HC3: Analyst Note

October 12, 2023 TLP:CLEAR Report: 202310121200

NoEscape Ransomware

Executive Summary

A relatively new threat actor and ransomware to the cybercriminal community, NoEscape ransomware emerged in May 2023, but is believed to be a rebrand of Avaddon, a now defunct ransomware group shut down in 2021. Unlike many of its contemporaries, however, the unknown developers of this ransomware claim that in lieu of using source code or leaks from other established ransomware families, they have constructed their malware and its associated infrastructure entirely from scratch. Using unique features and aggressive multi-extortion tactics, in just under a year, it has targeted multiple industries, including the Healthcare and Public Health (HPH) sector. Their recent activities highlight the prominence and influence they have as a Ransomware-as-a-Service (RaaS) group. What follows is an overview of the group, possible connections to the Avaddon threat group, an analysis of NoEscape's ransomware attacks, its target industries and victim countries, sample MITRE ATT&CK techniques, and recommended defense and mitigations against the ransomware.

Overview

Figure 1: NoEscape Logo, Desktop Wallpaper, and Ransom Note. *(Source: BleepingComputer)*

At its most basic form, NoEscape is a ransomware, which is a malicious software that encrypts files on a victim's computer and demands a ransom in exchange for the decryption key. It typically infiltrates a system either as a file dropped by other malware, or as a file unknowingly downloaded by users while visiting suspicious websites. It also distinguishes itself as a RaaS group, a type of ransomware that is offered as a service to other criminals who act as affiliates or customers.

NoEscape At A Glance	
Confirmed Name	NoEscape Virus
Threat Type	Ransomware Crypto Virus Files Locker Double Extortion
Encrypted Files Extension	Ransom extension
Ransom Demanding Message	HOW_TO_RECOVER_FILES.txt It can have different file name depending on the attacker group
Detection Names	Avast Win32:RansomX-gen [Ransom] Emsisoft Trojan.GenericKD.67371017 (B) Malwarebytes Ransom.Avaddon Kaspersky HEUR:Trojan-Ransom.Win32.Generic Sophos Mal/Generic-S

HC3: Analyst Note

October 12, 2023 TLP:CLEAR Report: 202310121200

	Microsoft Trojan:Win32/Noescape!ic
Distribution Methods	Infected E-mail Attachments Malicious Downloads Dropped by Other Malware
Consequences	Files are encrypted and locked untl the ransom payment Data Leak Double Extortion
Free Decryptor Available?	No

Technical Details

NoEscape ransomware is capable of encrypting data on Windows and Linux machines, as well as VMware ESXi. However, it can only execute on a Windows NT 10.0 operating system. The specific implementation and techniques may vary depending on the affiliate or customer using the RaaS. NoEscape is written in C++ and claims to be written from scratch, without recycling code from previous malware samples or ransomware products. This service has an interface which allows the customization of compiled executables, allowing operators to choose whether they want to optimize for speed or thoroughness of encryption, which file paths to prioritize or ignore, and which services to terminate before starting encryption.

NoEscape uses RSA and ChaCha20 encryption algorithms, can perform asynchronous LAN scanning, and can encrypt discovered network file shares and local drives. Shadow copies and system back-ups are deleted by NoEscape, which is standard practice for ransomware programs. A unique feature is the shared encryption, which allows a single encryption key to be used across all infected files in a network, facilitating efficient encryption and quick decryption if the ransom is paid. Victims of the ransomware find notes titled “HOW_TO_RECOVER_FILES.TXT” in each folder with encrypted files.

This ransomware variant is compatible with Windows safe mode – a series of scripts can be run to force a victim host to reboot in safe mode, where endpoint detection and response (EDR) products can be disabled more easily before running encryption routines. As a RaaS tool, NoEscape also comes with other features in addition to the standard file encryption functions, including a Tor admin panel, private chat functions for secret communications, and distributed denial-of-service (DDoS), call, and spam services at extra cost (“Available from $500k”).

Two NoEscape threat types are listed on Trend Micro’s threat encyclopedia: Ransom.Win32.NOESCAPE.A and Ransom.Win32.NOESCAPE.B. These were added on August 18, 2022 and March 29, 2023 respectively. As such, it is likely that some functionalities of the NoEscape RaaS tool were tested in the wild prior to the announcement of the affiliate program on May 22, 2023.

