CASE STUDY

Embargo Ransomware Attack: *Detection and Prevention.*

Cylerian, an end-to-end cybersecurity solutions, helped identify and thwart a ransomware attack on a company in the hospitality industry. The threat actor, believed to be affiliated with the "Embargo Ransomware Group," an offshoot of the ALPHV Blackcat group, gained access via a password spraying attempt against a VPN server, and was able to abuse account weaknesses to gain escalate access to critical systems and defeat an industry-leading EDR solution. The Cylerian platform's holistic approach to security enabled the victim enterprise to fully identify and mitigate the threat, preventing further data loss and operational disruption.

THREAT	INDUSTRY	DATE	LOCATION	IMPACT
+ Ransomware	+ Hospitality	+ August, 2024	+ United States	+ Stolen files/user data

01 ATTACK TIMELINE

01	INITIAL COMPROMISE	Though the initial vector is unknown, common attack techniques of ransomware operators include social engineering, and password re-use.
02	ESTABLISH FOOTHOLD	Attackers connected to a VPN server, without MFA, using stolen user credentials. Attackers leveraged a private VPN service to hide the command and control IP address.
03	INTERNAL RECON	The attackers used adfind, a common tool to enumerate Active Directory assets, to perform internal reconnaissance.
04	ESCALATE PRIVILEGES	The attackers performed password spraying. In addition, they harvested hashes of admin accounts using a technique called Kerberoasting.
05	MOVE LATERALLY	The attackers used PsExec along with domain administrator accounts to connect to internal servers, map out the network and find file shares of interest to steal data from.
06	DEFENSE EVASION	The attackers used signed malware to defeat the industry-leading EDR product. The malware is a variant of POORTRY and its loader, STONESTOP, to defeat EDR.
07	MAINTAIN PRESENCE	The attackers installed Anydesk, a common remote administration utility, to maintain persistence on the network.
08	COMPLETE MISSION	The attackers installed Rclone and Filezilla, well known tools, to transfer files. Cylerian helped remediate the environment before ransomware tools were deployed.

WEB
www.cylerian.com

SALES
sales@cylerian.com

PHONE
+1 (833) 295-7426

02 INDICATORS

A comprehensive platform that provides visibility across endpoints, networks, cloud and applications make it feasible to detect threats at each stage of an attack lifecycle. This table includes network and host-based indicators that can be used to detect the Embargo Ransomware group:

INDICATOR	PHASE	DETAILS
Anomalous Remote Access logins	INITIAL ACCESS	Cylerian used behavioral analytics to detect anomalous SSL VPN logins based on the source IP address.
Kerberoasting	CREDENTIAL ACCESS	Look for anomalous requests to kerberos service tickets in Windows security logs. Cylerian identified anomalous service ticket requests for kerberoastable domain admin accounts from the VPN IP address space.
ADFind	RECONNAISSANCE	Analyze process executions and command line arguments. Attackers passed [`objectcategory=computer`, `objectcategory=computer`, `objectcategory=group`, trustdmp] as arguments to adfind.
Anydesk	PERSISTENCE	Cylerian detected the use of Anydesk. Anydesk is a common remote administration tool but is also used by attackers.
Anomalous user logins	LATERAL MOVEMENT	Attackers leveraged compromised credentials to move laterally via RDP. Cylerian detected anomalous interactive logins using service accounts.
Common command-line reconnaissance	RECONNAISSANCE	Cylerian detected the following commands by attackers: `nltest /domain_trusts` · `nltest /dclist:<domain>` · `net group "domain admins" /domain`
PsExec	LATERAL MOVEMENT	PsExec and tools like it, like RemCom, are commonly used by attackers to move laterally. The use of such tools can be detected by most EDR tools by monitoring process executions and service creations.
Anomalous RDP Sessions	LATERAL MOVEMENT	There are several Windows Event IDs that reflect the source hostname, including 4624, 4625, 4778 and 4779 in the security logs and clipboard events in the Windows sysmon events. Cylerian detected anomalous hostnames across each of the data sources, including hostnames starting with "WIN-", and "hosted-by-vdsina[.]com".
Password Bruteforcing attempts	CREDENTIAL ACCESS	Cylerian detected password bruteforcing across multiple hosts from a machine in the VPN IP address space.
POORTRY + STONESTOP (Malware)	DEFENSE EVASION	Look for unusual service installations, especially of kernel drivers, in windows logs. In this particular case, Cylerian identified a service name containing 5 random characters and the driver signed by "Changsha Hengxiang Information Technology Co., Ltd.".
Disabling of Windows Defender	DEFENSE EVASION	Cylerian detected the disabling of Windows defender by monitoring for Event ID 5001 in the Microsoft-Windows-Windows Defender logs.
Rclone	EXFILTRATION	Analyze process executions and file creation events. The rclone configuration file consisting of FTP credentials was created as rclone.conf in the `c:\users\<username>\pictures` folder.
Large file transfers	EXFILTRATION	Cylerian detected large outbound traffic flow based on firewall logs. In this particular case, Cylerian identified a large transfer to the ASN: AS44812 (IPServer.su), a provider of dedicated and virtual servers hosted in Russia.
Filezilla	EXFILTRATION	Analyze process executions and file creation events. Cylerian detected a file named "recentservers.xml" in the `c:\users\<username>\appdata\roaming\filezilla` folder consisting of the IP address and protocol used for FTP file transfers.
Network traffic to uncommon cloud hosting providers	EXFILTRATION	Cylerian detected outbound network traffic to uncommon cloud hosting providers, including to: 194.190.152.0/24, owned by HIP Hosting, a provider in Russia and HOSTED-BY-VDSINA[.]COM
Outbound FTP traffic	EXFILTRATION	Cylerian detected outbound FTP traffic via firewall events.

About Cylerian

Cylerian is an industry leader in cybersecurity solutions, providing organizations with comprehensive visibility and control over their IT environments. With offices in Jersey City, NJ and Panama City, Panama, Cylerian enables companies of all sizes to leverage its unified, cloud-native platform to meet their security, observability and compliance needs. For more information, visit www.cylerian.com.

WEB
www.cylerian.com

SALES
sales@cylerian.com

PHONE
+1 (833) 295-7426