Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

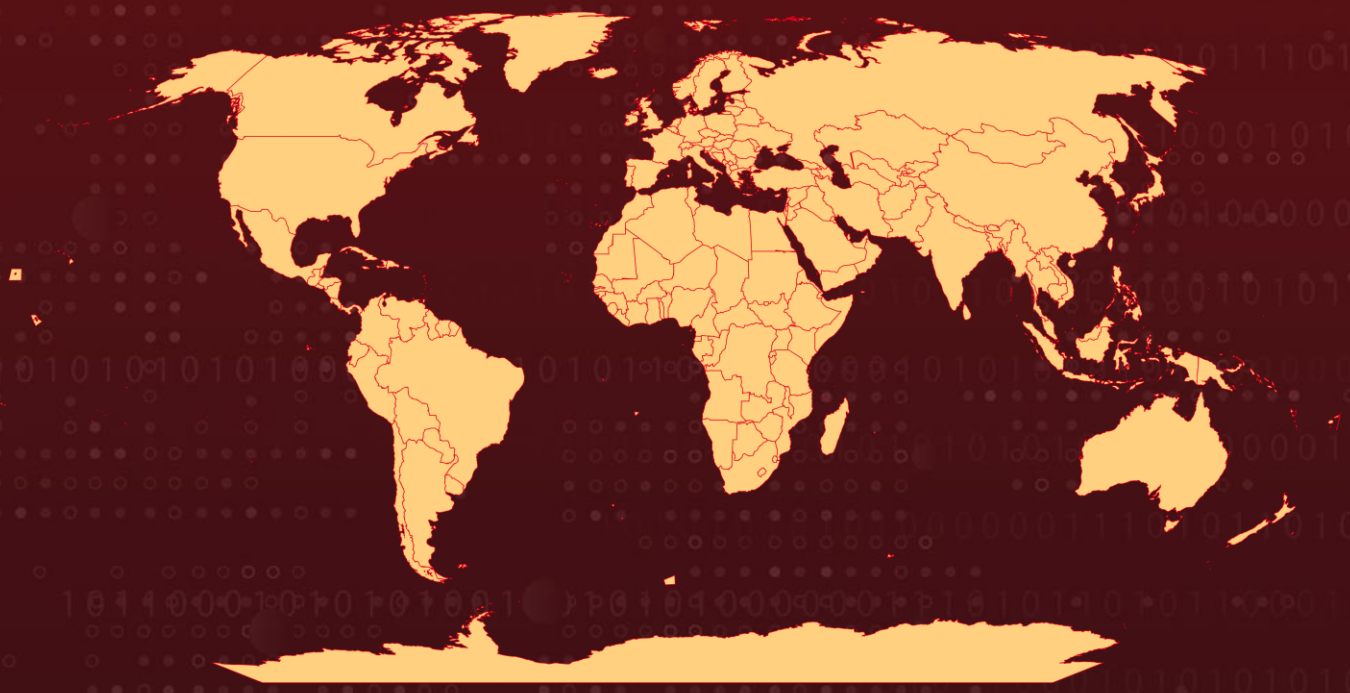
DragonForce Unleashes Chaos with Leaked Lockbit Builder

Date of Publication	Admiralty Code	TA Number
June 25, 2024	A1	TA2024243

Summary

First Seen: December 2023
Attack Region: Worldwide
Malware: DragonForce Ransomware
Attack: The DragonForce Ransomware, discovered in December 2023, has been associated with numerous high-profile cyberattacks. DragonForce has been observed utilizing a leaked Lockbit Black builder enabling them to customize and execute their operations with ease potentially amplifying the scale and impact of their malicious activities.

Attack Regions



Attack Details

#1 In December 2023, a recently identified ransomware group known as DragonForce gained prominence due to its targeting of high-profile entities. This group utilizes a tactic known as double extortion, where they first exfiltrate data from their victims before encrypting it. DragonForce has proven adept at infiltrating networks and efficiently encrypting data, blending conventional methods with innovative approaches to maximize their financial returns.

#2 One notable attack occurred in March 2024, when the Palau government was hit, crippling their computer systems. Ransom notes from both LockBit and DragonForce were found, indicating the use of a leaked LockBit builder tool rather than a direct connection to LockBit itself. There were also suspicions of a link to 'DragonForce Malaysia', a hacking group known for its activism, but they denied involvement via their Telegram channel.

#3 DragonForce leverages a leaked ransomware builder from LockBit to execute their attacks. They use a double extortion technique: locking victims out of their systems and stealing data, which they threaten to release on the dark web if their ransom demands aren't met.

#4 DragonForce typically initiates attacks through phishing emails or by exploiting vulnerabilities in Remote Desktop Protocols (RDP) and Virtual Private Networks (VPN). Once inside a network, they quickly spread and use strong encryption algorithms to lock down crucial systems and data.

#5 A particularly striking case involved the Ohio Lottery, where DragonForce claimed to have stolen over 600 GB of data, including three million records with names, email addresses, and social security numbers. As of now, they have listed 63 victims on their Data Leak Site, primarily targeting the US.

#6 DragonForce's use of the LockBit Black builder highlights the growing danger posed by leaked malware-building tools. These tools allow threat actors to easily customize and deploy ransomware, increasing the global risk. The accessibility of such advanced tools means these kinds of impactful attacks are likely to continue, underlining the need for robust cybersecurity measures and vigilance.

Recommendations

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, storing them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a ransomware attack, up-to- date backups enable recovery without paying the ransom.