Ransom and Payment

NoEscape ransomware leaves a ransom note on the victim’s computer, which contains a message to the victim that their network has been hacked and infected by the NoEscape group. The note serves as a communication channel through which the victims can follow the specified steps to engage with the ransomware developers. The ransom note also contains a “personal ID” required to log in to the threat actor’s Tor payment site and access the victim’s unique negotiation.

The ransom note usually contains a description of how to purchase the decryption tool from the

ransomware developers. The victims are required to pay the ransom in cryptocurrency, and the ransom amount varies depending on the severity of the attack and the specific ransomware variant. In previous attacks, NoEscape ransomware demands ranged between hundreds of thousands of dollars to over $10 million.

Target Industries

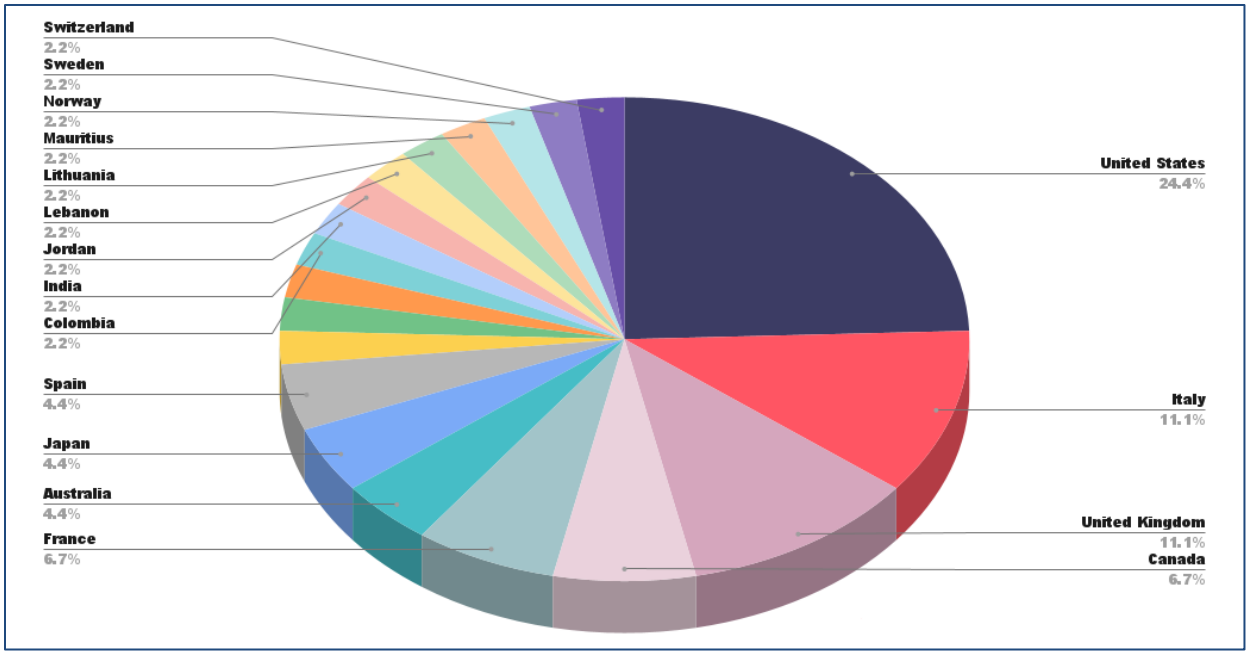

Figure 2: Distribution of Affected Countries by NoEscape Ransomware *(Source: SOCRadar)*

Since NoEscape operates as a RaaS, its targets vary depending on the affiliate and the buyer. Its creators, like many ransomware gangs, do not target Commonwealth of Independent States (CIS), or ex-Soviet Union republics, while disproportionately targeting the United States and several European countries as its preferred victims. The service allows operators and affiliates to take advantage of multi-extortion tactics, including triple extortion methods to maximize the impact of a successful attack.

