RegSvc.exe"** point to an effort to conceal or obfuscate the process's activities, which holds significance for malware analysts evaluating potential malicious behavior or the existence of unwanted programs. This is considered a true positive indication of malicious intent.