Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

ALC: Is It a Scareware or a Ransomware?

Date of Publication	Admiralty Code	TA Number
March 23, 2023	A1	TA2023155

Summary

First appeared: March 2023
Malware: ALC
Attack Region: Worldwide
Attack: ALC is a scareware posing as ransomware, as it does not encrypt files on the victim's device. ALC merely disables the task manager and displays a ransom notice on the locked screen.

Attack Regions

Attack Details

#1

The malevolent scareware named "ALC Ransomware" pretends to be ransomware. During execution, ALC disables the task manager, freezes the screen, and displays a ransom note with instructions for restoring the data. A ransom note named "RUS!.txt" is displayed by “AlcDif.exe” on the compromised device, which suggests that the scareware may be aimed at Russia and its associated entities.

#2

The ALC binary is a 64-bit PE executable with a console subsystem. Execution is swift, taking the malware only a few seconds to freeze the victim's screen. When the ALC file is executed, it occupies the entire screen, likely to intimidate victims by simulating a locked screen. The program only occupies the primary monitor if the victim uses multiple monitors. Additionally, the program has the capability to toggle Task Manager, disabling it upon the first run. However, running the program again will re-enable Task Manager.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5’s Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the ’Potential MITRE ATT&CK TTPs’ & ‘Indicators of Compromise (IoC)’ on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0040 Impact	T1129 Shared Modules	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1112 Modify Registry	T1056 Input Capture	T1012 Query Registry
T1082 System Information Discovery	T1490 Inhibit System Recovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	3e6d52e151154065eb9da3da48dc7a7d,b6f780c70f6dd53a28286cf2d23f2359,79058D9B0FDFDADA59C18DF8AC026224,7384C4FCCF3818EF77C6188D7104A0B5,8D1C52CB4E6A5EA02275637D26F90F60,2B410375146A9BB550EDCA0BAE42A1CB,9A5E23DCC123B4B7526CE1D61DAB6CA4
SHA256	2943a567bc05bc66ca6201dbc5f00bec3f774a47b1b94289a2ae8e79834c21a5,bbc6a34b48a4c71a4d9c2ae2d8c975f3b6caf2e17b86057ccbcb6686d1d5a642,bff07ae5ccea66b658783fcf940eaf6baa453b534af2ebe9b70f14923871d82f,dc50ac15414b7274533cde5e1b28bfaa85353de38d4b21a8cb996412c0f6e432,0abe1ab9c75395a4ca829028d9c8c6530bd3bfda49e4b856b6f3539b9aa36ea5,1c5377db817c03f3c2711d351e380611291b5935ba0e2b0de763e4ef470e5bab,456961cba9a8dfce1b66081c6a73c2f1ec676fcdedac24c678f890a3425e7260,48b074b48bde3f15ca28983f26e855bafd6f19e8240d938b14f31417b39d9fd2,7efa5acd25e6276d122b2e2b8055a64dc4c757fc6067d3307973327154a507ff,84d4ca11c23a20bb220c15dbe3a363fb774081b6106c351fc9d8eab4f3b5b62c
Email	Alc@cock[.]li

References

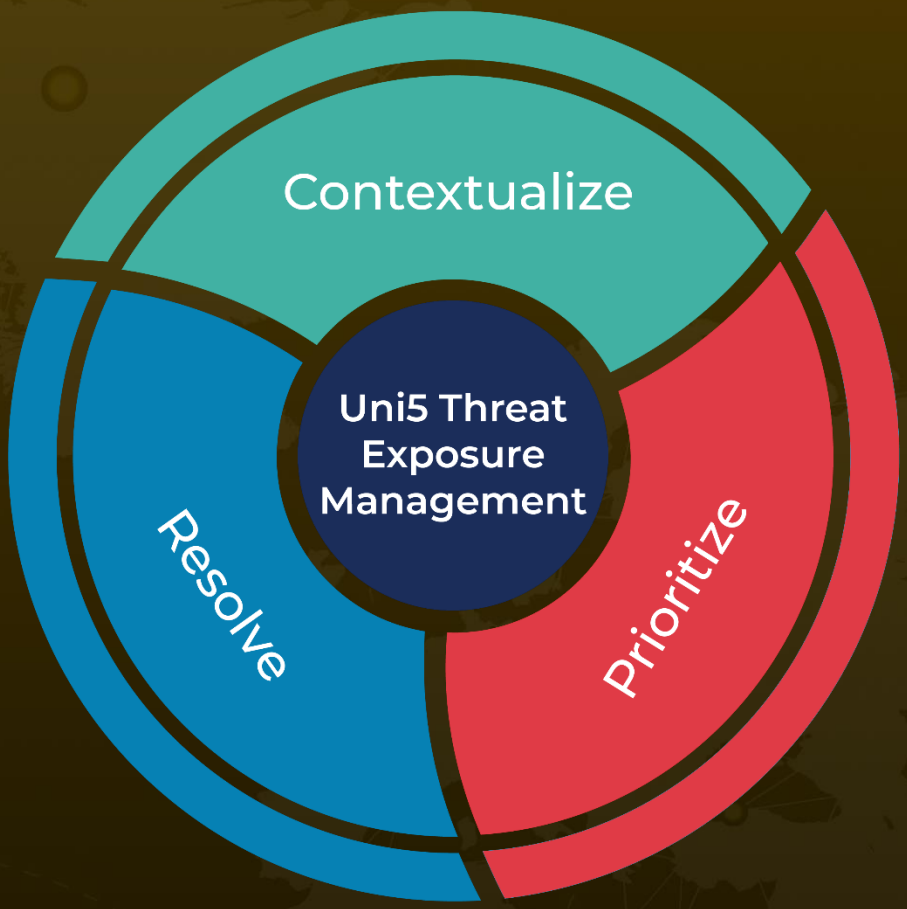
https://www.cyfirma.com/outofband/alc-scareware-pretends-to-be-a-ransomware/

https://www.fortinet.com/blog/threat-research/ransomware-roundup-sirattacker-acl

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 23, 2023 • 3:44 AM

More at www.hivepro.com