

# Crime Script Analysis Table: TU/e Cyberattack (January 2025)

Based on Cornish (1994) Seven-Stage Crime Script Framework

## Main Crime Script Table

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools	Page
1. PREPARATION	Pre-Jan 6, 2025	Adversary obtained leaked credentials and prepared attack infrastructure	<ul style="list-style-type: none"><li>• Obtained leaked credentials for account_lp2 and account_lp3 [p.11-12]</li><li>• Fox-IT found credentials in publicly available leak document [p.12]</li><li>• Researched TU/e infrastructure</li><li>• Identified VPN without MFA [p.11]</li><li>• Prepared exploitation tools</li></ul>	<b>TA0043: Reconnaissance</b> <ul style="list-style-type: none"><li>• T1589.001: Gather Victim Identity Information: Credentials</li><li>• T1590: Gather Victim Network Information</li><li>• T1592: Gather Victim Host Information</li></ul> <b>TA0042: Resource Development</b> <ul style="list-style-type: none"><li>• T1583.003: Acquire Infrastructure: Virtual Private Server</li><li>• T1588.002: Obtain Capabilities: Tool</li><li>• T1586.001: Compromise Accounts: Social Media Accounts</li></ul>	<ul style="list-style-type: none"><li>• Credential leak databases [p.11-12]</li><li>• VPS hosting infrastructure [p.11]</li><li>• Advanced IP Port Scanner [p.16, p.23]</li><li>• SoftPerfect Network Scanner [p.16, p.23]</li><li>• ShareFinder [p.16, p.23]</li><li>• AnyDesk [p.16-17, p.23]</li><li>• TeamViewer [p.16-17, p.23]</li><li>• CrackMapExec [p.5, p.12]</li></ul>	1 8 1 4 6 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools	Source
2. ENTRY	Jan 6, 2025	Adversary gained initial access via VPN using leaked credentials	<ul style="list-style-type: none"> <li>13:57 - Failed login: account_lp1 from ip_adversary_1 [p.11]</li> </ul>	<b>TA0001: Initial Access</b> <ul style="list-style-type: none"> <li>T1078: Valid Accounts</li> </ul>	<ul style="list-style-type: none"> <li>Leaked valid credentials [p.11-12]</li> </ul>	1
			<ul style="list-style-type: none"> <li>14:08 - <b>SUCCESSFUL LOGIN:</b> account_lp2 from ip_adversary_1 [p.11]</li> <li>14:13 - <b>SUCCESSFUL LOGIN:</b> account_lp3 from same IP [p.11]</li> <li>Established VPN access to internal network [p.11]</li> <li>Fox-IT considers this incident start [p.11, p.22]</li> </ul>	<b>TA0001: Initial Access</b> <ul style="list-style-type: none"> <li>T1078.002: Valid Accounts: Domain Accounts</li> <li>T1133: External Remote Services</li> <li>T1110.004: Brute Force: Credential Stuffing</li> </ul>	<ul style="list-style-type: none"> <li>VPS from hosting provider [p.11]</li> <li>VPN client software</li> </ul>	1
3. PRE-CONDITION (Initial Reconnaissance)	Jan 6-10, 2025	Adversary performed network reconnaissance and mapped Active Directory infrastructure	<ul style="list-style-type: none"> <li>15:14 (Jan 6) - account_lp2 connected to multiple systems [p.11]</li> <li>Connections atypical for account_lp2 [p.11]</li> <li>Rapid succession = automated authentications [p.11]</li> <li>Automated network reconnaissance [p.11]</li> <li>Mapped network infrastructure</li> <li>Identified domain controllers and AD structure [p.13]</li> <li>Located: SYSTEM_DC1_PROD, SYSTEM_DC2_PROD, SYSTEM_DC3_PROD, SYSTEM_DC4_PROD [p.13, p.24]</li> </ul>	<b>TA0007: Discovery</b> <ul style="list-style-type: none"> <li>T1087: Account Discovery</li> <li>T1087.002: Account Discovery: Domain Account</li> <li>T1018: Remote System Discovery</li> <li>T1046: Network Service Discovery</li> <li>T1069: Permission Groups Discovery</li> <li>T1069.002: Permission</li> </ul>	<ul style="list-style-type: none"> <li>Network scanning tools</li> <li>VPN access [p.11]</li> <li>Compromised user credentials [p.11]</li> </ul>	1 1 6 8 9 10

