The Nineteenth International Conference on Emerging Security Information, Systems and Technologies
SECURWARE 2025

PROF. DR. ALEXANDER LAWALL

Reconnaissance to Resilience:

A Threat-Led Kill Chain Perspective on Ransomware and Emerging AI-Driven Threats

Keynote
Barcelona, October 2025

PROF. DR. ALEXANDER LAWALL

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Academic Roles

- Program Director, B.Sc. & M.Sc. Cyber Security and Cyber Security Management
- Professor in Cyber Security (Distance & On-site Learning)

Expertise

- System & Network Security
- Web Application & Cloud Security
- IoT and Industrial IT Security

Professional Affiliations

- Leadership Committee, "Management of Information Security" (Society for Informatics, GI)
- Professional Lead, "Security & GRC in IT" (Summit Leipzig)
- Member, Association of Cyber Forensics and Threat Investigators (ACFTI)
- Member, Zentrum Digitalisierung Bayern (ZD.B)
- Conference Committees Board Chair (IARIA)
- Steering Committee of the Conference SECURWARE & IoT-AI (IARIA)

Research & Publications

- Focus Areas: Cyber Security, Information Security, Industry 4.0/5.0, IoT, Rights Management, AI in Cyber Security
- Publications in national/international Journals and Conferences
- Keynote Speaker, Program Chair, Panel Expert of International Conferences

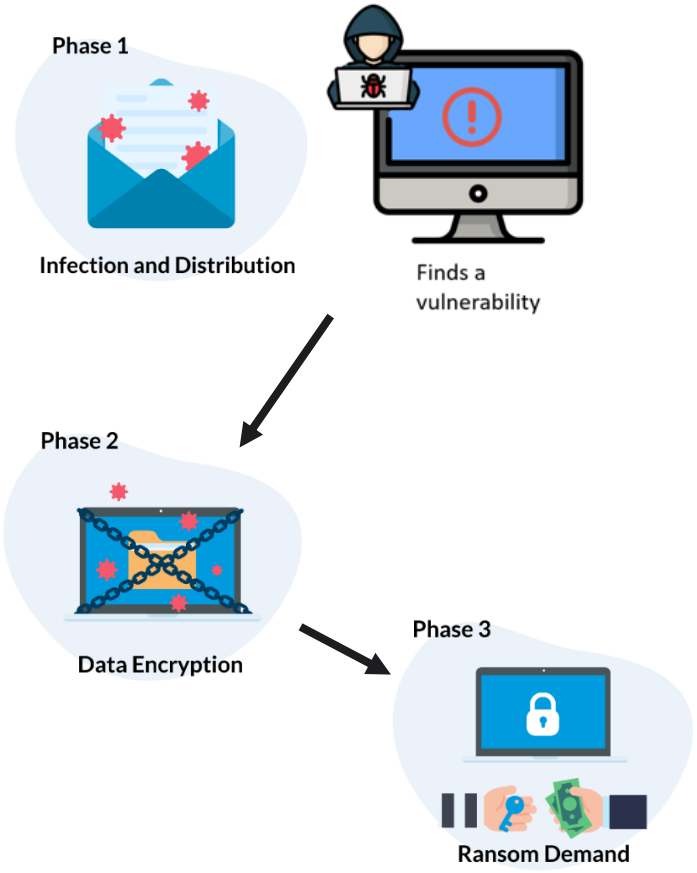
AGENDA

Introduction and Motivation	1
Threat-Led Kill Chain Perspective on Ransomware	2
New Trends in Ransomware	3
AI for Cyber Defense	4
Conclusion and Future Work	5

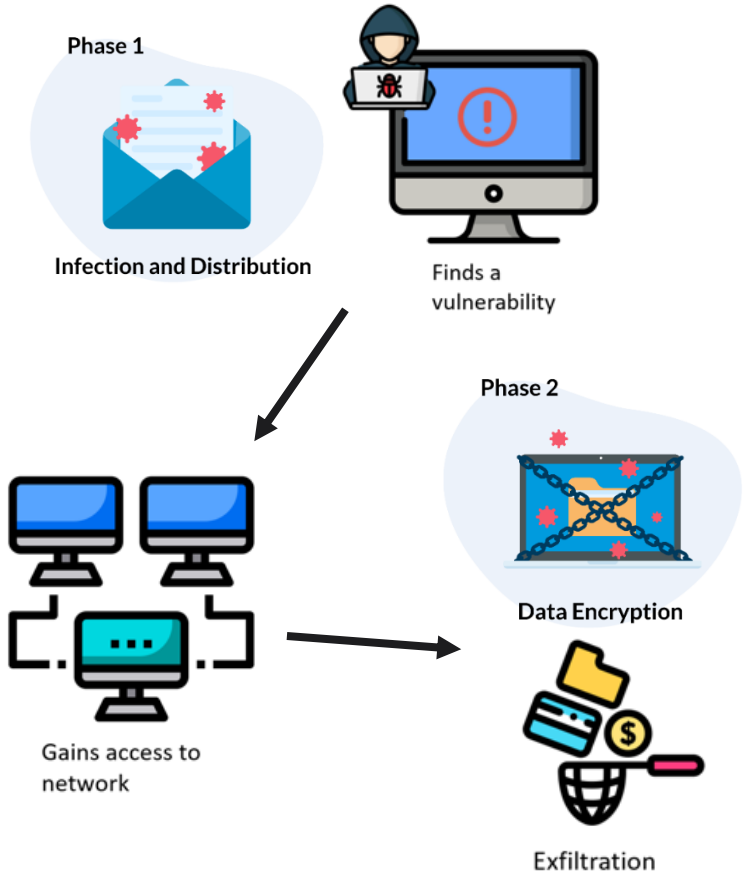
INTRODUCTION

Ransomware Variants

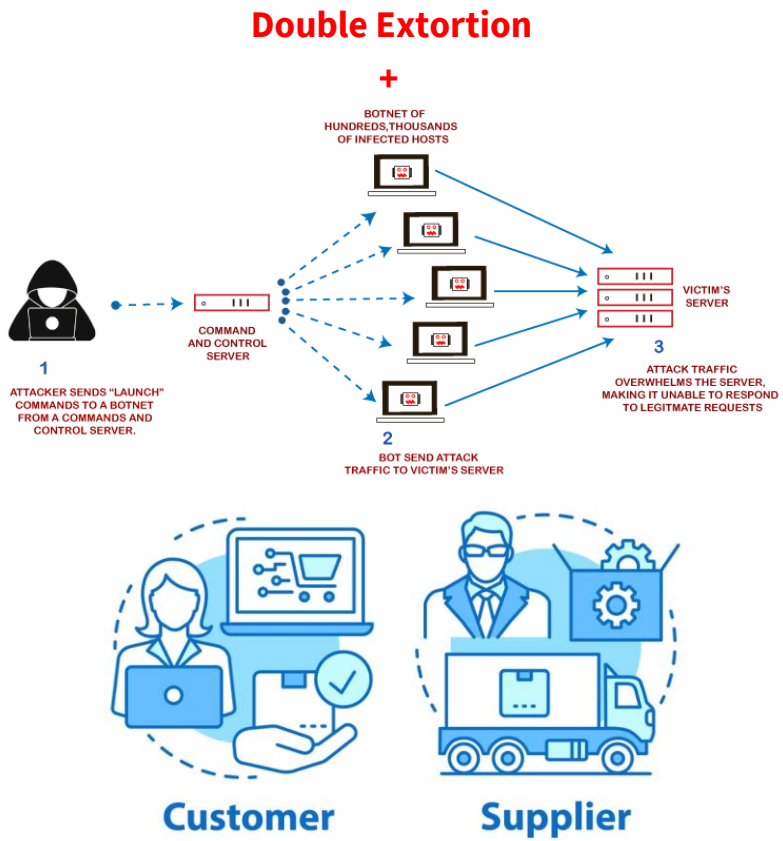
Single Extortion



Double Extortion



Triple Extortion



Quellen: https://www.xorlab.com/en/blog/how-to-protect-businesses-against-ransomware-attacks & https://blogs.manageengine.com/active-directory/log360/2021/03/10/ransomware-in-2021-what-has-changed-detection-and-mitigation-strategy.html & https://dribbble.com/shots/7605020-Start-your-dropshipping-business

