Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

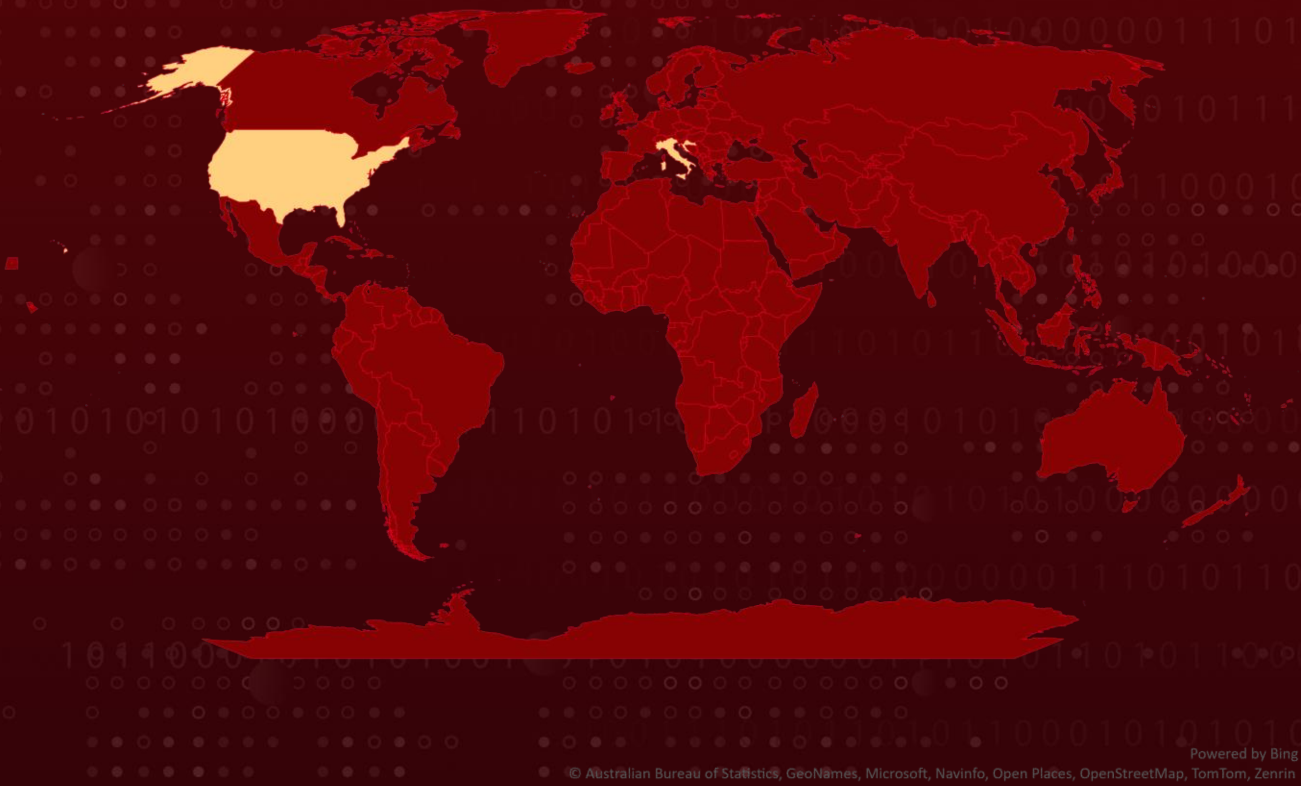
Eldorado: A New Ransomware Threat Targeting Windows and VMware

Date of Publication	Admiralty Code	TA Number
July 8, 2024	A1	TA2024263

Summary

First Appearance: March 2024
Malware: Eldorado ransomware
Targeted Countries: United States, Italy, Croatia
Affected Platforms: Windows, Linux, VMWare ESXi
Targeted Industries: Real Estate, Education, Professional Services, Health Care, Manufacturing, Telecommunications, Business Services, Administrative Services, Transportation, Government and Military
Attack: Eldorado, a new Golang based ransomware, targets Windows and VMware ESXi, affecting U.S. sectors like real estate, education, healthcare, and manufacturing. It uses ChaCha20 and RSA encryption, avoids critical system files to maintain usability, and self-deletes post-encryption.

Attack Regions


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 Eldorado is a new ransomware that emerged in March 2024, targeting both Windows and VMware ESXi virtual machines. It has already claimed 16 victims in the U.S., affecting sectors such as real estate, education, healthcare, and manufacturing.

#2 This ransomware is Go-based and utilizes the ChaCha20 algorithm for encryption, generating a unique 32-byte key and 12-byte nonce for each file. These keys and nonces are then encrypted using RSA with OAEP. Encrypted files are marked with the ".00000001" extension, and ransom notes are left in the Documents and Desktop folders.

#3 Eldorado also encrypts network shares via the SMB protocol, deletes shadow volume copies to prevent recovery, and skips certain file types like DLLs and executables to avoid system unusability. To evade detection, the ransomware is designed to self-delete after the encryption process.

