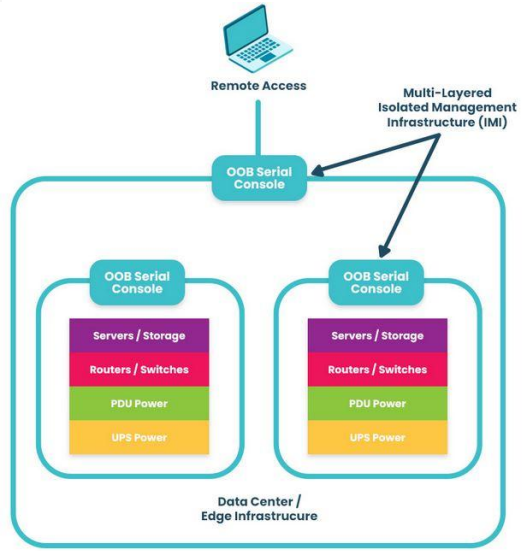
Castellum Labs



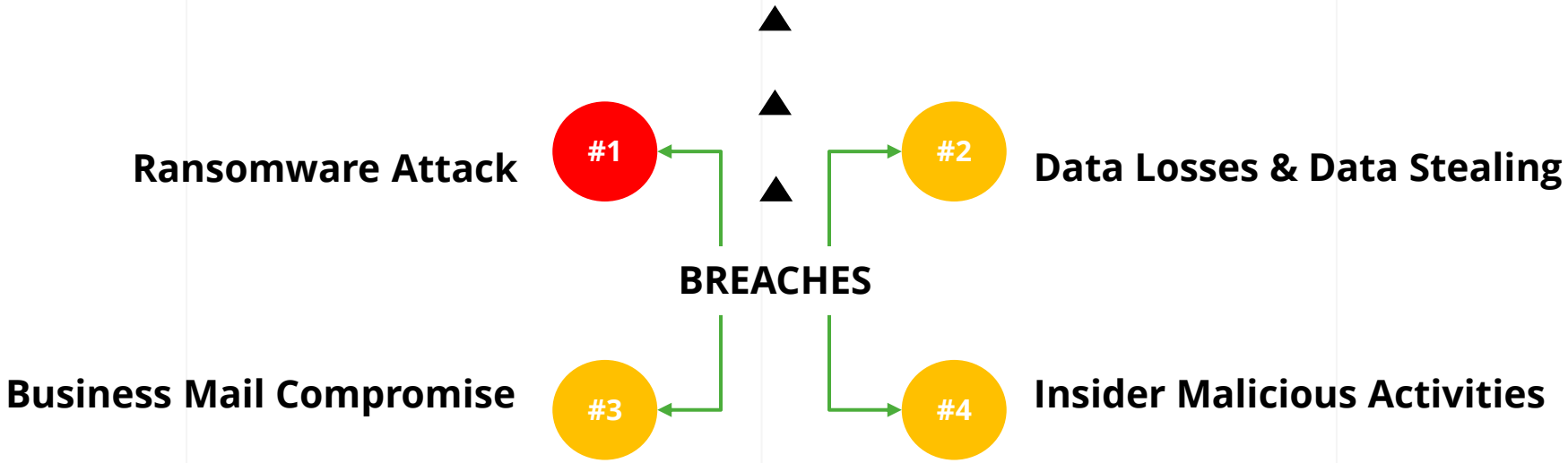
Castellum Labs

Ransomware Response & Forensic Services

www.castellumlabs.com

Responses, for Attacks & Breaches

A comprehensive capability of handling breach and attack situation, across all types & for all situations



Guiding Process for Response

Ransomware Incident Coordination

#1
Coordinate with triaging committee, assess severity of ransomware attack

#2
Gather IR team, pick people from system, network & cloud teams

#3
Scope the investigation for incident response and closure

#4
Collect IR documents and system, network and cloud data

Declared Incident

Follow Plan

Containment

Further containment actions to be decided and communicated to incident tech action coordinator

Biz Escalation

Communicate to biz along with incident summary page for potential PR and legal actions

Reporting

Collect evidences, decide about forensic needs and prepare incident reports

Termination

Communicate closure of incident to all PJL stakeholder along with incident closure statement

Feedback

Conduct post incident meeting for sharing learning, intelligence and corrections

MITRE Mapped Tracing Model, Ransomware

A sample of Lockbit Compromise Scenario's MITRE Mapping

Parallel Stages of Ransomware Response

Castellum's Three parallel approaches are adopted, for rescue, response and recovery