MOTIVATION

Ransomware Report Findings (Urgency)

Organizations experienced at least one **ransomware** attack in the **last two years**

57%

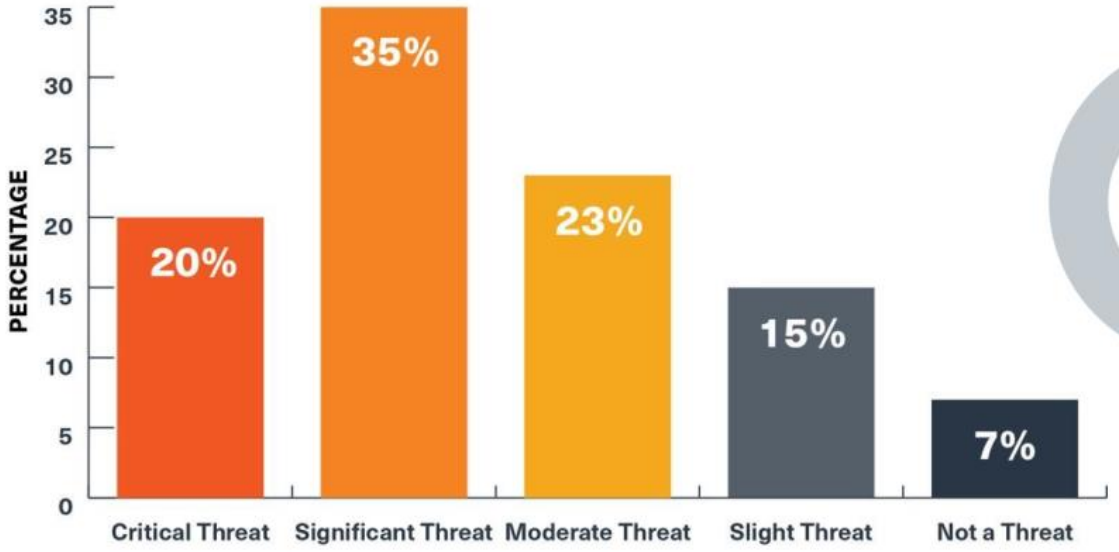
Those attacked were hit with **double or triple extortion**

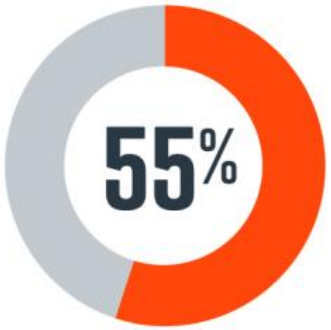
42%

Quelle: https://bullwall.com/ransomware-resilience-benchmark-report-2026/

MOTIVATION

Ransomware Report Findings (Criticality)





A majority see ransomware as a critical or significant threat to their business.

Quelle: https://bullwall.com/ransomware-resilience-benchmark-report-2026/

THREAT-LED KILL CHAIN PERSPECTIVE ON RANSOMWARE

Part 1/2 (2023)

RQ1: *What are the* ***dominating ransomware groups*** *identified by their* ***victim count****?*

RQ2: *What are the* ***Tactics, Techniques, and Procedures*** *employed by ransomware groups, and how are these* ***quantified*** *to understand their* ***prevalence*** *and variation?*

RQ3: *What are the related* ***mitigations*** *that can effectively reduce the risk of successful ransomware attacks based on the identified and quantified Tactics, Techniques and Procedures, and what is their* ***prioritization****?*

METHODOLOGY

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

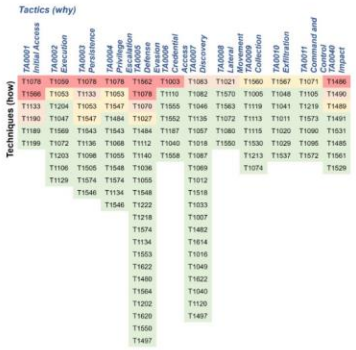
1 Identification of **Ransomware Groups**

Victim Count

Ransomware Group	Victim Count	Ransomware Group	Victim Count
LockBit	1832	Snatch	80
ALPHV	424	Cuba	70
CL0P	253	Sprite Spider	52
BlackBasta	244	RansomHouse	47
Hive	218	Frozen Spider	41
Royal	179	Stormous	29
BianLian	152	MedusaLocker	23
Everest	137	Qilin	19
Play	126	Monti	18
Ragnar Locker	97	Mallox	16
BlackByte	94	Daixin Team	9
Karakurt	87	Omega Lock	4

2 Threat Actor Profiles based on **TTPs**

OSINT, DLS, Dark/Deep Web



3 Prioritization of **Mitigations**

High Priority	M1026: Privileged Account Management M1018: User Account Management M1017: User Training				
Medium Priority	M1040: Behavior Prevention on Endpoint M1030: Network Segmentation M1028: Operation System Configuration M1049: Antimalware	M1027: Password Policies M1042: Disable or Remove Feature or Program M1053: Data Backup M1038: Execution Prevention			
Low Priority	M1031 M1015 M1022 M1024	M1032 M1035 M1021 M1054	M1036 M1013 M1047 M1025	M1043 M1051 M1045 M1050	M1048 M1016 M1041
Minor Priority	M1037 M1057 M1029 M1056	M1052 M1020 M1019 M1044			

Quelle: Alexander Lawall and Petra Beenken (2024). A Threat-Led Approach to Mitigating Ransomware Attacks: Insights from a Comprehensive Analysis of the Ransomware Ecosystem.
In Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (EICC '24). Association for Computing Machinery, New York, NY, USA, 210–216. https://doi.org/10.1145/3655693.3661321