This method refers to a three-pronged approach where data exfiltration and encryption is coupled with distributed denial-of-service (DDoS) attacks against the targets in an attempt to disrupt their business and coerce them into paying a ransom. The DDoS service is available for an added $500,000 fee, with the operators imposing conditions that forbid affiliates from striking entities located in CIS countries. Additional mechanisms are in place to reduce the chances of this malware running on hosts which are detected to be in CIS countries.

While examining NoEscape ransomware's target sectors, it can be inferred that it mostly targets organizations operating in the Professional Services, Manufacturing, and Information industries. However, its indiscriminate targeting of the HPH sector is a worrisome sign that more organizations in this field could be targeted soon. Of the known attack victims, one cybersecurity company noted only two victims in the healthcare sector as having been targeted by NoEscape.

HC3: Analyst Note

October 12, 2023 TLP:CLEAR Report: 202310121200

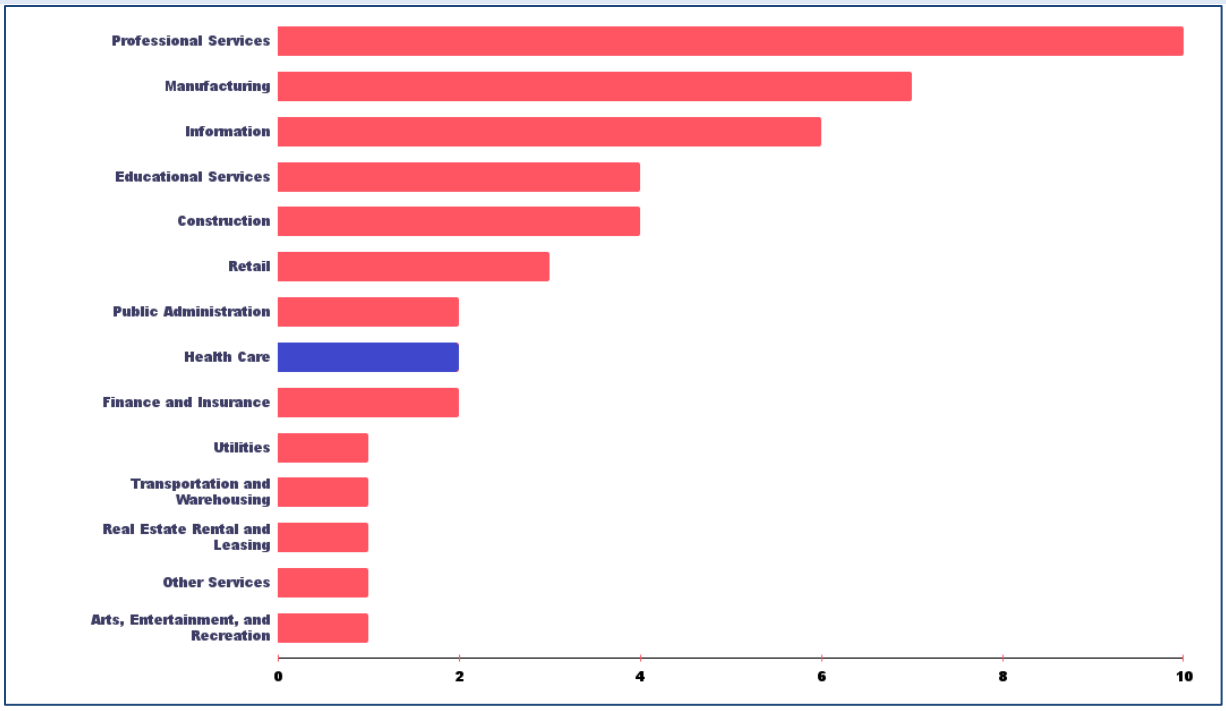

Figure 3: Distribution of Affected Sectors by NoEscape Ransomware (Emphasis added) *(Source: SOCRadar)*

Associations and Affiliates

While NoEscape ransomware launched in May 2023, it is believed to be a rebrand of Russian-speaking threat actor, Avaddon, a ransomware gang that shut down and released its decryption keys in 2021. The Avaddon ransomware operation launched in June 2020 using phishing campaigns to target corporate victims. However, in June 2021, a month after the Federal Bureau of Investigation and Australian law enforcement released Avaddon advisories, the ransomware gang suddenly shut down its operation and shared victims' decryption keys with a prominent cybersecurity company in an anonymous tip.