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools	Notes
				Groups Discovery: Domain Groups • T1482: Domain Trust Discovery		
				TA0008: Lateral Movement • T1021: Remote Services (reconnaissance attempts)		
4. INSTRUMENTAL PRE-CONDITION (Privilege Escalation Prep)	Jan 6-11, 2025	Adversary identified authentication protocol weaknesses to enable privilege escalation	• Identified DCs accepting NTLMv1 authentication [p.13-14, p.24] • Discovered lmcompatibilitylevel=1 on prod DCs [p.14, p.24] • Table 12: 4 prod DCs with level 1 [p.24] • Prepared coercion attack infrastructure [p.13-14] • Targeted ACCOUNT_DC4_PROD for credential theft [p.13-15] • Set up hash cracking capability [p.13-14]	TA0007: Discovery • T1201: Password Policy Discovery • T1033: System Owner/User Discovery  TA0004: Privilege Escalation (preparation) • T1558: Steal or Forge Kerberos Tickets (preparation)  TA0006: Credential Access (preparation) • T1003: OS	• NTLM relay tools • Hash cracking infrastructure [p.13-14] • Coercion attack tools [p.13-14]	• v 1 2 • 6 2 • t • 1 [

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools	Source
				Credential Dumping (preparation)		
				• T1212: Exploitation for Credential Access		
<b>5. INSTRUMENTAL INITIATION</b> (Privilege Escalation)	Jan 11, 2025 19:59-21:07	<b>Adversary executed coercion attack, performed DCSync, and obtained enterprise admin privileges</b>	<b>First DCSync Attempt (19:59):</b> [p.13] • Auth to SYSTEM_DC4_PROD using ACCOUNT_DC4_PROD • DCSync attempt - <b>UNSUCCESSFUL</b> (Defender detected)  <b>Coercion Attack (~19:59-20:59):</b> [p.13-14] • Table 4: NTLMv1 auths from DC accounts to DCs from VPN IPs [p.13] • Likely coerced SYSTEM_DC4_PROD into NTLMv1 auth [p.14] • Captured & cracked ACCOUNT_DC4_PROD NTLMv1 hash [p.14]  <b>Successful DCSync (20:59):</b> [p.13] • Auth to SYSTEM_DC1_PROD as ACCOUNT_DC4_PROD • DCSync attack - <b>SUCCESSFUL</b> [p.13] • Retrieved all NTLM	<b>TA0006: Credential Access</b> • T1557: Adversary-in-the-Middle • T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay • T1003.006: OS Credential Dumping: DCSync • T1212: Exploitation for Credential Access • T1556: Modify Authentication Process  <b>TA0004: Privilege Escalation</b> • T1078.002: Valid Accounts: Domain Accounts • T1068: Exploitation for Privilege	• Cracked DC computer account credentials [p.14-15] • DCSync tools [p.13] • Pass-the-hash capabilities [p.15]	• 6 2 • t • 1 1 