RESULTS AND ANALYSIS

Ransomware Groups ranked by their victim count

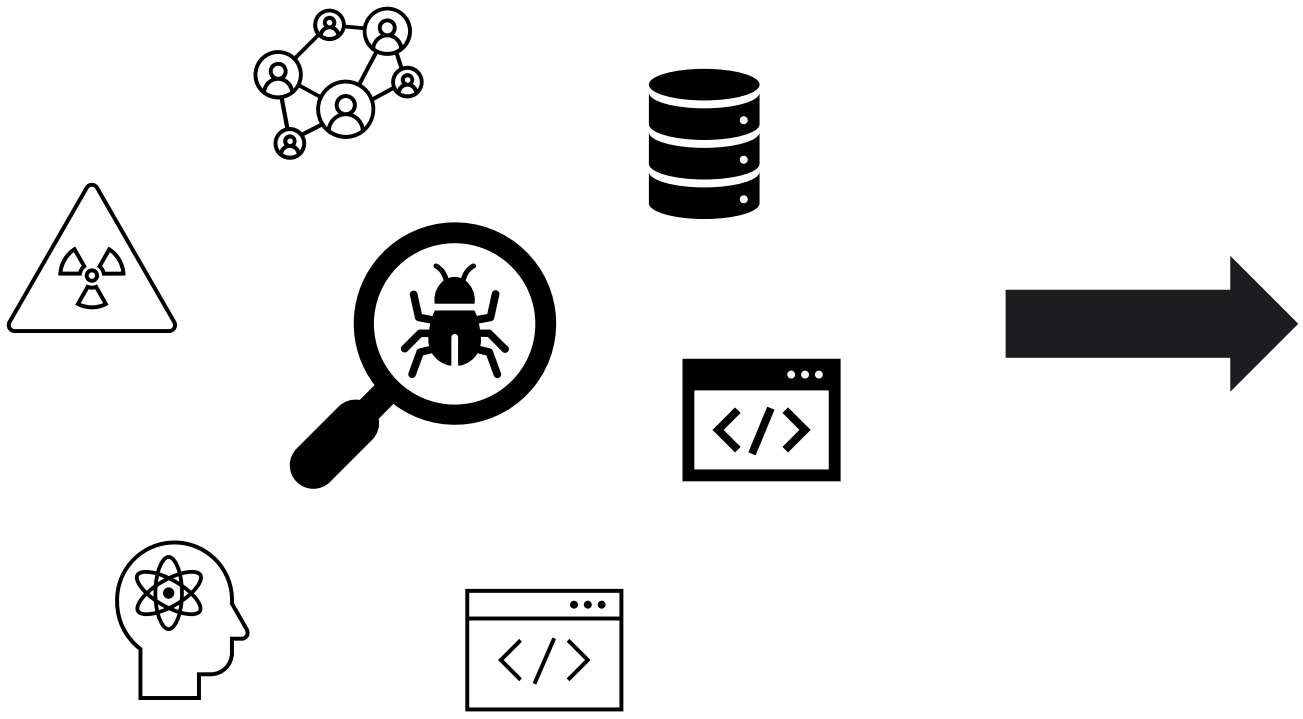


Table 1: Ransomware Groups ranked by Victim Count

Ransomware Group	Victim Count
LockBit	1832
ALPHV	424
CL0P	253
BlackBasta	244
Hive	218
Royal	179
BianLian	152
Everest	137
Play	126
Ragnar Locker	97
BlackByte	94
Karakurt	87
Snatch	80
Cuba	70
Sprite Spider	52
RansomHouse	47
Frozen Spider	41
Stormous	29
MedusaLocker	23
Qilin	19
Monti	18
Mallox	16
Daixin Team	9
Omega Lock	4

Quelle: Alexander Lawall and Petra Beenken (2024). A Threat-Led Approach to Mitigating Ransomware Attacks: Insights from a Comprehensive Analysis of the Ransomware Ecosystem.
In Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (EICC '24). Association for Computing Machinery, New York, NY, USA, 210–216. https://doi.org/10.1145/3655693.3661321

RESULTS AND ANALYSIS

Tactics, Techniques, and Procedures (quantified)

Table 1: Ransomware Groups ranked by Victim Count

Ransomware Group	Victim Count
LockBit	1832
ALPHV	424
CL0P	253
BlackBasta	244
Hive	218
Royal	179
BianLian	152
Everest	137
Play	126
Ragnar Locker	97
BlackByte	94
Karakurt	87
Snatch	80
Cuba	70
Sprite Spider	52
RansomHouse	47
Frozen Spider	41
Stormous	29
MedusaLocker	23
Qilin	19
Monti	18
Mallox	16
Daixin Team	9
Omega Lock	4

Collection of Techniques and Scores

- Information gathering for individual Ransomware Groups TTPs

Aggregation into Master Layer

- Consolidation of individual layers to master layer with all TTPs (**frequency** of TTPs -> Score)

Identification of Mitigations

- Identification of mitigations for each TTP

Summation of Technique Scores

- For each mitigation: sum all scores of related TTPs

RESULTS AND ANALYSIS

Tactics, Techniques, and Procedures (quantified)

Table 1: Ransomware Groups ranked by Victim Count

Ransomware Group	Victim Count
LockBit	1832
ALPHV	424
CL0P	253
BlackBasta	244
Hive	218
Royal	179
BianLian	152
Everest	137
Play	126
Ragnar Locker	97
BlackByte	94
Karakurt	87
Snatch	80
Cuba	70
Sprite Spider	52
RansomHouse	47
Frozen Spider	41
Stormous	29
MedusaLocker	23
Qilin	19
Monti	18
Mallox	16
Daixin Team	9
Omega Lock	4

Tactics (why)

Techniques (how)	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact
	T1078	T1059	T1078	T1078	T1562	T1003	T1083	T1021	T1560	T1567	T1071	T1486
	T1566	T1053	T1133	T1053	T1078	T1110	T1082	T1570	T1005	T1048	T1105	T1490
	T1133	T1204	T1053	T1547	T1070	T1555	T1046	T1563	T1119	T1041	T1219	T1489
	T1190	T1047	T1547	T1484	T1027	T1552	T1135	T1072	T1113	T1011	T1573	T1491
	T1189	T1569	T1543	T1543	T1484	T1187	T1057	T1080	T1115	T1020	T1090	T1531
	T1199	T1072	T1136	T1068	T1112	T1040	T1018	T1550	T1530	T1029	T1095	T1485
		T1203	T1098	T1055	T1140	T1558	T1087		T1213	T1537	T1572	T1561
		T1106	T1505	T1548	T1036		T1069		T1074			T1529
		T1129	T1574	T1574	T1055		T1012					
			T1546	T1134	T1548		T1518					
				T1546	T1222		T1033					
					T1218		T1007					
					T1574		T1482					
					T1134		T1614					
					T1553		T1016					
					T1622		T1049					
					T1480		T1622					
					T1564		T1040					
					T1202		T1120					
					T1620		T1497					
					T1550							
					T1497							

RESULTS AND ANALYSIS

Tactics, Techniques, and Procedures (quantified)

