A9X Defender & Zeus Ransomware

Executive Summary

Keeping your anti-virus protection updated is extremely important, if you want to protect your marine vessels from new malware attacks. Anti-Virus signatures need to be updated on a regular daily basis. Relying on weekly updates exposes your marine vessels to a serious risk of infection.

With A9X Defender, powered by Windows Defender, supplies a full daily engine and signature update. Updates are downloaded once by the communications PC and distributed across the network. Updates are optimized for maritime and are 100-to-1 times smaller than most updates.

At A9X Cyber Security, we never compromise on security. We streamline the update process to provide full, daily signature updates with comprehensive reporting, rather than a limited weekly snapshot.

Virus Background

The recent **Zeus Ransomware,** encrypts user data and then prompts them to visit a website to learn how to pay a ransom and get their files back. The ransomware also threatens to publish the stolen data on their website if victims don't pay the ransom. Zeon payloads are a Python-based executable packaged via pyInstaller and further obfuscated via pyArmor to avoid detection.

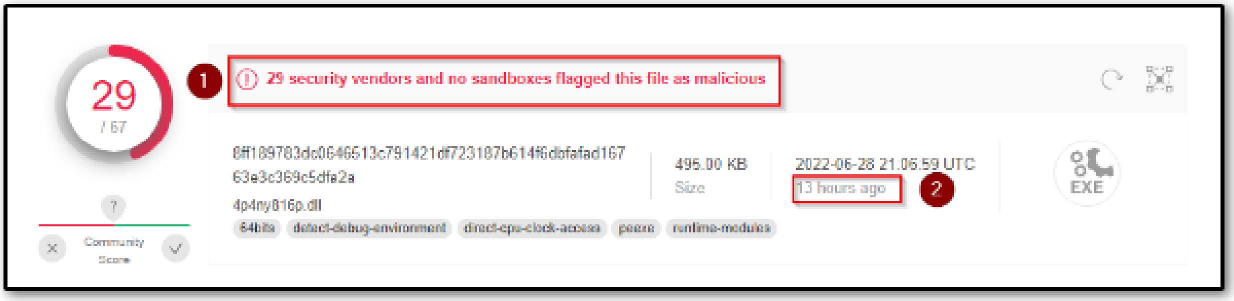
Testing

On 29th June 2022, we uploaded a sample of the Zeus ransomware to VirusTotal. Please see sample details were as below:

Family**:** Trojan:Win32/Casdet!rfn
MD5: fb5a4f129569e3d7aadba52083213e95
SHA256**:** 8ff189783dc0646513c791421df723187b614f6dbfafad16763e3c369c5dfa2a

Results

29 anti-virus applications detected the malware that was first uploaded 13 hours ago including A9X Defender:



29 / 67

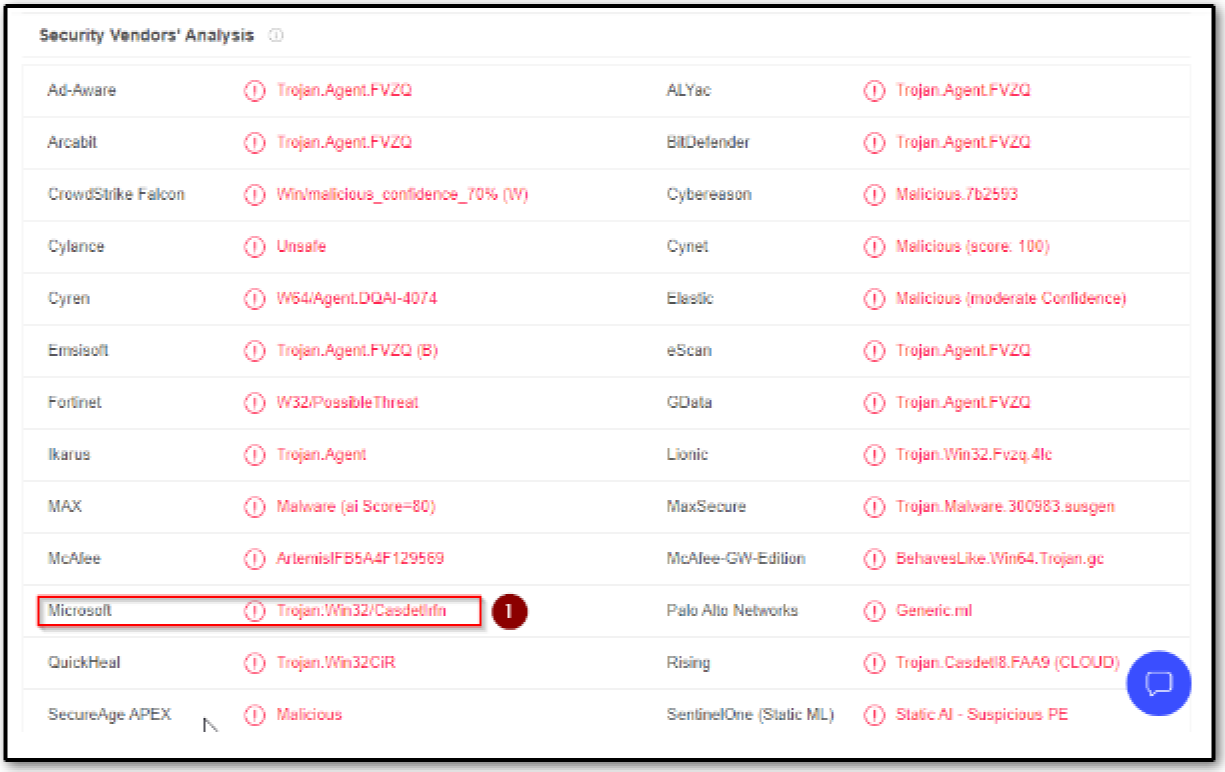
29 security vendors and no sandboxes flagged this file as malicious