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools	9
			hashes from SYSTEM_DC1_PROD [p.15]	Escalation		
			<ul style="list-style-type: none"> <li>Obtained hash for account_hp1 [p.15]</li> </ul>	<b>TA0008: Lateral Movement</b> <ul style="list-style-type: none"> <li>T1550.002: Use Alternate Authentication Material: Pass the Hash</li> </ul>		
			<b>Domain Compromise (21:07):</b> [p.15] <ul style="list-style-type: none"> <li>Auth using account_hp1 hash (pass-the-hash)</li> </ul>			
			<ul style="list-style-type: none"> <li><b>ENTERPRISE ADMIN ACHIEVED</b> [p.12, p.15]</li> </ul>			
6. INSTRUMENTAL ACTUALIZATION (Post-Exploitation)	Jan 11, 21:07 - Jan 12, 01:17	Adversary performed discovery, established persistence via accounts and remote tools, and targeted backup systems	<b>Discovery Activities:</b> [p.16] <ul style="list-style-type: none"> <li>22:43 - Advanced IP Scanner on system_srv2 [p.16]</li> <li>22:53 - SoftPerfect Scanner on tfe290 [p.16]</li> <li>23:56 - ShareFinder on SYSTEM_SRV4 [p.16]</li> <li>00:58 - Domain admin enumeration [p.20]</li> </ul> <b>Account Persistence:</b> [p.17] <ul style="list-style-type: none"> <li>Compromised: account_hp2 (22:00), account_hp3 (22:01)</li> <li>Created: account_hp4 (22:46), account_hp5 (23:11)</li> </ul> <b>Tool Persistence:</b> [p.16-17] <ul style="list-style-type: none"> <li>AnyDesk: system_srv1 (23:27), system_srv3 (23:29),</li> </ul>	<b>TA0007: Discovery</b> <ul style="list-style-type: none"> <li>T1046: Network Service Discovery</li> <li>T1135: Network Share Discovery</li> <li>T1087.002: Account Discovery: Domain Account</li> <li>T1069.002: Permission Groups Discovery: Domain Groups</li> <li>T1018: Remote System Discovery</li> </ul> <b>TA0003: Persistence</b> <ul style="list-style-type: none"> <li>T1136.002:</li> </ul>	<ul style="list-style-type: none"> <li>Enterprise admin privileges [p.12, p.18]</li> <li>AnyDesk [p.16-17]</li> <li>TeamViewer [p.16-17]</li> <li>Advanced IP Scanner [p.16]</li> <li>SoftPerfect Network Scanner [p.16]</li> <li>ShareFinder [p.16]</li> <li>PowerShell [p.17, p.20]</li> <li>CrackMapExec [p.5, p.12]</li> </ul>	

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools	9
			system_rootdc2_prod (00:23), system_dc1_prod (00:44) • TeamViewer: system_ws2 (22:36), system_ws1 (23:32), system_srv3 (23:58) • Confirmed connections to system_srv3 and system_srv1 [p.16]	Create Account: Domain Account • T1098: Account Manipulation • T1219: Remote Access Software • T1543: Create or Modify System Process		
			<b>Ransomware Prep:</b> [p.17] • 00:52 - Accessed Veeam backup on system_srv5 • 00:57 - Attempted to stop Veeam services  <b>Scope:</b> [p.18] • 14 hands-on-keyboard systems • 77 authentication-only systems • <b>Total: 91/350 systems accessed</b> [p.18, Table 9]	<b>TA0005: Defense Evasion</b> • T1562.001: Impair Defenses: Disable or Modify Tools  <b>TA0040: Impact</b> (preparation) • T1490: Inhibit System Recovery • T1485: Data Destruction (preparation)		
<b>7. DOING</b> (Criminal Objective - INTERRUPTED)	Jan 11-12, 2025	<b>Adversary prepared for ransomware deployment but was detected and contained</b>	<b>Intended (Not Achieved):</b> [p.20-21] • Ransomware deployment across domain (likely based on TTPs) • Mass system encryption • Double-extortion	<b>TA0009: Collection</b> • T1005: Data from Local System • T1039: Data from Network Shared Drive	• Full domain control [p.15, p.18] • Remote admin tools [p.16-17] • Multiple high-privileged accounts [p.17]	• ( 2 • ( t •