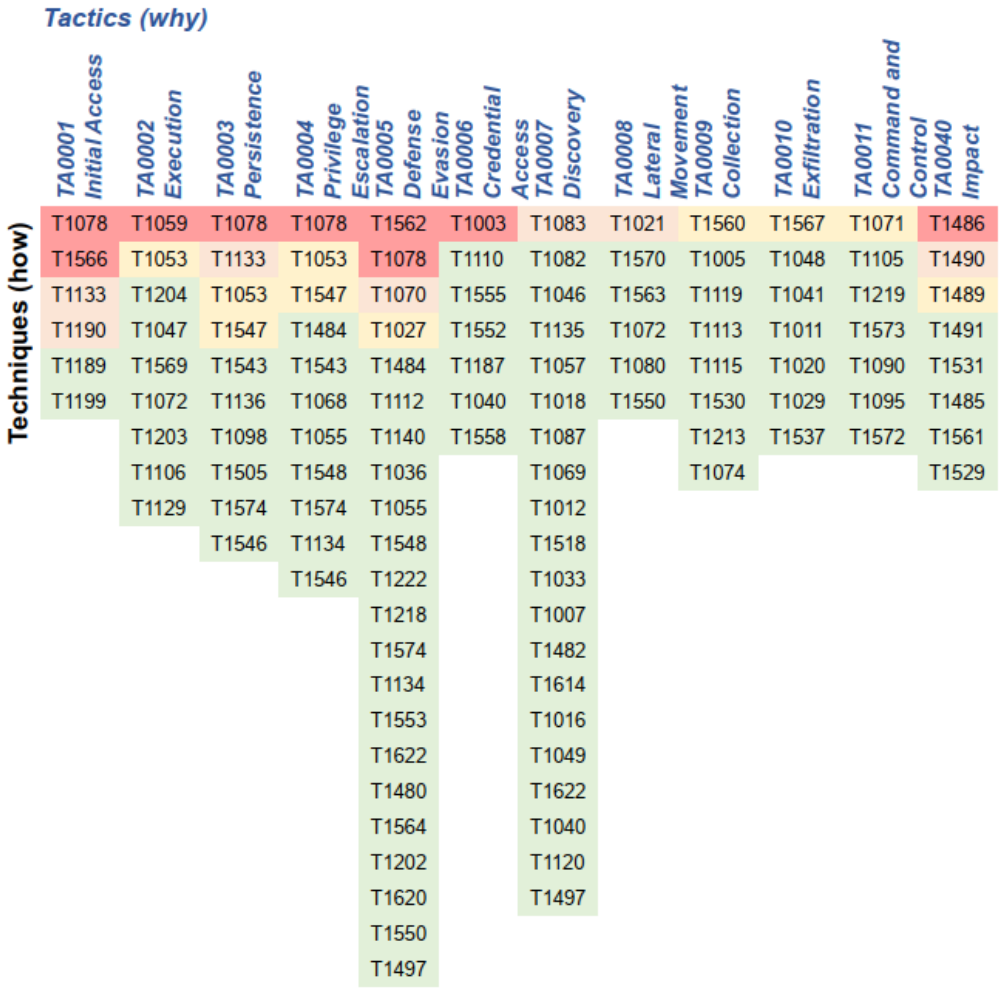


Table 2: Most Common Techniques/Sub-Techniques of Ransomware Groups

Techniques/Sub-Technique	Score	Percentage
T1486: Data Encrypted for Impact	23	96%
T1078: Valid Accounts	20	83%
T1490: Inhibit System Recovery	15	63%
T1133: External Remote Services	15	63%
T1083: File and Directory Discovery	14	58%
T1562.001: Disable or Modify Tools	14	58%
T1059.001: PowerShell	13	54%
T1190: Exploit Public-Facing Application	13	54%
T1489: Service Stop	12	50%
T1566: Phishing	12	50%

RESULTS AND ANALYSIS

Related Mitigations for Tactics, Techniques, and Procedures

Table 2: Most Common Techniques/Sub-Techniques of Ransomware Groups

Techniques/Sub-Technique	Score	Percentage
T1486: Data Encrypted for Impact	23	96%
T1078: Valid Accounts	20	83%
T1490: Inhibit System Recovery	15	63%
T1133: External Remote Services	15	63%
T1083: File and Directory Discovery	14	58%
T1562.001: Disable or Modify Tools	14	58%
T1059.001: PowerShell	13	54%
T1190: Exploit Public-Facing Application	13	54%
T1489: Service Stop	12	50%
T1566: Phishing	12	50%

Collection of Techniques and Scores

- Information gathering for individual Ransomware Groups TTPs

Aggregation into Master Layer

- Consolidation of individual layers to master layer with all TTPs (frequency of TTPs -> Score)

Identification of Mitigations

- Identification of mitigations for each TTP

Summation of Technique Scores

- For each mitigation: sum all scores of related TTPs

RESULTS AND ANALYSIS

Related Mitigations for Tactics, Techniques, and Procedures

Table 2: Most Common Techniques/Sub-Techniques of Ransomware Groups

Techniques/Sub-Technique	Score	Percentage
T1486: Data Encrypted for Impact	23	96%
T1078: Valid Accounts	20	83%
T1490: Inhibit System Recovery	15	63%
T1133: External Remote Services	15	63%
T1083: File and Directory Discovery	14	58%
T1562.001: Disable or Modify Tools	14	58%
T1059.001: PowerShell	13	54%
T1190: Exploit Public-Facing Application	13	54%
T1489: Service Stop	12	50%
T1566: Phishing	12	50%

Table 3: Mitigations to most Common Ransomware Techniques/Sub-Techniques

Mitigation	Score
M1026: Privileged Account Management	75
M1018: User Account Management	71
M1017: User Training	61
M1040: Behavior Prevention on Endpoint	51
M1030: Network Segmentation	50
M1028: Operating System Configuration	44
M1049: Antivirus/Antimalware	44
M1027: Password Policies	39
M1042: Disable or Remove Feature or Program	38
M1053: Data Backup	38
M1038: Execution Prevention	37

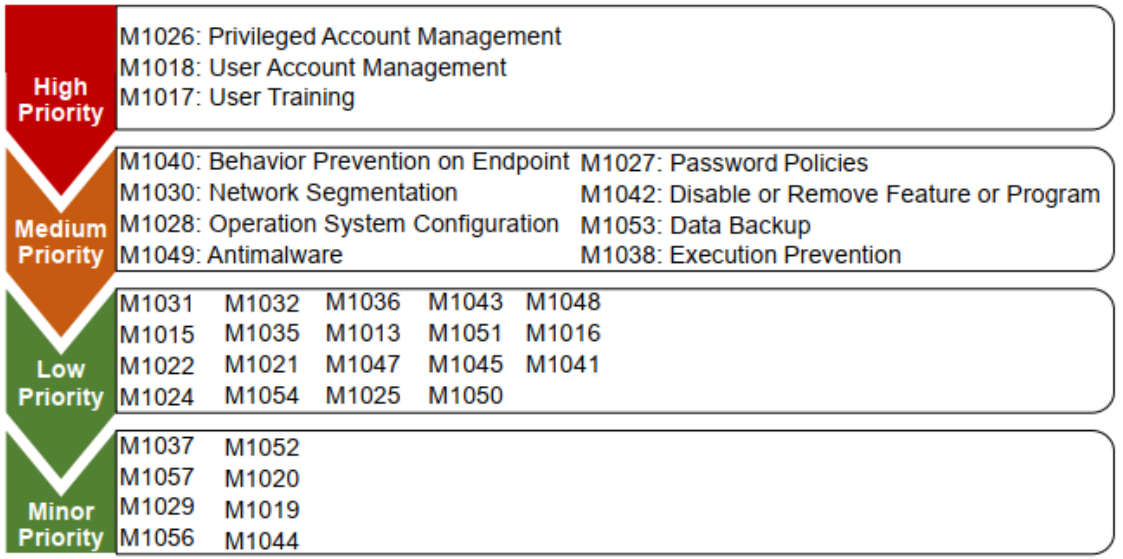
Quelle: Alexander Lawall and Petra Beenken (2024). A Threat-Led Approach to Mitigating Ransomware Attacks: Insights from a Comprehensive Analysis of the Ransomware Ecosystem.
In Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (EICC '24). Association for Computing Machinery, New York, NY, USA, 210–216. https://doi.org/10.1145/3655693.3661321

RESULTS AND ANALYSIS

Prioritization of Mitigations

Table 3: Mitigations to most Common Ransomware Techniques/Sub-Techniques

Mitigation	Score
M1026: Privileged Account Management	75
M1018: User Account Management	71
M1017: User Training	61
M1040: Behavior Prevention on Endpoint	51
M1030: Network Segmentation	50
M1028: Operating System Configuration	44
M1049: Antivirus/Antimalware	44
M1027: Password Policies	39
M1042: Disable or Remove Feature or Program	38
M1053: Data Backup	38
M1038: Execution Prevention	37



Quelle: Alexander Lawall and Petra Beenken (2024). A Threat-Led Approach to Mitigating Ransomware Attacks: Insights from a Comprehensive Analysis of the Ransomware Ecosystem. In Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (EICC '24). Association for Computing Machinery, New York, NY, USA, 210–216. https://doi.org/10.1145/3655693.3661321

CONCLUSION (PART 1: 2023)

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Table 1: Ransomware Groups ranked by Victim Count

Ransomware Group	Victim Count
LockBit	1832
ALPHV	424
CL0P	253
BlackBasta	244
Hive	218
Royal	179
BianLian	152
Everest	137
Play	126
Ragnar Locker	97
BlackByte	94
Karakurt	87
Snatch	80
Cuba	70
Sprite Spider	52
RansomHouse	47
Frozen Spider	41
Stormous	29
MedusaLocker	23
Qilin	19
Monti	18
Mallox	16
Daixin Team	9
Omega Lock	4

Tactics (why)

Techniques (how)