8ff189783dc0646513c791421df723187b614f6dbfafad167
63e3c369c5dfa2a
4p4ny816p.dll

495.00 KB
Size

2022-06-28 21:06:59 UTC
13 hours ago

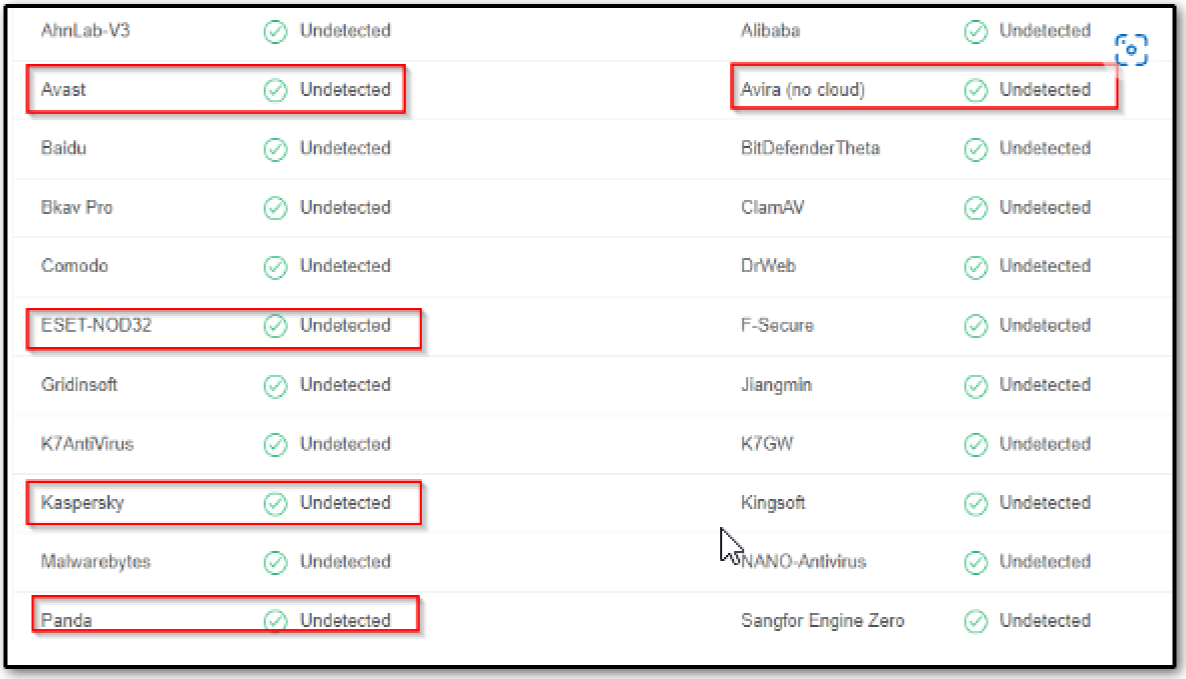
Notable applications that detected the malware included: BitDefender, Fortinet, CrowdStrike, Microsoft Defender, McAfee, TrendMicro and A9X Defender.



Security Vendors' Analysis

Ad-Aware	Trojan.Agent.FVZQ	ALYac	Trojan.Agent.FVZQ
Arcabit	Trojan.Agent.FVZQ	BitDefender	Trojan.Agent.FVZQ
CrowdStrike Falcon	Win/malicious_confidence_70% (W)	Cybereason	Malicious.7b2593
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W64/Agent.DQAI-4074	Elastic	Malicious (moderate Confidence)
Emsisoft	Trojan.Agent.FVZQ (B)	eScan	Trojan.Agent.FVZQ
Fortinet	W32/PossibleThreat	GData	Trojan.Agent.FVZQ
Ikarus	Trojan.Agent	Lionic	Trojan.Win32.Fvzq.4!c
MAX	Malware (ai Score=80)	MaxSecure	Trojan.Malware.300983.susgen
McAfee	Artemis!FB5A4F129569	McAfee-GW-Edition	BehavesLike.Win64.Trojan.gc
Microsoft	Trojan:Win32/Casdet!rfn	Palo Alto Networks	Generic.ml
QuickHeal	Trojan.Win32CiR	Rising	Trojan.Casdet!8.FAA9 (CLOUD)
SecureAge APEX	Malicious	SentinelOne (Static ML)	Static AI - Suspicious PE

The following Anti-Virus programs did not detect the malware:



AhnLab-V3	Undetected	Alibaba	Undetected
Avast	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
Comodo	Undetected	DrWeb	Undetected
ESET-NOD32	Undetected	F-Secure	Undetected
Gridinsoft	Undetected	Jiangmin	Undetected
K7AntiVirus	Undetected	K7GW	Undetected
Kaspersky	Undetected	Kingsoft	Undetected
Malwarebytes	Undetected	NANO-Antivirus	Undetected
Panda	Undetected	Sangfor Engine Zero	Undetected

Check Your Anti-Virus Systems

Anti-virus programs such as ESET and Kapersky are often relied on within the marine industry to protect your vessels against anti-virus attacks, however these are often not effective as shown above with the Zeus Ransomware. Select an anti-virus system that supplies a full daily engine and signature updates, and relies on compression technology to optimize the data transfer.

Chris Blunt
A9X Cyber Security Director of Operations