Stage 1
Containment Actions

- Find attack route
- Establish compromise state
- Block from further escalation

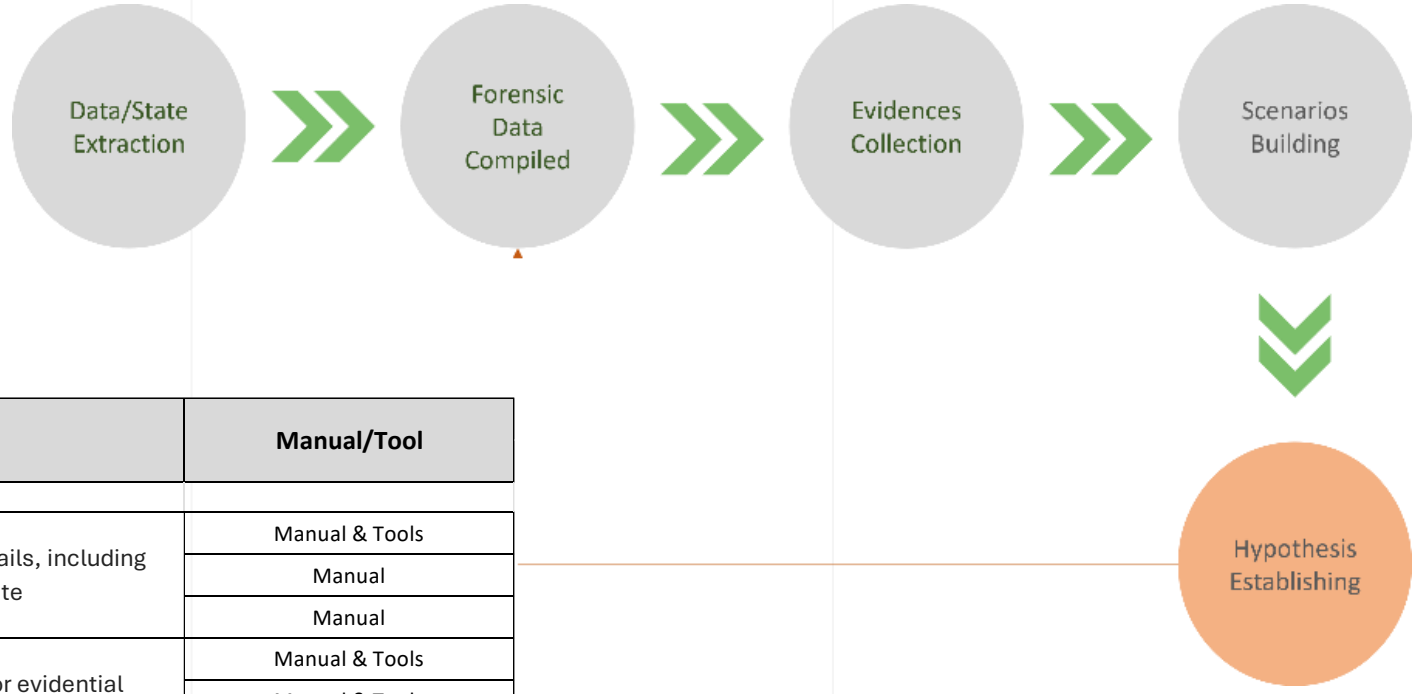
Stage 2
Forensic & Data Recovery

- Assess damage
- Recovery attempt for data
- Root cause analysis & conclusion

Stage 3
Cleanup & Ops Resumption

- Search and clean up
- Isolation completion
- Secure configurations

Forensic Methodology Sample



Investigation/Recovery Stages	Objective	Manual/Tool
Server Footprinting	Inventory of all server's details, including accesses & state	Manual & Tools
Network Footprinting		Manual
		Manual
Network Logs Forensic	Checking network logs for evidential correlation with server's events	Manual & Tools
Network Isolation Checks		Manual & Tools
		Manual
Affected Elements Scoping	Checking for all files on affected servers, to assess damage	Tools
Damage Inventory Building		Tools
		Manual
System Changes Detection	Detecting attacker's persistent model on servers and inventorizing system changes made by attacker	Manual
Attackers' Foothold Detection		Manual
		Manual
File Recovery Model	Detecting file encryption model and establishing decryption key for files	Manual & Tools
Key Detection for Recovery		Manual & Tools
		Manual & Tools
Attempt to Recover Files	Using decryption key to recover files and validating recovered files	Manual & Tools
Validation of Recovered Files		Manual & Tools

Roles and Responsibilities, Ransomware

Role	Nominated Person	Role/Function
Escalation/comm lead		Works on handling escalation
Tech action coordinator		Works on first response, all initial tech actions
Incident coordination lead		Overall incident coordination leader
Reporting lead/approver		Reviews final reports of incident
Regulatory lead		Decides if to do regulatory reporting
Media and PR lead		Decides if to prepare a media strategy
Legal point of contact		Reviews legal requirements of incident