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact
T1078	T1059	T1078	T1078	T1562	T1003	T1083	T1021	T1560	T1567	T1071	T1486
T1566	T1053	T1133	T1053	T1078	T1110	T1082	T1570	T1005	T1048	T1105	T1490
T1133	T1204	T1053	T1547	T1070	T1555	T1046	T1563	T1119	T1041	T1219	T1489
T1190	T1047	T1547	T1484	T1027	T1552	T1135	T1072	T1113	T1011	T1573	T1491
T1189	T1569	T1543	T1543	T1484	T1187	T1057	T1080	T1115	T1020	T1090	T1531
T1199	T1072	T1136	T1068	T1112	T1040	T1018	T1550	T1530	T1029	T1095	T1485
	T1203	T1098	T1055	T1140	T1558	T1087		T1213	T1537	T1572	T1561
	T1106	T1505	T1548	T1036		T1069		T1074			T1529
	T1129	T1574	T1574	T1055		T1012					
		T1546	T1134	T1548		T1518					
			T1546	T1222		T1033					
				T1218		T1007					
				T1574		T1482					
				T1134		T1614					
				T1553		T1016					
				T1622		T1049					
				T1480		T1622					
				T1564		T1040					
				T1202		T1120					
				T1620		T1497					
				T1550							
				T1497							

Table 3: Mitigations to most Common Ransomware Techniques/Sub-Techniques

Mitigation	Score
M1026: Privileged Account Management	75
M1018: User Account Management	71
M1017: User Training	61
M1040: Behavior Prevention on Endpoint	51
M1030: Network Segmentation	50
M1028: Operating System Configuration	44
M1049: Antivirus/Antimalware	44
M1027: Password Policies	39
M1042: Disable or Remove Feature or Program	38
M1053: Data Backup	38
M1038: Execution Prevention	37

High Priority	M1026: Privileged Account Management M1018: User Account Management M1017: User Training				
Medium Priority	M1040: Behavior Prevention on Endpoint M1030: Network Segmentation M1028: Operation System Configuration M1049: Antimalware	M1027: Password Policies M1042: Disable or Remove Feature or Program M1053: Data Backup M1038: Execution Prevention			
Low Priority	M1031 M1015 M1022 M1024	M1032 M1035 M1021 M1054	M1036 M1013 M1047 M1025	M1043 M1051 M1045 M1050	M1048 M1016 M1041
Minor Priority	M1037 M1057 M1029 M1056	M1052 M1020 M1019 M1044			

What are the **dominating ransomware groups** identified by their **victim count**?

What are the **Tactics, Techniques, and Procedures** employed by ransomware groups, and how are these **quantified** to understand their **prevalence** and variation?

What are the related **mitigations** that can effectively reduce the risk of successful ransomware attacks based on the identified and quantified Tactics, Techniques and Procedures, and what is their **prioritization**?

NEW TRENDS IN RANSOMWARE

Part 2/2 (2024/25)

RQ1: *How has the ransomware ecosystem evolved over the past two years, and what **key trends** currently characterize its structure and operations?*

RQ2: *What is the **impact** of these changes on the TTPs adopted by ransomware groups?*

RESULTS AND ANALYSIS

Ransomware Groups ranked by their victim count

Table 1: Ransomware Groups ranked by Victim Count

Ransomware Group	Victim Count
LockBit	1832
ALPHV	424
CL0P	253
BlackBasta	244
Hive	218
Royal	179
BianLian	152
Everest	137
Play	126
Ragnar Locker	97
BlackByte	94
Karakurt	87
Snatch	80
Cuba	70
Sprite Spider	52
RansomHouse	47
Frozen Spider	41
Stormous	29
MedusaLocker	23
Qilin	19
Monti	18
Mallox	16
Daixin Team	9
Omega Lock	4

Table 1 Ransomware Groups in Scope

Ransomware Group	Victim Count
LockBit 3.0	2920
Play News	706
BlackBasta	640
RansomHub	551
CL0P	549
8Base	433
Akira	420
BianLian	415
Dispossessor	347
Medusa	341
Qilin	303
Cactus	280
Hunters International	259
Everest	232
INC_Ransom	215
Black Suit	180
Rhysida	163
Meow Leaks	143
Kill Security	137
RansomHouse	131
FunkSec	115
DragonForce	114
RA Group	101
Fog	89
Lynx	85
...	...

RESULTS AND ANALYSIS

Tactics, Techniques, and Procedures (quantified)

Tactics (why)

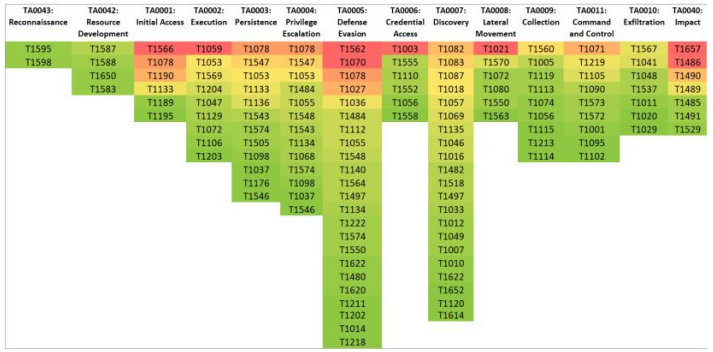
Techniques (how)

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact
T1078	T1059	T1078	T1078	T1562	T1003	T1083	T1021	T1560	T1567	T1071	T1486
T1566	T1053	T1133	T1053	T1078	T1110	T1082	T1570	T1005	T1048	T1105	T1490
T1133	T1204	T1053	T1547	T1070	T1555	T1046	T1563	T1119	T1041	T1219	T1489
T1190	T1047	T1547	T1484	T1027	T1552	T1135	T1072	T1113	T1011	T1573	T1491
T1189	T1569	T1543	T1543	T1484	T1187	T1057	T1080	T1115	T1020	T1090	T1531
T1199	T1072	T1136	T1068	T1112	T1040	T1018	T1550	T1530	T1029	T1095	T1485
	T1203	T1098	T1055	T1140	T1558	T1087		T1213	T1537	T1572	T1561
	T1106	T1505	T1548	T1036		T1069		T1074			T1529
	T1129	T1574	T1574	T1055		T1012					
		T1546	T1134	T1548		T1518					
			T1546	T1222		T1033					
				T1218		T1007					
				T1574		T1482					
				T1134		T1614					
				T1553		T1016					
				T1622		T1049					
				T1480		T1622					
				T1564		T1040					
				T1202		T1120					
				T1620		T1497					
				T1550							
				T1497							

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1595	T1587	T1566	T1059	T1078	T1078	T1562	T1003	T1082	T1021	T1560	T1071	T1567	T1657
T1598	T1588	T1078	T1053	T1547	T1547	T1070	T1555	T1083	T1570	T1005	T1219	T1041	T1486
	T1650	T1190	T1569	T1053	T1053	T1078	T1110	T1087	T1072	T1119	T1105	T1048	T1490
	T1583	T1133	T1204	T1133	T1484	T1027	T1552	T1018	T1080	T1113	T1090	T1537	T1489
		T1189	T1047	T1136	T1055	T1036	T1056	T1057	T1550	T1074	T1573	T1011	T1485
		T1195	T1129	T1543	T1548	T1484	T1558	T1069	T1563	T1056	T1572	T1020	T1491
			T1072	T1574	T1543	T1112		T1135		T1115	T1001	T1029	T1529
			T1106	T1505	T1134	T1055		T1046		T1213	T1095		
			T1203	T1098	T1068	T1548		T1016		T1114	T1102		
				T1037	T1574	T1140		T1482					
				T1176	T1098	T1564		T1518					
				T1546	T1037	T1497		T1497					
					T1546	T1134		T1033					
						T1222		T1012					
						T1574		T1049					
						T1550		T1007					
						T1622		T1010					
						T1480		T1622					
						T1620		T1652					
						T1211		T1120					
						T1202		T1614					
						T1014							
						T1218							