#4 Researchers highlight that Eldorado is a unique, standalone operation, not a rebrand of an existing group. Affiliates can customize parameters such as which directories to encrypt on Windows systems, though the Linux version offers fewer customization options.

#5 An interesting aspect of Eldorado is that it avoids encrypting critical system files. This ensures that the infected system remains functional, potentially giving the attackers more time to operate within the network. Additionally, Eldorado has a self-destruct mechanism that can be triggered, likely as an evasion tactic to avoid detection or analysis.

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with Eldorado ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.

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 Eldorado ransomware attack, up-to-date backups enable recovery without paying the ransom.

Access Control and Least Privilege: Enforce the principle of least privilege, ensuring that users and applications have only the minimum access required to perform their functions. This limits the potential impact of a ransomware attack.

Network Segmentation: Divide the network into segments to limit the spread of ransomware. This can help contain the damage and protect sensitive data.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0002 Execution	TA0007 Discovery	TA0005 Defense Evasion
TA0040 Impact	T1059 Command and Scripting Interpreter	T1204 User Execution	T1059.001 PowerShell
T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery	T1082 System Information Discovery	T1027 Obfuscated Files or Information
T1070 Indicator Removal	T1048 Exfiltration Over Alternative Protocol	T1070.004 File Deletion	T1083 File and Directory Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1375e5d7f672bfd43ff7c3e4a145a96b75b66d8040a5c5f98838f6eb0ab9f27b, 7f21d5c966f4fd1a042dad5051dfd9d4e7dfed58ca7b78596012f3f122ae66dd, cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d96736174a7, b2266ee3c678091874efc3877e1800a500d47582e9d35225c44ad379f12c70de, dc4092a476c29b855a9e5d7211f7272f04f7b4fca22c8ce4c5e4a01f22258c33, 8badf1274da7c2bd1416e2ff8c384348fc42e7d1600bf826c9ad695fb5192c74, cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d96736174a7
MD5	9d1fd92ea00c6eef88076dd55cad611e, 315a9d36ed86894269e0126b649fb3d6
TOR Address	hxxp[:]//dataleakypypu7uwblm5kttv726l3iripago6p336xjnbstkjwrlnlid[.]onion
Email	russoschwartz@onionmail[.]org
IPv4	173[.]44[.]141[.]152

References

https://www.group-ib.com/blog/eldorado-ransomware/

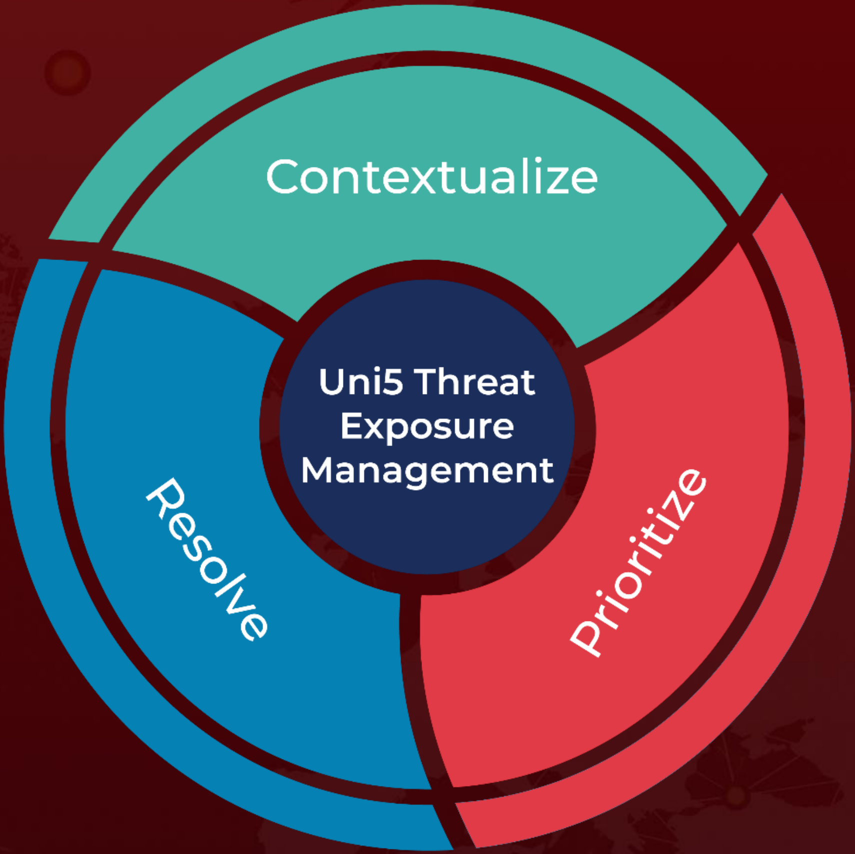
https://mobile.x.com/RakeshKrish12/status/1800479631507915095

https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/el-dorado

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

July 8, 2024 • 6:30 AM

More at www.hivepro.com