Sample Forensic Compilations

Steps to Analyze / Events to Detect, Trace and Analyze	Server - AD-VAULT
Unauthorized logins 4624 (Successful login) 4625 (Failed logins) 4648 (Explicit credential use) - Possible Pass-the-Hash attack 4672 (Special privileges at logon) - Admin logins **Service and system changes** 7036 (WinRM service state change) - Remote access enabled 6008 (Unexpected shutdown) - Potential malware crash 7034 (Service terminated unexpectedly) - Attack on critical services	**Found 4672 which is for special priviledge at logon** **Total count of 4672 events, 146,607** **1. Default App Pool, 4 logon with special privilege** **2. Administrator, 7791 logon with special privilege** **3. dd160$, 5 logon with special privilege** **3. iusr, 5 logon with special privilege** **4. jordan.page, 3862 logon with special privilege** **5. localservice,17 logon with special privilege** **6. networkservice, 5 logon with special privilege** **7. r[redacted]cial privilege** **8. s[redacted]cial privilege** **9. s[redacted]l privilege** **10. [redacted]al privilege** **11. [redacted]l privilege** **12. [redacted]om, 1 logon with special privilege - 21st Feb** **13. [redacted]om, 1 logon with special privilege - 21st Feb** **Unexpected system shutdown, 6008, four times** **(10th Feb, 11th Feb, 22nd Feb and 23rd Feb)** **Service Terminated Unexpectedly, 7034, 1 Time - 20th Feb** **System Audit Policies changed with event ID 4719, 1449**

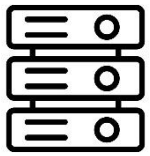
Forensic Analysis Flow (Sample)

Internal laptop
Nick's laptop

Team Viewer
Compromised

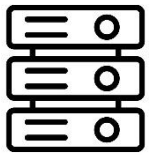
(Either a direct access or through a phishing)

RDP Access
Known Credentials



Domain Controller
Active Directory

RDP Access
Known Credentials



Critical Server Set
Three Servers

Large no of special privilege logons

System audit policy changes

New processes, "C"/"R" created (for copy/encryption)

Csrss.exe executed from unusual location

External connection made for extraction

.Play Ransomware

Play Ransomware Tools/Tech inititated

Data Copied & Encrypted
(Local on server)
(.play encryption)

Shutdowns & Server Controls

Data Extracted
(Taken to C2C)
(Taken to Darkweb)

Data Recovery Model

“Getting stolen files back and recovering them is the top priority”

#1
We found all locations where stolen files are kept

#2
We are extracting all 105 files (>500GB data)