RESULTS AND ANALYSIS

Paradigm Shift through AI



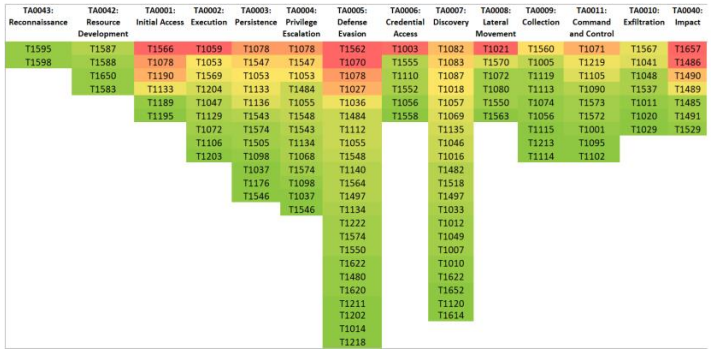
TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1595	T1587	T1566	T1059	T1078	T1078	T1562	T1003	T1082	T1021	T1560	T1071	T1567	T1657
T1598	T1588	T1078	T1053	T1547	T1547	T1070	T1555	T1083	T1570	T1005	T1219	T1041	T1486
	T1650	T1190	T1569	T1053	T1053	T1078	T1110	T1087	T1072	T1119	T1105	T1048	T1490
	T1583	T1133	T1204	T1133	T1484	T1027	T1552	T1018	T1080	T1113	T1090	T1537	T1489
		T1189	T1047	T1136	T1055	T1036	T1056	T1057	T1550	T1074	T1573	T1011	T1485
		T1195	T1129	T1543	T1548	T1484	T1558	T1069	T1563	T1056	T1572	T1020	T1491
			T1072	T1574	T1543	T1112		T1135		T1115	T1001	T1029	T1529
			T1106	T1505	T1134	T1055		T1046		T1213	T1095		
			T1203	T1098	T1068	T1548		T1016		T1114	T1102		
				T1037	T1574	T1140		T1482					
				T1176	T1098	T1564		T1518					
				T1546	T1037	T1497		T1497					
					T1546	T1134		T1033					
						T1222		T1012					
						T1574		T1049					
						T1550		T1007					
						T1622		T1010					
						T1480		T1622					
						T1620		T1652					
						T1211		T1120					
						T1202		T1614					
						T1014							
						T1218							

From Human Expertise to AI Automation

- First documented use of **ChatGPT (FraudGPT) and generative AI for malware development** by the group *FunkSec*
- AI lowers technical barriers → emergence of **“Ransomware-as-a-Service (RaaS) 2.0”**
- Automated generation of phishing campaigns, exploit scripts, and code obfuscation
- Enables **decentralized and opportunistic threat actors** with minimal coding skills
- Represents a **transformative shift** toward intelligent, self-learning cyber threats

RESULTS AND ANALYSIS

Paradigm Shift through AI

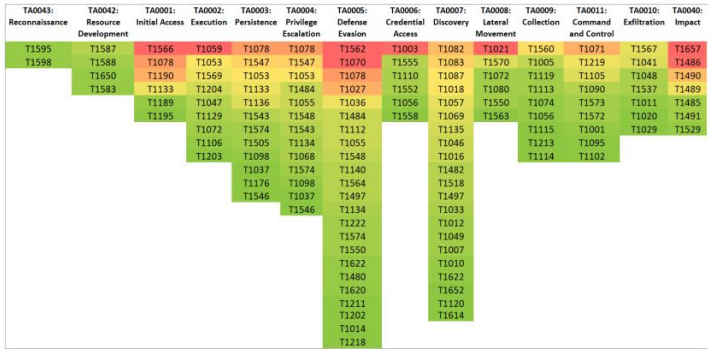


Key Observations from MITRE ATT&CK Heatmap

- **Red zones** = Most frequently used techniques:
  - *T1059* – Command-Line Execution
  - *T1486* – Data Encryption for Impact
  - *T1657* – Financial Theft
- **Emerging trends:**
  - Increased focus on **data exfiltration** and **cloud-based operations**
  - Broader integration of **AI-assisted automation** across all ATT&CK phases

RESULTS AND ANALYSIS

AI-Driven Shifts in TTP Focus



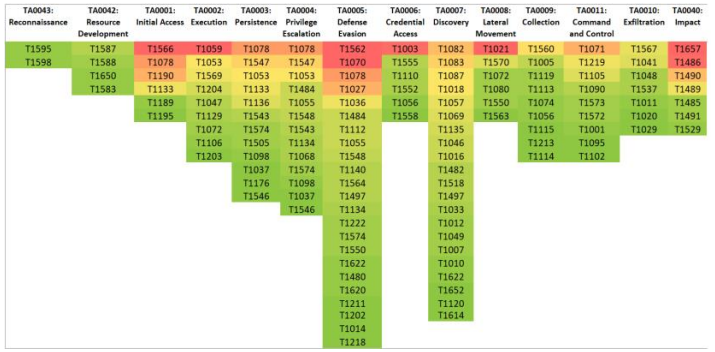
Tactic (MITRE)	Technique (MITRE)	AI Contribution
TA0001 – Initial Access	Exploit Public-Facing Applications (T1190)	Automated vulnerability scanning & exploitation
TA0005 – Defense Evasion	Encryption, Rootkits (T1211, T1014)	AI-assisted code mutation & obfuscation
TA0007 – Discovery	System Information Discovery (T1082)	AI-driven environment mapping & prioritization
TA0010 – Exfiltration	Cloud Storage Abuse (e.g., Mega, Drive)	Automated data packaging & transfer routines

Key takeaway:

AI enhances **efficiency**, **adaptability**, and **stealth** across every ransomware phase.

RESULTS AND ANALYSIS

Ransomware + AI = New Threat Models



TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1595	T1587	T1566	T1059	T1078	T1078	T1562	T1003	T1082	T1021	T1560	T1071	T1567	T1657
T1598	T1588	T1078	T1053	T1547	T1547	T1070	T1555	T1083	T1570	T1005	T1219	T1041	T1486
	T1650	T1190	T1569	T1053	T1053	T1078	T1110	T1087	T1072	T1119	T1105	T1048	T1490
	T1583	T1133	T1204	T1133	T1484	T1027	T1552	T1018	T1080	T1113	T1090	T1537	T1489
		T1189	T1047	T1136	T1055	T1036	T1056	T1057	T1550	T1074	T1573	T1011	T1485
		T1195	T1129	T1543	T1548	T1484	T1558	T1069	T1563	T1056	T1572	T1020	T1491
			T1072	T1574	T1543	T1112		T1135		T1115	T1001	T1029	T1529
			T1106	T1505	T1134	T1055		T1046		T1213	T1095		
			T1203	T1098	T1068	T1548		T1016		T1114	T1102		
				T1037	T1574	T1140		T1482					
				T1176	T1098	T1564		T1518					
				T1546	T1037	T1497		T1497					
					T1546	T1134		T1033					
						T1222		T1012					
						T1574		T1049					
						T1550		T1007					
						T1622		T1010					
						T1480		T1622					
						T1620		T1652					
						T1211		T1120					
						T1202		T1614					
						T1014							
						T1218							

Observed Trends

- **AI-driven automation** in reconnaissance and lateral movement
- **Adaptive attack decisions** through ML-based prioritization models
- **New impact tactics**: combination of encryption, financial theft, and extortion
- **Hybrid motivations:** blending cybercrime, hacktivism, and political influence
- The **human factor** is no longer the weakest link – **AI exploitation** is

RESULTS AND ANALYSIS

Tactics, Techniques, and Procedures (quantified)

Table 2: Most Common Techniques/Sub-Techniques of Ransomware Groups

Techniques/Sub-Technique	Score	Percentage
T1486: Data Encrypted for Impact	23	96%
T1078: Valid Accounts	20	83%
T1490: Inhibit System Recovery	15	63%
T1133: External Remote Services	15	63%
T1083: File and Directory Discovery	14	58%
T1562.001: Disable or Modify Tools	14	58%
T1059.001: PowerShell	13	54%
T1190: Exploit Public-Facing Application	13	54%
T1489: Service Stop	12	50%
T1566: Phishing	12	50%