File Monitoring and Logging: Implement file monitoring and logging to track sudden file access and modifications. Utilize File Integrity Monitoring (FIM) tools to oversee critical files and directories, receiving alerts for any changes. This approach helps detect and respond early to ransomware behavior, such as file encryption attempts.

Application whitelisting: Maintain a comprehensive inventory of approved applications and regularly update your whitelist to include only trusted software. This involves understanding your environment, defining strict criteria for allowed applications, and actively managing changes and updates to ensure ongoing security effectiveness.

Protect Remote Services: DragonForce Ransomware exploits exposed external remote services. To counter this, ensure remote access services are secured with strong passwords and, when possible, implement IP whitelisting. Grant only the essential permissions needed for operational and remote access and avoid using accounts with administrative privileges unless necessary.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0007 Discovery	TA0040 Impact	T1566 Phishing	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1204 User Execution	T1204.002 Malicious File	T1562 Impair Defenses

T1562.001 Disable or Modify Tools	**T1070** Indicator Removal	**T1070.004** File Deletion	**T1083** File and Directory Discovery
T1486 Data Encrypted for Impact	**T1082** System Information Discovery	**T1133** External Remote Services	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	d54bae930b038950c2947f5397c13f84
SHA1	e164bbaf848fa5d46fa42f62402a1c55330ef562
SHA256	1250ba6f25fd60077f698a2617c15f89d58c1867339bfd9ee8ab19ce9943304b
Tor Address	Z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion, 3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd[.]onion

Recent Breaches

https://www.altipal.com.co
https://accuratelockandhardware.com
https://monocon.com
https://www.persyn.be
https://www.wattcarmichael.com
https://www.maloneaccountants.ie
https://hardings-transport.com
https://cssltd.co.uk
https://motormunich.cat
https://dean-lumber.com
https://windcomservices.com
https://local1964.org
https://one.biremote.net
https://davisyounglaw.com
https://hoppecke-us.com
https://barretteyecare.com
https://parrish-mccall.com

https://evoevents.co.nz
https://seafrigo.com
https://thebus.org
https://www.aussizzgroup.com
https://www.palaugov.pw
https://www.kadushisoft.com
https://saintcecilias.london
https://www.swansea.com
https://www.online.majuhome.com.my
https://teamlocum.com
https://www.rigcon.com
https://vmab.se
https://www.npcitaly.com
https://www.speakindeacon.com
https://fullingtontours.com
https://www.greenlineva.com
https://tetonortho.com
https://www.dunbier.com
https://www.jdcpl.us
https://www.faison.com
https://www.erwat.co.za
https://artissimodesigns.com
https://crystalwindows.com
https://wardtlc.com
https://compressionleasing.com
https://westward360.com
https://geologics.com

References

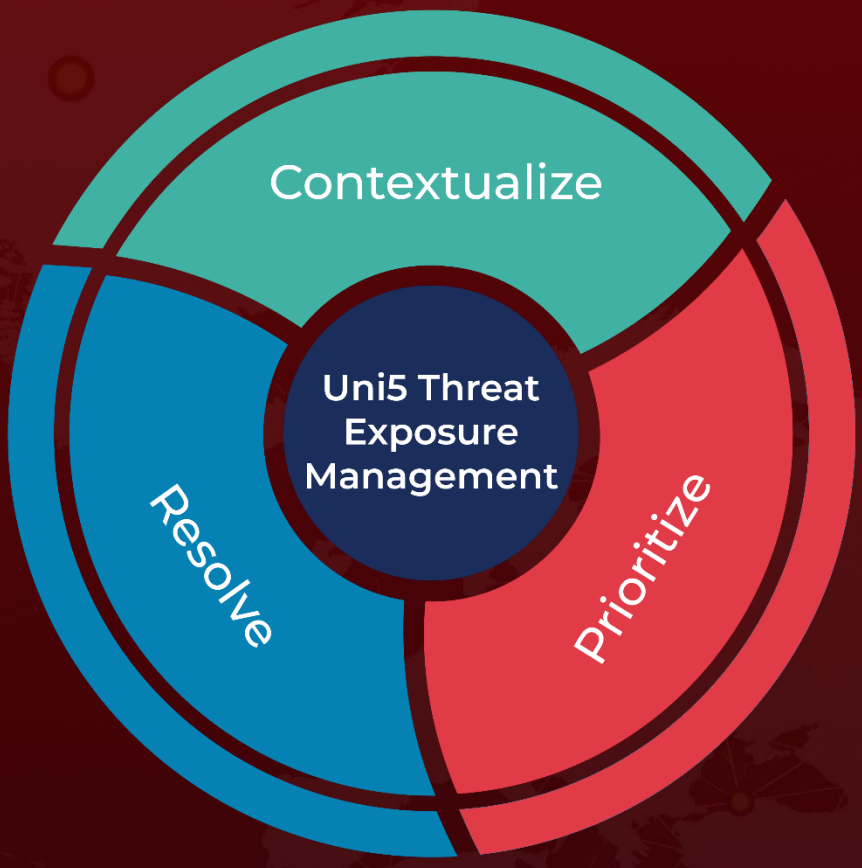
https://socradar.io/dark-web-profile-dragonforce-ransomware/

https://cyble.com/blog/lockbit-blacks-legacy-unraveling-the-dragonforce-ransomware-connection/

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

June 25, 2024 • 7:00 AM

More at www.hivepro.com