#3
Conducting quarantine and checks on all files

#4
Will place them on a cloid storage post checks

A.
Finding Content of .rar

B.
Itemizing File Names

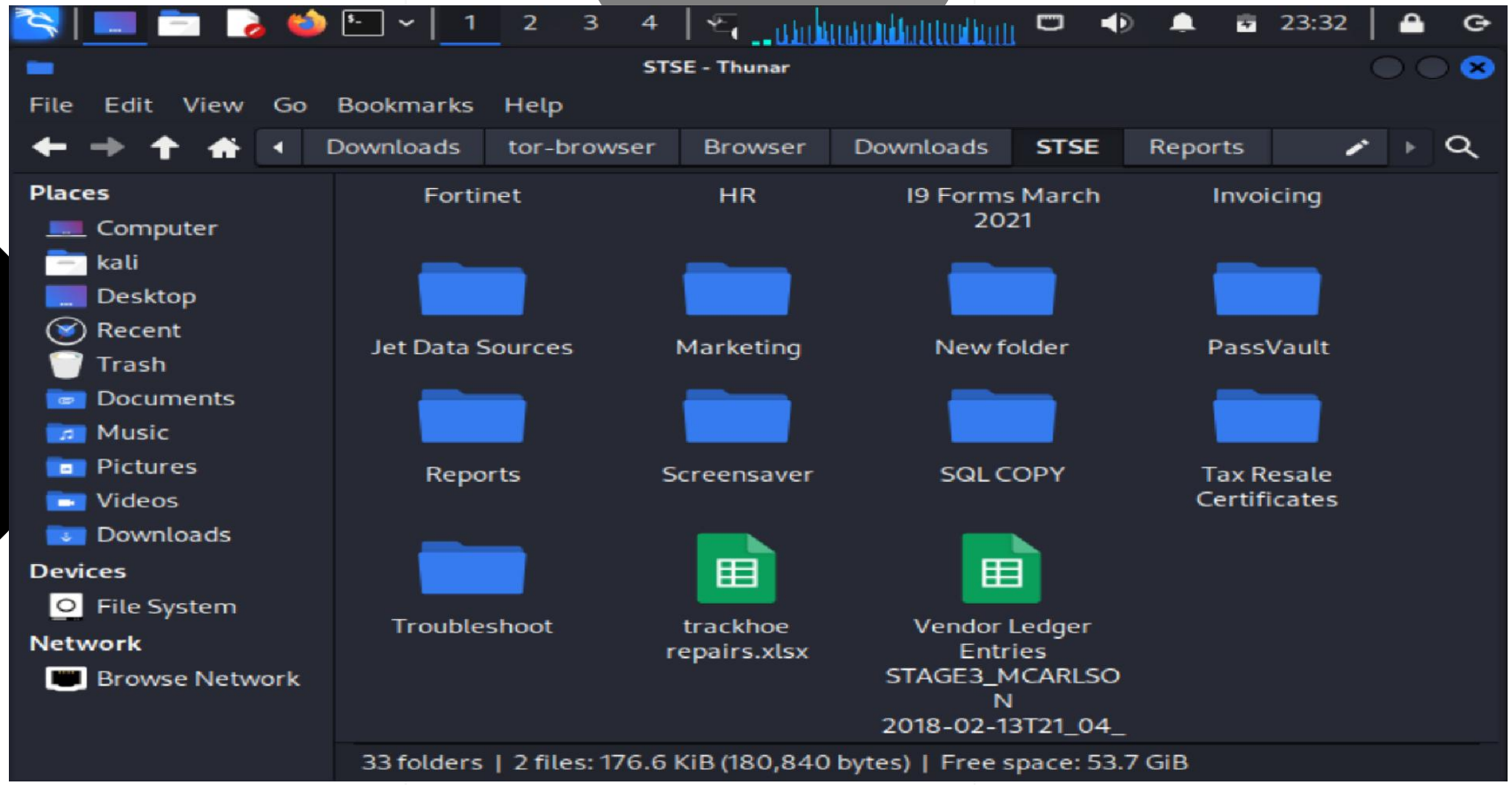
C.
Arranging .rar on Cloud

Data Recovery Model, Extractions Based

"We extract data from ransomware post sites, darkweb data dumps and other seller locations"

Data Sellers

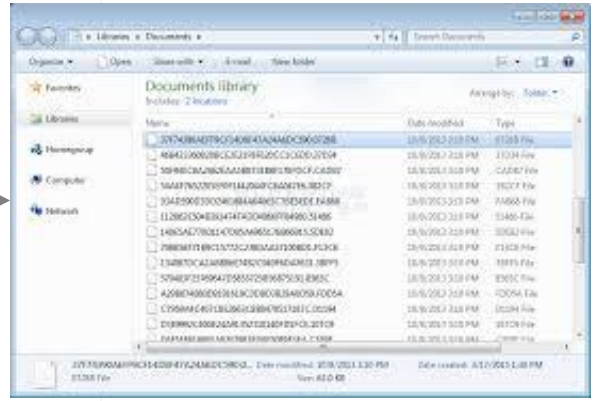
Darkweb Places



Data Recovery Model, Local Decryptions

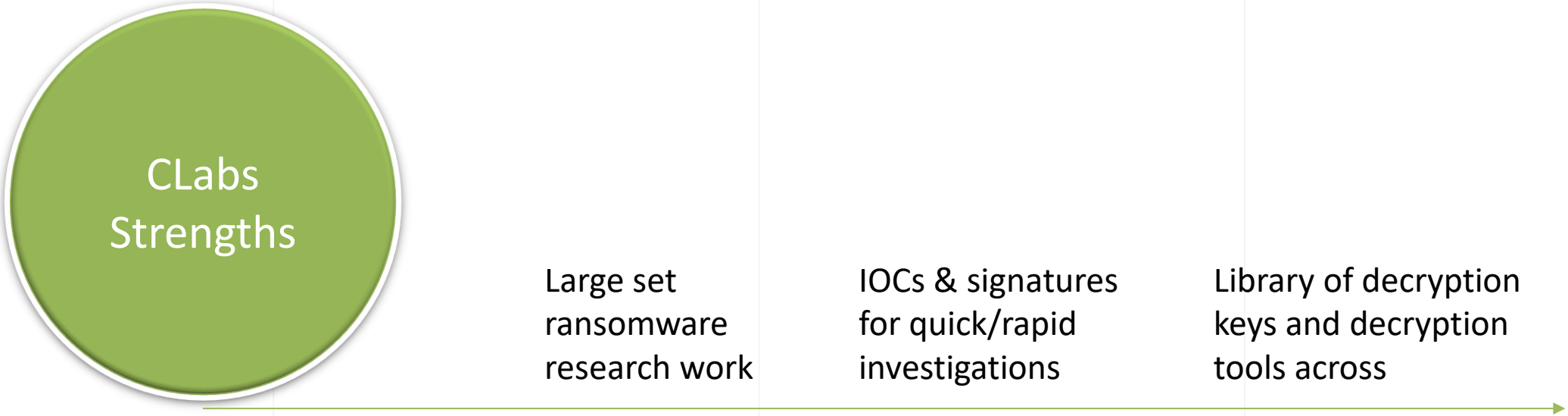
Castellum Labs Owned
Decryption Key Library