Table 2 Comparison of the Top 10 Techniques

Technique	2023	2024
T1657: Financial Theft	-	100%
T1486: Data Encrypted for Impact	96%	96%
T1190: Exploit Public-Facing Applications	54%	71%
T1490: Inhibit System Recovery	63%	67%
T1082: System Information Discovery	33%	67%
T1078: Valid Accounts	83%	63%
T1562.001: Disable or Modify Tools	58%	63%
T1083: File and Directory Discovery	58%	58%
T1021.001: Remote Desktop Protocol	42%	58%
T1070.004: File Deletion	29%	50%
T1133: External Remote Services	63%	46%
T1489: Service Stop	50%	46%
T1059.001: PowerShell	54%	42%
T1566: Phishing	50%	42%

RESULTS AND ANALYSIS

Related Mitigations for Tactics, Techniques, and Procedures

Table 2 Comparison of the Top 10 Techniques

Technique	2023	2024
T1657: Financial Theft	-	100%
T1486: Data Encrypted for Impact	96%	96%
T1190: Exploit Public-Facing Applications	54%	71%
T1490: Inhibit System Recovery	63%	67%
T1082: System Information Discovery	33%	67%
T1078: Valid Accounts	83%	63%
T1562.001: Disable or Modify Tools	58%	63%
T1083: File and Directory Discovery	58%	58%
T1021.001: Remote Desktop Protocol	42%	58%
T1070.004: File Deletion	29%	50%
T1133: External Remote Services	63%	46%
T1489: Service Stop	50%	46%
T1059.001: PowerShell	54%	42%
T1566: Phishing	50%	42%

Table 3 Comparison of the Top 10 Mitigations

Mitigation	2023	2024
M1018: User Account Management	71	95
M1026: Privileged Account Management	75	56
M1030: Network Segmentation	50	53
M1017: User Training	61	49
M1038: Execution Prevention	37	41
M1032: Multi-factor Authentication	25	40
M1053: Data Backup	38	39
M1042: Disable or Remove Feature or Program	38	35
M1028: Operating System Configuration	44	30
M1022: Restrict File and Directory Permissions	26	26

CONCLUSION (PART 2: 2024/25)

AI Redefines the TTP Paradigm

- **Several Changes** in top ransomware techniques from 2023 to 2024
- AI enables **scalable, adaptive, and difficult-to-detect** attack strategies
- Cyber defense must transition from **reactive** to **intelligence-driven** models
- Future threat landscape = **AI-driven evolution of TTP ecosystems**
- Continuous **TTP monitoring and re-mapping** are essential for resilience

➢ How can **AI for Cyber Defense systems** detect cyber attacks in real time?

AI FOR CYBER DEFENSE

RQ1: *How do ML-based IDS models perform on target network data compared to their original training datasets?*

RQ2: *Does integrating benign, target-specific data enhance IDS accuracy and generalization?*

DATASETS

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

CIC-IDS2017:

- ~2 million network flows
- Simpler network setup
- Used as target network in hybrid approach

CSE-CIC-IDS2018:

- ~16 million network flows (reduced by 95% benign traffic)
- Complex infrastructure (420 machines)
- Attack source in hybrid approach

Quelle: A. Lawall and T. Zöller, “Impact of Target Network-Specific Data on the Performance of Machine-Learning-Based Intrusion Detection System Models”, 2025 5th Intelligent Cybersecurity Conference (ICSC), Tampa, FL, USA, 2025, pp. 290-297, doi: 10.1109/ICSC65596.2025.11140289.

DATA PROCESSING & FEATURE SELECTION

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Preprocessing:

- Reduced benign traffic in CSE-CIC-IDS2018 by 95%
- Selected 7 attack categories present in both datasets
- Excluded attacks with fewer than 100 samples
- Removed incomplete records and handled infinite values

Feature Selection:

- Combined chi-squared tests and mutual information scores
- Applied correlation threshold of $|0.7|$ to reduce multicollinearity
- Selected 39 features from original 81 network flow features

EXPERIMENTAL SETUP

Model Architectures

FFNN:

- 2 dense layers (64, 32 neurons)
- Dropout (30%)
- L2 regularization
- ReLU activation

CNN:

- 3 convolutional layer
- Decreasing filters (120, 60, 30)
- Increasing kernel sizes (2, 3, 4)
- ReLU activation

Quelle: A. Lawall and T. Zöller, “Impact of Target Network-Specific Data on the Performance of Machine-Learning-Based Intrusion Detection System Models”, 2025 5th Intelligent Cybersecurity Conference (ICSC), Tampa, FL, USA, 2025, pp. 290-297, doi: 10.1109/ICSC65596.2025.11140289.

EXPERIMENTAL SETUP

Configurations

Baseline:

- Train and test on same dataset

Cross-Network:

- Train on A, test on B
- Train on B, test on A

Hybrid Approach:

- Benign traffic from target
- Attack traffic from source

Quelle: A. Lawall and T. Zöller, “Impact of Target Network-Specific Data on the Performance of Machine-Learning-Based Intrusion Detection System Models”, 2025 5th Intelligent Cybersecurity Conference (ICSC), Tampa, FL, USA, 2025, pp. 290-297, doi: 10.1109/ICSC65596.2025.11140289.

RESULTS

Baseline Results

Both architectures showed excellent performance when trained and tested on the same dataset:

Model	CIC-IDS2017	CSE-CIC-IDS2018
FFNN	0.98	0.98
CNN	1.00	1.00

- Strong detection capabilities across all attack categories
- CNN showed marginally better consistency across attack types
- High F1-scores for both malicious and benign traffic

Quelle: A. Lawall and T. Zöller, “Impact of Target Network-Specific Data on the Performance of Machine-Learning-Based Intrusion Detection System Models”, 2025 5th Intelligent Cybersecurity Conference (ICSC), Tampa, FL, USA, 2025, pp. 290-297, doi: 10.1109/ICSC65596.2025.11140289.

RESULTS

Cross-Network Generalization

Notable performance degradation when models were tested on different network environments:

Model	Training Set	Test Set	F1-Score
FFNN	CIC-IDS2017	CSE-CIC-IDS2018	0.36
FFNN	CSE-CIC-IDS2018	CIC-IDS2017	0.31
CNN	CIC-IDS2017	CSE-CIC-IDS2018	0.46
CNN	CSE-CIC-IDS2018	CIC-IDS2017	0.52

- CNN shows better generalization (avg. F1-score: 0.495) compared to FFNN (avg. F1-score: 0.345)

Quelle: A. Lawall and T. Zöller, “Impact of Target Network-Specific Data on the Performance of Machine-Learning-Based Intrusion Detection System Models”, 2025 5th Intelligent Cybersecurity Conference (ICSC), Tampa, FL, USA, 2025, pp. 290-297, doi: 10.1109/ICSC65596.2025.11140289.

RESULTS

Hybrid Approach Results

Integrating benign traffic from target network with attack traffic from source network:

Model	F1-Score	Comparison to Cross-Network
FFNN	0.35	Similar (0.31-0.36)
CNN	0.52	Similar (0.46-0.52)

- No significant improvement over direct cross-network testing
- Hybrid approach did not solve the generalization challenge
- CNN maintains better performance than FFNN

Quelle: A. Lawall and T. Zöller, “Impact of Target Network-Specific Data on the Performance of Machine-Learning-Based Intrusion Detection System Models”, 2025 5th Intelligent Cybersecurity Conference (ICSC), Tampa, FL, USA, 2025, pp. 290-297, doi: 10.1109/ICSC65596.2025.11140289.