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools	
		before execution	<p>scenario</p> <p><b>Accomplished:</b></p> <ul style="list-style-type: none"> <li>• ~2.1 GB data exfiltrated (Jan 5-12) [p.19]</li> <li>• Contents: VPN data, AD info (system names, usernames, password hashes) [p.19-20]</li> <li>• No large-scale data exfiltration [p.20, p.22]</li> <li>• ShareFinder results file deleted [p.16]</li> <li>• Full enterprise admin access [p.18]</li> <li>• Multiple persistence mechanisms [p.16-17]</li> <li>• Backup disruption attempted [p.17]</li> </ul> <p><b>DETECTION &amp; INTERRUPTION:</b> [p.5, p.12]</p> <ul style="list-style-type: none"> <li>• 21:55 (Jan 11) - SURFsoc alerted [p.5]</li> <li>• 63 security alerts generated [p.12]</li> <li>• 22:48 - Escalated to TU/e [p.5]</li> <li>• 23:20 - FoxCERT informed [p.5]</li> <li>• 00:15 (Jan 12) - Intake call [p.5]</li> <li>• <b>01:17 - Network isolated</b> [p.5, p.22]</li> <li>• Attack contained before ransomware [p.22]</li> </ul>	<ul style="list-style-type: none"> <li>• T1119: Automated Collection</li> <li>• <b>TA0010: Exfiltration</b></li> <li>• T1041: Exfiltration Over C2 Channel</li> <li>• T1020: Automated Exfiltration</li> <li>• <b>TA0011: Command and Control</b></li> <li>• T1071: Application Layer Protocol</li> <li>• T1132: Data Encoding</li> <li>• T1573: Encrypted Channel</li> <li>• <b>TA0040: Impact</b> (intended, not achieved)</li> <li>• T1486: Data Encrypted for Impact</li> <li>• T1490: Inhibit System Recovery</li> <li>• T1491: Defacement</li> </ul>	<ul style="list-style-type: none"> <li>• Backup access [p.17]</li> <li>• C2 infrastructure [p.19]</li> </ul>	1   • 6

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools	Findings
8. EXIT (Post-Crime)	Jan 12, 2025 onwards	Network isolation forced adversary exit; extensive forensic evidence remained for investigation	<p><b>Forced Exit:</b> [p.5, p.22]</p> <ul style="list-style-type: none"> <li>• 01:17 - Network disconnection terminated all connections [p.5]</li> <li>• VPN sessions terminated</li> <li>• C2 channels severed</li> <li>• Ransomware deployment prevented [p.22]</li> </ul> <p><b>Evidence Left:</b></p> <ul style="list-style-type: none"> <li>• Forensic artifacts on 91 systems [p.18]</li> <li>• 63 SOC alerts in SIEM [p.12]</li> <li>• VPN authentication logs [p.11, p.23, Table 11]</li> <li>• Windows Event logs [p.13-15]</li> <li>• Installed remote tools: AnyDesk, TeamViewer [p.16-17, p.23]</li> <li>• Created accounts: account_hp4, account_hp5 [p.17, p.23]</li> <li>• PowerShell history with Cyrillic comments [p.16-17, p.20]</li> <li>• Firewall logs showing 2.1 GB transfer [p.19]</li> <li>• IOCs [p.23, Table 10]</li> </ul> <p><b>Adversary Attribution:</b> [p.20-21]</p> <ul style="list-style-type: none"> <li>• Cyrillic characters (Russian language) [p.20]</li> <li>• Off-the-shelf tools = commodity ransomware</li> </ul>	<p>N/A - Post-Incident Activities:</p> <p><b>Defender Response:</b></p> <ul style="list-style-type: none"> <li>• Incident Response</li> <li>• Forensic Analysis</li> <li>• Threat Hunting</li> <li>• Malware Analysis</li> <li>• Indicators of Compromise (IOC) Collection</li> <li>• Timeline Reconstruction</li> <li>• Attribution Analysis</li> </ul>	<ul style="list-style-type: none"> <li>• N/A (Exit forced by defender) [p.5]</li> </ul>	•



Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools
			actor [p.20-21] <ul style="list-style-type: none"><li>• Non-stealthy techniques</li></ul> = not APT [p.20]		

Key Findings Summary

Category	Details
Attack Duration	January 6, 14:08 - January 12, 01:17, 2025 = <b>5 days, 11 hours, 9 minutes</b> [p.11, p.5, p.22]
Initial Access Method	Leaked credentials + VPN without MFA [p.11-12, p.22]
Privilege Escalation	NTLMv1 coercion attack → DCSync → Pass-the-hash [p.13-15, p.22]
Highest Privilege Obtained	Enterprise Administrator (full domain control over DOMAIN_1 and DOMAIN_2) [p.12, p.15, p.22]
Systems Compromised	91 systems (14 hands-on-keyboard, 77 authentication only) out of 350 total [p.18, p.22]
Data Exfiltrated	~2.1 GB (primarily AD info: system names, usernames, password hashes); no large-scale exfiltration found [p.19-20, p.22]
Threat Actor Profile	Ransomware operator (commodity, non-APT) with Russian language indicators [p.20-21, p.22]
Criminal Objective	Ransomware deployment (presumed based on TTPs, not achieved) [p.20, p.22]
Detection Point	SURFsoc alerts, January 11 at 21:55 (63 alerts generated) [p.5, p.12]
Containment Action	Network isolation, January 12 at 01:17 [p.5, p.22]
Outcome	Attack interrupted before ransomware deployment; swift containment prevented catastrophic damage [p.22]

# Critical Vulnerabilities Exploited

Vulnerability	Stage	Impact	Mitigation
No MFA on VPN [p.11]	Stage 2	Enabled initial access with leaked credentials [p.11-12]	Implement MFA on all remote access solutions [p.11]
NTLMv1 acceptance on domain controllers [p.14, p.24]	Stage 4-5	Enabled privilege escalation via coercion attack and hash cracking [p.13-15]	Disable NTLMv1, set lmcompatibilitylevel=5 on all DCs [p.14, p.24, Table 12]
Insufficient DC replication logging [p.15, p.24]	Stage 5	Delayed DCSync detection; only failure events logged [p.15, p.24, Table 13]	Enable success logging for Directory Service Replication events [p.15, p.24]
Leaked credentials in public breaches [p.11-12]	Stage 1-2	Provided valid access to VPN [p.11-12]	Credential monitoring, proactive password resets, breach notification monitoring [p.12]
Weak audit policies [p.15, p.24]	Stages 3-6	Limited visibility into adversary activities [p.13-18]	Comprehensive logging and SIEM integration [p.9, Table 2]
No EDR on domain controllers [p.9]	Stage 6	Delayed detection of remote administration tool installation [p.16-17]	Deploy EDR on all critical infrastructure [p.9, Table 2]

# MITRE ATT&CK Tactics Summary by Stage

Stage	Primary MITRE ATT&CK Tactics
1. Preparation	TA0043: Reconnaissance, TA0042: Resource Development
2. Entry	TA0001: Initial Access
3. Pre-condition	TA0007: Discovery, TA0008: Lateral Movement
4. Instrumental Pre-condition	TA0007: Discovery, TA0004: Privilege Escalation (prep), TA0006: Credential Access (prep)
5. Instrumental Initiation	TA0006: Credential Access, TA0004: Privilege Escalation, TA0008: Lateral Movement
6. Instrumental Actualization	TA0007: Discovery, TA0003: Persistence, TA0005: Defense Evasion, TA0040: Impact (prep)

Stage	Primary MITRE ATT&CK Tactics
7. Doing	TA0009: Collection, TA0010: Exfiltration, TA0011: Command and Control, TA0040: Impact (intended)
8. Exit	N/A - Post-Incident (Defender Response)

**Reference:** Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies*, 3, 151-196.