Decryption Tool Set



Key Strengths

Dozen of ransomware situations and response handled for mid to large customers across world



Additional Tool Sets Used

#	Tools/Components/Tech	Source	Comment
1	Forensic Data Extraction	Inhouse	
2	Elastic	Open Source	
3	Maltego	Open Source	
4	OCTI	Custom Stack	
5	Forensic Web Sites	Surface Web	

Custom forensic modules developed by our ransomware experts are used

Custom data extraction utilities developed by our ransomware experts/engineers

For a given situation, we also customize our scripts & utilities for response actions

Clear Visibility You Get …

Nicholas a/c in active state on servers

Does not seem like a coincidence that all privileged accesses of Nicholas on servers still exist

All four Servers carrying no hardening

It is possible that hardening or security configs were disabled knowingly with malicious intent, by someone

RDP connection to Nick's laptop from outside

Nick's laptop can be accessed through Team Viewers, so enabling RDP from outside does not make sense

Multiple privileged accounts on servers

Someone created multiple privileged accounts on server which is not a common activity by system admin

These are potential loopholes which were exploited during this attack and subsequent compromise

Comprehensive Forensic Report, A Glance

"Focus on data, exact scenario and evidence based conclusion & actions"

Summary of Play Ransomware Group

This section presents specific details of Play Ransomware attributes, IoCs and behavioral traits. A more detailed document for Play ransomware can be referred to get all compiled information about this ransomware.

- **File Extension:** .play
- **Ransom Note:** ReadMe.txt
- **Communication Method:** Email address only - marinachin@gmx.de, boitelswaniruxl@gmx.com, teilightomemaucd@gmx.com, derdiarikucisv@gmx.de, protexdamaraij5@gmx.de
- **Encryption Method:** Hybrid AES-RSA encryption
- **Attack Methodology:** Double extortion (exfiltrates data before encryption)
- **Targeted Industries:** Government, telecommunications, healthcare, and IT
- **Primary Geographical Targets:** Latin America, Europe, North America, and India
- **Official Decryption Availability:** No official decryptor available
- **Detection Names:** Avast (Win32:Malware-gen), Combo Cleaner (Trojan.GenericKD.39834878), ESET-NOD32 (A Variant Of Win32/Filecoder.OLN), Kaspersky (HEUR:Trojan-Ransom.Win32.Crypmodng.g), Microsoft (Ransom:Win32/Crypmodng!mclg)

Castellum Labs

Forensic Analysis
Detailed Report

Non-Standard Ports and AMI Executions

Log of non-standard ports were found open on the servers (all four critical servers). Though outward communication specifics could not be established because of missing (not available) firewall logs, existence of these ports presents a picture, where some may have been exploited during attack path. Following is the summary of the ports, which were found open on the critical server infrastructure.

Server	General Suspicious Ports	High Risk Open Ports
AD-Vault	50064 - Not a registered port 50063 - Not a registered port 49746 - Not a registered port 37014 - Unofficial port, used for IoT devices	445 – SMB 5939 - TeamViewer 5985 - WMI 80 and 8000 - Web
AD-Self-Service	50064 - Not a registered port 50063 - Not a registered port 49746 - Not a registered port 37014 - Unofficial port, used for IoT devices	3389 - RDP 445 – SMB 5939 – TeamViewer 5985 – Win Remote Mgmt 80 and 8000 - Web
	52657	49798 (Backdoor)

Comprehensive Forensic Report, A Glance

"Process level visibility is created, in ransomware attack flow & state"

Unexpected Shutdowns on Server

Many shutdowns were initiated on the servers, by placing a shutdown script in the scheduled runs. Following is the summary of the unexpected shutdowns which took place, during the course of attack, compromise and exfiltration phase.

Server	Count of Shutdowns	Date/Times
AD-Vault	Four Times	10th Feb, 11th Feb, 22nd Feb and 23rd Feb
AD-Self-Service	One Time	26th Feb
DC01	Nine Times	9th Feb, 16th Feb and 22nd Feb
AC01	Four Times	10th Feb, 11th Feb, 22nd Feb and 23rd Feb

Existence of Active User Accounts of Recently Exited Employees

A specific user's account was found on all four critical server class assets, who had left the organization one and half months before this attack took place. This account is in active assets and has not been deactivated at any time. This account has also lots of privileged logon activity on four servers, which have been forensically analyzed.

nicholas.kelehan

Process/File	Time of Execution	Server/Comment
Newfield.ps	2/21/2025 4:00:01 PM	DC01 (Power Shell command execution)
csrss.exe	2/24/2025 6:27:00 AM	DC01 (Run from unusual place, /usr/public/music)
dsregcmd.exe	Not known	DC01
calluxxprovider.vbs	Not known	AC01
cscript.exe	Not known	AC01
sc.exe	Not known	AC01

Castellum Labs

Forensic Analysis
Detailed Report

Unexpected Shutdowns on Server

Many shutdowns were initiated on the servers, by placing a shutdown script in the scheduled runs. Following is the summary of the unexpected shutdowns which took place, during the course of attack, compromise and exfiltration phase.