RESULTS

Attack-specific Analysis

Poor Generalization:

- Botnet Ares (F1≈0)
- DDoS-LOIC-HTTP (F1≈0)
- DoS GoldenEye (F1=0.05-0.50)
- DoS Hulk (F1=0-0.75)

Better Generalization:

- DoS Slowloris (F1=0.78-0.97)
- Infiltration-NMAP (F1=0.33-0.92)
- SSH-BruteForce (F1=0.66-1.00)

Quelle: A. Lawall and T. Zöller, “Impact of Target Network-Specific Data on the Performance of Machine-Learning-Based Intrusion Detection System Models”, 2025 5th Intelligent Cybersecurity Conference (ICSC), Tampa, FL, USA, 2025, pp. 290-297, doi: 10.1109/ICSC65596.2025.11140289.

RESULTS

Attack-specific Analysis: Feature Distribution

DDoS-LOIC-HTTP:

(High variability between datasets)

- Mean KS statistic: 0.380
- Standard deviation: 0.411

DoS Slowloris:

(more consistent)

- Mean KS statistic: 0.233
- Standard deviation: 0.229

Quelle: A. Lawall and T. Zöller, "Impact of Target Network-Specific Data on the Performance of Machine-Learning-Based Intrusion Detection System Models“, 2025 5th Intelligent Cybersecurity Conference (ICSC), Tampa, FL, USA, 2025, pp. 290-297, doi: 10.1109/ICSC65596.2025.11140289.

RESULTS

Attack-specific Analysis: Network Activation Analysis

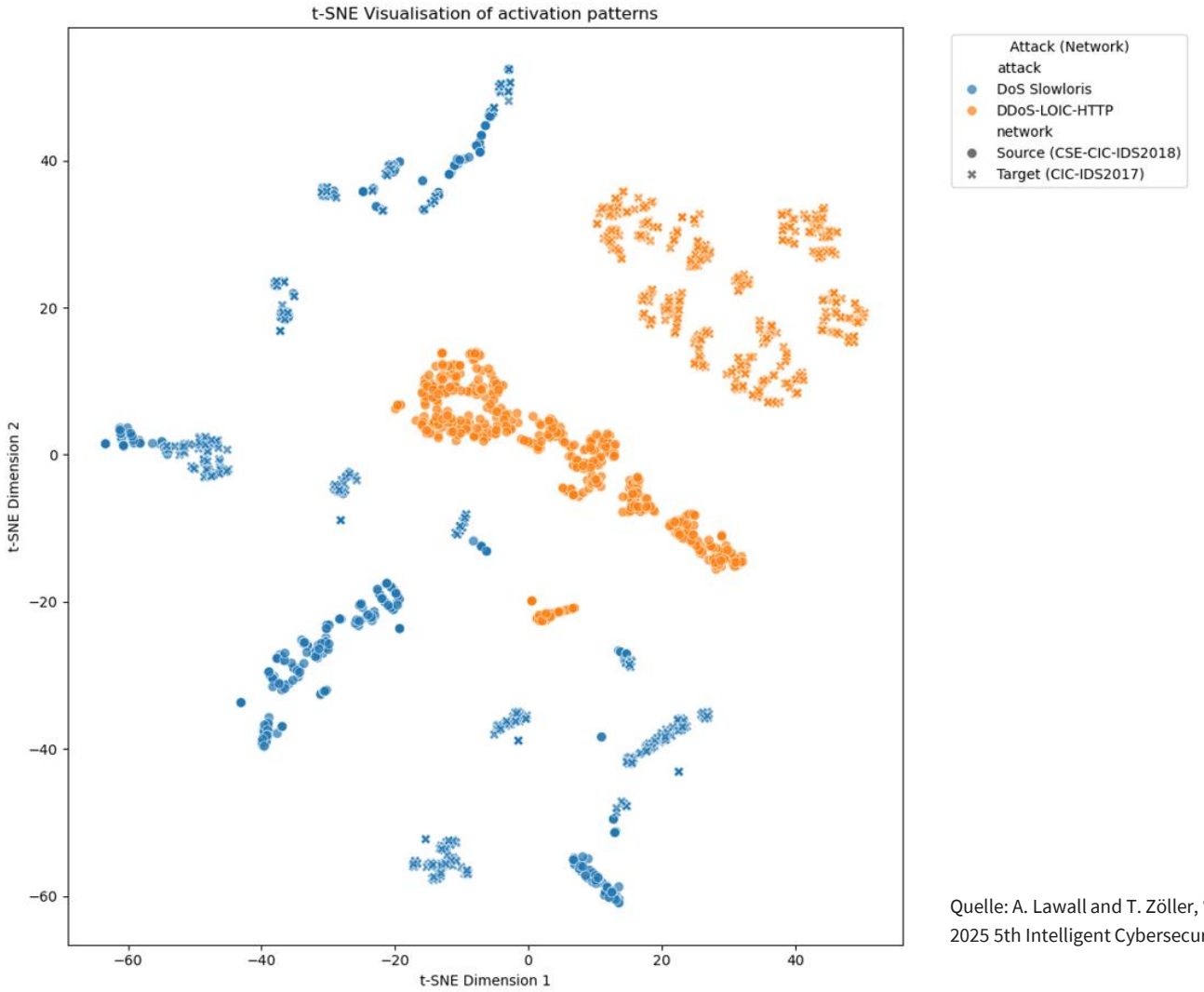
Metric	DDoS-LOIC-HTTP	DoS Slowloris
Pearson Correl. Coef.	0.346	0.944
Cosine Similarity	0.377	0.950
Euclidean Distance	12.397	2.544

- DoS Slowloris shows remarkably consistent internal representations across networks
- DDoS-LOIC-HTTP exhibits network-specific rather than attack-specific patterns

Quelle: A. Lawall and T. Zöller, “Impact of Target Network-Specific Data on the Performance of Machine-Learning-Based Intrusion Detection System Models”, 2025 5th Intelligent Cybersecurity Conference (ICSC), Tampa, FL, USA, 2025, pp. 290-297, doi: 10.1109/ICSC65596.2025.11140289.

RESULTS

Attack-specific Analysis: Why DoS Slowloris generalizes better?



Quelle: A. Lawall and T. Zöller, “Impact of Target Network-Specific Data on the Performance of Machine-Learning-Based Intrusion Detection System Models”, 2025 5th Intelligent Cybersecurity Conference (ICSC), Tampa, FL, USA, 2025, pp. 290-297, doi: 10.1109/ICSC65596.2025.11140289.

CONCLUSION AND FUTURE WORK

AI for Cyber Defense

- **Substantial performance drop when IDS models are deployed to new environments**
  - FFNN F1-scores drop from 0.98 to 0.31-0.36
  - CNN F1-scores drop from 1.00 to 0.46-0.52
- **CNN models generalize better than FFNN models**
- **Hybrid approach (target-specific benign data) provides limited improvement**
- **Attack detection generalization varies remarkably by attack type**
  - Some attacks maintain consistent detection rates (e.g., DoS Slowloris)
  - Others exhibit limited generalization (e.g., DDoS-LOIC-HTTP)

CONCLUSION AND FUTURE WORK

Future Work

- **Adaptive Threat Intelligence & AI Fusion**
  Continuous integration of ransomware TTP intelligence into AI-based defense pipelines for **real-time learning and adaptation**.

- **Cross-Network Resilience through Transfer Learning**
  Enhance IDS generalization with **federated learning**, **domain adaptation**, and **synthetic adversarial data** to overcome dataset bias.

KIDZ:
AI-supported detection of cyber attacks (espec. 0-day exploits) on IT infrastructures

https://www.iu.de/en/research/projects/kidz/

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

How will the threat landscape change when artificial intelligence also fully automates cyberattacks?

Can AI-driven defense truly think ahead – predicting and preventing cyberattacks before they occur?

Prof. Dr. Alexander Lawall
alexander.lawall@iu.org