Connection Between Avaddon and NoEscape Ransomware	
Encryption Similarities	Both Avaddon and NoEscape encryptors are nearly identical. The primary difference lies in the encryption algorithm. While Avaddon utilized AES for file encryption, NoEscape adopted the Salsa20 algorithm. Despite this difference, the encryption logic and file formats used by both ransomwares are strikingly similar.
Configuration Overlaps	Both ransomwares use the same configuration file and directives, further cementing the belief in their intertwined origins.
Tactical Resemblance	NoEscape's overall strategy mirrors that of Avaddon. From gaining access to corporate networks to employing double-extortion tactics, the parallels are evident.
Geographical Exemptions	Just like Avaddon, NoEscape refrains from targeting countries of the former Soviet Union. Victims from these regions are provided with free decryption keys.
Possible Rebranding	The emergence of NoEscape shortly after Avaddon's cessation, combined with the similarities, suggests a potential rebranding. Some researchers believe that key players from the Avaddon campaign have now integrated into the NoEscape group.

Since then, there has not been any known ransomware or extortion activity associated with the threat actors until NoEscape launched its ransomware operation in 2023. One ransomware expert affiliated with the cybersecurity company states that NoEscape's and Avaddon's ransomware encryptors are almost

identical, with only one notable change in encryption algorithms. Previously, the Avaddon encryptor utilized AES for file encryption, with NoEscape switching to the Salsa20 algorithm. Otherwise, the encryptors are virtually identical, with the encryption logic and file formats almost identical, including a unique way of "chunking of the RSA encrypted blobs."

Additionally, the cybersecurity company determined that the Avaddon and NoEscape encryptors use the same configuration file and directives as described in a Mandiant article. While it is possible that the NoEscape threat actors purchased the source code of the encryptor from Avaddon, the cybersecurity company has been told by numerous researchers that it is believed that some of the core Avaddon members are now part of the new ransomware operation.

Mandiant previously tracked Avaddon and analyzed its multiple versions, along with potential ransomware families with which it shares similarities. In April 2021, Mandiant identified numerous ransomware services advertising in Russian-speaking underground forums, using assorted brands, yet having certain degrees of relations with Avaddon as far back as 2019. Mandiant also observed previous RaaS services operating since 2019 to 2021 connected to Avaddon source code. The timeline of these services and the similarities in the code may be part of the rebuilding process, suggesting collaboration between threat actors or access to a shared source code by multiple threat actors.

In June 2020, Mandiant reported that Avaddon advertised the Avaddon ransomware affiliate program on the Russian-speaking forums exploit[.]in and xss[.]is. MedusaLocker is ransomware that was also advertised on the Russian-speaking forum xss[.]is, by the threat actor 'Scourge' and reported by Mandiant in October 2019. During 2020, the service continued to be active and was updated with new versions of the ransomware. The last activity from the threat actor in the forum was in February 2021.

Ako, also known as MedusaReborn, is ransomware that was initially observed around January 2020. Ako operations continued to be active during 2020, and their last publicly exposed victim was added to their shaming blog in July 2020. Mandiant determined that Ako ransomware shares numerous similarities with MedusaLocker and considers Ako to be a variant of MedusaLocker. See previous HC3 Analyst Note on MedusaLocker for additional analysis on this Russian-speaking group.