Type of Ransomware Handled

IOC's Akira Ransomware Group			
SHA-256 Hash	**Detection name**	**Description**	**Filename**
08207409e1d789aea68419b04354184490ce46339be071c6c185c75ab9d08cba	Ransomware:Win/Akira.A		AD32.exe
2727c73f3069457e9ad2197b3cda25aec864a2ab8da3c2790264d06e13d45c3d	Ransom:Win64/Akira.0e213770		N/A
2db4a15475f382e34875b37d7b27c3935c7567622141bc203fde7fe602bc8643	Ransom:Win64/Akira.ebd8110c		b6162bebd1
56f1014eb2d145c957f9bc0843f4e506735d7821e16355bcfbb6150b1b5f39db	Ransom:Win64/Akira.5c441871		w.exe
58e9cd249d947f829a6021cf6ab16c2ca8e83317dbe07a294e2035bb904d0cf3	Ransom:Win64/Akira.beea5f7e		w.exe
6270cef0c8cc45905556c40c9273391d71ef8d73c865d44d2254a8a4943ae5b4	Trojan[Ransom]/Win64.Akira		w.exe
7fe1619aa07d2ab169a2fa23feb22d7433bf07e856cda1402cf60205beddd7f	N/A		N/A
78642603005f826a3b47effb852da980a6483ffb9461e30842020848305c9353	Ransom:Win64/Akira.cfbdd435		N/A
7d5da695e6f9a421e3d3a94e384ce00e8ec58fac5b895b4cba5b66a6de7fafd5	Ransomware:Win/Akira.A		hessen.exe
99c1cd740fa749a163ce8cdf93722191c4ba5d97de81576623a8bbcb622473d6	HEUR:Trojan-Ransom.Win64.Akira.b		w.exe
b7bbfb66338a3413f981561115bd8ef8a4014479bcc320de563499cfc73a3de2	Trojan/Win.Generic.R631399		win.exe
c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddccd5bb37857e7bde6d2eb7	Ransom:Win64/Akira.8a1040d7		vrsaki.exe
ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d	Win64.Trojan-Ransom.Akira.B		win.exe
d5558ec7979a96fe1ddcb1f33053a1ac3416a9b65d4f27b5cc9fd0a816296184	Trojan/Win.Generic.R631399		win.exe
e5c8888f51369c2105d47a4998ad9b4053471bd98b4fd73a854207da09206ee2	Ransom:Win64/Akira.ed1b3865		akira.exe

Play Conti Funksec Cl0p **Akira** RansomHub Qilin Dragonforce INC Ransom Medusa Babuk LockBit 5.0 Rova +

- Large range of ransomware handling has been done by Castellum Labs in recent years
- We keep a track of the ransomware related developments across the internet
- A carefully built response model, using deep research model

Keep in Touch.

+91 8639953505 enquiry@castellumlabs.com www.castellumlabs.com

Too find details about Castellum Labs, see next few slides ....

About Castellum

- Services delivered by Global Cyber Capability Center using advance Platforms
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong Handpicked Team of 50+ with (best of security talent globally)
- Started by people with decades of product, services & deep tech experience
- Subscription & annual contract modeled services delivered globally
- Value + Impact from Day One, No Installation & No Deployment

Leadership Team

Rama

Advisor and Head – US Ops
(US based)

Senior business leader with 30 years of experience in US & India, across entire spectrum of IT industry in services & product companies

Head IT – Aryaka, Ex-PwC, Ex-IBM, Ex-VMWare, Ex-Malwarebytes, Ex-Infosys and Ex-NetApp

Rajeev Shukla

Founder & CEO
(India based)

Senior business leader with dozens of stints with MNCs for building data center, networking & cyber security businesses (product & services)

Ex-Vice President CA Technologies, Director and Product Line Manager – Sun Microsystems, Ex-Vice President – Quark, Ex-CTO – Cygilant, Ex- Chief Strategy Officer – GSS, Ex-CTO and Chief Product Officer - Sequretek

Rinky (Sukriti)

Head of Strategic Sales
(India based)

Seasoned operational leadership from NGO sector, with experience across Sales, HR, Operations and Legal

Started corporate journey with Castellum and handled variety of roles, HR, Pre-Sales & Sales

Some of Our Enterprise Customers

Across Sectors_> Banking / Insurance / Manufacturing / Pharma / Biotech / SaaS / IT-Services / e-Commerce/ Retail / Government / NGOs / FMCG /

Across Cities & Countries_> Mumbai / Bengaluru / Hyderabad / Delhi / Indore / Chennai / Kolkata / Bhopal / Pune /

Some More of Our Enterprise Customers

excelra

SYMBIOTEC
PHARMALAB (P) LIMITED

وزارة الصحـــة العامـــة
Ministry of Public Health
State of Qatar • دولـــة قطـــر

metro
BRANDS

DECATHLON

GOCL

PRISM JOHNSON LIMITED

ICRISAT
INTERNATIONAL CROPS RESEARCH
INSTITUTE FOR THE SEMI-ARID TROPICS

What Our Customers Say

Sathya Paul

CIO – ViaPlus

Dear Rajeev,

Thanks for Castellum Labs' work on our flagship product ChefDesk. Given that it is a billing product, security was always a key consideration and a must requirement for us. Castellum's work on ChefDesk has ensured we are on good footing on the security front.

I look forward to continuing our relationship with Castellum Labs to help us stay secure for all of our software products/platforms.

I will feel pleasure in recommending you and Castellum Labs to anyone in industry.

Thank you.

Regards,
Srinivas Guthula (CEO)
Zaravya Informatics Pvt Ltd

Sanjay Jha

CTO – Lets Venture

Dear Rajeev,

Being a global enterprise SaaS provider, security is at forefront of our thought process.

Castellum Labs' application security services on TrusTrace SaaS platform has helped us to get confidence on our security implementation when we launched the product.

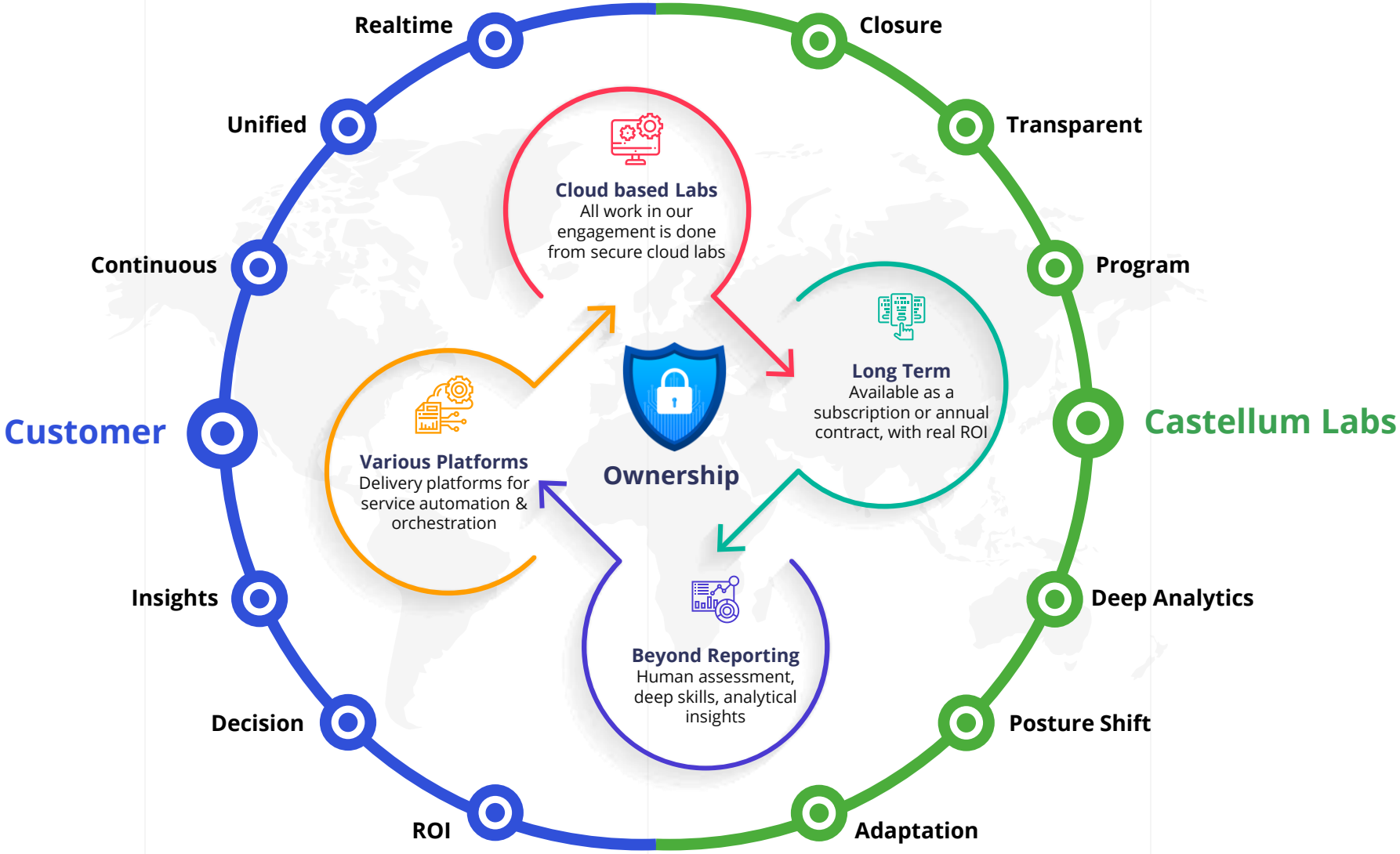
Professionalism, technology savviness and deep knowledge of your team are commendable.