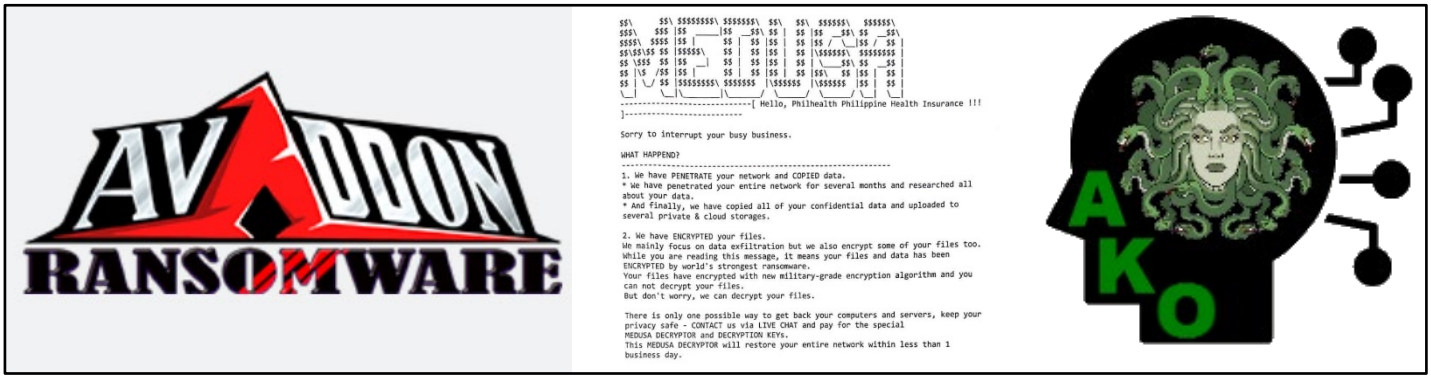

Figure 4: Logos for Avaddon, MedusaLocker, and Ako Ransomware Groups *(Source: BankInfoSecurity, Reddit, and ID-Ransomware Blog)*

Any direct association of NoEscape ransomware to active Russian-speaking threat actors remains unknown. However, strong evidence of its shared framework with Avaddon and Avaddon's affiliation with many former Russian-speaking threat actors shows a probable degree of affiliation. Much like NoEscape,

Avaddon had mandatory policies, to which their affiliates were prohibited from directing ransomware operations within CIS countries.

MITRE ATT&CK Techniques

NoEscape Ransomware uses the following MITRE ATT&CK techniques listed in the table below:

MITRE ATT&CK Tactics, Techniques, and Procedures of NoEscape Ransomware	
Initial Access	External Remote Services (T1133)
	Valid Accounts (T1078)
Execution	User Execution (T1204:002)
	Scheduled Task/Job (T1053.005)
Persistence	Registry Run Keys/Startup Folder (T1547.001)
	Valid Accounts (T1078)
Privilege Escalation	Valid Accounts (T1078)
Defense Evasion	Disable or Modify Tools (T1562.001)
	Software Packing (T1027.002)
	Process Injection (T1055)
	Indicator Removal on Host (T1070.004)
	Modify Registry (T1112)
	Deobfuscate/Decode Files or Information (T1140)
	Virtualization/Sandbox Evasion (T1497.001)
Credential Access	OS Credential Dumping (T1003)
Discovery	Account Discovery (T1078)
	Domain Trust Discovery (T1482)
	Permissions Group Discovery (T1069)
Lateral Movement	Remote Services (T1021)
	Remote Desktop Protocol (T1021.001)
Collection	Archive via Utility (T1560.001)
Command and Control	Web Protocols (T1071.001)
	Exfiltration to Cloud Storage (T1567.002)

Defense and Mitigations

Some best practices for protecting against NoEscape Ransomware and mitigating the impact of a successful attack include:

- **Regular Backups** Ensure that you maintain regular backups of your critical data. Store these backups in a secure location, preferably offline, to prevent them from being targeted by ransomware.
- **Update Software:** Keep all software, especially your operating system and security solutions, up to date. Regular updates often contain patches for known vulnerabilities that ransomware might exploit.
- **Email Caution:** Be wary of email attachments and links, especially from unknown senders. Phishing e-mails are a common method used by ransomware to infiltrate systems.

- **Strong Passwords:** Use strong, unique passwords for all accounts and enable multi-factor authentication wherever possible.
- **Security Solutions:** Invest in reliable cybersecurity solutions that offer real-time protection against malware and ransomware threats.
- **Educate and Train:** Regularly train and educate employees about the dangers of ransomware and how to recognize potential threats.
- **Incident Response Plan:** Have a well-defined incident response plan in place. In case of a ransomware attack, knowing the immediate steps to take can significantly reduce damage.
- **Avoid Suspicious Downloads:** Refrain from downloading files or software from untrusted sources or websites.
- **Network Security:** Implement firewalls and other network security measures to monitor and control incoming and outgoing network traffic.