Regards,
Madhav
trustrace

Srini Guthula

CEO – ChefDesk

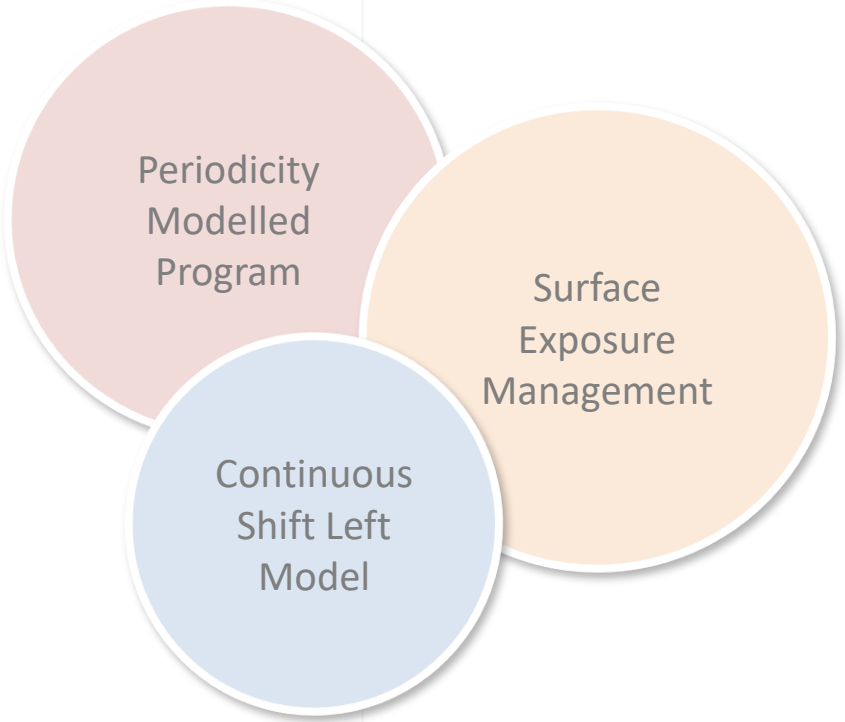
Enterprise Security, Not Transactional Projects



Cyber Transformation Services

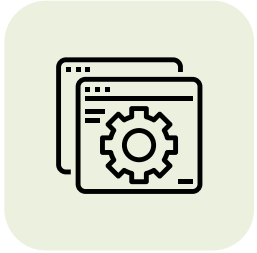
VAPT/VACA Programs

Red Team <> Blue Team Modeled
Annual Program for Vuln Management



Threat Intel & Hunt

Counter Intelligence Powered
Quarterly or Monthly Hunt/Runs



DevSecOps

AppSec Programs & DevSecOps
Transformational Project for Shift Left

Privacy Engineering

Adoption, Engineering & Compliance
Transformation Project for Continuous Privacy

Security Services (Projects) Portfolio

Cloud Workload & DC Hardening

Infrastructure Security

Simulations for Defense Capability

Breach & Attack Simulation

Implementations & Optimizations

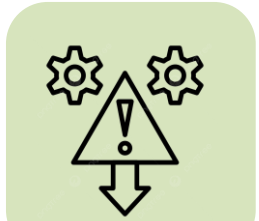
SOC / SIEM Adoption

PCI DSS and SOC 2 Type 1 and 2

Cyber Certifications

Employee Awareness

Phishing and Emp Awareness

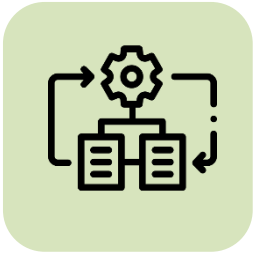


Incident Response

Runbooks, Process & Breach Handling

Security Assessments

Gap, Audit and Maturity



Automations & Insight

Security Data Lake & SecOps