Way Forward

NoEscape may be new to the cyber threat landscape, but in its short existance, it has proven to be a formidable adversary. Empirical evidence suggests that NoEscape is a rebranding of the Avaddon ransomware gang. However, unlike Avaddon, it has yet to be determined if there is a free decrypter that organizations can use to recover files for free. Until then, unless certain detection and prevention methods are put in place, a successful exploitation by NoEscape ransomware will almost certainly result in the encryption and exfiltration of significant quantities of data. The value of HPH data, in particular, signals that the healthcare industry will remain a viable target.

In addition to the aforementioned defense and mitigation strategies, HC3 recommends that HPH organizations utilize resources from CISA Stop Ransomware, HHS 405(d), and the H-ISAC to proactively and reactively aid healthcare organizations with cybersecurity awareness and guidance.

The probability of cyber threat actors targeting any industry remains high, but especially so for the Healthcare and Public Health sector. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with tools and resources necessary to prevent a cyberattack remains the best way forward for healthcare organizations.

Relevant HHS Reports

HC3: Alert – 2021 Trends Show Increased Globalized Threat of Ransomware (February 9, 2022)

HC3: Alert - Russian State-Sponsored and Criminal Cryber Threats to Critical Infrastructure (May 9, 2022)

HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (March 1, 2022)

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

HC3: Analyst Note – MedusaLocker Ransomware (February 24, 2023)

HC3: Analyst Note – The Russia-Ukraine Cyber Conflict and Potential Threats to the US Health Sector (March 1, 2022)

HC3: Threat Brief – An Analysis of the Russia/Ukraine Conflict (March 17, 2022)

HC3: Threat Brief – Ransomware Trends in Q1 2022 (May 5, 2022)

HC3: Threat Brief – Ransomware Trends 2021 (June 3, 2021)

References

Abrams, Lawrence. "Meet NoEscape: Avaddon ransomware gang's likely successor." BleepingComputer. July 17, 2023. https://www.bleepingcomputer.com/news/security/meet-noescape-avaddon-ransomware-gangs-likely-successor/

Bonaobra, Jeffrey Francis. "Ransom.Win32.NOESCAPE.A." TrendMicro. August 18, 2022. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Ransom.Win32.NOESCAPE.A/

"Dark Web Profile: NoEscape Ransomware." SOCRadar. September 20, 2023. https://socradar.io/dark-web-profile-noescape-ransomware/#:~:text=NoEscape%20Ransomware%20surfaced%20in%20June,a%20striking%20resemblance%20to%20Avaddon.

Dela Cruz, Rojan. "Ransom.Win32.NOESCAPE.B." TrendMicro. March 29, 2023. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Ransom.Win32.NOESCAPE.B/

Hernandez, Adrian Sanchez and Paul Tarter, Ervin James Ocampo. "One Source to Rule Them All: Changing AVADDON Ransomware." Mandiant. January 19, 2022. https://www.mandiant.com/resources/blog/chasing-avaddon-ransomware

Lakshmanan, Ravie. "New Linux Ransomware Strain BlackSuit Shows Striking Similarities to Royal." The Hacker News. June 3, 2023. https://thehackernews.com/2023/06/new-linux-ransomware-strain-blacksuit.html

Montini, Heloise. "NoEscape Ransomware: The Complete Guide." SalvageData. August 31, 2023. https://www.salvagedata.com/noescape-ransomware/

"NoEscape Ransomware: In-Depth Analysis, Detection, and Mitigation." SentinelOne. Accessed October 4, 2023. https://www.sentinelone.com/anthology/noescape/

"NoEscape Ransomware Report." Quorum Cyber. Accessed October 4, 2023. https://www.quorumcyber.com/malware-reports/noescape-ransomware-malware-report/

"Novel NoEscape ransomware operation believed to be Avaddon rebrand." SC Media. July 18, 2023. https://www.scmagazine.com/brief/novel-noescape-ransomware-operation-believed-to-be-avaddon-rebrand

"Ransomware group claimed to have hit a New Jersey cardiology group. Did they?" DataBreaches.net September 23, 2023. https://www.databreaches.net/ransomware-group-claimed-to-have-hit-a-new-jersey-cardiology-group-did-they/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback